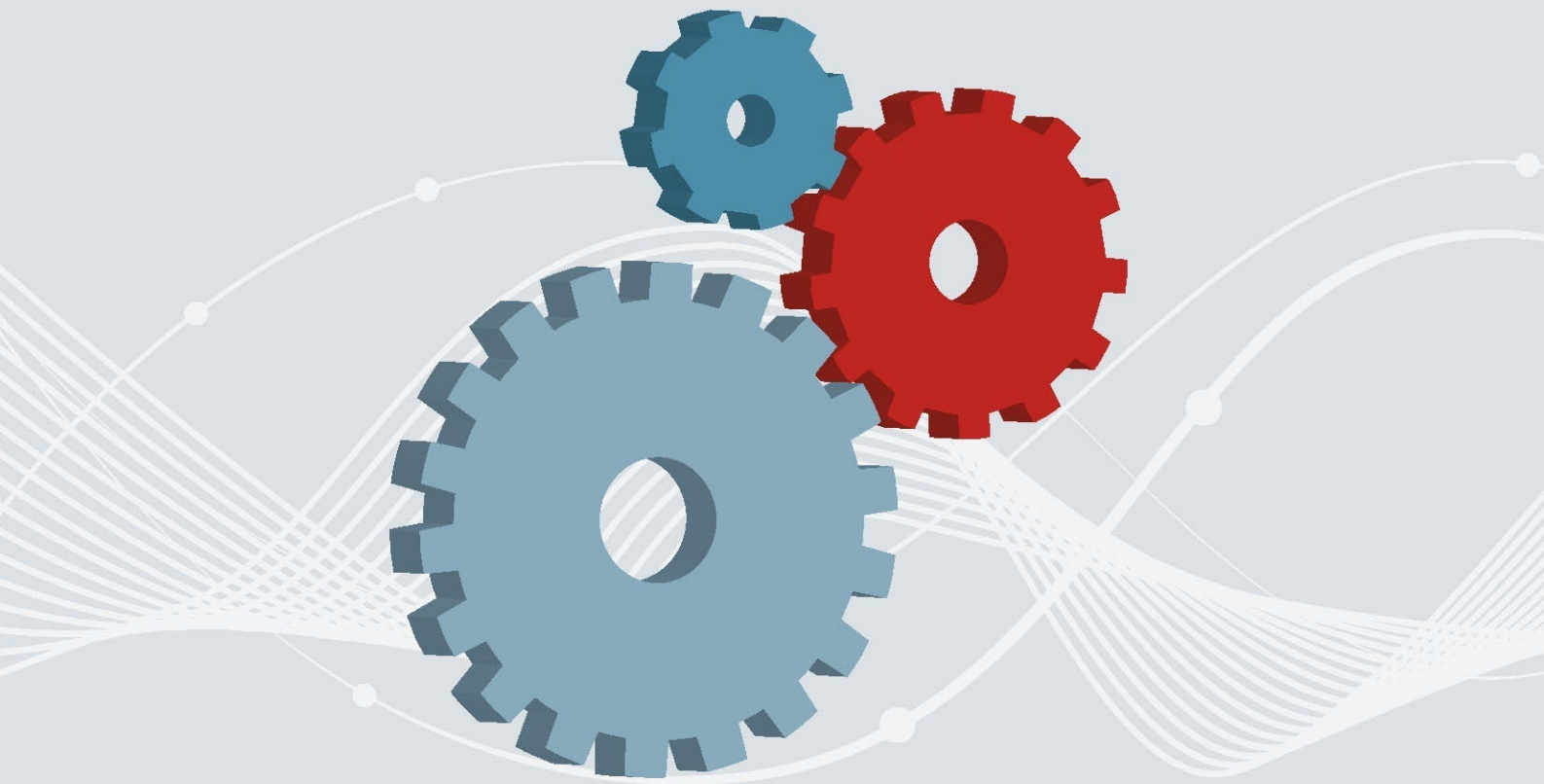
Bundesamt
für Sicherheit in der
Informationstechnik



# IT-Grundschutz-Kataloge

15. Ergänzungslieferung - 2016

# Vorwort

Immer mehr Behörden und Unternehmen setzen auf digitale Geschäftsprozesse, Technologien wie Cloud Computing oder den Einsatz mobiler Geräte zur Steigerung von Effizienz und Produktivität. Gleichzeitig führt dies zu einer steigenden Komplexität der IT-Infrastruktur. Die Digitalisierung dringt auch in solche Bereiche vor, die bisher keinen Zugang zum Internet hatten, beispielsweise bei Steuerungssystemen des Anlagen- und Maschinenparks. Mit steigender Komplexität der Systeme müssen auch vorhandene Sicherheitsmechanismen angepasst und neue Bereiche eingebunden werden.

Mit der 15. Ergänzungslieferung werden die IT-Grundschutz-Kataloge um Bausteine zur fortschreitenden Digitalisierung und Vernetzung erweitert, unter anderem zum Thema Serviceorientierte Architektur (SOA). Der SOA-Baustein beschreibt die spezifischen Gefährdungen von verteilten Services und erläutert Maßnahmen für die sichere Anwendung und Implementierung einer SOA. Der Schutz einzelner Informationsobjekte steht dabei besonders im Fokus. In einem weiteren Baustein sind Herausforderungen und Risiken beim Einsatz eingebetteter Systeme beschrieben sowie praktikable Maßnahmen aufgezeigt. Aufgrund der voranschreitenden Dezentralisierung der IT in Behörden und Unternehmen werden das Identitäts- und Berechtigungsmanagement zunehmend zu einer zentralen Herausforderung für die Verantwortlichen. Dieser elemantaren Bedeutung für die Informationssicherheit einer Instituion wird im Baustein Identitäts- und Berechtigungsmanagement nachgegangen. Die profunde Absicherung des Netz- und Systemmanagegements – theoretisch eine sehr grundlegende Notwendigkeit im Rahmen eines Sicherheitskonzepts – wird im gleichnamigen Baustein beschrieben.

Die vorliegende 15. Ergänzungslieferung der IT-Grundschutz-Kataloge ist die letzte, die in dieser Form veröffentlicht wird. In Verbindung mit der Modernisierung des IT-Grundschutz, der in Zusammenarbeit mit zahlreichen externen Experten und Anwendern rundum erneuert wird, erfahren auch die Kataloge eine Neuausrichtung. Der IT-Grundschutz soll an Institutionsgrößen und Rahmenbedingungen skalierbar sein und es ermöglichen, die schnelllebigen und kurzen Produkt- und Entwicklungszyklen der eingesetzten Systeme an die technischen, organisatorischen und rechtlichen Herausforderungen in der eigenen Institution anzupassen. In diesem Rahmen werden die IT-Grundschutz-Kataloge neu strukturiert.

Der IT-Grundschutz ist in einem sehr dynamischen Themengebiet verortet. Neben der weiter voranschreitenden Modernisierung der Methode bringen auch neue politische Rahmenbedingungen wie das IT-Sicherheitsgesetz weitere Anforderungen an die Betreiber und Anwender von IT-Systemen mit sich. Trotz aller Veränderungen gibt es auch Kontinuität und Verlässlichkeit, so bleibt die Anwendung der IT-Grundschutz-Methodik weiterhin ISO 27001 kompatibel.

Bonn, im Januar 2016

Dr. Hartmut Isselhorst, Abteilungspräsident Cyber-Sicherheit

# Dankesworte

Aufgrund der jährlichen Bedarfsabfrage bei registrierten Anwendern werden die IT-Grundschutz-Kataloge bedarfsorientiert weiterentwickelt. Für die Mitarbeit bei der Weiterentwicklung des IT-Grundschutzes und die engagierte Unterstützung bei der Fortschreibung der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge wird an dieser Stelle folgenden Beteiligten gedankt:

| **Inhalte** | **Personen** |
|---|---|
| Gesamtkoordination und Chefredaktion | Frau Isabel Münch, BSI |
| Redaktionelle Bearbeitung | Herr Christian Merz, BSI<br>Herr Ehad Qorri, BSI<br>Herr Christoph Wiemers, BSI |
| Baustein B 1.18 Identitäts- und Berechtigungsmanagement | Herr Michael Otter, BSI<br>Frau Isabel Münch, BSI<br>Herr Holger Görz, iSM Secu-Sys AG<br>Herr Prof. Dr. Dr. Gerd Rossa, iSM Secu-Sys AG |
| Baustein B 3.213 Client unter Windows 8 | Herr Frank Rustemeyer, HiSolutions<br>Herr Jörg Schäfer, HiSolutions<br>Herr Maximilian Winkler, BSI<br>Herr Holger Schildt, BSI |
| Baustein B 3.407 Eingebettetes System | Herr Eckhard Großmann, Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)<br>Herr Konrad Rosmus, IABG<br>Herr Christian Merz, BSI |
| Überarbeitung Baustein B 4.1 Lokale Netze | Herr Alex Essoh, BSI<br>Herr Christoph Wiemers, BSI<br>Herr Dr. Clemens Doubrava, BSI |
| Überarbeitung Baustein B 4.2 Netz- und Systemmanagement | Herr Christoph Wiemers, BSI<br>Herr Alex Essoh, BSI<br>Herr Dr. Clemens Doubrava, BSI |
| Baustein B 5.26 Serviceorientierte Architektur | Herr Eckhard Großmann, Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)<br>Herr Hartmut Seifert, IABG<br>Herr Christian Merz, BSI |
| Baustein B 5.27 Software-Entwicklung | Herr Christian Merz, BSI<br>Frau Isabel Münch, BSI<br>Herr Holger Schildt, BSI |
| Qualitätssicherung | Herr Sebastian Frank, Secumedia<br>Herr Christian Merz, BSI |

Neben der Aktualisierung und Überarbeitung von Bausteinen wurden zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der Informationssicherheit angepasst. Auch hier sei den Mitwirkenden gedankt.

Darüber hinaus sei allen gedankt, die sich durch konstruktive Kritik und praktische Verbesserungsvorschläge an der Verbesserung des IT-Grundschutzes und der IT-Grundschutz-Kataloge beteiligt haben.

Bei der Fortschreibung und Weiterentwicklung vorhergehender Versionen der IT-Grundschutz-Kataloge haben die nachfolgend aufgezählten Personen und Institutionen mitgewirkt. Auch ihnen sei hiermit Dank ausgesprochen:

| **Firmen und Personen** | |
|---|---|
| - Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder<br>- Atos Origin GmbH<br>Herr Herbert Blaauw, Herr Matthias Mönter<br>Herr Götz, Herr Jaster, Herr Pohl<br>Andreas Sesterhenn, Jörg Stockmann<br>Herr Erwan Smits, Herr Dominic Mylo<br>- AXA Versicherung AG<br>- Branchenverband OSE - Organisation pro Software Escrow<br>Herr Dr. Michael Eggers<br>- Computacenter AG & Co. OHG<br>Herr Marko Klaus<br>Frau Antje Straube<br>Herr Michael Broermann<br>- consecco<br>Herr Christian Aust<br>- ConSecur GmbH<br>Herr Nedon, Herr Eckardt<br>- Dataport<br>Herr Martin Meints<br>- Europäische Kommission<br>GD Informationsgesellschaft<br>Herr Achim Klabunde<br>- EUROSEC GmbH<br>Herr Fünfrocken, Frau Martina Seiler<br>Herr Vetter, Herr Dr. Zieschang<br>- KPMG AG<br>Herr Alexander Geschonneck<br>- Guide Share Europe<br>Arbeitskreis "Datenschutz und Datensicherheit"<br>- HiSolutions AG<br>Herr Timo Kob, Herr Ronny Frankenstein,<br>Herr Christoph Puppe, Herr Enno Ewers, Herr Frank Rustemeyer, Herr David Fuhr, Herr Dominik Oepen, Herr Alexander Papitsch, Herr Christoph Puppe<br>- INFODAS GmbH<br>Herr Dr. Gerhard Weck, Frau Sabine Kammerhofer | - Ingenieurbüro Mink<br>- Microsoft Deutschland GmbH<br>- Networkers AG<br>Herr Ludger Hötting, Herr Oliver Redeker, Herr Marcel Zamzow<br>- Novell GmbH<br>- Oracle Deutschland GmbH<br>- Orange Business Services<br>Herr Josef Ledermann<br>- Open Web Application Security Project - German Chapter<br>Herr Tobias Glemser (Tele-Consulting security \| networking \| training GmbH),<br>Herr Ralf Reinhardt (sic[!]sec GmbH)<br>- PERSICON Information Risk Management GmbH<br>Herr Knud Brandis, Herr Willy Wauschkuhn, Herr Prof. Dr. Rainer Rumpel, Herr Knut Haufe<br>- Röhm GmbH Chemische Fabrik<br>Datenschutzbeauftragter Herr Güldemeister<br>- SerNet GmbH<br>Herr Christoph Zauner<br>- T-Systems International GmbH<br>Herr Stephan Hüttinger, Herr Torsten Kullich, Herr Klaus Müller, Herr Stefan Morkovsky, Herr Axel Nennker, Herr Norbert Vogel<br>- TÜViT GmbH<br>Herr Adrian Altrhein, Herr Peter Herrmann, Herr Stephan Klein, Herr Mirco Przybylinski, Herr Jan Seebens, Frau Dr. Anja Wiedemann<br>- Verband der Chemischen Industrie e. V.<br>- Secumedia<br>Herr Sebastian Frank, Herr Elmar Török<br>- SIZ<br>Herr Gerhard Müller, Herr Detlef Zimmer, Herr Ulrich Schmidt<br>- Symantec Deutschland GmbH<br>- VZM GmbH<br>Herr Bruno Hecht, Herr Werner Metterhausen, Herr Rainer von zur Mühlen |

Folgende Autoren haben durch die Erstellung von Bausteinen ihr Fachwissen in die IT-Grundschutz-Kataloge einfließen lassen. Ihnen gebührt besonderer Dank, da ihr Engagement die Entstehung und Weiterentwicklung der IT-Grundschutz-Kataloge erst ermöglicht hat.

Bundesministerium des Innern: Herr Jörg-Udo Aden, Herr André Reisen, Herr Manfred Kramer, Herr Dr. Christian Mrugalla, Frau Dr. Lydia Tsintsifa

Bundesministerium für Bildung und Wissenschaft: Herr Frank Stefan Stumm

Bundesamt für Sicherheit in der Informationstechnik: Herr Heinz Altengarten, Herr Rainer Belz, Herr Thomas Biere, Frau Steffi Botzelmann, Frau Elke Cäsar, Herr Thomas Caspers, Herr Markus de Brün, Herr Björn Dehms, Herr Thorsten Dietrich, Herr Uwe Dornseifer, Herr Dr. Clemens Doubrava, Herr Günther Ennen, Herr Olaf Erber, Herr Alex Didier Essoh, Herr Frank W. Felzmann, Herr Michael Förtsch, Herr Dr. Kai Fuhrberg, Herr Heinz Gerwing, Herr Dr. Patrick Grete, Herr Karl Greuel, Herr Thomas Häberlen, Herr Dr. Dirk Häger, Herr Dr. Timo Hauschild, Herr Florian Hillebrand, Herr Dr. Hartmut Isselhorst, Frau Angelika Jaschob, Herr Harald Kelter, Herr Kurt Klinner, Herr Dr. Robert Krawczyk, Herr Michael Mehrhoff, Herr Christian Merz, Frau Isabel Münch, Frau Sabine Mull, Herr Dr. Frank Niedermeyer, Herr Dr. Harald Niggemann, Herr Michael Otter, Herr Jonas Paulzen, Herr Robert Rasten, Frau Martina Rohde, Frau Gabriele Scheer-Gumm, Herr Fabian Schelo, Herr Holger Schildt, Herr Dr. Arthur Schmidt, Herr Dr. Willibald Schneider, Herr Heiner Schorn, Herr Dr. Ernst Schulte-Geers, Herr Carsten Schulz, Herr Bernd Schweda, Frau Petra Simons-Felwor, Herr Martin Telzer, Herr Berthold Ternes, Frau Katja Vogel, Frau Anne-Kathrin Walter, Herr Frank Weber, Herr Helmut Weisskopf, Frau Jessika Welticke, Herr Maximilian Winkler

sowie: Herr Markus Balkenhol, Herr Marcel Birkner, Herr Werner Blechschmidt, Frau Anastasia Eifer, Herr Mounir Guiche, Herr Tobias Hödtke, Herr Björn Jacke, Herr Thomas Ledermüller, Herr Tim Lemmen, Frau Dr. Marie-Luise Moschgath, Herr Daniel Nowack, Herr Joachim Pöttinger, Herr Philipp Rothmann, Herr Michael Ruck, Frau Cornelia Schildt, Herr Michael Schwank, Herr Ranbir Singh Anand, Herr Herr Markus Steinkamp, Herr Felix Stolte, Herr Hristoforos Thomaidis, Herr Dr. Stefan Wolf

# Inhaltsverzeichnis - IT-Grundschutz-Kataloge

G 0.17. Verlust von Geräten, Datenträgern oder Dokumenten
G 0.18. Fehlplanung oder fehlende Anpassung
G 0.19. Offenlegung schützenswerter Informationen
G 0.20. Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21. Manipulation von Hard- oder Software
G 0.22. Manipulation von Informationen
G 0.23. Unbefugtes Eindringen in IT-Systeme
G 0.24. Zerstörung von Geräten oder Datenträgern
G 0.25. Ausfall von Geräten oder Systemen
G 0.26. Fehlfunktion von Geräten oder Systemen
G 0.27. Ressourcenmangel
G 0.28. Software-Schwachstellen oder -Fehler
G 0.29. Verstoß gegen Gesetze oder Regelungen
G 0.30. Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31. Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.32. Missbrauch von Berechtigungen
G 0.33. Personalausfall
G 0.34. Anschlag
G 0.35. Nötigung, Erpressung oder Korruption
G 0.36. Identitätsdiebstahl
G 0.37. Abstreiten von Handlungen
G 0.38. Missbrauch personenbezogener Daten
G 0.39. Schadprogramme
G 0.40. Verhinderung von Diensten (Denial of Service)
G 0.41. Sabotage
G 0.42. Social Engineering
G 0.43. Einspielen von Nachrichten
G 0.44. Unbefugtes Eindringen in Räumlichkeiten
G 0.45. Datenverlust
G 0.46. Integritätsverlust schützenswerter Informationen

G 1 Höhere Gewalt
G 1.1. Personalausfall
G 1.2. Ausfall von IT-Systemen
G 1.3. Blitz
G 1.4. Feuer
G 1.5. Wasser
G 1.6. Kabelbrand
G 1.7. Unzulässige Temperatur und Luftfeuchte
G 1.8. Staub, Verschmutzung
G 1.9. Datenverlust durch starke Magnetfelder
G 1.10. Ausfall eines Weitverkehrsnetzes
G 1.11. Technische Katastrophen im Umfeld
G 1.12. Beeinträchtigung durch Großveranstaltungen
G 1.13. Sturm
G 1.14. Datenverlust durch starkes Licht
G 1.15. Beeinträchtigung durch wechselnde Einsatzumgebung

G 1.16. Ausfall von Patchfeldern durch Brand
G 1.17. Ausfall oder Störung eines Funknetzes
G 1.18. Ausfall eines Gebäudes
G 1.19. Ausfall eines Dienstleisters oder Zulieferers

G 2 Organisatorische Mängel
G 2.1. Fehlende oder unzureichende Regelungen
G 2.2. Unzureichende Kenntnis über Regelungen
G 2.3. Fehlende, ungeeignete, inkompatible Betriebsmittel
G 2.4. Unzureichende Kontrolle der Sicherheitsmaßnahmen
G 2.5. Fehlende oder unzureichende Wartung
G 2.6. Unbefugter Zutritt zu schutzbedürftigen Räumen
G 2.7. Unerlaubte Ausübung von Rechten
G 2.8. Unkontrollierter Einsatz von Betriebsmitteln
G 2.9. Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
G 2.10. Nicht fristgerecht verfügbare Datenträger
G 2.11. Unzureichende Trassendimensionierung
G 2.12. Unzureichende Dokumentation der Verkabelung
G 2.13. Unzureichend geschützte Verteiler
G 2.14. Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
G 2.15. Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
G 2.16. Ungeordneter Benutzerwechsel bei tragbaren PCs
G 2.17. Mangelhafte Kennzeichnung der Datenträger
G 2.18. Ungeregelte Weitergabe von Datenträgern
G 2.19. Unzureichendes Schlüsselmanagement bei Verschlüsselung
G 2.20. Unzureichende oder falsche Versorgung mit Verbrauchsgütern
G 2.21. Mangelhafte Organisation des Wechsels zwischen den Benutzern
G 2.22. Fehlende oder unzureichende Auswertung von Protokolldaten
G 2.23. Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz
G 2.24. Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
G 2.25. Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
G 2.26. Fehlendes oder unzureichendes Test- und Freigabeverfahren
G 2.27. Fehlende oder unzureichende Dokumentation
G 2.28. Verstöße gegen das Urheberrecht
G 2.29. Softwaretest mit Produktionsdaten
G 2.30. Unzureichende Domänenplanung
G 2.31. Unzureichender Schutz des Windows NT Systems
G 2.32. Unzureichende Leitungskapazitäten
G 2.33. Nicht gesicherter Aufstellungsort von Novell Netware Servern
G 2.34. Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
G 2.35. Fehlende Protokollierung unter Windows 95
G 2.36. Ungeeignete Einschränkung der Benutzerumgebung
G 2.37. Unkontrollierter Aufbau von Kommunikationsverbindungen

G 2.38. Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen
G 2.39. Mangelhafte Konzeption eines DBMS
G 2.40. Mangelhafte Konzeption des Datenbankzugriffs
G 2.41. Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
G 2.42. Komplexität der NDS
G 2.43. Migration von Novell Netware 3.x nach Novell Netware Version 4
G 2.44. Inkompatible aktive Netzkomponenten
G 2.45. Konzeptionelle Schwächen des Netzes
G 2.46. Überschreiten der zulässigen Kabellänge
G 2.47. Ungesicherter Akten- und Datenträgertransport
G 2.48. Ungeeignete Entsorgung der Datenträger und Dokumente
G 2.49. Fehlende oder unzureichende Schulung der Telearbeiter
G 2.50. Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter
G 2.51. Mangelhafte Einbindung des Telearbeiters in den Informationsfluss
G 2.52. Erhöhte Reaktionszeiten bei IT-Systemausfall
G 2.53. Unzureichende Vertretungsregelungen für Telearbeit
G 2.54. Vertraulichkeitsverlust durch Restinformationen
G 2.55. Ungeordnete Groupware-Nutzung
G 2.56. Mangelhafte Beschreibung von Dateien
G 2.57. Nicht ausreichende Speichermedien für den Notfall
G 2.58. Novell Netware und die Datumsumstellung im Jahr 2000
G 2.59. Betreiben von nicht angemeldeten Komponenten
G 2.60. Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement
G 2.61. Unberechtigte Sammlung personenbezogener Daten
G 2.62. Ungeeigneter Umgang mit Sicherheitsvorfällen
G 2.63. Ungeordnete Faxnutzung
G 2.64. Fehlende Regelungen für das RAS-System
G 2.65. Komplexität der SAMBA-Konfiguration
G 2.66. Unzureichendes Sicherheitsmanagement
G 2.67. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten
G 2.68. Fehlende oder unzureichende Planung des Active Directory
G 2.69. Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory
G 2.70. Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory
G 2.71. Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory
G 2.72. Unzureichende Migration von Archivsystemen
G 2.73. Fehlende Revisionsmöglichkeit von Archivsystemen
G 2.74. Unzureichende Ordnungskriterien für Archive
G 2.75. Mangelnde Kapazität von Archivdatenträgern
G 2.76. Unzureichende Dokumentation von Archivzugriffen
G 2.77. Unzulängliche Übertragung von Papierdaten in elektronische Archive

G 2.78. Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
G 2.79. Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
G 2.80. Unzureichende Durchführung von Revisionen bei der Archivierung
G 2.81. Unzureichende Vernichtung von Datenträgern bei der Archivierung
G 2.82. Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen
G 2.83. Fehlerhafte Outsourcing-Strategie
G 2.84. Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
G 2.85. Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens
G 2.86. Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister
G 2.87. Verwendung unsicherer Protokolle in öffentlichen Netzen
G 2.88. Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
G 2.89. Mangelhafte Informationssicherheit in der Outsourcing-Einführungsphase
G 2.90. Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
G 2.91. Fehlerhafte Planung der Migration von Exchange
G 2.92. Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange
G 2.93. Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung
G 2.94. Unzureichende Planung des IIS-Einsatzes
G 2.95. Fehlendes Konzept zur Anbindung anderer Systeme an Exchange
G 2.96. Veraltete oder falsche Informationen in einem Webangebot
G 2.97. Unzureichende Notfallplanung bei einem Apache-Webserver
G 2.98. Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches
G 2.99. Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung
G 2.100. Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen
G 2.101. Unzureichende Notfallvorsorge bei einem Sicherheitsgateway
G 2.102. Unzureichende Sensibilisierung für Informationssicherheit
G 2.103. Unzureichende Schulung der Mitarbeiter
G 2.104. Inkompatibilität zwischen fremder und eigener IT
G 2.105. Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
G 2.106. Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen
G 2.107. Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement
G 2.108. Fehlende oder unzureichende Planung des SAP Einsatzes
G 2.109. Fehlende oder unzureichende Planung der Speicherlösung
G 2.110. Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken

G 2.111. Kompromittierung von Anmeldedaten bei Dienstleisterwechsel
G 2.112. Unzureichende Planung von VoIP
G 2.113. Unzureichende Planung der Netzkapazität beim Einsatz von VoIP
G 2.114. Uneinheitliche Windows-Server-Sicherheitseinstellungen bei SMB, RPC und LDAP
G 2.115. Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen ab Windows Server 2003
G 2.116. Datenverlust beim Kopieren oder Verschieben von Daten ab Windows Server 2003
G 2.117. Fehlende oder unzureichende Planung des WLAN-Einsatzes
G 2.118. Unzureichende Regelungen zum WLAN-Einsatz
G 2.119. Ungeeignete Auswahl von WLAN-Authentikationsverfahren
G 2.120. Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen
G 2.121. Unzureichende Kontrolle von WLANs
G 2.122. Ungeeigneter Einsatz von Multifunktionsgeräten
G 2.123. Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten
G 2.124. Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst
G 2.125. Fehlerhafte oder unzureichende Planung des Zugriffs auf den Verzeichnisdienst
G 2.126. Unzureichende Protokollierung von Änderungen am Active Directory
G 2.127. Unzureichende Planung von Datensicherungsmethoden für Domänen-Controller
G 2.128. Fehlende oder unzureichende Planung des VPN-Einsatzes
G 2.129. Fehlende oder unzureichende Regelungen zum VPN-Einsatz
G 2.130. Ungeeignete Auswahl von VPN-Verschlüsselungsverfahren
G 2.131. Unzureichende Kontrolle von VPNs
G 2.132. Mangelnde Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement
G 2.133. Mangelhaft festgelegte Verantwortlichkeiten beim Patch- und Änderungsmanagement
G 2.134. Unzureichende Ressourcen beim Patch- und Änderungsmanagement
G 2.135. Mangelhafte Kommunikation beim Patch- und Änderungsmanagement
G 2.136. Fehlende Übersicht über den Informationsverbund
G 2.137. Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen
G 2.138. Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement
G 2.139. Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement
G 2.140. Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement
G 2.141. Nicht erkannte Sicherheitsvorfälle

G 2.142. Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen
G 2.143. Informationsverlust beim Kopieren oder Verschieben von Daten auf Samba-Freigaben
G 2.144. Unzureichende Notfall-Planung bei einem Samba-Server
G 2.145. Unzureichende Sicherung von Trivial Database Dateien unter Samba
G 2.146. Verlust der Arbeitsfähigkeit von Vista-Clients durch fehlende Reaktivierung vor SP1
G 2.147. Fehlende Zentralisierung durch Peer-to-Peer
G 2.148. Fehlerhafte Planung der Virtualisierung
G 2.149. Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme
G 2.150. Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen
G 2.151. Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen
G 2.152. Fehlende oder unzureichende Planung des DNS-Einsatzes
G 2.153. Ungeeignete Sicherung des Übertragungsweges in einer Terminalserver Umgebung
G 2.154. Ungeeignete Anwendungen für den Einsatz auf Terminalservern
G 2.155. Fehlende oder unzureichende Planung von OpenLDAP
G 2.156. Kompatibilitätsprobleme beim Anheben der Active Directory-Funktionsebene
G 2.157. Mangelhafte Auswahl oder Konzeption von Webanwendungen
G 2.158. Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services
G 2.159. Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services
G 2.160. Fehlende oder unzureichende Protokollierung
G 2.161. Vertraulichkeits- und Integritätsverlust von Protokolldaten
G 2.162. Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten
G 2.163. Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten
G 2.164. Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten
G 2.165. Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten
G 2.166. Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten
G 2.167. Fehlende oder nicht ausreichende Vorabkontrolle
G 2.168. Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten
G 2.169. Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten
G 2.170. Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen

G 2.171. Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten
G 2.172. Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland
G 2.173. Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten
G 2.174. Fehlende oder unzureichende Datenschutzkontrolle
G 2.175. Unzureichende Isolation und Trennung von Cloud-Ressourcen
G 2.176. Mangelnde Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender
G 2.177. Fehlplanung von Cloud-Diensteprofilen
G 2.178. Unzureichendes Notfallmanagement beim Cloud-Diensteanbieter
G 2.179. Fehlende Herstellerunterstützung bei der Bereitstellung von Cloud-Diensten
G 2.180. Fehlerhafte Provisionierung und De-Provisionierung von Cloud-Diensten
G 2.181. Mangelhafte Planung und Konzeption des Einsatzes von Web-Services
G 2.182. Fehlendes oder unzureichendes Betreiberkonzept für Speicherlösungen
G 2.183. Fehlendes oder unzureichendes Zonenkonzept
G 2.184. Fehlendes oder unzureichendes Rechte- und Rollenkonzept in Cloud-Infrastrukturen
G 2.185. Fehlende oder unzureichende Softwarewartung (Maintenance) und fehlendes oder unzureichendes Patchlevel-Management
G 2.186. Fehlende oder unzureichende Regelungen / keine klare Abgrenzung von Verantwortlichkeiten bei Speicherlösungen
G 2.187. Fehlendes oder unzureichendes mandantenfähiges Administrationskonzept für Speicherlösungen
G 2.188. Unzureichende Vorgaben zum Lizenzmanagement bei Cloud-Nutzung
G 2.189. Fehlende oder unzureichende Strategie für die Cloud-Nutzung
G 2.190. Unzureichendes Administrationsmodell für die Cloud-Nutzung
G 2.191. Unzureichendes Rollen- und Berechtigungskonzept
G 2.192. Unzureichende Verfügbarkeit der erforderlichen personellen Ressourcen mit ausreichender Qualifikation
G 2.193. Fehlende Anpassung der Institution an die Nutzung von Cloud Services
G 2.194. Mangelhaftes Anforderungsmanagement bei Cloud-Nutzung
G 2.195. Mangelnde Überwachung der Service-Erbringung
G 2.196. Fehlende Kosten-Nutzen-Betrachtung der Cloud-Nutzung über den gesamten Lebenszyklus
G 2.197. Unzureichende Einbindung von Cloud Services in die eigene IT
G 2.198. Mangelnde Planung der Migration zu Cloud Services
G 2.199. Unzureichende Auswahl des Cloud-Diensteanbieters
G 2.200. Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs

G 2.201. Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern
G 2.202. Lock-in-Effekt
G 2.203. Integrierte Cloud-Funktionalität
G 2.204. TPM-Nutzung
G 2.205. Fehlendes Notfallvorsorgekonzept für serviceorientierte Architekturen
G 2.206. Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen
G 2.207. Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen
G 2.208. Unzureichende physische Absicherung der elektronischen Komponenten bei eingebetteten Systemen
G 2.209. Auswahl einer ungeeigneten Entwicklungsumgebung für Software
G 2.210. Unzureichend gesicherter Einsatz von Entwicklungsumgebungen
G 2.211. Auswahl eines ungeeigneten Vorgehensmodells zur Software-Entwicklung
G 2.212. Unzureichende Berücksichtigung von Konfigurationsoptionen bei der Software-Entwicklung
G 2.213. Fehlende oder unzureichende Qualitätssicherung des Softwareentwicklungsprozesses
G 2.214. Fehlende oder unzureichende Konzeption des Identitäts- und Berechtigungsmanagements

G 3 Menschliche Fehlhandlungen
G 3.1. Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten
G 3.2. Fahrlässige Zerstörung von Gerät oder Daten
G 3.3. Nichtbeachtung von Sicherheitsmaßnahmen
G 3.4. Unzulässige Kabelverbindungen
G 3.5. Unbeabsichtigte Leitungsbeschädigung
G 3.6. Gefährdung durch Reinigungs- oder Fremdpersonal
G 3.7. Ausfall der TK-Anlage durch Fehlbedienung
G 3.8. Fehlerhafte Nutzung von IT-Systemen
G 3.9. Fehlerhafte Administration von IT-Systemen
G 3.10. Falsches Exportieren von Dateisystemen unter Unix
G 3.11. Fehlerhafte Konfiguration von sendmail
G 3.12. Verlust der Datenträger beim Versand
G 3.13. Weitergabe falscher oder interner Informationen
G 3.14. Fehleinschätzung der Rechtsverbindlichkeit eines Fax
G 3.15. Fehlbedienung eines Anrufbeantworters
G 3.16. Fehlerhafte Administration von Zugangs- und Zugriffsrechten
G 3.17. Kein ordnungsgemäßer PC-Benutzerwechsel
G 3.18. Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
G 3.19. Speichern von Passwörtern unter WfW und Windows 95
G 3.20. Ungewollte Freigabe des Leserechtes bei Schedule+
G 3.21. Fehlbedienung von Codeschlössern
G 3.22. Fehlerhafte Änderung der Registrierung
G 3.23. Fehlerhafte Administration eines DBMS

G 3.24. Unbeabsichtigte Datenmanipulation
G 3.25. Fahrlässiges Löschen von Objekten
G 3.26. Ungewollte Freigabe des Dateisystems
G 3.27. Fehlerhafte Zeitsynchronisation
G 3.28. Ungeeignete Konfiguration der aktiven Netzkomponenten
G 3.29. Fehlende oder ungeeignete Segmentierung
G 3.30. Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners
G 3.31. Unstrukturierte Datenhaltung
G 3.32. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren
G 3.33. Fehlbedienung von Kryptomodulen
G 3.34. Ungeeignete Konfiguration des Managementsystems
G 3.35. Server im laufenden Betrieb ausschalten
G 3.36. Fehlinterpretation von Ereignissen
G 3.37. Unproduktive Suchzeiten
G 3.38. Konfigurations- und Bedienungsfehler
G 3.39. Fehlerhafte Administration des RAS-Systems
G 3.40. Ungeeignete Nutzung von Authentisierungsdiensten bei VPNs
G 3.41. Fehlverhalten bei der Nutzung von VPN-Diensten
G 3.42. Unsichere Konfiguration der VPN-Clients für den Fernzugriff
G 3.43. Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen
G 3.44. Sorglosigkeit im Umgang mit Informationen
G 3.45. Unzureichende Identifikationsprüfung von Kommunikationspartnern
G 3.46. Fehlerhafte Konfiguration eines Lotus Domino Servers
G 3.47. Fehlerhafte Konfiguration des Browser-Zugriffs auf Lotus Notes
G 3.48. Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen
G 3.49. Fehlerhafte Konfiguration des Active Directory
G 3.50. Fehlerhafte Konfiguration von Novell eDirectory
G 3.51. Falsche Vergabe von Zugriffsrechten im Novell eDirectory
G 3.52. Fehlerhafte Konfiguration des Intranet-Clientzugriffs auf Novell eDirectory
G 3.53. Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory
G 3.54. Verwendung ungeeigneter Datenträger bei der Archivierung
G 3.55. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen
G 3.56. Fehlerhafte Einbindung des IIS in die Systemumgebung
G 3.57. Fehlerhafte Konfiguration des Betriebssystems für den IIS
G 3.58. Fehlerhafte Konfiguration eines IIS
G 3.59. Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS
G 3.60. Fehlerhafte Konfiguration von Exchange
G 3.61. Fehlerhafte Konfiguration von Outlook
G 3.62. Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
G 3.63. Fehlerhafte Konfiguration eines Apache-Webservers
G 3.64. Fehlerhafte Konfiguration von Routern und Switches

G 3.65. Fehlerhafte Administration von Routern und Switches
G 3.66. Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS
G 3.67. Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems
G 3.68. Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
G 3.69. Fehlerhafte Konfiguration der Unix System Services unter z/OS
G 3.70. Unzureichender Dateischutz des z/OS-Systems
G 3.71. Fehlerhafte Systemzeit bei z/OS-Systemen
G 3.72. Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
G 3.73. Fehlbedienung der z/OS-Systemfunktionen
G 3.74. Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen
G 3.75. Mangelhafte Kontrolle der Batch-Jobs bei z/OS
G 3.76. Fehler bei der Synchronisation mobiler Endgeräte
G 3.77. Mangelhafte Akzeptanz von Informationssicherheit
G 3.78. Fliegende Verkabelung
G 3.79. Fehlerhafte Zuordnung von Ressourcen des SAN
G 3.80. Fehler bei der Synchronisation von Datenbanken
G 3.81. Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003
G 3.82. Fehlerhafte Konfiguration der VoIP-Middleware
G 3.83. Fehlerhafte Konfiguration von VoIP-Komponenten
G 3.84. Fehlerhafte Konfiguration der WLAN-Infrastruktur
G 3.85. Verletzung von Brandschottungen
G 3.86. Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten
G 3.87. Fehlerhafte Konfiguration von Verzeichnisdiensten
G 3.88. Falsche Vergabe von Zugriffsrechten
G 3.89. Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste
G 3.90. Fehlerhafte Administration von VPNs
G 3.91. Ausfall von VPN-Verbindungen durch Fehlbedienung
G 3.92. Fehleinschätzung der Relevanz von Patches und Änderungen
G 3.93. Falscher Umgang mit defekten Datenträgern
G 3.94. Fehlkonfiguration der Samba-Kommunikationsprotokolle
G 3.95. Fehlerhafte Konfiguration des Betriebssystems für einen Samba-Server
G 3.96. Fehlerhafte Konfiguration eines Samba-Servers
G 3.97. Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista
G 3.98. Verlust von BitLocker-verschlüsselten Daten
G 3.99. Fehlerhafte Netzanbindungen eines Virtualisierungsservers
G 3.100. Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme
G 3.101. Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen
G 3.102. Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen
G 3.103. Fehlerhafte Domain-Informationen
G 3.104. Fehlerhafte Konfiguration eines DNS-Servers
G 3.105. Ungenehmigte Nutzung von externen Dienstleistungen

G 4.20. Überlastung von Informationssystemen
G 4.21. Ausgleichsströme auf Schirmungen
G 4.22. Software-Schwachstellen oder -Fehler
G 4.23. Automatische Erkennung von Wechseldatenträgern
G 4.24. Dateinamenkonvertierung bei Datensicherungen unter Windows 95
G 4.25. Nicht getrennte Verbindungen
G 4.26. Ausfall einer Datenbank
G 4.27. Unterlaufen von Zugriffskontrollen über ODBC
G 4.28. Verlust von Daten einer Datenbank
G 4.29. Datenverlust einer Datenbank bei erschöpftem Speichermedium
G 4.30. Verlust der Datenbankintegrität/-konsistenz
G 4.31. Ausfall oder Störung von Netzkomponenten
G 4.32. Nichtzustellung einer Nachricht
G 4.33. Schlechte oder fehlende Authentikationsverfahren und -mechanismen
G 4.34. Ausfall eines Kryptomoduls
G 4.35. Unsichere kryptographische Algorithmen
G 4.36. Fehler in verschlüsselten Daten
G 4.37. Mangelnde Verlässlichkeit von Groupware
G 4.38. Ausfall von Komponenten eines Netz- und Systemmanagementsystems
G 4.39. Software-Konzeptionsfehler
G 4.40. Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients
G 4.41. Nicht-Verfügbarkeit des Mobilfunknetzes
G 4.42. Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs
G 4.43. Undokumentierte Funktionen
G 4.44. Ausfall von Novell eDirectory
G 4.45. Verzögerte Archivauskunft
G 4.46. Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung
G 4.47. Veralten von Kryptoverfahren
G 4.48. Ausfall der Systeme eines Outsourcing-Dienstleisters
G 4.49. Unsichere Default-Einstellungen auf Routern und Switches
G 4.50. Überlastung des z/OS-Betriebssystems
G 4.51. Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs
G 4.52. Datenverlust bei mobilem Einsatz
G 4.53. Unsichere Default-Einstellungen bei Speicherkomponenten
G 4.54. Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS
G 4.55. Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP
G 4.56. Ausfall der VoIP-Architektur
G 4.57. Störungen beim Einsatz von VoIP über VPNs
G 4.58. Schwachstellen beim Einsatz von VoIP-Endgeräten
G 4.59. Nicht-Erreichbarkeit bei VoIP durch NAT
G 4.60. Unkontrollierte Ausbreitung der Funkwellen
G 4.61. Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen
G 4.62. Verwendung unzureichender Steckdosenleisten

G 4.63. Verstaubte Lüfter
G 4.64. Komplexität von Druckern, Kopierern und Multifunktionsgeräten
G 4.65. Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten
G 4.66. Beeinträchtigung von Gesundheit und Umwelt durch Drucker, Kopierer und Multifunktionsgeräte
G 4.67. Ausfall von Verzeichnisdiensten
G 4.68. Störungen des Active Directory durch unnötige Dateireplizierung
G 4.69. Probleme bei der IPSec-Konfiguration
G 4.70. Unsichere Standard-Einstellungen auf VPN-Komponenten
G 4.71. Probleme bei der automatisierten Verteilung von Patches und Änderungen
G 4.72. Inkonsistenzen von Datenbanken im Trivial Database Format unter Samba
G 4.73. Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme von Windows-Versionen
G 4.74. Ausfall von IT-Komponenten in einer virtualisierten Umgebung
G 4.75. Störung der Netzinfrastruktur von Virtualisierungsumgebungen
G 4.76. Ausfall von Verwaltungsservern für Virtualisierungssysteme
G 4.77. Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen
G 4.78. Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse
G 4.79. Schwachstellen in der Bluetooth-Implementierung
G 4.80. Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen
G 4.81. Erweiterte Rechte durch Programmdialoge auf Terminalservern
G 4.82. Ausfall und Nichterreichbarkeit von Terminalservern
G 4.83. Fehlfunktionen selbstentwickelter Makros unter Outlook
G 4.84. Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services
G 4.85. Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services
G 4.86. Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen
G 4.87. Offenlegung vertraulicher Informationen bei Webanwendungen
G 4.88. EMV-untaugliche Stromversorgung
G 4.89. Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung
G 4.90. Ungewollte Preisgabe von Informationen durch Cloud Cartography
G 4.91. Unberechtigtes Wiedereinspielen von Snapshots
G 4.92. Inkompatibilität zwischen der Cloud-Administration und der Administration der Cloud-Elemente
G 4.93. Ausfall von Verwaltungsservern und Verwaltungssoftware
G 4.94. Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services
G 4.95. Ausfall von Komponenten einer Speicherlösung
G 4.96. Fehlfunktion von Komponenten einer Speicherlösung

G 4.97. Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister
G 4.98. Ausfall von Tools zur Administration von Cloud Services bei Cloud-Nutzung
G 4.99. Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen
G 4.100. Hardwareausfall und Hardwarefehler bei eingebetteten Systemen
G 4.101. Ausfall eines zentralen Identitäts- und Berechtigungsmanagement-Systems

G 5 Vorsätzliche Handlungen
G 5.1. Manipulation oder Zerstörung von Geräten oder Zubehör
G 5.2. Manipulation an Informationen oder Software
G 5.3. Unbefugtes Eindringen in ein Gebäude
G 5.4. Diebstahl
G 5.5. Vandalismus
G 5.6. Anschlag
G 5.7. Abhören von Leitungen
G 5.8. Manipulation von Leitungen
G 5.9. Unberechtigte IT-Nutzung
G 5.10. Missbrauch von Fernwartungszugängen
G 5.11. Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten
G 5.12. Abhören von Telefongesprächen und Datenübertragungen
G 5.13. Abhören von Räumen über TK-Endgeräte
G 5.14. Gebührenbetrug
G 5.15. Missbrauch von Leistungsmerkmalen von TK-Anlagen
G 5.16. Gefährdung bei Wartungs-/Administrierungsarbeiten
G 5.17. Gefährdung bei Wartungsarbeiten durch externes Personal
G 5.18. Systematisches Ausprobieren von Passwörtern
G 5.19. Missbrauch von Benutzerrechten
G 5.20. Missbrauch von Administratorrechten
G 5.21. Trojanische Pferde
G 5.22. Diebstahl bei mobiler Nutzung des IT-Systems
G 5.23. Schadprogramme
G 5.24. Wiedereinspielen von Nachrichten
G 5.25. Maskerade
G 5.26. Analyse des Nachrichtenflusses
G 5.27. Nichtanerkennung einer Nachricht
G 5.28. Verhinderung von Diensten
G 5.29. Unberechtigtes Kopieren der Datenträger
G 5.30. Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
G 5.31. Unbefugtes Lesen von Faxsendungen
G 5.32. Auswertung von Restinformationen in Faxgeräten und Faxservern
G 5.33. Vortäuschen eines falschen Absenders bei Faxsendungen
G 5.34. Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
G 5.35. Überlastung durch Faxsendungen
G 5.36. Absichtliche Überlastung des Anrufbeantworters
G 5.37. Ermitteln des Sicherungscodes

G 5.38. Missbrauch der Fernabfrage
G 5.39. Eindringen in Rechnersysteme über Kommunikationskarten
G 5.40. Abhören von Räumen mittels Rechner mit Mikrofon und Kamera
G 5.41. Missbräuchliche Nutzung eines Unix-Systems mit Hilfe von UUCP
G 5.42. Social Engineering
G 5.43. Makro-Viren
G 5.44. Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen
G 5.45. Ausprobieren von Passwörtern unter WfW und Windows 95
G 5.46. Maskerade unter WfW
G 5.47. Löschen des Post-Office unter WfW
G 5.48. IP-Spoofing
G 5.49. Missbrauch des Source-Routing
G 5.50. Missbrauch des ICMP-Protokolls
G 5.51. Missbrauch der Routing-Protokolle
G 5.52. Missbrauch von Administratorrechten bei Windows-Betriebssystemen
G 5.53. Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit
G 5.54. Vorsätzliches Herbeiführen eines Abnormal End
G 5.55. Login Bypass
G 5.56. Temporär frei zugängliche Accounts
G 5.57. Netzanalysetools
G 5.58. Hacking Novell Netware
G 5.59. Missbrauch von Administratorrechten unter Novell Netware Servern
G 5.60. Umgehen der Systemrichtlinien
G 5.61. Missbrauch von Remote-Zugängen für Managementfunktionen von Routern
G 5.62. Missbrauch von Ressourcen über abgesetzte IT-Systeme
G 5.63. Manipulationen über den ISDN-D-Kanal
G 5.64. Manipulation an Daten oder Software bei Datenbanksystemen
G 5.65. Verhinderung der Dienste eines Datenbanksystems
G 5.66. Unberechtigter Anschluss von IT-Systemen an ein Netz
G 5.67. Unberechtigte Ausführung von Netzmanagement-Funktionen
G 5.68. Unberechtigter Zugang zu den aktiven Netzkomponenten
G 5.69. Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz
G 5.70. Manipulation durch Familienangehörige und Besucher
G 5.71. Vertraulichkeitsverlust schützenswerter Informationen
G 5.72. Missbräuchliche Groupware-Nutzung
G 5.73. Vortäuschen eines falschen Absenders
G 5.74. Manipulation von Alias-Dateien oder Verteilerlisten
G 5.75. Überlastung durch eingehende E-Mails
G 5.76. Mailbomben
G 5.77. Mitlesen von E-Mails
G 5.78. DNS-Spoofing
G 5.79. Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen
G 5.80. Hoax

G 5.81. Unautorisierte Benutzung eines Kryptomoduls
G 5.82. Manipulation eines Kryptomoduls
G 5.83. Kompromittierung kryptographischer Schlüssel
G 5.84. Gefälschte Zertifikate
G 5.85. Integritätsverlust schützenswerter Informationen
G 5.86. Manipulation von Managementparametern
G 5.87. Web-Spoofing
G 5.88. Missbrauch aktiver Inhalte
G 5.89. Hijacking von Netz-Verbindungen
G 5.90. Manipulation von Adressbüchern und Verteillisten
G 5.91. Abschalten von Sicherheitsmechanismen für den RAS-Zugang
G 5.92. Nutzung des VPN-Clients als VPN-Server
G 5.93. Erlauben von Fremdnutzung von VPN-Komponenten
G 5.94. Missbrauch von SIM-Karten
G 5.95. Abhören von Raumgesprächen über Mobiltelefone
G 5.96. Manipulation von Mobiltelefonen
G 5.97. Unberechtigte Datenweitergabe über Mobiltelefone
G 5.98. Abhören von Mobiltelefonaten
G 5.99. Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
G 5.100. Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes/Domino
G 5.101. Hacking Lotus Notes/Domino
G 5.102. Sabotage
G 5.103. Missbrauch von Webmail
G 5.104. Ausspähen von Informationen
G 5.105. Verhinderung der Dienste von Archivsystemen
G 5.106. Unberechtigtes Überschreiben oder Löschen von Archivmedien
G 5.107. Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister
G 5.108. Ausnutzen von systemspezifischen Schwachstellen des IIS
G 5.109. Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver
G 5.110. Web-Bugs
G 5.111. Missbrauch aktiver Inhalte in E-Mails
G 5.112. Manipulation von ARP-Tabellen
G 5.113. MAC-Spoofing
G 5.114. Missbrauch von Spanning Tree
G 5.115. Überwindung der Grenzen zwischen VLANs
G 5.116. Manipulation der z/OS-Systemsteuerung
G 5.117. Verschleiern von Manipulationen unter z/OS
G 5.118. Unbefugtes Erlangen höherer Rechte im RACF
G 5.119. Benutzung fremder Kennungen unter z/OS-Systemen
G 5.120. Manipulation der Linux/zSeries Systemsteuerung
G 5.121. Angriffe über TCP/IP auf z/OS-Systeme
G 5.122. Missbrauch von RACF-Attributen unter z/OS
G 5.123. Abhören von Raumgesprächen über mobile Endgeräte
G 5.124. Missbrauch der Informationen von mobilen Endgeräten

G 5.125. Datendiebstahl mithilfe mobiler Endgeräte
G 5.126. Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten
G 5.127. Spyware
G 5.128. Unberechtigter Zugriff auf Daten durch Einbringen von Code in ein SAP System
G 5.129. Manipulation von Daten über das Speichersystem
G 5.130. Manipulation der Konfiguration einer Speicherlösung
G 5.131. SQL-Injection
G 5.132. Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003
G 5.133. Unautorisierte Benutzung web-basierter Administrationswerkzeuge
G 5.134. Fehlende Identifizierung zwischen Gesprächsteilnehmern
G 5.135. SPIT und Vishing
G 5.136. Missbrauch frei zugänglicher Telefonanschlüsse
G 5.137. Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation
G 5.138. Angriffe auf WLAN-Komponenten
G 5.139. Abhören der WLAN-Kommunikation
G 5.140. Auswertung von Restinformationen in Druckern, Kopierern und Multifunktionsgeräten
G 5.141. Datendiebstahl über mobile Datenträger
G 5.142. Verbreitung von Schadprogrammen über mobile Datenträger
G 5.143. Man-in-the-Middle-Angriff
G 5.144. Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff
G 5.145. Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement
G 5.146. Vertraulichkeitsverlust durch Auslagerungsdateien
G 5.147. Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes
G 5.148. Missbrauch von Virtualisierungsfunktionen
G 5.149. Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen
G 5.150. Kompromittierung des Hypervisor virtueller IT-Systeme
G 5.151. DNS-Flooding - Denial-of-Service
G 5.152. DNS-Hijacking
G 5.153. DNS-Amplification Angriff
G 5.154. DNS Information Leakage
G 5.155. Ausnutzen dynamischer DNS-Updates
G 5.156. Bot-Netze
G 5.157. Phishing und Pharming
G 5.158. Missbrauch sozialer Netzwerke
G 5.159. Erstellung von Bewegungsprofilen unter Bluetooth
G 5.160. Missbrauch der Bluetooth-Profile
G 5.161. Gefälschte Antworten auf XDMCP-Broadcasts bei Terminalservern
G 5.162. Umleiten von X-Window-Sitzungen
G 5.163. Angriffe auf Exchange-Systeme
G 5.164. Missbrauch von Programmierschnittstellen unter Outlook

G 5.165. Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services
G 5.166. Missbrauch einer Webanwendung durch automatisierte Nutzung
G 5.167. Fehler in der Logik von Webanwendungen und Web-Services
G 5.168. Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services
G 5.169. Unzureichendes Session-Management von Webanwendungen und Web-Services
G 5.170. Cross-Site Scripting (XSS)
G 5.171. Cross-Site Request Forgery (CSRF, XSRF, Session Riding)
G 5.172. Umgehung der Autorisierung bei Webanwendungen und Web-Services
G 5.173. Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services
G 5.174. Injection-Angriffe
G 5.175. Clickjacking
G 5.176. Kompromittierung der Protokolldatenübertragung bei zentraler Protokollierung
G 5.177. Missbrauch von Kurz-URLs oder QR-Codes
G 5.178. Missbrauch von Administratorrechten im Cloud-Management
G 5.179. Angriffe auf Protokolle
G 5.180. Angriffe auf Registries und Repositories
G 5.181. Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services
G 5.182. Manipulation von Routen (Routing Detours)
G 5.183. Angriffe auf XML
G 5.184. Informationsgewinnung über Web-Services
G 5.185. Erlangung physischen Zugangs auf SAN-Switches
G 5.186. Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing
G 5.187. Überwindung der logischen Netzseparierung
G 5.188. Unberechtigter Zugriff auf Daten innerhalb einer Cloud-Storage-Lösung
G 5.189. Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden
G 5.190. Missbrauch von Services
G 5.191. Manipulation der Abrechnungsinformationen
G 5.192. Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender
G 5.193. Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs
G 5.194. Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion
G 5.195. Ausnutzen von Schwachstellen in Backend-Anwendungen
G 5.196. Unterbinden einer Informations- und Dienstesynchronisation in einer verteilten SOA-Umgebung
G 5.197. Missbrauch von SAML-Token in SOA-Umgebungen
G 5.198. Missbrauch der WS-Notification-Broker in einer SOA
G 5.199. Ungenügende Absicherung der SOAP-Kommunikation

M 1.35. Sammelaufbewahrung tragbarer IT-Systeme
M 1.36. Sichere Aufbewahrung der Datenträger vor und nach Versand
M 1.37. Geeignete Aufstellung eines Faxgerätes
M 1.38. Geeignete Aufstellung eines Modems
M 1.39. Verhinderung von Ausgleichsströmen auf Schirmungen
M 1.40. Geeignete Aufstellung von Schutzschränken
M 1.41. Schutz gegen elektromagnetische Einstrahlung
M 1.42. Gesicherte Aufstellung von Novell Netware Servern
M 1.43. Gesicherte Aufstellung aktiver Netzkomponenten
M 1.44. Geeignete Einrichtung eines häuslichen Arbeitsplatzes
M 1.45. Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
M 1.46. Einsatz von Diebstahl-Sicherungen
M 1.47. Eigener Brandabschnitt
M 1.48. Brandmeldeanlage im Rechenzentrum
M 1.49. Technische und organisatorische Vorgaben für das Rechenzentrum
M 1.50. Rauchschutz
M 1.51. Brandlastreduzierung
M 1.52. Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur
M 1.53. Videoüberwachung
M 1.54. Brandfrühesterkennung / Löschtechnik
M 1.55. Perimeterschutz
M 1.56. Netzersatzanlage
M 1.57. Aktuelle Infrastruktur- und Baupläne
M 1.58. Technische und organisatorische Vorgaben für Serverräume
M 1.59. Geeignete Aufstellung von Speicher- und Archivsystemen
M 1.60. Geeignete Lagerung von Archivmedien
M 1.61. Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
M 1.62. Brandschutz von Patchfeldern
M 1.63. Geeignete Aufstellung von Access Points
M 1.64. Vermeidung elektrischer Zündquellen
M 1.65. Erneuerung der IT-Verkabelung
M 1.66. Beachtung von Normen bei der IT-Verkabelung
M 1.67. Dimensionierung und Nutzung von Schranksystemen
M 1.68. Fachgerechte Installation
M 1.69. Verkabelung in Serverräumen
M 1.70. Zentrale unterbrechungsfreie Stromversorgung
M 1.71. Funktionstests der technischen Infrastruktur
M 1.72. Baumaßnahmen während des laufenden Betriebs
M 1.73. Schutz eines Rechenzentrums gegen unbefugten Zutritt
M 1.74. EMV-taugliche Stromversorgung
M 1.75. Branderkennung in Gebäuden
M 1.76. Geeignete Auswahl und Nutzung eines lokalen Arbeitsplatzes
M 1.77. Klimatisierung für Menschen
M 1.78. Sicherheitskonzept für die Gebäudenutzung
M 1.79. Bildung von Sicherheitszonen
M 1.80. Zutrittskontrollsystem und Berechtigungsmanagement

M 1.81. Materielle Sicherung von eingebetteten Systemen

M 2 Organisation

M 2.1. Festlegung von Verantwortlichkeiten und Regelungen
M 2.2. Betriebsmittelverwaltung
M 2.3. Datenträgerverwaltung
M 2.4. Regelungen für Wartungs- und Reparaturarbeiten
M 2.5. Aufgabenverteilung und Funktionstrennung
M 2.6. Vergabe von Zutrittsberechtigungen
M 2.7. Vergabe von Zugangsberechtigungen
M 2.8. Vergabe von Zugriffsrechten
M 2.9. Nutzungsverbot nicht freigegebener Hard- und Software
M 2.10. Überprüfung des Hard- und Software-Bestandes
M 2.11. Regelung des Passwortgebrauchs
M 2.12. Betreuung und Beratung von IT-Benutzern
M 2.13. Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
M 2.14. Schlüsselverwaltung
M 2.15. Brandschutzbegehungen
M 2.16. Beaufsichtigung oder Begleitung von Fremdpersonen
M 2.17. Zutrittsregelung und -kontrolle
M 2.18. Kontrollgänge
M 2.19. Neutrale Dokumentation in den Verteilern
M 2.20. Kontrolle bestehender Verbindungen
M 2.21. Rauchverbot
M 2.22. Hinterlegen des Passwortes
M 2.23. Herausgabe einer PC-Richtlinie
M 2.24. Einführung eines IT-Passes
M 2.25. Dokumentation der Systemkonfiguration
M 2.26. Ernennung eines Administrators und eines Vertreters
M 2.27. Wartung einer TK-Anlage
M 2.28. Bereitstellung externer TK-Beratungskapazität
M 2.29. Bedienungsanleitung der TK-Anlage für die Benutzer
M 2.30. Regelung für die Einrichtung von Benutzern / Benutzergruppen
M 2.31. Dokumentation der zugelassenen Benutzer und Rechteprofile
M 2.32. Einrichtung einer eingeschränkten Benutzerumgebung
M 2.33. Aufteilung der Administrationstätigkeiten unter Unix
M 2.34. Dokumentation der Veränderungen an einem bestehenden System
M 2.35. Informationsbeschaffung über Sicherheitslücken des Systems
M 2.36. Geregelte Übergabe und Rücknahme eines tragbaren PC
M 2.37. Der aufgeräumte Arbeitsplatz
M 2.38. Aufteilung der Administrationstätigkeiten
M 2.39. Reaktion auf Verletzungen der Sicherheitsvorgaben
M 2.40. Rechtzeitige Beteiligung des Personal-/Betriebsrates
M 2.41. Verpflichtung der Mitarbeiter zur Datensicherung
M 2.42. Festlegung der möglichen Kommunikationspartner
M 2.43. Ausreichende Kennzeichnung der Datenträger beim Versand
M 2.44. Sichere Verpackung der Datenträger
M 2.45. Regelung des Datenträgeraustausches

M 2.46. Geeignetes Schlüsselmanagement
M 2.47. Ernennung eines Fax-Verantwortlichen
M 2.48. Festlegung berechtigter Faxbediener
M 2.49. Beschaffung geeigneter Faxgeräte
M 2.50. Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
M 2.51. Fertigung von Kopien eingehender Faxsendungen
M 2.52. Versorgung und Kontrolle der Verbrauchsgüter
M 2.53. Abschalten des Faxgerätes außerhalb der Bürozeiten
M 2.54. Beschaffung geeigneter Anrufbeantworter
M 2.55. Einsatz eines Sicherungscodes
M 2.56. Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter
M 2.57. Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche
M 2.58. Begrenzung der Sprechdauer
M 2.59. Auswahl eines geeigneten Modems in der Beschaffung
M 2.60. Sichere Administration eines Modems
M 2.61. Regelung des Modem-Einsatzes
M 2.62. Software-Abnahme- und Freigabe-Verfahren
M 2.63. Einrichten der Zugriffsrechte
M 2.64. Kontrolle der Protokolldateien
M 2.65. Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
M 2.66. Beachtung des Beitrags der Zertifizierung für die Beschaffung
M 2.67. Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
M 2.68. Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten
M 2.69. Einrichtung von Standardarbeitsplätzen
M 2.70. Entwicklung eines Konzepts für Sicherheitsgateways
M 2.71. Festlegung einer Policy für ein Sicherheitsgateway
M 2.72. Anforderungen an eine Firewall
M 2.73. Auswahl geeigneter Grundstrukturen für Sicherheitsgateways
M 2.74. Geeignete Auswahl eines Paketfilters
M 2.75. Geeignete Auswahl eines Application-Level-Gateways
M 2.76. Auswahl und Einrichtung geeigneter Filterregeln
M 2.77. Integration von Servern in das Sicherheitsgateway
M 2.78. Sicherer Betrieb eines Sicherheitsgateways
M 2.79. Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
M 2.80. Erstellung eines Anforderungskatalogs für Standardsoftware
M 2.81. Vorauswahl eines geeigneten Standardsoftwareproduktes
M 2.82. Entwicklung eines Testplans für Standardsoftware
M 2.83. Testen von Standardsoftware
M 2.84. Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
M 2.85. Freigabe von Standardsoftware
M 2.86. Sicherstellen der Integrität von Standardsoftware
M 2.87. Installation und Konfiguration von Standardsoftware
M 2.88. Lizenzverwaltung und Versionskontrolle von Standardsoftware
M 2.89. Deinstallation von Standardsoftware

M 2.90. Überprüfung der Lieferung
M 2.91. Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
M 2.92. Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
M 2.93. Planung des Windows NT Netzes
M 2.94. Freigabe von Verzeichnissen unter Windows NT
M 2.95. Beschaffung geeigneter Schutzschränke
M 2.96. Verschluss von Schutzschränken
M 2.97. Korrekter Umgang mit Codeschlössern
M 2.98. Sichere Installation von Novell Netware Servern
M 2.99. Sichere Einrichtung von Novell Netware Servern
M 2.100. Sicherer Betrieb von Novell Netware Servern
M 2.101. Revision von Novell Netware Servern
M 2.102. Verzicht auf die Aktivierung der Remote Console
M 2.103. Einrichten von Benutzerprofilen unter Windows 95
M 2.104. Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
M 2.105. Beschaffung von TK-Anlagen
M 2.106. Auswahl geeigneter ISDN-Karten in der Beschaffung
M 2.107. Dokumentation der ISDN-Karten-Konfiguration
M 2.108. Fernwartung der ISDN-Netzkoppelelemente
M 2.109. Rechtevergabe für den Fernzugriff
M 2.110. Datenschutzaspekte bei der Protokollierung
M 2.111. Bereithalten von Handbüchern
M 2.112. Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution
M 2.113. Regelungen für Telearbeit
M 2.114. Informationsfluss zwischen Telearbeiter und Institution
M 2.115. Betreuungs- und Wartungskonzept für Telearbeitsplätze
M 2.116. Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit
M 2.117. Erstellung eines Sicherheitskonzeptes für Telearbeit
M 2.118. Konzeption der sicheren E-Mail-Nutzung
M 2.119. Regelung für den Einsatz von E-Mail
M 2.120. Einrichtung einer Poststelle
M 2.121. Regelmäßiges Löschen von E-Mails
M 2.122. Einheitliche E-Mail-Adressen
M 2.123. Auswahl eines Groupware- oder Mailproviders
M 2.124. Geeignete Auswahl einer Datenbank-Software
M 2.125. Installation und Konfiguration einer Datenbank
M 2.126. Erstellung eines Datenbanksicherheitskonzeptes
M 2.127. Inferenzprävention
M 2.128. Zugangskontrolle einer Datenbank
M 2.129. Zugriffskontrolle einer Datenbank
M 2.130. Gewährleistung der Datenbankintegrität
M 2.131. Aufteilung von Administrationstätigkeiten bei Datenbanksystemen

M 2.132. Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
M 2.133. Kontrolle der Protokolldateien eines Datenbanksystems
M 2.134. Richtlinien für Datenbank-Anfragen
M 2.135. Gesicherte Datenübernahme in eine Datenbank
M 2.136. Einhaltung von Regelungen zu Arbeitsplatz und Arbeitsumgebung
M 2.137. Beschaffung eines geeigneten Datensicherungssystems
M 2.138. Strukturierte Datenhaltung
M 2.139. Ist-Aufnahme der aktuellen Netzsituation
M 2.140. Analyse der aktuellen Netzsituation
M 2.141. Entwicklung eines Netzkonzeptes
M 2.142. Entwicklung eines Netz-Realisierungsplans
M 2.143. Entwicklung eines Netzmanagement-Konzeptes
M 2.144. Verwendung von SNMP als Netzmanagement-Protokoll
M 2.145. Anforderungen an ein Netzmanagement-Tool
M 2.146. Sicherer Betrieb eines Netzmanagement-Systems
M 2.147. Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze
M 2.148. Sichere Einrichtung von Novell Netware 4.x Netzen
M 2.149. Sicherer Betrieb von Novell Netware 4.x Netzen
M 2.150. Revision von Novell Netware 4.x Netzen
M 2.151. Entwurf eines NDS-Konzeptes
M 2.152. Entwurf eines Zeitsynchronisations-Konzeptes
M 2.153. Dokumentation von Novell Netware 4.x Netzen
M 2.154. Erstellung eines Sicherheitskonzeptes gegen Schadprogramme
M 2.155. Identifikation potentiell von Computer-Viren betroffener IT-Systeme
M 2.156. Auswahl einer geeigneten Computer-Virenschutz-Strategie
M 2.157. Auswahl eines geeigneten Viren-Schutzprogramms
M 2.158. Meldung von Schadprogramm-Infektionen
M 2.159. Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen
M 2.160. Regelungen zum Schutz vor Schadprogrammen
M 2.161. Entwicklung eines Kryptokonzepts
M 2.162. Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte
M 2.163. Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
M 2.164. Auswahl eines geeigneten kryptographischen Verfahrens
M 2.165. Auswahl eines geeigneten kryptographischen Produktes
M 2.166. Regelung des Einsatzes von Kryptomodulen
M 2.167. Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten
M 2.168. IT-System-Analyse vor Einführung eines Systemmanagement-Systems
M 2.169. Entwickeln einer Systemmanagementstrategie
M 2.170. Anforderungen an ein Systemmanagement-System
M 2.171. Geeignete Auswahl eines Systemmanagement-Produktes

M 2.172. Entwicklung eines Konzeptes für Webangebote
M 2.173. Festlegung einer Webserver-Sicherheitsstrategie
M 2.174. Sicherer Betrieb eines Webservers
M 2.175. Aufbau eines Webservers
M 2.176. Geeignete Auswahl eines Internet Service Providers
M 2.177. Sicherheit bei Umzügen
M 2.178. Erstellung einer Sicherheitsleitlinie für die Faxnutzung
M 2.179. Regelungen für den Faxserver-Einsatz
M 2.180. Einrichten einer Fax-Poststelle
M 2.181. Auswahl eines geeigneten Faxservers
M 2.182. Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
M 2.183. Durchführung einer RAS-Anforderungsanalyse
M 2.184. Entwicklung eines RAS-Konzeptes
M 2.185. Auswahl einer geeigneten RAS-Systemarchitektur
M 2.186. Geeignete Auswahl eines RAS-Produktes
M 2.187. Festlegen einer RAS-Sicherheitsrichtlinie
M 2.188. Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
M 2.189. Sperrung des Mobiltelefons bei Verlust
M 2.190. Einrichtung eines Mobiltelefon-Pools
M 2.191. Etablierung des IT-Sicherheitsprozesses
M 2.192. Erstellung einer Leitlinie zur Informationssicherheit
M 2.193. Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
M 2.194. Erstellung einer Übersicht über vorhandene IT-Systeme
M 2.195. Erstellung eines Sicherheitskonzepts
M 2.196. Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan
M 2.197. Integration der Mitarbeiter in den Sicherheitsprozess
M 2.198. Sensibilisierung der Mitarbeiter für Informationssicherheit
M 2.199. Aufrechterhaltung der Informationssicherheit
M 2.200. Management-Berichte zur Informationssicherheit
M 2.201. Dokumentation des Sicherheitsprozesses
M 2.202. Erstellung eines Handbuchs zur IT-Sicherheit
M 2.203. Aufbau einer Informationsbörse zur IT-Sicherheit
M 2.204. Verhinderung ungesicherter Netzzugänge
M 2.205. Übertragung und Abruf personenbezogener Daten
M 2.206. Planung des Einsatzes von Lotus Notes/Domino
M 2.207. Sicherheitskonzeption für Lotus Notes/Domino
M 2.208. Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
M 2.209. Planung des Einsatzes von Lotus Notes im Intranet
M 2.210. Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
M 2.211. Planung des Einsatzes von Lotus Notes in einer DMZ
M 2.212. Organisatorische Vorgaben für die Gebäudereinigung
M 2.213. Inspektion und Wartung der technischen Infrastruktur
M 2.214. Konzeption des IT-Betriebs

M 2.215. Fehlerbehandlung
M 2.216. Genehmigungsverfahren für IT-Komponenten
M 2.217. Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
M 2.218. Regelung der Mitnahme von Datenträgern und IT-Komponenten
M 2.219. Kontinuierliche Dokumentation der Informationsverarbeitung
M 2.220. Richtlinien für die Zugriffs- bzw. Zugangskontrolle
M 2.221. Änderungsmanagement
M 2.222. Regelmäßige Kontrollen der technischen IT-Sicherheitsmaßnahmen
M 2.223. Sicherheitsvorgaben für die Nutzung von Standardsoftware
M 2.224. Vorbeugung gegen Schadprogramme
M 2.225. Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
M 2.226. Regelungen für den Einsatz von Fremdpersonal
M 2.227. Planung des Windows 2000 Einsatzes
M 2.228. Festlegen einer Windows 2000 Sicherheitsrichtlinie
M 2.229. Planung des Active Directory
M 2.230. Planung der Active Directory-Administration
M 2.231. Planung der Gruppenrichtlinien unter Windows
M 2.232. Planung der Windows-CA-Struktur ab Windows 2000
M 2.233. Planung der Migration von Windows NT auf Windows 2000
M 2.234. Konzeption von Internet-PCs
M 2.235. Richtlinien für die Nutzung von Internet-PCs
M 2.236. Planung des Einsatzes von Novell eDirectory
M 2.237. Planung der Partitionierung und Replikation im Novell eDirectory
M 2.238. Festlegung einer Sicherheitsrichtlinie für Novell eDirectory
M 2.239. Planung des Einsatzes von Novell eDirectory im Intranet
M 2.240. Planung des Einsatzes von Novell eDirectory im Extranet
M 2.241. Durchführung einer Anforderungsanalyse für den Telearbeitsplatz
M 2.242. Zielsetzung der elektronischen Archivierung
M 2.243. Entwicklung des Archivierungskonzepts
M 2.244. Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
M 2.245. Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung
M 2.246. Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
M 2.247. Planung des Einsatzes von Exchange und Outlook
M 2.248. Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000
M 2.249. Planung der Migration von Exchange-Systemen
M 2.250. Festlegung einer Outsourcing-Strategie
M 2.251. Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben
M 2.252. Wahl eines geeigneten Outsourcing-Dienstleisters
M 2.253. Vertragsgestaltung mit dem Outsourcing-Dienstleister
M 2.254. Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben

M 2.255. Sichere Migration bei Outsourcing-Vorhaben
M 2.256. Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb
M 2.257. Überwachung der Speicherressourcen von Archivmedien
M 2.258. Konsistente Indizierung von Dokumenten bei der Archivierung
M 2.259. Einführung eines übergeordneten Dokumentenmanagements
M 2.260. Regelmäßige Revision des Archivierungsprozesses
M 2.261. Regelmäßige Marktbeobachtung von Archivsystemen
M 2.262. Regelung der Nutzung von Archivsystemen
M 2.263. Regelmäßige Aufbereitung von archivierten Datenbeständen
M 2.264. Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung
M 2.265. Geeigneter Einsatz digitaler Signaturen bei der Archivierung
M 2.266. Regelmäßige Erneuerung technischer Archivsystem-Komponenten
M 2.267. Planen des IIS-Einsatzes
M 2.268. Festlegung einer IIS-Sicherheitsrichtlinie
M 2.269. Planung des Einsatzes eines Apache Webservers
M 2.270. Planung des SSL-Einsatzes beim Apache Webserver
M 2.271. Festlegung einer Sicherheitsstrategie für den WWW-Zugang
M 2.272. Einrichtung eines Internet-Redaktionsteams
M 2.273. Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
M 2.274. Vertretungsregelungen bei E-Mail-Nutzung
M 2.275. Einrichtung funktionsbezogener E-Mailadressen
M 2.276. Funktionsweise eines Routers
M 2.277. Funktionsweise eines Switches
M 2.278. Typische Einsatzszenarien von Routern und Switches
M 2.279. Erstellung einer Sicherheitsrichtlinie für Router und Switches
M 2.280. Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches
M 2.281. Dokumentation der Systemkonfiguration von Routern und Switches
M 2.282. Regelmäßige Kontrolle von Routern und Switches
M 2.283. Software-Pflege auf Routern und Switches
M 2.284. Sichere Außerbetriebnahme von Routern und Switches
M 2.285. Festlegung von Standards für z/OS-Systemdefinitionen
M 2.286. Planung und Einsatz von zSeries-Systemen
M 2.287. Batch-Job-Planung für z/OS-Systeme
M 2.288. Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
M 2.289. Einsatz restriktiver z/OS-Kennungen
M 2.290. Einsatz von RACF-Exits
M 2.291. Sicherheits-Berichtswesen und -Audits unter z/OS
M 2.292. Überwachung von z/OS-Systemen
M 2.293. Wartung von zSeries-Systemen
M 2.294. Synchronisierung von z/OS-Passwörtern und RACF-Kommandos
M 2.295. Systemverwaltung von z/OS-Systemen
M 2.296. Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren
M 2.297. Deinstallation von z/OS-Systemen
M 2.298. Verwaltung von Internet-Domainnamen

M 2.299. Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
M 2.300. Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways
M 2.301. Outsourcing des Sicherheitsgateway
M 2.302. Sicherheitsgateways und Hochverfügbarkeit
M 2.303. Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs
M 2.304. Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs
M 2.305. Geeignete Auswahl von Smartphones, Tablets oder PDAs
M 2.306. Verlustmeldung
M 2.307. Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses
M 2.308. Auszug aus Gebäuden
M 2.309. Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
M 2.310. Geeignete Auswahl von Laptops
M 2.311. Planung von Schutzschränken
M 2.312. Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit
M 2.313. Sichere Anmeldung bei Internet-Diensten
M 2.314. Verwendung von hochverfügbaren Architekturen für Server
M 2.315. Planung des Servereinsatzes
M 2.316. Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
M 2.317. Beschaffungskriterien für einen Server
M 2.318. Sichere Installation eines IT-Systems
M 2.319. Migration eines Servers
M 2.320. Geregelte Außerbetriebnahme eines Servers
M 2.321. Planung des Einsatzes von Client-Server-Netzen
M 2.322. Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
M 2.323. Geregelte Außerbetriebnahme eines Clients
M 2.324. Einführung von Windows auf Clients ab Windows XP planen
M 2.325. Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP
M 2.326. Planung der Gruppenrichtlinien für Clients ab Windows XP
M 2.327. Sicherheit beim Fernzugriff auf Clients ab Windows XP
M 2.328. Einsatz von Windows XP auf mobilen Rechnern
M 2.329. Einführung von Windows XP SP2
M 2.330. Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP
M 2.331. Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
M 2.332. Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen
M 2.333. Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen
M 2.334. Auswahl eines geeigneten Gebäudes
M 2.335. Festlegung der Sicherheitsziele und -strategie

M 2.336. Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene
M 2.337. Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse
M 2.338. Erstellung von zielgruppengerechten Sicherheitsrichtlinien
M 2.339. Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit
M 2.340. Beachtung rechtlicher Rahmenbedingungen
M 2.341. Planung des SAP Einsatzes
M 2.342. Planung von SAP Berechtigungen
M 2.343. Absicherung eines SAP Systems im Portal-Szenario
M 2.344. Sicherer Betrieb von SAP Systemen im Internet
M 2.345. Outsourcing eines SAP Systems
M 2.346. Nutzung der SAP Dokumentation
M 2.347. Regelmäßige Sicherheitsprüfungen für SAP Systeme
M 2.348. Sicherheit beim Customizing von SAP Systemen
M 2.349. Sicherheit bei der Software-Entwicklung für SAP Systeme
M 2.350. Aussonderung von SAP Systemen
M 2.351. Planung von Speicherlösungen
M 2.352. Erstellung einer Sicherheitsrichtlinie für NAS-Systeme
M 2.353. Erstellung einer Sicherheitsrichtlinie für SAN-Systeme
M 2.354. Einsatz einer hochverfügbaren SAN-Lösung
M 2.355. Auswahl von Lieferanten für eine Speicherlösung
M 2.356. Vertragsgestaltung mit Dienstleistern für Speicherlösungen
M 2.357. Aufbau eines Administrationsnetzes für Speichersysteme
M 2.358. Dokumentation der Systemeinstellungen von Speichersystemen
M 2.359. Überwachung und Verwaltung von Speicherlösungen
M 2.360. Sicherheits-Audits und Berichtswesen bei Speichersystemen
M 2.361. Außerbetriebnahme von Speicherlösungen
M 2.362. Auswahl einer geeigneten Speicherlösung
M 2.363. Schutz gegen SQL-Injection
M 2.364. Planung der Administration ab Windows 2003
M 2.365. Planung der Systemüberwachung unter Windows Server 2003
M 2.366. Nutzung von Sicherheitsvorlagen unter Windows Server 2003
M 2.367. Einsatz von Kommandos und Skripten ab Windows Server 2003
M 2.368. Umgang mit administrativen Vorlagen unter Windows ab Server 2003
M 2.369. Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003
M 2.370. Administration der Berechtigungen ab Windows Server 2003
M 2.371. Geregelte Deaktivierung und Löschung ungenutzter Konten
M 2.372. Planung des VoIP-Einsatzes
M 2.373. Erstellung einer Sicherheitsrichtlinie für VoIP
M 2.374. Umfang der Verschlüsselung von VoIP
M 2.375. Geeignete Auswahl von VoIP-Systemen
M 2.376. Trennung des Daten- und VoIP-Netzes
M 2.377. Sichere Außerbetriebnahme von VoIP-Komponenten
M 2.378. System-Entwicklung

M 2.379. Software-Entwicklung durch Endbenutzer
M 2.380. Ausnahmegenehmigungen
M 2.381. Festlegung einer Strategie für die WLAN-Nutzung
M 2.382. Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung
M 2.383. Auswahl eines geeigneten WLAN-Standards
M 2.384. Auswahl geeigneter Kryptoverfahren für WLAN
M 2.385. Geeignete Auswahl von WLAN-Komponenten
M 2.386. Sorgfältige Planung notwendiger WLAN-Migrationsschritte
M 2.387. Installation, Konfiguration und Betreuung eines WLANs durch Dritte
M 2.388. Geeignetes WLAN-Schlüsselmanagement
M 2.389. Sichere Nutzung von Hotspots
M 2.390. Außerbetriebnahme von WLAN-Komponenten
M 2.391. Frühzeitige Information des Brandschutzbeauftragten
M 2.392. Modellierung von Virtualisierungsservern und virtuellen IT-Systemen
M 2.393. Regelung des Informationsaustausches
M 2.394. Prüfung elektrischer Anlagen
M 2.395. Anforderungsanalyse für die IT-Verkabelung
M 2.396. Vorgaben zur Dokumentation und Kennzeichnung der IT-Verkabelung
M 2.397. Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten
M 2.398. Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten
M 2.399. Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten
M 2.400. Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten
M 2.401. Umgang mit mobilen Datenträgern und Geräten
M 2.402. Zurücksetzen von Passwörtern
M 2.403. Planung des Einsatzes von Verzeichnisdiensten
M 2.404. Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste
M 2.405. Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten
M 2.406. Geeignete Auswahl von Komponenten für Verzeichnisdienste
M 2.407. Planung der Administration von Verzeichnisdiensten
M 2.408. Planung der Migration von Verzeichnisdiensten
M 2.409. Planung der Partitionierung und Replikation im Verzeichnisdienst
M 2.410. Geregelte Außerbetriebnahme eines Verzeichnisdienstes
M 2.411. Trennung der Verwaltung von Diensten und Daten eines Active Directory
M 2.412. Schutz der Authentisierung beim Einsatz von Active Directory
M 2.413. Sicherer Einsatz von DNS für Active Directory
M 2.414. Computer-Viren-Schutz für Domänen-Controller
M 2.415. Durchführung einer VPN-Anforderungsanalyse
M 2.416. Planung des VPN-Einsatzes
M 2.417. Planung der technischen VPN-Realisierung

M 2.418. Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung
M 2.419. Geeignete Auswahl von VPN-Produkten
M 2.420. Auswahl eines Trusted-VPN-Dienstleisters
M 2.421. Planung des Patch- und Änderungsmanagementprozesses
M 2.422. Umgang mit Änderungsanforderungen
M 2.423. Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement
M 2.424. Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen
M 2.425. Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement
M 2.426. Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse
M 2.427. Abstimmung von Änderungsanforderungen
M 2.428. Skalierbarkeit beim Patch- und Änderungsmanagement
M 2.429. Erfolgsmessung von Änderungsanforderungen
M 2.430. Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs
M 2.431. Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen
M 2.432. Richtlinie für die Löschung und Vernichtung von Informationen
M 2.433. Überblick über Methoden zur Löschung und Vernichtung von Daten
M 2.434. Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten
M 2.435. Auswahl geeigneter Aktenvernichter
M 2.436. Vernichtung von Datenträgern durch externe Dienstleister
M 2.437. Planung des Einsatzes eines Samba-Servers
M 2.438. Sicherer Einsatz externer Programme auf einem Samba-Server
M 2.439. Konzeption und Organisation des Anforderungsmanagements
M 2.440. Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista
M 2.441. Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista
M 2.442. Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen
M 2.443. Einführung von Windows Vista SP1
M 2.444. Einsatzplanung für virtuelle IT-Systeme
M 2.445. Auswahl geeigneter Hardware für Virtualisierungsumgebungen
M 2.446. Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern
M 2.447. Sicherer Einsatz virtueller IT-Systeme
M 2.448. Überwachung der Funktion und Konfiguration virtueller Infrastrukturen
M 2.449. Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme
M 2.450. Einführung in DNS-Grundbegriffe
M 2.451. Planung des DNS-Einsatzes
M 2.452. Auswahl eines geeigneten DNS-Server-Produktes
M 2.453. Aussonderung von DNS-Servern

M 2.454. Planung des sicheren Einsatzes von Groupware-Systemen
M 2.455. Festlegung einer Sicherheitsrichtlinie für Groupware
M 2.456. Sichere Administration von Groupware-Systemen
M 2.457. Konzeption für die sichere Internet-Nutzung
M 2.458. Richtlinie für die Internet-Nutzung
M 2.459. Überblick über Internet-Dienste
M 2.460. Geregelte Nutzung von externen Dienstleistungen
M 2.461. Planung des sicheren Bluetooth-Einsatzes
M 2.462. Auswahlkriterien für die Beschaffung von Bluetooth-Geräten
M 2.463. Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten
M 2.464. Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung
M 2.465. Analyse der erforderlichen Systemressourcen von Terminalservern
M 2.466. Migration auf eine Terminalserver-Architektur
M 2.467. Planung von regelmäßigen Neustartzyklen von Terminalservern
M 2.468. Lizenzierung von Software in Terminalserver-Umgebungen
M 2.469. Geregelte Außerbetriebnahme von Komponenten einer Terminalserver-Umgebung
M 2.470. Durchführung einer Anforderungsanalyse für TK-Anlagen
M 2.471. Planung des Einsatzes von TK-Anlagen
M 2.472. Erstellung einer Sicherheitsrichtlinie für TK-Anlagen
M 2.473. Auswahl von TK-Diensteanbietern
M 2.474. Sichere Außerbetriebnahme von TK-Komponenten
M 2.475. Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten
M 2.476. Konzeption für die sichere Internet-Anbindung
M 2.477. Planung einer virtuellen Infrastruktur
M 2.478. Planung des sicheren Einsatzes von Mac OS X
M 2.479. Planung der Sicherheitsrichtlinien von Mac OS X
M 2.480. Nutzung der Exchange- und Outlook-Dokumentation
M 2.481. Planung des Einsatzes von Exchange für Outlook Anywhere
M 2.482. Regelmäßige Sicherheitsprüfungen für Exchange-Systeme
M 2.483. Sicherheit beim Customizing von Exchange-Systemen
M 2.484. Planung von OpenLDAP
M 2.485. Auswahl von Backends für OpenLDAP
M 2.486. Dokumentation der Architektur von Webanwendungen und Web-Services
M 2.487. Entwicklung und Erweiterung von Anwendungen
M 2.488. Web-Tracking
M 2.489. Planung der Systemüberwachung unter Windows Server 2008
M 2.490. Planung des Einsatzes von Virtualisierung mit Hyper-V
M 2.491. Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008
M 2.492. Integration der Lotus Notes/Domino-Umgebung in die vorhandene Sicherheitsinfrastruktur
M 2.493. Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino

M 2.494. Geeignete Auswahl von Komponenten für die Infrastruktur einer Lotus Notes/Domino-Umgebung
M 2.495. Aussonderung von Lotus Notes/Domino-Komponenten
M 2.496. Geregelte Außerbetriebnahme eines Protokollierungsservers
M 2.497. Erstellung eines Sicherheitskonzepts für die Protokollierung
M 2.498. Behandlung von Warn- und Fehlermeldungen
M 2.499. Planung der Protokollierung
M 2.500. Protokollierung von IT-Systemen
M 2.501. Datenschutzmanagement
M 2.502. Regelung der Verantwortlichkeiten im Bereich Datenschutz
M 2.503. Aspekte eines Datenschutzkonzeptes
M 2.504. Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten
M 2.505. Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten
M 2.506. Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten
M 2.507. Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten
M 2.508. Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten
M 2.509. Datenschutzrechtliche Freigabe
M 2.510. Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten
M 2.511. Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten
M 2.512. Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten
M 2.513. Dokumentation der datenschutzrechtlichen Zulässigkeit
M 2.514. Aufrechterhaltung des Datenschutzes im laufenden Betrieb
M 2.515. Datenschutzgerechte Löschung/Vernichtung
M 2.516. Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender
M 2.517. Vertragsgestaltung mit Dritt-Dienstleistern
M 2.518. Einsatz einer hochverfügbaren Firewall-Lösung
M 2.519. Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing
M 2.520. Sicheres und vollständiges Löschen von Cloud-Anwenderdaten
M 2.521. Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten
M 2.522. Berichtswesen und Kommunikation zu den Cloud-Anwendern
M 2.523. Sichere Automatisierung der Cloud-Regelprozesse
M 2.524. Modellierung von Cloud Management
M 2.525. Erstellung einer Sicherheitsrichtlinie für Speicherlösungen
M 2.526. Planung des Betriebs der Speicherlösung
M 2.527. Sicheres Löschen in SAN-Umgebungen

M 2.528. Planung der sicheren Trennung von Mandanten in Speicherlösungen
M 2.529. Modellierung von Speicherlösungen
M 2.530. Planung und Vorbereitung von Migrationen
M 2.531. Erarbeitung einer Sicherheitsrichtlinie für Web-Services
M 2.532. Anbieten von Web-Services für Dritte
M 2.533. Vertragliche Aspekte bei der Bereitstellung von Web-Services
M 2.534. Erstellung einer Cloud-Nutzungs-Strategie
M 2.535. Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung
M 2.536. Service-Definition für Cloud-Dienste durch den Anwender
M 2.537. Planung der sicheren Migration zu einem Cloud Service
M 2.538. Planung der sicheren Einbindung von Cloud Services
M 2.539. Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung
M 2.540. Sorgfältige Auswahl eines Cloud-Diensteanbieters
M 2.541. Vertragsgestaltung mit dem Cloud-Diensteanbieter
M 2.542. Sichere Migration zu einem Cloud Service
M 2.543. Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb
M 2.544. Auditierung bei Cloud-Nutzung
M 2.545. Modellierung der Cloud-Nutzung
M 2.546. Analyse der Anforderungen an neue Anwendungen
M 2.547. Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen
M 2.548. Erstellung eines Lastenheftes
M 2.549. Erstellung eines Mandantenkonzeptes
M 2.550. Geeignete Steuerung der Anwendungsentwicklung
M 2.551. Durchführung eines geeigneten und rechtskonformen Vergabeverfahrens
M 2.552. Erstellung eines Pflichtenheftes
M 2.553. Entwicklung eines Pflegekonzeptes für Anwendungen
M 2.554. Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen
M 2.555. Entwicklung eines Authentisierungskonzeptes für Anwendungen
M 2.556. Planung und Umsetzung von Test und Freigabe von Anwendungen
M 2.557. Konzeption eines Schulungsprogramms zur Informationssicherheit
M 2.558. Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs
M 2.559. Beschaffung von Windows 8
M 2.560. Integration eines SOA-basierten Need-to-share-Konzepts in das Sicherheitsmanagement
M 2.561. Erstellen spezifikationskonformer SOA-Implementierungen und Konfigurationen
M 2.562. Regelung des Einsatzes von eingebetteten Systemen
M 2.563. Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme
M 2.564. Beschaffungskriterien für eingebettete Systeme

M 2.565. Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen
M 2.566. Sichere Aussonderung eines eingebetteten Systems
M 2.567. Auswahl vertrauenswürdiger Entwicklungswerkzeuge
M 2.568. Testverfahren für Software
M 2.569. Definition von Rollen und Verantwortlichkeiten bei der Software-Entwicklung
M 2.570. Auswahl eines Vorgehensmodells zur Software-Entwicklung
M 2.571. Berücksichtigung von Compliance-Anforderungen für die Software-Entwicklung
M 2.572. Beschaffung von Werkzeugen zur Software-Entwicklung
M 2.573. Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung
M 2.574. Ausführliche Dokumentation der Software-Entwicklung
M 2.575. Regelmäßige Sicherheitsaudits für die Software-Entwicklungsumgebung
M 2.576. Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen
M 2.577. Auswahl geeigneter Kryptoverfahren für Netze
M 2.578. Installation, Konfiguration und Betreuung eines lokalen Netzes durch Dritte
M 2.579. Regelmäßige Audits des lokalen Netzes
M 2.580. Außerbetriebnahme von Netzkomponenten
M 2.581. Aufbau eines Administrationsnetzes für das Netzmanagement
M 2.582. Möglichkeiten zur Einrichtung eines Managementnetzes
M 2.583. Geeignete Auswahl eines Netzmanagement-Systems
M 2.584. Geregelte Außerbetriebnahme eines Netz- und Systemmanagement-Tools
M 2.585. Konzeption eines Identitäts- und Berechtigungsmanagements
M 2.586. Einrichtung, Änderung und Entzug von Berechtigungen
M 2.587. Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement

M 3 Personal
M 3.1. Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
M 3.2. Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
M 3.3. Vertretungsregelungen
M 3.4. Schulung vor Programmnutzung
M 3.5. Schulung zu Sicherheitsmaßnahmen
M 3.6. Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
M 3.7. Anlaufstelle bei persönlichen Problemen
M 3.8. Vermeidung von Störungen des Betriebsklimas
M 3.9. Ergonomischer Arbeitsplatz
M 3.10. Auswahl eines vertrauenswürdigen Administrators und Vertreters
M 3.11. Schulung des Wartungs- und Administrationspersonals
M 3.12. Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne

M 3.13. Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
M 3.14. Einweisung des Personals in den geregelten Ablauf der Informationsweitergabe und des Datenträgeraustausches
M 3.15. Informationen für alle Mitarbeiter über die Faxnutzung
M 3.16. Einweisung in die Bedienung des Anrufbeantworters
M 3.17. Einweisung des Personals in die Modem-Benutzung
M 3.18. Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
M 3.19. Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
M 3.20. Einweisung in die Bedienung von Schutzschränken
M 3.21. Sicherheitstechnische Einweisung der Telearbeiter
M 3.22. Vertretungsregelung für Telearbeit
M 3.23. Einführung in kryptographische Grundbegriffe
M 3.24. Schulung zur Lotus Notes Systemarchitektur für Administratoren
M 3.25. Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
M 3.26. Einweisung des Personals in den sicheren Umgang mit IT
M 3.27. Schulung zur Active Directory-Verwaltung
M 3.28. Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen
M 3.29. Schulung zur Administration von Novell eDirectory
M 3.30. Schulung zum Einsatz von Novell eDirectory Clientsoftware
M 3.31. Schulung zur Systemarchitektur und Sicherheit von Exchange-Systemen für Administratoren
M 3.32. Schulung zu Sicherheitsmechanismen von Outlook für Benutzer
M 3.33. Sicherheitsüberprüfung von Mitarbeitern
M 3.34. Einweisung in die Administration des Archivsystems
M 3.35. Einweisung der Benutzer in die Bedienung des Archivsystems
M 3.36. Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
M 3.37. Schulung der Administratoren eines Apache-Webservers
M 3.38. Administratorenschulung für Router und Switches
M 3.39. Einführung in die zSeries-Plattform
M 3.40. Einführung in das z/OS-Betriebssystem
M 3.41. Einführung in Linux und z/VM für zSeries-Systeme
M 3.42. Schulung des z/OS-Bedienungspersonals
M 3.43. Schulung der Administratoren des Sicherheitsgateways
M 3.44. Sensibilisierung des Managements für Informationssicherheit
M 3.45. Planung von Schulungsinhalten zur Informationssicherheit
M 3.46. Ansprechpartner zu Sicherheitsfragen
M 3.47. Durchführung von Planspielen zur Informationssicherheit
M 3.48. Auswahl von Trainern oder externen Schulungsanbietern
M 3.49. Schulung zur Vorgehensweise nach IT-Grundschutz
M 3.50. Auswahl von Personal
M 3.51. Geeignetes Konzept für Personaleinsatz und -qualifizierung
M 3.52. Schulung zu SAP Systemen
M 3.53. Einführung in SAP Systeme
M 3.54. Schulung der Administratoren des Speichersystems

M 3.55. Vertraulichkeitsvereinbarungen
M 3.56. Schulung der Administratoren für die Nutzung von VoIP
M 3.57. Szenarien für den Einsatz von VoIP
M 3.58. Einführung in WLAN-Grundbegriffe
M 3.59. Schulung zum sicheren WLAN-Einsatz
M 3.60. Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten
M 3.61. Einführung in Verzeichnisdienst-Grundlagen
M 3.62. Schulung zur Administration von Verzeichnisdiensten
M 3.63. Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten
M 3.64. Einführung in Active Directory
M 3.65. Einführung in VPN-Grundbegriffe
M 3.66. Grundbegriffe des Patch- und Änderungsmanagements
M 3.67. Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten
M 3.68. Schulung der Administratoren eines Samba-Servers
M 3.69. Einführung in die Bedrohung durch Schadprogramme
M 3.70. Einführung in die Virtualisierung
M 3.71. Schulung der Administratoren virtueller Umgebungen
M 3.72. Grundbegriffe der Virtualisierungstechnik
M 3.73. Schulung der Administratoren eines DNS-Servers
M 3.74. Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren
M 3.75. Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer
M 3.76. Einweisung der Benutzer in den Einsatz von Groupware und E-Mail
M 3.77. Sensibilisierung zur sicheren Internet-Nutzung
M 3.78. Korrektes Auftreten im Internet
M 3.79. Einführung in Grundbegriffe und Funktionsweisen von Bluetooth
M 3.80. Sensibilisierung für die Nutzung von Bluetooth
M 3.81. Schulung zum sicheren Terminalserver-Einsatz
M 3.82. Schulung zur sicheren Nutzung von TK-Anlagen
M 3.83. Analyse sicherheitsrelevanter personeller Faktoren
M 3.84. Einführung in Exchange-Systeme
M 3.85. Einführung in OpenLDAP
M 3.86. Schulung der Administratoren von OpenLDAP
M 3.87. Einführung in Lotus Notes/Domino
M 3.88. Zielgruppenspezifische Schulungen zu Lotus Notes/Domino
M 3.89. Schulung zur Administration der Protokollierung
M 3.90. Allgemeine Grundlagen für die zentrale Protokollierung
M 3.91. Schulung der Administratoren von Cloud-Infrastrukturen
M 3.92. Grundlegende Begriffe beim Einsatz von Speicherlösungen
M 3.93. Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme
M 3.94. Messung und Auswertung des Lernerfolgs
M 3.95. Lernstoffsicherung

M 3.96. Unterstützung des Managements für Sensibilisierung und Schulung
M 3.97. Schulung des Projektteams für die Software-Entwicklung
M 3.98. Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen

M 4 Hardware und Software

M 4.1. Passwortschutz für IT-Systeme
M 4.2. Bildschirmsperre
M 4.3. Einsatz von Viren-Schutzprogrammen
M 4.4. Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
M 4.5. Protokollierung bei TK-Anlagen
M 4.6. Revision der TK-Anlagenkonfiguration
M 4.7. Änderung voreingestellter Passwörter
M 4.8. Schutz des TK-Bedienplatzes
M 4.9. Einsatz der Sicherheitsmechanismen von X-Window
M 4.10. Schutz der TK-Endgeräte
M 4.11. Absicherung der TK-Anlagen-Schnittstellen
M 4.12. Sperren nicht benötigter TK-Leistungsmerkmale
M 4.13. Sorgfältige Vergabe von IDs
M 4.14. Obligatorischer Passwortschutz unter Unix
M 4.15. Gesichertes Login
M 4.16. Zugangsbeschränkungen für Benutzer-Kennungen und / oder Terminals
M 4.17. Sperren und Löschen nicht benötigter Accounts und Terminals
M 4.18. Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
M 4.19. Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
M 4.20. Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
M 4.21. Verhinderung des unautorisierten Erlangens von Administratorrechten
M 4.22. Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
M 4.23. Sicherer Aufruf ausführbarer Dateien
M 4.24. Sicherstellung einer konsistenten Systemverwaltung
M 4.25. Einsatz der Protokollierung im Unix-System
M 4.26. Regelmäßiger Sicherheitscheck des Unix-Systems
M 4.27. Zugriffsschutz am Laptop
M 4.28. Software-Reinstallation bei Benutzerwechsel eines Laptops
M 4.29. Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme
M 4.30. Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
M 4.31. Sicherstellung der Energieversorgung im mobilen Einsatz
M 4.32. Physikalisches Löschen der Datenträger vor und nach Verwendung
M 4.33. Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung

M 4.34. Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
M 4.35. Verifizieren der zu übertragenden Daten vor Versand
M 4.36. Sperren bestimmter Faxempfänger-Rufnummern
M 4.37. Sperren bestimmter Absender-Faxnummern
M 4.38. Abschalten nicht benötigter Leistungsmerkmale
M 4.39. Abschalten des Anrufbeantworters bei Anwesenheit
M 4.40. Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras
M 4.41. Einsatz angemessener Sicherheitsprodukte für IT-Systeme
M 4.42. Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
M 4.43. Faxgerät mit automatischer Eingangskuvertierung
M 4.44. Prüfung eingehender Dateien auf Makro-Viren
M 4.45. Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
M 4.46. Nutzung des Anmeldepasswortes unter WfW und Windows 95
M 4.47. Protokollierung der Sicherheitsgateway-Aktivitäten
M 4.48. Passwortschutz unter Windows-Systemen
M 4.49. Absicherung des Boot-Vorgangs für ein Windows-System
M 4.50. Strukturierte Systemverwaltung unter Windows NT
M 4.51. Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
M 4.52. Geräteschutz unter NT-basierten Windows-Systemen
M 4.53. Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
M 4.54. Protokollierung unter Windows NT
M 4.55. Sichere Installation von Windows NT
M 4.56. Sicheres Löschen unter Windows-Betriebssystemen
M 4.57. Deaktivieren der automatischen CD-ROM-Erkennung
M 4.58. Freigabe von Verzeichnissen unter Windows 95
M 4.59. Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
M 4.60. Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
M 4.61. Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
M 4.62. Einsatz eines D-Kanal-Filters
M 4.63. Sicherheitstechnische Anforderungen an den Telearbeitsrechner
M 4.64. Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
M 4.65. Test neuer Hard- und Software
M 4.66. Novell Netware - Sicherer Übergang ins Jahr 2000
M 4.67. Sperren und Löschen nicht benötigter Datenbank-Accounts
M 4.68. Sicherstellung einer konsistenten Datenbankverwaltung
M 4.69. Regelmäßiger Sicherheitscheck der Datenbank
M 4.70. Durchführung einer Datenbanküberwachung
M 4.71. Restriktive Handhabung von Datenbank-Links
M 4.72. Datenbank-Verschlüsselung
M 4.73. Festlegung von Obergrenzen für selektierbare Datensätze

M 4.74. Vernetzte Windows 95 Rechner
M 4.75. Schutz der Registry unter Windows-Systemen
M 4.76. Sichere Systemversion von Windows NT
M 4.77. Schutz der Administratorkonten unter Windows NT
M 4.78. Sorgfältige Durchführung von Konfigurationsänderungen
M 4.79. Sichere Zugriffsmechanismen bei lokaler Administration
M 4.80. Sichere Zugriffsmechanismen bei Fernadministration
M 4.81. Audit und Protokollierung der Aktivitäten im Netz
M 4.82. Sichere Konfiguration der aktiven Netzkomponenten
M 4.83. Update/Upgrade von Soft- und Hardware im Netzbereich
M 4.84. Nutzung der BIOS-Sicherheitsmechanismen
M 4.85. Geeignetes Schnittstellendesign bei Kryptomodulen
M 4.86. Sichere Rollenteilung und Konfiguration der Kryptomodule
M 4.87. Physikalische Sicherheit von Kryptomodulen
M 4.88. Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen
M 4.89. Abstrahlsicherheit
M 4.90. Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells
M 4.91. Sichere Installation eines Systemmanagementsystems
M 4.92. Sicherer Betrieb eines Systemmanagementsystems
M 4.93. Regelmäßige Integritätsprüfung
M 4.94. Schutz der Webserver-Dateien
M 4.95. Minimales Betriebssystem
M 4.96. Abschaltung von DNS
M 4.97. Ein Dienst pro Server
M 4.98. Kommunikation durch Paketfilter auf Minimum beschränken
M 4.99. Schutz gegen nachträgliche Veränderungen von Informationen
M 4.100. Sicherheitsgateways und aktive Inhalte
M 4.101. Sicherheitsgateways und Verschlüsselung
M 4.102. C2-Sicherheit unter Novell 4.11
M 4.103. DHCP-Server unter Novell Netware 4.x
M 4.104. LDAP Services for NDS
M 4.105. Erste Maßnahmen nach einer Unix-Standardinstallation
M 4.106. Aktivieren der Systemprotokollierung
M 4.107. Nutzung von Hersteller- und Entwickler-Ressourcen
M 4.108. Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11
M 4.109. Software-Reinstallation bei Arbeitsplatzrechnern
M 4.110. Sichere Installation des RAS-Systems
M 4.111. Sichere Konfiguration des RAS-Systems
M 4.112. Sicherer Betrieb des RAS-Systems
M 4.113. Nutzung eines Authentisierungsservers bei Remote-Access-VPNs
M 4.114. Nutzung der Sicherheitsmechanismen von Mobiltelefonen
M 4.115. Sicherstellung der Energieversorgung von Mobiltelefonen
M 4.116. Sichere Installation von Lotus Notes/Domino
M 4.117. Sichere Konfiguration eines Lotus Notes Servers

M 4.118. Konfiguration als Lotus Notes Server
M 4.119. Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
M 4.120. Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken
M 4.121. Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes
M 4.122. Konfiguration für den Browser-Zugriff auf Lotus Notes
M 4.123. Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes
M 4.124. Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
M 4.125. Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
M 4.126. Sichere Konfiguration eines Lotus Notes Clients
M 4.127. Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes
M 4.128. Sicherer Betrieb der Lotus Notes/Domino-Umgebung
M 4.129. Sicherer Umgang mit Notes-ID-Dateien
M 4.130. Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken
M 4.131. Verschlüsselung von Lotus Notes Datenbanken
M 4.132. Überwachung der Lotus Notes/Domino-Umgebung
M 4.133. Geeignete Auswahl von Authentikationsmechanismen
M 4.134. Wahl geeigneter Datenformate
M 4.135. Restriktive Vergabe von Zugriffsrechten auf Systemdateien
M 4.136. Sichere Installation von Windows 2000
M 4.137. Sichere Konfiguration von Windows 2000
M 4.138. Konfiguration von Windows Server als Domänen-Controller
M 4.139. Konfiguration von Windows 2000 als Server
M 4.140. Sichere Konfiguration wichtiger Windows 2000 Dienste
M 4.141. Sichere Konfiguration des DDNS unter Windows 2000
M 4.142. Sichere Konfiguration des WINS unter Windows 2000
M 4.143. Sichere Konfiguration des DHCP unter Windows 2000
M 4.144. Nutzung der Windows 2000 CA
M 4.145. Sichere Konfiguration von RRAS unter Windows 2000
M 4.146. Sicherer Betrieb von Windows Client-Betriebssystemen
M 4.147. Sichere Nutzung von EFS unter Windows
M 4.148. Überwachung eines Windows 2000/XP Systems
M 4.149. Datei- und Freigabeberechtigungen unter Windows
M 4.150. Konfiguration von Windows 2000 als Workstation
M 4.151. Sichere Installation von Internet-PCs
M 4.152. Sicherer Betrieb von Internet-PCs
M 4.153. Sichere Installation von Novell eDirectory
M 4.154. Sichere Installation der Novell eDirectory Clientsoftware
M 4.155. Sichere Konfiguration von Novell eDirectory
M 4.156. Sichere Konfiguration der Novell eDirectory Clientsoftware
M 4.157. Einrichten von Zugriffsberechtigungen auf Novell eDirectory
M 4.158. Einrichten des LDAP-Zugriffs auf Novell eDirectory
M 4.159. Sicherer Betrieb von Novell eDirectory
M 4.160. Überwachen von Novell eDirectory

M 4.161. Sichere Installation von Exchange-Systemen
M 4.162. Sichere Konfiguration von Exchange-Servern
M 4.163. Zugriffsrechte auf Exchange-Objekte
M 4.164. Browser-Zugriff auf Exchange 2000
M 4.165. Sichere Konfiguration von Outlook
M 4.166. Sicherer Betrieb von Exchange-Systemen
M 4.167. Überwachung und Protokollierung von Exchange 2000 Systemen
M 4.168. Auswahl eines geeigneten Archivsystems
M 4.169. Verwendung geeigneter Archivmedien
M 4.170. Auswahl geeigneter Datenformate für die Archivierung von Dokumenten
M 4.171. Schutz der Integrität der Index-Datenbank von Archivsystemen
M 4.172. Protokollierung der Archivzugriffe
M 4.173. Regelmäßige Funktions- und Recoverytests bei der Archivierung
M 4.174. Vorbereitung der Installation von Windows NT/2000 für den IIS
M 4.175. Sichere Konfiguration von Windows NT/2000 für den IIS
M 4.176. Auswahl einer Authentisierungsmethode für Webangebote
M 4.177. Sicherstellung der Integrität und Authentizität von Softwarepaketen
M 4.178. Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz
M 4.179. Schutz von sicherheitskritischen Dateien beim IIS-Einsatz
M 4.180. Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS
M 4.181. Ausführen des IIS in einem separaten Prozess
M 4.182. Überwachen des IIS-Systems
M 4.183. Sicherstellen der Verfügbarkeit und Performance des IIS
M 4.184. Deaktivieren nicht benötigter Dienste beim IIS-Einsatz
M 4.185. Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz
M 4.186. Entfernen von Beispieldateien und Administrations-Scripts des IIS
M 4.187. Entfernen der FrontPage Server-Erweiterung des IIS
M 4.188. Prüfen der Benutzereingaben beim IIS-Einsatz
M 4.189. Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz
M 4.190. Entfernen der RDS-Unterstützung des IIS
M 4.191. Überprüfung der Integrität und Authentizität der Apache-Pakete
M 4.192. Konfiguration des Betriebssystems für einen Apache-Webserver
M 4.193. Sichere Installation eines Apache-Webservers
M 4.194. Sichere Grundkonfiguration eines Apache-Webservers
M 4.195. Konfiguration der Zugriffssteuerung beim Apache-Webserver
M 4.196. Sicherer Betrieb eines Apache-Webservers
M 4.197. Servererweiterungen für dynamische Webseiten beim Apache-Webserver
M 4.198. Installation einer Applikation in einem chroot Käfig
M 4.199. Vermeidung problematischer Dateiformate
M 4.200. Umgang mit USB-Speichermedien
M 4.201. Sichere lokale Grundkonfiguration von Routern und Switches
M 4.202. Sichere Netz-Grundkonfiguration von Routern und Switches

M 4.203. Konfigurations-Checkliste für Router und Switches
M 4.204. Sichere Administration von Routern und Switches
M 4.205. Protokollierung bei Routern und Switches
M 4.206. Sicherung von Switch-Ports
M 4.207. Einsatz und Sicherung systemnaher z/OS-Terminals
M 4.208. Absichern des Start-Vorgangs von z/OS-Systemen
M 4.209. Sichere Grundkonfiguration von z/OS-Systemen
M 4.210. Sicherer Betrieb des z/OS-Betriebssystems
M 4.211. Einsatz des z/OS-Sicherheitssystems RACF
M 4.212. Absicherung von Linux für zSeries
M 4.213. Absichern des Login-Vorgangs unter z/OS
M 4.214. Datenträgerverwaltung unter z/OS-Systemen
M 4.215. Absicherung sicherheitskritischer z/OS-Dienstprogramme
M 4.216. Festlegung der Systemgrenzen von z/OS
M 4.217. Workload Management für z/OS-Systeme
M 4.218. Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen
M 4.219. Lizenzschlüssel-Management für z/OS-Software
M 4.220. Absicherung von Unix System Services bei z/OS-Systemen
M 4.221. Parallel-Sysplex unter z/OS
M 4.222. Festlegung geeigneter Einstellungen von Sicherheitsproxies
M 4.223. Integration von Proxy-Servern in das Sicherheitsgateway
M 4.224. Integration von VPN-Komponenten in ein Sicherheitsgateway
M 4.225. Einsatz eines Protokollierungsservers in einem Sicherheitsgateway
M 4.226. Integration von Virenscannern in ein Sicherheitsgateway
M 4.227. Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation
M 4.228. Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs
M 4.229. Sicherer Betrieb von Smartphones, Tablets und PDAs
M 4.230. Zentrale Administration von Smartphones, Tablets und PDAs
M 4.231. Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs
M 4.232. Sichere Nutzung von Zusatzspeicherkarten
M 4.233. Sperrung nicht mehr benötigter RAS-Zugänge
M 4.234. Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
M 4.235. Abgleich der Datenbestände von Laptops
M 4.236. Zentrale Administration von Laptops
M 4.237. Sichere Grundkonfiguration eines IT-Systems
M 4.238. Einsatz eines lokalen Paketfilters
M 4.239. Sicherer Betrieb eines Servers
M 4.240. Einrichten einer Testumgebung für einen Server
M 4.241. Sicherer Betrieb von Clients
M 4.242. Einrichten einer Referenzinstallation für Clients
M 4.243. Verwaltungswerkzeuge unter Windows Client-Betriebssystemen
M 4.244. Sichere Systemkonfiguration von Windows Client-Betriebssystemen
M 4.245. Basiseinstellungen für Windows Group Policy Objects
M 4.246. Konfiguration der Systemdienste auf Clients ab Windows XP

M 4.247. Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista
M 4.248. Sichere Installation von Windows Client-Betriebssystemen
M 4.249. Windows Client-Systeme aktuell halten
M 4.250. Auswahl eines zentralen, netzbasierten Authentisierungsdienstes
M 4.251. Arbeiten mit fremden IT-Systemen
M 4.252. Sichere Konfiguration von Schulungsrechnern
M 4.253. Schutz vor Spyware
M 4.254. Sicherer Einsatz von drahtlosen Tastaturen und Mäusen
M 4.255. Nutzung von IrDA-Schnittstellen
M 4.256. Sichere Installation von SAP Systemen
M 4.257. Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene
M 4.258. Sichere Konfiguration des SAP ABAP-Stacks
M 4.259. Sicherer Einsatz der ABAP-Stack Benutzerverwaltung
M 4.260. Berechtigungsverwaltung für SAP Systeme
M 4.261. Sicherer Umgang mit kritischen SAP Berechtigungen
M 4.262. Konfiguration zusätzlicher SAP Berechtigungsprüfungen
M 4.263. Absicherung von SAP Destinationen
M 4.264. Einschränkung von direkten Tabellenveränderungen in SAP Systemen
M 4.265. Sichere Konfiguration der Batch-Verarbeitung im SAP System
M 4.266. Sichere Konfiguration des SAP Java-Stacks
M 4.267. Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung
M 4.268. Sichere Konfiguration der SAP Java-Stack Berechtigungen
M 4.269. Sichere Konfiguration der SAP System Datenbank
M 4.270. SAP Protokollierung
M 4.271. Virenschutz für SAP Systeme
M 4.272. Sichere Nutzung des SAP Transportsystems
M 4.273. Sichere Nutzung der SAP Java-Stack Software-Verteilung
M 4.274. Sichere Grundkonfiguration von Speichersystemen
M 4.275. Sicherer Betrieb einer Speicherlösung
M 4.276. Planung des Einsatzes von Windows Server 2003
M 4.277. Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern
M 4.278. Sichere Nutzung von EFS unter Windows Server 2003
M 4.279. Erweiterte Sicherheitsaspekte für Windows Server 2003
M 4.280. Sichere Basiskonfiguration ab Windows Server 2003
M 4.281. Sichere Installation und Bereitstellung von Windows Server 2003
M 4.282. Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003
M 4.283. Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003
M 4.284. Umgang mit Diensten ab Windows Server 2003
M 4.285. Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003

M 4.286. Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003
M 4.287. Sichere Administration der VoIP-Middleware
M 4.288. Sichere Administration von VoIP-Endgeräten
M 4.289. Einschränkung der Erreichbarkeit über VoIP
M 4.290. Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP
M 4.291. Sichere Konfiguration der VoIP-Middleware
M 4.292. Protokollierung bei VoIP
M 4.293. Sicherer Betrieb von Hotspots
M 4.294. Sichere Konfiguration der Access Points
M 4.295. Sichere Konfiguration der WLAN-Clients
M 4.296. Einsatz einer geeigneten WLAN-Management-Lösung
M 4.297. Sicherer Betrieb der WLAN-Komponenten
M 4.298. Regelmäßige Audits der WLAN-Komponenten
M 4.299. Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten
M 4.300. Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten
M 4.301. Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte
M 4.302. Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten
M 4.303. Einsatz von netzfähigen Dokumentenscannern
M 4.304. Verwaltung von Druckern
M 4.305. Einsatz von Speicherbeschränkungen (Quotas)
M 4.306. Umgang mit Passwort-Speicher-Tools
M 4.307. Sichere Konfiguration von Verzeichnisdiensten
M 4.308. Sichere Installation von Verzeichnisdiensten
M 4.309. Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste
M 4.310. Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste
M 4.311. Sicherer Betrieb von Verzeichnisdiensten
M 4.312. Überwachung von Verzeichnisdiensten
M 4.313. Bereitstellung von sicheren Domänen-Controllern
M 4.314. Sichere Richtlinieneinstellungen für Domänen und Domänen-Controller
M 4.315. Aufrechterhaltung der Betriebssicherheit von Active Directory
M 4.316. Überwachung der Active Directory Infrastruktur
M 4.317. Sichere Migration von Windows Verzeichnisdiensten
M 4.318. Umsetzung sicherer Verwaltungsmethoden für Active Directory
M 4.319. Sichere Installation von VPN-Endgeräten
M 4.320. Sichere Konfiguration eines VPNs
M 4.321. Sicherer Betrieb eines VPNs
M 4.322. Sperrung nicht mehr benötigter VPN-Zugänge
M 4.323. Synchronisierung innerhalb des Patch- und Änderungsmanagements
M 4.324. Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement
M 4.325. Löschen von Auslagerungsdateien

M 4.326. Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver
M 4.327. Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen
M 4.328. Sichere Grundkonfiguration eines Samba-Servers
M 4.329. Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers
M 4.330. Sichere Installation eines Samba-Servers
M 4.331. Sichere Konfiguration des Betriebssystems für einen Samba-Server
M 4.332. Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server
M 4.333. Sichere Konfiguration von Winbind unter Samba
M 4.334. SMB Message Signing und Samba
M 4.335. Sicherer Betrieb eines Samba-Servers
M 4.336. Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag
M 4.337. Einsatz von BitLocker Drive Encryption
M 4.338. Einsatz von File und Registry Virtualization bei Clients ab Windows Vista
M 4.339. Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista
M 4.340. Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista
M 4.341. Integritätsschutz ab Windows Vista
M 4.342. Aktivierung des Last Access Zeitstempels ab Windows Vista
M 4.343. Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag
M 4.344. Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008
M 4.345. Schutz vor unerwünschten Informationsabflüssen
M 4.346. Sichere Konfiguration virtueller IT-Systeme
M 4.347. Deaktivierung von Snapshots virtueller IT-Systeme
M 4.348. Zeitsynchronisation in virtuellen IT-Systemen
M 4.349. Sicherer Betrieb von virtuellen Infrastrukturen
M 4.350. Sichere Grundkonfiguration eines DNS-Servers
M 4.351. Absicherung von Zonentransfers
M 4.352. Absicherung von dynamischen DNS-Updates
M 4.353. Einsatz von DNSSEC
M 4.354. Überwachung eines DNS-Servers
M 4.355. Berechtigungsverwaltung für Groupware-Systeme
M 4.356. Sichere Installation von Groupware-Systemen
M 4.357. Sicherer Betrieb von Groupware-Systemen
M 4.358. Protokollierung von Groupware-Systemen
M 4.359. Überblick über Komponenten eines Webservers
M 4.360. Sichere Konfiguration eines Webservers
M 4.361. Sichere Konfiguration von Webanwendungen
M 4.362. Sichere Konfiguration von Bluetooth

M 4.363. Sicherer Betrieb von Bluetooth-Geräten
M 4.364. Regelungen für die Aussonderung von Bluetooth-Geräten
M 4.365. Nutzung eines Terminalservers als grafische Firewall
M 4.366. Sichere Konfiguration von beweglichen Benutzerprofilen in Terminalserver-Umgebungen
M 4.367. Sichere Verwendung von Client-Applikationen für Terminalserver
M 4.368. Regelmäßige Audits der Terminalserver-Umgebung
M 4.369. Sicherer Betrieb eines Anrufbeantworters
M 4.370. Einsatz von Anoubis unter Unix
M 4.371. Konfiguration von Mac OS X Clients
M 4.372. Einsatz von FileVault unter Mac OS X
M 4.373. Deaktivierung nicht benötigter Hardware unter Mac OS X
M 4.374. Zugriffschutz der Benutzerkonten unter Mac OS X
M 4.375. Einsatz der Sandbox-Funktion unter Mac OS X
M 4.376. Festlegung von Passwortrichtlinien unter Mac OS X
M 4.377. Überprüfung der Signaturen von Mac OS X Anwendungen
M 4.378. Einschränkung der Programmzugriffe unter Mac OS X
M 4.379. Sichere Datenhaltung und sicherer Transport unter Mac OS X
M 4.380. Einsatz von Apple-Software-Restore unter Mac OS X
M 4.381. Verschlüsselung von Exchange-System-Datenbanken
M 4.382. Auswahl und Prüfung der OpenLDAP-Installationspakete
M 4.383. Sichere Installation von OpenLDAP
M 4.384. Sichere Konfiguration von OpenLDAP
M 4.385. Konfiguration der durch OpenLDAP verwendeten Datenbank
M 4.386. Einschränkung von Attributen bei OpenLDAP
M 4.387. Sichere Vergabe von Zugriffsrechten auf OpenLDAP
M 4.388. Sichere Authentisierung gegenüber OpenLDAP
M 4.389. Partitionierung und Replikation bei OpenLDAP
M 4.390. Sichere Aktualisierung von OpenLDAP
M 4.391. Sicherer Betrieb von OpenLDAP
M 4.392. Authentisierung bei Webanwendungen
M 4.393. Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services
M 4.394. Session-Management bei Webanwendungen und Web-Services
M 4.395. Fehlerbehandlung durch Webanwendungen und Web-Services
M 4.396. Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen
M 4.397. Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services
M 4.398. Sichere Konfiguration von Webanwendungen
M 4.399. Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen
M 4.400. Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services
M 4.401. Schutz vertraulicher Daten bei Webanwendungen
M 4.402. Zugriffskontrolle bei Webanwendungen

M 4.403. Verhinderung von Cross-Site Request Forgery (CSRF, XSRF, Session Riding)
M 4.404. Sicherer Entwurf der Logik von Webanwendungen
M 4.405. Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services
M 4.406. Verhinderung von Clickjacking
M 4.407. Protokollierung beim Einsatz von OpenLDAP
M 4.408. Übersicht über neue, sicherheitsrelevante Funktionen in Windows Server 2008
M 4.409. Beschaffung von Windows Server 2008
M 4.410. Einsatz von Netzwerkzugriffsschutz unter Windows
M 4.411. Sichere Nutzung von DirectAccess unter Windows
M 4.412. Sichere Migration von Windows Server 2003 auf Server 2008
M 4.413. Sicherer Einsatz von Virtualisierung mit Hyper-V
M 4.414. Überblick über Neuerungen für Active Directory ab Windows Server 2008
M 4.415. Sicherer Betrieb der biometrischen Authentisierung unter Windows
M 4.416. Einsatz von Windows Server Core
M 4.417. Patch-Management mit WSUS ab Windows Server 2008
M 4.418. Planung des Einsatzes von Windows Server 2008
M 4.419. Anwendungssteuerung ab Windows 7 mit AppLocker
M 4.420. Sicherer Einsatz des Wartungscenters unter Windows 7
M 4.421. Absicherung der Windows PowerShell
M 4.422. Nutzung von BitLocker To Go ab Windows 7
M 4.423. Verwendung der Heimnetzgruppen-Funktion ab Windows 7
M 4.424. Sicherer Einsatz älterer Software ab Windows 7
M 4.425. Verwendung der Tresor- und Cardspace-Funktion auf Clients ab Windows
M 4.426. Archivierung für die Lotus Notes/Domino-Umgebung
M 4.427. Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino
M 4.428. Audit der Lotus Notes/Domino-Umgebung
M 4.429. Sichere Konfiguration von Lotus Notes/Domino
M 4.430. Analyse von Protokolldaten
M 4.431. Auswahl und Verarbeitung relevanter Informationen für die Protokollierung
M 4.432. Sichere Konfiguration von Serverdiensten
M 4.433. Einsatz von Datenträgerverschlüsselung
M 4.434. Sicherer Einsatz von Appliances
M 4.435. Selbstverschlüsselnde Festplatten
M 4.436. Planung der Ressourcen für Cloud-Dienste
M 4.437. Planung von Cloud-Diensteprofilen
M 4.438. Auswahl von Cloud-Komponenten
M 4.439. Virtuelle Sicherheitsgateways (Firewalls) in Clouds
M 4.440. Verschlüsselte Speicherung von Cloud-Anwenderdaten
M 4.441. Multifaktor-Authentisierung für den Cloud-Benutzerzugriff
M 4.442. Zentraler Schutz vor Schadprogrammen in der Cloud-Infrastruktur

M 4.443. Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur
M 4.444. Patchmanagement für Cloud-Komponenten
M 4.445. Durchgängige Mandantentrennung von Cloud-Diensten
M 4.446. Einführung in das Cloud Management
M 4.447. Sicherstellung der Integrität der SAN-Fabric
M 4.448. Einsatz von Verschlüsselung für Speicherlösungen
M 4.449. Einführung eines Zonenkonzeptes
M 4.450. Absicherung der Kommunikation bei Web-Services
M 4.451. Aktuelle Web-Service Standards
M 4.452. Überwachung eines Web-Service
M 4.453. Einsatz eines Security Token Service (STS)
M 4.454. Schutz vor unerlaubter Nutzung von Web-Services
M 4.455. Autorisierung bei Web-Services
M 4.456. Authentisierung bei Web-Services
M 4.457. Sichere Mandantentrennung bei Webanwendungen und Web-Services
M 4.458. Planung des Einsatzes von Web-Services
M 4.459. Einsatz von Verschlüsselung bei Cloud-Nutzung
M 4.460. Einsatz von Federation Services
M 4.461. Portabilität von Cloud Services
M 4.462. Einführung in die Cloud-Nutzung
M 4.463. Sichere Installation einer Anwendung
M 4.464. Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb
M 4.465. Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs
M 4.466. Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs
M 4.467. Auswahl von Applikationen für Smartphones, Tablets und PDAs
M 4.468. Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs
M 4.469. Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion
M 4.470. Grundlagenwissen zu Windows 8
M 4.471. Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8
M 4.472. Datensparsamkeit bei Windows 8
M 4.473. Schutz vor Abhören von XML-Transportcontainern in einer SOA
M 4.474. Schutz vor Schwachstellen in Backend-Anwendungen einer SOA
M 4.475. Schutz vor Spoofing-Angriffen auf Identitätsdienste
M 4.476. Schutz einer WS-Notification-Subscription im Broker
M 4.477. Schutz einer WS-Notification
M 4.478. Schlüsselmittelverwaltung bei SOA
M 4.479. Schutz von Richtlinien in einer SOA
M 4.480. Schutz von WS-Resource in SOA-Umgebungen
M 4.481. Sichere Nutzung verbindungsloser SOAP-Kommunikation
M 4.482. Hardware-Realisierung von Funktionen eingebetteter Systeme

M 5.18. Einsatz der Sicherheitsmechanismen von NIS
M 5.19. Einsatz der Sicherheitsmechanismen von sendmail
M 5.20. Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
M 5.21. Sicherer Einsatz von telnet, ftp, tftp und rexec
M 5.22. Kompatibilitätsprüfung des Sender- und Empfängersystems
M 5.23. Auswahl einer geeigneten Versandart für Datenträger
M 5.24. Nutzung eines geeigneten Faxvorblattes
M 5.25. Nutzung von Sende- und Empfangsprotokollen
M 5.26. Telefonische Ankündigung einer Faxsendung
M 5.27. Telefonische Rückversicherung über korrekten Faxempfang
M 5.28. Telefonische Rückversicherung über korrekten Faxabsender
M 5.29. Gelegentliche Kontrolle programmierter Zieladressen und Protokolle
M 5.30. Aktivierung einer vorhandenen Callback-Option
M 5.31. Geeignete Modem-Konfiguration
M 5.32. Sicherer Einsatz von Kommunikationssoftware
M 5.33. Absicherung von Fernwartung
M 5.34. Einsatz von Einmalpasswörtern
M 5.35. Einsatz der Sicherheitsmechanismen von UUCP
M 5.36. Verschlüsselung unter Unix und Windows NT
M 5.37. Einschränken der Peer-to-Peer-Funktionalitäten in einem serverge-stützten Netz
M 5.38. Sichere Einbindung von DOS-PCs in ein Unix-Netz
M 5.39. Sicherer Einsatz der Protokolle und Dienste
M 5.40. Sichere Einbindung von DOS-PCs in ein Windows NT Netz
M 5.41. Sichere Konfiguration des Fernzugriffs unter Windows NT
M 5.42. Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT
M 5.43. Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT
M 5.44. Einseitiger Verbindungsaufbau
M 5.45. Sichere Nutzung von Browsern
M 5.46. Einsatz von Stand-alone-Systemen zur Nutzung des Internets
M 5.47. Einrichten einer Closed User Group
M 5.48. Authentisierung mittels CLIP/COLP
M 5.49. Callback basierend auf CLIP/COLP
M 5.50. Authentisierung mittels PAP/CHAP
M 5.51. Sicherheitstechnische Anforderungen an die Kommunikationsverbin-dung Telearbeitsrechner - Institution
M 5.52. Sicherheitstechnische Anforderungen an den Kommunikationsrech-ner
M 5.53. Schutz vor Mailbomben
M 5.54. Umgang mit unerwünschten E-Mails
M 5.55. Kontrolle von Alias-Dateien und Verteilerlisten
M 5.56. Sicherer Betrieb eines Mailservers
M 5.57. Sichere Konfiguration der Groupware-/Mail-Clients
M 5.58. Auswahl und Installation von Datenbankschnittstellen-Treibern
M 5.59. Schutz vor DNS-Spoofing bei Authentisierungsmechanismen
M 5.60. Auswahl einer geeigneten Backbone-Technologie
M 5.61. Geeignete physische Segmentierung

M 5.62. Geeignete logische Segmentierung
M 5.63. Einsatz von GnuPG oder PGP
M 5.64. Secure Shell
M 5.65. Einsatz von S-HTTP
M 5.66. Clientseitige Verwendung von SSL/TLS
M 5.67. Verwendung eines Zeitstempel-Dienstes
M 5.68. Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
M 5.69. Schutz vor aktiven Inhalten
M 5.70. Adreßumsetzung - NAT (Network Address Translation)
M 5.71. Intrusion Detection und Intrusion Response Systeme
M 5.72. Deaktivieren nicht benötigter Netzdienste
M 5.73. Sicherer Betrieb eines Faxservers
M 5.74. Pflege der Faxserver-Adressbücher und der Verteillisten
M 5.75. Schutz vor Überlastung des Faxservers
M 5.76. Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation
M 5.77. Bildung von Teilnetzen
M 5.78. Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung
M 5.79. Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung
M 5.80. Schutz vor Abhören der Raumgespräche über Mobiltelefone
M 5.81. Sichere Datenübertragung über Mobiltelefone
M 5.82. Sicherer Einsatz von SAMBA
M 5.83. Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN
M 5.84. Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
M 5.85. Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
M 5.86. Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes
M 5.87. Vereinbarung über die Anbindung an Netze Dritter
M 5.88. Vereinbarung über Datenaustausch mit Dritten
M 5.89. Konfiguration des sicheren Kanals unter Windows
M 5.90. Einsatz von IPSec unter Windows
M 5.91. Einsatz von Personal Firewalls für Clients
M 5.92. Sichere Internet-Anbindung von Internet-PCs
M 5.93. Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
M 5.94. Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
M 5.95. Sicherer E-Commerce bei der Nutzung von Internet-PCs
M 5.96. Sichere Nutzung von Webmail
M 5.97. Absicherung der Kommunikation mit Novell eDirectory
M 5.98. Schutz vor Missbrauch kostenpflichtiger Einwahlnummern
M 5.99. SSL/TLS-Absicherung für Exchange 2000
M 5.100. Absicherung der Kommunikation von und zu Exchange-Systemen
M 5.101. Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz
M 5.102. Installation von URL-Filtern beim IIS-Einsatz
M 5.103. Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz
M 5.104. Konfiguration des TCP/IP-Filters beim IIS-Einsatz
M 5.105. Vorbeugen vor SYN-Attacken auf den IIS

M 5.106. Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz
M 5.107. Verwendung von SSL im Apache-Webserver
M 5.108. Kryptographische Absicherung von Groupware bzw. E-Mail
M 5.109. Einsatz eines E-Mail-Scanners auf dem Mailserver
M 5.110. Absicherung von E-Mail mit SPHINX (S/MIME)
M 5.111. Einrichtung von Access Control Lists auf Routern
M 5.112. Sicherheitsaspekte von Routing-Protokollen
M 5.113. Einsatz des VTAM Session Management Exit unter z/OS
M 5.114. Absicherung der z/OS-Tracefunktionen
M 5.115. Integration eines Webservers in ein Sicherheitsgateway
M 5.116. Integration eines E-Mailservers in ein Sicherheitsgateway
M 5.117. Integration eines Datenbank-Servers in ein Sicherheitsgateway
M 5.118. Integration eines DNS-Servers in ein Sicherheitsgateway
M 5.119. Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway
M 5.120. Behandlung von ICMP am Sicherheitsgateway
M 5.121. Sichere Kommunikation von unterwegs
M 5.122. Sicherer Anschluss von Laptops an lokale Netze
M 5.123. Absicherung der Netzkommunikation unter Windows
M 5.124. Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen
M 5.125. Absicherung der Kommunikation von und zu SAP Systemen
M 5.126. Absicherung der SAP RFC-Schnittstelle
M 5.127. Absicherung des SAP Internet Connection Framework (ICF)
M 5.128. Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle
M 5.129. Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen
M 5.130. Absicherung des SANs durch Segmentierung
M 5.131. Absicherung von IP-Protokollen unter Windows Server 2003
M 5.132. Sicherer Einsatz von WebDAV unter Windows Server 2003
M 5.133. Auswahl eines VoIP-Signalisierungsprotokolls
M 5.134. Sichere Signalisierung bei VoIP
M 5.135. Sicherer Medientransport mit SRTP
M 5.136. Dienstgüte und Netzmanagement bei VoIP
M 5.137. Einsatz von NAT für VoIP
M 5.138. Einsatz von RADIUS-Servern
M 5.139. Sichere Anbindung eines WLANs an ein LAN
M 5.140. Aufbau eines Distribution Systems
M 5.141. Regelmäßige Sicherheitschecks in WLANs
M 5.142. Abnahme der IT-Verkabelung
M 5.143. Laufende Fortschreibung und Revision der Netzdokumentation
M 5.144. Rückbau der IT-Verkabelung
M 5.145. Sicherer Einsatz von CUPS
M 5.146. Netztrennung beim Einsatz von Multifunktionsgeräten
M 5.147. Absicherung der Kommunikation mit Verzeichnisdiensten
M 5.148. Sichere Anbindung eines externen Netzes mit OpenVPN

M 5.149. Sichere Anbindung eines externen Netzes mit IPSec
M 5.150. Durchführung von Penetrationstests
M 5.151. Sichere Konfiguration des Samba Web Administration Tools
M 5.152. Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste
M 5.153. Planung des Netzes für virtuelle Infrastrukturen
M 5.154. Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen
M 5.155. Datenschutz-Aspekte bei der Internet-Nutzung
M 5.156. Sichere Nutzung von Twitter
M 5.157. Sichere Nutzung von sozialen Netzwerken
M 5.158. Nutzung von Web-Speicherplatz
M 5.159. Übersicht über Protokolle und Kommunikationsstandards für Webserver
M 5.160. Authentisierung gegenüber Webservern
M 5.161. Erstellung von dynamischen Web-Angeboten
M 5.162. Planung der Leitungskapazitäten beim Einsatz von Terminalservern
M 5.163. Restriktive Rechtevergabe auf Terminalservern
M 5.164. Sichere Nutzung eines Terminalservers aus einem entfernten Netz
M 5.165. Deaktivieren nicht benötigter Mac OS X-Netzdienste
M 5.166. Konfiguration der Mac OS X Personal Firewall
M 5.167. Sicherheit beim Fernzugriff unter Mac OS X
M 5.168. Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services
M 5.169. Systemarchitektur einer Webanwendung
M 5.170. Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP
M 5.171. Sichere Kommunikation zu einem zentralen Protokollierungsserver
M 5.172. Sichere Zeitsynchronisation bei der zentralen Protokollierung
M 5.173. Nutzung von Kurz-URLs und QR-Codes
M 5.174. Absicherung der Kommunikation zum Cloud-Zugriff
M 5.175. Einsatz eines XML-Gateways
M 5.176. Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution
M 5.177. Serverseitige Verwendung von SSL/TLS

M 6 Notfallvorsorge
M 6.1. Erstellung einer Übersicht über Verfügbarkeitsanforderungen
M 6.2. Notfall-Definition, Notfall-Verantwortlicher
M 6.3. Erstellung eines Notfall-Handbuches
M 6.4. Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
M 6.5. Definition des eingeschränkten IT-Betriebs
M 6.6. Untersuchung interner und externer Ausweichmöglichkeiten
M 6.7. Regelung der Verantwortung im Notfall
M 6.8. Alarmierungsplan
M 6.9. Notfall-Pläne für ausgewählte Schadensereignisse
M 6.10. Notfall-Plan für DFÜ-Ausfall
M 6.11. Erstellung eines Wiederanlaufplans
M 6.12. Durchführung von Notfallübungen

M 6.13. Erstellung eines Datensicherungsplans
M 6.14. Ersatzbeschaffungsplan
M 6.15. Lieferantenvereinbarungen
M 6.16. Abschließen von Versicherungen
M 6.17. Alarmierungsplan und Brandschutzübungen
M 6.18. Redundante Leitungsführung
M 6.19. Datensicherung am PC
M 6.20. Geeignete Aufbewahrung der Backup-Datenträger
M 6.21. Sicherungskopie der eingesetzten Software
M 6.22. Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
M 6.23. Verhaltensregeln bei Auftreten von Schadprogrammen
M 6.24. Erstellen eines Notfall-Bootmediums
M 6.25. Regelmäßige Datensicherung der Server-Festplatte
M 6.26. Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
M 6.27. Sicheres Update des BIOS
M 6.28. Vereinbarung über Lieferzeiten lebensnotwendiger TK-Baugruppen
M 6.29. TK-Basisanschluss für Notrufe
M 6.30. Katastrophenschaltung
M 6.31. Verhaltensregeln nach Verlust der Systemintegrität
M 6.32. Regelmäßige Datensicherung
M 6.33. Entwicklung eines Datensicherungskonzepts
M 6.34. Erhebung der Einflussfaktoren der Datensicherung
M 6.35. Festlegung der Verfahrensweise für die Datensicherung
M 6.36. Festlegung des Minimaldatensicherungskonzeptes
M 6.37. Dokumentation der Datensicherung
M 6.38. Sicherungskopie der übermittelten Daten
M 6.39. Auflistung von Händleradressen zur Fax-Wiederbeschaffung
M 6.40. Regelmäßige Batterieprüfung/-wechsel
M 6.41. Übungen zur Datenrekonstruktion
M 6.42. Erstellung von Rettungsdisketten für Windows NT
M 6.43. Einsatz redundanter Windows-Server
M 6.44. Datensicherung unter Windows NT
M 6.45. Datensicherung unter Windows 95
M 6.46. Erstellung von Rettungsdisketten für Windows 95
M 6.47. Datensicherung bei der Telearbeit
M 6.48. Verhaltensregeln nach Verlust der Datenbankintegrität
M 6.49. Datensicherung einer Datenbank
M 6.50. Archivierung von Datenbeständen
M 6.51. Wiederherstellung einer Datenbank
M 6.52. Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
M 6.53. Redundante Auslegung der Netzkomponenten
M 6.54. Verhaltensregeln nach Verlust der Netzintegrität
M 6.55. Reduzierung der Wiederanlaufzeit für Novell Netware Server
M 6.56. Datensicherung bei Einsatz kryptographischer Verfahren
M 6.57. Erstellen eines Notfallplans für den Ausfall des Managementsystems

M 6.58. Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen
M 6.59. Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen
M 6.60. Festlegung von Meldewegen für Sicherheitsvorfälle
M 6.61. Eskalationsstrategie für Sicherheitsvorfälle
M 6.62. Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen
M 6.63. Untersuchung und Bewertung eines Sicherheitsvorfalls
M 6.64. Behebung von Sicherheitsvorfällen
M 6.65. Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
M 6.66. Nachbereitung von Sicherheitsvorfällen
M 6.67. Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
M 6.68. Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen
M 6.69. Notfallvorsorge und Ausfallsicherheit bei Faxservern
M 6.70. Erstellen eines Notfallplans für den Ausfall des RAS-Systems
M 6.71. Datensicherung bei mobiler Nutzung des IT-Systems
M 6.72. Ausfallvorsorge bei Mobiltelefonen
M 6.73. Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung
M 6.74. Notfallarchiv
M 6.75. Redundante Kommunikationsverbindungen
M 6.76. Erstellen eines Notfallplans für den Ausfall von Windows-Systemen
M 6.77. Erstellung von Rettungsdisketten für Windows 2000
M 6.78. Datensicherung unter Windows Clients
M 6.79. Datensicherung beim Einsatz von Internet-PCs
M 6.80. Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes
M 6.81. Erstellen von Datensicherungen für Novell eDirectory
M 6.82. Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen
M 6.83. Notfallvorsorge beim Outsourcing
M 6.84. Regelmäßige Datensicherung der System- und Archivdaten
M 6.85. Erstellung eines Notfallplans für den Ausfall des IIS
M 6.86. Schutz vor schädlichem Code auf dem IIS
M 6.87. Datensicherung auf dem IIS
M 6.88. Erstellen eines Notfallplans für den Webserver
M 6.89. Notfallvorsorge für einen Apache-Webserver
M 6.90. Datensicherung und Archivierung bei Groupware und E-Mail
M 6.91. Datensicherung und Recovery bei Routern und Switches
M 6.92. Notfallvorsorge bei Routern und Switches
M 6.93. Notfallvorsorge für z/OS-Systeme
M 6.94. Notfallvorsorge bei Sicherheitsgateways
M 6.95. Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs
M 6.96. Notfallvorsorge für einen Server
M 6.97. Notfallvorsorge für SAP Systeme
M 6.98. Notfallvorsorge und Notfallreaktion für Speicherlösungen

M 6.99. Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server
M 6.100. Erstellung eines Notfallplans für den Ausfall von VoIP
M 6.101. Datensicherung bei VoIP
M 6.102. Verhaltensregeln bei WLAN-Sicherheitsvorfällen
M 6.103. Redundanzen für die Primärverkabelung
M 6.104. Redundanzen für die Gebäudeverkabelung
M 6.105. Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten
M 6.106. Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes
M 6.107. Erstellung von Datensicherungen für Verzeichnisdienste
M 6.108. Datensicherung für Domänen-Controller
M 6.109. Notfallplan für den Ausfall eines VPNs
M 6.110. Festlegung des Geltungsbereichs und der Notfallmanagementstrategie
M 6.111. Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene
M 6.112. Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement
M 6.113. Bereitstellung angemessener Ressourcen für das Notfallmanagement
M 6.114. Erstellung eines Notfallkonzepts
M 6.115. Integration der Mitarbeiter in den Notfallmanagement-Prozess
M 6.116. Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse
M 6.117. Tests und Notfallübungen
M 6.118. Überprüfung und Aufrechterhaltung der Notfallmaßnahmen
M 6.119. Dokumentation im Notfallmanagement-Prozess
M 6.120. Überprüfung und Steuerung des Notfallmanagement-Systems
M 6.121. Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
M 6.122. Definition eines Sicherheitsvorfalls
M 6.123. Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen
M 6.124. Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung
M 6.125. Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen
M 6.126. Einführung in die Computer-Forensik
M 6.127. Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen
M 6.128. Schulung an Beweismittelsicherungswerkzeugen
M 6.129. Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen
M 6.130. Erkennen und Erfassen von Sicherheitsvorfällen
M 6.131. Qualifizieren und Bewerten von Sicherheitsvorfällen
M 6.132. Eindämmen der Auswirkung von Sicherheitsvorfällen
M 6.133. Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen

# Neues in der 15. Ergänzungslieferung der IT-Grundschutz-Kataloge

**Bedarfsorientierte Weiterentwicklung**

Aufgrund der jährlichen Bedarfsabfrage bei registrierten Anwendern wurden die IT-Grundschutz-Kataloge bedarfsorientiert weiterentwickelt. Die neuen und überarbeiteten Bausteine befassen sich mit folgenden Themen:

**Windows 8**

Der Baustein B 3.213 *Client unter Windows 8* ergänzt die Reihe von Bausteinen, die sich mit dem sicheren Einsatz von Windows-Betriebssystemen auf Client-PCs beschäftigen. Der vorliegende Baustein behandelt das Client-Betriebssystem Windows 8 und die Nachfolgeversion Windows 8.1. Hier wird der Anwender auf konzeptionelle Sicherheitsaspekte, aber auch auf Sicherheitsempfehlungen zu konkreten Konfigurationseinstellungen hingewiesen.

**Identitäts- und Berechtigungsmanagement**

Mit dem Baustein B 1.18 *Identitäts- und Berechtigungsmanagement* sind die Maßnahmen und Gefährdungen im Bezug auf ein Identitäts- und Berechtigungsmanagement in einem eigenen Baustein zusammengefasst worden. Erweitert wird der Baustein durch die generische Beschreibung von notwendigen Prozessen, die den geeigneten organisatorischen Rahmen für das Identitäts- und Berechtigungsmanagement darstellen. Ziel des Identitäts- und Berechtigungsmanagements ist es, Geschäftsprozesse, Informationen und IT-Systeme einer Institution durch geeignete Zutritts-, Zugangs- und Zugriffsberechtigungen angemessen zu schützen.

**Eingebettetes System**

Eingebettete Systeme sind in vielen Geräten oder Produkten vorhanden, um dort Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben zu übernehmen, häufig ohne dass sich die Benutzer dessen bewusst sind. Sie finden sich in vielen Bereichen, von der Medizintechnik bis hin zu Haushaltsgeräten. Der Baustein B 3.407 *Eingebettetes System* beschäftigt sich allgemein mit eingebetteten Systemen und ist für ein großes Spektrum unterschiedlicher eingebetteter Systeme anwendbar. Besondere Gefährdungen für eingebettete Systeme werden herausgestellt und durch entsprechende Maßnahmen behandelt.

**Überarbeitung Lokale Netze**

Der überarbeitete Baustein B 4.1 *Lokale Netze* beschreibt, wie die Rahmenbedingungen eines lokalen Netzes analysiert und dieses darauf aufbauend unter Sicherheitsgesichtspunkten konzipiert und betrieben werden kann. Im vorliegenden Baustein werden primär netzspezifische Aspekte wie geeignete Segmentierung, Auswahl einer geeigneten Topologie, Bildung von Teilnetzen etc. betrachtet.

**Überarbeitung Netz- und Systemmanagement**

Der überarbeitete Baustein B 4.2 *Netz- und Systemmanagement* beschreibt die Rahmenbedingungen für den Aufbau eines Netz- und Systemmanagementsystems. Dabei wird auf die Anforderungen, den Aufbau und den sicheren Betrieb eines solchen Systems näher eingegangen.

**Serviceorientierte Architektur**

Als serviceorientierte Architektur (SOA) wird ein allgemeiner Ansatz zur Umsetzung verteilter Systeme bezeichnet, um Institutionen mittels IT in ihren Geschäftsprozessen effizient zu unterstützen. Der Baustein B 5.26 *Serviceorientierte Architektur* zeigt die spezifischen Gefährdungen von verteilten Services auf und beschreibt Maßnahmen für die sichere Anwendung und Implementierung einer SOA. Hierbei wird insbesondere auch der Schutz einzelner Informationsobjekte beachtet.

**Software-Entwicklung**

Der Baustein B 5.27 *Software-Entwicklung* beschreibt die Vorgehensweise für Institutionen, die Software selbst oder von einem Auftragnehmer entwickeln lassen möchten. Neben der Fokussierung auf

die Informationssicherheit bei der Software-Entwicklung werden auch organisatorische und praktische Aspekte berücksichtigt.

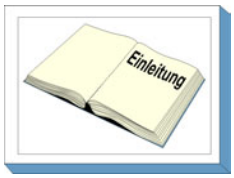
**Aktualisierung und Überarbeitung**

Darüber hinaus wurden zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der Informationssicherheit angepasst.

Weitere strukturelle Veränderungen wurden in der aktualisierten Ausgabe nicht durchgeführt. Die Nummerierung bestehender Gefährdungen und Maßnahmen blieb erhalten, sodass ein im Vorjahr auf Basis der IT-Grundschutz-Kataloge erstelltes Sicherheitskonzept fortgeschrieben werden kann. Es empfiehlt sich dennoch, die ausgewählten Maßnahmen bei der Bearbeitung komplett zu lesen, um Ergänzungen berücksichtigen zu können und um das Wissen zur Informationssicherheit aufzufrischen.

# 1 IT-Grundschutz - Basis für Informationssicherheit

## 1.1 Warum ist Informationssicherheit wichtig?




Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage zumindest teilweise mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für manche Institution existenzbedrohend sein kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

Mit dem IT-Grundschutz bietet das BSI eine einfache Methode an, um alle Informationen einer Institution angemessenen zu schützen. Mit der Kombination aus der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2 und den IT-Grundschutz-Katalogen stellt das BSI für die verschiedensten Einsatzumgebungen sowohl eine Sammlung von Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Auswahl und Anpassung geeigneter Maßnahmen zum sicheren Umgang mit Informationen zur Verfügung.

Nahezu alle Geschäftsprozesse und Fachaufgaben werden mittlerweile elektronisch gesteuert. Große Mengen von Informationen werden dabei digital gespeichert, elektronisch verarbeitet und in lokalen und globalen sowie in privaten und öffentlichen Netzen übermittelt. Viele öffentliche oder privatwirtschaftliche Aufgaben und Vorhaben können ohne IT überhaupt nicht mehr oder im besten Fall nur noch teilweise durchgeführt werden. Damit sind viele Institutionen in Verwaltung und Wirtschaft von dem einwandfreien Funktionieren der eingesetzten IT abhängig. Die jeweiligen Behörden- und Unternehmensziele können nur bei ordnungsgemäßem und sicheren IT-Einsatz erreicht werden.

Mit der Abhängigkeit von der IT erhöht sich auch der potenzielle soziale Schaden durch den Ausfall von Informationstechnik. Da IT an sich nicht frei von Schwachstellen ist, besteht ein durchaus berechtigtes Interesse, die von der IT verarbeiteten Daten und Informationen zu schützen und die Sicherheit der IT zu planen, zu realisieren und zu kontrollieren. Hierbei ist es aber wichtig, sich nicht nur auf die Sicherheit von IT-Systemen zu konzentrieren, da Informationssicherheit nicht nur eine Frage der Technik ist, sondern auch stark von den organisatorischen und personellen Rahmenbedingungen abhängt. Die Sicherheit der Betriebsumgebung, die Verlässlichkeit von Dienstleistungen, der richtige Umgang mit zu schützenden Informationen und viele andere wichtige Aspekte dürfen auf keinen Fall vernachlässigt werden.

Mängel im Bereich der Informationssicherheit können zu erheblichen Problemen führen. Die potentiellen Schäden lassen sich verschiedenen Kategorien zuordnen.

- Verlust der Verfügbarkeit: Wenn grundlegende Informationen nicht vorhanden sind, fällt dies meistens schnell auf, vor allem, wenn Aufgaben ohne diese nicht weitergeführt werden können. Läuft ein IT-System nicht, können beispielsweise keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind unmöglich, Produktionsprozesse stehen still. Aber auch wenn die Verfügbarkeit von bestimmten Informationen nur eingeschränkt ist, kann es zu Arbeitsbeeinträchtigungen in den Prozessen einer Institution kommen.
- Verlust der Vertraulichkeit von Informationen: Jeder Bürger möchte, dass mit seinen personenbezogenen Daten vertraulich umgegangen wird. Jedes Unternehmen weiß, dass interne, vertrauliche Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.

- Verlust der Integrität (Korrektheit von Informationen): Gefälschte oder verfälschte Daten können beispielsweise zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen. Seit einigen Jahren gewinnt auch der Verlust der Authentizität als ein Teilbereich der Integrität an Bedeutung: Daten werden einer falschen Person zugeordnet. Beispielsweise können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die "digitale Identität" wird gefälscht.

Informations- und Kommunikationstechnik spielt in immer mehr Bereichen des täglichen Lebens eine bedeutende Rolle, dabei ist das Innovationstempo seit Jahren unverändert hoch. Besonders erwähnenswert sind dabei folgende Entwicklungen:

- Steigender Vernetzungsgrad: Menschen, aber auch IT-Systeme arbeiten heutzutage nicht mehr isoliert voneinander, sondern werden immer stärker vernetzt. Die Vernetzung ermöglicht es, auf gemeinsame Datenbestände zuzugreifen und intensive Formen der Kooperation über geographische, politische oder institutionelle Grenzen hinweg zu nutzen. Damit entsteht nicht nur eine Abhängigkeit von den einzelnen IT-Systemen, sondern in starkem Maße auch von den Datennetzen. Sicherheitsmängel können dadurch schnell globale Auswirkungen haben.
- IT-Verbreitung und Durchdringung: Immer mehr Bereiche werden durch Informationstechnik unterstützt, häufig, ohne dass dies auffällt. Die erforderliche Hardware wird zunehmend kleiner und günstiger, so dass kleine und kleinste IT-Einheiten in alle Bereiche des Alltags integriert werden können. So gibt es beispielsweise Jacken mit integrierten PDAs, RFIDs zur Steuerung von Besucher- oder Warenströmen, IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können. Die Kommunikation der verschiedenen IT-Komponenten untereinander findet dabei zunehmend drahtlos statt. Dadurch werden auch Alltagsgegenstände über das Internet lokalisierbar und steuerbar.
- Verschwinden der Netzgrenzen: Bis vor kurzem ließen sich Geschäftsprozesse und Anwendungen eindeutig auf die IT-Systeme und die Kommunikationsstrecken dazwischen begrenzen. Ebenso ließ sich sagen, an welchen Standorten und bei welcher Institution diese angesiedelt waren. Durch Globalisierung und die Zunahme von drahtloser und spontaner Kommunikation verschwinden diese Grenzen zunehmend.
- Angriffe kommen schneller: Die beste Vorbeugung gegen Computer-Viren, Trojanische Pferde oder andere Angriffe auf IT-Systeme, Anwendungsprogramme und Protokolle ist die frühzeitige Information über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates. Mittlerweile sinkt allerdings die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten gezielten Massenangriffen darauf, so dass es immer wichtiger wird, ein gut aufgestelltes Informationssicherheitsmanagement und Warnsystem zu haben.
- Höhere Interaktivität von Anwendungen: Unter dem Stichwort Web 2.0 werden bereits vorhandene Techniken miteinander kombiniert, um so neue Anwendungs- und Nutzungsmodelle zu erschaffen. Darunter finden sich verschiedenste Anwendungsbereiche wie neue, soziale Kommunikationsplattformen, Portale für die gemeinsame Nutzung von Informationen, Bildern und Videos oder interaktive Web-Anwendungen. Durch die stärkere Integration von Benutzerrückmeldungen werden Informationen nicht nur schneller verbreitet, sondern es ist auch schwieriger, deren Weitergabe zu steuern.
- Verantwortung der Nutzer: Die beste Technik und schnellste Überbrückung von Sicherheitslücken führt nicht zu einer ausreichenden Informationssicherheit, wenn dabei der Risikofaktor Mensch nicht angemessen beachtet wird. Dabei geht es nicht nur darum, sicherheitskritische Situationen erkennen zu können, sondern vielmehr auch um das verantwortungsvolle Handeln des Einzelnen. Dazu ist es notwendig, Kenntnisse über Sicherheitsrisiken und Verhaltensregeln zu haben.

Angesichts der vorgestellten Gefährdungspotentiale und der steigenden Abhängigkeit stellen sich damit für jede Institution, sei es ein Unternehmen oder eine Behörde, bezüglich Informationssicherheit mehrere zentrale Fragen:

- Wie sorgfältig wird mit geschäftsrelevanten Informationen umgegangen?
- Wie sicher ist die Informationstechnik einer Institution?
- Welche Sicherheitsmaßnahmen müssen ergriffen werden?
- Wie müssen diese Maßnahmen konkret umgesetzt werden?
- Wie hält bzw. verbessert eine Institution das erreichte Sicherheitsniveau?

- Werden die personellen Aspekte der Informationssicherheit angemessen berücksichtigt?
- Wie hoch ist das Sicherheitsniveau anderer Institutionen, mit denen eine Kooperation stattfindet?
- Sind Notfallvorkehrungen getroffen, um im Gefährdungsfall schnell reagieren zu können?

Bei der Suche nach Antworten auf diese Fragen ist zu beachten, dass Informationssicherheit eine Kombination aus technischen, organisatorischen, personellen und baulich-infrastrukturellen Aspekten ist. Sinnvoll ist es, ein Informationssicherheitsmanagement einzuführen, das die mit Informationssicherheit verbundenen Aufgaben konzipiert, koordiniert und überwacht.

Vergleicht man jetzt die Geschäftsprozesse, Anwendungen und IT-Systeme aller Institutionen im Hinblick auf obige Fragen, so kristallisiert sich eine besondere Gruppe heraus. Die Vorgehensweisen und IT-Systeme in dieser Gruppe lassen sich wie folgt charakterisieren:

- Es sind typische Vorgehensweisen und IT-Systeme, d. h. es sind keine Individuallösungen, sondern sie sind weit verbreitet im Einsatz.
- Der Schutzbedarf der Informationen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit liegt im Rahmen des Normalen.
- Die Vorgehensweisen und IT-Systeme sind den üblichen Rahmenbedingungen unterworfen und unterliegen somit typischen Bedrohungen und Gefahren.

Gelingt es, für diese Gruppe der "typischen" Geschäftsprozesse, Anwendungen und IT-Systeme den gemeinsamen Nenner aller erforderlichen Sicherheitsmaßnahmen, die Standard-Sicherheitsmaßnahmen, zu beschreiben, so würde dies die Beantwortung obiger Fragen für diese "typischen" Anwendungsfälle erheblich erleichtern. Bereiche, die außerhalb dieser Gruppe liegen, seien es seltenere Individuallösungen oder IT-Systeme mit hohem Schutzbedarf, können sich dann zwar an den Standard-Sicherheitsmaßnahmen orientieren, bedürfen letztlich aber einer besonderen Betrachtung.

Die IT-Grundschutz-Kataloge beschreiben detailliert diese Standard-Sicherheitsmaßnahmen, die praktisch für jedes IT-System zu beachten sind. Sie umfassen:

- Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme mit "normalem" Schutzbedarf,
- eine Darstellung der pauschal angenommenen Gefährdungslage und
- ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe.

Eine ausführliche Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus sowie eine einfache Verfahrensweise zur Ermittlung des erreichten Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs findet sich in den BSI-Standards 100-1, 100-2 und 100-3 zum IT-Grundschutz.

Da der IT-Grundschutz auch international großen Anklang findet, werden die IT-Grundschutz-Kataloge und auch die meisten anderen Dokumente zum IT-Grundschutz zusätzlich in englischer Sprache digital zur Verfügung gestellt.

## 1.2 IT-Grundschutz: Ziel, Idee und Konzeption

In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme empfohlen. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für

hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.

Um den sehr heterogenen Bereich der Informationstechnik einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt der IT-Grundschutz das Baukastenprinzip. Die einzelnen Bausteine spiegeln typische Abläufe von Geschäftsprozessen und Bereiche des IT-Einsatzes wider, wie beispielsweise Notfall-Management, Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden. Diese Gefährdungslage bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren.

Die Vorgehensweise nach IT-Grundschutz hilft dabei, Sicherheitskonzepte einfach und arbeitsökonomisch zu erstellen. Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten Sicherheitsmaßnahmen auszuwählen und anschließend noch das verbleibende Restrisiko bewerten zu können. Diese Schritte sind beim IT-Grundschutz bereits für jeden Baustein durchgeführt und die für typische Einsatzszenarien passenden Sicherheitsmaßnahmen ausgewählt worden. Bei Anwendung des IT-Grundschutzes reduziert sich die Analyse auf einen Soll-Ist-Vergleich zwischen den in den IT-Grundschutz-Katalogen empfohlenen und den bereits realisierten Maßnahmen. Dabei festgestellte fehlende und noch nicht umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt. Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich eine ergänzende Sicherheitsanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen. Eine einfache Vorgehensweise hierzu ist im BSI-Standard 100-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschrieben.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die in den IT-Grundschutz-Katalogen nicht hinreichend behandelt werden, bieten diese dennoch eine wertvolle Arbeitshilfe. Die dann notwendige ergänzende Analyse kann sich auf die spezifischen Gefährdungen und Sicherheitsmaßnahmen für diese Komponenten oder Rahmenbedingungen konzentrieren.

Bei den in den IT-Grundschutz-Katalogen aufgeführten Maßnahmen handelt es sich um Standard-Sicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Basis-Sicherheit zu erreichen. Dabei stellen die Maßnahmen, die für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz gefordert werden, das Minimum dessen dar, was in jedem Fall vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Die als "zusätzlich" gekennzeichneten Maßnahmen haben sich ebenfalls in der Praxis bewährt, sie richten sich jedoch an Anwendungsfälle mit erhöhten Sicherheitsanforderungen.
Sicherheitskonzepte, die auf IT-Grundschutz basieren, können kompakt gehalten werden, da innerhalb des Konzepts jeweils nur auf die entsprechenden Maßnahmen in den IT-Grundschutz-Katalogen verwiesen werden muss. Dies fördert die Verständlichkeit und die Übersichtlichkeit. Um die Maßnahmenempfehlungen leichter umsetzbar zu machen, sind die Sicherheitsmaßnahmen in den IT-Grundschutz-Katalogen detailliert beschrieben. Bei der verwendeten Fachterminologie wird darauf geachtet, dass die Beschreibungen für diejenigen verständlich sind, die die Maßnahmen realisieren müssen.

Um die Realisierung der Maßnahmen zu vereinfachen, werden die IT-Grundschutz-Kataloge ebenso wie die meisten Informationen rund um IT-Grundschutz auch in elektronischer Form zur Verfügung gestellt. Darüber hinaus wird die Realisierung der Maßnahmen auch durch Hilfsmittel und Musterlösungen unterstützt, die teilweise durch das BSI und teilweise auch von IT-Grundschutz-Anwendern bereitgestellt werden.

Da die Informationstechnik sehr innovativ ist und sich ständig weiterentwickelt, sind die vorliegenden Kataloge auf Aktualisierbarkeit und Erweiterbarkeit angelegt. Das Bundesamt für Sicherheit in der Informationstechnik aktualisiert auf der Grundlage von Anwenderbefragungen die IT-Grundschutz-Kataloge ständig und erweitert sie um neue Themen.

Das BSI bietet allen Anwendern die Möglichkeit der freiwilligen, selbstverständlich kostenfreien Registrierung an. Registrierte Anwender erhalten regelmäßig Informationen über aktuelle Themen des IT-Grundschutzes und der Informationssicherheit. Die Registrierung ist außerdem die Grundlage für die Anwenderbefragungen. Nur durch den ständigen Erfahrungsaustausch mit den IT-Grundschutz-Anwendern ist eine bedarfsgerechte Weiterentwicklung möglich. Diese Bemühungen zielen letztlich darauf, aktuelle Empfehlungen zu typischen Informationssicherheitsproblemen aufzeigen zu können. Maßnahmenempfehlungen, die nicht ständig aktualisiert und erweitert werden, veralten sehr schnell oder müssen so generisch gehalten werden, dass sie ihren eigentlichen Nutzen, Sicherheitslücken zu identifizieren und die konkrete Umsetzung zu vereinfachen, verfehlen.

## 1.3 Aufbau der IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge lassen sich in verschiedene Bereiche untergliedern, die zum besseren Verständnis hier kurz erläutert werden sollen:

**Einstieg und Vorgehensweise**

In diesem einleitenden Teil wird die Konzeption IT-Grundschutz und die Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach IT-Grundschutz kurz vorgestellt. Eine ausführliche Beschreibung der Vorgehensweise nach IT-Grundschutz findet sich im BSI-Standard 100-2. Außerdem werden die Struktur der IT-Grundschutz-Kataloge und deren Nutzung erläutert.

**Informationssicherheitsmanagement**

Die Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und planmäßigen Informationssicherheitsprozess aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement oder kurz IS-Management bezeichnet.

Die Erfahrung zeigt, dass es ohne ein funktionierendes IS-Management praktisch nicht möglich ist, ein durchgängiges und angemessenes Sicherheitsniveau zu erzielen und zu erhalten. Daher wird im BSI-Standard 100-1 "Managementsysteme für Informationssicherheit (ISMS)" beschrieben, was ein solches Managementsystem leisten sollte und welche Aufgaben damit verbunden sind.

Aufbauend hierauf wird in Baustein B 1.0 *Sicherheitsmanagement* der IT-Grundschutz-Kataloge beschrieben, wie ein effizientes Informationssicherheitsmanagement aussehen sollte und welche Organisationsstrukturen dafür sinnvoll sind. Es wird außerdem ein systematischer Weg aufgezeigt, wie ein funktionierendes IS-Management eingerichtet und im laufenden Betrieb weiterentwickelt werden kann.

**Bausteine**

Die Bausteine der IT-Grundschutz-Kataloge enthalten jeweils eine Kurzbeschreibung für die betrachteten Komponenten, Vorgehensweisen und IT-Systeme sowie einen Überblick über die Gefährdungslage und die Maßnahmenempfehlungen. Die Bausteine sind nach dem IT-Grundschutz-Schichtenmodell in die folgenden Kataloge gruppiert:

B 1: Übergreifende Aspekte der Informationssicherheit
B 2: Sicherheit der Infrastruktur
B 3: Sicherheit der IT-Systeme
B 4: Sicherheit in Netzen
B 5: Sicherheit in Anwendungen

**Gefährdungskataloge**

Dieser Bereich enthält die ausführlichen Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden. Die Gefährdungen sind in sechs Kataloge gruppiert:

G 0: Elementare Gefährdungen
G 1: Höhere Gewalt
G 2: Organisatorische Mängel
G 3: Menschliche Fehlhandlungen
G 4: Technisches Versagen
G 5: Vorsätzliche Handlungen

Der Gefährdungskatalog G 0 *Elementare Gefährdungen* enthält verallgemeinerte und auf das wesentliche reduzierte grundlegende Gefährdungen. Dieser Katalog kann beispielsweise als Grundlage für Risikoanalysen benutzt werden.

**Maßnahmenkataloge**

Dieser Teil beschreibt die in den Bausteinen der IT-Grundschutz-Kataloge zitierten Sicherheitsmaßnahmen ausführlich. Die Maßnahmen sind in sechs Maßnahmenkataloge gruppiert:

M 1: Infrastruktur
M 2: Organisation
M 3: Personal
M 4: Hard- und Software
M 5: Kommunikation
M 6: Notfallvorsorge

**Aufbau der Bausteine**

Die zentrale Rolle der IT-Grundschutz-Kataloge spielen die Bausteine, deren Aufbau im Prinzip gleich ist. Jeder Baustein beginnt mit einer kurzen Beschreibung der betrachteten Komponente, der Vorgehensweise bzw. des IT-Systems.

Im Anschluss daran wird die Gefährdungslage dargestellt. Die Gefährdungen sind dabei nach den genannten Bereichen Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen unterteilt.

Um die Bausteine übersichtlich zu gestalten und um Redundanzen zu vermeiden, werden die Gefährdungstexte lediglich referenziert. Hier ein Beispiel für das Zitat einer Gefährdung innerhalb eines Bausteins:

- G 4.1 *Ausfall der Stromversorgung*

Im Kürzel G x.y steht der Buchstabe "G" für Gefährdung. Die Zahl x vor dem Punkt bezeichnet den Gefährdungskatalog (hier G 4 = Technisches Versagen) und die Zahl y nach dem Punkt bezeichnet die laufende Nummer der Gefährdung innerhalb des jeweiligen Katalogs. Es folgt der Titel der Gefährdung. Ein Einlesen in die Gefährdungen ist aus Gründen der Sensibilisierung und des Verständnisses der Maßnahmen empfehlenswert, aber für die Erstellung eines Sicherheitskonzepts nach IT-Grundschutz nicht zwingend erforderlich.

Den wesentlichen Teil eines jeden Bausteins bilden die Maßnahmenempfehlungen, die sich an die Gefährdungslage anschließen. Zunächst werden kurze Hinweise zum jeweiligen Maßnahmenbündel dargestellt, beispielsweise zur folgerichtigen Reihenfolge bei der Realisierung der notwendigen Maßnahmen.

In jedem Baustein wird für das betrachtete Themengebiet vor der Maßnahmen-Liste eine Übersicht in Form eines "Lebenszyklus" gegeben, welche Maßnahmen in welcher Phase der Bearbeitung zu welchem Zweck umgesetzt werden sollten. In der Regel können die folgenden Phasen identifiziert werden, wobei für jede dieser Phasen typische Arbeiten angegeben sind, die im Rahmen einzelner Maßnahmen

durchgeführt werden. Phasenübergreifend wirken dabei das Sicherheitsmanagement und die Revision, die den gesamten Lebenszyklus begleiten und kontrollieren.

| **Phase** | **typische Tätigkeiten** |
|---|---|
| Planung und Konzeption | - Definition des Einsatzzwecks<br>- Festlegung von Einsatzszenarien<br>- Abwägung des Risikopotentials<br>- Dokumentation der Einsatzentscheidung<br>- Erstellung des Sicherheitskonzepts<br>- Festlegung von Richtlinien für den Einsatz |
| Beschaffung (sofern erforderlich) | - Festlegung der Anforderungen an zu beschaffende Produkte (nach Möglichkeit auf Basis der Einsatzszenarien der Planungsphase)<br>- Auswahl der geeigneten Produkte |
| Umsetzung | - Konzeption und Durchführung des Testbetriebs<br>- Installation und Konfiguration entsprechend Sicherheitsrichtlinie<br>- Schulung und Sensibilisierung aller Betroffenen |
| Betrieb | - Sicherheitsmaßnahmen für den laufenden Betrieb (z. B. Protokollierung)<br>- Kontinuierliche Pflege und Weiterentwicklung<br>- Änderungsmanagement<br>- Organisation und Durchführung von Wartungsarbeiten<br>- Audit |
| Aussonderung (sofern erforderlich) | - Entzug von Berechtigungen<br>- Entfernen von Datenbeständen und Referenzen auf diese Daten<br>- Sichere Entsorgung von Datenträgern |
| Notfallvorsorge | - Konzeption und Organisation der Datensicherung<br>- Nutzung von Redundanz zur Erhöhung der Verfügbarkeit<br>- Umgang mit Sicherheitsvorfällen<br>- Erstellen eines Notfallplans |

Es finden sich nicht in allen Bausteinen für jede Phase entsprechende Maßnahmen. So enthält beispielsweise der Baustein "OpenLDAP" keine Maßnahme in der Beschaffungsphase, da dieser Baustein auf der Umsetzung des Bausteins "allgemeiner Verzeichnisdienst" basiert und hier die Auswahl eines Produkts bereits entschieden wurde.

Da alle Geschäftsprozesse, IT-Systeme und Einsatzbedingungen sich ständig ändern und weiterentwickelt werden, müssen die Phasen erfahrungsgemäß immer wieder durchlaufen werden. Dies sicherzustellen ist Aufgabe des Informationssicherheitsmanagements.

Analog zu den Gefährdungen sind die Maßnahmen in die Maßnahmenkataloge Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge gruppiert. Wie bei den Gefährdungen wird hier ebenfalls nur auf die entsprechende Maßnahme referenziert. Hier ein Beispiel für das Zitat einer empfohlenen Maßnahme innerhalb eines Bausteins:

- M 1.15 *Geschlossene Fenster und Türen* (A) Geschlossene Fenster und Türen

Im Kürzel M x.y bezeichnet "M" eine Maßnahme, die Zahl x vor dem Punkt den Maßnahmenkatalog (hier M 1 = Infrastruktur). Die Zahl y nach dem Punkt ist die laufende Nummer der Maßnahme innerhalb des jeweiligen Katalogs.

Mit dem Buchstaben in Klammern (hier (A)) wird zu jeder Maßnahme die Qualifizierungsstufe angegeben, also eine Einstufung, ob diese Maßnahme für die IT-Grundschutz-Qualifizierung gefordert wird. Folgende Einstufungen sind vorgesehen:

| **Qualifizierungsstufe** | **Beschreibung** |
|---|---|
| A (Einstieg) | Diese Maßnahmen müssen für alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz (Auditor-Testat "IT-Grundschutz Einstiegsstufe", Auditor-Testat "IT-Grundschutz Aufbaustufe" und ISO 27001-Zertifikat auf Basis von IT-Grundschutz) umgesetzt sein. Diese Maßnahmen sind essentiell für die Sicherheit innerhalb des betrachteten Bausteins. Sie sind vorrangig umzusetzen. |
| B (Aufbau) | Diese Maßnahmen müssen für das Auditor-Testat "IT-Grundschutz Aufbaustufe" und für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umgesetzt sein. Sie sind besonders wichtig für den Aufbau einer kontrollierbaren Informationssicherheit. Eine zügige Realisierung ist anzustreben. |
| C (Zertifikat) | Diese Maßnahmen müssen für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umgesetzt sein. Sie sind wichtig für die Abrundung der Informationssicherheit. Bei Engpässen können sie zeitlich nachrangig umgesetzt werden. |
| Z (zusätzlich) | Diese Maßnahmen müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz verbindlich umgesetzt werden. Sie stellen Ergänzungen dar, die vor allem bei höheren Sicherheitsanforderungen hilfreich sein können. |
| W (Wissen) | Diese Maßnahmen dienen der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der anderen Maßnahmen hilfreich sind. Sie müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz geprüft werden. |

Um ein Sicherheitskonzept nach IT-Grundschutz erstellen und den dabei notwendigen Soll-Ist-Vergleich durchführen zu können, ist es erforderlich, die Texte zu den jeweils in den identifizierten Bausteinen enthaltenen Maßnahmen im jeweiligen Maßnahmenkatalog sorgfältig zu lesen. Als Beispiel sei hier ein Auszug aus einer Maßnahme zitiert:

**M 2.11 Regelung des Passwortgebrauchs**

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Benutzer

[Maßnahmentext ...]

Prüffragen:

- Gibt es klare Regelungen zum Passwortgebrauch und die Passwortgestaltung?

[...]

Die Maßnahmentexte sind sinngemäß umzusetzen. Sie sind so geschrieben, dass sie auf möglichst viele Bereiche angewendet werden können. Bevor die Maßnahmenempfehlungen umgesetzt werden, ist immer zu überlegen, ob sie für die jeweilige Organisation oder den Informationsverbund angepasst werden müssen. Alle Änderungen sollten dokumentiert werden, damit die Gründe auch später noch nachvollziehbar sind.

Neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, werden Verantwortliche beispielhaft genannt. Verantwortlich für die Initiierung bezeichnet die Personen oder Rollen, die die Umsetzung einer Maßnahme typischerweise veranlassen sollten. Verantwortlich für die Umsetzung bezeichnet die Personen oder Rollen, die die Maßnahme realisieren sollten.

Am Ende der meisten Maßnahmen finden sich Prüffragen.

Diese sind so formuliert, dass sie als letzte Checkliste benutzt werden können, um die Umsetzung der Maßnahmen kontrollieren zu können. Sie geben Ziel und Grundrichtung der Sicherheitsempfehlungen vor und können damit als Basis für Revisionen und Zertifizierungsaudits benutzt werden. Nach der Beantwortung der Prüffragen kann eine Aussage getroffen werden, in wieweit in der Institution die Ziele der einzelnen Bausteine erfüllt wurden.

Prüffragen sind stets geschlossene Fragen, die mit "Ja" oder "Nein" beantwortet werden können. Dabei bedeutet ein "Ja", dass die jeweilige Anforderung erfüllt ist. Somit lassen sich die Prüffragen auch toolgestützt auswerten. Prüffragen sind allgemeiner und abstrakter formuliert als die Maßnahmentexte. Details zur konkreten Umsetzung von Empfehlungen finden sich in den jeweiligen Maßnahmen.

Nicht alle Maßnahmen haben zwingend Prüffragen, da Prüffragen nicht dem Aufbau von Sicherheitskonzepten dienen, sondern bei der Überprüfung der umgesetzten Sicherheitsmaßnahmen eingesetzt werden sollen. So enthalten beispielsweise viele Maßnahmen aus der Lebenszyklusphase "Beschaffung" keine Prüffragen, da hier Sicherheitsempfehlungen formuliert wurden, die vor dem Kauf von Systemen beachtet werden sollten. Bei einem Audit kann aber nur geprüft werden, ob die vorhandenen Systeme sicher betrieben werden.

Der Zusammenhang zwischen den für den IT-Grundschutz angenommenen Gefährdungen und den empfohlenen Maßnahmen kann den Maßnahmen-Gefährdungstabellen entnommen werden. Diese finden sich auf den IT-Grundschutz-Seiten der BSI-Webseite. Für jeden Baustein gibt es eine Maßnahmen-Gefährdungstabelle.

Als Beispiel sei ein Auszug aus der Maßnahmen-Gefährdungstabelle für den Baustein B 2.10 *Mobiler Arbeitsplatz* angeführt:

| **B 2.10** | **Phase** | **Stufe** | **G 1. 15** | **G 2. 1** | **G 2. 4** | **G 2. 47** | **G 2. 48** | **G 3. 3** | **G 3. 43** | **G 3. 44** | **G 5. 1** | **G 5. 2** | **G 5. 4** | **G 5. 71** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M 1.15 | BT | A | | X | | | | | | | X | X | X | X |
| M 1.23 | BT | A | | X | X | | | | | | X | X | X | X |
| M 1.46 | BT | Z | | | | | | | | | | | X | |
| M 1.61 | PK | A | X | | | | | X | | | X | | X | X |
| M 2.13 | AU | A | | X | | | X | X | | X | | | | X |

Alle Tabellen haben einen einheitlichen Aufbau. In der Kopfzeile sind die im dazugehörigen Baustein aufgelisteten Gefährdungen mit ihren Nummern eingetragen. In der ersten Spalte finden sich entspre-

chend die Nummern der Maßnahmen wieder. In der zweiten Spalte ist eingetragen, zu welcher Lebenszyklusphase die jeweilige Maßnahme für den betrachteten Baustein gehört. Aus Platzgründen werden hierbei für die einzelnen Lebenszyklusphasen folgende Abkürzungen verwendet: PK für "Planung und Konzeption", BE für "Beschaffung", UM für "Umsetzung", BT für "Betrieb", AU für "Aussonderung" und NV für "Notfallvorsorge". In der dritten Spalte ist notiert, welche Einstufung bezüglich einer IT-Grundschutz-Qualifizierung die einzelne Maßnahme für den betrachteten Baustein besitzt.

Die übrigen Spalten beschreiben den Zusammenhang zwischen Maßnahmen und Gefährdungen. Ist in einem Feld ein "X" eingetragen, so bedeutet dies, dass die korrespondierende Maßnahme gegen die entsprechende Gefährdung wirksam ist. Diese Wirkung kann schadensvorbeugender oder schadensmindernder Natur sein.

Zu beachten ist, dass in den Maßnahmen-Gefährdungstabellen nur die wichtigsten Gefährdungen angeführt sind, gegen die eine bestimmte Maßnahme wirkt. Dies bedeutet insbesondere, dass eine Maßnahme nicht automatisch überflüssig wird, wenn alle in der Tabelle zugeordneten Gefährdungen in einem bestimmten Anwendungsfall nicht relevant sind. Ob auf eine Standard-Sicherheitsmaßnahme verzichtet werden kann, muss immer im Einzelfall anhand der vollständigen Sicherheitskonzeption und nicht nur anhand der Maßnahmen-Gefährdungstabelle geprüft und dokumentiert werden.

Abschließend sei erwähnt, dass sämtliche Bausteine, Gefährdungen, Maßnahmen, Tabellen und Hilfsmittel in elektronischer Form verfügbar sind. Diese Texte können bei der Erstellung eines Sicherheitskonzeptes und bei der Realisierung von Maßnahmen weiterverwendet werden.

## 1.4 Anwendungsweisen der IT-Grundschutz-Kataloge


Für den erfolgreichen Aufbau eines kontinuierlichen und effektiven Sicherheitsprozesses müssen eine ganze Reihe von Aktionen durchgeführt werden. Hierfür bieten die IT-Grundschutz-Vorgehensweise (siehe BSI-Standard 100-2) sowie die IT-Grundschutz-Kataloge zahlreiche Hinweise zur Methodik und praktische Umsetzungshilfen. Enthalten sind ferner Lösungsansätze für verschiedene, die Informationssicherheit betreffende Aufgabenstellungen, beispielsweise Sicherheitskonzeption, Revision und Zertifizierung. Je nach vorliegender Aufgabenstellung sind dabei unterschiedliche Anwendungsweisen des IT-Grundschutzes zweckmäßig. Dieser Abschnitt dient dazu, durch Querverweise auf die entsprechenden Kapitel der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2 den direkten Einstieg in die einzelnen Anwendungsweisen zu erleichtern.

**Sicherheitsprozess und Management der Informationssicherheit**

Informationen sind wichtige Werte für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Je nach Art der Informationen stehen unterschiedliche Schutzziele im Vordergrund: So muss sichergestellt werden können, dass Informationen vertraulich behandelt werden, dass sie nicht absichtlich oder versehentlich geändert werden und dass sie dann zur Verfügung stehen, wenn sie benötigt werden.

Die meisten Informationen werden heutzutage zumindest teilweise mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Die Abhängigkeit vom ordnungsgemäßen Funktionieren der Informationstechnik hat in den letzten Jahren sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft stark zugenommen. Immer mehr Geschäftsprozesse werden auf die Informationstechnik verlagert oder mit ihr verzahnt. Ein Ende dieser Entwicklung ist nicht abzusehen. Zu einem vernünftigen Informationsschutz gehört daher auch die Absicherung der IT.

Informationssicherheit ist bei allen Geschäftsprozessen und Fachaufgaben relevant und daher als integraler Bestandteil der originären Aufgabe anzusehen. Der folgende Aktionsplan beinhaltet alle wesent-

lichen Schritte, die für einen kontinuierlichen Sicherheitsprozess notwendig sind, und ist somit als eine planmäßig anzuwendende, begründete Vorgehensweise zu verstehen, wie ein angemessenes Sicherheitsniveau erreicht und aufrechterhalten werden kann:

- Initiierung des Sicherheitsprozesses
    - Übernahme der Verantwortung durch die Leitungsebene
    - Konzeption und Planung des Sicherheitsprozesses
    - Erstellung der Leitlinie zur Informationssicherheit
    - Aufbau einer geeigneten Organisationsstruktur für das Informationssicherheitsmanagement
    - Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen
    - Einbindung aller Mitarbeiter in den Sicherheitsprozess
- Erstellung einer Sicherheitskonzeption
- Umsetzung der Sicherheitskonzeption und Realisierung der Sicherheitsmaßnahmen
- Aufrechterhaltung der Informationssicherheit im laufenden Betrieb und kontinuierliche Verbesserung

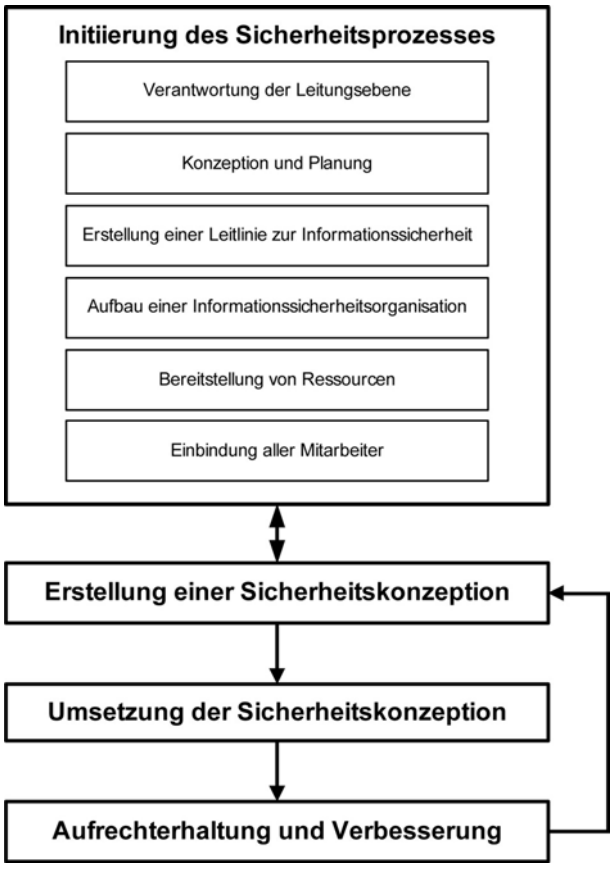



Abbildung: Phasen des Sicherheitsprozesses

Im BSI-Standard 100-2 wird der Ablauf ausführlich beschrieben. Außerdem wird im Baustein B 1.0 *Sicherheitsmanagement* der Sicherheitsprozess im Überblick dargestellt, und es wird eine detaillierte Erläuterung der einzelnen Aktionen in Form empfohlener Standard-Maßnahmen gegeben.

Zur Erstellung der Sicherheitskonzeption ist nach IT-Grundschutz eine Reihe von Schritten notwendig, die im Folgenden kurz dargestellt werden.

**Strukturanalyse**

Unter einem Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisato-

rische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Für die Erstellung eines Sicherheitskonzepts und insbesondere für die Anwendung von IT-Grundschutz ist es erforderlich, die Struktur des vorliegenden Informationsverbundes zu analysieren und zu dokumentieren. Bei der Strukturanalyse werden daher die Informationen, Anwendungen, IT-Systeme, Räume, Kommunikationsnetze, die zur Erfüllung der im Geltungsbereich festgelegten Geschäftsprozesse oder Fachaufgaben benötigt werden, erfasst.

Die einzelnen Schritte der Strukturanalyse werden im Detail in Kapitel 4.2 der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) in Form einer Handlungsanweisung beschrieben.

**Schutzbedarfsfeststellung**

Zweck der Schutzbedarfsfeststellung ist es zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch". Erläuterungen und praktische Hinweise zur Schutzbedarfsfeststellung sind Gegenstand von Kapitel 4.3 der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2).

**Modellierung**

Als Nächstes müssen die Bausteine der IT-Grundschutz-Kataloge in einem Modellierungsschritt auf die Zielobjekte des vorliegenden Informationsverbunds abgebildet werden.

In Kapitel 4.4 der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2 wird beschrieben, wie die Modellierung eines Informationsverbunds durch Bausteine aus den IT-Grundschutz-Katalogen vorgenommen werden sollte. Detaillierte Hinweise für die Verwendung des Schichtenmodells und der einzelnen Bausteine im Rahmen der Modellierung sind im Kapitel 2 der IT-Grundschutz-Kataloge enthalten. Das Ergebnis der Modellierung ist ein erster grober Entwurf des Sicherheitskonzepts.

**Basis-Sicherheitscheck**

Der Basis-Sicherheitscheck ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status Quo eines bestehenden (nach IT-Grundschutz modellierten) Informationsverbunds in Bezug auf den Umsetzungsgrad von Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge ermittelt. Als Ergebnis liegt eine Übersicht vor, in dem für jede relevante Maßnahme der Umsetzungsstatus "entbehrlich", "ja", "teilweise" oder "nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise umgesetzten Maßnahmen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Zielobjekte aufgezeigt. Kapitel 4.5 des BSI-Standards 100-2 beschreibt einen Aktionsplan für die Durchführung eines Basis-Sicherheitschecks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

**Weiterführende Sicherheitsmaßnahmen**

Die Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bieten im Normalfall einen angemessenen und ausreichenden Schutz. Insbesondere bei hohem oder sehr hohem Schutzbedarf ist jedoch zu prüfen, ob zusätzlich oder ersatzweise höherwertige Sicherheitsmaßnahmen erforderlich sind.

Im Rahmen der ergänzenden Sicherheitsanalyse (siehe Kapitel 4.6 des BSI-Standards 100-2) wird entschieden, für welche Zielobjekte des betrachteten Informationsverbunds eine Risikoanalyse erforderlich ist, um gegebenenfalls weiterführende Sicherheitsmaßnahmen festzulegen. Eine Methode zur Risikoanalyse auf der Basis von IT-Grundschutz wird im BSI-Standard 100-3 beschrieben.

Eine ergänzende Sicherheitsanalyse ist auch dann erforderlich, wenn Teile des Informationsverbunds nicht hinreichend mit den existierenden Bausteinen der IT-Grundschutz-Kataloge abgebildet werden können oder wenn besondere Einsatzszenarien vorliegen, die im IT-Grundschutz nicht vorgesehen sind.

**Umsetzung von Sicherheitskonzepten**

Damit das angestrebte Informationssicherheitsniveau erreicht wird, müssen bestehende Schwachstellen ermittelt und alle erforderlichen Maßnahmen identifiziert werden. Vor allem müssen alle Maßnahmen, die im Sicherheitskonzept vorgesehen sind, auch konsequent anhand eines Realisierungsplans umgesetzt werden. In Kapitel 5 des BSI-Standards 100-2 zur IT-Grundschutz-Vorgehensweise wird beschrieben, was bei der Umsetzungsplanung von Sicherheitsmaßnahmen zu beachten ist.

**Sicherheitsrevision**

Die in den IT-Grundschutz-Katalogen enthaltenen Sicherheitsmaßnahmen können auch für die Sicherheitsrevision genutzt werden. Hierzu wird die gleiche Vorgehensweise wie beim Basis-Sicherheitscheck empfohlen. Hilfreich und arbeitsökonomisch ist es, für jeden Baustein anhand der Maßnahmentexte eine speziell auf die eigene Institution angepasste Checkliste zu erstellen. Dies erleichtert die Revision und verbessert häufig die Reproduzierbarkeit der Ergebnisse.

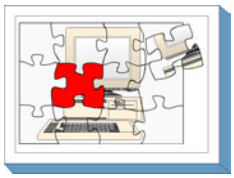
**Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz**

Die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge werden nicht nur für die Sicherheitskonzeption, sondern auch zunehmend als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann eine Institution nach innen und außen hin dokumentieren, dass sie sowohl ISO 27001 als auch IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat.

Das Niveau der Qualifizierung wird dabei in drei verschiedene Stufen unterteilt, die sich sowohl im Hinblick auf die Güte (d. h. den erforderlichen Umsetzungsgrad der Sicherheitsmaßnahmen) als auch in Bezug auf die Vertrauenswürdigkeit unterscheiden. Das Eingangsniveau kann durch einen zertifizierten Auditor nachgewiesen werden, das höchste Niveau erfordert zusätzlich eine Prüfung durch eine Zertifizierungsstelle. Das Prüfungsschema für Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz sowie das entsprechende Zertifizierungsschema für Auditoren sind auf dem Webserver des BSI erhältlich.

# 2 Schichtenmodell und Modellierung

## 2.1 Modellierung nach IT-Grundschutz



Bei der Umsetzung von IT-Grundschutz muss der betrachtete Informationsverbund mit Hilfe der vorhandenen Bausteine nachgebildet werden, also die relevanten Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen zusammengetragen werden. Dafür müssen die Strukturanalyse und eine Schutzbedarfsfeststellung vorliegen. Darauf aufbauend wird ein IT-Grundschutz-Modell des Informationsverbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten IT-Grundschutz-Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

Das erstellte IT-Grundschutz-Modell ist unabhängig davon, ob der Informationsverbund aus bereits im Einsatz befindlichen IT-Systemen besteht oder ob es sich um einen Informationsverbund handelt, der sich erst im Planungsstadium befindet. Jedoch kann das Modell unterschiedlich verwendet werden:

- Das IT-Grundschutz-Modell eines bereits realisierten Informationsverbunds identifiziert über die verwendeten Bausteine die relevanten Standard-Sicherheitsmaßnahmen. Es kann in Form eines Prüfplans benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschutz-Modell eines geplanten Informationsverbunds stellt hingegen ein Entwicklungskonzept dar. Es beschreibt über die ausgewählten Bausteine, welche Standard-Sicherheitsmaßnahmen bei der Realisierung des Informationsverbunds umgesetzt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht das folgende Bild:

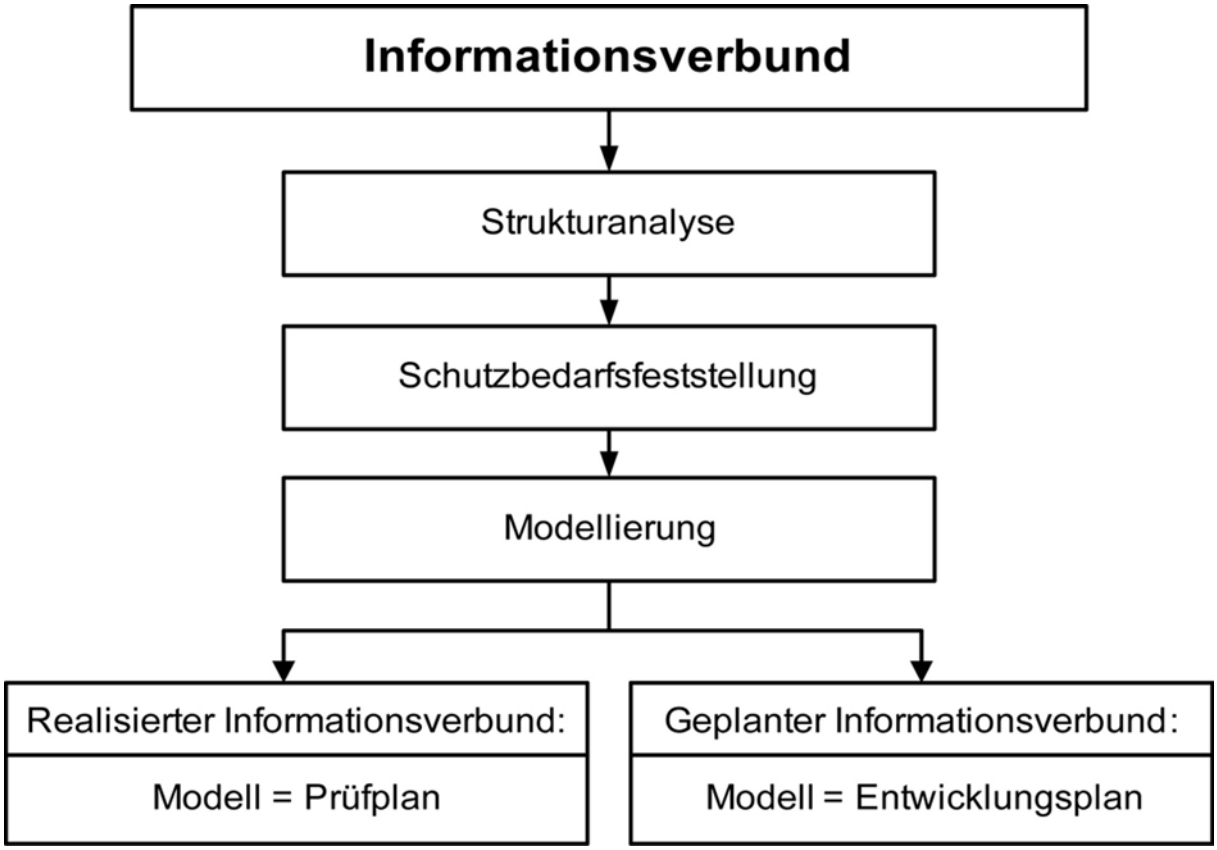



Abbildung: Ergebnis der Modellierung nach IT-Grundschutz

Typischerweise wird ein im Einsatz befindlicher Informationsverbund sowohl realisierte als auch in Planung befindliche Anteile besitzen. Das resultierende IT-Grundschutz-Modell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts.

Für die Abbildung eines im Allgemeinen komplexen Informationsverbunds auf die Bausteine der IT-Grundschutz-Kataloge bietet es sich an, die Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.

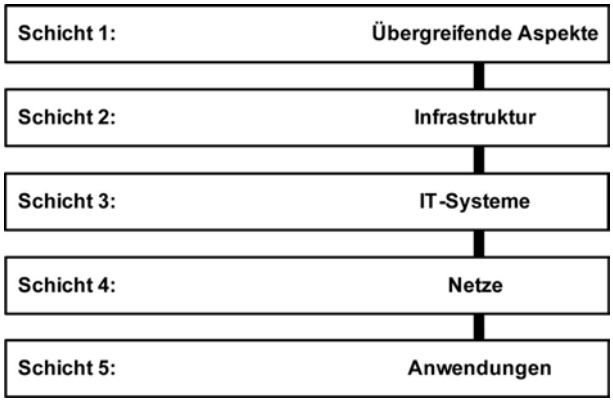



Abbildung: Schichten des IT-Grundschutz-Modells

Die Sicherheitsaspekte eines Informationsverbunds werden wie folgt den einzelnen Schichten zugeordnet:

- **Schicht 1** umfasst die übergreifenden Sicherheitsaspekte, die für sämtliche oder große Teile des Informationsverbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem Sicherheitsmanagement, Organisation, Datensicherungskonzept und Schutz vor Schadprogrammen.

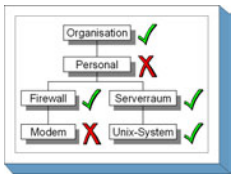
- **Schicht 2** befasst sich mit den baulich-physischen Gegebenheiten. In dieser Schicht werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft zum Beispiel die Bausteine Gebäude, Serverraum, Rechenzentrum und häuslicher Arbeitsplatz.
- **Schicht 3** betrifft die einzelnen IT-Systeme eines Informationsverbunds, die gegebenenfalls in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Einzelplatz-Systemen behandelt. In diese Schicht fallen beispielsweise die Bausteine TK-Anlage, Laptop sowie Client unter Windows Vista.
- **Schicht 4** betrachtet die Vernetzungsaspekte, die sich in erster Linie nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Netzmanagement, WLAN, VoIP sowie VPN.
- **Schicht 5** schließlich beschäftigt sich mit den eigentlichen Anwendungen, die im Informationsverbund genutzt werden. In dieser Schicht können unter anderem die Bausteine Groupware, Webserver, Faxserver und Datenbanken zur Modellierung verwendet werden.

Die Aufgabenstellung bei der Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten, usw.

Nachfolgend wird die Vorgehensweise der Modellierung für einen Informationsverbund detailliert beschrieben. Dabei wird besonderer Wert auf die Randbedingungen gelegt, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

Bei der Modellierung eines Informationsverbunds nach IT-Grundschutz kann das Problem auftreten, dass es Zielobjekte gibt, die mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet werden können. In diesem Fall sollte eine ergänzende Sicherheitsanalyse durchgeführt werden, wie in der IT-Grundschutz-Vorgehensweise beschrieben.

## 2.2 Zuordnung anhand Schichtenmodell




Bei der Modellierung eines Informationsverbunds ist es zweckmäßig, die Zuordnung der Bausteine anhand des Schichtenmodells vorzunehmen. Daran anschließend folgt schließlich die Vollständigkeitsprüfung.

**zu Schicht 1: Übergreifende Aspekte der Informationssicherheit**

In dieser Schicht werden alle Aspekte des Informationsverbunds modelliert, die den technischen Komponenten übergeordnet sind. Im Vordergrund stehen dabei Konzepte und die von diesen Konzepten abgeleiteten Regelungen. Diese Aspekte sollten für den gesamten Informationsverbund einheitlich geregelt sein, so dass die entsprechenden Bausteine in den meisten Fällen nur einmal für den gesamten Informationsverbund anzuwenden sind. Dem Informationssicherheitsmanagement, der Organisation des IT-Betriebs sowie der Schulung und Sensibilisierung des Personals kommt dabei eine besondere Bedeutung zu. Die Umsetzung der diesbezüglichen Maßnahmen ist von grundlegender Bedeutung für den sicheren Umgang mit geschäftsrelevanten Informationen und die sichere Nutzung von Informations- und Kommunikationstechnik. Unabhängig von den eingesetzten technischen Komponenten sind die entsprechenden Bausteine daher immer anzuwenden.

- Der Baustein B 1.0 *Sicherheitsmanagement* ist für den gesamten Informationsverbund einmal anzuwenden. Ein funktionierendes Informationssicherheitsmanagement ist die wesentliche Grundlage für die Erreichung eines angemessenen Sicherheitsniveaus. Im Fall von Outsourcing gelten für die

Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

- Der Baustein B 1.1 *Organisation* muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.2 *Personal* muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.3 *Notfallmanagement* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Verfügbarkeit haben oder wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei der Bearbeitung des Bausteins ist besonderes Augenmerk auf diese Komponenten zu richten. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.4 *Datensicherungskonzept* ist für den gesamten Informationsverbund einmal anzuwenden.
- Der Baustein B 1.5 *Datenschutz* dient für Anwender in Deutschland zur Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen eine Verarbeitung und sonstige Nutzung personenbezogener oder -beziehbarer Daten erfolgt. Dabei sollte dann geprüft werden, ob der Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Institution anzuwenden ist.
- Der Baustein B 1.6 *Schutz vor Schadprogrammen* ist für den gesamten Informationsverbund einmal anzuwenden.
- Der Baustein B 1.7 *Kryptokonzept* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Vertraulichkeit oder Integrität haben, oder wenn bereits kryptographische Verfahren im Einsatz sind.
- Der Baustein B 1.8 *Behandlung von Sicherheitsvorfällen* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf einen der drei Grundwerte haben, oder wenn der Ausfall des gesamten Informationsverbunds einen Schaden in den Kategorien hoch oder sehr hoch zur Folge hat. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.9 *Hard- und Software-Management* muss für jeden Informationsverbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden Informationsverbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.10 *Standardsoftware* ist zumindest einmal für den gesamten Informationsverbund anzuwenden. Gibt es innerhalb des Informationsverbunds Teilbereiche mit unterschiedlichen Anforderungen oder Regelungen für die Nutzung von Standardsoftware, sollte Baustein B 1.10 auf diese Teilbereiche jeweils getrennt angewandt werden.

- Der Baustein B 1.11 *Outsourcing* ist zumindest dann anzuwenden, wenn die folgenden Bedingungen alle erfüllt sind:

  - IT-Systeme, Anwendungen oder Geschäftsprozesse werden zu einem externen Dienstleister ausgelagert, und
  - die Bindung an den Dienstleister erfolgt auf längere Zeit, und
  - durch die Dienstleistung kann die Informationssicherheit des Auftraggebers beeinflusst werden, und
  - im Rahmen der Dienstleistungen erbringt der Dienstleister auch regelmäßig nennenswerte Tätigkeiten im Bereich Informationssicherheitsmanagement.

  Gibt es in einem Informationsverbund verschiedene ausgelagerte Komponenten bei unterschiedlichen Dienstleistern, ist der Baustein für jeden externen Dienstleister einmal anzuwenden. Für die Anwendung dieses Bausteins gelten besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.

- Der Baustein B 1.12 *Archivierung* ist auf den Informationsverbund anzuwenden, wenn aufgrund interner oder externer Vorgaben eine Langzeitarchivierung elektronischer Dokumente erforderlich ist oder bereits ein System zur Langzeitarchivierung elektronischer Dokumente betrieben wird.

- Der Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit* ist für den gesamten Informationsverbund einmal anzuwenden.

- Der Baustein B 1.14 *Patch- und Änderungsmanagement* ist zumindest bei größeren Informationsverbünden anzuwenden, also wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei kleineren und wenig komplexen Informationsverbünden reicht die Umsetzung von M 2.221 *Änderungsmanagement* aus.

- Der Baustein B 1.15 *Löschen und Vernichten von Daten* ist für den gesamten Informationsverbund einmal anzuwenden.

- Der Baustein B 1.16 *Anforderungsmanagement* ist für den gesamten Informationsverbund einmal anzuwenden.

- Der Baustein B 1.17 *Cloud-Nutzung* richtet sich an alle Institutionen, die bereits Cloud Services in Anspruch nehmen oder deren zukünftigen Einsatz planen. Die Gefährdungen und Maßnahmen des Bausteins gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell. Der Baustein Cloud-Nutzung ist immer auf einen konkreten Cloud Service anzuwenden. Nutzt eine Institution einen Verbund von Cloud Services, so sind alle Services einzeln zu modellieren. Die Schnittstelle zwischen den Services ist ebenfalls Gegenstand des Bausteins und muss für alle Services betrachtet werden.

- Der Baustein B 1.18 *Identitäts- und Berechtigungsmanagement* ist für den gesamten Informationsverbund einmal anzuwenden.

**zu Schicht 2: Sicherheit der Infrastruktur**

Die für den vorliegenden Informationsverbund relevanten baulichen Gegebenheiten werden mit Hilfe der Bausteine aus Schicht 2 "Sicherheit der Infrastruktur" modelliert. Jedem Gebäude, Raum oder Schutzschrank (bzw. Gruppen dieser Komponenten) wird dabei der entsprechende Baustein aus den IT-Grundschutz-Katalogen zugeordnet.

- Der Baustein B 2.1 *Allgemeines Gebäude* ist für jedes Gebäude bzw. jede Gebäudegruppe einmal anzuwenden.

- Der Baustein B 2.2 *Elektrotechnische Verkabelung* ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein B 2.1 *Allgemeines Gebäude*). Darüber hinaus kann der Baustein B 2.2 auch für einzelne Räume bzw. Raumgruppen, wie beispielsweise Serverräume oder Rechenzentren, angewendet werden, wenn diese Besonderheiten im Bezug auf die elektro-

technische Verkabelung aufweisen. Für die IT-Verkabelung ist zusätzlich der Baustein B 2.12 *IT-Verkabelung* anzuwenden.

- Der Baustein B 2.3 *Büroraum / Lokaler Arbeitsplatz* ist auf jeden Raum oder Bereich bzw. jede Gruppe von Räumen anzuwenden, in denen sich Mitarbeiter aufhalten, um dort ihre Aufgaben zu erledigen.
- Der Baustein B 2.4 *Serverraum* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Server oder TK-Anlagen betrieben werden. Server sind IT-Systeme, die Dienste im Netz zur Verfügung stellen. Für Räumlichkeiten, auf die der Baustein B 2.9 *Rechenzentrum* angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.
- Der Baustein B 2.5 *Datenträgerarchiv* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Datenträger gelagert oder archiviert werden.
- Der Baustein B 2.6 *Raum für technische Infrastruktur* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen technische Geräte betrieben werden, die keine oder nur wenig Bedienung erfordern (z. B. Verteilerschrank, Netzersatzanlage).
- Der Baustein B 2.7 *Schutzschränke* ist auf jeden Schutzschrank bzw. jede Gruppe von Schutzschränken einmal anzuwenden. Schutzschränke können gegebenenfalls als Ersatz für einen dedizierten Serverraum dienen.
- Der Baustein B 2.8 *Häuslicher Arbeitsplatz* ist auf jeden häuslichen Arbeitsplatz bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.
- Der Baustein B 2.9 *Rechenzentrum* ist auf jedes Rechenzentrum einmal anzuwenden. Als Rechenzentrum werden Einrichtungen und Räumlichkeiten bezeichnet, die für den Betrieb einer größeren, zentral für mehrere Stellen eingesetzten Datenverarbeitungsanlage erforderlich sind. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 *Serverraum* herangezogen werden.
- Der Baustein B 2.10 *Mobiler Arbeitsplatz* ist immer dann anzuwenden, wenn Mitarbeiter häufig nicht mehr nur innerhalb der Räumlichkeiten des Unternehmens bzw. der Behörde arbeiten, sondern an wechselnden Arbeitsplätzen außerhalb. Typische Zielobjekte für den Baustein B 2.10 sind Laptops.
- Der Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume* ist auf jeden solchen Raum bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.
- Der Baustein B 2.12 *IT-Verkabelung* ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein B 2.1 *Allgemeines Gebäude*). Darüber hinaus kann der Baustein B 2.12 auch für einzelne Räume bzw. Raumgruppen, wie beispielsweise Serverräume oder Rechenzentren, angewendet werden, wenn diese Besonderheiten im Bezug auf die IT-Verkabelung aufweisen. Für die elektrotechnische Verkabelung ist zusätzlich der Baustein B 2.2 *Elektrotechnische Verkabelung* anzuwenden.

**zu Schicht 3: Sicherheit der IT-Systeme**

Sicherheitsaspekte, die sich auf IT-Systeme beziehen, werden in dieser Schicht abgedeckt. Diese Schicht ist zur Übersichtlichkeit nach Servern, Clients, Netzkomponenten und Sonstiges sortiert.

Analog zum Bereich "Sicherheit der Infrastruktur" können die Bausteine des Bereichs "Sicherheit der IT-Systeme" sowohl auf einzelne IT-Systeme als auch auf Gruppen solcher IT-Systeme angewandt werden. Dies wird im Folgenden nicht mehr gesondert hervorgehoben.

**Server**

- Der Baustein B 3.101 *Allgemeiner Server* ist auf jedes IT-System anzuwenden, das Dienste (z. B. Datei- oder Druckdienste) als Server im Netz anbietet.

- Der Baustein B 3.102 *Server unter Unix* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.107 *S/390- und zSeries-Mainframe* ist auf jeden Großrechner anzuwenden, der vom Typ S/390 oder zSeries ist.
- Der Baustein B 3.108 Windows Server 2003 ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.109 *Windows Server 2008* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Server (und auch jeden Großrechner) muss neben dem Betriebssystem-spezifischen Baustein immer auch Baustein B 3.101 *Allgemeiner Server* angewandt werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Server zusammengefasst sind.

**Clients**

- Der Baustein B 3.201 *Allgemeiner Client* ist auf jeden Client anzuwenden. Clients sind Arbeitsplatz-Computer, die regelmäßig oder zumindest zeitweise in einem Netz betrieben werden (im Gegensatz zu Einzelplatz-Systemen).
- Der Baustein B 3.202 *Allgemeines nicht vernetztes IT-System* ist auf jedes Einzelplatz-System anzuwenden. Einzelplatz-Systeme sind Arbeitsplatz-Computer, die gar nicht oder nur in Ausnahmefällen in einem Netz betrieben werden (im Gegensatz zu Clients).
- Der Baustein B 3.203 *Laptop* ist auf jeden mobilen Computer (Laptop) anzuwenden.
- Der Baustein B 3.204 *Client unter Unix* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.208 *Internet-PC* ist auf jeden Computer anzuwenden, der *ausschließlich* für die Nutzung von Internet-Diensten vorgesehen ist und nicht mit dem internen Netz der Institution verbunden ist. In diesem speziellen Szenario brauchen *keine weiteren* Bausteine der IT-Grundschutz-Kataloge auf diesen Computer (bzw. diese Gruppe) angewandt werden.
- Der Baustein B 3.209 *Client unter Windows XP* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.210 *Client unter Windows Vista* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.211 *Client unter Mac OS X* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.212 *Client unter Windows 7* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.213 *Client unter Windows 8* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Client muss neben dem Betriebssystemspezifischen Baustein immer auch entweder Baustein B 3.201 *Allgemeiner Client* oder Baustein B 3.202 *Allgemeines nicht vernetztes IT-System* angewandt werden, da in diesen Bausteinen die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.

**Netzkomponenten**

- Der Baustein B 3.301 *Sicherheitsgateway (Firewall)* ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden. Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung (z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Geschäftspartnern). Aber auch bei einer Kopplung von zwei organisationsinternen

Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.

- Der Baustein B 3.302 *Router und Switches* ist in jedem aktiven Netz, das im vorliegenden Informationsverbund eingesetzt wird, anzuwenden.
- Der Baustein B 3.303 *Speicherlösungen / Cloud Storage* ist immer dann anzuwenden, wenn zentrale Speicherlösungen eingesetzt werden. Typische Zielobjekte für diesen Baustein sind NAS-Systeme (Network Attached Storage), SAN-Systeme (Storage Area Networks), Hybrid Storage, Objekt Storage und Cloud Storage.
- Der Baustein B 3.304 *Virtualisierung* ist auf jeden Virtualisierungsserver oder jede Gruppe von Virtualisierungsservern anzuwenden.
- Der Baustein B 3.305 *Terminalserver* ist auf jeden Terminalserver des betrachteten Informationsverbunds anzuwenden.

**Sonstiges**

- Der Baustein B 3.401 TK-Anlage ist auf jede TK-Anlage bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.402 *Faxgerät* ist auf jedes Faxgerät bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.404 *Mobiltelefon* sollte mindestens einmal angewandt werden, wenn die Benutzung von Mobiltelefonen in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist. Bestehen mehrere unterschiedliche Einsatzbereiche von Mobiltelefonen (beispielsweise mehrere Mobiltelefon-Pools), so ist der Baustein jeweils getrennt darauf anzuwenden.
- Der Baustein B 3.405 *Smartphones, Tablets und PDAs* sollte mindestens einmal angewandt werden, wenn die Benutzung von Smartphones, Tablets oder PDAs in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist. Der Baustein B 3.201 *Allgemeiner Client* muss hier nicht zusätzlich angewandt werden.
- Der Baustein B 3.406 *Drucker, Kopierer und Multifunktionsgeräte* sollte mindestens einmal pro Informationsverbund angewandt werden. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste.
- Der Baustein B 3.407 *Eingebettetes System* ist immer anzuwenden, wenn eingebettete Systeme verwendet werden, die nicht fest in einem umgebenden System installiert sind, das nur als Ganzes beschafft werden kann.

**zu Schicht 4: Sicherheit in Netzen**

In dieser Schicht werden Sicherheitsaspekte in Netzen behandelt, die nicht an bestimmten IT-Systemen (z. B. Servern) festgemacht werden können. Vielmehr geht es um Sicherheitsaspekte, die sich auf die Netzverbindungen und die Kommunikation zwischen den IT-Systemen beziehen.

Um die Komplexität zu verringern, ist es sinnvoll, bei der Untersuchung statt des Gesamtnetzes Teilbereiche jeweils einzeln zu betrachten. Die hierzu erforderliche Aufteilung des Gesamtnetzes in Teilnetze sollte anhand der beiden folgenden Kriterien vorgenommen werden:

- Im Rahmen der Schutzbedarfsfeststellung sind Verbindungen identifiziert worden, über die bestimmte Daten auf keinen Fall transportiert werden dürfen. Diese Verbindungen bieten sich als "Schnittstellen" zwischen Teilnetzen an, d. h. die Endpunkte einer solchen Verbindung sollten in verschiedenen Teilnetzen liegen. Umgekehrt sollten Verbindungen, die Daten mit hohem oder sehr hohem Schutzbedarf transportieren, möglichst keine Teilnetzgrenzen überschreiten. Dies führt zu einer Definition von Teilnetzen mit möglichst einheitlichem Schutzbedarf.

- Komponenten, die nur über eine Weitverkehrsverbindung miteinander verbunden sind, sollten nicht demselben Teilnetz zugeordnet werden, d. h. Teilnetze sollten sich nicht über mehrere Standorte oder Liegenschaften erstrecken. Dies ist sowohl aus Gründen der Übersichtlichkeit als auch im Hinblick auf eine effiziente Projektdurchführung wünschenswert.

Falls diese beiden Kriterien nicht zu einer geeigneten Aufteilung des Gesamtnetzes führen (beispielsweise weil einige resultierende Teilnetze zu groß oder zu klein sind), kann die Aufteilung in Teilnetze alternativ auch auf organisatorischer Ebene erfolgen. Dabei werden die Zuständigkeitsbereiche der einzelnen Administratoren(-Teams) als Teilnetze betrachtet.

Es ist nicht möglich, eine grundsätzliche Empfehlung darüber zu geben, welche Aufteilung in Teilnetze zu bevorzugen ist, falls die oben angegebenen Anforderungen mit dem vorliegenden Informationsverbund grundsätzlich nicht vereinbar sind. Stattdessen sollte im Einzelfall entschieden werden, welche Aufteilung des Gesamtnetzes im Hinblick auf die anzuwendenden Bausteine der IT-Grundschutz-Kataloge am praktikabelsten ist.

- Der Baustein B 4.1 *Lokale Netze* ist in der Regel auf jedes Teilnetz einmal anzuwenden. Sind die Teilnetze klein und liegen mehrere Teilnetze in der Zuständigkeit des selben Administrator-Teams kann es jedoch ausreichd sein den Baustein B 4.1 *Lokale Netze* auf diese Teilnetze insgesamt einmal anzuwenden.

- Der Baustein B 4.2 *Netz- und Systemmanagement* ist auf jedes Netz- bzw. Systemmanagement-System anzuwenden, das im vorliegenden Informationsverbund eingesetzt wird.

- Der Baustein B 4.3 *Modem* ist auf alle Außenverbindungen anzuwenden, die über Modems realisiert sind.

- Der Baustein B 4.4 *VPN* ist für jede Art von Fernzugriffen auf den Informationsverbund, also interne Netze oder IT-Systeme, einmal anzuwenden. Hierzu gehören Verbindungen über Datennetze, wie z. B. Site-to-Site-, End-to-End- oder Remote-Access-VPNs, und über Telekommunikationsverbindungen, wie z. B. über analoge Wählleitungen, ISDN- oder Mobiltelefonie.

- Der Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* ist auf alle Außenverbindungen anzuwenden, die über ISDN realisiert sind.

- Der Baustein B 4.6 *WLAN* ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standard-Reihe IEEE 802.11 und deren Erweiterungen realisiert sind.

- Der Baustein B 4.7 *VoIP* ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP-Technologie zum Einsatz kommt. Tauschen leitungsvermittelnde TK-Anlagen Informationen untereinander über ein IP-Netz aus, ist der Baustein B 4.7 VoIP ebenfalls anzuwenden.

- Der Baustein B 4.8 *Bluetooth* ist immer dann anzuwenden, wenn Bluetooth für Kommunikationsverbindungen benutzt wird bzw. IT-Komponenten mit Bluetooth-Schnittstellen in der Institution genutzt werden.

**zu Schicht 5: Sicherheit in Anwendungen**

In der untersten Schicht des zu modellierenden Informationsverbunds erfolgt die Nachbildung der Anwendungen. Moderne Anwendungen beschränken sich nur selten auf ein einzelnes IT-System. Insbesondere behörden- bzw. unternehmensweite Kernanwendungen sind in der Regel als Client-Server-Applikationen realisiert. In vielen Fällen greifen Server selbst wieder auf andere, nachgeschaltete Server, z. B. Datenbank-Systeme, zu. Die Sicherheit der Anwendungen muss daher unabhängig von den IT-Systemen und Netzen betrachtet werden.

- Die Empfehlungen des Bausteins B 5.1 *Peer-to-Peer-Dienste* wurden 2009 in den Baustein B 3.201 *Allgemeiner Client* integriert.

- Der Baustein B 5.2 *Datenträgeraustausch* sollte für jede Anwendung einmal herangezogen werden, die als Datenquelle für einen Datenträgeraustausch dient oder auf diesem Wege eingegangene Daten weiterverarbeitet.

- Der Baustein B 5.3 *Groupware* ist auf jedes Groupware-System (intern oder extern) des betrachteten Informationsverbunds anzuwenden.
- Der Baustein B 5.4 *Webserver* ist auf jeden Server des betrachteten Informationsverbunds anzuwenden, der Webseiten (z. B. Intranet oder Internet) zur Verfügung stellt.
- Der Baustein B 5.5 *Lotus Notes / Domino* ist auf jeden Server mit Lotus Domino und jeden Lotus Notes Client bzw. auf jede entsprechende Gruppe im Informationsverbund einmal anzuwenden.
- Der Baustein B 5.6 *Faxserver* ist auf jeden Faxserver bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 5.7 *Datenbanken* sollte pro Datenbanksystem bzw. pro Gruppe von Datenbanksystemen einmal angewandt werden.
- Der Baustein B 5.8 *Telearbeit* ist bei jedem Telearbeitsplatz bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 5.9 *Novell eDirectory* sollte auf jeden Verzeichnisdienst, der mit Hilfe von Novell eDirectory realisiert ist, einmal angewandt werden. Zusätzlich ist immer der Baustein B 5.15 *Allgemeiner Verzeichnisdienst* anzuwenden.
- Der Baustein B 5.12 *Microsoft Exchange/Outlook* ist - zusätzlich zu Baustein B 5.3 *Groupware* - auf jedes Workgroup- oder E-Mail-System anzuwenden, das auf Microsoft Exchange bzw. Outlook basiert.
- Der Baustein B 5.13 *SAP System* ist auf jede Applikation für Geschäftsprozesse (oder Gruppe solcher Applikationen) anzuwenden, die auf Software des Herstellers SAP basiert.
- Der Baustein B 5.14 *Mobile Datenträger* sollte mindestens einmal pro Informationsverbund angewandt werden.
- Der Baustein B 5.15 *Allgemeiner Verzeichnisdienst* sollte - unabhängig vom gewählten Produkt - auf jeden Verzeichnisdienst einmal angewandt werden.
- Der Baustein B 5.16 *Active Directory* sollte auf jeden Verzeichnisdienst, der mit Hilfe von Microsoft Active Directory realisiert ist, einmal angewandt werden. Zusätzlich ist immer der Baustein B 5.15 *Allgemeiner Verzeichnisdienst* anzuwenden.
- Der Baustein B 5.17 *Samba* ist auf jedem Samba-Server des betrachteten Informationsverbunds anzuwenden.
- Der Baustein B 5.18 *DNS-Server* ist auf jeden im Informationsverbund betriebenen DNS-Server bzw. auf jede Gruppe von DNS-Servern anzuwenden.
- Der Baustein B 5.19 Internet-Nutzung ist immer dann anzuwenden, wenn Internet-Dienste vom Arbeitsplatz genutzt werden sollen.
- Der Baustein B 5.20 *OpenLDAP* sollte auf jeden Verzeichnisdienst, der mit Hilfe von OpenLDAP realisiert ist, einmal angewandt werden. Zusätzlich ist immer der Baustein B 5.15 *Allgemeiner Verzeichnisdienst* anzuwenden.
- Der Baustein B 5.21 *Webanwendungen* ist auf jeden als Webanwendung ausgelegten Web-Dienst (z. B. Intranet oder Internet) des betrachteten Informationsverbunds anzuwenden.
- Der Baustein B 5.22 *Protokollierung* ist zumindest bei größeren Informationsverbünden anzuwenden, also wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei kleineren und wenig komplexen Informationsverbünden reicht die Umsetzung von M 2.500 *Protokollierung von IT-Systemen* aus.
- Der Baustein B 5.23 *Cloud Management* richtet sich an Cloud-Diensteanbieter (Cloud Service Provider) und ist auf jeden Server des Informationsverbunds anzuwenden, der zur Verwaltung der Cloud

Computing Plattform eingesetzt wird. Oft werden mehrere Server eingesetzt werden, um die vielfältigen Verwaltungsaufgaben durchführen zu können. In solchen Fällen ist jeder Server einzeln zu modellieren. Detaillierte Hinweise zur Modellierung finden sich in der W-Maßnahme M 2.524 *Modellierung von Cloud Management*.

- Der Baustein B 5.24 *Web-Services* ist auf jede als Web-Service ausgelegte Anwendung anzuwenden. Für komplexe Anwendungen, die einerseits als Web-Anwendung realisiert sind, andererseits aber auch Web-Services für andere IT-Systeme bereitstellen, soll neben dem vorliegenden Baustein auch der Baustein B 5.21 *Webanwendungen* modelliert werden.
- Der Baustein B 5.25 *Allgemeine Anwendungen* ist auf den Informationsverbund anzuwenden, wenn spezialisierte Anwendungssoftware eingesetzt wird. Hierzu gehört Individualsoftware, Standardsoftware mit eigenen Anpassungen, und Standardsoftware, entsprechend der Fachaufgaben und der Sicherheitsvorgaben konfiguriert wird.
- Der Baustein B 5.26 *Serviceorientierte Architektur* ist immer anzuwenden, wenn verteilte Services in Form einer SOA eingesetzt werden.
- Der Baustein B 5.27 *Software-Entwicklung* ist immer anzuwenden, wenn Software in der Institution eigenständig oder von einem externen Auftragnehmer entwickelt oder individuell angepasst wird.

**Prüfung auf Vollständigkeit**

Abschließend muss überprüft werden, ob die Modellierung des Gesamtsystems vollständig ist und keine Lücken aufweist. Es wird empfohlen, hierzu erneut den Netzplan oder eine vergleichbare Übersicht über den Informationsverbund heranzuziehen und die einzelnen Komponenten systematisch durchzugehen. Jede Komponente muss entweder einer Gruppe zugeordnet oder einzeln modelliert worden sein.

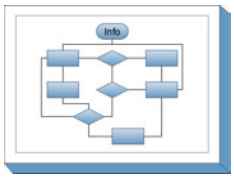
Falls das Gesamtnetz in der Schicht 4 in Teilnetze aufgeteilt wurde, muss geprüft werden, ob

- jedes Teilnetz vollständig nachgebildet wurde und
- durch die Summe aller Teilnetze das Gesamtnetz vollständig dargestellt wird.

Wichtig ist, dass nicht nur alle Hard- und Software-Komponenten in technischer Hinsicht nachgebildet sind, sondern dass auch die zugehörigen organisatorischen, personellen und infrastrukturellen Aspekte vollständig abgedeckt sind.

Falls sich bei der Überprüfung Lücken in der Modellierung zeigen, sind die entsprechenden fehlenden Bausteine hinzuzufügen. Andernfalls besteht die Gefahr, dass wichtige Bestandteile des Gesamtsystems oder wichtige Sicherheitsaspekte bei der Anwendung des IT-Grundschutzes nicht berücksichtigt werden.

# 3 Rollen




In den Maßnahmen werden neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, Verantwortliche für die Initiierung bzw. für die Umsetzung dieser Maßnahmen beispielhaft genannt. Da die Bezeichnungen der hier als Verantwortliche genannten Personen oder Rollen nicht in allen Organisationen einheitlich sind, wird für eine leichtere Zuordnung in diesem Kapitel eine kurze Beschreibung der wesentlichen Rollen dargestellt.

| **Verantwortliche** | **Rollenbeschreibung** |
|---|---|
| Administrator | Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems. |
| Änderungsmanager | Der Änderungsmanager (Change Manager) hat die Aufgabe, ein effizientes und effektives Patch- und Änderungsmanagement zu betreiben. Aufgabe des Änderungsmanager ist es, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten. |
| Anforderungsmanager | Der Anforderungsmanager (Compliance Manager) ist verantwortlich dafür, die für die Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren und deren Einhaltung zu prüfen. |
| Anwendungsentwickler | Ein Anwendungsentwickler ist ein mit der Planung, Entwicklung, Test oder Pflege von Programmen betrauter Experte. |
| Archivverwalter | Der Archivverwalter hat die Aufgaben Einrichtung, Betrieb, Überwachung und Wartung eines Archivsystems auf fachlicher Ebene. |
| Bauleiter | Ein Bauleiter ist für die Umsetzung von Baumaßnahmen zuständig. |
| Behörden-/Unternehmensleitung | Dies bezeichnet die Leitungsebene der Institution bzw. der betrachteten Organisationseinheit. |
| Benutzer | Ein Benutzer ist ein Mitarbeiter des Unternehmens bzw. der Behörde, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt.<br><br>IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben benutzt. |
| Beschaffer | Dies bezeichnet einen Mitarbeiter der Beschaffungsstelle, dessen Aufgabe die Beschaffung von Betriebsmitteln oder IT-Systemen ist. |

| Verantwortliche | Rollenbeschreibung |
|---|---|
| Beschaffungsstelle | Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab. |
| Brandschutzbeauftragter | Ein Brandschutzbeauftragter ist Ansprechpartner und Verantwortlicher in allen Fragen des Brandschutzes. Er ist u. a. zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen. |
| Datenschutzbeauftragter | Ein Datenschutzbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung bestellte Person, die auf den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde hinwirkt. |
| Entwickler | Mit Entwickler wird im Kontext des IT-Grundschutzes eine Person bezeichnet, die bei der Entwicklung von Software, Hardware oder ganzen Systemen mitarbeitet.<br><br>Im IT-Grundschutz werden unter der Rolle Entwickler verschiedene weitere Rollen zusammengefasst, wie z. B. Software-Architekt, Software-Designer, Software-Entwickler, Programmierer und Tester. |
| Errichterfirma | Es handelt sich hierbei um ein Unternehmen, das Gewerke oder aber auch Gebäude erstellt. |
| Fachabteilung | Eine Fachabteilung ist ein Teil einer Behörde bzw. eines Unternehmens, welche fachspezifische Aufgaben zu erledigen hat. Bei Bundes- und Landesbehörden ist eine Abteilung die übergeordnete Organisationsform mehrerer Referate, die inhaltlich zusammengehören. |
| Fachverantwortliche | Der Fachverantwortliche ist inhaltlich für ein oder mehrere Geschäftsprozesse oder Fachverfahren verantwortlich (so ist z. B. der Leiter des Referats "Vertrieb" der Fachverantwortliche für die Anwendung "automatisierter Vertrieb"). |
| Fax-Poststelle | Die Fax-Poststelle ist für alle organisatorischen und technischen Regelungen verantwortlich, die die Fax-Nutzung innerhalb einer Organisationseinheit betreffen. |
| Fax-Verantwortlicher | Der Fax-Verantwortliche ist für alle organisatorischen und technischen Regelungen verantwortlich, die die Fax-Nutzung innerhalb einer Organisationseinheit betreffen. |
| Haustechnik | Haustechnik bezeichnet die Organisationseinheit, die sich um die Einrichtungen der Infrastruktur in einem Gebäude oder in einer Liegenschaft kümmert. Betreute Gewerke können dabei z. B. sein: Elektrotechnik, Melde- und Steuerungstechnik, Siche- |

| Verantwortliche | Rollenbeschreibung |
|---|---|
| | rungstechnik, IT-Netze (Physikalischer Teil), Heizungs- und Sanitärtechnik, Aufzüge etc. |
| Informationssicherheitsmanagement | Informationssicherheitsmanagement oder kurz IS-Management (häufig auch IT-Sicherheitsmanagement) ist die Leitungs- und Koordinierungsaufgabe, die für eine angemessene Informationssicherheit im Unternehmen bzw. in der Behörde sorgt. Dieser Begriff wird jedoch häufig auch für Personen verwendet, die diese Leitungsaufgabe wahrnehmen. |
| Innerer Dienst | Der Innere Dienst ist eine Organisationseinheit, die alle zentralen Dienste für die Mitarbeiter koordiniert, z. B. Poststelle, Kopierer, Fahrdienst, Botendienst, Beseitigung technischer Störungen, Gebäudereinigung, Bereitstellung von Betriebsmitteln etc. |
| IS-Management-Team | Das IS-Management-Team (häufig auch IT-Sicherheitsmanagement-Team) unterstützt den IT-Sicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt. |
| IT-Betreuer | Zu den Aufgaben von IT-Betreuern zählen u. a. die Entgegennahme und Bearbeitung von Benutzeranfragen zu Problemen rund um die IT-Ausstattung. |
| IT-Sicherheitsbeauftragter | Ein IT-Sicherheitsbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung ernannte Person, die im Auftrag der Leitungsebene die Aufgabe Informationssicherheit koordiniert und innerhalb der Behörde bzw. des Unternehmens vorantreibt. |
| Leiter Beschaffung | Hiermit ist der Leiter der Beschaffungsstelle oder der Organisationseinheit gemeint, die für die Beschaffung zuständig ist. |
| Leiter Entwicklung | Dies bezeichnet den Leiter einer Entwicklungsabteilung für Hard- bzw. Software oder den Projektleiter eines Entwicklerteams. |
| Leiter Fachabteilung | Dies bezeichnet den Leiter einer Fachabteilung. |
| Leiter Haustechnik | Hiermit ist der Verantwortliche für die Haustechnik gemeint. |
| Leiter Innerer Dienst | Dies bezeichnet den Leiter des Inneren Dienstes bzw. den Verantwortlichen für die Bereitstellung zentraler Dienste. |
| Leiter IT | Hiermit ist der Leiter der IT-Abteilung bzw. das für die Informationstechnik zuständige Management gemeint. |
| Leiter Organisation | Dies bezeichnet den Leiter der Organisationseinheit, die u. a. für Regelung und Überwachung des allgemeinen Betriebs sowie für Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen verantwortlich ist. |

| Verantwortliche | Rollenbeschreibung |
|---|---|
| Leiter Personal | Hiermit ist der Leiter der Personalabteilung bzw. der für Personalfragen zuständigen Organisationseinheit gemeint. |
| Mitarbeiter | Ein Mitarbeiter ist Mitglied einer Fachabteilung, einer Behörde oder eines Unternehmens. |
| Notfallbeauftragter | Der Notfallbeauftragte steuert alle Aktivitäten rund um das Notfallmanagement. Er ist für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente, Regelungen und Maßnahmen zuständig. Er analysiert den Gesamtablauf der Notfallbewältigung nach einem Schadensereignis. |
| Personalabteilung | Die Personalabteilung ist unter Anderem für folgende Aufgaben zuständig:<br>- Personalwirtschaftliche Grundfragen<br>- Personalbedarfsplanung<br>- Personalangelegenheiten der Mitarbeiter<br>- Soziale Betreuung der Mitarbeiter<br>- Allgemeine Zusammenarbeit mit der Personalvertretung |
| Personalrat/Betriebsrat | Der Personal- bzw. Betriebsrat (Personalvertretung) ist für die Interessenvertretung der Mitarbeiter gegenüber der Behörden- bzw. Unternehmensleitung zuständig. |
| Planer | Mit dem allgemeinen Begriff "Planer" werden Rollen wie "Netzplaner" und "Bauplaner" zusammengefasst. Gemeint sind also Personen, die für die Planung und Konzeption bestimmter Aufgaben zuständig sind. |
| Poststelle | Die Poststelle ist die Sammelstelle einer Behörde oder eines Unternehmens für ankommende und ausgehende Post. Zu den Aufgabengebieten können auch Fax- und E-Mail-Dienstleistungen sowie das Scannen eingehender Dokumente im Rahmen eines elektronischen Workflows gehören. |
| Pressestelle | Die Pressestelle ist zuständig für alle ein- und ausgehenden Kontakte zu Presse und Medien. In vielen Fällen werden dort auch Anfragen von Privatpersonen und Firmen bearbeitet. |
| Revisor | Ein Revisor kontrolliert, ob die geplanten Maßnahmen adäquat umgesetzt wurden. |
| Telearbeiter | Ein Telearbeiter nimmt seine Tätigkeiten außerhalb der Büroräume des Unternehmens oder der Behörde wahr und verfügt über eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers. |
| Tester | Tester sind Personen, die gemäß eines Testplans nach vorher festgelegten Verfahren und Kriterien eine neue oder veränderte Software bzw. Hardwa- |

| Verantwortliche | Rollenbeschreibung |
|---|---|
| | re testen und die Testergebnisse mit den erwarteten Ergebnissen vergleichen. |
| TK-Anlagen-Verantwortlicher | Der TK-Anlagen-Verantwortliche ist für den ordnungsgemäßen Betrieb der Telekommunikationsanlagen und für entsprechende Regelungen zuständig. |
| Verantwortliche der einzelnen Anwendungen | Der Verantwortliche für die einzelne Anwendung ist nicht nur für den reibungslosen Betrieb der Anwendung zuständig, sondern auch für die Initiierung und Umsetzung von Sicherheitsmaßnahmen für diese Anwendung. |
| Verantwortliche für die Datensicherung | Der Verantwortliche für die Datensicherung ist zuständig für die Erstellung, Pflege, regelmäßige Aktualisierung und Umsetzung eines Datensicherungskonzeptes. |
| Vertragsmanagement | Vertragsmanagement ist die gemeinsame Fachaufgabe der Beschaffungsstelle und des Vertriebs und beinhaltet die Planung, Steuerung und Fortentwicklung aller Verträge mit Dienstleistern, Lieferanten und sonstigen Stellen, die zur Beschaffung oder zum Vertrieb von Gütern und Dienstleistungen der Institution notwendig sind. |
| Vertrieb | Der Vertrieb ist die zuständige Stelle für alle Aktivitäten, die für das Vertreiben von Gütern und Dienstleistungen einer Institution notwendig sind. |
| Vorgesetzte | Als Vorgesetzte werden die Mitarbeiter einer Institution bezeichnet, die gegenüber anderen, ihnen zugeordneten Mitarbeitern weisungsbefugt sind. |

# 4 Glossar und Begriffsdefinitionen

In diesem Glossar werden einige wichtige Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert.

## Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computernetze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzerkennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

## Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

## Application-Level-Gateway (ALG)

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog.

Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern.

## Authentisierung (englisch "authentication")

Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.

## Authentizität

Mit dem Begriff Authentizität wird die Echtheit der Identität eines Kommunikationspartners bzw. die Echtheit der Herkunft von Daten bezeichnet. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch im Bezug auf IT-Komponenten oder Anwendungen.

## Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

## Basis-Sicherheitscheck

Der Begriff bezeichnet gemäß IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Maßnahmen in einer Organisation bereits umgesetzt sind und welche grundlegenden Sicherheitsmaßnahmen noch fehlen.

## Baustein

Der Begriff dient zur Strukturierung von Empfehlungen der IT-Grundschutz-Kataloge. Bausteine sind die Einheiten innerhalb einer Schicht (z. B. IT-Systeme, Netze). Sie beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie Notfallmanagement) und besondere Einsatzformen (wie Häuslicher Arbeitsplatz). In jedem Baustein werden der betrachtete Aspekt bzw. die betrachtete IT-Komponente und die Gefährdungslage beschrieben sowie organisatorische und technische Sicherheitsmaßnahmen empfohlen.

## Bedrohung (englisch "threat")

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

## Benutzerkennung (häufig auch Benutzerkonto)

Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine Kombination aus Buchstaben und/oder Ziffern.

## BIA (Business Impact Analyse)

Eine Business Impact Analyse (Folgeschädenabschätzung) ist eine Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden. Es ist ein Verfahren, um kritische Ressourcen und Wiederanlaufanforderungen sowie die Auswirkungen von ungeplanten Geschäftsunterbrechungen zu identifizieren.

## Biometrie

Unter Biometrie ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale zu verstehen. Diese kann genutzt werden, um Benutzer auf Grundlage besonderer Merkmale eindeutig zu authentisieren. Ein oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris
- Fingerabdruck
- Gesichtsproportionen
- Stimme und Sprachverhalten
- Handschrift
- Tippverhalten am Rechner

## Blackbox-Test

Bei Blackbox-Tests wird das Verhalten von Außentätern simuliert, wobei vorausgesetzt wird, dass der Angreifer keine oder nur oberflächliche Informationen über sein Angriffsziel hat.

## Browser

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

## Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

## Client

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

## Computer-Virus

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

## Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Für den Begriff "Datenschutz" existieren zwei englische Übersetzungen: Dabei bezeichnet "data protection" den Datenschutz als Rechtsbegriff. "Privacy" zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld und mittlerweile auch im EU-Raum vermehrt genutzt.

## Datenschutz-Management

Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

## Datensicherheit

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist "Informationssicherheit".

## Datensicherung (englisch "Backup")

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustandes von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen

dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

## Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz.

DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter - Application-Level-Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

## Digitale Signatur

Eine digitale Signatur ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

## Ergänzende Sicherheitsanalyse

Diese Analyse ist nach IT-Grundschutz erforderlich, wenn Zielobjekte des betrachteten Informationsverbunds einen erhöhten Schutzbedarf haben, nicht geeignet modelliert werden können oder in untypischen Einsatzszenarien betrieben werden. Die Vorgehensweise hierzu ist im BSI-Standard 100-2 "IT-Grundschutz-Vorgehensweise" beschrieben. Die ergänzende Sicherheitsanalyse dient dazu festzustellen, für welche Teile des Informationsverbunds eine Risikoanalyse notwendig ist.

## Firewall

Eine Firewall (besser mit Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (siehe Sicherheitsgateway).

## Gefahr

"Gefahr" wird oft als übergeordneter Begriff gesehen, wohingegen unter "Gefährdung" eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Beispiel: Die Gefahr ist ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder einen Dieb entstehen, der die Festplatte stiehlt. Die Gefährdungen sind dann "defekter Datenträger" und "Diebstahl von Datenträgern". Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, "Gefahr" und "Gefährdung" als gleichbedeutend aufzufassen.

## Gefährdung (englisch "applied threat")

Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenverseuchte Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Computer-Viren-Typ ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

## Gefährdungskataloge

Gefährdungskataloge sind Teil der IT-Grundschutz-Kataloge und enthalten Beschreibungen möglicher Gefährdungen der Informationstechnik. Sie sind in die Schadensursachen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen gegliedert.

## Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit
- Nichtabstreitbarkeit

## Hintertür (englisch "backdoor")

Hintertüren sind Schadprogramme, die dazu dienen, einen unbefugten Zugang zu einem IT-System offen zu halten, der einen unbemerkten Einbruch in das System ermöglicht und dabei möglichst weitgehende Zugriffsrechte besitzt, beispielsweise um Angriffsspuren zu verstecken.

## Informationssicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

## Informationssicherheitsmanagement (IS-Management)

Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Aus den gleichen Gründen, die oben für die Begriffe "Informationssicherheit" und "IT-Sicherheit" genannt sind, wird im IT-Grundschutz noch häufig der Begriff "IT-Sicherheitsmanagement" verwendet.

## Informationstechnik (IT)

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

## Informationsverbund

Unter einem Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund

kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

## Infrastruktur

Beim IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die IT-Systeme und Netzkoppelelemente gehören nicht dazu.

## Institutionen

Mit dem Begriff Institutionen werden in diesem Dokument Unternehmen, Behörden und sonstige öffentliche oder private Organisationen bezeichnet.

## Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

## Intranet

Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch eine Firewall abgesichert.

## IS-Management-Team

In größeren Institutionen ist es sinnvoll, ein IS-Management-Team (häufig auch IT-Sicherheitsmanagement-Team) aufzubauen, das den IT-Sicherheitsbeauftragten unterstützt, beispielsweise indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

## IT-Grundschutz

IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen, Institutionen mit normalem Schutzbedarf hinreichend absichern.

## IT-Grundschutzanalyse

Zu einer IT-Grundschutzanalyse gehören die Modellierung mit der Ermittlung der notwendigen Sicherheitsmaßnahmen und der Basis-Sicherheitscheck, in dem ein Soll-Ist-Vergleich den aktuellen Umsetzungsgrad von Sicherheitsmaßnahmen in einem Unternehmen oder einer Behörde beschreibt.

## IT-Sicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und

Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

## IT-Sicherheitsbeauftragter

Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, der für alle Aspekte rund um die Informationssicherheit, Mitwirkung im Sicherheitsprozess und IS-Management-Team zuständig ist, die Leitlinie zur Informationssicherheit, das Sicherheitskonzept und andere Konzepte z. B. für Notfallvorsorge koordinierend erstellt und deren Umsetzung plant und überprüft.

Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution anders genannt. Häufige Titel sind IT-Sicherheitsbeauftragter oder kurz IT-SiBe, Chief Security Officer (CSO), Chief Information Security Officer (CISO) oder Information Security Manager. Mit dem Titel "Sicherheitsbeauftragter" werden dagegen häufig die Personen bezeichnet, die für Arbeitsschutz, Betriebssicherheit oder Werkschutz zuständig sind.

## IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

## Keylogger

Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

## Komponenten

Als Komponenten werden im IT-Grundschutz technische Zielobjekte (siehe dort) oder Teile von Zielobjekten bezeichnet.

## Kumulationseffekt

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, so dass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

## Leitlinie zur Informationssicherheit

Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

## Mandantenfähigkeit

Als mandantenfähig werden Anwendungen, IT-Systeme oder auch Dienstleistungen bezeichnet, bei denen die Prozesse, Informationen und Anwendungen eines Mandanten strikt von denen anderer Kunden getrennt sind, also keine Zugriffe oder Störungen von dem einen in den anderen Bereich möglich sind und somit auch deren Vertraulichkeit, Integrität oder Verfügbarkeit nicht beeinträchtigt werden kann.

## Maßnahmenkataloge

In den IT-Grundschutz-Katalogen werden zu jedem Baustein passende Maßnahmen empfohlen. Diese sind in Katalogen zusammengefasst, die in Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge gegliedert sind.

## Maximum-Prinzip

Nach dem Maximum-Prinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.

## Modellierung

Bei der Vorgehensweise nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen nachgebildet. Hierzu enthält Kapitel 2.2 der IT-Grundschutz-Kataloge für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.

## Netzplan

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

## Nichtabstreitbarkeit (englisch "non repudiation"):

Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

## Paketfilter

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr in einem Netz anhand spezieller Regeln filtern. Aufgabe eines Paketfilters ist es, Datenpakete anhand der Informationen in den Header-Daten der UDP/IP- bzw. TCP/IP-Schicht (z. B. IP-Adresse und Portnummer) weiterzuleiten oder zu verwerfen. Diese Entscheidung treffen Paketfilter anhand der vom Anwender vorgegebenen Filterregeln. Vielfach bieten die Paketfilter auch eine Möglichkeit zur "Network Address Translation" (NAT), bei der die Absender-Adressen von IP-Paketen durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes verdeckt.

## Patch

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

## Penetrationstest

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

## Privilegierte Berechtigungen

Privilegierte oder administrative Berechtigungen umfassen weitergehende Zugriffsmöglichkeiten auf IT-Systeme oder Software-Komponenten, als für normale Benutzer erforderlich sind. In der Regel werden privilegierte Berechtigungen nur solchen Rollen, Gruppen oder Personen zugewiesen, die überwiegend mit der Administration von Informationstechnik betraut sind. Dazu gehört unter anderem die betriebliche und/oder sicherheitstechnische Konfiguration.

## Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

## Qualifizierungsstufe

Die IT-Grundschutz-Methodik sieht drei Qualifizierungsstufen vor: "A" für die IT-Grundschutz-Einstiegsstufe, "B" für die IT-Grundschutz-Aufbaustufe, "C" für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz. Mit "Z" werden Maßnahmen bezeichnet, die Ergänzungen darstellen, die vor allem bei höheren Sicherheitsanforderungen hilfreich sein können. Mit "W" gekennzeichnete Maßnahmen dienen ausschließlich der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der anderen Maßnahmen hilfreich sind.

## Revision

Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-)Richtlinien. Die Revision sollte unabhängig und neutral sein.

## Risiko

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.

Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

## Risikoanalyse (englisch "Risk Assessment / Analysis")

Mit einer Risikoanalyse wird untersucht, welche schädigenden Ereignisse eintreten können, wie wahrscheinlich das Eintreten eines schädigenden Ereignisses ist und welche negativen Folgen der Schaden hätte.

## Rootkit

Ein Rootkit ist ein Schadprogramm, das manipulierte Versionen von Systemprogrammen enthält. Unter Unix sind dies typischerweise Programme wie login, ps, who, netstat etc. Die manipulierten Systemprogramme sollen es einem Angreifer ermöglichen, zu verbergen, dass er sich erfolgreich einen Zugriff mit Administratorenrechten verschafft hat, so dass er diesen Zugang später erneut benutzen kann.

## Schadfunktion

Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

## Schadprogramm / Schadsoftware / Malware

Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus "Malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

## Schutzbedarf

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

## Schutzbedarfsdefinitionen

Dies sind auf die jeweils betrachtete Institution angepasste Kriterien, anhand derer entschieden werden kann, welche Schutzbedarfskategorie auf eine IT-Komponente anzuwenden ist.

## Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit - Vertraulichkeit, Integrität oder Verfügbarkeit - entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

## Schwachstelle (englisch "vulnerability")

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

## Server

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (nämlich Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server. Zu häufiger Verwirrung führen X-Server, da ein X-Server-Prozess typischerweise auf einem Arbeitsplatzrechner, also einem Client in einem Server-Client-Netz, läuft.

## Sicherheitsgateway

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.

## Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

## Sicherheitskonzeption

Die Erstellung einer Sicherheitskonzeption ist eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

## Sicherheitsmaßnahme

Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als

auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde "safeguard", "security measure" oder "measure" gewählt. Im englischen Sprachraum wird neben "safeguard" außerdem häufig der Begriff "control" verwendet.

## Sicherheitspolitik

Hierbei handelt es sich um eine falsche Übersetzung des englischen Begriffs "Security Policy", siehe Sicherheitsrichtlinie.

## Sicherheitsrichtlinie (englisch "Security Policy")

In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

## Spyware

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

## Standardsoftware

Unter Standardsoftware wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

## Starke Authentisierung

Starke Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bezeichnet.

## Strukturanalyse

In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

## Trojanisches Pferd

Ein Trojanisches Pferd, oft auch (fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

## Verbindlichkeit

Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

## Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

## Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.

## Verteilungseffekt

Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen.

## Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

## VLAN

Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.

## VPN

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

## Wert (englisch "asset")

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

## WLAN

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

## Wurm

Bei (Computer-, Internet-, E-Mail-)Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.

## Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem:

- IT-Grundschutz-Zertifikat: Damit kann dokumentiert werden, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsmaßnahmen gemäß IT-Grundschutz-Vorgehensweise realisiert wurden. Dieses Zertifizierungsverfahren wurde durch die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz (siehe unten) abgelöst.

- ISO 27001-Zertifikate: Der ISO-Standard 27001 "Information technology - Security techniques - Information security management systems requirements specification" ermöglicht eine Zertifizierung des Informationssicherheitsmanagements.
- ISO 27001-Zertifikate auf der Basis von IT-Grundschutz: Seit Anfang 2006 können ISO 27001-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-Grundschutz-Auditors gehören eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen Sicherheitsmaßnahmen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es.
- Schlüsselzertifikat: Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehören.
- Zertifikate für IT-Produktsicherheit: Zertifiziert wird nach international anerkannten Sicherheitskriterien, wie z. B. den Common Criteria (ISO/IEC 15408). Auf dieser Basis können Produkte und Systeme unterschiedlichster Art evaluiert werden. Eine wesentliche Voraussetzung ist jedoch, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen.
- Zertifikat von Schutzprofilen (Profil-Zertifikate): Mit Schutzprofilen wird bei den Common Criteria Anwendergruppen und Herstellern die Möglichkeit gegeben, produktklassentypische und dienstleistungsspezifische Sicherheitsanforderungen festzulegen. Die Berücksichtigung von Schutzprofilen bei der Produktentwicklung erleichtert deren Evaluierung und führt zu Produkten, die in besonderem Maße den anwenderspezifischen Anforderungen entsprechen. Auch Schutzprofile können evaluiert und zertifiziert werden.

## Zielobjekt

Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus den IT-Grundschutz-Katalogen zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, wie beispielsweise Netze oder IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.

## Zugang

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet.

Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

## Zugriff

Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet.

Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

## Zutritt

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet.

Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

# B 1 Übergreifende Aspekte

# B 1.0 Sicherheitsmanagement


## Beschreibung

Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch kurz als IS-Management bezeichnet.

Der Begriff Informationssicherheit ist umfassender als der Begriff IT-Sicherheit und wird aufgrund dessen zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

Dieser Baustein soll aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes. Der Baustein baut auf dem BSI-Standard 100-1 *Managementsysteme für Informationssicherheit* und BSI-Standard 100-2 *Vorgehensweise nach IT-Grundschutz* auf und fasst die wichtigsten Aspekte zum Sicherheitsmanagement hieraus zusammen.

## Gefährdungslage

Gefährdungen im Umfeld des Sicherheitsmanagements können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

### Organisatorische Mängel

- G 2.66 *Unzureichendes Sicherheitsmanagement*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*
- G 2.106 *Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen*
- G 2.107 *Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement*

### Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für Informationssicherheit bewusst ist. Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen

umgesetzt wird (siehe M 2.336 *Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene*).

Weiterhin muss ein kontinuierlicher Sicherheitsprozess etabliert und eine für die jeweilige Institution passende Sicherheitsstrategie festgelegt werden (siehe M 2.335 *Festlegung der Sicherheitsziele und -strategie*). Die Leitungsebene muss hierfür wie für alle weiteren Sicherheitsfragen eine Person als Hauptverantwortlichen benennen. Diese ist dafür zuständig, eine geeignete Organisationsstruktur für Informationssicherheit aufzubauen und aufrechtzuerhalten (siehe M 2.193 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit*). Als eine der ersten Aktionen sollte eine Leitlinie zur Informationssicherheit erstellt werden (siehe M 2.192 *Erstellung einer Leitlinie zur Informationssicherheit*).

Informationssicherheit muss in allen Bereichen der Institution gelebt werden (siehe M 2.337 *Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse*). Dazu gehört neben der Erarbeitung eines Sicherheitskonzepts (siehe M 2.195 *Erstellung eines Sicherheitskonzepts*) auch die Integration der Mitarbeiter in den Sicherheitsprozess (siehe M 2.197 *Integration der Mitarbeiter in den Sicherheitsprozess*) sowie die Erstellung von zielgruppengerechten Sicherheitsrichtlinien (siehe M 2.338 *Erstellung von zielgruppengerechten Sicherheitsrichtlinien*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Sicherheitsmanagement" vorgestellt.

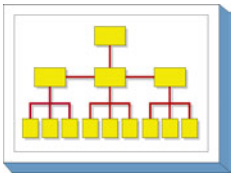
**Planung und Konzeption**
- M 2.192 (A) *Erstellung einer Leitlinie zur Informationssicherheit*
- M 2.335 (A) *Festlegung der Sicherheitsziele und -strategie*
- M 2.336 (A) *Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene*

**Umsetzung**
- M 2.193 (A) *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit*
- M 2.195 (A) *Erstellung eines Sicherheitskonzepts*
- M 2.197 (A) *Integration der Mitarbeiter in den Sicherheitsprozess*
- M 2.337 (A) *Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse*
- M 2.338 (Z) *Erstellung von zielgruppengerechten Sicherheitsrichtlinien*
- M 2.339 (Z) *Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit*
- M 2.475 (A) *Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten*

**Betrieb**
- M 2.199 (A) *Aufrechterhaltung der Informationssicherheit*
- M 2.200 (C) *Management-Berichte zur Informationssicherheit*
- M 2.201 (C) *Dokumentation des Sicherheitsprozesses*

**Notfallvorsorge**
- M 6.16 (Z) *Abschließen von Versicherungen*

# B 1.1 Organisation



## Beschreibung

In diesem Baustein werden allgemeine und übergreifende Maßnahmen im Organisationsbereich aufgeführt, die als organisatorische Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus erforderlich sind. Spezielle Maßnahmen organisatorischer Art, die in unmittelbarem Zusammenhang mit anderen Maßnahmen stehen (z. B. LAN-Administration), werden in den entsprechenden Bausteinen aufgeführt. Auf das ordnungsgemäße Management informationstechnischer Komponenten (Hardware oder Software) ausgerichtete Standard-Sicherheitsmaßnahmen befinden sich im Baustein B 1.9 *Hard- und Software-Management*.

## Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.5 *Fehlende oder unzureichende Wartung*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.8 *Unkontrollierter Einsatz von Betriebsmitteln*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*
- G 5.6 *Anschlag*
- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.68 *Unberechtigter Zugang zu den aktiven Netzkomponenten*
- G 5.102 *Sabotage*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Mindestschutzniveau kann in einer Institution nur erreicht werden, wenn übergreifende Regelungen zur Informationssicherheit verbindlich festgelegt werden. Hierzu sind eine Reihe von Maßnahmen umzusetzen, beginnend mit Festlegung und Zuweisung von verantwortlichen Personen für einzelne Objekte (z. B. Informationen, Geschäftsprozesse, Anwendungen, IT-Komponenten) über entsprechende organisatorische Handlungsanweisungen bis hin zur Behandlung von schützenswerten Betriebsmitteln. Die Schritte, die dabei im Sinne eines kontinuierlichen Informationssicherheitsprozesses durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Für die Initiierung und die Umsetzung der sich aus den Sicherheitszielen und Sicherheitsrichtlinien ergebenden Prozesse sind organisatorische und personelle Festlegungen zu treffen. Hierbei sind gegebenenfalls die Mitbestimmungsrechte der Personalvertretung zu wahren (siehe M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*). Die verschiedenen Organisationsebenen und die hier tätigen Personen benötigen konkrete Handlungsanweisungen und Verantwortlichkeiten zur Abwicklung der sie betreffenden Prozesse (siehe M 2.225 *Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten*).

Die strategischen Überlegungen sind in einem Betriebskonzept bezüglich ihrer Umsetzung im Unternehmen bzw. in der Behörde zu detaillieren.

Der Einsatz der erforderlichen Betriebsmittel ist auf die Aufgabenerfüllung und die Sicherheitsanforderungen abzustimmen und über eine Betriebsmittelverwaltung (siehe M 2.2 *Betriebsmittelverwaltung*) zu dokumentieren. Diese muss vollständig sein und durch entsprechende Prozesse auch jederzeit aktuell gehalten werden.

Voraussetzung für eine funktionierende Infrastruktur, die auch auf Störungen adäquat reagieren kann, sind Regelungen für Ersatzteilbeschaffung, Reparaturen und Wartungsarbeiten (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*). In Wartungsverträgen ist die terminliche und inhaltliche Wartung einzelner IT-Systeme (oder Gruppen) verbindlich zu regeln, ebenso wie die erforderlichen Zugänge (Remote, vor Ort) und die an die Sicherheitsanforderungen angepassten Reaktionszeiten des mit der Wartung beauftragten Personals.

Die Aufgabenverteilung und die hierfür erforderlichen Funktionen (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten.

**Betrieb**

Die festgelegten Konzeptionen werden in konkrete Handlungsanweisungen gefasst und für den Betrieb verbindlich verabschiedet. Mitarbeiterbezogene Regelungen müssen hierbei die komplette Laufbahn eines Mitarbeiters in der Institution vom Eintritt bis zum Austritt betrachten. Durch Anwendung des Need-to-Know-Prinzips und des Vier-Augen-Prinzips ist sicher zu stellen, das Berechtigungen auf den verschiedenen Ebenen (z. B. Zutritt zu Räumen, Zugang zu Informationssystemen) zielgerichtet vergeben werden und auch praktikabel sind (siehe M 2.6 *Vergabe von Zutrittsberechtigungen* und M 2.7 *Vergabe von Zugangsberechtigungen*).

Diese Berechtigungen sind zu dokumentieren und durch verschiedene Methoden zu unterstützen, wie z. B. kontrollierte und nachweisbare Ausgabe von Schlüsseln nur an Berechtigte, Authentisierung von Zugriffen, Zutrittskontrollsysteme für speziell gesicherte Bereiche und Kontrolle der Aktionen Betriebsfremder (siehe M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*). Die Zuordnung von Personen oder Personengruppen zu Rollen erleichtert die Verwaltung von Berechtigungen (siehe M 2.8 *Vergabe von Zugriffsrechten*). Werden Regelungen bewusst oder unbewusst verletzt, so müssen die hieraus ableitbaren Informations- und Eskalationsprozesse den Mitarbeitern bekannt sein, so dass eine zielgerichtete Reaktion auf die Verletzung erfolgen kann (siehe M 2.39 *Reaktion auf Verletzungen der Sicherheitsvorgaben*).

**Aussonderung**

Datenträger, Betriebs- und Sachmittel, die besonderen Schutzbedingungen unterliegen, sind so zu entsorgen, dass keine Rückschlüsse auf ihre Verwendung oder Inhalte gemacht werden können (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*). Hierzu sind entsprechende Regelungen, gegebenenfalls auch mit externen Firmen, zu treffen. Entsprechende Bestimmungen des Datenschutzes sind zu beachten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Organisation" vorgestellt:

**Planung und Konzeption**

- M 2.1 (A) *Festlegung von Verantwortlichkeiten und Regelungen*
- M 2.2 (C) *Betriebsmittelverwaltung*
- M 2.4 (B) *Regelungen für Wartungs- und Reparaturarbeiten*
- M 2.5 (A) *Aufgabenverteilung und Funktionstrennung*
- M 2.40 (A) *Rechtzeitige Beteiligung des Personal-/Betriebsrates*
- M 2.225 (B) *Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten*
- M 2.393 (A) *Regelung des Informationsaustausches*

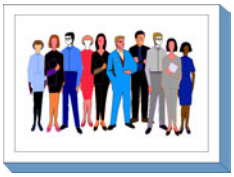
**Betrieb**

- M 2.6 (A) *Vergabe von Zutrittsberechtigungen*
- M 2.7 (A) *Vergabe von Zugangsberechtigungen*
- M 2.8 (A) *Vergabe von Zugriffsrechten*
- M 2.16 (B) *Beaufsichtigung oder Begleitung von Fremdpersonen*
- M 2.18 (Z) *Kontrollgänge*
- M 2.37 (C) *Der aufgeräumte Arbeitsplatz*
- M 2.39 (B) *Reaktion auf Verletzungen der Sicherheitsvorgaben*
- M 2.177 (Z) *Sicherheit bei Umzügen*
- M 5.33 (B) *Absicherung von Fernwartung*

**Aussonderung**

- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*

# B 1.2 Personal



## Beschreibung

In diesem Baustein werden die übergeordneten IT-Grundschutz-Maßnahmen erläutert, die im Bereich Personalwesen standardmäßig durchgeführt werden sollten. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Weggang ist eine Vielzahl von Maßnahmen erforderlich. Auch für den Umgang mit Externen, wie z. B. Besuchern oder Wartungstechnikern, müssen angemessene Sicherheitsmaßnahmen vorhanden sein. Personelle Empfehlungen, die an eine bestimmte Funktion gebunden sind, wie z. B. die Ernennung des Systemadministrators eines LAN, werden in den Bausteinen angeführt, die sich mit dem jeweiligen Themengebiet beschäftigen.

## Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.36 *Fehlinterpretation von Ereignissen*
- G 3.37 *Unproduktive Suchzeiten*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.23 *Schadprogramme*
- G 5.42 *Social Engineering*
- G 5.80 *Hoax*
- G 5.104 *Ausspähen von Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für das in einem Unternehmen oder einer Behörde tätige Personal sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer geregelten Einarbeitung neuer Mitarbeiter, über Schulungen, bis hin zu einem geregelten Ausscheiden eines Mitarbeiters. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Umsetzung**

Das Unternehmen bzw. die Behörde muss neuen Mitarbeitern bestehende Regelungen und Handlungsanweisungen bekannt machen (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*), damit diese zügig in die bestehenden Prozesse integriert werden können. Ebenso ist es unerlässlich, alle Mitarbeiter über Veränderungen dieser Regelungen und ihre spezifischen Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter zu unterrichten. Insbesondere bei sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter entsprechend zu verpflichten und die Vertrauenswürdigkeit von Mitarbeitern bestätigen zu lassen (siehe M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*). Besonderes Gewicht ist hierbei auf die Vertrauenswürdigkeit von Personen mit besonderen Funktionen und Berechtigungen zu legen (siehe M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters*).

**Betrieb**

Die Motivation aller Mitarbeiter, Informationssicherheit in den Betriebsprozessen zu akzeptieren und auch eigenverantwortlich umzusetzen, muss durch geeignete Schulungen (siehe M 3.5 *Schulung zu Sicherheitsmaßnahmen*) und durch detaillierte Kenntnisse der Anwendungen (siehe M 3.4 *Schulung vor Programmnutzung*) auf fachlicher Ebene motiviert und gefördert werden. Hierbei kommt der Ausbildung des Administrations- und Wartungspersonals (siehe M 3.11 *Schulung des Wartungs- und Administrationspersonals*) ein besonderer Stellenwert zu, da dieser Personenkreis aufgrund seiner weitgehenden Rechte im Umgang mit der IT eine hohe Verantwortung trägt.

Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, wenn dies von den Abläufen her gefordert wird (siehe M 3.3 *Vertretungsregelungen*).

Kommunikationsprobleme, persönliche Probleme, schlechtes Betriebsklima, weitreichende organisatorische Veränderungen und Ähnliches sind ebenfalls Faktoren, die zu Sicherheitsrisiken führen können. Für solche Fälle sollten Vertrauenspersonen und Anlaufstellen eingerichtet sein (siehe M 3.7 *Anlaufstelle bei persönlichen Problemen*).

**Funktionsänderungen**

Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt umgesetzt werden (siehe M 3.6 *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*). Bei kurzfristig ausscheidenden Mitarbeitern kann ein potentielles Risiko vorhanden sein, dass unberechtigterweise vertrauliche Informationen mitgenommen werden oder erst im nachhinein gezielte Manipulationen an Einrichtungen, IT-Systemen oder Daten bemerkt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Personal" vorgestellt:

**Planung und Konzeption**
- M 2.226 (A) *Regelungen für den Einsatz von Fremdpersonal*
- M 3.51 (Z) *Geeignetes Konzept für Personaleinsatz und -qualifizierung*
- M 3.83 (Z) *Analyse sicherheitsrelevanter personeller Faktoren*

**Beschaffung**
- M 3.50 (Z) *Auswahl von Personal*

**Umsetzung**
- M 3.1 (A) *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*
- M 3.10 (A) *Auswahl eines vertrauenswürdigen Administrators und Vertreters*
- M 3.33 (Z) *Sicherheitsüberprüfung von Mitarbeitern*
- M 3.55 (C) *Vertraulichkeitsvereinbarungen*

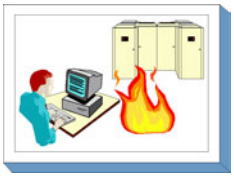
**Betrieb**
- M 3.3 (A) *Vertretungsregelungen*
- M 3.4 (A) *Schulung vor Programmnutzung*
- M 3.5 (A) *Schulung zu Sicherheitsmaßnahmen*
- M 3.7 (Z) *Anlaufstelle bei persönlichen Problemen*
- M 3.8 (Z) *Vermeidung von Störungen des Betriebsklimas*

- M 3.11 (A) *Schulung des Wartungs- und Administrationspersonals*

**Aussonderung**

- M 3.6 (A) *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*

# B 1.3 Notfallmanagement



## Beschreibung

Der Brand eines Rechenzentrums oder Bürogebäudes, erheblicher Personalausfall durch eine Pandemie, Hochwasser, flächendeckender, länger andauernder Stromausfall oder aber auch Kleinigkeiten, wie der Ausfall eines Servers, eines Outsourcing-Dienstleisters oder des Internets, können zu erheblichen Störungen oder gar Ausfällen von Geschäftsprozessen führen, welche enorme Schäden nach sich ziehen. Um Notfällen und Krisen für die Institution vorzubeugen, ist der Aufbau und Betrieb eines Notfallmanagement-Prozesses notwendig. Nur ein geplantes und organisiertes Vorgehen garantiert eine optimale Notfallvorsorge und Notfallbewältigung. Dies verringert die Wahrscheinlichkeit eines Auftretens eines Notfalls oder einer Krise sowie die Auswirkungen bei Eintreten und sichert somit das Überleben der Institution. Es sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen. Das Notfallmanagement wird auch betriebliches Kontinuitätsmanagement genannt.

Ein Notfall ist ein Schadensereignis, bei dem wesentliche Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Notfälle zeichnen sich dadurch aus, dass die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen innerhalb einer geforderten Zeit nicht wieder hergestellt werden kann und der Geschäftsbetrieb stark beeinträchtigt ist. Notfälle, welche die Kontinuität von Geschäftsprozessen beeinträchtigen, können eskalieren und sich zu einer Krise ausweiten. Unter einer Krise wird ein verschärfter Notfall verstanden, in dem die Existenz der Institution oder das Leben und die Gesundheit von Personen gefährdet sind.

Notfallmanagement umfasst die Bereiche der Notfallvorsorge mit Präventivmaßnahmen zur Vermeidung von Notfällen und Krisen sowie die Planung der Notfallbewältigung mit der Wiederherstellung von Geschäftsprozessen und Systemen (auf englisch Disaster Recovery Planning). Die Notfallbewältigung beinhaltet die Ausweichplanung (englisch Contingency Planning) und das Krisenmanagement (englisch Crisis Management) zur Bewältigung des Notfalls oder der Krise. Ziel des Notfallmanagements ist es, sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt. Eine ganzheitliche Betrachtung ist daher ausschlaggebend. Es sind alle Aspekte zu betrachten, die zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Schadensereignisses erforderlich sind, nicht nur die Ressourcen Informationen und Informationstechnik. IT-Notfallmanagement, Notfallmanagement im Rahmen und als Teilaufgabe des Sicherheitsmanagements, hat im wesentlichen zum Ziel, die Geschäftsfortführung durch Absicherung der Verfügbarkeit der IT-Services, der Anwendungen, der IT-Systeme und insbesondere der Informationen zu garantieren. IT-Notfallmanagement (englisch IT Service Continuity Management) ist Teil des ganzheitlichen Notfallmanagements und sollte auch nicht isoliert betrachtet werden.

Ein funktionierendes Notfallmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. In diesem Baustein werden daher generelle Empfehlungen für Organisationsstrukturen für das Notfallmanagement gegeben. Diese müssen an die spezifischen Gegebenheiten der jeweiligen Institution individuell angepasst werden.

Dieser Baustein soll aufzeigen, wie ein funktionierendes Notfallmanagement in einer Behörde oder einem Unternehmen eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu die wesentlichen Schritte in einem systematischen Notfallmanagement-Prozess und gibt Anleitungen zur Erstellung eines umfassenden Notfallkonzeptes. Der Baustein baut auf dem BSI-Standard 100-4 *Notfallmanagement* auf und fasst die wichtigsten Aspekte zum Notfallmanagement hieraus zusammen.

## Gefährdungslage

Die folgenden Gefährdungen werden stellvertretend für alle Gefährdungen betrachtet, durch die ein Ausfall von Geschäftsprozessen oder der Verfügbarkeit von Informationen herbeigeführt werden kann:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*
- G 1.10 *Ausfall eines Weitverkehrsnetzes*
- G 1.18 *Ausfall eines Gebäudes*
- G 1.19 *Ausfall eines Dienstleisters oder Zulieferers*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die Etablierung eines Notfallmanagement-Prozesses sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer strategischen Planung über die Analyse der relevanten Geschäftsprozesse bis hin zu konkreten Maßnahmen für die Ressourcen, die diesen Prozessen zugeordnet sind. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden müssen, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Einer der Grundpfeiler zum Erfolg des Notfallmanagements ist, dass die Leitungsebene hinter den Zielen des Notfallmanagements steht und sich ihrer Verantwortung dafür bewusst ist. Die Leitungsebene muss den Notfallmanagement-Prozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe M 6.111 *Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene*). Weiterhin muss ein kontinuierlicher Sicherheitsprozess etabliert und eine für die jeweilige Institution passende Notfallmanagementstrategie festgelegt werden (siehe M 6.110 *Festlegung des Geltungsbereichs und der Notfallmanagementstrategie*).

**Umsetzung**

Die Leitungsebene muss einen Hauptverantwortlichen für das Notfallmanagement aus der Leitungsebene benennen sowie einen Verantwortlichen für alle Belange und Fragen zum Notfallmanagement, einen Notfallbeauftragten. Letzterer ist dafür zuständig, eine geeignete Organisationsstruktur für das Notfallmanagement aufzubauen und aufrechtzuerhalten (siehe M 6.112 *Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement*).

**Betrieb**

Notfallmanagement muss in allen Bereichen der Institution gelebt werden (M 6.116 *Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse*). Dazu gehört neben der Erarbeitung eines Notfallkonzepts (siehe M 6.114 *Erstellung eines Notfallkonzepts*) auch die Integration der Mitarbeiter in den Notfallmanagement-Prozess (siehe M 6.115 *Integration der Mitarbeiter in den Notfallmanagement-Prozess*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Notfallmanagement" vorgestellt.

**Planung und Konzeption**

- M 6.110 (C) *Festlegung des Geltungsbereichs und der Notfallmanagementstrategie*
- M 6.111 (A) *Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene*

**Umsetzung**

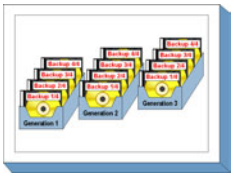
- M 6.112 (A) *Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement*
- M 6.113 (C) *Bereitstellung angemessener Ressourcen für das Notfallmanagement*
- M 6.114 (A) *Erstellung eines Notfallkonzepts*
- M 6.115 (C) *Integration der Mitarbeiter in den Notfallmanagement-Prozess*

- M 6.116 (C) *Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse*

**Betrieb**

- M 6.117 (B) *Tests und Notfallübungen*
- M 6.118 (A) *Überprüfung und Aufrechterhaltung der Notfallmaßnahmen*
- M 6.119 (C) *Dokumentation im Notfallmanagement-Prozess*
- M 6.120 (C) *Überprüfung und Steuerung des Notfallmanagement-Systems*

# B 1.4 Datensicherungskonzept



## Beschreibung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Die Konzeption einer angemessenen und funktionstüchtigen Datensicherung bedarf allerdings aufgrund der Komplexität einer geordneten Vorgehensweise. In diesem Baustein wird ein Weg beschrieben, wie für ein IT-System ein Datensicherungskonzept erstellt werden kann.

## Gefährdungslage

Für die mittels eines Datensicherungskonzepts zu schützenden Daten wird für den IT-Grundschutz folgende typische Gefährdung angenommen:

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine effektive Datensicherung einzurichten, sind eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme M 6.33 *Entwicklung eines Datensicherungskonzepts* beschrieben und werden durch die dort aufgeführten Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 6.33 begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datensicherungskonzept" vorgestellt, das vor allem für größere IT-Systeme oder IT-Systeme mit großem Datenvolumen sinnvoll ist. Die Bearbeitung der Maßnahmen sollte in der angegebenen Reihenfolge geschehen, um systematisch ein Datensicherungskonzept zu erarbeiten.

**Planung und Konzeption**

- M 6.33 (B) *Entwicklung eines Datensicherungskonzepts*
- M 6.34 (B) *Erhebung der Einflussfaktoren der Datensicherung*
- M 6.35 (B) *Festlegung der Verfahrensweise für die Datensicherung*
- M 6.36 (A) *Festlegung des Minimaldatensicherungskonzeptes*

**Beschaffung**

- M 2.137 (C) *Beschaffung eines geeigneten Datensicherungssystems*

**Umsetzung**

- M 2.41 (A) *Verpflichtung der Mitarbeiter zur Datensicherung*
- M 6.21 (C) *Sicherungskopie der eingesetzten Software*
- M 6.37 (A) *Dokumentation der Datensicherung*

**Betrieb**

- M 6.20 (A) *Geeignete Aufbewahrung der Backup-Datenträger*
- M 6.22 (A) *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*

**Notfallvorsorge**

- M 6.32 (A) *Regelmäßige Datensicherung*
- M 6.41 (A) *Übungen zur Datenrekonstruktion*

# B 1.5 Datenschutz


## Beschreibung

Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Aufgrund der engen Verflechtung von Datenschutz und Informationssicherheit werden in diesem Baustein zum Thema "Datenschutz" einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufbereitet und andererseits die Verbindung zur Informationssicherheit im IT-Grundschutz aufgezeigt.

Der IT-Grundschutz-Baustein "Datenschutz" wurde vom Bundesbeauftragten für den Datenschutz und Informationsfreiheit gemeinsam mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder sowie den Datenschutzaufsichtsbehörden der Länder erstellt. Er richtet sich an die privaten und öffentlichen Anwender für den IT-Grundschutz in Deutschland.

Da dieser Baustein auf der deutschen Gesetzgebung basiert, kann er in dieser Form außerhalb Deutschlands nur sinngemäß umgesetzt werden. Er kann nicht als Bestandteil einer formalen IT-Grundschutz-Zertifizierung angesehen werden

### Rechtliche Rahmenbedingungen bei der Verarbeitung personenbezogener Daten

Die Verfassung der Bundesrepublik Deutschland gewährleistet das Recht der Bürgerinnen und Bürger, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Aufgabe des Datenschutzes ist es nach § 1 Bundesdatenschutzgesetz (BDSG), "den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird". In den Datenschutzgesetzen der Länder finden sich ähnliche Aufgabenumschreibungen zum Schutz des "Rechts auf informationelle Selbstbestimmung". Das gesamte Datenschutzrecht bezieht sich nur auf personenbezogene Daten. Darunter sind "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" zu verstehen. Juristische Personen werden nicht erfasst.

Die folgenden Ausführungen beziehen sich ausschließlich auf deutsches Recht. Das jeweils im Einzelfall anzuwendende Recht richtet sich danach, ob die Daten verarbeitende Stelle eine öffentliche Stelle des Bundes, eines Landes oder ein privates nicht öffentliches Unternehmen ist. Für öffentliche Stellen des Bundes und für private Unternehmen gilt das Bundesdatenschutzgesetz, für öffentliche Stellen der Länder das jeweilige Landesdatenschutzgesetz. Die Struktur der Datenschutzgesetze ist weitgehend einheitlich, der Regelungsinhalt ist jedoch in einigen Bereichen unterschiedlich. Dies gilt für die Grundbegriffe der Datenverarbeitung, für die Zulässigkeit der Datenverarbeitung aufgrund einer Rechtsvorschrift oder einer Einwilligung und für die Rechte der Bürger. Darüber hinaus gibt es bereichsspezifische Spezialgesetze, die gegenüber den Regelungen der Bundes- und Landesdatenschutzgesetze vorrangig sind (z. B. Sozialgesetzbuch, Straßenverkehrsgesetz, Meldegesetze, Polizeigesetze).

Die folgenden Ausführungen beziehen sich auf die Vorschriften des BDSG und haben daher Geltung für öffentliche Stellen des Bundes und private Unternehmen. Bei öffentlichen Stellen der Länder sind die einzelnen Landesdatenschutzgesetze zu beachten.

### Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, landesspezifische Besonderheiten

Die Erhebung, Verarbeitung und Nutzung personenbezogener (bzw. - beziehbarer) Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung ist regelmäßig schriftlich zu erteilen. Zuvor ist der Betroffene auf den Zweck der Verarbeitung hinzuweisen. Bereits als Vorfrage für die Zulässigkeit der Datenverarbeitung ist von Bedeutung,

ob überhaupt personenbezogene Daten benötigt werden. Gestaltung und Auswahl von Datenverarbeitungsprogrammen haben sich nämlich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Dabei ist insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Weiterhin sind die Grundsätze der Erforderlichkeit und Zweckbindung der Datenverarbeitung zu berücksichtigen. Danach ist die Datenverarbeitung nur zulässig, wenn sie zur Aufgabenerfüllung erforderlich ist. Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden. Die Verarbeitung darf nur für vorher festgelegte Zwecke erfolgen. Eine Datenerhebung und -speicherung für noch nicht festgelegte Zwecke ist unzulässig. Zweckänderungen sind allein in den im Gesetz genannten Ausnahmefällen möglich. Generell ist darauf hinzuweisen, dass Landesdatenschutzgesetze in den jeweiligen Zusammenhängen unterschiedliche Abweichungen aufweisen, die im Einzelnen zu berücksichtigen sind.

**Datengeheimnis, Verpflichtung auf den Datenschutz, Unterrichtung**

Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Bei nicht öffentlichen Stellen sind die Beschäftigten bei Aufnahme ihrer Tätigkeit nach § 5 BDSG auf das Datengeheimnis zu verpflichten. Im öffentlichen Bereich bedarf es beim Bund und in den meisten Ländern keiner förmlichen Verpflichtung mehr. Hier greift eine entsprechende datenschutzrechtliche Unterrichtung. Auf Ausnahmen in den Landesdatenschutzgesetzen ist zu achten.

**Technische und organisatorische Maßnahmen**

Zum Schutz der personenbezogenen Daten sind von den Daten verarbeitenden Stellen die notwendigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Insbesondere sind dazu die in der Anlage zu § 9 BDSG enthaltenen "Gebote" einzuhalten, die 8 Kontrollziele (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Einhaltung der Zweckbestimmung) vorgeben. Die zu ergreifenden Maßnahmen werden im Gesetz nicht konkret beschrieben, da ihre Eignung vom jeweiligen Anwendungsfall und dem Schutzbedarf der personenbezogenen Daten abhängig ist und die technischen Maßnahmen einem permanenten Wandel unterliegen. Die in den Landesdatenschutzgesetzen enthaltenen Kontrollziele weichen von den Zielen des BDSG teilweise ab, teilweise werden abstraktere Ziele der informationstechnischen Sicherheit benannt und die konkrete Umsetzung in Sicherheitskonzepten verlangt.

**Besondere Datenarten, Vorabkontrolle, automatisierte Einzelentscheidungen oder Abrufverfahren**

Weist eine Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen auf wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG). Eine Vorabkontrolle ist nicht durchzuführen, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. In manchen Landesdatenschutzgesetzen ist eine Vorabkontrolle generell bei allen Verfahren vorgeschrieben, mit denen personenbezogene Daten durch öffentliche Stellen verarbeitet werden. Die Voraussetzungen hierfür können von den beim Bund geltenden Regelungen abweichen.

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen (§ 6a Abs. 1 BDSG).

Besonderer Schutzbedarf besteht auch bei automatisierten Abrufverfahren. Bei diesen Online-Verfahren trägt die empfangende Stelle die Verantwortung für die Zulässigkeit des Abrufs (§ 10 Abs. 4 Satz 1 BDSG). In manchen Landesdatenschutzgesetzen ist die Einrichtung von automatisierten Abrufverfahren an besondere rechtliche Voraussetzungen geknüpft.

**Rechte der Betroffenen**

Die Betroffenen haben nach dem BDSG und den landesspezifischen Datenschutzgesetzen insbesondere die folgenden Rechte:

- Recht auf Auskunft über die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und den Zweck der Speicherung.
- Recht auf Berichtigung, wenn unrichtige Daten gespeichert werden.
- Recht auf Sperrung, soweit die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.
- Recht auf Löschung, wenn die Speicherung der Daten unzulässig ist oder die Daten nicht mehr benötigt werden. An die Stelle einer Löschung tritt eine Sperrung, soweit Aufbewahrungsfristen entgegenstehen, der Grund zur Annahme besteht, dass die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigen würde oder die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohen Aufwand möglich ist.
- Recht auf Widerspruch gegen die Datenverarbeitung wegen der besonderen persönlichen Situation des Betroffenen, sofern die Datenverarbeitung nicht durch eine Rechtsvorschrift verlangt wird.
- Recht auf Schadensersatz wegen einer unzulässigen oder unrichtigen Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten.

Diese Rechte können nicht durch Verträge oder sonstige Rechtsgeschäfte ausgeschlossen oder beschränkt werden.

Darüber hinaus kann sich der Betroffene zu Fragen des Datenschutzes auch an den betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) oder die jeweils zuständige Aufsichtsbehörde wenden. Niemand darf benachteiligt oder gemaßregelt werden, weil er sich an den Datenschutzbeauftragten oder die Aufsichtsbehörde gewandt hat. Form- und Fristerfordernisse bestehen nicht.

**Ansprechpartner und Kontrollen**

Die Einhaltung der datenschutzrechtlichen Bestimmungen wird durch Datenschutz-Kontrollinstanzen überprüft:

**Die betrieblichen oder behördlichen Datenschutzbeauftragten** sind für die interne Datenschutzkontrolle zuständig. Sie sind der Unternehmens-/Behördenleitung unmittelbar zu unterstellen und bei der Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Die Beauftragten für den Datenschutz wirken auf die Einhaltung der Vorschriften über den Datenschutz hin. Ihnen ist von der verantwortlichen Stelle eine Übersicht über die automatisierten Verfahren im Betrieb/in der Behörde zur Verfügung zu stellen. Den größten Teil dieser Angaben hat der betriebliche Datenschutzbeauftragte jedermann in geeigneter Weise verfügbar zu machen. Der betriebliche/behördliche Datenschutzbeauftragte kann sich in Zweifelsfällen an die für die Datenschutzkontrolle zuständige Behörde wenden.

**Der Bundesbeauftragte für den Datenschutz** ist für die öffentlichen Stellen im Bundesbereich zuständig. Dazu gehören die Behörden der Bundesverwaltung und die sonstigen öffentlichen Stellen des Bundes, auch die bundesunmittelbaren Körperschaften. Seine Hauptaufgabe besteht darin, diese öffentlichen Stellen zu beraten und zu kontrollieren.

**Die Landesbeauftragten für den Datenschutz** sind zuständig für die Beratung und Überwachung der Behörden der Landesverwaltung und der sonstigen öffentlichen Stellen des Landes, wozu auch die Kommunalverwaltungen gehören.

**Die Datenschutzaufsichtsbehörden für die nicht öffentlichen Stellen** übernehmen im Bereich der Wirtschaft die Beratung und Überwachung. In einem Teil der Bundesländer wird diese Aufgabe durch

die Landesdatenschutzbeauftragten wahrgenommen. In den anderen Bundesländern ist die Aufgabe bei dem jeweils zuständigen Ministerium, meistens dem Innenministerium, angesiedelt.

Die Anschriften der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzaufsichtsbehörden für die nicht öffentlichen Stellen sind zu finden unter www.datenschutz.de.

**Datenschutz in den IT-Grundschutz-Katalogen**

Die in den IT-Grundschutz-Katalogen in den anderen Bausteinen enthaltenen Maßnahmen dienen der Informationssicherheit und damit auch dem Schutz von personenbezogenen Daten. Die nachfolgend dargestellten Gefährdungslagen beschränken sich auf zusätzliche Gefährdungen aus Sicht des Datenschutzes. Entsprechende Maßnahmen dazu werden anschließend empfohlen.

Wegen der oft schwierigen Rechtslage bei Datenschutzfragen in allgemeinen oder spezialrechtlichen Regelungen sollte zur Beurteilung der gesetzlichen Anforderungen und der daraus folgenden Maßnahmen für das Informationssicherheits- und Datenschutzkonzept fachkundige Unterstützung in Anspruch genommen werden.

## Gefährdungslage

Gefährdungen im Umfeld des Datenschutzes können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.162 *Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten*
- G 2.163 *Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten*
- G 2.164 *Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten*
- G 2.165 *Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten*
- G 2.166 *Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten*
- G 2.167 *Fehlende oder nicht ausreichende Vorabkontrolle*
- G 2.168 *Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten*
- G 2.169 *Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten*
- G 2.170 *Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen*
- G 2.171 *Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten*
- G 2.172 *Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland*
- G 2.173 *Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten*
- G 2.174 *Fehlende oder unzureichende Datenschutzkontrolle*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen eines Datenschutzmanagements müssen die rechtlichen Rahmenbedingungen beachtet und geeignete technische und organisatorische Maßnahmen getroffen werden, um den Datenschutz sicher zu stellen. Dazu gehören Maßnahmen in der Planungs- und Konzeptionsphase, im Zuge der Umsetzung, sowie beim Betrieb von IT-Systemen und -Verfahren.

Nachfolgend wird das ergänzende Maßnahmenbündel für den Bereich Datenschutz vorgestellt, das für alle IT-Systeme und IT-Verfahren anzuwenden ist, mit deren Hilfe personenbezogene Daten verarbeitet werden:

**Planung und Konzeption**

- M 2.501 (C) *Datenschutzmanagement*
- M 2.502 (B) *Regelung der Verantwortlichkeiten im Bereich Datenschutz*
- M 2.503 (A) *Aspekte eines Datenschutzkonzeptes*
- M 2.504 (A) *Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten*
- M 2.505 (A) *Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten*

**Umsetzung**

- M 2.506 (A) *Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten*
- M 2.507 (A) *Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten*
- M 2.508 (A) *Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten*
- M 2.509 (C) *Datenschutzrechtliche Freigabe*
- M 2.510 (A) *Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten*
- M 2.511 (A) *Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten*
- M 2.512 (A) *Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten*

**Betrieb**

- M 2.110 (A) *Datenschutzaspekte bei der Protokollierung*
- M 2.513 (Z) *Dokumentation der datenschutzrechtlichen Zulässigkeit*
- M 2.514 (A) *Aufrechterhaltung des Datenschutzes im laufenden Betrieb*
- M 2.515 (A) *Datenschutzgerechte Löschung/Vernichtung*

# B 1.6 Schutz vor Schadprogrammen

## Beschreibung

Jede Institution sollte geeignete vorbeugende Maßnahmen gegen Schadprogramme zusammenstellen sowie das Vorgehen im Fall einer Infektion mit Schadprogrammen regeln. Unter Schadprogrammen werden neben den klassischen Computer-Viren auch Trojanische Pferde, Computer-Würmer und weitere Schaden verursachende Software verstanden. Als Grundlage, um das Eindringen von Schadprogrammen in IT-Systeme zu verhindern, sollte ein Sicherheitskonzept gegen Schadprogramme entwickelt werden. Eine hundertprozentige Sicherheit ist auch beim Schutz vor Schadprogrammen nicht möglich. Im Bewusstsein des Restrisikos müssen Maßnahmen ergriffen werden, einem Eindringen von Schadprogrammen vorzubeugen. Ist eine vorbeugende Abwehr nicht gelungen, soll das Eindringen von Schadprogrammen zumindest aber so früh wie möglich entdeckt werden. Darüber hinaus werden in diesem Baustein Maßnahmen benannt, die der Schadensminderung dienen, wenn ein Schadprogramm nicht rechtzeitig entdeckt werden konnte. Wesentlich ist die konsequente Anwendung der Maßnahmen und die ständige Aktualisierung der eingesetzten technischen Methoden. Diese Forderung begründet sich durch die täglich neu auftretenden Schadprogramme bzw. durch ständig neue Variationen schon bekannter Schadprogramme. Durch die Weiterentwicklung von Betriebssystemen, Programmiersprachen und Anwendungsprogrammen entstehen regelmäßig neue Angriffspotentiale für Schadprogramme, so dass rechtzeitig geeignete Gegenmaßnahmen eingeleitet werden müssen.

Um für eine Gesamtorganisation einen effektiven Schutz gegen Schadprogramme zu erreichen, wird in diesem Baustein die Vorgehensweise zur Erstellung und Realisierung eines entsprechenden Sicherheitskonzeptes erläutert. Konkrete Maßnahmenempfehlungen zum Schutz vor Schadprogrammen für einzelne IT-Systeme finden sich in den systemspezifischen Bausteinen.

## Gefährdungslage

Für den IT-Grundschutz werden bezüglich Schadprogramme die folgenden typischen Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.8 *Unkontrollierter Einsatz von Betriebsmitteln*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.136 *Fehlende Übersicht über den Informationsverbund*

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.23 *Schadprogramme*
- G 5.28 *Verhinderung von Diensten*
- G 5.42 *Social Engineering*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.142 *Verbreitung von Schadprogrammen über mobile Datenträger*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Erstellung eines Sicherheitskonzeptes gegen Schadprogramme (siehe M 2.154 *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme*) muss zunächst ermittelt werden, welche der vorhandenen oder geplanten IT-Systeme in das Sicherheitskonzept einzubeziehen sind. Für diese IT-Systeme müssen die für die Umsetzung von Sicherheitsmaßnahmen relevanten Einflussfaktoren betrachtet werden. Darauf aufbauend können dann die technischen und organisatorischen Maßnahmen ausgewählt werden. Hierzu ist insbesondere die Auswahl geeigneter technischer Gegenmaßnahmen wie der Einsatz von Viren-Schutzprogrammen zu beachten (siehe M 2.157 *Auswahl eines geeigneten Viren-Schutzprogramms*). Neben der Einrichtung eines Meldewesens (siehe M 2.158 *Meldung von Schadprogramm-Infektionen*) und einer Koordinierung der Aktualisierung eingesetzter Schutzprodukte (siehe M 2.159 *Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen*) sind für die Umsetzung des Konzeptes eine Reihe von Regelungen zu vereinbaren.

Die wichtigsten vorbeugenden Maßnahmen gegen Schäden durch Schadsoftware sind der Einsatz von Viren-Schutzprogrammen sowie regelmäßige Datensicherungen (siehe M 6.32 *Regelmäßige Datensicherung*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Schutz vor Schadprogrammen" vorgestellt:

**Planung und Konzeption**
- M 2.154 (A) *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme*
- M 2.160 (A) *Regelungen zum Schutz vor Schadprogrammen*
- M 3.69 (W) *Einführung in die Bedrohung durch Schadprogramme*

**Beschaffung**
- M 2.157 (A) *Auswahl eines geeigneten Viren-Schutzprogramms*

**Umsetzung**
- M 4.84 (A) *Nutzung der BIOS-Sicherheitsmechanismen*

**Betrieb**
- M 2.34 (A) *Dokumentation der Veränderungen an einem bestehenden System*
- M 2.158 (A) *Meldung von Schadprogramm-Infektionen*
- M 2.159 (A) *Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen*
- M 2.224 (A) *Vorbeugung gegen Schadprogramme*
- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*

**Notfallvorsorge**
- M 6.23 (A) *Verhaltensregeln bei Auftreten von Schadprogrammen*
- M 6.24 (A) *Erstellen eines Notfall-Bootmediums*
- M 6.32 (A) *Regelmäßige Datensicherung*

# B 1.7 Kryptokonzept

## Beschreibung

Dieser Baustein beschreibt eine Vorgehensweise, wie in einer heterogenen Umgebung sowohl die lokal gespeicherten Daten als auch die zu übertragenen Daten wirkungsvoll durch kryptographische Verfahren und Techniken geschützt werden können. Dazu wird beschrieben, wie und wo in einer heterogenen Umgebung kryptographische Verfahren und die entsprechenden Komponenten eingesetzt werden können. Da beim Einsatz kryptographischer Verfahren sehr viele komplexe Einflussfaktoren zu betrachten sind, sollte hierfür ein Kryptokonzept erstellt werden.

In diesem Baustein wird daher beschrieben, wie ein Kryptokonzept erstellt werden kann. Beginnend mit der Bedarfsermittlung und der Erhebung der Einflussfaktoren geht es über die Auswahl geeigneter kryptographischer Lösungen und Produkte bis hin zur Sensibilisierung und Schulung der Anwender und zur Krypto-Notfallvorsorge.

Dieser Baustein kann auch herangezogen werden, wenn nur ein kryptographisches Produkt für eines der möglichen Einsatzfelder ausgewählt werden soll. Dann können einige der im folgenden beschriebenen Schritte ausgelassen werden und nur die für das jeweilige Einsatzfeld relevanten Teile bearbeitet werden.

Für die Umsetzung dieses Bausteins sollte ein elementares Verständnis der grundlegenden kryptographischen Mechanismen vorhanden sein. Ein Überblick über kryptographische Grundbegriffe findet sich in M 3.23 *Einführung in kryptographische Grundbegriffe*.

## Gefährdungslage

Kryptographische Verfahren werden eingesetzt zur Gewährleistung von

- Vertraulichkeit,
- Integrität,
- Authentizität und
- Nichtabstreitbarkeit.

Daher werden für den IT-Grundschutz primär die folgenden Gefährdungen für kryptographische Verfahren betrachtet:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.32 *Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren*
- G 3.33 *Fehlbedienung von Kryptomodulen*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.34 *Ausfall eines Kryptomoduls*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.36 *Fehler in verschlüsselten Daten*

**Vorsätzliche Handlungen**

- G 5.27 *Nichtanerkennung einer Nachricht*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.81 *Unautorisierte Benutzung eines Kryptomoduls*
- G 5.82 *Manipulation eines Kryptomoduls*

- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.84 *Gefälschte Zertifikate*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Darüber hinaus sind im Bereich kryptographische Verfahren im wesentlichen die folgenden Schritte durchzuführen:

Entwicklung eines Kryptokonzepts

Der Einsatz kryptographischer Verfahren wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, das angestrebte Sicherheitsniveau und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Daher sollte zunächst ein Konzept entwickelt werden, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines konkreten kryptographischen Verfahrens und der entsprechenden Produkte berücksichtigt werden und das gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist (siehe M 2.161 *Entwicklung eines Kryptokonzepts*).

Ermittlung der Anforderungen an die kryptographischen Verfahren

Es muss ein Anforderungskatalog erstellt werden, in dem die Einflussgrößen und die Entscheidungskriterien beschrieben werden, die einem Einsatz von kryptographischen Verfahren zugrunde liegen (siehe M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte* und M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*). Kryptographische Verfahren können auf den verschiedenen Schichten des ISO/OSI-Schichtenmodells eingesetzt werden. Je nach den festgestellten Anforderungen oder Gefährdungen ist der Einsatz auf bestimmten Schichten zu empfehlen (siehe auch M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*.

Auswahl eines geeigneten kryptographischen Produktes

Nachdem alle Rahmenbedingungen bestimmt worden sind, muss ein Produkt ausgewählt werden, das die im Kryptokonzept dargelegte Sicherheitsfunktionalität bietet (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*). Ein solches Produkt, im folgenden kurz Kryptomodul genannt, kann dabei aus Hardware, Software, Firmware oder aus einer diesbezüglichen Kombination sowie der zur Durchführung der Kryptoprozesse notwendigen Bauteilen wie Speicher, Prozessoren, Busse, Stromversorgung etc. bestehen. Ein Kryptomodul kann zum Schutz von sensiblen Daten bzw. Informationen in unterschiedlichsten Rechner- oder Telekommunikationssystemen Verwendung finden.

Geeigneter Einsatz der Kryptomodule

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an ein Kryptomodul gestellt werden. Neben der Sicherheit der durch das Kryptomodul zu schützenden Daten geht es schwerpunktmäßig auch darum, das Kryptomodul selbst gegen unmittelbare Angriffe und Fremdeinwirkung zu schützen (siehe M 2.166 *Regelung des Einsatzes von Kryptomodulen*).

Die sicherheitstechnischen Anforderungen an die IT-Systeme, auf denen die kryptographischen Verfahren eingesetzt werden, sind den jeweiligen systemspezifischen Bausteinen zu entnehmen. Bei Auswahl und Einsatz von Kryptomodulen sollte auch der Baustein B 3.407 *Eingebettetes System* beachtet werden.

Notfallvorsorge

Zur Notfallvorsorge gehören:

- die Datensicherung bei Einsatz kryptographischer Verfahren (siehe M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*), also die Sicherung der Schlüssel, der Konfigurationsdaten der eingesetzten Produkte, der verschlüsselten Daten,

- die Informationsbeschaffung über sowie die Reaktion auf Sicherheitslücken.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Kryptokonzept" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier verzichtet.

**Planung und Konzeption**

- M 2.161 (A) *Entwicklung eines Kryptokonzepts*
- M 2.162 (A) *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*
- M 2.163 (A) *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*
- M 2.164 (A) *Auswahl eines geeigneten kryptographischen Verfahrens*
- M 2.166 (A) *Regelung des Einsatzes von Kryptomodulen*
- M 3.23 (W) *Einführung in kryptographische Grundbegriffe*
- M 4.90 (W) *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*
- M 4.433 (Z) *Einsatz von Datenträgerverschlüsselung*
- M 4.435 (Z) *Selbstverschlüsselnde Festplatten*
- M 5.63 (Z) *Einsatz von GnuPG oder PGP*
- M 5.67 (Z) *Verwendung eines Zeitstempel-Dienstes*
- M 5.110 (Z) *Absicherung von E-Mail mit SPHINX (S/MIME)*

**Beschaffung**

- M 2.165 (A) *Auswahl eines geeigneten kryptographischen Produktes*
- M 4.85 (Z) *Geeignetes Schnittstellendesign bei Kryptomodulen*
- M 4.88 (A) *Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen*

**Umsetzung**

- M 2.46 (A) *Geeignetes Schlüsselmanagement*
- M 4.86 (A) *Sichere Rollenteilung und Konfiguration der Kryptomodule*
- M 4.87 (Z) *Physikalische Sicherheit von Kryptomodulen*
- M 4.89 (Z) *Abstrahlsicherheit*

**Notfallvorsorge**

- M 6.56 (A) *Datensicherung bei Einsatz kryptographischer Verfahren*
- M 6.162 (Z) *Reaktion bei praktischer Schwächung eines Kryptoverfahrens*

# B 1.8 Behandlung von Sicherheitsvorfällen


## Beschreibung

Um die Informationssicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen (Security Incident Handling oder auch Security Incident Response) im Vorfeld zu konzipieren und einzuüben. Als Sicherheitsvorfall wird dabei ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können die Ausspähung, Manipulation oder Zerstörung von Daten sein. Um Schäden zu vermeiden bzw. zu begrenzen, müssen Sicherheitsvorfälle schnell und effizient bearbeitet werden. Wenn hierbei auf ein vorgegebenes und erprobtes Verfahren aufgesetzt werden kann, können Reaktionszeiten minimiert werden.

Der Fokus dieses Bausteins liegt auf der Behandlung von Sicherheitsvorfällen aus Sicht der Informationstechnik. Trotz dieser klaren Trennung von anderen Sicherheitsvorfällen gibt es bei der Behandlung von Sicherheitsvorfällen auch Schnittstellen zu Vorfällen in anderen Bereichen zu beachten.

Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist dabei das Notfallmanagement (siehe Baustein B 1.3 *Notfallmanagement*). Im Rahmen des Notfallmanagements werden unter anderem konkret für geschäftsrelevante Prozesse, Bereiche und IT-Systeme der Ausfall kritischer Komponenten vorab analysiert, risikominimierende Maßnahmen geplant und eine Vorgehensweise zur Aufrechterhaltung oder Wiederherstellung der Verfügbarkeit festgelegt.

Typische Sicherheitsvorfälle sind beispielsweise

- Fehlkonfigurationen, die zur Offenlegung vertraulicher Daten, zu Verlust der Integrität schutzbedürftiger Daten oder zu Datenverlusten führen,
- Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten durch inhärente Fehler,
- Auftreten von Schadsoftware oder
- kriminelle Handlungen (etwa Hacking von Internet-Servern, Einbruch in IT-Systeme, Diebstahl von Daten, Sabotage oder Erpressung mit IT-Bezug).

Solche Sicherheitsvorfälle können zum Beispiel ausgelöst werden durch

- das Fehlverhalten von Benutzern, Administratoren oder externen Dienstleistern, das zu sicherheitskritischen Änderungen von Systemparametern führt und gegen interne Richtlinien oder Anweisungen verstößt,
- Verletzung von Zugriffsrechten,
- durchgeführte Änderungen an Software, Hardware oder Infrastruktur oder
- unzureichende Absicherung schutzbedürftiger Räume und Gebäude.

Alle Arten von Sicherheitsvorfällen müssen angemessen behandelt werden. Dies gilt sowohl für solche Sicherheitsvorfälle, gegen die die Institution sich konkret rüsten kann, wie z. B. Computer-Viren, als auch solche, die die Institution unerwartet treffen, wie beispielsweise ein Wasserrohrbruch.

In diesem Baustein wird ein systematischer Weg aufgezeigt, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt und dessen Umsetzung und Einbettung innerhalb eines Unternehmens bzw. einer Behörde sichergestellt werden kann. Der Aufwand zur Erstellung und Umsetzung eines solchen Konzepts ist nicht gering.

## Gefährdungslage

Sicherheitsvorfälle können durch eine Vielzahl von Gefährdungen ausgelöst werden. Eine große Sammlung von Gefährdungen, die kleinere oder größere Sicherheitsvorfälle verursachen können, findet sich in den Gefährdungskatalogen. In diesem Baustein werden daher stellvertretend für alle Gefährdungen, die sich im Umfeld von Sicherheitsvorfällen ereignen können, folgende Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.62 *Ungeeigneter Umgang mit Sicherheitsvorfällen*
- G 2.141 *Nicht erkannte Sicherheitsvorfälle*
- G 2.142 *Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um ein effektives System zur Behandlung von Sicherheitsvorfällen einzurichten, sind eine Reihe von Schritten zu durchlaufen und Maßnahmen umzusetzen.

**Planung und Konzeption**

Zunächst muss eine Vorgehensweise sowie Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen aufgebaut werden (siehe M 6.58 *Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen*). Es ist zu regeln, wer welche Verantwortung beim Auftreten von Sicherheitsvorfällen hat (siehe M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*).

Neben der Festlegung der Rollen, Verantwortlichkeiten und Verhaltensregeln müssen für die effektive Behandlung von Sicherheitsvorfällen die Betroffenen richtig mit deren Auswirkungen umgehen und Vorfälle unverzüglich melden (siehe M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

Es ist eine Eskalationsstrategie zu erarbeiten, wer in welchen Fällen hinzuzuziehen ist (siehe M 6.61 *Eskalationsstrategie für Sicherheitsvorfälle*). Außerdem muss festgelegt werden, in welcher Reihenfolge die aus einem Sicherheitsvorfall resultierenden Schäden bearbeitet werden sollen (siehe M 6.62 *Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen*).

**Umsetzung**

Neben der Prävention kommt auch der Detektion von Sicherheitsvorfällen sowie der Beweissicherung große Bedeutung zu (siehe M 6.67 *Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle* und M 6.127 *Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen*).

Zur kompetenten Behandlung von Sicherheitsvorfällen sollte frühzeitig ein Team mit erfahrenen und vertrauenswürdigen Spezialisten zusammengestellt werden (siehe M 6.123 *Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen*).

**Betrieb**

Sicherheitsvorfälle müssen zunächst als solche erkannt und erfasst werden (siehe M 6.130 *Erkennen und Erfassen von Sicherheitsvorfällen*), dann müssen sie analysiert und eine angemessene Lösung vorgeschlagen werden (siehe M 6.131 *Qualifizieren und Bewerten von Sicherheitsvorfällen* und M M 6.64 *Behebung von Sicherheitsvorfällen*). Die Maßnahmen zu Behebung von Sicherheitsvorfällen müssen geeignet überwacht und gesteuert werden (siehe M 6.133 *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen* und M 6.66 *Nachbereitung von Sicherheitsvorfällen*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Behandlung von Sicherheitsvorfällen" vorgestellt.

**Planung und Konzeption**

- M 6.58 (A) *Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen*
- M 6.59 (A) *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*
- M 6.60 (A) *Festlegung von Meldewegen für Sicherheitsvorfälle*
- M 6.61 (C) *Eskalationsstrategie für Sicherheitsvorfälle*
- M 6.62 (Z) *Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen*
- M 6.121 (A) *Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen*
- M 6.122 (C) *Definition eines Sicherheitsvorfalls*

**Umsetzung**

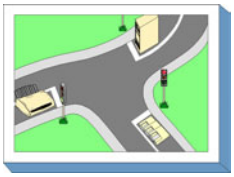
- M 6.67 (Z) *Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle*

- M 6.123 (Z) *Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen*
- M 6.124 (C) *Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung*
- M 6.125 (A) *Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen*
- M 6.126 (Z) *Einführung in die Computer-Forensik*
- M 6.127 (Z) *Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen*
- M 6.128 (Z) *Schulung an Beweismittelsicherungswerkzeugen*
- M 6.129 (C) *Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen*

**Betrieb**

- M 6.64 (A) *Behebung von Sicherheitsvorfällen*
- M 6.65 (A) *Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen*
- M 6.66 (B) *Nachbereitung von Sicherheitsvorfällen*
- M 6.68 (C) *Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen*
- M 6.130 (A) *Erkennen und Erfassen von Sicherheitsvorfällen*
- M 6.131 (A) *Qualifizieren und Bewerten von Sicherheitsvorfällen*
- M 6.132 (A) *Eindämmen der Auswirkung von Sicherheitsvorfällen*
- M 6.133 (A) *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen*
- M 6.134 (B) *Dokumentation von Sicherheitsvorfällen*

# B 1.9 Hard- und Software-Management



## Beschreibung

Um den notwendigen und erwünschten Sicherheitsgrad für die gesamte IT-Organisation zu erreichen, genügt es nicht, nur die einzelnen IT-Komponenten zu sichern. Es ist vielmehr erforderlich, auch alle Abläufe und Vorgänge, die diese IT-Systeme berühren, so zu gestalten, dass das angestrebte Niveau der Informationssicherheit erreicht und beibehalten wird. Es sind daher für alle diese Vorgänge Regelungen einzuführen und zu pflegen, die die Wirksamkeit der Sicherheitsmaßnahmen gewährleisten.

Den Schwerpunkt dieses Bausteins bilden dabei Regelungen, die sich spezifisch auf informationstechnische Hardware- oder Software-Komponenten beziehen, mit dem Ziel, einen ordnungsgemäßen IT-Betrieb in Bezug auf Management bzw. Organisation sicherzustellen. Sicherheit sollte integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

## Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.8 *Staub, Verschmutzung*
- G 1.19 *Ausfall eines Dienstleisters oder Zulieferers*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.10 *Nicht fristgerecht verfügbare Datenträger*
- G 2.15 *Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System*
- G 2.21 *Mangelhafte Organisation des Wechsels zwischen den Benutzern*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.24 *Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.11 *Fehlerhafte Konfiguration von sendmail*
- G 3.17 *Kein ordnungsgemäßer PC-Benutzerwechsel*
- G 3.35 *Server im laufenden Betrieb ausschalten*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*

- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.31 *Ausfall oder Störung von Netzkomponenten*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.38 *Ausfall von Komponenten eines Netz- und Systemmanagementsystems*
- G 4.39 *Software-Konzeptionsfehler*
- G 4.43 *Undokumentierte Funktionen*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.26 *Analyse des Nachrichtenflusses*
- G 5.68 *Unberechtigter Zugang zu den aktiven Netzkomponenten*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.82 *Manipulation eines Kryptomoduls*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.84 *Gefälschte Zertifikate*
- G 5.87 *Web-Spoofing*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Informationsverbund besteht aus einer Vielzahl von IT-Komponenten, die zunächst als Einzelkomponenten gemäß der Maßnahmenvorschläge aus den entsprechenden Bausteinen abgesichert werden sollten. Damit für alle eingesetzten IT-Komponenten das gleiche Sicherheitsniveau erreicht wird, sollten durch das Hard- und Software-Management einheitliche Regelungen vorgegeben werden.

Im Rahmen des Hard- und Software-Managements sind unabhängig von der Art der eingesetzten IT-Komponenten eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Aspekte der Informationssicherheit müssen frühzeitig in die strategische Ausrichtung und die Beschaffung von IT-Systemen mit einfließen, da sie ganz konkrete Auswirkungen auf die Aufgabendurchführung und den Ablauf von Geschäftsprozessen haben. Hierbei müssen die definierten Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die Anforderungen aus den geplanten Einsatzszenarien konsolidiert werden (siehe M 2.214 *Konzeption des IT-Betriebs*).

Die Beschaffung und der Einsatz von Hardware und Software erfordern spezifische Regelungen für die verschiedenen Benutzer.

Hierbei müssen die für einen sicheren Geschäftsablauf erforderlichen Sicherheitsparameter der IT-Systeme den Benutzern transparent gemacht werden (siehe M 2.223 *Sicherheitsvorgaben für die Nutzung von Standardsoftware*). Trotz intensiver Schulung müssen die Benutzer im laufenden Betrieb hinsichtlich Funktionalität der Programme und Sicherheit sowie bei auftretenden Problemen zielgerichtet und zügig unterstützt werden (siehe M 2.12 *Betreuung und Beratung von IT-Benutzern*). Hierzu sind Benutzerbetreuer und Help-Desks einzurichten.

Die für den sicheren Betrieb aller IT-Komponenten notwendigen Maßnahmen müssen in einer Sicherheitsrichtlinie festgelegt werden. Die Einhaltung des darin spezifizierten Sicherheitsniveaus erfordert neben den technischen Maßnahmen auch ein umfangreiches Regelwerk für den Benutzer, das diesem Hilfestellung und eine verbindliche und präzise Anleitung gibt. Potentielle Risikofaktoren und Schwach-

stellen wie Passwörter, Fremdpersonal, nicht freigegebene IT-Komponenten, Zugang zu den IT-Systemen müssen durch organisatorische Regelungen oder durch eine Kombination von organisatorischen und technischen Maßnahmen (siehe M 2.11 *Regelung des Passwortgebrauchs*) minimiert werden. Die Benutzer müssen regelmäßig für den sorgfältigen Umgang mit sicherheitskritischen Informationen und IT-Komponenten sensibilisiert werden.

Der effiziente und sichere Betrieb heterogener Netze erfordert strikte Richtlinien hinsichtlich Test, Installation und Dokumentation neuer Hardware und Software (siehe M 2.216 *Genehmigungsverfahren für IT-Komponenten*) sowie eine effiziente Benutzerverwaltung (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*). Der physikalische Zugang zu IT-Systemen sowie eine Authentisierung der Benutzer gegenüber den Anwendungen und Systemen (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*) sollte grundsätzlich unter Beachtung des Need-to-Know-Prinzips erfolgen.

Der Einsatz von externen Datenträgern kann ein hohes Sicherheitsrisiko darstellen, da vermeintliche Sicherheitsbarrieren häufig einfach ausgehebelt werden können. Regelungen der Verwendung, Kennzeichnung und Prüfungen z. B. auf Schadsoftware für CD-ROMs, Memory-Sticks und andere über USB anschließbare Geräte für den Datenaustausch, dienen ebenfalls zur Aufrechterhaltung eines sicheren IT-Betriebs (siehe M 2.3 *Datenträgerverwaltung*).

Aufgabe des Änderungsmanagements ist es, Änderungen an den aktuellen Konfigurationen einem formalen Dokumentations- und Freigabeprozess zu unterziehen (siehe M 2.221 *Änderungsmanagement*). Sicherheitskritische Aspekte müssen hierbei ebenso bewertet werden wie die Durchführung nach dem Vier-Augen-Prinzip und die aktuelle Dokumentation der Änderungen. Hierzu gehört auch, dass nur zugelassene Komponenten eingesetzt werden dürfen, da sonst ein kontrollierbarer Betrieb nicht möglich ist (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

**Beschaffung**

Für die Beschaffung von IT-Systemen müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden. Der formalen Freigabe eines neuen Produktes (siehe M 2.62 *Software-Abnahme- und Freigabe-Verfahren*) sollte eine funktionale Prüfung und eine Konsistenzprüfung hinsichtlich der geforderten Sicherheitseigenschaften vorausgehen (siehe M 4.65 *Test neuer Hard- und Software*).

**Umsetzung**

Die Umsetzung der Sicherheitsrichtlinie für den Betrieb erfordert Festlegungen für Sicherheitsmaßnahmen im Rahmen der Installation und ersten Konfiguration (siehe M 4.135 *Restriktive Vergabe von Zugriffsrechten auf Systemdateien*) sowie für den laufenden Betrieb der IT-Systeme.

Die strukturierte Datenhaltung mit konsequenter Trennung von Programm- und Arbeitsdateien (siehe M 2.138 *Strukturierte Datenhaltung*) sollte auf einer weitgehend einheitlichen Konfiguration der Systeme aufsetzen. Diese wiederum unterstützt eine zentral durchführbare Systemverwaltung (siehe M 2.69 *Einrichtung von Standardarbeitsplätzen*).

Die Sicherstellung einer durchgängigen Systemadministration - auch in Ausfallzeiten wie bei Krankheit oder Urlaub - lässt sich durch entsprechende Vertretungsregelungen erreichen (siehe M 2.26 *Ernennung eines Administrators und eines Vertreters*). Die Kompetenzen des Vertreters müssen transparent gemacht werden.

Die Dokumentation der Systemkonfiguration muss aktuell und verständlich sein und sollte werkzeugunterstützt erfolgen (siehe M 2.25 *Dokumentation der Systemkonfiguration*). Neben den physikalischen IT-Komponenten sind auch die logischen Netzstrukturen sowie die Rollen und Zugriffsrechte zu dokumentieren.

**Betrieb**

Durch die Systemadministration ist der laufende Betrieb mit unterschiedlichen Schwerpunkten aufrecht zu erhalten. Die durch Migration, Ausfall und Neuanschaffung erforderlichen Änderungen des IT-Bestandes (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*) müssen nach erfolg-

ter Freigabe im IT-Bestandsverzeichnis zeitnah nachgeführt werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System* und M 2.219 *Kontinuierliche Dokumentation der Informationsverarbeitung*).

Die laufende Beobachtung und Auswertung des Betriebes (siehe M 2.10 *Überprüfung des Hard- und Software-Bestandes* und M 2.64 *Kontrolle der Protokolldateien*) hinsichtlich Konformität und eventuellen Sicherheitsverletzungen sowie die Durchführung der entsprechenden Sicherheitsmaßnahmen (siehe M 2.215 *Fehlerbehandlung*) erfordern eine permanente Informationsbeschaffung über entsprechende Updates der unterschiedlichen Hersteller (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Durch Einspielen der erforderlichen Sicherheitspatches sollte die geforderte Sicherheit auch schon präventiv erreicht werden (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

**Aussonderung**

Bei der Außerbetriebnahme von IT-Systemen ist dafür zu sorgen, dass wichtige Daten nicht verloren gehen, sondern vor der Abgabe bzw. Verschrottung der IT-Systeme gesichert werden (siehe M 4.234 *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*). Fast noch wichtiger ist es jedoch, die Datenträger dieser Systeme anschließend so gründlich zu löschen (siehe B 1.15 *Löschen und Vernichten von Daten*), dass nicht im Nachhinein Unbefugte auf sensible Daten Zugriff erhalten, da in der Regel nach der Aussonderung keine Kontrolle darüber besteht, was mit den IT-Systemen weiter geschieht.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Hard- und Software-Management" vorgestellt:

**Planung und Konzeption**
- M 2.3 (B) *Datenträgerverwaltung*
- M 2.9 (A) *Nutzungsverbot nicht freigegebener Hard- und Software*
- M 2.12 (C) *Betreuung und Beratung von IT-Benutzern*
- M 2.24 (Z) *Einführung eines IT-Passes*
- M 2.30 (A) *Regelung für die Einrichtung von Benutzern / Benutzergruppen*
- M 2.214 (A) *Konzeption des IT-Betriebs*
- M 2.216 (C) *Genehmigungsverfahren für IT-Komponenten*
- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.221 (A) *Änderungsmanagement*
- M 2.223 (B) *Sicherheitsvorgaben für die Nutzung von Standardsoftware*
- M 4.134 (Z) *Wahl geeigneter Datenformate*
- M 4.434 (C) *Sicherer Einsatz von Appliances*
- M 5.68 (Z) *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*
- M 5.77 (Z) *Bildung von Teilnetzen*

**Beschaffung**
- M 2.62 (B) *Software-Abnahme- und Freigabe-Verfahren*

**Umsetzung**
- M 1.29 (Z) *Geeignete Aufstellung eines IT-Systems*
- M 1.32 (B) *Geeignete Aufstellung von Druckern und Kopierern*
- M 2.25 (A) *Dokumentation der Systemkonfiguration*
- M 2.26 (A) *Ernennung eines Administrators und eines Vertreters*
- M 2.38 (B) *Aufteilung der Administrationstätigkeiten*
- M 2.69 (B) *Einrichtung von Standardarbeitsplätzen*
- M 2.111 (A) *Bereithalten von Handbüchern*
- M 2.138 (B) *Strukturierte Datenhaltung*
- M 2.204 (A) *Verhinderung ungesicherter Netzzugänge*
- M 4.1 (A) *Passwortschutz für IT-Systeme*
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.65 (C) *Test neuer Hard- und Software*
- M 4.84 (A) *Nutzung der BIOS-Sicherheitsmechanismen*
- M 4.135 (A) *Restriktive Vergabe von Zugriffsrechten auf Systemdateien*
- M 5.87 (C) *Vereinbarung über die Anbindung an Netze Dritter*

- M 5.88 (C) *Vereinbarung über Datenaustausch mit Dritten*

**Betrieb**

- M 1.46 (Z) *Einsatz von Diebstahl-Sicherungen*
- M 2.10 (C) *Überprüfung des Hard- und Software-Bestandes*
- M 2.34 (A) *Dokumentation der Veränderungen an einem bestehenden System*
- M 2.35 (B) *Informationsbeschaffung über Sicherheitslücken des Systems*
- M 2.64 (A) *Kontrolle der Protokolldateien*
- M 2.110 (A) *Datenschutzaspekte bei der Protokollierung*
- M 2.215 (B) *Fehlerbehandlung*
- M 2.219 (A) *Kontinuierliche Dokumentation der Informationsverarbeitung*
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.107 (B) *Nutzung von Hersteller- und Entwickler-Ressourcen*
- M 4.109 (Z) *Software-Reinstallation bei Arbeitsplatzrechnern*
- M 4.254 (Z) *Sicherer Einsatz von drahtlosen Tastaturen und Mäusen*
- M 4.306 (Z) *Umgang mit Passwort-Speicher-Tools*
- M 4.345 (Z) *Schutz vor unerwünschten Informationsabflüssen*
- M 5.150 (Z) *Durchführung von Penetrationstests*

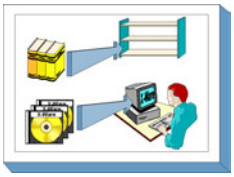
**Aussonderung**

- M 2.167 (B) *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*
- M 4.234 (B) *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*

**Notfallvorsorge**

- M 6.27 (C) *Sicheres Update des BIOS*
- M 6.137 (Z) *Treuhänderische Hinterlegung (Escrow)*

# B 1.10 Standardsoftware



## Beschreibung

Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten wird und im Allgemeinen über den Fachhandel, z. B. über Kataloge, erworben werden kann. Sie zeichnet sich dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

In diesem Baustein wird eine Vorgehensweise für den Umgang mit Standardsoftware unter Sicherheitsgesichtspunkten dargestellt. Dabei wird der gesamte Lebenszyklus von Standardsoftware betrachtet: Erstellung eines Anforderungskataloges, Vorauswahl eines geeigneten Produktes, Test, Freigabe, Installation, Lizenzverwaltung und Deinstallation.

Das Qualitätsmanagementsystem des Entwicklers der Standardsoftware fällt nicht in den Anwendungsbereich dieses Bausteins. Es wird vorausgesetzt, dass die Entwicklung der Software unter Beachtung gängiger Qualitätsstandards erfolgte.

Die beschriebene Vorgehensweise dient der Orientierung, um einen Sicherheitsprozess bezüglich Standardsoftware zu etablieren. Gegebenenfalls kann die hier aufgezeigte Vorgehensweise auch zum Vergleich mit einem bereits eingeführten Verfahren herangezogen werden.

## Gefährdungslage

Für den IT-Grundschutz von "Standardsoftware" werden die folgenden typischen Gefährdungen betrachtet:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.28 *Verstöße gegen das Urheberrecht*
- G 2.29 *Softwaretest mit Produktionsdaten*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.17 *Kein ordnungsgemäßer PC-Benutzerwechsel*

**Technisches Versagen**

- G 4.7 *Defekte Datenträger*
- G 4.22 *Software-Schwachstellen oder -Fehler*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*

- G 5.43 *Makro-Viren*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Standardsoftware sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über die Beschaffung bis zu ihrer Außerbetriebnahme. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Vor der Auswahl einer bestimmten Standardsoftware sollte ein Anforderungskatalog erstellt werden, anhand dessen ein Produkt nach objektiven und nachvollziehbaren Kriterien ausgewählt werden kann, so dass man ein gewisses Vertrauen haben kann, dass ein einigermaßen optimales Produkt zum Einsatz kommt. In dieser Phase sollten bei komplexeren Produkten auch die Verantwortlichen für deren Beschaffung und Einsatz festgelegt werden.

**Beschaffung**

Für die Beschaffung kann anhand der konkreten Vorgaben des Anforderungskatalogs geprüft werden, welches der am Markt vorhandenen Produkte die am besten geeignete Funktionalität aufweist.

**Umsetzung**

Durch Tests in angemessener Tiefe ist sicherzustellen, dass das ausgewählte Produkt über die in der Dokumentation angegebene Funktionalität auch tatsächlich verfügt. Sofern das Produkt auf breiter Basis einzusetzen ist, muss es in die vorhandenen Installationsverfahren eingebunden werden, und die Installation selbst ist zu dokumentieren. Eine Nutzung in der Fläche darf erst erfolgen, wenn das Produkt nach erfolgreichem Durchlaufen der Tests und nach Abschluss der Vorbereitungsarbeiten dafür freigegeben wurde.

**Betrieb**

Die Kontrolle der installierten Versionen und die Nachverfolgung der verfügbaren Lizenzen und deren Abgleich mit der installierten Anzahl der Produkte ist eine permanente Aufgabe während der Nutzung der Standardsoftware.

**Aussonderung**

Eine saubere Deinstallation von Standardsoftware erfordert häufig umfangreiche und komplexe Arbeiten, in einzelnen Fällen bis hin zur Neuinstallation von Rechnern.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Standardsoftware" vorgestellt. Je nach Art und Umfang der jeweiligen Standardsoftware muss erwogen werden, ob einzelne Maßnahmen nur reduziert umgesetzt werden. Die Maßnahmen M 2.79 bis M 2.89 stellen in der angegebenen Reihenfolge eine umfassende Beschreibung dar, wie der Lebenszyklus von Standardsoftware gestaltet werden kann. Sie werden durch die anderen genannten Maßnahmen ergänzt.

**Planung und Konzeption**

- M 2.79 (A) *Festlegung der Verantwortlichkeiten im Bereich Standardsoftware*
- M 2.80 (A) *Erstellung eines Anforderungskatalogs für Standardsoftware*
- M 2.82 (B) *Entwicklung eines Testplans für Standardsoftware*
- M 2.378 (Z) *System-Entwicklung*
- M 2.379 (Z) *Software-Entwicklung durch Endbenutzer*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*

**Beschaffung**

- M 2.66 (Z) *Beachtung des Beitrags der Zertifizierung für die Beschaffung*
- M 2.81 (B) *Vorauswahl eines geeigneten Standardsoftwareproduktes*

**Umsetzung**
- M 2.83 (B) *Testen von Standardsoftware*
- M 2.84 (A) *Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware*
- M 2.85 (A) *Freigabe von Standardsoftware*
- M 2.86 (B) *Sicherstellen der Integrität von Standardsoftware*
- M 2.87 (A) *Installation und Konfiguration von Standardsoftware*
- M 2.90 (A) *Überprüfung der Lieferung*
- M 4.42 (Z) *Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung*

**Betrieb**
- M 2.88 (A) *Lizenzverwaltung und Versionskontrolle von Standardsoftware*

**Aussonderung**
- M 2.89 (C) *Deinstallation von Standardsoftware*

# B 1.11 Outsourcing

## Beschreibung

Beim Outsourcing werden Arbeits- oder Geschäftsprozesse einer Institution ganz oder teilweise zu externen Dienstleistern ausgelagert. Outsourcing kann sowohl Nutzung und Betrieb von Hardware und Software, aber auch Dienstleistungen betreffen. Dabei ist es unerheblich, ob die Leistungen in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht werden. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wachdienstes. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe ergänzt wird: Mit Offshoring wird das Auslagern von Geschäfts- und Produktionsprozessen in Lokationen in einem anderem Land bezeichnet. Tasksourcing bezeichnet das Auslagern von einzelnen Aufgaben. Werden Dienstleistungen mit Bezug zur Informationssicherheit ausgelagert, wird von Security Outsourcing oder Managed Security Services gesprochen. Beispiele sind die Auslagerung des Firewall-Betriebs, die Überwachung des Netzes, Virenschutz oder der Betrieb eines Virtual Private Networks (VPN). Unter Application Service Provider (ASP) versteht man einen Dienstleister, der auf seinen eigenen Systemen einzelne Anwendungen oder Software für seine Kunden betreibt (E-Mail, SAP-Anwendungen, Archivierung, Web-Shops, Beschaffung). Auftraggeber und Dienstleister sind dabei über das Internet oder ein VPN miteinander verbunden. Beim Application Hosting ist ebenfalls der Betrieb von Anwendungen an einen Dienstleister ausgelagert, jedoch gehören im Gegensatz zum ASP-Modell die Anwendungen noch dem jeweiligen Kunden. Da die Grenzen zwischen klassischem Outsourcing und reinem ASP in der Praxis zunehmend verschwimmen, wird im Folgenden nur noch der Oberbegriff Outsourcing verwendet.

Das Auslagern und Umstrukturieren von Geschäfts- und Produktionsprozessen ist ein etablierter Bestandteil heutiger Organisationsstrategien. Der Trend zum Outsourcing scheint auch für die nächste Zukunft ungebrochen. Es gibt aber inzwischen auch publizierte Beispiele für gescheiterte Outsourcing-Projekte, wo der Auftraggeber den Outsourcing-Vertrag gekündigt hat und die ausgelagerten Geschäftsprozesse wieder in Eigenregie betreibt (Insourcing).

Die Gründe für Outsourcing sind vielfältig: die Konzentration einer Institution auf ihre Kernkompetenzen, die Möglichkeit einer Kostenersparnis (z. B. keine Anschaffungs- oder Betriebskosten für IT-Systeme), der Zugriff auf spezialisierte Kenntnisse und Ressourcen, die Freisetzung interner Ressourcen für andere Aufgaben, die Straffung der internen Verwaltung, die verbesserte Skalierbarkeit der Geschäfts- und Produktionsprozesse, die Erhöhung der Flexibilität sowie der Wettbewerbsfähigkeit einer Institution sind nur einige Beispiele.

Beim Auslagern von IT-gestützten Geschäftsprozessen werden die IT-Systeme und Netze der auslagernden Institution und ihres Outsourcing-Dienstleisters in der Regel eng miteinander verbunden, so dass Teile von internen Geschäftsprozessen unter Leitung und Kontrolle eines externen Dienstleisters ablaufen. Ebenso findet auf personeller Ebene ein intensiver Kontakt statt.

Durch die enge Verbindung zum Dienstleister und die entstehende Abhängigkeit von der Dienstleistungsqualität ergeben sich Risiken für den Auftraggeber, durch die im schlimmsten Fall sogar die Geschäftsgrundlage des Unternehmens oder der Behörde vital gefährdet werden können. (beispielsweise könnten sensitive interne Informationen gewollt oder ungewollt nach außen preisgegeben werden. Der Betrachtung von Sicherheitsaspekten und der Gestaltung vertraglicher Regelungen zwischen Auftraggeber und Outsourcing-Dienstleister kommt im Rahmen eines Outsourcing-Vorhabens somit eine zentrale Rolle zu.

Den Schwerpunkt dieses Bausteins bilden daher Maßnahmen, die sich mit Aspekten der Informationssicherheit beim Outsourcing beschäftigen. Dazu zählen ebenfalls geeignete Maßnahmen zur Kontrolle der vertraglich vereinbarten Ziele und Leistungen sowie der Sicherheitsmaßnahmen.

## Gefährdungslage

Die Gefährdungslage eines Outsourcing-Vorhabens ist ausgesprochen vielschichtig. Die Entscheidung über das Auslagern einer speziellen Aktivität beeinflusst nachhaltig die strategische Ausrichtung der Institution, die Definition ihrer Kernkompetenzen, die Ausgestaltung der Wertschöpfungskette und betrifft viele weitere wesentliche Belange eines Organisationsmanagements. Es sollten daher alle Anstrengungen unternommen werden, um Fehlentwicklungen des Unternehmens oder der Behörde frühzeitig zu erkennen und zu verhindern.

Die Gefährdungen können parallel auf physikalischer, technischer und auch menschlicher Ebene existieren und sind nachfolgend in den einzelnen Gefährdungskatalogen aufgeführt. Um die jeweils existierenden Risiken quantitativ bewerten zu können, müssen zuvor die institutionseigenen Werte und Informationen entsprechend ihrer strategischen Bedeutung für die Institution beurteilt und klassifiziert werden.

**Höhere Gewalt**

- G 1.10 *Ausfall eines Weitverkehrsnetzes*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.47 *Ungesicherter Akten- und Datenträgertransport*
- G 2.66 *Unzureichendes Sicherheitsmanagement*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.83 *Fehlerhafte Outsourcing-Strategie*
- G 2.84 *Unzulängliche vertragliche Regelungen mit einem externen Dienstleister*
- G 2.85 *Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens*
- G 2.86 *Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister*
- G 2.88 *Störung des Betriebsklimas durch ein Outsourcing-Vorhaben*
- G 2.89 *Mangelhafte Informationssicherheit in der Outsourcing-Einführungsphase*
- G 2.93 *Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.105 *Ungenehmigte Nutzung von externen Dienstleistungen*

**Technisches Versagen**

- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.34 *Ausfall eines Kryptomoduls*
- G 4.48 *Ausfall der Systeme eines Outsourcing-Dienstleisters*
- G 4.97 *Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister*

**Vorsätzliche Handlungen**

- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.42 *Social Engineering*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.107 *Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein ausgelagerter Geschäftsprozess oder Informationsverbund kann sowohl aus Komponenten bestehen, die sich ausschließlich im Einflussbereich des Outsourcing-Dienstleisters befinden, als auch aus Komponenten beim Auftraggeber. In der Regel gibt es in diesem Fall Schnittstellen zur Verbindung der

Systeme. Für jedes Teilsystem und für die Schnittstellenfunktionen muss IT-Grundschutz gewährleistet sein.

Ein Outsourcing-Vorhaben besteht aus mehreren Phasen, die im Folgenden kurz dargestellt sind.

**Phase 1: Strategische Planung des Outsourcing-Vorhabens**

Schon im Rahmen der strategischen Entscheidung, ob und in welcher Form ein Outsourcing-Vorhaben umgesetzt wird, müssen die sicherheitsrelevanten Gesichtspunkte herausgearbeitet werden. In der Maßnahme M 2.250 *Festlegung einer Outsourcing-Strategie* werden die wesentlichen Punkte vorgestellt, die zu beachten sind.

**Phase 2: Definition der wesentlichen Sicherheitsanforderungen**

Wenn die Entscheidung zum Outsourcing gefallen ist, müssen die wesentlichen übergeordneten Sicherheitsanforderungen für das Outsourcing-Vorhaben festgelegt werden. Diese Sicherheitsanforderungen sind die Basis für das Ausschreibungsverfahren (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*).

**Phase 3: Auswahl des Outsourcing-Dienstleisters**

Der Wahl des Outsourcing-Dienstleisters kommt eine besondere Bedeutung zu (siehe M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters*).

**Phase 4: Vertragsgestaltung**

Auf Basis des Pflichtenheftes muss nun ein Vertrag mit dem Partner ausgehandelt werden, der die gewünschten Leistungen inklusive Qualitätsstandards und Fristen im Einklang mit der vorhandenen Gesetzgebung festschreibt. Diese Verträge werden häufig als Service Level Agreements (SLA) bezeichnet. In diesem Vertrag müssen auch die genauen Modalitäten der Zusammenarbeit geklärt sein: Ansprechpartner, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der Sicherheitsvorkehrungen, Umgang mit vertraulichen Informationen, Verwertungsrechte, Weitergabe von Information an Dritte etc. (siehe hierzu M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister*).

**Phase 5: Erstellung eines Sicherheitskonzepts für den ausgelagerten Informationsverbund**

In enger Zusammenarbeit müssen Auftraggeber und Outsourcing-Dienstleister ein detailliertes Sicherheitskonzept (M 2.254 *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben*), das ein Notfallvorsorgekonzept (M 6.83 *Notfallvorsorge beim Outsourcing*) enthält, erstellen.

Phase 5 wird in der Regel erst nach Beendigung der Migrationsphase abgeschlossen werden können, weil sich während der Migration der IT-Systeme und Anwendungen immer wieder neue Erkenntnisse ergeben, die in das Sicherheitskonzept eingearbeitet werden müssen.

**Phase 6: Migrationsphase**

Besonders sicherheitskritisch ist die Migrations- oder Übergangsphase, die deshalb einer sorgfältigen Planung bedarf (siehe M 2.255 *Sichere Migration bei Outsourcing-Vorhaben*).

**Phase 7: Planung und Sicherstellen des laufenden Betriebs**

Wenn der Outsourcing-Dienstleister die Systeme bzw. Geschäftsprozesse übernommen hat, sind verschiedene Maßnahmen, wie regelmäßige Kontrollen und Durchführung von Systemwartungen, zur Aufrechterhaltung der Informationssicherheit im laufenden Betrieb notwendig (siehe M 2.256 *Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb*). Diese müssen im Vorfeld entsprechend geplant werden. Notfall- und Eskalationsszenarien müssen unbedingt in der Planung mit berücksichtigt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Outsourcing" vorgestellt.

**Planung und Konzeption**

- M 2.40 (A) *Rechtzeitige Beteiligung des Personal-/Betriebsrates*

- M 2.42 (A) *Festlegung der möglichen Kommunikationspartner*
- M 2.221 (A) *Änderungsmanagement*
- M 2.226 (A) *Regelungen für den Einsatz von Fremdpersonal*
- M 2.250 (A) *Festlegung einer Outsourcing-Strategie*
- M 2.251 (A) *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*
- M 2.254 (A) *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben*

**Beschaffung**

- M 2.252 (A) *Wahl eines geeigneten Outsourcing-Dienstleisters*

**Umsetzung**

- M 2.253 (A) *Vertragsgestaltung mit dem Outsourcing-Dienstleister*
- M 2.255 (A) *Sichere Migration bei Outsourcing-Vorhaben*
- M 2.460 (C) *Geregelte Nutzung von externen Dienstleistungen*
- M 3.33 (Z) *Sicherheitsüberprüfung von Mitarbeitern*
- M 5.87 (C) *Vereinbarung über die Anbindung an Netze Dritter*
- M 5.88 (C) *Vereinbarung über Datenaustausch mit Dritten*

**Betrieb**

- M 2.256 (A) *Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb*

**Aussonderung**

- M 2.307 (A) *Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses*

**Notfallvorsorge**

- M 6.83 (A) *Notfallvorsorge beim Outsourcing*

# B 1.12 Archivierung

## Beschreibung

Die Abbildung von Geschäftsprozessen und -unterlagen in elektronische Dokumente erfordert eine geeignete Ablage der entstehenden Daten für die spätere Verwendung, deren Wiederfinden und Aufbereitung. Dies betrifft sowohl Datensätze als auch elektronische Repräsentationen papierner Geschäftsdokumente und Belege. Die dauerhafte und unveränderbare Speicherung von elektronischen Dokumenten und anderen Daten wird als Archivierung bezeichnet.

Die Archivierung ist als Teil eines Prozesses zu sehen. Neben der Erzeugung, Bearbeitung und Verwaltung elektronischer Dokumente spielt die dauerhafte Speicherung (Archivierung) eine besondere Rolle, denn es wird üblicherweise erwartet, dass einerseits die Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind und andererseits deren Vertraulichkeit- und Integrität gewahrt bleibt. Unter Umständen sollen elektronische Dokumente zeitlich unbegrenzt verfügbar sein.

Die Spannweite der Realisierungsmöglichkeiten eines Archivsystems umfasst:

- kleine Archivsysteme, z. B. bestehend aus einen Archivserver mit angeschlossenem Massenspeicher (wie Festplatte oder Jukebox), bis hin zu
- komplexen, gegebenenfalls weltweit verteilten Archivsystemen zur organisationsweiten Archivierung von relevanten Geschäftsdaten, bestehend aus:
  - zentralen Archivserver-Komponenten mit RAID-Systemen, Jukeboxen oder der Anbindung an Storage Area Networks (SAN) für das zentrale Speichern von Dateien,
  - WORM-Medien für die revisionssichere, unveränderbare Speicherung von Daten,
  - Komponenten zur Indizierung von Dateien, Recherche und zur Umwandlung von Speicherformaten (Rendition),
  - dezentralen Cache-Servern für den schnellen Zugriff auf häufig benötigte Daten,
  - Client-Software, die einen direkten Zugriff auf Daten des Archivs erlaubt (z. B. auch aus Office-Anwendungen heraus).

Es ist zweckmäßig, elektronische Archivierung gegenüber Datensicherung abzugrenzen. Bei einer Datensicherung werden Kopien der System- und Nutzdaten angelegt. Die gesicherten Daten werden hierbei physikalisch vom IT-System getrennt und gefahrengeschützt gelagert. Kennzeichnend für elektronische Archivierung ist, dass Dokumente und Daten je nach Vorgaben über einen langen Zeitraum unveränderlich digital aufbewahrt werden. Dazu ist auch der Kontext zu erhalten, damit der jeweilige gespeicherte Vorgang rekonstruiert werden kann.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zur elektronischen Archivierung erstellt und wie der Aufbau eines Archivsystems und dessen Einbettung innerhalb eines Unternehmens bzw. einer Behörde sichergestellt werden kann. Der Aufwand zur Erstellung und Umsetzung eines solchen Konzepts ist nicht gering. Dieser Baustein sollte immer dann angewandt werden, wenn die zu archivierenden Daten langfristig für die Behörde bzw. das Unternehmen relevant sind.

## Gefährdungslage

Für die bei der elektronischen Archivierung zu betrachtenden Archivsysteme sowie die zugehörigen Organisationsprozesse werden im Rahmen des IT-Grundschutzes die folgenden typischen Gefährdungen angenommen:

### Höhere Gewalt

- G 1.2 *Ausfall von IT-Systemen*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.9 *Datenverlust durch starke Magnetfelder*
- G 1.14 *Datenverlust durch starkes Licht*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.72 *Unzureichende Migration von Archivsystemen*
- G 2.73 *Fehlende Revisionsmöglichkeit von Archivsystemen*
- G 2.74 *Unzureichende Ordnungskriterien für Archive*
- G 2.75 *Mangelnde Kapazität von Archivdatenträgern*
- G 2.76 *Unzureichende Dokumentation von Archivzugriffen*
- G 2.77 *Unzulängliche Übertragung von Papierdaten in elektronische Archive*
- G 2.78 *Unzulängliche Auffrischung von Datenbeständen bei der Archivierung*
- G 2.79 *Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung*
- G 2.80 *Unzureichende Durchführung von Revisionen bei der Archivierung*
- G 2.81 *Unzureichende Vernichtung von Datenträgern bei der Archivierung*
- G 2.82 *Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.35 *Server im laufenden Betrieb ausschalten*
- G 3.54 *Verwendung ungeeigneter Datenträger bei der Archivierung*
- G 3.55 *Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen*

**Technisches Versagen**

- G 4.7 *Defekte Datenträger*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.20 *Überlastung von Informationssystemen*
- G 4.26 *Ausfall einer Datenbank*
- G 4.30 *Verlust der Datenbankintegrität/-konsistenz*
- G 4.31 *Ausfall oder Störung von Netzkomponenten*
- G 4.45 *Verzögerte Archivauskunft*
- G 4.46 *Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung*
- G 4.47 *Veralten von Kryptoverfahren*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.6 *Anschlag*
- G 5.29 *Unberechtigtes Kopieren der Datenträger*
- G 5.82 *Manipulation eines Kryptomoduls*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.102 *Sabotage*
- G 5.105 *Verhinderung der Dienste von Archivsystemen*
- G 5.106 *Unberechtigtes Überschreiben oder Löschen von Archivmedien*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Darüber hinaus wird die im Folgenden beschriebene Vorgehensweise für die Einführung und den Betrieb von elektronischen Archivsystemen empfohlen. Bereits bei der Planung ist zu berücksichtigen, dass die eingesetzten Archivsysteme und -medien im Lauf der Zeit technologisch und physikalisch veralten werden. Daher schließt sich an eine Planungs- und Einführungs-/Betriebsphase eine Migrationsphase an, in der das bestehende Archivsystem oder Teile davon durch neue Technologien und Komponenten ersetzt werden. Die Migrationsphase umfasst auch die Übertragung der archivierten Daten und Dokumente in zukünftig verwendete Datenformate.

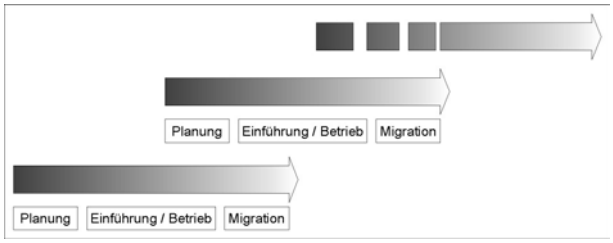



Abbildung: Planung von Migrationsschritten innerhalb der Archivierungssystem-Planung

Die einzelnen Phasen und die darin umzusetzenden Maßnahmen sind nachfolgend kurz erläutert.

**1. Planungsphase**

In der Planungsphase muss die Zielsetzung, die mit dem Einsatz des Archivsystems verbunden ist, formuliert werden (siehe M 2.242 *Zielsetzung der elektronischen Archivierung*). Hierbei müssen die relevanten organisatorischen, rechtlichen und technischen Anforderungen ermittelt werden, wobei auch abgeschätzt werden muss, wie sich die Anforderungen während der erwarteten Laufzeit des einzuführenden Archivsystems entwickeln werden (siehe M 2.244 *Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung*, M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung* und M 2.246 *Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung*). Die Ergebnisse müssen in einem Archivierungskonzept niedergelegt werden (siehe M 2.243 *Entwicklung des Archivierungskonzepts*).

**2. Einführung und Betrieb**

Bei der Einführung eines Archivsystems ist zunächst ein System auszuwählen, das den ermittelten Anforderungen genügt. Darüber hinaus sind der Aufstellungsort des Systems sowie der Lagerungsort der Archivmedien festzulegen (siehe M 4.168 *Auswahl eines geeigneten Archivsystems*, M 4.169 *Verwendung geeigneter Archivmedien*, M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*, M 1.59 *Geeignete Aufstellung von Speicher- und Archivsystemen*, M 1.60 *Geeignete Lagerung von Archivmedien*).

Neben dem Archivsystem als solches muss ein geeignetes übergeordnetes Dokumentenmanagement-System zur Verwaltung der Inhalte des Archivs eingeführt werden (siehe M 2.258 *Konsistente Indizierung von Dokumenten bei der Archivierung*, M 2.259 *Einführung eines übergeordneten Dokumentenmanagements*).

Es müssen die Regelungen für die Nutzung des Archivsystems sowie den Einsatz digitaler Signaturen festgelegt und die Administratoren und Benutzer geschult werden (siehe M 2.262 *Regelung der Nutzung von Archivsystemen*, M 2.265 *Geeigneter Einsatz digitaler Signaturen bei der Archivierung*, M 3.34 *Einweisung in die Administration des Archivsystems*, M 3.35 *Einweisung der Benutzer in die Bedienung des Archivsystems*).

Um die Ordnungsmäßigkeit langfristig sicherstellen zu können, ist der Archivierungsprozess kontinuierlich zu überwachen und auf Korrektheit zu prüfen. Darüber hinaus ist sicherzustellen, dass zu jedem Zeitpunkt genügend Medien zur Archivierung verfügbar sind (siehe M 2.257 *Überwachung der Speicherressourcen von Archivmedien*, M 2.260 *Regelmäßige Revision des Archivierungsprozesses* M 2.263 *Regelmäßige Aufbereitung von archivierten Datenbeständen*, M 4.171 *Schutz der Integrität der Index-Datenbank von Archivsystemen*, M 4.172 *Protokollierung der Archivzugriffe*, M 4.173 *Regelmäßige Funktions- und Recoverytests bei der Archivierung*, M 6.84 *Regelmäßige Datensicherung der System- und Archivdaten*).

In Abhängigkeit der konkret eingesetzten Archivsoftware müssen auch die in Baustein B 5.7 *Datenbanken* beschriebenen Maßnahmen umgesetzt werden.

**3. Migrationsphase**

Die Migrationsphase wird häufig durch Ereignisse wie die folgenden ausgelöst:

- Bei Systemkomponenten oder Datenformaten hat ein Technologiewechsel stattgefunden, daher sollten die Entwicklungen in diesem Bereich beobachtet werden (siehe M 2.261 *Regelmäßige Marktbeobachtung von Archivsystemen*).
- Systemkomponenten, insbesondere Datenträger, sind überaltert und müssen durch neue ersetzt werden (siehe M 2.266 *Regelmäßige Erneuerung technischer Archivsystem-Komponenten*).
- Die Nutzungskriterien für das Archivsystem haben sich geändert.
- Kryptographische Verfahren, Produkte bzw. Schlüssel müssen durch neue abgelöst werden (siehe M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*).

Nachfolgend wird das Maßnahmenbündel für den Einsatz elektronischer Archivsysteme vorgestellt:

**Planung und Konzeption**
- M 2.242 (A) *Zielsetzung der elektronischen Archivierung*
- M 2.243 (A) *Entwicklung des Archivierungskonzepts*
- M 2.244 (A) *Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung*
- M 2.245 (A) *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung*
- M 2.246 (A) *Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung*
- M 2.259 (Z) *Einführung eines übergeordneten Dokumentenmanagements*
- M 2.262 (A) *Regelung der Nutzung von Archivsystemen*
- M 2.265 (Z) *Geeigneter Einsatz digitaler Signaturen bei der Archivierung*

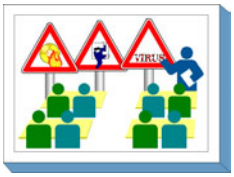
**Beschaffung**
- M 4.168 (B) *Auswahl eines geeigneten Archivsystems*
- M 4.169 (B) *Verwendung geeigneter Archivmedien*
- M 4.170 (B) *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*

**Umsetzung**
- M 1.59 (A) *Geeignete Aufstellung von Speicher- und Archivsystemen*
- M 2.266 (C) *Regelmäßige Erneuerung technischer Archivsystem-Komponenten*
- M 3.34 (A) *Einweisung in die Administration des Archivsystems*
- M 3.35 (A) *Einweisung der Benutzer in die Bedienung des Archivsystems*

**Betrieb**
- M 1.60 (A) *Geeignete Lagerung von Archivmedien*
- M 2.257 (C) *Überwachung der Speicherressourcen von Archivmedien*
- M 2.258 (A) *Konsistente Indizierung von Dokumenten bei der Archivierung*
- M 2.260 (B) *Regelmäßige Revision des Archivierungsprozesses*
- M 2.261 (B) *Regelmäßige Marktbeobachtung von Archivsystemen*
- M 2.263 (A) *Regelmäßige Aufbereitung von archivierten Datenbeständen*
- M 2.264 (B) *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*
- M 4.171 (A) *Schutz der Integrität der Index-Datenbank von Archivsystemen*
- M 4.172 (C) *Protokollierung der Archivzugriffe*
- M 4.173 (B) *Regelmäßige Funktions- und Recoverytests bei der Archivierung*

**Notfallvorsorge**
- M 6.84 (A) *Regelmäßige Datensicherung der System- und Archivdaten*

# B 1.13 Sensibilisierung und Schulung zur Informationssicherheit




## Beschreibung

In diesem Baustein wird beschrieben, wie ein effektives Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit aufgebaut und aufrechterhalten werden kann.

Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Hierfür müssen eine Sicherheitskultur und ein Sicherheitsbewusstsein (Awareness) aufgebaut und gepflegt werden. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Denn je mehr sie sich damit auskennen, desto eher akzeptieren sie entsprechende Sicherheitsmaßnahmen. Sie müssen auch über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Ziel der Sensibilisierung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen. Durch Schulungen zur Informationssicherheit sollen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten erwerben.

Eine angemessene Informationssicherheit sollte von allen Mitarbeitern als selbstverständlicher Teil ihrer Arbeitsumgebung verinnerlicht werden. Dies setzt in vielen Bereichen eine langfristige Verhaltensänderung voraus, besonders wenn Informationssicherheit mit Komfort- oder Funktionseinbußen verbunden ist. Um hier nachhaltige Ergebnisse zu erzielen, ist ein kontinuierlicher Prozess erforderlich. Daher muss die Institution ein durchgängiges Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erarbeiten und etablieren. Es sollte bereits bei der Einstellung von Mitarbeitern beginnen, unterschiedliche Zielgruppen mit deren Fähigkeiten, Arbeitsabläufen und benötigten Ressourcen berücksichtigen und die Mitarbeiter auch begleiten, wenn sich ihre Aufgaben oder Positionen verändern.

## Gefährdungslage

Für den IT-Grundschutz werden in diesem Baustein die folgenden typische Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.102 *Unzureichende Sensibilisierung für Informationssicherheit*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*
- G 2.141 *Nicht erkannte Sicherheitsvorfälle*
- G 2.201 *Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.42 *Social Engineering*
- G 5.102 *Sabotage*
- G 5.104 *Ausspähen von Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Sensibilisierungs- und Schulungsprogramm sollte auf die Institution zugeschnitten sein und die dort vorhandene Kultur (siehe M 3.83 *Analyse sicherheitsrelevanter personeller Faktoren*) sowie das notwendige Sicherheitsniveau berücksichtigen. In diesem Rahmen sind möglichst unterschiedliche und aufeinander abgestimmte Methoden und Medien zu verwenden.

**Planung und Konzeption**

Es ist für den Sicherheitsprozess sehr wichtig, dass dieser aktiv vom Management unterstützt wird. Hierfür muss es den Wert von Informationssicherheit für die Ziele der Institution erkannt und verinnerlicht haben (siehe M 3.44 *Sensibilisierung des Managements für Informationssicherheit*). Wie das Management den gesamten Lebenszyklus eines Sensibilisierungs- und Schulungsprogramms wirkungsvoll unterstützen kann, beschreibt Maßnahme M 3.96 *Unterstützung des Managements für Sensibilisierung und Schulung*.

Diese Unterstützung kann z. B. mit dem expliziten Auftrag zur Konzeption entsprechender Programme beginnen. Die notwendigen Schritte sind in den Maßnahmen M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit* und M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit* beschrieben. Wichtig ist hier insbesondere, die Zielgruppen zu definieren (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*).

**Beschaffung**

Um Sensibilisierungs- und Schulungsmaßnahmen vorzubereiten und durchzuführen, wird internes oder externes Personal benötigt (siehe M 3.48 *Auswahl von Trainern oder externen Schulungsanbietern*).

**Umsetzung**

In der Umsetzungsphase werden die Mitarbeiter den vorher definierten Zielgruppen zugeordnet und zielgruppenspezifisch geeignete Inhalte für Sensibilisierungs- und Schulungsmaßnahmen ausgewählt (siehe M 3.45 *Planung von Schulungsinhalten zur Informationssicherheit*). Auch sind Maßnahmen umzusetzen, durch die bei den Mitarbeitern die Ansprechpartner für Sicherheitsfragen bekannter werden (siehe M 3.46 *Ansprechpartner zu Sicherheitsfragen*).

Darüber hinaus werden für Sensibilisierungs- und Schulungsmaßnahmen diverse Ressourcen benötigt, beispielsweise Personal, geeignete Räumlichkeiten oder spezielles Equipment. Besondere Sicherheitsaspekte, die bei der Gestaltung von Schulungsräumen zu beachten sind, finden sich in Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume*.

**Betrieb, kontinuierliche Pflege und Weiterentwicklung**

Für eine erfolgreiche Lernstoffvermittlung müssen die richtigen Methoden und Medien eingesetzt werden (siehe M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit* und M 3.47 *Durchführung von Planspielen zur Informationssicherheit*).

Ein weiterer wichtiger Bestandteil von Schulungen zur Informationssicherheit ist der Umgang mit der Informationstechnik (siehe M 3.26 *Einweisung des Personals in den sicheren Umgang mit IT* und wei-

tere themenspezifische Maßnahmen). Besonders wenn neue Techniken eingeführt werden, sollten die Mitarbeiter frühzeitig über diese informiert sowie für Gefahrenpotenziale und Sicherheitsmaßnahmen sensibilisiert werden.

Um die Präsenz von vermittelten Lerninhalten zu verbessern, können Methoden der Lernstoffsicherung eingesetzt werden (siehe M 3.95 *Lernstoffsicherung*). Auch sollte regelmäßig überprüft werden, ob die Sensibilisierungs- und Schulungsmaßnahmen erfolgreich sind (siehe M 3.94 *Messung und Auswertung des Lernerfolgs*). Bei Bedarf müssen sie angepasst werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Sensibilisierung und Schulung zur Informationssicherheit" vorgestellt.

**Planung und Konzeption**

- M 2.312 (A) *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit*
- M 2.557 (A) *Konzeption eines Schulungsprogramms zur Informationssicherheit*
- M 3.44 (A) *Sensibilisierung des Managements für Informationssicherheit*
- M 3.51 (Z) *Geeignetes Konzept für Personaleinsatz und -qualifizierung*
- M 3.83 (Z) *Analyse sicherheitsrelevanter personeller Faktoren*
- M 3.93 (A) *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*
- M 3.96 (A) *Unterstützung des Managements für Sensibilisierung und Schulung*

**Beschaffung**

- M 3.48 (Z) *Auswahl von Trainern oder externen Schulungsanbietern*

**Umsetzung**

- M 3.45 (A) *Planung von Schulungsinhalten zur Informationssicherheit*
- M 3.46 (A) *Ansprechpartner zu Sicherheitsfragen*
- M 3.49 (B) *Schulung zur Vorgehensweise nach IT-Grundschutz*

**Betrieb**

- M 2.198 (A) *Sensibilisierung der Mitarbeiter für Informationssicherheit*
- M 3.26 (A) *Einweisung des Personals in den sicheren Umgang mit IT*
- M 3.47 (Z) *Durchführung von Planspielen zur Informationssicherheit*
- M 3.94 (C) *Messung und Auswertung des Lernerfolgs*
- M 3.95 (Z) *Lernstoffsicherung*

# B 1.14 Patch- und Änderungsmanagement

## Beschreibung

Aufgabe des Änderungsmanagements ist es, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozessen und Verfahren steuer- und kontrollierbar zu gestalten. Vor allem im Bereich der Informationstechnologie stehen viele Behörden und Unternehmen aufgrund der immer schneller fortschreitenden Entwicklung und den steigenden Anforderungen durch die Anwender vor der Herausforderung, die notwendigen Neuerungen an den Komponenten ihrer Systemlandschaft korrekt und zeitnah zu übernehmen.

Erfahrungen in Behörden und Unternehmen zeigen, dass Sicherheitslücken oder Störungen beim Betrieb häufig auf fehlerhafte oder nicht erfolgte Änderungen zurückzuführen sind. Fehlendes oder vernachlässigtes Patch- oder Änderungsmanagement führt schnell zu Lücken in der Sicherheit der einzelnen Komponenten und damit zu möglichen Angriffspunkten.

In diesem Baustein wird aufgezeigt, wie ein funktionierendes Patch- und Änderungsmanagement in einer Institution aufgebaut werden kann, wie der entsprechende Prozess zum Patch- und Änderungsmanagement kontrolliert und optimiert werden kann, damit Störungen im Betrieb vermieden sowie Sicherheitslücken minimiert und zeitnah beseitigt werden können. Die Beschreibungen konzentrieren sich dabei auf den IT-Betrieb, können aber auch sinngemäß in anderen Geschäftsprozessen umgesetzt werden. Mit Patch- und Änderungsmanagement wird in diesem Baustein die Aufgabe der Planung und Steuerung von Änderungen bezeichnet, auch wenn dieser Begriff in anderen Zusammenhängen teilweise für die Personen verwendet wird, die diese Aufgabe wahrnehmen.

Der Aufwand zur Erstellung und Umsetzung eines solchen Prozesses ist nicht gering. Daher sollte dieser Baustein vor allem bei größeren Informationsverbünden umgesetzt werden. Bei kleineren und wenig komplexen Informationsverbünden reicht unter Umständen die Umsetzung von M 2.221 *Änderungsmanagement* aus.

## Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.17 *Mangelhafte Kennzeichnung der Datenträger*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.28 *Verstöße gegen das Urheberrecht*
- G 2.132 *Mangelnde Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement*
- G 2.133 *Mangelhaft festgelegte Verantwortlichkeiten beim Patch- und Änderungsmanagement*
- G 2.134 *Unzureichende Ressourcen beim Patch- und Änderungsmanagement*
- G 2.135 *Mangelhafte Kommunikation beim Patch- und Änderungsmanagement*
- G 2.136 *Fehlende Übersicht über den Informationsverbund*
- G 2.137 *Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen*
- G 2.138 *Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement*
- G 2.139 *Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement*
- G 2.140 *Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement*

**Menschliche Fehlhandlungen**

- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.92 *Fehleinschätzung der Relevanz von Patches und Änderungen*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.71 *Probleme bei der automatisierten Verteilung von Patches und Änderungen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.145 *Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um ein effektives System zur Behandlung von Patches und Änderungen einzurichten, sind eine Reihe von Schritten zu durchlaufen.

**Planung und Konzeption**

Über das Patch- und Änderungsmanagement sollten alle Änderungen an Hard- und Softwareständen sowie deren Konfigurationen gesteuert und kontrolliert werden. Um alle Änderungen erfassen und bewerten zu können, sollten alle innerhalb des Patch- und Änderungsmanagements erfassten IT-Systeme diesem unterstellt sein (siehe M 2.423 *Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement*). Änderungen an Konfiguration und Zustand der Systeme sind damit nur noch über das Patch- und Änderungsmanagement möglich. Dies erfordert eine entsprechende Delegation der Verantwortung durch die Leitung der Behörde oder des Unternehmens. Die organisatorische Umsetzung des Patch- und Änderungsmanagements stellt eine Querschnittsfunktion durch verschiedene Abteilungen einer Institution dar. Insbesondere sind der IT-Betrieb, das Informationssicherheitsmanagement und die Fachabteilungen einzubinden.

Ein einzelner Patch- oder Änderungsvorgang beginnt mit einer Änderungsanforderung. Diese sollte zunächst erfasst und durch den Änderungsmanager kontrolliert werden. Zu dieser Änderung sollten Relevanz, Dringlichkeit, geplante Durchführung (Termin, Ablauf) sowie mögliche Risiken und Probleme zusammengestellt und erfasst werden (siehe M 2.421 *Planung des Patch- und Änderungsmanagementprozesses* und M 2.422 *Umgang mit Änderungsanforderungen*).

Das Patch- und Änderungsmanagement kann durch technische Hilfsmittel, beispielsweise zum automatischen Verteilen von Software, sinnvoll unterstützt werden. Werden für die Umsetzung des Patch- und Änderungsmanagements spezielle Tools eingesetzt, so muss sichergestellt werden, dass ein Konzept für deren Einsatz erstellt wird (siehe M 2.424 *Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen*).

**Beschaffung**

Es gibt unterschiedliche Produkte, die den Patch- und Änderungsmanagementprozess unterstützen. Um aus diesen Produkten eine geeignete Auswahl zu treffen, müssen vor der Beschaffung die Anforderungen an diese Werkzeuge, zum Beispiel welche Plattformen unterstützt werden müssen, festgelegt werden (siehe M 2.425 *Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement*).

**Umsetzung**

Bei der Umsetzung sollten alle vom Patch- und Änderungsmanagement betreuten IT-Systeme diesem einzeln oder gruppenweise unterstellt werden. Des Weiteren müssen Änderungen an diesen Systemen an einer zentralen Stelle dokumentiert werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

**Betrieb**

Je nach Größe und Komplexität eines Patches oder einer durchzuführenden Änderung wird empfohlen, in einem Durchführungsplan Tests, Kontroll- und Abbruchpunkte sowie Prioritäten für die Verteilung zu definieren. Dabei muss sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach der Änderung erhalten bleibt. Die Freigabe und Durchführung von Änderungen sollten abgestimmt und dabei Ressourcen und Interessen von Fachbereichen und IT-Betrieb berücksichtigt werden (siehe M 2.426 *Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse* und M 2.427 *Abstimmung von Änderungsanforderungen*).

Zur Qualitätssicherung und um Fehler erkennen beziehungsweise zukünftigen Fehlern vorbeugen zu können, sollte jeder Patch und jede Änderung, nachdem sie aufgespielt wurden, (siehe M 2.429 *Erfolgsmessung von Änderungsanforderungen*) bewertet werden.

Änderungen, insbesondere Softwareaktualisierungen, können manuell, aber auch mit Hilfe von geeigneten Tools durchgeführt werden. Bei Einsatz dieser Werkzeuge ist darauf zu achten, dass diese gegen Missbrauch besonders gesichert sind, und nicht zu einer Gefährdung der Gesamtsicherheit führen, da sie häufig mit Systemadministrator-Berechtigungen arbeiten. Tools bieten die Möglichkeit an vielen Systemen gleichzeitig Änderungen durchzuführen. Dadurch multiplizieren sich aber auch die Auswirkungen von Fehlern, so dass sehr sorgfältige Tests gemacht werden sollten, bevor die Änderung durchgeführt wird (siehe M 2.428 *Skalierbarkeit beim Patch- und Änderungsmanagement*). Zu berücksichtigen ist ebenfalls, dass umzustellende Systeme zeitweise oder permanent abgeschaltet bzw. nicht erreichbar sein könnten. Dies betrifft vor allem mobile Geräte wie zum Beispiel Laptops, Smartphones und PDAs (siehe M 4.323 *Synchronisierung innerhalb des Patch- und Änderungsmanagements*). Außerdem muss während des gesamten Patch- und Änderungsmanagementprozesses die Integrität und Authentizität der verwendeten Software technisch sicher gestellt werden (siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Die Autoupdate-Mechanismen verwendeter Software müssen, unabhängig von ihrem Einsatzgrad innerhalb des Patch- und Änderungsprozesses, betrachtet werden (siehe M 4.324 *Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement*).

**Aussonderung**

Werden Systeme zum Patch- und Änderungsmanagement außer Kraft gesetzt, sollten sie geregelt entsorgt werden. Vertiefende Informationen sind in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* zu finden.

**Notfallvorsorge**

Für die Notfallvorsorge müssen die einzelnen Notfallpläne der Anwendungen und IT-Systeme, die vom Patch- und Änderungsmanagement verwaltet werden, berücksichtigt werden (siehe B 1.3 *Notfallmanagement*). Da das Patch- und Änderungsmanagement zur technischen Umsetzung von Sicherheit in der Institution beiträgt, sollten geeignete technische Redundanz- und Ersatzsysteme bereitgestellt werden, um einem nicht kompensierbaren Ausfall entgegen zu wirken. Des Weiteren sind Vertreterregelungen von besonderer Bedeutung, um den Entscheidungs- und Freigabeprozess aufrecht zu erhalten.

**Planung und Konzeption**

- M 2.221 (A) *Änderungsmanagement*
- M 2.421 (B) *Planung des Patch- und Änderungsmanagementprozesses*
- M 2.422 (B) *Umgang mit Änderungsanforderungen*
- M 2.423 (A) *Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement*
- M 2.424 (A) *Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen*
- M 3.66 (W) *Grundbegriffe des Patch- und Änderungsmanagements*

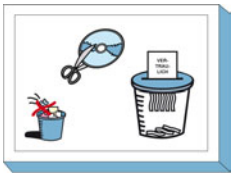
**Beschaffung**

- M 2.62 (B) *Software-Abnahme- und Freigabe-Verfahren*
- M 2.425 (C) *Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement*

**Umsetzung**
- M 4.65 (C) *Test neuer Hard- und Software*

**Betrieb**
- M 2.219 (A) *Kontinuierliche Dokumentation der Informationsverarbeitung*
- M 2.426 (C) *Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse*
- M 2.427 (C) *Abstimmung von Änderungsanforderungen*
- M 2.428 (Z) *Skalierbarkeit beim Patch- und Änderungsmanagement*
- M 2.429 (Z) *Erfolgsmessung von Änderungsanforderungen*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.177 (B) *Sicherstellung der Integrität und Authentizität von Softwarepaketen*
- M 4.323 (Z) *Synchronisierung innerhalb des Patch- und Änderungsmanagements*
- M 4.324 (C) *Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement*

# B 1.15 Löschen und Vernichten von Daten



## Beschreibung

Damit Informationen nicht in falsche Hände geraten, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger vollständig und zuverlässig zu löschen oder zu vernichten. Betrachtet werden müssen dabei sowohl schutzbedürftige Informationen, die auf Papier oder anderen analogen Datenträgern wie Mikrofilm (Video, Schmalfilm, Fotos, Schallplatten, Dokumente, Audiokassetten), als auch solche, die auf digitalen Datenträgern (elektronisch, magnetisch, optisch), wie beispielsweise DVD und CD gespeichert sind.

Wenn nicht oder nur unzureichend gelöschte Datenträger weitergegeben, verkauft oder ausgesondert werden, kann die unbeabsichtigte Weitergabe von Informationen erhebliche Schäden verursachen. Ein potentielles Risiko stellen vor allem kryptographische Schlüssel, Passwörter, vertrauliche Informationen und andere hochsensible Daten im Arbeitsspeicher oder in Auslagerungsdateien dar.

Daher muss jede Behörde und jedes Unternehmen eine Vorgehensweise zum sicheren Löschen haben. In diesem Baustein wird beschrieben, wie für eine Institution ein entsprechendes Konzept zum sicheren Löschen und Vernichten von Daten erstellt werden kann.

## Gefährdungslage

Für die zu schützenden und damit sicher zu löschenden Daten werden für den IT-Grundschutz folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.48 *Ungeeignete Entsorgung der Datenträger und Dokumente*
- G 2.54 *Vertraulichkeitsverlust durch Restinformationen*
- G 2.102 *Unzureichende Sensibilisierung für Informationssicherheit*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.31 *Unstrukturierte Datenhaltung*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.93 *Falscher Umgang mit defekten Datenträgern*

**Vorsätzliche Handlungen**

- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.146 *Vertraulichkeitsverlust durch Auslagerungsdateien*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für das sichere Löschen und Vernichten von Daten sind eine Reihe von Maßnahmen umzusetzen. Die dabei zu durchlaufenden Schritte, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Der Schwerpunkt der Aktivitäten befindet sich naturgemäß in der Lebenszyklusphase Aussonderung. Viele Datenträger werden jedoch auch während der anderen Phasen weitergegeben, so dass vorhandene Informationen, die nicht weitergegeben werden sollen, sicher gelöscht werden müssen.

**Planung und Konzeption**

Eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern verhindert den Missbrauch der gespeicherten Informationen (siehe M 2.431 *Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen*). Diese Vorgehensweise sollte allen Mitarbeitern in einer verständlichen Richtlinie vorliegen (siehe M 2.432 *Richtlinie für die Löschung und Vernichtung von Informationen*).

**Beschaffung**

Für die Beschaffung von Geräten zur Löschung oder Vernichtung von Daten müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und darauf basierend geeignete Produkte oder Dienstleistungen ausgewählt werden (siehe M 2.434 *Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten* und M 2.436 *Vernichtung von Datenträgern durch externe Dienstleister*).

**Umsetzung**

Alle Mitarbeiter sollten die festgelegten Vorgehensweisen zum Löschen von Informationen oder Vernichten von Datenträgern kennen (siehe M 3.67 *Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten*).

**Betrieb**

Alle Arten von Informationen sollten grundsätzlich nach klaren Strukturen verwaltet werden. Außerdem sollten sie nach Schutzbedarf kategorisiert werden. Dies erleichtert es, alle zu löschenden oder zu vernichtenden Informationen zu identifizieren und die Bereiche zu finden, wo diese verarbeitet und gespeichert wurden (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

**Aussonderung**

Bei der Außerbetriebnahme von Datenträgern und IT-Systemen sind verschiedene Maßnahmen zu ergreifen, damit weder wichtige Daten verloren gehen noch sensible Daten zurückbleiben. Entsprechende Sicherheitsempfehlungen finden sich in M 4.234 *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*. Zu den verschiedenen IT-Systemen finden sich Empfehlungen in den jeweiligen Bausteinen der IT-Grundschutz-Kataloge, wie beispielsweise in M 2.320 *Geregelte Außerbetriebnahme eines Servers* und M 2.323 *Geregelte Außerbetriebnahme eines Clients*.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Löschen und Vernichten von Daten" vorgestellt.

**Planung und Konzeption**

- M 2.3 (B) *Datenträgerverwaltung*
- M 2.431 (A) *Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen*
- M 2.432 (Z) *Richtlinie für die Löschung und Vernichtung von Informationen*
- M 2.433 (W) *Überblick über Methoden zur Löschung und Vernichtung von Daten*

**Beschaffung**

- M 2.434 (Z) *Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten*
- M 2.435 (Z) *Auswahl geeigneter Aktenvernichter*
- M 2.436 (Z) *Vernichtung von Datenträgern durch externe Dienstleister*

**Umsetzung**

- M 3.67 (C) *Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten*
- M 4.32 (B) *Physikalisches Löschen der Datenträger vor und nach Verwendung*
- M 4.64 (C) *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*
- M 4.325 (Z) *Löschen von Auslagerungsdateien*

**Betrieb**

- M 2.217 (B) *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*

**Aussonderung**

- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*
- M 2.167 (B) *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*
- M 4.234 (B) *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*

# B 1.16 Anforderungsmanagement


## Beschreibung

In jeder Institution gibt es aus den verschiedensten Richtungen gesetzliche, vertragliche, strukturelle und interne Richtlinien und Vorgaben, die beachtet werden müssen. Viele davon haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement. Die Anforderungen sind je nach Branche, Land und anderen Rahmenbedingungen unterschiedlich. Weiterhin unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen durch angemessene Überwachungsmaßnahmen sicherstellen (neudeutsch: Compliance).

Ziel des Anforderungsmanagements ist es, jederzeit den Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche der Institution zu haben und geeignete Maßnahmen zu identifizieren und umzusetzen, um Verstöße gegen diese Anforderungen zu vermeiden.

Diese Aufgabe wird typischerweise an einen Mitarbeiter übertragen. Die Rolle wird im Folgenden mit Anforderungsmanager bezeichnet. In einigen Unternehmen wird z. B. auch die Bezeichnung Compliance Manager benutzt. Sofern dies nicht durch andere Regelungen vorgeschrieben ist, müssen hierfür aber keine neuen Stellen geschaffen werden. Die Aufgabe kann beispielsweise vom Sicherheitsmanagement, der Revision, dem Controlling oder dem Justitiariat mit übernommen werden.

Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen, z. B. Sicherheitsmanagement, Datenschutzmanagement, Anforderungsmanagements, Controlling. Diese sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

In diesem Baustein werden ausgewählte Anforderungen betrachtet, die Auswirkungen auf die Gestaltung der Informationssicherheit in der Institution haben.

## Gefährdungslage

Stellvertretend für alle Gefährdungen im Umfeld des Anforderungsmanagements wird in diesem Baustein die folgende typische Gefährdung betrachtet:

### Organisatorische Mängel

- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*

### Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Anforderungsmanagements ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

### Planung und Konzeption

Es sollten Prozesse und Organisationsstrukturen etabliert sein, um den Überblick über die verschiedenen Anforderungen zu gewährleisten (siehe M 2.439 *Konzeption und Organisation des Anforderungsmanagements*). Neben den externen Regelungen, die die Institution betreffen, müssen auch die internen Richtlinien und Anforderungen definiert und transparent sein. Eine wichtige Grundlage, um alle geschäftsrelevanten Informationen, Geschäftsprozesse und Systeme angemessen abzusichern, ist die Einstufung von deren Schutzbedarf (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informatio-*

*nen, Anwendungen und Systemen*). In der Folge leiten sich daraus konkrete Sicherheitsvorgaben für diese Objekte ab.

**Umsetzung**

Die identifizierten Anforderungen werden durch die Managementprozesse der Institution, insbesondere auch durch den Sicherheitsprozess, umgesetzt. Mitarbeiter, aber auch Besucher und externe Dienstleister müssen auf ihre Sorgfaltspflichten im Umgang mit Informationen und IT-Systemen hingewiesen werden, bevor sie Zugang oder Zugriff darauf erhalten (siehe M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

**Betrieb**

Die Sicherheitsvorgaben, die die Institution zur Erfüllungen der Anforderungen erstellt hat, müssen dauerhaft eingehalten werden. Dies sollte regelmäßig überprüft werden (siehe M 2.199 *Aufrechterhaltung der Informationssicherheit*). Sowohl die eigenen Regelungen als auch die rechtlichen Rahmenbedingungen, denen eine Institution unterliegt, können sich ändern. Dies muss im Rahmen des Anforderungsmanagements berücksichtigt werden (siehe M 2.340 *Beachtung rechtlicher Rahmenbedingungen*).

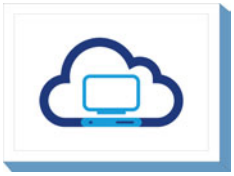
Nachfolgend wird das Maßnahmenbündel für den Bereich "Anforderungsmanagement" vorgestellt.

**Planung und Konzeption**
- M 2.163 (A) *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*
- M 2.205 (C) *Übertragung und Abruf personenbezogener Daten*
- M 2.439 (C) *Konzeption und Organisation des Anforderungsmanagements*

**Umsetzung**
- M 3.2 (A) *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*
- M 4.99 (C) *Schutz gegen nachträgliche Veränderungen von Informationen*

**Betrieb**
- M 2.199 (A) *Aufrechterhaltung der Informationssicherheit*
- M 2.217 (B) *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*
- M 2.340 (A) *Beachtung rechtlicher Rahmenbedingungen*
- M 2.380 (C) *Ausnahmegenehmigungen*
- M 3.26 (A) *Einweisung des Personals in den sicheren Umgang mit IT*

# B 1.17 Cloud-Nutzung



## Beschreibung

Mit Cloud Services nutzen Institutionen die Möglichkeit, IT-Infrastrukturen (zum Beispiel Rechenleistung, Speicherkapazitäten), IT-Plattformen (zum Beispiel Datenbanken, Applikations-Server) oder IT-Anwendungen (zum Beispiel Auftragssteuerung, Groupware) nach ihren spezifischen Bedürfnissen als Dienst über ein Netz zu beziehen. Dabei kann die Leistung sowohl in den Räumlichkeiten des Auftraggebers als auch bei einem externen Cloud-Diensteanbieter erbracht werden.

Die so ermöglichte bedarfsgerechte, skalierbare und flexible Nutzung von IT-Diensten wird unterstützt durch neuartige Geschäftsmodelle, bei denen die Abrechnung je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer erfolgen kann.

Nicht zuletzt aufgrund der genannten Eigenschaften erfreut sich Cloud Computing (zu Definitionen etc. siehe M 4.462 *Einführung in die Cloud-Nutzung*) bereits seit einigen Jahren wachsender Beliebtheit. Zahlreiche Studien belegen die steigende Nachfrage nach Cloud Services und prognostizieren diese auch für zukünftige Jahre.

In der Praxis zeigt sich jedoch häufig, dass die Vorteile, die sich Institutionen von der Cloud-Nutzung erwarten, oftmals nicht vollständig zum Tragen kommen, weil die diesbezüglich wichtigsten kritischen Erfolgsfaktoren nicht ausreichend betrachtet worden sind. Den nachfolgenden Aspekten kommt im Zusammenhang mit der Cloud-Nutzung durch Institutionen besondere Bedeutung zu:

- Strategische Planung des Einsatzes von Cloud-Diensten
- Sorgfältige Definition und Vereinbarung von (Sicherheits-)Anforderungen
- Sorgfältige Definition der Verantwortung und Schnittstellen, sowohl innerhalb einer Institution als auch nach außen
- Bewusstsein für ein erforderliches geändertes Rollenverständnis, sowohl aufseiten der IT als auch aufseiten der Anwender

Zusätzlich spielt im Zuge der Einführung von Cloud Services eine Reihe von Governance-Themen eine wichtige Rolle. Beispiele hierfür sind die Umsetzung von Mandantenfähigkeit, die Vertragsgestaltung, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutz-Aspekte.

### Thematische Abgrenzung

Im Sinne der IT-Grundschutz-Vorgehensweise umfasst Cloud-Nutzung alle Aspekte, die zur Nutzung einer Cloud-Umgebung erforderlich sind. Damit schließt Cloud-Nutzung insbesondere sowohl die Anwendung des Cloud Services durch Mitarbeiter der nutzenden Institution als auch die Administration des Cloud Services durch einen Cloud-Service-Administrator aufseiten der nutzenden Institution ein.

Ziel des vorliegenden Bausteins ist, Empfehlungen für die sichere Nutzung von Cloud-Diensten zu geben. Er richtet sich daher an alle Institutionen, die bereits Cloud Services in Anspruch nehmen oder deren zukünftigen Einsatz planen. Die Gefährdungen und Maßnahmen des Bausteins gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell.

Der Baustein ist so konzipiert, dass er immer auf einen konkreten Cloud Service anzuwenden ist. Nutzt eine Institution einen Verbund von Cloud Services, so ist jeder einzelne Service mithilfe des Bausteins zu modellieren (siehe M 2.545 *Modellierung der Cloud-Nutzung*). Die entstehende Schnittstelle zwischen den unterschiedlichen Services ist ebenfalls Gegenstand des Bausteins. Sie muss für alle Services betrachtet werden.

Der Baustein Cloud-Nutzung ist eng verwandt mit dem Baustein B 1.11 *Outsourcing*. In nahezu allen Bereitstellungsmodellen, abgesehen von der Nutzung einer Private Cloud On-Premise, stellt die Nutzung von Cloud Services eine Sonderform des Outsourcings dar. Die im Baustein Cloud-Nutzung beschriebenen Gefährdungen und Maßnahmen werden daher häufig auch im Outsourcing angewendet. Die Nutzung von Cloud Services ist jedoch durch eine Reihe von Besonderheiten gekennzeichnet, die sich in spezifischen Gefährdungen und dagegen wirkenden Maßnahmen ausschließlich in diesem Baustein wiederfinden.

Im Mittelpunkt des vorliegenden Bausteins stehen organisatorische und technische Maßnahmen, deren Umsetzung den identifizierten spezifischen Gefährdungen entgegenwirkt. Die beschriebenen Maßnahmen konzentrieren sich dabei vorwiegend auf Cloud-spezifische Aspekte. So wird es Institutionen durch Umsetzung der genannten Maßnahmen zusätzlich ermöglicht, die im Vorfeld beschriebenen kritischen Erfolgsfaktoren für die Cloud-Nutzung angemessen zu berücksichtigen.

Sicherheitsmaßnahmen, mit deren Hilfe die Erbringung der Cloud Services abgesichert wird, sind dagegen nicht Gegenstand des Bausteins, sondern sind im Baustein B 5.23 *Cloud Management* beschrieben. Gefährdungen und spezifische Sicherheitsmaßnahmen, die durch die Anbindung eines Cloud Services über entsprechende Schnittstellen (engl. API- Application Programming Interface) als relevant anzusehen sind, werden ebenfalls nicht im Baustein Cloud-Nutzung betrachtet. Hier sei auf den Baustein B 5.24 *Web-Services* verwiesen.

## Gefährdungslage

Für die Cloud-Nutzung werden für den IT-Grundschutz die folgenden typischen Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.10 *Ausfall eines Weitverkehrsnetzes*
- G 1.19 *Ausfall eines Dienstleisters oder Zulieferers*

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.84 *Unzulängliche vertragliche Regelungen mit einem externen Dienstleister*
- G 2.85 *Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens*
- G 2.86 *Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.93 *Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*
- G 2.188 *Unzureichende Vorgaben zum Lizenzmanagement bei Cloud-Nutzung*
- G 2.189 *Fehlende oder unzureichende Strategie für die Cloud-Nutzung*
- G 2.190 *Unzureichendes Administrationsmodell für die Cloud-Nutzung*
- G 2.191 *Unzureichendes Rollen- und Berechtigungskonzept*
- G 2.192 *Unzureichende Verfügbarkeit der erforderlichen personellen Ressourcen mit ausreichender Qualifikation*
- G 2.193 *Fehlende Anpassung der Institution an die Nutzung von Cloud Services*
- G 2.194 *Mangelhaftes Anforderungsmanagement bei Cloud-Nutzung*
- G 2.195 *Mangelnde Überwachung der Service-Erbringung*
- G 2.196 *Fehlende Kosten-Nutzen-Betrachtung der Cloud-Nutzung über den gesamten Lebenszyklus*
- G 2.197 *Unzureichende Einbindung von Cloud Services in die eigene IT*
- G 2.198 *Mangelnde Planung der Migration zu Cloud Services*
- G 2.199 *Unzureichende Auswahl des Cloud-Diensteanbieters*

**Menschliche Fehlhandlungen**

- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.122 *Fehlerhafte Nutzung eines Cloud Services*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.43 *Undokumentierte Funktionen*
- G 4.97 *Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister*
- G 4.98 *Ausfall von Tools zur Administration von Cloud Services bei Cloud-Nutzung*

**Vorsätzliche Handlungen**

- G 5.20 *Missbrauch von Administratorrechten*
- G 5.28 *Verhinderung von Diensten*
- G 5.190 *Missbrauch von Services*
- G 5.191 *Manipulation der Abrechnungsinformationen*

**Maßnahmenempfehlungen**

Um einen Informationsverbund abzusichern, müssen gemäß den Ergebnissen der Modellierung nach IT-Grundschutz zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden.

Alle Aspekte, die im Zuständigkeitsbereich des Cloud-Diensteanbieters liegen, sind durch den vorliegenden Baustein abgedeckt. Übernimmt die eigene IT die Rolle des Cloud-Diensteanbieters, beispielsweise in Verbindung mit dem Einsatz einer Private Cloud On-Premise, ist neben dem Baustein Cloud-Nutzung daher auch der Baustein Cloud Management anzuwenden.

Erfolgt die Administration des Cloud-Dienstes durch den Cloud-Service-Administrator aufseiten der nutzenden Institution über eine Management-Software, die Webservices verwendet, ist zusätzlich der Baustein B 5.24 *Web-Services* anzuwenden.

Weitere Hinweise zur Modellierung beim Einsatz von Cloud Services finden sich in der Maßnahme M 2.545 *Modellierung der Cloud-Nutzung*.

**Planung und Konzeption**

Die Entscheidung einer Institution zur Nutzung von Cloud Services ist strategischer Natur. Daher sollten relevante wirtschaftliche, technische und organisatorische Randbedingungen sowie sicherheitsrelevante Aspekte betrachtet werden und in die Erstellung einer Cloud-Nutzungs-Strategie einfließen. Die Maßnahme M 2.534 *Erstellung einer Cloud-Nutzungs-Strategie* bietet hierzu weitere Hilfestellung.

Nachdem die Cloud-Nutzungs-Strategie festgelegt worden ist, ergeben sich konkrete Sicherheitsvorgaben für die Umsetzung innerhalb der Institution. Diese sollten in ausreichend detaillierter Form in einer Sicherheitsrichtlinie für die Cloud-Nutzung (siehe hierzu Maßnahme M 2.535 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) dokumentiert werden.

Die ermittelten Anforderungen der Institution hinsichtlich Sicherheitsvorgaben, relevanten Schnittstellen und benötigten Service-Leveln sollten die Grundlage für die Service-Definition des zu verwendenden Cloud-Dienstes bilden. Nähere Angaben hierzu finden sich in der Maßnahme M 2.536 *Service-Definition für Cloud-Dienste durch den Anwender*.

Ist der zu nutzende Cloud-Dienst abschließend definiert, sind in der Folge umfangreiche Planungsmaßnahmen durchzuführen, um einen sicheren, fortlaufenden Betrieb von Cloud Services gewährleisten zu können. Ein besonderes Augenmerk sollte hierbei auf die Planung der sicheren Migration (siehe hierzu Maßnahme M 2.537 *Planung der sicheren Migration zu einem Cloud Service*) und die Planung der sicheren Einbindung von Cloud Services gerichtet werden (siehe Maßnahme M 2.538 *Planung der sicheren Einbindung von Cloud Services*). Diese Maßnahme konzentriert sich dabei auf unterschiedliche Aspekte, die über die Migrationsplanung hinaus betrachtet werden sollten.

Im Rahmen der geplanten sicheren Migration zu einem Cloud Service sollte die Institution ein Migrationskonzept erstellen, welches als Teil des Sicherheitskonzeptes für die Cloud-Nutzung auszulegen ist (siehe Maßnahme M 2.539 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*). Dabei sind verschiedene Cloud-spezifische Besonderheiten und Voraussetzungen zu beachten und entsprechend im Migrationskonzept darzustellen.

Sofern eine Institution besondere Anforderungen an einen Cloud Service hat, beispielsweise hinsichtlich der Vertraulichkeit der Informationen oder des problemlosen Zusammenspiels beim Einsatz mehrerer Services, sollten zusätzliche Sicherheitsmaßnahmen umgesetzt werden. Hier empfiehlt sich, die Vorgaben aus den Maßnahmen M 4.459 *Einsatz von Verschlüsselung bei Cloud-Nutzung* und M 4.461 *Portabilität von Cloud Services* umzusetzen.

Ebenfalls im Rahmen der Planungs- und Konzeptionsphase sind die Maßnahmen M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates* sowie M 2.42 *Festlegung der möglichen Kommunikationspartner* zu beachten und umzusetzen.

**Beschaffung**

Voraussetzung für die Auswahl eines geeigneten Cloud-Diensteanbieters ist ein möglichst detailliert erstelltes Anforderungsprofil. Die zuvor ermittelten Sicherheitsanforderungen sowie die erfolgte Definition der einzusetzenden Cloud Services liefern in Kombination mit einer durchgeführten Anforderungsanalyse die Basis für die Erstellung eines Lastenheftes. Dieses ist mit verfügbaren beziehungsweise angeforderten Angeboten von Cloud-Diensteanbietern abzugleichen. Nähere Angaben zu einer geeigneten Vorgehensweise bei der Auswahl eines Diensteanbieters finden sich in Maßnahme M 2.540 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*, in der auch mögliche Fallstricke vermerkt sind.

**Umsetzung**

Nach der Auswahl eines Cloud-Diensteanbieters sollten alle relevanten Aspekte des Cloud-Nutzungs-Vorhabens vertraglich festgehalten und geregelt werden. Der Vertrag sollte neben Aussagen zu IT-Sicherheitsanforderungen und Kriterien zur Messung von Servicequalität und Sicherheit auch Regelungen zu Auskunfts-, Mitwirkungs- und Revisionspflichten beinhalten. Alle wesentlichen Aspekte hierzu finden sich in Maßnahme M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*.

Im Rahmen der Umsetzungsphase erfolgt die Migration zu einem Cloud Service auf Basis eines Migrationskonzeptes, in dem Vorgaben zur geplanten Form der Migration (Testphase, Pilotphase etc.) sowie zu den technischen und organisatorischen Voraussetzungen für eine Migration festgeschrieben sind (siehe hierzu Maßnahme M 2.542 *Sichere Migration zu einem Cloud Service*).

**Betrieb**

Um die IT-Sicherheit im laufenden Cloud-Nutzungs-Betrieb aufrechtzuerhalten sind Dokumentationen und Richtlinien regelmäßig zu aktualisieren sowie regelmäßige Kontrollen, Abstimmungsrunden und die Planung und Durchführung von Übungen beziehungsweise Tests sicherzustellen. Weitere Informationen hierzu sind der Maßnahme M 2.543 *Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb* zu entnehmen.

Im Zusammenhang mit der Nutzung von Cloud Services wird die Durchführung von Audits als eine wichtige Maßnahme angesehen. Erfahrungen aus der Praxis haben gezeigt, dass die nutzende Institution Abweichungen zu vertraglichen Vereinbarungen, wie beispielsweise die Nicht-Einhaltung bestimmter Service-Level oder die Missachtung von Sicherheitsvorgaben häufig nur im Rahmen von Audits transparent machen kann. Die Maßnahme M 2.544 *Auditierung bei Cloud-Nutzung* liefert Hinweise zu relevanten Aspekten bei der Planung und Durchführung von Audits im Cloud-Umfeld.

**Aussonderung**

Damit ein Cloud-Nutzungs-Verhältnis geordnet beendet werden kann, müssen Eigentumsrechte an Hard- und Software sowie die Rückgabe der Datenbestände vom Dienstleister geklärt sein. Außerdem müssen alle erforderlichen Informationen für die Weiterführung des Betriebs von IT-Systemen und IT-Anwendungen ausreichend dokumentiert sein. Informationen hierzu sind in der Maßnahme M 2.307 *Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses* zusammengefasst.

**Notfallvorsorge**

Als wichtige Maßnahme zur Notfallvorsorge zählt die Erstellung eines IT-Notfallkonzeptes für die internen Prozesse bei Cloud-Nutzung (siehe hierzu Maßnahme M 6.155 *Erstellung eines Notfallkonzeptes*

*für einen Cloud Service*). In diesem sollten relevante organisatorische und technische Punkte thematisiert werden.

Stellt eine Institution fest, dass besondere Gegebenheiten eigens durchgeführte Datensicherungen erforderlich machen, sind in diesem Zusammenhang die Vorgaben der Maßnahme M 6.156 *Durchführung eigener Datensicherungen* umzusetzen.

Nachfolgend wird das Maßnahmenbündel für den Baustein Cloud-Nutzung vorgestellt.

**Planung und Konzeption**
- M 2.40 (A) *Rechtzeitige Beteiligung des Personal-/Betriebsrates*
- M 2.42 (A) *Festlegung der möglichen Kommunikationspartner*
- M 2.534 (A) *Erstellung einer Cloud-Nutzungs-Strategie*
- M 2.535 (A) *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*
- M 2.536 (A) *Service-Definition für Cloud-Dienste durch den Anwender*
- M 2.537 (A) *Planung der sicheren Migration zu einem Cloud Service*
- M 2.538 (A) *Planung der sicheren Einbindung von Cloud Services*
- M 2.539 (A) *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*
- M 2.545 (W) *Modellierung der Cloud-Nutzung*
- M 4.459 (Z) *Einsatz von Verschlüsselung bei Cloud-Nutzung*
- M 4.461 (Z) *Portabilität von Cloud Services*

**Beschaffung**
- M 2.540 (A) *Sorgfältige Auswahl eines Cloud-Diensteanbieters*

**Umsetzung**
- M 2.541 (A) *Vertragsgestaltung mit dem Cloud-Diensteanbieter*
- M 2.542 (A) *Sichere Migration zu einem Cloud Service*

**Betrieb**
- M 2.543 (A) *Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb*
- M 2.544 (C) *Auditierung bei Cloud-Nutzung*
- M 4.460 (Z) *Einsatz von Federation Services*
- M 4.462 (W) *Einführung in die Cloud-Nutzung*

**Aussonderung**
- M 2.307 (A) *Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses*

**Notfallvorsorge**
- M 6.155 (A) *Erstellung eines Notfallkonzeptes für einen Cloud Service*
- M 6.156 (Z) *Durchführung eigener Datensicherungen*

# B 1.18 Identitäts- und Berechtigungsmanagement

## Beschreibung

Ziel des Identitätsmanagements ist es, die Subjekte zweifelsfrei zu identifizieren, die auf Ressourcen einer Institution zugreifen, hier vor allem IT-Ressourcen. Zugreifende Subjekte können Personen oder auch IT-Komponenten oder kurz Benutzer sein. Mit Identitätsmanagement wird die Verwaltung der für die Identifikation, aber auch für die Authentisierung notwendigen Informationen bezeichnet.

Beim Berechtigungsmanagement geht es dann darum, ob und in welcher Granularität von diesen Subjekten Informationen oder Dienste genutzt werden können, ihnen also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern ist. Berechtigungsmanagement bezeichnet die Prozesse, die für die Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Die Übergänge zwischen beiden Begriffen sind fließend, daher wird im Folgenden der Begriff Identitäts- und Berechtigungsmanagement (englisch IAM - Identity and Access Management) benutzt. Durch ein Identitäts- und Berechtigungsmanagement wird gewährleistet, dass Benutzer ausschließlich auf die IT-Ressourcen und Informationen zugreifen dürfen, die sie für ihre Arbeit benötigen und für die sie autorisiert sind.

Ein Identitäts- und Berechtigungsmanagement muss folgende Anforderungen erfüllen:

- Aufbau und Umsetzung von Vorgehensweisen, um den Zugriff auf Informationen und den Zugang zu IT-Ressourcen steuern und kontrollieren zu können, vor allem den Umgang mit und die Verwaltung von Identitäten und Berechtigungen
- Registrierung von Benutzern, Zuweisung und Entzug von Rechten,
- Verwaltung von Benutzerkennungen und den dazugehörigen Berechtigungen,
- Kontrolle der Benutzerzugriffe.

Ein Identitäts- und Berechtigungsmanagement besteht sowohl aus organisatorischen sowie aus technischen Verfahren. Oftmals erfolgt das Identitäts- und Berechtigungsmanagement mit Bordmitteln und manuell. Diese Vorgehensweise führt zu hohen Administrationsaufwendungen sowie zu inkonsistenten und veralteten Benutzerdatenbeständen. Der Einsatz von IT-Anwendungen können bei der Durchführung unterstützen, sind aber nur ein Teil einer Lösung. Dieser Baustein zeigt auf, wie sichere Lösungen für einen strukturierten Umgang mit Benutzern und Berechtigungen aussehen sollten.

Berechtigungen dürfen nur eingeschränkt und aufgabenbezogen nach dem Prinzip der geringsten Berechtigungen eingerichtet werden. In den Räumlichkeiten und mittlerweile insbesondere den IT-Systemen einer Institution befindet sich ein großer Anteil des geistigen Eigentums dieser Institution. Die IT-Systeme unterstützen außerdem viele erfolgskritische Geschäftsprozesse eines Unternehmens bzw. einer Behörde. Durch ein Identitäts- und Berechtigungsmanagement wird sichergestellt, dass den Benutzern nur die notwendigen Berechtigungen zugeordnet werden. Eine dokumentierte Vorgehensweise der Zuweisung, Veränderung und dem Entzug von Berechtigungen ermöglicht es, Zutritt, Zugriff und Zugang zu Informationen steuern zu können, entsprechende Hintergrundsysteme ermöglichen es außerdem, die stattgefundenen Aktivitäten speichern und auswerten zu können. Im Schadensfall oder aufgrund rechtlicher Anforderungen können Aktivitäten ausgewertet und Benutzern zugeordnet werden.

## Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

### Organisatorische Mängel

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.214 *Fehlende oder unzureichende Konzeption des Identitäts- und Berechtigungsmanagements*

**Menschliche Fehlhandlungen**

- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.101 *Ausfall eines zentralen Identitäts- und Berechtigungsmanagement-Systems*

**Vorsätzliche Handlungen**

- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.24 *Wiedereinspielen von Nachrichten*
- G 5.42 *Social Engineering*
- G 5.104 *Ausspähen von Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Identitäts- und Berechtigungsmanagements sind unabhängig von der Art der eingesetzten IT-Komponenten eine Reihe von Maßnahmen umzusetzen. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Für Identitätsmanagementsysteme werden verschiedene Komponenten benötigt, dazu gehören Systeme zur Verwaltung von Personen- und Organisationsdaten (typischerweise Verzeichnisdienste, siehe hierzu den Baustein B 5.15 *Allgemeiner Verzeichnisdienst*) und Dienste für die Identifikation und Authentikation von Benutzern, z.B. über Verzeichnisdienste wie Novell Directory Services, Microsoft Active Directory oder RACF bei IBM Großrechnern.

**Planung und Konzeption**

In jeder Institution muss es eine geeignete Vorgehensweise für den Umgang mit Identitäten und Berechtigungen geben (siehe M 2.585 *Konzeption eines Identitäts- und Berechtigungsmanagements*). Zunächst sollten innerhalb der Institution die grundlegenden Rahmenbedingungen aus dem Sicherheitskonzept mit Bezug auf das Identitäts- und Berechtigungsmanagement definiert sein. Alle Vorgaben, z. B. Namenskonventionen und internen Abläufe, sollten in einer Richtlinie beschrieben werden (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*). Dazu gehören ebenfalls die Vorgaben zur Regelung des Passwortgebrauchs (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Wenn Mitarbeiter Aufgaben neu übernehmen, abgeben oder die Institution verlassen, müssen Berechtigungen angelegt, geändert oder gelöscht sowie ihre Benutzerkennungen deaktiviert werden (siehe M 2.586 *Einrichtung, Änderung und Entzug von Berechtigungen* Einrichtung, Änderung und Entzug von Berechtigungen).

Für weitergehende Managementanforderungen ist in der Wissensmaßnahme M 2.587 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* ein Beispiel für den Aufbau und die Organisation eines Identitäts- und Berechtigungsmanagements prozessual dargestellt.

**Beschaffung**

Bei der Beschaffung von Identitäts- und Berechtigungsmanagement-Systemen und Authentikationsmechanismen sollte bereits im Auswahlprozess der Schutzbedarf der zu verarbeitenden Informationen betrachtet werden. In M 4.499 *Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen* ist dies näher beschrieben.

**Umsetzung**

Der Zugang zu IT-Systemen sollte so geplant und umgesetzt werden, dass die Mitarbeiter nur auf die Informationen zugreifen können, die sie für ihre tägliche Arbeit benötigen. Zur Absicherung des Zugriffs sollten geeignete Authentikationsmechanismen verwendet werden (siehe M 4.1 *Passwortschutz für IT-Systeme*). Dabei sollten auch voreingestellte Passwörter unverzüglich geändert werden (siehe M 4.7 *Änderung voreingestellter Passwörter*).

Alle Mitarbeiter sollten im Umgang und dem Bewusstsein für sichere Passwörter regelmäßig geschult werden (siehe M 3.63 *Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten*).

**Betrieb**

Im Rahmen des Identitäts- und Berechtigungsmanagements werden Zutritt, Zugang und Zugriff für alle Mitarbeiter in die verschiedenen Bereiche einer Institution und auf alle Ressourcen geregelt (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*, M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*).

Alle Änderungen innerhalb des Identitäts- und Berechtigungsmanagement müssen schriftlich dokumentiert werden (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*)

**Notfallvorsorge**

Der Ausfall eines Identitäts- und Berechtigungsmanagement-Systems kann zur Folge haben, dass Benutzer sich nicht mehr anmelden können und Benutzerprofile nicht mehr geändert, angelegt und gelöscht werden können. Es ist zu untersuchen, inwieweit ein Ausfall des Identitäts- und Berechtigungsmanagement-Systems sicherheitskritische Auswirkungen auf die Geschäftsprozesse hat (siehe M 6.166 *Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Identitäts- und Berechtigungsmanagement" vorgestellt:

**Planung und Konzeption**

- M 2.5 (A) *Aufgabenverteilung und Funktionstrennung*
- M 2.11 (A) *Regelung des Passwortgebrauchs*
- M 2.30 (A) *Regelung für die Einrichtung von Benutzern / Benutzergruppen*
- M 2.220 (A) *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*
- M 2.585 (A) *Konzeption eines Identitäts- und Berechtigungsmanagements*
- M 2.586 (A) *Einrichtung, Änderung und Entzug von Berechtigungen*
- M 2.587 (W) *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement*
- M 4.133 (Z) *Geeignete Auswahl von Authentikationsmechanismen*
- M 4.250 (Z) *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*
- M 4.498 (Z) *Sicherer Einsatz von Single-Sign-On*
- M 5.34 (Z) *Einsatz von Einmalpasswörtern*

**Beschaffung**

- M 4.499 (Z) *Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen*

**Umsetzung**

- M 1.1 (A) *Einhaltung einschlägiger Normen und Vorschriften*
- M 2.555 (A) *Entwicklung eines Authentisierungskonzeptes für Anwendungen*
- M 4.1 (A) *Passwortschutz für IT-Systeme*
- M 4.7 (A) *Änderung voreingestellter Passwörter*

**Betrieb**

- M 2.6 (A) *Vergabe von Zutrittsberechtigungen*
- M 2.7 (A) *Vergabe von Zugangsberechtigungen*

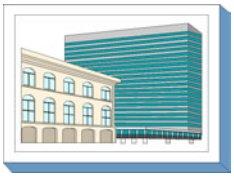
- M 2.8 (A) *Vergabe von Zugriffsrechten*
- M 2.22 (Z) *Hinterlegen des Passwortes*
- M 2.31 (A) *Dokumentation der zugelassenen Benutzer und Rechteprofile*
- M 2.65 (C) *Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System*
- M 2.402 (Z) *Zurücksetzen von Passwörtern*
- M 3.98 (C) *Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen*
- M 4.500 (C) *Sicherer Einsatz von Systemen für Identitäts- und Berechtigungsmanagement*

**Notfallvorsorge**

- M 6.166 (C) *Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System*

# B 2 Infrastruktur

# B 2.1 Allgemeines Gebäude



## Beschreibung

Gebäude bilden den äußeren Rahmen, um Geschäftsprozesse durchführen zu können. Ein Gebäude umgibt die stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik und gewährleistet für diese somit einen äußeren Schutz. Weiterhin ermöglichen die Infrastruktureinrichtungen eines Gebäudes häufig erst die Durchführung von Geschäftsprozessen und den IT-Betrieb. Daher ist einerseits das Bauwerk, also Wände, Decken, Böden, Dach, Fenster und Türen zu betrachten und andererseits alle gebäudeweiten Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung, Rohrpost etc.

Betrachtet wird ein Gebäude, das von einer oder mehreren Organisationseinheiten einer Institution genutzt wird. Diese können durchaus unterschiedliche Sicherheitsansprüche haben. Zudem muss in alle Überlegungen einfließen, dass ein Gebäude fast immer auch von Institutionsfremden (Bürgern, Kunden, Lieferanten) betreten werden kann und soll.

Wenn ein Gebäude von verschiedenen Parteien in unterschiedlicher Weise genutzt wird, so müssen Gestaltung und Ausstattung des Gebäudes und das Nutzungskonzept für das Gebäude zueinander passen. Es soll eine optimale Umgebung für die im Gebäude tätigen Menschen sichergestellt werden. Unberechtigte sollen dort keinen Zutritt erhalten, wo sie die Sicherheit beeinträchtigen könnten und die im Gebäude stationierte Technik soll sicher und effizient betrieben werden.

In diesem Baustein wird beschrieben, welche Maßnahmen eine Institution ergreifen sollte, um ein Gebäude aus Sicht der Informationssicherheit optimal zu nutzen. Auch wenn die Anforderungen an die Ausprägung der Maßnahmen von Art und Größe der Institution beeinflusst wird, können die Empfehlungen in diesem Baustein auch auf Betrachtungen von großen Liegenschaften mit mehreren Gebäuden oder auf die Nutzung einzelner Gebäudeteile in Mehrparteienhäusern übertragen werden.

## Gefährdungslage

Für den IT-Grundschutz eines Gebäudes werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.3 *Blitz*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.12 *Beeinträchtigung durch Großveranstaltungen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*

**Menschliche Fehlhandlungen**

- G 3.85 *Verletzung von Brandschottungen*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.2 *Ausfall interner Versorgungsnetze*
- G 4.3 *Ausfall vorhandener Sicherungseinrichtungen*
- G 4.88 *EMV-untaugliche Stromversorgung*

**Vorsätzliche Handlungen**

- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*

- G 5.6 *Anschlag*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Dieser Baustein betrachtet technische und nicht-technische Sicherheitsaspekte bei der Planung und Nutzung von typischen Gebäuden für Unternehmen und Behörden. Dabei wird der gesamte Lebenszyklus von Gebäuden betrachtet, beginnend von der Erstellung eines Anforderungskataloges, über Konzeption, Einrichtung, Nutzung bis hin zu Umbauten oder Auszug.

Die Verkabelung in einem Gebäude wird in den Bausteinen B 2.2 *Elektrotechnische Verkabelung* und B 2.12 *IT-Verkabelung* gesondert betrachtet, spezielle Räumlichkeiten wie Serverräume oder Archivräume in den jeweiligen Bausteinen der Schicht 2.

Bei der Nutzung von Gebäuden für den Geschäftsbetrieb von Behörden oder Unternehmen sind hinsichtlich der Informationssicherheit bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen. Bei einem Neubau können erforderliche Maßnahmen zu einem großen Teil schon in der Planungsphase durchgeführt werden.

Wenn es sich dagegen um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt, was eventuell mit Erweiterungs- bzw. Umbaumaßnahmen verbunden sein kann, sind die Möglichkeiten zur Realisierung einer adäquaten Informationssicherheit oft viel stärker eingeschränkt.

**Planung und Konzeption**

Die geplante Nutzung eines Gebäudes und der Schutzbedarf der dort betriebenen Geschäftsprozesse bestimmen, wie das Gebäude zu gestalten und unter Sicherheitsaspekten auszustatten ist. Beginnend bei einer Bewertung der Lage und Art des Grundstücks ist zu prüfen, ob das Gebäude dem vorgesehenen Zweck angemessen ist oder angemessen gestaltet werden kann.

Empfehlenswert bei der weiteren Planung oder Prüfung eines Bestandsgebäudes ist die Bildung eines Zonenmodells (siehe M 1.79 *Bildung von Sicherheitszonen*), anhand dessen dann eine am Schutzbedarf orientierte Planung der Nutzung des Gebäudes vorgenommen werden kann (siehe M 1.78 *Sicherheitskonzept für die Gebäudenutzung*). Daraus werden dann die Organisation von Zutrittsberechtigungen, beschrieben in der Maßnahme M 1.80 *Zutrittskontrollsystem und Berechtigungsmanagement*, die Ausführung von Türen und Fenstern und die weiteren Maßnahmen zur Sicherung und Überwachung abgeleitet.

Bei der Raumbelegungsplanung ist M 1.8 *Raumbelegung unter Berücksichtigung von Brandlasten* sowie, im Falle einer Nutzung eines bestehenden Gebäudes, M 1.13 *Anordnung schützenswerter Gebäudeteile* anzuwenden. Stets erforderlich ist auch, entsprechend der geplanten Raumnutzung, die zu erwartenden elektrischen Anschlusswerte zu bestimmen (siehe M 1.3 *Angepasste Aufteilung der Stromkreise*).

**Beschaffung**

Sowohl bei der Auswahl eines Standortes für einen Neubau, als auch bei der Bewertung einer Bestandsimmobilie sind die Maßnahmen M 1.16 *Geeignete Standortauswahl* und M 2.334 *Auswahl eines geeigneten Gebäudes* in Betracht zu ziehen.

**Bauphase und Vorbereitung für Nutzung**

Während der Bauphase sind alle in der Planungsphase als erforderlich bewerteten Schutzmaßnahmen umzusetzen. In der Bauphase sind in jedem Fall die Maßnahmen M 1.1 *Einhaltung einschlägiger Normen und Vorschriften* und M 1.6 *Einhaltung von Brandschutzvorschriften* anzuwenden. M 1.2 *Regelungen für Zutritt zu Verteilern* sowie M 2.14 *Schlüsselverwaltung* sind spätestens beim Einzug in ein Gebäude festzulegen. Ebenso ist eine Zutrittsregelung und ein Zutrittskontrollkonzept gemäß M 2.17 *Zutrittsregelung und -kontrolle* erforderlich.

**Gebäudenutzung**

Während der Gebäudenutzungsphase ist insbesondere die regelmäßige Anwendung von M 2.15 *Brandschutzbegehungen* vorzusehen, womit die Einhaltung der vorgegebenen Vorschriften zum Brandschutz überwacht wird. Durch die Anwendung und regelmäßige Überwachung der Maßnahme M 1.15 *Geschlossene Fenster und Türen* ist sicherzustellen, dass sich nur befugte Personen im Gebäude aufhalten und dass zumindest eine elementare Vorsorge gegen Einbrüche getroffen wird.

**Notfallvorsorge**

Um für den Notfall gerüstet zu sein, ist ein Alarmierungsplan zu erstellen, und in regelmäßigen Abständen sind auch Notfallübungen durchzuführen, da andernfalls zu erwarten ist, dass bei einem Notfall falsche Entscheidungen getroffen werden bzw. Unklarheit über die notwendigen Operationen herrscht (siehe M 6.17 *Alarmierungsplan und Brandschutzübungen*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Allgemeines Gebäude" vorgestellt:

**Planung und Konzeption**
- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.4 (B) *Blitzschutzeinrichtungen*
- M 1.7 (A) *Handfeuerlöscher*
- M 1.8 (A) *Raumbelegung unter Berücksichtigung von Brandlasten*
- M 1.10 (Z) *Sichere Türen und Fenster*
- M 1.11 (A) *Lagepläne der Versorgungsleitungen*
- M 1.12 (A) *Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile*
- M 1.14 (Z) *Selbsttätige Entwässerung*
- M 1.19 (Z) *Einbruchsschutz*
- M 1.50 (C) *Rauchschutz*
- M 1.74 (Z) *EMV-taugliche Stromversorgung*
- M 1.75 (A) *Branderkennung in Gebäuden*
- M 1.77 (Z) *Klimatisierung für Menschen*
- M 1.78 (C) *Sicherheitskonzept für die Gebäudenutzung*
- M 1.79 (Z) *Bildung von Sicherheitszonen*
- M 1.80 (Z) *Zutrittskontrollsystem und Berechtigungsmanagement*

**Beschaffung**
- M 1.16 (A) *Geeignete Standortauswahl*
- M 2.334 (Z) *Auswahl eines geeigneten Gebäudes*

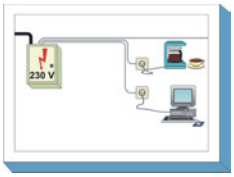
**Umsetzung**
- M 1.1 (A) *Einhaltung einschlägiger Normen und Vorschriften*
- M 1.2 (A) *Regelungen für Zutritt zu Verteilern*
- M 1.6 (A) *Einhaltung von Brandschutzvorschriften*
- M 1.17 (Z) *Pförtnerdienst*
- M 1.51 (A) *Brandlastreduzierung*
- M 2.17 (A) *Zutrittsregelung und -kontrolle*
- M 2.21 (A) *Rauchverbot*
- M 2.212 (B) *Organisatorische Vorgaben für die Gebäudereinigung*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*
- M 2.14 (A) *Schlüsselverwaltung*
- M 2.15 (B) *Brandschutzbegehungen*
- M 2.391 (B) *Frühzeitige Information des Brandschutzbeauftragten*

**Aussonderung**
- M 2.308 (Z) *Auszug aus Gebäuden*

**Notfallvorsorge**
- M 6.17 (A) *Alarmierungsplan und Brandschutzübungen*

# B 2.2 Elektrotechnische Verkabelung




## Beschreibung

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher.

Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb. Die IT-Verkabelung zur Kommunikation der IT-Systeme wird in einem separaten Baustein behandelt (siehe Baustein B 2.12 *IT-Verkabelung*). Da häufig gemeinsame Wege und Trassen für beide Arten der Verkabelung genutzt werden, sind die in beiden Bausteinen genannten Maßnahmen gemeinsam umzusetzen.

## Gefährdungslage

Für den IT-Grundschutz der elektrotechnischen Verkabelung werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.6 *Kabelbrand*

**Organisatorische Mängel**

- G 2.11 *Unzureichende Trassendimensionierung*
- G 2.12 *Unzureichende Dokumentation der Verkabelung*
- G 2.13 *Unzureichend geschützte Verteiler*

**Menschliche Fehlhandlungen**

- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*
- G 3.85 *Verletzung von Brandschottungen*

**Technisches Versagen**

- G 4.6 *Spannungsschwankungen/Überspannung/Unterspannung*
- G 4.62 *Verwendung unzureichender Steckdosenleisten*
- G 4.63 *Verstaubte Lüfter*

**Vorsätzliche Handlungen**

- G 5.8 *Manipulation von Leitungen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die elektrotechnische Verkabelung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Umsetzung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Wie beim Gebäude, so ist auch hier zu beachten, dass die Einflussmöglichkeiten beim Einzug in ein schon bestehendes Gebäude auch bei der Absicherung der Verkabelung wesentlich geringer sind als bei der Errichtung eines Neubaus.

**Planung und Konzeption**

In der Planungsphase werden die Grundlagen für eine leistungsfähige, gut abgesicherte Verkabelung gelegt.

Die mechanischen und elektrischen Eigenschaften der Verkabelung werden durch die Auswahl der einzusetzenden Kabeltypen und durch Kabelführung und -trassen und die Umgebungsbedingungen festge-

legt. Durch Auswahl geeigneter Kabeltypen und die typgerechte Verlegung muss die elektrotechnische Installation widerstandsfähig gegen Gefährdungen aus dem Umfeld gemacht werden. Bei der Planung sollte nach Möglichkeit auch darauf geachtet werden, dass Leitungen und Haupt- und Unterverteilungen des Gebäudes gegen Missbrauch in geeigneter Weise physisch abgesichert werden.

**Umsetzung**

Ein wesentliches Element des Brandschutzes ist die richtige Installation von Kabelkanälen, die durch eine fehlende Brandabschottung erhebliche Risiken verursachen können. Beim Einbau der Verkabelung ist auch auf eine ausführliche und korrekte Dokumentation zu achten, da es im nachhinein meist sehr schwierig oder sogar unmöglich ist, festzustellen, wo Kabel verlaufen und was sie verbinden.

**Betrieb**

Als Grundlage für einen sicheren und störungsfreien Betrieb müssen die Anlagen und ihre Nutzung regelmäßig geprüft werden (siehe M 2.394 *Prüfung elektrischer Anlagen*). Bei Arbeiten an Trassen ist sicherzustellen, dass der Brandschutzbeauftragte rechtzeitig in Planung und Ausführung mit einbezogen wird (siehe M 2.391 *Frühzeitige Information des Brandschutzbeauftragten*).

**Aussonderung**

Auch Elektrokabel, die nicht mehr benötigt werden, sind zu entfernen oder fachgerecht außer Betrieb zu nehmen (siehe M 5.1 *Entfernen oder Deaktivieren nicht benötigter Leitungen*).

**Notfallvorsorge**

Sofern erhöhte Anforderungen an die Verfügbarkeit gestellt werden, sollte die Verkabelung, gegebenenfalls einschließlich der externen Anschlüsse, redundant ausgelegt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "elektrotechnische Verkabelung" vorgestellt:

**Planung und Konzeption**
- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.5 (W) *Galvanische Trennung von Außenleitungen*
- M 1.20 (A) *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht*
- M 1.21 (A) *Ausreichende Trassendimensionierung*
- M 1.22 (Z) *Materielle Sicherung von Leitungen und Verteilern*
- M 1.25 (B) *Überspannungsschutz*

**Umsetzung**
- M 1.9 (A) *Brandabschottung von Trassen*
- M 1.64 (A) *Vermeidung elektrischer Zündquellen*
- M 2.19 (B) *Neutrale Dokumentation in den Verteilern*
- M 5.4 (A) *Dokumentation und Kennzeichnung der Verkabelung*
- M 5.5 (A) *Schadensmindernde Kabelführung*

**Betrieb**
- M 2.391 (B) *Frühzeitige Information des Brandschutzbeauftragten*
- M 2.394 (B) *Prüfung elektrischer Anlagen*

**Aussonderung**
- M 5.1 (A) *Entfernen oder Deaktivieren nicht benötigter Leitungen*

**Notfallvorsorge**
- M 6.18 (Z) *Redundante Leitungsführung*

# B 2.3 Büroraum / Lokaler Arbeitsplatz

## Beschreibung

Ein lokaler Arbeitsplatz ist der Bereich innerhalb der Institution, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort ihre Aufgaben zu erledigen. Dies kann beispielsweise ein Büroraum, eine Produktionsumgebung oder ein Verkaufsbereich sein.

Die Aufgaben können aus den verschiedensten Tätigkeiten bestehen, die auch teilweise oder ganz IT-unterstützt sein können: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Da sich ein lokaler Arbeitsplatz innerhalb der Institution befindet, können grundlegende infrastrukturelle Sicherheitsvorkehrungen wie Zugangskontrolle oder Brandschutz vorausgesetzt werden.

In diesem Baustein werden die typischen Gefährdungen und Maßnahmen für einen lokalen Arbeitsplatz beschrieben.

## Gefährdungslage

Für den IT-Grundschutz eines lokalen Arbeitsplatzes werden folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.14 *Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen*

**Menschliche Fehlhandlungen**

- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für lokale Arbeitsplätze sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung bis hin zu ihrer Nutzung. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Die Maßnahme M 1.76 *Geeignete Auswahl und Nutzung eines lokalen Arbeitsplatzes* beschreibt die grundlegenden Gestaltungsmöglichkeiten, die bei der Einrichtung eines Arbeitsplatzes beachtet werden sollten.

**Beschaffung**

Bei lokalen Arbeitsplätzen, bei denen die Benutzer den Zutritt nicht selber steuern können, also z. B. Bereiche mit Publikumsverkehr oder Großraumbüros, sollten Diebstahlsicherungen zum Schutz von Notebooks vorgesehen werden, da andernfalls die Gefahr relativ groß ist, dass solche Geräte in einem

unbewachten Augenblick "verschwinden". Ein hinreichend dreister Täter braucht nicht viel Zeit, um sich ein Notebook oder ein Smartphone zu verschaffen und den Raum damit zu verlassen.

**Umsetzung**

Auch für lokalen Arbeitsplätze sollte festgelegt werden, wer unter welchen Bedingungen Zutritt erhält. Insbesondere ist zu entscheiden, für welche Bereiche Publikumsverkehr vorgesehen wird und welche nur den Mitarbeitern des Unternehmens oder der Behörde offen stehen.

**Betrieb**

Die bearbeiteten Informationen müssen am lokalen Arbeitsplatz sorgfältig behandelt werden. Dazu gehören die Einhaltung der vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien.

Unter Beachtung der Zutrittsregelungen und des Zutrittsschutzes zum Gebäude ist auch festzulegen, ob Büros bei Abwesenheit der Mitarbeiter grundsätzlich zu verschließen sind. Je nach den baulichen Gegebenheiten muss auch dafür gesorgt werden, dass kein Zutritt über einen Balkon bzw. durch ein ungesichertes Fenster möglich ist.

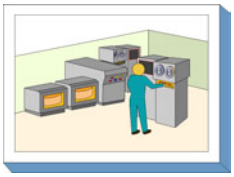
Nachfolgend wird das Maßnahmenbündel für den Bereich "Lokaler Arbeitsplatz" vorgestellt:

**Planung und Konzeption**
- M 1.76 (A) *Geeignete Auswahl und Nutzung eines lokalen Arbeitsplatzes*
- M 3.9 (Z) *Ergonomischer Arbeitsplatz*

**Umsetzung**
- M 2.17 (A) *Zutrittsregelung und -kontrolle*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*
- M 1.45 (A) *Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger*
- M 1.46 (Z) *Einsatz von Diebstahl-Sicherungen*
- M 2.37 (C) *Der aufgeräumte Arbeitsplatz*

# B 2.4 Serverraum



## Beschreibung

Der Serverraum dient in erster Linie zur Unterbringung von Servern, z. B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage. Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang oder weitere Hardware (Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein.

In einem Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum.

## Gefährdungslage

Für den IT-Grundschutz eines Serverraumes werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.16 *Ausfall von Patchfeldern durch Brand*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.2 *Ausfall interner Versorgungsnetze*
- G 4.6 *Spannungsschwankungen/Überspannung/Unterspannung*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Auswahl und Gestaltung eines Serverraums sind eine Reihe infrastruktureller und organisatorischer Maßnahmen umzusetzen, die in M 1.58 *Technische und organisatorische Vorgaben für Serverräume* beschrieben sind. Dabei sind bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen, je nachdem, ob ein Serverraum in einem neu zu errichtenden Gebäude eingerichtet werden soll oder ob es sich um eine Anmietung oder die Nutzung eines bestehenden Gebäudes

handelt. In diesem zweiten Fall sind die Möglichkeiten zur Realisierung einer adäquaten Informationssicherheit oft viel stärker eingeschränkt. Die Schritte, die bei der Gestaltung eines Serverraums durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Bei der Planung von Serverräumen ist durch eine Reihe von Maßnahmen zur Installation der Stromversorgung, einer eventuell notwendigen Klimatisierung und zum Brandschutz dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach Möglichkeit keine wasserführenden Leitungen in einem Serverraum vorhanden sein sollten, da Undichtigkeiten größere Schäden bis hin zum Ausfall des gesamten Informationsverbundes verursachen können. Bei erhöhten Verfügbarkeitsanforderungen sollten für Serverräume hinreichende Redundanzen in der technischen Infrastruktur geplant werden, um die Überbrückung einzelner Ausfälle zu ermöglichen.

**Umsetzung**

Nur diejenigen Personen, die zur Durchführung ihrer Aufgaben direkten Zugriff auf Server und sonstige im Serverraum installierte Geräte wie Kommunikationsverteiler, Firewalls etc. benötigen, sollten Zutritt zu einem Serverraum erhalten, und ein Rauchverbot sollte dort selbstverständlich sein.

**Betrieb**

Serverräume sollten grundsätzlich immer verschlossen sein, wenn sie nicht besetzt sind.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Serverraum" vorgestellt:

**Planung und Konzeption**
- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.7 (A) *Handfeuerlöscher*
- M 1.10 (Z) *Sichere Türen und Fenster*
- M 1.18 (Z) *Gefahrenmeldeanlage*
- M 1.24 (C) *Vermeidung von wasserführenden Leitungen*
- M 1.26 (Z) *Not-Aus-Schalter*
- M 1.27 (B) *Klimatisierung der Technik / in Technikräumen*
- M 1.28 (B) *Lokale unterbrechungsfreie Stromversorgung*
- M 1.31 (Z) *Fernanzeige von Störungen*
- M 1.52 (Z) *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur*
- M 1.58 (A) *Technische und organisatorische Vorgaben für Serverräume*
- M 1.62 (C) *Brandschutz von Patchfeldern*

**Umsetzung**
- M 2.17 (A) *Zutrittsregelung und -kontrolle*
- M 2.21 (A) *Rauchverbot*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*

# B 2.5 Datenträgerarchiv

## Beschreibung

Das Datenträgerarchiv dient der Lagerung von Datenträgern jeder Art. Im Rahmen des IT-Grundschutzes werden an den Archivraum hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Der Brandschutz kann entsprechend den Bedürfnissen des IT-Betreibers durch die Behältnisse, in denen die Datenträger aufbewahrt werden, realisiert werden.

Bei zentralen Datenträgerarchiven und Datensicherungsarchiven ist die Nutzung von Datensicherungsschränken (siehe Baustein B 2.7) empfehlenswert, um den Brandschutz, den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

Der Baustein B 2.5 *Datenträgerarchiv* eignet sich grundsätzlich auch für Papier-, Film- oder sonstige Akten, auch wenn er nicht primär auf diesen Anwendungsfall ausgerichtet ist. Einige Empfehlungen in den zugeordneten Maßnahmen müssen dann entsprechend uminterpretiert werden.

## Gefährdungslage

Für den IT-Grundschutz eines Datenträgerarchivs werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*

**Vorsätzliche Handlungen**

- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für das Datenträgerarchiv sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption bis zum täglichen Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Die Grundstruktur des Datenträgerarchivs und damit die wesentlichen Randbedingungen seiner Nutzung werden bei der Planung und Konzeption festgelegt. Hier bestehen naturgemäß bei der Einrichtung eines neuen Gebäudes größere Freiheiten. Wenn ein Datenträgerarchiv in einem schon existierenden Gebäude installiert werden soll, sind die verbleibenden Möglichkeiten der Strukturierung bei der Nutzung eines Gebäudes meist nur noch gering, vor allem bei angemieteten Gebäuden.

Mit der Auswahl des Raumes, in dem das Archiv untergebracht wird, stehen dessen Schutzeigenschaften schon zu einem großen Teil fest, und nachträgliche Korrekturen wie die Entfernung wasserführender Leitungen sind oft nur noch mit erheblichem Aufwand zu realisieren. Notwendige technische Installatio-

nen wie eine Klimatisierung oder der Einsatz einer Gefahrenmeldeanlage sollten daher nach Möglichkeit schon bei der Planung oder Auswahl des Datenträgerarchivs vorgesehen werden.

**Umsetzung**

Vor der Inbetriebnahme des Datenträgerarchivs sind organisatorische Regelungen festzulegen, die einen geordneten und sicheren Betrieb unterstützen.

**Betrieb**

Im laufenden Betrieb ist durch entsprechende Kontrolle zu gewährleisten, dass die vorgesehenen Regelungen in der Praxis tatsächlich angewendet werden. Hierzu gehört vor allem, dass gewährleistet wird, dass nur die Personen Zutritt haben, die dazu berechtigt sind, und dass das Archiv abgeschlossen ist, solange sich dort niemand aufhält.

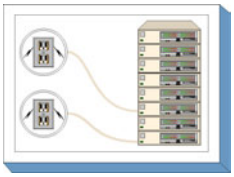
Nachfolgend wird das Maßnahmenbündel für den Bereich "Datenträgerarchiv" vorgestellt:

**Planung und Konzeption**
- M 1.7 (A) *Handfeuerlöscher*
- M 1.10 (Z) *Sichere Türen und Fenster*
- M 1.18 (Z) *Gefahrenmeldeanlage*
- M 1.24 (C) *Vermeidung von wasserführenden Leitungen*
- M 1.27 (B) *Klimatisierung der Technik / in Technikräumen*

**Umsetzung**
- M 2.17 (A) *Zutrittsregelung und -kontrolle*
- M 2.21 (A) *Rauchverbot*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*

# B 2.6 Raum für technische Infrastruktur



## Beschreibung

In Räumen für technische Infrastruktur sind in der Regel solche Geräte und Einrichtungen untergebracht, die keine oder nur eine seltene Bedienung durch einen Menschen benötigen. In der Regel wird es sich um Verteiler interner Versorgungsnetze handeln (z. B. Postkabeleingangsraum, Hochspannungsübergaberaum, Mittelspannungsübergaberaum, Niederspannungshauptverteiler). Eventuell werden in diesen Räumen auch die Sicherungen der Elektroversorgung untergebracht. Auch die Aufstellung sonstiger Geräte (USV, Sternkoppler, etc.) ist vorstellbar. Selbst ein Netzserver kann, wenn er keinen eigenen Raum hat (Baustein B 2.4 *Serverraum*), hier untergebracht sein.

## Gefährdungslage

Für den IT-Grundschutz eines Raums für technische Infrastruktur werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.2 *Ausfall interner Versorgungsnetze*
- G 4.6 *Spannungsschwankungen/Überspannung/Unterspannung*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Infrastrukturräume sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung bis hin zum laufenden Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Bei der Planung von Infrastrukturräumen ist durch eine Reihe von Maßnahmen zur Installation der Stromversorgung, einer eventuell notwendigen Klimatisierung und zum Brandschutz dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach

Möglichkeit keine wasserführenden Leitungen in einem solchen, meist unbesetzten, Raum vorhanden sein sollten, da Undichtigkeiten größere Schäden bis hin zum Ausfall des gesamten Informationsverbundes verursachen können. Bei erhöhten Sicherheitsanforderungen sollten Infrastrukturräume darüber hinaus durch besonders gesicherte Türen und Fenster auch gegen gewaltsames Eindringen geschützt werden, da sie oft bevorzugte Angriffsziele darstellen.

**Umsetzung**

Nur diejenigen Personen, die mit den entsprechenden technischen Wartungsaufgaben betraut sind, sollten Zutritt zu einem Infrastrukturraum erhalten, und ein Rauchverbot sollte dort selbstverständlich sein.

**Betrieb**

Räume für die technische Infrastruktur sollten grundsätzlich immer verschlossen sein, wenn die dort aufgestellten Geräte nicht so in Schränken verschlossen sind, dass keine unbefugte Nutzung möglich ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Raum für technische Infrastruktur" vorgestellt:

**Planung und Konzeption**
- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.7 (A) *Handfeuerlöscher*
- M 1.10 (Z) *Sichere Türen und Fenster*
- M 1.18 (Z) *Gefahrenmeldeanlage*
- M 1.24 (C) *Vermeidung von wasserführenden Leitungen*
- M 1.26 (Z) *Not-Aus-Schalter*
- M 1.27 (B) *Klimatisierung der Technik / in Technikräumen*
- M 1.31 (Z) *Fernanzeige von Störungen*

**Umsetzung**
- M 2.17 (A) *Zutrittsregelung und -kontrolle*
- M 2.21 (A) *Rauchverbot*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*

# B 2.7 Schutzschränke

## Beschreibung

Schutzschränke dienen zur Aufbewahrung von Datenträgern jeder Art oder zur Unterbringung von informationstechnischen Geräten ("Serverschrank"). Diese Schutzschränke sollen den Inhalt gegen unbefugten Zugriff und/oder gegen die Einwirkung von Feuer oder schädigenden Stoffen (z. B. Staub) schützen. Sie können als Ersatz für einen Serverraum oder ein Datenträgerarchiv (siehe Bausteine B 2.4 und B 2.5) eingesetzt werden, wenn die vorhandenen räumlichen oder organisatorischen Gegebenheiten eigene Räume nicht zulassen. Sollen ausschließlich Datenträger und inaktive IT-Geräte aufbewahrt werden, ist hierfür ein entsprechend geeigneter Datensicherungsschrank auf Grundlage der Normen EN 1047-1 und EN 1047-2 vorzuziehen.

Darüber hinaus können Schutzschränke auch in Serverräumen oder Datenträgerarchiven eingesetzt werden, um die Schutzwirkung der Räume zu erhöhen. Sie sind auch zu empfehlen, wenn in einem Serverraum Server aus unterschiedlichen Organisationsbereichen aufgestellt sind, die dem jeweils anderen Administrator nicht zugänglich sein sollen.

Um mit einem Schutzschrank einen mit den dedizierten Räumen vergleichbaren Schutz zu erreichen, sind eine Reihe von Maßnahmen, beginnend mit der geeigneten Auswahl bis zur Aufstellung und Nutzungsregelung, notwendig. Diese werden im vorliegenden Baustein vorgestellt.

## Gefährdungslage

Für den IT-Grundschutz von Schutzschränken werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*

**Menschliche Fehlhandlungen**

- G 3.21 *Fehlbedienung von Codeschlössern*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.2 *Ausfall interner Versorgungsnetze*
- G 4.3 *Ausfall vorhandener Sicherungseinrichtungen*
- G 4.4 *Leitungsbeeinträchtigung durch Umfeldfaktoren*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*
- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.53 *Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Auswahl und Einsatz von Schutzschränken sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zu ihrer Nutzung. Die Schritte, die

dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Vor der Beschaffung eines Schutzschranks sollte zunächst ein Konzept erstellt werden, das auf den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.311 *Planung von Schutzschränken*).

**Beschaffung**

Die Maßnahme M 2.95 *Beschaffung geeigneter Schutzschränke* nennt die wesentlichen Kriterien, die bei der Auswahl eines Schutzschranks zu beachten sind.

**Umsetzung**

Nur diejenigen Personen, die mit den entsprechenden technischen Wartungsaufgaben betraut sind, sollten Zutritt zum Schutzschrank erhalten, und sie sollten eine entsprechende Einweisung in die Bedienung des Schutzschranks erhalten. Ein Rauchverbot sollte für den Schutzschrankraum selbstverständlich sein. Hinweise für die Aufstellung eines Schutzschranks gibt die Maßnahme M 1.40 *Geeignete Aufstellung von Schutzschränken*.

**Betrieb**

Schutzschrankräume sollten grundsätzlich immer verschlossen sein, wenn die Schränke selbst nicht so ausgelegt sind, dass sie auch in ungeschützten Umgebungen aufgestellt werden können. Es ist darauf zu achten, dass die Schutzschränke immer korrekt verschlossen sind. Insbesondere bei Verwendung von Zahlenschlössern ist auf deren korrekte Bedienung zu achten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Schutzschränke" vorgestellt.

**Planung und Konzeption**
- M 1.7 (A) *Handfeuerlöscher*
- M 1.18 (Z) *Gefahrenmeldeanlage*
- M 1.24 (C) *Vermeidung von wasserführenden Leitungen*
- M 1.27 (B) *Klimatisierung der Technik / in Technikräumen*
- M 1.28 (B) *Lokale unterbrechungsfreie Stromversorgung*
- M 1.31 (Z) *Fernanzeige von Störungen*
- M 1.41 (Z) *Schutz gegen elektromagnetische Einstrahlung*
- M 2.311 (A) *Planung von Schutzschränken*

**Beschaffung**
- M 2.95 (C) *Beschaffung geeigneter Schutzschränke*

**Umsetzung**
- M 1.40 (A) *Geeignete Aufstellung von Schutzschränken*
- M 2.17 (A) *Zutrittsregelung und -kontrolle*
- M 2.21 (A) *Rauchverbot*
- M 3.20 (A) *Einweisung in die Bedienung von Schutzschränken*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 2.96 (A) *Verschluss von Schutzschränken*
- M 2.97 (A) *Korrekter Umgang mit Codeschlössern*

# B 2.8 Häuslicher Arbeitsplatz

## Beschreibung

Telearbeiter, freie Mitarbeiter oder Selbständige arbeiten typischerweise von häuslichen Arbeitsplätzen aus. Im Gegensatz zum Arbeitsplatz in einer Büroumgebung nutzt bei einem häuslichen Arbeitsplatz ein Mitarbeiter einen Arbeitsplatz im eigenen Wohnumfeld. Dabei muss eine hinreichende Trennung von beruflicher und privater Sphäre ermöglicht werden können. Arbeitsplätze in Wohnungen von Mitarbeitern, die dauerhaft genutzt werden, müssen zudem diverse rechtliche Anforderungen erfüllen, beispielsweise müssen sie arbeitsmedizinischen und ergonomischen Bestimmungen entsprechen.

Da bei einem häuslichen Arbeitsplatz nicht die infrastrukturelle Sicherheit, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist, vorausgesetzt werden kann und auch Besucher oder Familienangehörige Zutritt zu diesem Arbeitsplatz haben, müssen Sicherheitsmaßnahmen ergriffen werden, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen. In diesem Baustein werden die typischen Gefährdungen und Maßnahmen für einen häuslichen Arbeitsplatz beschrieben.

## Gefährdungslage

Für den IT-Grundschutz eines häuslichen Arbeitsplatzes werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.5 *Wasser*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.14 *Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen*
- G 2.47 *Ungesicherter Akten- und Datenträgertransport*
- G 2.48 *Ungeeignete Entsorgung der Datenträger und Dokumente*

**Menschliche Fehlhandlungen**

- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.69 *Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz*
- G 5.70 *Manipulation durch Familienangehörige und Besucher*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den häuslichen Arbeitsplatz ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Nutzung bis zur Entsorgung sensibler Datenträger und Ausdrucke. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Die Maßnahme M 1.44 *Geeignete Einrichtung eines häuslichen Arbeitsplatzes* nennt die grundlegenden Gestaltungsmöglichkeiten, die bei der Einrichtung eines Arbeitsplatzes in häuslicher Umgebung beachtet werden sollten.

**Umsetzung**

Für die kontrollierte Nutzung eines häuslichen Arbeitsplatzes ist zu regeln, welche Informationen am häuslichen Arbeitsplatz bearbeitet, zwischen dem Unternehmen bzw. der Behörde und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind.

**Betrieb**

Auch bei der Nutzung eines häuslichen Arbeitsplatzes ist die übliche Arbeitsdisziplin zu wahren. Dazu gehören Ordnung am Arbeitsplatz, die Einhaltung der vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien. Der häusliche Arbeitsplatz sollte auch so abgeschlossen werden, dass er keinem unzumutbaren Einbruchsrisiko ausgesetzt ist.

**Aussonderung**

Gerade am häuslichen Arbeitsplatz ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Hausmüll zu werfen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Häuslicher Arbeitsplatz" vorgestellt.

**Planung und Konzeption**
- M 1.19 (Z) *Einbruchsschutz*
- M 1.44 (A) *Geeignete Einrichtung eines häuslichen Arbeitsplatzes*
- M 3.9 (Z) *Ergonomischer Arbeitsplatz*

**Umsetzung**
- M 2.112 (A) *Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*
- M 2.37 (C) *Der aufgeräumte Arbeitsplatz*

**Aussonderung**
- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*

# B 2.9 Rechenzentrum

## Beschreibung

In den meisten Institutionen werden alle wesentlichen strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind sogar ohne IT nicht auszuführen. Die IT-Systeme der Institution selbst und auch deren Anbindung an externe Netze müssen in einer angemessenen Umgebung und Infrastruktur betrieben werden. Nur so lässt sich die nötige Verfügbarkeit der IT sicherstellen. Die Anforderungen an die Leistungsfähigkeit dieser Systeme und der Netzumgebung steigen stetig an. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, haben Behörden und Unternehmen jeglicher Größe ihre IT-Landschaft in Rechenzentren konzentriert.

Als Rechenzentrum werden die für den Betrieb von komplexen IT-Infrastrukturen (Server- und Speichersysteme, Systeme zur Datensicherung, aktive Netzkomponenten und TK-Systeme, zentrale Drucksysteme usw.) erforderlichen Einrichtungen (Klimatechnik, Elektroversorgung, überwachende und alarmierende Technik) und Räumlichkeiten (z. B. Rechnersaal, Räume für die aktiven Netzkomponenten, Technikräume, Archiv, Lager, Aufenthaltsraum usw.) bezeichnet. Die Abgrenzung vom Rechenzentrum zum Serverraum besteht vor allem darin, dass in einem Rechenzentrum eine räumliche Trennung der IT-Systeme und der unterstützenden Infrastruktur (Elektroversorgung, Klimatechnik usw.) obligatorisch ist. Ein Rechenzentrum sollte insgesamt einen Sicherheitsbereich bilden, der in sich noch mindestens in die organisatorisch und physisch getrennten Sicherheitsbereich "Infrastruktur" und "IT" aufgeteilt wird. Ein Rechenzentrum ist entweder ständig personell besetzt (Schichtdienst) oder es existiert in bedienerlosen Zeiten eine Rufbereitschaft (mit oder ohne Fernadministrationsmöglichkeit). In einem Rechenzentrum kann aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten als bei dezentraler Datenverarbeitung. In jedem Fall ist beim Einsatz einer Großrechenanlage der Baustein Rechenzentrum anzuwenden.

Gegenstand dieses Bausteins ist ein Rechenzentrum mittlerer Art und Güte. Die Sicherheitsanforderungen liegen zwischen denen eines Serverraums oder "Serverparks" und denen von Hochsicherheitsrechenzentren, wie sie beispielsweise im Bankenbereich eingesetzt werden. Neben den hier aufgeführten Standard-Sicherheitsmaßnahmen, die sich in der Praxis bewährt haben, sind in den meisten Fällen jedoch weitere, individuelle Sicherheitsmaßnahmen erforderlich, die die konkreten Anforderungen und das jeweilige Umfeld berücksichtigen (hierzu kann beispielsweise die Risikoanalyse basierend auf IT-Grundschutz verwendet werden). Gefährdungen aus den Bereichen Terrorismus oder höhere Gewalt wird durch die hier beschriebenen Standard-Sicherheitsmaßnahmen nur begrenzt Rechnung getragen.

Der Baustein richtet sich einerseits an Anwender, die ein Rechenzentrum betreiben und im Rahmen einer Revision prüfen möchten, ob sie geeignete Standard-Sicherheitsmaßnahmen umgesetzt haben. Auf der anderen Seite kann der Baustein Rechenzentrum auch dazu verwendet werden, überblicksartig die Sicherheitsmaßnahmen abzuschätzen, die bei einer Zentralisierung der IT in einem mittleren Rechenzentrum für einen sicheren Betrieb umgesetzt werden müssen. Um den Baustein überschaubar zu halten, wurde bewusst auf technische Details und planerische Größen verzichtet. Der Neubau eines Rechenzentrums sollte auch von großen IT-Abteilungen nicht ohne Hilfe eines erfahrenen Planungsstabes bzw. einer versierten Planungs- und Beratungsfirma in Betracht gezogen werden. Beim Outsourcing von Rechenzentrumsleistungen kann dieser Baustein dazu benutzt werden, die angebotenen Leistungen im Hinblick auf deren Sicherheitsniveau zu prüfen.

Im Gegensatz zum Schutzbedarf eines Serverraums (siehe dort) sind viele Sicherheitsmaßnahmen für ein Rechenzentrum nicht optional, sondern obligatorisch. Dazu gehören beispielsweise eine angemessene Gefahrenmeldeanlage und eine alternative Stromversorgung. Üblich und bewährt für einen sicheren IT-Betrieb ist eine Brandfrühesterkennung in Raum und Doppelboden von Rechnersaal und Technikräumen und gegebenenfalls auch eine automatische Löschanlage.

## Gefährdungslage

Für den IT-Grundschutz eines Rechenzentrums werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.3 *Blitz*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.6 *Kabelbrand*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.8 *Staub, Verschmutzung*
- G 1.11 *Technische Katastrophen im Umfeld*
- G 1.12 *Beeinträchtigung durch Großveranstaltungen*
- G 1.13 *Sturm*
- G 1.16 *Ausfall von Patchfeldern durch Brand*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.11 *Unzureichende Trassendimensionierung*
- G 2.12 *Unzureichende Dokumentation der Verkabelung*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.2 *Ausfall interner Versorgungsnetze*
- G 4.3 *Ausfall vorhandener Sicherungseinrichtungen*

**Vorsätzliche Handlungen**

- G 5.3 *Unbefugtes Eindringen in ein Gebäude*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*
- G 5.6 *Anschlag*
- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.68 *Unberechtigter Zugang zu den aktiven Netzkomponenten*
- G 5.102 *Sabotage*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Auswahl und Gestaltung eines Rechenzentrums sind eine Reihe infrastruktureller und organisatorischer Maßnahmen umzusetzen, die in M 1.49 *Technische und organisatorische Vorgaben für das Rechenzentrum* beschrieben sind. Dabei sind bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen, je nachdem, ob ein Rechenzentrum in einem neu zu errichtenden Gebäude eingerichtet werden soll oder ob es sich um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt. In diesem zweiten Fall sind die Möglichkeiten zur Realisierung einer adäquaten Informationssicherheit oft viel stärker eingeschränkt. Die Schritte, die bei der Gestaltung eines Rechenzentrums durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Grundprinzip bei der Planung eines Rechenzentrums ist die Trennung von "grober" und "feiner" Technik. Es müssen separate Räume für die IT-Systeme einerseits und die unterstützende Technik andererseits (Stromverteilungen, USV-Anlagen, Anlagen der Klimatechnik usw.) realisiert werden. Darauf aufbauend ist durch eine Reihe von Maßnahmen zur Installation der Stromversorgung und Klimatisierung und zum

Brand- und Rauchschutz dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach Möglichkeit keine wasserführenden Leitungen in einem Rechenzentrum vorhanden sein sollten, da Undichtigkeiten größere Schäden bis hin zum Ausfall des gesamten Informationsverbundes verursachen können. Zum physischen Schutz gehört dabei auch, dass sich ein Rechenzentrum im Gebäude möglichst in einem eigenen Brandabschnitt befinden sollte. Es sollte nicht von außen erkennbar sein.

In der Regel sollten auch hinreichende Redundanzen in der technischen Infrastruktur sowie eine Sekundär-Energieversorgung geplant werden, um die Überbrückung einzelner Ausfälle zu ermöglichen. Durch Installation von Überwachungsmaßnahmen, Fernanzeige von Störungen und einer geeigneten Löschtechnik ist Vorsorge zu treffen, dass eventuelle Schäden möglichst frühzeitig erkannt und geeignete Maßnahmen so schnell eingeleitet werden können, dass die Schadensausbreitung so gering wie möglich ist.

**Umsetzung**

Nur diejenigen Personen, die zur Durchführung ihrer Aufgaben direkten Zugriff auf Server und sonstige im Rechenzentrum installierte Geräte wie Kommunikationsverteiler, Firewalls etc. benötigen, sollten Zutritt zu IT-Räumen erhalten. Der Zutritt zu allen Räumen im Sicherheitsbereich, z. B. zur Wartung technischer Anlagen oder auch zur Reinigung der Räume, ist detailliert so zu regeln, dass nur vertrauenswürdiges Personal, und auch dieses möglichst nur unter Überwachung, Zutritt erhält. Ein Rauchverbot sollte dort ebenso selbstverständlich sein wie die Verfügbarkeit aktueller Infrastruktur- und Baupläne. Größere Mengen von Druckerpapier sind außerhalb des Rechenzentrums, in einem anderen Brandabschnitt, zu lagern, um die Brandlast zu reduzieren.

**Betrieb**

Rechenzentren sollten grundsätzlich immer verschlossen sein, wenn sie nicht besetzt sind. Personen die zum Beispiel für Wartungsarbeiten Zutritt zur technischen Infrastruktur benötigen, sollten im Sicherheitsbereich begleitet werden. Es ist sicherzustellen und regelmäßig zu prüfen, dass Meldungen der überwachenden und alarmierenden Technik so geleitet werden, dass eine angemessen schnelle Reaktion erfolgen kann.

**Notfallvorsorge**

Da Sicherheitsmaßnahmen, die nicht geübt werden, im Notfall nicht korrekt funktionieren, sind regelmäßige Brandschutzübungen erforderlich, zumal diese auch helfen, die Aktualität des Alarmierungsplans sicherzustellen. Um nach einem größeren Schaden schnell wieder Zugriff auf lebenswichtige Daten zu erhalten, sollten diese regelmäßig in einem separaten Notfallarchiv gesichert werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Rechenzentrum" vorgestellt:

**Planung und Konzeption**

- M 1.3 (A) *Angepasste Aufteilung der Stromkreise*
- M 1.7 (A) *Handfeuerlöscher*
- M 1.10 (Z) *Sichere Türen und Fenster*
- M 1.12 (A) *Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile*
- M 1.13 (Z) *Anordnung schützenswerter Gebäudeteile*
- M 1.18 (Z) *Gefahrenmeldeanlage*
- M 1.24 (C) *Vermeidung von wasserführenden Leitungen*
- M 1.25 (B) *Überspannungsschutz*
- M 1.26 (Z) *Not-Aus-Schalter*
- M 1.27 (B) *Klimatisierung der Technik / in Technikräumen*
- M 1.31 (Z) *Fernanzeige von Störungen*
- M 1.47 (B) *Eigener Brandabschnitt*
- M 1.48 (B) *Brandmeldeanlage im Rechenzentrum*
- M 1.49 (A) *Technische und organisatorische Vorgaben für das Rechenzentrum*
- M 1.50 (C) *Rauchschutz*
- M 1.52 (Z) *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur*

- M 1.53 (Z) *Videoüberwachung*
- M 1.54 (Z) *Brandfrühesterkennung / Löschtechnik*
- M 1.55 (Z) *Perimeterschutz*
- M 1.56 (A) *Netzersatzanlage*
- M 1.62 (C) *Brandschutz von Patchfeldern*
- M 1.70 (A) *Zentrale unterbrechungsfreie Stromversorgung*

**Umsetzung**

- M 1.57 (A) *Aktuelle Infrastruktur- und Baupläne*
- M 2.21 (A) *Rauchverbot*
- M 2.212 (B) *Organisatorische Vorgaben für die Gebäudereinigung*
- M 2.213 (A) *Inspektion und Wartung der technischen Infrastruktur*

**Betrieb**

- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*
- M 1.71 (C) *Funktionstests der technischen Infrastruktur*
- M 1.72 (Z) *Baumaßnahmen während des laufenden Betriebs*
- M 1.73 (A) *Schutz eines Rechenzentrums gegen unbefugten Zutritt*

**Notfallvorsorge**

- M 6.17 (A) *Alarmierungsplan und Brandschutzübungen*
- M 6.74 (Z) *Notfallarchiv*

# B 2.10 Mobiler Arbeitsplatz


## Beschreibung

IT-Benutzer werden immer mobiler und können, dank immer kleinerer und leistungsfähigerer Geräte, nahezu überall arbeiten. Daher werden dienstliche Aufgaben häufig nicht mehr nur in Räumen des Unternehmens bzw. der Behörde wahrgenommen, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, beispielsweise im Hotelzimmer, in der Eisenbahn oder beim Kunden.

In solchen Umgebungen kann aber nicht die infrastrukturelle Sicherheit, wie sie in einer gewerblichen oder behördlichen Büroumgebung anzutreffen ist, vorausgesetzt werden. Daher sind Sicherheitsmaßnahmen zu ergreifen, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen.

In diesem Baustein werden die typischen Gefährdungen und Maßnahmen für einen mobilen Arbeitsplatz beschrieben.

## Gefährdungslage

Für den IT-Grundschutz eines mobilen Arbeitsplatzes werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.15 *Beeinträchtigung durch wechselnde Einsatzumgebung*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.47 *Ungesicherter Akten- und Datenträgertransport*
- G 2.48 *Ungeeignete Entsorgung der Datenträger und Dokumente*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Auch für mobile Arbeitsplätze sind eine Reihe von Maßnahmen umzusetzen. Auch diese sollten angelehnt an das Lebenszyklus-Modell durchlaufen werden.

**Planung und Konzeption**

Die Maßnahme M 1.61 *Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes* beschreibt die grundlegenden Gestaltungsmöglichkeiten, die bei der Einrichtung eines Arbeitsplatzes in fremder Umgebung beachtet werden sollten.

**Umsetzung**

Für alle Arbeiten unterwegs ist zu regeln, welche Informationen außerhalb des Unternehmen bzw. der Behörde transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind. Dabei ist auch zu klären, unter welchen Rahmenbedingungen Mitarbeiter mit mobilen IT-Systemen Zugriff auf interne Daten ihrer Institution nehmen können.

**Betrieb**

Beim mobilen Arbeiten müssen nicht nur die mitgenommenen IT-Systeme (z. B. Laptop, PDA, Mobiltelefon), sondern auch die unterwegs bearbeiteten Informationen sorgfältig behandelt werden. Dazu gehören die Einhaltung der vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien.

**Aussonderung**

Gerade in fremden Umgebungen ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Hausmüll zu werfen.

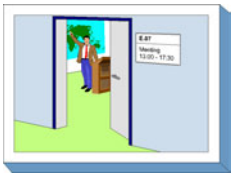
Nachfolgend wird das Maßnahmenbündel für den Bereich "Mobiler Arbeitsplatz" vorgestellt.

**Planung und Konzeption**
- M 1.61 (A) *Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes*
- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.309 (A) *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*
- M 2.430 (C) *Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs*

**Betrieb**
- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 1.23 (A) *Abgeschlossene Türen*
- M 1.46 (Z) *Einsatz von Diebstahl-Sicherungen*
- M 2.37 (C) *Der aufgeräumte Arbeitsplatz*
- M 2.389 (Z) *Sichere Nutzung von Hotspots*
- M 4.251 (A) *Arbeiten mit fremden IT-Systemen*

**Aussonderung**
- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*

# B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume



## Beschreibung

Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im wesentlichen dadurch aus, dass sie

- von wechselnden Personen bzw. Personenkreisen genutzt werden,
- sowohl durch eigenes Personal als auch durch Externe genutzt werden,
- eine in sich geschlossene Nutzung mit dem gleichen Kreis nutzende Personen meist nur kurze Zeit andauert, wenige Stunden bis zu wenigen Tagen,
- mitgebrachte IT-Systeme gemeinsam mit eigener IT betrieben werden (z. B. fremder Laptop am eigenen Beamer),
- die dort genutzten Informationen in der Regel lokal (z. B. auf Laptop oder mobilem Datenträger) vorhanden sind oder aus einem eigens eingerichteten Test- oder Trainingsnetz zur Verfügung gestellt werden. Teilweise ist sogar ein Anschluss an das LAN vorhanden, so dass auf institutionsinterne Daten zugegriffen werden kann.

Aus diesen extrem unterschiedlichen Nutzungen heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist. Das Hauptaugenmerk ist dabei, neben den üblichen Gefährdungen für Räume aller Art, die Gefährdung durch den "Spieltrieb" anwesender Personen.

## Gefährdungslage

Für den IT-Grundschutz von Besprechungs-, Veranstaltungs- und Schulungsräumen werden folgende Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.14 *Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen*
- G 2.104 *Inkompatibilität zwischen fremder und eigener IT*

**Menschliche Fehlhandlungen**

- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.78 *Fliegende Verkabelung*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.2 *Ausfall interner Versorgungsnetze*

**Vorsätzliche Handlungen**

- G 5.4 *Diebstahl*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

**Planung und Konzeption**

Die Nutzungsmöglichkeiten von Besprechungs-, Veranstaltungs- und Schulungsräumen variieren sehr stark.
Da hiervon auch die erforderlichen Sicherheitsmaßnahmen abhängen, sollte zunächst eine Nutzungsübersicht erstellt werden, welche die geplanten Einsatzszenarien berücksichtigt (siehe M 2.331 *Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).

Basierend auf dem Nutzungskonzept sollten geeignete Räumlichkeiten ausgewählt und ausgestattet werden (siehe M 2.332 *Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen*).

Wenn auf LANs oder das Internet zugegriffen werden soll, müssen die Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen sorgfältig abgesichert werden (siehe M 5.124 *Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen*).

**Umsetzung**

Es müssen Sicherheitsregelungen für Besprechungs-, Veranstaltungs- und Schulungsräume festgelegt sowie technisch und organisatorisch umgesetzt werden. Alle Mitarbeiter müssen darüber informiert werden, welche Nutzungsregelungen zu beachten sind (siehe M 2.333 *Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen*).

**Betrieb**

Auch in Besprechungs-, Veranstaltungs- und Schulungsräumen muss mit den Einrichtungen und der vorhandenen Technik sorgfältig umgegangen werden. Dazu gehören die Einhaltung der von der Institution vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien.

**Aussonderung**

Gerade in Besprechungs-, Veranstaltungs- und Schulungsräumen mit häufig wechselnden Benutzern ist es wichtig, Arbeitsmaterialien wie Datenträger und Papiere sorgsam zu entsorgen und nicht einfach liegen zu lassen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume" vorgestellt.

**Planung und Konzeption**

- M 2.331 (A) *Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen*
- M 2.332 (B) *Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen*
- M 3.9 (Z) *Ergonomischer Arbeitsplatz*
- M 5.77 (Z) *Bildung von Teilnetzen*
- M 5.124 (C) *Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen*

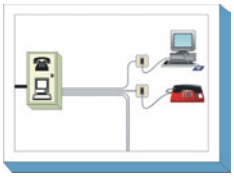
**Umsetzung**

- M 2.69 (B) *Einrichtung von Standardarbeitsplätzen*
- M 2.204 (A) *Verhinderung ungesicherter Netzzugänge*
- M 2.333 (A) *Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen*
- M 4.252 (C) *Sichere Konfiguration von Schulungsrechnern*

**Betrieb**

- M 1.15 (A) *Geschlossene Fenster und Türen*
- M 2.16 (B) *Beaufsichtigung oder Begleitung von Fremdpersonen*
- M 4.109 (Z) *Software-Reinstallation bei Arbeitsplatzrechnern*
- M 4.293 (Z) *Sicherer Betrieb von Hotspots*

# B 2.12 IT-Verkabelung



## Beschreibung

Die IT-Verkabelung umfasst alle Kommunikationskabel und passiven Komponenten (Rangier- bzw. Spleißverteiler, Patchfelder), die in eigener Hoheit der Institution betrieben werden. Sie ist also die physikalische Grundlage der internen Kommunikationsnetze einer Institution. Die IT-Verkabelung reicht von Übergabepunkten aus einem Fremdnetz (z. B. ISDN-Anschluss eines TK-Anbieters, DSL-Anbindung eines Internet-Providers) bis zu den Anschlusspunkten der Netzteilnehmer.

Aktive Netzkomponenten (Router, Switches etc.) sind nicht Gegenstand dieses Kapitels. Ebenso ist auch das Thema WLAN ausgeklammert. Beide Themen werden in eigenen Bausteinen der IT-Grundschutz-Kataloge behandelt. In diesem Baustein wird mit IT-Verkabelung die physische Grundlage eines hersteller- und anwendungsneutralen Kommunikationsnetzes, also eines Local Area Networks (LAN), bezeichnet. Eine Unterscheidung zwischen IT-Verkabelung zum Datentransport und TK-Verkabelung für Telekommunikationsdienste erfolgt nicht.

Die IT-Verkabelung als Teil der technischen Infrastruktur von Gebäuden und Liegenschaften wird nach der etablierten Betrachtungs- und Vorgehensweise der strukturierten Verkabelung in Primär-, Sekundär- und Tertiärbereich aufgeteilt.

Mit Primärbereich wird der Bereich der Kabelführung, der Gebäude miteinander verbindet, bezeichnet. Der Primärbereich überbrückt große Entfernungen mit hohen Übertragungsraten zwischen wenigen Anschlusspunkten. Eine Primärverkabelung in eigener Hoheit haben also nur Instanzen, die größere Liegenschaften mit mehreren Gebäuden betreiben. Wenn nur ein Gebäude zu betrachten ist, stellt der Hauptverteiler im Gebäude logisch den Primärbereich dar.

Mit Sekundärbereich wird die Verkabelung zwischen dem Gebäudeverteiler und Verteilern der Etagen oder Gebäudebereichen bezeichnet. Diese Verkabelung ist in vielen größeren Gebäuden anzutreffen.

Die Tertiärverkabelung ist die Anbindung der Endgeräte an einen zentralen Verteilpunkt (z. B. in der Etage). Sie ist immer vorhanden.

Eine oft betriebene Mischform der strukturierten Verkabelung liegt dann vor, wenn die Anbindung der Endgeräte direkt von einem zentralen Punkt im Serverraum oder einem Raum für technische Infrastruktur (häufig als "Netzwerkraum" oder "TK-Raum" bezeichnet) ausgeführt wird. In diesem Fall besteht die Sekundärverkabelung gegebenenfalls nur aus den Verbindungskabeln zwischen den Switches. Die Tertiärverkabelung reicht vom zentralen Verteilpunkt im Gebäude zu den Anschlussdosen in den Räumen.

## Gefährdungslage

Für den IT-Grundschutz der IT-Verkabelung werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.6 *Kabelbrand*

**Organisatorische Mängel**

- G 2.11 *Unzureichende Trassendimensionierung*
- G 2.12 *Unzureichende Dokumentation der Verkabelung*
- G 2.32 *Unzureichende Leitungskapazitäten*

**Menschliche Fehlhandlungen**

- G 3.4 *Unzulässige Kabelverbindungen*
- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*

**Technisches Versagen**

- G 4.4 *Leitungsbeeinträchtigung durch Umfeldfaktoren*

- G 4.5 *Übersprechen*
- G 4.21 *Ausgleichsströme auf Schirmungen*

**Vorsätzliche Handlungen**

- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Insbesondere der Baustein B 3.302 *Router und Switches* steht in engem Zusammenhang mit der IT-Verkabelung und ist im Einklang mit diesem Baustein anzuwenden. Wird im betrachteten Informationsverbund ein Funknetz eingesetzt, so ist zusätzlich der Baustein B 4.6 *WLAN* anzuwenden.

Für eine sichere IT-Verkabelung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Umsetzung bis zum Betrieb und zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Dabei ist zu berücksichtigen, dass die Einflussmöglichkeiten in Bezug auf die Absicherung der IT-Verkabelung beim Einzug in ein schon bestehendes Gebäude wesentlich geringer sind als bei der Errichtung eines Neubaus.

**Planung und Konzeption**

In der Planungsphase werden die Grundlagen für eine leistungsfähige, gut abgesicherte IT-Verkabelung gelegt. Ausgangspunkt ist eine Anforderungsanalyse (siehe M 2.395 *Anforderungsanalyse für die IT-Verkabelung*), mit der der aktuelle Bedarf eingeschätzt wird und ein Ausblick auf kommende Entwicklungen samt Folgenabschätzung für die IT-Verkabelung in der Institution vorgenommen wird.

Auf Grundlage dieser Anforderungsplanung wird die Netzstruktur festgelegt (siehe M 5.2 *Auswahl einer geeigneten Netz-Topologie*) und in das Gebäude eingepasst (siehe M 1.21 *Ausreichende Trassendimensionierung*). Die mechanischen und elektrischen Eigenschaften der Verkabelung werden weitgehend durch die Auswahl der einzusetzenden Kabeltypen festgelegt. Bei der Planung sollte nach Möglichkeit auch darauf geachtet werden, dass Leitungen und über das Gebäude verteilte Schaltschränke gegen Missbrauch in geeigneter Weise physisch gesichert werden.

**Umsetzung**

Ein wesentliches Element des Brandschutzes ist die richtige Installation von Kabelkanälen, die durch eine fehlende Brandabschottung erhebliche Risiken verursachen können. Beim Einbau der Verkabelung ist auch auf eine ausführliche und korrekte Dokumentation (siehe M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*) zu achten, da es im Nachhinein ohne eine solche meist sehr schwierig oder sogar unmöglich ist, festzustellen, wo Kabel verlaufen und was sie verbinden. Für einen störungsfreien Betrieb muss die IT-Verkabelung sachgerecht installiert werden (siehe M 1.68 *Fachgerechte Installation*).

Vor Inbetriebnahme ist die Installation der IT-Verkabelung abzunehmen (siehe M 5.142 *Abnahme der IT-Verkabelung*) und die Qualität der zugehörigen Dokumentation (siehe M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*) zu prüfen.

**Betrieb**

Um das Aufschalten ungenehmigter IT-Geräte zu verhindern, sollten jeweils nur die Verbindungen und Anschlussdosen aktiviert sein, die tatsächlich benötigt werden. Zusätzlich sollte durch regelmäßige Kontrollen sichergestellt werden, dass diese Aktivierung auch den tatsächlichen Erfordernissen entspricht (siehe M 2.20 *Kontrolle bestehender Verbindungen*). Zudem ist sicherzustellen, dass die Dokumentation aktuell gehalten wird (siehe M 5.143 *Laufende Fortschreibung und Revision der Netzdokumentation*).

**Aussonderung**

Wenn Komponenten der IT-Verkabelung nicht mehr benötigt werden, müssen sie entfernt werden (siehe M 5.144 *Rückbau der IT-Verkabelung*).

**Notfallvorsorge**

Sofern erhöhte Anforderungen an die Verfügbarkeit gestellt werden, sollte die Verkabelung, gegebenenfalls einschließlich der externen Anschlüsse, so redundant ausgelegt werden, dass ein Schaden an einer einzigen Stelle nicht zu einem Totalausfall aller Teilnehmeranschlüsse führen kann. Dazu sind gegebenenfalls Redundanzen der Verbindung zwischen Gebäuden (siehe M 6.103 *Redundanzen für die Primärverkabelung*) und innerhalb eines Gebäudes (siehe M 6.104 *Redundanzen für die Gebäudeverkabelung*) zu schaffen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "IT-Verkabelung" vorgestellt:

**Planung und Konzeption**
- M 1.20 (A) *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht*
- M 1.21 (A) *Ausreichende Trassendimensionierung*
- M 1.22 (Z) *Materielle Sicherung von Leitungen und Verteilern*
- M 1.65 (Z) *Erneuerung der IT-Verkabelung*
- M 1.66 (Z) *Beachtung von Normen bei der IT-Verkabelung*
- M 2.395 (A) *Anforderungsanalyse für die IT-Verkabelung*
- M 2.396 (Z) *Vorgaben zur Dokumentation und Kennzeichnung der IT-Verkabelung*
- M 5.2 (A) *Auswahl einer geeigneten Netz-Topologie*
- M 5.3 (A) *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*

**Umsetzung**
- M 1.9 (A) *Brandabschottung von Trassen*
- M 1.67 (C) *Dimensionierung und Nutzung von Schranksystemen*
- M 1.68 (A) *Fachgerechte Installation*
- M 1.69 (Z) *Verkabelung in Serverräumen*
- M 2.19 (B) *Neutrale Dokumentation in den Verteilern*
- M 5.4 (A) *Dokumentation und Kennzeichnung der Verkabelung*
- M 5.5 (A) *Schadensmindernde Kabelführung*
- M 5.142 (C) *Abnahme der IT-Verkabelung*

**Betrieb**
- M 1.39 (C) *Verhinderung von Ausgleichsströmen auf Schirmungen*
- M 2.20 (C) *Kontrolle bestehender Verbindungen*
- M 5.143 (B) *Laufende Fortschreibung und Revision der Netzdokumentation*

**Aussonderung**
- M 5.1 (A) *Entfernen oder Deaktivieren nicht benötigter Leitungen*
- M 5.144 (B) *Rückbau der IT-Verkabelung*

**Notfallvorsorge**
- M 6.103 (Z) *Redundanzen für die Primärverkabelung*
- M 6.104 (Z) *Redundanzen für die Gebäudeverkabelung*

# B 3 IT-Systeme

# B 3.101 Allgemeiner Server


## Beschreibung

Server sind IT-Systeme, die Dienste (Services) für andere IT-Systeme (Clients) im Netz anbieten. Sie werden typischerweise in zentralen, besonders gesicherten Räumlichkeiten betrieben, beispielsweise in einem Serverraum oder einem Rechenzentrum, und nicht als Arbeitsplatzrechner genutzt. Für Server stehen unterschiedliche Betriebssysteme zur Verfügung, unter anderem Unix bzw. Linux, Microsoft Windows und Novell Netware. Dieser Baustein betrachtet Sicherheitsaspekte, die unabhängig vom eingesetzten Betriebssystem für Server relevant sind. Für betriebssystemspezifische Sicherheitsaspekte existieren in den IT-Grundschutz-Katalogen eigenständige Bausteine, die zusätzlich auf die jeweils betroffenen Server anzuwenden sind. Die netzspezifischen Aspekte des Servereinsatzes werden im Baustein B 4.1 *Lokale Netze* behandelt.

## Gefährdungslage

Wie jedes IT-System ist auch ein Server vielfältigen Gefahren ausgesetzt. Generell gilt, dass die Gefährdungslage einzelner Rechner immer auch vom Einsatzszenario, beispielsweise der Nutzung als Dateiserver, Terminalserver bzw. Authentisierungsserver, abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen.

Für den IT-Grundschutz eines Servers werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.36 *Ungeeignete Einschränkung der Benutzerumgebung*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.6 *Spannungsschwankungen/Überspannung/Unterspannung*
- G 4.7 *Defekte Datenträger*
- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.20 *Überlastung von Informationssystemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.39 *Software-Konzeptionsfehler*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*

- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.26 *Analyse des Nachrichtenflusses*
- G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon und Kamera*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.75 *Überlastung durch eingehende E-Mails*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Servers sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Ein besonderes Gewicht ist dabei auf die konzeptionellen Planungsmaßnahmen zu legen, wenn der Server im Rahmen des Aufbaus eines neuen servergestützten Netzes installiert wird. Sofern die Installation dagegen als Ausbau eines schon existierenden Netzes erfolgt, können sich die Planungsmaßnahmen häufig darauf beschränken, auf die Konformität des neuen Servers mit den schon vorhandenen Strukturen zu achten. Die Maßnahmen zur Beschaffung und zum Betrieb des Servers sind dagegen in jedem Fall umzusetzen. Die Schritte, die zum Schutz eines Servers zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Im Vorfeld der eigentlichen Planung ist die generelle Architektur des Netzes festzulegen bzw. zu analysieren, aus der sich im Allgemeinen auch Vorgaben für die einzusetzenden Betriebssysteme (Server und Client) ergeben. Insbesondere ist dabei festzulegen, welche Ziele mit dem aufzubauenden Server verfolgt werden. Dazu sind die voraussichtlichen Einsatzszenarien zu beschreiben und der Einsatzzweck zu definieren.

Falls ein neues Netz aufgebaut wird, ist zunächst die Struktur des Netzes insgesamt zu planen, wobei Fragen wie die Festlegung einer Netztopographie und die Entscheidung über den Grad der Serverzentrierung (Terminalserver, "klassische" Client-Server-Architektur oder Nutzung von Peer-to-Peer-Funktionalität) zu klären sind. Hier sind die Maßnahmen des Bausteins B 1.9 *Hard- und Software-Management* heranzuziehen.

In einem weiteren Schritt folgt die Festlegung der auf der Ebene der Server und der Clients verwendeten Betriebssysteme und gegebenenfalls auch die Auswahl spezifischer Varianten (z. B. Windows XP gegenüber Windows 2007 oder Linux gegenüber einer herstellerspezifischen Variante von Unix).

Falls ein neues Netz aufgebaut wird, muss als genaue technische Grundlage für die weiteren Arbeiten der detaillierte Aufbau des Netzes geplant werden. Anzahl und Zusammenspiel der vorgesehenen Server sind festzulegen. Die Aufgaben der Server und die Art ihrer Nutzung durch die Clients sind zu bestimmen. Anhand der Anforderungen an die Verfügbarkeit muss festgelegt werden, bis zu welchem Grad redundante Strukturen im Netz vorzusehen sind. Hier sind auch die notwendigen Vorgaben für die Infrastruktur (vor allem Klimatisierung und Stromversorgung, siehe dazu M 1.28 *Lokale unterbrechungsfreie Stromversorgung*) festzulegen. Parallel dazu ist eine allgemeine Sicherheitsrichtlinie zu erarbeiten (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*), die anschließend durch systemspezifische Sicherheitsrichtlinien und detaillierte Richtlinien für den Einsatz der Hard- und Software im Netz zu ergänzen ist (siehe dazu die Bausteine zu den einzelnen Server-Betriebssystemen).

**Beschaffung**

Im nächsten Schritt muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Aufbauend auf Einsatzszenarien sind die Anforderungen an zu beschaffende Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. Mit der Beschaffung dieser Produkte ist dann die Grundlage für die Arbeiten des nächsten Schrittes gelegt.

**Umsetzung**

Die Benutzer bzw. die Administratoren haben einen wesentlichen Einfluss auf die Sicherheit eines Servers. Vor der tatsächlichen Inbetriebnahme müssen die Benutzer und Administratoren daher für den Umgang bzw. die Nutzung des aufzubauenden Servers geschult werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität in der Planung und in der Verwaltung eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben, so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist. Benutzern sollte insbesondere die Nutzung der verfügbaren Sicherheitsmechanismen vermittelt werden. Hier sind die Maßnahmen des Bausteins B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit* heranzuziehen.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation und Inbetriebnahme des Servers erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:

- Schon die Installation und Grundkonfiguration eines Servers muss mit besonderer Sorgfalt durchgeführt werden, um schwer reparierbare Fehler von vornherein zu vermeiden. Allgemeine Hinweise hierzu finden sich in M 2.318 *Sichere Installation eines IT-Systems* und M 4.237 *Sichere Grundkonfiguration eines IT-Systems*.
  Neben den allgemeinen Maßnahmen, die in diesem Baustein beschrieben sind, sind jeweils auch die weitergehenden Maßnahmen, die in den betreffenden Bausteinen für das jeweilige Betriebssystem empfohlen werden, umzusetzen.
- Nach der Installation und Grundkonfiguration der Server müssen gegebenenfalls übergeordnete Verwaltungsstrukturen konfiguriert werden. Dabei kommt unter anderem auch zum Tragen, für welchen Einsatzzweck die einzelnen Server geplant sind, beispielsweise als Dateiserver, Druckserver oder, im Falle von Thin Clients, als Terminalserver. Hier ist insbesondere die Maßnahme M 2.138 *Strukturierte Datenhaltung* wichtig, um einen kontrollierbaren Betrieb des Servers gewährleisten zu können.
- Nachdem die Installation und Grundkonfiguration des Servers abgeschlossen ist, kann die eigentliche Serversoftware installiert und konfiguriert werden. Die dafür notwendigen Schritte unterscheiden sich je nach Art und Einsatzzweck der Software teilweise erheblich und werden teilweise in eigenen Bausteinen behandelt. Prinzipiell wird empfohlen, für die Installation und Konfiguration der Serversoftware analog wie für die Konfiguration des Betriebssystems selbst vorzugehen:

  - Erstellung eines Installationskonzepts
  - Falls mehrere Server mit ähnlichen Einsatzgebieten und Konfiguration installiert werden sollen: Erstellen einer Referenzinstallation
  - Installation, Grundkonfiguration und Aktualisierung
  - Test

  Detailliertere Hinweise für die Sicherheit verschiedener Server-Anwendungen finden sich in den Bausteinen der Schicht 5.

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Client-Server-Netze ändern sich sehr häufig. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei im Detail zu beachtenden Aspekte sind in den Bausteinen zu den jeweiligen Serverbetriebssystemen enthalten. Dabei ist zu berücksichtigen, dass auch der Entzug von Berechtigungen sowie das Löschen nicht mehr benötigter Datenbestände so geregelt wird, dass durch veraltete Strukturen keine Sicherheitslücken entstehen. Eine wesentliche Hilfe ist dabei eine effiziente, umfassende Systemverwaltung, die sich jederzeit auf aktuelle Informationen über den Zustand des Systems und seiner Rechtestrukturen abstützen kann (siehe dazu M 4.24 *Sicherstellung einer konsistenten Systemverwaltung* und M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).
- Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Servers ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in M 4.93 *Regelmäßige Integritätsprüfung*, M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*. Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle. Die häufigen Sicherheitslücken der meisten Cli-

ent-Server-Systeme und die Vielzahl von Angriffen, die sich gegen diese Schwächen richten, fordern von den Administratoren, dass diese sich permanent über den Sicherheitsstatus der Systeme und über neue Bedrohungen informieren (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*) und rechtzeitig Gegenmaßnahmen einleiten (siehe dazu M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

**Aussonderung**

Ein Server darf nicht einfach ohne Ankündigung abgeschaltet werden. Wenn ein Server außer Betrieb genommen werden soll, dann müssen die Anwender rechtzeitig informiert werden und es muss eine Reihe von Punkten beachtet werden, um Ausfallzeiten und Datenverluste zu verhindern. Diese Punkte sind in M 2.320 *Geregelte Außerbetriebnahme eines Servers* beschrieben. Sollen die Dienste des Servers auf einen anderen Rechner migriert werden, so ist M 2.319 *Migration eines Servers* zu berücksichtigen.

Bei der Aussonderung eines Servers ist außerdem darauf zu achten, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass ein reines logisches Löschen und auch nicht das Neuformatieren der Platten mit den Mitteln des installierten Betriebssystems die Daten nicht von den Festplatten entfernt, so dass sie mit geeigneter Software, oft sogar ohne großen Aufwand, wieder rekonstruiert werden können. Entsprechende Hinweise finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*, die im Rahmen des übergeordneten Bausteins B 1.1 *Organisation* behandelt wird, und in M 4.234 *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern* im übergeordneten Baustein B 1.9 *Hard- und Software-Management*.

Die Aussonderung des Servers muss dokumentiert werden. Bestandsverzeichnisse und Netzpläne müssen aktualisiert werden und sofern sich durch die Aussonderung strukturelle Veränderungen des Informationsverbundes ergeben, sollte auch das Sicherheitskonzept entsprechend angepasst werden.

**Notfallvorsorge**

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen weiter verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein B 1.4 *Datensicherungskonzept* beschrieben.

Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich im Baustein B 1.3 *Notfallmanagement*. Hierzu gehört auch die Planung des Umgangs mit Sicherheitsvorfällen, die sich auf die Maßnahmen des Bausteins B 1.8 *Behandlung von Sicherheitsvorfällen* abstützen sollte. Einige Hinweise zu besonderen Aspekten, die bei der Notfallvorsorge für einen Server beachtet werden sollten, sind in M 6.96 *Notfallvorsorge für einen Server* beschrieben.

Es wird vorausgesetzt, dass der Server in einem Serverraum (siehe Baustein B 2.4 *Serverraum*), einem Serverschrank (siehe Baustein B 2.7 *Schutzschränke*) oder in einem Rechenzentrum (siehe Baustein B 2.9 *Rechenzentrum*) untergebracht ist. Die für die Serverbetriebssysteme umzusetzenden Maßnahmen sind den jeweiligen betriebssystemspezifischen Bausteinen zu entnehmen. Dies gilt analog auch für die angeschlossenen Clients. Die Maßnahmen des Bausteins B 1.9 *Hard- und Software-Management* bilden in jedem Fall den übergeordneten Rahmen für den Betrieb servergestützter Netze.

Darüber hinaus sind folgende weitere Maßnahmen umzusetzen:

**Planung und Konzeption**

- M 1.28 (B) *Lokale unterbrechungsfreie Stromversorgung*
- M 2.314 (Z) *Verwendung von hochverfügbaren Architekturen für Server*
- M 2.315 (A) *Planung des Servereinsatzes*
- M 2.316 (A) *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*
- M 4.250 (Z) *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*
- M 4.432 (A) *Sichere Konfiguration von Serverdiensten*
- M 5.10 (A) *Restriktive Rechtevergabe*

- M 5.138 (Z) *Einsatz von RADIUS-Servern*
- M 5.177 (B) *Serverseitige Verwendung von SSL/TLS*

**Beschaffung**

- M 2.317 (C) *Beschaffungskriterien für einen Server*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 2.204 (A) *Verhinderung ungesicherter Netzzugänge*
- M 2.318 (A) *Sichere Installation eines IT-Systems*
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.15 (A) *Gesichertes Login*
- M 4.16 (C) *Zugangsbeschränkungen für Benutzer-Kennungen und / oder Terminals*
- M 4.17 (A) *Sperren und Löschen nicht benötigter Accounts und Terminals*
- M 4.97 (Z) *Ein Dienst pro Server*
- M 4.237 (A) *Sichere Grundkonfiguration eines IT-Systems*
- M 4.305 (B) *Einsatz von Speicherbeschränkungen (Quotas)*

**Betrieb**

- M 2.22 (Z) *Hinterlegen des Passwortes*
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 4.24 (A) *Sicherstellung einer konsistenten Systemverwaltung*
- M 4.93 (Z) *Regelmäßige Integritätsprüfung*
- M 4.238 (A) *Einsatz eines lokalen Paketfilters*
- M 4.239 (A) *Sicherer Betrieb eines Servers*
- M 4.240 (Z) *Einrichten einer Testumgebung für einen Server*
- M 5.8 (B) *Regelmäßiger Sicherheitscheck des Netzes*
- M 5.9 (B) *Protokollierung am Server*

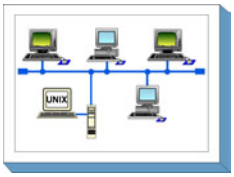
**Aussonderung**

- M 2.319 (C) *Migration eines Servers*
- M 2.320 (A) *Geregelte Außerbetriebnahme eines Servers*

**Notfallvorsorge**

- M 6.24 (A) *Erstellen eines Notfall-Bootmediums*
- M 6.96 (A) *Notfallvorsorge für einen Server*

# B 3.102 Server unter Unix




## Beschreibung

Unix-Server sind Rechner mit dem Betriebssystem Unix, die in einem Netz Dienste anbieten, die von anderen IT-Systemen in Anspruch genommen werden können. Das erste Unix-System wurde Anfang der 1970er Jahre entwickelt. Mittlerweile gibt es eine Vielzahl von Betriebssystemen, die der Unix-Familie zugeordnet werden. Hierbei wird zwischen

- klassischen Unix-Systemen oder Unix-Derivaten,
- zertifizierten UNIX-Systemen (UNIX ist ein Warenzeichen der Open Group, das nur zertifizierte Systeme tragen dürfen, die die entsprechende Spezifikation erfüllen) und
- funktionellen Unix-Systemen oder unix-ähnlichen Systemen.

Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux ist kein klassisches Unix (der Kernel basiert nicht auf dem ursprünglichen Quelltext, aus dem sich die verschiedenen Unix-Derivate entwickelt haben), sondern ein funktionelles Unix-System. In diesem Baustein werden alle Betriebssysteme der Unix-Familie betrachtet, also auch Linux als funktionelles Unix-System.

In diesem Baustein werden ausschließlich die für einen Unix-Server spezifischen Gefährdungen und Maßnahmen beschrieben, daher sind zusätzlich noch diejenigen für allgemeine Server aus Baustein B 3.101 zu betrachten.

## Gefährdungslage

Für den IT-Grundschutz eines Unix-Servers werden folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.15 *Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System*

**Menschliche Fehlhandlungen**

- G 3.10 *Falsches Exportieren von Dateisystemen unter Unix*
- G 3.11 *Fehlerhafte Konfiguration von sendmail*

**Technisches Versagen**

- G 4.11 *Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client*
- G 4.12 *Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client*

**Vorsätzliche Handlungen**

- G 5.41 *Missbräuchliche Nutzung eines Unix-Systems mit Hilfe von UUCP*
- G 5.89 *Hijacking von Netz-Verbindungen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Servers unter Unix sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb dieses Servers. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Die nachfolgenden Maßnahmen beziehen sich auf die sichere Konfigurierung und den sicheren Betrieb eines Unix-Servers, der in einem Netz Dienste für Clients anbietet. Die generelle Planung der Netzarchitektur wird im Baustein B 3.101 *Allgemeiner Server* festgelegt, in denen insbesondere die generelle

Netzarchitektur und netzweite Regelungen festgelegt werden. Die Vorgaben, die sich dort für die Server ergeben, sind zu beachten. Es ist sinnvoll, den Server in einem separaten Serverraum aufzustellen. Zu realisierende Maßnahmen sind im Baustein B 2.4 *Serverraum* beschrieben. Steht kein Serverraum zur Verfügung, sollte ein Serverschrank verwendet werden, vergleiche dazu den Baustein B 2.7 *Schutzschränke*.

Es ist ein Verfahren für die Vergabe von Benutzerkennungen festzulegen, durch das gewährleistet wird, dass privilegierte und unprivilegierte Benutzerkennungen klar getrennt sind. Weiterhin ist sicherzustellen, dass kein unkontrollierter Zugang zum Single-User-Modus möglich ist, da sonst alle für die Laufzeit des Systems festgelegten Sicherheitsmaßnahmen unterlaufen werden können.

**Beschaffung**

Die Anzahl der Server im Netz sowie deren Nutzung durch Clients sind ebenfalls im Baustein B 3.101 *Allgemeiner Server* festgelegt worden, ebenso wie die Anforderungen an die zu beschaffenden Produkte.

**Umsetzung**

Einige nachfolgend beschriebene Maßnahmen beziehen sich auf die Konfiguration der einzelnen Server, andere Maßnahmen müssen auf Servern und Clients eingesetzt werden, um wirksam zu werden. Für eventuell angeschlossene Clients sind die in den entsprechenden Bausteinen beschriebenen Maßnahmen zu realisieren.

Bei der Konfigurierung eines Unix-Servers ist nach der Installation mit der Maßnahme M 4.105 *Erste Maßnahmen nach einer Unix-Standardinstallation* zu beginnen. Hierbei sind, je nach Einsatzszenario (vergleiche B 3.101 *Allgemeiner Server*), Grundeinstellungen so vorzunehmen, dass nur benötigte Dienste aktiv sind bzw. die beschriebenen Vorkehrungen getroffen werden und die Systemprotokollierung aktiviert wird.

Ferner sind die Zugriffsrechte auf Benutzer- und Systemdateien und -verzeichnisse so nach einem übergreifenden Schema zu vergeben, dass nur diejenigen Benutzer und Prozesse Zugriff erhalten, die diesen wirklich benötigen, wobei insbesondere auf die durch *setuid* und *setgid* bestimmten Rechte zu achten ist (siehe dazu die Maßnahme M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*).

**Betrieb**

Um die Sicherheit eines Servers unter Unix im laufenden Betrieb zuverlässig aufrecht zu erhalten, ist es unabdingbar, durch regelmäßige Überprüfungen festzustellen, ob irgendwelche Lücken aufgetreten sind, und diese so schnell wie möglich zu schließen. Dabei sind auch die vom System erzeugten Protokolle auf eventuelle Unregelmäßigkeiten hin zu betrachten.

**Notfallvorsorge**

Da Unix-Systeme aufgrund ihrer Komplexität nach einem erfolgreichen Angriff oft auf schwer durchschaubare Weise kompromittiert sind, ist es wichtig, schon im Vorfeld Regeln festzulegen, nach denen bei einem echten oder vermuteten Verlust der Systemintegrität zu verfahren ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Server unter Unix" vorgestellt.

**Planung und Konzeption**

- M 2.33 (Z) *Aufteilung der Administrationstätigkeiten unter Unix*
- M 4.13 (A) *Sorgfältige Vergabe von IDs*
- M 4.18 (A) *Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus*
- M 5.16 (B) *Übersicht über Netzdienste*
- M 5.64 (Z) *Secure Shell*
- M 5.83 (Z) *Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN*

**Umsetzung**

- M 4.9 (A) *Einsatz der Sicherheitsmechanismen von X-Window*

- M 4.14 (A) *Obligatorischer Passwortschutz unter Unix*
- M 4.19 (A) *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*
- M 4.20 (B) *Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen*
- M 4.21 (A) *Verhinderung des unautorisierten Erlangens von Administratorrechten*
- M 4.22 (Z) *Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System*
- M 4.23 (B) *Sicherer Aufruf ausführbarer Dateien*
- M 4.105 (A) *Erste Maßnahmen nach einer Unix-Standardinstallation*
- M 4.106 (A) *Aktivieren der Systemprotokollierung*
- M 5.17 (A) *Einsatz der Sicherheitsmechanismen von NFS*
- M 5.18 (A) *Einsatz der Sicherheitsmechanismen von NIS*
- M 5.19 (A) *Einsatz der Sicherheitsmechanismen von sendmail*
- M 5.20 (A) *Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp*
- M 5.21 (A) *Sicherer Einsatz von telnet, ftp, tftp und rexec*
- M 5.35 (A) *Einsatz der Sicherheitsmechanismen von UUCP*
- M 5.72 (A) *Deaktivieren nicht benötigter Netzdienste*

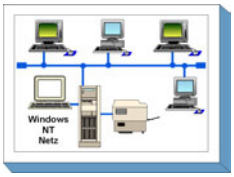
**Betrieb**

- M 4.25 (A) *Einsatz der Protokollierung im Unix-System*
- M 4.26 (C) *Regelmäßiger Sicherheitscheck des Unix-Systems*

**Notfallvorsorge**

- M 6.31 (A) *Verhaltensregeln nach Verlust der Systemintegrität*

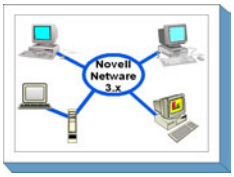
# B 3.103 Server unter Windows NT




Dieser Baustein ist 2009 mit der 11. Ergänzungslieferung entfallen.

Die letzte Version des Bausteins, die mit der 10. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

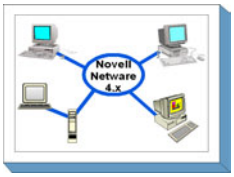
# B 3.104 Server unter Novell Netware 3.x




Dieser Baustein ist 2008 mit der 10. Ergänzungslieferung entfallen.

Die letzte Version des Bausteins, die mit der 9. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

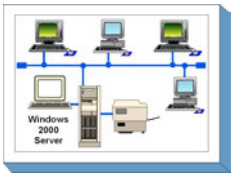
# B 3.105 Server unter Novell Netware Version 4.x




Dieser Baustein ist 2013 mit der 13. Ergänzungslieferung entfallen.

Die letzte Version des Bausteins, die mit der 12. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 3.106 Server unter Windows 2000




Dieser Baustein ist 2013 mit der 13. Ergänzungslieferung entfallen.

Die letzte Version des Bausteins, die mit der 12. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 3.107 S/390- und zSeries-Mainframe


## Beschreibung

Die IBM S/390- und zSeries-Systeme gehören zu den Server-Systemen, die allgemein als Mainframes ("Großrechner") bezeichnet werden. Mainframes haben sich von klassischen Einzelsystemen mit Stapelverarbeitung hin zu modernen Client-/Server-Systemen entwickelt. Sie bilden heute das obere Ende der Palette der angebotenen Server-Systeme.

In diesem Baustein werden nur Mainframes des Typs IBM zSeries bzw. IBM S/390 betrachtet. zSeries-Systeme mit dem Betriebssystem z/OS stellen eine logische Weiterentwicklung der OS/390-Architektur dar. Mit zSeries kommt z. B. die zusätzliche 64 Bit-Unterstützung hinzu. Beide Systemtypen existieren nebeneinander, wobei OS/390 als ein "auslaufendes" Betriebssystem betrachtet werden kann, da IBM den Service im Herbst 2004 eingestellt hat. Aus Gründen der Übersichtlichkeit wird in diesem Zusammenhang nur der Begriff "zSeries" für die Hardware und "z/OS" für das Betriebssystem verwendet.

### Historie

Die im Jahr 1964 eingeführte S/360-Architektur stellt die Basis für alle folgenden Weiterentwicklungen dar und findet sich noch heute in ihren wesentlichen Teilen auf den aktuellen zSeries-Systemen wieder. Der Namenswechsel, von "S/360" über "S/370" und "S/390" bis zur heutigen "zSeries", reflektiert die fortwährende Entwicklung der zugrundeliegenden Architektur. Aufgrund ihrer Abwärtskompatibilität unterstützt die Architektur neben neueren 64-Bit-Applikationen auch Programme im älteren 24- oder 31-Bit-Modus.

Trotz steigender Leistungsfähigkeit haben sich die physischen Abmessungen von Mainframe-Systemen stark verringert. Mainframe-Systeme haben heute ähnliche Abmessungen wie andere Systeme, die typischerweise in Rechenzentren betrieben werden.

### Überblick

Für zSeries-Systeme stehen Mechanismen zur Verfügung, mit denen eine hohe Verfügbarkeit und Skalierbarkeit erreicht werden kann. Die hohe Verfügbarkeit wird dabei durch redundante Auslegung der Komponenten erzielt. Zur Steigerung der Leistung und Verfügbarkeit können derzeit in einem zSeries-System bis zu 16 Prozessoren parallel betrieben und bis zu 32 zSeries-Systeme zu einem Cluster zusammengestellt werden. Dies wird als Parallel-Sysplex-Cluster bezeichnet.

Für die zSeries-Hardware sind verschiedene Betriebssysteme verfügbar (z. B. z/OS, VSE, z/VM oder TPF). Die Auswahl erfolgt in der Regel anhand der Parameter Rechnergröße und Einsatzzweck. Am häufigsten kommt jedoch das z/OS-Betriebssystem zum Einsatz. Um den Rahmen dieses Bausteins nicht zu sprengen, beschränken sich die Empfehlungen in diesem Baustein im Wesentlichen auf das Betriebssystem z/OS.

Durch die Erweiterung des früher auch als "MVS" bezeichneten z/OS-Betriebssystems um das Subsystem *Unix System Services* ist es möglich, parallel zu den klassischen Mainframe-Anwendungen auch Unix-basierte Anwendungen zu betreiben. Daneben ist für die zSeries-Hardware auch ein Linux-Betriebssystem verfügbar.

Einsatzbereiche für heutige z/OS-Systeme sind:

- klassische Stapelverarbeitung für große "Batch-Ketten",
- Stapelverarbeitung einschließlich der transaktionsorientierten Verarbeitung (z. B. IMS oder CICS),
- Datenbank-Server (z. B. DB2, IMS DB oder Oracle) oder
- Webserver und deren Anwendungen

Die in diesem Baustein beschriebenen Software-Komponenten beziehen sich hauptsächlich auf Produkte des Herstellers IBM. Es gibt darüber hinaus viele Produkte von Drittherstellern, die häufig in Großrechner-Umgebungen zum Einsatz kommen. Auf diese Produkte kann nur in Ausnahmefällen eingegangen werden, da sonst der Rahmen des Bausteins gesprengt würde.

Das z/OS-Betriebssystem besteht aus dem eigentlichen Betriebssystem (Kernel) mit Schnittstellen zu den Benutzerprozessen. Verschiedene Subsysteme steuern und unterstützen die Kommunikation. Die wichtigsten Subsysteme sind

- das *Job Entry Subsystem* (JES) für den Hintergrundbetrieb (Stapelverarbeitung oder Batch genannt),
- die *Time Sharing Option* (TSO) für den Vordergrundbetrieb (interaktiv) und
- die *Unix System Services* (Posix-kompatibles Unix-Subsystem).

Weitere Subsysteme sind z. B.

- der Transaktionsmanager IMS und die zugehörige Datenbank für die transaktionsorientierte Datenverarbeitung,
- der Transaktionsmanager CICS für die transaktionsorientierte Datenverarbeitung,
- die Datenbank DB2 für relationale Datenbanken und
- der *Communications Server* (SNA, TCP/IP) für Netzanbindungen.

Die Sicherheitsschnittstelle *System Authorization Facility* (SAF) ermöglicht es, das System und die Dateien vor unbefugten Zugriffen zu schützen. Die eigentlichen Sicherheitsfunktionen werden dabei von der Sicherheitssoftware RACF bereitgestellt. Als alternative Produkte sind an dieser Stelle auch *Top Secret* und *ACF2* zu nennen.

Die folgende Abbildung stellt die Zusammenhänge des Betriebssystemaufbaus stark vereinfacht dar:

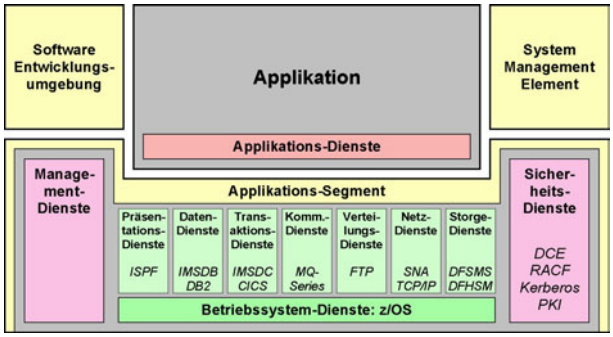



Abbildung: Prinzipieller Aufbau des z/OS-Betriebssystems

Eine Übersicht über die zSeries- und z/OS-Architektur und Erklärungen zu der Terminologie finden sich in den folgenden Maßnahmen:

- M 3.39 *Einführung in die zSeries-Plattform*
- M 3.40 *Einführung in das z/OS-Betriebssystem*
- M 3.41 *Einführung in Linux und z/VM für zSeries-Systeme*

## Gefährdungslage

Generell hängt die Gefährdungslage vom Einsatzszenario ab. Ein z/OS-System mit SNA-Anschluss an einem isolierten behörden- oder firmeninternen Netz ist z. B. in der Regel weniger gefährdet als ein z/OS-System, das an das Internet angeschlossen ist und dort Web-Services anbietet. Darüber hinaus spielt es eine Rolle, ob auf Daten nur lesend zugegriffen werden soll (z. B. bei einem Auskunftssystem) oder ob die Daten bearbeitet werden können. Gerade durch den Einsatz von Web-Servern oder Web-Applikationen mit Internet-Anbindung hat sich die Gefährdungslage der früher als "sehr sicher" geltenden Mainframe-Systeme stark erhöht.

Aufgrund der öffentlichen Netzanbindung von Mainframe-Systemen ergeben sich wesentlich stärkere Gefährdungen durch unsachgemäße oder fehlerhafte Konfiguration der Systeme oder durch fehlende oder unvollständig etablierte Prozesse, als es früher der Fall war.

Dies gilt sowohl für externe Anbindungen und darüber mögliche Angriffe, als auch für den internen Bereich. Mainframe-Systeme sind heute ähnlichen Gefährdungen ausgesetzt wie Unix- oder Windows-Systeme.

**Organisatorische Mängel**

- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.54 *Vertraulichkeitsverlust durch Restinformationen*
- G 2.99 *Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.66 *Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS*
- G 3.67 *Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems*
- G 3.68 *Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers*
- G 3.69 *Fehlerhafte Konfiguration der Unix System Services unter z/OS*
- G 3.70 *Unzureichender Dateischutz des z/OS-Systems*
- G 3.71 *Fehlerhafte Systemzeit bei z/OS-Systemen*
- G 3.72 *Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF*
- G 3.73 *Fehlbedienung der z/OS-Systemfunktionen*
- G 3.74 *Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen*
- G 3.75 *Mangelhafte Kontrolle der Batch-Jobs bei z/OS*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.50 *Überlastung des z/OS-Betriebssystems*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.21 *Trojanische Pferde*
- G 5.28 *Verhinderung von Diensten*
- G 5.57 *Netzanalysetools*
- G 5.116 *Manipulation der z/OS-Systemsteuerung*
- G 5.117 *Verschleiern von Manipulationen unter z/OS*
- G 5.118 *Unbefugtes Erlangen höherer Rechte im RACF*
- G 5.119 *Benutzung fremder Kennungen unter z/OS-Systemen*
- G 5.120 *Manipulation der Linux/zSeries Systemsteuerung*
- G 5.121 *Angriffe über TCP/IP auf z/OS-Systeme*
- G 5.122 *Missbrauch von RACF-Attributen unter z/OS*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines z/OS-Mainframe-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der strategischen Entscheidung, über Konzeption und Installation bis zum Betrieb. Nicht vergessen werden darf dabei die ordnungsgemäße Aussonderung eines Systems, wenn das Ende der Betriebsphase erreicht wird.

Parallel zur Betriebsphase muss die Notfallvorsorge sicherstellen, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. Sicherheitsmanagement und Revision stellen sicher, dass das Regelwerk auch eingehalten wird.

Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

**Strategie**

Vor Beginn einer jeden Planung findet eine Phase der strategischen Orientierung statt, die weitgehend auf den Anforderungen der Anwendungseigner basiert. Hier ist zu prüfen, ob die z/OS-Plattform für die Lösung der jeweiligen Aufgabenstellung geeignet ist.

Darüber hinaus kommt es auf die generelle Ausrichtung der IT-Landschaft des Rechenzentrums an. Gibt es noch keine z/OS-Plattform im Betrieb, muss der Aufbau des notwendigen Wissens des Betriebspersonals entsprechend vorbereitet werden. Als Hilfestellung für die strategische Planung dienen die Maßnahmen

- M 3.39 *Einführung in die zSeries-Plattform*,
- M 3.40 *Einführung in das z/OS-Betriebssystem* und
- M 3.41 *Einführung in Linux und z/VM für zSeries-Systeme*.

Sie geben einen Überblick über die einzelnen Funktionen von Hard- und Software und unterstützen damit das Verständnis für die z/OS-Plattform.

**Konzeption**

Sollte die strategische Entscheidung für den Einsatz eines z/OS-Mainframe-Systems gefallen sein, muss sich eine detaillierte Planung für den Einsatz dieses Systems anschließen. Die folgenden Maßnahmen sind dabei zu berücksichtigen:

- Vor der Anschaffung und Inbetriebnahme von zSeries-Systemen müssen verschiedene planerische Tätigkeiten durchgeführt werden (siehe M 2.286 *Planung und Einsatz von zSeries-Systemen*).
- Bei höheren Ansprüchen an die Verfügbarkeit oder die Skalierbarkeit empfiehlt sich der Einsatz eines Parallel-Sysplex-Clusters (siehe M 4.221 *Parallel-Sysplex unter z/OS*).
- Es müssen Sicherheitsrichtlinien für das z/OS-System und besonders auch für das Sicherheitssystem RACF (*Resource Access Control Facility*) geplant und festgelegt werden (siehe M 2.288 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*).
- Es müssen Standards für die z/OS-Systemdefinitionen festgelegt werden (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Es sollte ein Rollenkonzept für die Systemverwaltung von z/OS-Systemen eingeführt werden (siehe M 2.295 *Systemverwaltung von z/OS-Systemen*).

**Umsetzung**

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt worden sind, kann die Installation der zSeries-Hardware und des z/OS-Betriebssystems erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:

- Es ist eine sichere Grundkonfiguration der Autorisierungsmechanismen des z/OS-Betriebssystems erforderlich (siehe M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
- Wesentlich für die Absicherung der z/OS-Umgebung ist die entsprechende Konfiguration des Sicherheitssystems (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Für die Umsetzung der z/OS-Steuerung einschließlich der Fernsteuerungskonsole RSF (*Remote Support Facility*) sind die Empfehlungen in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals* zu beachten.

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Die Bereitstellung der Funktionalitäten des z/OS-Betriebssystems setzt einen sicheren Betrieb des z/OS-Betriebssystems voraus (siehe M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*).
- Es müssen die Dienstprogramme abgesichert werden, die zur Unterstützung von betrieblichen Funktionen des z/OS-Betriebssystems dienen und eine hohe Autorisierung benötigen (siehe M 4.215 *Absicherung sicherheitskritischer z/OS-Dienstprogramme*).
- Die erforderlichen Wartungsaktivitäten eines z/OS-Systems sind in der Maßnahme M 2.293 *Wartung von zSeries-Systemen* beschrieben.
- z/OS-Systeme oder Parallel-Sysplex-Cluster müssen im laufenden Betrieb überwacht werden (siehe M 2.292 *Überwachung von z/OS-Systemen*).

**Aussonderung**

Empfehlungen zur Deinstallation von z/OS-Systemen, etwa nach Abschluss des Regelbetriebs, finden sich in der Maßnahme M 2.297 *Deinstallation von z/OS-Systemen*.

**Notfallvorsorge**

Empfehlungen zur Notfallvorsorge finden sich in der Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme*.

**Sicherheitsmanagement und Revision**

Das Sicherheitsmanagement sollte den kompletten Lebenszyklus eines z/OS-Systems begleiten. Die folgenden Punkte sollten besonders beachtet werden:

- Bei der Vergabe und der Revision von Autorisierungen ist zu prüfen, ob die entsprechenden Mitarbeiter diese für ihre Tätigkeit benötigen. Dies gilt besonders für hohe Autorisierungen (siehe Maßnahme M 2.289 *Einsatz restriktiver z/OS-Kennungen*).
- Beim Betrieb eines z/OS-Systems ist regelmäßig zu kontrollieren, ob die Sicherheitsvorgaben eingehalten werden (siehe Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "S/390- und zSeries-Mainframe" vorgestellt.

**Planung und Konzeption**

- M 2.285 (Z) *Festlegung von Standards für z/OS-Systemdefinitionen*
- M 2.286 (Z) *Planung und Einsatz von zSeries-Systemen*
- M 2.287 (Z) *Batch-Job-Planung für z/OS-Systeme*
- M 2.288 (B) *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*
- M 2.295 (A) *Systemverwaltung von z/OS-Systemen*
- M 2.296 (Z) *Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren*
- M 3.39 (W) *Einführung in die zSeries-Plattform*
- M 3.40 (W) *Einführung in das z/OS-Betriebssystem*
- M 3.41 (W) *Einführung in Linux und z/VM für zSeries-Systeme*
- M 4.221 (C) *Parallel-Sysplex unter z/OS*

**Umsetzung**

- M 2.289 (A) *Einsatz restriktiver z/OS-Kennungen*
- M 2.290 (Z) *Einsatz von RACF-Exits*
- M 3.42 (A) *Schulung des z/OS-Bedienungspersonals*
- M 4.207 (A) *Einsatz und Sicherung systemnaher z/OS-Terminals*
- M 4.208 (B) *Absichern des Start-Vorgangs von z/OS-Systemen*
- M 4.209 (A) *Sichere Grundkonfiguration von z/OS-Systemen*
- M 4.211 (A) *Einsatz des z/OS-Sicherheitssystems RACF*
- M 4.212 (Z) *Absicherung von Linux für zSeries*
- M 4.213 (A) *Absichern des Login-Vorgangs unter z/OS*
- M 4.216 (C) *Festlegung der Systemgrenzen von z/OS*

- M 4.217 (C) *Workload Management für z/OS-Systeme*
- M 4.219 (C) *Lizenzschlüssel-Management für z/OS-Software*
- M 4.220 (B) *Absicherung von Unix System Services bei z/OS-Systemen*
- M 5.113 (Z) *Einsatz des VTAM Session Management Exit unter z/OS*
- M 5.114 (B) *Absicherung der z/OS-Tracefunktionen*

**Betrieb**

- M 2.291 (C) *Sicherheits-Berichtswesen und -Audits unter z/OS*
- M 2.292 (B) *Überwachung von z/OS-Systemen*
- M 2.293 (C) *Wartung von zSeries-Systemen*
- M 2.294 (Z) *Synchronisierung von z/OS-Passwörtern und RACF-Kommandos*
- M 4.210 (B) *Sicherer Betrieb des z/OS-Betriebssystems*
- M 4.214 (B) *Datenträgerverwaltung unter z/OS-Systemen*
- M 4.215 (B) *Absicherung sicherheitskritischer z/OS-Dienstprogramme*
- M 4.218 (Z) *Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen*

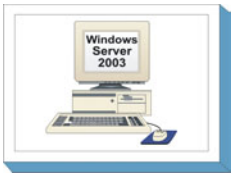
**Aussonderung**

- M 2.297 (B) *Deinstallation von z/OS-Systemen*

**Notfallvorsorge**

- M 6.93 (A) *Notfallvorsorge für z/OS-Systeme*

# B 3.108 Windows Server 2003




## Beschreibung

Das Software-Paket Windows Server 2003 ist das Nachfolgeprodukt zum Betriebssystem Windows 2000 Server. Windows Server 2003 ist in den Varianten *Standard Edition,Enterprise Edition*, *Web Edition* und *Datacenter Edition* erhältlich. Besonders weit verbreitet ist hierbei die Standard-Edition. Die Web-Edition bildet eine Teilmenge der Standard-Edition, die Enterprise-Edition enthält zusätzliche Funktionen, die nur in großen Umgebungen oder bei speziellen Anforderungen zum Einsatz kommen. Dazu gehören unter anderem die Funktionen *Fail-over-Cluster*, vollständige Terminalserver, netzgestützte UDDI-Datenbanken, unbegrenzte VPN- und RADIUS-Verbindungen, neue Zertifikatsdienste und der *Windows System Resource Manager* (WSRM). Jede dieser Editionen ist auch in einer 64-Bit-Version verfügbar, die sich in ihrem Funktionsumfang nicht signifikant von den 32-Bit-Versionen unterscheidet.

### Abgrenzung des Bausteins

Der Baustein *Windows Server 2003* bezieht sich in der Regel auf die Funktionen der Standard-Edition inklusive Service Pack 1. Er kann jedoch auch problemlos auf die Varianten Web-Edition und Enterprise-Edition angewendet werden. Andere Editionen wie z. B. die Datacenter-Edition und Windows Small Business Server 2003 enthalten zusätzliche, anwendungsspezifische Funktionalitäten, die hier nicht betrachtet werden.

Die vielfältigen Einsatzmöglichkeiten erfordern eine differenzierte Betrachtung und damit eine inhaltliche Abgrenzung dieses Bausteins. Windows Server 2003 kann einerseits als reine Plattform für zusätzlich erhältliche Serverapplikationen dienen und andererseits mit den vielen im Lieferumfang von Windows Server 2003 enthaltenen Applikationen für bestimmte Bereiche ein vollständiges Gesamtsystem bilden.

Die Aktivierung einiger Funktionen ist nur bei bestimmten Anwendungsszenarien eines Windows-Server 2003 Systems notwendig. Für solche Anwendungsszenarien werden in diesem Baustein übergreifende Rahmenaspekte erläutert. Betroffen sind u. a. die Funktionen *Network Load Balancing* (NLB), Hochverfügbarkeitscluster, *Application Server*, *Role Based Access Control* (RBAC), *Zertifikatdienste* (PKI) sowie *Routing und RAS*.

Sollte der Windows Server 2003 die Rolle eines Domänen Controller in einer Active Directory Gesamtstruktur übernehmen, so ist der Baustein B 5.16 *Active Directory* gemäß der Modellierungsanweisung anzuwenden.

Nicht näher betrachtet werden kostenlos von Microsoft erhältliche Zusatzpakete, die nicht im Standard-Lieferumfang enthalten sind. Hierzu zählen beispielsweise *Windows Sharepoint Services* (WSS), *Windows Software Update Service* (WSUS), *Rights Management Service* (RMS) oder *Microsoft Shared Computer Toolkit*.

Die folgenden mitgelieferten Komponenten werden ebenfalls nicht betrachtet, da ihr Einsatz die Berücksichtigung vieler nicht allgemeingültiger Aspekte erfordert:

- Windows Media Services
- Terminalserver

## Gefährdungslage

Für den IT-Grundschutz eines servergestützten Netzes unter dem Betriebssystem Windows Server 2003 werden die folgenden typischen Gefährdungen angenommen:

### Organisatorische Mängel

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*

- G 2.111 *Kompromittierung von Anmeldedaten bei Dienstleisterwechsel*
- G 2.114 *Uneinheitliche Windows-Server-Sicherheitseinstellungen bei SMB, RPC und LDAP*
- G 2.115 *Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen ab Windows Server 2003*
- G 2.116 *Datenverlust beim Kopieren oder Verschieben von Daten ab Windows Server 2003*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.48 *Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen*
- G 3.56 *Fehlerhafte Einbindung des IIS in die Systemumgebung*
- G 3.81 *Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003*

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*
- G 4.55 *Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP*

**Vorsätzliche Handlungen**

- G 5.7 *Abhören von Leitungen*
- G 5.52 *Missbrauch von Administratorrechten bei Windows-Betriebssystemen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.79 *Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.132 *Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003*
- G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Alle Überlegungen zu einem Windows Server 2003 sollten auf den im Baustein B 3.101 *Allgemeiner Server* enthaltenen Maßnahmen basieren. Die dort beschriebenen allgemeinen Maßnahmen werden im vorliegenden Baustein konkretisiert und ergänzt.

Server und Clients bilden eine Funktionseinheit. Daher muss auch der Baustein B 3.201 *Allgemeiner Client* und die darauf aufbauenden Betriebssystem-spezifischen Bausteine im Zusammenhang mit diesem Baustein beachtet werden.

**Planung und Konzeption**

Ist die allgemeine Planung des Servereinsatzes abgeschlossen und die Wahl des Betriebssystems auf Windows Server 2003 gefallen, müssen Teilkonzepte für den Servereinsatz unter Berücksichtigung aller geltenden übergeordneten Konzepte und Richtlinien erstellt werden. Die generelle Vorgehensweise bei der Planung wird in M 2.315 *Planung des Servereinsatzes* erläutert.

Für die darin genannten Themengebiete sind die spezifischen Empfehlungen aus den Maßnahmen M 4.276 *Planung des Einsatzes von Windows Server 2003* und M 2.364 *Planung der Administration ab Windows 2003* zu entnehmen.

Während der Planung müssen wichtige Entscheidungen über grundlegende Infrastrukturdienste gefällt werden. Maßgeblich ist M 5.152 *Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste*. In die Entscheidungen hinsichtlich der Konzeption der Infrastrukturdienste fließen die geplanten Rollen und die Hinweise aus den Hilfsmitteln zum IT-Grundschutz (siehe *DNS/WINS/DHCP als Infrastrukturdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) ein.

Zu planen sind weiterhin die Kommunikationsprotokolle des Servers (M 4.277 *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern*, M 5.131 *Absicherung von IP-Protokollen unter Windows Server 2003*).

Weitere übergreifende Funktionen können die Sicherheit des Servers erhöhen, z. B. WebDAV und *Encrypting File System* (EFS) (siehe M 5.132 *Sicherer Einsatz von WebDAV unter Windows Server 2003*, M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*), Netzwerklastenausgleich (*Network Load Balancing*, NLB), IPSec, Benutzerauthentisierung mittels Smart Card und andere. Hierbei sollten auch M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server*, M 4.279 *Erweiterte Sicherheitsaspekte für Windows Server 2003* beachtet werden.

Bei allen bisher genannten Schritten sind die Grundsätze aus M 5.10 *Restriktive Rechtevergabe* und M 5.9 *Protokollierung am Server* zu berücksichtigen. Spezifische Hilfestellungen geben M 2.370 *Administration der Berechtigungen ab Windows Server 2003* und M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*. Die dort genannten Empfehlungen für den Betrieb des Servers sollten auch schon bei der Planung von Berechtigungskonzepten berücksichtigt werden.

Im Rahmen der Planung des Servers sollte eine Sicherheitsrichtlinie erstellt und/oder bestehende Richtlinien ergänzt werden. Bei allen bisher genannten Schritten ergeben sich in Abhängigkeit von Einsatzzweck und Nutzdaten kritische Aspekte sowie individuelle Lösungen und Verfahrensweisen. Diese werden gesammelt. Dann wird anhand der individuellen Situation und Organisationsstruktur des Unternehmens oder der Behörde überlegt, welche Aspekte den Sicherheitsrichtlinien hinzugefügt werden sollen. Die Maßnahme M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server* schildert eine geeignete Herangehensweise.

**Beschaffung**

Nach Abschluss der konzeptionellen Planungsarbeiten und der Definition der Beschaffungskriterien für einen Server (siehe M 2.317 *Beschaffungskriterien für einen Server*) sollte in Abhängigkeit der Anzahl der zu beschaffenden Server ein geeignetes Lizenzmodell ausgewählt werden. Die Hilfsmittel zum IT-Grundschutz bieten hierbei Hilfestellung (siehe *Auswahl geeigneter Lizenzierungsmethoden für Windows XP/Server 2003* in *Hilfsmittel zum Windows Server 2003*).

**Umsetzung**

Nach der Planung von sicherheitsrelevanten Maßnahmen für Windows Server 2003 müssen diese im Rahmen der Umsetzung bzw. Installation und Konfiguration des Windows Server 2003 Systems realisiert werden.

Zur Gewährleistung eines angemessenen Sicherheitsniveaus sollten bei der Umsetzung (und später auch im Betrieb) eines Windows-Server-2003-Systems die folgenden Prämissen beachtet werden:

- Die Funktionalität ist auf die geplante und unbedingt benötigte zu reduzieren (auch im Hinblick auf Clients, die auf den Server zugreifen), um die Angriffsfläche zu minimieren und die Zahl von (potenziellen) Schwachstellen zu verringern (M 4.285 *Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003* sowie M 4.286 *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003* und M 4.284 *Umgang mit Diensten ab Windows Server 2003*).
- Die Konfiguration ist im Hinblick auf Sicherheit und Erfüllung der Aufgabe des Servers zu optimieren (Härten des Servers), so dass nur die tatsächlich notwendige Abwärtskompatibilität und Offenheit des Systems gegeben ist (M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* sowie M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003* und M 4.48 *Passwortschutz unter Windows-Systemen*).
- Es muss eine aktuelle und angemessene Dokumentation erstellt werden, die den Sicherheitsprozess bestmöglich unterstützt.

In der Maßnahme M 4.280 Sichere Basiskonfiguration von Windows Server 2003 sind eine Reihe von kleineren Funktionen sowie grundsätzliche Vorgehensweisen bei der Umsetzung erläutert, mit denen die oben genannten Prämissen erfüllt werden können.

Zur Installation und Konfiguration sollten Hilfsprogramme, sogenannte Assistenten, bevorzugt werden. Manuelle Einstellungen sollten nur wenn unbedingt notwendig vorgenommen werden. So wird einerseits Fehlkonfigurationen vorgebeugt und andererseits die Dokumentation vereinfacht (z. B.: "Assistent mit Standardeinstellungen sowie folgenden drei abweichenden Einstellungen konfiguriert..."). Administrative Hilfsmittel wie Vorlagen und Skripte (M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* und M 2.367 *Einsatz von Kommandos und Skripten ab Windows Server 2003*) unterstützen die Standardisierung und Dokumentation.

Sofern der Server neu aufgesetzt wird, fließen alle bisher genannten Schritte bei der Installation und Bereitstellung des Servers zusammen. Um hierfür einen sicheren und zuverlässigen Prozess zu etablieren, sollte M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003* umgesetzt werden.

**Betrieb**

Im Regelbetrieb ist neben der Gewährleistung einer aktuellen Dokumentation insbesondere der Umgang mit administrativen Vorlagen und die Administration der Berechtigungen von Bedeutung (M 2.368 *Umgang mit administrativen Vorlagen unter Windows ab Server 2003* und M 2.370 *Administration der Berechtigungen ab Windows Server 2003*).

Die Aufrechterhaltung der Sicherheit wird neben den im Baustein B 3.101 *Allgemeiner Server*, genannten Maßnahmen M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes* für einen Windows Server 2003 durch die Maßnahme M 2.369 *Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003* ergänzt bzw. konkretisiert.

**Aussonderung**

Zur geregelten Aussonderung eines Windows Servers 2003 sollten generell die im Baustein B 3.101 *Allgemeiner Server* beschriebenen Maßnahmenempfehlungen berücksichtigt werden. Zusätzlich ist in Bezug auf die Deaktivierung bzw. Löschung von einzelnen Konten die Maßnahme M 2.371 *Geregelte Deaktivierung und Löschung ungenutzter Konten* zu beachten.

**Notfallvorsorge**

Aspekte der Notfallplanung für einen Windows Server 2003 werden in den Maßnahmen M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server* und M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen* thematisiert.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Windows Server 2003" vorgestellt.

**Planung und Konzeption**

- M 2.232 (C) *Planung der Windows-CA-Struktur ab Windows 2000*
- M 2.364 (A) *Planung der Administration ab Windows 2003*
- M 2.365 (A) *Planung der Systemüberwachung unter Windows Server 2003*
- M 4.276 (A) *Planung des Einsatzes von Windows Server 2003*
- M 4.277 (C) *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern*
- M 4.278 (Z) *Sichere Nutzung von EFS unter Windows Server 2003*
- M 4.279 (Z) *Erweiterte Sicherheitsaspekte für Windows Server 2003*
- M 5.131 (A) *Absicherung von IP-Protokollen unter Windows Server 2003*
- M 5.132 (B) *Sicherer Einsatz von WebDAV unter Windows Server 2003*

**Umsetzung**

- M 2.366 (B) *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*
- M 2.367 (C) *Einsatz von Kommandos und Skripten ab Windows Server 2003*
- M 4.48 (A) *Passwortschutz unter Windows-Systemen*
- M 4.52 (A) *Geräteschutz unter NT-basierten Windows-Systemen*
- M 4.280 (A) *Sichere Basiskonfiguration ab Windows Server 2003*
- M 4.281 (A) *Sichere Installation und Bereitstellung von Windows Server 2003*
- M 4.282 (B) *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003*
- M 4.283 (B) *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003*
- M 4.284 (B) *Umgang mit Diensten ab Windows Server 2003*

- M 4.285 (A) *Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003*
- M 4.286 (A) *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003*
- M 5.90 (Z) *Einsatz von IPSec unter Windows*

**Betrieb**

- M 2.368 (C) *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*
- M 2.369 (A) *Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003*
- M 2.370 (A) *Administration der Berechtigungen ab Windows Server 2003*
- M 4.56 (C) *Sicheres Löschen unter Windows-Betriebssystemen*

**Aussonderung**

- M 2.371 (A) *Geregelte Deaktivierung und Löschung ungenutzter Konten*

**Notfallvorsorge**

- M 6.76 (C) *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*
- M 6.99 (A) *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server*

# B 3.109 Windows Server 2008


## Beschreibung

Mit Windows Server 2008 hat Microsoft ein Serverbetriebssystem auf den Markt gebracht, dass in Bezug auf die Sicherheit deutliche Verbesserungen gegenüber den Vorgängerversionen mitbringt. Mit dem Release Windows Server 2008 R2 sind weitere Verbesserungen und Erweiterungen verfügbar, die Windows 2008 zum Pendant zu Windows 7 auf der Clientseite machen.

Windows Server 2008 kann als Betriebssystem für Server mit unterschiedlichen Aufgaben eingesetzt werden, vom Windows-Domänencontroller über Active Directory Server und Datenbankserver bis hin zu Anwendungsservern oder Infrastrukturdiensten wie DHCP, DNS oder VPN. Nicht alle Funktionen müssen aktiviert werden, die Auswahl hängt von den Anwendungsszenarien ab. Dieser Baustein kann nicht alle Einsatzszenarien im Detail betrachten, sondern beschränkt sich auf die gemeinsame Betriebssystemplattform und wesentliche, übergreifende Sicherheitsfunktionen.

Dieser Baustein ist immer dann anzuwenden, wenn Windows Server 2008 als Betriebssystem verwendet wird, auch in der Ausführung als Windows Server Core. Mit Hilfe von Windows Server 2008 realisierte Dienste müssen unabhängig davon durch geeignete Bausteine der Schicht 5 (Anwendungen) oder durch eine ergänzende Risikoanalyse abgedeckt werden.

Soweit in diesem Baustein und den dazugehörigen Maßnahmen und Gefährdungen von Windows Server 2008 die Rede ist, schließt dies auch die Version R2 ein. Änderungen und Besonderheiten in R2 sind jeweils explizit ausgewiesen.

## Gefährdungslage

Die folgenden Gefährdungen sind beim Einsatz eines Servers mit dem Betriebssystem Windows Server 2008 relevant:

### Organisatorische Mängel

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.111 *Kompromittierung von Anmeldedaten bei Dienstleisterwechsel*
- G 2.114 *Uneinheitliche Windows-Server-Sicherheitseinstellungen bei SMB, RPC und LDAP*
- G 2.115 *Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen ab Windows Server 2003*
- G 2.116 *Datenverlust beim Kopieren oder Verschieben von Daten ab Windows Server 2003*
- G 2.156 *Kompatibilitätsprobleme beim Anheben der Active Directory-Funktionsebene*

### Menschliche Fehlhandlungen

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.27 *Fehlerhafte Zeitsynchronisation*
- G 3.48 *Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen*
- G 3.81 *Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003*
- G 3.97 *Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista*
- G 3.98 *Verlust von BitLocker-verschlüsselten Daten*

### Technisches Versagen

- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*
- G 4.55 *Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP*

**Vorsätzliche Handlungen**

- G 5.7 *Abhören von Leitungen*
- G 5.52 *Missbrauch von Administratorrechten bei Windows-Betriebssystemen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.79 *Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.132 *Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003*
- G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*

**Maßnahmenempfehlungen**

Die hier beschriebenen Maßnahmen ergänzen die Maßnahmen aus dem Baustein B 3.101 *Allgemeiner Server* um spezifische Aspekte für Server unter dem Betriebssystem Windows Server 2008. Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

**Planung und Konzeption**

Eine sorgfältige Planung ist für jeden eingesetzten Server unverzichtbar. In M 4.418 *Planung des Einsatzes von Windows Server 2008* sind die grundlegenden Empfehlungen hierfür zusammengefasst. Neuerungen gegenüber früheren Server-Betriebssystemen von Microsoft beschreibt M 4.408 *Übersicht über neue, sicherheitsrelevante Funktionen in Windows Server 2008*.

Im betrieblichen Umfeld werden üblicherweise Volumenlizenzverträge für die Beschaffung von Windows-Servern genutzt. Für die damit verbundene Aktivierung müssen die richtigen Voraussetzungen geschaffen werden, um die Verfügbarkeit der Systeme sicherzustellen (siehe M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*). Dazu gehört auch, die Reaktivierung vorzubereiten, die insbesondere nach Konfigurationsänderungen erforderlich werden kann (M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

Für einen sicheren Betrieb des Systems sind weitere Aspekte bereits in der Planungsphase zu berücksichtigen, von allgemeinen Festlegungen zur Systemadministration (M 2.364 *Planung der Administration ab Windows 2003*) über die Gruppenrichtlinien (M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*) bis hin zur Einbindung in eine Systemüberwachung (M 2.489 *Planung der Systemüberwachung unter Windows Server 2008*).

Je nach dem vorgesehenen Einsatzgebiet des Servers müssen weitere Aspekte geplant werden, z. B. für eine organisationseigene Public-Key-Infrastruktur (M 2.232 *Planung der Windows-CA-Struktur ab Windows 2000*) oder im Rahmen von Windows-basierten Virtualisierungslösungen (M 2.490 *Planung des Einsatzes von Virtualisierung mit Hyper-V*).

**Beschaffung**

Bevor ein Windows 2008 Serversystem beschafft wird, müssen dessen Anforderungen geklärt werden. Dies umfasst nicht nur die Hardware-Anforderungen, sondern es ist auch die richtige Edition auszuwählen (M 4.409 *Beschaffung von Windows Server 2008*) und die erforderliche Infrastruktur für die Aktivierung zu berücksichtigen (M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

**Umsetzung**

Um das Betriebssystem aufzusetzen, helfen die vom Hersteller bereitgestellten Vorlagen (M 2.491 *Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008*). Auf dieser Grundlage muss eine sichere Basiskonfiguration erstellt werden (M 4.280 *Sichere Basiskonfiguration ab Windows Server 2003*). Hierfür können, anders als bei früheren Windows Server-Versionen, weitgehend die Standardeinstellungen übernommen werden. Sofern durch Windows Server 2008 ein älteres Windows-Betriebssystem ersetzt wird, muss eine entsprechende Migrationsplanung erfolgen und umgesetzt werden (M 4.412 *Sichere Migration von Windows Server 2003 auf Server 2008*).

Wie schon bei früheren Windows Server-Versionen ist auch der Schutz der lokal angeschlossenen Geräte (M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen*), der Einsatz von Skripten und Skript-Umgebungen (M 2.367 *Einsatz von Kommandos und Skripten ab Windows Server 2003*), die Konfiguration der Systemdienste (M 4.284 *Umgang mit Diensten ab Windows Server 2003*) sowie ein ausreichender Passwortschutz (M 4.48 *Passwortschutz unter Windows-Systemen*) wichtig.

Für das Dateisystem ist festzulegen, ob eine Protokollierung des jeweils letzten Dateizugriffs genutzt werden soll. Diese Protokollierung erleichtert die Aufklärung von Sicherheitsvorfällen, kann aber negativen Einfluss auf die Performance haben und muss daher abgewogen werden (M 4.342 *Aktivierung des Last Access Zeitstempels ab Windows Vista*). Neue Funktionen wie die Benutzerkontensteuerung (M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*) und die Möglichkeit zum Integritätsschutz (M 4.341 *Integritätsschutz ab Windows Vista*) können für eine, im Vergleich zu früheren Versionen, verbesserte Systemsicherheit sorgen und sollten daher genutzt werden. Wird der Server als Active Directory eingesetzt, sind auch die Erläuterungen zu beachten, die in M 4.414 *Überblick über Neuerungen für Active Directory ab Windows Server 2008* zusammengestellt sind.

Bei erhöhtem Schutzbedarf empfehlen sich erweiterte Schutzmaßnahmen wie beispielsweise die Einrichtung von eingeschränkten Benutzerumgebungen (M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*), zusätzliche Maßnahmen zur Absicherung der Netzkommunikation (M 4.277 *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern* oder M 5.90 *Einsatz von IPSec unter Windows*) oder die Anwendungssteuerung mit dem Werkzeug AppLocker (M 4.419 *Anwendungssteuerung ab Windows 7 mit AppLocker*). Für die Verschlüsselung von Daten stehen Mechanismen auf Datenträger- und auf Dateisystemebene bereit (M 4.337 *Einsatz von BitLocker Drive Encryption* und M 4.147 *Sichere Nutzung von EFS unter Windows*).

**Betrieb**

Die wichtigsten regelmäßigen Betriebsaufgaben sind in M 2.369 *Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003* zusammengefasst und werden ergänzt durch die sichere Administration der Benutzerkonten und Berechtigungen (M 2.370 *Administration der Berechtigungen ab Windows Server 2003*). Das System sollte gezielt überwacht werden, damit Verfügbarkeitsprobleme und Sicherheitsvorfälle schnell erkannt werden (M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*).

Wie für alle IT-Systeme ist auch für Windows-Server ein funktionierendes Patch-Management ein zentrales Element für den Erhalt der Systemsicherheit. Hierfür steht mit den Windows Server Update Services (WSUS) ein Werkzeug von Microsoft selbst bereit (M 4.417 *Patch-Management mit WSUS ab Windows Server 2008*).

Benutzer und Administratoren des Servers müssen die Besonderheiten beim Löschen von Dateien beachten (M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*). Mit den neuen Möglichkeiten zur biometrischen Authentisierung per Fingerabdruck steht außerdem eine Alternative zur Passworteingabe bereit (M 4.415 *Sicherer Betrieb der biometrischen Authentisierung unter Windows*).

**Aussonderung**

Bei der Aussonderung von Windows-Servern sind die im Baustein B 3.101 *Allgemeiner Server* beschriebenen Maßnahmen umzusetzen. Zusätzlich müssen die einzelnen Konten deaktiviert bzw. gelöscht werden (M 2.371 *Geregelte Deaktivierung und Löschung ungenutzter Konten*).

**Notfallvorsorge**

Wie für alle anderen zentralen IT-Systeme muss auch für Windows-Server eine geeignete Notfallplanung erstellt werden (M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*). Ein zentrales Element der Notfallvorsorge ist die Datensicherung, die auch relevante Bereiche des Betriebssystems mit einbeziehen muss (M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server*). Bei erhöhten Anforderungen an die Verfügbarkeit kann über Redundanzen eine zusätzliche Vorsorge getroffen werden (M 6.43 *Einsatz redundanter Windows-Server*).

**Planung und Konzeption**

- M 2.232 (C) *Planung der Windows-CA-Struktur ab Windows 2000*
- M 2.326 (A) *Planung der Gruppenrichtlinien für Clients ab Windows XP*
- M 2.364 (A) *Planung der Administration ab Windows 2003*
- M 2.489 (A) *Planung der Systemüberwachung unter Windows Server 2008*
- M 2.490 (C) *Planung des Einsatzes von Virtualisierung mit Hyper-V*
- M 4.147 (Z) *Sichere Nutzung von EFS unter Windows*
- M 4.277 (C) *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern*
- M 4.336 (A) *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.337 (Z) *Einsatz von BitLocker Drive Encryption*
- M 4.340 (A) *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*
- M 4.341 (A) *Integritätsschutz ab Windows Vista*
- M 4.342 (Z) *Aktivierung des Last Access Zeitstempels ab Windows Vista*
- M 4.408 (W) *Übersicht über neue, sicherheitsrelevante Funktionen in Windows Server 2008*
- M 4.414 (W) *Überblick über Neuerungen für Active Directory ab Windows Server 2008*
- M 4.418 (A) *Planung des Einsatzes von Windows Server 2008*

**Beschaffung**

- M 4.409 (W) *Beschaffung von Windows Server 2008*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 2.367 (C) *Einsatz von Kommandos und Skripten ab Windows Server 2003*
- M 2.491 (B) *Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008*
- M 4.48 (A) *Passwortschutz unter Windows-Systemen*
- M 4.52 (A) *Geräteschutz unter NT-basierten Windows-Systemen*
- M 4.280 (A) *Sichere Basiskonfiguration ab Windows Server 2003*
- M 4.284 (B) *Umgang mit Diensten ab Windows Server 2003*
- M 4.410 (Z) *Einsatz von Netzwerkzugriffsschutz unter Windows*
- M 4.412 (Z) *Sichere Migration von Windows Server 2003 auf Server 2008*
- M 4.413 (Z) *Sicherer Einsatz von Virtualisierung mit Hyper-V*
- M 4.419 (Z) *Anwendungssteuerung ab Windows 7 mit AppLocker*
- M 5.90 (Z) *Einsatz von IPSec unter Windows*

**Betrieb**

- M 2.368 (C) *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*
- M 2.369 (A) *Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003*
- M 2.370 (A) *Administration der Berechtigungen ab Windows Server 2003*
- M 4.56 (C) *Sicheres Löschen unter Windows-Betriebssystemen*
- M 4.343 (Z) *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.344 (B) *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*
- M 4.411 (Z) *Sichere Nutzung von DirectAccess unter Windows*
- M 4.415 (Z) *Sicherer Betrieb der biometrischen Authentisierung unter Windows*
- M 4.416 (Z) *Einsatz von Windows Server Core*
- M 4.417 (B) *Patch-Management mit WSUS ab Windows Server 2008*

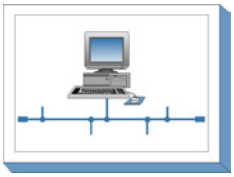
**Aussonderung**

- M 2.371 (A) *Geregelte Deaktivierung und Löschung ungenutzter Konten*
- M 2.410 (B) *Geregelte Außerbetriebnahme eines Verzeichnisdienstes*

**Notfallvorsorge**

- M 6.43 (Z) *Einsatz redundanter Windows-Server*
- M 6.76 (C) *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*
- M 6.99 (A) *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server*

# B 3.201 Allgemeiner Client



## Beschreibung

Betrachtet wird ein IT-System mit einem beliebigen Betriebssystem, das die Trennung von Benutzern zulässt (es sollte mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können). Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben.

Das IT-System kann auf einer beliebigen Plattform betrieben werden, es kann sich dabei um einen PC mit oder ohne Festplatte, aber auch um eine Unix-Workstation oder einen Apple Macintosh handeln. Das IT-System kann über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist.

Dieser Baustein bietet einen Überblick über Gefährdungen und Sicherheitsmaßnahmen, die für alle Clients unabhängig von der verwendeten Plattform und vom eingesetzten Betriebssystem zutreffen. Je nach dem eingesetzten Betriebssystem sind zusätzlich die weiterführenden Bausteine der IT-Grundschutz-Kataloge zu beachten.

## Gefährdungslage

Für den IT-Grundschutz eines allgemeinen Clients werden folgende Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.24 *Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.147 *Fehlende Zentralisierung durch Peer-to-Peer*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.17 *Kein ordnungsgemäßer PC-Benutzerwechsel*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.23 *Automatische Erkennung von Wechseldatenträgern*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.23 *Schadprogramme*
- G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon und Kamera*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz von Arbeitsplatzrechnern sollten im Hinblick auf die Informationssicherheit von Clients folgende Schritte durchlaufen werden:

**Planung des Einsatzes von Clients**

Für die sichere Nutzung von IT-Systemen müssen vorab die Rahmenbedingungen festgelegt werden. Dabei müssen die Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die geplanten Einsatzszenarien von Anfang an mit einbezogen werden (siehe M 2.321 *Planung des Einsatzes von Client-Server-Netzen*). Schon vor der Beschaffung der Rechner und Software sollte eine Sicherheitsrichtlinie für die Clients erstellt werden (siehe M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*).

Übergreifende Fragen der sicheren Nutzung von IT-Systemen werden im Baustein B 1.9 *Hard- und Software-Management* betrachtet.

**Beschaffung**

Für die Beschaffung von Clients, die typischerweise in größeren Mengen erfolgt, müssen ausgehend von den Einsatzszenarien Kriterien für die Auswahl geeigneter Produkte formuliert werden (siehe hierzu B 1.10 *Standardsoftware*). Auch bei der Beschaffung von Einzelsystemen ist es wichtig, dass das System zur vorhandenen Struktur passt, damit nicht für ein einzelnes System wegen dessen Besonderheiten ein unangemessen hoher Aufwand bei Integration und Betrieb entsteht.

Falls Hard- oder Software nicht die festgelegten Sicherheitsanforderungen erfüllen, sind weitere Maßnahmen erforderlich. Diese können organisatorischer Art sein (beispielsweise durch Regelungen, dass der Client ausschließlich hinter verschlossener Bürotür betrieben werden darf) oder es können Zusatzkomponenten beschafft werden, um die identifizierten Mankos auszugleichen.

Bei besonders hohen Anforderungen an die Verfügbarkeit der Clients ist für diese der Einsatz einer Unterbrechungsfreien Stromversorgung (USV) empfehlenswert. Dabei kann es sich beispielsweise um eine "Einzelplatz-USV" handeln, falls die hohen Anforderungen nur für einzelne Clients gelten, oder aber um einen eigenen entsprechend abgesicherten Stromkreis ("rote Steckdose"). Weitere Informationen finden sich in M 1.28 *Lokale unterbrechungsfreie Stromversorgung*.

**Umsetzung**

Um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen, sind eine sorgfältige Auswahl der Betriebssystem- und Softwarekomponenten, eine sichere Installation und sorgfältige Konfiguration wichtig. Die dabei zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem. Näheres dazu findet sich deswegen in spezifischen Bausteinen, beispielsweise in B 3.204 *Client unter Unix* oder B 3.210 *Client unter Windows Vista*.

- **Sichere Installation**
  Der Grundstein für die Sicherheit wird bereits bei der Vorbereitung der Installation gelegt. Vor der Installation sollte festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Die getroffenen Entscheidungen müssen so dokumentiert werden, dass gegebenenfalls nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für das System gewählt wurde (siehe M 4.237 *Sichere Grundkonfiguration eines IT-Systems*).
  Für die Installation sollten nur Installationsmedien benutzt werden, die aus einer sicheren Quelle stammen (beispielsweise direkt vom Hersteller oder Distributor des Betriebssystems oder Programms). Die Installation des Betriebssystems sollte wenn möglich durchgeführt werden, ohne dass das System an das Netz angeschlossen ist (Offline-Installation). Falls bei der Installation Teile der Pakete über das Netz geladen werden sollen, sollte für die Installation ein eigenes Netz (Testnetz) genutzt werden, das vom übrigen Netz getrennt ist. Von einem Nachladen von Paketen über das

Internet wird dringend abgeraten. Falls es in Ausnahmefällen erforderlich ist, ein System direkt im Produktionsnetz zu installieren, so muss durch geeignete zusätzliche Maßnahmen sichergestellt werden, dass auf das System während der Installation nicht von außen zugegriffen werden kann.
Bereits im Verlauf der Installation werden meist einige Grundeinstellungen zur Systemkonfiguration (unterschiedlich je nach Betriebssystem) vorgenommen.

- **Sichere Konfiguration**
  An die eigentliche Installation schließt sich die Grundkonfiguration eines Clients an. In dieser Phase wird die vorläufige Konfiguration, wie sie im Verlauf der Installation vom Installationsprogramm eingerichtet wurde, an die tatsächlichen Gegebenheiten und Anforderungen des Informationsverbunds angepasst, in dem der Client eingesetzt werden soll. Oft werden dabei weitere Programme installiert oder es werden Programme aus einer Standardkonfiguration entfernt, die Einstellungen für den Zugriff auf das Netz werden festgelegt und der Client wird für den Zugriff auf Verzeichnisdienste oder ähnliches konfiguriert. Außerdem werden nicht benötigte Benutzer-Kennungen gelöscht oder deaktiviert, und die Benutzer-Kennungen für die eigentlichen Benutzer werden angelegt.
  In dieser Phase werden auch die benötigten Anwendungsprogramme installiert und konfiguriert. Für die Installation und Konfiguration der Anwendungsprogramme sind analoge Sicherheitsaspekte wie für die Installation des Betriebssystems selbst zu beachten.
  Falls eine größere Anzahl ähnlich konfigurierter Clients installiert und konfiguriert werden soll, so bietet es sich an, dies nicht für jeden Client einzeln durchzuführen, sondern eine "generische" Installation zu erstellen, die anschließend auf die einzelnen Clients übertragen wird, und an der nur noch minimale Änderungen vor der Inbetriebnahme erforderlich sind. Eine solche generische Konfiguration kann erheblich zur Effizienz beitragen und das Risiko von Fehlern verringern helfen. Andererseits ist bei der Erstellung der Referenzinstallation besondere Sorgfalt erforderlich. Die vorgenommenen Einstellungen müssen nachvollziehbar dokumentiert sein.
  Ein wichtiger Grundsatz bei der Konfiguration von Clients ist, dass normale Bedienungsfehler der Anwender zu keinen gravierenden Schäden am System und an Daten anderer Benutzer führen sollten, und dass Anwender nicht durch einfache Neugierde Zugriff auf Informationen erlangen dürfen, die nicht für sie bestimmt sind. Mehr dazu findet sich in M 4.237 *Sichere Grundkonfiguration eines IT-Systems*.
  Nachdem der Client fertig konfiguriert ist, kann der Rechner an die Anwender übergeben werden. Falls die Anwender keine ausreichenden Kenntnisse des eingesetzten Betriebssystems, einzelner Anwendungsprogramme oder Tools besitzen, so müssen sie vorab geschult werden. Allgemeine Aspekte hierzu finden sich im Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit*.

**Betrieb**

Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist es, die Systeme durch die Installation und permanente Aktualisierung eines Virenscanners (siehe dazu auch B 1.6 *Schutz vor Schadprogrammen*) zu schützen. Daneben ist eine regelmäßige Datensicherung (siehe auch B 1.4 *Datensicherungskonzept*) eine grundlegende Voraussetzung dafür, dass Hardwaredefekte und Programm- oder Benutzerfehler nicht zu gravierenden Datenverlusten führen.

Ein Mittel zur Erkennung von Angriffen oder missbräuchlicher Nutzung ist die Überwachung des Systems. Dafür relevante Maßnahmen finden sich in M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes* sowie im Baustein B 1.9 *Hard- und Software-Management*.

Auch bei Clients ist es wichtig, dass die Administration auf sicheren Wegen erfolgt und dass die Arbeit der Administratoren nachvollziehbar ist. Die entsprechenden Aspekte sind in M 4.234 *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern* beschrieben.

**Aussonderung**

Bei der Aussonderung eines Clients muss zunächst sichergestellt werden, dass alle Benutzerdaten gesichert oder auf ein Ersatzsystem übertragen werden. Anschließend muss dafür gesorgt werden, dass keine sensitiven Daten auf den Festplatten des Rechners zurück bleiben. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder ein reines logisches Löschen noch das Neuformatieren der Platten

mit den Mitteln des installierten Betriebssystems die Daten wirklich von den Festplatten entfernt. Mit geeigneter Software können Daten, die auf diese Weise gelöscht wurden wieder rekonstruiert werden, oft sogar ohne großen Aufwand. Hinweise zum sicheren Löschen finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*. Nach der Aussonderung eines Clients müssen Bestandsverzeichnisse und Netzpläne aktualisiert werden.

**Notfallvorsorge**

Das notwendige Maß an Notfallvorsorge für einen allgemeinen Client ist stark vom individuellen Einsatzszenario abhängig. Oft wird als Notfallvorsorge für einen Client eine regelmäßige Datensicherung (siehe M 6.32 *Regelmäßige Datensicherung*) und das Erstellen eines bootfähigen Datenträgers für Notfälle (siehe M 6.24 *Erstellen eines Notfall-Bootmediums*) ausreichend sein. Für Clients mit besonderen Anforderungen an die Verfügbarkeit kann es sinnvoll sein, weitere Maßnahmen zu ergreifen, beispielsweise ein Austauschsystem bereit zu halten.

Abhängig vom eingesetzten Betriebssystem sind bei der Anwendung dieses Bausteins gegebenenfalls weitere Maßnahmen erforderlich. Diese finden sich in den jeweiligen Bausteinen.

Für den allgemeinen Client sind folgende Maßnahmen umzusetzen:

**Planung und Konzeption**
- M 2.23 (Z) *Herausgabe einer PC-Richtlinie*
- M 2.321 (A) *Planung des Einsatzes von Client-Server-Netzen*
- M 2.322 (A) *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*
- M 4.41 (Z) *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*
- M 5.66 (B) *Clientseitige Verwendung von SSL/TLS*
- M 5.152 (C) *Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste*

**Umsetzung**
- M 4.40 (C) *Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras*
- M 4.237 (A) *Sichere Grundkonfiguration eines IT-Systems*

**Betrieb**
- M 3.18 (A) *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*
- M 4.2 (A) *Bildschirmsperre*
- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*
- M 4.4 (C) *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*
- M 4.200 (Z) *Umgang mit USB-Speichermedien*
- M 4.238 (A) *Einsatz eines lokalen Paketfilters*
- M 4.241 (A) *Sicherer Betrieb von Clients*
- M 4.242 (Z) *Einrichten einer Referenzinstallation für Clients*
- M 5.45 (B) *Sichere Nutzung von Browsern*

**Aussonderung**
- M 2.323 (A) *Geregelte Außerbetriebnahme eines Clients*

**Notfallvorsorge**
- M 6.24 (A) *Erstellen eines Notfall-Bootmediums*
- M 6.32 (A) *Regelmäßige Datensicherung*

# B 3.202 Allgemeines nicht vernetztes IT-System

## Beschreibung

Betrachtet wird ein IT-System, das mit keinem anderen IT-System vernetzt ist. Es kann mit einem beliebigen Betriebssystem ausgestattet sein. Das IT-System kann auf einer beliebigen Plattform betrieben werden, es kann sich dabei um einen PC mit oder ohne Festplatte, aber auch um eine Unix-Workstation oder einen Apple Macintosh handeln. Das IT-System kann beispielsweise über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist. Ein eventuell vorhandener Drucker wird direkt am IT-System angeschlossen.

Dieses Kapitel bietet einen Überblick über Gefährdungen und Sicherheitsmaßnahmen, die für nicht vernetzte IT-Systeme typisch sind. Dieser Überblick ist unabhängig vom eingesetzten Betriebssystem. Dafür sind die weiterführenden Bausteine der IT-Grundschutz-Kataloge zu beachten.

## Gefährdungslage

Für den IT-Grundschutz eines allgemeinen nicht vernetzten IT-Systems werden folgende Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.21 *Mangelhafte Organisation des Wechsels zwischen den Benutzern*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.17 *Kein ordnungsgemäßer PC-Benutzerwechsel*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.7 *Defekte Datenträger*
- G 4.23 *Automatische Erkennung von Wechseldatenträgern*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.23 *Schadprogramme*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Allgemeines nicht vernetztes IT-System" vorgestellt. Ein Teil der hier genannten Maßnahmen ist in jedem Fall umzusetzen, auch wenn nur eine einzige Person dieses IT-System nutzt. Sollen an dem IT-System mehrere Benutzer arbeiten, so ist zusätzlich eine Administration des Rechners und eine Benutzertrennung unumgänglich. In diesem Fall sind auch die Maßnahmen und Gefährdungen zu betrachten, die für den Mehrbenutzerbetrieb relevant sind.

Abhängig vom eingesetzten Betriebssystem sind neben der Anwendung dieses Bausteins gegebenenfalls weitere Maßnahmen erforderlich, die in anderen Bausteinen beschrieben sind.

Für den Einsatz von nicht vernetzten Arbeitsplatzrechnern sollten im Hinblick auf die Informationssicherheit folgende Schritte durchlaufen werden:

- Richtlinien für die Nutzung von nicht vernetzten IT-Systemen
  Für die sichere Nutzung von IT-Systemen müssen verbindliche Richtlinien festgelegt werden. Dies umfasst beispielsweise, wer das System wann und wofür nutzen darf und auf welche Daten der Zugriff in welcher Weise gestattet wird. Diese Arbeiten werden im Rahmen der Umsetzung der Maßnahmen des Bausteins B 1.9 *Hard- und Software-Management* durchgeführt.
- Sichere Installation von nicht vernetzten IT-Systemen
  Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen. Die hier zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine, beispielsweise B 3.204 *Client unter Unix* oder B 3.209 *Client unter Windows XP*, zu realisieren. Dabei ist die Maßnahme M 4.15 *Gesichertes Login* von besonderer Bedeutung, da der technische Schutz nicht vernetzter Systeme zu einem großen Teil auf einer geeigneten Zugangskontrolle beruht. Zusätzliche Maßnahmen sind vor allem dann erforderlich, wenn mehrere Benutzer mit unterschiedlichen Berechtigungen auf dasselbe IT-System zugreifen sollen:
  - M 2.63 *Einrichten der Zugriffsrechte*
  - M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*
  - M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*
- Sichere Konfiguration der installierten Komponenten
  Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine zu realisieren. Auch hier sind zusätzliche Maßnahmen erforderlich, wenn eine Trennung der Rechte mehrerer Benutzer erforderlich ist. Zu beachten ist auch die Maßnahme M 4.7 *Änderung voreingestellter Passwörter*, weil nur zu häufig jede Zugangskontrolle dadurch illusorisch ist, dass die verwendeten Passwörter allgemein bekannt sind.
- Sicherer Betrieb von nicht vernetzten IT-Systemen
  Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist die Installation und permanente Aktualisierung eines Virenscanners. Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei nicht vernetzten IT-Systemen vor allem organisatorische Maßnahmen notwendig. Die notwendigen Maßnahmen werden im Rahmen der Umsetzung der Bausteine B 1.6 *Schutz vor Schadprogrammen* und B 1.9 *Hard- und Software-Management* realisiert und brauchen daher hier nicht weiter betrachtet zu werden. Spezifische Maßnahmen für Einzelsysteme sind dabei vor allem M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern* und M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*.
- Datensicherung der nicht vernetzten IT-Systeme (siehe M 6.32)
  Die Vorgehensweise und der erforderliche Umfang der Datensicherung richtet sich nach dem Einsatzszenario des IT-Systems (siehe Maßnahme M 6.32 *Regelmäßige Datensicherung*).

Für das allgemeine nicht vernetzte IT-System sind folgende Maßnahmen umzusetzen:

**Planung und Konzeption**
- M 2.23 (Z) *Herausgabe einer PC-Richtlinie*
- M 2.63 (A) *Einrichten der Zugriffsrechte*
- M 4.41 (Z) *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*

**Umsetzung**
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.15 (A) *Gesichertes Login*

**Betrieb**
- M 2.22 (Z) *Hinterlegen des Passwortes*
- M 3.18 (A) *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*
- M 4.2 (A) *Bildschirmsperre*
- M 4.4 (C) *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*
- M 4.30 (A) *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*

**Notfallvorsorge**
- M 6.32 (A) *Regelmäßige Datensicherung*

# B 3.203 Laptop

## Beschreibung

Unter einem Laptop oder Notebook wird ein PC verstanden, der aufgrund seiner Bauart transportfreundlich ist und mobil genutzt werden kann. Ein Laptop hat eine kompaktere Bauform als Arbeitsplatzrechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Er verfügt über eine Festplatte und meist auch über weitere Speichergeräte wie ein Disketten-, CD-ROM- oder DVD-Laufwerke sowie über Schnittstellen zur Kommunikation über verschiedene Medien (beispielsweise Modem, ISDN, LAN, USB, Firewire, WLAN). Laptops können mit allen üblichen Betriebssystemen wie Windows oder Linux betrieben werden. Daher ist zusätzlich der betriebssystemspezifische Client-Baustein zu betrachten.

Typischerweise wird ein Laptop zeitweise allein, ohne Anschluss an ein Rechnernetz betrieben, und von Zeit zu Zeit wird er zum Abgleich der Daten sowie zur Datensicherung mit dem Behörden- oder Unternehmensnetz verbunden. Häufig wird er auch während der mobilen Nutzung über Modem direkt mit externen Netzen, insbesondere mit dem Internet, verbunden, so dass er indirekt als Brücke zwischen dem LAN und dem Internet wirken kann.

Die Einrichtungen zur Datenfernübertragung (über Modem, ISDN-Karte, etc.) werden hier nicht behandelt (siehe Baustein B 4.3). Für den Laptop wird vorausgesetzt, dass er innerhalb eines bestimmten Zeitraums nur von einem Benutzer gebraucht wird. Ein anschließender Benutzerwechsel wird berücksichtigt.

## Gefährdungslage

Für den IT-Grundschutz eines Laptops werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.15 *Beeinträchtigung durch wechselnde Einsatzumgebung*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.8 *Unkontrollierter Einsatz von Betriebsmitteln*
- G 2.16 *Ungeordneter Benutzerwechsel bei tragbaren PCs*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.76 *Fehler bei der Synchronisation mobiler Endgeräte*

**Technisches Versagen**

- G 4.9 *Ausfall der internen Stromversorgung*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.52 *Datenverlust bei mobilem Einsatz*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*

- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*
- G 5.23 *Schadprogramme*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.124 *Missbrauch der Informationen von mobilen Endgeräten*
- G 5.125 *Datendiebstahl mithilfe mobiler Endgeräte*
- G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Einsatzes von Laptops sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

- Richtlinien für die Nutzung von Laptops
  Um Laptops sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.36 *Geregelte Übergabe und Rücknahme eines tragbaren PC* sowie Baustein B 3.201 *Allgemeiner Client*).
  Darauf aufbauend ist die Laptop-Nutzung zu regeln und Sicherheitsrichtlinien dafür zu erarbeiten (siehe M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*). Dies umfasst beispielsweise, wer das System wann und wofür nutzen darf und ob und in welcher Weise ein Anschluss an das Unternehmens- bzw. Behördennetz gestattet wird. Ebenso ist zu regeln, ob und in welcher Form bei mobiler Nutzung eine direkte Verbindung des Laptops mit dem Internet zulässig ist.
- Beschaffung von Laptops
  Für die Beschaffung von Laptops müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden (siehe M 2.310 *Geeignete Auswahl von Laptops*).
- Sichere Installation von Laptops
  Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der Laptops auszuschließen. Die hier zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine, beispielsweise B 3.204 *Client unter Unix* oder B 3.209 *Client unter Windows XP*, zu realisieren.
  Dabei ist die Maßnahme M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme* von besonderer Bedeutung, da bei Laptops ein relativ hohes Diebstahlsrisiko besteht und die normalen Funktionen der Zugangs- und Zugriffskontrolle ihre Wirksamkeit verlieren, wenn der Laptop unter der Kontrolle des Diebes steht.
- Sichere Konfiguration der installierten Komponenten
  Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig vom eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine zu realisieren. Auch hier sind zusätzliche Maßnahmen erforderlich, wenn eine Trennung der Rechte mehrerer Benutzer erforderlich ist. Zu beachten ist auch die Maßnahme M 4.7 *Änderung voreingestellter Passwörter*, weil nur zu häufig jede Zugangskontrolle dadurch illusorisch ist, dass die verwendeten Passwörter allgemein bekannt sind.
- Sicherer Betrieb von Laptops
  Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Laptops ist die Installation und permanente Aktualisierung eines Virenschutzprogramms. Laptops werden häufig über längere Zeit losgelöst vom Firmen- oder Behördennetz oder auch mit temporären Verbindungen zum Internet betrieben. Somit sind unter Umständen einerseits ihre Virendefinitionsdateien veraltet und sie sind andererseits einem hohen Infektionsrisiko ausgesetzt. Die im Baustein B 1.6 *Schutz vor Schadprogrammen* vorgesehenen Maßnahmen, vor allem die Maßnahme M 2.159 *Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen* sind daher für Laptops ganz besonders wichtig.

Diese Geräte können sonst bei Anschluss an ein Firmen- oder Behördennetz Infektionsquellen ersten Grades darstellen.
Sofern Laptops bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Soll ein Laptop, der direkt am Internet betrieben wurde, wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist. Erst wenn dies sichergestellt ist, darf der Anschluss an das lokale Netz erfolgen. Dies gilt auch für den Fall, dass der Anschluss an das Unternehmens- bzw. Behördennetz über ein Virtual Private Network (VPN) erfolgt, da Viren auch über verschlüsselte Kommunikationsverbindungen weiter verbreitet werden können.
Bei einem Wechsel zwischen netzgebundenem und mobilem Betrieb müssen die Datenbestände zwischen dem Server und dem Laptop synchronisiert werden. Es muss dabei gewährleistet werden, dass jederzeit erkennbar ist, ob sich die aktuellste Version der bearbeiteten Daten auf dem Laptop oder im Netz befindet (siehe M 4.235 *Abgleich der Datenbestände von Laptops*).
Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei Laptops vor allem organisatorische Maßnahmen notwendig. Die notwendigen Maßnahmen werden im Rahmen der Umsetzung des Bausteins B 1.9 *Hard- und Software-Management* realisiert und brauchen daher hier nicht weiter betrachtet zu werden. Um einen Überblick über die aktuell in das lokale Netz eingebundenen Laptops zu behalten und die Konfiguration aller Laptops jederzeit nachvollziehen zu können, ist eine zentrale Verwaltung dieser Geräte wichtig (siehe M 4.236 *Zentrale Administration von Laptops*).
Weitere spezifische Maßnahmen für Einzelsysteme sind vor allem M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern* und M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*.
Je nach der in einem Gebäude oder Büroraum gegebenen physischen Sicherheit kann es auch sinnvoll oder sogar notwendig sein, die Maßnahme M 1.46 *Einsatz von Diebstahl-Sicherungen* umzusetzen. Bei mobiler Nutzung ist in jedem Fall die Maßnahme M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz* anzuwenden, um den Laptop vor Diebstahl zu schützen.

- Aussonderung
  Bei Übergabe von Laptops an andere Benutzer, sei es im Rahmen des normalen Betriebs oder auch bei ihrer Aussonderung, ist darauf zu achten, dass keine schützenswerten Informationen mehr auf der Festplatte vorhanden sind. Hier sind vor allem die Maßnahmen M 2.36 *Geregelte Übergabe und Rücknahme eines tragbaren PC* sowie gegebenenfalls auch M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops* zu beachten.
- Datensicherung von Laptops
  Die Vorgehensweise und der erforderliche Umfang der Datensicherung richten sich nach dem Einsatzszenario des Laptops (siehe Maßnahme M 6.71 *Datensicherung bei mobiler Nutzung des IT-Systems*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Laptop" vorgestellt.

**Planung und Konzeption**
- M 2.36 (B) *Geregelte Übergabe und Rücknahme eines tragbaren PC*
- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.309 (A) *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*
- M 4.29 (Z) *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*

**Beschaffung**
- M 2.310 (Z) *Geeignete Auswahl von Laptops*

**Umsetzung**
- M 5.91 (A) *Einsatz von Personal Firewalls für Clients*
- M 5.121 (B) *Sichere Kommunikation von unterwegs*
- M 5.122 (A) *Sicherer Anschluss von Laptops an lokale Netze*

**Betrieb**
- M 1.33 (A) *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*

- M 1.34 (A) *Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz*
- M 1.35 (Z) *Sammelaufbewahrung tragbarer IT-Systeme*
- M 1.46 (Z) *Einsatz von Diebstahl-Sicherungen*
- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*
- M 4.27 (A) *Zugriffsschutz am Laptop*
- M 4.28 (Z) *Software-Reinstallation bei Benutzerwechsel eines Laptops*
- M 4.31 (A) *Sicherstellung der Energieversorgung im mobilen Einsatz*
- M 4.235 (B) *Abgleich der Datenbestände von Laptops*
- M 4.236 (Z) *Zentrale Administration von Laptops*
- M 4.255 (A) *Nutzung von IrDA-Schnittstellen*

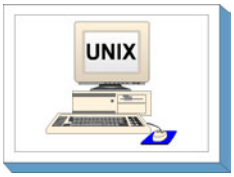
**Aussonderung**

- M 2.306 (A) *Verlustmeldung*

**Notfallvorsorge**

- M 6.71 (A) *Datensicherung bei mobiler Nutzung des IT-Systems*

# B 3.204 Client unter Unix




## Beschreibung

Betrachtet wird ein Unix-System, das entweder im Stand-Alone-Betrieb oder als Client in einem Netz genutzt wird. Es können Terminals, Laufwerke, Drucker und andere Geräte angeschlossen sein. Weiterhin kann eine graphische Benutzeroberfläche wie X-Window eingesetzt sein. Entsprechend können dann auch X-Terminals und graphische Eingabegeräte angeschlossen sein. Bei den weiteren Betrachtungen wird davon ausgegangen, dass ein Unix-System üblicherweise von mehreren Personen benutzt wird.

Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Obwohl Linux kein klassisches, sondern ein funktionelles Unix ist (der Kernel basiert nicht auf dem ursprünglichen Quelltext, aus dem sich die verschiedenen Unix-Derivate entwickelt haben), wird Linux ebenfalls in diesem Baustein betrachtet.

## Gefährdungslage

Für den IT-Grundschutz eines Unix-Systems werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.15 *Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.21 *Fehlbedienung von Codeschlössern*
- G 3.23 *Fehlerhafte Administration eines DBMS*

**Technisches Versagen**

- G 4.11 *Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client*
- G 4.12 *Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.41 *Missbräuchliche Nutzung eines Unix-Systems mit Hilfe von UUCP*
- G 5.89 *Hijacking von Netz-Verbindungen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Clients unter Unix sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Schon vor dem erstmaligen Einsatz eines Unix-Systems, gleichgültig ob es als Client, als Terminal- oder Anwendungsserver oder als Einzelplatz-System eingesetzt werden soll, sind eine Reihe von Festlegungen zu treffen, die die Grundlage eines geordneten, sicheren Betriebs bilden. Werden hier Fehler gemacht, so lassen sich diese im Nachhinein oft nur mit sehr hohem Aufwand korrigieren.

Es ist ein Verfahren für die Vergabe von User-IDs festzulegen, durch das gewährleistet wird, dass privilegierte und unprivilegierte Benutzerkennungen klar getrennt sind. Weiterhin ist sicherzustellen, dass kein unkontrollierter Zugang zum Single-User-Modus möglich ist, da sonst alle für die Laufzeit des Systems festgelegten Sicherheitsmaßnahmen unterlaufen werden können.

**Umsetzung**

Bei der Einrichtung eines Unix-Systems sind eine Reihe von Maßnahmen (siehe vor allem dazu M 4.105 *Erste Maßnahmen nach einer Unix-Standardinstallation*) zu treffen, die die Sicherheit dieses Systems "härten", also Lücken schließen, die nach einer Standardinstallation in der Regel vorhanden sind. Dazu gehört auch, dass nur die wirklich benötigten Netzdienste aktiviert werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*) und dass die Systemprotokollierung aktiviert wird.

Ferner sind die Zugriffsrechte auf Benutzer- und Systemdateien und -verzeichnisse so nach einem übergreifenden Schema zu vergeben, dass nur diejenigen Benutzer und Prozesse Zugriff erhalten, die diesen wirklich benötigen, wobei insbesondere auf die durch *setuid* und *setgid* bestimmten Rechte zu achten ist (siehe dazu M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*).

**Betrieb**

Um den Überblick über die Sicherheit eines Unix-Systems zu behalten, ist es unabdingbar, die vorhandenen Benutzerprofile und ihre Rechte zeitnah zu dokumentieren, diese Dokumentation immer auf dem aktuellen Stand zu halten und durch regelmäßige Überprüfungen mit der Realität abzugleichen. Die Sicherheit des Systems ist regelmäßig zu überprüfen, wobei auch die vom System erzeugten Protokolle auf eventuelle Unregelmäßigkeiten hin zu betrachten sind.

**Notfallvorsorge**

Da Unix-Systeme aufgrund ihrer Komplexität nach einem erfolgreichen Angriff oft auf schwer durchschaubare Weise kompromittiert sind, ist es wichtig, schon im Vorfeld Regeln festzulegen, nach denen bei einem echten oder vermuteten Verlust der Systemintegrität zu verfahren ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Client unter Unix" vorgestellt.

Für eventuell angeschlossene Rechner (z. B. Clients unter Windows) sind die in den entsprechenden Bausteinen beschriebenen Maßnahmen zu realisieren.

Darüber hinaus sind folgende weitere Maßnahmen umzusetzen:

**Planung und Konzeption**

- M 2.33 (Z) *Aufteilung der Administrationstätigkeiten unter Unix*
- M 4.13 (A) *Sorgfältige Vergabe von IDs*
- M 4.18 (A) *Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus*

- M 4.41 (Z) *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*
- M 5.64 (Z) *Secure Shell*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 4.9 (A) *Einsatz der Sicherheitsmechanismen von X-Window*
- M 4.14 (A) *Obligatorischer Passwortschutz unter Unix*
- M 4.16 (C) *Zugangsbeschränkungen für Benutzer-Kennungen und / oder Terminals*
- M 4.17 (A) *Sperren und Löschen nicht benötigter Accounts und Terminals*
- M 4.19 (A) *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*
- M 4.20 (B) *Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen*
- M 4.21 (A) *Verhinderung des unautorisierten Erlangens von Administratorrechten*
- M 4.22 (Z) *Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System*
- M 4.23 (B) *Sicherer Aufruf ausführbarer Dateien*
- M 4.105 (A) *Erste Maßnahmen nach einer Unix-Standardinstallation*
- M 4.106 (A) *Aktivieren der Systemprotokollierung*
- M 4.370 (Z) *Einsatz von Anoubis unter Unix*
- M 5.17 (A) *Einsatz der Sicherheitsmechanismen von NFS*
- M 5.18 (A) *Einsatz der Sicherheitsmechanismen von NIS*
- M 5.19 (A) *Einsatz der Sicherheitsmechanismen von sendmail*
- M 5.20 (A) *Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp*
- M 5.21 (A) *Sicherer Einsatz von telnet, ftp, tftp und rexec*
- M 5.35 (A) *Einsatz der Sicherheitsmechanismen von UUCP*
- M 5.72 (A) *Deaktivieren nicht benötigter Netzdienste*

**Betrieb**

- M 4.25 (A) *Einsatz der Protokollierung im Unix-System*
- M 4.26 (C) *Regelmäßiger Sicherheitscheck des Unix-Systems*

**Notfallvorsorge**

- M 6.31 (A) *Verhaltensregeln nach Verlust der Systemintegrität*

# B 3.205 Client unter Windows NT


Dieser Baustein ist 2009 mit der 11. Ergänzungslieferung entfallen.

Die letzte Version des Bausteins, die mit der 10. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 3.206 Client unter Windows 95


Dieser Baustein ist 2008 mit der 10. Ergänzungslieferung entfallen.

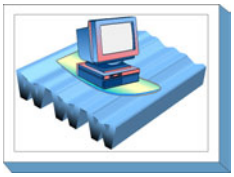
Die letzte Version des Bausteins, die mit der 9. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 3.207 Client unter Windows 2000


Dieser Baustein ist 2013 mit der 13. Ergänzungslieferung entfallen.

Die letzte Version des Bausteins, die mit der 12. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 3.208 Internet-PC



## Beschreibung

Die Nutzung des Internets zur Informationsbeschaffung und Kommunikation ist in weiten Bereichen der öffentlichen Verwaltung und Privatwirtschaft zur Selbstverständlichkeit geworden. Auch E-Commerce- und E-Government-Anwendungen gewinnen immer mehr an Bedeutung. Größtmöglichen Komfort bietet es dabei, den Mitarbeitern einer Institution einen Internet-Zugang direkt über den Arbeitsplatz-PC zur Verfügung zu stellen. Dieser ist jedoch meist in ein lokales Netz (LAN) eingebunden, so dass dadurch unter Umständen zusätzliche Bedrohungen für die Institution entstehen.

Um diese Probleme zu umgehen oder aus anderen anwendungsspezifischen Gründen stellen viele Behörden und Unternehmen eigenständige "Internet-PCs" zur Verfügung. Ein Internet-PC ist ein Computer, der über eine Internet-Anbindung verfügt, jedoch nicht mit dem internen Netz der Institution verbunden ist. Falls es sich um mehrere Internet-PCs handelt, können diese Computer auch untereinander vernetzt sein, beispielsweise um eine gemeinsame Internet-Anbindung zu nutzen. Internet-PCs dienen meist dazu, Mitarbeitern die Nutzung von Internet-Diensten zu ermöglichen und dabei zusätzliche Bedrohungen für das lokale Netz zu vermeiden.

Betrachtet wird ein Internet-PC auf der Basis eines Windows-Betriebssystems oder Linux. Für die Nutzung der Internet-Dienste kommen gängige Browser, wie z. B. Internet Explorer, Firefox oder Chrome, sowie E-Mail-Clients, wie z. B. Microsoft Outlook, Outlook Express, Thunderbird oder KMail, zum Einsatz. Je nach Einsatzszenario können weitere Programme für die Nutzung anderer Internet-Dienste, beispielsweise News, Instant Messaging oder Internet-Banking, installiert sein.

## Gefährdungslage

Für den IT-Grundschutz eines Internet-PCs werden die folgenden typischen Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.21 *Mangelhafte Organisation des Wechsels zwischen den Benutzern*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.43 *Makro-Viren*
- G 5.48 *IP-Spoofing*
- G 5.78 *DNS-Spoofing*
- G 5.87 *Web-Spoofing*

- G 5.88 *Missbrauch aktiver Inhalte*
- G 5.103 *Missbrauch von Webmail*
- G 5.143 *Man-in-the-Middle-Angriff*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ist geplant, in einem Unternehmen bzw. in einer Behörde einen oder mehrere Internet-PCs zur Verfügung zu stellen, sollten im Hinblick auf die Informationssicherheit folgende Schritte durchlaufen werden:

- Konzeption von Internet-PCs (siehe M 2.234 *Konzeption von Internet-PCs*)
  Zu Anfang müssen grundsätzliche Fragen des Einsatzes festgelegt werden, beispielsweise welche Internet-Dienste genutzt werden sollen und wer für die Administration des Internet-PCs zuständig ist.
- Richtlinien für die Nutzung von Internet-PCs (siehe M 2.235 *Richtlinien für die Nutzung von Internet-PCs*)
  Für die sichere Nutzung eines Internet-PCs müssen verbindliche Richtlinien festgelegt werden. Dies umfasst beispielsweise, wer den Internet-PC wann und wofür nutzen darf und ggf. wie Daten zwischen dem Internet-PC und dem Hausnetz transportiert werden.
- Sichere Installation von Internet-PCs (siehe M 4.151 *Sichere Installation von Internet-PCs*)
  Durch die Verbindung zum Internet ergeben sich für die auf dem Internet-PC installierten Anwendungen und für die gespeicherten Daten zusätzliche Gefährdungen. Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist daher besonders wichtig.
- Sichere Konfiguration der installierten Komponenten
  Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Dies betrifft insbesondere den verwendeten Browser (siehe M 5.93 *Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs*), den E-Mail-Client (siehe M 5.94 *Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs* ) und ggf. spezielle E-Business-Software.
- Sicherer Betrieb von Internet-PCs (siehe M 4.152 *Sicherer Betrieb von Internet-PCs*)
  Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb eines Internet-PCs ist das systematische und schnellstmögliche Einspielen sicherheitsrelevanter Patches und Updates. Neben dem Betriebssystem und dem Schutz vor Schadprogrammen sind auch Browser und E-Mail-Programm aktuell zu halten. Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sollten kritische Systemereignisse außerdem protokolliert werden.
- Datensicherung beim Einsatz von Internet-PCs (siehe M 6.79 *Datensicherung beim Einsatz von Internet-PCs*)

Die Vorgehensweise und der erforderliche Umfang der Datensicherung richtet sich nach dem Einsatzszenario des Internet-PC.

Der vorliegende Baustein gibt Empfehlungen zur Konzeption, Konfiguration und Betrieb eines solchen Internet-PCs. Wichtig ist dabei, dass die hier aufgeführten Maßnahmen nicht ausreichend sind für einen Standard-Arbeitsplatz-PC, auf dem in der Regel mehrere unterschiedliche Anwendungen betrieben und mit dem schützenswerte Daten verarbeitet werden. Dieses Maßnahmenbündel richtet sich ausschließlich an das spezielle Einsatzszenario "Internet-PC". Geeignete Sicherheitsempfehlungen für Standard-Arbeitsplatz-PCs sind in anderen Client-Bausteinen der Schicht 3 beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Internet-PC" vorgestellt.

**Planung und Konzeption**

- M 2.234 (A) *Konzeption von Internet-PCs*
- M 2.235 (A) *Richtlinien für die Nutzung von Internet-PCs*
- M 4.41 (Z) *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*
- M 5.66 (B) *Clientseitige Verwendung von SSL/TLS*
- M 5.92 (B) *Sichere Internet-Anbindung von Internet-PCs*

**Umsetzung**

- M 4.151 (B) *Sichere Installation von Internet-PCs*

- M 5.91 (A) *Einsatz von Personal Firewalls für Clients*
- M 5.98 (C) *Schutz vor Missbrauch kostenpflichtiger Einwahlnummern*

**Betrieb**

- M 2.313 (A) *Sichere Anmeldung bei Internet-Diensten*
- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*
- M 4.152 (B) *Sicherer Betrieb von Internet-PCs*
- M 5.59 (A) *Schutz vor DNS-Spoofing bei Authentisierungsmechanismen*
- M 5.93 (A) *Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs*
- M 5.94 (A) *Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs*
- M 5.95 (B) *Sicherer E-Commerce bei der Nutzung von Internet-PCs*
- M 5.96 (A) *Sichere Nutzung von Webmail*

**Notfallvorsorge**

- M 6.79 (A) *Datensicherung beim Einsatz von Internet-PCs*

# B 3.209 Client unter Windows XP


## Beschreibung

Betrachtet werden Arbeitsplatz-PCs (APCs) mit dem Betriebssystem Windows XP Professional. Windows XP ist das Nachfolgeprodukt von Windows 2000 Professional. Die Sicherheit eines solchen Betriebssystems spielt eine wichtige Rolle für die Sicherheit in einem Informationsverbund, da Schwachstellen auf der Betriebssystemebene die Sicherheit aller Anwendungen und des gesamten Netzes beeinträchtigen können. Der vorliegende Baustein beschreibt die Sicherheitsmaßnahmen, die für einen APC mit Windows XP umzusetzen sind. Die Maßnahmen beziehen sich insbesondere auf die Planung und den Betrieb eines Windows XP Clients in einer Domänenumgebung, auf Installationen von Windows XP auf Einzelplatzrechnern wird nur am Rande eingegangen. Die serverspezifischen Sicherheitsmaßnahmen, die beim Betrieb der Clients in einer Domänenumgebung relevant sind, sind in den Server-Bausteinen der Schicht 3 beschrieben (siehe z. B. Baustein B 3.106 *Server unter Windows 2000*).

## Gefährdungslage

Wie jedes IT-System sind auch Clients unter Microsoft Windows XP vielfältigen Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten aus. Daher kommt der korrekten Konfiguration des Systems und seiner Komponenten eine wichtige Rolle zu. Generell gilt, dass die Gefährdungslage einzelner Rechner immer auch vom Einsatzszenario abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen. Es ist zu beachten, dass bei nicht vernetzten PCs alle Angriffe (siehe "Vorsätzliche Handlungen") den lokalen Zugang zum Gerät (Konsole) erfordern.

Für den IT-Grundschutz einzelner PCs unter dem Betriebssystem Windows XP werden folgende typische Gefährdungen angenommen.

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.22 *Fehlerhafte Änderung der Registrierung*
- G 3.48 *Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.7 *Defekte Datenträger*
- G 4.23 *Automatische Erkennung von Wechseldatenträgern*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.7 *Abhören von Leitungen*

- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.43 *Makro-Viren*
- G 5.52 *Missbrauch von Administratorrechten bei Windows-Betriebssystemen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.79 *Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Aufgrund der oben aufgeführten besonderen Gefährdungen für vernetzte Geräte werden einige Maßnahmen ausdrücklich herausgestellt. Vor allem Maßnahmen zum Schutz gegen Angriffe aus dem Netz müssen hierbei sorgfältig durchgeführt werden. Eine effiziente, zentralisierte Verwaltung der Clients leistet einen wichtigen Beitrag zur Aufrechterhaltung eines hohen Sicherheitsstandards. Einheitliche Konfigurationsvorgaben erleichtern die Überwachung von ungewollten Änderungen der Konfiguration, Änderungen der Sicherheitsvorgaben können schneller auf allen Clients wirksam werden und Softwareaktualisierungen können schneller verteilt werden. Die Mehrzahl der empfohlenen Maßnahmen aus dem Bereich Hardware/Software lassen sich mit zentral vorgegebenen Gruppenrichtlinien umsetzen. Wenn in der Organisation der Einsatz von Microsoft Active Directory vorgesehen ist, muss dieser Einsatz gründlich geplant werden.

Einen Sonderfall stellt die Verwaltung von Windows XP Clients in Windows NT Domänenumgebungen dar. In diesem Fall stehen als Werkzeug zur zentralen Verwaltung nur die Windows NT Systemrichtlinien zur Verfügung. Aufgrund der technischen Beschränkungen dieser Lösung wird der Einsatz von Systemrichtlinien für Windows XP jedoch nicht empfohlen. Für die Verwaltung von Clients unter Windows XP sollte der Einsatz von Active Directory Gruppenrichtlinien erwogen werden.

Clients unter Windows XP können anstatt in Domänen auch in Arbeitsgruppen verwendet werden. Die Verwaltung sämtlicher Sicherheitsmerkmale erfolgt in diesem Fall lokal auf jedem einzelnen Client. Freigegebene Ressourcen auf einzelnen Rechnern lassen sich nur schwer zentral verwalten und überwachen. Ein Problem stellt auch die Datensicherung dar. Aufgrund der Vernetzung können jedoch einige netzbasierte Maßnahmen angewendet werden, z. B. die Verwendung von Sicherheitsvorlagen zur Konfiguration und die automatische Aktualisierung des Betriebssystems mithilfe des Software Update Service.

Für die erfolgreiche und sichere Konfiguration von Clients unter Windows XP sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb.

Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Nach der Entscheidung, Windows XP als Client-Betriebssystem einzusetzen, sollte zunächst der Einsatz geplant werden (siehe Maßnahme M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* ). Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*), die einerseits die bereits bestehenden Sicherheitsrichtlinien im Windows XP-Kontext umsetzt und andererseits die für Windows XP spezifischen Erweiterungen definiert.

In einer vernetzten Umgebung wird der Einsatz eines zentralen Verwaltungssystems empfohlen. Hierfür kann z. B. Microsoft Active Directory zum Einsatz kommen. Insbesondere die Verwendung von Gruppenrichtlinien ermöglicht eine relativ einfache zentrale Umsetzung von Sicherheitsvorgaben. Beim Betrieb eines Windows XP Einzelsystems ist der Einsatz lokaler Gruppenrichtlinien empfehlenswert. Die

Maßnahme M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* enthält die entsprechenden Empfehlungen zum Einsatz von Gruppenrichtlinien zur Konfiguration und Verwaltung eines Windows XP Systems.

Weitere Aspekte müssen in der Planungsphase berücksichtigt werden. Diese betreffen vor allem die sichere Konfiguration eines Windows XP Systems. Folgende Maßnahmen sind hierfür relevant:

- M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*
- M 4.245 *Basiseinstellungen für Windows Group Policy Objects*
- M 4.246 *Konfiguration der Systemdienste auf Clients ab Windows XP*
- M 5.123 *Absicherung der Netzkommunikation unter Windows*
- M 4.247 *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*

Wird in einem Unternehmen bzw. einer Behörde der Einsatz von Windows XP spezifischen Fernzugriffsmöglichkeiten beabsichtigt, so müssen in der Planungsphase die entsprechenden Technologien ausgewählt und damit verbundene Sicherheitsaspekte evaluiert werden (siehe dazu die Maßnahme M 2.327 *Sicherheit beim Fernzugriff auf Clients ab Windows XP*).

Soll Windows XP zum Einsatz auf mobilen Rechnern kommen, so müssen bereits in der Planungsphase spezifische Sicherheitsaspekte berücksichtigt werden. Die Maßnahme M 2.328 *Einsatz von Windows XP auf mobilen Rechnern* fasst die für Windows XP spezifischen Aspekte zusammen.

Windows XP bietet einige Verwaltungswerkzeuge an, die bereits in der Planungs- bzw. Testphase helfen können, Konfigurationsfehler zu vermeiden, was zweifellos einen Sicherheitsgewinn bringt.

Die Maßnahme M 4.243 *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen* fasst die wichtigsten Werkzeuge zusammen.

**Umsetzung**

In der Umsetzungsphase werden alle Maßnahmen ergriffen, die den sicheren Betrieb vorbereiten und gewährleisten. Dazu zählen insbesondere Maßnahmen zur Sicherheit bei der Installation und Grundkonfiguration des Systems.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation von Windows XP Systemen erfolgen. Die Installation muss mit besonderer Sorgfalt durchgeführt werden. In M 4.248 *Sichere Installation von Windows Client-Betriebssystemen* sind die relevanten Empfehlungen zusammengefasst. Die für die Konfiguration eines Windows XP Systems zu beachtenden Aspekte müssen während der Planungsphase ermittelt worden sein.

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Ein Windows XP System ändert sich in der Regel täglich. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei zu beachtenden Aspekte sind in M 4.146 *Sicherer Betrieb von Windows Client-Betriebssystemen* zusammengefasst.
- Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Windows XP Netzes ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in M 4.148 *Überwachung eines Windows 2000/XP Systems*. Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle.
- Windows XP Systeme sind wie auch andere IT-Systeme den allgemeinen Sicherheitsrisiken ausgesetzt. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs entschieden zu verringern, müssen Windows XP Systeme aktuell gehalten werden. Die entsprechenden Empfehlungen sind M 4.249 *Windows Client-Systeme aktuell halten* zu finden.
- Für die bereits im Betrieb befindlichen Windows XP Systeme müssen die aus dem Einspielen des Service Packs 2 resultierende Auswirkungen berücksichtigt werden (siehe dazu M 2.329 *Einführung von Windows XP SP2*).

- Eine regelmäßige Prüfung der geltenden Sicherheitseinstellungen und generell der existierenden Sicherheitsrichtlinien ist maßgebend für die Sicherheit der Windows XP Systeme im laufenden Betrieb. Die dabei zu beachtenden Aspekte sind in M 2.330 *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP* Sicherheitsrichtlinien und ihrer Umsetzung zusammengefasst.
- Windows XP bietet einige Verwaltungswerkzeuge an, deren Einsatz auch aus Sicherheitssicht empfehlenswert ist, da mit ihrer Hilfe unter anderem auch Konfigurationsfehler vermieden werden können. Im Weiteren sind diese Werkzeuge bei der Fehleranalyse bzw. bei der Revision nützlich (siehe dazu M 4.243 *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*).

**Aussonderung**

Wenn ein Windows XP APC stillgelegt wird, ist dafür Sorge zu tragen, dass die gespeicherten Daten nicht in falsche Hände geraten oder missbräuchlich verwendet werden können. Zu den gespeicherten Daten gehören auch Passwörter, Cookies, temporäre Internetdateien usw. Gleichzeitig ist zu beachten, dass bei Archivierung der Daten der Zugriff erhalten bleibt, auch wenn beispielsweise der bisherige Benutzer eines APCs die Organisation verlassen hat. Die gleichen Anforderungen gelten, wenn ein APC von einem Benutzer zu einem anderen Benutzer umgesetzt wird.

**Notfallvorsorge**

Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich in M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*. Hinweise zur Datensicherung sind in M 6.78 *Datensicherung unter Windows Clients* enthalten.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Windows XP Client" vorgestellt.

**Planung und Konzeption**

- M 2.324 (A) *Einführung von Windows auf Clients ab Windows XP planen*
- M 2.325 (A) *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*
- M 2.326 (A) *Planung der Gruppenrichtlinien für Clients ab Windows XP*
- M 2.327 (B) *Sicherheit beim Fernzugriff auf Clients ab Windows XP*
- M 2.328 (B) *Einsatz von Windows XP auf mobilen Rechnern*
- M 4.147 (Z) *Sichere Nutzung von EFS unter Windows*
- M 4.243 (Z) *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*
- M 4.244 (A) *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*
- M 4.245 (A) *Basiseinstellungen für Windows Group Policy Objects*
- M 4.246 (A) *Konfiguration der Systemdienste auf Clients ab Windows XP*
- M 4.247 (A) *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*
- M 5.123 (B) *Absicherung der Netzkommunikation unter Windows*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 3.28 (A) *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*
- M 4.48 (A) *Passwortschutz unter Windows-Systemen*
- M 4.49 (A) *Absicherung des Boot-Vorgangs für ein Windows-System*
- M 4.52 (A) *Geräteschutz unter NT-basierten Windows-Systemen*
- M 4.57 (A) *Deaktivieren der automatischen CD-ROM-Erkennung*
- M 4.75 (A) *Schutz der Registry unter Windows-Systemen*
- M 4.149 (A) *Datei- und Freigabeberechtigungen unter Windows*
- M 4.248 (A) *Sichere Installation von Windows Client-Betriebssystemen*
- M 5.89 (A) *Konfiguration des sicheren Kanals unter Windows*
- M 5.90 (Z) *Einsatz von IPSec unter Windows*

**Betrieb**

- M 2.329 (A) *Einführung von Windows XP SP2*
- M 2.330 (B) *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP*

- M 4.56 (C) *Sicheres Löschen unter Windows-Betriebssystemen*
- M 4.146 (A) *Sicherer Betrieb von Windows Client-Betriebssystemen*
- M 4.148 (B) *Überwachung eines Windows 2000/XP Systems*
- M 4.249 (A) *Windows Client-Systeme aktuell halten*

**Notfallvorsorge**

- M 6.76 (C) *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*
- M 6.78 (A) *Datensicherung unter Windows Clients*

# B 3.210 Client unter Windows Vista


## Beschreibung

Der vorliegende Baustein behandelt das Client-Betriebssystem Windows Vista in der Version Enterprise, kurz Windows Vista Enterprise. Wenn notwendig, werden abweichende Besonderheiten von Windows Vista Business und Windows Vista Ultimate dargestellt.

Windows Vista ist das Nachfolgeprodukt zu Microsofts Betriebssystem Windows XP Professional bzw. Home. Die Sicherheit eines Client-Betriebssystems wie Windows Vista spielt eine wichtige Rolle für die Sicherheit im gesamten Informationsverbund. Schwachstellen im Betriebssystem eines Clients gefährden die Sicherheit aller IT-Systeme und letztlich des gesamten Informationsverbundes.

Der Schwerpunkt im vorliegenden Baustein liegt auf dem Betrieb von Clients in einer Domänenumgebung. Wichtige abweichende Sachverhalte, die speziell für Windows Vista auf Einzelplatzrechnern oder in einer Arbeitsgruppe gelten, werden als solche hervorgehoben.

Die Server-spezifischen Sicherheitsmaßnahmen, die beim Betrieb der Clients in einer Domänenumgebung relevant sind, werden in den Server-Bausteinen wie B 3.106 *Server unter Windows 2000* und B 3.108 *Windows Server 2003* beschrieben.

Clients mit einem Microsoft-Betriebssystem bilden wegen ihrer hohen Verbreitung ein attraktives Ziel für Angreifer. Dies zeigen die zahlreichen publizierten Sicherheitslücken und Angriffe. Microsoft hat daher in Windows Vista gegenüber den vorangegangenen Windows-Versionen einige Änderungen implementiert, die das Sicherheitsniveau des Clients verbessern sollen. Außerdem hat Microsoft bestehende Sicherheitsmerkmale früherer Windows Versionen weiter entwickelt und dann in Windows Vista übernommen. Hierzu zählt etwa das Sicherheitscenter aus Windows XP mit Service Pack 2. Beispiele für Vista-spezifische Sicherheitsmerkmale sind:

- *BitLocker Drive Encryption* als Festplattenverschlüsselung für den Schutz vertraulicher Daten (nur in Windows Vista Enterprise und Ultimate verfügbar).
- *Benutzerkontensteuerung (User Account Control, UAC)* zum Schutz der Systemintegrität beim Arbeiten mit Administratorkonten.
- *Geschützter Modus des Internet Explorer IE7* als Schutz gegen unbemerktes Herunterladen und Ausführen von Schadcode beim Surfen im Internet (setzt UAC voraus) sowie weitere Sicherheitsmerkmale zum Schutz der Integrität von Benutzer- und Systemdaten.
- *Datei- und Registry-Virtualisierung* zur sicheren Ausführung von Alt-Anwendungen als Standardbenutzer, die vor Windows Vista nur unter dem Administrator-Konto genutzt werden konnten (setzt UAC voraus).

Neben neuen und geänderten Sicherheitsmerkmalen zeichnet sich Windows Vista insbesondere durch zahlreiche Änderungen bezüglich der Abläufe und Anforderungen zur Aktivierung aus.

## Gefährdungslage

Moderne IT-Systeme sind im täglichen Betrieb einer Vielzahl von Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe bestimmte Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten oder konzeptionelle Schwächen in der Systemarchitektur aus.

Generell gilt, dass die Gefährdungslage einzelner IT-Systeme immer auch vom Einsatzszenario abhängt und diese Einzelgefährdungen in die Gefährdung des Gesamtsystems eingehen. Es ist zu beachten, dass bei nicht vernetzten IT-Systemen alle Angriffe (siehe "Vorsätzliche Handlungen") den lokalen Zugang zum IT-System erfordern.

Für den IT-Grundschutz einzelner IT-Systeme unter dem Betriebssystem Windows Vista werden folgende typische Gefährdungen angenommen.

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.62 *Ungeeigneter Umgang mit Sicherheitsvorfällen*
- G 2.146 *Verlust der Arbeitsfähigkeit von Vista-Clients durch fehlende Reaktivierung vor SP1*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.22 *Fehlerhafte Änderung der Registrierung*
- G 3.48 *Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen*
- G 3.97 *Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista*
- G 3.98 *Verlust von BitLocker-verschlüsselten Daten*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.7 *Defekte Datenträger*
- G 4.23 *Automatische Erkennung von Wechseldatenträgern*
- G 4.73 *Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme von Windows-Versionen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.23 *Schadprogramme*
- G 5.52 *Missbrauch von Administratorrechten bei Windows-Betriebssystemen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.79 *Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um einen Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Windows Vista Systeme sind in der Regel Teil eines Informationsverbundes. Daraus ergeben sich besondere Angriffsmöglichkeiten. Windows Vista stellt bereits einige Sicherheitsmaßnahmen in der Grundkonfiguration bereit. Andere Sicherheitsmaßnahmen müssen durch die Verantwortlichen erst umgesetzt werden. Die zentrale Konfiguration und Durchsetzung von technischen Sicherheitsmaßnahmen kann durch Active Directory (AD) unterstützt werden.

Wo die zentrale Konfigurationsmöglichkeit mittels Active Directory nicht gegeben ist, müssen technische Maßnahmen dezentral auf den einzelnen Clients über lokale Sicherheitsrichtlinien eingestellt werden. Dazu können Konfigurationsdateien zentral erstellt und mittels geeigneter Mechanismen auf die Clients übertragen und dort installiert werden.

Bei der Beschreibung der Konfigurationen wird im Folgenden von einer Windows Server 2003 Domänenstruktur in der AD-Funktionsebene "Windows Server 2003" ausgegangen.

Für die sichere Konfiguration von Clients unter Windows Vista sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Bei Einsatz von Windows Vista muss zunächst die geeignete Version ausgewählt (siehe M 2.440 *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*) und ihr Einsatz geplant werden (siehe M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* ). Dabei ist zu unterscheiden, ob eine Einsatzumgebung vollkommen neu entsteht, oder ob eine bestehende Umgebung auf das Betriebssystem Windows Vista migriert wird. Für den Einsatz von Windows Vista ist eine Sicherheitsrichtlinie zu erarbeiten. Es kann eine bereits existierende Sicherheitsrichtlinie an die Eigenschaften von Windows Vista angepasst werden oder eine neue, speziell auf die Eigenschaften von Windows Vista zugeschnittene Richtlinie erarbeitet werden (siehe M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*).

In einer Domänenumgebung können verschiedene Sicherheitseinstellungen mittels eines zentralen Verwaltungswerkzeugs wie Active Directory erstellt und gepflegt werden. Andere Sicherheitseinstellungen können zentral erzeugt und mit geeigneten Mitteln auf die Clients übertragen werden. In der Maßnahme M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* werden Hinweise und Empfehlungen zur Konfiguration von Clients unter Windows Vista gegeben.

Windows Vista unterstützt die Möglichkeit der Fernadministration des Clients und stellt Möglichkeiten zur Verfügung, mittels Windows Vista per Fernadministration auf andere Systeme zuzugreifen. Wenn diese Möglichkeiten genutzt werden sollen, müssen in der Planungsphase bereits entsprechende Überlegungen getroffen werden, damit sich keine unberechtigten Personen auf dem Client anmelden können. Die relevanten Aspekte sind in der Maßnahme M 2.327 *Sicherheit beim Fernzugriff auf Clients ab Windows XP* beschrieben.

Soll Windows Vista auf mobilen Rechnern zum Einsatz kommen, müssen bereits in der Planungsphase entsprechende Sicherheitsaspekte berücksichtigt werden. Die Maßnahme M 2.442 *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen* nennt die für Windows Vista spezifischen Aspekte.

Von besonderer Bedeutung für den Einsatz von Windows Vista ist die Aktivierung des Systems. Hintergründe nennt die Maßnahme M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*.

**Umsetzung**

In der Umsetzungsphase werden alle Maßnahmen ergriffen, die den sicheren Betrieb konkret vorbereiten. Dazu zählen insbesondere Maßnahmen zur Sicherheit bei der Installation und Grundkonfiguration des Systems.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation von Windows Vista Systemen erfolgen. Die Installation muss mit besonderer Sorgfalt durchgeführt werden. In M 4.248 *Sichere Installation von Windows Client-Betriebssystemen* sind die relevanten Empfehlungen zusammengefasst. Die für die Konfiguration eines Windows Vista Systems zu beachtenden Aspekte müssen während der Planungsphase ermittelt worden sein.

**Betrieb**

Die Umsetzung wird idealerweise zunächst in einer Testinstallation vorgenommen. Nach erfolgreichem Test erfolgt die Installation von Windows Vista auf den dafür vorgesehenen Clients und der Übergang zum Regelbetrieb. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Ein Windows Vista System wird häufig von einer Vielzahl von Benutzern mit höchst unterschiedlichen Bedürfnissen und Anforderungen an das System eingesetzt. Dies hat zur Folge, dass eine entsprechende Zahl von Benutzerprofilen anzulegen und zu pflegen ist.
- Die im Regelbetrieb zu beachtenden Aspekte sind in M 4.146 *Sicherer Betrieb von Windows Client-Betriebssystemen* zusammengefasst.
- Ein Mittel zur Aufrechterhaltung der Sicherheit eines Windows Vista Systems ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hierfür relevanten Empfehlungen finden sich in M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*.
- Windows Vista Systeme sind wie andere IT-Systeme den allgemeinen Sicherheitsrisiken ausgesetzt. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs auf ein akzeptables Maß zu verringern, müssen Windows Vista Systeme aktuell gehalten werden. Die entsprechenden Empfehlungen sind in M 4.249 *Windows Client-Systeme aktuell halten* zu finden.
- Für die bereits im Betrieb befindlichen Windows Vista Systeme müssen die aus dem Einspielen von Service Packs und Hotfixes resultierenden Auswirkungen berücksichtigt werden.
- Eine regelmäßige Prüfung der geltenden Sicherheitseinstellungen und generell der existierenden Sicherheitsrichtlinien ist ein wichtiger Beitrag zur Sicherheit der Windows Vista Systeme im laufenden Betrieb. Die dabei zu beachtenden Aspekte sind in M 2.330 *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP* zusammengefasst.
- Windows Vista bietet einige Verwaltungswerkzeuge an, deren Einsatz auch aus Sicherheitssicht empfehlenswert ist, da mit ihrer Hilfe unter anderem auch sicherheitsrelevante Konfigurationsfehler vermieden werden können. Im Weiteren sind diese Werkzeuge bei der Fehleranalyse bzw. bei der Revision nützlich (siehe M 4.243 *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*).
- Ein im Betrieb befindliches Windows Vista System muss unter bestimmten Voraussetzungen reaktiviert werden. Hinweise und Empfehlungen zur Reaktivierung finden sich in M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*.

**Aussonderung**

Auf Arbeitsplatz-PCs, die einen Bereich verlassen oder ausgesondert werden, sind lokal gespeicherte Benutzerdaten zu löschen. Dies gilt auch für defekte Datenträger, die ausgetauscht werden. Können Daten auf Datenträgern nicht mehr zuverlässig gelöscht werden, ist der Datenträger in geeigneter Weise zu zerstören. Empfehlungen hierzu finden sich in B 1.15 *Löschen und Vernichten von Daten*.

Es ist zu beachten, dass ein Zugriff auf archivierte Daten gemäß den Archivierungsfristen erhalten bleiben muss, auch wenn das ursprünglich aufzeichnende IT-System ausgesondert wird.

**Notfallvorsorge**

Neben der Absicherung im laufenden Betrieb spielt auch die Notfallvorsorge eine wichtige Rolle. Hinweise zur Notfallvorsorge finden sich in M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*. Empfehlungen zur Datensicherung sind in M 6.78 *Datensicherung unter Windows Clients* enthalten.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Client unter Windows Vista" vorgestellt.

**Planung und Konzeption**

- M 2.324 (A) *Einführung von Windows auf Clients ab Windows XP planen*
- M 2.325 (A) *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*
- M 2.326 (A) *Planung der Gruppenrichtlinien für Clients ab Windows XP*
- M 2.327 (B) *Sicherheit beim Fernzugriff auf Clients ab Windows XP*
- M 2.440 (A) *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*
- M 2.441 (A) *Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista*

- M 2.442 (B) *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen*
- M 4.147 (Z) *Sichere Nutzung von EFS unter Windows*
- M 4.243 (Z) *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*
- M 4.244 (A) *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*
- M 4.245 (A) *Basiseinstellungen für Windows Group Policy Objects*
- M 4.246 (A) *Konfiguration der Systemdienste auf Clients ab Windows XP*
- M 4.247 (A) *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*
- M 4.336 (A) *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.337 (Z) *Einsatz von BitLocker Drive Encryption*
- M 4.338 (A) *Einsatz von File und Registry Virtualization bei Clients ab Windows Vista*
- M 4.339 (B) *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*
- M 4.340 (A) *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*
- M 4.341 (A) *Integritätsschutz ab Windows Vista*
- M 4.342 (Z) *Aktivierung des Last Access Zeitstempels ab Windows Vista*
- M 5.123 (B) *Absicherung der Netzkommunikation unter Windows*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 3.28 (A) *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*
- M 4.48 (A) *Passwortschutz unter Windows-Systemen*
- M 4.49 (A) *Absicherung des Boot-Vorgangs für ein Windows-System*
- M 4.75 (A) *Schutz der Registry unter Windows-Systemen*
- M 4.149 (A) *Datei- und Freigabeberechtigungen unter Windows*
- M 4.248 (A) *Sichere Installation von Windows Client-Betriebssystemen*
- M 5.89 (A) *Konfiguration des sicheren Kanals unter Windows*
- M 5.90 (Z) *Einsatz von IPSec unter Windows*

**Betrieb**

- M 2.330 (B) *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP*
- M 2.443 (A) *Einführung von Windows Vista SP1*
- M 4.56 (C) *Sicheres Löschen unter Windows-Betriebssystemen*
- M 4.146 (A) *Sicherer Betrieb von Windows Client-Betriebssystemen*
- M 4.249 (A) *Windows Client-Systeme aktuell halten*
- M 4.343 (Z) *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.344 (B) *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*

**Notfallvorsorge**

- M 6.76 (C) *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*
- M 6.78 (A) *Datensicherung unter Windows Clients*

# B 3.211 Client unter Mac OS X


## Beschreibung

Dieser Baustein behandelt das Client-Betriebssystem Mac OS X der Firma Apple. Das X in Mac OS X steht für die römische Ziffer 10, kann aber auch als eine Anlehnung an das X in Unix, Linux, AIX und anderen Unix-Derivaten gesehen werden.

Mac OS X basiert auf Darwin, dem frei verfügbaren Unix-Betriebssystem der Firma Apple. Darwin ist ein Open Source-Kernel, der auf FreeBSD basiert. Der größte Unterschied zwischen FreeBSD und Mac OS X ist die in FreeBSD fehlende grafische Oberfläche "Aqua".

Mac OS X kann und darf nur auf IT-Systemen der Firma Apple installiert werden. In abgewandelter Form wird Mac OS auch in anderen Apple-Produkten wie dem iPhone, iPad oder iPod touch eingesetzt. Die Grundlage dieses Bausteins ist die Client-Version "Snow Leopard" (Mac OS 10.6), jedoch kann er auf alle Versionen von Mac OS X angewendet werden, in denen die behandelten Softwarekomponenten (z. B. *FileVault* ab Version 10.3, *Dashboard* ab Version 10.4 oder *Time Machine* ab Version 10.5) vertreten sind.

Die Sicherheit eines Betriebssystems spielt eine wichtige Rolle für die Sicherheit in einem Informationsverbund. Schwachstellen auf der Betriebssystemebene können die Sicherheit aller Anwendungen und des gesamten Netzes beeinträchtigen. Der Schwerpunkt in diesem Baustein liegt auf der Absicherung eines IT-Systems unter Mac OS X, das als Stand-Alone-System oder als Client in einem Client-Server-Netz betrieben wird.

## Gefährdungslage

Für den IT-Grundschutz einzelner IT-Systeme unter dem Betriebssystem Mac OS X werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.108 *Fehlerhafte Konfiguration von Mac OS X*
- G 3.109 *Unsachgemäßer Umgang mit FileVault-Verschlüsselung*

**Technisches Versagen**

- G 4.7 *Defekte Datenträger*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*

- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon und Kamera*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein gemäß den Ergebnissen der Modellierung nach IT-Grundschutz weitere Bausteine umgesetzt werden. Dazu zählt der Baustein B 3.201 *Allgemeiner Client*. Wird Mac OS X auf einem Laptop betrieben, muss auch der Baustein B 3.203 *Laptop* angewendet werden.

In diesem Baustein werden Maßnahmen beschrieben, um einen Client unter Mac OS X mit einem normalen Schutzbedarf abzusichern. Es werden ausschließlich Anwendungen betrachtet, die im Standardfunktionsumfang von Mac OS X enthalten sind.

Für die sichere Konfiguration von Clients unter Mac OS X sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Clients unter Mac OS X sollten in einer Institution nicht eingesetzt werden, ohne dass deren Einsatz geplant und mit den internen Sicherheitsvorgaben abgestimmt wurde, wie in M 2.478 *Planung des sicheren Einsatzes von Mac OS X* beschrieben. Dazu müssen die unter anderem die Voraussetzungen für die Nutzung von Mac OS X geklärt und Hinweise zum Benutzer- und Administrationskonzept sowie Ratschläge zu einem angemessenen Umfang von Datensicherung und Verschlüsselung erstellt werden. In M 4.375 *Einsatz der Sandbox-Funktion unter Mac OS X* wird eine Methode beschrieben, um die Rechte von Anwendungen unter Mac OS X einzuschränken. Im Vorfeld muss dazu geklärt werden, welche Anwendungen in einer Sandbox ausgeführt und welche Zugriffsrechte diesen Anwendungen gewährt werden sollen. Ebenfalls muss der Einsatz der Programmzugriffs-Steuerung unter Mac OS X geplant werden, da je nach Einsatzgebiet eine striktere Client-Konfiguration vorgenommen werden muss. Hinweise sind in M 4.378 *Einschränkung der Programmzugriffe unter Mac OS X* zu finden. Da die Passwortstärke einen hohen Beitrag zur Sicherheit eines IT-Systems leistet, muss im Vorfeld geplant werden, welche Eigenschaften ein Passwort haben muss. Es sollten mindestens die Empfehlungen in M 4.376 *Festlegung von Passwortrichtlinien unter Mac OS X* umgesetzt werden.

**Umsetzung**

Bei der Installation eines Clients unter Mac OS X ist eine Reihe von Maßnahmen umzusetzen, die die Sicherheit des Systems erhöhen. Das "Härten" des Systems erhöht die Sicherheit, indem Lücken geschlossen werden, die im Regelfall nach einer Standardinstallation vorhanden sind. Unter M 4.371 *Konfiguration von Mac OS X Clients* sind entsprechende Empfehlungen zu finden. Im Anschluss sollte für jedes Benutzerkonto die Maßnahme M 4.374 *Zugriffschutz der Benutzerkonten unter Mac OS X* umgesetzt werden, um das Sicherheitsniveau für jedes Konto anzuheben. Der Einsatz der Personal Firewall von Mac OS X ist in keinem Fall ein Ersatz für ein Sicherheitsgateway, sie sollte aber dennoch aktiviert und angemessen konfiguriert werden. Informationen dazu sind in der Maßnahme M 5.166 *Konfiguration der Mac OS X Personal Firewall* enthalten. Um den Benutzerordner zu verschlüsseln, kann die Maßnahme M 4.372 *Einsatz von FileVault unter Mac OS X* angewendet werden.

Damit ein Client unter Mac OS X im Netz möglichst wenig Dienste anbietet und dadurch weniger Angriffsmöglichkeiten bietet, sollten möglichst viele Netzdienste deaktiviert werden (siehe M 5.165 *Deaktivieren nicht benötigter Mac OS X-Netzdienste*). Ebenso kann es sinnvoll sein, nicht benötigte Hardware zu deaktivieren, beispielsweise um den Missbrauch von Rechner-Mikrofonen oder Kameras zu verhindern (siehe M 4.373 *Deaktivierung nicht benötigter Hardware unter Mac OS X*).

**Betrieb**

Der reibungslose Betrieb von Mac OS X Clients sollte durch regelmäßige Kontrollen und Auswertungen der Protokolldateien sichergestellt werden. Hierbei sollten vor allem Unregelmäßigkeiten genauer betrachtet werden. Informationen dazu sind in den Maßnahmen M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems* und M 4.25 *Einsatz der Protokollierung im Unix-System* zu finden. Sollen vertrauliche Informationen transportiert oder außerhalb des Benutzerordners gespeichert werden, müssen die Benutzer über die Maßnahme M 4.379 *Sichere Datenhaltung und sicherer Transport unter Mac OS X* informiert und geschult werden. Die Administratoren müssen zusätzlich über die Maßnahme M 4.377 *Überprüfung der Signaturen von Mac OS X Anwendungen* Anwendungen informiert werden, um jede neue Anwendung auf ihre gültige Signatur überprüfen zu können.

**Aussonderung**

Bei der Aussonderung oder Stilllegung eines Systems ist sicherzustellen, dass Dritte keinen Zugriff auf sicherheitsrelevante Informationen erhalten. Daher sind nicht nur Wechseldatenträger, sondern auch lokal gespeicherte Benutzerdaten zuverlässig zu löschen, wenn das Speichermedium oder das IT-System ausgesondert wird. Um Informationen unter Mac OS X sicher zu löschen, ist die Maßnahme M 6.148 *Aussonderung eines Mac OS X Systems* umzusetzen.

**Notfallvorsorge**

Um nach einem Hardwareausfall oder Datenverlust möglichst zeitnah in den Normalbetrieb zurückkehren zu können, sollten die Empfehlungen der Maßnahmen M 6.146 *Datensicherung und Wiederherstellung von Mac OS X Clients* und M 6.147 *Wiederherstellung von Systemparametern beim Einsatz von Mac OS X* umgesetzt werden. Die Maßnahme M 4.380 *Einsatz von Apple-Software-Restore unter Mac OS X* enthält zusätzliche Informationen, um eine identische Kopie von einem System zu erzeugen. Dieses Systemabbild kann dazu verwendet werden, um einen Client unter Mac OS X wiederherzustellen oder um ein Standard-Image über das Netz auf alle Mac OS X Clients aufzuspielen.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Mac OS X" vorgestellt:

**Planung und Konzeption**
- M 2.478 (A) *Planung des sicheren Einsatzes von Mac OS X*
- M 2.479 (A) *Planung der Sicherheitsrichtlinien von Mac OS X*
- M 4.374 (C) *Zugriffschutz der Benutzerkonten unter Mac OS X*
- M 4.375 (Z) *Einsatz der Sandbox-Funktion unter Mac OS X*
- M 4.376 (C) *Festlegung von Passwortrichtlinien unter Mac OS X*
- M 4.378 (Z) *Einschränkung der Programmzugriffe unter Mac OS X*
- M 5.64 (Z) *Secure Shell*

**Umsetzung**
- M 4.106 (A) *Aktivieren der Systemprotokollierung*
- M 4.371 (C) *Konfiguration von Mac OS X Clients*
- M 4.372 (C) *Einsatz von FileVault unter Mac OS X*
- M 4.373 (C) *Deaktivierung nicht benötigter Hardware unter Mac OS X*
- M 5.165 (C) *Deaktivieren nicht benötigter Mac OS X-Netzdienste*
- M 5.166 (Z) *Konfiguration der Mac OS X Personal Firewall*
- M 5.167 (C) *Sicherheit beim Fernzugriff unter Mac OS X*

**Betrieb**
- M 4.25 (A) *Einsatz der Protokollierung im Unix-System*
- M 4.26 (C) *Regelmäßiger Sicherheitscheck des Unix-Systems*
- M 4.377 (Z) *Überprüfung der Signaturen von Mac OS X Anwendungen*
- M 4.379 (B) *Sichere Datenhaltung und sicherer Transport unter Mac OS X*

**Aussonderung**
- M 6.148 (C) *Aussonderung eines Mac OS X Systems*

**Notfallvorsorge**
- M 4.380 (Z) *Einsatz von Apple-Software-Restore unter Mac OS X*
- M 6.31 (A) *Verhaltensregeln nach Verlust der Systemintegrität*
- M 6.146 (A) *Datensicherung und Wiederherstellung von Mac OS X Clients*

- M 6.147 (A) *Wiederherstellung von Systemparametern beim Einsatz von Mac OS X*

# B 3.212 Client unter Windows 7


## Beschreibung

Der vorliegende Baustein behandelt das Client-Betriebssystem Microsoft Windows 7 in der Version Enterprise, kurz Windows 7 Enterprise. Wenn notwendig, werden abweichende Besonderheiten von Windows 7 Professional und Windows 7 Ultimate dargestellt.

Windows 7 ist das Nachfolgeprodukt zu Microsofts Betriebssystem Windows Vista. Die Sicherheit eines Client-Betriebssystems wie Windows 7 spielt eine wichtige Rolle für die Sicherheit im gesamten Informationsverbund. Schwachstellen im Betriebssystem eines Clients gefährden die Sicherheit aller IT-Systeme, Informationen und letztlich des gesamten Informationsverbundes.

Der Schwerpunkt des vorliegenden Bausteins liegt auf dem Einsatz von Clients in einer Domänenumgebung. Wichtige abweichende Sachverhalte, die speziell für Windows 7 auf Einzelplatzrechnern oder in einer Arbeitsgruppe gelten, werden als solche hervorgehoben.

Microsoft hat in Windows 7 gegenüber den vorangegangenen Windows-Versionen einige Änderungen integriert, die das Sicherheitsniveau verbessern sollen. Außerdem hat Microsoft bestehende Sicherheitsmerkmale früherer Windows Versionen weiter entwickelt und in Windows 7 übernommen. Hierzu zählt etwa das Sicherheitscenter aus Windows XP mit Service Pack 2 und Vista, das unter Windows 7 zum Wartungscenter erweitert wurde.

Beispiele für Windows 7-spezifische Sicherheitsmerkmale sind:

- AppLocker zum Schutz vor Installation und Ausführung nicht freigegebener Software (nur in Windows 7 Enterprise und Ultimate verfügbar)
- BitLocker To Go zur Verschlüsselung von Wechseldatenträgern durch Benutzer ohne Administratorrechte

Die Server-spezifischen Sicherheitsmaßnahmen, die beim Betrieb der Clients in einer Domänenumgebung relevant sind, werden in Server-Bausteinen wie B 3.101 *Allgemeiner Server*, B 3.108 *Windows Server 2003* und Windows B 3.109 *Windows Server 2008* beschrieben.

Moderne IT-Systeme sind im täglichen Betrieb einer Vielzahl von Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe bestimmte Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten oder konzeptionelle Schwächen in der Systemarchitektur aus. Clients mit einem Microsoft-Betriebssystem bilden wegen ihrer hohen Verbreitung ein attraktives Ziel für Angreifer. Dies zeigen die zahlreichen publizierten Sicherheitslücken und Angriffe.

IT-Systeme unter dem Betriebssystem Windows 7 sind folgenden typischen Gefährdungen ausgesetzt:

## Gefährdungslage

Moderne IT-Systeme sind im täglichen Betrieb einer Vielzahl von Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe bestimmte Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten oder konzeptionelle Schwächen in der Systemarchitektur aus. Clients mit einem Microsoft-Betriebssystem bilden wegen ihrer hohen Verbreitung ein attraktives Ziel für Angreifer. Dies zeigen die zahlreichen publizierten Sicherheitslücken und Angriffe.

IT-Systeme unter dem Betriebssystem Windows 7 sind folgenden typischen Gefährdungen ausgesetzt:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*

- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.62 *Ungeeigneter Umgang mit Sicherheitsvorfällen*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.22 *Fehlerhafte Änderung der Registrierung*
- G 3.48 *Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen*
- G 3.97 *Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista*
- G 3.98 *Verlust von BitLocker-verschlüsselten Daten*
- G 3.112 *Unautorisierte oder falsche Nutzung von Images bei der Nutzung von Windows DISM*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.7 *Defekte Datenträger*
- G 4.23 *Automatische Erkennung von Wechseldatenträgern*
- G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*
- G 4.55 *Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP*
- G 4.73 *Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme von Windows-Versionen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.23 *Schadprogramme*
- G 5.52 *Missbrauch von Administratorrechten bei Windows-Betriebssystemen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.79 *Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Windows 7 stellt bereits einige Sicherheitsmechanismen in der Grundkonfiguration bereit. Andere Sicherheitsmechanismen müssen durch die Verantwortlichen erst eingerichtet werden. Die zentrale Konfiguration und Durchsetzung von technischen Sicherheitsmaßnahmen kann durch Active Directory (AD) unterstützt werden.

Wo die zentrale Konfigurationsmöglichkeit mittels AD nicht gegeben ist, müssen technische Maßnahmen dezentral auf den einzelnen Clients über lokale Sicherheitsrichtlinien eingerichtet werden. Dazu können Konfigurationsdateien zentral erstellt und mittels geeigneter Mechanismen auf die Clients übertragen und dort installiert werden.

Bei der Beschreibung der Konfigurationen wird im Folgenden von einer Windows Server 2003/2008 Domänenstruktur in der AD-Funktionsebene "Windows Server 2003/2008" ausgegangen.

Für die sichere Konfiguration von Clients unter Windows 7 sind eine Reihe von Maßnahmen erforderlich, beginnend mit der Konzeption über die Umsetzung (Installation/Konfiguration) bis zum Betrieb. Die

Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Bei Einsatz von Windows 7 muss zunächst die geeignete Version ausgewählt (siehe M 2.440 *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*) und ihr Einsatz geplant werden (siehe M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* ). Dabei ist zu unterscheiden, ob eine Einsatzumgebung vollkommen neu entsteht, oder ob eine bestehende Umgebung auf das Betriebssystem Windows 7 migriert wird. Für den Einsatz von Windows 7 ist eine Sicherheitsrichtlinie zu erarbeiten. Es kann eine bereits existierende Sicherheitsrichtlinie an die Eigenschaften von Windows 7 angepasst oder eine neue, speziell auf die Eigenschaften von Windows 7 zugeschnittene Richtlinie erarbeitet werden (siehe M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*).

In einer Domänenumgebung können verschiedene Sicherheitseinstellungen mittels eines zentralen Verwaltungswerkzeugs wie Active Directory erstellt und gepflegt werden. Andere Sicherheitseinstellungen können zentral erzeugt und mit geeigneten Mitteln auf die Clients übertragen werden. In der Maßnahme M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* werden Hinweise und Empfehlungen zur Konfiguration von Clients unter Windows 7 gegeben.

Windows 7 unterstützt die Möglichkeit der Fernadministration der Clients und stellt außerdem Mittel zur Verfügung, durch Windows 7 per Fernadministration auf andere Systeme zuzugreifen. In der Planungsphase müssen bereits entsprechende Festlegungen getroffen werden, damit sich über die Fernadministration keine unberechtigten Personen auf dem Client anmelden können. Die relevanten Aspekte sind in der Maßnahme M 2.327 *Sicherheit beim Fernzugriff auf Clients ab Windows XP* beschrieben.

Um Windows 7 auf mobilen Rechnern einzusetzen, müssen bereits in der Planungsphase entsprechende Sicherheitsaspekte berücksichtigt werden. Die Maßnahme M 2.442 *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen* nennt die für Windows Vista und Windows 7-spezifischen Aspekte.

**Umsetzung**

In der Umsetzungsphase werden alle Maßnahmen ergriffen, die den sicheren Betrieb konkret vorbereiten. Dazu zählen insbesondere Maßnahmen zur Sicherheit bei der Installation und Grundkonfiguration des Systems.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, können die Windows 7 Systeme installiert werden. Die Installation muss mit besonderer Sorgfalt durchgeführt werden, siehe M 4.248 *Sichere Installation von Windows Client-Betriebssystemen*. Die für die Konfiguration eines Windows 7 Systems zu beachtenden Aspekte müssen während der Planungsphase ermittelt worden sein.

Um Software, die für ältere Windows-Versionen geschrieben wurden, unter Windows 7 sicher ausführen zu können, ist es notwendig, die verschiedenen Techniken (beispielsweise VirtualPC XP-Mode) zu kennen und diese sicher anzuwenden (siehe M 4.424 *Sicherer Einsatz älterer Software ab Windows 7*).

Windows 7 verfügt standardmäßig über viele Funktionen, die sich hauptsächlich an Privatanwender richten. Dazu gehört beispielsweise die Heimnetzgruppe für die Freigabe und den Zugriff auf Dienste in einem lokalen Netz. Diese müssen im Umfeld einer Institution eingeschränkt werden (siehe M 4.423 *Verwendung der Heimnetzgruppen-Funktion ab Windows 7*), um einen sicheren Betrieb eines Windows 7 Client im Netz zu gewährleisten.

Windows 7 muss vor dem dauerhaften Einsatz aktiviert werden . Hintergründe nennt M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*.

**Betrieb**

Die Umsetzung wird idealerweise zunächst in einer Testinstallation vorgenommen. Nach erfolgreichem Test erfolgt die Installation von Windows 7 auf den dafür vorgesehenen Clients und der Übergang zum Regelbetrieb. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Die im Regelbetrieb zu beachtenden Aspekte sind in M 4.146 *Sicherer Betrieb von Windows Client-Betriebssystemen* zusammengefasst.
- Ein Mittel zur Aufrechterhaltung der Sicherheit eines Windows 7 Systems ist die Überwachung des Systems beziehungsweise seiner Einzelkomponenten. Die hierfür relevanten Empfehlungen finden sich in M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*.
- Windows 7 Systeme sind wie andere IT-Systeme Sicherheitsrisiken ausgesetzt. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs auf ein akzeptables Maß zu verringern, müssen Windows 7 Systeme aktuell gehalten werden. Die entsprechenden Empfehlungen sind in M 4.249 *Windows Client-Systeme aktuell halten* zu finden.
- Für die zentrale Überwachung und Konfiguration der Sicherheitseinstellungen, Wartungseinstellungen und Problembehandlungen bietet Windows 7 die Funktion "Wartungscenter" an. Um den sicheren Einsatz des Wartungscenters zu gewährleisten, ist die Maßnahme M 4.420 *Sicherer Einsatz des Wartungscenters unter Windows 7* umzusetzen.
- Eine regelmäßige Prüfung der geltenden Sicherheitseinstellungen und generell der existierenden Sicherheitsrichtlinien ist ein wichtiger Beitrag zur Sicherheit der Windows 7 Systeme im laufenden Betrieb. Die dabei zu beachtenden Aspekte sind in M 2.330 *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP* zusammengefasst.
- Windows 7 bietet einige Verwaltungswerkzeuge an, deren Einsatz auch aus Sicherheitssicht empfehlenswert ist, da mit ihrer Hilfe unter anderem sicherheitsrelevante Konfigurationsfehler vermieden werden können. Im Weiteren sind diese Werkzeuge bei der Fehleranalyse oder bei der Revision nützlich (siehe M 4.243 *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*).
- Ein im Betrieb befindliches Windows 7 System muss unter bestimmten Voraussetzungen erneut aktiviert werden. Hinweise und Empfehlungen zur Reaktivierung finden sich in M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*.
- Bei Windows 7 kann, neben der unter Windows Vista eingeführten Festplattenverschlüsselung (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*), auch BitLocker To Go für die Verschlüsselung von Wechseldatenträgern genutzt werden. Die sicherheitsrelevanten Aspekte hinsichtlich der Nutzung dieser Applikation sind in der Maßnahme M 4.422 *Nutzung von BitLocker To Go ab Windows 7* beschrieben.

**Aussonderung**

Auf Clients, die einen Bereich verlassen oder ausgesondert werden, sind lokal gespeicherte Benutzerdaten zu löschen. Dies gilt auch für defekte Datenträger, die ausgetauscht werden. Können Daten auf Datenträgern nicht mehr zuverlässig gelöscht werden, ist der Datenträger in geeigneter Weise zu zerstören. Empfehlungen hierzu finden sich in B 1.15 *Löschen und Vernichten von Daten*.

Es ist zu beachten, dass ein Zugriff auf archivierte Daten gemäß den Archivierungsfristen erhalten bleiben muss, auch wenn das ursprünglich aufzeichnende IT-System ausgesondert wird.

**Notfallvorsorge**

Neben der Absicherung im laufenden Betrieb spielt auch die Notfallvorsorge eine wichtige Rolle. Hinweise zur Notfallvorsorge finden sich in M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*. Empfehlungen zur Datensicherung sind in M 6.78 *Datensicherung unter Windows Clients* enthalten.

**Maßnahmenbündel**

Nachfolgend wird das Maßnahmenbündel für den Baustein "Client unter Windows 7" vorgestellt.

**Planung und Konzeption**

- M 2.324 (A) *Einführung von Windows auf Clients ab Windows XP planen*
- M 2.325 (A) *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*

- M 2.326 (A) *Planung der Gruppenrichtlinien für Clients ab Windows XP*
- M 2.327 (B) *Sicherheit beim Fernzugriff auf Clients ab Windows XP*
- M 2.440 (A) *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*
- M 2.441 (A) *Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista*
- M 2.442 (B) *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen*
- M 4.147 (Z) *Sichere Nutzung von EFS unter Windows*
- M 4.243 (Z) *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*
- M 4.244 (A) *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*
- M 4.245 (A) *Basiseinstellungen für Windows Group Policy Objects*
- M 4.246 (A) *Konfiguration der Systemdienste auf Clients ab Windows XP*
- M 4.247 (A) *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*
- M 4.336 (A) *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.337 (Z) *Einsatz von BitLocker Drive Encryption*
- M 4.338 (A) *Einsatz von File und Registry Virtualization bei Clients ab Windows Vista*
- M 4.339 (B) *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*
- M 4.340 (A) *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*
- M 4.341 (A) *Integritätsschutz ab Windows Vista*
- M 4.342 (Z) *Aktivierung des Last Access Zeitstempels ab Windows Vista*
- M 4.425 (B) *Verwendung der Tresor- und Cardspace-Funktion auf Clients ab Windows*
- M 5.123 (B) *Absicherung der Netzkommunikation unter Windows*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 3.28 (A) *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*
- M 4.48 (A) *Passwortschutz unter Windows-Systemen*
- M 4.49 (A) *Absicherung des Boot-Vorgangs für ein Windows-System*
- M 4.75 (A) *Schutz der Registry unter Windows-Systemen*
- M 4.149 (A) *Datei- und Freigabeberechtigungen unter Windows*
- M 4.248 (A) *Sichere Installation von Windows Client-Betriebssystemen*
- M 4.419 (Z) *Anwendungssteuerung ab Windows 7 mit AppLocker*
- M 4.421 (C) *Absicherung der Windows PowerShell*
- M 4.423 (B) *Verwendung der Heimnetzgruppen-Funktion ab Windows 7*
- M 4.424 (Z) *Sicherer Einsatz älterer Software ab Windows 7*
- M 5.89 (A) *Konfiguration des sicheren Kanals unter Windows*
- M 5.90 (Z) *Einsatz von IPSec unter Windows*

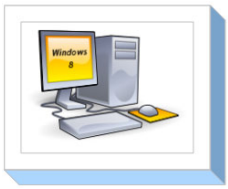
**Betrieb**

- M 2.330 (B) *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP*
- M 4.56 (C) *Sicheres Löschen unter Windows-Betriebssystemen*
- M 4.146 (A) *Sicherer Betrieb von Windows Client-Betriebssystemen*
- M 4.249 (A) *Windows Client-Systeme aktuell halten*
- M 4.343 (Z) *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.344 (B) *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*
- M 4.420 (A) *Sicherer Einsatz des Wartungscenters unter Windows 7*
- M 4.422 (Z) *Nutzung von BitLocker To Go ab Windows 7*

**Notfallvorsorge**

- M 6.76 (C) *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*
- M 6.78 (A) *Datensicherung unter Windows Clients*

# B 3.213 Client unter Windows 8




## Beschreibung

Mit Windows 8 hat Microsoft ein Client-Betriebssystem auf den Markt gebracht, bei dem einerseits die mit Windows 7 eingeführten Techniken und Komponenten fortentwickelt wurden, das andererseits aber insbesondere auf den Einsatz auf portablen Geräte ohne Hardware-Tastatur ausgerichtet ist, die bedient werden, indem der Bildschirm direkt berührt und damit als Eingabegerät verwendet wird.

Dies erfordert insbesondere ein neues Bedienkonzept für Anwendungen. Microsoft hat dazu neben den klassischen Desktop-Anwendungen auch eine Klasse mobiler Anwendungen zur Nutzung unter Windows 8 vorgesehen, die sogenannten "Apps". Apps sind konsequent auf die Steuerung durch Berührung ausgelegt. Zusätzlich können sie als "Kachel" auf dem Bildschirm Anzeigefunktionen wahrnehmen. Einige Anwendungen, allen voran der mit Windows 8 ausgelieferte Internet-Explorer, stehen entsprechend in zwei Varianten für Windows 8 zur Verfügung. Desktop-Anwendung und App können dabei auch parallel auf demselben System installiert sein und wechselseitig genutzt werden. Viele andere Anwendungen sind allerdings nur in der Desktop-Variante oder als App verfügbar.

Seit der Markteinführung von Windows 8 hat Microsoft einige Verbesserungen vorgenommen und in das Betriebssystem integriert, das damit die Versionsnummer 8.1 erhält. Dieser Baustein geht davon aus, dass eine Windows-8.1-Version im Einsatz ist. Soweit für die beschriebenen Sicherheitsmaßnahmen Abweichungen für Windows 8 bestehen, sind diese in den Texten ausgewiesen.

Die Struktur des Bausteins orientiert sich an der Struktur des Bausteins B 3.212 *Client unter Windows 7*, so dass bei einem Migrationsprojekt von Windows 7 auf Windows 8 eine leichte Anpassung der vorhandenen Sicherheitsrichtlinien möglich ist. Besondere Aufmerksamkeit muss in diesem Fall auf die integrierte Unterstützung des Trusted Platform Modules (TPM) sowie die Integration von Cloud-Funktionen in das Betriebssystem gerichtet werden, da für diese Bereiche in der Regel neue Sicherheitsabwägungen getroffen und dokumentiert werden müssen. Gleiches gilt auch für den Einsatz von Apps in der Institution sowie für die erweiterten Schutzmechanismen für Anwendungen. Hierzu finden sich Hinweise in den Hilfsmitteln zu diesem Baustein.

## Gefährdungslage

Die folgenden Gefährdungen sind beim Einsatz eines Client-Systems mit dem Betriebssystem Windows 8 relevant:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.62 *Ungeeigneter Umgang mit Sicherheitsvorfällen*
- G 2.202 *Lock-in-Effekt*
- G 2.203 *Integrierte Cloud-Funktionalität*
- G 2.204 *TPM-Nutzung*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*

- G 3.22 *Fehlerhafte Änderung der Registrierung*
- G 3.48 *Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen*
- G 3.97 *Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista*
- G 3.98 *Verlust von BitLocker-verschlüsselten Daten*
- G 3.112 *Unautorisierte oder falsche Nutzung von Images bei der Nutzung von Windows DISM*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.7 *Defekte Datenträger*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.23 *Automatische Erkennung von Wechseldatenträgern*
- G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*
- G 4.55 *Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP*
- G 4.73 *Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme von Windows-Versionen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.23 *Schadprogramme*
- G 5.52 *Missbrauch von Administratorrechten bei Windows-Betriebssystemen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.79 *Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Windows 8 stellt bereits einige Sicherheitsmechanismen in der Grundkonfiguration bereit. Andere Sicherheitsmechanismen müssen durch die Verantwortlichen erst eingerichtet werden. Die zentrale Konfiguration und Durchsetzung von technischen Sicherheitsmaßnahmen kann durch ein Active Directory (AD) unterstützt werden.

Wo die zentrale Konfigurationsmöglichkeit mittels AD nicht gegeben ist, müssen technische Maßnahmen dezentral auf den einzelnen Clients über lokale Sicherheitsrichtlinien eingerichtet werden. Dazu können Konfigurationsdateien zentral erstellt und mittels geeigneter Mechanismen auf die Clients übertragen und dort installiert werden.

Für die sichere Konfiguration von Clients unter Windows 8 sind eine Reihe von Maßnahmen erforderlich, beginnend mit der Konzeption über die Umsetzung (Installation/Konfiguration) bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Der sichere Einsatz von Windows-Clients setzt eine sorgfältige Planung voraus. Die dabei zu beachtenden Aspekte sind in der Maßnahme M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* beschrieben. Ist ein mobiler Einsatz vorgesehen, sind weitere Aspekte zu beachten (M 2.442 *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen*).

Zunächst ist die richtige Windows-Version für das Einsatzumfeld auszuwählen (M 2.440 *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*). Im betrieblichen Umfeld werden üblicherweise Volumenlizenzverträge für die Beschaffung von Windows-Lizenzen genutzt. Für die damit verbundene Aktivierung müssen die richtigen Voraussetzungen geschaffen werden, um die Verfügbarkeit

der Systeme sicherzustellen (M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

In der Planungsphase müssen auch die Sicherheitsvorgaben für den Einsatz von Windows 8 erarbeitet und in Form von Sicherheitsrichtlinien dokumentiert werden (M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP* Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP). Die Windows-eigenen Schutzfunktionen sollten genutzt werden, insbesondere die Benutzerkontensteuerung (M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*) und der Integritätsschutz (M 4.341 *Integritätsschutz ab Windows Vista*). Vorhandene Funktionen zur lokalen Speicherung von Passwörtern sollten nach Möglichkeit im betrieblichen Umfeld nicht genutzt werden (M 4.425 *Verwendung der Tresor- und Cardspace-Funktion auf Clients ab Windows* ).

In einer Windows-Domäne sollten die Sicherheitsvorgaben soweit wie möglich zentral über Gruppenrichtlinien konfiguriert und an die Clients ausgerollt werden (M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* und M 4.245 *Basiseinstellungen für Windows Group Policy Objects*).

Werden Clients von einer früheren Windows-Version migriert, so ist vorab die Kompatibilität der eingesetzten Anwendungen zu prüfen (M 2.441 *Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista*). Besonderheiten von Windows beim Umgang mit Legacy-Software sind dabei zu beachten (M 4.338 *Einsatz von File und Registry Virtualization bei Clients ab Windows Vista*).

Bei erhöhtem Schutzbedarf empfiehlt sich der Einsatz von Verschlüsselungsmechanismen auf dem Client. Windows 8 bringt hierfür EFS (M 4.147 *Sichere Nutzung von EFS unter Windows*) und BitLocker (M 4.337 *Einsatz von BitLocker Drive Encryption*) mit. Bestehen besondere Anforderungen an die Nachvollziehbarkeit der Informationsverarbeitung auf dem Client-System, sollte der Einsatz von Zeitstempeln für den Dateizugriff aktiviert werden (M 4.342 *Aktivierung des Last Access Zeitstempels ab Windows Vista*).

**Beschaffung**

Im Zuge der Beschaffung von Windows-8-Systemen sind einige Fragen zu klären, unter anderem zu den eingesetzten Editionen und der Auswahl einer 32- oder 64-Bit-Variante. Hilfestellung hierzu gibt M 2.559 *Beschaffung von Windows 8*.

**Umsetzung**

Wenn Windows-Clients aufgesetzt werden, müssen verschiedene Schutz-Aspekte berücksichtigt werden (M 4.248 *Sichere Installation von Windows Client-Betriebssystemen*). Die Manipulation von Client-Systemen sollte erschwert werden, indem der Boot-Vorgang geeignet abgesichert wird (M 4.49 *Absicherung des Boot-Vorgangs für ein Windows-System*), alle eingerichteten Benutzerkonten durch Passwörter geeigneter Stärke geschützt werden (M 4.48 *Passwortschutz unter Windows-Systemen*) und gegebenenfalls die Benutzerumgebung geeignet eingeschränkt wird (M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*).

Weitere wichtige Schutzmaßnahmen bestehen darin, die Registry abzusichern (M 4.75 *Schutz der Registry unter Windows-Systemen*) und die PowerShell einzuschränken (M 4.421 *Absicherung der Windows PowerShell*) sowie die Kommunikation mit der Domäne zu schützen (M 5.89 *Konfiguration des sicheren Kanals unter Windows*). Soweit ältere Software eingesetzt wird, sind gegebenenfalls ergänzende Schutzmaßnahmen erforderlich (M 4.424 *Sicherer Einsatz älterer Software ab Windows 7*).

Um die verarbeiteten Daten vor unbefugtem Zugriff zu schützen, müssen die Datei- und Freigabeberechtigungen restriktiv vergeben werden (M 4.149 *Datei- und Freigabeberechtigungen unter Windows*). Der Einsatz von Heimnetzgruppen sollte dabei unterbunden oder zumindest geregelt werden (M 4.423 *Verwendung der Heimnetzgruppen-Funktion ab Windows 7*).

Insbesondere die in Windows 8 integrierten Cloud-Funktionen bergen die Gefahr eines ungewollten Abflusses von Daten über die Systembenutzung. Entsprechende Gegenmaßnahmen finden sich in M 4.472 *Datensparsamkeit bei Windows 8*.

Bei erhöhtem Schutzbedarf kann die Kommunikation mit IPSec abgesichert werden (M 5.90 *Einsatz von IPSec unter Windows*). Mit AppLocker kann die Ausführung von Anwendungen kontrolliert und so ein guter Schutz gegen Schadsoftware und Manipulationen erzielt werden (M 4.419 *Anwendungssteuerung ab Windows 7 mit AppLocker*).

Die Benutzer der Client-Systeme müssen zu sicherheitsrelevanten Aspekten des Betriebssystems geeignet geschult werden (M 3.28 *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen* Schulung zu Sicherheitsmechanismen für Benutzer bei Windows-Client-Betriebssystemen).

**Betrieb**

Maßnahmen für den sicheren Betrieb von Windows-8-Clients sind in der Maßnahme M 4.146 *Sicherer Betrieb von Windows Client-Betriebssystemen* zusammengestellt. Angesichts immer wieder neuer veröffentlichter Sicherheitslücken ist es besonders wichtig, das Systems fortlaufend zu aktualisieren (M 4.249 *Windows Client-Systeme aktuell halten*).

Weitere betriebliche Aufgaben umfassen insbesondere, die Clients zu überwachen (M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*) und ihre Sicherheit regelmäßig zu überprüfen (M 2.330 *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP*).

Daten können auch dadurch ungewollt in die Hände Dritter gelangen, dass sie nicht vollständig gelöscht werden, wenn entsprechende Gegenmaßnahmen fehlen (M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*). Um Daten mit Hilfe von Wechselmedien sicher auszutauschen, kann zusätzlich die Verschlüsselungslösung BitLocker To Go eingesetzt werden (M 4.422 *Nutzung von BitLocker To Go ab Windows 7*).

**Notfallvorsorge**

Ein Ausfall in Client-Systemen ist in vielen Fällen unkritisch, da in der Institution ausreichend Ersatzgeräte vorhanden sind. Wenn jedoch besondere Hardware oder Software benötigt wird oder die Clients mobil eingesetzt werden, kann sich die Notfallvorsorge aufwändiger gestalten. Daher sollten auch Client-Systeme in einer Notfallplanung geeignet berücksichtigt werden (M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*). Eine zentrale Maßnahme ist dabei vor allem, die clientseitigen Programme und Daten regelmäßig zu sichern (M 6.78 *Datensicherung unter Windows Clients*).

**Planung und Konzeption**

- M 2.324 (A) *Einführung von Windows auf Clients ab Windows XP planen*
- M 2.325 (A) *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*
- M 2.326 (A) *Planung der Gruppenrichtlinien für Clients ab Windows XP*
- M 2.327 (B) *Sicherheit beim Fernzugriff auf Clients ab Windows XP*
- M 2.440 (A) *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*
- M 2.441 (A) *Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista*
- M 2.442 (B) *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen*
- M 4.147 (Z) *Sichere Nutzung von EFS unter Windows*
- M 4.243 (Z) *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*
- M 4.244 (A) *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*
- M 4.245 (A) *Basiseinstellungen für Windows Group Policy Objects*
- M 4.246 (A) *Konfiguration der Systemdienste auf Clients ab Windows XP*
- M 4.247 (A) *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*
- M 4.336 (A) *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.337 (Z) *Einsatz von BitLocker Drive Encryption*
- M 4.338 (A) *Einsatz von File und Registry Virtualization bei Clients ab Windows Vista*
- M 4.339 (B) *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*
- M 4.340 (A) *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*

- M 4.341 (A) *Integritätsschutz ab Windows Vista*
- M 4.342 (Z) *Aktivierung des Last Access Zeitstempels ab Windows Vista*
- M 4.425 (B) *Verwendung der Tresor- und Cardspace-Funktion auf Clients ab Windows*
- M 4.470 (W) *Grundlagenwissen zu Windows 8*
- M 4.471 (W) *Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8*
- M 5.123 (B) *Absicherung der Netzkommunikation unter Windows*

**Beschaffung**

- M 2.559 (A) *Beschaffung von Windows 8*

**Umsetzung**

- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 3.28 (A) *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*
- M 4.48 (A) *Passwortschutz unter Windows-Systemen*
- M 4.49 (A) *Absicherung des Boot-Vorgangs für ein Windows-System*
- M 4.75 (A) *Schutz der Registry unter Windows-Systemen*
- M 4.149 (A) *Datei- und Freigabeberechtigungen unter Windows*
- M 4.248 (A) *Sichere Installation von Windows Client-Betriebssystemen*
- M 4.419 (Z) *Anwendungssteuerung ab Windows 7 mit AppLocker*
- M 4.421 (C) *Absicherung der Windows PowerShell*
- M 4.423 (B) *Verwendung der Heimnetzgruppen-Funktion ab Windows 7*
- M 4.424 (Z) *Sicherer Einsatz älterer Software ab Windows 7*
- M 4.472 (Z) *Datensparsamkeit bei Windows 8*
- M 5.89 (A) *Konfiguration des sicheren Kanals unter Windows*
- M 5.90 (Z) *Einsatz von IPSec unter Windows*

**Betrieb**

- M 2.330 (B) *Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP*
- M 4.56 (C) *Sicheres Löschen unter Windows-Betriebssystemen*
- M 4.146 (A) *Sicherer Betrieb von Windows Client-Betriebssystemen*
- M 4.249 (A) *Windows Client-Systeme aktuell halten*
- M 4.343 (Z) *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*
- M 4.344 (B) *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*
- M 4.420 (A) *Sicherer Einsatz des Wartungscenters unter Windows 7*
- M 4.422 (Z) *Nutzung von BitLocker To Go ab Windows 7*

**Notfallvorsorge**

- M 6.76 (C) *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*
- M 6.78 (A) *Datensicherung unter Windows Clients*

# B 3.301 Sicherheitsgateway (Firewall)


## Beschreibung

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln. Dazu wird die technisch mögliche auf die in einer Sicherheitsleitlinie ordnungsgemäß definierte Kommunikation eingeschränkt. Sicherheit bei der Netzkopplung bedeutet hierbei die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen.

Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet-Intranet dar. Vielmehr können auch zwei organisationsinterne Netze unterschiedlich hohen Schutzbedarf besitzen, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Personalabteilung, in dem besonders schutzwürdige, personenbezogene Daten übertragen werden.

Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs "Firewall" soll verdeutlichen, dass zur Absicherung von Netzübergängen heute oft nicht mehr ein einzelnes Gerät verwendet wird, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs ("Intrusion Detection").

In diesem Baustein werden ausschließlich die für ein Sicherheitsgateway spezifischen Gefährdungen und Maßnahmen beschrieben. Zusätzlich sind noch die Gefährdungen und Maßnahmen zu betrachten, die für das IT-System, mit dem das Sicherheitsgateway realisiert wird, spezifisch sind. Oftmals werden Komponenten von Sicherheitsgateways auf einem Unix-System implementiert, in diesem Fall sind zusätzlich zu den im Folgenden beschriebenen Gefährdungen und Maßnahmen die in Baustein B 3.102 *Server unter Unix* beschriebenen zu beachten.

## Gefährdungslage

Für den IT-Grundschutz eines Sicherheitsgateways werden die folgenden typischen Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.24 *Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes*
- G 2.101 *Unzureichende Notfallvorsorge bei einem Sicherheitsgateway*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.11 *Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client*
- G 4.12 *Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client*
- G 4.20 *Überlastung von Informationssystemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.39 *Software-Konzeptionsfehler*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.24 *Wiedereinspielen von Nachrichten*

- G 5.25 *Maskerade*
- G 5.28 *Verhinderung von Diensten*
- G 5.39 *Eindringen in Rechnersysteme über Kommunikationskarten*
- G 5.48 *IP-Spoofing*
- G 5.49 *Missbrauch des Source-Routing*
- G 5.50 *Missbrauch des ICMP-Protokolls*
- G 5.51 *Missbrauch der Routing-Protokolle*
- G 5.78 *DNS-Spoofing*
- G 5.143 *Man-in-the-Middle-Angriff*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Sicherheitsgateway schützt nicht vor Angriffen, die innerhalb des internen Netzes erfolgen. Um das interne Netz gegen Angriffe von Innentätern zu schützen, müssen auch beim Einsatz eines Sicherheitsgateways alle erforderlichen Sicherheitsmaßnahmen umgesetzt sein. Wenn es sich bei dem internen Netz beispielsweise um ein Unix- bzw. PC-Netz handelt, sind die in den jeweiligen Bausteinen beschriebenen Sicherheitsmaßnahmen umzusetzen.

Das Sicherheitsgateway sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann das Sicherheitsgateway alternativ in einem Serverschrank aufgestellt werden (siehe Baustein B 2.7 *Schutzschränke*). Soll das Sicherheitsgateway nicht in Eigenregie, sondern von einem Dienstleister betrieben werden, so ist der Baustein B 1.11 *Outsourcing* anzuwenden. Insbesondere sollten die Empfehlungen in M 5.116 *Integration eines E-Mailservers in ein Sicherheitsgateway* beachtet werden.

Für den erfolgreichen Aufbau eines Sicherheitsgateways sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb der Komponenten. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Um Netze mit unterschiedlichem Schutzbedarf miteinander zu verbinden, sollte zunächst ein Konzept für die Netzkopplung mit Hilfe eines Sicherheitsgateways erstellt werden (siehe M 2.70 *Entwicklung eines Konzepts für Sicherheitsgateways*). Hierfür sind unter anderem zu betrachten:

- Festlegung der Sicherheitsziele
- Anpassung der Netzstruktur
- grundlegende Voraussetzungen

In einer sogenannten Policy für das Sicherheitsgateway ist festzulegen, welche Informationen, Dienste und Protokolle wie behandelt werden, also z. B. welche Dienste zugelassen werden und wer sie nutzen darf (siehe M 2.71 *Festlegung einer Policy für ein Sicherheitsgateway*). Dazu gehören die Aspekte:

- Auswahl der Kommunikationsanforderungen
- Auswahl der Dienste (Vor der Diensteauswahl sollten die Erläuterungen und Randbedingungen aus M 5.39 *Sicherer Einsatz der Protokolle und Dienste* gelesen werden.)
- Organisatorische Regelungen

Außerdem muss eine Sicherheitsrichtlinie für das Sicherheitsgateway erstellt werden, in der Regelungen und Hinweise zum sicheren Betrieb und zur sicheren Administration des Sicherheitsgateways bzw. seiner einzelnen Komponenten beschrieben sind (siehe M 2.299 *Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway*).

Um die Netze der Institution sicher ans Internet anzubinden, muss zusätzlich eine Konzeption für die Art der Internet-Anbindung und deren zuverlässige Absicherung ausgearbeitet werden (siehe M 2.476 *Konzeption für die sichere Internet-Anbindung*).

**Beschaffung**

Vor der Beschaffung der Komponenten des Sicherheitsgateways sollte ein für die jeweilige Institution passender Grundaufbau für das Sicherheitsgateway ausgewählt werden (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*). Kriterien für die Beschaffung von Paketfiltern und Application-Level-Gateways finden sich in M 2.74 *Geeignete Auswahl eines Paketfilters* und M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*.

Es gibt verschiedene Möglichkeiten, einen Internetzugang herzustellen. Neben der passenden Zugangstechnik muss auch ein Internet Service Provider (ISP) ausgewählt werden. Dieser sorgt für den Anschluss an einen Einwahlknoten und kann auch weitere Leistungen anbieten (siehe M 2.176 *Geeignete Auswahl eines Internet Service Providers*).

**Umsetzung**

Um ein Sicherheitsgateway geeignet aufzubauen, sollten unter anderem folgende Aspekte umgesetzt werden:

- Filterregeln aufstellen und implementieren (siehe M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln*)
- Umsetzung der IT-Grundschutz-Maßnahmen für die Komponenten des Sicherheitsgateways
- Umsetzung der IT-Grundschutz-Maßnahmen, die IT-Systeme des internen Netzes überprüfen
- Randbedingungen für sicheren Einsatz der einzelnen Protokolle und Dienste beachten (siehe M 5.39 *Sicherer Einsatz der Protokolle und Dienste*)
- Einbindung weiterer Komponenten (siehe M 2.77 *Integration von Servern in das Sicherheitsgateway*)

**Betrieb**

Um ein Sicherheitsgateway dauerhaft sicher zu betreiben, sind eine Reihe von Maßnahmen erforderlich (siehe M 2.78 *Sicherer Betrieb eines Sicherheitsgateways*). Dazu gehören unter anderem:

- Regelmäßige Kontrolle der Einstellungen auf Korrektheit und Aktualität
- Anpassung an Änderungen und Tests
- Protokollierung der Sicherheitsgateway-Aktivitäten sowie Auswertung der Protokolldaten (siehe M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*)
- Notfallvorsorge für das Sicherheitsgateway (ergänzend siehe Baustein B 1.3 *Notfallmanagement*
- Datensicherung (siehe Baustein B 1.4 *Datensicherungskonzept*)

**Aussonderung**

Komponenten des Sicherheitsgateways können eine Vielzahl sicherheitsrelevanter Daten wie Konfigurations- oder Passwortdateien enthalten. Daher müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden, bevor sie ausgesondert werden (siehe M 2.300 *Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways*).

**Notfallvorsorge**

Fehler oder Ausfälle eines Sicherheitsgateways oder auch nur einzelner Komponenten können unmittelbare und schwerwiegende Auswirkungen haben. Daher muss ausreichende Vorsorge für Notfälle getroffen werden (siehe M 6.49 *Datensicherung einer Datenbank*).

Es kann verschiedene Gründe geben, sich gegen den Einsatz eines Sicherheitsgateways zu entscheiden. Dies können die Anschaffungskosten oder der Administrationsaufwand sein, aber auch die Tatsache, dass die bestehenden Restrisiken nicht in Kauf genommen werden können. Falls trotzdem ein Anschluss an das Internet gewünscht ist, kann alternativ ein Stand-alone-System eingesetzt werden (siehe M 5.46 *Einsatz von Stand-alone-Systemen zur Nutzung des Internets*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Sicherheitsgateway" vorgestellt.

**Planung und Konzeption**
- M 2.70 (A) *Entwicklung eines Konzepts für Sicherheitsgateways*
- M 2.71 (A) *Festlegung einer Policy für ein Sicherheitsgateway*
- M 2.299 (A) *Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway*
- M 2.301 (Z) *Outsourcing des Sicherheitsgateway*
- M 2.476 (A) *Konzeption für die sichere Internet-Anbindung*

**Beschaffung**
- M 2.73 (A) *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*
- M 2.74 (A) *Geeignete Auswahl eines Paketfilters*
- M 2.75 (A) *Geeignete Auswahl eines Application-Level-Gateways*
- M 2.176 (Z) *Geeignete Auswahl eines Internet Service Providers*

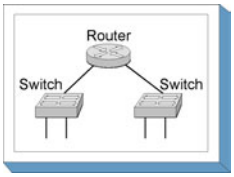
**Umsetzung**
- M 2.76 (A) *Auswahl und Einrichtung geeigneter Filterregeln*
- M 2.77 (A) *Integration von Servern in das Sicherheitsgateway*
- M 3.43 (C) *Schulung der Administratoren des Sicherheitsgateways*
- M 4.224 (Z) *Integration von VPN-Komponenten in ein Sicherheitsgateway*

**Betrieb**
- M 2.78 (A) *Sicherer Betrieb eines Sicherheitsgateways*
- M 2.302 (Z) *Sicherheitsgateways und Hochverfügbarkeit*
- M 4.47 (A) *Protokollierung der Sicherheitsgateway-Aktivitäten*
- M 4.100 (C) *Sicherheitsgateways und aktive Inhalte*
- M 4.101 (C) *Sicherheitsgateways und Verschlüsselung*
- M 4.222 (B) *Festlegung geeigneter Einstellungen von Sicherheitsproxies*
- M 4.223 (B) *Integration von Proxy-Servern in das Sicherheitsgateway*
- M 4.225 (Z) *Einsatz eines Protokollierungsservers in einem Sicherheitsgateway*
- M 4.226 (Z) *Integration von Virenscannern in ein Sicherheitsgateway*
- M 4.227 (C) *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*
- M 5.39 (A) *Sicherer Einsatz der Protokolle und Dienste*
- M 5.46 (A) *Einsatz von Stand-alone-Systemen zur Nutzung des Internets*
- M 5.59 (A) *Schutz vor DNS-Spoofing bei Authentisierungsmechanismen*
- M 5.70 (A) *Adreßumsetzung - NAT (Network Address Translation)*
- M 5.71 (Z) *Intrusion Detection und Intrusion Response Systeme*
- M 5.115 (Z) *Integration eines Webservers in ein Sicherheitsgateway*
- M 5.116 (Z) *Integration eines E-Mailservers in ein Sicherheitsgateway*
- M 5.117 (Z) *Integration eines Datenbank-Servers in ein Sicherheitsgateway*
- M 5.118 (Z) *Integration eines DNS-Servers in ein Sicherheitsgateway*
- M 5.119 (Z) *Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway*
- M 5.120 (A) *Behandlung von ICMP am Sicherheitsgateway*

**Aussonderung**
- M 2.300 (C) *Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways*

**Notfallvorsorge**
- M 6.94 (C) *Notfallvorsorge bei Sicherheitsgateways*

# B 3.302 Router und Switches




## Beschreibung

Netze spielen eine immer wichtigere Rolle als Teile der IT-Infrastruktur, weil Anwendungen heutzutage vermehrt über lokale Netze oder Weitverkehrsnetze betrieben werden. Die Verfügbarkeit, Integrität und Vertraulichkeit der Netze muss sichergestellt sein und mindestens den Anforderungen der Anwendungen an den Schutz dieser drei Grundwerte der Informationssicherheit entsprechen.

Ein Netz besteht aus aktiver und passiver Netztechnik. Als passive Netztechnik wird in erster Linie die strukturierte Verkabelung verstanden. Hierzu gehören Patch-Felder (über Steckfelder konfigurierbare Kabelverteiler), Schutzschränke und Anschlussdosen am Arbeitsplatz. Zur aktiven Netztechnik gehören beispielsweise Hubs, Bridges, Switches und Router. In modernen Netzen ersetzen Switches heutzutage vielfach Hubs sowie Bridges. Ein Ausfall einer oder mehrerer Komponenten der aktiven Netztechnik (Router und Switches) kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Da diese Komponenten die Basis und das Rückgrat der IT-Infrastruktur bilden, müssen Router und Switches vor unerlaubten Zugriffen und Manipulationen geschützt werden.

Die Funktionsweise von Routern ist in M 2.276 *Funktionsweise eines Routers* beschrieben. Die Maßnahme M 2.277 *Funktionsweise eines Switches* beschreibt die Funktionsweise eines Switches. Die wichtigsten funktionalen Unterschiede der in der folgenden Abbildung dargestellten aktiven Netzkomponenten werden kurz erklärt.

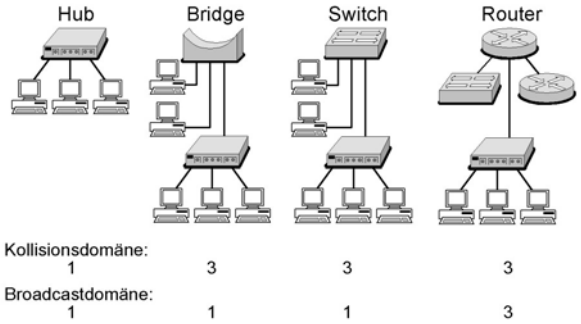



Abbildung: Hub, Bridge, Switch und Router

### Kollisionsdomäne

Unter einer Kollisionsdomäne wird ein einzelnes Segment beim Netzzugangsverfahren CSMA/CD (Carrier Sense Multipe Access with Collision Detection) verstanden. Alle Geräte, die im selben Segment angeschlossen sind, sind Bestandteil dieser Kollisionsdomäne. Versuchen zwei Geräte, zum gleichen Zeitpunkt ein Paket ins Netz zu senden, so spricht man von einer Kollision. Beide Geräte warten dann einen bestimmten Zeitraum zufällig gewählter Länge und versuchen dann erneut, das Paket zu senden. Durch diese Wartezeit verringert sich die effektive Bandbreite, die den Geräten zur Verfügung steht.

### Broadcast-Domäne

Broadcast-Informationen sind nicht an ein bestimmtes Endgerät gerichtet, sondern an alle "benachbarten" Endgeräte. Diejenigen Geräte in einem Netz, die die jeweiligen Broadcast-Informationen der anderen Geräte empfangen, bilden zusammen eine Broadcast-Domäne. Geräte, die in einer Broadcast-Domäne zusammen gefasst sind, müssen sich nicht in derselben Kollisionsdomäne befinden. Beim IP-Protokoll spricht man in diesem Fall auch von einem IP-Subnetz. Beispielsweise bilden die Stationen mit den IP-Adressen von 192.168.1.1 bis 192.168.1.254 in einem IP-Subnetz mit einer Subnetzmaske von 255.255.255.0 eine Broadcast-Domäne.

**Hub**

Hubs arbeiten auf der OSI Schicht 1 (Bitübertragungsschicht). Alle angeschlossenen Geräte befinden sich in derselben Kollisionsdomäne und damit auch in derselben Broadcast-Domäne. Hubs werden heutzutage durch Access-Switches (siehe M 2.277 *Funktionsweise eines Switches*) abgelöst.

**Bridge**

Bridges verbinden Netze auf der OSI Schicht 2 (Sicherungsschicht) und segmentieren Kollisionsdomänen. Jedes Segment bzw. Port an einer Bridge bildet eine eigene Kollisionsdomäne. Alle angeschlossenen Stationen sind im Normalfall Bestandteil einer Broadcast-Domäne. Bridges können auch dazu dienen, Netze mit unterschiedlichen Topographien (Ethernet, Token Ring, FDDI, etc.) auf der OSI Schicht 2 miteinander zu verbinden (transparent bridging, translational bridging). Hauptsächlich wurden Bridges zur Lastverteilung in Netzen eingesetzt. Die Entlastung wird dadurch erzielt, dass eine Bridge als zentraler Übergang zwischen zwei Netzsegmenten nicht mehr jedes Datenpaket weiterleitet. Eine Bridge hält eine interne MAC-Adresstabelle vor, aus der hervorgeht, in welchem angeschlossenen Segment entsprechende MAC-Adressen vorhanden sind. Wenn die Bridge beispielsweise aus dem Teilsegment A ein Datenpaket für eine Station im Teilsegment B erhält, wird das Datenpaket weitergeleitet. Falls die Bridge hingegen ein Datenpaket aus dem Teilsegment A für eine Station aus dem Teilsegment A empfängt, wird dieses Datenpaket nicht in das Teilsegment B übertragen. Dadurch wird eine Entlastung des Teilsegments B erreicht. Heutzutage werden Bridges durch Switches ersetzt.

**Layer-2-Switch**

Herkömmliche Layer-2-Switches verbinden Netze auf der OSI Schicht 2. Jeder Switch-Port bildet eine eigene Kollisionsdomäne. Normalerweise sind alle angeschlossenen Stationen Bestandteil einer Broadcast-Domäne. Das bedeutet, dass ein Layer-2-Switch die Ziel-MAC-Adresse im MAC-Header als Entscheidungskriterium dafür verwendet, auf welchen Port eingehende Datenpakete weitergeleitet werden. Trotz der vergleichbaren Funktionsweise gibt es zwei wesentliche Unterschiede zu Bridges:

- Ein Switch verbindet in der Regel wesentlich mehr Teilsegmente miteinander als eine Bridge.
- Der Aufbau eines Switches basiert auf sogenannten Application Specific Interface Circuits (ASICs). Dadurch ist ein Switch in der Lage, Datenpakete wesentlich schneller als eine Bridge von einem Segment in ein anderes zu transportieren. Unterschiedliche Switching-Technologien sind in M 2.277 *Funktionsweise eines Switches* beschrieben.

Gelegentlich werden Switches auch als *Multiport Bridges* bezeichnet.

**Router**

Router arbeiten auf der OSI Schicht 3 (Netzschicht) und vermitteln Datenpakete anhand der Ziel-IP-Adresse im IP-Header. Jedes Interface an einem Router stellt eine eigene Broadcast-Domäne und damit auch eine Kollisionsdomäne dar. Router sind in der Lage, Netze mit unterschiedlichen Topographien zu verbinden. Router werden verwendet, um lokale Netze zu segmentieren oder um lokale Netze über Weitverkehrsnetze zu verbinden. Ein Router identifiziert eine geeignete Verbindung zwischen dem Quellsystem beziehungsweise Quellnetz und dem Zielsystem beziehungsweise Zielnetz. In den meisten Fällen geschieht dies durch die Weitergabe des Datenpaketes an den nächsten Router, den sogenannten Next Hop. Weitergehende Aspekte sind in M 2.276 *Funktionsweise eines Routers* beschrieben.

Router müssen jedes IP-Paket vor der Weiterleitung analysieren. Dies führt zu Verzögerungen und damit im Vergleich zu "klassischen" Switches zu einem geringeren Datendurchsatz.

**Layer-3-Switch und Layer-4-Switch**

Layer-3- und Layer-4-Switches sind Switches, die zusätzlich eine Routing-Funktionalität bieten. Layer-2-Switches verwenden die Ziel-MAC-Adresse im MAC-Header eines Paketes zur Entscheidung, zu welchem Port Datenpakete weitergeleitet werden. Ein Layer-3-Switch behandelt Datenpakete beim ersten Mal wie ein Router (Ziel-IP-Adresse im IP-Header). Alle nachfolgenden Datenpakete des Senders an diesen Empfänger werden daraufhin jedoch auf der OSI Schicht 2 (Ziel-MAC-Adresse im MAC-Header)

weitergeleitet. Dadurch kann ein solcher Switch eine wesentlich höhere Durchsatzrate erzielen als ein herkömmlicher Router.

Ein weiteres Unterscheidungsmerkmal zwischen einem Router und einem Layer-3-Switch ist die Anzahl von Ports zum Anschluss von einzelnen Endgeräten. Ein Layer-3-Switch verfügt in der Regel über eine wesentlich größere Portdichte.

Durch die Routing-Funktion können Layer-3 oder Layer-4-Switches in lokalen Netzen herkömmliche LAN-to-LAN-Router ersetzen.

**Abgrenzung**

In diesem Baustein werden Gefährdungen und Maßnahmen beim Einsatz von Routern und Switches beschrieben. Die Abgrenzung zwischen Routern und Switches wird durch die Einführung der Bezeichnungen Layer-2-Switch, Layer-3-Switch oder Layer-4-Switch durch verschiedene Hersteller erschwert. Durch die Verschmelzung der Funktionen von Routern und Switches kann der Großteil der beschriebenen Maßnahmen sowohl auf Router als auch auf Switches angewendet werden.

Es ist eine große Auswahl von unterschiedlichen Routern und Switches von verschiedenen Herstellern am Markt verfügbar. Die Beschreibung der Maßnahmen und Gefährdungen in diesem Baustein ist so gehalten, dass sie so weit wie möglich herstellerunabhängig ist.

Neben den übergreifenden Aspekten und den infrastrukturellen Maßnahmen ist bei dem Einsatz von Routern und Switches der Baustein B 4.1 *Lokale Netze* zu berücksichtigen. Speziell bei der Einbindung der aktiven Netzkomponenten in ein umfassendes Netz- und Systemmanagement ist der Baustein B 4.2 *Netz- und Systemmanagement* von Bedeutung. Bei der Verwendung eines Routers als Paketfilter oder als Einwahlmöglichkeit sind zusätzlich die Bausteine B 3.301 *Sicherheitsgateway (Firewall)* und B 4.4 *VPN* zu berücksichtigen.

Neben eigens dafür hergestellten Geräten bieten auch verschiedene Betriebssysteme (beispielsweise diverse Unix-Derivate, Windows 2000, etc.) Routing-Funktionalität. Das bedeutet, dass ein Router aus einem entsprechenden Rechner mit zwei oder mehr Netzwerkkarten und einem Standardbetriebssystem bestehen kann. In kleineren lokalen Netzen kann dies unter Umständen eine kostengünstige Alternative sein. Neben den in diesem Baustein beschriebenen Sicherheitsmaßnahmen sind beim Betrieb eines solchen Routers die Sicherheitsmaßnahmen des eingesetzten Betriebssystems (Unix, Windows 2000, etc.) zu berücksichtigen.

## Gefährdungslage

Neben den Gefährdungen, die generell für den Großteil der IT-Systeme gelten, existieren für aktive Netzkomponenten eine Reihe spezieller Gefährdungen.

Diese Gefährdungen basieren oft auf bekannten Schwachstellen in den verwendeten Protokollen, wie TCP, UDP, IP oder ICMP. Durch Schwachstellen in dynamischen Routing-Protokollen können beispielsweise Routing-Tabellen auf Routern modifiziert werden. Die oft fehlende oder unzureichende Möglichkeit zur Authentisierung auf aktiven Netzkomponenten ist als weitere Gefährdung anzufügen.

Aktive Netzkomponenten werden oft mit einer unsicheren Default-Konfiguration ausgeliefert (siehe G 4.49 *Unsichere Default-Einstellungen auf Routern und Switches*), die bei der Inbetriebnahme der Geräte geprüft werden sollte. Für die sichere Trennung von Teilnetzen mit unterschiedlichem Schutzbedarf wird gelegentlich die Nutzung von virtuellen Netzen (VLANs) vorgeschlagen. Es sind jedoch einige Angriffsmethoden bekannt, die es ermöglichen, die Grenzen zwischen VLANs zu überwinden und unberechtigt auf andere VLANs zuzugreifen (siehe G 5.115 *Überwindung der Grenzen zwischen VLANs*).

Nachfolgend ist die Gefährdungslage beim Einsatz von Routern und Switches als Übersicht dargestellt:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*

- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.44 *Inkompatible aktive Netzkomponenten*
- G 2.54 *Vertraulichkeitsverlust durch Restinformationen*
- G 2.98 *Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches*

**Menschliche Fehlhandlungen**

- G 3.64 *Fehlerhafte Konfiguration von Routern und Switches*
- G 3.65 *Fehlerhafte Administration von Routern und Switches*

**Technisches Versagen**

- G 4.49 *Unsichere Default-Einstellungen auf Routern und Switches*

**Vorsätzliche Handlungen**

- G 5.4 *Diebstahl*
- G 5.51 *Missbrauch der Routing-Protokolle*
- G 5.66 *Unberechtigter Anschluss von IT-Systemen an ein Netz*
- G 5.112 *Manipulation von ARP-Tabellen*
- G 5.113 *MAC-Spoofing*
- G 5.114 *Missbrauch von Spanning Tree*
- G 5.115 *Überwindung der Grenzen zwischen VLANs*

**Maßnahmenempfehlungen**

Die diesem Baustein zugeordneten Sicherheitsmaßnahmen orientieren sich an dem Lebenszyklus der aktiven Netzkomponenten. Es werden Maßnahmen beschrieben, die in folgende Zyklen kategorisiert sind:

- Planung und Konzeption des Einsatzes von Routern und Switches
  Der Einsatz von Routern und Switches muss sorgfältig geplant werden. Die Funktionen von Routern und Switches sind in M 2.276 *Funktionsweise eines Routers* und M 2.277 *Funktionsweise eines Switches* beschrieben. Typische Einsatzszenarien von Routern und Switches, die bei der Planung und Konzeption hilfreich sein können, sind in M 2.278 *Typische Einsatzszenarien von Routern und Switches* zu finden.
- Festlegung einer Sicherheitsstrategie für Router und Switches
  Vor der Beschaffung aktiver Netzkomponenten (siehe M 2.280 *Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches*) ist eine Sicherheitsstrategie für den sicheren Betrieb der Geräte festzulegen und zu dokumentieren (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*). Anschließend können geeignete Netzkoppelelemente ausgewählt werden, die anschließend sicher in die bestehende Netzinfrastruktur zu integrieren sind. In dieser Phase ist es zudem wichtig, die Administratoren für die sichere Administration zu schulen (siehe M 3.38 *Administratorenschulung für Router und Switches*).
- Konfiguration und Inbetriebnahme von Routern und Switches
  Bei der Konfiguration und Inbetriebnahme von Routern und Switches ist eine Reihe von wichtigen Sicherheitsmaßnahmen zu berücksichtigen. Unsichere Default-Konfigurationen von Netzkomponenten stellen oft ein erhebliches Sicherheitsrisiko dar. Deswegen muss die Konfiguration bei der Inbetriebnahme überprüft und angepasst werden.
  Bei der Inbetriebnahme von Routern und Switches spielt die sichere Einrichtung der Systeme eine große Rolle (siehe M 4.201 *Sichere lokale Grundkonfiguration von Routern und Switches* und M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches*). Beim Einsatz von Routern muss zudem darauf geachtet werden, dass die Routing-Protokolle sicher eingesetzt werden. Abhängig vom Einsatzzweck sollten auf Routern Access Control Lists (ACLs) konfiguriert werden (siehe M 5.111 *Einrichtung von Access Control Lists auf Routern*). Hierbei, aber auch im normalen Betrieb, muss die Systemkonfiguration sorgfältig dokumentiert werden (siehe M 2.281 *Dokumentation der Systemkonfiguration von Routern und Switches*).
  Router werden außerdem oft zur sicheren Einwahl und zur Etablierung von virtuellen privaten Netzen (VPNs) verwendet. Bei der Einrichtung von VLANs auf Switches sind einige Sicherheitsaspekte zu berücksichtigen. Zusammenfassend ist in M 4.203 *Konfigurations-Checkliste für Router und Switches* eine Checkliste zur sicheren Konfiguration von Routern und Switches dokumentiert.

- Sicherer Betrieb von Routern und Switches
  Hinweise zum sicheren Betrieb von Routern und Switches finden sich in M 2.282 *Regelmäßige Kontrolle von Routern und Switches*, M 2.283 *Software-Pflege auf Routern und Switches* und M 6.91 *Datensicherung und Recovery bei Routern und Switches* gegeben. Aspekte der Protokollierung auf Routern und Switches werden in M 4.205 *Protokollierung bei Routern und Switches* beschrieben. Sicherheitsaspekte, die im Fall einer Störung wichtig sind, werden in M 6.92 *Notfallvorsorge bei Routern und Switches* beschrieben.
- Sicherheitsaspekte bei der Außerbetriebnahme von Routern und Switches
  Gespeicherte Konfigurationsdateien und Log-Dateien auf Routern und Switches verraten Informationen über die Netzstruktur. Bei der Außerbetriebnahme aktiver Netzkomponenten sind die Hinweise aus M 2.284 *Sichere Außerbetriebnahme von Routern und Switches* zu berücksichtigen.

Nachfolgend sind die beim Einsatz von Routern und Switches zu berücksichtigenden Maßnahmen aufgelistet:

**Planung und Konzeption**
- M 2.276 (Z) *Funktionsweise eines Routers*
- M 2.277 (Z) *Funktionsweise eines Switches*
- M 2.278 (Z) *Typische Einsatzszenarien von Routern und Switches*
- M 2.279 (A) *Erstellung einer Sicherheitsrichtlinie für Router und Switches*

**Beschaffung**
- M 2.280 (C) *Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches*

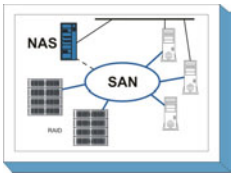
**Umsetzung**
- M 1.43 (A) *Gesicherte Aufstellung aktiver Netzkomponenten*
- M 3.38 (B) *Administratorenschulung für Router und Switches*
- M 4.201 (A) *Sichere lokale Grundkonfiguration von Routern und Switches*
- M 4.202 (A) *Sichere Netz-Grundkonfiguration von Routern und Switches*
- M 4.203 (A) *Konfigurations-Checkliste für Router und Switches*
- M 5.111 (C) *Einrichtung von Access Control Lists auf Routern*

**Betrieb**
- M 2.281 (A) *Dokumentation der Systemkonfiguration von Routern und Switches*
- M 2.282 (A) *Regelmäßige Kontrolle von Routern und Switches*
- M 2.283 (B) *Software-Pflege auf Routern und Switches*
- M 4.204 (C) *Sichere Administration von Routern und Switches*
- M 4.205 (C) *Protokollierung bei Routern und Switches*
- M 4.206 (C) *Sicherung von Switch-Ports*
- M 5.112 (C) *Sicherheitsaspekte von Routing-Protokollen*

**Aussonderung**
- M 2.284 (C) *Sichere Außerbetriebnahme von Routern und Switches*

**Notfallvorsorge**
- M 6.91 (C) *Datensicherung und Recovery bei Routern und Switches*
- M 6.92 (C) *Notfallvorsorge bei Routern und Switches*

# B 3.303 Speicherlösungen / Cloud Storage




## Beschreibung

Speicherlösungen dienen Institutionen zur Speicherung ihrer digitalen Daten. Das stetige Wachstum dieser Daten und das zunehmende Aufkommen unstrukturierter Daten bedingen den effizienten Einsatz moderner Speicherlösungen innerhalb einer Institution. Dabei unterliegen die Anforderungen an solche Speicherlösungen ebenfalls einem Wandel, der sich beispielsweise an folgenden Aspekten beobachten lässt:

- Die Daten einer Institution sollen jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein. Dadurch gelten für moderne Speicherlösungen häufig gestiegene Verfügbarkeitsanforderungen.
- Die Veränderung der Arbeitsweise hin zur Arbeit in verteilten Teams bedingt in vielen Institutionen eine wachsende Vielfalt von Anwendungen, die Zugriff auf Daten benötigen.
- Die zunehmende Digitalisierung sämtlicher Informationen in einer Institution macht es notwendig, dass weitreichende rechtliche Vorgaben (Compliance-Anforderungen) beachtet und eingehalten werden.
- Speicherlösungen sollen dynamisch an die sich stetig ändernden Anforderungen anpassbar sein und Speicherplatz zentral bereitstellen können.

In der Vergangenheit wurden Speicherlösungen oft durch den direkten Anschluss eines Speichermediums an einen Server umgesetzt. Diese sogenannten Direct-Attached-Storage (DAS)-Systeme können die aktuellen und zukünftigen Anforderungen in der Regel jedoch nicht mehr abdecken. Daneben bringen sie häufig stark steigende Kosten durch wachsenden Hardware- und Administrationsbedarf mit sich. Außerdem funktionieren neue Techniken wie die Live-Migration von Daten innerhalb von und über Speichersysteme hinweg nicht mit DAS. Direct-Attached-Storage-Lösungen können zudem nicht effizient verwaltet werden. Der Einsatz zentraler Speicherlösungen wird somit bereits seit Längerem als notwendig angesehen und ist in der Praxis weit verbreitet. In diesem Zusammenhang behandelt dieser Baustein:

- Speicherlösungen: Eine Speicherlösung besteht aus einem oder mehreren Speichernetzen sowie mindestens einem Speichersystem.
- Speichernetze: Speichernetze ermöglichen einerseits den Zugriff auf die Speichersysteme, andererseits die Replikation von Daten zwischen Speichersystemen.
- Speichersysteme: Als Speichersystem wird die zentrale Instanz bezeichnet, die für andere Systeme Speicherplatz zur Verfügung stellt. Der Einsatz eines Speichersystems erlaubt daneben den zeitgleichen Zugriff mehrerer Systeme (z. B. virtueller und physischer Server, Clients) auf den vorhandenen Speicherplatz.

Datensicherungsgeräte, die an das Speichersystem oder an das Speichernetz angeschlossen sind, werden im Baustein B 1.12 *Archivierung* betrachtet. Konzeptionelle Aspekte der Datensicherung werden im Baustein B 1.4 *Datensicherungskonzept* erläutert.

Die Realisierung zentraler Speicherlösungen ist in Abhängigkeit vom Einsatzszenario und den damit verbundenen Anforderungen auf unterschiedliche Art und Weise möglich:

**Network Attached Storage (NAS)** stellt über die Protokolle NFS (Network File System) und CIFS (Common Internet File System) Zugriffe auf die Speichersysteme zur Verfügung. Der Hauptanwendungsfall besteht darin, Fileserverdienste zur Verfügung zu stellen. Viele Anbieter verwenden deshalb den Begriff "Filer" für solche Systeme.

Für NAS-Systeme ist daher auch zusätzlich der Baustein B 3.101 *Allgemeiner Server* anzuwenden.

**Storage Area Networks (SAN)** werden in der Regel durch ein dediziertes Speichernetz zwischen Speichersystemen und angeschlossenen Servern oder Endgeräten geschaffen. SANs wurden für die seriel-

le, sehr schnelle und kontinuierliche Übertragung großer Datenmengen konzipiert. Sie basieren heute für hochverfügbare, hochperformante Installationen auf der Implementierung des Fibre-Channel- oder IP-Protokolls sowie alternativ auf einer entsprechenden Kombination in Form von Fibre Channel over Ethernet (FCoE).

Für Speichernetze ist daher auch der Baustein B 4.1 *Lokale Netze* anzuwenden.

Neben diesen weitverbreiteten Speichersystemen und Speichernetzen sind weitere Varianten zu betrachten:

Speichersysteme, die sowohl über NAS als auch SAN Daten zur Verfügung stellen können, werden oft unter der Bezeichnung **Hybrid-Storage** oder kombiniertes Speichersystem (**Unified Storage**) geführt. Nach außen kann ein solches Speichersystem sowohl als NAS als auch als SAN betrieben werden. Dieser Mischbetrieb wird dadurch ermöglicht, dass entsprechende Systemkomponenten eingesetzt und entsprechend konfiguriert werden. So kann sich ein Speichersystem sowohl für einige Anwendungen per Ethernet-Anschluss als "Filer" präsentieren und somit Fileservices über CIFS und NFS zur Verfügung stellen als auch für andere Server per Fibre Channel, Fibre Channel over Ethernet oder iSCSI Speicherkapazität zugänglich machen.

Für Hybrid-Systeme sind daher auch die Bausteine B 3.101 *Allgemeiner Server* und B 4.1 *Lokale Netze* anzuwenden.

**Objekt-Storage** (oftmals auch als **Object-based Storage** bezeichnet) ermöglicht gegenüber den traditionellen blockbasierten und filebasierten Zugriffsmethoden einen objektbasierten Zugriff auf Daten.

Objektbasierende Speicherlösungen speichern Daten in Verbindung mit den zugehörigen Metadaten auf einem Datenträger in Form von Objekten und nicht in Form von Dateien. Mittels der Vergabe einer eindeutigen Objekt-ID (Hash-Wert), die in den Metadaten des Objekts festgehalten wird, kann das Objekt eindeutig identifiziert werden. Der Zugriff auf einen objektbasierenden Speicher erfolgt über eine führende Anwendung. Die Anwendung greift hierbei über eine spezielle Schnittstelle (Application Programming Interface (API)) und deren mögliche Kommandos oder direkt per IP auf den Objekt-Storage zu. Im Falle eines Zugriffs per API muss die führende Applikation die herstellerspezifische API des Objekt-Storage unterstützen. Objekt-Storage wird vor allem im Bereich Archivierung, Dokumentenmanagement und beim Ablegen von Objekten in einer Cloud eingesetzt.

Für objektbasierende Speicherlösungen sind daher auch zusätzlich die Bausteine B 3.101 *Allgemeiner Server* und B 5.24 *Web-Services* anzuwenden.

Im Zusammenhang mit Weiterentwicklungen im Speicherumfeld etabliert sich zunehmend auch der Begriff des **Cloud Storage**. Hierunter sind Speicherlösungen als Basis für Cloud-Services zu verstehen. Die Speicherlösung an sich bleibt dabei weitgehend unverändert, jedoch liegt eine von den klassischen SAN- oder NAS-Architekturen abweichende Art des Zugriffs auf die gespeicherten Daten vor. Dieser wird in der Regel mittels Web-Service-Schnittstelle (via Representional State Transfer REST & Simple Object Access Protocol SOAP) realisiert.

Eine besondere Herausforderung im Zusammenhang mit Cloud-Storage ist die Mandantenfähigkeit der Gesamtlösung. Aus Anwendersicht sind daher zusätzlich die Bausteine B 1.17 *Cloud-Nutzung* und B 5.24 *Web-Services* zu modellieren. Aus Betreibersicht ist daneben der Baustein B 5.23 *Cloud Management* zu beachten.

## Gefährdungslage

Für den IT-Grundschutz von Speicherlösungen werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.9 *Datenverlust durch starke Magnetfelder*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*

- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.5 *Fehlende oder unzureichende Wartung*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.48 *Ungeeignete Entsorgung der Datenträger und Dokumente*
- G 2.54 *Vertraulichkeitsverlust durch Restinformationen*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.82 *Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.109 *Fehlende oder unzureichende Planung der Speicherlösung*
- G 2.182 *Fehlendes oder unzureichendes Betreiberkonzept für Speicherlösungen*
- G 2.183 *Fehlendes oder unzureichendes Zonenkonzept*
- G 2.184 *Fehlendes oder unzureichendes Rechte- und Rollenkonzept in Cloud-Infrastrukturen*
- G 2.185 *Fehlende oder unzureichende Softwarewartung (Maintenance) und fehlendes oder unzureichendes Patchlevel-Management*
- G 2.186 *Fehlende oder unzureichende Regelungen / keine klare Abgrenzung von Verantwortlichkeiten bei Speicherlösungen*
- G 2.187 *Fehlendes oder unzureichendes mandantenfähiges Administrationskonzept für Speicherlösungen*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.24 *Unbeabsichtigte Datenmanipulation*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.79 *Fehlerhafte Zuordnung von Ressourcen des SAN*

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*
- G 4.53 *Unsichere Default-Einstellungen bei Speicherkomponenten*
- G 4.95 *Ausfall von Komponenten einer Speicherlösung*
- G 4.96 *Fehlfunktion von Komponenten einer Speicherlösung*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.28 *Verhinderung von Diensten*
- G 5.57 *Netzanalysetools*
- G 5.89 *Hijacking von Netz-Verbindungen*
- G 5.102 *Sabotage*
- G 5.129 *Manipulation von Daten über das Speichersystem*
- G 5.130 *Manipulation der Konfiguration einer Speicherlösung*
- G 5.185 *Erlangung physischen Zugangs auf SAN-Switches*
- G 5.186 *Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing*
- G 5.187 *Überwindung der logischen Netzseparierung*
- G 5.188 *Unberechtigter Zugriff auf Daten innerhalb einer Cloud-Storage-Lösung*
- G 5.189 *Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden*

**Maßnahmenempfehlungen**

Um einen Inforationsverbund abzusichern, müssen, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz, zusätzlich zu diesem Baustein, noch weitere Bausteine umgesetzt werden.

Um eine Speicherlösung sicher aufbauen sowie betreiben zu können, sind eine Reihe von Maßnahmen umzusetzen. Beginnend mit der strategischen Entscheidung, welche Art von Speicherlösung zu wählen ist, folgt deren Konzeption und die Beschaffung der entsprechenden Komponenten. Die Installation und Konfiguration der Speicherlösung führt schließlich zum Übergang in die Betriebsphase, an deren Ende Maßnahmen zur ordnungsgemäßen Aussonderung der Speicherlösung umzusetzen sind.

Parallel zur Betriebsphase muss durch eine geeignete Notfallvorsorgeplanung sichergestellt werden, dass der Betrieb auch im Notfall aufrechterhalten werden kann. Informationssicherheitsmanagement und Revision stellen begleitend die Einhaltung des Regelwerks sicher.

Der schrittweise Aufbau und Betrieb einer Speicherlösung sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

**Planung und Konzeption**

Nachdem die Anforderungen analysiert worden sind, sollte durch die Verantwortlichen entschieden werden, welche Ausprägung der beschriebenen Speicherlösungen idealerweise zukünftig innerhalb der Institution einzusetzen ist. Dabei ist in einem ersten Schritt zu klären, welche Technik geeignet erscheint, um die ermittelten Anforderungen angemessen abzudecken (siehe M 2.362 *Auswahl einer geeigneten Speicherlösung* und M 2.351 *Planung von Speicherlösungen*).

Als Ausgangspunkt der Planung ist grundsätzlich die mit zentraler Speicherkapazität zu versorgende Anwendung zu betrachten. Nur auf diesem Weg lassen sich die Sicherheitsanforderungen an das Speichersystem und das Speichernetz und somit an die Speicherlösung in ihrer Gesamtheit sinnvoll definieren. Wichtige Parameter bei der Planung sind das über die Betriebszeit zu erwartende Wachstum des Speicherplatzes, der von der Anwendung benötigt wird, sowie die erforderliche Leistungsfähigkeit und die Sicherheitsanforderungen. Dabei muss die Auslegung der Speicherkomponenten durch absehbare Entwicklungen und fundierte Wachstumsprognosen so definiert werden, dass diese zentralen IT-Komponenten auf Dauer den Anforderungen der Institution genügen können. Die abgeleiteten Anforderungen an die einzusetzende Speicherlösung sollten im Anschluss in einer Sicherheitsrichtlinie festgehalten werden (siehe M 2.525 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen*).

Ergibt sich aus der Anforderungsanalyse, dass es notwendig ist, eine mandantenfähigen Speicherlösung einzusetzen, so ist festzulegen, wie die Trennung der Mandanten umgesetzt werden soll (siehe M 2.528 *Planung der sicheren Trennung von Mandanten in Speicherlösungen*). Bei höheren Anforderungen an die Verfügbarkeit oder die Skalierbarkeit empfiehlt sich der Einsatz einer hochverfügbaren Speicherlösung (siehe M 2.354 *Einsatz einer hochverfügbaren SAN-Lösung*). Als weitere umzusetzende Maßnahmen bei einem erhöhten Schutzbedarf, insbesondere hinsichtlich der Vertraulichkeit und Integrität der gespeicherten Daten, empfiehlt sich der Einsatz von Verschlüsselungsmechanismen oder die Einführung eines Zonenkonzeptes (siehe M 4.448 *Einsatz von Verschlüsselung für Speicherlösungen* und M 4.449 *Einführung eines Zonenkonzeptes*).

Neben der reinen Abschätzung und Planung der benötigten Speicherkapazität ist insbesondere frühzeitig die geeignete Aufstellung der Speicherlösung zu prüfen (siehe M 1.59 *Geeignete Aufstellung von Speicher- und Archivsystemen*). Dabei ist kritisch zu hinterfragen, ob die Serverräume oder das Rechenzentrum technisch und organisatorisch geeignet sind, um Speicherlösungen dort unterzubringen. Die eigentliche Aufstellung erfolgt im Rahmen der Umsetzungsphase.

Mit der Planung eines Speichersystems muss auch die Planung eines angemessenen Datensicherungskonzeptes einhergehen. Dazu ist das Datensicherungskonzept (B 1.4 *Datensicherungskonzept*) der Institution organisatorisch und technisch an die Anforderungen anzupassen, die sich aus dem Einsatz der gewählten Speicherlösung ergeben.

**Beschaffung**

Nachdem die grundsätzliche Definition der Anforderungen an die einzusetzende Speicherlösung abgeschlossen worden ist, sind die Angebote möglicher Hersteller und Lieferanten zu prüfen, und ein geeigneter Anbieter ist auszuwählen (siehe M 2.355 *Auswahl von Lieferanten für eine Speicherlösung*).

In der Folge sind, im Rahmen der Vertragsgestaltung mit den gewählten Dienstleistern, Service Level Agreements (kurz SLAs) zu treffen. Die Ausprägung der SLAs sollte sich in realistischer Weise mit den ermittelten Anforderungen der Planungsphase decken (siehe M 2.356 *Vertragsgestaltung mit Dienstleistern für Speicherlösungen*).

**Umsetzung**

Nachdem die organisatorischen und planerischen Vorarbeiten abgeschlossen sind, kann die Speicherlösung implementiert werden. Die erfolgreiche Umsetzung der geplanten Speicherlösung erfordert dabei sowohl die Abstimmung der erkennbaren Anforderungen des Betriebs mit den ermittelten Sicherheitsvorgaben als auch die Dokumentation einer Reihe weiterer Regelungen, Anforderungen und Einstellungen (siehe M 2.526 *Planung des Betriebs der Speicherlösung*).

Weiterhin sind aus Sicherheitssicht für die Umsetzungsphase insbesondere die folgenden Maßnahmen zu beachten:

- Es ist eine sichere Grundkonfiguration der Speicherlösung vorzunehmen (siehe M 4.274 *Sichere Grundkonfiguration von Speichersystemen*).
- Die Administration der Speicherlösung sollte möglichst über ein separates, abgesichertes Netz erfolgen (siehe M 2.357 *Aufbau eines Administrationsnetzes für Speichersysteme*).
- Alle Administratoren müssen auf den Umgang mit der ausgewählten Speicherlösung geschult werden (siehe M 3.54 *Schulung der Administratoren des Speichersystems*).

Der Aufbau einer Speicherlösung bedingt in der Regel die Umsetzung einer logischen Zuordnung zwischen Servern und den weiteren Komponenten der Speicherlösung. Diese ist nach den schriftlich spezifizierten Anforderungen und Planungen der vorangegangenen Phasen vorzunehmen (siehe M 5.130 *Absicherung des SANs durch Segmentierung*).

Mit den Erkenntnissen der Testphase ist eine Systemdokumentation anzufertigen, die sowohl die eingesetzte Hard- und Software vollumfänglich erfasst als auch alle vorzunehmenden Schritte zur Installation und individuellen Konfiguration der Speicherlösung beschreibt (siehe M 2.358 *Dokumentation der Systemeinstellungen von Speichersystemen*).

**Betrieb**

Nach erfolgreicher Erstinstallation und Durchlauf einer Testphase kann der Regelbetrieb aufgenommen werden. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Die bedarfsgerechte Bereitstellung der Funktionalität einer Speicherlösung setzt deren sicheren Betrieb voraus. Vor diesem Hintergrund müssen unter anderem jene Dienstprogramme abgesichert werden, die der Unterstützung betrieblicher Funktionen der Speicherlösung dienen und daher umfangreiche Berechtigungen benötigen (siehe M 4.275 *Sicherer Betrieb einer Speicherlösung*).
- Während des Regelbetriebs einer Speicherlösung werden Daten erfasst, gespeichert und weiterverarbeitet. Sofern diese Daten nicht mehr benötigt werden, müssen Maßnahmen ergriffen werden, die eine sichere Löschung gewährleisten (siehe M 2.527 *Sicheres Löschen in SAN-Umgebungen*).
- Speicherlösungen müssen im laufenden Betrieb überwacht und gewartet werden (siehe M 2.359 *Überwachung und Verwaltung von Speicherlösungen*).
- Neben der Überwachung und Wartung, die vor allem die technische Verfügbarkeit sicherstellen soll, müssen weitere sicherheitsrelevante Aspekte kontrolliert werden (siehe M 2.360 *Sicherheits-Audits und Berichtswesen bei Speichersystemen*).
- Als zusätzliche Maßnahme bei erhöhtem Schutzbedarf hinsichtlich der Integrität der SAN-Fabric empfiehlt sich der Einsatz von Storage-Protokollen mit erweiterten Sicherheitsmerkmalen (siehe M 4.447 *Sicherstellung der Integrität der SAN-Fabric*).

**Aussonderung**

Empfehlungen zur Deinstallation von Einzelkomponenten und von Komplettsystemen, etwa nach Beendigung des Regelbetriebs, finden sich in der Maßnahme M 2.361 *Außerbetriebnahme von Speicherlösungen*.

**Notfallvorsorge**

Der Einsatz von Speicherlösungen erfordert die Überarbeitung und Anpassung vorhandener IT-Notfallpläne. Empfehlungen zur Notfallvorsorge finden sich in der Maßnahme M 6.98 *Notfallvorsorge und Notfallreaktion für Speicherlösungen*.

Nachfolgend wird das Maßnahmenbündel für diesen Baustein vorgestellt.

**Planung und Konzeption**
- M 2.351 (A) *Planung von Speicherlösungen*
- M 2.354 (Z) *Einsatz einer hochverfügbaren SAN-Lösung*
- M 2.362 (A) *Auswahl einer geeigneten Speicherlösung*
- M 2.525 (A) *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen*
- M 2.528 (Z) *Planung der sicheren Trennung von Mandanten in Speicherlösungen*
- M 2.529 (W) *Modellierung von Speicherlösungen*
- M 3.92 (W) *Grundlegende Begriffe beim Einsatz von Speicherlösungen*
- M 4.448 (Z) *Einsatz von Verschlüsselung für Speicherlösungen*
- M 4.449 (Z) *Einführung eines Zonenkonzeptes*

**Beschaffung**
- M 2.355 (C) *Auswahl von Lieferanten für eine Speicherlösung*
- M 2.356 (C) *Vertragsgestaltung mit Dienstleistern für Speicherlösungen*

**Umsetzung**
- M 1.59 (A) *Geeignete Aufstellung von Speicher- und Archivsystemen*
- M 2.357 (B) *Aufbau eines Administrationsnetzes für Speichersysteme*
- M 2.358 (A) *Dokumentation der Systemeinstellungen von Speichersystemen*
- M 2.526 (A) *Planung des Betriebs der Speicherlösung*
- M 3.54 (A) *Schulung der Administratoren des Speichersystems*
- M 4.80 (B) *Sichere Zugriffsmechanismen bei Fernadministration*
- M 4.274 (A) *Sichere Grundkonfiguration von Speichersystemen*
- M 5.130 (B) *Absicherung des SANs durch Segmentierung*

**Betrieb**
- M 2.359 (B) *Überwachung und Verwaltung von Speicherlösungen*
- M 2.360 (B) *Sicherheits-Audits und Berichtswesen bei Speichersystemen*
- M 2.527 (B) *Sicheres Löschen in SAN-Umgebungen*
- M 4.275 (A) *Sicherer Betrieb einer Speicherlösung*
- M 4.447 (Z) *Sicherstellung der Integrität der SAN-Fabric*

**Aussonderung**
- M 2.361 (C) *Außerbetriebnahme von Speicherlösungen*

**Notfallvorsorge**
- M 6.1 (A) *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*
- M 6.98 (A) *Notfallvorsorge und Notfallreaktion für Speicherlösungen*

# B 3.304 Virtualisierung

## Beschreibung

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Mehrere solcher Virtualisierungsserver können häufig zu einer virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Die Virtualisierung von IT-Systemen bietet vielfältige Vorteile für den IT-Betrieb in einem Informationsverbund. Es können Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der Server effizienter genutzt werden. Durch die damit verbundene Zentralisierung und Konsolidierung sowie die vereinfachte Bereitstellung von IT-Systemen können im Bereich Personal und Administration ebenfalls Kostenvorteile erreicht werden. Die Möglichkeiten der Virtualisierung stellen aber auch gleichzeitig eine neue Herausforderung für den Betrieb des Informationsverbundes dar. Da durch den Einsatz der Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund berührt werden, müssen Wissen und Erfahrungen aus den unterschiedlichsten Bereichen zusammengeführt werden.

Der Einsatz von Virtualisierungsservern und virtuellen IT-Systemen muss in der Schutzbedarfsfeststellung für den vorliegenden Informationsverbund berücksichtigt werden. Es ist zu beachten, dass der Schutzbedarf des Virtualisierungsservers durch den Schutzbedarf der auf ihm betriebenen virtuellen IT-Systeme beeinflusst wird. Probleme auf einem Virtualisierungsserver oder einem virtuellen IT-System können sich möglicherweise auch auf alle anderen virtuellen IT-Systeme, die auf dem selben Virtualisierungsserver betrieben werden, auswirken.

In diesem Baustein wird beschrieben, wie die Virtualisierung von IT-Systemen in den Informationsverbund eingeführt werden kann und unter welchen Voraussetzungen virtuelle Infrastrukturen im Informationsverbund sicher betrieben werden können.

### Thematische Abgrenzung

In diesem Baustein wird nur die Virtualisierung vollständiger IT-Systeme behandelt, andere Techniken, die teilweise ebenfalls mit dem Wort "Virtualisierung" in Verbindung gebracht werden (Anwendungsvirtualisierung mittels Terminalservern, Storage-Virtualisierung etc.), sind nicht Gegenstand dieses Bausteins. Es werden Virtualisierungsserver und virtuelle IT-Systeme betrachtet, in denen Betriebssysteme ablaufen, die häufig auch direkt auf physischen IT-Systemen zum Einsatz kommen.

Im Bereich der Software-Entwicklung werden die Begriffe Virtuelle Maschine und Virtuelle-Maschinen-Monitor (VMM) manchmal auch für bestimmte Laufzeitumgebungen, beispielsweise beim Einsatz von Java oder Dot-NET (Microsoft .NET), verwendet. Solche Laufzeitumgebungen werden in diesem Baustein ebenfalls nicht betrachtet.

## Gefährdungslage

Für den sicheren Betrieb von Virtualisierungsservern und virtuellen IT-Systemen gibt es auf Grund der vielfältigen Funktionen der Virtualisierungsserver und der Manipulationsmöglichkeiten für virtuelle IT-Systeme einige neue organisatorische und technische Gefährdungen. Dies hängt damit zusammen, dass ein neuer Infrastrukturbestandteil, nämlich die Virtualisierungsinfrastruktur für IT-Objekte, entsteht. Auch können virtuelle IT-Systeme neue Zustände einnehmen. So kann sich ein System, das ausgeschaltet wurde, dennoch im Zustand *laufend* befinden, wenn es durch die Virtualisierungssoftware lediglich eingefroren wurde. Zudem werden Lebenszyklen von virtuellen IT-Systemen in der Regel in wesentlich kürzeren Zeitabständen durchlaufen.

In virtuellen Infrastrukturen werden für den IT-Grundschutz die folgenden typischen Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.29 *Softwaretest mit Produktionsdaten*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.60 *Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement*
- G 2.148 *Fehlerhafte Planung der Virtualisierung*
- G 2.149 *Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme*
- G 2.150 *Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen*
- G 2.151 *Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen*

**Menschliche Fehlhandlungen**

- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.28 *Ungeeignete Konfiguration der aktiven Netzkomponenten*
- G 3.36 *Fehlinterpretation von Ereignissen*
- G 3.79 *Fehlerhafte Zuordnung von Ressourcen des SAN*
- G 3.99 *Fehlerhafte Netzanbindungen eines Virtualisierungsservers*
- G 3.100 *Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme*
- G 3.101 *Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen*
- G 3.102 *Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen*

**Technisches Versagen**

- G 4.74 *Ausfall von IT-Komponenten in einer virtualisierten Umgebung*
- G 4.75 *Störung der Netzinfrastruktur von Virtualisierungsumgebungen*
- G 4.76 *Ausfall von Verwaltungsservern für Virtualisierungssysteme*
- G 4.77 *Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen*
- G 4.78 *Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse*

**Vorsätzliche Handlungen**

- G 5.29 *Unberechtigtes Kopieren der Datenträger*
- G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*
- G 5.147 *Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes*
- G 5.148 *Missbrauch von Virtualisierungsfunktionen*
- G 5.149 *Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen*
- G 5.150 *Kompromittierung des Hypervisor virtueller IT-Systeme*

**Maßnahmenempfehlungen**

Um einen Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Für die Modellierung von Virtualisierungsservern und virtuellen IT-Systemen ist Folgendes zu beachten:

- Der Baustein B 3.304 *Virtualisierung* ist auf jeden Virtualisierungsserver oder jede Gruppe von Virtualisierungsservern anzuwenden. Ein Virtualisierungsserver ist ein physisches IT-System (Client oder Server), auf dem virtuelle IT-Systeme betrieben werden. Neben dem Baustein B 3.304 müssen auch die jeweils relevanten Server- oder Client-Bausteine der Schicht 3 auf die Virtualisierungsserver angewandt werden.
- Neben physischen IT-Systemen und Virtualisierungsservern müssen auch virtuelle IT-Systeme (virtuelle Maschinen, VMs) mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen modelliert werden. VMs werden grundsätzlich in der gleichen Weise wie physische IT-Systeme modelliert, das heißt, es werden die jeweils relevanten Bausteine der Schichten 3 und 5 herangezogen. Da es in der Praxis oft vorkommt, dass viele VMs eingerichtet werden, ist eine sinnvolle Modellierung der VMs häufig nur durch geeignete Gruppenbildung möglich. Für die Gruppenbildung gelten bei VMs die gleichen Regeln wie für physische IT-Systeme. Prinzipiell können auch solche VMs zu einer Gruppe zusammengefasst werden, die auf verschiedenen physischen IT-Systemen ablaufen. Weitere Hin-

weise zur Modellierung virtueller IT-Systeme finden sich in der Maßnahme M 2.392 *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen*.

**Planung und Konzeption**

Bei der Planung einer virtuellen IT-Infrastruktur müssen eine Reihe von Rahmenbedingungen bedacht werden. Neben den Fragen nach der zur nutzenden Virtualisierungstechnik und entsprechenden Produkten (siehe M 2.477 *Planung einer virtuellen Infrastruktur*) sowie nach der Eignung der in Frage kommenden Systeme bezüglich der Virtualisierung (M 2.444 *Einsatzplanung für virtuelle IT-Systeme*) ist insbesondere die zukünftige Netzstruktur zu planen (M 5.153 *Planung des Netzes für virtuelle Infrastrukturen*). Weiterhin sind auch eine Reihe von organisatorischen Regelungen anzupassen.

Da sich Virtualisierungsserver besonders für den Aufbau von Test- und Entwicklungsumgebungen eignen, sollten detaillierte Regelungen getroffen werden, wie mit den in diesen Umgebungen verarbeiteten Daten umgegangen werden soll (M 2.82 *Entwicklung eines Testplans für Standardsoftware*).

**Beschaffung**

Bei der Auswahl der Hardware für Virtualisierungsserver ist darauf zu achten, dass Systeme beschafft werden, die für die gewählte Virtualisierungslösung geeignet sind. Die Systeme müssen leistungsfähig genug sein, um für alle geplanten virtuellen IT-Systeme genügend Performance bereitstellen zu können (M 2.445 *Auswahl geeigneter Hardware für Virtualisierungsumgebungen*).

**Umsetzung**

Der Aufbau der virtuellen Infrastruktur bzw. die Installation der Virtualisierungsserver selbst kann gemäß der eingeübten Vorgehensweisen der Organisation durchgeführt werden (B 3.101 *Allgemeiner Server*). Der Komplexitätsgrad eines Virtualisierungsprojektes insgesamt sollte jedoch nicht unterschätzt werden, daher sind einige Besonderheiten bei der Konfiguration der Netze (M 5.154 *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen*) und der Gestaltung des administrativen Zugangs zu den Virtualisierungsservern (M 2.446 *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*) zu beachten.

Für die Bereitstellung virtueller IT-Systeme auf den Virtualisierungsservern müssen organisatorische Maßnahmen für die Installation der virtuellen IT-Systeme (M 2.447 *Sicherer Einsatz virtueller IT-Systeme*) durch technische Maßnahmen ergänzt werden (M 4.346 *Sichere Konfiguration virtueller IT-Systeme*), um deren sicheren Betrieb zu gewährleisten.

Auf den eigentlichen Virtualisierungsservern sollten möglichst nur solche Dienste betrieben werden, die zur Virtualisierungstechnik gehören. Andere Dienste sollten in den virtualisierten Instanzen (oder auf Systemen außerhalb der virtuellen Infrastruktur) bereitgestellt werden.

**Betrieb**

Die Maßnahmen M 2.448 *Überwachung der Funktion und Konfiguration virtueller Infrastrukturen* und M 4.349 *Sicherer Betrieb von virtuellen Infrastrukturen* von virtuellen Infrastrukturen bilden die Grundlage für den sicheren Betrieb sowohl der Virtualisierungsserver als auch der virtuellen IT-Systeme. Weiterhin ist die Maßnahme M 4.348 *Zeitsynchronisation in virtuellen IT-Systemen* zu beachten.

**Notfallvorsorge**

Bei der Notfallvorsorge für Virtualisierungsserver sollte berücksichtigt werden, dass das potentielle Schadensausmaß umso höher ist, je mehr virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden. Daher muss der Schutzbedarf der Gesamtheit der virtuellen IT-Systeme auf den Schutzbedarf der Virtualisierungskomponenten abgebildet werden (M 6.138 *Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Virtualisierung" vorgestellt.

**Planung und Konzeption**

- M 2.82 (B) *Entwicklung eines Testplans für Standardsoftware*

- M 2.314 (Z) *Verwendung von hochverfügbaren Architekturen für Server*
- M 2.392 (A) *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen*
- M 2.444 (A) *Einsatzplanung für virtuelle IT-Systeme*
- M 2.477 (A) *Planung einer virtuellen Infrastruktur*
- M 3.70 (W) *Einführung in die Virtualisierung*
- M 3.71 (B) *Schulung der Administratoren virtueller Umgebungen*
- M 5.153 (B) *Planung des Netzes für virtuelle Infrastrukturen*

**Beschaffung**

- M 2.445 (C) *Auswahl geeigneter Hardware für Virtualisierungsumgebungen*

**Umsetzung**

- M 2.83 (B) *Testen von Standardsoftware*
- M 2.446 (B) *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*
- M 2.447 (A) *Sicherer Einsatz virtueller IT-Systeme*
- M 3.72 (W) *Grundbegriffe der Virtualisierungstechnik*
- M 4.97 (Z) *Ein Dienst pro Server*
- M 4.346 (A) *Sichere Konfiguration virtueller IT-Systeme*
- M 4.347 (Z) *Deaktivierung von Snapshots virtueller IT-Systeme*
- M 5.154 (B) *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen*

**Betrieb**

- M 2.448 (B) *Überwachung der Funktion und Konfiguration virtueller Infrastrukturen*
- M 2.449 (Z) *Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme*
- M 4.348 (C) *Zeitsynchronisation in virtuellen IT-Systemen*
- M 4.349 (A) *Sicherer Betrieb von virtuellen Infrastrukturen*

**Notfallvorsorge**

- M 6.138 (C) *Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten*

# B 3.305 Terminalserver

## Beschreibung

Terminalserver stellen zentral Ressourcen bereit, die mehrere Clients nutzen können. Diese Ressourcen können Bestandteile des Server-Betriebssystems, Standard-Anwendungen oder Kommandozeilen sein. Auf diese Weise können Applikationen bereitgestellt werden, ohne dass sie auf den Clients installiert werden müssen. In der Regel können mehrere Clients über das Netz gleichzeitig auf die vom Terminalserver angebotenen Applikationen zugreifen.

Terminalserver stellen ein besonders zentralisiertes Szenario einer Client-Server Architektur dar. Anwendungen werden auf den leistungsstarken Terminalservern installiert, von den Clients werden diese gestartet, gesteuert und dargestellt. Diese Ein- und Ausgaben können auf verhältnismäßig einfach ausgestatteten Arbeitsplatz-Rechnern (Fat-Clients) mit der entsprechenden Client-Software verarbeitet werden. Zudem existieren Lösungen, die mit dedizierten Terminals (Thin-Clients) funktionieren.

In diesem Baustein wird ein systematischer Weg aufgezeigt, wie ein Konzept zum Einsatz von Terminalservern innerhalb einer Institution erstellt und wie deren Umsetzung und Einbettung sichergestellt werden kann. Er ist auf jeden Terminalserver des betrachteten Informationsverbunds anzuwenden.

### Abgrenzung des Bausteins

Bestandteil dieses Bausteins sind lediglich die für Terminalserver spezifischen Gefährdungen und Maßnahmen. Daher muss zusätzlich der Baustein B 3.101 *Allgemeiner Server* berücksichtigt werden. Wird auf dem Terminalserver-Client ein eigenständiges Betriebssystem ausgeführt und wird dieses nicht von dem Server bezogen, so ist des Weiteren der Baustein B 3.201 *Allgemeiner Client* zu betrachten. Terminalserver-Dienste existieren für zahlreiche Betriebssysteme z. B. Unix bzw. Linux, Microsoft Windows und z/OS. Die einzelnen Umsetzungen unterscheiden sich in vielen Punkten sehr stark, beispielsweise durch die

- Verwendung des benutzten Übertragungsprotokolls,
- Anforderungen an die Übertragungsraten des Netzes,
- Anforderungen an die Geschwindigkeit des Servers,
- Nutzung von verteilten Ressourcen und Geräten und
- insbesondere durch die unterschiedliche Konfiguration und Administration des unter diesem Dienst operierenden Betriebssystems.

Für die Sicherheit eines Terminalservers ist es daher unabdingbar, zusätzlich die Bausteine anzuwenden, die das konkrete Betriebssystem beschreiben.

## Gefährdungslage

Für den IT-Grundschutz eines Terminalservers gestützten Netzes werden die folgenden typischen Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.36 *Ungeeignete Einschränkung der Benutzerumgebung*
- G 2.153 *Ungeeignete Sicherung des Übertragungsweges in einer Terminalserver Umgebung*
- G 2.154 *Ungeeignete Anwendungen für den Einsatz auf Terminalservern*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*

- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.38 *Konfigurations- und Bedienungsfehler*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.12 *Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.81 *Erweiterte Rechte durch Programmdialoge auf Terminalservern*
- G 4.82 *Ausfall und Nichterreichbarkeit von Terminalservern*

**Vorsätzliche Handlungen**

- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.23 *Schadprogramme*
- G 5.112 *Manipulation von ARP-Tabellen*
- G 5.161 *Gefälschte Antworten auf XDMCP-Broadcasts bei Terminalservern*
- G 5.162 *Umleiten von X-Window-Sitzungen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Terminalservers sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb dieses Servers. Die Schritte, die dabei durchlaufen werden, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Bei der Planung eines Terminalservers müssen eine Reihe von Rahmenbedingungen bedacht werden. Im ersten Schritt sollte die allgemeine Sicherheitsrichtlinie um eine detaillierte Richtlinie für Terminalserver ergänzt werden (siehe M 2.464 *Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung*). Die hierin schriftlich festgehaltenen Maßgaben sowie Zielsetzungen müssen die individuellen Bedingungen und Anforderungen einer sicheren Terminalserver-Umgebung widerspiegeln. Bei der Migration einer bestehenden Client-Server-Architektur auf eine Terminalserver-gestützte Umgebung muss vor der Umsetzung eingehend überprüft werden, ob die zu migrierenden Anwendungen überhaupt dafür geeignet sind (M 2.466 *Migration auf eine Terminalserver-Architektur*).

Innerhalb von Mehrbenutzerumgebungen, wie sie Terminalserver-Systeme darstellen, ist die Abschottung der Anwender voneinander sowie gegenüber riskanten Systemfunktionen von erheblicher Bedeutung. Um einen störungsfreien Betrieb zu gewährleisten und die Vertraulichkeit der innerhalb einzelner Benutzersitzungen verarbeiteten Daten zu schützen, müssen die Rechte restriktiv vergeben werden (siehe M 5.163 *Restriktive Rechtevergabe auf Terminalservern*).

Terminalserver können dazu benutzt werden, dass Clients auf Inhalte in unsicheren Netzen, beispielsweise auf Internetseiten mit aktiven Inhalten, zugreifen können. Anstatt des Clients kommuniziert der Terminalserver über das unsichere Netz, dem Client werden nur die Inhalte übermittelt. Ein Terminalserver, der anstelle des Clients auf das unsichere Netz zugreift, wird als grafische Firewall bezeichnet (siehe Maßnahme M 4.365 *Nutzung eines Terminalservers als grafische Firewall*).

**Beschaffung**

Sollen Anwendungen, die bislang in einer Client-Server basierten Netzarchitektur genutzt werden, auf einen Terminalserver zentral bereitgestellt werden, sind lizenzrechtlich relevante Verträge im Vorfeld der Migration zu prüfen und eventuell neue Software zu beschaffen (siehe M 2.468 *Lizenzierung von Software in Terminalserver-Umgebungen*).

**Umsetzung**

Die Verwaltung der Terminalserver-Infrastruktur ist für Administratoren sowie für Benutzer ohne Vorerfahrung in einigen Punkten erklärungsbedürftig. Alle Personen, die mit einem Terminalserver-System arbeiten, sollten daher geschult werden (siehe M 3.81 *Schulung zum sicheren Terminalserver-Einsatz*).

**Betrieb**

Es muss verhindert werden, dass die Anwender die Benutzerumgebung auf den Terminalservern verändern und nur auf Ressourcen zugreifen können, auf die sie auch zugreifen sollen (siehe M 4.367 *Sichere Verwendung von Client-Applikationen für Terminalserver*). Läuft die Verbindung zwischen Terminalservern und deren Clients über ein unsicheres Netz, sind Vorkehrungen zu treffen, damit die Kommunikation nicht belauscht, verändert oder gestört werden kann (siehe M 5.164 *Sichere Nutzung eines Terminalservers aus einem entfernten Netz*).

**Aussonderung**

Sollen Terminalserver, an Terminalserver angeschlossene Clients oder Infrastruktur-Komponenten einer Terminalserver-Umgebung außer Betrieb genommen werden, sollte die Maßnahme M 2.469 *Geregelte Außerbetriebnahme von Komponenten einer Terminalserver-Umgebung* berücksichtigt werden.

**Notfallvorsorge**

Da vom Ausfall einer Terminalserver-Umgebung zumeist eine größere Anzahl Anwender betroffen sein können, sind Maßnahmen zu ergreifen, damit bei einem Ausfall der Schaden verringert wird. Durch Terminalserver-Verbünde können auch hohe Anforderungen an die Verfügbarkeit erfüllt werden (siehe M 6.142 *Einsatz von redundanten Terminalservern*).

Fällt ein Terminalserver-Client aus, stehen die Anwendungen auf dem Terminalserver dem betroffenen Benutzer nicht mehr zur Verfügung. Daher könnten beim Einsatz von Terminals ohne eigenes Betriebssystem (Thin-Clients) Ersatzmaschinen bereitgehalten werden (M 6.143 *Bereitstellung von Terminalserver-Clients aus Depot-Wartung*).

Werden vorsorglich die Applikationen sowohl auf dem Terminalserver als auch auf den Client-PCs installiert, kann bei einem Ausfall vorübergehend ein Notfallbetrieb aufrecht erhalten werden (M 6.144 *Konfiguration von Terminalserver-Clients für die duale Nutzung als normale Client-PCs*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Terminalserver" vorgestellt.

**Planung und Konzeption**
- M 2.464 (A) *Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung*
- M 2.465 (A) *Analyse der erforderlichen Systemressourcen von Terminalservern*
- M 2.466 (A) *Migration auf eine Terminalserver-Architektur*
- M 2.467 (C) *Planung von regelmäßigen Neustartzyklen von Terminalservern*
- M 4.250 (Z) *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*
- M 4.365 (Z) *Nutzung eines Terminalservers als grafische Firewall*
- M 5.64 (Z) *Secure Shell*
- M 5.162 (A) *Planung der Leitungskapazitäten beim Einsatz von Terminalservern*
- M 5.163 (A) *Restriktive Rechtevergabe auf Terminalservern*

**Beschaffung**
- M 2.468 (Z) *Lizenzierung von Software in Terminalserver-Umgebungen*

**Umsetzung**
- M 3.81 (C) *Schulung zum sicheren Terminalserver-Einsatz*
- M 4.9 (A) *Einsatz der Sicherheitsmechanismen von X-Window*
- M 4.106 (A) *Aktivieren der Systemprotokollierung*
- M 4.366 (B) *Sichere Konfiguration von beweglichen Benutzerprofilen in Terminalserver-Umgebungen*
- M 5.72 (A) *Deaktivieren nicht benötigter Netzdienste*

**Betrieb**
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*

- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*
- M 4.367 (B) *Sichere Verwendung von Client-Applikationen für Terminalserver*
- M 4.368 (B) *Regelmäßige Audits der Terminalserver-Umgebung*
- M 5.164 (B) *Sichere Nutzung eines Terminalservers aus einem entfernten Netz*

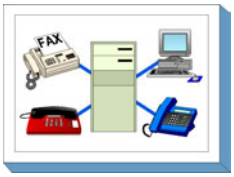
**Aussonderung**

- M 2.469 (A) *Geregelte Außerbetriebnahme von Komponenten einer Terminalserver-Umgebung*

**Notfallvorsorge**

- M 6.142 (Z) *Einsatz von redundanten Terminalservern*
- M 6.143 (C) *Bereitstellung von Terminalserver-Clients aus Depot-Wartung*
- M 6.144 (Z) *Konfiguration von Terminalserver-Clients für die duale Nutzung als normale Client-PCs*

# B 3.401 TK-Anlage




## Beschreibung

Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone einer Institution intern verbunden und extern an ein öffentliches Telefonnetz (Public Switched Telephone Network, PSTN) angeschlossen werden. Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich mittels TK-Anlagen Daten, Texte, Grafiken und Bewegtbilder zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien übermittelt werden. Je nach Anbindung und genutzter Datennetze können in einer Institution Telekommunikationsanlagen in verschiedenen Ausprägungen eingesetzt werden:

- Klassische TK-Anlagen
  Klassische TK-Anlagen nutzen zum Verbindungsaufbau und zur Übertragung je nach vorhandener Technik ein separates Netz als TK-Infrastruktur. An die Anlage können beispielsweise Telefone, Faxgeräte, Modems und Anrufbeantworter angeschlossen werden.
- VoIP-System
  Bei Voice over IP (VoIP) wird anstatt einer separaten TK-Infrastruktur mit eigener Verkabelung ein IP-Datennetz genutzt, um die Endgeräte an die TK-Anlage anzuschließen. Die Endgeräte kommunizieren bei VoIP mit der TK-Anlage oder anderen VoIP-Geräten über IP-basierte Signalisierungs- und Medientransportprotokolle. Der Übergang in das öffentliche Telefonnetz erfolgt über ein Gateway innerhalb der Institution.
- Hybrid System / Hybrid Anlage
  Aufgrund der zunehmenden Bedeutung von VoIP werden TK-Anlagen angeboten, die die klassische Telefonie mit VoIP-Telefonie vereinen. Sogenannte Hybridanlagen verfügen neben den Bestandteilen einer klassischen TK-Anlage zusätzlich über einen Anschluss an das Datennetz, über den IP-Telefone mit der TK-Anlage kommunizieren können. Mit einer Hybrid-Anlage können die klassische digitale oder analoge Telefonie und VoIP gleichzeitig betrieben werden. Auch ist es möglich, mit einer Hybrid-Anlage schrittweise auf eine VoIP-Infrastruktur zu migrieren.
- IP-Anlagenanschluss
  Bei der Nutzung von VoIP kann der PSTN-Anschluss auch bei einem externen Anbieter liegen. Das (interne) VoIP-System kommuniziert auch nach außen primär über das Internet (IP) mit dem externen Dienstleister. Diese Variante wird IP-Anlagenanschluss genannt.

Generell lässt sich sagen, dass die großen TK-Anbieter das herkömmliche Telefonnetz durch einheitliche IP-basierte Lösungen (Next Generation Network) ablösen, da dann nicht mehr zwischen Daten- und Sprachtransport unterschieden werden muss. Dies wird auch Auswirkungen auf die Schnittstelle zwischen einer internen Telefonanlage und dem TK-Diensteanbieter haben.

In diesem Baustein werden vor allem die für die klassischen TK-Anlagen spezifischen Gefährdungen und Maßnahmen betrachtet. Der Baustein sollte für jede TK-Anlage unabhängig von der später verwendeten Technologie herangezogen werden. Für alle Bereiche, die über die klassische TK-Anlage hinausgehen, sind zusätzlich die entsprechenden Bausteine umzusetzen, beispielsweise zu VoIP (B 4.7 *VoIP*) oder den mobilen und drahtlosen Systemen (z. B. B 3.404 *Mobiltelefon*).

## Gefährdungslage

Für den IT-Grundschutz einer TK-Anlage werden die folgenden typischen Gefährdungen betrachtet:

### Höhere Gewalt

- G 1.2 *Ausfall von IT-Systemen*
- G 1.10 *Ausfall eines Weitverkehrsnetzes*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.5 *Fehlende oder unzureichende Wartung*

**Menschliche Fehlhandlungen**

- G 3.7 *Ausfall der TK-Anlage durch Fehlbedienung*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*

**Vorsätzliche Handlungen**

- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.11 *Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten*
- G 5.12 *Abhören von Telefongesprächen und Datenübertragungen*
- G 5.13 *Abhören von Räumen über TK-Endgeräte*
- G 5.14 *Gebührenbetrug*
- G 5.15 *Missbrauch von Leistungsmerkmalen von TK-Anlagen*
- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.42 *Social Engineering*
- G 5.44 *Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Dazu kann beispielsweise der Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* gehören, der auf alle Außenverbindungen anzuwenden ist, die über ISDN realisiert werden. Auch die Bausteine B 3.404 *Mobiltelefon*, B 4.6 *WLAN* und B 4.7 *VoIP* sind, wo zutreffend, zu beachten. Die zentralen Einrichtungen einer TK-Anlage sollten in einem Raum aufgestellt werden, der den Anforderungen an einen Serverraum (Baustein B 2.4 *Serverraum*) oder einen Raum für technische Infrastruktur (Baustein B 2.6 *Raum für technische Infrastruktur*) genügt. Für die Verkabelung der TK-Anlage wird auf den Baustein B 2.2 *Elektrotechnische Verkabelung* hingewiesen.

Für die TK-Anlage sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Beschaffung und den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Zur Planung der TK-Anlage sollte die Maßnahme M 2.471 *Planung des Einsatzes von TK-Anlagen* beachtet werden. Eine Richtlinie zum Betrieb und der korrekten Nutzung der TK-Anlage sollte erstellt werden (M 2.472 *Erstellung einer Sicherheitsrichtlinie für TK-Anlagen*).

**Beschaffung**

Die Maßnahme M 2.105 *Beschaffung von TK-Anlagen* nennt die wesentlichen Kriterien, die bei der Auswahl einer TK-Anlage zu beachten sind.

**Umsetzung**

Bei der Installation sind unbedingt die vom Hersteller voreingestellten Passwörter zu ändern, da die Anlage sonst von beliebigen Angreifern manipuliert werden kann. Ebenso sind alle Schnittstellen abzusichern. Bei der Konfiguration ist nach der Grundregel zu verfahren, dass alle nicht benötigten Leistungsmerkmale abzuschalten sind, weil sie unnötige Risiken mit sich bringen (siehe M 5.14 *Absicherung interner Remote-Zugänge von TK-Anlagen* und M 5.15 *Absicherung externer Remote-Zugänge von TK-Anlagen*).

Nur diejenigen Personen, die mit den entsprechenden technischen Wartungsaufgaben betraut sind, sollten Zutritt zu dem Technikraum, in dem die TK-Anlage aufgestellt ist, erhalten.

**Betrieb**

Die Administrationsarbeiten an der TK-Anlage sollten nach Möglichkeit protokolliert werden, um nachvollziehen zu können, ob sicherheitsrelevante Einstellungen verändert wurden, siehe M 4.5 *Protokollierung bei TK-Anlagen*. Bei hohen Sicherheitsanforderungen an den Betrieb der TK-Anlage ist eine regelmäßige Revision der Konfigurationseinstellungen erforderlich (siehe M 4.6 *Revision der TK-Anlagenkonfiguration*). Da die Sicherheit häufig durch die ungeeignete Bedienung der Endgeräte durch die Benutzer unterlaufen wird, sollten die Mitarbeiter in die korrekte Nutzung eingewiesen und regelmäßig für mögliche Gefährdungen sensibilisiert werden (siehe M 3.82 *Schulung zur sicheren Nutzung von TK-Anlagen*).

**Notfallvorsorge**

Es müssen geeignete Maßnahmen zur Notfallvorsorge für die TK-Anlage getroffen werden. Zusätzlich sind ihre Konfigurationsdaten regelmäßig zu sichern, um die Anlage nach einem eventuellen Ausfall schnell wieder hochfahren und korrekt konfigurieren zu können (siehe M 6.145 *Notfallvorsorge für TK-Anlagen*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "TK-Anlage" vorgestellt:

**Planung und Konzeption**
- M 2.27 (Z) *Wartung einer TK-Anlage*
- M 2.470 (A) *Durchführung einer Anforderungsanalyse für TK-Anlagen*
- M 2.471 (A) *Planung des Einsatzes von TK-Anlagen*
- M 2.472 (A) *Erstellung einer Sicherheitsrichtlinie für TK-Anlagen*
- M 2.473 (A) *Auswahl von TK-Diensteanbietern*

**Beschaffung**
- M 2.105 (W) *Beschaffung von TK-Anlagen*

**Umsetzung**
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.10 (C) *Schutz der TK-Endgeräte*
- M 4.11 (B) *Absicherung der TK-Anlagen-Schnittstellen*
- M 4.369 (C) *Sicherer Betrieb eines Anrufbeantworters*
- M 5.14 (A) *Absicherung interner Remote-Zugänge von TK-Anlagen*
- M 5.15 (A) *Absicherung externer Remote-Zugänge von TK-Anlagen*

**Betrieb**
- M 3.82 (B) *Schulung zur sicheren Nutzung von TK-Anlagen*
- M 4.5 (B) *Protokollierung bei TK-Anlagen*
- M 4.6 (C) *Revision der TK-Anlagenkonfiguration*

**Aussonderung**
- M 2.474 (B) *Sichere Außerbetriebnahme von TK-Komponenten*

**Notfallvorsorge**
- M 6.26 (B) *Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten*
- M 6.145 (C) *Notfallvorsorge für TK-Anlagen*

# B 3.402 Faxgerät


## Beschreibung

Betrachtet wird die Informationsübermittlung in Form eines Fax. Hierbei werden von einer Vorlage die darauf aufgezeichneten Inhalte vom Sendegerät Punkt für Punkt abgetastet und übertragen und von einem Empfangsgerät ebenso wieder aufgebaut. Für die Maßnahmenauswahl im Bereich IT-Grundschutz wurde nicht nach dem verwendeten Übertragungsstandard (z. B. CCITT Gruppe 3) unterschieden. In diesem Baustein werden als technische Basis des Faxversands ausschließlich marktübliche Stand-Alone-Faxgeräte betrachtet, nicht jedoch Fax-Einschubkarten oder Faxserver (siehe Baustein B 5.6 *Faxserver*).

## Gefährdungslage

Für den IT-Grundschutz werden bei der Informationsübermittlung per Fax folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.20 *Unzureichende oder falsche Versorgung mit Verbrauchsgütern*

**Menschliche Fehlhandlungen**

- G 3.14 *Fehleinschätzung der Rechtsverbindlichkeit eines Fax*

**Technisches Versagen**

- G 4.14 *Verblassen spezieller Faxpapiere*
- G 4.15 *Fehlerhafte Faxübertragung*

**Vorsätzliche Handlungen**

- G 5.7 *Abhören von Leitungen*
- G 5.30 *Unbefugte Nutzung eines Faxgerätes oder eines Faxservers*
- G 5.31 *Unbefugtes Lesen von Faxsendungen*
- G 5.32 *Auswertung von Restinformationen in Faxgeräten und Faxservern*
- G 5.33 *Vortäuschen eines falschen Absenders bei Faxsendungen*
- G 5.34 *Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes*
- G 5.35 *Überlastung durch Faxsendungen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Faxgeräte sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Beschaffung über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

### Beschaffung

Die Maßnahme M 2.49 *Beschaffung geeigneter Faxgeräte* nennt die wesentlichen Kriterien, die bei der Auswahl eines Faxgeräts zu beachten sind.

### Umsetzung

Bei der Installation des Faxgeräts ist darauf zu achten, dass es unter den Gesichtspunkten der Nutzbarkeit, Bedienbarkeit und Verwendung zweckmäßig aufgestellt wird. Die Mitarbeiter, die das Gerät benutzen sollen, sind in seine Bedienung einzuweisen.

**Betrieb**

Im laufenden Betrieb ist darauf zu achten, dass notwendige Verbrauchsgüter geeignet bevorratet werden, damit keine Nachrichten nur deshalb verloren gehen, weil zu einem bestimmten Zeitpunkt kein Papier oder kein Toner vorhanden ist. In der Regel ist es zweckmäßig, alle Sendungen durch ein geeignetes Faxvorblatt zu kennzeichnen und leichter identifizierbar zu machen. Durch regelmäßige Kontrollen der Sende- und Empfangsprotokolle lässt sich ein eventueller Missbrauch des Faxgeräts leichter aufdecken, und eine gelegentliche Kontrolle programmierter Zieladressen hilft zu vermeiden, dass Sendungen versehentlich an den falschen Empfänger gehen.

**Aussonderung**

Bei der Entsorgung von Verbrauchsgütern und Ersatzteilen ist zu beachten, dass bei bestimmten Geräten Abbilder gesendeter oder empfangener Faxsendungen auf Zwischenträgerfolien, Belichtungstrommeln oder auch auf Papier vorhanden sind, so dass diese Materialien nicht so entsorgt werden dürfen, dass später Unbefugte darauf Zugriff erhalten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Faxgerät" vorgestellt:

**Beschaffung**
- M 2.49 (Z) *Beschaffung geeigneter Faxgeräte*

**Umsetzung**
- M 1.37 (A) *Geeignete Aufstellung eines Faxgerätes*
- M 2.47 (B) *Ernennung eines Fax-Verantwortlichen*
- M 3.15 (A) *Informationen für alle Mitarbeiter über die Faxnutzung*
- M 4.36 (Z) *Sperren bestimmter Faxempfänger-Rufnummern*
- M 4.37 (Z) *Sperren bestimmter Absender-Faxnummern*

**Betrieb**
- M 2.48 (Z) *Festlegung berechtigter Faxbediener*
- M 2.51 (Z) *Fertigung von Kopien eingehender Faxsendungen*
- M 2.52 (C) *Versorgung und Kontrolle der Verbrauchsgüter*
- M 2.53 (Z) *Abschalten des Faxgerätes außerhalb der Bürozeiten*
- M 4.43 (Z) *Faxgerät mit automatischer Eingangskuvertierung*
- M 5.24 (Z) *Nutzung eines geeigneten Faxvorblattes*
- M 5.25 (A) *Nutzung von Sende- und Empfangsprotokollen*
- M 5.26 (Z) *Telefonische Ankündigung einer Faxsendung*
- M 5.27 (Z) *Telefonische Rückversicherung über korrekten Faxempfang*
- M 5.28 (Z) *Telefonische Rückversicherung über korrekten Faxabsender*
- M 5.29 (C) *Gelegentliche Kontrolle programmierter Zieladressen und Protokolle*

**Aussonderung**
- M 2.50 (B) *Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen*

**Notfallvorsorge**
- M 6.39 (C) *Auflistung von Händleradressen zur Fax-Wiederbeschaffung*

# B 3.403 Anrufbeantworter


Dieser Baustein ist 2011 mit der 12. Ergänzungslieferung entfallen.

Die wesentlichen Inhalte dieses Bausteins sind in den Baustein B 3.401 *TK-Anlage* und dort in die Maßnahme M 4.369 *Sicherer Betrieb eines Anrufbeantworters* integriert worden.

Die letzte Version des Bausteins, die mit der 11. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 3.404 Mobiltelefon

## Beschreibung

In diesem Baustein werden digitale Mobiltelefone nach dem GSM-Standard (Global System for Mobile communication, D- und E-Netze), UMTS (Universal Mobile Telecommunications System) und LTE (Long Term Evolution) betrachtet. Bei LTE werden Telefonate über Datenpakete abgewickelt, sodass dann zusätzlich Baustein B 4.7 *VoIP* zu betrachten ist. Handelt es sich beim Mobiltelefon um ein Smartphone, ist auch Baustein B 3.405 *Smartphones, Tablets und PDAs* und gegebenenfalls Baustein B 3.203 *Laptop* umzusetzen. Verwendet das Mobiltelefon VPN-Techniken, um sich beispielsweise mit dem Netz der Institution zu verbinden, sollte außerdem Baustein B 4.4 *VPN* betrachtet werden.

Um ein Mobiltelefon mit einem Mobilfunknetz zu verbinden, braucht es eine SIM-Karte (SIM - Subscriber Identity Module). Damit kann in den Mobilfunknetzen zwischen Benutzer und Gerät unterschieden werden.

Ein Mobiltelefon ist durch seine international eindeutige Seriennummer (IMEI - International Mobile Equipment Identity) gekennzeichnet. Der Benutzer wird durch seine auf der SIM-Karte gespeicherte Kundennummer (IMSI - International Mobile Subscriber Identity) identifiziert. Sie wird dem Teilnehmer beim Vertragsabschluss vom Mobilfunkanbieter zugeteilt. Sie ist zu unterscheiden von den ihm zugewiesenen Telefonnummern (MSISDN) (mindestens eine) . Durch diese Trennung ist es möglich, dass ein Teilnehmer mit seiner SIM-Karte verschiedene Mobiltelefone nutzen kann

Auf der SIM-Karte wird unter anderem die teilnehmerbezogene Rufnummer (MSISDN) gespeichert. Ebenso sind dort die kryptografischen Algorithmen für die Authentisierung und Nutzdatenverschlüsselung (zwischen Mobiltelefon und Basisstation) implementiert.

## Gefährdungslage

Für den IT-Grundschutz werden im Zusammenhang mit Mobiltelefonen folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.200 *Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*
- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*
- G 3.123 *Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs*

**Technisches Versagen**

- G 4.32 *Nichtzustellung einer Nachricht*
- G 4.41 *Nicht-Verfügbarkeit des Mobilfunknetzes*
- G 4.42 *Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*

- G 5.27 *Nichtanerkennung einer Nachricht*
- G 5.94 *Missbrauch von SIM-Karten*
- G 5.95 *Abhören von Raumgesprächen über Mobiltelefone*
- G 5.96 *Manipulation von Mobiltelefonen*
- G 5.97 *Unberechtigte Datenweitergabe über Mobiltelefone*
- G 5.98 *Abhören von Mobiltelefonaten*
- G 5.99 *Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen*
- G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*
- G 5.192 *Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Für Mobiltelefone sind eine Reihe von Maßnahmen erforderlich, beginnend mit der Planung über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Es sollte eine Sicherheitsrichtlinie erstellt werden, die umzusetzende Maßnahmen zum sicheren Umgang mit Mobiltelefonen beschreibt (siehe M 2.188 *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung*). Bei häufigem und wechselndem dienstlichen Gebrauch von Mobiltelefonen, die vom Unternehmen oder der Behörde zur Verfügung gestellt werden, kann es sinnvoll sein, diese Telefone in einer Sammelaufbewahrung zu halten (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).

**Umsetzung**

Es gibt verschiedene Sicherheitsmechanismen bei Mobiltelefonen, abhängig vom eingesetzten Mobiltelefon, von der SIM-Karte und vom gewählten Netzbetreiber. M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen* gibt einen Überblick über die wichtigsten Sicherheitsfunktionen dieser Geräte und beschreibt, wie diese genutzt werden könnten.

**Betrieb**

Damit Mobiltelefone geordnet und zuverlässig genutzt werden können, müssen einige Maßnahmen umgesetzt werden, zu denen die Sicherstellung der Energieversorgung und bei Bedarf auch der Schutz vor Rufnummernermittlung gehören (siehe M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen* und M 5.79 *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung*) Falls mit dem Gerät Daten übertragen werden, sind ebenfalls einige spezifische Maßnahmen zu beachten, um einerseits eine zuverlässige Funktionsweise zu gewährleisten und andererseits gegen Missbrauch geschützt zu sein (siehe M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Wird das Telefon verloren, sollte die SIM-Karte dieses Telefons unverzüglich gesperrt werden, um Missbrauch und unnötige Kosten zu verhindern (siehe M 2.189 *Sperrung des Mobiltelefons bei Verlust*). Für die speziellen Gefährdungen der Informationssicherheit durch Mobiltelefone müssen die betreffenden Mitarbeiter besonders sensibilisiert werden (siehe M 2.558 *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*).

**Aussonderung**

Da sich auf Mobiltelefonen in der Regel vertrauliche Daten befinden, muss geregelt werden, wie die Geräte auszusondern sind. In Maßnahme M 4.465 *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs* werden Empfehlungen gegeben. Falls die Geräte herausnehmbare Speicherkarten besitzen, ist für diese Karten Maßnahme M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* anzuwenden, die beschreibt, wie die herausnehmbaren Speicherkarten entsorgt werden.

**Notfallvorsorge**

In der Maßnahme M 6.72 *Ausfallvorsorge bei Mobiltelefonen* werden wichtige Vorkehrungen beschrieben, durch die sich der Benutzer vor Ausfall und bei Verlust eines Mobiltelefons schützen kann.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Mobiltelefonen vorgestellt.

**Planung und Konzeption**
- M 2.188 (A) *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung*
- M 2.190 (Z) *Einrichtung eines Mobiltelefon-Pools*

**Umsetzung**
- M 4.114 (A) *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*

**Betrieb**
- M 2.189 (A) *Sperrung des Mobiltelefons bei Verlust*
- M 2.558 (A) *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*
- M 4.115 (B) *Sicherstellung der Energieversorgung von Mobiltelefonen*
- M 4.255 (A) *Nutzung von IrDA-Schnittstellen*
- M 5.78 (Z) *Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung*
- M 5.79 (Z) *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung*
- M 5.80 (Z) *Schutz vor Abhören der Raumgespräche über Mobiltelefone*
- M 5.81 (B) *Sichere Datenübertragung über Mobiltelefone*

**Aussonderung**
- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*
- M 4.465 (A) *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs*

**Notfallvorsorge**
- M 6.72 (C) *Ausfallvorsorge bei Mobiltelefonen*

# B 3.405 Smartphones, Tablets und PDAs


## Beschreibung

Dieser Baustein beschäftigt sich mit mobilen Endgeräten zur Datenerfassung, -bearbeitung und -kommunikation. Diese gibt es in verschiedenen Geräteklassen, die sich nach Abmessungen und Leistungsmerkmalen unterscheiden. Dazu gehören unter anderem:

- Organizer, um Adressen und Termine zu verwalten.
- PDAs mit und ohne eigene Tastatur, bei denen die Dateneingabe über das Display oder die Tastatur erfolgt. Der primäre Einsatzzweck ist das Erfassen und Bearbeiten von Terminen, E-Mails, Adressen und kleinen Notizen.
- Smartphones, also Mobiltelefone mit Computer-Funktionen und eingebauter Schnittstelle zur Datenübertragung. Beim Einsatz von Smartphones ist zusätzlich Baustein B 3.404 *Mobiltelefon* und gegebenenfalls Baustein B 3.203 *Laptop* umzusetzen.
- Tablets, bei denen es sich in der Regel um große Smartphones mit oder ohne Telefonfunktion handelt. Geräte, die größer als übliche Smartphones, aber noch kleiner als übliche Tablets sind, werden auch Smartlets oder Phablets genannt. Der Einsatzbereich ist identisch mit Smartphones, nur dass hier komfortabler Daten verarbeitet, Dokumente gelesen und im Internet gesurft werden kann. Beim Einsatz von Tablets mit Telefonfunktion ist zusätzlich Baustein B 3.404 *Mobiltelefon* umzusetzen.
- Den Übergang zu "echten" Notebooks stellen sogenannte Sub-Notebooks (Netbooks, Ultrabooks, etc.) dar, die wesentlich kleiner als normale Notebooks sind und daher beispielsweise weniger Peripheriegeräte und Anschlussmöglichkeiten bieten, die aber unter anderem für die Vorführung von Präsentationen geeignet sind. Viele Tablets lassen sich auch um eine Tastatur erweitern und sind dann wie ein Laptop zu benutzen. Beim Einsatz von Sub-Notebooks oder Tablets ist zusätzlich der Baustein B 3.203 *Laptop* umzusetzen.

Die Übergänge zwischen den verschiedenen Gerätetypen sind fließend und außerdem dem ständigen Wandel der Technik unterworfen. Eine typische Anforderung an Smartphones, Tablets und PDAs ist die Nutzung von Standard-Office-Anwendungen auch unterwegs. Hierfür werden angepasste Varianten von Textverarbeitungs-, Tabellenkalkulations-, E-Mail- bzw. Kalenderprogrammen angeboten. Die Geräte werden aber auch zunehmend für sicherheitskritische Applikationen eingesetzt, wie beispielsweise die Nutzung als Authentisierungstoken für Zugriffe auf Unternehmensnetze (z. B. Generierung von Einmalpasswörtern), Speicherung von Patientendaten oder die Führung von Kundenkarteien.

In diesem Baustein werden diejenigen Sicherheitseigenschaften von Smartphones, Tablets und PDAs betrachtet, die für die Anwender bei der Nutzung relevant sind. Es soll ein systematischer Weg aufgezeigt werden, wie Smartphones, Tablets und PDAs sicher in Institutionen eingesetzt werden können, wie Sicherheitskonzepte für diese Endgeräte erstellt und fortentwickelt werden sollten und wie auf diese Weise Smartphones, Tablets und PDAs sicher in einem Informationsverbund eingebettet werden können.

## Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von Smartphones, Tablets und PDAs folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.15 *Beeinträchtigung durch wechselnde Einsatzumgebung*

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*

- G 2.200 *Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*
- G 3.76 *Fehler bei der Synchronisation mobiler Endgeräte*
- G 3.123 *Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs*

**Technisches Versagen**

- G 4.42 *Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs*
- G 4.51 *Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs*
- G 4.52 *Datenverlust bei mobilem Einsatz*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*
- G 5.23 *Schadprogramme*
- G 5.123 *Abhören von Raumgesprächen über mobile Endgeräte*
- G 5.124 *Missbrauch der Informationen von mobilen Endgeräten*
- G 5.125 *Datendiebstahl mithilfe mobiler Endgeräte*
- G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*
- G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*
- G 5.193 *Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs*
- G 5.194 *Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion*

**Maßnahmenempfehlungen**

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Smartphones, Tablets und PDAs sind eine Reihe von Maßnahmen erforderlich, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Phasen, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Um Smartphones, Tablets und PDAs sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.303 *Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs*). Darauf aufbauend ist die Nutzung von Smartphones, Tablets und PDAs zu regeln und es sind Sicherheitsrichtlinien dafür zu erarbeiten (siehe M 2.304 *Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs*). Auf Smartphones, Tablets und PDAs können verschiedene Applikationen (Apps) installiert werden. Die Anwendungen müssen ausgewählt und sicher ausgeführt werden (siehe M 4.467 *Auswahl von Applikationen für Smartphones, Tablets und PDAs*).

**Beschaffung**

Für die Beschaffung von Smartphones, Tablets und PDAs müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf geeignete Geräte ausgewählt werden (siehe M 4.305 *Einsatz von Speicherbeschränkungen (Quotas)*). Auch muss geprüft werden, ob zusätzliche Sicherheitswerkzeuge anzuschaffen sind, die die Sicherheit von Smartphones, Tablets und

PDAs bis zu einem gewissen Grad erhöhen können (siehe M 4.231 *Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs*).

**Umsetzung**

Über mobile Endgeräte wie Laptops, Smartphones, Tablets oder PDAs soll auch häufig unterwegs auf Daten aus dem Internet oder dem internen Netz einer Institution zugegriffen werden. Dafür sollten zusätzliche Aspekte zum Schutz der Informationen berücksichtigt werden (siehe M 5.121 *Sichere Kommunikation von unterwegs*).

**Betrieb**

Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten (Smartphones/Tablets/PDA, Synchronisationssoftware, Software zum zentralen Geräte-Management) unterschiedlich konfiguriert werden. Dies betrifft vor allem die Endgeräte selber (siehe M 4.228 *Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs*), die Synchronisationsumgebung (siehe M 4.229 *Sicherer Betrieb von Smartphones, Tablets und PDAs*) und spezielle Software zum zentralen Geräte-Management (siehe M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs*). Damit Smartphones, Tablets und PDAs sicher eingesetzt werden können, müssen auch damit gekoppelte Arbeitsplatz-Rechner und hier vor allem die Synchronisationsschnittstelle sicher konfiguriert sein. Geeignete Sicherheitsempfehlungen für Standard-Arbeitsplatz-PCs sind in den Client-Bausteinen der Schicht 3 beschrieben.

**Aussonderung**

Bei Ausfall, Defekt, Zerstörung oder Diebstahl eines Smartphones, Tablets oder PDAs, sollte es in jeder Organisation klare Meldewege und Ansprechpartner geben (siehe M 2.306 *Verlustmeldung*). Zudem ist organisatorisch sicherzustellen, dass Smartphones, Tablets und PDAs auf geeignete Weise ausgesondert werden (siehe M 4.465 *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs*).

**Notfallvorsorge**

Ein Smartphone, Tablet oder PDA kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Daher sollten entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren (siehe M 6.95 *Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs*). Ebenso müssen entsprechende Empfehlungen umgesetzt werden, damit bei einem Diebstahl oder Verlust nicht alle Daten auf dem Endgerät verloren gehen oder in fremde Hänge gelangen (siehe M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*).

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Smartphones, Tablets und PDAs vorgestellt.

**Planung und Konzeption**

- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.303 (A) *Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs*
- M 2.304 (A) *Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs*
- M 4.467 (B) *Auswahl von Applikationen für Smartphones, Tablets und PDAs*
- M 4.468 (B) *Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs*

**Beschaffung**

- M 2.305 (B) *Geeignete Auswahl von Smartphones, Tablets oder PDAs*
- M 4.231 (Z) *Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs*

**Umsetzung**

- M 5.121 (B) *Sichere Kommunikation von unterwegs*

**Betrieb**

- M 1.33 (A) *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*
- M 2.558 (A) *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*

- M 4.3 (A) *Einsatz von Viren-Schutzprogrammen*
- M 4.31 (A) *Sicherstellung der Energieversorgung im mobilen Einsatz*
- M 4.228 (A) *Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs*
- M 4.229 (C) *Sicherer Betrieb von Smartphones, Tablets und PDAs*
- M 4.230 (Z) *Zentrale Administration von Smartphones, Tablets und PDAs*
- M 4.232 (Z) *Sichere Nutzung von Zusatzspeicherkarten*
- M 4.255 (A) *Nutzung von IrDA-Schnittstellen*
- M 4.466 (C) *Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs*
- M 4.469 (A) *Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion*
- M 5.173 (Z) *Nutzung von Kurz-URLs und QR-Codes*
- M 5.176 (B) *Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution*

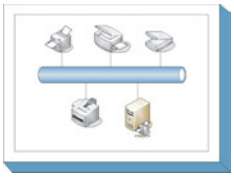
**Aussonderung**

- M 2.306 (A) *Verlustmeldung*
- M 4.465 (A) *Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs*

**Notfallvorsorge**

- M 6.95 (C) *Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs*
- M 6.159 (C) *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*

# B 3.406 Drucker, Kopierer und Multifunktionsgeräte



## Beschreibung

Zur Grundausstattung in Büroumgebungen gehören typischerweise Kopierer sowie bei IT-Arbeitsplätzen Drucker. Arbeitsergebnisse müssen oft auf Papier ausgegeben, bearbeitet und archiviert werden. Sehr häufig ist es aber nicht effizient, jeden einzelnen Arbeitsplatz mit einem Drucker auszustatten. Daher werden oft zentrale Netzdrucker, Kopierer oder Multifunktionsgeräte eingesetzt, auf denen die Benutzer ihre Dokumente ausdrucken oder vervielfältigen können.

Das direkte Versenden der Druckaufträge von den Arbeitsplatz-PCs an die Netzdrucker ist meist unerwünscht. Ein zentraler Server, der die Aufträge annimmt und auf die verfügbaren Druckern verteilt, bietet oft mehr Vor- als Nachteile. Daher gehört in der Regel ein Druckserver ebenfalls zu der Druckinfrastruktur.

Die Integration der papierverarbeitenden Geräte in ein Netz ist in vielen Fällen nicht nur auf Drucker beschränkt. Netzfähige Dokumentenscanner können beispielsweise für eine Vielzahl von Benutzern bereitgestellt werden, damit diese Papierdokumente digitalisieren können. In Verbindung mit einem Drucker kann ein Scanner beispielsweise wie ein Kopierer betrieben werden.

Dieser Baustein behandelt die Sicherheit von vernetzten Druckern, Druckservern, Dokumentenscannern, Kopierern und Multifunktionsgeräten. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste. Aus Gründen der Lesbarkeit werden nicht alle Gerätetypen überall einzeln benannt. Da aber beispielsweise für digitale Kopierer ähnliche Sicherheitsempfehlungen wie für Netzdrucker zu beachten sind, gelten für diese Geräte die Maßnahmen analog.

## Gefährdungslage

Wie jedes IT-System sind auch Drucker, digitale Kopierer, netzfähige Scanner und Multifunktionsgeräte vielfältigen Gefahren ausgesetzt. Für den IT-Grundschutz dieser Systeme werden die folgenden typischen Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.8 *Unkontrollierter Einsatz von Betriebsmitteln*
- G 2.15 *Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System*
- G 2.20 *Unzureichende oder falsche Versorgung mit Verbrauchsgütern*
- G 2.122 *Ungeeigneter Einsatz von Multifunktionsgeräten*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.86 *Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten*

**Technisches Versagen**

- G 4.43 *Undokumentierte Funktionen*
- G 4.64 *Komplexität von Druckern, Kopierern und Multifunktionsgeräten*
- G 4.65 *Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten*
- G 4.66 *Beeinträchtigung von Gesundheit und Umwelt durch Drucker, Kopierer und Multifunktionsgeräte*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.140 *Auswertung von Restinformationen in Druckern, Kopierern und Multifunktionsgeräten*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei Druckservern handelt es sich in der Regel um gewöhnliche IT-Systeme, die als ein entsprechender Server betrieben werden. In diesem Fall ist zusätzlich der Baustein B 3.101 *Allgemeiner Server* und der jeweilige betriebssystem-spezifische Server-Baustein zu berücksichtigen. Soll Samba als Druckserver auf Unix-Server eingesetzt werden oder sollen Unix-Clients auf Druckerfreigaben über Samba zugreifen dürfen, ist der Baustein B 5.17 *Samba* anzuwenden.

Für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten sollten im Hinblick auf die Informationssicherheit insbesondere die Teilbereiche

- Informations- und Kommunikationsverschlüsselung (Schutz der digitalen Daten),
- Systemschutz (Schutz der Geräte) und
- Dokumentenzugriff (Schutz der gedruckten Dokumente)

betrachtet werden.

**Planung und Konzeption**

Der Einsatz von Netzdruckern, Kopierern und Multifunktionsgeräten muss sorgfältig geplant werden (siehe M 2.397 *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*). In der Maßnahme M 4.304 *Verwaltung von Druckern* sind vertiefende Informationen zu den Bestandteilen und der Gestaltung typischer Druckerlandschaften zu finden. Die Sicherheitsanforderungen an Netzdrucker müssen in die allgemeine Sicherheitsstrategie der Institution integriert sein.

Viele der in Verbindung mit Druckern auftretenden Probleme können nicht immer mit technischen Maßnahmen gelöst werden. Die Benutzer müssen über eine sicherheitsbewusste Bedienung der Drucker informiert und hierauf verpflichtet werden (siehe M 2.397 *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*).

Neben klassischen Druckern sollten auch artverwandte Geräte berücksichtigt werden. Hierzu gehören beispielsweise Multifunktionsgeräte (M 5.146 *Netztrennung beim Einsatz von Multifunktionsgeräten*) und Dokumentenscanner (M 4.303 *Einsatz von netzfähigen Dokumentenscannern*).

**Beschaffung**

Anhand der Einsatzszenarien sind die Anforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen (siehe M 2.399 *Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten*).

**Umsetzung**

Sind alle Planungsschritte durchlaufen und alle Komponenten beschafft, geht es um die Inbetriebnahme der Geräte. Dabei kommt es auch darauf an, wo die Geräte positioniert werden (siehe M 1.32 *Geeignete Aufstellung von Druckern und Kopierern*) und wie der Zugriff auf die Geräte beschränkt wird (M 4.301 *Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte*).

Wie jedes IT-System sollten auch netzfähige Drucker, Kopierer und Scanner vor unberechtigter Nutzung geschützt werden (siehe M 4.299 *Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten*). Aber auch die Medien, auf denen die (digitalen) Informationen übertragen und abgelegt werden, müssen angemessen geschützt werden. Dies wird in der Maßnahme M 4.300 *Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten* beschrieben.

Neben der Druckhardware sind die Softwarekomponenten, wie Druckserver oder -clients, für einen sicheren Betrieb wichtig. In Abhängigkeit vom eingesetzten Betriebssystem und Drucksystem sind entsprechende Maßnahmen und Bausteine, wie M 5.145 *Sicherer Einsatz von CUPS* oder B 5.17 *Samba* umzusetzen.

**Betrieb**

Im Regelbetrieb ist neben der Protokollierung wichtiger Ereignisse (siehe M 4.302 *Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten*) auch die Versorgung der Geräte mit Verbrauchsgütern (siehe M 2.52 *Versorgung und Kontrolle der Verbrauchsgüter*) von hoher Bedeutung.

**Aussonderung**

Sehr oft sind im Speicher der Drucker, Kopierer, Scanner und Multifunktionsgeräte schutzbedürftige Informationen abgelegt. Bei der Entsorgung der Geräte muss die Maßnahme M 2.400 *Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten* berücksichtigt werden.

**Notfallvorsorge**

Aspekte der Notfallplanung für vernetzte Drucker, Kopierer, Dokumentenscanner und Multifunktionsgeräte werden in der Maßnahme M 6.105 *Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten* thematisiert.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Drucker, Kopierer und Multifunktionsgeräte" vorgestellt.

**Planung und Konzeption**
- M 2.397 (A) *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*
- M 2.398 (A) *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*

**Beschaffung**
- M 2.399 (W) *Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten*

**Umsetzung**
- M 1.32 (B) *Geeignete Aufstellung von Druckern und Kopierern*
- M 4.299 (Z) *Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten*
- M 4.300 (Z) *Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten*
- M 4.301 (C) *Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte*
- M 5.145 (A) *Sicherer Einsatz von CUPS*

**Betrieb**
- M 2.52 (C) *Versorgung und Kontrolle der Verbrauchsgüter*
- M 4.302 (C) *Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten*
- M 4.303 (C) *Einsatz von netzfähigen Dokumentenscannern*
- M 4.304 (W) *Verwaltung von Druckern*
- M 5.146 (C) *Netztrennung beim Einsatz von Multifunktionsgeräten*

**Aussonderung**
- M 2.13 (A) *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*
- M 2.400 (A) *Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten*

**Notfallvorsorge**
- M 6.105 (C) *Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten*

# B 3.407 Eingebettetes System

## Beschreibung

Eingebettete Systeme sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind, dort Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben übernehmen und dabei oft nicht direkt vom Benutzer wahrgenommen werden. Ist ein eingebettetes System betriebsmittelarm, d.h. sind seine Ressourcen hinsichtlich Speicher, CPU und Energie extrem beschränkt und verfügt es über keine Benutzerschnittstelle, wird von einem tief eingebetteten System gesprochen. Beispiele für solche tief eingebetteten Systeme sind Herzschrittmacher und Subsysteme von Autos und Flugzeugen.

Eingebettete Systeme finden sich sowohl im Bereich der Hochtechnologie, wie z. B. der Luft- und Raumfahrt, der Medizintechnik, der Telekommunikation und der Automobil-Technik, als auch im Consumer- und Haushaltsgerätebereich.

Ein eingebettetes System ist dadurch charakterisiert, dass es, anders als z. B. ein PC, eine oder mehrere genau definierte Aufgaben hat. Es bildet soft- und hardwaremäßig eine funktionale Einheit, die nur diese definierten Aufgaben erfüllt. Die Software eingebetteter Systeme wird als Firmware bezeichnet und ist zumeist in einem Flash-Speicher, einem EPROM, EEPROM oder ROM gespeichert und durch den Anwender nicht oder nur mit speziellen Mitteln bzw. Funktionen austauschbar. Sie besteht im Wesentlichen aus dem Bootloader, dem Betriebssystem und der Anwendung, wobei spezialisierte Systeme auf ein Betriebssystem verzichten. Eingebettete Systeme sind zwar spezialisierte Geräte aber im Gegensatz zur reinen Hardwareimplementierung (ASIC) universelle Rechner. Als Plattformen kommen unterschiedliche CPU-Architekturen oder flexible hochintegrierte Field Programmable Gate Array (FPGA) Bausteine in Frage.

Eingebettete Systeme haben entweder keine Bedienschnittstelle oder nutzen Spezialperipherie, wie z.B. funktionelle Tasten, Drehschalter und auf den jeweiligen Einsatzzweck hin konzipierte Anzeigen. Das Spektrum an Ausgabeeinheiten reicht von einer einfachen Signallampe über LCDs bis hin zu komplexen Cockpit-Anzeigen. Eingebettete Systeme kommunizieren häufig über Datenbusse, die in komplexen Systemen heterogen vernetzt sind. Zusätzlich können über mehrere unterschiedliche und mehrkanalige Ein-/Ausgabeports Peripheriekomponenten wie Sensoren und Aktoren, angebunden sein. Einige Arten eingebetteter Systeme verfügen über ein Webinterface, über das per Browser Konfigurationseinstellungen vorgenommen werden können.

Die Anforderungen an eingebettete Systeme sind applikationsspezifisch, lassen sich aber wie folgt charakterisieren:

- Robuste, störungsarme Funktion
- Komplexität von Hard- und Software an Applikation angepasst
- Antwortverhalten meist innerhalb definierter Zeitvorgaben
- Mehrere unterschiedliche Schnittstellen (Datenbus, analoge und digitale I/O-Ports)
- Direkte Interaktion mit Sensoren und Aktoren

Dieser Baustein beschäftigt sich allgemein mit eingebetteten Systemen und soll für ein großes Spektrum unterschiedlicher eingebetteter Systeme anwendbar sein. Auf dedizierte Sicherheitseigenschaften etwa von Bedien- und Anzeigesystemen oder spezifischen Hard- und Software-Architekturen wird nicht näher eingegangen.

Eine besondere Anwendung eines eingebetteten Systems sind Chipkarten. Die Karten besitzen in der Regel einen Prozessor, Arbeitsspeicher und I/O-Interfaces. Auch für Smartcards gilt, dass zwar grundsätzliche Sicherheitsaspekte in diesem Baustein angesprochen werden, allerdings keine spezifischen Aspekte betrachtet werden.

Der Baustein ist grundsätzlich für einen Informationsverbund mit einem oder mehreren eingebetteten Systemen anzuwenden, wenn diese den folgenden Kriterien entsprechen:

- Das eingebettete System wird separat beschafft und ist kein integrierter Bestandteil eines umgebenden Systems.
- Es ist möglich, die Prozesse der Auswahl, Beschaffung und ggf. Herstellung des eingebetteten Systems zu überwachen und zu beeinflussen.
- Die Umsetzung der Maßnahmen dieses Bausteins ist möglich und überprüfbar.
- Das eingebettete System bietet keine direkte Benutzerinteraktion.

## Gefährdungslage

Für den IT-Grundschutz eingebetteter Systeme werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.29 *Softwaretest mit Produktionsdaten*
- G 2.206 *Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen*
- G 2.207 *Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen*
- G 2.208 *Unzureichende physische Absicherung der elektronischen Komponenten bei eingebetteten Systemen*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.39 *Software-Konzeptionsfehler*
- G 4.43 *Undokumentierte Funktionen*
- G 4.100 *Hardwareausfall und Hardwarefehler bei eingebetteten Systemen*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.23 *Schadprogramme*
- G 5.141 *Datendiebstahl über mobile Datenträger*
- G 5.201 *Einspielen (Flashen) von manipulierten Software-Updates/-Upgrades bei eingebetteten Systemen*
- G 5.202 *Seitenkanalangriffe auf eingebettete Systeme*
- G 5.203 *Physikalischer Eingriff in ein eingebettetes System*
- G 5.204 *Eindringen und Manipulation über die Kommunikationsschnittstelle von eingebetteten Systemen*
- G 5.205 *Einsatz gefälschter Komponenten*
- G 5.206 *Reverse Engineering*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

**Planung und Konzeption**

Eine sorgfältige Planung und Konzeption ist für eingebettete Systeme unverzichtbar. Wird ein eingebettetes System selbst entwickelt oder ein Entwicklungsauftrag vergeben, sind die Grundsätze sicherer Entwicklung zu berücksichtigen (siehe M 2.378 *System-Entwicklung*). Entwicklungswerkzeuge müssen

fehlerfrei sein und dürfen nicht unerkannt manipuliert werden können (siehe M 2.567 *Auswahl vertrauenswürdiger Entwicklungswerkzeuge*). Um bei erhöhtem Schutzbedarf das geforderte Sicherheitsniveau für ein eingebettetes System nachzuweisen, ist eine Überprüfung nach anerkannten Kriterien durchzuführen (siehe M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*).

Die Sicherheitseigenschaften bzw. der Rahmen für Sicherheitsfunktionen eines eingebetteten Systems werden bereits durch konzeptionelle Festlegungen eingegrenzt. Bei der grundsätzlichen Entscheidung zur Software-Hardware-Aufteilung sind die unterschiedlichen Sicherheitseigenschaften der Realisierungen in Software oder Hardware zu berücksichtigen (siehe M 4.482 *Hardware-Realisierung von Funktionen eingebetteter Systeme*). Zur Erhöhung der Systemstabilität sollte, falls erforderlich, ein hardware- oder softwarebasierter Speicherschutz implementiert werden (siehe M 4.484 *Speicherschutz bei eingebetteten Systemen*). Das verwendete Betriebssystem sollte dem aktuellen Stand der Technik entsprechend absturzsicher sein und wenig Angriffspunkte aufweisen (siehe M 4.485 *Sicheres Betriebssystem für eingebettete Systeme*). Um die Integrität und Vertraulichkeit von Programmen und Nutzdaten zu sichern, sollten kryptografische Verfahren eingesetzt werden (siehe M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*). In einem Hardware-Sicherheitsmodule (Trusted Platform Module) können Schlüssel sicher erzeugt und abgelegt werden und somit Informationen und Komponenten sicher authentifiziert werden (siehe M 4.483 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*).

Bereits in der Planungsphase sollen Regelungen für den späteren Betrieb festgelegt werden (siehe M 2.562 *Regelung des Einsatzes von eingebetteten Systemen*).

**Beschaffung**

Bevor ein eingebettetes System beschafft wird, müssen dessen Anforderungen ermittelt werden. Die Kriterienliste muss auch die erforderlichen Sicherheitseigenschaften umfassen (siehe M 2.564 *Beschaffungskriterien für eingebettete Systeme*). Die beschafften Systeme oder Komponenten müssen genau der Spezifikation entsprechen und der Beschaffungsprozess muss so gestaltet sein, dass er nicht manipulierbar ist. (siehe M 2.563 *Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme*).

**Umsetzung**

Eingebettete Systeme sind in der Entwicklung und vor Aufnahme des Echtbetriebes im erforderlichen Umfang zu testen (siehe M 2.568 *Testverfahren für Software*). Sie sind gegen physische Manipulationen zu schützen (siehe M 4.487 *Tamper-Schutz (Erkennung, Verhinderung, Abwehr) bei eingebetteten Systemen*). Es dürfen nur die benötigten physikalischen und logischen Schnittstellen vorhanden sein und ein Zugang darf nur nach erfolgreicher Authentisierung möglich sein (siehe M 4.488 *Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen*). Der Bootprozess darf nicht kompromittierbar sein (siehe M 4.489 *Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen*).

**Betrieb**

Falls das eingebettete System in rauer Umgebung betrieben wird, sollte es entsprechend geschützt sein (siehe M 1.81 *Materielle Sicherung von eingebetteten Systemen*).

Änderungen an Konfigurationsparametern und der Firmware müssen sorgfältig geplant, durchgeführt und dokumentiert werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System* und M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen* sowie M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Im operativen Betrieb darf ein eingebettetes System keine Codeelemente enthalten, die nicht Bestandteil der Systemfunktionalität sind (siehe M 4.491 *Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen*). Kryptovariablen dürfen nicht kompromittierbar sein (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen* und M 2.46 *Geeignetes Schlüsselmanagement*). Falls ein Webserver integriert ist, dürfen nur die benötigten Komponenten und Funktionen installiert bzw. aktiviert werden und es sind gleichwertige Sicherheitsmechanismen zu konfigurieren wie bei Webservern im Bürobereich (siehe M 4.492 *Sichere Konfiguration und Nutzung eines eingebetteten Webservers*).

Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines eingebetteten Systems ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Sicherheitsrelevante Ereignisse im Betrieb eines eingebetteten Systems sind im Rahmen der technischen Möglichkeiten zu dokumentieren (siehe M 2.565 *Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen*). Darüber hinaus sollten sämtliche Baugruppen eines eingebetteten Systems mit erhöhten Anforderungen an die Verfügbarkeit und Integrität integrierte Selbsttesteinrichtungen besitzen und nutzen (siehe M 4.490 *Automatische Überwachung der Baugruppenfunktion (BIST) bei eingebetteten Systemen*).

**Aussonderung**

Mit der Aussonderung eines eingebetteten Systems dürfen keine vertraulichen Informationen zu Hardware, Software und Daten an Unberechtigte gelangen (siehe M 2.566 *Sichere Aussonderung eines eingebetteten Systems*).

**Notfallvorsorge**

Bei erhöhten Anforderungen an die Verfügbarkeit sollten Mechanismen vorhanden sein, um die letzte funktionierende Konfiguration und den Auslieferungszustand wiederherzustellen (siehe M 6.163 *Wiederherstellung von eingebetteten Systemen*).

Befinden sich auf einem eingebetteten System eingestufte Informationen, muss es eine Notlöschfähigkeit besitzen (siehe ebenfalls M 6.163 *Wiederherstellung von eingebetteten Systemen*).

**Planung und Konzeption**
- M 2.378 (Z) *System-Entwicklung*
- M 2.562 (A) *Regelung des Einsatzes von eingebetteten Systemen*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*
- M 4.482 (C) *Hardware-Realisierung von Funktionen eingebetteter Systeme*
- M 4.483 (C) *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*
- M 4.484 (C) *Speicherschutz bei eingebetteten Systemen*
- M 4.485 (A) *Sicheres Betriebssystem für eingebettete Systeme*
- M 4.486 (Z) *Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe*

**Beschaffung**
- M 2.66 (Z) *Beachtung des Beitrags der Zertifizierung für die Beschaffung*
- M 2.563 (Z) *Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme*
- M 2.564 (A) *Beschaffungskriterien für eingebettete Systeme*
- M 2.567 (Z) *Auswahl vertrauenswürdiger Entwicklungswerkzeuge*

**Umsetzung**
- M 2.46 (A) *Geeignetes Schlüsselmanagement*
- M 2.568 (A) *Testverfahren für Software*
- M 4.487 (Z) *Tamper-Schutz (Erkennung, Verhinderung, Abwehr) bei eingebetteten Systemen*
- M 4.488 (A) *Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen*
- M 4.489 (C) *Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen*

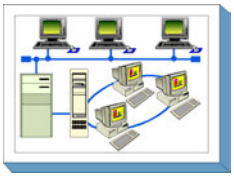
**Betrieb**
- M 1.81 (A) *Materielle Sicherung von eingebetteten Systemen*
- M 2.34 (A) *Dokumentation der Veränderungen an einem bestehenden System*
- M 2.565 (A) *Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.177 (B) *Sicherstellung der Integrität und Authentizität von Softwarepaketen*
- M 4.490 (A) *Automatische Überwachung der Baugruppenfunktion (BIST) bei eingebetteten Systemen*
- M 4.491 (A) *Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen*
- M 4.492 (B) *Sichere Konfiguration und Nutzung eines eingebetteten Webservers*

**Aussonderung**
- M 2.566 (C) *Sichere Aussonderung eines eingebetteten Systems*

**Notfallvorsorge**
- M 6.163 (A) *Wiederherstellung von eingebetteten Systemen*

# B 4 Netze

# B 4.1 Lokale Netze



## Beschreibung

Ein Local Area Network (LAN) ist ein Zusammenschluss von netzfähigen IT-Systemen, wie z. B. Clients, Server, Router oder Switches innerhalb eines räumlich begrenzten Gebiets. Um die IT-Systeme zu vernetzen, können unterschiedliche Übertragungsmedien eingesetzt werden, wie beispielsweise verdrillte Kupferkabel oder Lichtwellenleiter. Zunehmend werden die Daten auch drahtlos übertragen, z. B. per WLAN. Neben den IT-Systemen und der Verkabelung sind die eingesetzten LAN-Techniken und insbesondere die zugrunde liegende Topologie wesentliche Bestandteile eines LANs.

Die Verkabelung sowie die anwendungsbezogenen IT-Systeme, wie beispielsweise Server oder Clients, werden im Baustein B 2.12 *IT-Verkabelung* beziehungsweise in den entsprechenden Bausteinen der Schicht 3 behandelt, so dass im vorliegenden Baustein primär netzspezifische Aspekte (geeignete Segmentierung, Auswahl einer geeigneten Netztopologie, Bildung von Teilnetzen etc.) betrachtet werden.

Ethernet ist die am häufigsten eingesetzte LAN-Technik und gilt als der de-facto LAN-Standard. Daher werden in diesem Baustein nur Ethernet-LANs sowie die zugehörigen Netzkomponenten, wie z. B. Router und Switches betrachtet. FDDI, Token Ring und Token Bus gelten als veraltet und werden kaum noch verwendet. Bei der Auswahl aktiver Netzkomponenten wird der Fokus auf Router und Switches gelegt. Shared LANs unter dem Einsatz von Repeatern, Hubs und Bridges werden heutzutage nicht mehr betrieben. Fragestellungen im Zusammenhang mit einer WAN-Anbindung werden im vorliegenden Baustein ebenfalls nicht behandelt. Hier sei unter anderem auf den Baustein B 3.301 *Sicherheitsgateway (Firewall)* verwiesen.

Dieser Baustein beschreibt einen Leitfaden, wie ein lokales Netz analysiert und darauf aufbauend unter Sicherheitsaspekten konzipiert und betrieben werden kann. Damit richtet er sich an die Stelle einer Institution, die für den Netzbetrieb verantwortlich ist und das entsprechende fachliche Wissen besitzt.

## Gefährdungslage

Für den IT-Grundschutz eines lokalen Netzes werden pauschal die folgenden Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*
- G 1.3 *Blitz*
- G 1.4 *Feuer*
- G 1.5 *Wasser*
- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.8 *Staub, Verschmutzung*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.44 *Inkompatible aktive Netzkomponenten*
- G 2.45 *Konzeptionelle Schwächen des Netzes*
- G 2.46 *Überschreiten der zulässigen Kabellänge*

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.28 *Ungeeignete Konfiguration der aktiven Netzkomponenten*
- G 3.29 *Fehlende oder ungeeignete Segmentierung*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*

**Technisches Versagen**

- G 4.1 *Ausfall der Stromversorgung*
- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.31 *Ausfall oder Störung von Netzkomponenten*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.5 *Vandalismus*
- G 5.6 *Anschlag*
- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.28 *Verhinderung von Diensten*
- G 5.66 *Unberechtigter Anschluss von IT-Systemen an ein Netz*
- G 5.67 *Unberechtigte Ausführung von Netzmanagement-Funktionen*
- G 5.68 *Unberechtigter Zugang zu den aktiven Netzkomponenten*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Hierzu zählen zwingend die Bausteine B 4.2 *Netz- und Systemmanagement*, B 2.12 *IT-Verkabelung* und B 3.302 *Router und Switches*.

Weiterhin müssen die aktiven Netzkomponenten gesichert aufgestellt sein, also beispielsweise in Räumen für technische Infrastruktur (z. B. Verteilerräumen) untergebracht werden, so dass auch die Maßnahmen aus dem Baustein B 2.6 *Raum für technische Infrastruktur* realisiert werden müssen.

Für den sicheren Einsatz eines lokalen Netzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Analyse der aktuellen Netzsituation über die Konzeption bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Die Absicherung eines LANs beginnt in der Planungsphase. Der erste Schritt ist immer die Erhebung und daran anschließende Analyse der vorliegenden Netzsituation. Basierend auf den Ergebnissen der Analyse kann dann das LAN konzipiert und realisiert werden, um die vorher festgelegten Netz-Anforderungen zu erfüllen. Besondere Aufmerksamkeit bei der Planung und Konzeption eines LANs ist der Netz-Segmentierung zu widmen. Nur durch eine geeignete physische und gegebenenfalls logische Segmentierung kann verhindert werden, dass Angriffe auf ein Teilnetz die Funktionsfähigkeit anderer Teilnetze beeinträchtigen.

Außerdem muss eine Sicherheitsrichtlinie für das LAN erstellt werden, in der Regelungen und Hinweise zum sicheren Betrieb und zur sicheren Administration des LANs beschrieben sind (siehe M 2.576 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen*).

**Umsetzung**

Sind alle Komponenten beschafft und geht es um die Einrichtung des LANs, so hat die Konfiguration der unterschiedlichen LAN-Komponenten und insbesondere der aktiven Netzkomponenten (siehe M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*) während der Installation stets gemäß der Sicherheitsrichtlinie und der festgelegten Strategie zu erfolgen.

**Betrieb**

Ist das LAN in Betrieb genommen und wurden alle LAN-Anwender ausreichend geschult, so ist zum einen durch regelmäßige Audits (siehe M 2.579 *Regelmäßige Audits des lokalen Netzes*) sicherzustellen, dass alle getroffenen Sicherheitseinstellungen noch aktuell sind und durch regelmäßige Sicherheitschecks (siehe M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*), ob diese Einstellungen auch greifen. Durch den Einsatz einer Netz-Management-Software kann das LAN zentral administriert werden (siehe M 2.146 *Sicherer Betrieb eines Netzmanagement-Systems*).

**Aussonderung**

Werden LAN-Komponenten außer Betrieb genommen, so sind entsprechende Konfigurationseinstellungen, wieder auf Standard-Werte zurückzusetzen und eventuell auf den LAN-Komponenten gespeicherte Informationen oder Zugangsinformationen zu löschen (M 2.580 *Außerbetriebnahme von Netzkomponenten*).

**Notfallvorsorge**

Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, muss ein Notfallplan für den Ausfall des lokalen Netzes (siehe M 6.165 *Erstellen eines Notfallplans für den Ausfall des lokalen Netzes*) erstellt werden. Hierzu gehört insbesondere auch eine regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*).

Nachfolgend wird das komplette Maßnahmenbündel für den Bereich Lokale Netze vorgestellt.

**Planung und Konzeption**

- M 2.139 (A) *Ist-Aufnahme der aktuellen Netzsituation*
- M 2.140 (Z) *Analyse der aktuellen Netzsituation*
- M 2.141 (B) *Entwicklung eines Netzkonzeptes*
- M 2.576 (A) *Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen*
- M 2.577 (Z) *Auswahl geeigneter Kryptoverfahren für Netze*
- M 4.79 (A) *Sichere Zugriffsmechanismen bei lokaler Administration*
- M 5.2 (A) *Auswahl einer geeigneten Netz-Topologie*
- M 5.13 (A) *Geeigneter Einsatz von Elementen zur Netzkopplung*
- M 5.60 (A) *Auswahl einer geeigneten Backbone-Technologie*
- M 5.61 (A) *Geeignete physische Segmentierung*
- M 5.62 (C) *Geeignete logische Segmentierung*
- M 5.77 (Z) *Bildung von Teilnetzen*

**Umsetzung**

- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.80 (B) *Sichere Zugriffsmechanismen bei Fernadministration*
- M 4.82 (A) *Sichere Konfiguration der aktiven Netzkomponenten*
- M 5.7 (A) *Netzverwaltung*

**Betrieb**

- M 2.578 (Z) *Installation, Konfiguration und Betreuung eines lokalen Netzes durch Dritte*
- M 2.579 (B) *Regelmäßige Audits des lokalen Netzes*
- M 4.81 (B) *Audit und Protokollierung der Aktivitäten im Netz*
- M 4.83 (C) *Update/Upgrade von Soft- und Hardware im Netzbereich*

- M 5.8 (B) *Regelmäßiger Sicherheitscheck des Netzes*

**Aussonderung**

- M 2.580 (C) *Außerbetriebnahme von Netzkomponenten*

**Notfallvorsorge**

- M 6.52 (A) *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*
- M 6.53 (Z) *Redundante Auslegung der Netzkomponenten*
- M 6.54 (B) *Verhaltensregeln nach Verlust der Netzintegrität*
- M 6.75 (Z) *Redundante Kommunikationsverbindungen*
- M 6.165 (C) *Erstellen eines Notfallplans für den Ausfall des lokalen Netzes*

# B 4.2 Netz- und Systemmanagement

## Beschreibung

Ein Managementtool für ein im Allgemeinen lokales Rechnernetz (LAN) dient dazu, möglichst alle im lokale Netz angesiedelten Netz-Komponenten zentral zu verwalten. Außerdem gibt ein solches System Auskunft über den aktuellen Status des Netzes und der darin enthaltenen Komponenten. Auf diese Weise kann ein Netzmanagementtool helfen, Sicherheit im Netz zu etablieren. Grundsätzlich kann zwischen Netzmanagement und Systemmanagement unterschieden werden. Die Unterschiede ergeben sich durch die jeweils verwalteten Komponenten.

Das Netzmanagement umfasst die Gesamtheit der Vorkehrungen und Aktivitäten, um sicherzustellen, dass ein Netz effektiv eingesetzt wird. Hierzu gehört beispielsweise die Überwachung der Netzkomponenten auf ihre korrekte Funktion, das Monitoring der Netzperformance und die zentrale Konfiguration der Netzkomponenten. Netzmanagement ist in erster Linie eine organisatorische Problemstellung, deren Lösung lediglich mit technischen Mitteln unterstützt werden kann.

Systemmanagement befasst sich in erster Linie mit dem Management verteilter IT-Systeme. Hierzu gehört beispielsweise eine zentrale Verwaltung der Benutzer, Softwareverteilung, Management der Anwendungen usw. In einigen Bereichen, wie z. B. dem Konfigurationsmanagement (dem Überwachen und Konsolidieren von Konfigurationen eines Systems oder einer Netzkomponente), sind Netz- und Systemmanagement nicht klar zu trennen.

Im Folgenden wird das (Software-) Tool, das zum Verwalten eines Netzes und dessen Komponenten dient, immer als "Managementsystem" bezeichnet, die damit verwalteten Komponenten werden als "verwaltetes System" bezeichnet. Im Englischen werden hier die Begriffe "management system" und "managed system" verwendet, dies gilt insbesondere für den Bereich Netzmanagement.

Prinzipiell ist die Architektur von Managementsoftware zentralistisch aufgebaut: Es gibt eine zentrale Managementstation oder -konsole, von der aus die Systemadministratoren das ihnen anvertraute Netz mit den darin befindlichen Hard- und Software-Komponenten verwalten können. Insbesondere die Systeme zum Netzmanagement bauen darauf auf.

Einem Netzmanagement-System liegt in der Regel ein Modell zugrunde, das zwischen "Manager", "Agent" (auch "Managementagent") und "verwalteten Objekten" (auch "managed objects") unterscheidet. Die weiteren Bestandteile sind das zur Kommunikation verwendete Protokoll zwischen Manager und den Agenten, sowie eine Informationsdatenbank, die so genannte "MIB" (Management Information Base). Die MIB muss sowohl dem Manager als auch jedem Managementagenten zur Verfügung stehen. Konzeptionell werden Managementagenten und deren MIB als Teil des verwalteten Systems angesehen.

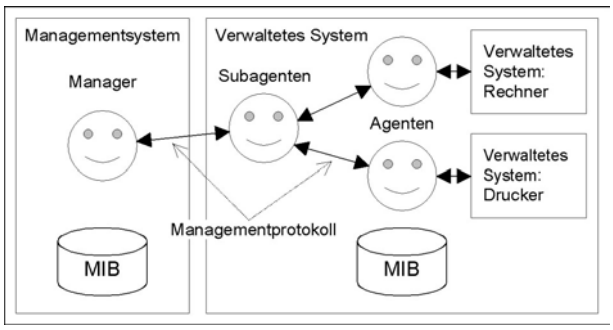



Abbildung: Netzmanagementsystem

Ein Agent ist für ein oder mehrere zu verwaltende Objekte zuständig. Es ist möglich, die Agenten hierarchisch zu organisieren: Ein Agent ist dann für die ihm zugeordneten Unteragenten zuständig. Am En-

de einer jeden auf diese Art entstehenden Befehlskette steht immer ein zu verwaltendes Objekt. Ein zu verwaltendes Objekt ist entweder ein physisch vorhandenes Objekt (Gerät), wie ein Rechner, ein Drucker oder ein Router, oder ein Softwareobjekt, wie z. B. ein Hintergrundprozess zur Verwaltung von Druckaufträgen. Bei Geräten, die über ein Managementsystem verwaltet werden können, ist der Managementagent in der Regel schon vom Hersteller in das Gerät "fest" eingebaut. Versteht dieser das vom Manager verwendete Kommunikationsprotokoll nicht, ist z. B. ein Software-Managementagent nötig, der die Protokollumsetzung beherrscht. In ähnlicher Weise können Software-Komponenten den Managementagenten schon enthalten, oder es wird ein spezieller Managementagent benötigt, der für die Verwaltung dieser Software-Komponente konzipiert ist.

Um die einzelnen Komponenten des zu verwaltenden Systems anzusprechen, tauschen der Manager und die jeweiligen Agenten Informationen aus. Die Art des zur Kommunikation verwendeten Protokolls bestimmt maßgeblich die Mächtigkeit und insbesondere die Sicherheit des Managementsystems.

Prinzipiell können Managementsysteme bezüglich des verwendeten Kommunikationsprotokolls in drei Kategorien unterteilt werden (siehe auch M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll*):

- Es wird SNMP (Simple Network Management Protocol) benutzt, das weit verbreitete Standardprotokoll des TCP/IP-basierten Systemmanagements.
- Es wird CMIP (Common Management Information Protocol) benutzt. CMIP wird hauptsächlich zum Management von Telekommunikationsnetzen eingesetzt und hat in der TCP/IP-basierten Kommunikation keine Bedeutung.
- Es wird ein herstellerspezifisches Protokoll benutzt. Es existiert meist die Möglichkeit, so genannte Adapter zum Einbinden der Standardprotokolle zu verwenden, wobei in der Regel lediglich eine SNMP-Anbindung existiert.

Systemmanagementsysteme sind zwar in der Regel auch zentralistisch ausgelegt, um das Verwalten des Systems von einer Managementstation aus zu erlauben, die konkrete Architektur hängt jedoch davon ab, wie groß die Systeme, die verwaltet werden können, sein dürfen und welcher Funktionsumfang angeboten wird. Hier reicht die Palette von einfachen Sammlungen von Management-Tools, die ohne Integration nebeneinander in kleinen Netzen eingesetzt werden, bis hin zu Managementplattformen, die ein weltumspannendes Firmennetz mit mehreren tausend Rechnern verwalten können.

Bestimmte Managementplattformen benutzen proprietäre Protokolle zur Kommunikation zwischen den Komponenten. Diese Systeme weisen in der Regel ein wesentlich höheres Leistungsspektrum auf und dienen nicht nur dem Netz- und Systemmanagement, sondern bieten unternehmens- bzw. behördenweites Ressourcenmanagement an.

## Gefährdungslage

Für den IT-Grundschutz eines Managementsystems werden die folgenden typischen Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.59 *Betreiben von nicht angemeldeten Komponenten*
- G 2.60 *Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement*
- G 2.61 *Unberechtigte Sammlung personenbezogener Daten*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.28 *Ungeeignete Konfiguration der aktiven Netzkomponenten*
- G 3.34 *Ungeeignete Konfiguration des Managementsystems*
- G 3.35 *Server im laufenden Betrieb ausschalten*
- G 3.36 *Fehlinterpretation von Ereignissen*

**Technisches Versagen**

- G 4.31 *Ausfall oder Störung von Netzkomponenten*
- G 4.38 *Ausfall von Komponenten eines Netz- und Systemmanagementsystems*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.28 *Verhinderung von Diensten*
- G 5.66 *Unberechtigter Anschluss von IT-Systemen an ein Netz*
- G 5.67 *Unberechtigte Ausführung von Netzmanagement-Funktionen*
- G 5.86 *Manipulation von Managementparametern*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Hierzu zählen zwingend die Bausteine B 4.1 *Lokale Netze*, B 2.12 *IT-Verkabelung* und B 3.302 *Router und Switches*.

Das zu verwaltende System besteht aus einzelnen Clients, Servern, aktiven Netzkomponenten (Netzkoppelelementen) und passiven Netzkomponenten (Verkabelung und Patchfelder). Jede dieser Komponenten ist ein potentielles Sicherheitsrisiko für das gesamte Netz. Diese Risiken können im Allgemeinen nicht alleine durch die Einführung von Managementsoftware vollständig beseitigt werden. Dies gilt schon deshalb, weil in der Regel nicht alle Systeme in gleichem Maße durch ein Managementsystem erfasst werden. Als Grundvoraussetzung für die Systemsicherheit muss eine institutionsweiten Sicherheitsrichtlinie festgelegt werden, die sich im betrachteten Fall insbesondere in der sicheren Konfiguration von Hard- und Software niederschlagen muss. Aus diesem Grund sollten neben den oben erwähnten Bausteinen insbesondere auch die Bausteine der Schicht 3 betrachtet werden.

Da Netz- und Systemmanagementsysteme von einem zentralistischen Ansatz ausgehen, kommt der zentralen Managementstation unter Sicherheitsgesichtspunkten eine besondere Bedeutung zu. Diese ist daher besonders zu schützen. Zentrale Komponenten eines Netz- und Systemmanagementsystems sollten daher in Räumen aufgestellt werden, die den Anforderungen an einen Serverraum (vergleiche Baustein B 2.4 *Serverraum*) entsprechen. Wenn kein Serverraum zur Verfügung steht, können sie alternativ in einem Serverschrank aufgestellt werden (vergleiche Baustein B 2.7 *Schutzschränke*).

Für den erfolgreichen Aufbau eines Netz- und Systemmanagementsystems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb.Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Grundlegend für die Einführung eines Managementsystems ist die Erstellung eines Konzepts für das Netzmanagement (siehe M 2.143 *Entwicklung eines Netzmanagement-Konzeptes* ) und einer Strategie für das Systemmanagement (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*). Konzept und Strategie müssen sich an der Größe und Struktur des zu verwaltenden Netzes orientieren und zukünftige Entwicklungen des Netzes berücksichtigen.

Eng mit der Entscheidung für ein Netzmanagement-Tool verknüpft ist die Wahl eines Netzmanagement-Protokolls (M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll*). Die Auswahl eines Systemmanagement-Tools wird von der Analyse der im Netz enthaltenen IT beeinflusst (M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagement-Systems*).

Es muss verhindert werden, dass Managementinformationen, die zwischen der zentralen Komponente des Managementsystems und den zu verwaltenden IT-Systemen übertragen werden, abgehört bzw. manipuliert werden können (siehe M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll* sowie M 2.581 *Aufbau eines Administrationsnetzes für das Netzmanagement* ).

Schon in der Planungsphase sollten Protokollierung inklusive Auswertung der gesammelten Protokollinformationen vorbereitet werden (siehe M 2.499 *Planung der Protokollierung* ). Neben deren Absicherung ist hierfür eine einheitliche Systemzeit für alle Komponenten, die protokolliert werden, wesentlich, da sonst eine Auswertung der Protokolldaten erschwert wird (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation* Einsatz eines lokalen NTP-Servers zu Zeitsynchronisation ).

Aufgrund der Komplexität des Netz- und Systemmanagements sowie der hohen Anforderungen an die Verfügbarkeit des Netzes ist darauf zu achten, dass die Administratoren ausreichen geschult sind (siehe M 3.11 *Schulung des Wartungs- und Administrationspersonals*).

**Beschaffung**

Neben dem Management-Konzept und der Auswahl des Netzmanagement-Protokolls gibt es noch weitere Aspekte, die bei der Wahl eines Management-Tools berücksichtigt werden müssen (siehe M 2.145 *Anforderungen an ein Netzmanagement-Tool*, M 2.170 *Anforderungen an ein Systemmanagement-System*, M 2.583 *Geeignete Auswahl eines Netzmanagement-Systems* und M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*).

**Umsetzung**

Beim Aufbau einer neuen Systemlandschaft muss auch ein Management-Tool installiert werden (siehe M 4.497 *Sichere Installation eines Netzmanagement-Systems* und M 4.91 *Sichere Installation eines Systemmanagementsystems*).

In den meisten Fällen dürfte hingegen ein bereits existierendes Netz mit vorhandenen Systemen und ein entsprechendes Netz- und Systemmanagement vorhanden sein. Ein Missbrauch des Management-Tools kann zu Angriffen auf das gemanagte Netz bzw. die darin enhaltenen Systeme führen. Das Management-Tool muss daher gegen unerlaubte lokale Zugriffe sowie Fernzugriffe geschützt werden (siehe M 4.79 *Sichere Zugriffsmechanismen bei lokaler Administration* und M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration*).

**Betrieb**

Für den sicheren Betrieb des Netz- und Systemmanagement-Systems sind einige Grundregeln zu beachten (siehe M 2.146 *Sicherer Betrieb eines Netzmanagement-Systems* und M 4.92 *Sicherer Betrieb eines Systemmanagementsystems*).

Ein besonderer Schwerpunkt liegt außerdem auf der Behandlung von Warn- und Fehlermeldungen (siehe M 2.498 *Behandlung von Warn- und Fehlermeldungen*) und der Protokollierung der Netzaktivitäten (siehe M 4.81 *Audit und Protokollierung der Aktivitäten im Netz*).

**Notfallvorsorge**

Durch die Wichtigkeit der Netze und Systeme für IT-gestützte Prozesse müssen auch für das Netz- und Systemmanagement Notfallpläne für den Fall eines Ausfalls vorgehalten werden (siehe M 6.57 *Erstellen eines Notfallplans für den Ausfall des Managementsystems*). Das Netz und die angeschlossenen Systeme arbeiten zwar auch weiter, falls das Management-System nicht zur Verfügung steht, gerade für den sicheren Betrieb eines Netzes ist aber das Netzmanagement-System essentiell.

Um im Falle eines Ausfall des Netzes schnell reagieren zu können, ist es zwingend erforderlich, die wesentlichen Konfigurationen der Netzelemente gesichert wieder einspielenen zu können (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*).

Nachfolgend wird das Maßnahmenbündel für den Baustein Netz- und Systemmanagement vorgestellt.

**Planung und Konzeption**

- M 2.143 (A) *Entwicklung eines Netzmanagement-Konzeptes*
- M 2.144 (A) *Verwendung von SNMP als Netzmanagement-Protokoll*
- M 2.168 (A) *IT-System-Analyse vor Einführung eines Systemmanagement-Systems*
- M 2.169 (A) *Entwickeln einer Systemmanagementstrategie*
- M 2.581 (B) *Aufbau eines Administrationsnetzes für das Netzmanagement*

- M 2.582 (W) *Möglichkeiten zur Einrichtung eines Managementnetzes*
- M 4.277 (C) *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern*

**Beschaffung**

- M 2.145 (B) *Anforderungen an ein Netzmanagement-Tool*
- M 2.170 (A) *Anforderungen an ein Systemmanagement-System*
- M 2.171 (A) *Geeignete Auswahl eines Systemmanagement-Produktes*
- M 2.583 (C) *Geeignete Auswahl eines Netzmanagement-Systems*

**Umsetzung**

- M 2.498 (C) *Behandlung von Warn- und Fehlermeldungen*
- M 4.91 (A) *Sichere Installation eines Systemmanagementsystems*
- M 4.497 (A) *Sichere Installation eines Netzmanagement-Systems*

**Betrieb**

- M 2.146 (A) *Sicherer Betrieb eines Netzmanagement-Systems*
- M 3.11 (A) *Schulung des Wartungs- und Administrationspersonals*
- M 4.81 (B) *Audit und Protokollierung der Aktivitäten im Netz*
- M 4.92 (A) *Sicherer Betrieb eines Systemmanagementsystems*

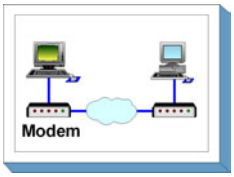
**Aussonderung**

- M 2.584 (A) *Geregelte Außerbetriebnahme eines Netz- und Systemmanagement-Tools*

**Notfallvorsorge**

- M 6.52 (A) *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*
- M 6.57 (C) *Erstellen eines Notfallplans für den Ausfall des Managementsystems*

# B 4.3 Modem




## Beschreibung

Über ein Modem wird eine Datenendeinrichtung, z. B. ein PC, über das öffentliche Telefonnetz mit anderen Datenendeinrichtungen verbunden, um Informationen austauschen zu können. Ein Modem wandelt die digitalen Signale aus der Datenendeinrichtung in analoge elektrische Signale um, die über das Telefonnetz übertragen werden können. Damit zwei IT-Systeme über Modem kommunizieren können, muss auf den IT-Systemen die entsprechende Kommunikationssoftware installiert sein.

Unterschieden werden externe, interne und PCMCIA-Modems. Ein externes Modem ist ein eigenständiges Gerät mit eigener Stromversorgung, das üblicherweise über eine serielle Schnittstelle mit dem IT-System verbunden wird. Als internes Modem werden Steckkarten mit Modem-Funktionalität, die über keine eigene Stromversorgung verfügen, bezeichnet. Ein PCMCIA-Modem ist eine scheckkartengroße Einsteckkarte, die über eine PCMCIA-Schnittstelle üblicherweise in Laptops eingesetzt wird.

In diesem Baustein wird Datenübertragung über ISDN nicht betrachtet, dazu siehe die Bausteine B 3.401 *TK-Anlage* und B 4.5 *LAN-Anbindung eines IT-Systems über ISDN*.

## Gefährdungslage

In diesem Kapitel werden für den IT-Grundschutz beim Einsatz eines Modems folgende Gefährdungen angenommen:

**Menschliche Fehlhandlungen**

- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.5 *Unbeabsichtigte Leitungsbeschädigung*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.12 *Abhören von Telefongesprächen und Datenübertragungen*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.23 *Schadprogramme*
- G 5.25 *Maskerade*
- G 5.39 *Eindringen in Rechnersysteme über Kommunikationskarten*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz eines Modems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Beschaffung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Schon vor dem Einsatz eines Modems sollte geprüft werden, ob die lokalen Gegebenheiten die Installation eines Überspannungsschutzes erforderlich machen. Auch sollte festgelegt werden, wer unter welchen Umständen das Modem benutzen darf.

**Beschaffung**

Die Maßnahme M 2.59 *Auswahl eines geeigneten Modems in der Beschaffung* nennt die wesentlichen Kriterien, die bei der Auswahl eines Modems zu beachten sind.

**Umsetzung**

Vor der Inbetriebnahme ist das Modem geeignet zu konfigurieren, wobei unbedingt darauf zu achten ist, dass eventuell vorhandene, vom Hersteller vorgegebene Passwörter geändert werden. Die Installation eines Modems darf nicht dazu führen, dass hierdurch ein zusätzlicher, ungesicherter Zugang zu einem Rechnernetz, beispielsweise an einer Firewall vorbei, entsteht.

**Betrieb**

Damit nicht durch die Nutzung eines Modems ein zusätzliches Sicherheitsrisiko entsteht, muss für eine sichere Administration und Nutzung gesorgt werden. Dies lässt sich nur dann erreichen, wenn das Personal in diesem Bereich entsprechend geschult wird. Dazu gehört auch, dass sich die Mitarbeiter bewusst sind, dass über eine Modem-Verbindung Viren eingeschleppt werden können und dass sie daher besonders dafür Sorge zu tragen haben, dass alle übertragenen Daten auf Viren geprüft werden.

Um externe Angriffe über die Modem-Verbindung zu erschweren, sollte überlegt werden, ob das Modem so konfiguriert werden kann, dass alle Verbindungen von innen nach außen aufgebaut werden müssen und eingehende Verbindungen über ein Callback-Verfahren durchgeschaltet werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Modem" vorgestellt.

**Planung und Konzeption**
- M 2.42 (A) *Festlegung der möglichen Kommunikationspartner*
- M 2.61 (A) *Regelung des Modem-Einsatzes*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*
- M 5.32 (A) *Sicherer Einsatz von Kommunikationssoftware*

**Beschaffung**
- M 2.59 (Z) *Auswahl eines geeigneten Modems in der Beschaffung*

**Umsetzung**
- M 1.38 (A) *Geeignete Aufstellung eines Modems*
- M 2.46 (A) *Geeignetes Schlüsselmanagement*
- M 2.204 (A) *Verhinderung ungesicherter Netzzugänge*
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 5.30 (W) *Aktivierung einer vorhandenen Callback-Option*
- M 5.31 (A) *Geeignete Modem-Konfiguration*

**Betrieb**
- M 2.60 (A) *Sichere Administration eines Modems*
- M 3.17 (A) *Einweisung des Personals in die Modem-Benutzung*
- M 4.33 (A) *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung*
- M 5.44 (Z) *Einseitiger Verbindungsaufbau*

# B 4.4 VPN

## Beschreibung

Die zunehmende Vernetzung von Rechnern und Rechnerverbünden hat einen Wandel im Kommunikationsverhalten von Behörden und Unternehmen bewirkt. Kommunikationsnetze werden zur Suche nach Informationen eingesetzt, um Aufgaben effizient zu erledigen, vor allem aber zunehmend als universelles Transportmedium für Daten. Mit Hilfe von Virtuellen Privaten Netzen (VPNs) können Sicherheitsmaßnahmen realisiert werden, um schutzbedürftige Daten über nicht-vertrauenswürdige Netze wie dem Internet zu übertragen.

Unter der Bausteinnummer B 4.4 wurde in früheren Fassungen der IT-Grundschutz-Kataloge das Thema "Remote Access" behandelt. Der vorliegende Baustein enthält Empfehlungen zu den Anwendungsfällen Site-to-Site-, End-to-End- oder End-to-Site-VPNs. Die für Remote Access erforderlichen Standard-Sicherheitsmaßnahmen sind unter der Überschrift Remote-Access-VPNs (End-to-Site-VPNs) in diesem Baustein integriert.

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes, wie beispielsweise dem Internet, betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. Die sichere Authentisierung der Kommunikationspartner ist auch dann möglich, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Bei VPNs wird grundsätzlich zwischen folgenden Varianten oder Kombinationen hieraus unterschieden:

- Site-to-Site-VPN: Hierbei werden zwei Computernetze über ein VPN verbunden, beispielsweise um die Außenstellen einer Institution sicher anzubinden.
- End-to-End-VPN: Bei dieser Variante wird zwischen zwei Endgeräten ein VPN aufgebaut. Werden im speziellen zwei Server mit einem VPN verbunden, wird dies auch oft als Host-to-Host-Verbindung bezeichnet.
- End-to-Site-VPN (oder auch Remote-Access-VPN): Hierbei wird zwischen einem Endgerät und einem Netz ein VPN aufgebaut. Diese Variante wird typischerweise eingesetzt, wenn ein mobiler Benutzer von unterwegs mit seinem Laptop über einen VPN-Einwahlknoten auf das LAN seiner Institution zugreifen will. Diese Art des Zugriffs wird auch als Fernzugriff bezeichnet.

Site-to-Site-VPNs dienen zur Vernetzung dezentraler LANs mehrerer Zweigstellen innerhalb eines Unternehmens oder einer Behörde. Mittels eines End-to-End-VPNs können Geschäftspartner oder Kunden auf ein zentrales IT-System einer Institution zugreifen. Bei einem Remote-Access-VPN können sich die Mitarbeiter von extern in das Firmen-LAN bzw. Behörden-LAN einwählen.

## Gefährdungslage

Der vorliegende Baustein behandelt Gefährdungen, die beim Einsatz von VPNs relevant sind. Hierzu zählen organisatorische Mängel, wie beispielsweise eine unzureichende Planung, aber auch menschliche Fehlhandlungen (z. B. durch mangelhafte Administration). Zusätzlich sind VPNs auf Grund der Übertragung von internen Daten über nicht-vertrauenswürdige Netze einer permanenten Gefahr ausgesetzt.

Für den IT-Grundschutz beim VPN-Einsatz werden folgende Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.16 *Ungeordneter Benutzerwechsel bei tragbaren PCs*

- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.24 *Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.128 *Fehlende oder unzureichende Planung des VPN-Einsatzes*
- G 2.129 *Fehlende oder unzureichende Regelungen zum VPN-Einsatz*
- G 2.130 *Ungeeignete Auswahl von VPN-Verschlüsselungsverfahren*
- G 2.131 *Unzureichende Kontrolle von VPNs*

**Menschliche Fehlhandlungen**

- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.40 *Ungeeignete Nutzung von Authentisierungsdiensten bei VPNs*
- G 3.41 *Fehlverhalten bei der Nutzung von VPN-Diensten*
- G 3.42 *Unsichere Konfiguration der VPN-Clients für den Fernzugriff*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.90 *Fehlerhafte Administration von VPNs*
- G 3.91 *Ausfall von VPN-Verbindungen durch Fehlbedienung*

**Technisches Versagen**

- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.57 *Störungen beim Einsatz von VoIP über VPNs*
- G 4.69 *Probleme bei der IPSec-Konfiguration*
- G 4.70 *Unsichere Standard-Einstellungen auf VPN-Komponenten*

**Vorsätzliche Handlungen**

- G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.92 *Nutzung des VPN-Clients als VPN-Server*
- G 5.93 *Erlauben von Fremdnutzung von VPN-Komponenten*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen gemäß den Ergebnissen der Modellierung nach IT-Grundschutz zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden.

Für den erfolgreichen Aufbau eines VPNs sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer Anforderungsanalyse, über Planung, Konzeption und Installation bis hin zum sicheren Betrieb. Besonders wichtig ist die Durchführung einer entsprechenden Notfallplanung, um im Fehlerfall eine rasche Wiederherstellung der Kommunikationsverbindung garantieren zu können.

Nachfolgend werden die erforderlichen Maßnahmen für eine ordnungsgemäße Einführung eines VPNs sowie dessen sicheren Betrieb aufgeführt:

**Planung des Einsatzes von VPNs**

Ist die Entscheidung gefallen, für bestimmte Verbindungen ein VPN einzusetzen, so muss dessen Aufbau geplant und konzipiert werden. Dabei können innerhalb einer Institution verschiedene VPN-Varianten zum Einsatz kommen. Der erste Schritt ist immer die Festlegung der notwendigen Anforderungen an ein solches System (siehe M 2.415 *Durchführung einer VPN-Anforderungsanalyse*). Erst nachdem die Anforderungen klar definiert worden sind, kann damit begonnen werden, ein entsprechendes Konzept (M 2.416 *Planung des VPN-Einsatzes* und M 2.417 *Planung der technischen VPN-Realisierung*) zu erstellen.

Besondere Aufmerksamkeit ist der Definition einer eigenen VPN-Sicherheitsrichtlinie zu widmen, welche auf die allgemeine Leitlinie für Informationssicherheit abgestimmt werden muss. Die dabei zu berücksichtigenden Aspekte sind in M 2.418 *Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung* zusammengefasst.

**Beschaffung**

Die geeignete Auswahl eines VPN-Produktes ist entscheidend dafür, die geplanten Anforderungen entsprechend umsetzen zu können. Bei der Auswahl der VPN-Komponenten sind daher die in M 2.419 *Geeignete Auswahl von VPN-Produkten* gegebenen Empfehlungen zu beachten. Wird ein externer Dienstleister beauftragt, ein VPN bereitzustellen, sind die in M 2.420 *Auswahl eines Trusted-VPN-Dienstleisters* vorgestellten Aspekte zu berücksichtigen.

**Umsetzung**

Nach Abschluss der organisatorischen und planerischen Vorarbeiten kann mit der Installation des VPNs begonnen werden. Dabei ist insbesondere M 4.319 *Sichere Installation von VPN-Endgeräten* zu beachten. Ist die grundlegende Installation erfolgt, so muss das System in einen sicheren Betriebszustand überführt werden, damit anschließend der laufende Betrieb aufgenommen werden kann (siehe M 4.320 *Sichere Konfiguration eines VPNs*). Um die VPN-Endpunkte ausreichend zu schützen, müssen diese gemäß M 4.224 *Integration von VPN-Komponenten in ein Sicherheitsgateway* in die Sicherheitsinfrastruktur eingebunden werden.

**Betrieb**

Auch im laufenden Betrieb muss die Sicherheit des VPNs dauerhaft gewährleistet werden. Die Empfehlungen hierzu sind in der Maßnahme M 4.321 *Sicherer Betrieb eines VPNs* zusammengefasst.

**Aussonderung**

In Vergessenheit geratene VPN-Zugänge oder Zugänge von Partnern, mit denen die Kooperation bereits beendet wurde, stellen unnötige Sicherheitslücken dar und sind schnellstmöglich zu sperren. Hierfür sind die in M 4.322 *Sperrung nicht mehr benötigter VPN-Zugänge* dargestellten Empfehlungen zu beachten.

**Notfallvorsorge**

Abhängig von den Anforderungen an die Verfügbarkeit kann eine Betriebsunterbrechung des VPNs zu mehr oder minder großen Problemen führen. Um dem entgegenzuwirken, muss ein entsprechendes Notfallkonzept erstellt werden. Die hierfür notwendigen Empfehlungen sind in M 6.109 *Notfallplan für den Ausfall eines VPNs* beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Bereich "VPN" vorgestellt.

**Planung und Konzeption**
- M 2.415 (A) *Durchführung einer VPN-Anforderungsanalyse*
- M 2.416 (A) *Planung des VPN-Einsatzes*
- M 2.417 (B) *Planung der technischen VPN-Realisierung*
- M 2.418 (A) *Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung*
- M 3.65 (W) *Einführung in VPN-Grundbegriffe*
- M 4.113 (Z) *Nutzung eines Authentisierungsservers bei Remote-Access-VPNs*
- M 5.76 (Z) *Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation*
- M 5.77 (Z) *Bildung von Teilnetzen*

**Beschaffung**
- M 2.419 (C) *Geeignete Auswahl von VPN-Produkten*
- M 2.420 (C) *Auswahl eines Trusted-VPN-Dienstleisters*

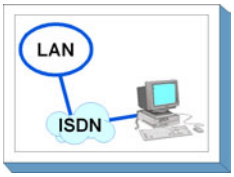
**Umsetzung**
- M 4.224 (Z) *Integration von VPN-Komponenten in ein Sicherheitsgateway*
- M 4.319 (A) *Sichere Installation von VPN-Endgeräten*
- M 4.320 (A) *Sichere Konfiguration eines VPNs*
- M 5.122 (A) *Sicherer Anschluss von Laptops an lokale Netze*
- M 5.148 (C) *Sichere Anbindung eines externen Netzes mit OpenVPN*
- M 5.149 (C) *Sichere Anbindung eines externen Netzes mit IPSec*

**Betrieb**
- M 4.321 (A) *Sicherer Betrieb eines VPNs*

**Aussonderung**
- M 4.322 (B) *Sperrung nicht mehr benötigter VPN-Zugänge*

**Notfallvorsorge**
- M 6.109 (A) *Notfallplan für den Ausfall eines VPNs*

# B 4.5 LAN-Anbindung eines IT-Systems über ISDN




## Beschreibung

ISDN (Integrated Services Digital Network) ist ein digitales Telekommunikationsnetz, über das verschiedene Dienste, wie Telefon und Telefax, genutzt sowie Daten und Bilder übertragen werden können.

In diesem Kapitel wird die Anbindung eines abgesetzten IT-Systems an ein lokales Netz über ein öffentliches ISDN-Netz betrachtet. Hierbei erfolgt die Anbindung auf Seiten des abgesetzten IT-Systems mittels einer ISDN-Adapterkarte mit S0-Schnittstelle. Die Anbindung des LAN wird über einen Router hergestellt, der über eine S2M-Schnittstelle mit einem öffentlichen ISDN-Netz verbunden ist.

Diese Form der Anbindung eines entfernt stehenden IT-Systems kommt typischerweise für die Anbindung von Telearbeitsplätzen in Betracht.

## Gefährdungslage

Für den Grundschutz werden die folgenden Gefährdungen als typisch für die LAN-Anbindung eines IT-Systems über ISDN angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.6 *Unbefugter Zutritt zu schutzbedürftigen Räumen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.24 *Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*

**Technisches Versagen**

- G 4.25 *Nicht getrennte Verbindungen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.14 *Gebührenbetrug*
- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.25 *Maskerade*
- G 5.39 *Eindringen in Rechnersysteme über Kommunikationskarten*
- G 5.48 *IP-Spoofing*
- G 5.61 *Missbrauch von Remote-Zugängen für Managementfunktionen von Routern*
- G 5.63 *Manipulationen über den ISDN-D-Kanal*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

In diesem Kapitel steht die Gewährleistung einer sicheren Kommunikation im Vordergrund. Die für die kommunizierenden IT-Systeme weiterhin erforderlichen Maßnahmen sind den jeweiligen Bausteinen zu entnehmen.

Für die LAN-Anbindung eines IT-Systems über ISDN sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zum laufenden Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Die sichere Nutzung von Fernzugriff auf IT-Systeme erfordert die Beachtung einer Reihe von Maßnahmen zum Schutz der Kommunikation (siehe Maßnahme M 5.32 *Sicherer Einsatz von Kommunikationssoftware*).

**Beschaffung**

Die Maßnahme M 2.106 *Auswahl geeigneter ISDN-Karten in der Beschaffung* nennt eine Reihe wichtiger Kriterien, die bei der Auswahl von ISDN-Karten zu beachten sind.

**Umsetzung**

Bei der Installation des ISDN-Zugangs ist nach der Grundregel zu verfahren, dass alle nicht benötigten Dienste und Funktionalitäten abzuschalten sind, weil sie nur unnötige Risiken mit sich bringen. Die tatsächlich genutzten Funktionen sind durch geeignete Konfiguration so gut wie möglich abzusichern, wozu unbedingt auch die sofortige Änderung eventueller vom Hersteller vorgegebener Passwörter gehört. Die vorgesehene Konfiguration ist zu dokumentieren, und diese Dokumentation ist bei Änderungen zu aktualisieren.

Ein wesentlicher Aspekt bei der Installation eines ISDN-Zugangs ist noch, dass hierdurch die vorhandene Sicherheit eines Rechnernetzes nicht unterlaufen werden darf. Insbesondere darf hierdurch auf keinen Fall eine Verbindung mit externen Netzen entstehen, die ein vorhandenes Firewall-System überbrückt und damit weitestgehend unwirksam macht.

**Betrieb**

Durch regelmäßige Kontrollen der erzeugten Protokolldateien lässt sich ein eventueller Missbrauch der ISDN-Verbindung leichter aufdecken. Eine gelegentliche Kontrolle programmierter Zieladressen und Protokolle hilft zu vermeiden, dass versehentlich Verbindungen mit einem falschen Kommunikationspartner aufgebaut werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich LAN-Anbindung eines IT-Systems über ISDN vorgestellt.

**Planung und Konzeption**
- M 2.42 (A) *Festlegung der möglichen Kommunikationspartner*
- M 2.108 (Z) *Fernwartung der ISDN-Netzkoppelelemente*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*
- M 4.62 (Z) *Einsatz eines D-Kanal-Filters*
- M 5.32 (A) *Sicherer Einsatz von Kommunikationssoftware*
- M 5.47 (Z) *Einrichten einer Closed User Group*

**Beschaffung**
- M 2.106 (C) *Auswahl geeigneter ISDN-Karten in der Beschaffung*

**Umsetzung**
- M 1.43 (A) *Gesicherte Aufstellung aktiver Netzkomponenten*
- M 2.46 (A) *Geeignetes Schlüsselmanagement*

- M 2.107 (A) *Dokumentation der ISDN-Karten-Konfiguration*
- M 2.109 (A) *Rechtevergabe für den Fernzugriff*
- M 2.204 (A) *Verhinderung ungesicherter Netzzugänge*
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.59 (A) *Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten*
- M 4.60 (A) *Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten*
- M 4.61 (A) *Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten*
- M 5.48 (A) *Authentisierung mittels CLIP/COLP*
- M 5.49 (A) *Callback basierend auf CLIP/COLP*
- M 5.50 (A) *Authentisierung mittels PAP/CHAP*

**Betrieb**

- M 5.29 (C) *Gelegentliche Kontrolle programmierter Zieladressen und Protokolle*

# B 4.6 WLAN

## Beschreibung

Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. Mit WLAN werden hier drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

Aufgrund der einfachen Installation werden WLANs auch für temporär zu installierende Netze, wie z. B. auf Messen oder kleineren Veranstaltungen, verwendet. Darüber hinaus besteht die Möglichkeit, an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen Netzzugänge über so genannte Hotspots anzubieten. Dadurch wird den mobilen Benutzern Verbindungen in das Internet oder in ihr Firmennetz ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WLAN-Komponente des mobilen Endgeräts (z. B. über einen WLAN-USB-Stick oder entsprechende WLAN Netzkarte) statt.

Die Mehrzahl der derzeit am Markt verfügbaren WLAN Komponenten basieren auf der 2003 vom IEEE verabschiedeten Erweiterung 802.11g, die eine Übertragungsgeschwindigkeit von bis zu 54 Mbit/s definiert. Darüber hinaus gibt es einige Systeme, die nur die 1999 veröffentlichte Erweiterung IEEE 802.11b unterstützen, mit der bis zu 11 Mbit/s erreicht werden können. Beide Erweiterungen funken dabei im lizenzfreien 2,4 GHz Frequenzbereich.

Die Sicherheitsmechanismen sind im Standard IEEE 802.11 und in der Erweiterung IEEE 802.11i definiert. Im ursprünglichen Standard 802.11 ist Wired Equivalent Privacy (WEP) als Sicherheitsmechanismus definiert, WEP kann jedoch aufgrund mehrerer Schwachstellen nicht mehr als ausreichend sicher eingestuft werden. Aus diesem Grund entwickelte die Hersteller-Vereinigung WiFi-Alliance den Sicherheitsmechanismus Wi-Fi Protected Access (WPA). Hierbei wird neben einer Erweiterung der statischen Schlüssel, den sogenannten Pre-Shared Keys, auch eine dynamische Schlüsselverwaltung mittels TKIP eingeführt. Diese Mechanismen wurden in großen Teilen in die 2004 veröffentlichte offizielle Erweiterung IEEE 802.11i integriert, wobei dort, wie auch bei WPA2, der Advanced Encryption Standard (AES) zur Verschlüsselung verwendet wird, anstelle von RC4 bei WEP und WPA. Weiterhin ist in IEEE 802.11i das Counter Mode with CBC-MAC Protocol (CCMP) als Implementierungsmethode für AES zur Verschlüsselung und Integritätsprüfung definiert. Dieses Verfahren ist langfristig tragbar, erfordert aber im Gegensatz zu der TKIP-Variante neue Hardware. Als Authentisierungsmethode definiert die Erweiterung 802.11i das Extensible Authentication Protocol (EAP) gemäß dem Standard IEEE 802.1X. Weitere technische Hinweise zum sicheren Einsatz von WLAN ist beispielsweise in der Technischen Richtlinie *Sicheres WLAN* des BSI nachzulesen.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zum Einsatz von WLANs innerhalb einer Institution erstellt und wie deren Umsetzung und Einbettung sichergestellt werden kann.

## Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von WLANs folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.17 *Ausfall oder Störung eines Funknetzes*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*

- G 2.117 *Fehlende oder unzureichende Planung des WLAN-Einsatzes*
- G 2.118 *Unzureichende Regelungen zum WLAN-Einsatz*
- G 2.119 *Ungeeignete Auswahl von WLAN-Authentikationsverfahren*
- G 2.120 *Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen*
- G 2.121 *Unzureichende Kontrolle von WLANs*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.84 *Fehlerhafte Konfiguration der WLAN-Infrastruktur*

**Technisches Versagen**

- G 4.60 *Unkontrollierte Ausbreitung der Funkwellen*
- G 4.61 *Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen*

**Vorsätzliche Handlungen**

- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.137 *Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation*
- G 5.138 *Angriffe auf WLAN-Komponenten*
- G 5.139 *Abhören der WLAN-Kommunikation*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz

Im Rahmen des WLAN-Einsatzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Die Absicherung eines WLANs beginnt bereits in der Planungsphase. Nur durch eine durchdachte Strategie (siehe M 2.381 *Festlegung einer Strategie für die WLAN-Nutzung*) und die Auswahl des richtigen WLAN-Standards und den damit verbundenen Kryptoverfahren (siehe M 2.383 *Auswahl eines geeigneten WLAN-Standards* und M 2.384 *Auswahl geeigneter Kryptoverfahren für WLAN*) ist bereits der Grundstein für ein sicheres WLAN gelegt. Die Maßnahme M 3.58 *Einführung in WLAN-Grundbegriffe* hilft dabei, sich in der Begriffswelt für die Absicherung eines WLANs zurechtzufinden.

Alle getroffenen Entscheidungen über Sicherheitseinstellungen, ausgewählten WLAN-Standards, sowie die Regelungen für die Nutzung und Administration des WLANs, sind in einer WLAN-Sicherheitsrichtlinie niederzuschreiben (siehe M 2.382 *Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung*).

**Beschaffung**

Bei der Auswahl der WLAN-Komponenten ist die Maßnahme M 2.385 *Geeignete Auswahl von WLAN-Komponenten* anzuwenden. WLANs unterliegen einem schnellen Wandel bei Standards, Protokollen und Sicherheitsmechanismen. Daher befinden sich WLANs häufig in der Migration.

Für solche Migrationsphasen einzelner WLAN-Komponenten oder ganzer WLAN-Bereiche ist die Maßnahme M 2.386 *Sorgfältige Planung notwendiger WLAN-Migrationsschritte* zu beachten.

**Umsetzung**

Sind alle Komponenten beschafft und geht es um die Einrichtung des WLANs, so ist es nicht unerheblich, an welcher Stelle die Access Points positioniert werden (siehe M 1.63 *Geeignete Aufstellung von Access Points*) oder wie das WLAN mit der eventuell bereits vorhandenen kabelgebundenen Infrastruktur verbunden wird (siehe M 5.139 *Sichere Anbindung eines WLANs an ein LAN*). Aber auch die Konfiguration der unterschiedlichen WLAN-Komponenten, wie Access Points (siehe M 4.294 *Sichere Konfiguration*

*der Access Points*) oder WLAN-Clients (siehe M 4.295 *Sichere Konfiguration der WLAN-Clients*), ist während der Installation stets gemäß der Sicherheitsrichtlinie und der festgelegten Strategie zu erfolgen.

In jedem Fall sind die Benutzer und Administratoren des WLANs ausreichend zu schulen, um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren bei einer unsachgemäßen Verwendung des WLANs hinzuweisen und zu sensibilisieren (siehe M 3.59 *Schulung zum sicheren WLAN-Einsatz*).

Sollte das WLAN durch einen externen Dienstleister installiert, konfiguriert bzw. betreut werden, so ist auf jeden Fall die Maßnahme M 2.387 *Installation, Konfiguration und Betreuung eines WLANs durch Dritte* anzuwenden.

**Betrieb**

Ist das WLAN in Betrieb genommen und wurden alle WLAN-Anwender ausreichend geschult, so ist zum einen durch regelmäßige Audits (siehe M 4.298 *Regelmäßige Audits der WLAN-Komponenten*) sicherzustellen, dass alle getroffenen Sicherheitseinstellungen noch aktuell sind und durch regelmäßig Sicherheitschecks (siehe M 5.141 *Regelmäßige Sicherheitschecks in WLANs*), ob diese Einstellungen auch greifen. Darüber hinaus ist stets ein sicherer Betrieb aller WLAN-Komponenten zu gewährleisten (siehe M 4.297 *Sicherer Betrieb der WLAN-Komponenten*).

Unumgänglich ist ein Schlüsselmanagement für die im WLAN benutzten kryptographischen Schlüssel zur Absicherung der Kommunikation (siehe M 2.388 *Geeignetes WLAN-Schlüsselmanagement*). Eine WLAN-Management-Lösung kann die Verwaltung der Schlüssel erleichtern und das WLAN kann zentral administriert werden (siehe M 4.296 *Einsatz einer geeigneten WLAN-Management-Lösung*).

**Aussonderung**

Werden WLAN-Komponenten außer Betrieb genommen, so sind entsprechende Konfigurationseinstellungen, wie z. B. Netzname oder SSID, wieder auf Standard-Werte zurückzusetzen und eventuell auf der WLAN-Komponente gespeicherte Informationen zur Absicherung des Netzverkehrs über das WLAN oder Zugangsinformationen zu löschen (siehe M 2.390 *Außerbetriebnahme von WLAN-Komponenten*).

**Notfallvorsorge**

Wurden Angriffe auf ein WLAN erkannt, so müssen sowohl die Benutzer, als auch die Administratoren des WLANs wissen, wie sie sich zu verhalten haben (siehe M 6.102 *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*). Hieraus ergibt sich ein Notfallplan, welche Schritte notwendig und welche Personen zu informieren sind, wenn ein Sicherheitsvorfall eintritt. Darüber hinaus kann es notwendig sein, ein redundantes WLAN aufzubauen, um schnell einen Ersatz für wichtige Kommunikationsverbindungen zu schaffen. Dabei ist stets darauf zu achten, dass das redundante WLAN denselben Sicherheitsanforderungen wie das normale WLANs entspricht. Für das redundante WLAN sind daher ebenfalls alle Maßnahmen dieses Bausteins anzuwenden, da es als eigenes WLAN zu betrachten ist. Allgemeine Hinweise zu redundanten Kommunikationsverbindungen stehen in der Maßnahme M 6.75 *Redundante Kommunikationsverbindungen*.

Damit WLANs sicher eingesetzt werden können, müssen auch damit gekoppelte Clients sicher konfiguriert sein und regelmäßig gewartet und administriert werden. Geeignete Sicherheitsempfehlungen für Clients sind in den entsprechenden Bausteinen der IT-Grundschutz-Kataloge beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von WLANs vorgestellt.

**Planung und Konzeption**

- M 2.381 (A) *Festlegung einer Strategie für die WLAN-Nutzung*
- M 2.382 (A) *Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung*
- M 2.383 (A) *Auswahl eines geeigneten WLAN-Standards*
- M 2.384 (A) *Auswahl geeigneter Kryptoverfahren für WLAN*
- M 3.58 (W) *Einführung in WLAN-Grundbegriffe*
- M 5.138 (Z) *Einsatz von RADIUS-Servern*

**Beschaffung**

- M 2.385 (B) *Geeignete Auswahl von WLAN-Komponenten*

- M 2.386 (Z) *Sorgfältige Planung notwendiger WLAN-Migrationsschritte*

**Umsetzung**

- M 1.63 (B) *Geeignete Aufstellung von Access Points*
- M 2.387 (Z) *Installation, Konfiguration und Betreuung eines WLANs durch Dritte*
- M 3.59 (C) *Schulung zum sicheren WLAN-Einsatz*
- M 4.294 (A) *Sichere Konfiguration der Access Points*
- M 4.295 (A) *Sichere Konfiguration der WLAN-Clients*
- M 5.139 (A) *Sichere Anbindung eines WLANs an ein LAN*
- M 5.140 (C) *Aufbau eines Distribution Systems*

**Betrieb**

- M 2.388 (B) *Geeignetes WLAN-Schlüsselmanagement*
- M 2.389 (Z) *Sichere Nutzung von Hotspots*
- M 4.293 (Z) *Sicherer Betrieb von Hotspots*
- M 4.296 (C) *Einsatz einer geeigneten WLAN-Management-Lösung*
- M 4.297 (A) *Sicherer Betrieb der WLAN-Komponenten*
- M 4.298 (B) *Regelmäßige Audits der WLAN-Komponenten*
- M 5.141 (B) *Regelmäßige Sicherheitschecks in WLANs*

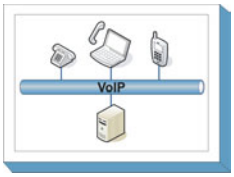
**Aussonderung**

- M 2.390 (C) *Außerbetriebnahme von WLAN-Komponenten*

**Notfallvorsorge**

- M 6.75 (Z) *Redundante Kommunikationsverbindungen*
- M 6.102 (A) *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*

# B 4.7 VoIP




## Beschreibung

Für die Übertragung der Signalisierungsinformationen, zum Beispiel bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten, wie Sprache oder Video, werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils für den Aufbau und die Aufrechterhaltung einer Multimediaverbindung benötigt. Bei einigen Technologien wird nur ein Protokoll sowohl für die Signalisierung als auch den Medientransport benötigt.

Dieser Baustein betrachtet die Sicherheitsaspekte der Endgeräte und Vermittlungseinheiten (Middleware). Die hier beschriebenen Komponenten gleichen hinsichtlich ihrer Funktionalität den im Baustein B 3.401 *TK-Anlage* beschriebenen Telekommunikationsanlagen.

## Gefährdungslage

Auch beim Einsatz von VoIP sind eine Reihe von Gefährdungen zu berücksichtigen. Viele davon lassen sich auf die Datennetze zurückführen, die für VoIP genutzt werden. Hierzu gehören zahlreiche Angriffe auf die Vertraulichkeit, wie beispielsweise Sniffen, und auf die Verfügbarkeit.

Generell gilt, dass die Gefährdungslage der einzelnen Komponenten immer auch vom Einsatzszenario, beispielsweise der Nutzung als Endgerät oder Middleware, abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen.

Für den IT-Grundschutz beim Einsatz von VoIP werden folgende Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.112 *Unzureichende Planung von VoIP*
- G 2.113 *Unzureichende Planung der Netzkapazität beim Einsatz von VoIP*

**Menschliche Fehlhandlungen**

- G 3.7 *Ausfall der TK-Anlage durch Fehlbedienung*
- G 3.82 *Fehlerhafte Konfiguration der VoIP-Middleware*
- G 3.83 *Fehlerhafte Konfiguration von VoIP-Komponenten*

**Technisches Versagen**

- G 4.56 *Ausfall der VoIP-Architektur*
- G 4.57 *Störungen beim Einsatz von VoIP über VPNs*
- G 4.58 *Schwachstellen beim Einsatz von VoIP-Endgeräten*
- G 4.59 *Nicht-Erreichbarkeit bei VoIP durch NAT*

**Vorsätzliche Handlungen**

- G 5.11 *Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten*
- G 5.12 *Abhören von Telefongesprächen und Datenübertragungen*
- G 5.13 *Abhören von Räumen über TK-Endgeräte*
- G 5.14 *Gebührenbetrug*
- G 5.15 *Missbrauch von Leistungsmerkmalen von TK-Anlagen*
- G 5.134 *Fehlende Identifizierung zwischen Gesprächsteilnehmern*
- G 5.135 *SPIT und Vishing*
- G 5.136 *Missbrauch frei zugänglicher Telefonanschlüsse*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Da VoIP über Datennetze betrieben wird, muss der Baustein B 4.1 *Lokale Netze* für eine Sicherheitsbetrachtung hinzugezogen werden. Weiterhin sind die im Datennetz befindlichen aktiven Netzkomponenten zu berücksichtigen. Diese werden im Baustein B 3.302 *Router und Switches* betrachtet.

Statt auf Spezialgeräten, sogenannten Appliances, wird VoIP sehr oft auf gewöhnlichen IT-Systemen betrieben. Für den Betrieb einer Middleware-Komponente wird auf dem IT-System ein entsprechender Netzdienst benötigt. Daher ist in diesem Fall der Baustein B 3.101 *Allgemeiner Server* zu berücksichtigen.

Als *Softphone* wird eine client-seitige Software bezeichnet, die es erlaubt, einen Multimedia-PC mit Mikrofon als Telefonie-Endgerät zu nutzen. Wird ein Softphone verwendet, ist auf den beteiligten Client der Baustein B 3.201 *Allgemeiner Client* anzuwenden. Weiterhin muss sowohl bei der Middleware als auch beim Softphone der Baustein für das Betriebssystem, das auf dem jeweiligen IT-System genutzt wird, berücksichtigt werden, beispielsweise B 3.102 *Server unter Unix* beziehungsweise B 3.209 *Client unter Windows XP*.

Für den Einsatz von VoIP sollten im Hinblick auf die Informationssicherheit folgende Schritte bezüglich der Endgeräte und der Middleware durchlaufen werden:

**Planung des Einsatzes von VoIP**

Der Einsatz von VoIP muss sorgfältig geplant werden (siehe M 2.372 *Planung des VoIP-Einsatzes*). In der Maßnahme M 3.57 *Szenarien für den Einsatz von VoIP* werden mögliche Einsatzbereiche von VoIP vorgestellt. Die Auswahl eines Signalisierungsprotokolls spielt eine wichtige Rolle, weil die verschiedenen Hersteller von VoIP-Geräten oft nur ein Protokoll unterstützen. Da die Signalisierungsprotokolle untereinander nicht kompatibel sind, beeinflusst die Entscheidung für ein Signalisierungsprotokoll die Auswahl der VoIP-Komponenten. In der Maßnahme M 5.133 *Auswahl eines VoIP-Signalisierungsprotokolls* werden die verbreitetsten Protokolle skizziert.

Beim Telefonieren über VoIP können die gleichen Probleme wie bei jeder anderen Kommunikation über IP auftreten. Viele der von IP-Datennetzen bekannten Angriffe auf die Vertraulichkeit und Integrität können direkt für VoIP übernommen werden. Schutz hiergegen bietet unter anderem eine Verschlüsselung der Signalisierungs- oder Medientransportinformationen. Welche Inhalte in welchen Netzen geschützt werden sollten, verdeutlicht die Maßnahme M 2.374 *Umfang der Verschlüsselung von VoIP*. Die Maßnahmen M 5.134 *Sichere Signalisierung bei VoIP* und M 5.135 *Sicherer Medientransport mit SRTP* vertiefen die Funktionsweise der Verschlüsselung für Signalisierungs- und Medientransportinformationen.

Parallel dazu ist die allgemeine Sicherheitsrichtlinie um eine detaillierte Richtlinie für den Einsatz von VoIP zu ergänzen (siehe M 2.373 *Erstellung einer Sicherheitsrichtlinie für VoIP*).

**Beschaffung**

Im nächsten Schritt sollte die Beschaffung der Endgeräte und der VoIP-Middleware erfolgen. Dabei können Softwarelösungen oder Appliances eingesetzt werden. Aufbauend auf die Einsatzszenarien sind die Anforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. In der Maßnahme M 2.375 *Geeignete Auswahl von VoIP-Systemen* sind Empfehlungen für die Auswahl zu finden.

**Umsetzung**

Um auf die Einführung oder den Umstieg auf VoIP vorbereitet zu sein, sollten die Administratoren ausreichend geschult werden (siehe M 3.56 *Schulung der Administratoren für die Nutzung von VoIP*).

Neben VoIP-spezifischen Änderungen muss oft das bestehende IP-Datennetz angepasst werden. In einigen Fällen bietet es sich an, zwei Datennetze parallel zu betreiben. Die nicht immer unproblematische Trennung des VoIP-Sprachnetzes vom restlichen Datennetz, die in M 2.376 *Trennung des Daten- und VoIP-Netzes* beschrieben wird, kann durch logische oder physikalische Segmentierung erfolgen. Daneben sollte auch der Zugriff auf die VoIP-Komponenten abgesichert werden (siehe Maßnahme M 4.289 *Einschränkung der Erreichbarkeit über VoIP*). Falls keine physische Trennung erfolgt, sollten Regelungen für die priorisierte Weiterleitung von VoIP-Paketen getroffen werden, um einer Netzüberla-

stung vorzubeugen. Diese werden unter anderem in der Maßnahme M 5.136 *Dienstgüte und Netzmanagement bei VoIP* vorgestellt.

Besonders für die Erreichbarkeit aus einem öffentlichen Netz müssen Vorkehrungen getroffen werden. Diese betrifft unter anderem die Anpassung des Übergangs zwischen dem öffentlichen und privaten Netz. Beispielsweise kann die Übersetzung von privaten IP-Adressen in öffentliche IP-Adressen über Network Adress Translation (NAT) sehr aufwendig sein (siehe Maßnahme M 5.137 *Einsatz von NAT für VoIP*). Aber auch für den Sicherheitsgateway gelten besondere Voraussetzungen, die in Maßnahme M 4.290 *Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP* beschrieben sind.

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen, siehe M 4.287 *Sichere Administration der VoIP-Middleware* und M 4.288 *Sichere Administration von VoIP-Endgeräten*. Um auf Probleme reagieren zu können, müssen wichtige Ereignisse protokolliert und ausgewertet werden. Empfehlungen hierfür sind in Maßnahme M 4.292 *Protokollierung bei VoIP* zu finden.

Eine Benutzer-Schulung über die Benutzung eines Telefons ist oft nicht wirtschaftlich und sinnvoll, auch wenn typische Büro-Endgeräte heutzutage hochkomplex sind. Dennoch sollten die Anwender über grundlegende Gefährdungen informiert werden, siehe hierzu die Maßnahmen M 3.12 *Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne* und M 3.13 *Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen*.

**Aussonderung**

Sehr oft sind im Speicher der VoIP-Komponenten schutzbedürftige Informationen abgelegt. Bei der Entsorgung der Komponenten sollte die Maßnahme M 2.377 *Sichere Außerbetriebnahme von VoIP-Komponenten* berücksichtigt werden.

**Notfallvorsorge**

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen wieder verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein B 1.4 *Datensicherungskonzept* beschrieben. Darüber hinaus sollte das Datensicherungskonzept um die Datensicherung der VoIP-Komponeten, wie sie in Maßnahme M 6.101 *Datensicherung bei VoIP* beschrieben ist, erweitert werden.

Einige Hinweise zu besonderen Aspekten, die bei der Notfallvorsorge für einen VoIP-Server beachtet werden sollten, sind in Maßnahme M 6.100 *Erstellung eines Notfallplans für den Ausfall von VoIP* beschrieben.

Für den Einsatz von VoIP sind folgende Maßnahmen umzusetzen:

**Planung und Konzeption**
- M 2.28 (Z) *Bereitstellung externer TK-Beratungskapazität*
- M 2.372 (A) *Planung des VoIP-Einsatzes*
- M 2.373 (A) *Erstellung einer Sicherheitsrichtlinie für VoIP*
- M 2.374 (C) *Umfang der Verschlüsselung von VoIP*
- M 3.57 (W) *Szenarien für den Einsatz von VoIP*
- M 5.133 (A) *Auswahl eines VoIP-Signalisierungsprotokolls*
- M 5.134 (C) *Sichere Signalisierung bei VoIP*
- M 5.135 (C) *Sicherer Medientransport mit SRTP*

**Beschaffung**
- M 2.375 (C) *Geeignete Auswahl von VoIP-Systemen*

**Umsetzung**
- M 1.30 (A) *Absicherung der Datenträger mit TK-Gebührendaten*
- M 2.29 (B) *Bedienungsanleitung der TK-Anlage für die Benutzer*
- M 2.376 (C) *Trennung des Daten- und VoIP-Netzes*
- M 3.56 (A) *Schulung der Administratoren für die Nutzung von VoIP*

- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.10 (C) *Schutz der TK-Endgeräte*
- M 4.287 (A) *Sichere Administration der VoIP-Middleware*
- M 4.288 (A) *Sichere Administration von VoIP-Endgeräten*
- M 4.289 (A) *Einschränkung der Erreichbarkeit über VoIP*
- M 4.290 (C) *Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP*
- M 5.136 (B) *Dienstgüte und Netzmanagement bei VoIP*
- M 5.137 (C) *Einsatz von NAT für VoIP*

**Betrieb**

- M 3.12 (B) *Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne*
- M 3.13 (B) *Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen*
- M 4.5 (B) *Protokollierung bei TK-Anlagen*
- M 4.6 (C) *Revision der TK-Anlagenkonfiguration*
- M 4.291 (A) *Sichere Konfiguration der VoIP-Middleware*
- M 4.292 (A) *Protokollierung bei VoIP*

**Aussonderung**

- M 2.377 (B) *Sichere Außerbetriebnahme von VoIP-Komponenten*

**Notfallvorsorge**

- M 6.29 (Z) *TK-Basisanschluss für Notrufe*
- M 6.100 (A) *Erstellung eines Notfallplans für den Ausfall von VoIP*
- M 6.101 (A) *Datensicherung bei VoIP*

# B 4.8 Bluetooth


## Beschreibung

Bluetooth ist ein offener Industriestandard für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking). Die Entwicklung von Bluetooth geht auf eine Initiative der Bluetooth Special Interest Group (Bluetooth SIG) im Jahre 1998 zurück, der eine große Zahl von Herstellern angehört.

Mit Bluetooth können mobile Endgeräte über eine Funkschnittstelle schnell und einfach miteinander verbunden werden. Verschiedene in den Geräten definierte Bluetooth-Profile ermöglichen dann die Übertragung von Daten, Sprachsignalen, Steuerungsinformationen bis hin zur Bereitstellung von Diensten, wie beispielsweise FTP oder Modem- und Netzdiensten. Bluetooth funkt, genauso wie WLAN, im lizenzfreien ISM-Band zwischen 2,402 GHz und 2,480 GHz, hat jedoch nur eine Reichweite von circa 100 m, benötigt aber, im Gegensatz zu Infrarot, keine Sichtverbindung zwischen den einzelnen Endgeräten. Bluetooth wird vornehmlich bei mobilen Endgeräten wie Mobiltelefone, PDAs oder Laptops eingesetzt.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie Bluetooth-fähige Endgeräte einer Institution sicher verwendet werden können.

## Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von Bluetooth folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.17 *Ausfall oder Störung eines Funknetzes*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*

**Technisches Versagen**

- G 4.60 *Unkontrollierte Ausbreitung der Funkwellen*
- G 4.79 *Schwachstellen in der Bluetooth-Implementierung*
- G 4.80 *Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen*

**Vorsätzliche Handlungen**

- G 5.28 *Verhinderung von Diensten*
- G 5.143 *Man-in-the-Middle-Angriff*
- G 5.159 *Erstellung von Bewegungsprofilen unter Bluetooth*
- G 5.160 *Missbrauch der Bluetooth-Profile*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Damit Bluetooth sicher eingesetzt werden kann, müssen auch damit gekoppelte Clients sicher konfiguriert sein. Geeignete Sicherheitsempfehlungen für Clients sind in den Bausteinen der Schicht 3 beschrieben.

Im Rahmen des Bluetooth-Einsatzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Um Bluetooth sicher und effektiv einsetzen zu können, sollte ein Konzept erstellt werden, das auf der Gesamt-Sicherheitsstrategie der Institution sowie den Anforderungen aus den geplanten Einsatzszenarien beruht. Darauf aufbauend ist die Bluetooth-Nutzung in der Behörde bzw. im Unternehmen zu regeln und eine Sicherheitsrichtlinie dafür zu erarbeiten (siehe M 2.461 *Planung des sicheren Bluetooth-Einsatzes*).

**Beschaffung**

Für die Beschaffung von Bluetooth-Komponenten müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden (siehe M 2.462 *Auswahlkriterien für die Beschaffung von Bluetooth-Geräten*).

**Umsetzung**

Je nach Sicherheitsanforderungen müssen die Bluetooth-Komponenten unterschiedlich konfiguriert werden (siehe M 4.362 *Sichere Konfiguration von Bluetooth*). Benutzer und Administratoren sind ausreichend zu schulen, um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren bei einer unsachgemäßen Verwendung von Bluetooth-Komponenten hinzuweisen und zu sensibilisieren (siehe M 3.80 *Sensibilisierung für die Nutzung von Bluetooth*).

**Betrieb**

Bluetooth-Geräte müssen im Betrieb angemessen abgesichert werden (siehe M 4.363 *Sicherer Betrieb von Bluetooth-Geräten*).

**Aussonderung**

Werden Bluetooth-Geräte außer Betrieb genommen, so sind alle sensiblen Informationen wie Zugangsinformationen zu löschen (siehe M 4.364 *Regelungen für die Aussonderung von Bluetooth-Geräten*).

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Bluetooth vorgestellt.

**Planung und Konzeption**
- M 2.461 (A) *Planung des sicheren Bluetooth-Einsatzes*
- M 3.79 (W) *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*

**Beschaffung**
- M 2.462 (Z) *Auswahlkriterien für die Beschaffung von Bluetooth-Geräten*

**Umsetzung**
- M 3.80 (A) *Sensibilisierung für die Nutzung von Bluetooth*
- M 4.362 (A) *Sichere Konfiguration von Bluetooth*

**Betrieb**
- M 2.463 (Z) *Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten*
- M 4.363 (A) *Sicherer Betrieb von Bluetooth-Geräten*

**Aussonderung**
- M 4.364 (A) *Regelungen für die Aussonderung von Bluetooth-Geräten*

# B 5 Anwendungen

# B 5.1 Peer-to-Peer-Dienste


Der Baustein ist 2009 mit der 11. Ergänzungslieferung entfallen.

Der Baustein B 5.1 *Peer-to-Peer-Dienste* befasste sich ursprünglich mit Clients, die sich Ressourcen in einem lokalen Netz gegenseitig zur Verfügung stellen und fokussierte hauptsächlich auf Windows-Clients. Beispiele hierfür waren der Zugriff auf freigegebene Verzeichnisse von Festplatten oder Drucker, die lokal an dem Client ("Peer") angeschlossen sind. Diese Freigaben können oft direkt vom Betriebssystem verwaltet werden, ohne dass zusätzliche Software installiert werden muss.

Mittlerweile hat sich allerdings eine Begriffsverschiebung ergeben. Obwohl in heutigen Betriebssystemen Ressourcen weiterhin mit wenig Aufwand anderen Benutzern im lokalen Netz freigegeben werden können, wird der Begriff "Peer-to-Peer" (oft als "P2P" abgekürzt) meist für den Datenaustausch von Informationen im Internet verwendet. Hierfür werden im Gegensatz zum vorher in diesem Baustein behandelten lokalen Datenaustausch typischerweise keine Betriebssystemfunktionalitäten benutzt, sondern spezielle Applikationen installiert, die entweder über einen Server oder direkt eine Verbindung zu einem anderen Peer aufbauen können, um Informationen auszutauschen. Diese Server und Peers müssen sich nicht im lokalen Netz, sondern können sich auch im Internet befinden. Somit können Informationen auch mit unbekannten Personen ausgetauscht werden. Der Informationsaustausch zwischen IT-Benutzern mit Hilfe von Peer-to-Peer-Diensten im Internet wird oft als "File-Sharing" bezeichnet.

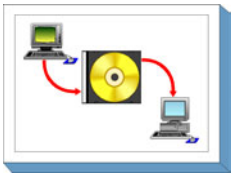
**Aufgrund der damit verbundenen Sicherheitsrisiken sollten Institutionen Peer-to-Peer-Dienste nicht für den Austausch von Informationen im Internet ("File-Sharing") zulassen.**

Der Einsatz von Peer-to-Peer-Diensten kann hingegen in lokalen Netzen (Freigabe von Verzeichnissen und Druckern) in Ausnahmefällen sinnvoll sein. Allerdings ist es in lokalen Netzen zur gemeinsamen Nutzung von Ressourcen die bessere Lösung, hierfür zentrale Server einzusetzen. Damit also mehrere Benutzer auf Speicherfreigaben zugreifen und sich somit Informationen teilen können, sollten in einem LAN statt lokalen Freigaben zentrale Server zur Verfügung gestellt werden. Sollen sich mehrere Benutzer einen Drucker teilen können, sollte dieser über einen Druckserver verwaltet werden.

Vertiefende Informationen zu Peer-to-Peer-Diensten sind in der Gefährdung G 2.147 *Fehlende Zentralisierung durch Peer-to-Peer* und in der Maßnahme M 5.152 *Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste* zu finden.

Die letzte Version des Bausteins, die mit der 10. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 5.2 Datenträgeraustausch



## Beschreibung

Betrachtet wird in diesem Baustein der Austausch von digitalen, aber auch analogen Datenträgern, um Informationen zwischen verschiedenen Kommunikationspartnern und IT-Systemen zu übertragen. Auch bei einer breitbandigen Netzanbindung kann es auch beim elektronischen Datenaustausch aus verschiedenen Gründen sinnvoll oder notwendig sein, hierfür Datenträger zu übermitteln. Ein Grund kann sein, dass es keine oder keine hinreichend vertrauenswürdige Vernetzung zwischen den betroffenen IT-Systemen gibt. Datenträger können bei persönlichen Treffen oder auch per Versand ausgetauscht werden. Typischerweise verwendete Datenträger sind Disketten, Wechselplatten (magnetisch, magneto-optisch), CD-ROMs, DVDs, Magnetbänder, Kassetten und auch Flash-Speicher wie USB-Sticks und USB-Festplatten. Dabei sollte nicht vergessen werden, dass auch Papierdokumente Datenträger sind, für die dieselben Sicherheitsanforderungen zu beachten sind, abhängig vom Schutzbedarf der jeweiligen Informationen.

Daneben wird in diesem Baustein auch die Speicherung der Daten auf dem Sender- und Empfänger-System, soweit es in direktem Zusammenhang mit dem Datenträgeraustausch steht, sowie der Umgang mit den Datenträgern vor bzw. nach dem Transfer berücksichtigt.

## Gefährdungslage

Für den IT-Grundschutz im Rahmen des Austausches von Datenträgern werden folgende typische Gefährdungen angenommen:

### Höhere Gewalt

- G 1.7 *Unzulässige Temperatur und Luftfeuchte*
- G 1.8 *Staub, Verschmutzung*
- G 1.9 *Datenverlust durch starke Magnetfelder*

### Organisatorische Mängel

- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.10 *Nicht fristgerecht verfügbare Datenträger*
- G 2.17 *Mangelhafte Kennzeichnung der Datenträger*
- G 2.18 *Ungeregelte Weitergabe von Datenträgern*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*

### Menschliche Fehlhandlungen

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.12 *Verlust der Datenträger beim Versand*
- G 3.13 *Weitergabe falscher oder interner Informationen*

### Technisches Versagen

- G 4.7 *Defekte Datenträger*

### Vorsätzliche Handlungen

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.23 *Schadprogramme*
- G 5.29 *Unberechtigtes Kopieren der Datenträger*
- G 5.43 *Makro-Viren*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Datenträgeraustausch sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über den täglichen Betrieb bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Im Vorfeld des Datenträgeraustausches ist zu klären und verbindlich festzulegen, mit welchen Kommunikationspartnern ein Austausch stattfinden darf, und in der Datenträgerverwaltung sind die Varianten von Datenträgern festzulegen und zu kennzeichnen, die für den Austausch mit externen Stellen vorzusehen sind. Außerdem ist festzulegen, wie die Datenträger in der eigenen Institution, beim Transport und beim Empfänger zu schützen sind.

**Beschaffung**

Die Auswahl geeigneter Datenträger ist mit den Kommunikationspartnern abzustimmen. Bei der Entscheidung, welche Arten von Datenträgern geeignet sind, kann M 4.169 *Verwendung geeigneter Archivmedien* hilfreich sein.

**Umsetzung**

Um eventuelle Schäden durch unsachgemäße Behandlung der Datenträger beim Transport so gering wie möglich zu halten, sollte eine geeignete Versandart festgelegt werden, die, je nach verwendetem Datenträger (z. B. Schriftstücke, CD-ROM, Magnetband) durchaus unterschiedlich sein kann.

**Betrieb**

Bei der Durchführung des Datenträgeraustauschs ist eine Reihe von Maßnahmen zu beachten, um mögliche Schäden zu vermeiden bzw. in ihren Auswirkungen zu minimieren. Dazu gehören die sichere Aufbewahrung und Verpackung der Datenträger sowie eine eindeutige Kennzeichnung, um die Verwechslungsgefahr zu verringern. Zur allgemeinen Hygiene gehört bei digitalen Datenträgern eine Überprüfung auf Computer-Viren vor dem Versenden oder der Übergabe und ebenfalls nach dem Empfang.

**Aussonderung**

Wenn magnetische Datenträger mit unterschiedlichen Kommunikationspartnern ausgetauscht werden, sollten diese Datenträger vor ihrer erneuten Verwendung physikalisch gelöscht werden, um die Übermittlung von Informationsresten an den falschen Empfänger zu vermeiden.

**Notfallvorsorge**

Da es nie auszuschließen ist, dass Datenträger beim Transport verloren gehen, sollten die übermittelten Daten zumindest so lange noch lokal in einer Kopie vorgehalten werden, bis der korrekte Empfang des Datenträgers bestätigt wurde. Je nach Art und Zweck des Datenträgeraustausches kann auch eine längere Speicherung als Beweismittel für spätere Konflikte erforderlich sein.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datenträgeraustausch" vorgestellt.

**Planung und Konzeption**

- M 2.3 (B) *Datenträgerverwaltung*
- M 2.42 (A) *Festlegung der möglichen Kommunikationspartner*
- M 2.45 (A) *Regelung des Datenträgeraustausches*
- M 2.393 (A) *Regelung des Informationsaustausches*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*

**Umsetzung**

- M 2.46 (A) *Geeignetes Schlüsselmanagement*

- M 4.32 (B) *Physikalisches Löschen der Datenträger vor und nach Verwendung*
- M 4.64 (C) *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*
- M 5.22 (B) *Kompatibilitätsprüfung des Sender- und Empfängersystems*
- M 5.23 (A) *Auswahl einer geeigneten Versandart für Datenträger*

**Betrieb**

- M 1.36 (A) *Sichere Aufbewahrung der Datenträger vor und nach Versand*
- M 2.43 (A) *Ausreichende Kennzeichnung der Datenträger beim Versand*
- M 2.44 (A) *Sichere Verpackung der Datenträger*
- M 3.14 (B) *Einweisung des Personals in den geregelten Ablauf der Informationsweitergabe und des Datenträgeraustausches*
- M 4.33 (A) *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung*
- M 4.35 (Z) *Verifizieren der zu übertragenden Daten vor Versand*

**Notfallvorsorge**

- M 6.38 (A) *Sicherungskopie der übermittelten Daten*

# B 5.3 Groupware


## Beschreibung

Als Groupware werden Anwendungen bezeichnet, die dabei helfen, die in Arbeitsgruppen anfallenden Abläufe und Geschäftsprozesse über IT-Systeme zu unterstützen und zu organisieren. Im Fokus von Groupware liegt die Unterstützung von Arbeitsgruppen bei der Zusammenarbeit, bei der Terminabstimmung, -Koordination sowie bei der täglichen Kommunikation. Unter dem Begriff Groupware-System werden der Groupware-Anwendungsserver, die zugehörigen Groupware-Clients und die erforderlichen Groupware-Dienste zusammengefasst.

Groupware ist unter anderem dazu gedacht, in Institutionen den internen und externen Austausch von Nachrichten, wie z. B. E-Mails, zu ermöglichen, Nachrichten können daher mit Groupware verwaltet, zugestellt, gefiltert und versendet werden. Ebenso werden typische Kommunikationsanwendungen wie Newsgroups, Kalender und Aufgabenlisten sowie Unified Messaging angeboten und von Groupware-Systemen verwaltet.

Der Funktionsumfang von Groupware-Systemen ist sehr unterschiedlich, eine der Grundfunktionen ist im Allgemeinen E-Mail, so dass in diesem Baustein auch allgemeine Sicherheitsanforderungen an E-Mail-Systeme mitbehandelt werden.

Software für Groupware-Systeme wird von vielen Herstellern angeboten. Beispiele hierfür sind Microsoft Exchange und Outlook (siehe B 5.12 *Microsoft Exchange/Outlook* ) und Lotus Notes (B 5.5 *Lotus Notes / Domino*). Daneben gibt es auch zahlreiche andere Groupware-Systeme oder -Komponenten, die auf frei verfügbaren Quellen basieren.

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Groupware-Systemen unabhängig vom eingesetzten Produkt. Dazu gehören auch allgemeine Sicherheitsaspekte eines E-Mail-Systems, Verschlüsselung und Digitale Signatur, Behandlung aktiver Inhalte, Einsatz von Anti-Viren-Software und vieles mehr. Für produktspezifische Sicherheitsaspekte existieren in den IT-Grundschutz-Katalogen weitere Bausteine, die zusätzlich auf das jeweilige Groupware-System anzuwenden sind.

## Gefährdungslage

Für den IT-Grundschutz im Rahmen eines Groupware-Systems werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.54 *Vertraulichkeitsverlust durch Restinformationen*
- G 2.55 *Ungeordnete Groupware-Nutzung*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.13 *Weitergabe falscher oder interner Informationen*

**Technisches Versagen**

- G 4.20 *Überlastung von Informationssystemen*
- G 4.32 *Nichtzustellung einer Nachricht*

- G 4.37 *Mangelnde Verlässlichkeit von Groupware*

**Vorsätzliche Handlungen**

- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.23 *Schadprogramme*
- G 5.24 *Wiedereinspielen von Nachrichten*
- G 5.25 *Maskerade*
- G 5.26 *Analyse des Nachrichtenflusses*
- G 5.27 *Nichtanerkennung einer Nachricht*
- G 5.28 *Verhinderung von Diensten*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.72 *Missbräuchliche Groupware-Nutzung*
- G 5.73 *Vortäuschen eines falschen Absenders*
- G 5.75 *Überlastung durch eingehende E-Mails*
- G 5.77 *Mitlesen von E-Mails*
- G 5.110 *Web-Bugs*
- G 5.111 *Missbrauch aktiver Inhalte in E-Mails*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Sicherheitsmaßnahmen für Groupware betreffen die eingesetzten Clients sowie im eigenen Bereich betriebene Server. Entsprechend müssen die Clients und Server abgesichert werden. Dies ist jedoch nicht Bestandteil dieses Bausteins. Für deren sicheren Betrieb sind die entsprechenden Bausteine der Schicht 3 umzusetzen. Von besonderer Bedeutung sind auch die von den Benutzern einzuhaltenden Sicherheitsvorkehrungen und Anweisungen.

Groupware-Systeme werden in der Regel im Umfeld mit weiteren Systemen eingesetzt, die den Zugriff auf das interne Netz von außen kontrollieren. Hierbei sind insbesondere Sicherheitsgateways und Systeme zur Fernwartung zu nennen, mit denen die Groupware zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der für die Groupware spezifischen Maßnahmen stets auch die entsprechenden Empfehlungen aus den jeweiligen Bausteinen zusätzlich betroffener Systeme zu berücksichtigen. Dazu gehören unter anderem die folgenden Bausteine:

- B 3.301 *Sicherheitsgateway (Firewall)*, sofern Groupware-Systeme in einer Firewall-Umgebung eingesetzt werden.
- B 4.4 *VPN*, wenn der Zugriff auf das Groupware-System über VPN erfolgt.

Für den erfolgreichen Aufbau eines Groupware-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit strategischen Entscheidungen, über Planung, Konzeption und Installation bis zum Betrieb.

**Planung und Konzeption**

Ist die Entscheidung für ein Groupware-System gefallen, muss der Einsatz geplant und konzipiert werden. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 2.454 *Planung des sicheren Einsatzes von Groupware-Systemen* zusammengefasst. Die Sicherheit eines Groupware-Systems kann bereits in der Planungs- und Konzeptionsphase entscheidend beeinflusst werden, indem sicherheitsrelevante Aspekte berücksichtigt werden.

**Umsetzung**

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt worden sind, kann die Installation eines Groupware-Systems erfolgen. Dabei ist die Maßnahme M 4.356 *Sichere Installation von Groupware-Systemen* zu beachten.

Maßnahmen für die spezifische Benutzerschulung finden sich in M 3.74 *Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren* und M 3.75 *Schulung zu Sicherheitsme-*

*chanismen von Groupware-Clients für Benutzer*, da ausreichende Kenntnisse bei Benutzern und Administratoren von Groupware-Systemen die Sicherheit beeinflussen.

Die reine Installation eines Groupware-Systems stellt nur einen geringen Anteil der Arbeiten dar, die in der Umsetzungsphase durchzuführen sind. Der überwiegende Arbeitsaufwand fällt nach der Installation durch die Erstkonfiguration des Groupware-Systems an. Durch die erste Konfiguration werden die Basissicherheit bei der Betriebsaufnahme und die Rahmenbedingungen für die zukünftige Sicherheit des Groupware-Systems festgelegt.

Die sichere Administration muss geplant werden (siehe M 2.456 *Sichere Administration von Groupware-Systemen*).

Groupware-Systeme sind verteilt aufgebaut und kommunizieren über verschiedene Schnittstellen miteinander oder mit anderen externen Client- oder Server-Systemen. Daher ist es wichtig, die Kommunikation angemessen abzusichern. Generell kann ein Groupware-System viele unterschiedliche Kommunikationskanäle nutzen, die auch von den installierten Applikationen und Modulen abhängen. In der Regel werden jedoch einige wenige Basis-Kommunikationsmechanismen und -Schnittstellen genutzt. Die relevante Einstiegsmaßnahme ist M 2.456 *Sichere Administration von Groupware-Systemen*.

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Damit Sicherheitsprobleme zeitnah bemerkt werden, muss das Groupware-System angemessen überwacht werden. Hinweise dazu finden sich in M 4.358 *Protokollierung von Groupware-Systemen*.

Da ein Groupware-System immer Veränderungen unterworfen ist, die sich meist aus veränderten Anforderungen oder Einsatzszenarien ableiten, muss sichergestellt werden, dass das gewünschte Sicherheitsniveau aufrecht erhalten wird (siehe hierzu M 2.221 *Änderungsmanagement* bzw. B 1.14 *Patch- und Änderungsmanagement*).

**Notfallvorsorge**

Parallel zur Betriebsphase muss die Notfallvorsorge sicherstellen, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. Informationssicherheitsmanagement und Revision stellen sicher, dass das Regelwerk auch eingehalten wird. Empfehlungen zur Notfallvorsorge für Groupware-Systeme finden sich in der Maßnahme M 6.140 *Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen*.

Nachfolgend wird das Maßnahmenbündel für Groupware vorgestellt:

**Planung und Konzeption**
- M 2.42 (A) *Festlegung der möglichen Kommunikationspartner*
- M 2.274 (A) *Vertretungsregelungen bei E-Mail-Nutzung*
- M 2.454 (A) *Planung des sicheren Einsatzes von Groupware-Systemen*
- M 2.455 (A) *Festlegung einer Sicherheitsrichtlinie für Groupware*

**Beschaffung**
- M 2.123 (Z) *Auswahl eines Groupware- oder Mailproviders*

**Umsetzung**
- M 2.122 (Z) *Einheitliche E-Mail-Adressen*
- M 2.456 (A) *Sichere Administration von Groupware-Systemen*
- M 3.74 (A) *Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren*
- M 3.75 (C) *Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer*
- M 4.64 (C) *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*
- M 4.355 (A) *Berechtigungsverwaltung für Groupware-Systeme*
- M 4.356 (A) *Sichere Installation von Groupware-Systemen*
- M 5.57 (A) *Sichere Konfiguration der Groupware-/Mail-Clients*

**Betrieb**
- M 3.76 (C) *Einweisung der Benutzer in den Einsatz von Groupware und E-Mail*
- M 4.199 (B) *Vermeidung problematischer Dateiformate*

- M 4.357 (A) *Sicherer Betrieb von Groupware-Systemen*
- M 4.358 (B) *Protokollierung von Groupware-Systemen*
- M 5.54 (B) *Umgang mit unerwünschten E-Mails*
- M 5.56 (A) *Sicherer Betrieb eines Mailservers*
- M 5.108 (Z) *Kryptographische Absicherung von Groupware bzw. E-Mail*
- M 5.109 (Z) *Einsatz eines E-Mail-Scanners auf dem Mailserver*

**Notfallvorsorge**

- M 6.90 (C) *Datensicherung und Archivierung bei Groupware und E-Mail*
- M 6.140 (C) *Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen*

# B 5.4 Webserver


## Beschreibung

Das Internet ist eines der zentralen Medien der heutigen Informationsgesellschaft. Die Informationsangebote im Internet werden von Servern bereitgestellt, die Daten, meist Dokumente in Form von HTML-Seiten, an entsprechende Clientprogramme ausliefern. Dies erfolgt typischerweise über die Protokolle HTTP (*Hypertext Transfer Protocol*) oder HTTPS (*HTTP über SSL* bzw. *TLS*, d. h. HTTP geschützt durch eine verschlüsselte Verbindung). Neben dem Einsatz im Internet werden Webserver auch in zunehmendem Maße für interne Informationen und Anwendungen in Firmennetzen (Intranet) eingesetzt. Ein Grund dafür ist, dass sie eine einfache und standardisierte Schnittstelle zwischen Server-Anwendungen und Benutzern bieten und entsprechende Client-Software (Webbrowser) für praktisch jede Betriebssystemumgebung kostenlos verfügbar ist.

Die Bezeichnung *Webserver* (oder auch *WWW-Server*) wird meist sowohl für das *Programm* benutzt, welches die HTTP-Anfragen beantwortet, als auch für den *Rechner*, auf dem dieses Programm läuft. Bei Webservern sind verschiedene Sicherheitsaspekte zu beachten.

Da ein Webserver ein öffentlich zugängliches System darstellt, sind eine sorgfältige Planung vor dem Aufbau eines Webservers und die sichere Installation und Konfiguration des Systems und seiner Netzumgebung von großer Bedeutung. Das Thema Sicherheit umfasst bei Webservern auch deswegen eine relativ große Anzahl von Gebieten, weil auf einem Webserver meist neben der reinen Webserver-Anwendung noch weitere Serveranwendungen vorhanden sind, die zum Betrieb des Webservers erforderlich sind und deren sicherer Betrieb ebenfalls gewährleistet sein muss. Beispielsweise werden die Daten meist über das Netz (etwa per *FTP* oder *SCP*) auf den Server übertragen oder es wird Zugriff auf eine Datenbank benötigt.

Die Bereitstellung von dynamischen Inhalten und weit über HTML hinaus gehende Funktionen werden durch Webanwendungen realisiert, die nicht Gegenstand dieses Bausteins sind.

## Gefährdungslage

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen als typisch im Zusammenhang mit einem Webserver und der Nutzung des Internets angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.28 *Verstöße gegen das Urheberrecht*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.96 *Veraltete oder falsche Informationen in einem Webangebot*
- G 2.100 *Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.37 *Unproduktive Suchzeiten*
- G 3.38 *Konfigurations- und Bedienungsfehler*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.39 *Software-Konzeptionsfehler*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.28 *Verhinderung von Diensten*
- G 5.48 *IP-Spoofing*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.78 *DNS-Spoofing*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.87 *Web-Spoofing*
- G 5.88 *Missbrauch aktiver Inhalte*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

In diesem Baustein werden die für einen Webserver spezifischen Gefährdungen und Maßnahmen beschrieben. Darüber hinaus muss für die Sicherheit des verwendeten Servers der Baustein B 3.101 *Allgemeiner Server* umgesetzt werden, sowie je nach dem eingesetzten Betriebssystem beispielsweise die Bausteine B 3.102 *Server unter Unix* oder B 3.108 *Windows Server 2003*. Falls das Webangebot Inhalte enthält, die von einer Webanwendung dynamisch aus einer Datenbank erzeugt werden, ist auch der Baustein B 5.7 *Datenbanken* zu berücksichtigen. Insbesondere dann, wenn der Webserver aus dem Internet heraus angesprochen werden kann, sollte auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen* beachtet werden. Werden auf dem Webserver Webanwendungen angeboten, so sind die Maßnahmen des Bausteins B 5.21 *Webanwendungen* umzusetzen.

Für die sichere Anbindung eines Webservers an öffentliche Netze (z. B. das Internet) ist Baustein B 3.301 *Sicherheitsgateway (Firewall)* zu betrachten, ebenso wie für den Zusammenschluss mehrerer Intranets zu einem übergreifenden Intranet. Die kontrollierte Anbindung externer Anschlusspunkte (z. B. von Telearbeitsplätzen via ISDN) wird im Baustein B 5.8 *Telearbeit* behandelt.

Ein Webserver sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann der Webserver alternativ in einem Serverschrank aufgestellt werden (siehe Baustein B 2.7 *Schutzschränke*). Wird der Webserver nicht bei der Organisation selbst, sondern bei einem externen Dienstleister betrieben, so muss Baustein B 1.11 *Outsourcing* betrachtet werden.

Für den erfolgreichen und sicheren Aufbau eines Webservers ist eine Reihe von Maßnahmen umzusetzen. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Bevor ein Webserver eingerichtet wird, sollte in einer Webserver-Sicherheitsstrategie beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind (siehe M 2.173 *Festlegung einer Webserver-Sicherheitsstrategie*).

Ein wichtiger Aspekt der Sicherheit eines Webservers ist bereits relevant, bevor dieser überhaupt existiert: Planung und Organisation des Webangebots. Nur dann, wenn geklärt ist, welche Ziele mit dem Webangebot erreicht werden sollen und welche Inhalte oder Anwendungen zu diesem Zweck angeboten werden, kann durch entsprechende Maßnahmen dafür gesorgt werden, dass Sicherheitsprobleme so weit wie möglich vermieden werden. Der Aspekt der Sicherheit muss daher bereits sehr früh in der Planungsphase berücksichtigt werden, um die entstehende Architektur entsprechend sicher auslegen zu können (siehe M 2.172 *Entwicklung eines Konzeptes für Webangebote* ).

Im Weiterem müssen die Informationen regelmäßig gepflegt und aktualisiert werden. Bei der Betreuung eines Webangebots sind oft mehrere Organisationseinheiten beteiligt, häufig werden die technische

und die inhaltliche Betreuung von verschiedenen Stellen übernommen. Für das möglichst reibungslose Funktionieren des Webangebots müssen daher entsprechende organisatorische Rahmenbedingungen geschaffen werden. Idealerweise sollte eine Redaktion für das Webangebot eingerichtet werden (M 2.272 *Einrichtung eines Internet-Redaktionsteams*).

Bei der Planung und Konzeption, wie die Informationen auf den Webserver bereitgestellt werden sollen, sollten aktive Inhalte vermieden werden (siehe M 4.360 *Sichere Konfiguration eines Webservers*).

**Beschaffung**

Ein Webserver kann auch über einen Dienstleister betrieben werden. Basierend auf der Webserver-Sicherheitsstrategie und den daraus resultierenden Anforderungen muss ein geeigneter Anbieter ausgewählt werden (siehe M 2.176 *Geeignete Auswahl eines Internet Service Providers*).

**Umsetzung**

Nachdem die Planung abgeschlossen und die Webserver-Applikation auf dem Betriebssystem des Servers installiert ist, muss der Web-Server sicher eingerichtet (siehe M 2.175 *Aufbau eines Webservers*) und konfiguriert (siehe M 4.360 *Sichere Konfiguration eines Webservers*) werden. Die Dateien und Verzeichnisse auf einem Webserver müssen gegen unbefugte Veränderungen, aber eventuell auch gegen unbefugten lesenden Zugriff geschützt werden (siehe M 4.94 *Schutz der Webserver-Dateien*).

**Betrieb**

Nachdem der Webserver installiert und konfiguriert wurde, wird der Regelbetrieb aufgenommen. Durch die M 2.174 *Sicherer Betrieb eines Webservers* soll sichergestellt werden, dass die relevanten Systeme des Informationsverbundes auf einem aktuellen Sicherheitsstand gehalten werden. Hierzu muss der Webserver regelmäßig aktualisiert (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*) und die Updates müssen auf Manipulationen untersucht werden (siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

**Notfallvorsorge**

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen wieder verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein B 1.4 *Datensicherungskonzept* beschrieben.

Im Rahmen der Notfallvorsorge ist ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind. Hierfür muss ein Notfallplan für den Webserver erstellt werden (siehe M 6.88 *Erstellen eines Notfallplans für den Webserver*). Ergänzend hierzu sollten die Maßnahmen des Baustein B 1.3 *Notfallmanagement* berücksichtigt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "*Webserver*" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier aus Redundanzgründen verzichtet.

**Planung und Konzeption**

- M 2.172 (A) *Entwicklung eines Konzeptes für Webangebote*
- M 2.173 (A) *Festlegung einer Webserver-Sicherheitsstrategie*
- M 2.272 (Z) *Einrichtung eines Internet-Redaktionsteams*
- M 2.298 (B) *Verwaltung von Internet-Domainnamen*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*
- M 4.176 (B) *Auswahl einer Authentisierungsmethode für Webangebote*
- M 4.359 (W) *Überblick über Komponenten eines Webservers*
- M 5.64 (Z) *Secure Shell*
- M 5.159 (W) *Übersicht über Protokolle und Kommunikationsstandards für Webserver*
- M 5.160 (W) *Authentisierung gegenüber Webservern*
- M 5.177 (B) *Serverseitige Verwendung von SSL/TLS*

**Beschaffung**
- M 2.176 (Z) *Geeignete Auswahl eines Internet Service Providers*

**Umsetzung**
- M 2.175 (A) *Aufbau eines Webservers*
- M 4.64 (C) *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*
- M 4.94 (A) *Schutz der Webserver-Dateien*
- M 4.95 (A) *Minimales Betriebssystem*
- M 4.96 (Z) *Abschaltung von DNS*
- M 4.98 (A) *Kommunikation durch Paketfilter auf Minimum beschränken*
- M 4.360 (B) *Sichere Konfiguration eines Webservers*
- M 5.161 (W) *Erstellung von dynamischen Web-Angeboten*

**Betrieb**
- M 2.174 (A) *Sicherer Betrieb eines Webservers*
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 4.33 (A) *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.177 (B) *Sicherstellung der Integrität und Authentizität von Softwarepaketen*
- M 5.59 (A) *Schutz vor DNS-Spoofing bei Authentisierungsmechanismen*

**Notfallvorsorge**
- M 6.88 (B) *Erstellen eines Notfallplans für den Webserver*

# B 5.5 Lotus Notes / Domino

## Beschreibung

Lotus Notes wird als Groupware-Plattform oder auch als Collaboration-Plattform beschrieben. Hinter diesen Begriffen verbirgt sich eine zunehmend komplexere Software, die Kommunikation, Zusammenarbeit und Informationsmanagement als Schwerpunkte hat. Der Umfang erstreckt sich hierbei von der Ebene von Arbeitsgruppen oder Projekten bis hin zu institutionsübergreifenden Dimensionen.

Der vorliegende Baustein betrachtet die Kernprodukte der Lotus-Produktpalette: den Lotus Domino Server und die diversen Lotus Notes Clients. Im Fokus des Bausteins liegen die Releases 8.0.x und 8.5.x, wobei viele Betrachtungen auch für frühere Releasestände anwendbar sind.

Neben einer angemessenen Absicherung der für den Betrieb der Lotus Notes/Domino-Plattform benötigten Infrastruktur (Räumlichkeiten, spezielle Infrastruktur für die Server, Hardware, Netzkomponenten) müssen auch die unterhalb der Domino- und Notes-Komponenten eingesetzten Betriebssysteme gemäß IT-Grundschutz abgesichert werden.

Werden weitere Komponenten für den Betrieb der Lotus Notes/Domino-Plattform verwendet, wie z. B. DB2-Datenbanken, so ist dies in der Modellierung des Informationsverbundes zu berücksichtigen und es sind die entsprechenden IT-Grundschutz-Bausteine (in diesem Fall der Baustein B 5.7 *Datenbanken*) anzuwenden.

## Gefährdungslage

Für den IT-Grundschutz von Lotus Notes/Domino werden die folgenden typischen Gefährdungen angenommen:

### Organisatorische Mängel

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.28 *Verstöße gegen das Urheberrecht*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.38 *Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen*
- G 2.40 *Mangelhafte Konzeption des Datenbankzugriffs*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*

### Menschliche Fehlhandlungen

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*
- G 3.46 *Fehlerhafte Konfiguration eines Lotus Domino Servers*
- G 3.80 *Fehler bei der Synchronisation von Datenbanken*
- G 3.113 *Fehlerhafte Konfiguration eines Lotus Notes Clients oder eines Fremdclients mit Zugriff auf Lotus Domino*

### Technisches Versagen

- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.26 *Ausfall einer Datenbank*
- G 4.28 *Verlust von Daten einer Datenbank*

- G 4.30 *Verlust der Datenbankintegrität/-konsistenz*
- G 4.32 *Nichtzustellung einer Nachricht*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.47 *Veralten von Kryptoverfahren*
- G 4.52 *Datenverlust bei mobilem Einsatz*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.8 *Manipulation von Leitungen*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*
- G 5.27 *Nichtanerkennung einer Nachricht*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.84 *Gefälschte Zertifikate*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.90 *Manipulation von Adressbüchern und Verteillisten*
- G 5.100 *Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes/Domino*
- G 5.101 *Hacking Lotus Notes/Domino*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine gemäß den Ergebnissen der Modellierung nach IT-Grundschutz umgesetzt werden.

Für einen sicheren Betrieb von Lotus Notes/Domino müssen zunächst die Bausteine für die eingesetzte IT-Infrastruktur einschließlich der Betriebssysteme, Bausteine für eingesetzte Sicherheitskomponenten wie B 3.301 *Sicherheitsgateway (Firewall)* und B 1.6 *Schutz vor Schadprogrammen* umgesetzt werden. Vor allem ist aber zusätzlich der Baustein B 5.3 *Groupware* anzuwenden, der allgemeine Empfehlungen für die generelle Absicherung von Groupware-Systemen enthält.

In dem vorliegenden Baustein werden nicht alle technischen Optionen der Lotus Notes/Domino-Plattform im Detail betrachtet, um den Rahmen des IT-Grundschutzes nicht zu sprengen. Beispielsweise wird das Clustering auf Anwendungsebene, das bei hohem und sehr hohem Schutzbedarf bezüglich Verfügbarkeit als Maßnahme zur Sicherstellung der Verfügbarkeit eingesetzt werden kann, nicht im Detail behandelt.

Für den erfolgreichen Aufbau eines Notes-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation, den Betrieb bis zur Aussonderung des Systems. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Als Einstieg empfiehlt es sich, zunächst die Maßnahme M 3.87 *Einführung in Lotus Notes/Domino* zu betrachten, die einen Überblick über den Aufbau und Begrifflichkeiten eines Notes-Systems bietet.

Ist die Entscheidung für ein Notes-System gefallen, muss der Einsatz des Notes-Systems geplant und konzipiert werden. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* zusammengefasst. Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*), die einerseits die bereits bestehenden Sicherheitsrichtlinien im Kontext von Lotus Notes umsetzt und andererseits Notes-spezifische Erweiterungen definiert.

Die in der IT der Institution eingesetzten Sicherheitskomponenten sind zu berücksichtigen und in die Konzeption einzubringen. Hinweise zum Zusammenspiel einer Lotus Notes/Domino-Umgebung mit vor-

handenen Sicherheitskomponenten finden sich in der Maßnahme M 2.492 *Integration der Lotus Notes/Domino-Umgebung in die vorhandene Sicherheitsinfrastruktur*.

**Beschaffung**

Nach Abschluss der konzeptionellen Planungsarbeiten und der Definition der Beschaffungskriterien für ein Notes-System sollte in Abhängigkeit der Anzahl der ausgewählten Komponenten (siehe M 2.494 *Geeignete Auswahl von Komponenten für die Infrastruktur einer Lotus Notes/Domino-Umgebung*) ein geeignetes Lizenzmodell ausgewählt werden. Die Maßnahme M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino* bietet hierbei Unterstützung.

**Umsetzung**

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation des Notes-Systems erfolgen. Die Installation kann erst dann als abgeschlossen betrachtet werden, wenn die Notes-Systeme in einen sicheren Zustand gebracht wurden (siehe M 4.116 *Sichere Installation von Lotus Notes/Domino*). In der folgenden Konfigurationsphase ist die Maßnahme M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* zu beachten.

**Betrieb**

Ein Notes-System ist in der Regel ständigen Veränderungen unterworfen. Daher müssen sicherheitsrelevante Konfigurationsparameter kontinuierlich angepasst werden. Daneben hängt die Sicherheit in einem Client-Server-basierten System auch von der Sicherheit aller Teilsysteme ab.

Allgemeine Empfehlungen zum Betrieb (inklusive Anwendungsentwicklung und Anwendungsintegration mit Lotus Notes/Domino) sind in M 4.128 *Sicherer Betrieb der Lotus Notes/Domino-Umgebung* enthalten. Um rechtzeitig bei aufkommenden Problemen reagieren zu können, sollten die Maßnahmen M 4.132 *Überwachung der Lotus Notes/Domino-Umgebung* und M 4.427 *Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino* berücksichtigt werden.

**Aussonderung**

Wird entschieden, eine Lotus Notes/Domino-Umgebung nicht weiter zu betreiben, müssen alle wichtigen Informationen auf das Nachfolgesystem portiert werden und anschließend die verbliebenen Daten sicher gelöscht werden. Aber auch wenn nur Teile einer Lotus Notes/Domino-Umgebung auszusondern sind, sind einige Punkte zu beachten, die in M 2.495 *Aussonderung von Lotus Notes/Domino-Komponenten* näher dargestellt sind.

**Notfallvorsorge**

Neben dem normalen Betrieb einer Lotus Notes/Domino-Umgebung ist auch der Notbetrieb zu berücksichtigen und durch die Verantwortlichen eine entsprechende Notfallplanung zu erstellen (siehe M 6.73 *Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Lotus Notes/Domino" vorgestellt:

**Planung und Konzeption**
- M 2.206 (A) *Planung des Einsatzes von Lotus Notes/Domino*
- M 2.207 (A) *Sicherheitskonzeption für Lotus Notes/Domino*
- M 2.492 (B) *Integration der Lotus Notes/Domino-Umgebung in die vorhandene Sicherheitsinfrastruktur*
- M 3.87 (W) *Einführung in Lotus Notes/Domino*

**Beschaffung**
- M 2.493 (Z) *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*
- M 2.494 (B) *Geeignete Auswahl von Komponenten für die Infrastruktur einer Lotus Notes/Domino-Umgebung*

**Umsetzung**
- M 3.88 (B) *Zielgruppenspezifische Schulungen zu Lotus Notes/Domino*

- M 4.116 (A) *Sichere Installation von Lotus Notes/Domino*
- M 4.429 (A) *Sichere Konfiguration von Lotus Notes/Domino*

**Betrieb**

- M 4.128 (A) *Sicherer Betrieb der Lotus Notes/Domino-Umgebung*
- M 4.132 (C) *Überwachung der Lotus Notes/Domino-Umgebung*
- M 4.426 (C) *Archivierung für die Lotus Notes/Domino-Umgebung*
- M 4.427 (C) *Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino*
- M 4.428 (C) *Audit der Lotus Notes/Domino-Umgebung*

**Aussonderung**

- M 2.495 (C) *Aussonderung von Lotus Notes/Domino-Komponenten*

**Notfallvorsorge**

- M 6.73 (B) *Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung*

# B 5.6 Faxserver


## Beschreibung

Betrachtet wird die Informationsübermittlung in Form eines Fax. Für die Maßnahmenauswahl im Bereich IT-Grundschutz wird nicht nach dem verwendeten Übertragungsstandard (z. B. CCITT Gruppe 3) unterschieden. In diesem Baustein werden als technische Basis des Fax-Verkehrs ausschließlich Faxserver betrachtet. Ein Faxserver in diesem Sinne ist eine Applikation, die auf einem IT-System installiert ist und in einem Netz für andere IT-Systeme die Dienste Faxversand und/oder Faxempfang zur Verfügung stellt.

Faxserver werden in der Regel in bereits bestehende E-Mailsysteme integriert. So ist es u. a. möglich, dass eingehende Fax-Dokumente durch den Faxserver per E-Mail an den Benutzer zugestellt werden. Abzusendende Dokumente werden entweder über eine Druckerwarteschlange oder per E-Mail an den Faxserver übergeben. Durch die Integration des Faxservers in ein E-Mail-System ist es auch möglich, "Serienbriefe" wahlweise per Fax und per E-Mail zu versenden. Sofern ein Adressat über einen E-Mail-Zugang verfügt, erhält er die Nachricht kostengünstig per E-Mail, ansonsten per Fax. Das von einem Faxserver gesendete oder empfangene Dokument ist eine Grafik-Datei, die nicht unmittelbar in Textverarbeitungssystemen weiterverarbeitet werden kann. Möglich ist aber auf jeden Fall die Archivierung. Dies kann durch die Faxserver-Software oder auch in Dokumentenmanagementsystemen erfolgen.

Faxserver gibt es für eine Reihe von Betriebssystemen wie z. B. für verschiedene Unix-Derivate, Microsoft Windows und Novell Netware. Überlegungen zu Gefährdungen und Maßnahmen, die durch das jeweils verwendete Betriebssystem bedingt werden, sind nicht Gegenstand dieses Bausteins. Vielmehr sind hierzu der Baustein B 3.101 *Allgemeiner Server* und der jeweilige betriebssystemspezifische Baustein zu bearbeiten.

Faxserver verfügen häufig zusätzlich über den Binary-Transfer-Mode. Hiermit werden beliebige Daten, die nicht im Fax-Format vorliegen, übertragen. Es handelt sich dabei nicht um Faxübertragungen. Daher werden spezielle Gefährdungen und Maßnahmen, die diesen Dienst betreffen, nicht in diesem Baustein betrachtet. Wird der Binary-Transfer-Mode zugelassen, so ist zusätzlich der Baustein B 4.3 *Modem* zu bearbeiten.

## Gefährdungslage

Für den IT-Grundschutz werden bei der Informationsübermittlung per Fax mittels eines Faxservers folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.63 *Ungeordnete Faxnutzung*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.14 *Fehleinschätzung der Rechtsverbindlichkeit eines Fax*

**Technisches Versagen**

- G 4.15 *Fehlerhafte Faxübertragung*
- G 4.20 *Überlastung von Informationssystemen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.24 *Wiedereinspielen von Nachrichten*

- G 5.25 *Maskerade*
- G 5.27 *Nichtanerkennung einer Nachricht*
- G 5.30 *Unbefugte Nutzung eines Faxgerätes oder eines Faxservers*
- G 5.31 *Unbefugtes Lesen von Faxsendungen*
- G 5.32 *Auswertung von Restinformationen in Faxgeräten und Faxservern*
- G 5.33 *Vortäuschen eines falschen Absenders bei Faxsendungen*
- G 5.35 *Überlastung durch Faxsendungen*
- G 5.39 *Eindringen in Rechnersysteme über Kommunikationskarten*
- G 5.90 *Manipulation von Adressbüchern und Verteillisten*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Zunächst sollte eine übergreifende Sicherheitsleitlinie für den Faxserver erarbeitet werden (siehe M 2.178 *Erstellung einer Sicherheitsleitlinie für die Faxnutzung*) und ein geeigneter Faxserver beschafft werden (siehe M 2.181 *Auswahl eines geeigneten Faxservers*). Hieraus müssen Regelungen abgeleitet werden. Schließlich sind Verantwortliche für den Einsatz des Faxservers zu benennen (siehe M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* und M 2.180 *Einrichten einer Fax-Poststelle*). Sowohl die Sicherheitsleitlinie als auch die daraus folgenden Regelungen und die Benennung von Verantwortlichen sollte schriftlich erfolgen. Die dort erarbeiteten Festlegungen sollten sodann in konkrete Sicherheitsmaßnahmen umgesetzt werden. Neben dem sicheren Betrieb des Faxservers ist von besonderer Bedeutung, dass von den Benutzern die entsprechenden Sicherheitsvorkehrungen und Anweisungen eingehalten werden.

Nachfolgend wird das Maßnahmenbündel für die Applikation "Faxserver" vorgestellt:

**Planung und Konzeption**
- M 2.178 (A) *Erstellung einer Sicherheitsleitlinie für die Faxnutzung*
- M 2.179 (A) *Regelungen für den Faxserver-Einsatz*

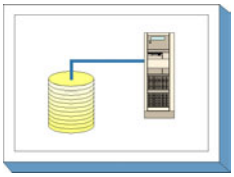
**Beschaffung**
- M 2.181 (C) *Auswahl eines geeigneten Faxservers*

**Umsetzung**
- M 2.180 (A) *Einrichten einer Fax-Poststelle*
- M 3.10 (A) *Auswahl eines vertrauenswürdigen Administrators und Vertreters*
- M 3.15 (A) *Informationen für alle Mitarbeiter über die Faxnutzung*
- M 4.36 (Z) *Sperren bestimmter Faxempfänger-Rufnummern*
- M 4.37 (Z) *Sperren bestimmter Absender-Faxnummern*

**Betrieb**
- M 5.24 (Z) *Nutzung eines geeigneten Faxvorblattes*
- M 5.25 (A) *Nutzung von Sende- und Empfangsprotokollen*
- M 5.26 (Z) *Telefonische Ankündigung einer Faxsendung*
- M 5.27 (Z) *Telefonische Rückversicherung über korrekten Faxempfang*
- M 5.28 (Z) *Telefonische Rückversicherung über korrekten Faxabsender*
- M 5.73 (A) *Sicherer Betrieb eines Faxservers*
- M 5.74 (A) *Pflege der Faxserver-Adressbücher und der Verteillisten*
- M 5.75 (Z) *Schutz vor Überlastung des Faxservers*

**Notfallvorsorge**
- M 6.69 (B) *Notfallvorsorge und Ausfallsicherheit bei Faxservern*

# B 5.7 Datenbanken



## Beschreibung

Datenbanksysteme (DBS) sind ein weithin genutztes Hilfsmittel zur rechnergestützten Organisation, Erzeugung, Veränderung und Verwaltung großer Datensammlungen und stellen in vielen Unternehmen und Organisationen die zentrale Informationsbasis zu ihrer Aufgabenerfüllung bereit. Ein DBS besteht aus dem so genannten Datenbankmanagement-System (DBMS) und einer oder mehrerer Datenbanken.

Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die persistent im DBS abgelegt werden.

Das DBMS bildet die Schnittstelle zwischen den Datenbanken und dient den Benutzern zur Daten-Verwaltung und Veränderung. Die zentralen Aufgaben eines DBMS sind im Wesentlichen die Bereitstellung verschiedener Sichten auf die Daten (Views), die Konsistenzprüfung der Daten (Integritätssicherung), die Autorisationsprüfung, die Behandlung gleichzeitiger Zugriffe verschiedener Benutzer (Synchronisation) und das Bereitstellen einer Datensicherungsmöglichkeit, um im Falle eines Systemausfalls zeitnah Daten wiederherstellen zu können.

Moderne Datenbanksysteme sind überwiegend Bestandteil einer 3-Tier-Architektur. Als Erweiterung der 2-Tier-Architektur (Client-/Server-Architektur) wird hier zwischen Client und Server als dritte Ebene ein Applikationsserver zur Bereitstellung der Datenbank-Anwendungen eingeführt. Durch diese Architektur kann eine Kosteneinsparung aufgrund einer verringerten Client-Ausstattung und einer vereinfachten Datenbankadministration insbesondere bei der Software-Verteilung erreicht werden. Den Anwendern können auf diese Art mit geringem Aufwand neue Software-Versionen zur Verfügung gestellt werden, die durch den Anwender automatisch vom Datenbanksystem über den Applikations-Server bezogen werden.

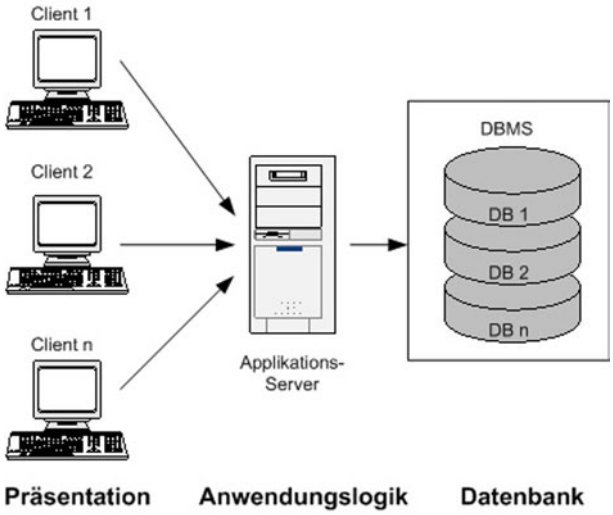



Abbildung: 3-Tier-Architektur eines DBMS

Ein Datenbanksystem muss die parallele Verarbeitung verschiedener Benutzeraufträge (so genannte Transaktionen) ermöglichen. Wesentlich dafür ist die Einhaltung der folgenden vier Eigenschaften, die unter dem ACID-Prinzip bekannt sind:

- Atomarität (**A**tomicity)
  Eine Transaktion ist die kleinste, nicht mehr zerlegbare Einheit von Verarbeitungsschritten und wird nur vollständig oder gar nicht ausgeführt. Sollte es bei der Ausführung zu einem Fehler bzw. Abbruch kommen, werden alle innerhalb der Transaktion bereits getätigten Änderungen an der Datenbank wieder zurückgenommen.

- Konsistenz (**C**onsistency)
  Eine Transaktion überführt eine Datenbank immer von einem konsistenten Zustand in einen anderen konsistenten Zustand, d.h. alle Integritätsbedingungen der Datenbank werden eingehalten.
- Isolation (**I**solation)
  Jede Transaktion läuft isoliert und in jeder Hinsicht unabhängig von anderen Transaktionen ab. Dazu gehört auch, dass jeder Transaktion nur diejenigen Daten aus der Datenbank zur Verfügung gestellt werden, die Teil eines konsistenten Zustands sind. Sollten parallele Transaktionen um Ressourcen konkurrieren, so müssen die Transaktionen serialisiert werden.
- Persistenz (**D**urability)
  Die Ergebnisse einer erfolgreich beendeten Transaktion bleiben in der Datenbank persistent.

Datenbanksysteme sind Standardsoftware und werden von den unterschiedlichsten Herstellern auf dem Markt angeboten. Soll eine Datenbank zur Verarbeitung von Daten eingesetzt werden, so ist im ersten Schritt ein geeignetes DBS auszuwählen. Die zugehörigen Gefährdungen und Maßnahmen aus dem Baustein B 1.10 *Standardsoftware* sind deshalb zu beachten.

Datenbanken können nicht losgelöst von der Umgebung betrachtet werden, in der sie eingesetzt werden. Ein Einzelplatz-PC ist ebenso denkbar wie ein Großrechnerumfeld oder vernetzte Unix- bzw. Windows-Systeme. Dementsprechend sind in Abhängigkeit des Einsatzumfeldes die Bausteine der entsprechenden Schichten 3 bis 5 zu berücksichtigen.

## Gefährdungslage

Neben den grundlegenden Gefährdungen, die prinzipiell für IT-Systeme gelten, existieren Gefährdungen, die speziell die Verfügbarkeit von Datenbanken sowie die Vertraulichkeit oder die Integrität der gespeicherten Daten bedrohen.

Generell steht die Gefährdungslage in Abhängigkeit vom Einsatzszenario und berechtigten Benutzerkreis. Beispielsweise ergibt sich eine erhöhte Gefährdungslage, wenn, anders als gegenüber identifizierbaren Benutzerkreisen innerhalb einer Behörde oder eines Unternehmens, Zugriffe anonymer Benutzern (z. B. Internet-Zugriffe) erlaubt werden.

Eine weiterer Aspekt ergibt sich aus der steigenden Komplexität des DBMS, der sich unter anderem auch in örtlich weit voneinander getrennter Datenhaltung begründet und den damit einhergehenden Anforderungen an sichere Kommunikationswege und konsistente Daten-Synchronisation.

Für den IT-Grundschutz von Datenbanken werden die folgenden Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.38 *Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen*
- G 2.39 *Mangelhafte Konzeption eines DBMS*
- G 2.40 *Mangelhafte Konzeption des Datenbankzugriffs*
- G 2.41 *Mangelhafte Organisation des Wechsels von Datenbank-Benutzern*
- G 2.57 *Nicht ausreichende Speichermedien für den Notfall*
- G 2.110 *Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken*

**Menschliche Fehlhandlungen**

- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.23 *Fehlerhafte Administration eines DBMS*
- G 3.24 *Unbeabsichtigte Datenmanipulation*
- G 3.80 *Fehler bei der Synchronisation von Datenbanken*

**Technisches Versagen**

- G 4.26 *Ausfall einer Datenbank*
- G 4.27 *Unterlaufen von Zugriffskontrollen über ODBC*
- G 4.28 *Verlust von Daten einer Datenbank*
- G 4.30 *Verlust der Datenbankintegrität/-konsistenz*

**Vorsätzliche Handlungen**

- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.64 *Manipulation an Daten oder Software bei Datenbanksystemen*
- G 5.65 *Verhinderung der Dienste eines Datenbanksystems*
- G 5.131 *SQL-Injection*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Als zentraler Informationsspeicher einer Behörde oder eines Unternehmens empfiehlt es sich, den Datenbank-Server in einem separaten Serverraum aufzustellen oder in einem zentralen Rechenzentrum unterzubringen. Zu realisierende Maßnahmen sind in den Bausteinen B 2.4 *Serverraum* und B 2.9 *Rechenzentrum* beschrieben.

Wird der Datenbank-Server in einem Schutzschrank aufgestellt, ist der Baustein B 2.7 *Schutzschränke* bei der Maßnahmenumsetzung zu berücksichtigen.

Sollen für den Zugriff auf eine Datenbank mobile Endgeräte wie beispielsweise entsprechend ausgestattete Mobiltelefone oder PDAs eingesetzt werden, sind die Bausteine B 3.404 *Mobiltelefon* beziehungsweise B 3.405 *Smartphones, Tablets und PDAs* zu berücksichtigen.

Die Gliederung der Sicherheitsmaßnahmen dieses Bausteins orientiert sich an dem Lebenszyklus eines Datenbanksystems. Für den sicheren Einsatz von Datenbanksystemen sollten unter anderem folgende Schritte durchlaufen werden:

**1. Planung**

Datenbanksysteme sind komplexe Produkte, deren Einsatz und Betrieb systematisch geplant werden muss. Dies mündet unter anderem in einen Anforderungskatalog an die zu beschaffende Software (siehe M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*) sowie in ein Datenbanksicherheitskonzept (siehe M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*).

**2. Schulung der Administratoren und Beschaffung der Software**

Bevor die Datenbank-Software produktiv eingesetzt werden kann, müssen die zuständigen Administratoren für den sicheren Betrieb des Datenbanksystems geschult werden (siehe M 3.11 *Schulung des Wartungs- und Administrationspersonals*). Diese Schulungsmaßnahme sollte nach Möglichkeit bereits vor der Beschaffung des Datenbanksystems (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*) erfolgen, damit die zuständigen Administratoren frühzeitig effektiv in die Konzeption und den Aufbau einbezogen werden können.

**3. Erstellung eines Datenbankkonzeptes / Datenbankmodells**

Vor dem Produktivbetrieb des Datenbanksystems ist ein Datenbankkonzept zu erstellen, das sowohl die Installation und Konfiguration der Datenbank-Komponenten, als auch die Struktur der anwendungsspezifischen Datenbank beschreibt. Darüber hinaus ist ein praxisorientiertes Benutzerkonzept zu erstellen. Je nach Volumen und Einsatzbereich der Datenbank sowie der gewählten Datenbank-Standardsoftware kann ein solches Konzept sehr umfangreich sein (M 2.125 *Installation und Konfiguration einer Datenbank*, M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*, M 2.128 *Zugangskontrolle einer Datenbank* und M 2.129 *Zugriffskontrolle einer Datenbank*).

**4. Betrieb des Datenbanksystems**

Die Inbetriebnahme und der Betrieb des Datenbanksystems erfordern neben der Umsetzung des Datenbankkonzeptes eine kontinuierliche Überwachung, um die Verfügbarkeit, die Integrität sowie die Vertraulichkeit der Daten sicherzustellen. Die hierfür wichtigsten Maßnahmen betreffen die Aspekte Dokumentation (M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*, M 2.34 *Dokumentation*

*der Veränderungen an einem bestehenden System*), Administration (M 2.130 *Gewährleistung der Datenbankintegrität*, M 2.133 *Kontrolle der Protokolldateien eines Datenbanksystems*) sowie die Nutzung der Datenbank (M 2.65 *Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System*, M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*).

**5. Notfallvorsorge**

Neben der Umsetzung der Maßnahmen zur Einführung und zum störungsfreien Betrieb eines Datenbanksystems gilt es, Ausfällen unterschiedlicher Art vorzubeugen und deren Auswirkungen möglichst gering zu halten. Hierzu sind die datenbankspezifischen Gegebenheiten zu berücksichtigen, um nach einem System- bzw. Datenbankausfall den gestellten Anforderungen hinsichtlich eines zeitnahen Wiederanlaufs des DBS gerecht zu werden und das Risiko eines Datenverlustes zu minimieren (M 6.49 *Datensicherung einer Datenbank*, M 6.50 *Archivierung von Datenbeständen*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Datenbanken" vorgestellt:

**Planung und Konzeption**
- M 2.80 (A) *Erstellung eines Anforderungskatalogs für Standardsoftware*
- M 2.126 (A) *Erstellung eines Datenbanksicherheitskonzeptes*
- M 2.132 (A) *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen*
- M 2.134 (B) *Richtlinien für Datenbank-Anfragen*
- M 2.363 (B) *Schutz gegen SQL-Injection*
- M 5.58 (B) *Auswahl und Installation von Datenbankschnittstellen-Treibern*

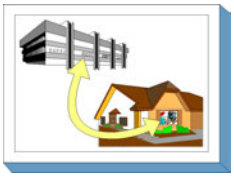
**Beschaffung**
- M 2.124 (B) *Geeignete Auswahl einer Datenbank-Software*

**Umsetzung**
- M 2.125 (A) *Installation und Konfiguration einer Datenbank*
- M 2.135 (C) *Gesicherte Datenübernahme in eine Datenbank*
- M 4.7 (A) *Änderung voreingestellter Passwörter*
- M 4.71 (C) *Restriktive Handhabung von Datenbank-Links*
- M 4.73 (C) *Festlegung von Obergrenzen für selektierbare Datensätze*

**Betrieb**
- M 2.31 (A) *Dokumentation der zugelassenen Benutzer und Rechteprofile*
- M 2.34 (A) *Dokumentation der Veränderungen an einem bestehenden System*
- M 2.65 (C) *Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System*
- M 2.127 (B) *Inferenzprävention*
- M 2.128 (A) *Zugangskontrolle einer Datenbank*
- M 2.129 (A) *Zugriffskontrolle einer Datenbank*
- M 2.130 (A) *Gewährleistung der Datenbankintegrität*
- M 2.131 (C) *Aufteilung von Administrationstätigkeiten bei Datenbanksystemen*
- M 2.133 (A) *Kontrolle der Protokolldateien eines Datenbanksystems*
- M 3.18 (A) *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*
- M 4.67 (B) *Sperren und Löschen nicht benötigter Datenbank-Accounts*
- M 4.68 (A) *Sicherstellung einer konsistenten Datenbankverwaltung*
- M 4.69 (B) *Regelmäßiger Sicherheitscheck der Datenbank*
- M 4.70 (C) *Durchführung einer Datenbanküberwachung*
- M 4.72 (Z) *Datenbank-Verschlüsselung*
- M 5.117 (Z) *Integration eines Datenbank-Servers in ein Sicherheitsgateway*

**Notfallvorsorge**
- M 6.48 (A) *Verhaltensregeln nach Verlust der Datenbankintegrität*
- M 6.49 (A) *Datensicherung einer Datenbank*
- M 6.50 (Z) *Archivierung von Datenbeständen*
- M 6.51 (B) *Wiederherstellung einer Datenbank*

# B 5.8 Telearbeit



## Beschreibung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ausschließlich oder zeitweise außerhalb der Gebäude des Arbeit- bzw. Auftraggebers verrichtet wird. Die Erledigung der Tätigkeiten wird durch eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers unterstützt.

Es gibt verschiedene Formen von Telearbeit. So kann sie als heimbasierte Telearbeit in der Wohnung des Mitarbeiters oder auch als mobile Telearbeit von unterwegs erbracht werden. Es ist ebenfalls möglich, dass die Mitarbeiter im Rahmen der On-Site-Telearbeit bei Kunden oder Lieferanten eingesetzt werden und dort mit der Ausstattung des eigenen Arbeitgebers arbeiten. Eine weitere Möglichkeit ist die Telearbeit in sogenannten Telecentern oder auch Satelliten- oder Nachbarschaftsbüros.

Bei der heimbasierten Telearbeit wird zwischen der ausschließlich zu Hause erbrachten Arbeit und der alternierenden Telearbeit unterschieden. Bei der alternierenden Telearbeit arbeiten die Arbeitnehmer wechselweise an ihrem Arbeitsplatz beim Arbeitgeber und am häuslichen Arbeitsplatz.

Dieser Baustein konzentriert sich auf die Formen der Telearbeit, die teilweise oder ganz im häuslichen Umfeld durchgeführt werden. Es wird davon ausgegangen, dass zwischen dem Arbeitsplatz zu Hause und der Institution eine Telekommunikationsverbindung besteht, die den Austausch von Daten oder gegebenenfalls auch den Zugriff auf Daten in der Institution ermöglicht.

Die Maßnahmenempfehlungen dieses Bausteins umfassen vier verschiedene Bereiche:

- die Organisation der Telearbeit,
- den Telearbeitsrechner des Telearbeiters,
- die Kommunikationsverbindung zwischen Telearbeitsrechner und Institution und
- den Kommunikationsrechner der Institution zur Anbindung des Telearbeitsrechners.

Die in diesem Baustein aufgeführten Maßnahmenempfehlungen konzentrieren sich auf zusätzliche Sicherheitsanforderungen für die IT-Systeme, die für die Telearbeit eingesetzt werden, und auch auf die bei der Telearbeit verarbeiteten Informationen. Insbesondere für die technischen Anteile der Telearbeit (Telearbeitsrechner, Kommunikationsverbindung und Kommunikationsrechner) werden sicherheitstechnische Anforderungen formuliert, die bei der konkreten Ausgestaltung durch geeignete IT-Systeme realisiert werden müssen.

## Gefährdungslage

Für den IT-Grundschutz der Telearbeit werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.1 *Personalausfall*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.24 *Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes*
- G 2.49 *Fehlende oder unzureichende Schulung der Telearbeiter*
- G 2.50 *Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter*
- G 2.51 *Mangelhafte Einbindung des Telearbeiters in den Informationsfluss*
- G 2.53 *Unzureichende Vertretungsregelungen für Telearbeit*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.30 *Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners*

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.10 *Missbrauch von Fernwartungszugängen*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.21 *Trojanische Pferde*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den sicheren Einsatz von Telearbeit sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zur Notfallvorsorge. Die Schritte, die dabei zu durchlaufen sind und die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Maßnahmen zur infrastrukturellen Sicherheit des Telearbeitsplatzes werden im Baustein B 2.8 *Häuslicher Arbeitsplatz* beschrieben. Für das als Telearbeitsrechner eingesetzte IT-System muss außerdem der passende Client-Baustein umgesetzt werden.

**Planung und Konzeption**

Es sollte ein Konzept für Telearbeit erstellt werden, in dem die Sicherheitsziele, der Schutzbedarf der bei der Telearbeit zu bearbeitenden Informationen sowie die Risiken und Sicherheitsmaßnahmen aufgezeigt werden (siehe M 2.117 *Erstellung eines Sicherheitskonzeptes für Telearbeit*).

Sichere Telearbeit setzt organisatorische Regelungen und personelle Maßnahmen voraus. Besonders zu beachten sind die speziellen Verpflichtungen der Telearbeiter und deren Einweisung in die Nutzungsregelungen der Kommunikation. Sie sind in den folgenden Maßnahmen beschrieben:

- M 2.113 *Regelungen für Telearbeit*
- M 2.116 *Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit*
- M 2.117 *Erstellung eines Sicherheitskonzeptes für Telearbeit*
- M 3.21 *Sicherheitstechnische Einweisung der Telearbeiter*

**Umsetzung**

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, können die Telearbeitsrechner, Kommunikationsrechner und andere IT-Systeme installiert werden. Dabei sind folgende Maßnahmen zu beachten:

- Sicherheit des Telearbeitsrechners: Der Telearbeitsrechner muss so gestaltet sein, dass im unsicheren Einsatzumfeld eine sichere Nutzung möglich ist. Insbesondere darf nur eine autorisierte Person den Telearbeitsrechner offline und online nutzen können. Dabei sind insbesondere die Sicherheitsanforderungen aus M 4.63 *Sicherheitstechnische Anforderungen an den Telearbeitsrechner* zu beachten.

- Sichere Kommunikation zwischen Telearbeitsrechner und Institution: Da die Kommunikation über öffentliche Netze (also z. B. über ISDN- oder DSL-Anbindungen) ausgeführt wird, sind besondere Sicherheitsanforderungen für die Kommunikation zwischen Telearbeitsrechner und Institution zu erfüllen. Sie sind in M 5.51 *Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution* beschrieben. Für die Anbindung des Telearbeitsrechners über öffentliche Netze ist Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* zu beachten. Für die Anbindung des Telearbeitsrechners über ein Virtuelles Privates Netz (VPN) ist der Baustein B 4.4 *VPN* zu beachten.
- Sicherheit des Kommunikationsrechners der Institution: Dieser Rechner stellt eine quasi öffentlich zugängliche Schnittstelle dar, über die der Telearbeiter die IT und die Daten der Institution nutzen kann. Da hier ein Missbrauch durch Dritte verhindert werden muss, sind besondere Sicherheitsanforderungen zu erfüllen, die in M 5.52 *Sicherheitstechnische Anforderungen an den Kommunikationsrechner* beschrieben sind.

**Betrieb**

Die Benutzer haben einen wesentlichen Einfluss auf die Sicherheit bei der Telearbeit. Die Telearbeiter müssen daher zur Einhaltung der Sicherheitsvorgaben und für die Nutzung der IT-Systeme geschult werden (siehe M 3.21 *Sicherheitstechnische Einweisung der Telearbeiter*).

**Notfallvorsorge**

Alle relevanten Daten, die im Rahmen der Telearbeit erstellt oder verändert wurden, müssen gesichert werden (siehe M 6.47 *Datensicherung bei der Telearbeit*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Telearbeit" vorgestellt.

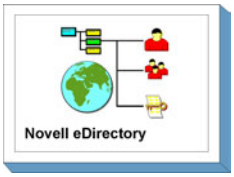
**Planung und Konzeption**
- M 2.113 (A) *Regelungen für Telearbeit*
- M 2.114 (A) *Informationsfluss zwischen Telearbeiter und Institution*
- M 2.115 (B) *Betreuungs- und Wartungskonzept für Telearbeitsplätze*
- M 2.116 (A) *Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit*
- M 2.117 (A) *Erstellung eines Sicherheitskonzeptes für Telearbeit*
- M 2.205 (C) *Übertragung und Abruf personenbezogener Daten*
- M 2.241 (C) *Durchführung einer Anforderungsanalyse für den Telearbeitsplatz*

**Umsetzung**
- M 4.63 (A) *Sicherheitstechnische Anforderungen an den Telearbeitsrechner*
- M 5.51 (A) *Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution*
- M 5.52 (A) *Sicherheitstechnische Anforderungen an den Kommunikationsrechner*

**Betrieb**
- M 3.21 (A) *Sicherheitstechnische Einweisung der Telearbeiter*

**Notfallvorsorge**
- M 6.47 (B) *Datensicherung bei der Telearbeit*

# B 5.9 Novell eDirectory




## Beschreibung

Novell eDirectory ist ein komplexes und vielseitiges Produkt, welches

- einerseits innerhalb eines Behörden- oder Unternehmensnetzes das Management der eingebundenen Ressourcen und deren Benutzer plattformübergreifend übernehmen kann und
- andererseits auch als Internet-Informationsbasis mit gesicherten und standardisierten Zugriffsmöglichkeiten via geeigneter Clients einsetzbar ist.

Diese beiden Szenarien ergeben völlig unterschiedliche Gefährdungen für den Einsatz und den Betrieb eines solchen Systems. Vor allem eine Kombination dieser Einsatzszenarien stellt vom Standpunkt der Informationssicherheit eine Herausforderung dar.

Entsprechend muss für die Sicherheit der in einem eDirectory-Verzeichnis gespeicherten Daten stets auch die Sicherheit des zugrunde liegenden Betriebssystems mit berücksichtigt werden. Letzteres ist jedoch nicht Bestandteil dieses Bausteins und es wird deshalb auf die entsprechenden Beschreibungen zum sicheren Betrieb des genutzten Betriebssystems in den Bausteinen der Schicht 3 verwiesen. Ebenso muss eine Grundabsicherung des Novell eDirectory als Verzeichnisdienst vorgenommen werden. Hierbei ist in jedem Fall der Baustein B 5.15 *Allgemeiner Verzeichnisdienst* zusätzlich zu diesem Baustein anzuwenden.

*eDirectory* ist aus dem Verzeichnisdienst *Novell Directory Services* (NDS) hervorgegangen, das Bestandteil des Betriebssystems *Netware 4* war. Dies war seinerzeit die herausragende Neuerung gegenüber dem Betriebssystem *Netware 3*. Inzwischen positioniert Novell diese Verzeichnisdienste als eigenständiges Produkt *eDirectory* vollständig unabhängig vom Netware-Betriebssystem. eDirectory lässt sich dabei auf einer Vielzahl von Betriebssystemen installieren und betreiben. In der Literatur und in den Quellen wird jedoch häufig weiterhin von "den Novell Directory Services" gesprochen und NDS mit eDirectory synonym gesetzt.

In diesem Baustein wird speziell die eDirectory-Version 8.6 betrachtet, und zwar die englische Version. Die Software unterstützt die Plattformen Netware, Windows NT/2000, Linux sowie Sun Solaris.

eDirectory kann mit spezieller Clientsoftware verwendet werden, wie dem Novell Client für die Windows-Betriebssysteme. Diese Clients sind in den Bootvorgang des jeweiligen Rechners integriert und übernehmen die Authentisierung der Benutzer gegen den Verzeichnisdienst eDirectory. Auch für Unix-Betriebssysteme (Linux, Solaris) gibt es eine ähnliche Möglichkeit, die den Mechanismus der *Pluggable Authentication Modules* (PAM) nutzt. Dabei kommen die *Novell Account Management Modules* zum Einsatz. Auch hier werden Benutzer beim Login gegen den eDirectory-Verzeichnisdienst authentisiert.

Eine andere Möglichkeit bietet der Zugriff über die LDAP-Schnittstelle. Durch die Verwendung dieser standardisierten Schnittstelle ist die Nutzung des eDirectorys auch mit anderen Applikationen und Systemen möglich. Für den Einsatz im Internet ist generell das LDAP-Protokoll die Zugriffsmethode.

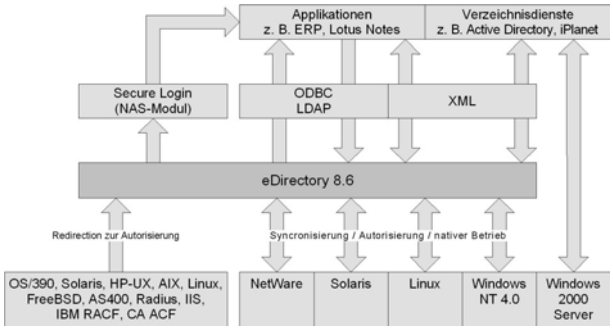



Abbildung: Architekturskizze

Weiterhin bietet die eDirectory-Software eine Vielzahl von Tools, unter anderem den *iMonitor*, der Überwachungs- und Diagnosemöglichkeiten über die Server eines Verzeichnisdienstes von einem Web-Browser aus zur Verfügung stellt.

## Gefährdungslage

Aufgrund der Vielzahl an Funktionen und der Komplexität der Software ist ein eDirectory-Verzeichnisdienst einer Reihe von Gefährdungen ausgesetzt. Hinzu kommen die Gefährdungen, die das eingesetzte Betriebssystem betreffen, insbesondere den allgemeinen Serverzugriff und das Dateisystem.

Für den IT-Grundschutz eines Novell eDirectory-Systems werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.69 *Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory*
- G 2.70 *Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory*
- G 2.71 *Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.34 *Ungeeignete Konfiguration des Managementsystems*
- G 3.35 *Server im laufenden Betrieb ausschalten*
- G 3.36 *Fehlinterpretation von Ereignissen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.50 *Fehlerhafte Konfiguration von Novell eDirectory*
- G 3.51 *Falsche Vergabe von Zugriffsrechten im Novell eDirectory*
- G 3.52 *Fehlerhafte Konfiguration des Intranet-Clientzugriffs auf Novell eDirectory*
- G 3.53 *Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.34 *Ausfall eines Kryptomoduls*
- G 4.44 *Ausfall von Novell eDirectory*

**Vorsätzliche Handlungen**

- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*

- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.65 *Verhinderung der Dienste eines Datenbanksystems*
- G 5.78 *DNS-Spoofing*
- G 5.81 *Unautorisierte Benutzung eines Kryptomoduls*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz der eDirectory-Komponenten sollte bereits bei der Planung ein spezifisches Sicherheitskonzept erstellt werden, welches sich konsistent in das bestehende organisationsweite Sicherheitskonzept integrieren lässt. Das eDirectory-System muss so konfiguriert werden, dass bereits bestehende Sicherheitsanforderungen umgesetzt werden, und hat darüber hinaus weitere, eDirectory-spezifische Anforderungen durchzusetzen.

Ein eDirectory-System wird in der Regel im Umfeld mit weiteren Systemen eingesetzt, welche den Zugriff auf das interne Netz von außen kontrollieren. Hierbei sind insbesondere Firewall-Systeme und Systeme zur Fernwartung zu nennen, mit denen eDirectory zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der eDirectory-spezifischen Maßnahmen stets auch die entsprechenden Maßnahmen aus den jeweiligen Bausteinen zusätzlich betroffener Systeme mit zu berücksichtigen. Neben den Bausteinen aus der Schicht 3 sind unter anderem auch die folgenden Bausteine zu nennen:

- B 3.301 *Sicherheitsgateway (Firewall)*, sofern eDirectory-Systeme in einer Firewall-Umgebung eingesetzt werden
- B 4.4 *VPN*, wenn der Zugriff auf das eDirectory-System über ein VPN erfolgt
- B 5.7 *Datenbanken*, allgemein

Für die sichere Implementierung eines eDirectory-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Installation bis hin zum Betrieb. Die einzelnen Schritte sowie die jeweiligen Maßnahmen, die auf diesem Weg zu beachten sind, sind nachstehend zusammengefasst:

- Nach der Entscheidung, eDirectory als Verzeichnissystem einzusetzen, muss Software und eventuell zusätzlich benötigte Hardware beschafft werden. Da eDirectory verschiedene Einsatzmöglichkeiten zulässt (siehe oben), hängt die gegebenenfalls zu beschaffende Hardware von den geplanten Einsatzszenarien ab. Daher sind folgende Maßnahmen zu ergreifen:
  - Zunächst muss der Einsatz des eDirectory-Systems geplant werden (siehe Maßnahmen M 2.236 *Planung des Einsatzes von Novell eDirectory* und M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*).
  - Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*), die einerseits bereits bestehende Sicherheitsrichtlinien im Kontext von eDirectory umsetzt und gleichzeitig eDirectory-spezifische Ergänzungen konsistent definiert.
  - Vor der tatsächlichen Verwendung des eDirectory-Systems im Regelbetrieb müssen die Benutzer und Administratoren auf den Umgang mit dem Produkt geschult werden. Insbesondere für Administratoren empfiehlt sich eine intensive Beschäftigung mit der Materie, die auf einen umfassenden Kenntnisstand bezüglich der Sicherheit der eingesetzten Betriebssysteme aufsetzen sollte (siehe M 3.29 *Schulung zur Administration von Novell eDirectory*). Benutzern sollten die verfügbaren Sicherheitsmechanismen der eingesetzten Clients detailliert vermittelt werden (siehe M 3.30 *Schulung zum Einsatz von Novell eDirectory Clientsoftware*).
- Nachdem die organisatorischen und planerischen Vorbereitungen durchgeführt wurden, kann die Installation des eDirectory-Systems erfolgen. Folgende Maßnahmen sind dabei zu ergreifen:
  - Die Installation kann erst dann als abgeschlossen angesehen werden, wenn die eDirectory-Systeme in einen sicheren Zustand überführt wurden (siehe M 4.153 *Sichere Installation von Novell eDirectory* und M 4.154 *Sichere Installation der Novell eDirectory Clientsoftware*).

Dadurch wird sichergestellt, dass in der anschließenden Konfigurationsphase nur berechtigte Administratoren auf das eDirectory-System zugreifen können.
  - Nach der "Rohinstallation" erfolgt eine erstmalige Konfiguration des eDirectory-Systems, siehe M 4.155 *Sichere Konfiguration von Novell eDirectory*, M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*, M 4.157 *Einrichten von Zugriffsberechtigungen auf Novell eDirectory*, sowie M 4.158 *Einrichten des LDAP-Zugriffs auf Novell eDirectory*.
- Nach der Konfiguration und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Dabei sind unter Sicherheitsgesichtspunkten folgende Aspekte zu beachten:
  - Ein eDirectory-System ist in der Regel kontinuierlichen Veränderungen unterworfen. Entsprechend müssen die sicherheitsrelevanten Konfigurationsparameter ständig angepasst werden. Weiterhin hängt die Sicherheit bei einer verteilten Softwarearchitektur von der Sicherheit sämtlicher Teilsysteme ab. Dies gilt insbesondere für die eDirectory-Clientsoftware. Die für den sicheren Betrieb relevanten Maßnahmen sind in M 4.159 *Sicherer Betrieb von Novell eDirectory* und M 4.160 *Überwachen von Novell eDirectory*, sowie der Maßnahme zur Kommunikationssicherung (siehe M 5.97 *Absicherung der Kommunikation mit Novell eDirectory*) zusammengefasst.
  - Neben den Maßnahmen zur Absicherung des laufenden Betriebs sind auch die Maßnahmen zur Notfallvorsorge von zentraler Bedeutung. Hinweise zu diesem Thema finden sich in M 6.81 *Erstellen von Datensicherungen für Novell eDirectory*.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Novell eDirectory" vorgestellt:

**Planung und Konzeption**
- M 2.236 (A) *Planung des Einsatzes von Novell eDirectory*
- M 2.237 (B) *Planung der Partitionierung und Replikation im Novell eDirectory*
- M 2.238 (A) *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*
- M 2.239 (A) *Planung des Einsatzes von Novell eDirectory im Intranet*
- M 2.240 (A) *Planung des Einsatzes von Novell eDirectory im Extranet*

**Umsetzung**
- M 3.29 (A) *Schulung zur Administration von Novell eDirectory*
- M 3.30 (A) *Schulung zum Einsatz von Novell eDirectory Clientsoftware*
- M 4.153 (A) *Sichere Installation von Novell eDirectory*
- M 4.154 (A) *Sichere Installation der Novell eDirectory Clientsoftware*
- M 4.155 (A) *Sichere Konfiguration von Novell eDirectory*
- M 4.156 (A) *Sichere Konfiguration der Novell eDirectory Clientsoftware*
- M 4.157 (A) *Einrichten von Zugriffsberechtigungen auf Novell eDirectory*
- M 4.158 (B) *Einrichten des LDAP-Zugriffs auf Novell eDirectory*

**Betrieb**
- M 4.159 (A) *Sicherer Betrieb von Novell eDirectory*
- M 4.160 (B) *Überwachen von Novell eDirectory*
- M 5.97 (B) *Absicherung der Kommunikation mit Novell eDirectory*

**Notfallvorsorge**
- M 6.81 (A) *Erstellen von Datensicherungen für Novell eDirectory*

# B 5.10 Internet Information Server

Dieser Baustein ist 2011 mit der 12. Ergänzungslieferung entfallen.

Für die Modellierung von Webservern ist der Baustein B 5.4 *Webserver* umzusetzen.

Die letzte Version des Bausteins, die mit der 11. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 5.11 Apache Webserver

Dieser Baustein ist 2011 mit der 12. Ergänzungslieferung entfallen.

Für die Abbildung von Webservern ist der Baustein B 5.4 *Webserver* umzusetzen.

Die letzte Version des Bausteins, die mit der 11. Ergänzungslieferung veröffentlicht wurde, kann weiterhin unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten abgerufen werden.

# B 5.12 Microsoft Exchange/Outlook

## Beschreibung

Microsoft Exchange ist ein Managementsystem für elektronische Nachrichten, das überdies Funktionen im Bereich der Workflow-Unterstützung bietet. Es ist unter anderem dazu gedacht, in mittleren bis großen Institutionen den internen und externen Austausch von Nachrichten, wie z. B. E-Mails, zu ermöglichen. Die Nachrichten können mit Exchange verwaltet, zugestellt, gefiltert und versendet werden. Ebenso werden typische Kommunikationsanwendungen wie Newsgroups, Kalender und Aufgabenlisten sowie Unified Messaging (Vereinheitlichung ein- und ausgehender Nachrichten) angeboten und von Exchange verwaltet.

Microsoft Outlook ist ein E-Mail-Client, der Bestandteil des Office Paketes von Microsoft ist. Neben den reinen E-Mail-Funktionen bietet er eine Reihe von Zusatzfunktionen, die Geschäftsprozessabwicklungen (z. B. Kommunikation, Messaging) in Unternehmen und Behörden erleichtern sollen.

In diesem Baustein werden Sicherheitsempfehlungen gegeben, die sich in der Regel auf die Funktionen von Microsoft Exchange 2010 bzw. Microsoft Outlook 2010 beziehen. Sie können in ähnlicher Form auch für Vor- und Nachgängerversionen verwendet werden.

## Gefährdungslage

Für den IT-Grundschutz von Kommunikationssystemen auf der Basis von Microsoft Exchange Servern und Microsoft Outlook Clients werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.1 *Personalausfall*
- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.55 *Ungeordnete Groupware-Nutzung*
- G 2.91 *Fehlerhafte Planung der Migration von Exchange*
- G 2.92 *Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange*
- G 2.95 *Fehlendes Konzept zur Anbindung anderer Systeme an Exchange*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.60 *Fehlerhafte Konfiguration von Exchange*
- G 3.61 *Fehlerhafte Konfiguration von Outlook*

**Technisches Versagen**

- G 4.20 *Überlastung von Informationssystemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.26 *Ausfall einer Datenbank*
- G 4.28 *Verlust von Daten einer Datenbank*
- G 4.32 *Nichtzustellung einer Nachricht*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.83 *Fehlfunktionen selbstentwickelter Makros unter Outlook*

**Vorsätzliche Handlungen**

- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*
- G 5.23 *Schadprogramme*
- G 5.77 *Mitlesen von E-Mails*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.84 *Gefälschte Zertifikate*
- G 5.135 *SPIT und Vishing*
- G 5.163 *Angriffe auf Exchange-Systeme*
- G 5.164 *Missbrauch von Programmierschnittstellen unter Outlook*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für einen sicheren Betrieb eines Microsoft-Exchange-Systems sind auch allgemeine Informationssicherheitsaspekte eines E-Mail-Systems zu behandeln, wie z. B. die Frage der Internet-Anbindung, eventuelle unterliegende Verschlüsselungsmaßnahmen, Behandlung aktiver Inhalte, Einsatz von Anti-Viren-Software und vieles mehr. Diesbezüglich wird auf den Baustein B 5.3 *Groupware* verwiesen. Die dort dargestellten Gefährdungen und Maßnahmen besitzen im Kontext von Microsoft Exchange/Outlook uneingeschränkte Gültigkeit.

Zu diesem Baustein sind außerdem auf den IT-Grundschutz-Webseiten Hilfsmittel veröffentlicht, die die Hinweise und Sicherheitsvorgaben zu Microsoft Exchange Server 2010 und Microsoft Outlook 2010 konkretisieren. Diese Hilfsmittel sind als detaillierte Verweise auf die hier aufgeführten Maßnahmen zu verstehen. Es werden zu allen jeweils relevanten Maßnahmen entsprechende Empfehlungen und Sicherheitsmaßnahmen zur vorliegenden Version der betrachteten Komponente ausformuliert.

Die Umsetzung der Aspekte in den nachfolgenden Maßnahmen wird durch Sicherheitsvorgaben für

- Microsoft Exchange Server 2010 und
- Microsoft Outlook 2010

in den Hilfsmitteln zu den IT-Grundschutz-Katalogen weiter erläutert und unterstützt.

Die Sicherheit von Windows-Betriebssystemen spielt eine zentrale Rolle für die Sicherheit von Microsoft-Exchange-Systemen. Dies gilt sowohl für die Server als auch die Clients des betrachteten Netzes. Entsprechend muss die Sicherheit des zugrunde liegenden Betriebssystems mit berücksichtigt werden. Letzteres ist jedoch nicht Bestandteil dieses Bausteins. Es wird deshalb auf die entsprechenden Beschreibungen zum sicheren Betrieb des genutzten Betriebssystems in den Bausteinen der Schicht 3 der IT-Grundschutz-Kataloge verwiesen. Von besonderer Bedeutung sind auch die von den Benutzern einzuhaltenden Sicherheitsvorkehrungen und Anweisungen.

Ein Exchange-System wird in der Regel im Umfeld mit weiteren Systemen eingesetzt, die den Zugriff auf das interne Netz von außen kontrollieren. Hierbei sind insbesondere Sicherheitsgateways und Systeme zur Fernwartung zu nennen, mit denen Microsoft Exchange zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der für Microsoft Exchange bzw. Outlook spezifischen Maßnahmen stets auch die entsprechenden Empfehlungen aus den jeweiligen Bausteinen zusätzlich betroffener Systeme zu berücksichtigen. Neben den Bausteinen der Schicht 3 sind unter anderem auch die folgenden Bausteine zu berücksichtigen:

- B 3.301 *Sicherheitsgateway (Firewall)*, sofern Exchange-Systeme in DMZ-Umgebungen eingesetzt werden.
- B 4.4 *VPN*, wenn der Zugriff auf das Exchange-System über VPN erfolgt.

Die Schritte, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

**Planungs- und Konzeptionsphase**

Ist die Entscheidung für ein Exchange-System gefallen, muss dessen sicherer Einsatz geplant und konzipiert werden. Die dabei zu berücksichtigenden Aspekte sind in M 2.247 *Planung des Einsatzes von Exchange und Outlook* zusammengefasst. Die Sicherheit eines Exchange-Systems kann bereits in der Planungs- und Konzeptionsphase entscheidend beeinflusst werden, indem sicherheitsrelevante Aspekte berücksichtigt werden.

Besondere Aufmerksamkeit ist der Planung der Sicherheit in solchen Szenarien zu widmen, in denen Microsoft-Exchange-Systeme in typischen Internet-Szenarien eingesetzt wird. Hier muss M 2.481 *Planung des Einsatzes von Exchange für Outlook Anywhere* umgesetzt werden.

**Umsetzung**

Nachdem die organisatorischen Vorarbeiten durchgeführt worden sind, kann die Installation eines Microsoft-Exchange-Systems erfolgen. Dabei ist die Maßnahme M 4.161 *Sichere Installation von Exchange-Systemen* zu beachten.

Benutzer und Administratoren von Exchange-Systemen müssen ausreichend geschult werden.

Die reine Installation eines Microsoft-Exchange-Systems stellt nur einen geringen Anteil der Arbeiten dar, die in der Umsetzungsphase durchzuführen sind. Der überwiegende Arbeitsaufwand fällt nach der Installation durch die Erstkonfiguration des Microsoft-Exchange-Systems an. Durch die erste Konfiguration werden die Basissicherheit bei der Betriebsaufnahme und die Rahmenbedingungen für die zukünftige Sicherheit des Microsoft-Exchange-Systems festgelegt.

Kern eines jeden Microsoft-Exchange-Systems ist die Datenbank und die darin gehaltenen Tabellen mit den Daten. Sicherheitsprobleme im Bereich der Datenbank betreffen immer die Gesamtsicherheit des Systems. Die Empfehlungen zur Konfiguration von Exchange-Servern und Datenbank sind zusammengefasst in M 4.162 *Sichere Konfiguration von Exchange-Servern*.

Microsoft-Exchange-Systeme sind verteilt aufgebaut und kommunizieren daher über verschiedene Schnittstellen miteinander und mit anderen externen Client- oder Server-Systemen. Die Absicherung der Kommunikation ist daher eine wichtige Aufgabe (M 5.100 *Absicherung der Kommunikation von und zu Exchange-Systemen*).

Ein Microsoft-Exchange-System muss an die lokalen funktionalen Anforderungen (z. B. Geschäftsprozesse) einer Behörde oder eines Unternehmens angepasst werden. Dies geschieht durch das sogenannte Customizing (Anpassung an den Kunden), siehe M 2.483 *Sicherheit beim Customizing von Exchange-Systemen*.

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Damit Sicherheitsverstöße bemerkt werden, muss eine entsprechende Überwachung des Microsoft-Exchange-Systems erfolgen (M 4.166 *Sicherer Betrieb von Exchange-Systemen* und M 2.482 *Regelmäßige Sicherheitsprüfungen für Exchange-Systeme*).

Da ein Microsoft-Exchange-System immer Veränderungen unterworfen ist, die sich meist aus veränderten Anforderungen oder Einsatzszenarien ableiten, muss sichergestellt werden, dass das gewünschte Sicherheitsniveau aufrecht erhalten wird (siehe hierzu B 1.14 *Patch- und Änderungsmanagement*). Dies trifft insbesondere für Eigenentwicklungen zu (siehe M 2.379 *Software-Entwicklung durch Endbenutzer*).

**Notfallvorsorge**

Empfehlungen zur Notfallvorsorge für Microsoft-Exchange-Systeme finden sich in der Maßnahme M 4.166 *Sicherer Betrieb von Exchange-Systemen*.

**Planung und Konzeption**

- M 2.247 (A) *Planung des Einsatzes von Exchange und Outlook*
- M 2.249 (B) *Planung der Migration von Exchange-Systemen*

- M 2.480 (W) *Nutzung der Exchange- und Outlook-Dokumentation*
- M 2.481 (B) *Planung des Einsatzes von Exchange für Outlook Anywhere*
- M 3.84 (W) *Einführung in Exchange-Systeme*
- M 4.381 (Z) *Verschlüsselung von Exchange-System-Datenbanken*

**Umsetzung**

- M 2.483 (C) *Sicherheit beim Customizing von Exchange-Systemen*
- M 3.31 (A) *Schulung zur Systemarchitektur und Sicherheit von Exchange-Systemen für Administratoren*
- M 3.32 (A) *Schulung zu Sicherheitsmechanismen von Outlook für Benutzer*
- M 4.161 (A) *Sichere Installation von Exchange-Systemen*
- M 4.162 (A) *Sichere Konfiguration von Exchange-Servern*
- M 4.163 (A) *Zugriffsrechte auf Exchange-Objekte*
- M 4.165 (A) *Sichere Konfiguration von Outlook*
- M 5.100 (B) *Absicherung der Kommunikation von und zu Exchange-Systemen*

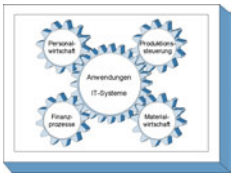
**Betrieb**

- M 2.482 (B) *Regelmäßige Sicherheitsprüfungen für Exchange-Systeme*
- M 4.166 (A) *Sicherer Betrieb von Exchange-Systemen*

**Notfallvorsorge**

- M 6.149 (A) *Datensicherung unter Exchange*

# B 5.13 SAP System




## Beschreibung

SAP Systeme werden in Unternehmen und Behörden eingesetzt, um interne und externe Unternehmens- bzw. Behörden- und Geschäftsabläufe zu automatisieren und technisch zu unterstützen (Enterprise Resource Planning, ERP). Ein SAP System verarbeitet daher typischerweise vertrauliche Daten, so dass ein entsprechender Schutz aller Systemkomponenten und Daten gewährleistet und das Schutzniveau an die Gefährdungslage angepasst werden muss. Daneben spielen auch Integrität und Verfügbarkeit eine wichtige Rolle.

SAP bietet eine umfangreiche Palette an Systemen, Komponenten und Funktionen an, so dass mit dem Begriff "SAP System" nicht eindeutig eine bestimmte Installation oder Gruppe von Komponenten gekennzeichnet werden kann. Im Rahmen dieses Bausteines kann nicht auf alle verfügbaren SAP Produkte eingegangen werden, die Darstellung beschränkt sich daher auf eine typische und in der Praxis häufig anzutreffende Kerninstallation.

Ein Beispiel für ein typisches SAP System ist ein mySAP ERP System, früher SAP R/3 genannt, mit den Enterprise Core Components Human Capital Management (HCM), Finanzen & Controlling (FI/CO), Material Management (MM), Verkauf & Vertrieb (SD), Logistik (PP), Projektmanagement (PS) und Qualitätsmanagement (QM). Als Kernkomponente fungiert hier der so genannte SAP NetWeaver ApplicationServer (ehemals SAP Web Application Server). Weitere Bestandteile der aktuellen NetWeaver-Plattform (derzeit NetWeaver 04) sind SAP XI als Daten-Integrationsplattform zwischen einzelnen SAP Systemen und auch zwischen SAP und Nicht-SAP Systemen sowie das SAP Enterprise Portal als Integrationsplattform für Anwendungen und Anwender. Auch diese beiden Bestandteile werden auf dem SAP NetWeaver ApplicationServer ausgeführt.

Ein kurzer Überblick über SAP Systeme und wichtige Fachbegriffe aus dem SAP Umfeld finden sich in der Maßnahme M 3.53 *Einführung in SAP Systeme*.

Die Gefährdungen und Maßnahmen dieses Bausteines orientieren sich hauptsächlich am SAP NetWeaver ApplicationServer, der vorrangigen technischen Basiskomponente der NetWeaver Plattform. Da auch diese Basiskomponente bereits in mehreren Versionen vorliegt und sich diese in den angebotenen Funktionen unterscheiden, wird bewusst auf die Darstellung versionsbezogener Unterschiede verzichtet. Auf diese Weise wird erreicht, dass der Baustein über längere Zeit angewendet werden kann und auch für bestehende SAP R/3 Systeme eingesetzt werden kann. Im Fokus der Maßnahmen und Gefährdungen steht dabei die Grundabsicherung eines SAP Systems auf Ebene der so genannten Basis-Administration. Die applikations- oder modulbezogene (z. B. HCM, FI) Absicherung ist nicht Teil dieses Bausteines. Da viele Applikationen und Module jedoch die Sicherheitsmechanismen der Basiskomponente nutzen, können die angegebenen Maßnahmen auch hier mit entsprechenden Anpassungen angewendet werden.

Ziel des Bausteines ist nicht, die bestehende, umfangreiche Dokumentation von SAP zu reproduzieren, sondern empfohlene sicherheitsrelevante Vorgehensweisen und beachtenswerte Besonderheiten darzustellen. Ansonsten kann auf die existierende SAP Dokumentation verwiesen werden, die detaillierte technische Darstellungen enthält. Die relevanten SAP Dokumentationen sind zentral in M 2.346 *Nutzung der SAP Dokumentation* zusammengestellt. IT-Sicherheitsbeauftragten und Administratoren hilft der Baustein nicht nur bei der Planung des SAP Einsatzes, er nennt auch die wichtigsten technischen Aspekte, die auch Sicht der Informationssicherheit zu beachten sind.

## Gefährdungslage

Der vorliegende Baustein behandelt Gefährdungen der SAP NetWeaver Basiskomponente SAP NetWeaver ApplicationServer, die im Rahmen der so genannten Basisadministration dieser Komponente in Intranet- und Internet-Szenarien relevant sind.

Generell hängt die Gefährdungslage von SAP Systemen vom Einsatzszenario ab. Ein SAP System in einem isolierten Behörden- oder Unternehmensnetz ist in der Regel weniger gefährdet als ein System, das an das Internet angeschlossen ist. Aber auch in internen Netzen kann mangelnder Schutz auf Netz- oder SAP System-Ebene dazu führen, dass unberechtigte Zugriffsmöglichkeiten bestehen. Dann spielt es eine Rolle, ob auf Daten nur lesend zugegriffen werden kann oder ob die Daten auch verändert werden können. Dies ist generell für Behörden und Unternehmen kritisch und wird beispielsweise auch bei Prüfungen untersucht, die auf dem Sarbanes Oxley Act basieren. In diesem Kontext sind speziell die Probleme unzureichender Berechtigungen und fehlender Funktionstrennung relevant.

Gerade durch den Einsatz von Web-Technologien, wie HTTP-basierten Zugriffsmöglichkeiten und Web-Applikationen mit Internet-Anbindung, hat sich die Gefährdungslage von SAP Systemen stark erhöht. Aufgrund der öffentlichen Netzanbindung von SAP Systemen ergeben sich daher in Folge von unsachgemäßer oder fehlerhafter Konfiguration wesentlich stärkere Gefährdungen. Dies gilt auch für fehlende oder unvollständig etablierte Prozesse, insbesondere in Outsourcing-Szenarien.

**Höhere Gewalt**

- G 1.1 *Personalausfall*

**Organisatorische Mängel**

- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.108 *Fehlende oder unzureichende Planung des SAP Einsatzes*

**Menschliche Fehlhandlungen**

- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.7 *Abhören von Leitungen*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.128 *Unberechtigter Zugriff auf Daten durch Einbringen von Code in ein SAP System*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines SAP Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der strategischen Entscheidung, über Planung, Konzeption und Installation bis zum Betrieb. Nicht vergessen werden darf dabei die ordnungsgemäße Aussonderung eines Systems, wenn das Ende der Betriebsphase erreicht wird.

Parallel zur Betriebsphase muss die Notfallvorsorge sicherstellen, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. Informationssicherheitsmanagement und Revision stellen sicher, dass das Regelwerk auch eingehalten wird.

Die Schritte, die dabei zu durchlaufen sind sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

**Planungs- und Konzeptionsphase**

Ist die Entscheidung für ein SAP System gefallen, muss der Einsatz des SAP Systems geplant und konzipiert werden. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 2.341 *Planung des SAP Einsatzes* zusammengefasst. Wichtig ist dabei, wie die Berechtigungen für die Benutzer eines SAP Systems geplant werden. Die dabei relevanten Themen sind in der Maßnahme M 2.342 *Planung von SAP Berechtigungen* enthalten. Es ist zu bedenken, dass die Sicherheit eines SAP Systems bereits

in der Planungs- und Konzeptionsphase entscheidend beeinflusst werden kann, indem sicherheitsrelevante Aspekte berücksichtigt werden. Maßnahmen für die SAP spezifische Benutzerschulung finden sich in M 3.52 *Schulung zu SAP Systemen*, da ausreichende Kenntnisse bei Benutzern und Administratoren von SAP Systemen die Sicherheit beeinflussen.

Besondere Aufmerksamkeit ist der Planung der Sicherheit in solchen Szenarien zu widmen, in denen SAP Systeme einer besonderen Gefährdung ausgesetzt sind. Dabei kann es sich um typische Internet-Szenarien handeln, so dass die Empfehlungen der Maßnahme M 2.344 *Sicherer Betrieb von SAP Systemen im Internet* umgesetzt werden müssen. Es kann sich aber auch um Intranet-Szenarien handeln, beispielsweise wenn ein SAP System von einem Behörden- oder Unternehmensportal aus angesprochen werden soll. Hier werden dann die Empfehlungen der Maßnahme M 2.343 *Absicherung eines SAP Systems im Portal-Szenario* relevant. Ein häufiges Szenario, das mit spezifischen Gefährdungen verbunden ist, ist das Outsourcing eines SAP Systems, denn hier erfolgen Konfiguration und Administration durch behörden- oder unternehmensfremde Personen. Für diesen Fall finden sich Hinweise und Empfehlungen in der Maßnahme M 2.345 *Outsourcing eines SAP Systems*.

**Umsetzungsphase**

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt worden sind, kann die Installation eines SAP Systems erfolgen. Dabei ist die Maßnahme M 4.256 *Sichere Installation von SAP Systemen* zu beachten.

Die reine Installation eines SAP Systems stellt nur einen geringen Anteil der Arbeiten dar, die in der Umsetzungsphase durchzuführen sind. Der überwiegende Arbeitsaufwand fällt nach der Installation durch die Erstkonfiguration des SAP Systems an. Durch die erste Konfiguration werden die Grundsicherheit bei der Betriebsaufnahme und die Rahmenbedingungen für die zukünftige Sicherheit des SAP Systems festgelegt und definiert. Daher sind in der Umsetzungsphase folgende Aspekte zu berücksichtigen:

Die Erstkonfiguration ist sowohl für den ABAP-Stack als auch für den Java-Stack erforderlich. Es sind insbesondere Situationen zu vermeiden, in denen einer der beiden Stacks unkonfiguriert bleibt, da er nicht genutzt wird. Die entsprechenden Empfehlungen finden sich in folgenden Maßnahmen:

- M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*
- M 4.266 *Sichere Konfiguration des SAP Java-Stacks*

Kern eines jeden SAP Systems ist die Datenbank und die darin gehaltenen Tabellen mit den Daten. Die Datenbank speichert nicht nur die Geschäftsdaten einer Behörden oder Unternehmens, sondern auch die internen Funktionen und Verwaltungsinformationen des SAP Systems. Sicherheitsprobleme im Bereich der Datenbank betreffen daher sofort immer die Gesamtsicherheit des SAP Systems. Die Datenbank-bezogenen Maßnahmen sind zusammengefasst in:

- M 4.269 *Sichere Konfiguration der SAP System Datenbank*

SAP Systeme sind verteilt aufgebaut und kommunizieren daher über verschiedene Schnittstellen miteinander oder mit anderen externen Client- oder Server-Systemen. Die Absicherung der Kommunikation ist daher eine wichtige Aufgabe. Generell kann ein SAP System viele unterschiedliche Kommunikationskanäle nutzen, die auch von den installierten Applikationen und Modulen abhängen. In der Regel werden jedoch einige wenige Basis-Kommunikationsmechanismen und -Schnittstellen genutzt. Die relevante Einstiegsmaßnahme ist:

- M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*

Ein SAP System muss an die lokalen funktionalen Anforderungen einer Behörde oder eines Unternehmens angepasst werden. Dies geschieht durch das so genannte Customizing (Anpassung an den Kunden). Die in diesem Kontext relevante Maßnahme ist:

- M 2.348 *Sicherheit beim Customizing von SAP Systemen*

**Betrieb**

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

Damit Sicherheitsverstöße bemerkt werden, muss eine entsprechende Überwachung des SAP Systems erfolgen. Hinweise dazu finden sich in den Maßnahmen:

- M 4.270 *SAP Protokollierung*
- M 2.347 *Regelmäßige Sicherheitsprüfungen für SAP Systeme*

Neuere Versionen der SAP Software bieten die Möglichkeit, ein Computer-Viren-Schutzprogramm anzuschließen, so dass beispielsweise Dokumente und Daten, die an das SAP System gesandt werden, auf Viren geprüft werden können. Hinweise dazu finden sich in:

- M 4.271 *Virenschutz für SAP Systeme*

Da ein SAP System immer Veränderungen unterworfen ist, die sich meist aus veränderten Anforderungen oder Einsatzszenarien ableiten, muss sichergestellt werden, dass das gewünschte Sicherheitsniveau aufrecht erhalten wird (siehe hierzu M 2.221 *Änderungsmanagement* bzw. B 1.14 *Patch- und Änderungsmanagement*). Dies trifft insbesondere für Eigenentwicklungen zu. Die im diesen Kontext relevante Maßnahmen ist:

- M 2.349 *Sicherheit bei der Software-Entwicklung für SAP Systeme*

Neuer Code oder andere veränderbare Komponenten müssen in das System eingebracht werden. Dazu steht für ABAP-bezogene Veränderungen das SAP Transportsystem zur Verfügung. Für die Software-Verteilung im Bereich des Java-Stacks wird hingegen ein anderer Mechanismus eingesetzt. In beiden Fällen muss eine Absicherung erfolgen, damit die Mechanismen nicht missbraucht werden können. Die relevanten Maßnahmen sind:

- M 4.272 *Sichere Nutzung des SAP Transportsystems*
- M 4.273 *Sichere Nutzung der SAP Java-Stack Software-Verteilung*

**Aussonderung**

Empfehlungen zur Deinstallation von SAP Systemen, etwa nach Abschluss des Regelbetriebs, finden sich in der Maßnahme M 2.350 *Aussonderung von SAP Systemen*.

**Notfallvorsorge**

Empfehlungen zur Notfallvorsorge für SAP Systeme finden sich in der Maßnahme M 6.97 *Notfallvorsorge für SAP Systeme*.

Nachfolgend werden alle Maßnahmen für SAP Systeme vorgestellt:

**Planung und Konzeption**

- M 2.341 (A) *Planung des SAP Einsatzes*
- M 2.342 (A) *Planung von SAP Berechtigungen*
- M 2.343 (C) *Absicherung eines SAP Systems im Portal-Szenario*
- M 2.344 (C) *Sicherer Betrieb von SAP Systemen im Internet*
- M 2.345 (C) *Outsourcing eines SAP Systems*
- M 2.346 (A) *Nutzung der SAP Dokumentation*
- M 3.52 (A) *Schulung zu SAP Systemen*
- M 3.53 (W) *Einführung in SAP Systeme*

**Umsetzung**

- M 4.256 (A) *Sichere Installation von SAP Systemen*
- M 4.257 (A) *Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene*
- M 4.258 (A) *Sichere Konfiguration des SAP ABAP-Stacks*
- M 4.259 (A) *Sicherer Einsatz der ABAP-Stack Benutzerverwaltung*
- M 4.260 (A) *Berechtigungsverwaltung für SAP Systeme*

- M 4.261 (B) *Sicherer Umgang mit kritischen SAP Berechtigungen*
- M 4.262 (C) *Konfiguration zusätzlicher SAP Berechtigungsprüfungen*
- M 4.263 (A) *Absicherung von SAP Destinationen*
- M 4.264 (A) *Einschränkung von direkten Tabellenveränderungen in SAP Systemen*
- M 4.265 (B) *Sichere Konfiguration der Batch-Verarbeitung im SAP System*
- M 4.266 (A) *Sichere Konfiguration des SAP Java-Stacks*
- M 4.267 (A) *Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung*
- M 4.268 (A) *Sichere Konfiguration der SAP Java-Stack Berechtigungen*
- M 4.269 (A) *Sichere Konfiguration der SAP System Datenbank*
- M 5.125 (B) *Absicherung der Kommunikation von und zu SAP Systemen*
- M 5.126 (A) *Absicherung der SAP RFC-Schnittstelle*
- M 5.127 (B) *Absicherung des SAP Internet Connection Framework (ICF)*
- M 5.128 (B) *Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle*
- M 5.129 (C) *Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen*

**Betrieb**

- M 2.347 (B) *Regelmäßige Sicherheitsprüfungen für SAP Systeme*
- M 2.348 (C) *Sicherheit beim Customizing von SAP Systemen*
- M 2.349 (C) *Sicherheit bei der Software-Entwicklung für SAP Systeme*
- M 4.270 (A) *SAP Protokollierung*
- M 4.271 (C) *Virenschutz für SAP Systeme*
- M 4.272 (A) *Sichere Nutzung des SAP Transportsystems*
- M 4.273 (A) *Sichere Nutzung der SAP Java-Stack Software-Verteilung*

**Aussonderung**

- M 2.350 (A) *Aussonderung von SAP Systemen*

**Notfallvorsorge**

- M 6.97 (A) *Notfallvorsorge für SAP Systeme*

# B 5.14 Mobile Datenträger

## Beschreibung

In diesem Baustein werden die grundsätzlichen Sicherheitseigenschaften mobiler Datenträger betrachtet. Mobile Datenträger können eingesetzt werden für

- den Datenaustausch (siehe Baustein B 5.2 *Datenträgeraustausch*),
- den Datentransport zwischen IT-Systemen, die nicht miteinander vernetzt sind, oder zwischen verschiedenen Lokationen (siehe z. B. B 5.8 *Telearbeit*),
- die Archivierung oder Speicherung von Sicherheitskopien (Backup), falls andere automatisierte Verfahren nicht zweckmäßig sind (siehe Bausteine B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*),
- die Speicherung von Daten, die zu sensitiv sind, um sie auf Arbeitsplatzrechnern oder Servern zu speichern,
- die mobile Datennutzung oder Datenerzeugung (z. B. MP3-Player, Digitalkamera, etc.).

Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern, hierzu gehören unter anderem Disketten, Wechselplatten (magnetisch, magneto-optisch), CD-ROMs, DVDs, Magnetbänder, Kassetten, USB-Festplatten und auch Flash-Speicher wie USB-Sticks. Durch diese Vielzahl an Formen und Einsatzgebieten werden nicht immer alle erforderlichen Sicherheitsbetrachtungen vorgenommen.

Datenträger können danach klassifiziert werden, ob sie nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind. Sie können auch nach weiteren Kriterien unterteilt werden, beispielsweise

- nach der Art der Datenspeicherung: analoge oder digitale Datenträger
- wie sie bearbeitet werden können: ohne technische Hilfsmittel, wie z. B. Papier, oder nur mit technischen Hilfsmitteln, wie z. B. Mikrofilme oder Tonbänder
- nach ihrer Bauform: auswechselbare Datenträger, externe Datenspeicher oder Datenträger, die in andere Geräte integriert sind.

Auswechselbare Datenträger, teilweise auch als Wechselmedien bezeichnet, werden in ein Laufwerk eingelegt. Beispiele hierfür sind Disketten, CD-ROMs, DVDs, Magnetbänder und Kassetten. Externe Datenspeicher, wie beispielsweise USB-Sticks und externe Festplatten, können hingegen direkt an ein IT-System angeschlossen werden. Beispiele für Datenträger, die in anderen Geräten integriert sind, sind die Speicherkomponenten in Mobiltelefonen, MP3-Playern und Digitalkameras.

Neben den digitalen Datenträgern sind auch Informationen auf Papier, Mikrofilmen oder anderen analogen Datenträgern bei der Sicherheitskonzeption zu berücksichtigen. Dies betrifft insbesondere das Drucken, Kopieren und Einscannen von Dokumenten sowie die Nutzung von Fax-Diensten. Weitere Hinweise hierzu finden sich in den Bausteinen B 3.406 *Drucker, Kopierer und Multifunktionsgeräte* und B 3.402 *Faxgerät*.

In diesem Baustein wird einerseits aufgezeigt, wie die auf mobilen Datenträgern gespeicherten Informationen sicher genutzt werden können und andererseits wie einer unbefugten Weitergabe von Informationen über mobile Datenträger vorgebeugt werden sollte.

## Gefährdungslage

Für den IT-Grundschutz bei der Nutzung von mobilen Datenträgern werden folgende typische Gefährdungen angenommen:

### Höhere Gewalt

- G 1.9 *Datenverlust durch starke Magnetfelder*
- G 1.15 *Beeinträchtigung durch wechselnde Einsatzumgebung*

**Organisatorische Mängel**

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.10 *Nicht fristgerecht verfügbare Datenträger*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*

**Technisches Versagen**

- G 4.7 *Defekte Datenträger*
- G 4.52 *Datenverlust bei mobilem Einsatz*

**Vorsätzliche Handlungen**

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.4 *Diebstahl*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.23 *Schadprogramme*
- G 5.141 *Datendiebstahl über mobile Datenträger*
- G 5.142 *Verbreitung von Schadprogrammen über mobile Datenträger*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den sicheren Umgang mit mobilen Datenträgern sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

**Planung und Konzeption**

Es sollte ein Konzept für den sicheren Umgang mit mobilen Datenträgern erstellt werden, in dem für die verschiedenen Arten von mobilen Datenträgern Risiken und Sicherheitsmaßnahmen aufgezeigt werden (siehe M 2.401 *Umgang mit mobilen Datenträgern und Geräten*).

**Beschaffung**

Die Auswahl geeigneter Datenträger ist abzustimmen. Für die Entscheidung, welche Arten von Datenträgern eingesetzt werden, sollte M 4.169 *Verwendung geeigneter Archivmedien* berücksichtigt werden.

**Betrieb**

Basierend auf den jeweiligen Sicherheitsanforderungen sollten anhand von Einsatzszenarien Sicherheitshinweise für alle Mitarbeiter erstellt werden (siehe M 3.60 *Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten*).

Die Laufwerke und die Schnittstellen der IT-Systeme sollten gemäß den Sicherheitsvorgaben abgesichert werden (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).

**Aussonderung**

Wenn Datenträger weitergegeben werden, sollten sie vor ihrer erneuten Verwendung oder Aussonderung physikalisch gelöscht werden, damit keine sensiblen Informationen in die falschen Hände geraten (siehe M 4.32 *Physikalisches Löschen der Datenträger vor und nach Verwendung*).

**Notfallvorsorge**

Wichtige Informationen, die auf mobilen Datenträgern gespeichert sind, sollten noch an einer anderen Stelle gespeichert sein, um einem Verlust vorzubeugen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Mobile Datenträger" vorgestellt.

**Planung und Konzeption**
- M 2.3 (B) *Datenträgerverwaltung*
- M 2.218 (C) *Regelung der Mitnahme von Datenträgern und IT-Komponenten*
- M 2.401 (C) *Umgang mit mobilen Datenträgern und Geräten*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*

**Umsetzung**
- M 4.32 (B) *Physikalisches Löschen der Datenträger vor und nach Verwendung*

**Betrieb**
- M 3.60 (C) *Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten*
- M 4.4 (C) *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*
- M 4.200 (Z) *Umgang mit USB-Speichermedien*
- M 4.232 (Z) *Sichere Nutzung von Zusatzspeicherkarten*

**Aussonderung**
- M 2.306 (A) *Verlustmeldung*

**Notfallvorsorge**
- M 6.38 (A) *Sicherungskopie der übermittelten Daten*

# B 5.15 Allgemeiner Verzeichnisdienst


## Beschreibung

Ein Verzeichnisdienst stellt in einem Computernetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. Mit einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel zu einer Benutzerkennung Namen und Vornamen des Benutzers, die Personalnummer und der Rechnername. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden aber nur einmal von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen, Zertifikate für elektronische Signaturen
- Ressourcen-Verwaltung, z. B. für Computer, Drucker, Scanner und andere Peripherie-Geräte
- Benutzer-Verwaltung, z. B. zur Verwaltung von Benutzerkonten und Benutzerberechtigungen
- Authentisierung, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise abgerufen werden, während Schreibzugriffe, wie das Erstellen, Ändern oder Löschen von Einträgen, seltener notwendig sind.

Die Daten in einem Verzeichnisdienst sind in der Regel objektbasiert in einer Baumstruktur logisch angeordnet. Die Struktur kann politische, geografische oder organisatorische Verhältnisse der Daten im Verzeichnis abbilden. Die Objekte werden in, gegebenenfalls verteilten, Verzeichnissen und Datenbanken hierarchisch gespeichert. Ausgehend von einem Wurzelobjekt (Root) verzweigen die Objekte in Eltern-Kind-Beziehungen bis hin zu den Blättern. Während Objekte, die selbst Objekte enthalten, als Containerobjekte bezeichnet werden, werden die Objekte am Ende des Baumes Blattobjekte genannt.

Software für Verzeichnisdienste wird von vielen Herstellern angeboten. Beispiele hierfür sind Active Directory von Microsoft (siehe B 5.16 *Active Directory*) und Novell eDirectory (siehe B 5.9 *Novell eDirectory*). Andere Verzeichnisdienste basieren auf dem frei verfügbaren OpenLDAP (sie B 5.20 *OpenLDAP*), das in vielen Unix-basierten Systemen Verwendung findet, aber beispielsweise auch von Mac OS X genutzt wird.

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Verzeichnisdiensten unabhängig vom eingesetzten Produkt. Für produktspezifische Sicherheitsaspekte existieren in den IT-Grundschutz-Katalogen weitere Bausteine, die zusätzlich auf den jeweiligen Verzeichnisdienst anzuwenden sind.

## Gefährdungslage

Verzeichnisdienste sind einer Reihe von direkten Gefährdungen ausgesetzt. Hinzu kommen indirekte Gefährdungen, die in Zusammenhang mit dem darunter liegenden Betriebssystem stehen.

Für den IT-Grundschutz von Verzeichnisdiensten werden die folgenden Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.123 *Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten*

- G 2.124 *Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst*
- G 2.125 *Fehlerhafte oder unzureichende Planung des Zugriffs auf den Verzeichnisdienst*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*
- G 3.87 *Fehlerhafte Konfiguration von Verzeichnisdiensten*
- G 3.88 *Falsche Vergabe von Zugriffsrechten*
- G 3.89 *Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.67 *Ausfall von Verzeichnisdiensten*

**Vorsätzliche Handlungen**

- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.65 *Verhinderung der Dienste eines Datenbanksystems*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.78 *DNS-Spoofing*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.144 *Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Verzeichnisdienste können sowohl bereits in ein Betriebssystem integriert sein, wie Active Directory in Windows Server ab Windows 2000, als auch in eigenständigen Software-Komponenten, wie dem quelloffenen OpenLDAP angeboten werden. Entsprechend muss für die Sicherheit der in einem Verzeichnis gespeicherten Daten stets auch die Sicherheit des zugrunde liegenden Betriebssystems mit berücksichtigt werden. Letzteres ist jedoch nicht Bestandteil dieses Bausteins. Es wird deshalb auf die entsprechenden Beschreibungen zum sicheren Betrieb des genutzten Betriebssystems in den Bausteinen der Schicht 3 verwiesen.

Ebenso wird beim Einsatz eines Verzeichnisdienstes auch die Behandlung der übergreifenden Aspekte vorausgesetzt, die in den relevanten Bausteinen der Schicht 1 zu finden sind. Die Sicherheitsanforderungen des Verzeichnisdienstes sollten daher bei der Erstellung von übergreifenden Konzepten (siehe beispielsweise B 1.6 *Schutz vor Schadprogrammen*) mit einbezogen werden.

Im Rahmen der sicheren Implementierung eines Verzeichnisdienstes ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Als Einstieg empfiehlt es sich zunächst die Maßnahme M 3.61 *Einführung in Verzeichnisdienst-Grundlagen* zu betrachten, die einen Überblick über den Aufbau und die Begrifflichkeiten eines Verzeichnisdienstes beinhaltet.

Um eine Entscheidung zu treffen, welche Art von Verzeichnisdienst in der Institution eingesetzt werden kann, ist zunächst eine Anforderungsanalyse vorzunehmen. Auf dieser Grundlage muss anschließend

der Einsatz des Verzeichnisdienstes geplant werden (siehe Maßnahmen M 2.403 *Planung des Einsatzes von Verzeichnisdiensten* und M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst*). Dabei ist die Verteilung der administrativen Aufgaben von wesentlicher Bedeutung (siehe Maßnahme M 2.407 *Planung der Administration von Verzeichnisdiensten*).

In diesem Zusammenhang ist eine Sicherheitskonzeption und eine -richtlinie zu erarbeiten (siehe M 2.404 *Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste* und M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*,). Diese müssen sich in den Kontext bereits bestehender Sicherheitskonzepte und -richtlinien eingliedern und gleichzeitig spezifische Ergänzungen für Verzeichnisdienste definieren.

Wenn aufgrund von Umstrukturierungen oder Aktualisierungen im Informationsverbund ein Verzeichnisdienst zu migrieren ist, sind ebenfalls umfangreiche planerische und konzeptionelle Arbeiten erforderlich (siehe Maßnahme M 2.408 *Planung der Migration von Verzeichnisdiensten*).

**Beschaffung**

Nach der Entscheidung einen Verzeichnisdienst einzusetzen, muss die dafür notwendige Software und eventuell zusätzlich benötigte Hardware beschafft werden. Da ein Verzeichnisdienst verschiedene Einsatzmöglichkeiten zulässt, hängt die Auswahl und Beschaffung (siehe Maßnahme M 2.406 *Geeignete Auswahl von Komponenten für Verzeichnisdienste*) von den geplanten Einsatzszenarien ab.

**Umsetzung**

Nachdem die organisatorischen und planerischen Vorbereitungen durchgeführt wurden und die Entscheidung über die Beschaffung des Verzeichnisdienstes getroffen ist, kann der Verzeichnisdienst installiert werden. Folgende Maßnahmen sind dabei zu ergreifen:

Die Installation dient dem erstmaligen Aufbau eines Verzeichnisdienstes (siehe M 4.308 *Sichere Installation von Verzeichnisdiensten*) und gilt erst dann als abgeschlossen, wenn der Verzeichnisdienst in einen sicheren Zustand überführt wurde. So ist sichergestellt, dass in der anschließenden Konfigurationsphase nur berechtigte Administratoren auf den Verzeichnisdienst zugreifen können.

Nach der Installation erfolgt eine erstmalige Konfiguration des Verzeichnisdienstes (siehe Maßnahmen M 4.307 *Sichere Konfiguration von Verzeichnisdiensten*, M 4.309 *Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste* und M 4.310 *Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste*).

Die Benutzer und Administratoren des Verzeichnisdienstes sind ausreichend zu schulen, um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren bei einer unsachgemäßen Verwendung des Verzeichnisdienstes hinzuweisen und zu sensibilisieren (siehe Maßnahmen M 3.62 *Schulung zur Administration von Verzeichnisdiensten* und M 3.63 *Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten*).

**Betrieb**

Nach der Konfiguration und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Dabei sind unter Sicherheitsgesichtspunkten folgende Aspekte zu beachten:

Verzeichnisdienste sind naturgemäß kontinuierlichen Veränderungen unterworfen. Entsprechend müssen die sicherheitsrelevanten Konfigurationsparameter ständig angepasst werden (siehe Maßnahme M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Die für den sicheren Betrieb relevanten Aspekte finden sich in M 4.311 *Sicherer Betrieb von Verzeichnisdiensten* sowie speziell zur Kommunikationssicherung in M 5.147 *Absicherung der Kommunikation mit Verzeichnisdiensten*.

Um den Sicherheitszustand eines Verzeichnisdienstes nachvollziehen zu können, ist es ratsam, diesen kontinuierlich zu überwachen (siehe M 4.312 *Überwachung von Verzeichnisdiensten*).

**Aussonderung**

Wird entschieden, einen Verzeichnisdienst nicht weiter zu betreiben, sind insbesondere die verbliebenen Daten und Rechte sicher zu löschen. Aber auch wenn nur Teile eines Verzeichnisdienstes ausge-

sondert werden, sind einige Punkte zu beachten, die M 2.410 *Geregelte Außerbetriebnahme eines Verzeichnisdienstes* näher erläutert.

**Notfallvorsorge**

Neben den Maßnahmen zur Absicherung des Verzeichnisdienstes im laufenden Betrieb besitzen auch die Maßnahmen zur Notfallvorsorge eine relevante Bedeutung. Hinweise zu diesem Thema finden sich in M 6.106 *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes* sowie in M 6.107 *Erstellung von Datensicherungen für Verzeichnisdienste*.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Verzeichnisdienst" vorgestellt:

**Planung und Konzeption**
- M 2.403 (A) *Planung des Einsatzes von Verzeichnisdiensten*
- M 2.404 (A) *Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste*
- M 2.405 (A) *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*
- M 2.407 (A) *Planung der Administration von Verzeichnisdiensten*
- M 2.408 (Z) *Planung der Migration von Verzeichnisdiensten*
- M 2.409 (B) *Planung der Partitionierung und Replikation im Verzeichnisdienst*
- M 3.61 (W) *Einführung in Verzeichnisdienst-Grundlagen*

**Beschaffung**
- M 2.406 (B) *Geeignete Auswahl von Komponenten für Verzeichnisdienste*

**Umsetzung**
- M 3.62 (A) *Schulung zur Administration von Verzeichnisdiensten*
- M 3.63 (A) *Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten*
- M 4.307 (A) *Sichere Konfiguration von Verzeichnisdiensten*
- M 4.308 (A) *Sichere Installation von Verzeichnisdiensten*
- M 4.309 (A) *Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste*
- M 4.310 (B) *Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste*

**Betrieb**
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.311 (A) *Sicherer Betrieb von Verzeichnisdiensten*
- M 4.312 (B) *Überwachung von Verzeichnisdiensten*
- M 5.147 (C) *Absicherung der Kommunikation mit Verzeichnisdiensten*

**Aussonderung**
- M 2.410 (B) *Geregelte Außerbetriebnahme eines Verzeichnisdienstes*

**Notfallvorsorge**
- M 6.106 (Z) *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes*
- M 6.107 (C) *Erstellung von Datensicherungen für Verzeichnisdienste*

# B 5.16 Active Directory


## Beschreibung

Active Directory ist ein von Microsoft entwickelter Verzeichnisdienst, der mit dem Betriebssystem Windows 2000 Server erstmalig eingeführt wurde. Ausgehend von den Active Directory-Funktionen des Betriebssystems Microsoft Windows 2000 Server wurden dem Active Directory-Dienst der Windows-Server-2003-Familie weitere Schlüsselfunktionen hinzugefügt.

Active Directory wird hauptsächlich in IT-Netzen mit überwiegend Microsoft-Komponenten eingesetzt. Active Directory speichert Informationen über Objekte innerhalb eines IT-Netzes, z. B. über Benutzer oder Computer, und erleichtert es Anwendern und Administratoren, diese Informationen bereitzustellen, zu organisieren, zu nutzen und zu überwachen. Als ein objektbasierter Verzeichnisdienst ermöglicht Active Directory die Verwaltung von Objekten und deren Beziehung untereinander, die die eigentliche Netzumgebung ausmachen. Active Directory stellt zentrale Steuerungs- und Kontrollmöglichkeiten des jeweiligen Netzes bereit. Der Einsatz eines solchen Verzeichnisdienstes bietet sich vor allem dort an, wo z. B. die Anzahl der im Netz eingesetzten Clients eine dezentrale Verwaltung erschwert. Ohne einen Verzeichnisdienst könnte die Zuverlässigkeit lokal vorzunehmender Einstellungen, wie z. B. Umsetzung der Vorgaben aus Sicherheitsrichtlinien, aufgrund des hohen personellen Aufwandes nicht mehr gewährleistet werden. Verwaltungsaufgaben innerhalb des Netzes wie z. B. Passwortänderungen, Kontenerstellung und Zugriffsrechte können durch den Einsatz eines Verzeichnisdienstes effizienter durchgeführt werden.

### Abgrenzung des Bausteins

In diesem Baustein werden die für Active Directory spezifischen Gefährdungen und Maßnahmen betrachtet. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten finden sich im Baustein B 5.15 *Allgemeiner Verzeichnisdienst*. Die dort beschriebenen allgemeinen Maßnahmen werden im vorliegenden Baustein konkretisiert und ergänzt.

## Gefährdungslage

Für den IT-Grundschutz eines Active Directory werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.68 *Fehlende oder unzureichende Planung des Active Directory*
- G 2.126 *Unzureichende Protokollierung von Änderungen am Active Directory*
- G 2.127 *Unzureichende Planung von Datensicherungsmethoden für Domänen-Controller*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.49 *Fehlerhafte Konfiguration des Active Directory*
- G 3.88 *Falsche Vergabe von Zugriffsrechten*
- G 3.89 *Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*

- G 4.13 *Verlust gespeicherter Daten*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.67 *Ausfall von Verzeichnisdiensten*
- G 4.68 *Störungen des Active Directory durch unnötige Dateireplizierung*

**Vorsätzliche Handlungen**

- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.65 *Verhinderung der Dienste eines Datenbanksystems*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.78 *DNS-Spoofing*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.144 *Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Vor allem ist aber zusätzlich der Baustein B 5.15 *Allgemeiner Verzeichnisdienst* anzuwenden, der allgemeine Empfehlungen für die generelle Absicherung von Verzeichnisdiensten enthält.

Voraussetzung für eine angemessene Absicherung der im Active Directory verarbeiteten Daten ist die entsprechende Absicherung des darunterliegenden Serverbetriebssystems. Die Absicherung der Microsoft-Windows-Server-Betriebssysteme ist nicht Teil dieses Bausteins, sondern wird in den entsprechenden Bausteinen der Schicht 3 behandelt. Daher sind in Abhängigkeit vom gewählten Betriebssystem der Baustein B 3.108 *Windows Server 2003* oder B 3.109 *Windows Server 2008* ebenfalls für den sicheren Betrieb eines Active Directory zu berücksichtigen.

Für den erfolgreichen Aufbau eines Active Directory sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Als Einstieg empfiehlt es sich zunächst die Maßnahme M 3.64 *Einführung in Active Directory* zu betrachten, die einen Überblick über die Aufbau und Begrifflichkeiten eines Active Directory bietet.

Vor der eigentlichen Einrichtung des Active Directory ist im Vorfeld die Organisationsstruktur der Institution zu ermitteln, um aus dieser eine möglichst optimale Konfiguration für das Active Directory ableiten zu können. Die Maßnahme M 2.229 *Planung des Active Directory* erläutert die Vorgehensweise in der Planungsphase und das Domänenkonzept des Active Directory.

M 2.230 *Planung der Active Directory-Administration* beschäftigt sich mit der Basisstruktur zur Verwaltung einer Domäne und vermittelt die Aufgaben und Anwendungen der einzelnen administrativen Rollen.

Die Maßnahme M 2.231 *Planung der Gruppenrichtlinien unter Windows* befasst sich mit den Gruppenrichtlinien für Windows Betriebssysteme, die auch mittels Active Directory verwaltet werden können. Des Weiteren wird der organisatorische Aufbau und die Rechteanpassung von administrativen Benutzerkonten in der Maßnahme M 2.411 *Trennung der Verwaltung von Diensten und Daten eines Active Directory* erläutert. Hieraus ergeben sich auch die Empfehlungen aus M 2.412 *Schutz der Authentisierung beim Einsatz von Active Directory*, wo Anpassungen zur Absicherungen des Verzeichnisdienstes vorgestellt werden.

Um den Integritätsschutz einer produktiv eingesetzten Active Directory-Umgebung durch die Sicherung der DNS-Komponenten gewährleisten zu können, ist die Maßnahme M 2.413 *Sicherer Einsatz von DNS für Active Directory* zu berücksichtigen. Darüber hinaus ist M 2.414 *Computer-Viren-Schutz für Domä-*

*nen-Controller* zu den spezifischen Besonderheiten für den Einsatz von Virenschutzprogramme auf Domänen-Controllern zu berücksichtigen.

**Beschaffung**

Nach Abschluss der konzeptionellen Planungsarbeiten und der Definition der Beschaffungskriterien für einen Server sollte in Abhängigkeit der Anzahl der zu beschaffenden Server und des ausgewählten Betriebssystems ein geeignetes Lizenzmodell ausgewählt werden. Fällt die Wahl auf Windows Server 2003, so bieten die Hilfsmittel zum IT-Grundschutz hierbei eine Unterstützung (siehe *Auswahl geeigneter Lizenzierungsmethoden für Windows XP/Server 2003* in *Hilfsmittel zum Windows Server 2003*).

**Umsetzung**

Um einen einheitlichen Sicherheitsstandard zu erhalten, ist die Maßnahme M 4.318 *Umsetzung sicherer Verwaltungsmethoden für Active Directory* zu beachten. Des Weiteren sind die für die Administration des Verzeichnisdienstes zuständigen Personen auf Basis M 3.27 *Schulung zur Active Directory-Verwaltung* mit den ihnen zugeteilten Aufgabenbereichen vertraut zu machen.

Aufgrund ihrer für die gesamte Netzumgebung zentralen Bedeutung ist für die Domänen-Controller eines Unternehmens ein ausreichender physikalischer Schutz sicherzustellen (siehe M 4.313 *Bereitstellung von sicheren Domänen-Controllern*). Um darüber hinaus den Sicherheitsstandard im Netz aufrecht erhalten zu können und Manipulationen der Domänen-Struktur und deren Domänen-Controllern zu verhindern, sind die in M 4.314 *Sichere Richtlinieneinstellungen für Domänen und Domänen-Controller* erwähnten Richtlinien entsprechend umzusetzen.

Unter Umständen ergibt sich bei der Umsetzung gleichzeitig eine Migration von bereits bestehenden Windows Verzeichnisdiensten. Die Maßnahme M 4.317 *Sichere Migration von Windows Verzeichnisdiensten* beschäftigt sich hierbei insbesondere mit der Verzeichnisdienst-Migration von bestehenden Windows-NT-Serversystemen.

**Betrieb**

Durch die Maßnahmen M 4.315 *Aufrechterhaltung der Betriebssicherheit von Active Directory* und M 4.316 *Überwachung der Active Directory Infrastruktur* soll sichergestellt werden, dass die relevanten Systeme des Informationsverbundes auf einem aktuellen Sicherheitsstand gehalten werden. Darüber hinaus ergeben sich durch die Relevanz der Domänen-Controller gesonderte Anforderungen an die Systemeinstellungen, welche in der Maßnahme M 4.138 *Konfiguration von Windows Server als Domänen-Controller* beschrieben sind.

Neben dem zugrunde liegenden Betriebssystem ist auch das Active Directory selbst sorgfältig zu administrieren (siehe M 4.315 *Aufrechterhaltung der Betriebssicherheit von Active Directory*). Um rechtzeitig bei aufkommenden Problemen reagieren zu können, sollte die entsprechende Maßnahme M 4.316 *Überwachung der Active Directory Infrastruktur* berücksichtigt werden. Diese befasst sich nicht nur mit den Rückmeldungen bei der Überschreitung definierter Schwellenwerte, sondern auch mit der Protokollierung durchgeführter Systemänderungen.

**Aussonderung**

Die zur geregelten Aussonderung eines Domänen-Controller zu berücksichtigen Aspekte werden in der Maßnahme M 2.410 *Geregelte Außerbetriebnahme eines Verzeichnisdienstes* näher beschrieben.

**Notfallvorsorge**

Aspekte der Notfallplanung für Active Directory wird in der Maßnahme M 6.108 *Datensicherung für Domänen-Controller* thematisiert.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Active Directory" vorgestellt:

**Planung und Konzeption**
- M 2.229 (A) *Planung des Active Directory*
- M 2.230 (A) *Planung der Active Directory-Administration*

- M 2.231 (A) *Planung der Gruppenrichtlinien unter Windows*
- M 2.411 (A) *Trennung der Verwaltung von Diensten und Daten eines Active Directory*
- M 2.412 (B) *Schutz der Authentisierung beim Einsatz von Active Directory*
- M 2.413 (C) *Sicherer Einsatz von DNS für Active Directory*
- M 2.414 (B) *Computer-Viren-Schutz für Domänen-Controller*
- M 3.64 (W) *Einführung in Active Directory*

**Umsetzung**

- M 3.27 (A) *Schulung zur Active Directory-Verwaltung*
- M 4.313 (A) *Bereitstellung von sicheren Domänen-Controllern*
- M 4.314 (A) *Sichere Richtlinieneinstellungen für Domänen und Domänen-Controller*
- M 4.317 (Z) *Sichere Migration von Windows Verzeichnisdiensten*
- M 4.318 (A) *Umsetzung sicherer Verwaltungsmethoden für Active Directory*
- M 5.89 (A) *Konfiguration des sicheren Kanals unter Windows*

**Betrieb**

- M 4.138 (A) *Konfiguration von Windows Server als Domänen-Controller*
- M 4.315 (A) *Aufrechterhaltung der Betriebssicherheit von Active Directory*
- M 4.316 (B) *Überwachung der Active Directory Infrastruktur*

**Aussonderung**

- M 2.410 (B) *Geregelte Außerbetriebnahme eines Verzeichnisdienstes*

**Notfallvorsorge**

- M 6.108 (C) *Datensicherung für Domänen-Controller*

# B 5.17 Samba


## Beschreibung

In diesem Baustein werden die grundsätzlichen Sicherheitseigenschaften von Samba betrachtet. Samba ist ein frei verfügbarer Authentisierungs-, Datei- und Druckdienst und ermöglicht Interoperabilität zwischen Microsoft Windows und der Unix-Welt. Samba führt eine Vielzahl unterschiedlicher Protokolle und Techniken zusammen. Dazu gehört beispielsweise das Server Message Block Protokoll (SMB), auch bekannt unter dem neueren Namen Common Internet File System (CIFS). Als Samba-Server werden Server bezeichnet, auf denen Samba als Authentisierungs-, Datei- und Druckdienst betrieben wird. Dies sind in der Regel Unix-Server.

Samba besteht aus mehreren Komponenten, die unterschiedliche Funktionen bereitstellen, von denen die wichtigsten im Folgenden kurz genannt werden. Die wichtigste Applikation bei Samba ist "smbd". Hierüber werden die Anmelde-, Datei- und Druckdienste für andere SMB-Clients bereitgestellt. Weiterhin sind noch die Applikation "nmbd", die verschiedene NetBIOS Namensdienste anbietet, und die Applikation "winbindd" zu nennen.

Dieser Baustein betrachtet Samba in der Version 3. Auf Unterschiede zwischen verschiedenen Unterversionsnummern der Version 3 wird, wenn nötig, explizit hingewiesen. Dieser Baustein ist auf jeden Server des betrachteten Informationsverbunds, auf dem Samba als Serverdienst betrieben wird, anzuwenden.

## Gefährdungslage

Für den IT-Grundschutz eines Samba-Servers werden folgende typische Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.143 *Informationsverlust beim Kopieren oder Verschieben von Daten auf Samba-Freigaben*
- G 2.144 *Unzureichende Notfall-Planung bei einem Samba-Server*
- G 2.145 *Unzureichende Sicherung von Trivial Database Dateien unter Samba*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.94 *Fehlkonfiguration der Samba-Kommunikationsprotokolle*
- G 3.95 *Fehlerhafte Konfiguration des Betriebssystems für einen Samba-Server*
- G 3.96 *Fehlerhafte Konfiguration eines Samba-Servers*

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*
- G 4.72 *Inkonsistenzen von Datenbanken im Trivial Database Format unter Samba*

**Vorsätzliche Handlungen**

- G 5.7 *Abhören von Leitungen*
- G 5.21 *Trojanische Pferde*
- G 5.28 *Verhinderung von Diensten*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Alle Sicherheitsüberlegungen zu einem Samba-Server sollten auf den in Baustein B 3.101 *Allgemeiner Server* enthaltenen Maßnahmen basieren. Da Samba in der Regel auf einem Unix-Betriebssystem eingesetzt wird, müssen auch die im Baustein B 3.102 *Server unter Unix* aufgeführten Maßnahmen berücksichtigt werden. Die in diesen Bausteinen beschriebenen allgemeinen Maßnahmen werden im vorliegenden Baustein konkretisiert und ergänzt.

**Planung und Konzeption**

Ist die allgemeine Planung des Servereinsatzes abgeschlossen, müssen Teilkonzepte für den Einsatz von Samba, unter Berücksichtigung aller geltenden übergeordneten Konzepte und Richtlinien, erstellt werden. Die generelle Vorgehensweise bei der Planung wird in M 2.315 *Planung des Servereinsatzes* erläutert. Während der Planung müssen unter anderem wichtige Entscheidungen über grundlegende Netzdienste (beispielsweise WINS) getroffen werden. In die Entscheidung hinsichtlich der Konzeption der Netzdienste sollten die in M 2.437 *Planung des Einsatzes eines Samba-Servers* angeführten Maßnahmen einfließen.

**Beschaffung**

Nach Abschluss der konzeptionellen Planungsarbeiten muss die Integrität und Authentizität der zur Installation zu verwendenden Pakete (Quelltext- oder Binärpakete) überprüft werden (siehe M 4.327 *Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen*).

**Umsetzung**

Bevor Samba auf dem Serverrechner installiert wird, muss zunächst das Betriebssystem geeignet konfiguriert und abgesichert werden (siehe M 4.331 *Sichere Konfiguration des Betriebssystems für einen Samba-Server*). Bei der eigentlichen Installation und der anschließenden Grundkonfiguration sind eine Reihe von Punkten zu beachten, die in M 4.330 *Sichere Installation eines Samba-Servers*, M 4.326 *Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver*, M 4.332 *Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server* und M 5.151 *Sichere Konfiguration des Samba Web Administration Tools* beschrieben werden. Außerdem sollte darauf geachtet werden, dass Samba keine unsicheren externen Programme einbindet (siehe M 2.438 *Sicherer Einsatz externer Programme auf einem Samba-Server*). Wie in M 2.437 *Planung des Einsatzes eines Samba-Servers* erwähnt, können unter Umständen auch die in M 4.333 *Sichere Konfiguration von Winbind unter Samba* erwähnten Maßnahmen relevant sein. Weiterhin sind die in M 4.329 *Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers* genannten Maßnahmen zu beachten.

Die Administratoren müssen für die sichere Installation und den sicheren Betrieb eines Samba-Servers geschult werden. Wichtige Aspekte, die eine solche Schulung abdecken sollte, sind in M 3.68 *Schulung der Administratoren eines Samba-Servers* beschrieben.

**Betrieb**

Im Regelbetrieb muss eine aktuelle Dokumentation gewährleistet sein. Weiterhin sind die in M 4.335 *Sicherer Betrieb eines Samba-Servers* beschriebene Aspekte zu beachten.

**Notfallvorsorge**

Spezielle Aspekte für einen Samba-Server, die zusätzlich zu M 6.96 *Notfallvorsorge für einen Server* berücksichtigt werden müssen, sind in M 6.135 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers* und M 6.136 *Erstellen eines Notfallplans für den Ausfall eines Samba-Servers* zusammengefasst.

Nachfolgend wird das Maßnahmenbündel für den Samba-Server vorgestellt. Die Maßnahmen aus anderen relevanten Bausteinen (beispielsweise M 6.96 *Notfallvorsorge für einen Server* aus B 3.101 *Allgemeiner Server*) werden aus Gründen der Übersichtlichkeit hier nicht noch einmal aufgeführt.

**Planung und Konzeption**
- M 2.437 (A) *Planung des Einsatzes eines Samba-Servers*
- M 4.147 (Z) *Sichere Nutzung von EFS unter Windows*
- M 4.326 (A) *Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver*

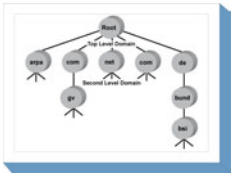
**Beschaffung**
- M 4.327 (C) *Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen*

**Umsetzung**
- M 2.438 (Z) *Sicherer Einsatz externer Programme auf einem Samba-Server*
- M 3.68 (B) *Schulung der Administratoren eines Samba-Servers*
- M 4.328 (A) *Sichere Grundkonfiguration eines Samba-Servers*
- M 4.329 (C) *Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers*
- M 4.330 (B) *Sichere Installation eines Samba-Servers*
- M 4.331 (C) *Sichere Konfiguration des Betriebssystems für einen Samba-Server*
- M 4.332 (A) *Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server*
- M 4.333 (C) *Sichere Konfiguration von Winbind unter Samba*
- M 4.334 (Z) *SMB Message Signing und Samba*
- M 5.151 (C) *Sichere Konfiguration des Samba Web Administration Tools*

**Betrieb**
- M 4.335 (B) *Sicherer Betrieb eines Samba-Servers*

**Notfallvorsorge**
- M 6.135 (B) *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers*
- M 6.136 (B) *Erstellen eines Notfallplans für den Ausfall eines Samba-Servers*

# B 5.18 DNS-Server



## Beschreibung

In diesem Baustein werden die grundsätzlichen Sicherheitseigenschaften des Domain Name System (DNS) und der hierfür benötigten Server betrachtet. DNS ist ein Netzdienst, um Hostnamen von IT-Systemen in IP-Adressen umzuwandeln. Im üblichen Fall wird zu einem Hostnamen die entsprechende IP-Adresse gesucht (Vorwärtsauflösung). Ist hingegen die IP-Adresse bekannt und der Hostname wird gesucht, wird dies als Rückwärtsauflösung bezeichnet. DNS kann mit einem Telefonbuch verglichen werden, dass Namen nicht in Telefonnummern, sondern in IP-Adressen auflöst. Dies stellt eine Vereinfachung für die Benutzer dar. Diese müssen statt schwer zu merkender Zahlen in Form von IP-Adressen nur den Hostnamen eines Rechners kennen, um eine Verbindung zu ihm aufzubauen. Welche Namen zu welchen IP-Adressen gehören, wird im Domain-Namensraum verwaltet. Dieser ist hierarchisch aufgebaut und wird von DNS-Servern zur Verfügung gestellt. DNS-Server verwalten den Domain-Namensraum im Internet, werden aber auch häufig im internen Netz der INstitution eingesetzt. Auf den Rechnern der Benutzer arbeiten sogenannte Resolver (Koordinatenumrechner), über die Anfragen an DNS-Server gestellt werden und die als Antwort Informationen über den Domain-Namensraum zurückliefern. Die Bezeichnung DNS-Server steht im eigentlichen Sinne für das verwendete Programm, wird jedoch meist auch als Synonym für den Rechner benutzt, auf dem dieses Programm betrieben wird.

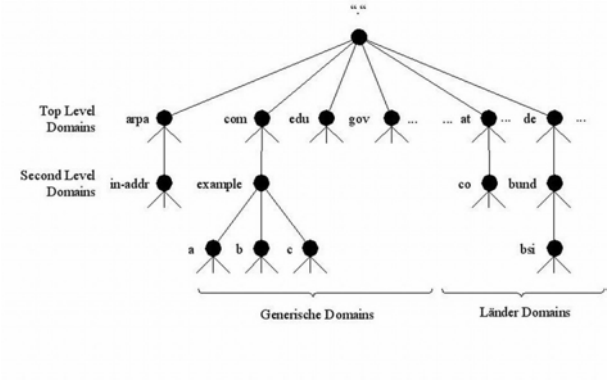



Abbildung: Domain-Namensraum

Das Internet ist eine öffentliche Umgebung, und auch Informationsverbünde betreiben IT-Systeme, die über das Internet erreichbar sein sollen, beispielsweise einen Webserver oder einen Mailserver. Um eine Internet-Verbindung herstellen zu können, wird DNS benötigt. Hierbei wird von dem Kommunikationspartner eine entsprechende DNS-Anfrage an einen DNS-Server gestellt. Dieser DNS-Server muss daher in diesem Fall aus dem öffentlichen Netz erreichbar sein und stellt damit ein öffentlich zugängliches IT-System dar. Eine sorgfältige Planung und fachgerechte Umsetzung ist für den reibungslosen Betrieb wichtig, denn eine funktionierende Namensauflösung ist für eine Vielzahl von Anwendungen ist eine Grundvoraussetzung. Aus diesem Grund liegt der Fokus des Bausteins auf der Verfügbarkeit und der Integrität von DNS-Servern, sowie auf Problemen, die im Zuge eines DNS-Server-Betriebs auftreten können.

In diesem Baustein werden die für einen DNS-Server spezifischen Gefährdungen und Maßnahmen beschrieben. Der Baustein ist dann anzuwenden, wenn in einem Informationsverbund DNS-Server betrieben werden. Um die Sicherheit von DNS-Servern zu gewährleisten, müssen weitere Bausteine umgesetzt werden.

## Gefährdungslage

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen als typisch im Zusammenhang mit einem DNS-Server angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.100 *Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen*
- G 2.152 *Fehlende oder unzureichende Planung des DNS-Einsatzes*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.103 *Fehlerhafte Domain-Informationen*
- G 3.104 *Fehlerhafte Konfiguration eines DNS-Servers*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*

**Vorsätzliche Handlungen**

- G 5.78 *DNS-Spoofing*
- G 5.151 *DNS-Flooding - Denial-of-Service*
- G 5.152 *DNS-Hijacking*
- G 5.153 *DNS-Amplification Angriff*
- G 5.154 *DNS Information Leakage*
- G 5.155 *Ausnutzen dynamischer DNS-Updates*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen grundsätzlich zu diesem Baustein weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Dies sind insbesondere der Baustein B 3.101 *Allgemeiner Server* und abhängig vom eingesetzten Betriebssystem die Bausteine B 3.102 *Server unter Unix*, B 3.106 *Server unter Windows 2000* oder B 3.108 *Windows Server 2003*.

Aufgrund dessen, dass zumindest ein Teil der betriebenen DNS-Server eines Informationsverbundes mit dem Internet kommuniziert, sind die Bausteine B 1.8 *Behandlung von Sicherheitsvorfällen* und Baustein B 3.301 *Sicherheitsgateway (Firewall)* zu beachten, um eine sichere Anbindung zu gewährleisten.

DNS-Server verwalten alle Namensinformationen eines Informationsverbunds und beinhalten somit Informationen über die gesamte Netzinfrastruktur. Aus diesem Grund sollte ein DNS-Server in einem Serverraum oder zumindest in einem abgesicherten Serverschrank aufgestellt werden, siehe dazu die korrespondierenden Bausteine B 2.4 *Serverraum* und B 2.7 *Schutzschränke*. Im Falle von Outsourcing ist zusätzlich Baustein B 1.11 *Outsourcing* zu beachten.

In diesem Baustein werden die für einen DNS-Server spezifischen Gefährdungen und Maßnahmen beschrieben.

**Planung und Konzeption**

Bevor mit der Auswahl der Software und der Planung der Infrastruktur begonnen werden kann, sollte geprüft werden, ob der gewünschte Domainname noch verfügbar ist. Da bei einer Registrierung die zuständigen DNS-Server angegeben werden müssen, sollte die Maßnahme M 2.298 *Verwaltung von Internet-Domainnamen* berücksichtigt werden. Ist der Einsatz von DNSSEC geplant, ist es von grundlegender Bedeutung, ein Konzept zur Verwaltung der kryptografischen Schlüsseln zu erstellen, wie es in M 2.46 *Geeignetes Schlüsselmanagement* beschrieben wird. Bei der Planung wird festgelegt, welche Domain-Informationen einen erhöhten Schutzbedarf haben. Im Weiteren muss entschieden werden, wie hoch die Leistungskapazität eines DNS-Servers sein muss. Dies betrifft einerseits das IT-System selbst, vor allem den Hauptspeicher, und andererseits die Bandbreite der Netzanbindung. Es sollte in diesem Zuge auch geplant werden, wie die DNS-Server in der Netzinfrastruktur des Informationsverbunds in-

tegriert werden (M 2.451 *Planung des DNS-Einsatzes*) und die Zugriffsrechte (M 2.8 *Vergabe von Zugriffsrechten*) vergeben werden. Das Ergebnis der planerischen Tätigkeiten muss schriftlich festgehalten werden.

**Beschaffung**

Es gibt unterschiedliche Softwareprodukte im Bereich der DNS-Server. Um eine geeignete Wahl zu treffen, müssen die potenziellen Produkte auf die Erfüllung benötigter Funktionalitäten und Sicherheit laut Planungsdokument analysiert werden (M 2.452 *Auswahl eines geeigneten DNS-Server-Produktes*).

**Umsetzung**

Abhängig vom gewählten DNS-Server müssen die Administratoren geschult werden (M 3.73 *Schulung der Administratoren eines DNS-Servers*). Durch die Schulung wird sicher gestellt, dass die zuständigen Administratoren mit den einzelnen Konfigurationsmöglichkeiten vertraut sind. Auf Basis der Schulung und einer ordentlichen Planung sollte eine sichere Konfiguration erarbeitet werden, die die Verfügbarkeit von DNS und die Integrität der gelieferten Informationen sicherstellt: M 4.350 *Sichere Grundkonfiguration eines DNS-Servers*, M 4.198 *Installation einer Applikation in einem chroot Käfig*, M 4.351 *Absicherung von Zonentransfers*, M 4.352 *Absicherung von dynamischen DNS-Updates*.

**Betrieb**

Während des laufenden Betriebs ist es wichtig, sich über aktuelle Sicherheitslücken zu informieren, um eventuell vorhandene Softwareaktualisierungen zu installieren oder anderweitige Sicherheitsvorkehrungen einzuführen, nachzulesen im Baustein B 1.14 *Patch- und Änderungsmanagement*. Im Weiteren sollte durch Paketfilterregeln die Kommunikation des DNS-Servers mit anderen DNS-Servern und Clients auf ein Minimum beschränkt werden (M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken*). Um einen reibungslosen Betrieb zu gewährleisten und eventuelle Störungen oder Anomalien festzustellen, sollte ein DNS-Server laufend überwacht werden (siehe M 4.354 *Überwachung eines DNS-Servers*).

Manuelle Änderungen an der Konfiguration bzw. an den DNS Informationen sollten nur nach vorheriger Sicherung der Domain-Informationen durchgeführt werden, um diese im Fehlerfall zurückspielen zu können, siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*.

**Aussonderung**

Werden DNS-Server außer Betrieb gesetzt, sollten diese geregelt entsorgt werden (siehe dazu M 2.453 *Aussonderung von DNS-Servern*).

**Notfallvorsorge**

Im Rahmen der Notfallvorsorge sollten Notfallpläne für die relevanten Gefährdungslagen erstellt werden (M 6.139 *Erstellen eines Notfallplans für DNS-Server*). Da DNS eine grundlegende Funktionalität für die Kommunikation über Netze zur Verfügung stellt, sollte überlegt werden, geeignete Redundanzsysteme bereit zu halten.

**Planung und Konzeption**
- M 2.298 (B) *Verwaltung von Internet-Domainnamen*
- M 2.450 (W) *Einführung in DNS-Grundbegriffe*
- M 2.451 (A) *Planung des DNS-Einsatzes*

**Beschaffung**
- M 2.176 (Z) *Geeignete Auswahl eines Internet Service Providers*
- M 2.452 (C) *Auswahl eines geeigneten DNS-Server-Produktes*

**Umsetzung**
- M 2.32 (Z) *Einrichtung einer eingeschränkten Benutzerumgebung*
- M 2.46 (A) *Geeignetes Schlüsselmanagement*
- M 3.73 (A) *Schulung der Administratoren eines DNS-Servers*
- M 4.95 (A) *Minimales Betriebssystem*
- M 4.97 (Z) *Ein Dienst pro Server*

- M 4.98 (A) *Kommunikation durch Paketfilter auf Minimum beschränken*
- M 4.198 (Z) *Installation einer Applikation in einem chroot Käfig*
- M 4.350 (A) *Sichere Grundkonfiguration eines DNS-Servers*
- M 4.351 (B) *Absicherung von Zonentransfers*
- M 4.352 (B) *Absicherung von dynamischen DNS-Updates*
- M 4.353 (Z) *Einsatz von DNSSEC*

**Betrieb**

- M 2.8 (A) *Vergabe von Zugriffsrechten*
- M 2.35 (B) *Informationsbeschaffung über Sicherheitslücken des Systems*
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.354 (B) *Überwachung eines DNS-Servers*
- M 5.118 (Z) *Integration eines DNS-Servers in ein Sicherheitsgateway*

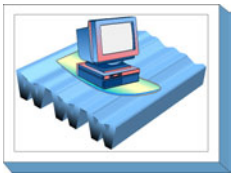
**Aussonderung**

- M 2.453 (C) *Aussonderung von DNS-Servern*

**Notfallvorsorge**

- M 6.139 (A) *Erstellen eines Notfallplans für DNS-Server*

# B 5.19 Internet-Nutzung



## Beschreibung

In den meisten Institutionen ist heute die Nutzung von Internet-Diensten am Arbeitsplatz selbstverständlich und notwendig. Hierzu gehören beispielsweise E-Mail, die Nutzung von Informationsangeboten und Internet-Dienstleistungen, Online-Banking, E-Commerce- und E-Government-Anwendungen. Je nach Art der Aufgaben und des Arbeitsplatzes kann zusätzlich die Nutzung von Instant Messaging, sozialen Netzwerken, Webkonferenzen und weiteren Diensten hinzukommen.

Die meisten Internet-Dienste können über Browser oder über andere Anwendungen heraus genutzt werden, die bereits in Standard-Betriebssystemen vorhanden sind. In einigen Einsatzszenarien wird für die Nutzung von Internet-Diensten spezielle Software benötigt wie beispielsweise für die Nutzung von Instant Messaging, für das Lesen von News oder das Online-Banking.

Dieser Baustein ist immer dann anzuwenden, wenn mit einem Browser oder spezieller Software auf das Internet zugegriffen werden soll (außer E-Mail). Der Baustein behandelt keine Netze und weiteren Verbindungen. Für diese sind die entsprechenden Bausteine anzuwenden. Die sichere Einbindung von E-Mail ist im Baustein B 5.3 *Groupware* beschrieben.

In diesem Baustein werden die für die Internet-Nutzung spezifischen Gefährdungen und Maßnahmen beschrieben. Darüber hinaus müssen für die sichere Anbindung an das Internet weitere Bausteine wie beispielsweise die entsprechenden Bausteine zu Netzen sowie B 3.301 *Sicherheitsgateway (Firewall)* und B 1.6 *Schutz vor Schadprogrammen* umgesetzt werden. Zur Absicherung der Clients ist der Baustein B 3.201 *Allgemeiner Client* sowie eventuell zusätzlich ein betriebssystem-spezifischer Baustein umzusetzen. Nicht in diesem Baustein betrachtet sind eigenständige Internet-PCs (siehe hierzu B 3.208 *Internet-PC*), die eine Sonderform der Internet-Nutzung bilden.

## Gefährdungslage

Für den IT-Grundschutz bei der Internet-Nutzung werden die folgenden typischen Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.10 *Ausfall eines Weitverkehrsnetzes*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*
- G 3.105 *Ungenehmigte Nutzung von externen Dienstleistungen*
- G 3.106 *Ungeeignetes Verhalten bei der Internet-Nutzung*
- G 3.107 *Rufschädigung*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.28 *Verhinderung von Diensten*
- G 5.42 *Social Engineering*

- G 5.48 *IP-Spoofing*
- G 5.78 *DNS-Spoofing*
- G 5.87 *Web-Spoofing*
- G 5.88 *Missbrauch aktiver Inhalte*
- G 5.156 *Bot-Netze*
- G 5.157 *Phishing und Pharming*
- G 5.158 *Missbrauch sozialer Netzwerke*
- G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die sichere Internet-Nutzung sollten in einem Unternehmen bzw. in einer Behörde im Hinblick auf die Informationssicherheit folgende Schritte durchlaufen werden:

**Planung und Konzeption**

Zu Anfang müssen grundsätzliche Fragen der Internet-Nutzung festgelegt werden, beispielsweise welche Internet-Dienste in der Institution genutzt werden sollen, wer welche Internet-Dienste nutzen darf, welche Regeln dabei zu beachten sind und wie die internen IT-Systeme, die das Internet nutzen dürfen, zu schützen sind (siehe M 2.457 *Konzeption für die sichere Internet-Nutzung*).

Für die sichere Internet-Nutzung muss eine verbindliche Richtlinie festgelegt werden, die beispielsweise umfasst, wer welche Internet-Dienste wann und wofür nutzen darf (siehe M 2.458 *Richtlinie für die Internet-Nutzung*). Für E-Mail ist ein eigener Baustein vorhanden, in dem eine Richtlinie für die E-Mail-Nutzung enthalten ist.

**Umsetzung**

Sowohl Benutzer als auch Administratoren haben einen wesentlichen Einfluss auf die sichere Internet-Nutzung. Benutzer und Administratoren müssen daher für den Umgang mit den eingesetzten IT-Komponenten bzw. die Nutzung der Internet-Dienste geschult werden (siehe M 3.77 *Sensibilisierung zur sicheren Internet-Nutzung*).

**Betrieb**

Je nach Sicherheitsanforderungen müssen die beteiligten IT-Komponenten unterschiedlich konfiguriert werden. Dies betrifft die Sicherheitsgateways und die Netzkoppel-Elemente, aber auch die Server und Clients. Bei den Clients ist insbesondere der verwendete Browser (siehe M 5.45 *Sichere Nutzung von Browsern* und M 5.155 *Datenschutz-Aspekte bei der Internet-Nutzung*), der E-Mail-Client (siehe dazu auch Baustein B 5.3 *Groupware*) und die Software für die genutzten Web-Applikationen abzusichern.

**Notfallvorsorge**

Da die Internet-Nutzung betriebskritisch sein kann, ist einem Ausfall vorzubeugen. Dazu müssen auch Ausweichverfahren für die Internet-Anwendungen feststehen (siehe M 6.141 *Festlegung von Ausweichverfahren bei der Internet-Nutzung*). Außerdem müssen Reaktionen auf durch die Internet-Nutzung verursachte Sicherheitsvorfälle festgelegt werden (siehe auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Internet-Nutzung" vorgestellt.

**Planung und Konzeption**

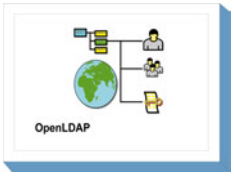
- M 2.457 (A) *Konzeption für die sichere Internet-Nutzung*
- M 2.458 (A) *Richtlinie für die Internet-Nutzung*
- M 2.459 (W) *Überblick über Internet-Dienste*
- M 5.66 (B) *Clientseitige Verwendung von SSL/TLS*
- M 5.69 (A) *Schutz vor aktiven Inhalten*

**Umsetzung**
- M 2.460 (C) *Geregelte Nutzung von externen Dienstleistungen*
- M 3.77 (A) *Sensibilisierung zur sicheren Internet-Nutzung*

**Betrieb**
- M 2.313 (A) *Sichere Anmeldung bei Internet-Diensten*
- M 3.78 (Z) *Korrektes Auftreten im Internet*
- M 5.45 (B) *Sichere Nutzung von Browsern*
- M 5.155 (Z) *Datenschutz-Aspekte bei der Internet-Nutzung*
- M 5.156 (Z) *Sichere Nutzung von Twitter*
- M 5.157 (Z) *Sichere Nutzung von sozialen Netzwerken*
- M 5.158 (Z) *Nutzung von Web-Speicherplatz*
- M 5.173 (Z) *Nutzung von Kurz-URLs und QR-Codes*

**Notfallvorsorge**
- M 6.141 (C) *Festlegung von Ausweichverfahren bei der Internet-Nutzung*

# B 5.20 OpenLDAP




## Beschreibung

In diesem Baustein werden die grundsätzlichen Sicherheitseigenschaften von OpenLDAP beschrieben. OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Benutzer oder Computer, in einer definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Benutzerverwaltungen.

OpenLDAP stellt eine Referenz-Implementierung für einen Server im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open Source Software steht OpenLDAP für eine Vielzahl von Betriebssystemen zur Verfügung.

### Abgrenzung des Bausteins

In diesem Baustein werden die für OpenLDAP spezifischen Gefährdungen und Maßnahmen betrachtet. Dabei wird die Version 2.4 von OpenLDAP zugrunde gelegt. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten befinden sich im Baustein B 5.15 *Allgemeiner Verzeichnisdienst*. Die dort beschriebenen Maßnahmen werden im vorliegenden Baustein konkretisiert und ergänzt. Der vorliegende Baustein ist auf jeden Server des betrachteten Informationsverbunds anzuwenden, auf dem der slapd-Daemon von OpenLDAP betrieben wird.

## Gefährdungslage

Für den IT-Grundschutz von OpenLDAP werden folgende typische Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.28 *Verstöße gegen das Urheberrecht*
- G 2.155 *Fehlende oder unzureichende Planung von OpenLDAP*

**Menschliche Fehlhandlungen**

- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.13 *Weitergabe falscher oder interner Informationen*
- G 3.88 *Falsche Vergabe von Zugriffsrechten*
- G 3.110 *Fehlerhafte Konfiguration von OpenLDAP*
- G 3.111 *Unzureichende Trennung von Offline- und Online-Zugriffen auf OpenLDAP*

**Technisches Versagen**

- G 4.10 *Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.67 *Ausfall von Verzeichnisdiensten*

**Vorsätzliche Handlungen**

- G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*

- G 5.20 *Missbrauch von Administratorrechten*
- G 5.21 *Trojanische Pferde*
- G 5.65 *Verhinderung der Dienste eines Datenbanksystems*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.78 *DNS-Spoofing*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.144 *Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um die mit OpenLDAP verarbeiteten Daten angemessen absichern zu können, muss das darunterliegende Serverbetriebssystem entsprechend geschützt sein. Dessen Absicherung ist nicht Teil dieses Bausteins, sondern wird in den entsprechenden Bausteinen der Schicht B 3 behandelt. Kommt beispielsweise Unix als Plattform zum Einsatz, ist der Baustein B 3.102 *Server unter Unix* zu berücksichtigen.

Für den sicheren Einsatz von OpenLDAP ist eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Ist die allgemeine Planung des Verzeichnisdienstes abgeschlossen, müssen Teilkonzepte für den Einsatz von OpenLDAP, unter Berücksichtigung aller geltenden übergeordneten Konzepte und Richtlinien, erstellt werden. Als Einstieg empfiehlt es sich, zunächst die Maßnahme M 3.85 *Einführung in OpenLDAP* zu betrachten, die einen Überblick über Aufbau und Begrifflichkeiten von OpenLDAP bietet. Die generelle Vorgehensweise wird in M 2.484 *Planung von OpenLDAP* erläutert. Während der Planung müssen unter anderem wichtige Entscheidungen über den Einsatz von Backends getroffen werden, siehe M 2.485 *Auswahl von Backends für OpenLDAP*. Bevor OpenLDAP eingerichtet wird, ist im Vorfeld eine spezifische Sicherheitsrichtlinie für OpenLDAP zu erstellen (siehe M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*).

**Beschaffung**

Nach Abschluss der konzeptionellen Planungsarbeiten muss die Integrität und Authentizität der zur Installation zu verwendenden Pakete (Quelltext- oder Binärpakete) überprüft werden (siehe M 4.382 *Auswahl und Prüfung der OpenLDAP-Installationspakete*).

**Umsetzung**

Bevor OpenLDAP auf einem IT-System installiert wird, muss zunächst dessen Betriebssystem geeignet konfiguriert und abgesichert werden. Außerdem müssen im Rahmen der Planung ermittelte notwendige Programme zur Unterstützung installiert sein. Bei der eigentlichen Installation und der anschließenden Grundkonfiguration sind eine Reihe von Punkten zu beachten, die in M 4.383 *Sichere Installation von OpenLDAP*, M 4.384 *Sichere Konfiguration von OpenLDAP*, M 4.385 *Konfiguration der durch OpenLDAP verwendeten Datenbank*, M 4.386 *Einschränkung von Attributen bei OpenLDAP*, M 4.387 *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*, M 4.388 *Sichere Authentisierung gegenüber OpenLDAP* sowie M 4.389 *Partitionierung und Replikation bei OpenLDAP* beschrieben werden.

Die sichere Installation von OpenLDAP ist kein einmaliger Vorgang. Statt dessen ist die Software, wie in der Maßnahme M 4.390 *Sichere Aktualisierung von OpenLDAP* beschrieben, auf einem aktuellen Stand zu halten.

Die Administratoren müssen für die sichere Installation und den sicheren Betrieb von OpenLDAP geschult werden. Wichtige Aspekte, die eine solche Schulung abdecken sollte, sind in M 3.86 *Schulung der Administratoren von OpenLDAP* beschrieben.

**Betrieb**

Im Regelbetrieb muss eine aktuelle Dokumentation gewährleistet sein. Weiterhin ist neben dem zugrunde liegenden Betriebssystem auch OpenLDAP selbst sorgfältig zu administrieren (siehe M 4.391 *Sicherer Betrieb von OpenLDAP*). Um aufkommende Probleme rechtzeitig erkennen zu können, sollte die entsprechende Maßnahme M 4.407 *Protokollierung beim Einsatz von OpenLDAP* berücksichtigt werden. Zum Schutz der Vertraulichkeit und der Integrität der übermittelten Daten ist außerdem stets eine gesicherte Kommunikation zwischen dem OpenLDAP-Server und den Clients aufrecht zu erhalten (siehe M 5.170 *Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP*).

**Aussonderung**

Aspekte, die bei der geregelten Aussonderung einer OpenLDAP-Installation zu berücksichtigen sind, werden in der Maßnahme M 2.410 *Geregelte Außerbetriebnahme eines Verzeichnisdienstes* näher beschrieben.

**Notfallvorsorge**

Aspekte der Notfallplanung für OpenLDAP werden in der Maßnahme M 6.106 *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes* thematisiert. Das Vorgehen zur Datensicherung bei OpenLDAP wird in M 6.150 *Datensicherung beim Einsatz von OpenLDAP* beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Baustein "OpenLDAP" vorgestellt:

**Planung und Konzeption**
- M 2.405 (A) *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*
- M 2.484 (A) *Planung von OpenLDAP*
- M 2.485 (A) *Auswahl von Backends für OpenLDAP*
- M 3.85 (W) *Einführung in OpenLDAP*

**Beschaffung**
- M 4.382 (C) *Auswahl und Prüfung der OpenLDAP-Installationspakete*

**Umsetzung**
- M 3.86 (A) *Schulung der Administratoren von OpenLDAP*
- M 4.383 (B) *Sichere Installation von OpenLDAP*
- M 4.384 (A) *Sichere Konfiguration von OpenLDAP*
- M 4.385 (B) *Konfiguration der durch OpenLDAP verwendeten Datenbank*
- M 4.386 (B) *Einschränkung von Attributen bei OpenLDAP*
- M 4.387 (A) *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*
- M 4.388 (B) *Sichere Authentisierung gegenüber OpenLDAP*
- M 4.389 (B) *Partitionierung und Replikation bei OpenLDAP*

**Betrieb**
- M 4.390 (C) *Sichere Aktualisierung von OpenLDAP*
- M 4.391 (B) *Sicherer Betrieb von OpenLDAP*
- M 4.407 (B) *Protokollierung beim Einsatz von OpenLDAP*
- M 5.170 (C) *Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP*

**Aussonderung**
- M 2.410 (B) *Geregelte Außerbetriebnahme eines Verzeichnisdienstes*

**Notfallvorsorge**
- M 6.150 (B) *Datensicherung beim Einsatz von OpenLDAP*

# B 5.21 Webanwendungen

## Beschreibung

Webanwendungen stellen Funktionen und dynamische Inhalte über das Internetprotokoll HTTP (*Hypertext Transfer Protocol*) bzw. HTTPS (HTTP über SSL bzw. TLS, d. h. geschützt durch eine verschlüsselte Verbindung) zur Verfügung. Dazu werden auf einem Server Dokumente und Benutzeroberflächen (z. B. Bedienelemente und Eingabemasken) erzeugt und an entsprechende Clientprogramme (Web-Browser) ausgeliefert.

Webanwendungen werden gewöhnlich auf der Grundlage von Frameworks entwickelt. Diese stellen ein Rahmenwerk für häufig wiederkehrende Aufgaben zur Verfügung (z. B. für Sicherheitskomponenten). Für eine Webanwendung werden häufig mehrere Frameworks für verschiedene Bereiche (z. B. Zugriff auf Datenbanken, Formatierung der Ausgaben) und Komponenten (z. B. Authentisierung, Session-Management) eingesetzt. Daher müssen bereits in der Planungsphase Sicherheitsaspekte bei der Auswahl der Frameworks sowie der Software-Architektur berücksichtigt werden.

Um eine Webanwendung zu betreiben, sind in der Regel mehrere IT-Systemkomponenten notwendig. Hierzu gehören üblicherweise ein Webserver zur Auslieferung der Daten, ein Applikationsserver für den Betrieb der Anwendung und zusätzliche Hintergrundsysteme, die als Datenquellen über unterschiedliche Schnittstellen angebunden sind (z. B. Datenbank oder Verzeichnisdienst).

Webanwendungen werden sowohl in öffentlichen IT-Netzen (z. B. dem Internet) als auch in Firmennetzen (Intranet) zur Bereitstellung von Daten und Anwendungen eingesetzt. Dabei müssen Webanwendungen Sicherheitsmechanismen umsetzen, die den Schutz der Daten gewährleisten und Missbrauch verhindern.

Typische Sicherheitskomponenten bzw. -mechanismen einer Webanwendung sind:

- Authentisierung
  Für den Zugriff auf geschützte Ressourcen der Webanwendung müssen sich die Benutzer gegenüber der Authentisierungskomponente ausweisen (z. B. durch Zugangsdaten).
- Autorisierung
  Vor dem Zugriff auf geschützte Ressourcen und Funktionen muss geprüft werden, ob die Benutzer über ausreichend Rechte verfügen.
- Ein- und Ausgabevalidierung
  Ein- und Ausgabedaten müssen geprüft und gefiltert werden, damit die Verarbeitung von schadhaften Daten (z. B. ausführbarer Schadcode) vermieden wird.
- Session-Management
  Da das Internetprotokoll HTTP keine Zuordnung zusammengehörender Anfragen zu einem Benutzer unterstützt, erfolgt diese Zuordnung durch das Session-Management der Webanwendung.
- Fehlerbehandlung
  Auftretende Fehler müssen so behandelt werden, dass die Daten der Webanwendung auch im Fehlerfall geschützt werden.
- Protokollierung
  Ereignisse müssen von der Webanwendung derart erfasst werden, dass durchgeführte Aktionen und sicherheitsrelevante Vorfälle auch zu einem späteren Zeitpunkt nachvollzogen werden können.

### Abgrenzung des Bausteins

In diesem Baustein werden die für Webanwendungen spezifischen Gefährdungen und Maßnahmen betrachtet. Während Webserver die Webseiten ausliefern (siehe auch B 5.4 *Webserver*), stellen Webanwendungen Funktionen zur Verfügung und bereiten dynamische Inhalte zur Auslieferung durch den Webserver vor. Der Baustein B 5.4 *Webserver* beinhaltet auch die redaktionelle Planung des Webauftritts sowie das Notfallmanagement, das deshalb in diesem Baustein nicht nochmals behandelt wird.

Da Web-Services ähnlich wie Webanwendungen Geschäftslogik abbilden, lässt sich ein Großteil der Gefährdungen und Maßnahmen von Webanwendungen auch auf die Logik-Komponenten von Web-Services übertragen.

Bei herkömmlichen Webanwendungen werden Funktionalitäten innerhalb dieser Anwendung angeboten. Im Gegensatz dazu werden diese bei SOAP-basierten Web Services (*Simple Object Access Protocol*) als lose gekoppelte, unabhängige, austauschbare Dienste über standardisierte Schnittstellen von einem Service Provider angeboten. Anders als Webanwendungen bereiten Web-Services üblicherweise die Ausgabe von Ergebnissen nicht für einen Browser auf, sondern stellen sie in strukturierter, maschinenlesbarer Form (z. B. SOAP-Nachrichten) zur weiteren automatisierten Verarbeitung zur Verfügung. Dabei werden diese Daten durch unterschiedliche Komponenten des Web-Service (z. B. durch einen Parser oder durch Ver- und Entschlüsselungskomponenten) aufbereitet. Die sicherheitsrelevanten Aspekte bei der Realisierung einer Service-orientierten Architektur (SOA) werden im vorliegenden Baustein nicht betrachtet.

## Gefährdungslage

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen als typisch im Zusammenhang mit einer Webanwendung angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.157 *Mangelhafte Auswahl oder Konzeption von Webanwendungen*
- G 2.158 *Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services*
- G 2.159 *Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services*

**Menschliche Fehlhandlungen**

- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.84 *Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services*
- G 4.85 *Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services*
- G 4.86 *Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen*
- G 4.87 *Offenlegung vertraulicher Informationen bei Webanwendungen*

**Vorsätzliche Handlungen**

- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.28 *Verhinderung von Diensten*
- G 5.87 *Web-Spoofing*
- G 5.88 *Missbrauch aktiver Inhalte*

- G 5.131 *SQL-Injection*
- G 5.165 *Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services*
- G 5.166 *Missbrauch einer Webanwendung durch automatisierte Nutzung*
- G 5.167 *Fehler in der Logik von Webanwendungen und Web-Services*
- G 5.168 *Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services*
- G 5.169 *Unzureichendes Session-Management von Webanwendungen und Web-Services*
- G 5.170 *Cross-Site Scripting (XSS)*
- G 5.171 *Cross-Site Request Forgery (CSRF, XSRF, Session Riding)*
- G 5.172 *Umgehung der Autorisierung bei Webanwendungen und Web-Services*
- G 5.173 *Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services*
- G 5.174 *Injection-Angriffe*
- G 5.175 *Clickjacking*

**Maßnahmenempfehlungen**

Um Webanwendungen abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Der Betrieb einer Webanwendung setzt den Einsatz weiterer Komponenten voraus. Daher muss der Baustein B 3.101 *Allgemeiner Server* und abhängig von dem eingesetzten Betriebssystem beispielsweise Baustein B 3.102 *Server unter Unix* oder B 3.108 *Windows Server 2003* berücksichtigt werden. Darüber hinaus wird für den Betrieb einer Webanwendung ein Webserver (siehe B 5.4 *Webserver*) benötigt.

Funktionalität oder Daten werden bei Webanwendungen gewöhnlich in Hintergrundsystemen ausgelagert (z. B. Datenbank und Identitätsspeicher). Aus diesem Grund sind in Abhängigkeit der eingesetzten Hintergrundsysteme weitere Bausteine, wie beispielsweise B 5.7 *Datenbanken* und B 5.15 *Allgemeiner Verzeichnisdienst* (bzw. B 5.16 *Active Directory*), zu berücksichtigen.

Verarbeitet die Webanwendung personenbezogene Daten oder wertet sie Nutzerdaten aus (z. B. Abrufstatistiken, Benutzerprofile), muss zusätzlich Baustein B 1.5 *Datenschutz* beachtet werden.

Wird die Webanwendung von externen Dienstleistern betrieben oder entwickelt, ist zusätzlich der Baustein B 1.11 *Outsourcing* zu betrachten.

Für eine sichere Webanwendung sind eine Reihe von Maßnahmen umzusetzen. Die zu durchlaufenden Phasen, sowie die Maßnahmen, die in den jeweiligen Phasen zu beachtet sind, werden im Folgenden aufgeführt.

**Planung und Konzeption**

Bei der Planung einer Webanwendung muss üblicherweise entschieden werden, ob die Anforderungen an die Webanwendung durch Standardprodukte abgedeckt werden können oder eine Eigenentwicklung notwendig ist. Wird eine Webanwendung auf Basis von Standardsoftware umgesetzt, so sind gewöhnlich Anpassungen erforderlich, die über reine Konfigurationsänderungen hinausgehen und oft auch Entwicklungsarbeiten mit einschließen. Daher müssen auch Webanwendungen, die auf Standardsoftware basieren, häufig die Vorgaben an die Entwicklung und Erweiterung von Webanwendungen erfüllen (siehe M 2.487 *Entwicklung und Erweiterung von Anwendungen*).

Bereits in der Entwurfsphase einer Webanwendung müssen Sicherheitsaspekte beachtet werden, um die zu verarbeitenden Daten zu schützen (siehe M 5.169 *Systemarchitektur einer Webanwendung*). Hierbei müssen auch die Integration der Hintergrundsysteme (z. B. Datenbank) und deren sichere Anbindung miteinbezogen werden (siehe M 5.168 *Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services*).

Werden personenbezogene Daten von Webanwendungen verarbeitet, aufgezeichnet oder ausgewertet (z. B. Nutzerverhalten), sind die rechtlichen Rahmenbedingungen bei der Planung von techni-

schen Lösungen zu berücksichtigen (siehe M 2.110 *Datenschutzaspekte bei der Protokollierung* und M 2.488 *Web-Tracking*).

**Beschaffung**

Soll eine Webanwendung mit verfügbarer Standardsoftware realisiert werden, muss ein passendes Produkt ausgewählt werden (siehe M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*).

**Umsetzung**

Vor der Übernahme einer Webanwendung in den Wirkbetrieb müssen die Sicherheitsfunktionen konfiguriert oder entwickelt werden. Die dafür umzusetzenden Komponenten müssen die Webanwendung vor bekannten Bedrohungen und Angriffstechniken schützen (siehe z. B. M 2.363 *Schutz gegen SQL-Injection*).

Darüber hinaus sind die kontextbezogene Validierung und Filterung der Daten (siehe M 4.392 *Authentisierung bei Webanwendungen*) und der Schutz von Benutzer-Sitzungen durch das Session-Management (siehe M 4.394 *Session-Management bei Webanwendungen und Web-Services*) wesentliche Sicherheitskomponenten einer Webanwendung.

**Betrieb**

Nachdem eine Webanwendung das Abnahme- und Freigabeverfahren erfolgreich durchlaufen hat und betriebsbereit konfiguriert wurde, kann der Regelbetrieb aufgenommen werden.

Insbesondere bei der Nutzung der Webanwendung über öffentliche Netze (z. B. Internet) besteht die Gefahr, dass bekannt gewordene Schwachstellen ausgenutzt werden. Daher müssen Prozesse definiert werden, um das angestrebte Sicherheitsniveau der Webanwendung dauerhaft aufrecht erhalten zu können (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* und M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

Es muss sichergestellt werden, dass von Webanwendungen übermittelte Daten keine sicherheitsrelevanten Informationen beinhalten, die einem Angreifer Hinweise zur Umgehung von Sicherheitsmechanismen geben (siehe M 4.400 *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*).

Für den hohen Schutzbedarf sind Penetrationstests auf die Webanwendung durchzuführen, um das Sicherheitsniveau der Webanwendung zu überprüfen und mögliche Schwachstellen schnell abzustellen (M 5.150 *Durchführung von Penetrationstests*).

Nachfolgend werden die Maßnahmen für Webanwendungen vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier aus Gründen der Redundanz verzichtet.

**Planung und Konzeption**

- M 2.1 (A) *Festlegung von Verantwortlichkeiten und Regelungen*
- M 2.11 (A) *Regelung des Passwortgebrauchs*
- M 2.63 (A) *Einrichten der Zugriffsrechte*
- M 2.80 (A) *Erstellung eines Anforderungskatalogs für Standardsoftware*
- M 2.363 (B) *Schutz gegen SQL-Injection*
- M 2.486 (A) *Dokumentation der Architektur von Webanwendungen und Web-Services*
- M 2.487 (B) *Entwicklung und Erweiterung von Anwendungen*
- M 2.488 (W) *Web-Tracking*
- M 4.176 (B) *Auswahl einer Authentisierungsmethode für Webangebote*
- M 4.404 (A) *Sicherer Entwurf der Logik von Webanwendungen*
- M 5.168 (A) *Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services*
- M 5.169 (A) *Systemarchitektur einer Webanwendung*
- M 5.177 (B) *Serverseitige Verwendung von SSL/TLS*

**Beschaffung**

- M 2.62 (B) *Software-Abnahme- und Freigabe-Verfahren*

**Umsetzung**

- M 4.392 (A) *Authentisierung bei Webanwendungen*
- M 4.393 (B) *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*
- M 4.394 (A) *Session-Management bei Webanwendungen und Web-Services*
- M 4.395 (B) *Fehlerbehandlung durch Webanwendungen und Web-Services*
- M 4.396 (B) *Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen*
- M 4.398 (B) *Sichere Konfiguration von Webanwendungen*
- M 4.399 (A) *Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen*
- M 4.400 (B) *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*
- M 4.401 (B) *Schutz vertraulicher Daten bei Webanwendungen*
- M 4.402 (A) *Zugriffskontrolle bei Webanwendungen*
- M 4.403 (C) *Verhinderung von Cross-Site Request Forgery (CSRF, XSRF, Session Riding)*
- M 4.405 (C) *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*
- M 4.406 (Z) *Verhinderung von Clickjacking*

**Betrieb**

- M 2.8 (A) *Vergabe von Zugriffsrechten*
- M 2.31 (A) *Dokumentation der zugelassenen Benutzer und Rechteprofile*
- M 2.34 (A) *Dokumentation der Veränderungen an einem bestehenden System*
- M 2.35 (B) *Informationsbeschaffung über Sicherheitslücken des Systems*
- M 2.64 (A) *Kontrolle der Protokolldateien*
- M 2.110 (A) *Datenschutzaspekte bei der Protokollierung*
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 3.5 (A) *Schulung zu Sicherheitsmaßnahmen*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.397 (C) *Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services*
- M 5.150 (Z) *Durchführung von Penetrationstests*

# B 5.22 Protokollierung

## Beschreibung

Unter Protokollierung beim Betrieb von IT-Systemen ist die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst beziehungsweise worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?" Für einen verlässlichen IT-Betrieb sollten sicherheitskritische Ereignisse im Informationsverbund protokolliert werden. Ziel der Protokollierung ist es, wesentliche Veränderungen an IT-Systemen und Anwendungen nachvollziehen zu können, um deren Sicherheit nachvollziehen zu können. Eine Protokollierung wird in vielen Informationsverbünden eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe zeitnah entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Dienste können anhand von Protokolldaten nachvollzogen werden.

Protokollierung kann lokal oder zentral durchgeführt werden. Um einen Gesamtüberblick über einen Informationsverbund zu erhalten, kann ein zentraler Protokollierungsserver eingesetzt werden, der die unterschiedlichen Protokolldaten zusammenführt, diese analysiert und überwacht. So lassen sich durch die Analyse und Korrelation von Daten beispielsweise Angriffe, die auf mehrere Systeme ausgeführt werden, erkennen.

Einige typische Anwendungsbeispiele für eine zentrale Protokollierung sind:

- Sammlung von Meldungen der Sicherheitsgateways hinsichtlich geblockter Verbindungsversuche
- Zentraler Anlaufpunkt für Warnmeldungen, wenn Massenspeicherquotas überschritten werden
- Archiv für forensische Ermittlungen, nachdem ein Angriff auf IT-Systeme bekannt wurde

Dieser Baustein betrachtet alle spezifischen Gefährdungen und Maßnahmen, die in einem Informationsverbund unabhängig von den eingesetzten Betriebssystemen für eine angemessene Protokollierung und Überwachung relevant sind. Der Aufwand zur Erstellung und Umsetzung eines solchen Prozesses ist nicht gering. Daher sollte dieser Baustein vor allem bei größeren Informationsverbünden umgesetzt werden und wenn in einem Informationsverbund zentral protokolliert werden soll. Bei kleineren und weniger komplexen Informationsverbünden reicht unter Umständen die Umsetzung von M 2.500 *Protokollierung von IT-Systemen* aus.

## Gefährdungslage

Für den IT-Grundschutz bei der Protokollierung werden die folgenden typischen Gefährdungen betrachtet.

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.61 *Unberechtigte Sammlung personenbezogener Daten*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.160 *Fehlende oder unzureichende Protokollierung*
- G 2.161 *Vertraulichkeits- und Integritätsverlust von Protokolldaten*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*

- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.114 *Fehlerhafte Administration bei der Protokollierung*
- G 3.115 *Fehlerhafte Auswahl von relevanten Protokolldaten*
- G 3.116 *Fehlende Zeitsynchronisation bei der Protokolldatenauswertung*

**Technisches Versagen**

- G 4.89 *Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung*

**Vorsätzliche Handlungen**

- G 5.20 *Missbrauch von Administratorrechten*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.85 *Integritätsverlust schützenswerter Informationen*
- G 5.143 *Man-in-the-Middle-Angriff*
- G 5.176 *Kompromittierung der Protokolldatenübertragung bei zentraler Protokollierung*

**Maßnahmenempfehlungen**

Um die Sicherheit des betrachteten Informationsverbundes gewährleisten zu können, müssen zusätzlich zu diesem Baustein noch weitere Bausteine, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz, umgesetzt werden.

Die genutzten Protokollierungsdienste können sowohl bereits in ein Betriebssystem integriert sein als auch in eigenständigen Software-Komponenten angeboten werden. Um den Protokollierungsdienst und die gespeicherten Protokolldaten abzusichern, muss die Sicherheit des zugrunde liegenden Betriebssystems gewährleistet werden. Dies ist jedoch nicht Bestandteil dieses Bausteins. Dafür sind die betriebssystem-spezifischen Bausteine der Schicht 3 umzusetzen, vor allem B 3.101 *Allgemeiner Server* und B 3.201 *Allgemeiner Client*.

Für eine erfolgreiche Protokollierung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb der Komponenten. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Um eine Protokollierung in einem Informationsverbund zu realisieren, muss geplant werden, wie diese technisch und organisatorisch aufgebaut wird (siehe M 2.499 *Planung der Protokollierung* und M 2.500 *Protokollierung von IT-Systemen*). Ebenso Bestandteil der Planung ist, wie ein Sicherheitskonzept erstellt werden kann (siehe M 2.497 *Erstellung eines Sicherheitskonzepts für die Protokollierung*) und wie die Zugriffsrechte auf Protokollierungsdienste und Protokolldaten vergeben werden (siehe M 2.8 *Vergabe von Zugriffsrechten*).

Bei zentraler Protokollierung muss überlegt werden, wie der zentrale Protokollierungsserver in die Netzinfrastruktur des Informationsverbundes integriert werden kann (siehe M 2.499 *Planung der Protokollierung* und M 3.90 *Allgemeine Grundlagen für die zentrale Protokollierung*).

**Umsetzung**

Die zuständigen Administratoren müssen in den entsprechenden Verfahren geschult werden, insbesondere für den sicheren Betrieb eines zentralen Protokollierungsservers. Dies wird in M 3.89 *Schulung zur Administration der Protokollierung* beschrieben. Des Weiteren ist für einen effektiven Betrieb einer IT-Frühwarnung entscheidend, dass bei aufgetretenen Sicherheitsvorfällen unverzüglich ein Alarm ausgelöst wird. Hierbei muss festgelegt werden, wer, wann und wie benachrichtigt wird und über welche Meldewege alarmiert werden soll (siehe M 6.151 *Alarmierungskonzept für die Protokollierung*).

**Betrieb**

Die gesammelten Protokollinformationen können lokal oder an einem zentralen Protokollierungsserver ausgewertet werden (siehe M 4.430 *Analyse von Protokolldaten*). Im Fall einer zentralen Analyse müssen die Protokollinformationen über das Netz an einen zentralen Server übertragen werden. Hierbei ist die Kommunikation zwischen den beteiligten IT-Systemen ausreichend abzusichern (siehe M 5.171 *Si-*

*chere Kommunikation zu einem zentralen Protokollierungsserver*). Bevor die Protokolldaten effizient ausgewertet werden können, müssen diese zuerst entsprechend vorbereitet werden (siehe M 4.431 *Auswahl und Verarbeitung relevanter Informationen für die Protokollierung*).

**Aussonderung**

Werden Festplatten aus Protokollierungsservern entsorgt oder gelöscht, ist darauf zu achten, dass vertrauliche und personenbezogene Daten vollständig gelöscht werden. Weitere Informationen hierzu sind in der Maßnahme M 2.496 *Geregelte Außerbetriebnahme eines Protokollierungsservers* zu finden.

**Notfallvorsorge**

Im Rahmen der Notfallvorsorge sollten Notfallpläne für die relevanten Gefährdungslagen erstellt werden (siehe M 6.96 *Notfallvorsorge für einen Server*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Protokollierung" vorgestellt.

**Planung und Konzeption**
- M 2.1 (A) *Festlegung von Verantwortlichkeiten und Regelungen*
- M 2.497 (A) *Erstellung eines Sicherheitskonzepts für die Protokollierung*
- M 2.499 (A) *Planung der Protokollierung*
- M 2.500 (A) *Protokollierung von IT-Systemen*
- M 3.90 (W) *Allgemeine Grundlagen für die zentrale Protokollierung*
- M 5.66 (B) *Clientseitige Verwendung von SSL/TLS*
- M 5.68 (Z) *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*
- M 5.177 (B) *Serverseitige Verwendung von SSL/TLS*

**Umsetzung**
- M 2.498 (C) *Behandlung von Warn- und Fehlermeldungen*
- M 3.10 (A) *Auswahl eines vertrauenswürdigen Administrators und Vertreters*
- M 3.89 (A) *Schulung zur Administration der Protokollierung*
- M 6.151 (A) *Alarmierungskonzept für die Protokollierung*

**Betrieb**
- M 2.8 (A) *Vergabe von Zugriffsrechten*
- M 2.64 (A) *Kontrolle der Protokolldateien*
- M 2.110 (A) *Datenschutzaspekte bei der Protokollierung*
- M 4.225 (Z) *Einsatz eines Protokollierungsservers in einem Sicherheitsgateway*
- M 4.227 (C) *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*
- M 4.430 (A) *Analyse von Protokolldaten*
- M 4.431 (A) *Auswahl und Verarbeitung relevanter Informationen für die Protokollierung*
- M 5.9 (B) *Protokollierung am Server*
- M 5.171 (A) *Sichere Kommunikation zu einem zentralen Protokollierungsserver*
- M 5.172 (A) *Sichere Zeitsynchronisation bei der zentralen Protokollierung*

**Aussonderung**
- M 2.167 (B) *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*
- M 2.496 (A) *Geregelte Außerbetriebnahme eines Protokollierungsservers*

**Notfallvorsorge**
- M 6.96 (A) *Notfallvorsorge für einen Server*

# B 5.23 Cloud Management

## Beschreibung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste (skalierbare) Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle.

Der Baustein Cloud Management wendet sich an Cloud-Diensteanbieter (Cloud Service Provider). Dabei macht es keinen Unterschied, ob sie ihre Cloud-Dienste (Cloud Services) intern (Private Cloud) oder extern (Public Cloud) anbieten und welches Servicemodell (Infrastructure as a Service, Platform as a Service oder Software as a Service) sie gewählt haben.

Eine wesentliche Aufgabe des Cloud-Diensteanbieters ist das Cloud Management, also Bereitstellung, Verwaltung und Betrieb der angebotenen Cloud-Dienste (Cloud Services).

Um die Betriebsprozesse des Cloud Managements zu beschreiben, wird ein Cloud Computing Referenzmodell genutzt, das die wesentlichen Aspekte des Cloud Computings abdeckt. Dem Baustein liegt das Referenzmodell (Cloud Reference Framework) der Internet Engineering Task Force (IETF) zugrunde, das bei der Erstellung des Bausteins als sogenannter Internet-Draft vorliegt.

Das Referenzmodell ist in Schichten für Cloud-Dienste, Virtualisierung (virtuelle Maschinen, in denen die Cloud-Dienste laufen) und physische Komponenten (als Träger der virtuellen Maschinen) aufgebaut und beschreibt deren Zusammenwirken. Diese Schichten werden als *horizontale* Schichten bezeichnet.

Übergreifend zu diesen Schichten führt das Referenzmodell das Cloud Management als *vertikale* Schicht ein, die alle horizontalen Schichten betrifft. Insbesondere zählt *Security* (also Sicherheitsmanagement und Sicherheitsmaßnahmen) zum Cloud Management.

Zu den typischen Aufgaben eines Cloud Diensteanbieters im Cloud Management zählen:

- die Bereitstellung eines Dienste-Katalogs mit der Beschreibung der angebotenen Cloud-Dienste;
- die Provisionierung (Bereitstellung) bzw. De-Provisionierung von Cloud-Ressourcen (hierzu zählen: virtuelle Maschinen, virtuelle Datenspeicher, virtuelle Netze) und Cloud-Diensteprofilen (definierte Konfigurationen für Cloud-Ressourcen, mit deren Hilfe die angebotenen Dienste bereitgestellt werden);
- die Zuweisung der physischen und virtuellen Ressourcen zu den Cloud-Benutzern (engl.: cloud service user) und die Konfiguration dieser Ressourcen;
- das Zugangs- und Zugriffsmanagement für die Cloud-Ressourcen und die Authentisierung von Zugang und Zugriff;
- die Überwachung der bereitgestellten Cloud-Dienste und -Ressourcen, um die vereinbarte Dienstgüte einzuhalten;
- die für den Kunden nachvollziehbare Abrechnung der in Anspruch genommenen Cloud-Dienste (anhand des Dienste-Katalogs).

Das Cloud Management und die hierfür notwendigen Prozesse werden in der Wissensmaßnahme M 4.446 *Einführung in das Cloud Management* beschrieben.

Das Cloud Management besteht nicht nur aus Tätigkeiten, die nur oder speziell beim Cloud Computing anfallen, sondern auch aus denen, die allgemein zum Management des IT-Betriebs oder von IT-Dienstleistungen gehören. Insbesondere sind dies:

- Sicherheitsmanagement,
- Störungsmanagement,
- System- und Anwendungsmanagement,
- Netzmanagement,

- Aussonderung von Komponenten und sichere Löschung/Vernichtung,
- Notfallvorsorge.

**Thematische Abgrenzung**

Das Ziel des vorliegenden Bausteins ist es, Empfehlungen für sichere Bereitstellung, Verwaltung und Betrieb von Cloud-Diensten zu geben. Es werden sinnvolle und angemessene Sicherheitsanforderungen an das Cloud Management beschrieben, die einen Schutz der bereitgestellten Dienste und zugrunde liegenden Informationen, Anwendungen und Systeme aus der "Wolke" heraus gewährleisten.

Der Baustein benennt konkrete und detaillierte Gefährdungen und Maßnahmen für das Cloud Management. Wo sich Cloud Management mit dem allgemeinen Management von IT-Betrieb und IT-Dienstleistungen überschneidet (siehe oben), beschränkt er sich auf die Anteile, die spezifisch für Cloud Computing sind.

Im Mittelpunkt des Bausteins Cloud Management stehen somit die Sicherheitsaspekte, die mit den originären Eigenschaften von Cloud Computing in Verbindung stehen wie beispielsweise Mandantenfähigkeit (engl.: multi-tenancy), *Orchestrierung* und Automatisierung von Prozessen sowie Provisionierung und De-Provisionierung von IT-Ressourcen.

Vorrangig richten sich die Gefährdungen und Maßnahmen dieses Bausteins an Cloud-Diensteanbieter, die Private Cloud Services für Unternehmen und Behörden bereitstellen. Die grundsätzlichen Sicherheitsempfehlungen sind ebenso für Public Cloud Services und hybride Cloud-Angebote (gemeinsame Nutzung von mehreren Cloud-Infrastrukturen über standardisierte Schnittstellen) anwendbar, wobei hier zusätzlich der Baustein *Cloud-Nutzung* beachtet werden muss.

Sicherheitsmaßnahmen, mit denen Cloud-Anwendungen selbst abgesichert werden können, sind nicht Gegenstand dieses Bausteins, sondern werden in den Bausteinen B 5.21 *Webanwendungen* und B 5.24 *Web-Services* beschrieben. Sicherheitsaspekte, die bei der Nutzung von Cloud-Diensten relevant sind, werden ebenfalls nicht im vorliegenden Baustein betrachtet. Hier sei auf den Baustein B 1.17 *Cloud-Nutzung* verwiesen. Der Baustein behandelt auch nicht die Absicherung der zugrunde liegenden IT-Systeme (virtuelle und physische) und Anwendungen sowie deren Verwaltung. Auch hierfür wird auf die entsprechenden Bausteine verwiesen, z. B. für Virtualisierung, Netzmanagement und Speicherlösungen.

## Gefährdungslage

Für das Cloud Management werden für den IT-Grundschutz die folgenden typischen Gefährdungen angenommen:

**Organisatorische Mängel**

- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.137 *Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen*
- G 2.160 *Fehlende oder unzureichende Protokollierung*
- G 2.175 *Unzureichende Isolation und Trennung von Cloud-Ressourcen*
- G 2.176 *Mangelnde Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender*
- G 2.177 *Fehlplanung von Cloud-Diensteprofilen*
- G 2.178 *Unzureichendes Notfallmanagement beim Cloud-Diensteanbieter*
- G 2.179 *Fehlende Herstellerunterstützung bei der Bereitstellung von Cloud-Diensten*
- G 2.180 *Fehlerhafte Provisionierung und De-Provisionierung von Cloud-Diensten*

**Menschliche Fehlhandlungen**

- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.36 *Fehlinterpretation von Ereignissen*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.114 *Fehlerhafte Administration bei der Protokollierung*

- G 3.117 *Fehlerhafte Automatisierung beim Cloud Management*
- G 3.118 *Ungeeignete Konfiguration von Cloud-Diensten und Cloud-Verwaltungssystemen*

**Technisches Versagen**

- G 4.20 *Überlastung von Informationssystemen*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.90 *Ungewollte Preisgabe von Informationen durch Cloud Cartography*
- G 4.91 *Unberechtigtes Wiedereinspielen von Snapshots*
- G 4.92 *Inkompatibilität zwischen der Cloud-Administration und der Administration der Cloud-Elemente*
- G 4.93 *Ausfall von Verwaltungsservern und Verwaltungssoftware*

**Vorsätzliche Handlungen**

- G 5.23 *Schadprogramme*
- G 5.28 *Verhinderung von Diensten*
- G 5.114 *Missbrauch von Spanning Tree*
- G 5.178 *Missbrauch von Administratorrechten im Cloud-Management*

**Maßnahmenempfehlungen**

Um einen Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine Cloud-Infrastruktur im IT-Grundschutz abzubilden müssen verschiedene Elemente berücksichtigt werden: physische Komponenten (Hardware), Virtualisierungsserver, virtuelle Maschinen (IaaS) und Cloud-Anwendungen (PaaS und SaaS). Für die Modellierung von Cloud Management sind diese Elemente wie folgt zu beachten:

- **Physische Komponenten (Hardware)**: Für die Hardware der Cloud-Infrastruktur (wie Server und angebundene Speichersysteme) müssen die passenden IT-Grundschutz-Bausteine der Schicht 3 angewendet werden (z. B. B 3.101 *Allgemeiner Server* oder B 3.303 *Speicherlösungen / Cloud Storage*).
- **Virtualisierungsserver**: Der Baustein B 3.304 *Virtualisierung* ist auf jeden Virtualisierungsserver oder jede Gruppe von Virtualisierungsservern anzuwenden. Ein Virtualisierungsserver ist ein physisches IT-System (Client oder Server), auf dem virtuelle IT-Systeme betrieben werden. Neben dem Baustein B 3.304 *Virtualisierung* müssen auch die jeweils relevanten Server- oder Client-Bausteine der Schicht 3 auf die Virtualisierungsserver angewandt werden. Der Baustein *Cloud Management* wird auf dem Server für die Verwaltungssoftware der Cloud-Infrastruktur modelliert.
- **Virtuelle Maschinen**: Virtuelle IT-Systeme (virtuelle Maschinen, VMs) werden mithilfe der Bausteine aus den IT-Grundschutz-Katalogen modelliert. VMs werden grundsätzlich genauso wie physische IT-Systeme modelliert, das heißt, es werden die jeweils relevanten Bausteine der Schichten 3 und 5 herangezogen. Da es in der Praxis oft vorkommt, dass viele VMs eingerichtet werden, ist eine sinnvolle Modellierung der VMs häufig nur durch geeignete Gruppenbildung möglich.
- **Cloud-Anwendungen**: Cloud-Anwendungen werden über die jeweils relevanten Bausteine der Schicht 5 mit Bezug zu den jeweiligen virtuellen Maschinen abgebildet. Hier werden z. B. Bausteine wie B 5.7 *Datenbanken*, B 5.4 *Webserver* oder B 5.21 *Webanwendungen* modelliert.

Weitere Hinweise zur Modellierung virtueller IT-Systeme finden sich in der Maßnahme M 2.524 *Modellierung von Cloud Management*).

**Planung und Konzeption**

Wenn eine Umgebung für Cloud Computing geplant wird, müssen eine Reihe von Rahmenbedingungen berücksichtigt werden. Hier sind zum einen die physischen und virtuellen IT-Infrastrukturen für eine effiziente Bereitstellung zu planen. Bei der Auswahl von Komponenten muss auf Eignung, Kompatibilität und einfache Verwaltung geachtet werden (M 4.436 *Planung der Ressourcen für Cloud-Dienste*).

Zum anderen müssen Cloud-Diensteprofile entwickelt werden. Hierbei ist insbesondere darauf zu achtehn, dass die (automatische) Skalierbarkeit der Resourcen gewährleistet ist (M 4.437 *Planung von Cloud-Diensteprofilen*). Cloud-Diensteprofile werden in einem Satz aus Informationen definiert, der die

Cloud-Ressourcen und die zugrunde liegende Konfiguration beschreibt. In Cloud-Diensteprofilen muss insbesondere deren (automatische) Skalierbarkeit berücksichtigt werden.

**Beschaffung**

Bei der Auswahl der Hardware für Cloud-Umgebungen ist darauf zu achten, dass Systeme beschafft werden, die für eine reibungslose Zusammenarbeit von Virtualisierungslösung, Hardware und Cloud-Verwaltungssoftware geeignet sind. Die Systeme müssen leistungsfähig genug sein, um für alle durch Cloud-Anwender genutzten Cloud-Dienste zu den vereinbarten Zeiten genügend Leistung (Rechenleistung, Durchsatz, Antwortzeiten) bereitstellen zu können (M 4.438 *Auswahl von Cloud-Komponenten* ).

**Umsetzung**

Nachdem Planung und Beschaffung abgeschlossen sind, müssen die Cloud-Komponenten (Cloud-Infrastruktur und Zugriffswege) sicher konfiguriert werden. Da der Zugriff auf Cloud-Angebote zumeist webbasiert über unsichere Netze erfolgt, müssen die Zugriffswege abgesichert werden (M 5.174 *Absicherung der Kommunikation zum Cloud-Zugriff*).

Bevor Cloud-Dienste angeboten werden, müssen die zuständigen Administratoren für den sicheren Betrieb der Cloud-Komponenten geschult werden (M 3.91 *Schulung der Administratoren von Cloud-Infrastrukturen*).

**Betrieb**

Beim Betrieb von Cloud Computing Plattformen sorgt das Cloud Management für die Provisionierung und De-Provisionierung von Cloud Resourcen, Automatisierung von Prozessen, Mandantentrennung und Überwachung der bereitgestellten Cloud-Ressourcen.

Das Cloud Management sorgt im Betrieb der Cloud-Dienste für die korrekte und leistungsfähige Einstellung der Cloud-Infrastruktur und der Dienste. Ein wichtiger Bestandteil ist hier die geregelte Orchestrierung, also die Provisionierung und Deprovisionierung von Cloud-Ressourcen (M 2.521 *Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten*). Hierbei werden die Cloud-Komponenten konfiguriert und die Konfigurationseinstellungen regelmäßig kontrolliert.

Automatisierung bringt große Flexibilität und betriebliche Erleichterung mit sich, birgt zugleich jedoch großes Schadenspotential bei Fehlkonfigurationen in der Cloud-Verwaltungssoftware. Daher müssen hier sorgfältige Kontrollen eingerichtet und durchgeführt werden (M 2.523 *Sichere Automatisierung der Cloud-Regelprozesse*).

Eine zentrale Anforderung an Cloud-Angebote ist "Mandantentrennung", also die sichere Trennung von Anwendungen, IT-Systemen und Daten unterschiedlicher Cloud-Anwender. Solche Sicherheitsmaßnahmen zur Trennung können auf verschiedenen Schichten des IT-Grundschutzes eingerichtet werden (z. B. Netze, Speichernetze, Virtualisierung) und daher auch über Bausteine anderer Schichten umgesetzt. Das Cloud Management muss übergreifend sicherstellen, dass die Mandantentrennung durchgängig über alle Komponenten der Cloud-Infrastruktur korrekt funktioniert (M 4.445 *Durchgängige Mandantentrennung von Cloud-Diensten*).

Da die Cloud-Infrastruktur hoch-integriert ist und über ein zentrales Cloud Management verfügt, muss eine zentrale Protokollierung eingeführt und der Baustein B 5.22 *Protokollierung* umgesetzt werden. Hierbei sind spezifische Maßnahmen zur Protokollierung und Monitoring der Cloud-Ressourcen, der Cloud-Leistung sowie der Cloud-Dienstenutzung zu beachten (M 4.443 *Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur*). Zum einen geht es für den Cloud-Diensteanbieter darum, die Auslastung und Nutzung seiner Ressourcen zu kontrollieren, um gegebenenfalls Engpässe zu erkennen, aber zum anderen auch darum, den Cloud-Anwendern die zugesicherten Leistungen nachzuweisen (M 2.522 *Berichtswesen und Kommunikation zu den Cloud-Anwendern*).

**Notfallvorsorge**

In den Verträgen zwischen Cloud-Anwendern und Cloud-Diensteanbietern werden Dienstgüten (Verfügbarkeitszeiten, Ausfallzeiten) vereinbart. Um die vereinbarte Dienstgüten erbringen zu können, soll-

te auch das Notfallmanagement und hier insbesondere die Notfallvorsorge in das Cloud-Management integriert werden.

Hierfür können existierende Bestandteile der Notfallvorsorge des Cloud-Diensteanbieters, auch aus anderen Teilen seines IT-Betriebs für das Cloud Management übernommen und gegebenenfalls um Cloud-spezifische Anteile erweitert werden (M 6.152 *Notfallvorsorge und regelmäßige Datensicherung im Cloud Computing*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Cloud Management" vorgestellt.

**Planung und Konzeption**
- M 2.516 (Z) *Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender*
- M 2.517 (A) *Vertragsgestaltung mit Dritt-Dienstleistern*
- M 2.524 (W) *Modellierung von Cloud Management*
- M 4.436 (A) *Planung der Ressourcen für Cloud-Dienste*
- M 4.437 (A) *Planung von Cloud-Diensteprofilen*

**Beschaffung**
- M 4.438 (A) *Auswahl von Cloud-Komponenten*

**Umsetzung**
- M 2.38 (B) *Aufteilung der Administrationstätigkeiten*
- M 3.91 (B) *Schulung der Administratoren von Cloud-Infrastrukturen*
- M 4.439 (Z) *Virtuelle Sicherheitsgateways (Firewalls) in Clouds*
- M 4.440 (Z) *Verschlüsselte Speicherung von Cloud-Anwenderdaten*
- M 4.441 (Z) *Multifaktor-Authentisierung für den Cloud-Benutzerzugriff*
- M 5.174 (A) *Absicherung der Kommunikation zum Cloud-Zugriff*
- M 6.151 (A) *Alarmierungskonzept für die Protokollierung*

**Betrieb**
- M 2.518 (C) *Einsatz einer hochverfügbaren Firewall-Lösung*
- M 2.519 (A) *Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing*
- M 2.520 (C) *Sicheres und vollständiges Löschen von Cloud-Anwenderdaten*
- M 2.521 (A) *Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten*
- M 2.522 (B) *Berichtswesen und Kommunikation zu den Cloud-Anwendern*
- M 2.523 (C) *Sichere Automatisierung der Cloud-Regelprozesse*
- M 4.430 (A) *Analyse von Protokolldaten*
- M 4.442 (C) *Zentraler Schutz vor Schadprogrammen in der Cloud-Infrastruktur*
- M 4.443 (B) *Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur*
- M 4.444 (A) *Patchmanagement für Cloud-Komponenten*
- M 4.445 (A) *Durchgängige Mandantentrennung von Cloud-Diensten*
- M 4.446 (W) *Einführung in das Cloud Management*
- M 5.71 (Z) *Intrusion Detection und Intrusion Response Systeme*

**Notfallvorsorge**
- M 6.152 (A) *Notfallvorsorge und regelmäßige Datensicherung im Cloud Computing*
- M 6.153 (C) *Einsatz von redundanten Cloud-Management-Komponenten*

# B 5.24 Web-Services


## Beschreibung

Web-Services im Sinne dieses Bausteins sind alle IT-Services, die von einem Betreiber für einen oder mehrere Dienstnehmer (engl.: Consumer) bereitgestellt und über netzbasierte Schnittstellen, in der Regel auf der Grundlage des HTTP-Protokolls, aufgerufen werden können.

In der Abgrenzung zu Webanwendungen (siehe Baustein B 5.21 *Webanwendungen*) verfügt der Web-Service dabei über keine Client-Komponente oder visualisierbare Web-Oberfläche, sondern bietet seine Funktionalität über eine definierte Schnittstelle an, die vom Consumer des Web-Service (in der Regel automatisiert) aufgerufen wird. Web-Services können dabei auch von anderen Web-Services aufgerufen werden und mit diesen zusammen eine komplexere übergeordnete Funktionalität realisieren. Die Zusammenstellung verschiedener Web-Services zur Realisierung einer bestimmten Funktionalität wird dabei als Orchestrierung bezeichnet und kann anhand von standardisierten Schnittstellenbeschreibungen auch dynamisch erfolgen. Solche komplexen Architekturen werden als Service-orientierte Architekturen (SOA) bezeichnet und können sich auch über Organisationsgrenzen hinweg erstrecken.

An den Schnittstellen kommen typischerweise entweder das XML-basierte SOAP oder das objektorientierte REST-Konzept zum Einsatz. Für Web-Services und ihre Schnittstellen sind zahlreiche Standards publiziert, die in der W-Maßnahme M 4.451 *Aktuelle Web-Service Standards* in diesem Baustein vorgestellt werden.

Dieser Baustein betrachtet Web-Services stets aus der Sicht des Betreibers. Intitutionen, die ausschließlich als Consumer von Web-Services agieren, modellieren diesen Baustein entsprechend nicht, sondern verwenden geeignete Bausteine wie B 1.11 *Outsourcing* oder B 1.17 *Cloud-Nutzung*.

Obwohl Webanwendungen und Web-Services über Gemeinsamkeiten verfügen und teilweise überlappende Sicherheitsmaßnahmen erfordern, wurden im Sinne einer einfacheren Anwendung der IT-Grundschutz-Kataloge beide Bausteine jeweils in sich vollständig erstellt, sodass diese Bausteine alternativ anzuwenden sind, je nachdem, ob die betrachtete Anwendung über eine Benutzer-Oberfläche verfügt (Anwendung des Bausteins Webanwendungen) oder über eine standardisierte Schnittstelle aufgerufen wird (Anwendung des Bausteins Web-Service). Für komplexe Anwendungen, die einerseits eine Web-Anwendung sind, andererseits aber auch Web-Services für andere IT-Systeme bereitstellen, sollen beide Bausteine zusammen modelliert werden.

## Gefährdungslage

Die folgenden Gefährdungen sind beim Einsatz von Web-Services relevant:

### Organisatorische Mängel

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.61 *Unberechtigte Sammlung personenbezogener Daten*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.158 *Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services*
- G 2.159 *Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services*
- G 2.160 *Fehlende oder unzureichende Protokollierung*
- G 2.181 *Mangelhafte Planung und Konzeption des Einsatzes von Web-Services*

**Menschliche Fehlhandlungen**

- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.38 *Konfigurations- und Bedienungsfehler*
- G 3.119 *Fehlerhafte Anwendung von Standards*
- G 3.120 *Fehler bei der Orchestrierung*
- G 3.121 *Konfigurations- und Administrationsfehler bei Web-Services*

**Technisches Versagen**

- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.84 *Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services*
- G 4.85 *Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services*
- G 4.87 *Offenlegung vertraulicher Informationen bei Webanwendungen*
- G 4.94 *Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services*

**Vorsätzliche Handlungen**

- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.28 *Verhinderung von Diensten*
- G 5.87 *Web-Spoofing*
- G 5.131 *SQL-Injection*
- G 5.165 *Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services*
- G 5.167 *Fehler in der Logik von Webanwendungen und Web-Services*
- G 5.168 *Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services*
- G 5.169 *Unzureichendes Session-Management von Webanwendungen und Web-Services*
- G 5.172 *Umgehung der Autorisierung bei Webanwendungen und Web-Services*
- G 5.173 *Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services*
- G 5.174 *Injection-Angriffe*
- G 5.179 *Angriffe auf Protokolle*
- G 5.180 *Angriffe auf Registries und Repositories*
- G 5.181 *Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services*
- G 5.182 *Manipulation von Routen (Routing Detours)*
- G 5.183 *Angriffe auf XML*
- G 5.184 *Informationsgewinnung über Web-Services*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Einsatzes von Web-Services sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Die hier beschriebenen Maßnahmen decken die vorstehenden Gefährdungen für den normalen Schutzbedarf ab.

**Planung und Konzeption**

Wie bei jeder anderen Art von Anwendung gilt auch für Web-Services, dass die Weichen für eine sichere Realisierung in der Planungsphase gestellt werden. Dies bedeutet insbesondere klare Verantwortlichkeiten, wie in der Maßnahme M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen* gefordert.

Funktionalität, Architektur und Realisierung des Web-Services müssen geplant (M 4.458 *Planung des Einsatzes von Web-Services* ) und dokumentiert (M 2.486 *Dokumentation der Architektur von Webanwendungen und Web-Services*) sein. Je nachdem, ob der Web-Service durch Lösungen Dritter oder durch Eigenentwicklung realisiert wird, sind die Maßnahmen M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* beziehungsweise M 2.487 *Entwicklung und Erweiterung von Anwendungen* zu berücksichtigen. Sofern der Web-Service ein bereits vorhandenes System ablöst oder Daten daraus übernimmt, muss auch die Migration in die Planungsphase eingeschlossen werden (M 2.530 *Planung und Vorbereitung von Migrationen* ).

Ein weiterer wichtiger Aspekt für die Planung sind Sicherheitsaspekte des Web-Service. Die dazu vorgesehenen Maßnahmen sollten schriftlich festgehalten werden (M 2.531 *Erarbeitung einer Sicherheitsrichtlinie für Web-Services* ) und umfassen konzeptionelle Maßnahmen gegen SQL-Injections (M 2.363 *Schutz gegen SQL-Injection*) ebenso wie Maßnahmen zur sicheren Trrennung der Daten verschiedener Mandanten und Nutzer (M 4.457 *Sichere Mandantentrennung bei Webanwendungen und Web-Services*) und Konzepte zur Absicherung der Schnittstellen (M 5.168 *Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services*).

**Beschaffung**

Die Beschaffung von Komponenten und Lösungen für Web-Services muss nachvollziehbar und geordnet ablaufen und die Prozesse für die Abnahme und Freigabe von IT-Komponenten berücksichtigen (M 2.62 *Software-Abnahme- und Freigabe-Verfahren*). Bietet der Betreiber den Web-Service auch Dritten zur Nutzung an, sind die in der Maßnahme M 2.533 *Vertragliche Aspekte bei der Bereitstellung von Web-Services* beschriebenen Aspekte bei der Vertragsgestaltung mit den Consumern zu berücksichtigen.

**Umsetzung**

Insbesondere dann, wenn Web-Services als Dienstleistung für Dritte angeboten werden, müssen sicherheitsrelevante Fragen zwischen Anbieter und Consumer geklärt und geregelt werden (Maßnahme M 2.532 *Anbieten von Web-Services für Dritte*).

Bei der Realisierung von Web-Services sind einerseits Maßnahmen für die sichere Web-Entwicklung zu beachten, wie sie auch für Webanwendungen gelten: Von der Validierung von Ein- und Ausgabedaten (M 4.393 *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*) über ein robustes Session-Management (M 4.394 *Session-Management bei Webanwendungen und Web-Services*) bis zur Vermeidung der Preisgabe unnötiger Informationen in der Fehlerbehandlung und in den Schnittstellenbeschreibungen (M 4.395 *Fehlerbehandlung durch Webanwendungen und Web-Services* und M 4.400 *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*).

Darüber hinaus sind spezifische Sicherheitsprobleme von Web-Services zu adressieren: Dies umfasst einerseits die sichere Identifizierung und Authentisierung von Web-Service-Dienstnehmer (M 4.456 *Authentisierung bei Web-Services*) einschließlich von Maßnahmen zur Verhinderung der Nutzung durch Unberechtigte (M 4.454 *Schutz vor unerlaubter Nutzung von Web-Services*). Sofern die Architektur des Web-Services dafür einen Secure-Token-Service (STS) vorsieht, finden sich Hinweise zur richtigen Umsetzung in der Maßnahme M 4.453 *Einsatz eines Security Token Service (STS)*.

Andererseits muss bei jedem Aufruf des Web-Service sichergestellt werden, dass die aufgerufene Funktionalität durch die Berechtigungen des Aufrufers abgedeckt ist (M 4.454 *Schutz vor unerlaubter Nutzung von Web-Services*). Die Kommunikation zwischen Web-Service und Aufrufer muss geeignet geschützt werden (M 4.450 *Absicherung der Kommunikation bei Web-Services*), insbesondere wenn sie über unsichere Netze erfolgt.

Ist die Schnittstelle des Web-Service für einen größeren Personenkreis oder gar aus öffentlichen Netzen heraus erreichbar, sollten entsprechende Maßnahmen gegen Angriffe auf die Verfügbarkeit des Web-Service umgesetzt werden (M 4.405 *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*). Um die Robustheit des Web-Service gegen Angriffe zu erhöhen, kann zusätzlich der Einsatz eines XML-Gateways erwogen werden (M 5.175 *Einsatz eines XML-Gateways*).

**Betrieb**

Fragen des sicheren Betriebs von Web-Services umfassen zunächst die Dokumentation und Einrichtung von Berechtigungen für die Consumer (auch wenn der Web-Service durch Anwendungen oder andere Web-Services automatisiert aufgerufen wird, siehe M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).

Nutzer und Administratoren müssen mit den für sie relevanten Sicherheitsmaßnahmen ausreichend vertraut sein (M 3.5 *Schulung zu Sicherheitsmaßnahmen*).

Der Betrieb des Web-Service muss durch geeignete Maßnahmen zur Protokollierung nachvollziehbar sein (M 4.397 *Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services*). Da von der Protokollierung in der Regel auch personenbezogene Daten betroffen sind, müssen dabei die Anforderungen des Datenschutzes geeignet berücksichtigt werden (M 2.110 *Datenschutzaspekte bei der Protokollierung*). Um sicherheitsrelevante Vorfälle rechtzeitig zu erkennen, muss eine Kontrolle der Protokolldateien sichergestellt werden (M 2.64 *Kontrolle der Protokolldateien*), gegebenenfalls durch automatisierte Systeme.

Veränderungen im laufenden Betrieb müssen sorgfältig durchgeführt (M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*) und dokumentiert werden (M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*). Insbesondere ist darauf zu achten, dass bekannt werdende Sicherheitslücken im Web-Service oder einer der von ihm genutzten Komponenten, Frameworks oder Bibliotheken dem Betreiber zur Kenntnis gelangen (M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*) und nach Möglichkeit behoben oder in anderer Form geeignet behandelt werden (M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

Der ordnungsgemäße, sichere und störungsfreie Betrieb des Web-Service muss durch geeignete Überwachungsmaßnahmen sichergestellt werden (M 4.452 *Überwachung eines Web-Service*). Regelmäßige Schwachstellentests dienen zusätzlich der Prävention von Angriffen (M 5.150 *Durchführung von Penetrationstests*).

**Notfallvorsorge**

Ein geeignetes Datensicherungskonzept ist auch für Web-Services eine zentrale Maßnahme der Notfallvorsorge (M 6.32 *Regelmäßige Datensicherung*). Weitere Maßnahmen zur Vorsorge und Bewältigung von Notfällen sind in der Maßnahme M 6.154 *Notfallmanagement für Web-Services* zusammengefasst.

**Planung und Konzeption**

- M 2.1 (A) *Festlegung von Verantwortlichkeiten und Regelungen*
- M 2.80 (A) *Erstellung eines Anforderungskatalogs für Standardsoftware*
- M 2.363 (B) *Schutz gegen SQL-Injection*
- M 2.486 (A) *Dokumentation der Architektur von Webanwendungen und Web-Services*
- M 2.487 (B) *Entwicklung und Erweiterung von Anwendungen*
- M 2.530 (B) *Planung und Vorbereitung von Migrationen*
- M 2.531 (A) *Erarbeitung einer Sicherheitsrichtlinie für Web-Services*
- M 4.451 (W) *Aktuelle Web-Service Standards*
- M 4.457 (B) *Sichere Mandantentrennung bei Webanwendungen und Web-Services*
- M 4.458 (A) *Planung des Einsatzes von Web-Services*
- M 5.168 (A) *Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services*

**Beschaffung**

- M 2.62 (B) *Software-Abnahme- und Freigabe-Verfahren*
- M 2.533 (C) *Vertragliche Aspekte bei der Bereitstellung von Web-Services*

**Umsetzung**

- M 2.532 (B) *Anbieten von Web-Services für Dritte*
- M 4.393 (B) *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*
- M 4.394 (A) *Session-Management bei Webanwendungen und Web-Services*
- M 4.395 (B) *Fehlerbehandlung durch Webanwendungen und Web-Services*
- M 4.400 (B) *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*
- M 4.405 (C) *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*
- M 4.450 (A) *Absicherung der Kommunikation bei Web-Services*
- M 4.453 (Z) *Einsatz eines Security Token Service (STS)*
- M 4.454 (A) *Schutz vor unerlaubter Nutzung von Web-Services*
- M 4.455 (A) *Autorisierung bei Web-Services*
- M 4.456 (A) *Authentisierung bei Web-Services*
- M 5.175 (Z) *Einsatz eines XML-Gateways*

**Betrieb**

- M 2.8 (A) *Vergabe von Zugriffsrechten*
- M 2.31 (A) *Dokumentation der zugelassenen Benutzer und Rechteprofile*
- M 2.34 (A) *Dokumentation der Veränderungen an einem bestehenden System*
- M 2.35 (B) *Informationsbeschaffung über Sicherheitslücken des Systems*
- M 2.64 (A) *Kontrolle der Protokolldateien*
- M 2.110 (A) *Datenschutzaspekte bei der Protokollierung*
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 3.5 (A) *Schulung zu Sicherheitsmaßnahmen*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.397 (C) *Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services*
- M 4.452 (A) *Überwachung eines Web-Service*
- M 5.150 (Z) *Durchführung von Penetrationstests*

**Notfallvorsorge**

- M 6.32 (A) *Regelmäßige Datensicherung*
- M 6.154 (B) *Notfallmanagement für Web-Services*

# B 5.25 Allgemeine Anwendungen

## Beschreibung

In Unternehmen und Behörden werden Geschäftsprozesse oder Fachverfahren betrieben, die durch spezialisierte Anwendungssoftware (kurz Anwendungen) unterstützt werden. Hierfür sind in den IT-Grundschutz-Katalogen keine spezifischen IT-Grundschutz-Bausteine, also keine spezifischen Gefährdungslagen und Maßnahmen, vorhanden. Gleichzeitig beschreiben aber zahlreiche Bausteine der Schicht 1 einen umfassenden Managementrahmen, also Prozesse und Vorgehensmodelle, die für alle Phasen des Lebenszyklus beim Einsatz von Anwendungen relevant sind. Insbesondere sind hier zu nennen:

**Grundsätzlich:**

- B 1.3 *Notfallmanagement*
- B 1.4 *Datensicherungskonzept*
- B 1.9 *Hard- und Software-Management*
- B 1.10 *Standardsoftware*
- B 1.14 *Patch- und Änderungsmanagement*
- B 1.16 *Anforderungsmanagement*

**Im Bedarfsfall:**

- B 1.7 *Kryptokonzept*
- B 1.11 *Outsourcing*
- B 1.12 *Archivierung*

Bis auf wenige Ausnahmen richten sich diese Bausteine und die darin enthaltenen Maßnahmen an das Informationssicherheitsmanagement und die IT-Betriebsleitung. Die Perspektive der Verantwortlichen für Auswahl, Inbetriebnahme, Betrieb und Aussonderung einer Anwendung tritt dabei in den Hintergrund.

Dieser Baustein fasst aus Sicht der Verantwortlichen für Anwendungen wesentliche Anforderungen an die Informationssicherheit zusammen. Er referenziert dabei wesentliche Maßnahmen aus den oben genannten Bausteinen und verweist somit auf die dort beschriebenen Prozesse. Führen diese Prozesse im jeweiligen ISMS zu Rahmenkonzepten, etwa für den Einsatz von Verschlüsselung, Datensicherung oder Notfallvorsorge, so ist es sinnvoll, diese Konzepte bezogen auf die jeweilige betrachtete Anwendung fortzuschreiben.

Dieser Baustein deckt die folgenden Typen von Anwendungen ab:

- Individualsoftware, die durch interne oder externe Entwickler erstellt wurde,
- Standardsoftware mit eigenen Anpassungen, zum Beispiel durch Programmänderungen oder durch Entwicklung spezifischer Module (Customizing) und
- Standardsoftware, die wie vom Hersteller geliefert eingesetzt und nur entsprechend der Fachaufgaben und der Sicherheitsvorgaben konfiguriert wird.

Fokus dieses Bausteins sind komplexe Anwendungen, die für spezifische fachliche Aufgaben konzipiert sind, wie Personalverwaltungssoftware oder wie Verfahren zur Verwaltung von Sozialdaten oder Meldedaten. Fach- oder funktionsübergreifende Standardsoftware, die fachlich nicht fokussiert ist und wie Office-Anwendungen für viele Branchen nutzbar ist, wird in B 1.10 *Standardsoftware* behandelt.

Je nach Typ der Anwendung können dabei einige der in diesem Baustein vorgeschlagenen Maßnahmen entbehrlich sein.

Unabhängig vom Geschäftsprozess oder Verwaltungsverfahren, in dem die Anwendung eingesetzt wird, werden in diesem Baustein wesentliche, übergreifende Gefährdungen und Standardsicherheitsmaß-

nahmen beschrieben. Eine Ergänzung dieses Bausteins um spezifische Bausteine für bestimmte Anwendungen ist möglich, wie beispielsweise die bereits etablierten Bausteine B 5.13 *SAP System* und B 5.21 *Webanwendungen*.

## Gefährdungslage

Für den IT-Grundschutz von Anwendungen werden die folgenden typischen Gefährdungen betrachtet:

**Organisatorische Mängel**

- G 2.3 *Fehlende, ungeeignete, inkompatible Betriebsmittel*
- G 2.5 *Fehlende oder unzureichende Wartung*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.9 *Mangelhafte Anpassung an Veränderungen beim IT-Einsatz*
- G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.61 *Unberechtigte Sammlung personenbezogener Daten*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.84 *Unzulängliche vertragliche Regelungen mit einem externen Dienstleister*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*
- G 2.151 *Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen*
- G 2.154 *Ungeeignete Anwendungen für den Einsatz auf Terminalservern*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*

**Technisches Versagen**

- G 4.2 *Ausfall interner Versorgungsnetze*
- G 4.13 *Verlust gespeicherter Daten*
- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.39 *Software-Konzeptionsfehler*
- G 4.43 *Undokumentierte Funktionen*
- G 4.99 *Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*

**Maßnahmenempfehlungen**

Um den betrachteten Informationsverbund abzusichern, müssen, zusätzlich zu diesem Baustein, noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Anwendungen sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über die Beschaffung bis zu ihrer Außerbetriebnahme und der Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

**Planung und Konzeption**

Bevor eine neue Anwendung beschafft oder programmiert wird, müssen die Rahmenbedingungen für den Einsatz geklärt werden (siehe M 2.546 *Analyse der Anforderungen an neue Anwendungen*). Dazu gehört M 2.547 *Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen*.

Je nach Einsatzzweck kann eine Anwendung fertig eingekauft werden, die eventuell angepasst werden muss, oder es muss eine spezielle Anwendungssoftware entwickelt werden. Dafür sollte ein Anforderungskatalog (siehe M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*) bzw. ein Lastenheft (siehe M 2.548 *Erstellung eines Lastenheftes*) erstellt werden.

**Beschaffung**

Anhand der konkreten Vorgaben des Anforderungskatalogs kann geprüft werden, ob ein am Markt vorhandenes Produkt für den Einsatzzweck geeignet ist. Anderenfalls sollten andere Lösungen überlegt werden, beispielsweise könnten externe Dienstleister mit der Entwicklung einer passenden Anwendungssoftware beauftragt werden (siehe auch M 2.551 *Durchführung eines geeigneten und rechtskonformen Vergabeverfahrens*).

Stützt sich die Institution bei Beschaffung, Entwicklung oder Betrieb der Anwendung auf Dienstleister ab, sollten geeignete vertragliche Rahmenbedingungen geschaffen werden (siehe M 2.554 *Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen*).

**Umsetzung**

Aufbauend auf dem Lastenheft ist zur Anwendungsentwicklung ein Pflichtenheft zu erstellen (siehe M 2.552 *Erstellung eines Pflichtenheftes*). Im Rahmen des Pflichtenheftes sind auch eine Reihe von Teilkonzepten zu berücksichtigen. Diese sollten die Pflege der Anwendung (siehe M 2.553 *Entwicklung eines Pflegekonzeptes für Anwendungen*), die geeignete Behandlung der Nutzerauthentisierung (siehe M 2.555 *Entwicklung eines Authentisierungskonzeptes für Anwendungen*) und die Protokollierung (siehe M 2.500 *Protokollierung von IT-Systemen*) beinhalten.

Bei der Inbetriebnahme der Anwendung sind Test und Freigabe (siehe M 2.556 *Planung und Umsetzung von Test und Freigabe von Anwendungen*), die sichere Installation (siehe M 4.463 *Sichere Installation einer Anwendung*) sowie die geeignete Schulung von Administratoren und Anwendern (siehe M 3.4 *Schulung vor Programmnutzung*) zu berücksichtigen.

**Betrieb**

In der Phase des Betriebes einer Anwendung ist dafür Sorge zu tragen, dass die Sicherheit gewährleistet bleibt (siehe M 4.464 *Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb*).

**Aussonderung**

Wird eine Anwendung auf eine neue betriebliche Infrastruktur migriert, oder wird die Anwendung endgültig außer Betrieb genommen, so sind in der abgelösten betrieblichen Umgebung die Deinstallation (siehe M 2.89 *Deinstallation von Standardsoftware*), die Löschung und Vernichtung von nicht mehr benötigten Daten (siehe M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*) und Außerbetriebnahme der bisherigen betrieblichen Infrastruktur (siehe M 4.234 *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*) zu planen und umzusetzen.

**Notfallvorsorge**

Hinweise zur anwendungsspezifischen Planung der Notfallvorsorge sind in der Maßnahme M 6.158 *Notfallvorsorge für Anwendungen* zusammengefasst. Wurde die Anwendung durch Dienstleister entwickelt und kann fehlende Unterstützung durch den Dienstleister, zum Beispiel durch Insolvenz, die Existenz der Institution gefährden, so ist eine Hinterlegung des Quellcodes zu empfehlen (siehe M 6.137 *Treuhänderische Hinterlegung (Escrow)*). Bei hohem Schutzbedarf hinsichtlich der Verfügbarkeit ist die Erstellung eines Verfügbarkeitskonzeptes zu empfehlen (siehe M 6.157 *Entwicklung eines Redundanzkonzeptes für Anwendungen*).

**Planung und Konzeption**
- M 2.40 (A) *Rechtzeitige Beteiligung des Personal-/Betriebsrates*
- M 2.546 (A) *Analyse der Anforderungen an neue Anwendungen*
- M 2.547 (A) *Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen*
- M 2.548 (A) *Erstellung eines Lastenheftes*
- M 2.549 (C) *Erstellung eines Mandantenkonzeptes*
- M 2.550 (C) *Geeignete Steuerung der Anwendungsentwicklung*

**Beschaffung**
- M 2.551 (Z) *Durchführung eines geeigneten und rechtskonformen Vergabeverfahrens*

- M 2.554 (Z) *Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen*

**Umsetzung**

- M 2.552 (A) *Erstellung eines Pflichtenheftes*
- M 2.553 (C) *Entwicklung eines Pflegekonzeptes für Anwendungen*
- M 2.555 (A) *Entwicklung eines Authentisierungskonzeptes für Anwendungen*
- M 2.556 (A) *Planung und Umsetzung von Test und Freigabe von Anwendungen*
- M 4.463 (A) *Sichere Installation einer Anwendung*

**Betrieb**

- M 3.4 (A) *Schulung vor Programmnutzung*
- M 4.464 (B) *Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb*

**Aussonderung**

- M 2.89 (C) *Deinstallation von Standardsoftware*
- M 2.167 (B) *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*
- M 4.234 (B) *Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern*

**Notfallvorsorge**

- M 6.137 (Z) *Treuhänderische Hinterlegung (Escrow)*
- M 6.157 (Z) *Entwicklung eines Redundanzkonzeptes für Anwendungen*
- M 6.158 (B) *Notfallvorsorge für Anwendungen*

# B 5.26 Serviceorientierte Architektur

## Beschreibung

Serviceorientierte Architekturen (SOA) beschreiben einen allgemeinen Ansatz zur Umsetzung verteilter Systeme, um Institutionen mittels IT in ihren Geschäftsprozessen effizient zu unterstützen. Die einzelnen Aktivitäten innerhalb eines Geschäftsprozesses werden dabei von Diensten übernommen, die so auch für andere Aktivitäten in anderen Geschäftsprozessen wiederverwendbar sind. Durch Zusammensetzen der Dienste (Orchestrierung) lassen sich dann zum Beispiel neue Geschäftsprozesse umsetzen. Das SOA-Konzept verspricht viele bestehende Probleme bei der Integration und Interaktion unterschiedlicher Teilsysteme zu lösen.

Ausgangspunkt für die Darstellung in diesem Baustein ist das Referenzmodell SOA-RM (Reference Model for Service Oriented Architecture, Version 1.0) der OASIS (Organization for the Advancement of Structured Information Standards), das sich unter anderem auf eine infrastrukturbezogene Diensteumgebung abstützt, repräsentiert in einem Enterprise Service Bus (ESB) und einem anwendungsunabhängigen Transportprotokoll, wie dem Simple Object Access Protocol (SOAP). Für die Sicherheitsarchitektur im Bereich der Anwendungssicherheit ist SOAP maßgebend. SOAP ist ein Protokollstandard des W3C, der auch die notwendigen Sicherheitsprotokollelemente wie WS-Security bereitstellt. Weiterhin ermöglicht SOAP die standardisierte Kommunikation zwischen verteilten Applikationen und Objekten insbesondere im SOA/ESB-Umfeld. Allerdings können auch andere XML-Transportcontainer wie REST (Representational State Transfer) verwendet werden. Aufgrund der Flexibilität von SOAP wird diese Spezifikation hier bevorzugt.

Das Referenzmodell der OASIS für SOA geht über reine Webanwendungen, wie sie in den Bausteinen B 5.21 *Webanwendungen* und B 5.24 *Web-Services* enthalten sind, hinaus und beschreibt ein allgemeines Modell, wie Dienste und Dienstprofile, auch und gerade in der Verteilung durch Benutzer verwendet und zu neuen Fähigkeiten verbunden werden können. Um eine solche Dienstenutzung von unterschiedlichen Diensteerbringern zu ermöglichen, werden standardisierte Dienstzugangspunkte genutzt.

In den meisten serviceorientierten Architekturen wird zum Nachrichtenaustausch SOAP und als Transportmedium HTTP verwendet. SOAP als Kommunikationsprotokoll und HTTP als Transportprotokoll unterstützen in ihrer Basisform keinerlei Sicherheitsanforderungen. Daten werden vielmehr im Klartext übermittelt. SOAP-Nachrichten werden vorwiegend mittels HTTP über SSL 3.0 beziehungsweise TLS 1.0 oder 1.2 (HTTPS) ausgetauscht.

In SOAP-basierten Plattformen wird für mittels SOAP übertragene Informationsobjekte zusätzlich ein "Objektschutz" eingeführt und zusammen mit der ursprünglichen SOAP-Nachricht übermittelt. Dieser Objektschutz kann grundsätzlich aus den folgenden Elementen bestehen:

- Angabe über die Einstufung des Informationsobjektes,
- Angabe über den Ersteller und/oder die berechtigten Benutzer,
- Angabe über den Integritätsschutz und
- Angabe über den Vertraulichkeitsschutz.

Als primäre Technik hierfür hat sich der OASIS-Standard WS-Security etabliert. WS-Security setzt auf bereits existierende Standards wie XML-Verschlüsselung, XML-Signaturen und X.509-Zertifikaten auf. WS-Security ist eine grundlegende Erweiterung des SOAP-Standards, um den Anforderungen hinsichtlich Integrität, Vertraulichkeit und Authentizität von Nachrichten sowie beteiligter Entitäten gerecht zu werden. Dabei wird die Authentisierung und Autorisierung basierend auf SAML (Security Assertion Markup Language) eingesetzt.

Der Zugriff auf SOAP-basierte Informationsobjekte in IT-Systemen unterliegt unterschiedlichen Zugriffsbeschränkungen, solange diese Objekte nicht als frei zugänglich deklariert sind. Die wesentlichen Kriterien hierbei sind die Klassifikation, wie der Einstufungsgrad und zusätzliche Kennzeichnungen, der

beabsichtigte Empfängerkreis und falls erforderlich ein Verfallsdatum für die Information, oder Teile von dieser, im Informationsobjekt.

Zugriffsinformationen zu Informationsobjekten werden in einem Label vermerkt. Um diese Zusatzinformationen (Metainformationen) während der gesamten Lebensdauer eines Informationsobjektes fälschungssicher zu machen, müssen diese fest an das Informationsobjekt gebunden werden, wie auch alle anderen Bestandteile der SOAP-Nachricht. Dies geschieht normalerweise durch eine zusätzliche Signatur.

Der Baustein stellt die Gefährdungen von serviceorientierten Architekturen vor und beschreibt Maßnahmen, um den Informationsverbund angemessen abzusichern.

## Gefährdungslage

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen als typisch im Zusammenhang mit serviceorientierten Architekturen angenommen:

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.66 *Unzureichendes Sicherheitsmanagement*
- G 2.205 *Fehlendes Notfallvorsorgekonzept für serviceorientierte Architekturen*

**Menschliche Fehlhandlungen**

- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*
- G 3.124 *Fehlende und ungenügende Implementierungen bzw. Konfigurationen in einer SOA*

**Technisches Versagen**

- G 4.22 *Software-Schwachstellen oder -Fehler*
- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.48 *Ausfall der Systeme eines Outsourcing-Dienstleisters*
- G 4.74 *Ausfall von IT-Komponenten in einer virtualisierten Umgebung*
- G 4.87 *Offenlegung vertraulicher Informationen bei Webanwendungen*

**Vorsätzliche Handlungen**

- G 5.7 *Abhören von Leitungen*
- G 5.18 *Systematisches Ausprobieren von Passwörtern*
- G 5.23 *Schadprogramme*
- G 5.28 *Verhinderung von Diensten*
- G 5.83 *Kompromittierung kryptographischer Schlüssel*
- G 5.87 *Web-Spoofing*
- G 5.143 *Man-in-the-Middle-Angriff*
- G 5.170 *Cross-Site Scripting (XSS)*
- G 5.174 *Injection-Angriffe*
- G 5.179 *Angriffe auf Protokolle*
- G 5.180 *Angriffe auf Registries und Repositories*
- G 5.181 *Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services*
- G 5.183 *Angriffe auf XML*
- G 5.184 *Informationsgewinnung über Web-Services*
- G 5.195 *Ausnutzen von Schwachstellen in Backend-Anwendungen*
- G 5.196 *Unterbinden einer Informations- und Dienstesynchronisation in einer verteilten SOA-Umgebung*
- G 5.197 *Missbrauch von SAML-Token in SOA-Umgebungen*
- G 5.198 *Missbrauch der WS-Notification-Broker in einer SOA*
- G 5.199 *Ungenügende Absicherung der SOAP-Kommunikation*
- G 5.200 *Manipulation von Richtlinien in einer SOA*

**Maßnahmenempfehlungen**

Um einen Informationsverbund abzusichern, müssen gemäß den Ergebnissen der Modellierung nach IT-Grundschutz zusätzlich zu diesem Baustein weitere Bausteine umgesetzt werden. Bereits in übergreifenden Bausteinen und in entsprechenden System-, Netz- und Anwendungsbausteinen angeführte Maßnahmen werden hier nicht nochmals genannt. Diese Bausteine und Maßnahmen sind im Einzelfall so anzuwenden, dass sie auch für eine SOA sinnvoll sind.

Für serviceorientierte Architekturen sollten die folgenden gemäß den Lebenszyklusphasen strukturierten Maßnahmen umgesetzt werden.

**Planung und Konzeption**

Bei der Planung einer serviceorientierten Umgebung müssen eine Reihe von Rahmenbedingungen bedacht werden. Im ersten Schritt ist eine Sicherheitsarchitektur für SOA-basierte Systeme zu erstellen, die eine sichere, verteilte Dienstenutzung, auch über Domänengrenzen hinweg, ermöglicht (siehe z. B. M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen*, M 2.378 *System-Entwicklung* sowie M 2.561 *Erstellen spezifikationskonformer SOA-Implementierungen und Konfigurationen*). Bei der Kommunikation von SOA-basierten Systemen untereinander sollten bei durchgängigen, homogenen XML-Transportcontainern integrierte Sicherheitsmechanismen verwendet werden. Als primäre Technik hierfür hat sich der OASIS-Standard WS-Security etabliert. Dabei sollte eine Authentisierung und Autorisierung basierend auf SAML (Security Assertion Markup Language) eingesetzt werden.

**Umsetzung**

Bei der Umsetzung eines SOA-basierten Ansatzes ist darauf zu achten, dass die Kommunikation zwischen den Teilnehmern (z. B. Client, Server) abgesichert ist (M 4.450 *Absicherung der Kommunikation bei Web-Services*) und die Ressourcen vor einer Blockade geschützt sind (siehe M 4.405 *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*). Außerdem muss eine geeignete Ein- und Ausgabevalidierung umgesetzt werden (siehe M 4.393 *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*). Wenn innerhalb einer SOA vertrauliche Daten übertragen werden, sind zudem die XML-Transportcontainer zu schützen (siehe M 4.473 *Schutz vor Abhören von XML-Transportcontainern in einer SOA*). Weiterhin sollten durch vorgeschaltete Authentisierungs- und Autorisierungsmechanismen die Angriffschancen auf die Backend-Anwendungen eingeschränkt werden (siehe M 4.474 *Schutz vor Schwachstellen in Backend-Anwendungen einer SOA*).

**Betrieb**

Es muss verhindert werden, dass die Benutzer die Benutzerumgebung in einer verteilten SOA-Umgebung verändern. Außerdem ist sicherzustellen, dass sie nur auf Ressourcen zugreifen können, auf die sie auch zugreifen sollen (siehe M 4.453 *Einsatz eines Security Token Service (STS)* sowie M 4.480 *Schutz von WS-Resource in SOA-Umgebungen*). Läuft die Verbindung zwischen einem Service-Consumer und einem Service-Provider über ein unsicheres Netz, sind Vorkehrungen zu treffen, damit die Kommunikation nicht belauscht, verändert oder gestört werden kann (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

**Notfallvorsorge**

Ein Ausfall einzelner Dienste innerhalb einer SOA-Umgebung sollte weitestgehend durch die Nutzung redundanter Diensterbringer ausgeglichen werden können (siehe M 6.161 *Redundante Hardware-Komponenten in serviceorientierten Architekturen*). Da vom Ausfall einzelner Service-Provider zumeist eine größere Anzahl Anwender betroffen sein kann, sind Maßnahmen zu ergreifen, damit der daraus resultierende Schaden verringert wird. In einem Business Continuity Plan sind daher alle Maßnahmen zu beschreiben, die erforderlich sind, falls es aufgrund eines Ausfalls einzelner Service-Provider nur noch zu einem eingeschränkten Betrieb innerhalb einer SOA-Umgebung kommt (siehe M 6.160 *Notfallvorsorgekonzept für SOA-Umgebungen*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "SOA" vorgestellt.

**Planung und Konzeption**

- M 2.1 (A) *Festlegung von Verantwortlichkeiten und Regelungen*
- M 2.378 (Z) *System-Entwicklung*
- M 2.560 (Z) *Integration eines SOA-basierten Need-to-share-Konzepts in das Sicherheitsmanagement*
- M 2.561 (W) *Erstellen spezifikationskonformer SOA-Implementierungen und Konfigurationen*
- M 5.68 (Z) *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*

**Umsetzung**

- M 2.447 (A) *Sicherer Einsatz virtueller IT-Systeme*
- M 4.393 (B) *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*
- M 4.400 (B) *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*
- M 4.405 (C) *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*
- M 4.450 (A) *Absicherung der Kommunikation bei Web-Services*
- M 4.453 (Z) *Einsatz eines Security Token Service (STS)*
- M 4.454 (A) *Schutz vor unerlaubter Nutzung von Web-Services*
- M 4.473 (B) *Schutz vor Abhören von XML-Transportcontainern in einer SOA*
- M 4.474 (C) *Schutz vor Schwachstellen in Backend-Anwendungen einer SOA*
- M 4.475 (B) *Schutz vor Spoofing-Angriffen auf Identitätsdienste*
- M 5.175 (Z) *Einsatz eines XML-Gateways*

**Betrieb**

- M 3.5 (A) *Schulung zu Sicherheitsmaßnahmen*
- M 4.476 (B) *Schutz einer WS-Notification-Subscription im Broker*
- M 4.477 (B) *Schutz einer WS-Notification*
- M 4.478 (C) *Schlüsselmittelverwaltung bei SOA*
- M 4.479 (B) *Schutz von Richtlinien in einer SOA*
- M 4.480 (C) *Schutz von WS-Resource in SOA-Umgebungen*
- M 4.481 (C) *Sichere Nutzung verbindungsloser SOAP-Kommunikation*
- M 5.147 (C) *Absicherung der Kommunikation mit Verzeichnisdiensten*
- M 5.150 (Z) *Durchführung von Penetrationstests*

**Notfallvorsorge**

- M 6.160 (A) *Notfallvorsorgekonzept für SOA-Umgebungen*
- M 6.161 (Z) *Redundante Hardware-Komponenten in serviceorientierten Architekturen*
- M 6.162 (Z) *Reaktion bei praktischer Schwächung eines Kryptoverfahrens*

# B 5.27 Software-Entwicklung

## Beschreibung

Häufig hat verfügbare Standardsoftware nicht den erwarteten Funktionsumfang oder entspricht nicht den gewünschten Anforderungen. Ebenso existieren in vielen Institutionen bereits individuell entwickelte Software-Produkte, die veraltet sind oder um zusätzliche Funktionen erweitert werden müssen, um sie an neue bzw. geänderte Geschäftsprozesse anzupassen. Diese Anforderungen kann oft nur eine eigenentwickelte Software erfüllen.

Der Baustein Software-Entwicklung beschäftigt sich mit allen relevanten Aspekten, die von Institutionen bei der Verwendung von eigenentwickelter Software zu beachten sind. Hierzu werden Vorbereitung, Abwicklung und Inbetriebnahme seitens der Institution betrachtet und dementsprechende Gefährdungen und Maßnahmen ausgewählt.

Der Baustein stellt keine vollständige Anleitung zur generellen Vorgehensweise bei der Software-Entwicklung dar, sondern konzentriert sich auf die relevanten Aspekte der Informationssicherheit bei der Software-Entwicklung. Mit diesem Baustein werden die Bausteine B 5.25 *Allgemeine Anwendungen* und B 1.10 *Standardsoftware* um konkrete Umsetzungshinweise zur Eigenentwicklung von Software erweitert.

## Gefährdungslage

Für die Software-Entwicklung werden für den IT-Grundschutz die folgenden typischen Gefährdungen angenommen:

**Höhere Gewalt**

- G 1.2 *Ausfall von IT-Systemen*

**Organisatorische Mängel**

- G 2.1 *Fehlende oder unzureichende Regelungen*
- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.4 *Unzureichende Kontrolle der Sicherheitsmaßnahmen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.26 *Fehlendes oder unzureichendes Test- und Freigabeverfahren*
- G 2.27 *Fehlende oder unzureichende Dokumentation*
- G 2.28 *Verstöße gegen das Urheberrecht*
- G 2.29 *Softwaretest mit Produktionsdaten*
- G 2.66 *Unzureichendes Sicherheitsmanagement*
- G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*
- G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*
- G 2.209 *Auswahl einer ungeeigneten Entwicklungsumgebung für Software*
- G 2.210 *Unzureichend gesicherter Einsatz von Entwicklungsumgebungen*
- G 2.211 *Auswahl eines ungeeigneten Vorgehensmodells zur Software-Entwicklung*
- G 2.212 *Unzureichende Berücksichtigung von Konfigurationsoptionen bei der Software-Entwicklung*
- G 2.213 *Fehlende oder unzureichende Qualitätssicherung des Softwareentwicklungsprozesses*

**Menschliche Fehlhandlungen**

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.32 *Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren*

**Technisches Versagen**

- G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*
- G 4.35 *Unsichere kryptographische Algorithmen*
- G 4.39 *Software-Konzeptionsfehler*

**Vorsätzliche Handlungen**

- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.21 *Trojanische Pferde*
- G 5.23 *Schadprogramme*
- G 5.28 *Verhinderung von Diensten*
- G 5.71 *Vertraulichkeitsverlust schützenswerter Informationen*
- G 5.84 *Gefälschte Zertifikate*
- G 5.85 *Integritätsverlust schützenswerter Informationen*

**Maßnahmenempfehlungen**

Um einen Informationsverbund abzusichern, müssen gemäß den Ergebnissen der Modellierung nach IT-Grundschutz zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden.

Wenn die entwickelte Software im Produktivbetrieb eingesetzt wird, ist für die organisatorischen Aspekte der übergreifende Bausteins B 1.10 *Standardsoftware* zusätzlich zu beachten. Weiterhin beschreibt der Baustein B 5.25 *Allgemeine Anwendungen* Vorgehensweisen zum Einsatz von Software und ist immer gemeinsam mit diesem Baustein umzusetzen. Insbesondere die Phasen Betrieb, Aussonderung und Notfallvorsorge gelten hier gleichermaßen für individuell entwickelte Software. Bei der Entwicklung von Webanwendungen ist B 5.21 *Webanwendungen* zu beachten.

**Planung und Konzeption**

Eine sorgfältige Planung und Konzeption ist essenziell bei der Entwicklung von Software. Es sind die Verantwortlichkeiten festzulegen (siehe M 2.569 *Definition von Rollen und Verantwortlichkeiten bei der Software-Entwicklung*) und ein Vorgehensmodell auszuwählen (siehe M 2.570 *Auswahl eines Vorgehensmodells zur Software-Entwicklung*). Bei der gesamten Software-Entwicklung sind gesetzliche und regulatorische Vorgaben zu berücksichtigen (siehe M 2.571 *Berücksichtigung von Compliance-Anforderungen für die Software-Entwicklung*).

**Beschaffung**

Es muss eine geeignete Entwicklungsumgebung ausgewählt werden (siehe M 4.493 *Auswahl einer Entwicklungsumgebung für die Software-Entwicklung* und M 2.567 *Auswahl vertrauenswürdiger Entwicklungswerkzeuge*). Werkzeuge für die Software-Entwicklung sollten nach standardisierten, dokumentierten Vorgehensweisen beschafft werden (siehe M 2.572 *Beschaffung von Werkzeugen zur Software-Entwicklung*).

**Umsetzung**

Während der Software-Entwicklung muss die Entwicklungsumgebung sicher eingesetzt werden (siehe M 4.494 *Sicherer Einsatz einer Entwicklungsumgebung*). Das Design der Software muss möglichst sicher sein (siehe M 4.495 *Sicheres Systemdesign bei der Software-Entwicklung*) und ebenfalls möglichst sicher implementiert werden (siehe M 2.573 *Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung* und M 4.42 *Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung*). Die Ergebnisse der Software-Entwicklung müssen vor der produktiven Inbetriebnahme ausreichend getestet werden (siehe M 2.568 *Testverfahren für Software*). Der gesamte Entwicklungsprozess muss vollständig dokumentiert werden (siehe M 2.574 *Ausführliche Dokumentation der Software-Entwicklung*) und die beteiligten Mitarbeiter sind entsprechend zu schulen (siehe M 3.97 *Schulung des Projektteams für die Software-Entwicklung*).

**Betrieb**

Zur Inbetriebnahme muss die Software sicher installiert werden (siehe M 4.496 *Sichere Installation der entwickelten Software*). Relevante Patches und Updates müssen umgehend angewendet werden (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Änderungen an der Konfiguration müssen sorgfältig durchgeführt werden (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Die Integrität der Software ist regelmäßig zu überprüfen (siehe M 4.93 *Regelmäßige Integritätsprüfung*).

**Aussonderung**

Individuell entwickelte Software ist bei der Aussonderung analog zu Standardsoftware (siehe B 1.10 *Standardsoftware* und B 5.25 *Allgemeine Anwendungen*) zu behandeln.

**Notfallvorsorge**

Um eventuellen Ausfällen vorzubeugen, sind Maßnahmen zur Notfallvorsorge zu treffen (siehe M 6.164 *Notfallvorsorge bei der Software-Entwicklung*). Damit sich die Software-Entwicklung bei unerwarteten Datenverlusten auf den Entwicklungssystemen nicht verzögert, sind die Entwicklungsdaten regelmäßig zu sichern (siehe M 6.32 *Regelmäßige Datensicherung*).

**Planung und Konzeption**
- M 2.164 (A) *Auswahl eines geeigneten kryptographischen Verfahrens*
- M 2.569 (A) *Definition von Rollen und Verantwortlichkeiten bei der Software-Entwicklung*
- M 2.570 (A) *Auswahl eines Vorgehensmodells zur Software-Entwicklung*
- M 2.571 (A) *Berücksichtigung von Compliance-Anforderungen für die Software-Entwicklung*
- M 4.34 (Z) *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*

**Beschaffung**
- M 2.567 (Z) *Auswahl vertrauenswürdiger Entwicklungswerkzeuge*
- M 2.572 (Z) *Beschaffung von Werkzeugen zur Software-Entwicklung*
- M 4.493 (Z) *Auswahl einer Entwicklungsumgebung für die Software-Entwicklung*

**Umsetzung**
- M 2.568 (A) *Testverfahren für Software*
- M 2.573 (A) *Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung*
- M 2.574 (Z) *Ausführliche Dokumentation der Software-Entwicklung*
- M 3.97 (C) *Schulung des Projektteams für die Software-Entwicklung*
- M 4.42 (Z) *Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung*
- M 4.95 (A) *Minimales Betriebssystem*
- M 4.494 (B) *Sicherer Einsatz einer Entwicklungsumgebung*
- M 4.495 (A) *Sicheres Systemdesign bei der Software-Entwicklung*

**Betrieb**
- M 2.273 (A) *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*
- M 2.575 (Z) *Regelmäßige Sicherheitsaudits für die Software-Entwicklungsumgebung*
- M 4.33 (A) *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung*
- M 4.78 (A) *Sorgfältige Durchführung von Konfigurationsänderungen*
- M 4.93 (Z) *Regelmäßige Integritätsprüfung*
- M 4.496 (C) *Sichere Installation der entwickelten Software*

**Notfallvorsorge**
- M 6.32 (A) *Regelmäßige Datensicherung*
- M 6.41 (A) *Übungen zur Datenrekonstruktion*
- M 6.164 (A) *Notfallvorsorge bei der Software-Entwicklung*

# G 0 Gefährdungskatalog Elementare Gefährdungen

# G 0.1 Feuer

Feuer können schwere Schäden an Menschen, Gebäuden und deren Einrichtung verursachen. Neben direkten durch Feuer verursachten Schäden lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- unsachgemäße Lagerung brennbarer Materialien (z. B. Altpapier),
- Nichtbeachtung der einschlägigen Normen und Vorschriften zur Brandvermeidung,
- fehlende Brandmeldeeinrichtungen (z. B. Rauchmelder),
- fehlende oder nicht einsatzbereite Handfeuerlöscher oder automatische Löscheinrichtungen (z. B. Gaslöschanlagen),
- mangelhaften vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen oder Verwendung ungeeigneter Dämmmaterialien zur Wärme- und Schallisolierung).

**Beispiele:**

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte, wie z. B. Kaffeemaschinen oder Tischleuchten, unsachgemäß installiert oder aufgestellt sind und dadurch Brände verursachen.

# G 0.2 Ungünstige klimatische Bedingungen

Ungünstige klimatische Bedingungen wie Hitze, Frost oder hohe Luftfeuchtigkeit können zu Schäden verschiedenster Art führen, beispielsweise zu Fehlfunktionen in technischen Komponenten oder zur Beschädigung von Speichermedien. Häufige Schwankungen der klimatischen Bedingungen verstärken diesen Effekt. Ungünstige klimatische Bedingungen können auch dazu führen, dass Menschen nicht mehr arbeiten können oder sogar verletzt oder getötet werden.

Jeder Mensch und jedes technische Gerät hat einen Temperaturbereich, innerhalb dessen seine normale Arbeitsweise bzw. ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Umgebungstemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Arbeitsausfällen, Betriebsstörungen oder zu Geräteausfällen kommen.

So wird z. B. in einem Serverraum durch die darin befindlichen Geräte elektrische Energie in Wärme umgesetzt und daher der Raum aufgeheizt. Bei unzureichender Lüftung kann die zulässige Betriebstemperatur der Geräte überschritten werden. Bei Sonneneinstrahlung in den Raum können Temperaturen über 50°C erreicht werden.

Zu Lüftungszwecken werden oft unerlaubt Fenster von Serverräumen geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

Bei der Lagerung von digitalen Langzeitspeichermedien können zu große Temperaturschwankungen oder zu große Luftfeuchtigkeit zu Datenfehlern und reduzierter Speicherdauer führen. Einige Hersteller geben die optimalen Lagerbedingungen für Langzeitspeichermedien mit Temperaturen von 20 bis 22°C und einer Luftfeuchtigkeit von 40% an. Auch analoge Speichermedien, wie Papier oder Mikrofilme, benötigen bestimmte Lagerbedingungen. Wird Papier beispielsweise zu feucht gelagert, kann es schimmeln oder sich auflösen.

**Beispiele:**

- Bei hochsommerlichen Temperaturen und unzureichender Kühlung kann es bei IT-Geräten zu temperaturbedingten Ausfällen kommen.
- Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen.
- Durch zu hohe Temperaturen können magnetische Datenträger entmagnetisiert werden.

# G 0.3 Wasser

Durch Wasser kann die Integrität und Verfügbarkeit von Informationen beeinträchtigt werden, die auf analogen und digitalen Datenträgern gespeichert sind. Auch Informationen im Arbeitsspeicher von IT-Systemen sind gefährdet. Der unkontrollierte Eintritt von Wasser in Gebäude oder Räume kann beispielsweise bedingt sein durch:

- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Besonders wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

Probleme können außerdem durch Frost entstehen. Beispielsweise können Rohre in frostgefährdeten Bereichen undicht werden, wenn darin Wasser bei anhaltendem Frost stillsteht. Auch eine vorhandene Wärmedämmung wird mit der Zeit vom Frost überwunden.

**Beispiel:**

- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskartonelementen verkleidet war. Als eine Verbindung der Wasserleitung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils komplett abgeschaltet werden musste.

# G 0.4 Verschmutzung, Staub, Korrosion

Viele IT-Geräte enthalten neben der Elektronik auch mechanisch arbeitende Komponenten, wie z. B. bei Fest- und Wechselplatten, DVD-Laufwerken, Druckern, Scannern etc., aber auch Lüftern von Prozessoren und Netzteilen. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch folgende Tätigkeiten in größerem Maße entstehen:

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor).

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den direkten Schaden am Gerät, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

Die Geräte und die Infrastruktur können außerdem durch Korrosion angegriffen werden. Dies kann sich nicht nur auf die IT, sondern sogar auf die Sicherheit von Gebäuden negativ auswirken.

Durch Korrosion können auch indirekt weitere Gefährdungen entstehen. So kann beispielsweise Wasser aus korrodierten Stellen austreten (siehe G 0.3 *Wasser*).

Insgesamt können Verschmutzung, Staub oder Korrosion somit zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Als Folge kann die ordnungsgemäße Informationsverarbeitung beeinträchtigt werden.

**Beispiele:**

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Der Mitarbeiter hatte hierzu sein Büro für kurze Zeit verlassen. Nach Rückkehr an seinen Arbeitsplatz stellte er fest, dass sein PC nicht mehr funktionierte. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

# G 0.5 Naturkatastrophen

Unter Naturkatastrophen werden natürliche Veränderungen verstanden, die verheerende Auswirkungen auf Menschen und Infrastrukturen haben. Ursachen für eine Naturkatastrophe können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen und Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Zyklone. Je nach Standort der Institution ist diese den Risiken durch die verschiedenen Arten von Naturkatastrophen unterschiedlich stark ausgesetzt.

**Beispiele:**
- Für Rechenzentren in Hochwasser-gefährdeten Gebieten besteht oft in besonderem Maße die Gefahr, dass unkontrolliert Wasser in das Gebäude eindringt (Überschwemmungen oder Anstieg des Grundwasserspiegels).
- Die Häufigkeit von Erdbeben und somit auch das damit verbundene Risiko hängen stark von der geografischen Lage ab.
- Extrem erhöhte Solar-Aktivität hat in der Vergangenheit bereits mehrfach zu Beeinträchtigungen von Telekommunikationsinfrastrukturen und der Energieversorgung geführt.

Unabhängig von der Art der Naturkatastrophe besteht auch in nicht unmittelbar betroffenen Gebieten die Gefahr, dass Versorgungseinrichtungen, Kommunikationsverbindungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden. Besonders der Ausfall zentraler Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) kann sehr hohe Schäden nach sich ziehen. Betriebs- und Service-Personal kann aufgrund von großflächig eingerichteten Sperrbereichen der Zutritt zur Infrastruktur verwehrt werden.

**Beispiele:**
- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum "überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist von keiner Versicherung gedeckt.
- Ein IT-System wird an einem Standort untergebracht, dessen geografische Lage für vulkanische Aktivität bekannt ist (zeitweilig aussetzendes Phänomen, bei dem die Emissionsphasen mit zum Teil langen Ruhephasen abwechseln).

# G 0.6 Katastrophen im Umfeld

Eine Behörde bzw. ein Unternehmen kann Schaden nehmen, wenn sich im Umfeld ein schwerer Unglücksfall ereignet, zum Beispiel ein Brand, eine Explosion, die Freisetzung giftiger Substanzen oder das Austreten gefährlicher Strahlung. Gefahr besteht dabei nicht nur durch das Ereignis selbst, sondern auch durch die häufig daraus resultierenden Aktivitäten, beispielsweise Sperrungen oder Rettungsmaßnahmen.

Die Liegenschaften einer Institution können verschiedenen Gefährdungen aus dem Umfeld ausgesetzt sein, unter anderem durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetriebe oder Wohngebiete.

Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Solche Maßnahmen können auch dazu führen, dass Mitarbeiter ihre Arbeitsplätze nicht erreichen können oder Personal evakuiert werden muss. Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

**Beispiel:**

- Bei einem Brand in einem chemischen Betrieb in unmittelbarer Nähe eines Rechenzentrums (ca. 1000 m Luftlinie) entstand eine mächtige Rauchwolke. Das Rechenzentrum besaß eine Klima- und Lüftungsanlage, die über keine Außenluftüberwachung verfügte. Nur durch die Aufmerksamkeit eines Mitarbeiters (der Unfall geschah während der Arbeitszeit), der die Entstehung und Ausbreitung verfolgte, konnte die Außenluftzufuhr rechtzeitig manuell abgeschaltet werden.

# G 0.7 Großereignisse im Umfeld

Großveranstaltungen aller Art können zu Behinderungen des ordnungsgemäßen Betriebs einer Behörde bzw. eines Unternehmens führen. Hierzu gehören unter anderem Straßenfeste, Konzerte, Sportveranstaltungen, Arbeitskämpfe oder Demonstrationen. Ausschreitungen im Zusammenhang mit solchen Veranstaltungen können zusätzliche Auswirkungen, wie die Einschüchterung von Mitarbeitern bis hin zur Gewaltanwendung gegen das Personal oder das Gebäude, nach sich ziehen.

**Beispiele:**

- Während der heißen Sommermonate fand eine Demonstration in der Nähe eines Rechenzentrums statt. Die Situation eskalierte und es kam zu Gewalttätigkeiten. In einer Nebenstraße stand noch ein Fenster des Rechenzentrumsbereiches auf, durch das ein Demonstrant eindrang und die Gelegenheit nutzte, Hardware mit wichtigen Daten zu entwenden.
- Beim Aufbau einer Großkirmes wurde aus Versehen eine Stromleitung gekappt. Dies führte in einem hierdurch versorgten Rechenzentrum zu einem Ausfall, der jedoch durch die vorhandene Netzersatzanlage abgefangen werden konnte.

# G 0.8 Ausfall oder Störung der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Neben Störungen im Versorgungsnetz können jedoch auch Abschaltungen bei nicht angekündigten Arbeiten oder Kabelbeschädigungen bei Tiefbauarbeiten dazu führen, dass die Stromversorgung ausfällt.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Viele Infrastruktur-Einrichtungen sind heute vom Strom abhängig, z.B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen und Sprinkleranlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druck-Erzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig. Bei längeren Stromausfällen kann der Ausfall der Infrastruktur-Einrichtungen dazu führen, dass keinerlei Tätigkeiten mehr in den betroffenen Räumlichkeiten durchgeführt werden können.

Neben Ausfällen können auch andere Störungen der Stromversorgung den Betrieb beeinträchtigen. Überspannung kann beispielsweise zu Fehlfunktionen oder sogar zu Beschädigungen von elektrischen Geräten führen.

Zu beachten ist außerdem, dass durch Ausfälle oder Störungen der Stromversorgung in der Nachbarschaft unter Umständen auch die eigenen Geschäftsprozesse betroffen sein können, beispielsweise wenn Zufahrtswege blockiert werden.

**Beispiele:**

- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien (nach etwa 40 Minuten) fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die Energieversorger ihre Abschaltpläne geheim.
- Im November 2005 waren nach heftigen Schneefällen in Niedersachsen und Nordrhein-Westfalen viele Gemeinden tagelang ohne Stromversorgung, weil viele Hochspannungsmasten unter der Schnee- und Eislast umgestürzt waren. Die Wiederherstellung der Stromversorgung dauerte einige Tage.

# G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Für viele Geschäftsprozesse werden heutzutage zumindest zeitweise intakte Kommunikationsverbindungen benötigt, sei es über Telefon, Fax, E-Mail oder andere Dienste über Nah- oder Weitverkehrsnetze. Fallen einige oder mehrere dieser Kommunikationsverbindungen über einen längeren Zeitraum aus, kann dies beispielsweise dazu führen, dass

- Geschäftsprozesse nicht mehr weiterbearbeitet werden können, weil benötigte Informationen nicht abgerufen werden können,
- Kunden die Institution nicht mehr für Rückfragen erreichen können,
- Aufträge nicht abgegeben oder beendet werden können.

Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorhanden sind.

Zu ähnlichen Problemen kann es kommen, wenn die benötigten Kommunikationsnetze gestört sind, ohne jedoch vollständig auszufallen. Kommunikationsverbindungen können beispielsweise eine erhöhte Fehlerrate oder andere Qualitätsmängel aufweisen. Falsche Betriebsparameter können ebenfalls zu Beeinträchtigungen führen.

**Beispiele:**

- Das Internet ist heute für viele Institutionen zu einem unverzichtbaren Kommunikationsmedium geworden, unter anderem zum Abruf wichtiger Informationen, zur Außendarstellung sowie zur Kommunikation mit Kunden und Partnern. Unternehmen, die sich auf Internet-basierte Dienstleistungen spezialisiert haben, sind natürlich in besonderem Maße von einer funktionierenden Internet-Anbindung abhängig.
- Im Zuge der Konvergenz der Netze werden Sprach- und Datendienste häufig über die gleichen technischen Komponenten transportiert (z. B. VoIP). Dadurch steigt jedoch die Gefahr, dass bei einer Störung der Kommunikationstechnik die Sprachdienste und die Datendienste gleichzeitig ausfallen.

# G 0.10 Ausfall oder Störung von Versorgungsnetzen

Es gibt in einem Gebäude eine Vielzahl von Netzen, die der grundlegenden Ver- und Entsorgung und somit als Basis für alle Geschäftsprozesse einer Institution einschließlich der IT dienen. Beispiele für solche Versorgungsnetze sind:

- Strom,
- Telefon,
- Kühlung,
- Heizung bzw. Lüftung,
- Wasser und Abwasser,
- Löschwasserspeisungen,
- Gas,
- Melde- und Steueranlagen (z. B. für Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen.

Der Ausfall oder die Störung eines Versorgungsnetzes kann unter anderem dazu führen, dass Menschen nicht mehr im Gebäude arbeiten können oder dass der IT-Betrieb und somit die Informationsverarbeitung beeinträchtigt wird.

Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

**Beispiele:**

- Ein Ausfall von Heizung oder Lüftung kann zur Folge haben, dass alle Mitarbeiter die betroffenen Gebäude verlassen müssen. Dies kann unter Umständen hohe Schäden nach sich ziehen.
- Der Ausfall der Stromversorgung wirkt nicht nur auf die IT direkt, sondern auch auf alle anderen Netze, die mit elektrisch betriebener Steuer- und Regeltechnik ausgestattet sind. Selbst in Abwasserleitungen sind unter Umständen elektrische Hebepumpen vorhanden.
- Der Ausfall der Wasserversorgung beeinträchtigt eventuell die Funktion von Klimaanlagen.

# G 0.11 Ausfall oder Störung von Dienstleistern

Kaum eine Institution arbeitet heute noch ohne Dienstleister wie Zulieferer oder Outsourcing-Anbieter. Wenn Organisationseinheiten von Dienstleistern abhängig sind, kann durch Ausfälle externer Dienstleistungen die Aufgabenbewältigung beeinträchtigt werden. Der teilweise oder vollständige Ausfall eines Outsourcing-Dienstleisters oder eines Zulieferers kann sich erheblich auf die betriebliche Kontinuität auswirken, insbesondere bei kritischen Geschäftsprozessen. Es gibt verschiedene Ursachen für solche Ausfälle, beispielsweise Insolvenz, einseitige Kündigung des Vertrags durch den Dienstleister oder Zulieferer, betriebliche Probleme beispielsweise durch Naturgewalten oder Personalausfall. Probleme können auch entstehen, wenn die vom Dienstleister erbrachten Leistungen nicht den Qualitätsanforderungen des Auftraggebers entsprechen.

Zu beachten ist außerdem, dass Dienstleister ebenfalls häufig auf Unterauftragnehmer zurückgreifen, um ihre Leistungen gegenüber dem Auftraggeber zu erbringen. Störungen, Qualitätsmängel und Ausfälle seitens der Unterauftragnehmer können dadurch indirekt zu Beeinträchtigungen beim Auftraggeber führen.

Auch durch Ausfälle von IT-Systemen beim Dienstleister oder der Kommunikationsanbindungen zu diesem können Geschäftsprozesse beim Auftraggeber beeinträchtigt werden.

Eine gegebenenfalls notwendige Rückholung ausgelagerter Prozesse kann stark erschwert sein, beispielsweise weil die ausgelagerten Verfahren nicht hinreichend dokumentiert sind oder weil der bisherige Dienstleister die Rückholung nicht unterstützt.

**Beispiele:**

- Ein Unternehmen hat seine Server in einem Rechenzentrum eines externen Dienstleisters installiert. Nach einem Brand in diesem Rechenzentrum war die Finanzabteilung des Unternehmens nicht mehr handlungsfähig. Es entstanden erhebliche finanzielle Verluste für das Unternehmen.
- Die Just-in-Time-Produktion eines Unternehmens war von der Zulieferung von Betriebsmitteln externer Dienstleister abhängig. Nachdem ein LKW durch einen Defekt beim Dienstleister ausfiel, verzögerte sich die Lieferung dringend benötigter Teile drastisch. Eine Reihe von Kunden konnte dadurch nicht fristgerecht beliefert werden.
- Ein Bankinstitut wickelte alle Geldtransporte mit einem Werttransportunternehmen ab. Das Werttransportunternehmen meldete überraschend Konkurs an. Die Vereinbarung und Tourenplanung mit einem neuen Werttransporter dauerte mehrere Tage. Als Folge kam es zu erheblichen Problemen und Zeitverzögerungen bei der Geldversorgung und -entsorgung der Bankfilialen.

# G 0.12 Elektromagnetische Störstrahlung

Informationstechnik setzt sich heute zu einem großen Teil aus elektronischen Komponenten zusammen. Zwar wird zunehmend auch optische Übertragungstechnik eingesetzt, dennoch enthalten beispielsweise Computer, Netzkoppelelemente und Speichersysteme in der Regel sehr viele elektronische Bauteile. Durch elektromagnetische Störstrahlung, die auf solche Bauteile einwirkt, können elektronische Geräte in ihrer Funktion beeinträchtigt oder sogar beschädigt werden. Als Folge kann es unter anderem zu Ausfällen, Störungen, falschen Verarbeitungsergebnissen oder Kommunikationsfehlern kommen.

Auch drahtlose Kommunikation kann durch elektromagnetische Störstrahlung beeinträchtigt werden. Hierzu reicht unter Umständen eine ausreichend starke Störung der verwendeten Frequenzbänder.

Weiterhin können Informationen, die auf bestimmten Arten von Datenträgern gespeichert sind, durch elektromagnetische Störstrahlung gelöscht oder verfälscht werden. Dies betrifft insbesondere magnetisierbare Datenträger (Festplatten, Magnetbänder etc.) und Halbleiter-Speicher. Auch eine Beschädigung solcher Datenträger durch elektromagnetische Störstrahlung ist möglich.

Es gibt viele unterschiedliche Quellen elektromagnetischer Felder oder Strahlung, zum Beispiel Funknetze wie WLAN, Bluetooth, GSM, UMTS etc., Dauermagnete und kosmische Strahlung. Außerdem strahlt jedes elektrische Gerät mehr oder weniger starke elektromagnetische Wellen ab, die sich unter anderem durch die Luft und entlang metallischer Leiter (z. B. Kabel, Klimakanäle, Heizungsrohre etc.) ausbreiten können.

In Deutschland enthält das Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) Regelungen zu diesem Thema.

# G 0.13 Abfangen kompromittierender Strahlung

Elektrische Geräte strahlen elektromagnetische Wellen ab. Bei Geräten, die Informationen verarbeiten (z. B. Computer, Bildschirme, Netzkoppelelemente, Drucker), kann diese Strahlung auch die gerade verarbeiteten Informationen mit sich führen. Derartige informationstragende Abstrahlung wird bloßstellende oder kompromittierende Abstrahlung genannt. Ein Angreifer, der sich beispielsweise in einem Nachbarhaus oder in einem in der Nähe abgestellten Fahrzeug befindet, kann versuchen, diese Abstrahlung zu empfangen und daraus die verarbeiteten Informationen zu rekonstruieren. Die Vertraulichkeit der Informationen ist damit in Frage gestellt. Eine mögliche Zielsetzung eines solchen Angriffes ist Industriespionage.

Die Grenzwerte des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) reichen im Allgemeinen nicht aus, um das Abfangen der bloßstellenden Abstrahlung zu verhindern. Falls dieses Risiko nicht akzeptiert werden kann, müssen deshalb in aller Regel zusätzliche Schutzmaßnahmen getroffen werden.

Bloßstellende Abstrahlung ist nicht auf elektromagnetische Wellen beschränkt. Auch aus Schallwellen, zum Beispiel bei Druckern oder Tastaturen, können unter Umständen nützliche Informationen gewonnen werden.

Zu beachten ist außerdem, dass bloßstellende Abstrahlung in bestimmten Fällen auch durch äußere Manipulation von Geräten verursacht oder verstärkt werden kann. Wird zum Beispiel ein Gerät mit elektromagnetischen Wellen bestrahlt, kann es passieren, dass die reflektierten Wellen vertrauliche Informationen mit sich führen.

# G 0.14 Ausspähen von Informationen / Spionage

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Unternehmen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Die aufbereiteten Informationen können dann beispielsweise eingesetzt werden, um einem anderem Unternehmen bestimmte Wettbewerbsvorteile zu verschaffen, Personen zu erpressen oder ein Produkt nachbauen zu können.

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen, beispielsweise indem Informationen aus mehreren öffentlich zugänglichen Quellen zusammengeführt werden, die einzeln unverfänglich aussehen, aber in anderen Zusammenhängen kompromittierend sein können. Da vertrauliche Daten häufig nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischem Weg ausgespäht werden.

**Beispiele:**

- Viele IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Benutzerkennung- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist es einem Angreifer unter Umständen möglich, dieses auszulesen.
- Um Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN für die verwendete ec- oder Kreditkarte eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass ein Angreifer einem Kunden bei der Eingabe der PIN ohne Mühe über die Schulter schauen kann. Wenn der Angreifer hinterher die Karte stiehlt, kann er damit das Konto plündern.
- Um Zugriffsrechte auf einem PC zu erhalten oder diesen anderweitig zu manipulieren, kann ein Angreifer dem Benutzer ein Trojanisches Pferd schicken, das er als vorgeblich nützliches Programm einer E-Mail beigefügt hat. Neben unmittelbaren Schäden können über Trojanische Pferde vielfältige Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausgespäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.
- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können Kollegen, aber auch Besucher eventuell Gespräche mithören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

# G 0.15 Abhören

Mit Abhören werden gezielte Angriffe auf Kommunikationsverbindungen, Gespräche, Geräuschquellen aller Art oder IT-Systeme zur Informationssammlung bezeichnet. Dies beginnt beim unbemerkten, heimlichen Belauschen eines Gesprächs und reicht bis zu hoch technisierten komplexen Angriffen, um über Funk oder Leitungen gesendete Signale abzufangen, z. B. mit Hilfe von Antennen oder Sensoren.

Nicht nur wegen des geringen Entdeckungsrisikos ist das Abhören von Leitungen oder Funkverbindungen eine nicht zu vernachlässigende Gefährdung der Informationssicherheit. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich der erforderliche Aufwand zum Abhören unterscheidet die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischen Aufwand feststellbar.

Besonders kritisch ist die ungeschützte Übertragung von Authentisierungsdaten bei Klartextprotokollen wie HTTP, FTP oder Telnet, da diese durch die klare Strukturierung der Daten leicht automatisch zu analysieren sind.

Der Entschluss, irgendwo Informationen abzuhören, wird im Wesentlichen durch die Frage bestimmt, ob die Informationen den technischen bzw. den finanziellen Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig.

**Beispiele:**

- Bei Telefonaten kann für einen Angreifer nicht nur das Abhören von Gesprächen interessant sein. Auch die Informationen, die bei der Signalisierung übertragen werden, können von einem Angreifer missbraucht werden, z. B. falls durch eine fehlerhafte Einstellung im Endgerät das Passwort bei der Anmeldung im Klartext übertragen wird.
- Bei ungeschützter oder unzureichend geschützter Funkübertragung (z. B. wenn ein WLAN nur mit WEP abgesichert wird), kann ein Angreifer leicht die gesamte Kommunikation abhören.
- E-Mails können während ihres gesamten Weges durch das Netz gelesen werden, wenn sie nicht verschlüsselt sind. Unverschlüsselte E-Mails sollten daher nicht mit klassischen Briefen, sondern mit Postkarten verglichen werden.

# G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Wenn durch den Diebstahl vertrauliche Informationen offengelegt werden, kann dies weitere Schäden nach sich ziehen. Neben Servern und anderen teuren IT-Systemen werden auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig gestohlen. Es gibt aber auch Fälle, in denen gezielt Datenträger, wie Dokumente oder USB-Sticks, entwendet wurden, um an die darauf gespeicherten vertraulichen Informationen zu gelangen.

**Beispiele:**

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptographisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Ob Akten kopiert oder manipuliert wurden, konnte nicht zweifelsfrei ausgeschlossen werden.
- In Großbritannien gab es eine Reihe von Datenpannen, bei denen vertrauliche Unterlagen offengelegt wurden, weil Datenträger gestohlen wurden. In einem Fall wurden bei der britischen Luftwaffe mehrere Computer-Festplatten gestohlen, die sehr persönliche Informationen enthielten, die zur Sicherheitsüberprüfung von Mitarbeitern erfasst worden waren.
- Ein Mitarbeiter eines Call-Centers erstellte, kurz bevor er das Unternehmen verlassen musste, Kopien einer großen Menge von vertraulichen Kundendaten. Nach seinem Ausscheiden aus dem Unternehmen hat er diese Daten dann an Wettbewerber verkauft. Da anschließend Details über den Vorfall an die Presse gelangten, verlor das Call-Center viele wichtige Kunden.

# G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

Es gibt eine Vielzahl von Ursachen, die zu einem Verlust von Geräten, Datenträgern und Dokumenten führen können. Hierdurch ist unmittelbar die Verfügbarkeit betroffen, es können aber auch vertrauliche Informationen in fremde Hände gelangen, wenn die Datenträger nicht komplett verschlüsselt sind. Durch die Wiederbeschaffung von Geräten oder Datenträgern entstehen Kosten, aber auch, wenn diese wieder auftauchen, können Informationen offengelegt oder unerwünschte Programme aufgespielt worden sein.

Besonders mobile Endgeräte und mobile Datenträger können leicht verloren gehen. Auf kleinen Speicherkarten können heute riesige Datenmengen gespeichert werden. Es kommt aber auch immer wieder vor, dass Dokumente in Papierform versehentlich liegen gelassen werden, beispielsweise in Gaststätten oder Verkehrsmitteln.

**Beispiele:**

- Eine Mitarbeiterin nutzt in der Straßenbahn die Fahrt zum Arbeitsplatz, um einige Unterlagen zu sichten. Als sie hektisch an der Zielhaltestelle aussteigt, lässt sie die Papiere versehentlich auf ihrem Nachbarplatz liegen. Zwar sind die Unterlagen nicht vertraulich, in der Folge müssen jedoch mehrere Unterschriften hochrangiger Führungskräfte erneut eingeholt werden.
- Auf einer Großveranstaltung fällt einem Mitarbeiter beim Suchen in seiner Aktentasche versehentlich und unbemerkt eine Speicherkarte mit vertraulichen Kalkulationen auf den Boden. Der Finder sichtet den Inhalt auf seinem Laptop und verkauft die Informationen an die Konkurrenz.
- Ein Hersteller sendet CDs mit Software-Updates zur Fehlerbehebung per Post an seine Kunden. Einige dieser CDs gehen auf dem Versandweg verloren, ohne dass Absender oder Empfänger darüber informiert werden. Als Folge kommt es bei den betroffenen Kunden zu Fehlfunktionen der Software.

# G 0.18 Fehlplanung oder fehlende Anpassung

Wenn organisatorische Abläufe, die direkt oder indirekt der Informationsverarbeitung dienen, nicht sachgerecht gestaltet sind, kann dies zu Sicherheitsproblemen führen. Obwohl jeder einzelne Prozessschritt korrekt durchgeführt wird, kommt es oft zu Schäden, weil Prozesse insgesamt fehlerhaft definiert sind.

Eine weitere mögliche Ursache für Sicherheitsprobleme sind Abhängigkeiten mit anderen Prozessen, die selbst keinen offensichtlichen Bezug zur Informationsverarbeitung haben. Solche Abhängigkeiten können bei der Planung leicht übersehen werden und dadurch Beeinträchtigungen während des Betriebes auslösen.

Sicherheitsprobleme können außerdem dadurch entstehen, dass Aufgaben, Rollen oder Verantwortung nicht eindeutig zugewiesen sind. Unter anderem kann es dadurch passieren, dass Abläufe verzögert, Sicherheitsmaßnahmen vernachlässigt oder Regelungen missachtet werden.

Gefahr besteht auch, wenn Geräte, Produkte, Verfahren oder andere Mittel zur Realisierung der Informationsverarbeitung nicht sachgerecht eingesetzt werden. Die Auswahl eines ungeeigneten Produktes oder Schwachstellen beispielsweise in der Anwendungsarchitektur oder im Netzdesign können zu Sicherheitsproblemen führen.

**Beispiele:**

- Wenn Wartungs- oder Reparaturprozesse nicht auf die fachlichen Anforderungen abgestimmt sind, kann es dadurch zu inakzeptablen Ausfallzeiten kommen.
- Es kann ein erhöhtes Risiko durch Angriffe auf die eigenen IT-Systeme entstehen, wenn sicherheitstechnische Anforderungen bei der Beschaffung von Informationstechnik nicht berücksichtigt werden.
- Wenn benötigtes Verbrauchsmaterial nicht zeitgerecht zur Verfügung gestellt wird, können die davon abhängigen IT-Verfahren ins Stocken geraten.
- Es können Schwachstellen entstehen, wenn bei der Planung eines IT-Verfahrens ungeeignete Übertragungsprotokolle ausgewählt werden.

Die Informationstechnik und das gesamte Umfeld einer Behörde bzw. eines Unternehmens ändern sich ständig. Sei es, dass Mitarbeiter ausscheiden oder hinzukommen, neue Hard- oder Software beschafft wird oder ein Zulieferbetrieb Konkurs anmeldet. Werden die dadurch notwendigen organisatorischen und technischen Anpassungen nicht oder nur ungenügend berücksichtigt, können sich Gefährdungen ergeben.

**Beispiele:**

- Durch bauliche Änderungen im Gebäude werden bestehende Fluchtwege verändert. Da die Mitarbeiter nicht ausreichend unterrichtet wurden, kann das Gebäude nicht in der erforderlichen Zeit geräumt werden.
- Bei der Übermittlung elektronischer Dokumente wird nicht darauf geachtet, ein für die Empfängerseite lesbares Datenformat zu verwenden.

# G 0.19 Offenlegung schützenswerter Informationen

Vertrauliche Daten und Informationen dürfen nur den zur Kenntnisnahme berechtigten Personen zugänglich sein. Neben der Integrität und der Verfügbarkeit gehört die Vertraulichkeit zu den Grundwerten der Informationssicherheit. Für vertrauliche Informationen (wie Passwörter, personenbezogene Daten, Firmen- oder Amtsgeheimnisse, Entwicklungsdaten) besteht die inhärente Gefahr, dass diese durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen offengelegt werden.

Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (USB-Sticks, CDs oder DVDs),
- in gedruckter Form auf Papier (Ausdrucke, Akten) und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie Informationen offengelegt werden, kann sehr unterschiedlich sein, zum Beispiel:

- unbefugtes Auslesen von Dateien,
- unbedachte Weitergabe, z. B. im Zuge von Reparaturaufträgen,
- unzureichende Löschung oder Vernichtung von Datenträgern,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen,
- Infektion von IT-Systemen mit Schadprogrammen,
- Mitlesen am Bildschirm oder Abhören von Gesprächen.

Werden schützenswerte Informationen offengelegt, kann dies schwerwiegende Folgen für eine Institution haben. Unter anderem kann der Verlust der Vertraulichkeit zu folgenden negativen Auswirkungen für eine Institution führen:

- Verstoß gegen Gesetze, zum Beispiel Datenschutz, Bankgeheimnis,
- Negative Innenwirkung, zum Beispiel Demoralisierung der Mitarbeiter,
- Negative Außenwirkung, zum Beispiel Beeinträchtigung der Beziehungen zu Geschäftspartnern, verlorenes Vertrauen von Kunden,
- Finanzielle Auswirkungen, zum Beispiel Schadensersatzansprüche, Bußgelder, Prozesskosten,
- Beeinträchtigung des informationellen Selbstbestimmungsrechtes.

Ein Verlust der Vertraulichkeit wird nicht immer sofort bemerkt. Oft stellt sich erst später heraus, z. B. durch Presseanfragen, dass Unbefugte sich Zugang zu vertraulichen Informationen verschafft haben.

**Beispiel:**

- Käufer von gebrauchten Rechnern, Festplatten, Mobiltelefonen oder ähnlichen Geräten finden darauf immer wieder höchst vertrauliche Informationen wie Patientendaten oder Kontonummern.

# G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Wenn Informationen, Software oder Geräte verwendet werden, die aus unzuverlässigen Quellen stammen oder deren Herkunft und Korrektheit nicht ausreichend geprüft wurden, kann der Einsatz hohe Gefahren mit sich bringen. Dies kann unter anderem dazu führen, dass geschäftsrelevante Informationen auf einer falschen Datenbasis beruhen, dass Berechnungen falsche Ergebnisse liefern oder dass falsche Entscheidungen getroffen werden. Ebenso können aber auch Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden.

**Beispiele:**

- Ein Empfänger kann durch E-Mails, deren Herkunft er nicht geprüft hat, dazu verleitet werden, bestimmte Aktionen durchzuführen, die sich für ihn oder andere nachteilig auswirken. Beispielsweise kann die E-Mail interessante Anhänge oder Links enthalten, die beim Anklicken dazu führen, dass Schadsoftware beim Empfänger installiert wird. Der Absender der E-Mail kann dabei gefälscht oder dem eines bekannten Kommunikationspartners nachgeahmt sein.
- Die Annahme, dass eine Angabe wahr ist, weil es "in der Zeitung steht" oder "im TV ausgestrahlt wurde", ist nicht immer gerechtfertigt. Dadurch können falsche Aussagen in geschäftskritische Berichte eingearbeitet werden.
- Die Zuverlässigkeit von Informationen, die über das Internet verbreitet werden, ist sehr unterschiedlich. Wenn Ausführungen ohne weitere Quellenprüfungen aus dem Internet übernommen werden, können daraus Fehlentscheidungen resultieren.
- Wenn Updates oder Patches aus nicht vertrauenswürdigen Quellen eingespielt werden, kann dies zu unerwünschten Nebenwirkungen führen. Wenn die Herkunft von Software nicht überprüft wird, besteht ein erhöhtes Risiko, dass IT-Systeme mit schädlichem Code infiziert werden.

# G 0.21 Manipulation von Hard- oder Software

Als Manipulation wird jede Form von gezielten, aber heimlichen Eingriffen bezeichnet, um Zielobjekte aller Art unbemerkt zu verändern. Manipulationen an Hard- oder Software können unter anderem aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden. Im Fokus können dabei Geräte aller Art, Zubehör, Datenträger (z. B. DVDs, USB-Sticks), Applikationen, Datenbanken oder ähnliches stehen.

Manipulationen an Hard- und Software führen nicht immer zu einem unmittelbaren Schaden. Wenn jedoch die damit verarbeiteten Informationen beeinträchtigt werden, kann dies alle Arten von Sicherheitsauswirkungen nach sich ziehen (Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit). Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse der Täter sind und je tiefgreifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen. Manipulationen können dadurch auch erhebliche Ausfallzeiten nach sich ziehen.

**Beispiele:**

- In einem Schweizer Finanzunternehmen hatte ein Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Dadurch war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Durch Manipulationen an Geldausgabeautomaten ist es Angreifern mehrfach gelungen, die auf Zahlungskarten gespeicherten Daten unerlaubt auszulesen. In Verbindung mit ausgespähten PINs wurden diese Daten dann später missbraucht, um Geld zulasten der Karteninhaber abzuheben.

# G 0.22 Manipulation von Informationen

Informationen können auf vielfältige Weise manipuliert werden, z. B. durch fehlerhaftes oder vorsätzlich falsches Erfassen von Daten, inhaltliche Änderung von Datenbank-Feldern oder von Schriftverkehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.

Archivierte Dokumente stellen meist schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.

Manipulationen an Informationen können unter anderem aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden.

**Beispiel:**

- Eine Mitarbeiterin hat sich über die Beförderung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin unerlaubt Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das veröffentlichte Jahresergebnis des Unternehmens genommen.

# G 0.23 Unbefugtes Eindringen in IT-Systeme

Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass darüber unbefugt auf das IT-System zugegriffen wird.

**Beispiele:**

- Wenn eine Benutzerkennung und das zugehörige Passwort ausgespäht werden, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.
- Über unzureichend gesicherte Fernwartungszugänge könnten Hacker unerlaubt auf IT-Systeme zugreifen.
- Bei unzureichend gesicherten Schnittstellen von aktiven Netzkomponenten ist es denkbar, dass Angreifer einen unberechtigten Zugang zur Netzkomponente erlangen. Wenn es ihnen außerdem gelingt, die lokalen Sicherheitsmechanismen zu überwinden, also z.B. an administrative Berechtigungen gelangt sind, könnten sie alle Administrationstätigkeiten ausüben.
- Viele IT-Systeme haben Schnittstellen für den Einsatz austauschbarer Datenspeicher, wie z. B. Zusatzspeicherkarten oder USB-Speichermedien. Bei einem unbeaufsichtigten IT-System mit der entsprechenden Hard- und Software besteht die Gefahr, dass hierüber große Datenmengen unbefugt ausgelesen oder Schadprogramme eingeschleust werden können.

# G 0.24 Zerstörung von Geräten oder Datenträgern

Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, Geräte, Zubehör, Schriftstücke und andere Datenträger (z. B. DVDs, USB-Sticks) oder ähnliches zu zerstören. Die Zerstörung von Datenträgern oder IT-Systemen kann erhebliche Ausfallzeiten für Geschäftsprozesse nach sich ziehen.

Durch Fahrlässigkeit, unsachgemäße Verwendung aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Datenträgern kommen, die den Betrieb des IT-Systems empfindlich stören können.

Es besteht außerdem die Gefahr, dass durch die Zerstörung wichtige Informationen verloren gehen, die nicht oder nur mit großem Aufwand rekonstruiert werden können.

**Beispiele:**

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteillüfter mit einem hinter dem Server versteckt aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt, und der Server fiel für mehrere Tage aus.
- Ein Mitarbeiter hatte sich über das wiederholte Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Hierbei wurde die Festplatte durch Fußtritte gegen den Rechner so stark beschädigt, dass sie unbrauchbar wurde. Die hier gespeicherten Daten konnten nur teilweise wieder durch ein Backup vom Vortag rekonstruiert werden.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen.

# G 0.25 Ausfall von Geräten oder Systemen

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs und damit dem Ausfall wichtiger Geschäftsprozesse führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. Server und Netzkoppelelemente. Auch der Ausfall von einzelnen Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des gesamten Informationsverbunds beitragen.

Ursache für den Ausfall eines IT-Systems ist nicht immer technisches Versagen (z. B. G 0.8 *Ausfall oder Störung der Stromversorgung*). Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 0.24 *Zerstörung von Geräten oder Datenträgern*) oder vorsätzliche Handlungen (z. B. G 0.16 *Diebstahl von Geräten, Datenträgern oder Dokumenten*, G 0.41 *Sabotage*) zurückführen. Auch mangelnde Wartung, beispielsweise durch Ausfall des Wartungspersonals, kann zu technischem Versagen führen. Durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können ebenfalls Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.

Werden auf einem IT-System zeitkritische Anwendungen betrieben, sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

**Beispiele:**

- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider (ISP) führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Als Folge waren mehrere vom ISP betriebene Webserver tagelang nicht erreichbar.

# G 0.26 Fehlfunktion von Geräten oder Systemen

Geräte und Systeme, die der Informationsverarbeitung dienen, haben heute häufig viele Funktionen und sind deshalb entsprechend komplex aufgebaut. Grundsätzlich betrifft dies sowohl Hardware- als auch Software-Komponenten. Durch die Komplexität gibt es in solchen Komponenten viele unterschiedliche Fehlerquellen. Als Folge kommt es immer wieder dazu, dass Geräte und Systeme nicht wie vorgesehen funktionieren und dadurch Sicherheitsprobleme entstehen.

Ursachen für Fehlfunktionen gibt es viele, zum Beispiel Materialermüdung, Fertigungstoleranzen, konzeptionelle Schwächen, Überschreitung von Grenzwerten, nicht vorgesehene Einsatzbedingungen oder fehlende Wartung. Da es keine perfekten Geräte und Systeme gibt, muss eine gewisse Restwahrscheinlichkeit für Fehlfunktionen ohnehin immer akzeptiert werden.

Durch Fehlfunktionen von Geräten oder Systemen können alle Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) beeinträchtigt werden. Hinzu kommt, dass Fehlfunktionen unter Umständen auch über einen längeren Zeitraum unbemerkt bleiben können. Dadurch kann es beispielsweise passieren, dass Berechnungsergebnisse verfälscht und nicht rechtzeitig korrigiert werden.

**Beispiele:**

- Aufgrund eines verstopften Lüftungsgitters kommt es zur Überhitzung eines Speichersystems, das daraufhin nicht komplett ausfällt, sondern nur sporadische Fehlfunktionen aufweist. Erst einige Wochen später wird bemerkt, dass die gespeicherten Informationen unvollständig sind.
- Eine wissenschaftliche Standard-Anwendung wird genutzt, um eine statistische Analyse für einen vorab erhobenen Datenbestand durchzuführen, der in einer Datenbank gespeichert ist. Laut Dokumentation ist die Anwendung jedoch für das eingesetzte Datenbank-Produkt nicht freigegeben. Die Analyse scheint zwar zu funktionieren, durch Stichproben stellt sich allerdings heraus, dass die berechneten Ergebnisse falsch sind. Als Ursache wurden Kompatibilitätsprobleme zwischen der Anwendung und der Datenbank identifiziert.

# G 0.27 Ressourcenmangel

Wenn die vorhandenen Ressourcen in einem Bereich unzureichend sind, kann es zu Engpässen in der Versorgung mit diesen Ressourcen bis hin zu Überlastungen und Ausfällen kommen. Je nach Art der betroffenen Ressourcen können durch ein kleines Ereignis, dessen Eintritt zudem vorhersehbar war, im Endeffekt eine Vielzahl von Geschäftsprozessen beeinträchtigt werden. Ressourcenmangel kann im IT-Betrieb und bei Kommunikationsverbindungen auftreten, aber auch in anderen Bereichen einer Institution. Werden für bestimmte Aufgaben nur unzureichende personelle, zeitliche und finanzielle Ressourcen zur Verfügung gestellt, kann das vielfältige negative Auswirkungen haben. Es kann beispielsweise passieren, dass die in Projekten notwendigen Rollen nicht mit geeigneten Personen besetzt werden. Wenn Betriebsmittel wie Hard- oder Software nicht mehr ausreichen, um den Anforderungen gerecht zu werden, können Fachaufgaben unter Umständen nicht erfolgreich bearbeitet werden.

Häufig können personelle, zeitliche, finanzielle, technische und sonstige Mängel im Regelbetrieb für einen begrenzten Zeitraum noch ausgeglichen werden. Unter hohem Zeitdruck werden sie jedoch, beispielsweise in Notfall-Situationen, umso deutlicher.

Ressourcen können auch absichtlich überlastet werden, wenn jemand einen intensiven Bedarf an einem Betriebsmittel vorsätzlich generiert und dadurch eine intensive und dauerhafte Störung des Betriebsmittels provoziert, siehe auch G 0.40 *Verhinderung von Diensten (Denial of Service)*.

**Beispiele:**

- Überlastete Elektroleitungen erhitzen sich, dies kann bei ungünstiger Verlegung zu einem Schwelbrand führen.
- Werden neue Anwendungen mit einem höheren als zum Planungszeitpunkt berücksichtigten Bandbreitenbedarf auf dem Netz betrieben, kann dies zu einem Verlust der Verfügbarkeit des gesamten Netzes führen, wenn die Netzinfrastruktur nicht ausreichend skaliert werden kann.
- Wenn die Administratoren wegen Überlastung die Protokoll-Dateien der von ihnen betreuten IT nur sporadisch kontrollieren, werden eventuell Angriffe nicht zeitnah erkannt.
- Webserver können durch eine hohe Menge zeitgleich eintreffender Anfragen so überlastet werden, dass ein geregelter Zugriff auf Daten fast unmöglich wird.
- Wenn sich ein Unternehmen in einem Insolvenzverfahren befindet, kann es passieren, dass kein Geld für dringend benötigte Ersatzteile vorhanden ist oder dass wichtige Dienstleister nicht bezahlt werden können.

# G 0.28 Software-Schwachstellen oder -Fehler

Für jede Software gilt: je komplexer sie ist, desto häufiger treten Fehler auf. Auch bei intensiven Tests werden meist nicht alle Fehler vor der Auslieferung an die Kunden entdeckt. Werden Software-Fehler nicht rechtzeitig erkannt, können die bei der Anwendung entstehenden Abstürze oder Fehler zu weitreichenden Folgen führen. Beispiele hierfür sind falsche Berechnungsergebnisse, Fehlentscheidungen der Leitungsebene und Verzögerungen beim Ablauf der Geschäftsprozesse.

Durch Software-Schwachstellen oder -Fehler kann es zu schwerwiegenden Sicherheitslücken in einer Anwendung, einem IT-System oder allen damit vernetzten IT-Systemen kommen. Solche Sicherheitslücken können unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder Manipulationen vorzunehmen.

**Beispiele:**

- Die meisten Warnmeldungen der Computer Emergency Response Teams (CERTs) in den letzten Jahren bezogen sich auf sicherheitsrelevante Programmierfehler. Dies sind Fehler, die bei der Erstellung von Software entstehen und dazu führen, dass diese Software von Angreifern missbraucht werden kann. Ein großer Teil dieser Fehler wurde durch Speicherüberläufe (Buffer Overflow) hervorgerufen.
- Internet-Browser sind heute eine wichtige Software-Komponente auf Clients. Browser werden häufig nicht nur zum Zugriff auf das Internet, sondern auch für interne Web-Anwendungen in Unternehmen und Behörden genutzt. Software-Schwachstellen oder -Fehler in Browsern können deshalb die Informationssicherheit insgesamt besonders stark beeinträchtigen.

# G 0.29 Verstoß gegen Gesetze oder Regelungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind (beispielsweise durch ein unzureichendes Sicherheitsmanagement), kann dies zu Verstößen gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern führen. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution bzw. ihrer Geschäftsprozesse und Dienstleistungen ab. Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale Vorschriften zu beachten sein. Folgende Beispiele verdeutlichen dies:

- Der Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt. Dazu gehören das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze, aber auch eine Vielzahl bereichsspezifischer Regelungen.
  Werden bei der Kommunikation zwischen zwei Geschäftsbereichen personenbezogene Daten (z. B. vertrauliche Patientendaten) ungeschützt über öffentliche Netze übertragen, kann dies unter Umständen rechtliche Konsequenzen nach sich ziehen.
- Die Geschäftsführung eines Unternehmens ist dazu verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Hierzu gehört auch die Beachtung anerkannter Sicherheitsmaßnahmen. In Deutschland gelten verschiedene Rechtsvorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), GmbHG (Gesetz betreffend die Gesellschaften mit beschränkter Haftung) oder AktG (Aktiengesetz), aus denen sich zu Risikomanagement und Informationssicherheit entsprechende Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen.
- Die ordnungsmäßige Verarbeitung von buchungsrelevanten Daten ist in verschiedenen Gesetzen und Vorschriften geregelt. In Deutschland sind dies unter anderem das Handelsgesetzbuch (z. B. HGB §§ 238 ff.) und die Abgabenordnung (AO). Die ordnungsmäßige Verarbeitung von Informationen umfasst natürlich deren sichere Verarbeitung. Beides muss in vielen Ländern regelmäßig nachgewiesen werden, beispielsweise durch Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses. Falls hierbei gravierende Sicherheitsmängel festgestellt werden, kann kein positiver Prüfungsbericht erstellt werden.
- In vielen Branchen (z.B. der Automobil-Industrie) ist es üblich, dass Hersteller ihre Zulieferer zur Einhaltung bestimmter Qualitäts- und Sicherheitsstandards verpflichten. In diesem Zusammenhang werden zunehmend auch Anforderungen an die Informationssicherheit gestellt. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, aber auch Vertragsauflösungen bis hin zum Verlust von Geschäftsbeziehungen nach sich ziehen.

Nur wenige Sicherheitsanforderungen ergeben sich unmittelbar aus Gesetzen. Die Gesetzgebung orientiert sich jedoch im Allgemeinen am Stand der Technik als allgemeine Bewertungsgrundlage für den Grad der erreichbaren Sicherheit. Stehen bei einer Institution die vorhandenen Sicherheitsmaßnahmen in keinem gesunden Verhältnis zu den zu schützenden Werten und dem Stand der Technik, kann dies gravierende Folgen haben.

# G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Ohne geeignete Mechanismen zur Zutritts-, Zugriffs- und Zugangskontrolle kann eine unberechtigte Nutzung von Geräten und Systemen praktisch nicht verhindert oder erkannt werden. Bei IT-Systemen ist der grundlegende Mechanismus die Identifikation und Authentisierung von Benutzern. Aber selbst bei IT-Systemen mit einer starken Identifikations- und Authentisierungsfunktion ist eine unberechtigte Nutzung denkbar, wenn die entsprechenden Sicherheitsmerkmale (Passwörter, Chipkarten, Token etc.) in falsche Hände gelangen. Auch bei der Vergabe und Pflege von Berechtigungen können viele Fehler gemacht werden, beispielsweise wenn Berechtigungen zu weitreichend oder an unautorisierte Personen vergeben oder nicht zeitnah aktualisiert werden.

Unbefugte können durch die unberechtigte Nutzung von Geräten und Systemen an vertrauliche Informationen gelangen, Manipulationen vornehmen oder Störungen verursachen.

Ein besonders wichtiger Spezialfall der unberechtigten Nutzung ist die unberechtigte Administration. Wenn Unbefugte die Konfiguration oder die Betriebsparameter von Hardware- oder Software-Komponenten ändern, können daraus schwere Schäden resultieren.

**Beispiel:**

- Bei der Kontrolle von Protokollierungsdaten stieß ein Netzadministrator auf zunächst unerklärliche Ereignisse, die an verschiedenen Tagen, aber häufig am frühen Morgen und am Nachmittag aufgetreten sind. Bei näherer Untersuchung stellte sich heraus, dass ein WLAN-Router unsicher konfiguriert war. Wartende Personen an der Bushaltestelle vor dem Firmengebäude haben diesen Zugang genutzt, um während der Wartezeit mit ihren mobilen Endgeräten im Internet zu surfen.

# G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann deren Sicherheit beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. Dies führt häufig zu Störungen oder Ausfällen. Je nachdem, welche Arten von Geräten oder Systemen falsch genutzt werden, können aber auch Vertraulichkeit und Integrität von Informationen verletzt werden.

Ein besonders wichtiger Spezialfall der fehlerhaften Nutzung ist die fehlerhafte Administration. Fehler bei der Installation, Konfiguration, Wartung und Pflege von Hardware- oder Software-Komponenten können schwere Schäden nach sich ziehen.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu Sicherheitsvorfällen führen.

Gleichermaßen können durch die fehlerhafte Bedienung von IT-Systemen oder Anwendungen auch Daten versehentlich gelöscht oder verändert werden. Dadurch könnten aber auch vertrauliche Informationen an die Öffentlichkeit gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

Wenn Strom- oder Netzkabel ungeschützt verlegt werden, können sie unbeabsichtigt beschädigt werden, wodurch Verbindungen ausfallen können. Geräteanschlussleitungen können herausgerissen werden, wenn Mitarbeiter oder Besucher darüber stolpern.

# G 0.32 Missbrauch von Berechtigungen

Abhängig von ihren Rollen und Aufgaben erhalten Personen entsprechende Zutritts-, Zugangs- und Zugriffsberechtigungen. Auf diese Weise soll einerseits der Zugang zu Informationen gesteuert und kontrolliert werden, und andererseits soll es den Personen ermöglicht werden, bestimmte Aufgaben zu erledigen. Beispielsweise benötigen Personen oder Gruppen bestimmte Berechtigungen, um Anwendungen ausführen zu können oder Informationen bearbeiten zu können.

Eine missbräuchliche Nutzung von Berechtigungen liegt vor, wenn vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten außerhalb des vorgesehenen Rahmens genutzt werden. Ziel dabei ist häufig, sich persönliche Vorteile zu verschaffen oder einer Institution oder bestimmten Personen zu schaden.

In nicht wenigen Fällen verfügen Personen aus historischen, systemtechnischen oder anderen Gründen über höhere oder umfangreichere Zutritts-, Zugangs- oder Zugriffsrechte, als sie für ihre Tätigkeit benötigen. Diese Rechte können unter Umständen für Angriffe missbraucht werden.

**Beispiele:**

- Je feingranularer die Zugriffsrechte auf Informationen gestaltet werden, desto größer ist oft auch der Pflegeaufwand, um diese Berechtigungen auf dem aktuellen Stand zu halten. Es besteht deshalb die Gefahr, dass bei der Vergabe der Zugriffsrechte zu wenig zwischen den unterschiedlichen Rollen differenziert wird und dadurch der Missbrauch der Berechtigungen erleichtert wird.
- Bei verschiedenen Anwendungen werden Zugriffsberechtigungen oder Passwörter in Systembereichen gespeichert, auf die auch andere Benutzer zugreifen können. Dadurch könnten Angreifer die Berechtigungen ändern oder Passwörter auslesen.
- Personen mit zu großzügig vergebenen Berechtigungen könnten versucht sein, auf fremde Dateien zuzugreifen, beispielsweise eine fremde E-Mail einzusehen, weil bestimmte Informationen dringend benötigt werden.

# G 0.33 Personalausfall

Der Ausfall von Personal kann erhebliche Auswirkungen auf eine Institution und deren Geschäftsprozesse haben. Personal kann beispielsweise durch Krankheit, Unfall, Tod oder Streik unvorhergesehen ausfallen. Des weiteren ist auch der vorhersagbare Personalausfall bei Urlaub, Fortbildung oder einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird. Ein Personalausfall kann auch durch einen internen Wechsel des Arbeitsplatzes verursacht werden.

In allen Fällen kann die Konsequenz sein, dass entscheidende Aufgaben aufgrund des Personalausfalls nicht mehr wahrgenommen werden können. Dies ist besonders dann kritisch, wenn die betroffene Person in einem Geschäftsprozess eine Schlüsselstellung einnimmt und aufgrund fehlenden Fachwissens anderer nicht ersetzt werden kann. Störungen des IT-Betriebs können die Folge sein. Dadurch können auch andere Bereiche und Prozesse der Institution massiv beeinträchtigt werden.

Ein Personalausfall kann zusätzlich einen empfindlichen Verlust von Wissen und Geheimnissen nach sich ziehen, der die nachträgliche Übertragung der Tätigkeiten auf andere Personen unmöglich macht.

**Beispiele:**

- Aufgrund längerer Krankheit blieb der Netzadministrator einer Firma vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben, da es nur diesen in den Netzbetrieb eingearbeiteten Administrator gab. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
- Während des Urlaubs eines Administrators musste in einer Institution auf die Backup-Medien im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kurz zuvor geändert und war nur diesem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Administrator nicht eher im Urlaub erreichbar war.
- Im Falle eine Pandemie fällt nach und nach längerfristig immer mehr Personal aus, sei es durch die Krankheit selbst, durch die notwendige Pflege von Angehörigen oder durch die Betreuung von Kindern. Auch aus Angst vor Ansteckung in öffentlichen Verkehrsmitteln oder in der Institution bleiben einige Mitarbeiter vom Dienst fern. Als Folge können nur noch die notwendigsten Arbeiten erledigt werden. Die erforderliche Wartung der Systeme, sei es der zentrale Server oder die Klimaanlage im Rechenzentrum, ist nicht mehr zu leisten. Nach und nach fallen dadurch immer mehr Systeme aus.

# G 0.34 Anschlag

Durch einen Anschlag kann eine Institution, bestimmte Bereiche der Institution oder einzelne Personen bedroht werden. Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: geworfene Ziegelsteine, Explosion durch Sprengstoff, Schusswaffengebrauch, Brandstiftung. Ob und in welchem Umfang eine Institution der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von ihren Aufgaben und vom politisch-sozialen Klima ab. Unternehmen und Behörden, die in politisch kontrovers diskutierten Bereichen agieren, sind stärker bedroht als andere. Institutionen in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Orten. Für die Einschätzung der Gefährdung oder bei Verdacht auf Bedrohungen durch politisch motivierte Anschläge können in Deutschland die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

Für Archive ist bei dieser Einschätzung als besonderer Umstand zu berücksichtigen, dass darin eine große Anzahl von Dokumenten und Daten auf vergleichsweise kleinem Raum gespeichert wird. Dies können z. B. Krankendaten, Verträge, Urkunden oder Testamente sein. Deren Vernichtung kann weitreichende Auswirkungen haben, nicht nur auf die speichernde Stelle, sondern auch auf andere Benutzer. Beispielsweise kann es in einem solchen Fall notwendig werden, die vernichteten Informationen mit großem Aufwand neu zu ermitteln und zu erfassen. Unter Umständen sind bestimmte Informationen sogar unwiederbringlich verloren. Anschläge auf papiergebundene und elektronische Archive können daher erhebliche Schäden verursachen.

**Beispiele:**

- In den 1980er-Jahren wurde ein Sprengstoffanschlag auf das Rechenzentrum einer großen Bundesbehörde in Köln verübt. Durch die große Durchschlagskraft des Sprengkörpers wurden nicht nur Fenster und Wände, sondern auch viele IT-Systeme im Rechenzentrum zerstört.
- Bei dem Anschlag auf das World-Trade-Center in New York am 11. September 2001 wurden nicht nur viele Menschen getötet, sondern es wurden auch zahlreiche IT-Einrichtungen zerstört. Als Folge hatten mehrere Unternehmen erhebliche Schwierigkeiten, ihre Geschäftstätigkeiten fortzusetzen.

# G 0.35 Nötigung, Erpressung oder Korruption

Nötigung, Erpressung oder Korruption können dazu führen, dass die Sicherheit von Informationen oder Geschäftsprozessen beeinträchtigt wird. Durch Androhung von Gewalt oder anderen Nachteilen kann ein Angreifer beispielsweise versuchen, das Opfer zur Missachtung von Sicherheitsrichtlinien oder zur Umgehung von Sicherheitsmaßnahmen zu bringen (Nötigung).

Anstatt zu drohen, können Angreifer auch gezielt Geld oder andere Vorteile anbieten, um Mitarbeiter oder andere Personen zum Instrument für Sicherheitsverletzungen zu machen (Korruption). Beispielsweise besteht die Gefahr, dass ein bestechlicher Mitarbeiter vertrauliche Dokumente an Unbefugte weiterleitet.

Durch Nötigung oder Korruption können grundsätzlich alle Grundwerte der Informationssicherheit beeinträchtigt werden. Angriffe können unter anderem darauf abzielen, vertrauliche Informationen an Unbefugte zu leiten, geschäftskritische Informationen zu manipulieren oder den reibungslosen Ablauf von Geschäftsprozessen zu stören.

Besondere Gefahr besteht, wenn sich solche Angriffe gegen hochrangige Führungskräfte oder Personen in besonderen Vertrauensstellungen richten.

# G 0.36 Identitätsdiebstahl

Beim Identitätsdiebstahl täuscht ein Angreifer eine falsche Identität vor, er benutzt also Informationen über eine andere Person, um in deren Namen aufzutreten. Hierfür werden Daten wie beispielsweise Geburtsdatum, Anschrift, Kreditkarten- oder Kontonummern benutzt, um sich beispielsweise auf fremde Kosten bei einem Internet-Dienstleister anzumelden oder sich auf andere Weise zu bereichern. Identitätsdiebstahl führt häufig auch direkt oder indirekt zur Rufschädigung, aber verursacht auch einen hohen Zeitaufwand, um die Ursachen aufzuklären und negative Folgen für die Betroffenen abzuwenden. Einige Formen des Identitätsbetrugs werden auch als Maskerade bezeichnet.

Identitätsdiebstahl tritt besonders dort häufig auf, wo die Identitätsprüfung zu nachlässig gehandhabt wird, vor allem, wenn hierauf teure Dienstleistungen basieren.

Eine Person, die über die Identität seines Kommunikationspartners getäuscht wurde, kann leicht dazu gebracht werden, schutzbedürftige Informationen zu offenbaren.

**Beispiele:**

- Bei verschiedenen E-Mail-Providern und Auktionsplattformen im Internet reichte es zur Anmeldung anfangs, sich einen Phantasienamen auszudenken und diesen mit einer passenden Adresse aus dem Telefonbuch zu unterlegen. Zunächst konnten sich Angreifer auch unter erkennbar ausgedachten Namen anmelden, beispielsweise von Comicfiguren. Als dann schärfere Plausibilitätstests eingeführt wurden, sind hierfür auch Namen, Adressen und Kontonummern von echten Personen verwendet worden. Die Betroffenen haben hiervon erst erfahren, als die ersten Zahlungsaufforderungen bei ihnen eintrafen.
- Die Absender-Adressen von E-Mails lassen sich leicht fälschen. Es passiert immer wieder, dass Anwendern auf diese Weise vorgetäuscht wird, dass eine E-Mail von einem vertrauenswürdigen Kommunikationspartner stammt. Ähnliche Angriffe sind durch die Manipulation der Rufnummernanzeige bei Sprachverbindungen oder durch die Manipulation der Absenderkennung bei Faxverbindungen möglich.
- Ein Angreifer kann durch eine Maskerade versuchen, sich in eine bereits bestehende Verbindung einzuhängen, ohne sich selber authentisieren zu müssen, da dieser Schritt bereits von den originären Kommunikationsteilnehmern durchlaufen wurde.

# G 0.37 Abstreiten von Handlungen

Personen können aus verschiedenen Gründen abstreiten, bestimmte Handlungen begangen zu haben, beispielsweise weil diese Handlungen gegen Anweisungen, Sicherheitsvorgaben oder sogar Gesetze verstoßen. Sie könnten aber auch leugnen, eine Benachrichtigung erhalten zu haben, zum Beispiel weil sie einen Termin vergessen haben. Im Bereich der Informationssicherheit wird daher häufig die Verbindlichkeit hervorgehoben, eine Eigenschaft, über die sichergestellt werden soll, dass erfolgte Handlungen nicht unberechtigt abgestritten werden können. Im englischen Sprachraum wird dafür der Begriff Non-Repudiation (Nichtabstreitbarkeit) verwendet.

Bei Kommunikation wird zusätzlich unterschieden, ob ein Kommunikationsteilnehmer den Nachrichtenempfang ableugnet (Repudiation of Receipt) oder den Versand (Repudiation of Origin). Den Nachrichtenempfang abzuleugnen kann unter anderem bei finanziellen Transaktionen von Bedeutung sein, z. B. wenn jemand bestreitet, eine Rechnung fristgemäß erhalten zu haben. Ebenso kann es passieren, dass ein Kommunikationsteilnehmer den Nachrichtenversand ableugnet, z.B. also eine getätigte Bestellung abstreitet. Nachrichtenversand oder -empfang kann beim Postversand ebenso abgeleugnet werden wie bei Fax- oder E-Mail-Nutzung.

**Beispiel:**

- Ein dringend benötigtes Ersatzteil wird elektronisch bestellt. Nach einer Woche wird das Fehlen reklamiert, inzwischen sind durch den Produktionsausfall hohe Kosten entstanden. Der Lieferant leugnet, je eine Bestellung erhalten zu haben.

# G 0.38 Missbrauch personenbezogener Daten

Personenbezogene Daten sind fast immer besonders schützenswerte Informationen. Typische Beispiele sind Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Wenn der Schutz personenbezogener Daten nicht ausreichend gewährleistet ist, besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Ein Missbrauch personenbezogener Daten kann beispielsweise vorliegen, wenn eine Institution zu viele personenbezogene Daten sammelt, sie ohne Rechtsgrundlage oder Einwilligung erhoben hat, sie zu einem anderen als dem bei der Erhebung zulässigen Zweck nutzt, personenbezogene Daten zu spät löscht oder unberechtigt weitergibt.

**Beispiele:**

- Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder erstmals gespeichert worden sind. Es ist daher unzulässig, Protokolldateien, in denen die An- und Abmeldung von Benutzern an IT-Systemen ausschließlich für die Zugriffskontrolle festgehalten werden, zur Anwesenheits- und Verhaltenskontrolle zu nutzen.
- Personen, die Zugriff auf personenbezogene Daten haben, könnten diese unbefugt weitergeben. Beispielsweise könnte ein Mitarbeiter am Empfang eines Hotels die Anmeldedaten von Gästen an Werbefirmen verkaufen.

# G 0.39 Schadprogramme

Ein Schadprogramm ist eine Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Zu den typischen Arten von Schadprogrammen gehören unter anderem Viren, Würmer und Trojanische Pferde. Schadprogramme werden meist heimlich, ohne Wissen und Einwilligung des Benutzers aktiv.

Schadprogramme bieten heutzutage einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können Schadprogramme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren.

Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch der Imageverlust und der finanzielle Schaden, der durch Schadprogramme entstehen kann, sind von großer Bedeutung.

**Beispiele:**

- In der Vergangenheit verbreitete sich das Schadprogramm W32/Bugbear auf zwei Wegen: Es suchte in lokalen Netzen nach Computern mit Freigaben, auf die schreibender Zugriff möglich war, und kopierte sich darauf. Zudem schickte es sich selbst als HTML-E-Mail an Empfänger im E-Mail-Adressbuch von befallenen Computern. Durch einen Fehler in der HTML-Routine bestimmter E-Mail-Programme wurde das Schadprogramm dort beim Öffnen der Nachricht ohne weiteres Zutun des Empfängers ausgeführt.
- Das Schadprogramm W32/Klez verbreitete sich in verschiedenen Varianten. Befallene Computer schickten den Virus an alle Empfänger im E-Mail-Adressbuch des Computers. Hatte dieser Virus einen Computer befallen, verhinderte er durch fortlaufende Manipulationen am Betriebssystem die Installation von Viren-Schutzprogrammen verbreiteter Hersteller und erschwerte so die Desinfektion der befallenen Computer erheblich.

# G 0.40 Verhinderung von Diensten (Denial of Service)

Es gibt eine Vielzahl verschiedener Angriffsformen, die darauf abzielen, die vorgesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte zu verhindern. Der Oberbegriff für solche Angriffe ist "Verhinderung von Diensten" (englisch: "Denial of Service"). Häufig wird auch die Bezeichnung "DoS-Angriff" verwendet.

Solche Angriffe können unter anderem von verärgerten Mitarbeitern oder Kunden, aber auch von Mitbewerbern, Erpressern oder politisch motivierten Tätern ausgehen. Das Ziel der Angriffe können geschäftsrelevante Werte aller Art sein. Typische Ausprägungen von DoS-Angriffen sind

- Störungen von Geschäftsprozessen, z. B. durch Überflutung der Auftragsannahme mit fehlerhaften Bestellungen,
- Beeinträchtigungen der Infrastruktur, z. B. durch Blockieren der Türen der Institution,
- Herbeiführen von IT-Ausfällen, indem z. B. Dienste eines Servers im Netz gezielt überlastet werden.

Diese Art von Angriffen steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass sie den eigentlichen Nutzern nicht mehr zur Verfügung stehen. Bei IT-basierten Angriffen können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Arbeitsspeicher, Plattenplatz, Übertragungskapazität.

**Beispiel:**

- Im Frühjahr 2007 fanden über einen längeren Zeitraum starke DoS-Angriffe auf zahlreiche Internet-Angebote in Estland statt. Dadurch kam es in Estland zu erheblichen Beeinträchtigungen bei der Nutzung von Informationsangeboten und Dienstleistungen im Internet.

# G 0.41 Sabotage

Sabotage bezeichnet die mutwillige Manipulation oder Beschädigung von Sachen oder Prozessen mit dem Ziel, dem Opfer dadurch Schaden zuzufügen. Besonders attraktive Ziele können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

Die komplexe Infrastruktur eines Rechenzentrums kann durch gezielte Beeinflussung wichtiger Komponenten, gegebenenfalls durch Täter von außen, vor allem aber durch Innentäter, punktuell manipuliert werden, um Betriebsstörungen hervorzurufen. Besonders bedroht sind hierbei nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur sowie zentrale Versorgungspunkte, die organisatorisch oder technisch gegebenenfalls auch nicht überwacht werden und für Externe leicht und unbeobachtet zugänglich sind.

**Beispiele:**

- In einem großen Rechenzentrum führte die Manipulation an der USV zu einem vorübergehenden Totalausfall. Der Täter hatte wiederholt die USV von Hand auf Bypass geschaltet und dann die Hauptstromversorgung des Gebäudes manipuliert. Insgesamt fanden in drei Jahren vier Ausfälle statt. Teilweise kam es sogar zu Hardware-Schäden. Die Betriebsunterbrechungen dauerten zwischen 40 und 130 Minuten.
- Innerhalb eines Rechenzentrums waren auch sanitäre Einrichtungen untergebracht. Durch Verstopfen der Abflüsse und gleichzeitiges Öffnen der Wasserzufuhr drang Wasser in zentrale Technikkomponenten ein. Die auf diese Weise verursachten Schäden führten zu Betriebsunterbrechungen des Produktivsystems.
- Für elektronische Archive stellt Sabotage ein besonderes Risiko dar, da hier meist auf kleinem Raum viele schützenswerte Dokumente verwahrt werden. Dadurch kann unter Umständen durch gezielte, wenig aufwendige Manipulationen ein großer Schaden verursacht werden.

# G 0.42 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:

- Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
- Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich "nur eine Aushilfe" oder eine "wichtige" Persönlichkeit.

Eine weitere Strategie beim systematischen Social Engineering ist der Aufbau einer längeren Beziehung zum Opfer. Durch viele unwichtige Telefonate im Vorfeld kann der Angreifer Wissen sammeln und Vertrauen aufbauen, das er später ausnutzen kann.

Solche Angriffe können auch mehrstufig sein, indem in weiteren Schritten auf Wissen und Techniken aufgebaut wird, die in vorhergehenden Stufen erworben wurden.

Viele Anwender wissen, dass sie Passwörter an niemanden weitergeben dürfen. Social Engineers wissen dies und müssen daher über andere Wege an das gewünschte Ziel gelangen. Beispiele hierfür sind:

- Ein Angreifer kann das Opfer bitten, ihm unbekannte Befehle oder Applikationen auszuführen, z. B. weil dies bei einem IT-Problem helfen soll. Dies kann eine versteckte Anweisung für eine Änderung von Zugriffsrechten sein. So kann der Angreifer an sensible Informationen gelangen.
- Viele Benutzer verwenden zwar starke Passwörter, aber dafür werden diese für mehrere Konten genutzt. Wenn ein Angreifer einen nützlichen Netzdienst (wie ein E-Mail-Adressensystem) betreibt, an dem die Anwender sich authentisieren müssen, kann er an die gewünschten Passwörter und Logins gelangen. Viele Benutzer werden die Anmeldedaten, die sie für diesen Dienst benutzen, auch bei anderen Diensten verwenden.

Wenn sich Angreifer unerlaubt Passwörter oder andere Authentisierungsmerkmale verschaffen, beispielsweise mit Hilfe von Social Engineering, wird dies häufig auch als "Phishing" (Kunstwort aus "Password" und "Fishing") bezeichnet.

Beim Social Engineering tritt der Angreifer nicht immer sichtbar auf. Oft erfährt das Opfer niemals, dass es ausgenutzt wurde. Ist dies erfolgreich, muss der Angreifer nicht mit einer Strafverfolgung rechnen und besitzt außerdem eine Quelle, um später an weitere Informationen zu gelangen.

# G 0.43 Einspielen von Nachrichten

Angreifer senden bei dieser Angriffsform speziell vorbereitete Nachrichten an Systeme oder Personen mit dem Ziel, für sich selbst einen Vorteil oder einen Schaden für das Opfer zu erreichen. Um die Nachrichten geeignet zu konstruieren, nutzen die Angreifer beispielsweise Schnittstellenbeschreibungen, Protokollspezifikationen oder Aufzeichnungen über das Kommunikationsverhalten in der Vergangenheit.

Es gibt zwei in der Praxis wichtige Spezialfälle des Einspielens von Nachrichten:

- Bei einer "Replay-Attacke" (Wiedereinspielen von Nachrichten) zeichnen Angreifer gültige Nachrichten auf und spielen diese Information zu einem späteren Zeitpunkt (nahezu) unverändert wieder ein. Es kann auch ausreichen, nur Teile einer Nachricht, wie beispielsweise ein Passwort, zu benutzen, um unbefugt in ein IT-System einzudringen.
- Bei einer "Man-in-the-Middle-Attacke" nimmt der Angreifer unbemerkt eine Vermittlungsposition in der Kommunikation zwischen verschiedenen Teilnehmern ein. In der Regel täuscht er hierzu dem Absender einer Nachricht vor, der eigentliche Empfänger zu sein, und er täuscht dem Empfänger vor, der eigentliche Absender zu sein. Wenn dies gelingt, kann der Angreifer dadurch Nachrichten, die nicht für ihn bestimmt sind, entgegennehmen und vor der Weiterleitung an den eigentlichen Empfänger auswerten und gezielt manipulieren.

Eine Verschlüsselung der Kommunikation bietet keinen Schutz vor Man-in-the-Middle-Attacken, wenn keine sichere Authentisierung der Kommunikationspartner stattfindet.

**Beispiele:**

- Ein Angreifer zeichnet die Authentisierungsdaten (z. B. Benutzerkennung und Passwort) während des Anmeldevorgangs eines Benutzers auf und verwendet diese Informationen, um sich Zugang zu einem System zu verschaffen. Bei rein statischen Authentisierungsprotokollen kann damit auch ein verschlüsselt übertragenes Passwort benutzt werden, um unbefugt auf ein fremdes System zuzugreifen.
- Um finanziellen Schaden beim Arbeitgeber (Unternehmen oder Behörde) zu verursachen, gibt ein Mitarbeiter eine genehmigte Bestellung mehrmals auf.

# G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Wenn Unbefugte in ein Gebäude oder einzelne Räumlichkeiten eindringen, kann dies verschiedene andere Gefahren nach sich ziehen. Dazu gehören beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen. Bei qualifizierten Angriffen ist die Zeitdauer entscheidend, in der die Täter ungestört ihr Ziel verfolgen können.

Häufig wollen die Täter wertvolle IT-Komponenten oder andere Waren, die leicht veräußert werden können, stehlen. Ziel eines Einbruchs kann es jedoch unter anderem auch sein, an vertrauliche Informationen zu gelangen, Manipulationen vorzunehmen oder Geschäftsprozesse zu stören.

Durch das unbefugte Eindringen in Räumlichkeiten können somit mehrere Arten von Schäden entstehen:

- Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und/oder Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.
- Entwendete, beschädigte oder zerstörte Geräte oder Komponenten müssen repariert oder ersetzt werden.
- Es können Schäden durch die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Anwendungen entstehen.

**Beispiele:**

- Bei einem nächtlichen Einbruch in ein Bürogebäude konnten die Täter keine lohnende Beute machen. Aus Frustration darüber leerten sie die Pulverlöscher in die Büroräume. Der Einbruchschaden war gering, der Vandalismusschaden dagegen durch die Reinigungskosten und Arbeitsunterbrechungen unverhältnismäßig hoch.
- Bei einem Einbruch in ein Unternehmen an einem Wochenende wurde nur Bagatellschaden durch Aufhebeln eines Fensters angerichtet, lediglich eine Kaffeekasse und kleinere Einrichtungsgegenstände wurden entwendet. Bei einer Routinekontrolle wurde jedoch später festgestellt, dass ein zentraler Server genau zum Zeitpunkt des Einbruchs geschickt manipuliert wurde.

# G 0.45 Datenverlust

Ein Datenverlust ist ein Ereignis, das dazu führt, dass ein Datenbestand nicht mehr wie erforderlich genutzt werden kann (Verlust der Verfügbarkeit). Eine häufige Form des Datenverlustes ist, dass Daten unbeabsichtigt oder unerlaubt gelöscht werden, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware.

Ein Datenverlust kann jedoch auch durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern entstehen. Dieses Risiko ist bei mobilen Endgeräten und mobilen Datenträgern häufig besonders hoch.

Weiterhin ist zu beachten, dass viele mobile IT-Systeme nicht immer online sind. Die auf diesen Systemen gespeicherten Daten befinden sich daher nicht immer auf dem aktuellsten Stand. Wenn Datenbestände zwischen mobilen IT-Systemen und stationären IT-Systemen synchronisiert werden, kann es durch Unachtsamkeit oder Fehlfunktion zu Datenverlusten kommen.

**Beispiele:**

- Der PDA fällt aus der Hemdtasche und zerschellt auf den Fliesen, ein Mobiltelefon wird statt der Zeitung vom Hund apportiert, leider mit Folgen. Solche und ähnliche Ereignisse sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Es gibt Schadprogramme, die gezielt Daten auf infizierten IT-Systemen löschen. Bei einigen Schädlingen wird die Löschfunktion nicht sofort bei der Infektion ausgeführt, sondern erst, wenn ein definiertes Ereignis eintritt, zum Beispiel wenn die Systemuhr ein bestimmtes Datum erreicht.
- Viele Internet-Dienste können genutzt werden, um online Informationen zu speichern. Wenn das Passwort vergessen wird und nicht hinterlegt ist, kann es passieren, dass auf die gespeicherten Informationen nicht mehr zugegriffen werden kann, sofern der Dienstleister kein geeignetes Verfahren zum Zurücksetzen des Passwortes anbietet.
- Festplatten und andere Massenspeichermedien haben nur eine begrenzte Lebensdauer. Wenn keine geeigneten Redundanzmaßnahmen getroffen sind, kann es durch technische Defekte zu Datenverlusten kommen.

# G 0.46 Integritätsverlust schützenswerter Informationen

Die Integrität von Informationen kann durch verschiedene Ursachen beeinträchtigt werden, z. B. durch Manipulationen, Fehlverhalten von Personen, Fehlbedienung von Anwendungen, Fehlfunktionen von Software oder Übermittlungsfehler.

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- Bei der Datenübertragung kann es zu Übertragungsfehlern kommen.
- Durch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.
- Durch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die häufig lange Zeit nicht bemerkt werden.
- Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

Wenn Informationen nicht mehr integer sind, kann es zu einer Vielzahl von Problemen kommen:

- Informationen können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden.
- Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an den falschen Empfänger ausgelöst werden, die Absenderangaben von E-Mails könnten manipuliert werden oder vieles mehr.
- Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden.
- Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.
- Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

# G 1 Gefährdungskatalog Höhere Gewalt

# G 1.1 Personalausfall

Der Ausfall von Personal kann erhebliche Auswirkungen auf eine Institution und deren Geschäftsprozesse haben. Personal kann beispielsweise durch Krankheit, Unfall, Tod oder Streik unvorhergesehen ausfallen. Des weiteren ist auch der vorhersagbare Personalausfall bei Urlaub, Fortbildung oder einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird.

In allen Fällen kann die Konsequenz sein, dass entscheidende Aufgaben aufgrund des Personalausfalls nicht mehr wahrgenommen werden können. Dies ist besonders dann kritisch, wenn die betroffene Person in einem Geschäftsprozess eine Schlüsselstellung einnimmt und aufgrund fehlenden Fachwissens anderer nicht ersetzt werden kann. Störungen des IT-Betriebs können die Folge sein. Dadurch können auch andere Bereiche und Prozesse der Institution massiv gestört werden.

Ein Personalausfall kann zusätzlich einen empfindlichen Verlust von Wissen und Geheimnissen nach sich ziehen, der die nachträgliche Übertragung der Tätigkeiten auf andere Personen unmöglich macht.

**Beispiele:**

- Aufgrund längerer Krankheit blieb der Netzadministrator einer Firma vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben, da es nur diesen in den Netzbetrieb eingearbeiteten Administrator gab. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
- Während des Urlaubs eines Administrators musste in einer Institution für Datensicherungszwecke auf die Backupbänder im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kurz zuvor kürzlich geändert und ist war nur diesem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Administrator nicht schneller im Urlaub erreicht werden konnte.
- Im Falle eine Pandemie fällt nach und nach längerfristig immer mehr Personal aus, sei es durch die Krankheit selbst, durch die Notwendigkeit Angehörige zu pflegen oder Kinder zu betreuen, die nicht mehr zur Schule oder in Kindergarten können, oder einfach aus Angst vor Ansteckung in öffentlichen Verkehrsmitteln oder in der Institution. Nur noch die notwendigsten Arbeiten können erledigt werden. Die erforderliche Wartung der Systeme, sei es der zentrale Server oder die notwendige Klimaanlage im Rechenzentrum, ist nicht mehr zu leisten. Nach und nach fallen dadurch immer mehr Systeme aus.

# G 1.2 Ausfall von IT-Systemen

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs und damit dem Ausfall wichtiger Geschäftsprozesse führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. LAN-Server oder Netzkoppelelemente. Auch der Ausfall von einzelnen Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des gesamten Informationsverbunds beitragen.

Ursache für den Ausfall eines IT-Systems ist nicht immer technisches Versagen (z. B. G 4.1 *Ausfall der Stromversorgung*). Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*) oder vorsätzliche Handlungen (z. B. G 5.4 *Diebstahl*, G 5.102 *Sabotage*) zurückführen. Auch mangelnde Wartung, beispielsweise durch Ausfall des Wartungspersonals, kann zu technischem Versagen führen. Auch durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.

Werden auf einem IT-System zeitkritische Anwendungen betrieben, sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

**Beispiele:**

- Durch Spannungsspitzen in der Stromversorgung wird das Netzteil eines wichtigen IT-Systems zerstört. Da es sich um ein älteres Modell handelt, steht nicht unmittelbar ein Ersatz bereit. Die Reparatur nimmt einen Tag in Anspruch, in dieser Zeit ist der gesamte IT-Betrieb nicht verfügbar.
- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider (ISP) führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Bis alle Folgeprobleme behoben waren, waren mehrere der vom ISP betriebenen Webserver tagelang nicht erreichbar.
- In elektronischen Archiven kann der Zeitpunkt der erstmaligen Archivierung als Entstehungszeitpunkt von Dokumenten fehlinterpretiert werden, wenn keine anderweitigen Beweisverfahren, z. B. Zeitstempeldienste, zur Beglaubigung eingesetzt werden. Dies gilt vor allem für Geschäftsprozesse, in denen die elektronische Archivierung von massenhaft anfallenden Belegdaten transparent eingebunden ist. Im vorliegenden Fall konnte aufgrund des Ausfalls einer Archivkomponente ein Teil von Belegdaten erst um einen Tag verzögert archiviert werden. Durch die Verwendung von WORM-Medien wurde die Reihenfolge der physischen Archivierung der Geschäftsbelege trotzdem nachweisbar dokumentiert. Es wurde jedoch kein Nachweis für die ansonsten nicht auftretende Verzögerung durch die ausgefallene Archivkomponente geführt. Dadurch entstand bei einer späteren Prüfung der Eindruck einer nachträglichen Manipulation.

# G 1.3 Blitz

Der Blitz ist die wesentliche während eines Gewitters bestehende Gefährdung für ein Gebäude und die darin befindliche Informationstechnik. Blitze erreichen bei Spannungen von mehreren 100.000 Volt Ströme bis zu 200.000 Ampere. Diese enorme elektrische Energie wird innerhalb von 50-100 Mikrosekunden freigesetzt und abgebaut. Ein Blitz mit diesen Werten, der in einem Abstand von ca. 2 km einschlägt, verursacht auf elektrischen Leitungen im Gebäude immer noch Spannungsspitzen, die zur Zerstörung empfindlicher elektronischer Geräte führen können. Diese indirekten Schäden nehmen mit abnehmender Entfernung zu.

Schlägt der Blitz direkt in ein Gebäude ein, werden durch die dynamische Energie des Blitzes Schäden hervorgerufen. Dies können Beschädigungen des Baukörpers (Dach und Fassade), Schäden durch auftretende Brände oder Überspannungsschäden an elektrischen Geräten sein.

Über das regional unterschiedliche Blitzschlagrisiko erteilen verschiedene kommerzielle Wetterdienste kostenpflichtige Auskünfte. Hierzu gehören in Deutschland unter anderem der Deutsche Wetterdienst (www.dwd.de) oder der Blitz-Informations-Dienst von Siemens (BLIDS, www.blids.de).

**Beispiele:**

- Auf einem deutschen Großflughafen schlug ein Blitz in unmittelbarer Nähe neben dem Tower ein. Trotz der installierten äußeren Blitzschutzanlage (Blitzableiter) wurde die automatische Löschanlage im IT-Bereich ausgelöst und dadurch der gesamte Flughafenbetrieb für 2 Stunden lahmgelegt.
- Neben direkten Schäden haben Blitzschläge auch oft weitreichendere Folgen. Häufig finden sich Meldungen wie diese: Im April 1999 führte ein Blitzeinschlag in eine Hochspannungsleitung im Raum Darmstadt zu einem kurzzeitigen Stromausfall, von dem ca. 80.000 Personen betroffen waren.

# G 1.4 Feuer

Neben direkten durch das Feuer verursachten Schäden an einem Gebäude oder dessen Einrichtung lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brands kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- unsachgemäße Lagerung brennbarer Materialien (z. B. Altpapier),
- Nichtbeachtung der einschlägigen Normen und Vorschriften zur Brandvermeidung,
- fehlende Brandmeldeeinrichtungen (z. B. Rauchmelder),
- fehlende oder nicht einsatzbereite Handfeuerlöscher oder automatische Löscheinrichtungen (z. B. Gaslöschanlagen),
- mangelhaften vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen oder Verwendung ungeeigneter Dämmmaterialien zur Wärme- und Schallisolierung).

**Beispiele:**

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte wie z. B. Kaffeemaschinen oder Tischleuchten unsachgemäß installiert oder aufgestellt sind und dadurch Brände verursachen.

# G 1.5 Wasser

Der unkontrollierte Eintritt von Wasser in Gebäuden oder Räumen kann beispielsweise bedingt sein durch:

- Regen, Hochwasser, Überschwemmung,
- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

**Beispiele:**

- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum "überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist nicht von einer Versicherung abgedeckt.
- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskartonelementen verkleidet war. Als eine Verbindung der Wasserleitung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils komplett abgeschaltet werden musste.

# G 1.6 Kabelbrand

Wenn ein Kabel in Brand gerät, sei es durch Selbstentzündung oder durch Beflammung, hat dies verschiedene Folgen:

- Durch Zerstörung der Aderisolierung können Kurzschlüsse oder Körperschlüsse auftreten, die zum Ansprechen der entsprechenden Schutzorgane (Schutzschalter oder Sicherung) führen und so die Versorgung unterbrechen.
- Die Verbindung einzelner Adern oder des gesamten Kabels kann unterbrochen werden. Besonders kritisch ist eine Unterbrechung nur des Schutzleiters (PE), während aktive Leiter (L und N) noch in Betrieb sind. Die Schutzmaßnahmen sind in diesem Fall wirkungslos. Eine unmittelbare Gefahr ergibt sich im TNC-Netz bei Ausfall des PEN-Leiters. Geräte der Schutzklasse 1 würden in einem solchen Fall am Gehäuse plötzlich spannungsführend. Die Gefahr des Stromschlages ist offensichtlich.
- Es können sich aggressive Gase entwickeln. Diese können zum einen korrosiv sein, also die Informations- und Kommunikationstechnik in Mitleidenschaft ziehen. Sie können aber auch toxisch sein, also zu Personenschäden (z. B. Vergiftung) führen. Korrosive Gase können auch dazu führen, dass z. B. bei Stahlbetondecken und -wänden tragende Gebäudestrukturen angegriffen werden und somit statische Probleme bei der Sanierung eines Kabelbrandschadens entstehen.
- An Kabeln, deren Isolationsmaterial nicht flammwidrig bzw. selbstverlöschend ist, kann sich ein Feuer ausbreiten. Selbst Brandabschottungen verhindern dies nicht vollständig, sie verzögern nur die Ausbreitung.
- Bei dicht gepackten Trassen kann es zu Schwelbränden kommen, die über längere Zeit unentdeckt bleiben und so zur Ausbreitung des Feuers führen, lange bevor es offen ausbricht. Eine Erwärmung der Kabel hat eine verminderte Leitfähigkeit zur Folge, der Schleifenwiderstand erhöht sich. Hierdurch kann eine zusätzliche Erwärmung auftreten, die den kritischen Prozess noch unterstützt.

Kabelbrände bewirken in der Entstehungsphase häufig nur einen geringen Anstieg der Temperatur. Damit besteht die zusätzliche Gefährdung, dass eine erhebliche Verrauchung durch "kalten" Brandrauch entsteht, bevor Rauchmelder ansprechen, die an der Raumdecke angebracht sind.

**Beispiel:**

- In einem Verwaltungsgebäude wurden die vorhandenen Elektroleitungen aus Kostengründen nicht ersetzt, sondern wider besseres Wissen überlastet. Die notwendigen Anpassungsarbeiten wurden nicht durchgeführt, da in Kürze ein neues Verwaltungsgebäude bezogen werden sollte.
- Die überlasteten Leitungen erhitzten sich und durch die sehr dichte Verlegung kam es zu einem Hitzestau, der dann zu einem Schwelbrand führte. Dieser wurde erst entdeckt, als die Leitungen durch die große Hitze versagten. Bis die vom Brand betroffenen Arbeitsplätze wieder ordnungsgemäß benutzt werden konnten, vergingen mehrere Tage.

# G 1.7 Unzulässige Temperatur und Luftfeuchte

Jedes Gerät hat einen Temperaturbereich, innerhalb dessen seine ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Raumtemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Betriebsstörungen und zu Geräteausfällen kommen.

So wird z. B. in einem Serverraum durch die darin befindlichen Geräte elektrische Energie in Wärme umgesetzt und daher der Raum aufgeheizt. Bei unzureichender Lüftung kann die zulässige Betriebstemperatur der Geräte überschritten werden. Bei Sonneneinstrahlung in den Raum sind Temperaturen über 50°C nicht unwahrscheinlich.

Zu Lüftungszwecken werden oft die Fenster des Serverraumes geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

Bei der Lagerung von digitalen Langzeitspeichermedien können zu große Temperaturschwankungen oder zu große Luftfeuchtigkeit zu Datenfehlern und reduzierter Speicherdauer führen. Einige Hersteller geben die optimalen Lagerbedingungen für Langzeitspeichermedien mit Temperaturen von 20 bis 22°C und einer Luftfeuchtigkeit von 40% an. Auch analoge Speichermedien wie Papier oder Mikrofilme benötigen bestimmte Lagerbedingungen. Wird Papier beispielsweise zu feucht gelagert, kann es schimmeln oder sich auflösen.

**Beispiel:**

- In einer Bonner Behörde wurde die gesamte Steuerungs- und Auswerteelektronik einer Sicherungseinrichtung in einem Raum untergebracht, der gerade genug Platz ließ, um die Türen der Geräteschränke zu öffnen. Aus Sicherheitsgründen waren sowohl die Schränke als auch der Raum mit festen Türen verschlossen.
- Nach der Fertigstellung der Anlage im Herbst lief die Anlage störungsfrei. Im folgenden Sommer zeigten sich zuerst unerklärliche Funktionsfehler und bald Totalabstürze des Systems, alles ohne erkennbare Systematik. Tagelanges Suchen mit hohem technischen und personellem Aufwand bei geöffneten Türen erbrachte keine Ergebnisse. Nur durch Zufall wurde schließlich die Überhitzung der Anlage bei Außentemperaturen über 30°C als Ursache der Störungen erkannt und durch ein Kühlgerät erfolgreich abgestellt.

# G 1.8 Staub, Verschmutzung

Trotz zunehmender Elektronik in der IT kommt sie noch nicht ohne mechanisch arbeitende Komponenten aus. Zu nennen sind Fest- und Wechselplatten, Drucker, Scanner etc, aber auch Lüfter von Prozessoren und Netzteile. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor)

in größerem Maße entstehen, die entsprechende Ausfälle der Hardware verursachen können.

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den Schaden, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

**Beispiele:**

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Normalpapier-Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Der Mitarbeiter hatte hierzu sein Büro für kurze Zeit verlassen. Nach Rückkehr an seinen Arbeitsplatz stellte er fest, dass sein PC nicht mehr funktionierte. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

# G 1.9 Datenverlust durch starke Magnetfelder

Typische Datenträger mit magnetisierbaren Speichermedien sind Disketten, Wechselplatten, Kassetten und Bänder. Informationen werden über Schreib-/Leseköpfe aufgebracht. Die derart magnetisierten Datenträger sind empfindlich gegenüber magnetischer Störstrahlung, so dass die Nähe zu solchen Strahlungsquellen vermieden werden sollte.

Je nach Stärke der Strahlung führt diese zu mehr oder weniger großen Datenverlusten. Besonders kritisch ist dies bei Dateien, die aufgrund ihrer internen Formatierung bereits durch geringfügige Veränderungen gänzlich unbrauchbar werden (z. B. PostScript-Dateien, Datenbanken).

**Beispiele** für Quellen magnetischer Störstrahlung sind:

- Elektromotoren,
- Transformatoren,
- Ausweiselesegeräte auf Magnetfeldbasis.

# G 1.10 Ausfall eines Weitverkehrsnetzes

Weitverkehrsnetze, die auch als Wide Area Networks (WAN) bezeichnet werden, wurden für die Sprach- und Datenübertragung über große Entfernungen entwickelt und können verschiedene LANs, aber auch einzelne Rechner miteinander verbinden.

WANs werden im allgemeinen von Telekommunikationsverwaltungen, aber auch von privaten Netzbetreibern betreut. Es kommt auch vor, dass sie bestimmten Institutionen gehören und nur von diesen genutzt werden. Die Qualität der Kommunikationsverbindungen kann daher unterschiedlich sein.

Die Ursachen für den Ausfall eines WAN können vielfältig sein. Daher ist es möglich, dass sich ein Netzausfall lediglich auf einzelne Benutzer, einen Anbieter oder eine bestimmte Region auswirkt. Häufig stören solche Ausfälle nur kurz, es gibt aber auch immer wieder längere Ausfälle, die massive andere Probleme nach sich ziehen können.

Die Art und Weise der Netzausfälle spielt eine Rolle, wenn auf den IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische Anwendungen betrieben werden. Die durch einen Netzausfall möglichen Schäden und Folgeschäden können entsprechend hoch ausfallen, wenn keine Ausweichmöglichkeiten wie beispielsweise die Anbindung an ein zweites Kommunikationsnetz oder Ausweichverfahren zu Internet-Diensten vorgesehen bzw. festgelegt sind.

**Beispiele:**

- Bei einem großen Internet-Provider fiel ein zentraler Server-Knoten aus. Der Versuch, auf einen redundanten Server-Knoten umzuschalten, scheiterte. Dadurch waren etwa 250.000 bei diesem Anbieter gehostete Domains einige Tage nicht erreichbar.
- Durch den gleichzeitigen Bruch von drei benachbarten Tiefseekabeln im Mittelmeer vor Ägypten wurden im Dezember 2008 90 Prozent des Internetverkehrs zwischen Europa, dem Nahen Osten und Asien lahmgelegt.

# G 1.11 Technische Katastrophen im Umfeld

Probleme im Umfeld einer Behörde bzw. eines Unternehmens können zu Schwierigkeiten im Betrieb bis hin zu Arbeitsausfällen führen. Dies können technische Unglücksfälle, Havarien, aber auch gesellschaftliche oder politische Unruhen wie Demonstrationen oder Krawalle sein (siehe auch G 1.12 *Beeinträchtigung durch Großveranstaltungen*).

Die Liegenschaften einer Organisation können verschiedenen Gefährdungen aus dem Umfeld durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetrieben oder Wohngebieten ausgesetzt sein. Diese können beispielsweise durch Brände, Explosionen, Stäube, Gase, Sperrungen, Strahlung, Emissionen (chemische Industrie) verursacht sein.

Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

**Beispiel:**

Bei einem Brand in einem chemischen Betrieb in unmittelbarer Nähe eines Rechenzentrums (ca. 1.000 m Luftlinie) entstand eine mächtige Rauchwolke. Das Rechenzentrum besaß eine Klima- und Lüftungsanlage, die über keine Außenluftüberwachung verfügte. Nur durch die Aufmerksamkeit eines Mitarbeiters (der Unfall geschah während der Arbeitszeit), der die Entstehung und Ausbreitung verfolgte, konnte die Außenluftzufuhr rechtzeitig manuell abgeschaltet werden.

# G 1.12 Beeinträchtigung durch Großveranstaltungen

Großveranstaltungen aller Art können zu Behinderungen des ordnungsgemäßen Betriebs einer Behörde bzw. eines Unternehmens führen. Hierzu gehören u. a. Straßenfeste, Konzerte, Sportveranstaltungen, Arbeitskämpfe oder Demonstrationen. Ausschreitungen im Umfeld solcher Veranstaltungen können zusätzlich Auswirkungen wie die Einschüchterung bis hin zur Gewaltanwendung gegen das Personal oder das Gebäude nach sich ziehen.

**Beispiele:**

- Während der heißen Sommermonate fand eine Demonstration in der Nähe eines Rechenzentrums statt. Die Situation eskalierte und es kam zu Gewalttätigkeiten. In einer Nebenstraße stand noch ein Fenster des Rechenzentrumsbereiches auf, durch das ein Demonstrant eindrang und die Gelegenheit nutzte, IT-Hardware mit wichtigen Daten zu entwenden.
- Beim Aufbau einer Großkirmes wurde aus Versehen eine Stromleitung gekappt. Dies führte in einem hierdurch versorgten Rechenzentrum zu einem Ausfall, der jedoch durch die vorhandene Netzersatzanlage abgefangen werden konnte.

# G 1.13 Sturm

Die Auswirkungen eines Sturms oder Orkans auf Außeneinrichtungen, die zum Betrieb eines Rechenzentrums mittelbar benötigt werden, werden häufig unterschätzt. Außeneinrichtungen können hierdurch beschädigt oder abgerissen werden. Abgerissene und vom Sturm fortgeschleuderte Gegenstände können weitere Folgeschäden verursachen. Weiterhin können dadurch technische Komponenten in ihrer Funktion beeinträchtigt werden.

**Beispiele:**

- Kühlleitungen der Klimaanlage eines Rechenzentrums waren auf dem Dach als flexible Hart-PVC-Schläuche verlegt, aber über weite Strecken auf der Dachhaut weder beschwert noch befestigt. Sie wurden vom Orkan gepackt und vom Dach des Gebäudes gefegt. Dabei rissen sie aus den Verbindungen. Die Kühlflüssigkeit lief aus und das System musste für mehrere Stunden stillgelegt werden. Für die Dauer des Sturmes konnten wegen der Gefahr, vom Dach geweht zu werden, keinerlei Reparaturen vorgenommen werden. Der Serverpark fiel für fast 12 Stunden aus. Er versorgt ca. 12.000 Nutzer.
- In einem anderen Fall stürzte eine Lamellenwand, welche die Rückkühlwerke auf dem Dach des Prozessrechenzentrums eines Industriebetriebs optisch verkleidete, ein. Die scharfen Kanten der Bleche durchschnitten die Elektroleitungen der Rückkühlwerke. Es gab einen Kurzschluss mit Lichtbogen, der die vom Sturm mit hoch gerissene Dachhaut in Brand steckte. Gleichzeitig wirkte die umgestürzte Verkleidung geringfügig als Windschutz - ließ aber genug Wind durch, um das Feuer zu entfachen. Der Brand setzte sich in der Isolierung zwischen Trapezblech und Dichtungsbahnen fort. Nur durch einen glücklichen Zufall konnte ein Totalschaden verhindert werden.

# G 1.14 Datenverlust durch starkes Licht

Typische Datenträger mit optischen Speichermedien sind CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-R, DVD+R, DVD-RAM, DVD-RW und MO. Informationen werden sowohl über Laser aufgebracht als auch gelesen, nur bei der MO wird magnetisch geschrieben und optisch ausgelesen. Die derart beschriebenen Datenträger sind empfindlich gegenüber starkem Licht, insbesondere im UV-Bereich, so dass die Nähe zu solchen Lichtquellen vermieden werden sollte.

Je nach Stärke und Dauer der Strahlung führt diese zu mehr oder weniger großen Datenverlusten. Besonders kritisch ist dies bei Dateien, die aufgrund ihrer internen Formatierung bereits durch geringfügige Veränderungen gänzlich unbrauchbar werden (z. B. PostScript-Dateien, Datenbanken oder verschlüsselte Dateien).

**Beispiele** für starke Lichtquellen sind:

- Sonnenlicht (vor allem an wolkenfreien Sommertagen oder in Höhenlagen),
- Halogenlampen,
- spezielle Leuchtstofflampen.

Aktuelle Untersuchungen haben ergeben, dass die negativen Auswirkungen von Sonnenlicht oder anderen UV-Lichtquellen je nach Art der optischen Speichermedien unterschiedlichen schwerwiegend sind. Bei kommerziell vervielfältigten CD-/DVD-ROMs können diese als geringfügig betrachtet werden. Bei einmal beschreibbaren Datenträgern (CD-R, DVD-R, DVD+R) ist direktes Sonnenlicht über einen längeren Zeitraum schädlich, da dieses die optischen Eigenschaften der Aufzeichnungsschicht verändern kann. Auf mehrfach beschreibbare optische Speichermedien wie CD-/DVD-RW hat Licht minimale Auswirkungen. Bei allen Datenträgern treten die meisten Schäden durch die Hitzewirkung von direktem Sonnenlicht auf.

# G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Mobile Datenträger und Geräte werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch einer Vielzahl von Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen, ebenso wie Staub oder Feuchtigkeit. Zu anderen Problemen, die durch die Mobilität der Geräte entstehen, gehören beispielsweise Transportschäden.

Ein weiterer wichtiger Aspekt bei mobilen Datenträgern und Geräten ist, dass sie oft in Bereichen mit unterschiedlichem Sicherheitsniveau benutzt werden. Bei einigen Umgebungen ist das Sicherheitsniveau den Benutzern bekannt, bei anderen nicht. Besonders Smartphones, Tablets, PDAs, Laptops und ähnliche mobile Endgeräte sind nicht nur beweglich, sondern können auch einfach mit anderen IT-Systemen kommunizieren. Daher müssen auch die Probleme betrachtet werden, die durch diese Interaktion ausgelöst werden. Innerhalb der eigenen Institution können Mitarbeiter die Vertrauenswürdigkeit von IT-Systemen weitgehend einschätzen, in fremden Umgebungen ist das jedoch schwierig. Die Kommunikation mit unbekannten IT-Systemen und Netzen birgt immer ein Gefährdungspotenzial für das eigene mobile Endgerät. So können bei der Kontaktaufnahme mit anderen IT-Systemen beispielsweise auch Schadprogramme mit übertragen oder sensible Informationen kopiert werden.

Daher muss nach der Rückkehr von mobilen Datenträgern und IT-Systemen immer kritisch hinterfragt werden, wo dieser USB-Stick, PDA oder Laptop schon überall gewesen ist, um dann die entsprechenden Vorsichtsmaßnahmen einzuleiten.

Ein weiteres Problem bei der Nutzung von fremden Infrastrukturen, wie z. B. beim Herunterladen von Informationsangeboten auf Messen, ist die häufig unzureichende Transparenz der angebotenen Dienste. Viele Diensteanbieter sammeln Kundendaten, um Profile zu erstellen, die sie zu Werbezwecken verwenden oder an Dritte weiterverkaufen. Solche Profile enthalten beispielsweise Informationen über Aufenthaltsorte und das Kommunikationsverhalten des Benutzers (welche Dienste, wann, wie oft, mit wem). Auch Anwendungen, die vollständig auf dem eigenen mobilen Endgerät ablaufen, sammeln unter Umständen Daten (z. B. über Nutzungshäufigkeit und -art) und geben sie weiter, sobald das Gerät online geht.

Immer wieder werden mobile Datenträger und Geräte verloren oder gestohlen. Je kleiner und begehrter solche Geräte sind, wie beispielsweise Smartphones, Tablets oder PDAs, desto höher ist dieses Risiko. Neben dem materiellen Verlust kann dabei durch den Verlust bzw. die Offenlegung wichtiger Daten weiterer Schaden entstehen.

# G 1.16 Ausfall von Patchfeldern durch Brand

Patchfelder und Leitungsverteiler, auf die die internen Leitungen des Hausnetzes und die externen des öffentlichen Netzes auflaufen, können durch einen Brand so stark beschädigt werden, dass eine reibungslose Datenübertragung darüber nicht mehr möglich ist. Der Schaden wird dabei nicht ausschließlich durch die Hitze des Feuers verursacht. Allein schon der Brandrauch kann die empfindliche Anschlusstechnik massiv beschädigen. Der Einsatz von Löschmitteln (Wasser, Pulver, Schaum) führt zu weiteren Schäden.

Nach einem solchen Schadensereignis ist es dann in der Regel nicht mehr möglich, bereitstehende Ersatz-Hardware einfach an derart beschädigte Patchfelder bzw. Leitungsverteiler anzuschließen, um so zumindest einen Notbetrieb rasch wieder aufnehmen zu können.

Im Allgemeinen sind sehr umfangreiche, kosten- und zeitintensive Reparaturarbeiten erforderlich, die mit einem längeren Ausfall der IT einhergehen.

# G 1.17 Ausfall oder Störung eines Funknetzes

In Funknetzen werden Informationen mittels elektromagnetischer Funkwellen übertragen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die drahtlose Kommunikation stören und im Extremfall den Betrieb des WLAN verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z. B. Bluetooth-Geräte, andere WLANs, Mikrowellenöfen, medizinische Geräte, Funk-Überwachungskameras, etc.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-Of-Service-Angriff erfolgen. Darüber hinaus sind auch Denial-Of-Service-Angriffe möglich, z. B. durch wiederholtes Senden bestimmter Steuer- und Managementsignale, die zum Verlust der Verfügbarkeit des Funknetzes führen können.

**Beispiele:**

- Bei einer ungeeignet gewählten Montageposition für eine Außenantenne und mangelhaft geplantem Blitz- und Witterungsschutz kann ein WLAN durch Blitzeinschlag oder Witterungseinflüsse ausfallen.
- Bei WLAN-Systemen, die nach dem Standard IEEE 802.11b und IEEE 802.11g im ISM-Band-Band bei 2,4 GHz operieren, können Störungen durch eine Vielzahl anderer in diesem Frequenzband zugelassener Funksysteme, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze, hervorgerufen werden.

# G 1.18 Ausfall eines Gebäudes

Gebäude können unvorhergesehen unbenutzbar werden. Dies kann durch die teilweise oder vollständige Zerstörung verursacht sein, beispielsweise durch Feuer, Sturm, Hochwasser, Erdbeben oder Explosion. Ein Ausfall eines Gebäudes kann jedoch auch dadurch verursacht sein, dass der Zutritt nicht mehr möglich ist. Dieses kann beispielsweise ausgelöst worden sein durch

- Sperrung der Gebäudeumgebung bei einem Chemieunfall, einem Bombenfund (und einer damit verbundenen anschließenden Sprengung), Hochwasser, Flächenbrand oder weiträumiger Absperrung durch einschneidender Bodenveränderungen (Kraterentstehung) aufgrund von Tiefbaumaßnahmen (z. B. U-Bahnbau),
- Ausfall der zentralen Zutrittskontrollanlage, Streik des Wachpersonals oder
- Sperrung des Gebäudes wegen Asbestverseuchung oder weil gesetzlich vorgeschriebene Brandschutzmaßnahmen nicht eingehalten worden sind und dadurch eine Gebäudenutzung vom Amtswegen untersagt wurde.

Je nach Art der Gebäudenutzung, z. B. Rechenzentren, Bürogebäude, Lagerräume, Produktionshallen oder Filialen, sind die Auswirkungen auf den Geschäftsbetrieb unterschiedlich stark.

# G 1.19 Ausfall eines Dienstleisters oder Zulieferers

Kaum eine Institution arbeitet heute noch ohne Dienstleister wie Zulieferer, Outsourcing- oder Cloud-Diensteanbieter. Wenn Organisationseinheiten von Dienstleistern abhängig sind, können Ausfälle der externen Dienste wie zum Beispiel bei IT-Systemen oder infrastrukturellen Anbindungen zu einer Beeinträchtigung der Aufgabenbewältigung führen. Der teilweise oder vollständige Ausfall eines Outsourcing- oder Cloud-Dienstleisters oder eines Zulieferers kann sich erheblich auf die betriebliche Kontinuität auswirken, insbesondere bei kritischen Geschäftsprozessen. Die Ursache eines Ausfalls kann dabei unterschiedlichster Natur sein, wie Insolvenz, einseitige Kündigung des Vertrags durch den Dienstleister oder den Zulieferer, betriebliche Probleme durch beispielsweise Naturgewalten oder Personalausfall, Qualitätsprobleme oder Imageschäden. Charakteristisch für den Cloud-Computing-Markt ist daneben eine hohe Dynamik, die häufig Übernahmen von Cloud-Diensteanbietern durch Konkurrenten nach sich zieht. Eine damit einhergehende Umstellung des Service-Portfolios kann die Service-Verfügbarkeit für den Anwender beeinträchtigen.

Bei extern betriebenen IT-Systemen und Anwendungen kann bei unzureichender Strukturierung oder Isolation der IT-Systeme des Dienstleisters bereits der Ausfall eines Systems eines anderen Kunden dazu führen, dass Geschäftsprozesse beim Auftraggeber beeinträchtigt werden. Dies kann immer dann ein Problem sein, wenn einzelne IT-Komponenten für verschiedene Kunden eines Dienstleisters gemeinsam genutzt werden. Dann kann unter Umständen ein Fehler im Datenbestand eines beliebigen Kunden des Outsourcing- oder Cloud-Dienstleisters dazu führen, dass beispielsweise bei der Host-Verarbeitung die Batch-Verarbeitung mehrerer Kunden eingestellt werden muss, wenn diese schlecht oder fehlerhaft konfiguriert ist. Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen auslagernder Institution und Outsourcing- oder Cloud-Dienstleister ausfällt.

**Beispiele:**

- Ein Unternehmen hat seine Server in einem Rechenzentrum eines externen Dienstleisters installiert. Nach einem Brand in diesem Rechenzentrum war die Finanzabteilung des Unternehmens nicht mehr handlungsfähig. Es entstanden erhebliche finanzielle Verluste für das Unternehmen.
- Die Just-in-Time-Produktion eines Unternehmens war von der Zulieferung von Betriebsmitteln externer Dienstleister abhängig. Nachdem ein LKW durch einen Defekt beim Dienstleister ausfiel, verzögerte sich die Lieferung dringend benötigter Teile drastisch. Dadurch verzögerte sich die Produktion.
- Ein Bankinstitut wickelte alle Geldtransporte mit einem Werttransportunternehmen ab. Das Werttransportunternehmen meldete überraschend Konkurs an. Die Vereinbarung und Tourenplanung mit einem neuen Werttransporter dauerten mehrere Tage und führten zu erheblichen Problemen und Zeitverzögerungen bei der Geldversorgung und -entsorgung der Bankfilialen. Dieser Fall hatte für das Bankinstitut einen großen Reputationsschaden zur Folge.
- Durch Kündigung von Personal, als Folge der Übernahme durch einen anderen Provider, gehen dem Cloud-Diensteanbieter Know-how-Träger verloren. Dadurch entstehen bei der Übernahme des Betriebs Unstimmigkeiten, wie beispielsweise Unklarheiten bezüglich der Umsetzung der Dienstleistung, und es kommt dazu, dass Dienstgütevereinbarungen (SLA) nicht eingehalten werden und vertraglich vereinbarte Dienste ausfallen.

# G 2 Gefährdungskatalog Organisatorische Mängel

G 2.27 Fehlende oder unzureichende Dokumentation

G 2.28 Verstöße gegen das Urheberrecht

G 2.29 Softwaretest mit Produktionsdaten

G 2.30 Unzureichende Domänenplanung **- entfallen**

G 2.31 Unzureichender Schutz des Windows NT Systems **- entfallen**

G 2.32 Unzureichende Leitungskapazitäten

G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern **- entfallen**

G 2.34 Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen **- entfallen**

G 2.35 Fehlende Protokollierung unter Windows 95 **- entfallen**

G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

G 2.38 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

G 2.39 Mangelhafte Konzeption eines DBMS

G 2.40 Mangelhafte Konzeption des Datenbankzugriffs

G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern

G 2.42 Komplexität der NDS **- entfallen**

G 2.43 Migration von Novell Netware 3.x nach Novell Netware Version 4 **- entfallen**

G 2.44 Inkompatible aktive Netzkomponenten

G 2.45 Konzeptionelle Schwächen des Netzes

G 2.46 Überschreiten der zulässigen Kabellänge

G 2.47 Ungesicherter Akten- und Datenträgertransport

G 2.48 Ungeeignete Entsorgung der Datenträger und Dokumente

G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter

G 2.50 Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter

G 2.51 Mangelhafte Einbindung des Telearbeiters in den Informationsfluss

G 2.52 Erhöhte Reaktionszeiten bei IT-Systemausfall **- entfallen**

G 2.53 Unzureichende Vertretungsregelungen für Telearbeit

G 2.54 Vertraulichkeitsverlust durch Restinformationen

G 2.55 Ungeordnete Groupware-Nutzung

G 2.56 Mangelhafte Beschreibung von Dateien **- entfallen**

G 2.57 Nicht ausreichende Speichermedien für den Notfall

G 2.58 Novell Netware und die Datumsumstellung im Jahr 2000 **- entfallen**

G 2.59 Betreiben von nicht angemeldeten Komponenten

G 2.60 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement

G 2.61 Unberechtigte Sammlung personenbezogener Daten

G 2.62 Ungeeigneter Umgang mit Sicherheitsvorfällen

G 2.63 Ungeordnete Faxnutzung

G 2.64 Fehlende Regelungen für das RAS-System **- entfallen**

G 2.65 Komplexität der SAMBA-Konfiguration **- entfallen**

G 2.66 Unzureichendes Sicherheitsmanagement

G 2.67 Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

G 2.68 Fehlende oder unzureichende Planung des Active Directory

G 2.69 Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory

G 2.70 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory

G 2.71 Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory

G 2.72 Unzureichende Migration von Archivsystemen

G 2.73 Fehlende Revisionsmöglichkeit von Archivsystemen

G 2.74 Unzureichende Ordnungskriterien für Archive

G 2.75 Mangelnde Kapazität von Archivdatenträgern

G 2.76 Unzureichende Dokumentation von Archivzugriffen

G 2.77 Unzulängliche Übertragung von Papierdaten in elektronische Archive

G 2.78 Unzulängliche Auffrischung von Datenbeständen bei der Archivierung

G 2.79 Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung

G 2.80 Unzureichende Durchführung von Revisionen bei der Archivierung

G 2.81 Unzureichende Vernichtung von Datenträgern bei der Archivierung

G 2.82 Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen

G 2.83 Fehlerhafte Outsourcing-Strategie

G 2.84 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister

G 2.85 Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens

G 2.86 Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister

G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen

G 2.88 Störung des Betriebsklimas durch ein Outsourcing-Vorhaben

G 2.89 Mangelhafte Informationssicherheit in der Outsourcing-Einführungsphase

G 2.90 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister **- entfallen**

G 2.91 Fehlerhafte Planung der Migration von Exchange

G 2.92 Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange

G 2.93 Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung

G 2.94 Unzureichende Planung des IIS-Einsatzes **- entfallen**

G 2.95 Fehlendes Konzept zur Anbindung anderer Systeme an Exchange

G 2.96 Veraltete oder falsche Informationen in einem Webangebot

G 2.97 Unzureichende Notfallplanung bei einem Apache-Webserver **- entfallen**

G 2.98 Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches

G 2.99 Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung

G 2.123 Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

G 2.124 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

G 2.125 Fehlerhafte oder unzureichende Planung des Zugriffs auf den Verzeichnisdienst

G 2.126 Unzureichende Protokollierung von Änderungen am Active Directory

G 2.127 Unzureichende Planung von Datensicherungsmethoden für Domänen-Controller

G 2.128 Fehlende oder unzureichende Planung des VPN-Einsatzes

G 2.129 Fehlende oder unzureichende Regelungen zum VPN-Einsatz

G 2.130 Ungeeignete Auswahl von VPN-Verschlüsselungsverfahren

G 2.131 Unzureichende Kontrolle von VPNs

G 2.132 Mangelnde Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement

G 2.133 Mangelhaft festgelegte Verantwortlichkeiten beim Patch- und Änderungsmanagement

G 2.134 Unzureichende Ressourcen beim Patch- und Änderungsmanagement

G 2.135 Mangelhafte Kommunikation beim Patch- und Änderungsmanagement

G 2.136 Fehlende Übersicht über den Informationsverbund

G 2.137 Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen

G 2.138 Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement

G 2.139 Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement

G 2.140 Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement

G 2.141 Nicht erkannte Sicherheitsvorfälle

G 2.142 Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

G 2.143 Informationsverlust beim Kopieren oder Verschieben von Daten auf Samba-Freigaben

G 2.144 Unzureichende Notfall-Planung bei einem Samba-Server

G 2.145 Unzureichende Sicherung von Trivial Database Dateien unter Samba

G 2.146 Verlust der Arbeitsfähigkeit von Vista-Clients durch fehlende Reaktivierung vor SP1

G 2.147 Fehlende Zentralisierung durch Peer-to-Peer

G 2.148 Fehlerhafte Planung der Virtualisierung

G 2.149 Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme

G 2.150 Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen

G 2.151 Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen

G 2.152 Fehlende oder unzureichende Planung des DNS-Einsatzes

G 2.153 Ungeeignete Sicherung des Übertragungsweges in einer Terminalserver Umgebung

G 2.154 Ungeeignete Anwendungen für den Einsatz auf Terminalservern

G 2.155 Fehlende oder unzureichende Planung von OpenLDAP

G 2.156 Kompatibilitätsprobleme beim Anheben der Active Directory-Funktionsebene

G 2.157 Mangelhafte Auswahl oder Konzeption von Webanwendungen

G 2.158 Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services

G 2.159 Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services

G 2.160 Fehlende oder unzureichende Protokollierung

G 2.161 Vertraulichkeits- und Integritätsverlust von Protokolldaten

G 2.162 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten

G 2.163 Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten

G 2.164 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten

G 2.165 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten

G 2.166 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten

G 2.167 Fehlende oder nicht ausreichende Vorabkontrolle

G 2.168 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten

G 2.169 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten

G 2.170 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen

G 2.171 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten

G 2.172 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland

G 2.173 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten

G 2.174 Fehlende oder unzureichende Datenschutzkontrolle

G 2.175 Unzureichende Isolation und Trennung von Cloud-Ressourcen

G 2.176 Mangelnde Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender

G 2.177 Fehlplanung von Cloud-Diensteprofilen

G 2.178 Unzureichendes Notfallmanagement beim Cloud-Diensteanbieter

G 2.179 Fehlende Herstellerunterstützung bei der Bereitstellung von Cloud-Diensten

G 2.180 Fehlerhafte Provisionierung und De-Provisionierung von Cloud-Diensten

G 2.181 Mangelhafte Planung und Konzeption des Einsatzes von Web-Services

G 2.182 Fehlendes oder unzureichendes Betreiberkonzept für Speicherlösungen

G 2.183 Fehlendes oder unzureichendes Zonenkonzept

G 2.184 Fehlendes oder unzureichendes Rechte- und Rollenkonzept in Cloud-Infrastrukturen

G 2.185 Fehlende oder unzureichende Softwarewartung (Maintenance) und fehlendes oder unzureichendes Patchlevel-Management

G 2.186 Fehlende oder unzureichende Regelungen / keine klare Abgrenzung von Verantwortlichkeiten bei Speicherlösungen

G 2.187 Fehlendes oder unzureichendes mandantenfähiges Administrationskonzept für Speicherlösungen

G 2.188 Unzureichende Vorgaben zum Lizenzmanagement bei Cloud-Nutzung

G 2.189 Fehlende oder unzureichende Strategie für die Cloud-Nutzung

G 2.190 Unzureichendes Administrationsmodell für die Cloud-Nutzung

G 2.191 Unzureichendes Rollen- und Berechtigungskonzept

G 2.192 Unzureichende Verfügbarkeit der erforderlichen personellen Ressourcen mit ausreichender Qualifikation

G 2.193 Fehlende Anpassung der Institution an die Nutzung von Cloud Services

G 2.194 Mangelhaftes Anforderungsmanagement bei Cloud-Nutzung

G 2.195 Mangelnde Überwachung der Service-Erbringung

G 2.196 Fehlende Kosten-Nutzen-Betrachtung der Cloud-Nutzung über den gesamten Lebenszyklus

G 2.197 Unzureichende Einbindung von Cloud Services in die eigene IT

G 2.198 Mangelnde Planung der Migration zu Cloud Services

G 2.199 Unzureichende Auswahl des Cloud-Diensteanbieters

G 2.200 Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs

G 2.201 Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern

G 2.202 Lock-in-Effekt

G 2.203 Integrierte Cloud-Funktionalität

G 2.204 TPM-Nutzung

| | |
|---|---|
| G 2.205 | Fehlendes Notfallvorsorgekonzept für serviceorientierte Architekturen |
| G 2.206 | Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen |
| G 2.207 | Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen |
| G 2.208 | Unzureichende physische Absicherung der elektronischen Komponenten bei eingebetteten Systemen |
| G 2.209 | Auswahl einer ungeeigneten Entwicklungsumgebung für Software |
| G 2.210 | Unzureichend gesicherter Einsatz von Entwicklungsumgebungen |
| G 2.211 | Auswahl eines ungeeigneten Vorgehensmodells zur Software-Entwicklung |
| G 2.212 | Unzureichende Berücksichtigung von Konfigurationsoptionen bei der Software-Entwicklung |
| G 2.213 | Fehlende oder unzureichende Qualitätssicherung des Softwareentwicklungsprozesses |
| G 2.214 | Fehlende oder unzureichende Konzeption des Identitäts- und Berechtigungsmanagements |

# G 2.1 Fehlende oder unzureichende Regelungen

Die Bedeutung übergreifender organisatorischer Regelungen und Vorgaben für das Ziel Informationssicherheit nimmt mit dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.

Von der Frage der Zuständigkeiten angefangen bis hin zur Verteilung von Kontrollaufgaben kann das Spektrum der Regelungen sehr umfangreich sein. Auswirkungen von fehlenden oder unzureichenden Regelungen werden beispielhaft in den anderen Gefährdungen des Gefährdungskatalogs G2 beschrieben.

Vielfach werden nach Veränderungen technischer, organisatorischer oder personeller Art, die wesentlichen Einfluss auf die Informationssicherheit haben, bestehende Regelungen nicht angepasst. Veraltete Regelungen können einem störungsfreien Betrieb entgegen stehen. Probleme können auch dadurch entstehen, dass Regelungen unverständlich oder zusammenhanglos formuliert sind und dadurch missverstanden werden.

Dass Regelungsdefizite zu Schäden führen können, machen folgende **Beispiele** deutlich:

- Durch eine mangelhafte Betriebsmittelverwaltung kann der termingerechte Arbeitsablauf in einem Rechenzentrum schon durch eine unterbliebene Druckerpapierbestellung stark beeinträchtigt werden.
- Neben einer Beschaffung von Handfeuerlöschern muss auch deren regelmäßige Wartung geregelt sein, um sicherzustellen, dass diese im Brandfall auch funktionstüchtig sind.
- Bei einem Wasserschaden wird festgestellt, dass dieser auch den darunter liegenden Serverraum in Mitleidenschaft zieht. Durch eine unzureichende Schlüsselverwaltung kann der Wasserschaden im Serverraum allerdings nicht unmittelbar behoben werden, weil keiner darüber informiert ist, wo sich der Schlüssel zum Serverraum gerade befindet. Dadurch steigt der Schaden erheblich.

# G 2.2 Unzureichende Kenntnis über Regelungen

Regelungen lediglich festzulegen sichert noch nicht, dass sie beachtet werden und der Betrieb störungsfrei ist. Allen Mitarbeitern müssen die geltenden Regelungen auch bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, darf sich nicht mit den Aussagen entschuldigen lassen: "Ich habe nicht gewusst, dass ich dafür zuständig bin." oder "Ich habe nicht gewusst, wie ich zu verfahren hatte."

**Beispiele:**

- Werden Mitarbeiter nicht darüber unterrichtet, wie sie korrekt mit mobilen Datenträgern und E-Mails umzugehen haben, besteht die Gefahr, dass hierüber Schadprogramme im Unternehmen bzw. in der Behörde verbreitet werden. Durch falsches Verhalten könnten auch vertrauliche Daten versehentlich in die Hände Unbefugter geraten.
- In einer Bundesbehörde wurden farblich unterschiedliche Papierkörbe aufgestellt, von denen eine Farbe für die Entsorgung zu vernichtender Unterlagen bestimmt war. Die meisten Mitarbeiter waren über diese Regelung nicht unterrichtet.
- In einer Bundesbehörde gab es eine Vielzahl von Regelungen zur Durchführung von Datensicherungen, die nach und nach mündlich zwischen dem IT-Sicherheitsbeauftragten und dem IT-Referat vereinbart worden waren. Eine Nachfrage ergab, dass die betroffenen Mitarbeiter die getroffenen "Vereinbarungen" nicht kannten und auch nicht wussten, wer ihr Ansprechpartner für Fragen der Datensicherung war. Die Regelungen waren auch nicht dokumentiert. Viele Benutzer haben darum z. B. von den lokalen Daten ihres Arbeitsplatzrechners keine Datensicherung angefertigt, obwohl nur auf den Servern kontinuierliche Datensicherungen zentral durchgeführt wurden.
- In einem Rechenzentrum wurde als neue Regelung festgelegt, dass wegen Problemen mit der Einbruch- und Brandmeldeanlage die Pförtnerloge auch nachts besetzt werden sollte. Der Pförtnerdienst war jedoch über diese Regelung vom Sicherheitsverantwortlichen nicht informiert worden. Als Folge war das Rechenzentrum für mehrere Wochen nachts unzureichend geschützt.
- In einer Institution existiert die Regelung, dass der Verlust eines Mobiltelefons sofort einer Leitstelle gemeldet werden muss, damit die SIM-Karte gesperrt werden kann. Einem Mitarbeiter war diese Regelung nicht bekannt. Er gab den Verlust erst Tage später nach seiner Rückkehr von einer Dienstreise an. In der Zwischenzeit wurden mit dem verlorenen Mobiltelefon jedoch diverse Premium-Dienste angerufen und Kurzmitteilungen an diese Dienste geschickt. Dadurch entstand ein erheblicher wirtschaftlicher Schaden.

# G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel

Eine nicht ausreichende Bereitstellung von Betriebsmitteln kann einen Betrieb erheblich beeinträchtigen. Störungen können sich ergeben, wenn benötigte Betriebsmittel nicht in ausreichender Menge vorhanden sind oder nicht termingerecht bereit gestellt werden.

Ebenso kann es vorkommen, dass ungeeignete oder sogar inkompatible Betriebsmittel beschafft werden, die infolgedessen nicht eingesetzt werden können.

**Beispiele:**

- Für den neu angemieteten Internet-Anschluss wird vergessen, das Entgelt für die Einrichtung an den Betreiber zu überweisen mit der Folge, dass der Anschluss nicht freigeschaltet wird. Das IT-Verfahren, das diesen Anschluss nutzen soll, kann daher nur mit Verspätung in Betrieb genommen werden.
- Ein ungeeignetes Betriebsmittel ist zum Beispiel eine komplexe und zeitkritische Anwendung, z. B. eine grafikintensive CAD-Anwendung, die auf einem nicht ausreichend leistungsfähigen Rechner installiert werden soll.
- Ein Beispiel für inkompatible Betriebsmittel sind Verbindungskabel unterschiedlicher Pin-Belegung zum Anschluss von Druckern.
- Bei der Vielzahl von Möglichkeiten, Daten zwischen zwei IT-Systemen auszutauschen, taucht häufig das Problem auf, dass jeder der beiden Rechner mindestens drei Schnittstellen zum Datenaustausch besitzt, diese aber leider nicht kompatibel sind. Typische Fragen vor jedem Datenaustausch sind beispielsweise: Diskette, CD-ROM, DVD, USB-Stick, Bluetooth?
- Auf den Arbeitsplatz-PCs soll eine neue Version des Betriebssystems aufgespielt werden. Teilweise sind allerdings verwendete Hardwarekomponenten mit der neuen Betriebssystem-Version nicht lauffähig, da keine Treiberunterstützung für die neue Betriebssystem-Version angeboten wird.
- Der Speicherplatz der Festplatten bei PCs und Servern und auch der mobilen Datenträger steigt ständig. Leider wird häufig vergessen, IT-Komponenten und Datenträger zu beschaffen, die für eine regelmäßige Datensicherung ausreichend Kapazität bieten.

# G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen

Werden bereits eingeführte Sicherheitsmaßnahmen (z. B. Klassifizierung von Informationen, Datensicherung, Zutrittskontrolle, Vorgaben für Verhalten bei Notfällen) nicht konsequent umgesetzt und regelmäßig kontrolliert, kann es sein, dass sie nicht wirksam sind oder missachtet werden. Mängel, die bei einer Kontrolle festgestellt werden, lassen sich meist ohne Schaden abstellen. Wenn Verstöße erst anlässlich eines Schadensfalls auffallen, kann oft nicht mehr rechtzeitig und der jeweiligen Situation angemessen reagiert werden.

Darüber hinaus gibt es Sicherheitsmaßnahmen, die nur wirksam sind, wenn Verantwortliche sie kontrollieren. Hierzu zählen beispielsweise Protokollierungsfunktionen, deren Sicherheitseigenschaften erst zum Tragen kommen, wenn die Protokolldaten ausgewertet werden.

**Beispiele:**

- Zur Vorbereitung von Straftaten kommt es vor, dass Schließzylinder in Außentüren und Toren von nicht autorisierten Personen ausgetauscht werden. Gerade wenn es sich um Zugänge handelt, die selten genutzt werden oder lediglich als Notausgänge vorgesehen sind, werden diese bei Streifengängen nur in Panikrichtung geprüft. Die Funktionalität der Schließzylinder wird dabei oft vernachlässigt. Zur Vorbereitung von Straftaten kommt es vor, dass Schließzylinder in Außentüren und Toren von nicht autorisierten Personen ausgetauscht werden. Gerade wenn es sich um Zugänge handelt, die selten genutzt werden oder lediglich als Notausgänge vorgesehen sind, werden diese bei Streifengängen nur in Panikrichtung geprüft. Die Funktionalität der Schließzylinder wird dabei oft vernachlässigt.
- Die Sicherheitsleitlinie einer Institution schreibt vor, dass die eingesetzten Smartphones nicht "gerootet" werden dürfen bzw. dass kein "Jailbreak" durchgeführt werden darf, da so die Sicherheitseigenschaften des Betriebssystems umgangen werden können. Solche modifizierten Smartphones sind innerhalb einer Institution nicht mehr sicher einsetzbar. Wird diese Vorgabe nicht überprüft, ist es möglich, dass Mitarbeiter mit einem unsicheren Smartphone auf das Netz oder schützenswerte Informationen der Institution zugreifen.
- In einer Behörde werden einige Unix-Server zur externen Datenkommunikation eingesetzt. Aufgrund der zentralen Bedeutung dieser IT-Systeme sieht das Sicherheitskonzept vor, dass die Unix-Server wöchentlich einer Integritätsprüfung unterworfen werden. Da nicht regelmäßig kontrolliert wird, ob diese Überprüfungen tatsächlich stattfinden, fällt erst bei der Klärung eines Sicherheitsvorfalls auf, dass die IT-Abteilung auf solche Integritätsprüfungen verzichtet hat. Als Grund wurde die mangelhafte personelle Ausstattung der Abteilung genannt.
- In einem Unternehmen wurde die Rolle des z/OS-Security-Auditors nicht besetzt. Dies hatte zur Folge, dass die Einstellungen im RACF im Laufe der Zeit nicht mehr den Sicherheitsvorgaben des Unternehmens entsprachen. Erst nach einem Produktionsausfall wurde bemerkt, dass einige Anwender mehr Rechte hatten, als sie für ihre Tätigkeit benötigten. Eine für die Produktion wichtige Anwendung war von ihnen versehentlich gestoppt worden. In einem Unternehmen wurde die Rolle des z/OS-Security-Auditors nicht besetzt. Dies hatte zur Folge, dass die Einstellungen im RACF im Laufe der Zeit nicht mehr den Sicherheitsvorgaben des Unternehmens entsprachen. Erst nach einem Produktionsausfall wurde bemerkt, dass einige Anwender mehr Rechte hatten, als sie für ihre Tätigkeit benötigten.

Eine für die Produktion wichtige Anwendung war von ihnen versehentlich gestoppt worden.

# G 2.5 Fehlende oder unzureichende Wartung

Die Funktionsfähigkeit der eingesetzten Technik muss gewährleistet bleiben. Durch regelmäßige Wartung kann die Funktionsfähigkeit der eingesetzten Technik gefördert werden. Werden Wartungsarbeiten nicht oder nur unzureichend durchgeführt, können daraus unabsehbar hohe Schäden oder Folgeschäden entstehen.

**Beispiele:**

- Die Batterien einer unterbrechungsfreien Stromversorgung (USV) verfügen infolge fehlender Wartung über eine unzureichende Kapazität (zu geringer Säuregehalt). Die USV kann einen Stromausfall nicht mehr ausreichend lange überbrücken.
- Die Feuerlöscher verfügen aufgrund fehlender Wartung nicht mehr über einen ausreichenden Druck, so dass ihre brandbekämpfende Wirkung nicht mehr gewährleistet ist.
- Der Laserdrucker fällt aufgrund von Überhitzung aus, weil ein Lüftungsgitter nicht vorschriftsmäßig gereinigt wurde.
- Im Serverraum stehen viele Geräte mit eigener Hitzeentwicklung. Kommen dazu noch hochsommerliche Temperaturen und eine nicht ausreichende Klimatisierung (z. B. fehlende oder defekte Klimaanlage) des Raumes, kann es vereinzelt zu temperaturbedingten Geräteausfällen aufgrund von Überhitzung kommen. Klimaanlagen, die fest installiert sind, müssen daher regelmäßig gewartet und gereinigt werden, um eine verlässliche und störungsfreie Funktion sicherzustellen.

# G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Alle Räume, in denen schutzbedürftige Informationen aufbewahrt bzw. weiterverarbeitet oder in denen schutzbedürftige Geräte betrieben werden, werden dadurch zu schutzbedürftigen Räumen. Beispiele hierfür sind Büroräume, aber auch Archive, in denen Datenträger und Akten zentral aufbewahrt werden. Ebenso hierzu zählen Technik-Verteilräume mit zentralen Komponenten wie Stromverteiler, Netzkoppelelemente und Server.

Unbefugte Personen können in solchen Räumen durch vorsätzliche Handlungen (z. B. Manipulationen oder Vandalismus), aber auch durch unbeabsichtigtes Fehlverhalten (z. B. aufgrund mangelnder Fachkenntnisse) Schäden verursachen. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann der Betriebsablauf schon dadurch gestört werden, falls untersucht werden muss, wie ein solcher Vorfall möglich war oder ob Schäden aufgetreten sind oder Manipulationen vorgenommen wurden.

Eindringlinge könnten beispielsweise Passwörter zurückgesetzt, direkt auf die Server zugegriffen oder aktive Netzkomponenten manipuliert haben. Außerdem könnten sie sensible Informationen auf Papier oder Datenträgern entwendet oder verändert haben.

Nicht nur Räume auf dem Betriebsgelände müssen vor unbefugtem Zutritt geschützt werden, sondern auch dienstlich genutzte Räume im häuslichen Umfeld. Einbruchsicherungen (z. B. abschließbare Fenstergriffe, Sicherheitsschlösser und Sicherheitsverriegelung und -verglasung an Haustüren) werden im privaten Umfeld für häusliche Arbeitsplätze oft aus Kostengründen nicht realisiert. Dadurch ist beispielsweise bei Telearbeitsplätzen der Schutz vor Einbrüchen niedriger als innerhalb eines Unternehmens oder einer Behörde.

**Beispiele:**

- Die gesamte zentrale IT eines Unternehmens wurde in einem Serverraum untergebracht, der mit einer restriktiven und modernen Zutrittsbeschränkung ausgestattet wurde. Im Sommer wird aber festgestellt, dass die Klimatisierung für die vielen IT-Systeme nicht ausreichend ist. Daher wurden zur Kühlung an heißen Tagen Fenster und Türen weit geöffnet. Kurze Zeit später war ein neuer, noch nicht aktivierter Server spurlos verschwunden.
- Ein Mitarbeiter hatte zuhause zwar ein separates Arbeitszimmer für die Telearbeit eingerichtet, aber es nicht konsequent abgeschlossen. Als die Kleinkinder kurz unbeaufsichtigt waren, spielten sie in dem nicht verschlossenen Arbeitszimmer. Dabei wurden wichtige Dokumente als Malgrundlage verwendet. Außerdem wurden die Öffnungen des Rechners mit Spielzeug und Keksen verstopft, was zu einem Totalausfall der IT führte.
- In einem Unternehmen konnte jeder Mitarbeiter alle Druckerräume betreten. Dadurch gelang es einem Angreifer, physikalisch auf einen zentralen Drucker zuzugreifen und diesen umzukonfigurieren. Dies führte dazu, dass alle zu druckenden Dokumente auf die integrierte Festplatte des Druckers geschrieben und anschließend nicht gelöscht wurden. Als die Festplatte voll war, hat er sie gegen eine leere ausgetauscht und die volle auf seinem Rechner ausgewertet.
  Obwohl der Angreifer nicht in der Entwicklungsabteilung tätig war, konnte er auf diese Weise eine Vielzahl von wichtigen Entwicklungsdokumenten unbemerkt aufzeichnen und an die Konkurrenz verkaufen, bevor diese Quelle aufflog.

- Beim Reinigungspersonal wird eine Urlaubsvertretung eingesetzt. Die Urlaubsvertretung übernimmt eigenmächtig, obwohl sie dafür nicht eingewiesen wurde, die Reinigung des Rechenzentrums. Dort öffnet sie den alarmüberwachten Notausgang und löst hierdurch einen Fehlalarm aus.
- Bei einem Einbruch in einem Bürogebäude sind auf den ersten Blick nur die Kaffeekasse und zwei neue Laptops verschwunden. Trotzdem müssen alle Akten gesichtet werden, ob wesentliche Teile fehlen und alle IT-Systeme daraufhin geprüft werden, ob unbefugt auf sie zugegriffen wurde.
- Auch ein vorhandener Zutrittsschutz kann versagen, wenn er nicht angemessen ist. Ein gutes Schloss ist beispielsweise wertlos, wenn weder die Tür stark genug ist noch die Scharniere fachmännisch montiert wurden.

# G 2.7 Unerlaubte Ausübung von Rechten

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um Informationen, Geschäftsprozesse und IT-Systeme vor unbefugtem Zugriff zu schützen. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, kann sich eine Vielzahl von Gefahren für die Vertraulichkeit und Integrität von Daten oder die Verfügbarkeit von Rechnerleistung ergeben.

**Beispiele:**

- Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar. Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar.
- Ein Mitarbeiter ist erkrankt. Ein Zimmerkollege weiß aufgrund von Beobachtungen, wo dieser sein Passwort auf einem Merkzettel aufbewahrt und verschafft sich Zugang zum Rechner des anderen Mitarbeiters. Da er erst kürzlich durch ein Telefonat mitbekommen hat, dass der Kollege noch eine fachliche Stellungnahme abzugeben hatte, nimmt er hier unberechtigterweise diese Aufgabe im Namen seines Kollegen wahr, obwohl er zu der Thematik nicht auf dem aktuellen Sachstand ist. Eine daraus folgende Erstellung einer Ausschreibungsunterlage in der Verwaltungsabteilung fordert im Pflichtenheft daher eine längst veraltete Hardwarekomponente, weil die dortigen Mitarbeiter der fachlichen Stellungnahme des erfahrenen Kollegen uneingeschränkt vertraut haben.

# G 2.8 Unkontrollierter Einsatz von Betriebsmitteln

Betriebsmittel - gleich welcher Art - dürfen nur entsprechend dem Verwendungszweck eingesetzt werden. Die für die Beschaffung und den Einsatz der Betriebsmittel verantwortlichen Personen müssen sowohl den unkontrollierten Einsatz verhindern als auch den korrekten Einsatz überwachen. Wird jedoch der Einsatz von Betriebsmitteln nicht ausreichend kontrolliert, können als Folge vielfältige Gefährdungen auftreten.

**Beispiele:**

- Der Einsatz privater Datenträger durch Mitarbeiter kann zu einem Befall der dienstlichen APC durch Schadprogramme führen.
- Falsche Reinigungsmittel können zu einer Beschädigung von Monitoren führen.
- Ungeeignete Tinte für Tintenstrahldrucker kann zu einer Verunreinigung oder Fehlfunktion des Druckers führen.
- In einem Betrieb wurde der Verbrauch von DVDs nicht kontrolliert. Erst bei einer zufälligen Plausibilitätsprüfung stellte sich heraus, dass im letzten halben Jahr unerklärbar viele DVDs verbraucht worden waren. Bei Nachfragen stellte sich heraus, dass viele Mitarbeiter diese benutzten, um kleinere Datenmengen für den Datenaustausch aufzuspielen. Anschließend hatten sie die DVDs weggeworfen, weil ihnen nicht erklärt worden war, dass DVDs im Multi-Session-Mode mehrmals verwendet werden können, wenn nur geringe Datenmengen darauf gespeichert werden.

# G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

Die speziell für den Einsatz von Informationstechnik geschaffenen organisatorischen Regelungen, aber auch das gesamte Umfeld einer Behörde bzw. eines Unternehmens unterliegen ständigen Veränderungen. Sei es nur, dass Mitarbeiter ausscheiden oder hinzukommen, Mitarbeiter das Büro wechseln, neue Hardware oder Software beschafft wird, der Zulieferbetrieb für die Betriebsmittel Konkurs anmeldet. Dass sich bei einer ungenügenden Berücksichtigung der vorzunehmenden organisatorischen Anpassungen Gefährdungen ergeben, zeigen folgende **Beispiele:**

- Durch bauliche Änderungen im Gebäude werden bestehende Fluchtwege verändert. Da die Mitarbeiter nicht ausreichend unterrichtet wurden, ist die Räumung des Gebäudes nicht in der erforderlichen Zeit möglich.
- Durch eine Umstellung eines IT-Verfahrens werden größere Mengen an Druckerpapier benötigt. Da die Beschaffungsstelle nicht unterrichtet wurde, kommt es zu Engpässen im IT-Betrieb.
- Beim Empfang elektronischer Dokumente oder Dateien werden diese nicht automatisch auf Schadprogramme überprüft, da kein entsprechendes Viren-Schutzprogramm vorhanden ist.
- Bei der Übermittlung elektronischer Dokumente wird nicht darauf geachtet, ein für die Empfängerseite lesbares Datenformat zu verwenden
- Durch eine zunehmende Nutzung von Cloud-Diensten und die rasante Entwicklung der Überwachungs- und Abhörtechnik sind vertrauliche Dokumente möglicherweise nicht mehr ausreichend geschützt.
- Der Einsatz und die wachsende Vielfalt von Apps birgt neue Sicherheitsrisiken, wenn deren Herkunft und Berechtigungen nicht ausreichend geprüft werden.

# G 2.10 Nicht fristgerecht verfügbare Datenträger

Die korrekte Verwendung von Datenträgern ist für viele Geschäftsprozesse und IT-Verfahren von besonderer Bedeutung. Bereits geringfügige Fehler, z. B. mangelhafte Kennzeichnung, falscher Aufbewahrungsort, fehlende Ein- oder Ausgabebestätigungen im Datenträgerarchiv, können dazu führen, dass ein Datenträger nicht in der erforderlichen Zeit aufgefunden werden kann. Die resultierenden Verzögerungen können zu erheblichen Schäden führen.

**Beispiele:**

- Bei der Erstellung eines Geschäftsberichts stellt sich in einer Firma heraus, dass der unterschriebene Prüfbericht des Wirtschaftsprüfers in den Akten nicht auffindbar war. Da dieser aber zwingend im Original benötigt wurde, entstand ein hoher Aufwand bei der Suche im gesamten Aktenbestand. Obwohl der Bericht schließlich gefunden wurde, konnte der Geschäftsbericht nicht zum geplanten Termin fertig gestellt werden.
- Datensicherungsbänder werden versehentlich in ein externes Datensicherungsarchiv ausgelagert. Eine erforderliche Datenrekonstruktion wird erheblich verzögert, weil die Wiederbeschaffung der Bänder nicht unverzüglich möglich ist.
- Datensicherungsbänder unterschiedlichen Inhalts werden versehentlich gleich gekennzeichnet. Der Archivverwalter gibt unabsichtlich das aktuellere Magnetband zum Löschen frei. Folglich steht nur noch eine überalterte Datensicherung zur Verfügung.
- Bandverwaltungssysteme im z/OS-Betriebssystem verwenden Batch-Jobs, um Datensicherungsbänder mit erreichtem *Expiration Date* zu erkennen und zum Überschreiben frei zu geben. Bricht dieser Batch-Job ab oder läuft erst gar nicht an, so stehen unter Umständen nicht genug Leerbänder (*Scratch Tapes*) für die Folgesicherungen zur Verfügung und es kann zu Engpässen in der Bandverarbeitung kommen.

# G 2.11 Unzureichende Trassendimensionierung

Bei der Planung von Netzen, Serverräumen oder Rechenzentren wird oft der Fehler begangen, die funktionale, kapazitive oder sicherheitstechnische Auslegung ausschließlich am aktuellen Bedarf auszurichten. Dabei wird übersehen, dass

- die Kapazitäten des Netzes und der Rechner aufgrund steigender Datenvolumina oder Einsatz neuer Dienste und Dienstleistungen erweitert werden müssen,
- Änderungen technischer Standards bauliche oder sicherheitstechnische Anpassungen nach sich ziehen können,
- Erweiterungen des Netzes aus geänderten betrieblichen Erfordernissen oft nötig werden,
- neue Anforderungen an das Netz sogar die Verlegung anderer Kabel erforderlich machen.

**Beispiele:**

- Eine Erweiterung von Netzen ist nur in dem Umfang möglich, wie es die vorhandenen, verlegten Kabel zulassen oder der zur Verfügung stehende Platz für zusätzliche Kabel erlaubt. Gerade in geschlossenen Trassen (Rohre, estrichüberdeckte Fußbodenkanäle etc.) ist es trotz noch vorhandenen Platzes oft nicht möglich, zusätzliche Kabel einzuziehen, ohne neue und alte Kabel zu beschädigen. Als Ausweg bleibt dann nur, die vorhandenen Kabel aus der Trasse herauszuziehen und alle Kabel, die alten und die neuen, gleichzeitig neu einzuziehen. Die dadurch entstehenden Betriebsbeeinträchtigungen und Kosten sind beträchtlich.
- Die Planung eines Rechenzentrums erfolgte zunächst allein unter ästhetischen Gesichtspunkten. Infrastrukturelle und sicherheitstechnische Anforderungen standen im Hintergrund und wurden erst nach der Rohbauerstellung konkreter definiert. Die Fertigstellung des Baus verzögerte sich, weil erforderliche Trassen nicht zur Verfügung standen und Räume nicht bedarfsgerecht dimensioniert oder positioniert waren. Änderungen während des späteren Betriebs waren nur unter großen Umständen zu bewältigen.
- In einem Unternehmen wurde nach zehn Jahren Betriebszeit eine vollständig neue Netzstruktur und IT-Verkabelung geplant. Auf Nachfrage stellte sich heraus, dass im folgenden Jahr eine Erneuerung der TK-Anlage und der TK-Verkabelung geplant war, die bislang zusammen mit der IT-Verkabelung in derselben Trasse geführt wurde. Ohne Koordinierung dieser beiden Maßnahmen wären doppelte Arbeiten an den Trassen erforderlich geworden und es wären möglicherweise zu kleine Trassen geplant worden.

# G 2.12 Unzureichende Dokumentation der Verkabelung

Ist aufgrund unzureichender Dokumentation die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Es kann nicht davon ausgegangen werden, dass alle Kabel und Leitungen in den Installationszonen gemäß DIN 18015-3 "Elektrische Anlagen in Wohngebäuden - Teil 3: Leitungsführung und Anordnung der Betriebsmittel" oder ähnlicher Normen installiert sind. Insbesondere durch Betonleerverrohrung oder Verkabelung während des Betonbaus können sich systembedingt Veränderungen der Lage der Verkabelung während des Betonierens ergeben. Auch die Bauweise mit Gipskarton-Ständerwänden führt häufig zu einer unkoordinierten Verkabelung. Wenn Kabel und Leitungen in Böden oder Decken verlegt sind, kann eine geometrische oder eine direkte Leitungsführung gewählt worden sein. Auch zufällige Anordnungen sind möglich, so dass bei Böden und Decken keine Rückschlüsse über Leitungsführungen an Hand von sichtbaren Betriebsmitteln (Leuchten, Schalter, Tanks etc.) möglich ist. Bei Ausfall durch Beschädigung von Leitungen kann es zu längeren Ausfallzeiten oder unter Umständen sogar zu lebensbedrohenden Gefahren, z. B. durch Stromschlag, kommen.

Eine unzureichende Dokumentation erschwert zudem die Prüfung, Wartung und Reparatur von Leitungen.

# G 2.13 Unzureichend geschützte Verteiler

Unterverteilungen des Stromversorgungsnetzes sind vielfach frei zugänglich und unverschlossen in Fluren oder Treppenhäusern untergebracht. Dadurch ist es jedermann möglich, diese Verteiler zu öffnen, Manipulationen vorzunehmen und gegebenenfalls einen Stromausfall herbeizuführen. Ferner kann von solchen Verteilern eine unmittelbare Gefahr ausgehen, da nach Entnahme von Schraubsicherungen und deren Sockeln ein direktes Berühren spannungsführender Teile möglich ist. Offenstehende Türen an den Verteilerkästen können zudem den Verkehrsweg behindern, auch Verletzungen durch Klemmen und Quetschen an den Scherkanten sind möglich.

# G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Arbeitsplatz oder das Arbeitsumfeld (z. B. Störungen durch Lärm oder Staub) können dazu führen, dass die zur Verfügung stehende IT nicht oder nicht optimal genutzt werden kann.

Die meisten der denkbaren Störungen wirken sich nicht direkt auf die IT aus. Vielmehr werden die Benutzer in der Form beeinflusst, dass sie ihren Aufgaben nicht mit entsprechender Konzentration nachgehen können. Die Störungen reichen von Lärm oder starkem, unorganisiertem Kundenverkehr bis zu ungünstiger Beleuchtung, schlechter Belüftung und ähnlichem. Als erste Anzeichen solcher Störungen kann sich die Aufgabenerledigung verlangsamen und die Anzahl kleiner Fehler zunehmen (Zeichendreher, Schreibfehler). Dadurch wird nicht nur das direkte Arbeitsergebnis beeinträchtigt. Auch die gespeicherten Daten enthalten eventuell Fehler, die Integrität der Daten wird vermindert.

# G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System

Durch verschiedene Unix-Programme ist es möglich, Daten abzufragen, die das IT-System über die Benutzer speichert. Hiervon sind auch solche Daten betroffen, die Auskunft über das Leistungsprofil eines Benutzers geben können. Datenschutzrechtliche Gesichtspunkte müssen deshalb genauso beachtet werden wie die Gefahr, dass solche Informationen Missbrauchsmöglichkeiten erleichtern.

**Beispiel:**

Mit einem einfachen Programm, das in einem bestimmten Zeitintervall die Informationen, die der Befehl *who* liefert, auswertet, kann jeder Benutzer ein genaues Nutzungsprofil für einen Account erstellen. z. B. lassen sich auf diese Weise die Abwesenheitszeiten des oder der Systemadministratoren feststellen, um diese Zeiten für unberechtigte Handlungen zu nutzen. Desweiteren lässt sich feststellen, welche Terminals für einen privilegierten Zugang zugelassen sind.

Weitere Programme mit ähnlichen Missbrauchsmöglichkeiten sind *finger* oder *ruser*.

# G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs

Der Benutzerwechsel bei tragbaren PC wie Laptops oder Notebooks wird oftmals durch die einfache Übergabe des Gerätes vorgenommen. Dies hat zur Folge, dass meist nicht sichergestellt wird, dass auf dem Gerät keine schutzbedürftigen Daten mehr gespeichert sind und dass das Gerät nicht mit einem Computer-Virus verseucht ist. Zudem ist nach einiger Zeit nicht mehr nachvollziehbar, wer den tragbaren PC wann genutzt hat oder wer ihn zurzeit benutzt. Der ungeordnete Benutzerwechsel ohne Speicherkontrollen und ohne entsprechende Dokumentation kann damit zur Einschränkung der Verfügbarkeit des Geräts und zum Vertraulichkeitsverlust von Restdaten der Festplatte führen.

# G 2.17 Mangelhafte Kennzeichnung der Datenträger

Wenn Datenträger unzureichend gekennzeichnet sind, ist häufig bereits nach kurzer Zeit nicht mehr nachvollziehbar, wem der Datenträger gehört, welche Informationen darauf gespeichert sind oder welchem Zweck sie dienen. Beim Datenträgeraustausch ist ohne eine ordnungsgemäße Kennzeichnung der ausgetauschten Datenträger für den Empfänger oft nicht einmal feststellbar, wer den Datenträger übersandt hat oder ob Zugriffsrestriktionen zu beachten sind. Wenn mehrere Datenträger ein- und desselben Absenders eingehen, kann bei fehlender Kennzeichnung die Reihenfolge verwechselt werden.

**Beispiele:**

- An das BSI werden häufig Freiumschläge gesandt, mit der Bitte um Zusendung von Broschüren oder CDs. Immer wieder kommt es dabei vor, dass weder im Anschreiben noch auf dem Rückumschlag eine Anschrift vermerkt ist.
- Der Absender verschickt an den Empfänger eine DVD mit Informationen, bei denen großes Gewicht auf deren Integrität gelegt wird. Am nächsten Tag stellt der Absender fest, dass die Daten fehlerhaft waren, verschickt eine korrigierte Version und kündigt diese beim Empfänger telefonisch an. Auf dem Postweg überholt nun die zweite DVD die erste, so dass der Empfänger aufgrund mangelhafter Kennzeichnung glaubt, die zuerst erhaltene DVD enthielt die falschen Daten.
- Vor einer Software-Änderung wurden wichtige Anwendungsdaten zur Datensicherung auf CD-ROMs gebrannt. Da dies als kurzfristige Aktion geplant war, wurden die CD-ROMs nicht ordnungsgemäß beschriftet, nur durchnummeriert. Obwohl darauf vertrauliche Kundendaten gespeichert waren, blieben die CD-ROMs nach der erfolgreichen Installation offen in einem Büro liegen. Als dies nach einigen Wochen auffiel, fehlte bereits die Hälfte der CD-ROMs.

# G 2.18 Ungeregelte Weitergabe von Datenträgern

Bei einer ungeregelten Weitergabe bzw. ungeordneter Zustellung von Datenträgern besteht die Gefahr, dass vertrauliche, auf den Datenträgern gespeicherte Informationen in unbefugte Hände gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

**Beispiele:**

- Eine fehlerhafte Adressierung beim Versand kann dazu führen, dass Datenträger einem unautorisierten Empfänger übergeben werden.
- Eine unzureichende Verpackung kann zu einer Beschädigung der Datenträger führen, aber auch einen unbefugten Zugriff ermöglichen, der nicht festgestellt werden kann.
- Eine fehlende Festlegung der Verantwortung beim Empfänger kann zur Folge haben, dass ein eingegangener Datenträger erst verspätet bearbeitet wird.
- Eine nicht festgelegte Versandart kann bewirken, dass der Datenträger zu spät zugestellt wird, da die falsche Versandart ausgewählt wurde.
- Wenn nicht klar geregelt ist, wer auf Seiten des Absenders zuständig ist, die Datenträger zu erstellen und zu versenden, kann dies zur Folge haben, dass Termine nicht eingehalten werden können, weil die Informationen nicht rechtzeitig beim Empfänger eingetroffen sind.

# G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Werden zum Schutz der Vertraulichkeit zu übermittelnder Daten Verschlüsselungssysteme eingesetzt, so kann aufgrund eines unzureichenden Schlüsselmanagements der gewünschte Schutz unterlaufen werden, wenn

- die kryptographischen Schlüssel in einer ungesicherten Umgebung erzeugt oder aufbewahrt werden,
- ungeeignete oder leicht zu erratende Schlüssel eingesetzt werden und
- die zur Verschlüsselung bzw. Entschlüsselung eingesetzten Schlüssel den Kommunikationspartner nicht auf einem sicheren Weg erreichen.

**Beispiele:**

- Einfachstes Negativbeispiel ist der Versand der verschlüsselten Informationen und des benutzten Schlüssels auf demselben Datenträger. In diesem Fall kann jeder, der in den Besitz des Datenträgers gelangt, die Informationen entschlüsseln, vorausgesetzt, dass das bei der Verschlüsselung eingesetzte Verfahren bekannt ist.
- Kryptographische Schlüssel werden im Allgemeinen durch Zufallsprozesse erzeugt und eventuell nachträglich verändert. Wenn die verwendete Zufallsquelle ungeeignet ist, können Schlüssel erzeugt werden, die unsicher sind.
- Insbesondere bei Masterkeys ist es für die Sicherheit entscheidend, dass keine schwachen kryptographischen Schlüssel erzeugt werden. Dies können Schlüssel sein, die leicht zu erraten oder für die Verschlüsselung ungeeignet sind (Beispiel: schwache und semischwache DES-Schlüssel). Wenn bei der Ableitung von Schlüsseln aus Masterkeys nicht überprüft wird, ob dabei ein schwacher Schlüssel erzeugt wurde, kann ein schwacher Schlüssel im Wirkbetrieb zum Einsatz kommen.
- Werden bei Triple-DES identische Teilschlüssel verwendet, wirkt die Triple-DES-Verschlüsselung nur wie eine einfache DES-Verschlüsselung. Der Sicherheitsgewinn geht verloren.
- In serviceorientierten Architekturen (SOA), insbesondere in solchen, die stark verteilt sind, ist es notwendig, die kryptographischen Schlüssel automatisch zu generieren und zu verwalten. Schlüsselgenerierung und -verwaltung unterliegen hier besonderen Risiken, falls sie nicht ausreichend abgesichert sind.
- Aber nicht nur die Offenlegung, sondern auch der Verlust von kryptographischen Schlüsseln kann zu großen Problemen führen. Kryptographische Schlüssel können

  - verloren oder vergessen werden,
  - nicht mehr zugreifbar sein, zum Beispiel wenn der Schlüsselinhaber die Firma verlassen hat oder
  - zerstört werden, indem sie versehentlich gelöscht oder verändert werden, beispielsweise durch Datenträgerversagen oder Bitfehler.

  Wenn die Schlüssel nicht mehr verfügbar sind, können damit geschützte Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden.

# G 2.20 Unzureichende oder falsche Versorgung mit Verbrauchsgütern

Viele im Büroalltag eingesetzte Geräte wie Faxgeräte, Drucker, Datensicherungslaufwerke usw. benötigen für einen reibungslosen und unterbrechungsfreien Betrieb Verbrauchsgüter in ausreichender Menge. Fehlen Verbrauchsgüter, kann der Betriebsablauf empfindlich gestört werden. In Notfällen kann die Handlungsfähigkeit stark beeinträchtigt sein und hohe Folgekosten verursachen, weil Verbrauchsgüter nicht in ausreichender Menge zur Verfügung stehen.

**Beispiele:**

- Eingehende Faksimiles können nicht ausgedruckt werden, obwohl sie ordnungsgemäß empfangen wurden, wenn der Papier- oder der Tonervorrat aufgebraucht sind. Der Puffer-Speicher kann aufgrund seiner begrenzten Speicherkapazität die Abweisung oder den Verlust von Fax-Sendungen nur herauszögern, aber nicht langfristig verhindern.
- Es wird ein neues Bandlaufwerk beschafft, das mit den alten Bändern nicht kompatibel ist. Neue passende Bänder sind nicht beschafft worden, daher können tagelang keine Datensicherungen angefertigt werden.
- Ein wichtiger Druckjob steht an. Die beschaffte Tonerkartusche zur Reserve passt jedoch nicht für den Drucker.

# G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern

Arbeiten mehrere Benutzer zeitlich versetzt an einem Einzelplatz-IT-System, so findet zwangsläufig ein Wechsel zwischen den Benutzern statt. Ist dieser nicht ausreichend organisiert und geregelt, wird er unter Umständen nicht sicherheitsgerecht durchgeführt. Hierdurch können Missbrauchsmöglichkeiten entstehen, wenn z. B.

- laufende Anwendungen nicht korrekt abgeschlossen werden,
- aktuelle Daten nicht gespeichert werden,
- Restdaten im Hauptspeicher oder in temporären Dateien verbleiben,
- der vorhergehende Benutzer sich nicht am IT-System abmeldet und
- der neue Benutzer sich nicht ordnungsgemäß am IT-System anmeldet.

# G 2.22 Fehlende oder unzureichende Auswertung von Protokolldaten

In vielen IT-Systemen und Anwendungen sind Funktionalitäten integriert, um bestimmte Ereignisse in ihrem zeitlichen Ablauf protokollieren zu können. Dadurch werden in einem Informationsverbund oft große Mengen an Protokolldaten erzeugt, die sich nur schwer und mit einem hohen Zeitaufwand auswerten lassen. Allerdings ist eine sinnvolle Auswertung dieser Protokolldaten notwendig, um beispielsweise Fehleranalysen durchführen und erfolgte Angriffe identifizieren zu können.

Im Lebenszyklus eines IT-Systems kommen verschiedene Protokollierungskonzepte zum Einsatz. So werden während der Entwicklungsphase ausführliche Protokolle erstellt, um die Problemanalyse bei Fehlern zu erleichtern.

In der Einführungsphase werden Protokolle genutzt, um unter anderem die Performance des IT-Systems in der Produktivumgebung zu optimieren oder um die Wirksamkeit des Sicherheitskonzepts erstmals in der Praxis zu überprüfen.

In der Produktivphase dienen Protokolle hauptsächlich dazu, den ordnungsgemäßen Betrieb sicherzustellen. Über Protokolldaten werden dann unter anderem nachträglich Sicherheitsverletzungen im IT-System oder Angriffsversuche identifiziert. Die Protokollierung kann auch der Täterermittlung und in Folge der Abschreckung von potenziellen Tätern dienen. Über eine regelmäßige Auswertung der Protokolldaten lassen sich die Daten für Präventivmaßnahmen wie ein Frühwarnsystem heranziehen, wodurch unter Umständen vorsätzliche Angriffe auf ein IT-System frühzeitig erkannt oder vereitelt werden können.

**Zentrale Protokollierung**

Werden Protokolldaten an zentraler Stelle ausgewertet, ist es möglich, dass bei der großen Menge an Daten wichtige Informationen übersehen und zum Beispiel Angriffe nicht entdeckt werden. Aus diesem Grund gibt es Systeme, die den Administrator bei der Auswertung der Protokolldaten unterstützen oder die Daten sogar selbstständig auswerten. Je nach Produkt können die Informationen der verschiedenen Datenquellen miteinander vereint und zu einer Protokollmeldung verarbeitet werden. Es besteht jedoch die Gefahr, dass die Protokolldaten eventuell nicht mehr auf ihre ursprüngliche Datenquelle zurückgeführt werden können, sodass auch nicht mehr auf Anhieb nachvollzogen werden kann, wo das Ereignis ursprünglich aufgetreten ist.

Weitere Probleme bei der Auswertung können durch falsch eingestellte Filterfunktionen der Analysewerkzeuge entstehen. Das kann dazu führen, dass Protokolldaten, die für die Störungserkennung, Fehlersuche oder Frühwarnung erforderlich sind, nicht ausgewertet werden.

**Beispiele:**

- Ein Angreifer versucht, den Datenbank-Server durch eine DoS-Attacke zum Absturz zu bringen. Dieser Angriff wird auf dem betreffenden IT-System protokolliert. Der Angriff bleibt aber durch die fehlende Auswertung der Protokolldaten unentdeckt, und der Angreifer kann die DoS-Attacke bis zum Erfolg wiederholen.
- Bei einem Angriff auf einen Webserver wurde eine RPC-Sicherheitslücke dazu benutzt, um in das System einzudringen. Zwar hat der Webserver entsprechende Protokolldaten erzeugt, diese wurden jedoch aufgrund feh-

lerhafter Filtereinstellungen am zentralen Protokollierungsserver verworfen. Somit wurde kein automatischer Alarm ausgelöst, und der Angriff blieb unentdeckt.

# G 2.23 Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz

Diese Gefährdung ist mit Version 2006 entfallen.

# G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes

Bei einem nicht durch eine Firewall geschützten Netz, das mit einem externen Netz wie dem Internet gekoppelt ist, können aus dem externen Netz verschiedene Daten des internen Netzes wie z. B. Mailadressen, IP-Nummern, Rechnernamen und Benutzernamen abgerufen werden. Dadurch lassen sich Rückschlüsse auf die interne Netzstruktur und dessen Anwender ziehen. Je mehr Informationen ein Angreifer über potentielle Angriffsziele hat, desto mehr Angriffsmöglichkeiten hat er. Wenn ein Angreifer z. B. Benutzernamen eines IT-Systems kennt, kann er versuchen, die zugehörigen Passwörter zu erraten oder über Wörterbuchattacken herauszufinden (siehe G 5.18 *Systematisches Ausprobieren von Passwörtern*).

# G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Wird neue Hard- oder Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, kann es passieren, dass Fehler in der Hard- oder Software nicht erkannt werden oder dass die notwendigerweise einzuhaltenden Installationsparameter nicht erkannt bzw. nicht beachtet werden. Diese Hardware-, Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Test- und Freigabeverfahren resultieren, stellen eine erhebliche Gefährdung für den IT-Betrieb dar.

Im Vertrauen auf eine problemlose Installation neuer Hard- bzw. Software wird oftmals übersehen, dass mögliche Schäden in keinem Verhältnis zu dem Aufwand stehen, den ein geordnetes Test- und Freigabeverfahren erfordert. Programme oder IT-Systeme werden unzureichend getestet und mit Fehlern in eine Produktionsumgebung eingebracht. Die Fehler wirken sich in der Folge störend auf den bis zu diesem Zeitpunkt problemlosen Betrieb aus.

**Beispiele** für solche Schäden werden nachfolgend aufgezeigt:

- Programme oder Programm-Updates lassen sich nicht sinnvoll nutzen, da für ein annehmbares Verarbeitungstempo mehr Ressourcen (z. B. Hauptspeicher, Prozessorkapazität) als erwartet benötigt werden. Wird dies nicht im Test erkannt, kann das zu erheblichen Fehl- oder Folgeinvestitionen führen. Nicht selten führten Entscheidungen gegen weitere Investitionen dazu, dass IT-Systeme oder Anwendungen zwar gekauft und bezahlt, jedoch nie benutzt wurden.
- Eingeübte Arbeitsabläufe werden nach Installation neuer Software maßgeblich behindert. Der mit der Installation des Programms beabsichtigte Nutzen stellt sich erst bedeutend später ein, da die Mitarbeiter im Vorfeld nicht geschult bzw. nicht über die neuen Funktionen des Programms informiert wurden.
- Durch das Einspielen eines Updates einer DBMS-Standardsoftware, das mit Fehlern behaftet ist, steht die Datenbank nicht mehr zur Verfügung oder es kommt zu Datenverlust.
- Einige Software-Produkte installieren den Microsoft SQL Server Express (SSE) als Datenbank, ohne dass dies vom Benutzer bemerkt wird. Hierbei handelt sich um eine Ausprägung des Microsoft SQL Servers mit den typischen Gefährdungen eines Datenbanksystems. Oft sind die Benutzer des Produktes bzw. die Administratoren, die das Produkt installieren, nicht ausreichend über diese Gefährdungen informiert und versäumen, sicherheitsrelevante Maßnahmen zu ergreifen. So wird häufig in Verbindung mit SSE ein Benutzerkonto in der Datenbank für den Administrator angelegt, das in der Grundinstallation über keinen Passwortschutz verfügt. Auf diese Weise können Angreifer einen Vollzugriff auf die Daten und gegebenenfalls sogar auf das Betriebssystem erhalten.
- In einer Bank wurden die Betriebssysteme zahlreicher Netzkomponenten aktualisiert. Danach blockierte die neue Version eines Paketfilters den Kommunikationsport einer selten genutzten, aber enorm wichtigen Funktion des kritischen datenbankbasierten Handelssystems. Dies hatte zur Folge, dass die Kunden der Bank nicht mehr auf die Anwendung zugreifen und wichtige Dienste nutzen konnten. Durch Regressforderungen erlitt die Bank einen finanziellen Schaden.

# G 2.27 Fehlende oder unzureichende Dokumentation

Verschiedene Formen der Dokumentation können betrachtet werden: die Produktbeschreibung, die Administrator- und Benutzerdokumentation zur Anwendung des Produktes und die Systemdokumentation.

Eine fehlende oder unzureichende Dokumentation der eingesetzten IT-Komponenten kann sowohl im Auswahl- und Entscheidungsprozess für ein Produkt, als auch bei einem Schadensfall im Wirkbetrieb erhebliche Auswirkungen haben.

Bei einer unzureichenden Dokumentation kann sich im Schadensfall, beispielsweise durch den Ausfall von Hardware bzw. Fehlfunktionen von Programmen, die Fehlerdiagnose und -behebung erheblich verzögern oder völlig undurchführbar sein.

Dies gilt auch für die Dokumentation von Leitungswegen und Verkabelungen innerhalb der Gebäude-Infrastruktur. Ist aufgrund unzureichender Dokumentation die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Dabei kann es zu längeren Ausfallzeiten (Eintritt eines Notfalls) oder unter Umständen sogar zu lebensbedrohenden Gefahren, zum Beispiel durch Stromschlag, kommen.

**Beispiele:**

- Wenn von einem Programm Arbeitsergebnisse in temporären Dateien zwischengespeichert werden, ohne dass dies ausreichend dokumentiert ist, kann dies dazu führen, dass die temporären Dateien nicht angemessen geschützt und vertrauliche Informationen offengelegt werden. Durch fehlenden Zugriffsschutz auf diese Dateien oder eine nicht korrekte physikalische Löschung der nur temporär genutzten Bereiche können Informationen Unbefugten zugänglich werden.
- Bei Installation eines neuen Softwareproduktes werden bestehende Konfigurationen abgeändert. Andere, bislang fehlerfrei laufende Programme, sind danach falsch parametrisiert und stürzen gegebenenfalls ab. Durch eine detaillierte Dokumentation der Veränderung bei der Installation von Software ließe sich der Fehler schnell lokalisieren und beheben.
- In einer größeren Behörde wurde die Verkabelung der IT durch eine externe Firma vorgenommen. Die Anfertigung einer Dokumentation war im Leistungsumfang nicht enthalten. Da nach Fertigstellung der Verkabelung mit der Firma kein Wartungsvertrag abgeschlossen wurde, verfügte die Behörde nicht über die notwendige Dokumentation. Erweiterungen des Netzes konnten nur mit erheblichen Verzögerungen vorgenommen werden (siehe auch G 2.12 *Unzureichende Dokumentation der Verkabelung*).
- In einer z/OS-Installation wurden jeden Abend automatisch Batch-Jobs zur Verarbeitung von Anwendungsdaten gestartet. Für die Verarbeitung war es wichtig, dass die Batch-Jobs in der richtigen Reihenfolge abliefen. Als eines Abends die Automation versagte, mussten die Jobs manuell gestartet werden. Aufgrund fehlender Dokumentation wurden die Batch-Jobs in der falschen Reihenfolge gestartet. Dies führte zu Abbrüchen in der Verarbeitung der Anwendungsdaten und zu Verzögerungen in der Produktion um mehrere Stunden.
- Fehlende Datenblätter von (flüchtigen) Halbleiterspeichern wie SRAM (Static Random Access Memory) und DRAM (Dynamic Random Access

Memory) können dazu führen, dass die Speicher nicht ordnungsgemäß gelöscht und damit vertrauliche Informationen bekannt werden können.

- In einem Unternehmen sollten USB-Sticks (nichtflüchtige Speicher) ausgemustert werden. Die Produktbeschreibungen waren nicht aufzufinden. Die USB-Sticks wurden daher mit dem vorhandenen Löschtool behandelt. Auf herstellerspezifische Besonderheiten konnte jedoch nicht eingegangen werden, so dass nicht alle Daten ordnungsgemäß und sicher gelöscht wurden.

# G 2.28 Verstöße gegen das Urheberrecht

Der Einsatz nicht-lizenzierter Software kann einen Verstoß gegen das Urheberrecht darstellen und sowohl zu zivil- als auch strafrechtlichen Konsequenzen führen.

Behörden und Unternehmen, in denen Raubkopien zum Einsatz kommen, können im Rahmen des Organisationsverschuldens, unabhängig von der Schuldform (Vorsatz oder Fahrlässigkeit) vom Urheberrechtseigentümer schadensersatzpflichtig gemacht werden.

**Beispiele:**

- In einem Unternehmen wurde eine große Anzahl Benutzeroberflächen eingesetzt, ohne dass die hierfür erforderlichen Lizenzen erworben wurden. Die Kosten für die erforderliche Nachlizenzierung sowie den Schadensersatz an den Urheberrechtseigentümer beliefen sich auf ein Vielfaches der Lizenzgebühren.
- In einem Unternehmen ist Software installiert, deren Lizenzschlüssel nur für bestimmte Versionen gültig ist. Wird nun eine neue Version dieser Software eingespielt, ohne dass die Lizenzbedingungen geprüft werden, kann dies die Funktionsfähigkeit der Software beeinträchtigen oder sogar zivil- oder strafrechtliche Konsequenzen haben.
- Die Installation von Software wurde in einer Firma nicht über einen unternehmenseinheitlichen Änderungsprozess freigegeben und gesteuert. Jede Abteilung installierte die von ihr benötigte Software selbstständig. Da niemand die Zahl der installierten Instanzen mit der Zahl der erworbenen Lizenzen abgeglichen hat, wurde die Anzahl der gekauften Lizenzen teilweise über-, teilweise unterschritten. Ersteres kann Regressforderungen sowie ein strafrechtliches Vorgehen des Herstellers der Software gegen das Unternehmen zur Folge haben. Letzteres führt dazu, dass vorhandene Ressourcen nicht vernünftig genutzt werden.

# G 2.29 Softwaretest mit Produktionsdaten

Vielfach ist zu beobachten, dass Softwaretests mit Produktionsdaten vollzogen werden. Als wesentliche Gründe werden hierfür angeführt, dass nur im direkten Vergleich mit vorhandenen Arbeitsergebnissen eine abschließende Beurteilung über die Funktion und Performance des Produktes möglich ist. Darüber hinaus sind mangelndes Sicherheitsbewusstsein, überzogenes Vertrauen in die zu testende Software und Unkenntnis über mögliche schädliche Auswirkungen ursächlich für diese Vorgehensweise.

Beim Test mit Produktionsdaten kann es zu folgenden Problemen kommen:

- Software wird mit Kopien von Produktionsdaten in isolierter Testumgebung getestet:
  Wenn neue Software mit nicht anonymisierten Daten getestet wird, erhalten evtl. nicht befugte Mitarbeiter, bzw. Dritte, die mit dem Softwaretest beauftragt worden sind, hierbei Einblick in Dateien mit evtl. vertraulichen Informationen.
- Software wird mit Produktionsdaten im Wirkbetrieb getestet:
  Fehlfunktionen von Software während des Testens können über den oben geschilderten Fall hinaus beispielsweise dazu führen, dass neben der Vertraulichkeit der Produktionsdaten auch deren Integrität und Verfügbarkeit beeinträchtigt werden.
  Aufgrund der Inkompatibilität unterschiedlicher Programme können Seiteneffekte auftreten, die bei anderen Systemkomponenten zu nachhaltigen Beeinträchtigungen führen können. Bei vernetzten Systemen kann das von Performanceverlusten bis hin zum Systemabsturz des Netzes reichen.
  Durch fehlerhaftes Verhalten der zu testenden Software oder Bedienfehler können Produktionsdaten ungewollt verändert werden. Möglicherweise wird diese Veränderung nicht festgestellt. Da Datenbestände, um unnötige Redundanz zu vermeiden, zunehmend durch unterschiedliche Programme gemeinsam genutzt werden, können sich diese Fehler auch auf andere IT-Anwendungen auswirken. Im Schadensfall ist nicht nur der Aufwand für die Rekonstruktion der Daten notwendig, darüber hinaus müssen bereits erstellte Arbeitsergebnisse auf ihre Integrität überprüft werden.

# G 2.30 Unzureichende Domänenplanung

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 2.31 Unzureichender Schutz des Windows NT Systems

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 2.32 Unzureichende Leitungskapazitäten

Bei der Planung von Netzen wird oft der Fehler begangen, die Kapazitätsauslegung ausschließlich anhand des aktuellen Bedarfs vorzunehmen. Dabei wird übersehen, dass die Kapazitätsanforderungen an Netze stetig steigen, z. B. wenn neue IT-Systeme in das Netz integriert werden, neue Dienste im Netz angeboten werden oder das übertragene Datenvolumen zunimmt.

Reicht die Kapazität eines Netzes nicht mehr aus, dann kann die Übertragungsrate sinken, die Zugriffszeiten können sich erhöhen und gegebenenfalls kann auch die Erreichbarkeit im Netz für die jeweiligen Benutzer stark eingeschränkt werden.

**Beispiel:**

In einem Gebäude werden zusätzliche PC-Arbeitsplätze geschaffen, indem Räume zu Großraumbüros umgewidmet werden. Der Anschluss der Endgeräte wird durch Switches im jeweiligen Büro und durch "fliegende" Verkabelung realisiert. Mit der Einführung neuerer System- und Anwendungssoftware, die stetig Updates aus dem Internet oder von Management-Servern der Institution lädt, kommt es zu gravierenden Störungen normaler Arbeitsabläufe, weil das Datenvolumen der Updates die vorhandene Leitungskapazität überfordert.

# G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 2.34 Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 2.35 Fehlende Protokollierung unter Windows 95

Der Inhalt dieser Gefährdung wurde in G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten* integriert und ist mit der Version 1999 entfallen.

# G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Die meisten Betriebssysteme bieten die Möglichkeit, die Benutzerumgebung individuell für jeden Benutzer einzuschränken. Wo dies nicht der Fall ist, können hierfür im Allgemeinen spezielle Sicherheitsprodukte eingesetzt werden. Dabei bestehen prinzipiell zwei Möglichkeiten:

- Bestimmte Funktionalitäten werden erlaubt, alle anderen sind verboten.
- Bestimmte Funktionalitäten werden verboten, alle anderen sind erlaubt.

In beiden Fällen besteht die Möglichkeit, den Benutzer derart einzuschränken, dass dieser wesentliche Funktionen nicht mehr ausführen kann oder dass sogar ein sinnvolles und effizientes Arbeiten mit dem IT-System nicht mehr möglich ist.

Eine weitere Form, die Benutzerumgebung einzuschränken, besteht in der Begrenzung des nutzbaren Speicherplatzes. Reicht der zur Verfügung stehende Speicherplatz nicht mehr aus, so können keine weiteren Informationen gespeichert werden. Je nach Art und Aufteilung des betroffenen IT-Systems können hiervon eine Vielzahl von Benutzern und Anwendungen betroffen sein. Wenn dabei auf eine Trennung zwischen Daten- und Systempartition verzichtet wurde, kann das gesamte IT-System ausfallen, weil beispielsweise kein Speicherplatz für Auslagerungen des Arbeitsspeichers ("Swap") mehr vorhanden ist.

**Beispiele:**

- In einer Firma hatte der Administrator den Benutzern durch enge Quotas nur sehr wenig Speicherplatz auf dem Mailserver zur Verfügung gestellt, um die Benutzer zu disziplinieren. Diese sollten angehalten werden, die Mails nicht in den Eingangspostfächern, sondern in den jeweiligen Arbeitsverzeichnissen zu speichern. Dadurch liefen die E-Mail-Postfächer allerdings schon nach wenigen Mails über und die Benutzer konnten keine weiteren E-Mails empfangen.
- In einer Behörde war festgelegt worden, dass bestimmte sicherheitsrelevante Informationen wie Anmeldeversuche ein Jahr lang protokolliert werden sollten. Da für die Protokoll-Daten aber zu wenig Platz auf dem Server vorhanden war, wurden diese immer automatisch nach einer Woche gelöscht. Als auffiel, dass geschäftsrelevante Daten manipuliert worden waren, konnte zwar eine Sicherheitslücke entdeckt werden, es ließ sich aber nicht mehr nachvollziehen, wie und durch wen diese ausgenutzt worden war.

# G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

Beim Einsatz von Kommunikationskarten innerhalb eines IT-Systems (Fax-, Modem- oder ISDN-Karten) ist für den Benutzer nicht immer offensichtlich, was außer seinen Nutz- und Protokollinformationen zusätzlich übertragen wird. Nach Aktivierung einer Kommunikationskarte ist es grundsätzlich möglich, dass diese, ohne Initiierung durch den Benutzer, Verbindungen zu einer nicht gewünschten Gegenstelle aufbaut oder, über dem Benutzer nicht bekannte Remote-Funktionalitäten, durch Dritte angesprochen wird.

**Beispiele:**

- Bei der erstmaligen Konfiguration einer Faxkarte wurde der Benutzer vom Installationsprogramm nach der Landesvorwahl von Schweden gefragt. Zu vermuten ist, dass der Kartenhersteller über den Einsatz seines Produkts, eventuell aus Gründen des Produkt-Marketings, informiert werden wollte.
- Eine große Anzahl von Modem-Karten unterstützt den ferngesteuerten Zugriff auf IT-Systeme. Zwar lassen sich diese Zugriffe über teilweise sogar auf den Karten integrierte Mechanismen (Callback-Option und Rufnummernauthentisierung) absichern, voreingestellt ist dies jedoch nicht. Ein so konfiguriertes IT-System lässt sich, über die Modemkarte, von außen vollständig manipulieren.

# G 2.38 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

Jede Datenbank-Standardsoftware stellt in der Regel eine Reihe von Sicherheitsmechanismen bereit, mittels derer die Daten vor unberechtigtem Zugriff oder Ähnlichem geschützt werden können. Sie sind jedoch nicht unbedingt automatisch aktiv, sondern müssen vom Datenbank-Administrator meistens manuell eingeschaltet werden. Wird davon kein Gebrauch gemacht, so kann weder die Vertraulichkeit noch die Integrität der Daten gewährleistet werden. In diesem Fall ist es dann meistens nicht möglich, solche Schutzverletzungen zu erkennen und zu protokollieren. Der Verlust bzw. die Manipulation von Daten bis hin zur Zerstörung der Datenbank selbst kann die Folge sein.

**Beispiel:**

Bei der Datenbank MS Access ist die Aktivierung des Passwortschutzes optional. Hierdurch kann es auf einfache Weise zu einem unberechtigten Zugang zum Datenbanksystem und damit auch zu einem unberechtigten Zugriff auf die dort gespeicherten Daten kommen. Eine Kontrolle der Datenbanknutzung ist in diesem Fall nicht möglich.

# G 2.39 Mangelhafte Konzeption eines DBMS

In der Konzeption eines Datenbank-Managementsystems (DBMS) werden die Anforderungen an Auswahl, Aufbau, Betrieb und eventuell Erweiterung des geplanten Systems festgelegt.

Die Auswahl und der Einsatz einer Datenbank-Standardsoftware erfordert sorgfältige Planung, Installation und Konfiguration des Datenbank-Managementsystems (DBMS), um einen störungsfreien Einsatz zu gewährleisten. Die Vielzahl möglicher Gefährdungen sollen durch die nachfolgenden Beispiele verdeutlicht werden.

**Auswahl einer ungeeigneten Datenbank-Standardsoftware**

- Es wird ein DBMS ausgewählt, welches in der geplanten Einsatzumgebung nicht lauffähig ist. Dies kann daraus resultieren, dass das DBMS an ein bestimmtes Betriebssystem gebunden ist oder die Mindestanforderungen an die Hardware nicht erfüllt werden.
- Das ausgewählte DBMS stellt ein Sicherheitsrisiko dar, weil die vom Hersteller zur Verfügung gestellten Sicherheitsmechanismen nicht ausreichen, um die geforderte Verfügbarkeit, Integrität und Vertraulichkeit der Daten zu gewährleisten.

**Fehlerhafte Installation bzw. Konfiguration der Datenbank-Standardsoftware**

Die empfohlenen Sicherheitsmaßnahmen werden fehlerhaft, unvollständig oder gar nicht durchgeführt.

**Beispiele:**

- Die Kontrolldateien eines Datenbanksystems werden nicht gespiegelt bzw. die gespiegelte Kontrolldatei wird nicht auf einer anderen Festplatte abgelegt. Ein Plattencrash führt dabei mit großer Wahrscheinlichkeit zur Zerstörung der Datenbank.
- Während der Installation wird der automatisch erzeugten Systemadministrator-Kennung ein triviales Passwort zugewiesen, das nachfolgend nicht abgeändert wird.
- Die physikalischeVerteilung der Daten ist unzureichend (falls das DBMS eine physikalische Verteilung vorsieht). Werden anwendungsspezifische Daten nicht physikalisch voneinander getrennt gespeichert, kann bereits der Ausfall einer einzigen Festplatte zu einem Komplettausfall aller Anwendungen führen.
- Durch falsche Parametereinstellungen kann der Zugriff auf bestimmte Daten verhindert werden.
- Durch eine falsche Ländereinstellung in einer Datenbank-Software kann die Darstellung von Umlauten unmöglich gemacht werden.

**Fehlerhafte Konzeption der Datenbank**

Im Datenbankkonzept werden neben den einzelnen Tabellen und ihren Spalten und Schlüsseln auch die Relationen der Tabellen untereinander dargestellt.

Einem Element einer Tabelle können kein, ein oder mehrere Elemente einer anderen Tabelle zugeordnet sein. Aus diesen Relationen ergeben sich Restriktionen, die bei Lösch-, Update- oder Einfüge-Operationen zu erfüllen sind, um die Datenbank-Integrität zu erhalten.

**Beispiel:**
- Jeder Einwohner muss einen Wohnort haben. Einwohner können mehrere Wohnorte besitzen. Sollte ein Einwohner sterben, so fallen auch alle zugeordneten Wohnorte weg. Mehrere Einwohner können sich einen Wohnort teilen. Wohnorte können leer stehen.

In der Datenbank wird eine solche Relation durch eine zusätzliche Tabelle dargestellt, die für jedes Element der Relation (im Beispiel Einwohner / Wohnort) als Verweise auf die Datensätze die Schlüssel der zugehörigen Datensätze der einzelnen Tabellen enthält. Wenn ein Datensatz in der Tabelle der Einwohner oder der Wohnorte gelöscht wurde, darf es auch in der Tabelle zur Zuordnungsrelation keinen Verweis mehr auf diesen Datensatz geben. Die Einhaltung solcher Bedingungen kann in der Datenbank selbst definert werden, durch Bedingungen oder automatisch ablaufende Prozeduren.

Aus dem Zusammenwirken dieser Konstrukte kann es zu kaskadierenden Datenbankoperationen kommen, die aber in verschiedenen DBMS durch unterschiedliche Einschränkungen begrenzt werden.

Fehlende Relationen zwischen einzelnen Tabellen können, wenn nicht die Anwendung diese Funktionalität nachbildet, zu einem Verlust der sogenannten referenziellen Datenbankintegrität führen.

**Beispiele:**
- Ein Wohnort wird ohne Prüfung gelöscht, ob diesem noch Einwohner zugeordnet sind.
- Werden Datenbanktrigger falsch eingesetzt, kann es zu Inkonsistenzen der Daten kommen, wenn die Anwendung dies nicht selbst berücksichtigt.
- Ein Einwohner verstirbt und wird daher aus der Datenbank gelöscht. Nachdem die Löschoperation durchgeführt ist, werden durch einen Delete-Trigger alle Datensätze in der zusätzlichen Tabelle gelöscht, die die verschiedenen Wohnorte des verstorbenen Einwohners beschreiben.
- Durch eine mangelhafte Konzeption des Einsatzes von Datenbanktriggern kann es zu einem Verlust der Datenintegrität oder unkontrollierten Datenmanipulationen kommen.

# G 2.40 Mangelhafte Konzeption des Datenbankzugriffs

Die Benutzer greifen über ein Datenbank-Managementsystem (DBMS) auf eine oder mehrere Datenbanken zu. Dieser Zugriff geschieht direkt oder aber von einer Anwendung aus. Um die Integrität einer Datenbank zu gewährleisten, müssen alle Datenbankzugriffe von einer zentralen Stelle aus kontrolliert werden. Bei mangelhafter Konzeption des Datenbankzugriffs kann es unter anderem zu folgenden Sicherheitsproblemen kommen:

**Benutzerberechtigungen**

- Ist der Berechtigungsumfang für die Benutzer zu restriktiv definiert, kann dies dazu führen, dass bestimmte Arbeiten von diesen nicht durchgeführt werden können.
- Ist der Berechtigungsumfang dagegen zu umfangreich, kann dies dazu führen, dass Daten unberechtigt manipuliert bzw. eingesehen werden können.
- Wird den Benutzern erlaubt, direkt auf die Datenbank zuzugreifen (im Gegensatz zum Zugriff aus einer Anwendung heraus), so besteht prinzipiell die Gefahr des Integritätsverlustes der Datenbank durch Datenmanipulationen, deren Auswirkungen die Benutzer nicht unbedingt abschätzen können.

**Hinweis:** Wie die eigentlichen Daten einer Datenbank werden auch die Eigenschaften der einzelnen Datenbankobjekte, wie z. B. Struktur, Indizes, Schlüssel einer Tabelle, wiederum in Tabellen gespeichert, auf die über SQL-Befehle zugegriffen werden kann.

- Werden Datenbankobjekte nicht explizit durch ein entsprechendes Berechtigungs- und Zugriffskonzept geschützt, so besteht die Gefahr, dass die Datenbankobjekte selbst manipuliert werden (Manipulation von Feldern einer Tabelle oder von Tabellen-Indizes etc.). Dies kann zu einer Vielzahl von Problemen bis hin zur Zerstörung der Datenbank führen.

**Hinweis:** Für die Vergabe von Zugriffsrechten entsteht durch den Einsatz von Data-Warehouse, Online Analytic Processing (OLAP)-Systemen und Query-Tools häufig ein Sicherheitskonflikt. Einerseits sollen möglichst viele Daten aus heterogenen Datenquellen für die Entscheidungsträger zur Auswertung herangezogen werden können, andererseits müssen sensible Daten vor unberechtigtem Zugriff geschützt werden. Die Herausforderung besteht darin, die Zugriffsrechte so zu gestalten, dass sie sowohl dem Datenschutz und den Anforderungen an die Vertraulichkeit sensibler Daten als auch den Analyseanforderungen gerecht werden.

**Remote-Zugriff**

- Wird die Datenbank in einem Netz zur Verfügung gestellt, können bei mangelnden Sicherheitsvorkehrungen im Bereich des Remote-Zugriffs auf die Datenbank sowohl Daten manipuliert als auch unberechtigt eingesehen werden (siehe hierzu auch G 5.64 *Manipulation an Daten oder Software bei Datenbanksystemen*).

**Datenbankabfragen**

- Ohne eine aufgabenspezifische Einschränkung der Zugriffsrechte für die verschiedenen Benutzergruppen kann es zum Verlust der Vertraulichkeit schutzbedürftiger Daten durch unautorisierten Zugriff kommen.
- Die Anfragen und Aufrufe von Benutzern oder Anwendungen an die Datenbank müssen einer gemeinsam vereinbarten Syntax oder einem nor-

mierten Sprachumfang folgen, der vom jeweils angesprochenen DBMS zur Verfügung gestellt wird (z. B. ANSI-SQL-99 für eine relationale Datenbank). Hält sich die aufrufende Seite nicht an diese Syntax, kann dies dazu führen, dass Datenbankanfragen vom DBMS nicht bearbeitet werden können und zurückgewiesen werden. Diese Gefährdung besteht insbesondere, wenn DBMS verschiedener Anbieter eingesetzt und von einer zentralen Anwendung angesprochen werden.
- Die Verwendung von nicht exakt formulierten Datenbankabfragen kann dazu führen, dass durch eine Änderung der Datenbankobjekte die Datenbankabfrage falsche oder unerwartete Ergebnisse liefert. Unter Umständen kann auch das gesamte Datenbanksystem durch sinnlose Anfragen so in Anspruch genommen werden, dass der eigentliche Zweck nicht mehr erfüllt werden kann.

**Beispiele:**
- Die Abfrage "SELECT * FROM Tabelle" liefert alle Attribute bzw. Felder eines Tupels bzw. Datensatzes. Die Reihenfolge der Felder wird dabei von der technischen Struktur der Tabelle vorgegeben. Wird nun ein Feld in der Tabelle hinzugefügt oder gelöscht, d. h. die technische Struktur der Tabelle wird verändert, so hat dies unter Umständen fatale Auswirkungen auf eine Anwendung, in der eine solche Datenbankabfrage benutzt wird.
- Es werden vorsätzlich viele weit gefasste Abfragen an die Datenbank gerichtet, um die Ansprechbarkeit der Datenbank zu verhindern (siehe G 5.65 *Verhinderung der Dienste eines Datenbanksystems*).

# G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern

Teilen sich mehrere Benutzer einer Datenbank den gleichen Arbeitsplatz, so besteht die Gefahr von ungewollten oder gezielten Datenmanipulationen, wenn der Wechsel zwischen den Benutzern nicht organisiert ist bzw. der Wechsel nicht ordnungsgemäß durchgeführt wird. Auch ist dann die Vertraulichkeit der Daten nicht mehr gewährleistet.

**Beispiel:**

Wird eine Anwendung, die auf eine Datenbank zugreift, vor einem Benutzerwechsel nicht ordnungsgemäß verlassen, so führen die unterschiedlichen Berechtigungsprofile der betroffenen Benutzer zu den oben genannten Gefährdungen. Auch wird dabei der Protokollmechanismus der Datenbank unterlaufen, da dieser die Datenmodifikationen und Aktivitäten der aktiven Benutzer-Kennung festhält. Diese Kennung stimmt aber in einem solchen Fall nicht mit dem tatsächlichen Benutzer überein. Dadurch können Datenmodifikationen nicht mehr eindeutig einem Benutzer zugeordnet werden.

# G 2.42 Komplexität der NDS

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 2.43 Migration von Novell Netware 3.x nach Novell Netware Version 4

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 2.44 Inkompatible aktive Netzkomponenten

Werden in einem Netz Kommunikationsverfahren eingesetzt, die nicht oder noch nicht vollständig standardisiert sind, kann dies zu Inkompatibilitäten zwischen den eingesetzten Netzkomponenten führen. Der Grund dafür liegt darin, dass manchmal Hersteller der Komponenten aufgrund fehlender oder nur teilweise vorhandener Standards gezwungen sind, proprietäre Implementierungen einzusetzen.

Inkompatibilitätsprobleme dieser Art können insbesondere dann entstehen, wenn bestehende Netze um aktive Netzkomponenten anderer Hersteller ergänzt werden oder wenn Netze mit Netzkomponenten unterschiedlicher Hersteller aufgebaut werden.

Werden aktive Netzkomponenten mit unterschiedlichen Implementierungen des selben Kommunikationsverfahrens gemeinsam in einem Netz betrieben, kann es zu einem Verlust der Verfügbarkeit einzelner Teilbereiche, zum Ausfall bestimmter Dienste oder sogar des gesamten Netzes kommen.

# G 2.45 Konzeptionelle Schwächen des Netzes

Die Planung des Auf- und Ausbaus eines Netzes ist ein kritischer Erfolgsfaktor für den Netzbetrieb. Insbesondere bei den immer kürzer werdenden Innovationszyklen in der IT können sich Netze, die auf Grund ihrer Konzeption neuen Erfordernissen nicht angepasst werden können, schnell zu einem Engpass entwickeln. Darüber hinaus können Fehler, die bei der Konzeption eines Netzes begangen werden, dazu führen, dass Vertraulichkeit und Integrität der übertragenen Informationen nicht mehr gewährleistet werden können:

- Abhängig von einer Anforderungsermittlung von Netzteilnehmern (z. B. Arbeitsgruppen) an die Vertraulichkeit der Daten und die Integrität des Netzes muss das Netz entsprechend konzipiert worden sein. Ansonsten können vertrauliche Daten einer Arbeitsgruppe von anderen, hierzu unbefugten Netzteilnehmern mitgelesen werden. Unter diesem Aspekt kann die Vertraulichkeit auch durch den Umzug von Arbeitsgruppenteilnehmern oder der ganzen Arbeitsgruppe verloren gehen, wenn es nicht möglich ist, im Netz neue vertrauliche Bereiche einzurichten bzw. zu ändern. Diese Gefährdung betrifft analog die Integrität des Netzes bzw. von Netzsegmenten.
- Werden neue Anwendungen mit einem höheren als zum Planungszeitpunkt berücksichtigten Durchsatz auf dem Netz betrieben, kann dies schnell zu einem Verlust der Verfügbarkeit des gesamten Netzes führen, wenn die Netzinfrastruktur in Folge konzeptioneller Schwächen nicht mehr ausreichend skaliert werden kann (Verlust der Verfügbarkeit durch Überlastung). Abhängig von der gewählten Segmentierung des Netzes kann der Verlust der Verfügbarkeit auch nur einzelne Segmente des Netzes betreffen.

**Beispiel:**

In den heute noch häufig vorzufindenden, bedarfsorientiert gewachsenen Netzen sind aus historischen Gründen vielfach Backbone-Segmente mit niedriger maximaler Bitübertragungsrate, wie z. B. Ethernet-Segmente mit geringer Bitübertragungsrate, vorhanden. Durch diese Beschränkung des Durchsatzes im Backbone-Bereich ist bei hoher zusätzlicher Last die Verfügbarkeit des gesamten Netzes betroffen.

# G 2.46 Überschreiten der zulässigen Kabellänge

Je nach Kabeltyp und Topologie sehen die betreffenden Standards maximale Kabellängen vor, um die Funktionsfähigkeit des Netzes im Sinne dieser Standards zu garantieren. Überhöhte Kabellängen verlängern die Signallaufzeiten über das für das betreffende Übertragungsverfahren vorgesehene Maß hinaus, so dass die Verfügbarkeit des jeweiligen Netzsegments oder die Kommunikationsbandbreite herabgesetzt wird.

Neben einer Verlängerung der Signallaufzeit erhöhen längere Kabel die Dämpfung. Bei Überschreitung der Kabellängen im Hinblick auf den betreffenden Standard kann die Dämpfung des Kabels so groß werden, dass die verschiedenen Signalpegel nicht mehr, wie im Standard festgelegt, voneinander unterschieden werden können. Die Kommunikation über die betreffenden Adern oder Glasfasern kann in diesem Fall nicht über die gesamte Länge sichergestellt werden.

# G 2.47 Ungesicherter Akten- und Datenträgertransport

Werden Dokumente, Datenträger oder Akten zwischen der Institution und anderen Stellen, zum Beispiel dem häuslichen Arbeitsplatz, transportiert, besteht die Gefahr, dass sie

- auf dem Transportweg verloren gehen,
- auf dem Transportweg entwendet werden,
- auf dem Transportweg gelesen oder manipuliert werden und
- an einen falschen Empfänger übergeben werden.

Insbesondere wenn es sich um Unikate handelt, können Zerstörung, Vertraulichkeitsverlust oder Manipulation größere Schäden verursachen.

# G 2.48 Ungeeignete Entsorgung der Datenträger und Dokumente

Wenn Datenträger oder Dokumente nicht geeignet entsorgt werden, können hieraus unter Umständen Informationen extrahiert werden, die Dritten nicht in die Hände fallen sollten.

**Beispiele:**
- Angreifer müssen nicht immer komplizierte technische Attacken austüfteln, um über Schwachstellen in IT-Systemen an Informationen zu gelangen. Viel einfacher und erfolgreicher kann die Informationsgewinnung aus der Mülltonne (Dumpster Diving) sein. Büromüll, wie beispielsweise Disketten, CD-ROMs, interne Telefonbücher oder auch die aktuellen Erfolgsbilanzen, ist im Allgemeinen nicht besonders schmutzig und kann sehr viele interessante und weiterverwertbare Informationen enthalten.
- CD-ROMs können zur Wiederverwertung an vielen Stellen abgegeben werden. Leider wird hierbei häufig nicht bedacht, dass auch CD-ROMs mit "alten" Datensicherungen oder anderen Dateien für Externe noch interessante Informationen enthalten können. Das Zerkratzen der Oberfläche reicht hier nicht, um Interessierte an der Auswertung von Informationen erfolgreich zu hindern.

Auch alte oder defekte IT-Systeme enthalten häufig eine Vielzahl von spannenden Informationen. So hat eine Test-Kaufreihe einer Computer-Zeitschrift ergeben, dass auf 90 % der gebraucht gekauften Festplatten noch die vollständigen Informationen der vorherigen Besitzer enthalten waren.

**Beispiele:**
- Zwei Wissenschaftler vom Massachusetts Institute of Technology haben untersucht, wie viele sensitive Daten über den Handel mit gebrauchten Computern und Computerkomponenten in die Hände Unbefugter gelangen. Ihre Untersuchung ergab, dass nur 10 % der IT-Komponenten so gesäubert worden waren, dass keine Daten rekonstruiert werden konnten. Die übrigen Platten enthielten unter anderem Pornographie, Liebesbriefe, Kreditkartennummern oder Patientendaten. Der "Hauptgewinn" war eine Festplatte, die zuvor offensichtlich in einem Geldautomaten eingebaut war, und auf der neben Kontonummern und Kontoständen auch ein Teil der verwendeten Software zu finden war.
- Der Käufer eines ausgemusterten Behördencomputers wandte sich an Datenschutzbeauftragte und Presse, nachdem er darauf die nur scheinbar gelöschten Daten eines Nachlassgerichtes rekonstruieren konnte.

Sind für Telearbeiter am häuslichen Arbeitsplatz keine geeigneten Möglichkeiten vorhanden, um Datenträger und Dokumente geeignet zu entsorgen, wandern diese erfahrungsgemäß meist in den Hausmüll. Auch dort, wo unterwegs gearbeitet wird, besteht die bedauerliche Neigung, Entwürfe und anderes "Unnützes" direkt in die nächsten Papierkörbe zu geben oder einfach liegen zu lassen, sei es im Hotel oder in der Bahn.

**Beispiel:**
- So wurden bereits aus Patientenakten von den Nachbarskindern Papierflugzeuge gebastelt. Diese waren von einem Telearbeiter als Altpapier zur Entsorgung vor die Haustür gestellt worden. Da die brisanten Papierflugzeuge anschließend überall in der Nachbarschaft zu finden waren, war dies bald als Nachricht über den schlechten Datenschutz einer Klinik in der Lokalpresse zu lesen.

# G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter

Telearbeiter sind am häuslichen Arbeitsplatz weitestgehend auf sich allein gestellt. Das bedeutet, dass sie sich besser mit der eingesetzten IT auskennen müssen als ihre Kollegen in der Institution, die meist kurzfristig auf IT-Systemspezialisten vor Ort zurückgreifen können. Ist der Telearbeiter nicht ausreichend im Umgang mit der IT geschult, kann dies bei Problemen zu erhöhten Ausfallzeiten führen, da ggf. ein IT-Betreuer aus der Institution zum häuslichen Arbeitsplatz des Telearbeiters fahren muss, um dort die Probleme zu beseitigen.

**Beispiel:**

Der Telearbeiter sollte in der Lage sein, selbstständig Sicherungskopien seiner Daten herzustellen. Wird dem Telearbeiter ein zusätzliches Speichermedium (z. B. Bandlaufwerk) zur Verfügung gestellt, so muss er in den Gebrauch eines solchen eingewiesen werden.

# G 2.50 Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter

Üblicherweise hat ein Telearbeiter keine festen Arbeitszeiten am häuslichen Arbeitsplatz. Lediglich feste Zeiten der Erreichbarkeit werden vereinbart. Bei alternierender Telearbeit sind seine Arbeitszeiten zwischen häuslichem Arbeitsplatz und dem innerbetrieblichen Arbeitsplatz verteilt. Ergibt sich kurzfristig das Problem, dass Informationen vom Telearbeiter eingeholt oder Informationen an den Telearbeiter übergeben werden müssen, kann es aufgrund der schwierigen Erreichbarkeit zu Verzögerungen kommen. Selbst eine Übermittlung der Informationen über E-Mail verkürzt nicht notwendigerweise die Reaktionszeit, da nicht sichergestellt werden kann, dass der Telearbeiter die E-Mail zeitnah liest.

# G 2.51 Mangelhafte Einbindung des Telearbeiters in den Informationsfluss

Da Telearbeiter nicht täglich in der Institution sind, sondern überwiegend zu Hause arbeiten, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit Vorgesetzten und Arbeitskollegen teilzuhaben. Es besteht die Gefahr, dass sie vom betrieblichen Geschehen abgeschnitten werden und sich dadurch auch die Identifizierung mit der Institution verringert.

Darüber hinaus ist nicht auszuschließen, dass durch einen mangelhaften Informationsfluss für Informationssicherheit notwendige Informationen nicht ausreichend oder nicht rechtzeitig den Telearbeiter erreichen. Beispielsweise kann die kurzfristige Weitergabe von Computer-Viren-Meldungen erschwert sein.

# G 2.52 Erhöhte Reaktionszeiten bei IT-Systemausfall

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen.

# G 2.53 Unzureichende Vertretungsregelungen für Telearbeit

Die Aufgaben des Telearbeiters sind in der Regel so konzipiert, dass er weitestgehend selbständig arbeiten kann. Dies birgt die Gefahr in sich, dass es im Krankheitsfall schwierig ist, eine entsprechende Vertretung für den Telearbeiter bereitzustellen. Insbesondere kann es zu Problemen führen, die erforderlichen Unterlagen oder die Daten aus dem Telearbeitsrechner für den Vertreter bereitzustellen, wenn keine Zutrittsmöglichkeiten zum häuslichen Arbeitsplatz des Telearbeiters bestehen.

# G 2.54 Vertraulichkeitsverlust durch Restinformationen

Bei elektronischer Datenübermittlung oder Datenträgerweitergabe passiert es immer wieder, dass dabei auch Informationen weitergegeben werden, die die Institution nicht verlassen sollten. Als mögliche Ursachen für die unbeabsichtigte Weitergabe von Informationen lassen sich folgende Beispiele anführen:

- Eine Datei enthält Textpassagen, die als "versteckt" oder "verborgen" formatiert sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind.
- Dateien, die mit Standardsoftware wie Textverarbeitungsprogrammen oder Tabellenkalkulationen erstellt worden sind, können Zusatzinformationen über Verzeichnisstrukturen, Versionsstände, Bearbeiter, Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten. Besonders hervorzuheben sind in diesem Zusammenhang Funktionen, die mehreren Bearbeitern das gemeinsame Bearbeiten eines Dokuments erlauben. Solche Funktionen löschen Textpassagen, die ein Bearbeiter löscht oder überschreibt, nicht wirklich aus dem Dokument, sondern markieren diese nur als gelöscht und erlauben es späteren Bearbeitern, Änderungen ganz oder teilweise rückgängig zu machen. Praktisch alle aktuellen Office-Suites (beispielsweise Microsoft Office und OpenOffice) bieten diese Möglichkeit. Werden die Daten solcher Änderungen nicht vor der Weitergabe entfernt, so erhält der Empfänger neben dem tatsächlichen Dokument unter Umständen eine große Menge weiterer Informationen.
- Praktisch alle aktuellen Office-Suites besitzen die Möglichkeit der Schnellspeicherung von erstellten Dokumenten. Dies führt dazu, dass nur die Änderungen an einem Dokument gespeichert werden. Dieser Vorgang nimmt vergleichsweise weniger Zeit in Anspruch als ein vollständiger Speichervorgang, bei dem die Office-Suite das vollständige überarbeitete Dokument speichert. Ein vollständiger Speichervorgang erfordert weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil ist jedoch, dass bei einer Schnellspeicherung die Datei unter Umständen Textfragmente enthalten kann, die der Verfasser nicht weitergeben möchte.
- Eine weitere Möglichkeit, wie Informationen weitergegeben werden können, die nicht für Externe bestimmt sind, stellen Funktionen dar, die es beispielsweise erlauben, in ein Textdokument oder eine Präsentation eine Tabelle aus einem Tabellenkalkulationsdokument so einzubetten, dass die Tabelle direkt im Textdokument bearbeitet werden kann. Wird ein solches Textdokument weitergegeben, so können unter Umständen sehr viel mehr Informationen aus dem Tabellenkalkulationsdokument übertragen werden, als im Textdokument sichtbar sind.
- Auf z/OS-Systemen werden gelöschte Member nicht sofort in der Bibliothek (*PDS - Partitioned Dataset*) überschrieben. Lediglich der Eintrag des Members im Verzeichnis (*Directory*) des *PDS* wird gelöscht. Erst wenn im *PDS* freier Speicherplatz benötigt wird, werden die Informationen des alten Members überschrieben. Noch nicht überschriebene Daten lassen sich mit Hilfsprogrammen auslesen.
- Werden in z/OS-Systemen Dateien auf einer Festplatte gelöscht, so wird die Datei im *Volume Table of Content (VTOC)* als gelöscht gekennzeichnet, die Datei selbst auf der Festplatte jedoch nicht gelöscht. Die Datei wird erst überschrieben, wenn neue Daten auf der Festplatte gespeichert werden sollen und kein freier Platz verfügbar ist. Gelingt es, die Speicherstelle der Datei aus dem *VTOC* auszulesen, so ist es möglich, die Datei

mit speziellen Programmen zu editieren und wieder herzustellen. Dies gilt ebenso für Bänder, die zwar als Leer-Bänder gekennzeichnet, aber noch nicht überschrieben sind.

**Restinformationen auf Datenträgern**

Bei den meisten Dateisystemen werden Dateien, die vom Benutzer über einen Löschbefehl gelöscht werden, nicht wirklich in dem Sinn gelöscht, dass die Information anschließend nicht mehr vorhanden ist. Normalerweise werden lediglich die Verweise auf die Datei aus den Verwaltungsinformationen des Dateisystems (etwa aus der Dateizuordnungstabelle (*File Allocation Table*) beim FAT-Dateisystem) gelöscht und die zu der Datei gehörenden Blöcke als "frei" markiert. Der tatsächliche Inhalt der Blöcke auf dem Datenträger bleibt jedoch erhalten und kann mit entsprechenden Werkzeugen rekonstruiert werden.

Wenn Datenträger an Dritte weitergegeben werden, beispielsweise

- wenn ein Rechner ausinventarisiert wurde und verkauft wird,
- wenn ein defektes Gerät zur Reparatur gegeben oder im Rahmen der Garantie ausgetauscht wird oder
- wenn ein Datenträger im Rahmen des Datenträgeraustauschs an einen Geschäftspartner weitergegeben wird

können auf diese Weise sensitive Informationen nach außen gelangen.

**Beispiele:**

- Die Forscher Simson Garfinkel und Abhi Shelat vom MIT kauften zwischen 2000 und 2002 bei verschiedenen Händlern über das Online-Auktionshaus eBay eine größere Anzahl gebrauchter Festplatten und untersuchten diese auf enthaltene Restinformationen. Sie fanden eine erschreckende Menge an Daten, beispielsweise

  - interne Vermerke von Unternehmen, bei denen es um Personalsachen ging,
  - eine große Anzahl von Kreditkartennummern,
  - medizinische Informationen,
  - E-Mails

  und vieles mehr. Ihre Ergebnisse veröffentlichten sie in einem Journal der IEEE.
- Ein Benutzer verwendete einen alternativen Editor und entdeckte per Zufall, dass eine kurz vor der Veröffentlichung stehende Datei diverse URLs enthielt, inklusive Benutzername und Passwort für einen WWW-Server.
- Eine Behörde hatte mit dem Programm Microsoft Powerpoint erstellte Präsentationen in Dateiform an Externe weitergegeben. Später stellte sich heraus, dass neben den Präsentationen auch Informationen über die Rechnerumgebung des Benutzers mitgeliefert worden waren, wie etwa darüber, welche Newsgruppen ein Benutzer abonniert hat und welche News er schon gelesen hat.
- Zwei Verkäufer konkurrierender Firmen tauschten ihre Präsentationen aus, die sie bei einer Veranstaltung gehalten hatten. Eines der Powerpoint-Dokumente enthielt eine kleine Tabelle mit Endkunden-Preisen für die Produkte der einen Firma. Beim Öffnen der Präsentation entdeckte der Empfänger, dass diese kleine Tabelle Teil eines sehr umfangreichen Tabellenkalkulationsdokuments war, das in die Präsentation eingebettet worden war, und das die gesamte Preiskalkulation des Konkurrenzunternehmens enthielt.

# G 2.55 Ungeordnete Groupware-Nutzung

Wenn die Nutzung von Groupware-Systemen nicht ausreichend geregelt ist, besteht die Gefahr, dass sensitive Daten Unbefugten zur Kenntnis gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

**Beispiele:**

- Eine fehlerhafte Adressierung von E-Mails kann dazu führen, dass E-Mails an unautorisierte Empfänger übersandt werden.
  Werden Verteilerlisten nicht gepflegt, können E-Mails Empfängern zugestellt werden, die von der Versendung hätten ausgeschlossen sein müssen.
- Fehlende oder mangelhafte organisatorische Regelungen beim Empfänger können zur Folge haben, dass eine empfangene E-Mail erst verspätet bearbeitet wird.
- Fehlende oder mangelhafte organisatorische Regelungen beim Absender können zur Folge haben, dass ein terminlich zugesichertes Absenden der Daten nicht eingehalten werden kann.
- Werden beim Datenaustausch über Groupware-Anwendungen die Daten nicht gut genug beschrieben, so ist für die anderen Benutzer oft nicht nachvollziehbar, wer diese eingestellt oder übersandt hat, welche Informationen sie enthalten, ob sie noch aktuell sind oder welchem Zweck sie dienen.
- Ein Mitarbeiter einer Bundesbehörde hat alle E-Mails von seinem dienstlichen Postfach an sein privates E-Mail-Postfach weitergeleitet. Der private PC dieses Mitarbeiters wurde von einer Schadsoftware kompromittiert und es kam zum Datenabfluss aller dienstlichen Daten im privaten Postfach, darunter vertrauliche Vorgänge und Zugriffsdaten. Diese Informationen wurden für weitere Angriffe auf dienstliche Systeme der Behörde genutzt.

# G 2.56 Mangelhafte Beschreibung von Dateien

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 2.57 Nicht ausreichende Speichermedien für den Notfall

Wenn Daten nach ihrer Zerstörung wiederhergestellt werden müssen, ist es vielen Fällen notwendig, die gesicherten Daten zunächst auf getrennten Speichermedien wiedereinzuspielen. Dies ist insbesondere bei komplexeren Datenstrukturen wie z. B. bei Datenbanken notwendig, da die Wiederherstellung nicht immer reibungslos und fehlerfrei funktioniert. Wird die hierfür benötigte Speicherkapazität nicht für den Notfall vorgehalten, kann es durch übereiltes Handeln während des Notfalls zu weiteren Datenverlusten kommen.

**Beispiel:**

In einem Unternehmen mit einer großer Datenbank-Applikation wurde die Datenbank als inkonsistent vom Datenbankmanagementsystem (DBMS) gemeldet. Daraufhin nahm das Systemmanagement die Datenbank außer Betrieb und restaurierte den letzten gesicherten Datenbestand im Produktionssystem. Von der scheinbar korrupten Datenbank wurden nur Log- und Konfigurationsdateien vorher gesichert. Durch diese Aktion gingen alle Datenänderungen seit der letzten Sicherung verloren, da aufgrund eines bis dahin unbekannten Fehlers im DBMS das Nachfahren der Änderungen nicht möglich war. Die Analyse der Log- und Konfigurationsdateien ergab dann, dass die Datenbank in Wirklichkeit gar nicht inkonsistent gewesen war. Hätte ausreichend Plattenplatz zur Verfügung gestanden, um die Rekonstruktion parallel durchzuführen, wäre das alte produktive System ohne Datenverlust nach Erkennung und Behebung der nur scheinbaren Inkonsistenz wieder einsatzbereit gewesen.

# G 2.58 Novell Netware und die Datumsumstellung im Jahr 2000

Diese Gefährdung ist mit der Version November 2004 entfallen.

# G 2.59 Betreiben von nicht angemeldeten Komponenten

In der Regel sollten alle Komponenten eines Netzes der Systemadministration bekannt sein. Es muss auf organisatorischer Ebene gewährleistet sein, dass neue Komponenten bei der Systemadministration angemeldet und freigegebenen werden, z. B. durch eine automatische Meldung der Beschaffungsstelle oder einen entsprechenden Antrag der die Komponenten betreibenden Organisationseinheit.

Nicht angemeldete Komponenten stellen ein Sicherheitsrisiko dar, da sie nicht in organisatorische innerbetriebliche Abläufe und Kontrollen eingebunden sind. Dies kann einerseits zu Gefahren für die Benutzer der nicht angemeldeten Komponenten führen (z. B. Datenverlust, da das System nicht in die Datensicherung eingebunden ist), aber auch zur Gefährdung anderer Netzkomponenten, z. B. können durch nicht erfasste Zugangspunkte zum Netz Schwachstellen entstehen, wenn diese schlecht oder gar nicht gegen unbefugten Zugriff abgesichert sind. Da eine solche Komponente nicht der Kontrolle des Netzmanagements und/oder des Systemmanagements unterliegt, können insbesondere Fehlkonfigurationen des lokalen Systems zu einem Sicherheitsloch führen.

**Beispiel:**

Der Administrator wartet über das Systemmanagementsystem die Passwörter (Community Names) für das verwendete Netzmanagementsystem, welches auf SNMP basiert. Eine Arbeitsgruppe beschließt den Kauf eines neuen Netz-PCs, vergisst diesen jedoch der zentralen Administration zu melden. Die Installationseinstellung für das Passwort (Community Name) des lokalen SNMP-Dämons lautet "public". Dieses Passwort ist wohl bekannt. Angreifer können nun einen SNMP-basierten Angriff starten, da sie vollen Zugriff auf die SNMP-Daten besitzen. Der so kompromittierte PC kann als Ausgangspunkt für weitere Angriffe auf das interne Netz dienen. So könnten dort z. B. Passwort-Sniffer installiert werden.

# G 2.60 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement

Werden für die Bereiche Netzmanagement und/oder Systemmanagement keine organisationsübergreifenden Managementstrategien festgelegt, kann es insbesondere in mittleren und großen Netzen mit mehreren Managementdomänen durch Fehlkoordination der einzelnen Subdomänen zu schwerwiegenden Problemen durch Fehlkonfiguration kommen, die bis hin zu völligem Systemzusammenbruch auf Netzebene führen können.

Aus diesem Grund ist die Festlegung und Durchsetzung einer Managementstrategie zwingend erforderlich. Im folgenden werden einige Beispiele für Probleme durch eine fehlende oder unzureichende Strategie für das Netz- und Systemmanagement gegeben.

**Fehlende Bedarfsanalyse vor Festlegung der Managementstrategie**

Um eine Netz- und/oder Systemmanagementstrategie festlegen zu können, ist eine vorangehende Bedarfsanalyse durchzuführen. Ohne die Feststellung des Managementbedarfs (etwa: Welche verwaltbaren Netzkoppelelemente existieren? Wie dynamisch ist der zu verwaltende Softwarebestand?) können Anforderungen an die Managementstrategie nicht formuliert werden. Da die Managementstrategie zudem Einfluss auf das zu beschaffende Softwareprodukt hat, kann dies zu Fehlentscheidungen führen.

Wird dann z. B. ein Managementprodukt eingeführt, das einen zu geringen Funktionsumfang besitzt, so kann diese Funktionslücke zusätzlich zu einem Sicherheitsproblem werden, da die nötige Funktion "von Hand" bereitgestellt werden muss. In größeren Systemen kann dies dann leicht zu Fehlkonfigurationen führen.

**Beschaffung von nicht managebaren Komponenten**

Wird ein Rechnerverbund mit Hilfe eines Netz- und/oder eines Systemmanagementsystems verwaltet, so ist bei der Beschaffung neuer Komponenten darauf zu achten, dass sie in das jeweilige Managementsystem integrierbar sind, damit sie in das Management einbezogen werden können. Ist dies nicht der Fall, so fällt mindestens zusätzlicher Verwaltungsaufwand an, da auch auf den nicht mit dem Managementsystem verwalteten Komponenten die festgelegte Managementstrategie durchgesetzt werden muss. Da jedoch diese Komponenten insbesondere nicht in die automatisierten Verwaltungsabläufe des Managementsystems integriert sind, kann es hier zu Fehlkonfigurationen kommen. Dies birgt durch nicht abgestimmte Konfigurationen ein Sicherheitsrisiko.

**Nicht koordiniertes Managen von benachbarten Bereichen (Communities, Domänen)**

Existieren in einem durch ein Managementsystem verwalteten Rechnernetz mehrere Verwaltungsbereiche, die jeweils von einem eigenen Systemmanager betreut werden, so sind deren Kompetenzen durch die Managementstrategie eindeutig festzulegen. Ist dies nicht der Fall, kann es durch unkoordiniertes Management einzelner Komponenten zu Sicherheitsproblemen kommen.

Werden z. B. einerseits einzelne Komponenten wie Netzkoppelelemente fälschlicherweise von zwei Verwaltungsbereichen verwaltet (dies kann etwa geschehen, wenn keine unterschiedlichen SNMP-"Passwörter" (Community

Strings) verwendet werden), so führt das unkoordinierte Einstellen von Konfigurationsparametern unter Umständen zu Sicherheitslücken.

Werden andererseits Komponenten (etwa Drucker) gemeinsam von zwei Verwaltungsbereichen genutzt und wurde z. B. die Vertrauensstellung des jeweils anderen Verwaltungsbereiches (z. B. Windows NT Netzwerkfreigaben) nicht korrekt eingerichtet, so kann dies unbeabsichtigt zu Sicherheitsproblemen führen, wenn nun auch unberechtigten Dritten der Zugriff gestattet wird.

**Nicht integrierte Verwaltungssoftware**

Beim Verwalten von mittleren und großen Systemen kann es vorkommen, dass nach Einführung des Managementsystems neue Komponenten in das System integriert werden sollen, deren Verwaltung Funktionen erfordern, die das eingesetzte Managementsystem nicht unterstützt. Dies gilt insbesondere für den Bereich Applikationsmanagement. Wird zur Verwaltung der neuen Komponente nun eine Verwaltungssoftware eingesetzt, die nicht in das eingesetzte Managementsystem integriert werden kann (z. B. über eine Programmierschnittstelle, oder durch den Einsatz von so genannten Gateways), so ist ein koordiniertes Einbinden in das Managementsystem nicht möglich. Dadurch unterliegt die neue Komponente jedoch nicht dem "automatisierten" Management, was ein Verwalten "von Hand" nötig macht. Die festgelegte Managementstrategie muss nun für zwei Systeme umgesetzt werden, dies kann jedoch zu Fehlkonfigurationen führen, die Sicherheitslücken bedingen können.

# G 2.61 Unberechtigte Sammlung personenbezogener Daten

Beim Einsatz von Managementsystemen fallen im Rahmen des normalen Ablaufes auch viele Protokolldaten an, die in der Regel automatisch erzeugt und ausgewertet werden. Dies trifft im besonderen Maße auf die Bereiche der Netz- und Systemüberwachung zu. Ohne ausführliche Protokollierung der Systemaktivitäten ist es z. B. auch nicht möglich, Sicherheitsverletzungen aufzudecken. Eine Anforderung im Rahmen der Überwachung ist jedoch auch die eindeutige Zuordnung bestimmter Zugriffe zu Benutzern. Damit müssen die überwachten Benutzeraktivitäten aber personenbezogen protokolliert werden. In der Regel wird durch die Managementstrategie organisationsübergreifend und im Einvernehmen mit dem Datenschutzbeauftragten festgelegt, welche Benutzeraktivitäten aus Sicherheitsgründen überwacht werden sollen. Hierüber sind die betroffenen Benutzer entsprechend zu informieren. Die Einhaltung der durch die Managementstrategie festgelegten Vorgaben ist jedoch im Rahmen der Systemrevision zu überprüfen. Es ist zudem möglich, dass das Managementsystem im Rahmen einer regulären Funktion temporäre Protokolldateien erstellt, die z. B. im wenig geschützten Bereich für temporäre Dateien abgelegt werden. Die Protokolldateien sind dann potentiell zumindest für die Zeit ihrer Existenz zugreifbar und können zudem Benutzerinformationen enthalten.

# G 2.62 Ungeeigneter Umgang mit Sicherheitsvorfällen

In der Praxis kann nie ausgeschlossen werden, dass Sicherheitsvorfälle auftreten. Dies gilt auch dann, wenn eine Vielzahl von Sicherheitsmaßnahmen umgesetzt ist. Wird auf akute Sicherheitsvorfälle nicht angemessen reagiert, so können sich daraus unter Umständen große Schäden bis hin zu Katastrophen entwickeln.

Beispiele dafür sind:

- Es treten zunächst sporadisch, dann massenhaft neue Computer-Viren mit Schadfunktionen auf. Erfolgt keine rechtzeitige Reaktion, können unter Umständen ganze Organisationseinheiten arbeitsunfähig werden.
- Auf einem Webserver finden sich unerklärlich veränderte Inhalte. Wird dies nicht als Hinweis auf mögliche Hacker-Attacken weiterverfolgt, können weitere Angriffe auf den Server unter Umständen auch zu großem Imageverlust führen.
- In den Protokolldateien einer Firewall finden sich auffällige Einträge. Wird nicht zeitnah untersucht, ob dies Anzeichen für einen Hacking-Versuch sind, können Angreifer die Firewall mit einem erfolgreichen Angriff unbemerkt überwinden und in das interne Netz der Institution eindringen.
- Es werden Sicherheitslücken in den verwendeten IT-Systemen bekannt. Werden diese Informationen nicht rechtzeitig beschafft und notwendige Gegenmaßnahmen nicht zügig umgesetzt, so besteht die Gefahr, dass die Sicherheitslücken von Angreifern ausgenutzt werden.
- Es ergeben sich Hinweise auf manipulierte Unternehmensdaten. Wird dies nicht zum Anlass genommen, den Manipulationen nachzugehen, so können auch unerkannte Manipulationen schwere Folgeschäden nach sich ziehen, wie zum Beispiel fehlerhafte Lagerbestände, falsche Buchhaltung oder unkontrolliert abgeflossene Finanzmittel.
- Werden die Hinweise auf Kompromittierung von vertraulichen Unternehmensdaten nicht weiterverfolgt, können weitere vertrauliche Daten abfließen.

Diese Beispiele verdeutlichen, dass Sicherheitsvorfälle frühzeitig erkannt und die zuständigen Stellen schnell benachrichtigt werden müssen. Eine zügige Reaktion und eine Unterrichtung der potentiell Betroffenen zur Schadensminimierung oder -prävention ist hierbei extrem wichtig.

Wenn für die Behandlung von Sicherheitsvorfällen keine geeignete Vorgehensweise vorgegeben ist, können in der Eile und unter Stress falsche Entscheidungen getroffen werden, die unter anderem dazu führen können,

- dass Pressevertreter falsche Auskünfte erhalten,
- dass betroffene Systeme bzw. Komponenten nicht der Situation angemessen behandelt werden und zu früh oder zu spät abgeschaltet werden,
- dass Dritte durch die eigenen Systeme geschädigt werden können,
- dass keinerlei Ausweich- oder Wiederherstellungsmaßnahmen vorgesehen sind, wie z. B. der Austausch kompromittierter Komponenten oder Wiederherstellung von Daten.

# G 2.63 Ungeordnete Faxnutzung

Bei ungeordneter Nutzung von Faxgeräten oder Faxservern besteht die Gefahr, dass sensitive Daten Unbefugten zur Kenntnis gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

**Beispiele:**

- Eine fehlerhafte Adressierung kann dazu führen, dass ein Fax an einen unautorisierten Empfänger übersandt wird. Werden Adressbücher und Verteillisten nicht gepflegt, können Faxe Empfängern zugestellt werden, die von der Versendung hätten ausgeschlossen sein müssen.
- Eine fehlerhafte Administration eines Faxservers kann dazu führen, dass eingehende Faxe an Mitarbeiter zugestellt werden, die von dem Inhalt keine Kenntnis erlangen sollen.
- Fehlende oder mangelhafte organisatorische Regelungen beim Empfänger können zur Folge haben, dass ein empfangenes Fax erst verspätet bearbeitet wird.
- Fehlende oder mangelhafte organisatorische Regelungen beim Absender können zur Folge haben, dass ein terminlich zugesichertes Absenden einer Nachricht per Fax nicht eingehalten werden kann.
- Fehlende Sensibilisierung der Benutzer bei der Verwendung von Faxservern kann dazu führen, dass versehentlich ein Entwurf versandt wird, der so die Organisation nicht verlassen sollte.

# G 2.64 Fehlende Regelungen für das RAS-System

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in G 2.129 *Fehlende oder unzureichende Regelungen zum VPN-Einsatz* integriert.

# G 2.65 Komplexität der SAMBA-Konfiguration

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen. Das Thema SAMBA wird in dem Baustein B 5.17 *Samba* weitergeführt.

# G 2.66 Unzureichendes Sicherheitsmanagement

Die Vielzahl der Methoden und Vorgehensweisen, wie Informationen in Geschäftsprozessen behandelt, verarbeitet und gespeichert werden, kann schnell dazu führen, dass der Schutzbedarf geschäftskritischer Informationen falsch eingeschätzt wird und diese daher unzureichend geschützt werden. Ein organisiertes Vorgehen bei der Planung, Durchführung und Kontrolle des Sicherheitsprozesses ist daher zwingend erforderlich. Die Erfahrung zeigt, dass es nicht genügt, lediglich die Umsetzung von Sicherheitsmaßnahmen anzuordnen, da die einzelnen Betroffenen, insbesondere die IT-Benutzer, dadurch häufig aufgrund fehlender Fachkenntnisse und unzureichender zeitlicher Ressourcen überfordert sind. In der Konsequenz wird es häufig unterlassen, überhaupt Sicherheitsmaßnahmen umzusetzen, so dass kein befriedigender Sicherheitszustand erreicht wird. Selbst wenn ein angemessenes Sicherheitsniveau einmal erreicht wurde, muss der Sicherheitsprozess ständig angepasst und verbessert werden, um ihn dauerhaft im laufenden Betrieb aufrechtzuerhalten.

Ein unzureichendes Sicherheitsmanagement ist häufig Symptom einer mangelhaften Gesamtorganisation des Sicherheitsprozesses. Beispiele für konkrete Gefährdungen, die aus einem unzureichenden Sicherheitsmanagement resultieren, sind:

- *Fehlende persönliche Verantwortung:* Wird in einer Institution kein Sicherheitsmanagement-Team eingerichtet bzw. kein IT-Sicherheitsbeauftragter ernannt und die persönliche Verantwortung für die Umsetzung von Einzelmaßnahmen nicht eindeutig festgelegt, so ist es wahrscheinlich, dass viele Mitarbeiter ihre Verantwortung für die Informationssicherheit durch Verweis auf übergeordnete Hierarchie-Ebenen ablehnen. Als Folge werden Sicherheitsmaßnahmen nicht umgesetzt, da diese zunächst fast immer einen Mehraufwand im gewohnten Arbeitsablauf darstellen.
- *Mangelnde Unterstützung durch die Leitungsebene:* IT-Sicherheitsbeauftragte entstammen in der Regel nicht der Ebene der Behörden- bzw. Unternehmensleitung. Werden die Sicherheitsverantwortlichen nicht uneingeschränkt durch die Leitungsebene unterstützt, kann es schwierig werden, die notwendigen Maßnahmen auch von Personen, die in der Linienstruktur über ihnen stehen, wirksam einzufordern. In diesem Fall ist der Sicherheitsprozess nicht vollständig durchführbar.
- *Unzureichende strategische und konzeptionelle Vorgaben:* In vielen Institutionen wird zwar ein Sicherheitskonzept erstellt, dessen Inhalt dann aber häufig nur wenigen Insidern bekannt ist. Dies führt dazu, dass die Vorgaben an Stellen, an denen organisatorischer Aufwand zu betreiben wäre, bewusst oder unbewusst nicht eingehalten werden. Sofern das Sicherheitskonzept strategische Zielsetzungen enthält, werden diese vielfach als bloße Sammlung von Absichtserklärungen betrachtet und keine ausreichenden Ressourcen für deren Umsetzung zur Verfügung gestellt. Vielfach wird fälschlicherweise davon ausgegangen, dass in einer automatisierten Umgebung Sicherheit automatisch produziert werde. Schadensfälle in der eigenen oder in ähnlich strukturierten Institutionen sind bisweilen Auslöser für mehr oder minder heftigen Aktionismus, bei dem häufig bestenfalls Teilaspekte verbessert werden.
- *Unzureichende oder fehlgeleitete Investitionen:* Die Leitungsebene einer Institution muss durch regelmäßige und mit klaren Priorisierungen versehene Sicherheitsberichte über den Sicherheitszustand der Geschäftsprozesse, IT-Systeme und Anwendungen und über vorhandene Mängel un-

terrichtet werden. Ohne ausreichende Informationen geht die Leitungsebene von falschen Voraussetzungen aus. Dann ist es wahrscheinlich, dass nicht genügend Ressourcen für den Sicherheitsprozess bereitgestellt oder diese nicht sachgerecht eingesetzt werden. In letzterem Fall kann es dazu kommen, dass einem übertrieben hohen Sicherheitsniveau in einem Teilbereich schwerwiegende Mängel in einem anderen gegenüberstehen. Häufig ist auch zu beobachten, dass teure technische Sicherungssysteme falsch eingesetzt werden und somit unwirksam sind oder sogar selbst zur Gefahrenquelle werden.

- *Unzureichende Durchsetzbarkeit von Sicherheitsmaßnahmen:* Zur Erreichung eines durchgehenden und angemessenen Sicherheitsniveaus ist es erforderlich, dass unterschiedliche Zuständigkeitsbereiche innerhalb einer Institution miteinander kooperieren. Fehlende strategische Leitaussagen und unklare Zielsetzungen führen mitunter zu unterschiedlicher Interpretation der Bedeutung der Informationssicherheit. Dies kann zur Konsequenz haben, dass die notwendige Kooperation wegen vermeintlich fehlender Notwendigkeit oder ungenügender Priorisierung der Aufgabe "Informationssicherheit" letztlich unterbleibt und somit die Durchsetzbarkeit der Sicherheitsmaßnahmen nicht gegeben ist.
- *Fehlende Aktualisierung im Sicherheitsprozess:* Neue Geschäftsprozesse, Anwendungen und IT-Systeme sowie neue Bedrohungen beeinflussen permanent den Sicherheitszustand innerhalb einer Institution. Fehlt ein effektives Revisionskonzept, das auch das Bewusstsein für die neuen Bedrohungen stärkt, verringert sich das Sicherheitsniveau und aus der realen Sicherheit wird schleichend eine gefährliche Scheinsicherheit.

# G 2.67 Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Wenn die Vergabe von Zutritts-, Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe.

Bei der Einführung von Identitätsmanagement-Systemen oder Revisionen stellt sich häufig heraus, dass verschiedene Personen in unterschiedlichsten Organisationseinheiten für die Vergabe von Berechtigungen zuständig sind. Dies führt schnell dazu, dass Benutzer Berechtigungen auf "Zuruf" erhalten oder umgekehrt nur über unnötig komplizierte Wege an diese kommen. Dadurch können einerseits fehlende Berechtigungen die tägliche Arbeit behindern, andererseits kann es so dazu kommen, dass Berechtigungen ohne Erfordernis vergeben werden und so ein Sicherheitsrisiko darstellen.

In vielen Institutionen ist die Verwaltung von Zugangs- und Zugriffsrechten eine extrem arbeitsintensive Aufgabe, weil sie schlecht geregelt ist oder die falschen Tools dafür eingesetzt werden. Dadurch kann z. B. viel "Handarbeit" erforderlich sein, die gleichzeitig wiederum sehr fehleranfällig ist. Außerdem sind in diesem Prozess dann auch häufig viele unterschiedliche Rollen und Personengruppen eingebunden, so dass hier auch leicht der Überblick über durchgeführte Aufgaben verloren geht.

Weiterhin gibt es auch Institutionen, in denen kein Überblick über alle auf den verschiedenen IT-Systemen eingerichteten Benutzer und deren Rechteprofil vorhanden ist. Typischerweise führt das dazu, dass sich immer wieder Zutrittsberechtigungen oder Accounts von Benutzern finden, die die Behörde bzw. das Unternehmen längst verlassen haben oder die durch wechselnde Tätigkeiten zu viele Rechte aufgehäuft haben.

Wenn die Tools zur Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten schlecht ausgewählt wurden, sind diese oft nicht flexibel genug, um auf Änderungen in der Organisationsstruktur oder auf Wechsel der IT-Systeme angepasst zu werden.

Die Rollentrennung von Benutzern kann falsch vorgenommen worden sein, so dass Sicherheitslücken entstehen, beispielsweise durch falsche Zuordnung von Benutzern in Gruppen oder zu großzügige Rechtevergabe. Benutzer können Rollen zugeordnet werden, die nicht ihren Aufgaben entsprechen (zu viel oder zu wenig Rechte) oder die sie aufgrund ihrer Aufgaben nicht haben dürfen (Rollenkonflikte).

# G 2.68 Fehlende oder unzureichende Planung des Active Directory

Die globale Struktur des Active Directory, also die Gliederung in Domänen, hat weitreichende Auswirkungen auf die Sicherheit der Ressourcen, die im Active Directory verwaltet werden. Problematische Aspekte ergeben sich hier besonders dann, wenn für die verschiedenen Domänen unterschiedliche Sicherheitsanforderungen bestehen oder Domänen zu verschiedenen Organisationsbereichen gehören.

Bei fehlender oder unzureichender Planung können sich beispielsweise folgende domänenübergreifende Gefährdungen ergeben:

- Alle Domänen in einem Active Directory müssen das gleiche Schema verwenden. Soll auch nur in einer Domäne eine Software installiert werden, die eine Schema-Änderung benötigt, müssen alle anderen Domänen diese Änderung mittragen. Inkompatible Schema-Änderungen durch verschiedene Softwareprodukte können dann dazu führen, dass Software nicht installiert werden kann oder fehlerhaft abläuft.
- Bestimmte Benutzerdaten aus dem Active Directory ("Global Catalog") stehen in jeder Domäne zur Verfügung. Dabei könnten die Anforderungen des Datenschutzes verletzt werden, wenn Art und Detailtiefe dieser Informationen vorab nicht ausreichend abgestimmt wurden.
- Administratoren der "Forest Root Domain" haben weitreichende Befugnisse auch in anderen Domänen. Ist der Zeitraum zu lange, bis ein Administratorkonto automatisch gesperrt wird, können die Administratorrechte von Dritten ausgenutzt werden.
- Ist eine Domäne auf mehrere Standorte verteilt, die nur unzureichend miteinander vernetzt sind, kann es zu lange dauern, bis eine Kontosperrung an allen Standorten wirksam wird. Infolgedessen kann sich ein Benutzer, dessen Konto gesperrt worden ist, unter Umständen an anderen Standorten noch am System anmelden.

Auch innerhalb einer Domäne muss der Aufbau des Active Directory sorgfältig geplant werden, da sich sonst folgende Gefährdungen ergeben:

- Werden Rechner und Benutzerkonten in den voreingestellten Containern "Computer" und "Benutzer" unterhalb der Domäne angeordnet, ist keine Gruppenrichtlinien-Konfiguration entsprechend verschiedener Typen von Benutzerkonten oder verschiedener Computertypen möglich. Dadurch könnte beispielsweise eine durch Gruppenrichtlinien erzwungene Einschränkung von Rechten auf einem betroffenen Computertyp umgangen werden.
- Werden Organisations-Einheiten (Organizational Units, OUs) tief geschachtelt, so kann die Struktur der Domäne unüberschaubar werden, so dass das Active Directory anfälliger für Fehlkonfigurationen wird. Zudem sinkt die Performance des Active-Directory-Dienstes mit der Schachtelungstiefe, wenn OUs zu tief, d. h. über mehr als 4 Ebenen, geschachtelt werden.

# G 2.69 Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory

Als Werkzeug für das Ressourcenmanagement in Netzen ist eDirectory für den Einsatz in einer heterogenen IT-Umgebung unter einer Vielzahl unterstützter Betriebssysteme ausgelegt. Die Sicherheit des Gesamtsystems ist naturgemäß abhängig von der Sicherheit jedes Teilsystems. Die Betriebssystemsicherheit und speziell die Sicherheit des Dateisystems sind die Basis, auf die sich die Sicherheit von eDirectory stützt.

Da sich eDirectory sowie die einsetzbare Clientsoftware auf einer Vielzahl von Betriebssystemen installieren und betreiben lassen, kann sich daraus eine hohe Vielfalt der bei den eingesetzten Betriebssystemen jeweils vorzunehmenden Sicherheitseinstellungen ergeben. Dies erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse sämtlicher involvierter Betriebssysteme voraus. Es besteht deshalb die Gefahr, dass der Einsatz von eDirectory nicht detailliert und tief genug geplant wird, wenn die Gesamtlösung sehr heterogen ist.

Für den Einsatz im Intranet ist speziell die Planung der Baumstruktur und die Abbildung der Unternehmensinfrastruktur darin von großer Bedeutung. Bei fehlerhafter Planung besteht die Gefahr von Inkonsistenzen und übermäßiger Komplexität im Aufbau des Verzeichnisdienstes. Daraus können in der Folge Fehlkonfigurationen und falscher oder unzulänglicher Betrieb des Systems resultieren.

Die globale Baumstruktur des eDirectory-Verzeichnisdienstes hat weitreichende Auswirkungen auf die Sicherheit einer eDirectory-Installation. Problematische Aspekte ergeben sich hier besonders dann, wenn die verschiedenen Teilbäume unterschiedliche Sicherheitsanforderungen haben oder zu verschiedenen Organisationsbereichen gehören. Durch die impliziten Vererbungsmechanismen und die Komplexität der Regeln für die Berechnung der tatsächlich wirksamen, effektiven Rechte einzelner Objekte stellt dies hohe Anforderungen an die Planung des Systems.

Die implizit eingesetzte CA (Zertifizierungsstelle) ist wesentlicher Bestandteil der Sicherheit von eDirectory. Auch hier kann eine fehlerhafte Planung die Sicherheit des Verzeichnisdienstes beeinträchtigen.

Die Planung der Zugriffsmöglichkeiten auf den Verzeichnisdienst ist ein Kernthema für die Systemsicherheit. Dies gilt sowohl für den Einsatz im Intranet als auch besonders für den Einsatz von eDirectory als LDAP-Server im Internet.

Weiterhin ist die Planung der Administration des Verzeichnisdienstes ein wichtiges Thema. eDirectory erlaubt die Umsetzung eines Rollen-basierten Administrationskonzeptes sowie die Delegation von Administrationsaufgaben. Dies ist speziell unter dem Aspekt der Sicherheitsadministration wichtig. Die Planung der Administration erfordert äußerste Sorgfalt und Umsicht, anderenfalls besteht die Gefahr, dass unautorisierte Systemnutzer ungewollte Zugriffsmöglichkeiten erhalten.

Darüber hinaus bietet die eDirectory-Software das *iMonitor-Tool*, welches einen Web-basierten Monitorzugriff auf die eDirectory-Server und das Verzeichnissystem gestattet. Eine fehlerhafte Planung des Einsatzes dieser Funk-

tionalität erlaubt unter Umständen unautorisierten Benutzern den Zugang zu Interna der eDirectory-Installation.

Ein wichtiger Punkt im Betrieb von eDirectory ist auch die Partitionierung des Verzeichnisdienstes und dessen Replikation. Hier kann eine unzulängliche Planung mangelhafte Performance, Inkonsistenzen in der Datenhaltung bis hin zu Datenverlusten zur Folge haben.

Der eDirectory-Verzeichnisdienst erlaubt eine rollenbasierte Administration der Verzeichnisdatenbank sowie die Delegation einzelner Administrationsaufgaben. Die Planung der Administrationsrollen und der Delegationsmöglichkeiten hat dabei in Übereinstimmung mit der festzulegenden Sicherheitsrichtlinie (siehe M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*) zu erfolgen. Bei fehlender oder fehlerhafter Planung der Administrationsaufgaben besteht die Gefahr, dass das System unsicher oder unzulänglich administriert wird.

eDirectory erlaubt die Synchronisation von Verzeichnisdaten mit weiteren Verzeichnisdiensten via DirXML. DirXML besteht aus einem Kern (*engine*) und spezialisierten Treibern (z. B. für Windows 2000 Active Directory, Lotus Notes, SAP R/3, Netscape, etc.) für den Austausch von Verzeichnisinformationen im XML-Format. Dabei können die fremden Verzeichnisdienste über einen so genannten *Publisher Channel* dem eDirectory Änderungen mitteilen. Bei entsprechenden Rechten, die vom jeweils betrachteten Zielsystem abhängen, werden diese Änderungen dann auch im eDirectory aktiv. Die externen Verzeichnisse können sich umgekehrt beim eDirectory einschreiben, um Änderungen des eDirectory-Informationsstandes über diesen Kanal (*subscriber channel*) zu erfahren und ihr Verzeichnis daraufhin abzugleichen. Diese Synchronisation bedarf einer detaillierten Planung, da anderenfalls sensitive Daten unter Umständen ungewollt automatisiert nach außen vervielfältigt werden. Umgekehrt können unter Umständen ungewollt bestehende Daten auf diesem Weg überschrieben werden. Um die Daten beim Transport zu schützen, kann SSL eingesetzt werden. Hierbei können Fehler in der Planung den Verlust von Integrität und Vertraulichkeit von Verzeichnisdaten nach sich ziehen.

Nicht zuletzt ist die Verwendung von Login-Skripts für Benutzer und Benutzergruppen zu planen. Bei fehlender oder unzulänglicher Planung können hierbei Inkonsistenzen zur festgelegten Sicherheitsrichtlinie auftreten.

Darüber hinaus können sich bei fehlender oder unzureichender Planung auch folgende Probleme ergeben:

- Der Administrationszugriff auf das System kann unzureichend gesichert sein,
- der Betrieb der Public-Key-Infrastruktur kann unzulänglich sein,
- die Systemperformance zu gering sein und
- es kann zu Datenverlusten kommen, sofern Replikation und Backup nicht ausreichend berücksichtigt wurden.

# G 2.70 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory

Die Partitionierung und die Replizierung des eDirectory-Verzeichnisdienstes ist ein wesentlicher Aspekt bei der Planung des Einsatzes.

Bei der Partitionierung handelt es sich um eine Aufteilung der Verzeichnisdaten des eDirectory in einzelne Teilbereiche (Partitionen). Diese Aufteilung kann nicht beliebig erfolgen, sondern muss gewissen Regeln entsprechen, die sich aus der Logik der hierarchischen Baumstruktur ergeben. Zweck der Partitionierung ist zum einen eine Lastverteilung des Verzeichnissystems auf mehrere Teile, zum anderen kann damit eine physikalische Trennung der Aufbewahrungsorte von Verzeichnisdaten - z. B. den Standorten einer Organisation entsprechend - erreicht werden. Weiterhin können Partitionen auch Verwaltungseinheiten des Verzeichnissystems darstellen.

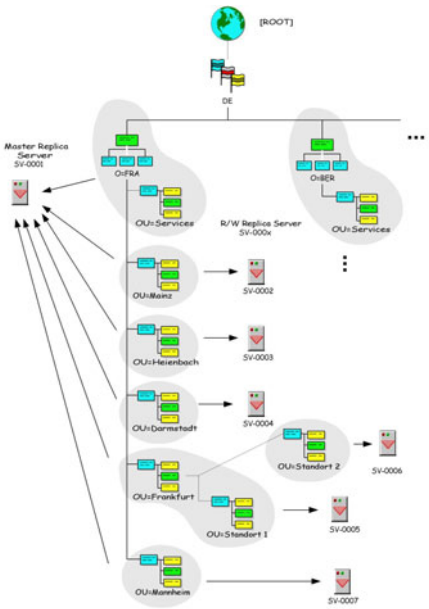



Abbildung: Beispiel für einen partitionierten eDirectory Verzeichnisdienst

Die Replizierung von Partitionen des eDirectory dient in erster Linie der Erhöhung der Verfügbarkeit und der Lastverteilung des Verzeichnissystems. Weiter wird durch die Redundanz in der Datenhaltung die Ausfallsicherheit verbessert.

Die Planung ist auch deshalb von entscheidender Bedeutung, da nachträgliche Änderungen an den Partitions- und Replikationseinstellungen zwar möglich sind, jedoch unter Umständen Inkonsistenzen nach sich ziehen können.

Bei Änderungen am eDirectory dauert es naturgemäß eine gewisse Zeit, bis sich die neuen Einstellungen überall hin ausgebreitet haben. Somit kann sich ein Zeitfenster ergeben, innerhalb dessen das eDirectory inkonsistent ist. Solche Inkonsistenzen können vor allem in der Definition der Authentisierungsdaten oder auch der Zugriffsrechte auf eDirectory-Objekte ein Problem darstellen.

Eine Partitionierung des eDirectory-Verzeichnisses hat direkte Konsequenzen für die Vererbung von Zugriffsrechten (Access Control Lists, ACL). Um die Vererbungsregeln bei einem bestehenden eDirectory-Baum zu erhalten, wird bei einer Partitionierung dem Wurzelobjekt der neuen Partition die übergeordnete ACL als *inherited ACL* vom System zur Kenntnis gebracht.

Die Festlegung der Partitionierung des eDirectory-Verzeichnisdienstes hat direkte Auswirkung auf die Replizierungsaktivitäten des Gesamtsystems. Um effizient über den Gesamtbaum nach Objekten suchen zu können (*Tree walking*), legt das eDirectory automatisch so genannte *Subordinate Reference Replicas* an, welche im Wesentlichen Sprungadressen enthalten. Ist die Planung unzulänglich (z. B. bei zu flacher Baumstruktur), so werden hier sehr umfassende Replizierungsringe erzeugt. Wird ein Replizierungsring sehr groß, so besteht eine gewisse Wahrscheinlichkeit, dass zumindest ein eDirectory-Server des Ringes momentan nicht erreichbar ist. In einem solchen Fall werden Fehler- und Statusmeldungen auf jedem weiteren eDirectory-Server des Replizierungsrings erzeugt. Dies kann zu erhöhtem Administrationsaufwand führen, der sich über große Teile des Verzeichnisbaums erstrecken kann.

Außerdem kann eine fehlerhafte oder unzureichende Planung der Partitionierung und der Replizierung des Verzeichnisdienstes auch zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und einer insgesamt schlechten Systemperformance bis hin zu Systemausfällen führen.

# G 2.71 Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory

Die LDAP-Zugriffsmöglichkeit auf den Verzeichnisdienst von eDirectory ist ein wesentliches Leistungsmerkmal des Softwareprodukts. Der Zugriff durch die Benutzer erfolgt über das LDAP v3-Protokoll, welches einen weitverbreiteten Internet-Standard darstellt. Betreiber, die eDirectory als eBusiness-Plattform verwenden, stellen ihren Benutzern dabei in der Regel spezielle Clients zur Verfügung. Einfache Web-Browser oder E-Mail-Clients können jedoch ebenfalls als LDAP-Clients agieren.

Die LDAP-Schnittstelle ist außerdem auch dazu geeignet, dass Netzapplikationen und deren Services darüber auf den Verzeichnisdienst zugreifen. Dieser Zugriff bedarf eingehender Planung, insbesondere auch in Bezug auf die für den sinnvollen Einsatz der Anwendungen benötigten eDirectory-Rechte.

Die Planung des LDAP-Zugriffs hängt also wesentlich vom Einsatzszenario des eDirectory ab. Prinzipiell gibt es aus Sicht des eDirectory drei verschiedene Verbindungsarten für einen LDAP-Client:

- als [Public] Objekt (*Anonymous Bind*): Hierbei werden keine Authentisierungsinformationen abgefragt und das [Public] Objekt besitzt standardmäßig stets das uneingeschränkte Browse-Recht auf den Verzeichnisbaum.
- als Proxy User (*Proxy User Anonymous Bind*): Diese Konfigurationsmöglichkeit kann anstelle des anonymen Login gewählt werden. Der Proxy User ist dabei eDirectory-seitig entsprechend zu konfigurieren.
- als NDS User (*NDS User Bind*): Hierbei meldet sich der Benutzer mit seinen eDirectory-Rechten am Verzeichnisdienst an. Das entsprechende Benutzerobjekt muss beim eDirectory angelegt sein.

Es muss in der Planung berücksichtigt werden, ob und welche Daten im Klartext gemäß den organisationsinternen Sicherheitsrichtlinien übertragen werden dürfen. Dies gilt für den Einsatz im Intranet sowie besonders für die Anbindung an das Internet.

Dabei geht es z. B. darum, ob Benutzerpasswörter im Klartext übermittelt werden dürfen und wie konsequent der Einsatz der SSL-Verschlüsselung umgesetzt wird. Damit unterstützt eDirectory entsprechend dem Standard LDAP v3 zwei Verbindungsarten:

- *anonymous bind*: ohne Benutzername und Passwort,
- *clear-text password bind*: Benutzername und Klartextpasswort zur Authentisierung.

Zusätzlich wird LDAP über SSL unterstützt. Seitens eDirectory muss konfiguriert werden, ob die ersten beiden Verbindungsarten unterstützt werden.

Außerdem wird SSL in zwei Modi unterstützt: ein- und zweiseitige Authentisierung. Bei beidseitiger Authentisierung müssen die erforderlichen Credentials, unter anderem das Wurzelzertifikat der Zertifizierungsstelle, allgemein zugänglich sein.

Durch die oben beschriebene Vielfalt der Konfigurationsoptionen für den LDAP-Zugriff auf den eDirectory-Verzeichnisdienst können sich schnell Fehlkonfigurationen ergeben. Konsequenzen solcher Fehlkonfigurationen könnten sein:

- Falsche Vergabe von Zugriffsrechten,

- unautorisierte Zugriffsmöglichkeiten auf den eDirectory-Verzeichnisdienst,
- Übermittlung von Benutzerpasswörtern im Klartext,
- Ausspähen von unverschlüsselten Informationen,
- Fehler beim LDAP-Zugriff, insbesondere für netzbasierte Anwendungen, sowie
- unzureichende Produktivität des Gesamtsystems.

# G 2.72 Unzureichende Migration von Archivsystemen

Archivierte Daten sollen typischerweise über einen sehr langen Zeitraum gespeichert bleiben. Während dieses Zeitraums können die zugrundeliegenden technischen Systemkomponenten, Speichermedien und Datenformate physikalisch bzw. technologisch altern und dadurch unbrauchbar werden. Außerdem können sich im Laufe der Zeit Probleme mit der Kompatibilität der verwendeten Datenformate ergeben.

Wenn auf die Alterung des bestehenden Systems nicht reagiert wird, ist langfristig damit zu rechnen, dass

- archivierte Rohdaten physikalisch nicht mehr von den Archivmedien lesbar sind,
- archivierte Daten durch physikalische Fehler an Archivsystem und -medien verändert werden,
- Ersatzteile für Hardware-Komponenten nicht mehr lieferbar sind,
- Ergänzungen für Software-Komponenten nicht mehr lieferbar sind,
- verwendete Datenformate nicht mehr den Integritätsanforderungen entsprechen,
- elektronische Signaturen unbrauchbar werden,
- verschlüsselte Daten für Unberechtigte lesbar werden.

Auch wenn rechtzeitig Systemkomponenten ausgetauscht oder die Daten kopiert werden, so können trotzdem noch Probleme durch die Verwendung kryptographischer Verfahren auftreten. Beispielsweise könnten Schwachstellen in integritätssichernden Verfahren entstehen, da Verschlüsselungs- und Signaturalgorithmen im Laufe der Zeit und mit steigender Rechenleistung an Schutzwirkung verlieren können (siehe auch G 2.79 *Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung*).

**Beispiele:**

- Durch physikalische Langzeiteinflüsse (Materialverschleiß, Verformung, Verkratzen von Medienoberflächen, Weichmacher) können Datenträger beschädigt werden. Je nach Verwendungszweck des betroffenen Datenträgers als System- oder Archivmedium kann der Betrieb des Archivsystems gestört oder die auf den Archivmedien gespeicherten Daten verloren gehen.
- Der Hersteller eines Archivsystems hatte in den Kontextdaten für Dokumente ein Debug-Feld vorgesehen. In der Pilotphase des Archivsystems wurden Dokumente aus dem normalen Geschäftsbetrieb zu Testzwecken archiviert, wobei der Teststatus in der Debug-Information festgehalten wurde. Beim Übergang in die Betriebsphase wurden die Testdokumente dann nicht gelöscht, da sie auf WORM-Datenträgern archiviert waren, sondern es wurden die mit der betreffenden Debug-Information markierten Dokumente nicht mehr angezeigt. Das Nachfolgesystem wurde von einem anderen Hersteller geliefert, der Debug-Informationen auf eine andere Weise darstellte. Bei der anschließenden Migration der Archivdaten auf das neue Archivsystem wurde jedoch versehentlich das alte Debug-Feld nicht ausgewertet. Die alten Testdokumente befanden sich nach der Migration der Daten weiterhin im Archiv, tauchten bei einer späteren Recherche jedoch plötzlich als vermeintlich authentische Dokumente auf.
- Elektronische Signaturverfahren könnten durch Ausprobieren der Signaturschlüssel oder durch mathematische Verfahren kompromittiert werden. Sofern dies innerhalb des Archivierungszeitraums eintritt, ist es möglich, elektronische Signaturen auch rückwirkend zu fälschen.

# G 2.73 Fehlende Revisionsmöglichkeit von Archivsystemen

Die Revision eines Archivierungsvorgangs muss sowohl organisatorische als auch technische Kriterien berücksichtigen. Die Prüfung von Archivsystemen muss daher neben der Begutachtung der Systemkonfiguration auch die Prüfung der Vergabe und Nutzung von Zugriffsrechten umfassen.

Wenn das ausgewählte Archivsystem hierbei nicht die notwendige technische Unterstützung liefert, z. B. in Form von speziellen Benutzerkonten für die Revision, Monitoring-Werkzeugen, integritätsgeschützten Protokolldateien (siehe G 2.76 *Unzureichende Dokumentation von Archivzugriffen*), kann der Prüfungsvorgang sehr aufwendig werden. Dadurch besteht außerdem die Gefahr, dass dieser nur unvollständig stattfindet und wesentliche Punkte übersehen werden. Der Revisionsvorgang des Archivierungsprozesses kann hierdurch insgesamt gefährdet werden.

Mittelbar können sich hieraus rechtliche und wirtschaftliche Nachteile ergeben, z. B. durch den Wegfall der Nachweiskraft archivierter Dokumente.

# G 2.74 Unzureichende Ordnungskriterien für Archive

Elektronische Archive können sehr große Datenmengen beinhalten. Zur Ablage und zum Wiederauffinden einzelner Datensätze dienen Ordnungskriterien, die in Indexdaten des Dokumentenmanagementsystems (DMS) und Indexdaten des Archivsystems zu unterscheiden sind.

Ordnungskriterien des DMS dienen dazu, den Kontext und Inhaltsangaben zusammen mit dem jeweiligen Dokument zu verwalten. Eine ungeeignete Auswahl von Kontextkriterien hätte hier zur Folge, dass archivierte Dokumente nicht oder nur mit großem Aufwand wieder zu recherchieren wären oder die Semantik archivierter Dokumente nicht eindeutig bestimmbar wäre. Eine große Zahl von Kontextkriterien andererseits steigert den Verwaltungsaufwand und reduziert mit wachsender Zahl archivierter Dokumente die Performance des Dokumentenmanagementsystems.

Ordnungskriterien des Archivsystems hingegen sind eher technischer Natur. Sie dienen der Identifikation einzelner Rohdaten und der Organisation der Ablage der Rohdaten auf Speichermedien. Ihre Auswahl wird in der Regel nicht durch das DMS, sondern durch den Aufbau des Archivservers und der zugrundeliegenden Speicherarchitektur bestimmt. Eine wesentliche Anforderung ist die Eindeutigkeit der Dokumentkennung. Sollte diese Anforderung verletzt werden, d. h. wenn zwei Dokumente dieselbe Dokumentkennung erhalten, so kann je nach Suchverfahren beim Abrufen ein falsches Dokument an das DMS zurückgegeben und dort mit einem neuen Dokumentkontext versehen werden. Das nicht gefundene Dokument wäre zwar physikalisch vorhanden, würde aber nicht mehr eindeutig einem Vorgang im DMS zuzuordnen sein.

Die Revisionssicherheit des Archivierungsprozesses bezieht sich wesentlich auf die eindeutige Kennzeichnung aller verwalteten Dokumente sowie die Nachweisbarkeit der Verknüpfung von Dokument und Kontextinformationen.

# G 2.75 Mangelnde Kapazität von Archivdatenträgern

Eine falsche Einschätzung des Datenaufkommens bei der Archivierung kann dazu führen, dass zu kleine Archivmedien verwendet werden und daher die Archivierung unvollständig oder verzögert erfolgt.

Bei der Abschätzung des benötigten Datenvolumens wird häufig nur die erwartete maximale Größe der zu speichernden Dokumente als einzige Einflussgröße zugrundegelegt. Tatsächlich jedoch kann der Speicherbedarf bei Archivsystemen ein Vielfaches davon betragen, da hierbei auch die Art der Datenablage sowie die Änderungshäufigkeit von Dokumenten einen wesentlichen Einfluss haben.

Bei einer Archivierung auf WORM-Medien (Write Once Read Multiple) werden beispielsweise die Dokumente zwangsläufig in mehreren Versionen abgelegt, d. h. nach jeder Änderung wird ein neues Dokument gespeichert. Dadurch kann sich auch bei kleinen Dokumenten mit hoher Änderungsfrequenz ein hohes Datenvolumen ergeben. Alte Versionen der Dokumente können nachträglich nicht mehr vom Archivmedium gelöscht werden. Neben Kapazitätsengpässen kann dies auch zu Datenschutz- oder Vertraulichkeitsproblemen führen, da Daten nur als "zu löschen" markiert, aber nicht tatsächlich gelöscht werden.

# G 2.76 Unzureichende Dokumentation von Archivzugriffen

Ebenso wie bei anderen IT-Systemen bestehen auch bei Archivsystemen Manipulationsmöglichkeiten, wenn diese schlecht geschützt sind. Benutzer könnten versuchen, gefälschte Dokumente in das Archiv einzubringen und durch Angabe entsprechender Kontextinformationen diese Dokumente bestehenden Verwaltungsvorgängen zuzuweisen oder komplett neue Vorgänge zu fälschen. Systemadministratoren könnten Manipulationen am Archivsystem vorbei durchführen und die Manipulation durch Veränderung von Protokolldateien verbergen.

Üblicherweise wird Protokolldateien ein geringerer Wert beigemessen als den zu archivierenden Dokumenten selbst. Dies äußert sich häufig in geringeren Aufbewahrungsfristen für Protokolldateien und im weniger sorgsamen Umgang mit Protokolldateien.

Wenn archivierte Dokumente in spätere Verwaltungsvorgänge einfließen sollen, ist es unerlässlich, die Authentizität nachweisen zu können, also korrekte von manipulierten Dokumenten unterscheiden und im Falle von strittigen Dokumenten die Dokumenthistorie belegen zu können. Dies wird gefährdet durch

- eine nicht ausreichende Protokollierung der Archivzugriffe, insbesondere der Speichervorgänge,
- einen nicht ausreichenden Schutz der Protokolldaten vor Manipulation durch Benutzer sowie Systemadministratoren,
- den Verlust von Protokolldaten,
- zu kurze Aufbewahrungsfristen der Protokolldaten.

Sofern die zu archivierenden Dokumente nach Vertraulichkeitsstufen klassifiziert sind, muss auch immer nachvollziehbar sein, wer zu welchem Zeitpunkt Einsicht in Dokumente genommen hat. Dies ist nicht mehr gewährleistet, wenn Lesezugriffe und Suchanfragen nicht dokumentiert werden.

**Beispiele:**

- Im Rahmen einer Archiv-Recherche wird ein Dokument aufgefunden, das in einem laufenden Verwaltungsvorgang eine Person in bestimmter Weise belastet. Anhand der mitgespeicherten Kontextinformationen wird das Dokument als authentisch bewertet. Das Dokument wurde aber seinerzeit von einem Unberechtigten erzeugt, der bewusst falsche Kontextinformationen (u. a. Ersteller des Dokuments und Erstelldatum) angegeben hatte, um später die fragliche Person belasten zu können. Da die Protokolldateien der Archivzugriffe zwischenzeitlich gelöscht wurden, kann dies aber nun nicht mehr erkannt werden. Der betroffene Mitarbeiter wird dadurch fälschlich belastet.
- Ein Benutzer mit administrativen Privilegien manipuliert Dateien im Cache-Bereich des Archivsystems, bevor diese auf dauerhaften Medien abgelegt werden. Die Manipulation ist nicht nachvollziehbar, da der Benutzer am Archivsystem vorbei sowohl die Daten selbst als auch die Protokolldateien manipuliert hat.

# G 2.77 Unzulängliche Übertragung von Papierdaten in elektronische Archive

In vielen elektronischen Archiven werden regelmäßig Dokumente gespeichert, die ursprünglich nur in Papierform vorlagen und daher in eine elektronische Form übertragen werden müssen. Dies erfolgt unter Wahrung ausgewählter Merkmale des Originaldokuments. Je nach Verwendungszweck des Dokuments ergeben sich hier unterschiedliche Anforderungen. Dies kann die Übereinstimmung des äußeren Erscheinungsbilds der Kopie mit dem Original sein, wenn beispielsweise eine Bilddatei verwendet wird. Es kann auch die Übereinstimmung von Textausschnitten, z. B. unter Verwendung einer Textdatei, oder die Abbildung weiterer Merkmale, z. B. Biometriedaten oder Kontextdaten, gefordert sein.

Die Ablage als Text- oder Bilddatei allein reicht für den Nachweis der Originaltreue des Dokuments nicht immer aus, da sowohl Manipulationen als auch Fehler auftreten können:

- Mit Text- und Bildverarbeitungsprogrammen können bestehende Dokumente manipuliert werden.
- Durch Fehler beim Einscannen kann die Semantik der aufgenommenen Daten verfälscht werden, wodurch Fehlinterpretationen und -berechnungen ausgelöst werden können. Beispielsweise könnten wichtige Teile des Dokuments beim Scanvorgang vergessen werden.

In einigen Archivierungsszenarien ist vorgesehen, die in Papierform vorliegenden Dokumente nach dem Einscannen aus Platzgründen zu vernichten. Hierbei muss davon ausgegangen werden, dass nach Vernichtung des Originaldokumentes der spätere Nachweis der Originaltreue von Kopie und Dokument nicht mehr direkt erbracht werden kann.

Dies bedeutet, dass alle für spätere Nachweiszwecke notwendigen Merkmale des Originaldokuments bereits in der Phase der Übertragung in elektronischer Form erfasst und nachvollziehbar mitgespeichert werden müssen. Werden hierbei Merkmale nicht berücksichtigt oder vergessen (z. B. die Anzahl der Seiten eines Originaldokumentes), kann das die Nachweiskraft der Dokumente erheblich einschränken, da Nacherhebungen von Merkmalen des Originaldokuments oftmals nicht mehr möglich sind

Eine unzulängliche Vorgehensweise bei der Übertragung der Dokumente gefährdet die Wirksamkeit und Nachvollziehbarkeit des nachfolgenden Verarbeitungsprozesses für Dokumente und letztlich die Korrektheit der archivierten Dokumente.

**Beispiele:**

- Der eingehende Schriftverkehr einer Behörde wird zur späteren elektronischen Weiterverarbeitung eingescannt und im Archiv abgelegt. Gelegentlich wird jedoch vergessen, die Rückseite eines Briefes einzuscannen. Da der eingehende Schriftverkehr nach dem Einscannen vernichtet wird, kann der Originalzustand des Briefes nicht mehr nachgewiesen werden.
- Beim Einscannen und automatischen Erfassen von Text werden Passagen ausgelassen oder verfälscht, die vom OCR-Programm (Optical Character Recognition - Verfahren zur Erkennung von Text aus Bilddateien) nicht korrekt erkannt worden sind. Das kann z. B. in schwacher Farbe oder undeutlicher Schrift gedruckten Text betreffen, aber auch handschriftliche Ergänzungen in Dokumenten oder ein verwischtes Druckbild von Tinten-

strahldruckern. Falsch erkannte Rechnungsbeträge (nicht erkannte Kommata, etc.) sind ebenfalls eine mögliche Fehlerquelle für spätere Missverständnisse.

- Manuelle Unterschriften unter Dokumenten werden als Bild eingescannt. Bei einem späteren Rechtsstreit über die Echtheit von Dokument und Unterschrift kann ein graphologisches Gutachten keine eindeutige Aussage mehr liefern, da die vorgelegte Bilddatei mit einem Bildbearbeitungsprogramm manipuliert bzw. ein anderes Dokument kopiert worden sein könnte. Merkmale des Originaldokuments, wie z. B. Beschaffenheit und Zusammensetzung des verwendeten Papiers oder die Andruckstärke bei der händischen Unterschrift, sind nicht mehr nachvollziehbar.

# G 2.78 Unzulängliche Auffrischung von Datenbeständen bei der Archivierung

Datenträger können physikalisch wie technologisch veralten. Datenformate werden ebenfalls gelegentlich um neue syntaktische bzw. strukturelle Merkmale erweitert. Beides kann dazu führen, dass archivierte Daten nicht mehr lesbar sind (siehe G 2.72 *Unzureichende Migration von Archivsystemen*).

Daher sollten elektronisch archivierte Dokumente in größeren Zeitabständen auf neue Datenträger kopiert bzw. in neue, aktuellere Datenformate übertragen werden. Hierbei besteht die Gefahr, dass Daten bei der Übertragung auf neue Datenträger aus ihrem Dokumentkontext gelöst werden oder beim Umkopieren in andere Datenformate unbeabsichtigt semantische Änderungen vorgenommen werden.

Daneben bestehen Manipulationsmöglichkeiten während der Übertragung der Daten auf ein neues Speichermedium. Hierbei können selbst auf WORM-Medien abgelegte Daten "geändert" werden.

Nach der Migration der Datenbestände kann die Notwendigkeit bestehen, alte Datenträger zu vernichten. Hierzu wird auf die Gefährdung G 2.81 *Unzureichende Vernichtung von Datenträgern bei der Archivierung* verwiesen.

**Beispiele:**
- Im Rahmen der Migration der Datenbestände werden Vorversionen von versioniert gespeicherten Dokumenten aus Platzgründen gelöscht, obwohl diese aus Nachweisgründen noch benötigt werden.
- Es werden Dateien, die ursprünglich auf WORM-Medien änderungssicher ("revisionssicher") gespeichert waren, auf neue Datenträger übertragen. Dabei werden Dateien während des Kopiervorgangs ausgetauscht, d. h. einzelne Dateien werden nicht auf das neue Medium übernommen, stattdessen werden gefälschte Dateien eingefügt.

# G 2.79 Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung

Die Algorithmen und Schlüssellängen, die bei digitalen Signaturen verwendet werden, müssen in regelmäßigen Abständen an den aktuellen Stand der Technik angepasst werden, damit ihre Schutzwirkung gewährleistet ist (siehe G 4.47 *Veralten von Kryptoverfahren*). Das bedeutet, dass die verwendeten kryptographischen Schlüssel und die zugehörigen Zertifikate nur eine begrenzte Zeit zuverlässige Gültigkeit besitzen. Gemessen an der angestrebten Archivierungsdauer sind dies verhältnismäßig kurze Zeiträume. Um die Beweiskraft digitaler Signaturen zu erhalten, muss daher rechtzeitig die elektronische Signatur jedes einzelnen Dokuments erneuert werden.

Bei der regelmäßigen Neusignatur der archivierten Dokumente können u. a. folgende Sicherheitsprobleme auftreten:

- Wenn Dokumente mit einer vormals ungültigen oder fehlenden elektronischen Signatur fälschlicherweise eine gültige neue Signatur erhalten, so können diese Dokumente fortan fälschlicherweise als authentisch angesehen werden.
- Es könnte passieren, dass Dokumente bei einer Neusignatur vergessen werden, d. h. keine neue gültige Signatur erhalten, obwohl sie vormals gültig signiert waren. Dadurch kann die Authentizität bzw. Integrität des betreffenden Dokuments fortan möglicherweise nicht mehr nachgewiesen werden, wenn kein alternativer Nachweis anhand anderer Merkmale möglich ist.
- Zum Zeitpunkt der Neusignatur könnte das zu Grunde liegende kryptographische Verfahren bereits kompromittiert oder der ursprüngliche Signaturschlüssel bekannt geworden sein (z. B. durch massiven Rechenaufwand ermittelt). Dadurch könnten Unbefugte Dokumente erzeugen und mit einer technisch gültigen Signatur, gegebenenfalls auch mit beliebigen Zeitsignaturen (Zeitstempel), versehen. Gelingt es, diese Dokumente in den Prozess der Neusignatur einzubringen, so können diese Dokumente fälschlicherweise als authentisch angesehen werden.

# G 2.80 Unzureichende Durchführung von Revisionen bei der Archivierung

Die elektronische Archivierung stellt sehr hohe Anforderungen an den Prozess der Umwandlung von Papierdokumenten in elektronische Dokumente. Die bei der Archivierung auszuführenden Tätigkeiten sollten in einer Verfahrensdokumentation genau beschrieben sein und durch eine Protokollierung, die aufzeichnet, welcher Benutzer wann welche Aktivitäten im Archiv ausgeführt hat, nachvollziehbar gemacht werden.

Zu seltene und zu ungenaue Überprüfung der Arbeitsvorgänge bei der Archivierung oder der aufgezeichneten Protokolldaten kann mittelbar dazu führen, dass die Ordnungsmäßigkeit des Archivierungsprozesses und damit die Richtigkeit der archivierten Dokumente selbst angezweifelt wird.

# G 2.81 Unzureichende Vernichtung von Datenträgern bei der Archivierung

Archivsysteme mit ihren Speichermedien bieten alleine für sich in der Regel keinen Zugriffsschutz auf die gespeicherten Daten. Diese Funktion wird stattdessen vom übergeordneten Dokumenten-Management-System (DMS) erfüllt. Sind Archivdatenträger außerhalb der Archivumgebung (Archivsystem und DMS) zugänglich, ist davon auszugehen, dass jeder, der das Medium lesen kann, auf die dort gespeicherten Informationen zugreifen kann.

Besonders wenn archivierte Daten auf neue Datenträger umkopiert werden, besteht ein erhebliches Risiko, dass alte, nicht mehr gebrauchte Archivmedien, die nicht ordnungsgemäß und vollständig zerstört werden, zur Informationsgewinnung missbraucht werden.

Auch bei verschlüsselt archivierten Daten kann eine nicht ordnungsgemäße Vernichtung von Datenträgern ein Problem darstellen, da die Sicherheit von Kryptoalgorithmen immer nur zeitlich begrenzt garantiert werden kann (siehe G 4.47 *Veralten von Kryptoverfahren*). Eine einmalige Verschlüsselung schützt deshalb nicht dauerhaft vor Datenmissbrauch.

# G 2.82 Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen

Aufgrund der Sensitivität der gespeicherten Daten sowie der sehr langen Aufbewahrungszeit sind bei Speicher- oder Archivsystemen erhebliche Anforderungen an die Qualität der Datenspeicherung zu stellen. Die Wahl des Aufstellungsortes für das Speicher- oder das Archivsystem hat hierauf hohen Einfluss.

In diesem Zusammenhang sind folgende potentielle Sicherheitsprobleme zu beachten:

- **Unzulängliche klimatische Bedingungen**
  Eine zu hohe oder zu niedrige Temperatur kann ebenso wie eine zu hohe Luftfeuchtigkeit zu Fehlfunktionen in technischen Komponenten von Archiv- und Speichersystemen und zur Beschädigung von Archiv- und Speichermedien führen. Häufige Schwankungen der klimatischen Bedingungen verstärken diesen Effekt. Auch durch Sekundärschäden können derartige Klimabelastungen hervorgerufen werden. Ein Beispiel dafür ist die Ausdünstung von Wänden, die nach einem Brand im Nachbarraum auftreten kann.
- **Unzureichender physikalischer Schutz**
  Durch unzureichenden Schutz des Speicher- oder Archivsystems gegen unbefugten Zutritt und Zugriff können vorsätzliche Handlungen (z. B. Diebstahl, Manipulation oder Sabotage) begünstigt werden.
- **Unzureichender Schutz gegen sonstige Umgebungseinflüsse**
  Auch durch sonstige Umgebungseinflüsse (z. B. Erschütterungen oder eine hohe Staubbelastung) können Schäden an technischen Komponenten des Archivsystems oder an Speichermedien hervorgerufen werden. Besonders ärgerlich ist das, wenn die schädigenden Einflüsse sogar vorhersehbar waren, wie z. B. bei Bauarbeiten.

**Beispiel:**

Durch Ansiedlung des zentralen IT-Bereichs nahe an Produktionsanlagen kommt es dort gelegentlich zu Erschütterungen. Als Folge treten immer wieder Störungen in den technischen Komponenten des Archivsystems auf, das ebenfalls im IT-Bereich betrieben wird.

# G 2.83 Fehlerhafte Outsourcing-Strategie

Die Entscheidung, ein Outsourcing-Vorhaben durchzuführen, ist eine weitreichende Entscheidung. Durch diese begibt sich ein Unternehmen oder eine Behörde in ein enges Abhängigkeitsverhältnis zu dem Outsourcing-Dienstleister. Daher haben diesbezügliche Fehlentscheidungen langfristige und schwerwiegende Folgen. Diese können organisatorische, technische und auch gravierende finanzielle Auswirkungen sein.

Sicherheitsprobleme (z. B. bei mangelhafter Verfügbarkeit) beim Outsourcing-Dienstleister können nicht nur teuer, sondern auch existenzbedrohend sein. Jedoch können auch Fehleinschätzungen der auslagernden Organisation gravierende Folgen haben. Wird beispielsweise der Aufwand (z. B. Erstellung von Dokumentationen, Tests, Absicherung von Systemen) unterschätzt, so sind zeitliche Verzögerungen zu erwarten. Um verlorene Zeit einzuholen und Geld zu sparen, wird erfahrungsgemäß häufig der Testaufwand reduziert, was zu Abstrichen bei der Sicherheit führen kann.

# G 2.84 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister

Wenn Situationen eintreten, die nicht eindeutig vertraglich geregelt sind, können (zum Beispiel im Rahmen eines Outsourcing- oder Cloud-Computing-Vorhabens) Nachteile für den Auftraggeber entstehen.

So kann beispielsweise bei Outsourcing oder Nutzung von Cloud-Diensten der Auftraggeber verantwortlich gemacht werden, die zwar im Einflussbereich des Dienstleisters liegen, aber vertraglich nicht eindeutig geregelt sind.

Ein Hauptgrund für Probleme zwischen den Vertragspartnern sind zu optimistische Kostenschätzungen. Wenn sich herausstellt, dass der Dienstleister den Service nicht zu den kalkulierten und angebotenen Kosten erbringen kann oder Uneinigkeit darüber besteht, was "selbstverständlich" ist, kann dies direkt zu Sicherheitsproblemen führen. Erfahrungsgemäß wird an der Informationssicherheit gespart, wenn in anderen Bereichen ein Kostendruck entsteht, dem so begegnet werden kann, ohne dass Folgen unmittelbar sichtbar werden. Es ist daher von entscheidender Bedeutung, wie die vertraglichen Regelungen zwischen Auftraggeber und Auftragnehmer ausgestaltet sind. Nur, was von Anfang an vertraglich fixiert ist, wird auch später sicher in die Tat umgesetzt!

Cloud-Diensteanbieter und Outsourcing-Dienstleister erbringen ihre Services häufig mittels der Dienste Dritter. Bestehen hier unzureichende vertragliche Vereinbarungen, kann dies auch Auswirkungen auf die Service-Erbringung haben. Werden in den vertraglichen Regelungen bestehende Abhängigkeiten zwischen Diensteanbieter und Dritten nicht beachtet, kann dies zu einem Mangel an Transparenz hinsichtlich der Vorgänge beim Diensteanbieter und zu Unsicherheiten bei den Verantwortungsbereichen oder der Einhaltung vereinbarter Dienstgüten führen.

Weitere **Beispiele** für Folgen aus unzulänglichen vertraglichen Regelungen mit externen Dienstleistern sind:

- Der Auftraggeber kann seiner Auskunftspflicht gegenüber Aufsichtsbehörden oder Wirtschaftsprüfern nicht nachkommen, wenn der Dienstleister keinen Zutritt zu seinen Räumlichkeiten oder keinen Zugang zu den notwendigen Unterlagen gewährt.
- Der Auftraggeber muss sich für Verstöße gegen geltende Gesetze verantworten, wenn der Dienstleister nicht auf die Einhaltung dieser Gesetze verpflichtet wurde.
- Aufgaben, Leistungsparameter und Aufwände wurden ungenügend oder missverständlich beschrieben, sodass aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden.
- Der Auftraggeber kann neuen Anforderungen (zum Beispiel fachliche, gesetzliche Vorschriften, Verfügbarkeit, technische Entwicklung) nicht nachkommen, wenn Änderungsmanagement und Systemanpassungen nicht ausreichend vertraglich geregelt wurden.
- Bei Outsourcing-Vorhaben ist die Behörden- beziehungsweise Unternehmensleitung des Auftraggebers unter Umständen voll verantwortlich für

die ausgelagerten Geschäftsbereiche, kann dieser Verantwortung aber wegen fehlender Kontrollmöglichkeiten nicht gerecht werden.
- Ausgelagerte Daten oder Systeme werden ungenügend geschützt, wenn ihr Schutzbedarf oder besser die daraus resultierenden Anforderungen an die Sicherheit dem Outsourcing-Dienstleister unbekannt sind.
- Die Dienstleistungsqualität ist schlecht, und es gibt keine Eingriffsmöglichkeiten, weil keine Sanktionen vertraglich festgelegt wurden.
- Der Dienstleister zieht qualifiziertes Personal ab oder Vertreter des Stammpersonals sind nicht ausreichend vorbereitet, was zu Sicherheitsproblemen führen kann.

Besondere Probleme treten häufig dann auf, wenn Dienstleistungsverträge beendet werden (siehe G 2.85 *Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens*) und diese Situation nur unzureichend vertraglich geregelt wurde.

# G 2.85 Unzureichende Regelungen für das Ende eines Outsourcing- oder eines Cloud-Nutzungs-Vorhabens

Nutzt eine Institution die Services eines Outsourcing- oder Cloud-Diensteanbieters, so kommt es in der Regel zu Know-how-Verlust beim Auftraggeber und zu einer Abhängigkeit des Auftraggebers vom Dienstleister. Daher können unzureichende Regelungen für eine mögliche Kündigung des Vertragsverhältnisses gravierende Folgen für den Auftraggeber haben. Dies ist erfahrungsgemäß immer dann besonders problematisch, wenn ein aus Sicht des Auftraggebers kritischer Fall unerwartet eintritt, wie beispielsweise Insolvenz oder Verkauf des Outsourcing- oder Cloud-Dienstleisters.

**Beispiele:**
- Ein Konkurrent des Auftraggebers kauft den Outsourcing- oder Cloud-Dienstleister.
- Eine nationale Sicherheitsbehörde hat Prozesse zu einem Rechenzentrum ausgelagert, das später von einem ausländischen Unternehmen gekauft wird.
- Es gibt juristische Auseinandersetzungen zwischen Auftraggeber und Diensteanbieter wegen schlechter Dienstleistungsqualität oder gravierender Sicherheitsmängel, in deren Folge ein Vertragspartner den Vertrag kündigen möchte.

Ohne ausreichende interne Vorsorge sowie genaue Vertragsregelungen besteht immer die Gefahr, dass sich der Auftraggeber nur schwer aus dem abgeschlossenen Vertrag mit dem Outsourcing- oder Cloud-Dienstleister lösen kann. In diesem Fall ist es schwierig bis unmöglich, den ausgelagerten Bereich beispielsweise auf einen anderen Dienstleister zu übertragen oder ihn wieder in das eigene Unternehmen einzugliedern, falls dies notwendig erscheint.

Im Folgenden sind beispielhaft weitere Probleme aufgelistet, die in dieser Situation auftreten können:

- Durch unflexible Regelungen zum Kündigungsrecht kann der Vertrag nicht im Sinne des Auftraggebers bedarfsgerecht beendet werden.
- Zu kurze Kündigungszeiten führen bei Kündigung durch den Dienstleister dazu, dass keine Zeit für einen geordneten Übergang bleibt.
- Unzureichende Regelungen über das Eigentumsrecht an eingesetzter Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) können einen geregelten Übergang, beispielsweise auf einen neuen Outsourcing-Dienstleister, verhindern.
- Unzureichende Regelungen über das Überlassen von Dokumentationen können dazu führen, dass die IT-Systeme nicht geregelt weiterbetrieben werden.
- Unzureichende Regelungen für das Löschen von Daten, auch von Datensicherungen, beim Outsourcing- oder Cloud-Dienstleister können dazu führen, dass vertrauliche Daten Dritten bekannt werden.
- Der Auftraggeber kann seine Aufgaben unter Umständen nicht mehr erfüllen, da die Verfügbarkeit nicht mehr gewährleistet ist.
- In der Endphase des Auflösungsprozesses sind eventuell Daten und Systeme nicht mehr ausreichend geschützt, da diese als "Alt-Systeme" angesehen werden.
- Fehlende Regelungen (zum Beispiel auch Datenformate) zur Herausgabe der gespeicherten Informationen (Nutzdaten) durch den Diensteanbieter

führen zu Verzögerungen beim Wechsel auf einen anderen Anbieter oder beim Eingliedern der Dienstleistung in die Institution.
- Die Interoperabilität von Cloud Services ist bei einem Wechsel des Diensteanbieters oder beim Eingliedern in die Institution nicht gewährleistet, da keine entsprechenden Regelungen getroffen wurden.
- Der Wechsel von einem Outsourcing- oder Cloud-Diensteanbieter zu einem anderen Dienstleister bedingt unter Umständen Support-Leistungen durch den bestehenden Auftragnehmer. Wird die Verpflichtung zu deren Erbringung nicht vertraglich geregelt, kann der Diensteanbieter den Support verwehren oder dafür zusätzliche Kosten in Rechnung stellen.

# G 2.86 Abhängigkeit von einem Outsourcing- oder Cloud-Dienstleister

Nutzt eine Institution die Services eines Outsourcing- oder Cloud-Diensteanbieters, begibt sie sich immer in die Abhängigkeit vom entsprechenden Dienstleister. Daraus ergeben sich folgende typische Gefahren:

- Bei ausgelagerten Geschäftsprozessen geht intern das entsprechende Know-how verloren.
- Mitarbeiter des Auftraggebers verlassen das Unternehmen oder werden versetzt und nehmen ihr Know-how mit.
- IT-Systeme und Ressourcen werden dem Outsourcing-Dienstleister überlassen, sodass über diese keine vollständige Kontrolle mehr besteht.
- Auftraggeber und Auftragnehmer schätzen den Schutzbedarf der ausgelagerten Informationen unterschiedlich ein, beispielsweise aufgrund von Missverständnissen in der Kommunikation oder einer anderen Sicherheitskultur. Damit können dann die ergriffenen Sicherheitsmaßnahmen unzureichend oder falsch gelagert sein.

Aus einer zu großen Abhängigkeit können sich außerdem folgende Konsequenzen ergeben, die es zu beachten gilt:

- Insourcing ist im Allgemeinen teuer und im Extremfall sogar unmöglich.
- Ein Wechsel des Dienstleisters ist im Allgemeinen schwierig und kann zu existenzbedrohenden Situationen (Verfügbarkeit, Kosten) führen.
- Auf Veränderung der Rahmenbedingungen (zum Beispiel Eigentümerwechsel beim Outsourcing- oder Cloud-Dienstleister, Änderung der Gesetzeslage, Zweifel an der Zuverlässigkeit des Outsourcing- oder Cloud-Dienstleisters) kann unter Umständen nicht angemessen reagiert werden.

Erkennt der Outsourcing- oder Cloud-Dienstleister eine große Abhängigkeit des Auftraggebers, so können sich zudem auch folgende Probleme ergeben:

- Der Dienstleister führt drastische Preiserhöhungen durch.
- Es kommt zu schlechter Dienstleistungsqualität.
- Die Drohung, die Dienstleistung sofort einzustellen, wird als Druckmittel (zum Beispiel bei Kündigung des Vertrages oder bei Streitigkeiten) benutzt.

# G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen

Bei der Kommunikation über öffentliche Netze, insbesondere das Internet, existiert eine Reihe von Gefahren, die aus der Verwendung unsicherer Protokolle entstehen.

Eine wichtige Gefahr ist, dass vertrauliche Informationen in fremde Hände gelangen können. Als unsichere Protokolle müssen insbesondere solche Protokolle gelten, bei denen Informationen im Klartext übertragen werden. Da der Weg der Datenpakete im Internet nicht vorhersagbar ist, können in diesem Fall die übertragenen Informationen an verschiedensten Stellen mitgelesen werden. Besonders kritisch ist dies, wenn es sich um

- Authentisierungsdaten wie Benutzernamen und Passwörter,
- Autorisierungsdaten, beispielsweise Transaktionsnummern beim Electronic Banking oder Electronic Brokerage,
- andere vertrauliche Informationen, beispielsweise in Dokumenten, die per E-Mail verschickt werden, handelt.

Protokolle, bei denen sämtliche Informationen im Klartext übertragen werden, sind beispielsweise

- das Hypertext Transfer Protocol *HTTP*, das bei der Kommunikation zwischen Webbrowsern und Webservern verwendet wird,
- das *TELNET* Protokoll, das noch an einigen Stellen für Remote Logins verwendet wird,
- das File Transfer Protocol *FTP*, das noch häufig für den Zugriff auf Server benutzt wird, die Dateien zum Download bereitstellen,
- das Simple Mail Transfer Protocol *SMTP*, das zur Übertragung von E-Mail verwendet wird,
- die Protokolle *rsh* (Remote Shell), *rlogin* (Remote Login) und andere verwandte Protokolle.

Bei solchen Protokollen können sämtliche übertragenen Informationen auf jedem Rechner, über den eine entsprechende Verbindung läuft, mitgelesen und gegebenenfalls auch verändert werden. Kritisch ist beispielsweise die Übertragung von Kreditkartennummern oder Passwörtern über HTTP-Verbindungen im Internet.

Mittels Password-Sniffings können in einem ersten Schritt Passwörter bei der Übertragung zu einem System abgefangen werden. Dies erlaubt dem Angreifer anschließend auf dieses IT-System zu gelangen, um dann weitere Angriffe lokal auf dem Rechner durchzuführen.

Bei den erwähnten Protokollen (besonders bei *HTTP* oder *TELNET*) drohen auch sogenannte Man-in-the-middle-Angriffe oder Session Hijacking (siehe G 5.89 *Hijacking von Netz-Verbindungen*). Bei dieser Art von Angriffen ist ein Angreifer nicht nur dazu in der Lage, Informationen mitzulesen, sondern kann darüber hinaus aktiv Schaden anrichten, indem laufende Transaktionen verändert werden. Beispielsweise können Preise oder Bestellmengen bei Geschäften über das Internet so verändert werden, dass der Besteller nur die Artikel oder Lieferadresse sieht und bestätigt bekommt, die er eingibt, während der Angreifer eine wesentlich höhere Menge und eine andere Lieferadresse an den Verkäufer schickt.

Neben den erwähnten Protokollen, bei denen sämtliche Informationen im Klartext übertragen werden, existieren auch solche, bei denen zumindest die Über-

tragung der Authentisierungsdaten verschlüsselt erfolgt. Dabei droht jedoch immer noch das Mitlesen der übertragenen Nutzinformation.

# G 2.88 Störung des Betriebsklimas durch ein Outsourcing-Vorhaben

Outsourcing-Vorhaben haben je nach Art und Umfang nicht nur Auswirkungen auf die Geschäftsprozesse, sondern auch auf das Personal innerhalb eines Unternehmens oder einer Behörde. Dabei sind neben den vom Auftraggeber erwarteten Positiveffekten aus Sicht der Arbeitnehmer jedoch auch negative Effekte möglich. **Beispiele** dafür sind:

- Im Outsourcing-Bereich kann es zu einem Stellenabbau und damit verbunden zu Versetzungen oder Kündigungen von Mitarbeitern kommen.
- Durch die Auslagerung von Geschäftsvorfällen werden gewohnte Arbeitsprozesse geändert.
- Vor, während oder nach der Einführung eines Outsourcing-Vorhabens kann es zu hohen Arbeitsbelastungen kommen.
- Durch die Zusammenarbeit mit Mitarbeitern eines Outsourcing-Dienstleisters oder externen Beratern kann es erforderlich sein, dass einzelne Mitarbeiter Kompetenzen und Zuständigkeiten abgeben müssen. Genauso kann sich aber auch ergeben, dass Mitarbeiter neue Zuständigkeiten übernehmen müssen und sich dadurch überfordert fühlen.
- Durch Umstrukturierungen im Zusammenhang mit einem Outsourcing-Vorhaben kann es auch dazu kommen, dass Mitarbeiter den Arbeitgeber wechseln müssen (z. B. Übergang zu einer Tochterfirma oder Übernahme durch den Outsourcing-Dienstleister). Dabei kann der Mitarbeiter auch dazu gezwungen sein, schlechtere Bedingungen zu akzeptieren oder dies zumindest so empfinden.

Durch diese oder ähnlich Veränderungen kann das Betriebsklima nachhaltig gestört werden. Mögliche Gefährdungspotenziale sind unter anderem:

- Mitarbeiter oder ehemalige Mitarbeiter können Racheakte verüben.
- Die Mitarbeiter sind schlecht motiviert und vernachlässigen unabsichtlich oder mutwillig Pflichten, insbesondere Sicherheitsmaßnahmen.
- Know-how-Träger (wie beispielsweise IT-Leiter und Administratoren) können während der Einführungsphase kündigen. In Folge könnte dadurch das Outsourcing-Vorhaben nicht bedarfsgerecht oder gar nicht umgesetzt werden, was wiederum existenzbedrohend sein kann. Oftmals ist der Outsourcing-Dienstleister sogar darauf angewiesen, dass die entscheidenden Know-how-Träger geordnet zu ihm wechseln.

# G 2.89 Mangelhafte Informationssicherheit in der Outsourcing-Einführungsphase

Ein Outsourcing-Vorhaben wird in der Regel in mehreren Schritten umgesetzt. Die Einführungsphase geht meist mit drastischen internen Veränderungen auf Seiten des Auftraggebers einher. Zusätzlich wird ein Outsourcing-Vorhaben von stringenten terminlichen und finanziellen Randbedingungen begleitet. Oft bleibt keine Zeit für regelmäßige Sicherheitskontrollen und Audits. Um Termine und Budgets während der Einführungsphase einzuhalten, leidet oftmals die Arbeitsqualität und Sicherheitskonzepte werden vernachlässigt. Dies hat jedoch gravierenden Einfluss auf die Informationssicherheit. Mögliche weitere Gefährdungen der Informationssicherheit sind unter anderem:

- Der Betrieb von Übergangslösungen erfolgt unter geringen Sicherheitsstandards. Dabei wird häufig argumentiert: "Hauptsache, es läuft!" Oft werden solche Übergangslösungen dann jedoch aus verschiedenen Gründen auf Jahre hin weiterbetrieben.
- Aus Zeit- und Ressourcengründen werden "Altsysteme" vernachlässigt, während an den neuen Systemen gearbeitet wird.

Ausgelöst durch die hohe Arbeitsbelastung und den Zeitdruck werden die Probleme durch bewusste oder unbewusste Nachlässigkeiten oder Fehler verstärkt. Gründe können sein:

- Während der Einführungsphase muss ein Parallelbetrieb der von der Auslagerung betroffenen Systeme erfolgen.
- Durch die Anbindung an den Outsourcing-Dienstleister entstehen viele neue organisatorische und technische Schnittstellen.
- Mitarbeiter müssen in neue Aufgaben eingearbeitet werden, so dass zusätzlich Ressourcen gebunden sind.
- Ein Outsourcing-Vorhaben geht einher mit dem Einsatz neuer Soft- und Hardware. Gefahren resultieren dabei aus fehlerhaften oder gänzlich fehlenden Tests, aus Unerfahrenheit mit neuen Sicherheitsmechanismen, aus Installations- und Administrationsfehlern oder aber aus Softwarefehlern.

Sicherheitsmängel können sich jedoch auch aus organisatorischen Schwächen während der Einführungsphase ergeben. Die Gründe können beispielsweise folgende sein:

- Die Zusammenarbeit zwischen den Mitarbeitern des Auftraggebers und denen des Outsourcing-Dienstleister oder externer Berater funktioniert nicht richtig. Ursachen können etwa Kommunikationsprobleme technischer oder persönlicher Art sein. Da am Anfang auch die Ansprechpartner der Gegenseite noch unbekannt sind, können in dieser Phase außerdem Angriffe über "Social Engineering" besonders leicht erfolgreich sein.
- Entscheidungshierarchien funktionieren noch nicht oder Ansprechpartner und Zuständigkeiten sind noch nicht geklärt oder wechseln häufig. Als Folge werden Entscheidungen gar nicht oder nur sehr zögerlich getroffen. Das führt dann unter Umständen dazu, dass Sicherheitsvorschriften nicht eingehalten, umgangen oder nicht kontrolliert werden.

Diese Gesamtproblematik führte beispielsweise auch für ein namhaftes Finanzinstitut zu Problemen: Während an der Einrichtung eines neuen Webservers gearbeitet wurde, wurde das "Altsystem" nicht mehr ausreichend gewartet und war Ziel eines Angriffes, bei dem Kundendaten kompromittiert wurden. Das Ereignis wurde durch die Medien einem Millionenpublikum bekannt gemacht.

# G 2.90 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister

Diese Gefährdung ist mit der 14. Ergänzungslieferung entfallen. Die Inhalte wurden in G 4.97 *Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister* integriert.

# G 2.91 Fehlerhafte Planung der Migration von Exchange

Microsoft Exchange-Systeme werden in der Praxis häufiger migriert als neu installiert. Um auf eine neue Version des Microsoft Exchange-Servers zu migrieren, wird teilweise vorausgesetzt, auch das Betriebssystem auf eine neuere Version anzuheben.

Neue Betriebssysteme bringen ebenfalls Anforderungen an das bestehende Domänenkonzept und die existierenden Verzeichnisdienste mit. Dazu müssen aus Sicherheitssicht planerische und organisatorische Leistungen erbracht werden, die sorgfältig und grundlegend neu geplant werden müssen.

Folgende Sicherheitsprobleme können bei einer fehlerhaften Planung der Migration auftreten:

- Die Konfigurationen könnten falsch oder inkonsistent abgebildet werden, da dies eine Neukonzeption der bisherigen Infrastruktur umfasst. Weiterhin könnte eine fehlerhafte Anbindung an den Verzeichnisdienst zur Folge haben, dass die Richtlinien und die Access Control Lists (ACL) nicht wirksam sind.
- Durch fehlerhafte Protokolleinstellungen oder sonstige Fehlkonfigurationen kann ein Funktionsausfall ausgelöst werden.
- Unter Umständen wird die Administration des Systems unsachgemäß geplant und die Administrationsgrenzen unklar definiert. Eventuell müssen entsprechende Alt-Konzepte überarbeitet und angepasst werden. Wird für Administratoren die Rechtevergabe falsch geplant, so kann dies zu Sicherheitslücken oder auch zur Behinderung der Administration des Systems führen.
- Die geforderten organisationsweiten Sicherheitsrichtlinien könnten durch eine falsche Planung der Migration der Sicherheitseinstellungen ungenügend umgesetzt werden. Dies betrifft sowohl die Zugriffsmöglichkeiten auf den Server an sich als auch auf die dort gespeicherten Daten.
- Daten und Informationen könnten bei der Migration verloren gehen, besonders wenn das System während der Migrationsphase abstürzt.
- Durch notwendige Nachbesserungen der Konfiguration an den Produktivsystemen könnte sich ein Produktivitätsausfall ergeben.

# G 2.92 Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange

Exchange bietet die Möglichkeit, über einen Browser auf das eigene E-Mail-Konto zuzugreifen. Hierzu werden die Internet Information Services (IIS) verwendet, die fester Bestandteil der Installation von Exchange Server sind.

Wenn diese Funktionalität unsachgemäß geplant und fehlerhaft geregelt wird, kann dadurch ermöglicht werden, unkontrolliert von außen auf das interne Netz zuzugreifen.

Fehlkonfigurationen betreffen in erster Linie die Authentisierung des Webclients gegenüber dem Exchange Server sowie die geschützte Übertragung der Informationen über das Netz. Sind die geforderten Authentisierungsmethoden zu schwach, so können unter Umständen Unbefugte auf E-Mail-Daten und Systemressourcen zugreifen. Sind die eingesetzten Verschlüsselungsmechanismen nicht hinreichend stark, so können Daten abgehört werden. Bei nicht ausreichenden Authentisierungs- und Verschlüsselungsmechanismen können bestehende Verbindungen unter Umständen durch unbefugte Dritte übernommen werden. Weiterhin können über diesen Kanal Viren oder anderer schädlicher Code auf den Exchange Server gelangen.

Das Gefahrenpotential ist darüber hinaus vielfältig. Beispiele für weitere mögliche Folgen sind:

- E-Mail-Adressen und -Inhalte könnten ausgespäht werden.
- Unbefugte könnten Zugriff auf E-Mail-Funktionen erlangen.
- Spam-Angriffe könnten ermöglicht werden.
- Unbefugte könnten interne Informationen über das Unternehmen bzw. die Behörde erlangen.
- Es könnten sich direkte Angriffsmöglichkeiten auf das interne Netz ergeben.

# G 2.93 Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung

Versäumnisse im Bereich der Notfallvorsorge haben beim Outsourcing oder bei der Nutzung von Cloud Services schnell gravierende Folgen. Zusätzliche Schwierigkeiten ergeben sich dadurch, dass Probleme generell auf drei kritische Bereiche verteilt sein können:

- IT-Systeme beim Auftraggeber
- IT-Systeme beim Outsourcing- oder Cloud-Dienstleister
- Schnittstellen (zum Beispiel Netzanbindung, Router, Telekommunikations-Provider) zwischen Auftraggeber und Dienstleister

Im Falle eines Fehlers muss dieser zunächst korrekt lokalisiert werden, was je nach Fehlerart schwierig ist, da unterschiedliche Fehler zu gleichen Symptomen führen können, zum Beispiel Ausfall der Kommunikationsverbindung und Ausfall eines Systems beim Dienstleister. Erst nachdem der Fehler identifiziert worden ist, können sinnvolle Notfallmaßnahmen eingeleitet werden.

Versäumnisse bei den Notfallvorsorgekonzepten für die IT-Systeme von Auftraggeber beziehungsweise Dienstleister sowie der Schnittstellen führen im Falle eines Teil- oder Totalausfalls immer zu unnötig langen Ausfallzeiten mit entsprechenden Folgen für die Produktivität beziehungsweise Dienstleistung des Auftraggebers. Daneben kann die mangelhafte Abstimmung von Notfallszenarien zwischen Auftraggeber und Dienstleister zu Lücken in der Notfallvorsorge führen.

# G 2.94 Unzureichende Planung des IIS-Einsatzes

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 2.95 Fehlendes Konzept zur Anbindung anderer Systeme an Exchange

Die in Institutionen vorhandenen Informationsverbünde sind meist heterogen, sowohl in Bezug auf die verwendeten Betriebssysteme als auch in Bezug auf die Anwendungen. Diese spiegeln häufig die Historie des Wachsens und Zusammenwachsens der Organisationsstruktur im Unternehmen bzw. in der Behörde wider.

Microsoft Exchange-Systeme sind eng mit dem Betriebssystem Microsoft Windows verzahnt und harmonieren nur durch sogenannte Konnektoren mit Fremdsystemen. Da in Microsoft Exchange nicht in jeder Version alle Konnektoren unterstützt werden, ist auch über die Weiterführung bestehender Konnektoren im Rahmen einer Migration nachzudenken (siehe G 2.91 *Fehlerhafte Planung der Migration von Exchange*).

Aus Sicherheitssicht können unter Microsoft Windows Server getroffene Sicherheitseinstellungen, die sich auf das Microsoft Exchange-System beziehen, außerhalb des homogenen Microsoft-Umfeldes keine Gültigkeit haben.

Ebenso können natürlich auch umgekehrt die festgelegten Sicherheitsrichtlinien der Fremdsysteme keine Gültigkeit für das Microsoft Exchange-System haben. Bei der separaten Administration verschiedener Teilsysteme können stets Inkonsistenzen auftreten.

Eine unsachgemäße Anbindung fremder Systeme kann zudem den Verlust von Daten oder eine Blockade des Systems zur Folge haben.

# G 2.96 Veraltete oder falsche Informationen in einem Webangebot

Die Korrektheit und Aktualität der Informationen, die eine Organisation in einem Webangebot veröffentlicht, hat nicht nur Einfluss auf den Erfolg des Webangebots alleine. Werden im Internet falsche Informationen veröffentlicht, so kann das Ansehen der Organisation in der Öffentlichkeit empfindlichen Schaden nehmen.

In manchen Fällen drohen auch finanzielle Verluste oder rechtliche Konsequenzen (beispielsweise Abmahnungen), wenn falsche Informationen veröffentlicht werden. Noch schlimmer können die Auswirkungen sein, wenn irrtümlich interne (vertrauliche oder gar geheime) Informationen auf den Webserver gelangen, die eigentlich gar nicht veröffentlicht werden dürften.

Selbst dann, wenn bestimmte Informationen auf dem Webserver nur veraltet sind, kann dies nachteilige Auswirkungen haben. Wenn beispielsweise veraltete Kontaktinformationen veröffentlicht werden, kann dies zu einer Störung der betroffenen Geschäftsprozesse führen.

**Beispiel:**

- Im Jahr 2002 fanden Reporter auf dem Webserver eines schwedischen Unternehmens eine Datei mit einem Quartalsbericht dieses Unternehmens, der erst einige Tage später hätte veröffentlicht werden sollen. Dies führte unter anderem zu zeitweiligen Kursverlusten der Aktien des Unternehmens.

# G 2.97 Unzureichende Notfallplanung bei einem Apache-Webserver

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 2.98 Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches

Bei der Planung des Einsatzes aktiver Netzkomponenten stehen meistens die Aspekte Funktionalität und Leistungsfähigkeit im Vordergrund. Wenn der Betrieb von Routern und Switches, als zentrale Elemente in Netzen, nicht in das unternehmensweite Sicherheitskonzept eingebunden wird, kann der sichere Einsatz dieser Komponenten nicht sichergestellt werden.

Die Fehler bei der Planung des Einsatzes von Routern und Switches fallen meist in eine der folgenden Kategorien:

**Unzureichende Berücksichtigung des Einsatzzwecks der Geräte**

Bei der Planung des Einsatzes von Routern und Switches ist in erster Linie der Einsatzzweck dieser Komponenten entscheidend. Oft wird der Einsatzzweck der Komponenten bei der Planung nicht ausreichend berücksichtigt, beispielsweise beim Einsatz von VLAN. Entgegen öfters gehörter Werbeaussagen wurden VLANs nicht entwickelt, um Sicherheitsanforderungen bei der Trennung von Netzen zu erfüllen. VLANs bieten eine Vielzahl von Angriffspunkten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind.

Auch bei der Planung des Einsatzes von Routing-Protokollen können Fehler gemacht werden. Wenn Router im Bereich von demilitarisierten Zonen (DMZs) eingesetzt werden kann die Verwendung von dynamischen Routing-Protokollen die Verfügbarkeit, Vertraulichkeit und die Integrität des zu schützenden Netzes gefährden.

**Unzureichende Berücksichtigung von Sicherheitsmechanismen**

Bei der Planung werden oft die vorhandenen Sicherheitsmechanismen (sowohl im bestehenden Netz als auch bei den Netzkomponenten, deren Einsatz geplant wird) nicht ausreichend berücksichtigt. Beispielsweise können zusätzliche Maßnahmen erforderlich werden, falls ein Gerät bestimmte Sicherheitsmechanismen nicht unterstützt. Wenn dies nicht bereits in der Planungsphase berücksichtigt wird, kann es später zu Problemen führen, wenn die Notwendigkeit erkannt wird.

Ein wichtiger Punkt, der beispielsweise bei der Planung oft nicht berücksichtigt wird, ist die Einrichtung eines gesonderten Administrationsnetzes (Out-of-Band Management). Falls die gewählten oder vorhandenen Geräte nur unsichere Protokolle wie SNMPv1, SNMPv2 oder Telnet unterstützen, so ist die Einrichtung eines Administrationsnetzes unbedingt erforderlich. Dies wird in vielen Fällen nicht beachtet, mit der Folge, dass später unter Umständen die Einrichtung des Administrationsnetzes auf Schwierigkeiten stößt, weil die notwendigen Anschlüsse nicht vorhanden sind.

**Fehlende oder mangelhafte Information und Dokumentation**

Gelegentlich sind in der Planungsphase notwendige Informationen nicht vorhanden, da entweder keine entsprechende Dokumentation vom Anbieter zur Verfügung gestellt wurde oder die betreffenden Dokumente nicht berücksichtigt werden. Fehlentscheidungen, die auf Grund mangelhafter Dokumentation gemacht wurden, sind oft nur schwer zu korrigieren, wenn sich beispielsweise

später herausstellt, dass ein Gerät bestimmte Funktionen nicht oder nur unzureichend unterstützt.

# G 2.99 Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung

Das Ressourcenangebot der zSeries-Architektur gestattet den Betrieb mehrerer Produktions- und Testsysteme auf einem physischen Rechner. Daraus resultiert ein hohes Gefahrenpotential, weil eine fehlerhafte Abgrenzung der zSeries-Systemumgebungen unter Umständen den ungewollten Zugriff auf fremde Ressourcen ermöglicht.

**Shared DASD (Direct Access Storage Device)**

- Im LPAR-Betrieb ist es möglich, die Platten eines z/OS-Betriebssystems so zu konfigurieren, dass sie durch alle z/OS-Systeme des Rechners verwendet werden können (durch Konfiguration entsprechender Subchannel-Adressen über den *Host Configuration DefinitionProzess*). Damit verbunden ist die Gefahr, dass die Datentrennung zwischen den LPARs nicht mehr gewährleistet ist.
- Es ist möglich, Platten einer LPAR1 an einer anderen LPAR2 *Online* zu setzen. Die Daten der neuen Platte stehen dann an der LPAR2 zur Verfügung und können entsprechend den RACF-Definitionen dieser LPAR2 bearbeitet werden. Sind die RACF-Definitionen der LPAR2 schwächer als die der LPAR1, können die Daten unter Umständen unbefugt manipuliert oder gelesen werden.

**Unsachgemäße Trennung Test-Produktion**

Sicherheitsprobleme können auch durch eine unsachgemäße Trennung von Test- und Produktionsumgebungen entstehen. Werden Test und Produktion auf unterschiedlichen LPARs (noch besser unterschiedlichen zSeries Systemen) betrieben, ist die Abgrenzung leichter zu realisieren. Der Betrieb von Test und Produktion auf der gleichen LPAR ist prinzipiell möglich (hier sollte auf jeden Fall die Gefährdung G 3.70 *Unzureichender Dateischutz des z/OS-Systems* beachtet werden), jedoch ist die Trennung hierbei ungleich schwieriger. Werden die Umgebungen nicht richtig voneinander abgegrenzt, so ist es möglich, dass Testdaten in die Produktion gelangen bzw. Produktionsdaten zum Testen verwendet werden. Beides beinhaltet ein hohes Gefahrenpotential.

**Beispiel:**

- Ein Outsourcing-Dienstleister betrieb in seinem Rechenzentrum die Anwendungen von zwei konkurrierenden Unternehmen aus dem Bereich der Automobilindustrie auf dem gleichen z/OS-System. Aufgrund einer unsicheren Konfiguration war es dem Kunden B möglich, Platten des Kunden A online zu nehmen. Kunde B nutzte dies aus, um sich durch Ausspähen der Daten Wettbewerbsvorteile gegenüber dem Kunden A zu verschaffen.

# G 2.100 Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen

Internet-Domainnamen (meist einfach "Domains" genannt) können nicht beliebig gewählt werden, sondern müssen bei einem Registrar angemeldet werden. Ein Registrar kann Namen für eine oder mehrere sogenannte "Top-Level-Domains" vergeben (beispielsweise verwaltet die DeNIC GmbH die Top-Level-Domain *.de*). Domains werden nicht "gekauft", sondern nur für einen bestimmten Zeitraum registriert. Ist dieser Zeitraum abgelaufen, muss die Registrierung gegen Zahlung einer Gebühr verlängert werden. Im Zusammenhang mit der Registrierung und dem Verlängern der Registrierung von Domainnamen werden häufig Fehler gemacht, die gegebenenfalls erhebliche Kosten und einen Ansehensverlust der Institutionen zur Folge haben können. Einige dieser Fehler werden im Folgenden kurz erläutert:

**Nichtberücksichtigung "verwandter" Domainnamen**

Oft wird nur der "richtige" Domainname registriert, den die Organisation benutzen möchte, etwa *institutionsname.de*. Dabei wird übersehen, dass "verwandte" Domainnamen wie *institutionsname.com* oder *institutionsname.info* von Internetbenutzern, welche die Domain der Firma nicht kennen, ausprobiert werden.

Es kommt häufig vor, dass "verwandte" Domainnamen von unseriösen Anbietern registriert werden, die unter dem Namen beispielsweise Websites mit einem Konkurrenzangebot betreiben. Zwar können solche Angebote oft gerichtlich untersagt und abgeschaltet werden, da ein solcher Prozess in der Regel längere Zeit dauert, könnte während dessen das Ansehen der Organisation beträchtlichen Schaden nehmen.

Beispielsweise musste eine deutsche Universität im Jahr 2000 gerichtlich gegen einen Pornografieanbieter vorgehen, der den Domainnamen der Universität mit der *.com* Endung benutzte. Im Jahr 2004 gelang es einem Jugendlichen, sich durch Ausnutzung eines Verfahrensfehlers im Registrierungsprozess für kurze Zeit die deutsche Domain eines Online-Auktionshauses übertragen zu lassen. Weiterhin kann ein Betrüger einen "verwandten" Domainnamen dazu benutzen, einen Webauftritt aufzubauen, der dem echten Webauftritt täuschend ähnlich sieht. Solche sogenannten Phishing-Angriffe sollen Besucher dazu verleiten, Zugangsdaten für den echten Webauftritt oder Kreditkarteninformationen für Bezahlvorgänge einzugeben. Die Betrüger benutzen diese Daten, um sich Zugang zum echten Webserver zu verschaffen oder mit den gestohlenen Kreditkarteninformationen einzukaufen.

**Verletzung von Markenrechten**

Bei der Registrierung von Domainnamen wird oft nicht geprüft, ob der gewählte Name registrierte Markennamen anderer Institutionen verletzt. Solche Markenrechtsverletzungen werden meist vom Markeninhaber prompt bemerkt. Die Inhaber oder auf Abmahnungen spezialisierte Anwälte und Organisationen recherchieren regelmäßig nach neuen Domains, die eventuell Markenrechte verletzen, und verschicken kostenpflichtige Abmahnungen. Zusätzlich kann der Inhaber einer Marke gerichtlich die Rückgabe oder Löschung der Domain verlangen. Dies kann erhebliche Kosten und Imageschäden nach sich ziehen.

**Fehler bei der Verlängerung von Domainnamen und beim Wechsel des Registrars**

Die Registrierung eines Domainnamens muss regelmäßig gegen Zahlung einer Verwaltungsgebühr bei einem Registrar "verlängert" werden. Wird die Gebühr nicht rechtzeitig bezahlt, geht das Recht am Domainnamen verloren und andere Organisationen können den Domainnamen registrieren. Ist der betreffende Domainname nicht institutionsspezifisch, gibt es im schlimmsten Fall keine Möglichkeit, die verlorene Domain zurück zu erhalten. Eine derart verwaiste Domain könnte von der Konkurrenz registriert werden oder von einer Organisation, die von dort aus anstößige oder gar illegale Inhalte verbreitet.

Zu einer weiteren Gefährdung kann es führen, wenn unseriöse Registrare Kunden ihrer Konkurrenten anrufen und behaupten, die Registrierung sei abgelaufen und müsste gegen eine erneute Zahlung erneuert werden. Bezahlen die Kunden diese Gebühr, stimmen sie gleichzeitig dem Wechsel zu einem anderen Registrar zu.

Auch ein gewollter Wechsel des Registrars, beispielsweise aufgrund besserer Konditionen, kann zu Problemen führen. Wenn beim Wechsel Fehler auftreten, wird die Registrierung beim bisherigen Registrar aufgelöst, die Neuregistrierung beim zukünftigen Registrar jedoch nicht bzw. zeitverzögert durchgeführt, kann in dieser Zeitspanne die Domain prinzipiell von jedem registriert werden. Der Domainname kann oft nur durch beträchtlichen zeitlichen und finanziellen Aufwand oder gar nicht mehr zurückerlangt werden.

# G 2.101 Unzureichende Notfallvorsorge bei einem Sicherheitsgateway

Eine unzureichende Planung für Notfälle kann Probleme, die beim Betrieb eines Sicherheitsgateways auftreten, wesentlich verschlimmern und Ausfallzeiten verlängern.

Zusätzlich zu allgemeinen Fehlern, die oft im Bereich Notfallvorsorge gemacht werden, können bei einem Sicherheitsgateway einige spezielle Fehler gemacht werden, die eine schnelle Reaktion auf Zwischenfälle sehr erschweren oder gar unmöglich machen können. Einige dieser Fehler werden im folgenden beschrieben.

- Existieren keine Planungen für das Vorgehen bei Notfällen und keine entsprechenden Handlungsanweisungen, so ist eine effiziente Reaktion meist überhaupt nicht möglich. Bei komplexen Systemen wie mehrstufigen Sicherheitsgateways kann es zu zusätzlichen Problemen kommen, wenn Abhängigkeiten zwischen einzelnen Komponenten nicht bekannt oder nicht dokumentiert sind, oder wenn sie bei der Planung nicht korrekt berücksichtigt werden.
- Sind für wichtige Hardwarekomponenten keine Austauschteile beziehungsweise -geräte verfügbar und sind mit den Herstellern oder Lieferanten keine entsprechenden Vereinbarungen (beispielsweise Service-Level-Agreements oder Vor-Ort-Austausch innerhalb eines garantierten Zeitraums) getroffen, so kann dies zu erheblichen Ausfallzeiten und Kosten führen.
- Existiert keine oder nur eine unzureichende Dokumentation der Konfiguration und der wichtigsten Betriebsparameter, so kann es sehr schwierig sein, nach einem Notfall überhaupt wieder eine funktionierende Konfiguration herzustellen. Schlechte Dokumentation kann auch dazu führen, dass Konfigurationsfehler zunächst nicht entdeckt werden und bei auftretenden Problemen eine aufwendige Fehlersuche erforderlich wird.
- Sind die für eine Fehlerdiagnose benötigten Werkzeuge und Programme nicht verfügbar oder sind die Administratoren nicht in der Lage, diese richtig einzusetzen, so kann dies zu erheblichen Verzögerungen führen.
- Werden wichtige Daten bei der Protokollierung nicht erfasst, so kann dies die korrekte Einschätzung von Art und Schwere eines Vorfalls erschweren oder unmöglich machen.
- Bei der Systemwiederherstellung nach einem Notfall kann es wünschenswert sein, einen älteren Stand der Konfiguration wieder herzustellen. Wird für die Konfigurationsdaten (insbesondere die Paketfilterregeln) keine Versionsverwaltung durchgeführt, so kann dies schwierig oder gar unmöglich sein.

# G 2.102 Unzureichende Sensibilisierung für Informationssicherheit

Die Aktivitäten zur Sensibilisierung für Fragen der Informationssicherheit müssen sich an den Geschäftsprozessen und der IT-Umgebung der jeweiligen Institution orientieren, um auch die richtigen Bereiche zu adressieren. Dadurch muss unter Umständen eine Vielzahl von Themengebieten angesprochen werden. Hierfür müssen die Schulungsaktivitäten sorgfältig geplant und organisiert werden. Die Erfahrung zeigt, dass es nicht genügt, lediglich die Umsetzung von bestimmten Sensibilisierungsmaßnahmen anzuordnen. Folgende Fallstricke erschweren häufig eine nachhaltige Sensibilisierung:

- Es fehlt Unterstützung durch das Management der verschiedenen Ebenen, was dazu führen kann, dass
  - Mitarbeiter von verschiedenen Bereichen für Schulungen zur Informationssicherheit nicht freigestellt werden,
  - die Teilnahme weder seitens der Mitarbeiter noch seitens der Vorgesetzte ernst genommen wird, da auch die Vorgesetzten die Bedeutung von Informationssicherheit für den Organisationserfolg nicht kommunizieren oder sogar Informationssicherheit als unwesentlich abtun.
- Die Planung der Sensibilisierungsmaßnahmen ist mangelhaft.
- Das Ziel des Sensibilisierungsprogramms ist nicht oder unklar definiert.
- Es findet keine Erfolgskontrolle statt. Wenn aber Erfolgsmeldungen und generelle Rückmeldungen über die Aktivitäten zur Sensibilisierung fehlen, entzieht das Management schnell die Unterstützung oder priorisiert solche Projekte niedriger.
- Es werden nur einzelne Aktionen und Schulungen zur Informationssicherheit durchgeführt. Wenn diese nicht in Zusammenhang mit anderen Sicherheitsmaßnahmen stehen, können diese unter Umständen mehr Schaden als Nutzen anrichten. Beispielsweise können Mitarbeiter hierdurch verwirrt oder demotiviert werden.
- Es werden zu wenige finanzielle oder personelle Ressourcen zur Durchführung von Kampagnen zur Informationssicherheit zur Verfügung gestellt. Häufig werden teure Sicherheitskomponenten angeschafft oder mit hohem Aufwand Sicherheitskonzeptionen erarbeitet, ohne dass die Benutzer in deren Anwendung bzw. Umsetzung geschult werden. Dadurch können auch gut durchdachte Sicherheitslösungen sinnlos werden.

# G 2.103 Unzureichende Schulung der Mitarbeiter

IT-Benutzer aller Art werden häufig zu wenig in der Bedienung der von ihnen eingesetzten IT-Systeme geschult. Dies trifft leider sogar öfters auf Administratoren und Benutzerbetreuer zu. Vielfach werden teure Systeme und Anwendungen angeschafft, aber keine oder nur unzureichend Mittel für die Schulung der IT-Benutzer bereitgestellt.

Dies kann durch unabsichtliche Fehlbedienungen, falsche Konfiguration und ungeeignete Betriebsmittel zu gravierenden Sicherheitsproblemen führen. Häufig wenden Benutzer neu eingeführte Sicherheitsprogramme deswegen nicht an, weil sie nicht wissen, wie sie bedient werden und eine selbstständige Einarbeitung oft als zu zeitaufwendig im täglichen Arbeitsablauf gesehen wird. Daher reicht die Beschaffung und Installation einer Sicherheitssoftware noch lange nicht aus.

**Beispiele:**

- Während der Datenerfassung erschien eine dem Benutzer nicht bekannte Fehlermeldung. Da bei den meisten Fehlermeldungen das Anklicken von "ok" bisher keinen Schaden verursachte, wählte er an diesem Fall auch "ok". Nur diesmal bewirkte dies das Herunterfahren des Systems und folglich den Verlust der bis dahin eingegebenen Daten.
- Ein teures Firewall-System wurde beschafft. Der Administrator eines anderen IT-Systems wurde "durch Handauflegen" zum Administrator dieses Firewall-Systems bestimmt. Da er als unabkömmlich galt und alle verfügbaren Mittel für die System-Beschaffung verwendet worden waren, wurde er aber weder in der Bedienung der System-Plattform noch für den eingesetzten Firewall-Typ ausgebildet. Externe Seminare wurden aus Geldmangel verweigert, nicht einmal zusätzliche Handbücher angeschafft. Zwei Monate nach Inbetriebnahme des Firewall-Systems stellte sich heraus, dass durch eine Fehlkonfiguration der Firewall interne Systeme aus dem Internet frei zugänglich waren.
- In einem Unternehmen wurde die Migration auf ein neues Betriebssystem vorbereitet. Der dafür verantwortliche Mitarbeiter war zwar ein ausgezeichneter Kenner der bis dahin eingesetzten Plattform, kannte sich aber mit den diskutierten neuen Systemen nicht aus und erhielt auch keine dem entsprechende Schulung. Daher besuchte er einige kostenfreie Veranstaltungen eines Herstellers, dessen Produkte er auch danach favorisierte. Dies führte zu einer kostenintensiven Fehlentscheidung durch Einführung eines ungeeigneten Produktes.
- Für die Internet-Nutzung während der Dienstreisen wurden auf den Notebooks der Mitarbeiter Personal Firewalls installiert. Die Mitarbeiter wurden nicht dazu geschult, eine Abstimmung der Einstellungen der Firewall mit den Bedürfnissen der Mitarbeiter fand nicht statt. Viele Mitarbeiter haben daraufhin die Firewall abgeschaltet, um problemlos alle Internet-Seiten zu erreichen, die sie brauchten. Das Ergebnis war, dass schon nach einigen Wochen viele der Rechner mit Schadprogrammen verseucht waren. Neben dem Datenverlust war der Ansehensschaden erheblich, da sich ein Schadprogramm über Mails an Kunden weitergesendet hatte.

# G 2.104 Inkompatibilität zwischen fremder und eigener IT

Bei der zunehmenden Mobilität von IT-Systemen und IT-Benutzern tritt häufiger das Problem auf, dass sich IT-Systeme aufgrund von Inkompatibilität nicht wie geplant nutzen lassen. Dies ist natürlich ärgerlich, wenn IT-Geräte extra mitgenommen wurden, sich aber nicht nutzen lassen. Darüber hinaus können Versuche, die IT-Systeme doch zu verbinden, zu Schäden an den Geräten oder den gespeicherten Daten führen.

**Beispiele:**

- Ein Laptop ist mit allen wichtigen Daten für ein Kundengespräch vorbereitet worden. Dieser lässt sich aber beim Kunden nicht mit der dortigen IT koppeln und auch die Daten können wegen unterschiedlicher Schnittstellen nicht auf einen anderen Rechner dort transferiert werden. Dadurch sind die Aufwände und Bemühungen, die in die Vorbereitungen des Gesprächs gesteckt wurden, vergebens.
- Beim Versuch, zwischen zwei IT-Systemen Daten auszutauschen, wird ein Treiber-Problem gemeldet. Auf Anraten eines anderen Besprechungsteilnehmers wird auf dem einem IT-System ein neuer Treiber installiert. Dies führt dazu, dass sich das System nicht mehr starten lässt.

# G 2.105 Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind (beispielsweise durch ein unzureichendes Sicherheitsmanagement), kann dies zu Verstößen gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern führen. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution beziehungsweise ihrer Geschäftsprozesse und Dienstleistungen ab. Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale und internationale Vorschriften zu beachten sein. Verfügt eine Institution über unzureichende Kenntnisse hinsichtlich internationaler Gesetzesvorgaben (zum Beispiel Datenschutz, Informationspflicht, Insolvenzrecht, Haftung oder Informationszugriff für Dritte), erhöht dies das Risiko entsprechender Verstöße. Es drohen rechtliche Konsequenzen.

Folgende Beispiele verdeutlichen mögliche Ausprägungen:

- Der Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt. Dazu gehören das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze, aber auch eine Vielzahl branchenspezifischer Regelungen. Werden bei der Kommunikation zwischen zwei Geschäftsbereichen personenbezogene Daten (zum Beispiel vertrauliche Patientendaten) ungeschützt über öffentliche Netze übertragen, kann dies unter Umständen rechtliche Konsequenzen nach sich ziehen.
- Die Geschäftsführung eines Unternehmens ist dazu verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Hierzu gehört auch die Beachtung anerkannter Sicherheitsmaßnahmen. In Deutschland gelten verschiedene Rechtsvorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), GmbHG (Gesetz betreffend die Gesellschaften mit beschränkter Haftung) oder AktG (Aktiengesetz), aus denen sich zu Risikomanagement und Informationssicherheit Handlungs- und Haftungsverpflichtungen der Geschäftsführung beziehungsweise des Vorstands eines Unternehmens ableiten lassen.
- Die ordnungsmäßige Verarbeitung von buchungsrelevanten Daten ist in verschiedenen Gesetzen und Vorschriften geregelt. In Deutschland sind dies unter anderem das Handelsgesetzbuch (zum Beispiel HGB §§ 238 ff.) und die Abgabenordnung (AO). Die ordnungsmäßige Verarbeitung von Informationen umfasst natürlich deren sichere Verarbeitung. Beides muss in vielen Ländern regelmäßig nachgewiesen werden, beispielsweise durch Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses. Falls hierbei gravierende Sicherheitsmängel festgestellt werden, kann kein positiver Prüfungsbericht erstellt werden.
- In vielen Branchen (zum Beispiel der Automobil-Industrie) ist es üblich, dass Hersteller ihre Zulieferer zur Einhaltung bestimmter Qualitäts- und Sicherheitsstandards verpflichten. In diesem Zusammenhang werden zunehmend auch Anforderungen an die Informationssicherheit gestellt. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, aber auch Vertragsauflösungen bis hin zum Verlust von Geschäftsbeziehungen nach sich ziehen.
- Um Skaleneffekte zu erzielen, bieten viele Cloud-Dienstleister ihre Services in einem internationalen Umfeld an. Damit unterliegen die Anbieter oft anderen nationalen Gesetzgebungen. Für den Cloud-Anwender ist

es oft sehr schwierig, die einschlägigen Gesetze und Verordnungen (zum Beispiel Datenschutz, Informationspflicht, Insolvenzrecht, Haftung, Informationszugriff für Dritte) zu kennen und richtig zu bewerten.
- Cloud-Diensteanbieter geben unzureichend Auskunft über den Speicherort der Daten. So ist nicht klar, welche staatlichen Stellen auf die Informationen zugreifen können.

Nur wenige Sicherheitsanforderungen ergeben sich unmittelbar aus Gesetzen. Die Gesetzgebung orientiert sich jedoch im Allgemeinen am Stand der Technik als allgemeine Bewertungsgrundlage für den Grad der erreichbaren Sicherheit. Stehen bei einer Institution die vorhandenen Sicherheitsmaßnahmen in keinem gesunden Verhältnis zu den zu schützenden Werten und dem Stand der Technik, kann dies gravierende Folgen haben.

# G 2.106 Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen

Sicherheitsvorfälle können durch ein singuläres Ereignis oder eine Verkettung unglücklicher Umstände ausgelöst werden und dazu führen, dass Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und IT-Systemen beeinträchtigt werden. Dies wirkt sich dann schnell negativ auf wesentliche Fachaufgaben und Geschäftsprozesse der betroffenen Institution aus. Auch wenn nicht alle Sicherheitsvorfälle in der Öffentlichkeit bekannt werden, können sie trotzdem zu negativen Auswirkungen in den Beziehungen zu Geschäftspartnern und Kunden führen. Dabei ist es nicht einmal so, dass die beträchtlichsten und weitreichendsten Sicherheitsvorfälle durch die größten Sicherheitsschwachstellen ausgelöst wurden. In vielen Fällen hat die Verkettung kleiner Ursachen zu riesigen Schäden geführt.

**Beispiele:**

- Ein Computerproblem führte dazu, dass an allen US-amerikanischen Flughäfen für mehr als zwei Stunden von zwei Fluglinien keine Maschinen starten konnten. Als Ursache wurde eine Fehlfunktion in einer Datenbank genannt, die laufende Informationen über die anstehenden Flüge bereitstellt. Als Folge konnten hunderte Flüge nicht starten, auch im Anschluss gab es massive Verspätungen, mehrere Tausend Passagiere saßen fest.
- Fehlende Plausibilitätskontrollen führen immer wieder dazu, dass kleine Fehler in Benutzereingaben erhebliche Auswirkungen nach sich ziehen. So brach an der Londoner Börse der FTSE-Index um 200 Punkte ein, nachdem ein Broker versehentlich eine Null zuviel an eine Order gehängt hatte.
  Bei einer Hotelkette wurde statt dessen eine Null bei der Eingabe in die Angebotsdatenbank vergessen, was dazu führte, dass Luxusappartements im Südpazifik für ein Zehntel des eigentlichen Preises angeboten wurden.
- Nach einem fehlgeschlagenen Software-Update war bei einem großen Unternehmen das Netz für mehr als 16 Stunden nicht mehr verfügbar. Dadurch konnten 5000 Mitarbeiter nicht ihren normalen Tätigkeiten nachgehen und 1700 Kundenanfragen nicht bearbeitet werden. Wichtige Termine konnten dadurch nicht eingehalten werden. Neben der ohnehin hohen Belastung für die Administration fielen zusätzlich 6000 Anfragen an den Benutzersupport an.

# G 2.107 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Informationssicherheit ist eine Voraussetzung dafür, dass alle Geschäftsprozesse und Abläufe in einer Institution einwandfrei funktionieren. Gleichzeitig ist aber aufgrund der Vielfältigkeit dieses Themas eine absolute Informationssicherheit praktisch nicht erreichbar. Aus diesem Grund ist es essenziell, beim Sicherheitsmanagement die richtigen Prioritäten zu setzen und an denjenigen Stellen zu investieren, die den größten Mehrwert für die Institution bringen. Dies ist eine Entscheidung, die nur mit Hilfe eines institutionsübergreifenden Sicherheitsmanagements getroffen werden kann.

Mit Hilfe des Sicherheitsmanagements werden die tatsächlichen Sicherheitsanforderungen der Institution festgelegt und die Risiken bei ihrer Nichteinhaltung betrachtet. Auf dieser Basis muss entschieden werden, ob

- Ressourcen in Schutzmaßnahmen investiert werden,
- durch Umstrukturierung oder Verlagerung von Aufgaben sich der Aufwand für den Schutz auf ein vertretbares Maß reduziert,
- Risiken akzeptiert werden.

Diese Überlegungen sind für das Vorgehen in Bezug auf Informationssicherheit grundlegend und müssen in entsprechenden Dokumentationen festgehalten werden. Fehlendes oder unzureichendes Sicherheitsmanagement kann dementsprechend zu folgenden Fehlern führen:

- Oft wird in teure Sicherheitslösungen investiert, ohne dass eine Basis an notwendigen organisatorischen Regelungen vorhanden ist. Nicht geklärte Zuständigkeiten und Verantwortlichkeiten können trotz teurer Investitionen zu schweren Sicherheitsvorfällen führen.
  **Vorfall aus der Praxis:** In einem Unternehmen wurde eine teure Firewall beschafft, jedoch die Administratoren nur unzureichend geschult und Verantwortlichkeiten nicht klar zugewiesen. Aufgrund dessen wurde die Firewall nicht sicher und für die Sicherheitsbedürfnisse des Unternehmens angemessen konfiguriert. Es kam zu Sicherheitsvorfällen, da immer wieder Dienste durch unterschiedliche Administratoren freigeschaltet wurden und bestimmte Funktionalitäten weitgehend ungenutzt blieben.
- Häufig wird in den Bereichen einer Institution in Informationssicherheit investiert, die entsprechende Mittel zur Verfügung haben und deren Verantwortliche für Informationssicherheit besonders sensibilisiert sind. Andere Bereiche, die vielleicht für die Erfüllung der Fachaufgaben und der Erreichung der Geschäftsziele wichtiger sind, werden aufgrund von knappen Mitteln oder Desinteresse der Verantwortlichen vernachlässigt.
  **Vorfall aus der Praxis:** Um die Verfügbarkeit der Anwendung "Buchhaltung" zu erhöhen, wurde ein teures Cluster-System angeschafft. Die für den Kundendienst notwendigen Anwendungen laufen dagegen aufgrund von knappen finanziellen Mitteln in dem Bereich immer noch auf einem alten Server, der jederzeit ausfallen könnte. Die Verfügbarkeit der Kundendienst-Anwendung ist für das Unternehmen sehr wichtig, aufgrund von fehlender Prioritätensetzung bei der Mittelvergabe jedoch nicht berücksichtigt worden.
- Bei Investitionen in einzelnen Teilbereichen ist es erforderlich, das gesamte Sicherheitskonzept zu betrachten.

**Vorfall aus der Praxis:** Eine Abteilung wird mit einer neuen Sicherheitslösung ausgerüstet. Die Stromversorgung bleibt jedoch weiterhin mit einer alten und lange nicht getesteten USV sehr schlecht gesichert. Im Gesamtsystem verbleiben dadurch weiterhin erhebliche Sicherheitslücken.

- Durch die einseitige Erhöhung des Schutzes einzelner Grundwerte kann sich der Gesamtschutz verringern.
  **Vorfall aus der Praxis:** Durch den Einsatz einer hochwertigen Verschlüsselungsroutine bei der Rechnungserstellung wird die Geschwindigkeit der Arbeitsabläufe stark beeinträchtigt. Bei der Auswahl wurde nicht berücksichtigt, dass die Verfügbarkeit der Systeme mindestens genauso wichtig wie ihre Vertraulichkeit ist.
- Ein inhomogener und unkoordinierter Einsatz von IT-Produkten kann zu hohem finanziellen und personellen Ressourceneinsatz führen.
  **Vorfall aus der Praxis:** In einem großen Unternehmen beschäftigten sich mehrere Bereiche unabhängig voneinander mit Informationssicherheit. Es stellte sich heraus, dass zwei Bereiche unabhängig voneinander jeweils Firmenlizenzen eines Viren-Suchprogramms eingekauft hatten. Zusätzlich fanden sich im gesamten Unternehmen verschiedene Verschlüsselungsprodukte für den selben Einsatzzweck. Dies führte zu Problemen bei der Administration und zu einer erhöhten Fehleranfälligkeit.

# G 2.108 Fehlende oder unzureichende Planung des SAP Einsatzes

Wird ein SAP System ohne ausreichende Planung eingesetzt, so kann dies zu einer Vielzahl von Problemen führen. Unter anderem kommt es dabei immer auch zu Sicherheitsproblemen. Im Folgenden sind nur einige Probleme dargestellt, die jedoch deutlich machen, dass eine gute Planung vor dem Einsatz eines SAP Systems notwendig ist:

- In einem mittelständischen Unternehmen soll ein SAP System eingeführt werden. Es wurde sich für eine Installation auf einem Rechner entschieden (Single-Host-Installation). Aus Zeitgründen wurde keine Ressourcen-Planung durchgeführt. Aus Kostengründen wurde ein Rechner aus einer Sonderaktion eines Computerherstellers beschafft. Nach der Installation zeigt sich, dass der Rechner mit zu wenig Hauptspeicher ausgerüstet ist und aufgrund von Hardwarebeschränkungen auch nicht mit viel mehr Speicher bestückt werden kann. Durch die Notwendigkeit, neue, geeignete Hardware zu beschaffen, entstehen Verzögerungen und erhebliche Mehrkosten.
- Durch fehlende Planung der Aufgabentrennung im Rahmen des Administrationskonzeptes kann ein Administrator auf alle HR-Daten eines R/3 Systems zugreifen.
- Die Zuständigkeiten und Abläufe für das Änderungsmanagement und das Notfallkonzept eines SAP Systems wurden nicht geplant. Daher haben Entwickler vollen Zugriff auf das Produktivsystem, da der Zugriff für "Notreparaturen unbedingt erforderlich ist". Ein Zugriff auf alle Konten- und Kreditkarten-Daten der Unternehmenskunden ist somit möglich.
- Besitzen Personen Entwickler-Zugriffsmöglichkeiten auf produktive SAP Systeme (diese werden über das Berechtigungsobjekt S_DEVELOP vergeben), so können diese Personen die Sicherheitsmechanismen des SAP Systems unterlaufen und unberechtigt auf Funktionen und Daten zugreifen.
- Können Transaktionen eines SAP Systems unberechtigt aufgerufen werden, so kann dies weitreichende Folgen haben. In der Regel kann dann auf Funktionen und Daten zugegriffen werden, die dem Zugreifer nicht verfügbar sein sollen. Sind administrative Transaktionen betroffen, kann die Systemsicherheit unter Umständen vollständig unterlaufen werden.
- Bestehen für einen Angreifer Zugriffsmöglichkeiten auf der Betriebssystem-Ebene eines SAP Systems, so kann der Angreifer in die Konfiguration des SAP Systems eingreifen. So ist beispielsweise der Zugriff auf die Profil-Parameter möglich, durch die unter anderem auch die Zugriffsbarrieren reduziert werden können (z. B. Kontosperr-Einstellungen). Für den Java-Stack kann auf Konfigurationsdateien zugegriffen werden, die dann modifiziert werden können. Dadurch kann die Sicherheit drastisch reduziert sein. Ist der Rechner, auf dem die Datenbank des SAP Systems läuft, betroffen, können die Datenbankinhalte auch sehr einfach durch Datei-Kopien erlangt werden. Die Sicherheitsmechanismen des SAP Systems werden damit unterlaufen.
- Standardinstallationen sind in der Regel nicht sofort auf die Sicherheitsanforderungen eines Produktivbetriebs ausgelegt. Werden Komponenten mit Standardkonfiguration dennoch produktiv betrieben, so ist die Gefahr groß, dass die System- und Datensicherheit gefährdet ist. Angriffsmöglichkeiten können durch verschiedene unkonfigurierte Schnittstellen entstehen und reichen von unberechtigtem Zugriff auf Funktionen und Daten bis hin zu Durchgriffen auf das Betriebssystem unter den Berechtigungen des SAP Systems.

- Werden die (öffentlich bekannten) Standardpasswörter wichtiger Benutzer wie "SAP*" oder "DDIC" im ABAP-Stack oder "Administrator" oder "System" im Java-Stack nicht verändert, so können Angreifer Administrator-Zugriffmöglichkeiten erlangen. Damit kann ein Angreifer auf alle Daten des SAP Systems zugreifen und administrative Funktionen ausführen.
- Wird ein SAP System ausgesondert und dessen Identität (IP, SID) nicht durch ein Ersatzsystem übernommen, so kann die unvollständige Aussonderung dazu führen, dass Angreifer ein eigenes SAP System aufsetzen, das die Identität des ausgesonderten Systems übernimmt. Zugriffe anderer SAP Systeme über bestehende Destinationen werden dann vom Angreifersystem akzeptiert. Damit können dort Daten abgerufen und auch gespeichert werden. Diese enthalten auch Authentisierungsinformationen, die für den Anmeldeprozess benötigt werden. Oft werden technische Benutzer in mehreren Systemen gleichartig verwendet, so dass dadurch auch Zugriffsmöglichkeiten auf andere Systeme bestehen können.
- Ist für ein SAP System die HTTP-basierte RFC-SOAP-Schnittstelle aktiviert (ABAP-ICF-Dienst oder JAVA-Stack-SOAP-Dienst), so können Benutzer RFC-fähige Bausteine über die HTTP-Schnittstelle aufrufen. In der Regel ist dies in Szenarien, in denen der SAP System-Zugriff über einen Browser erfolgt, nicht gewünscht. Dennoch können in diesem Fall RFC-Aufrufe durchgeführt werden, so dass je nach Berechtigungseinstellung auch unberechtigte Zugriffe auf Daten ermöglicht werden.
- Werden wichtige Systemereignisse nicht protokolliert oder die Protokolleinträge nicht ausgewertet, so können Angriffe oder Sicherheitsverletzungen nicht erkannt werden. Erfolgreichen Angriffen kann nicht begegnet oder nachgegangen werden. Daher kann unbemerkt ein unberechtigter Zugriff auf Daten oder Funktionen bestehen.

# G 2.109 Fehlende oder unzureichende Planung der Speicherlösung

Der Betrieb von Speicherlösungen erfordert sorgfältige Planung, Installation und Konfiguration, um einen störungsfreien Einsatz gewährleisten zu können. Mögliche Gefährdungen aufgrund fehlender oder unzureichender Planung können in folgenden Aspekten Ausdruck finden:

- Die Anforderungen einer Institution hinsichtlich des benötigten Speicherplatzes, ausreichender Performance sowie der Verfügbarkeit eingesetzter Speicherlösungen steigen stetig. Bei unzureichender Dimensionierung der eingesetzten Speicherlösung kann diesen wachsenden Anforderungen nicht in jedem Fall entsprochen werden.
  **Beispiel:** Je nach Anwendungsanforderung ist die bereitgestellte I/O-Performance auf den Platten ein limitierender Faktor für das Gesamtsystem.
- Die Gründe für eine unzureichende Dimensionierung bei der Planung von Speicherlösungen liegen in der Regel in einer fehlenden Ist-Analyse. Auch die fehlende oder unzureichende Trendanalyse bzw. Prognose bezüglich zukünftiger Entwicklungen innerhalb des eigenen IT-Verbundes trägt unter Umständen zum Einsatz falsch dimensionierter Speicherlösungen bei.
- In virtuellen Speicherumgebungen bietet das sogenannte Thin Provisioning die Möglichkeit, ein kostensparendes Verfahren zur Bereitstellung von Speicherkapazität einzusetzen. Thin Provisioning macht sich zunutze, dass moderne Speicherlösungen virtuelle Festplatten zur Verfügung stellen, deren Kapazität nach außen größer erscheint als physisch vorhanden. Überschreitet die vom Server physisch genutzte Kapazität einen bestimmten Schwellenwert, wird aus einem vorhandenen Speicherpool zusätzlich freie Kapazität für den Abnehmer bereitgestellt. Ist der Schwellenwert aufgrund unzureichender Planung etwa zu niedrig ausgelegt oder wird dieser von vielen Abnehmern innerhalb eines kurzen Zeitraums überschritten, kann dies zu einer Überbuchung der insgesamt verfügbaren Speicherkapazitäten führen.
- Ein falsch gewähltes SAN-Design kann als Folge mangelnder oder unzureichender Planung der Speicherlösung eine Gefährdung für die Institution darstellen. Fehlende SAN-Ports, schlechte Leitungskapazität durch zu hohe Dämpfung, fehlende Inter-Switch-Link-Verbindungen (ISL-Verbindungen) sowie eine unzureichende Lastverteilung an den SAN-Switchen können einen reibungslosen Betrieb verhindern und beispielsweise die Verletzung vertraglicher Vereinbarungen und somit finanzielle Schäden mit sich bringen.
- Im Falle der Notwendigkeit zum Aufbau und Betrieb einer hochverfügbaren Speicherlösung sollte das Hauptaugenmerk auf eine sorgfältige und ausführliche Planung gelegt werden. Vorrangiges Ziel ist die Vermeidung von sogenannten Single Points of Failure (SPOF), also der Abhängigkeit einer an sich redundant ausgelegten Infrastruktur von der Funktion einer einzelnen Komponente.
- Die Anforderungen einer Anwendung an deren Performance sowie Interoperabilitätsanforderungen bezüglich der vorhandenen Hard- und Software können den Einsatz von bestimmten Produkten erzwingen. Wenn diese Aspekte nicht rechtzeitig in der Planung berücksichtigt werden, kann dies teure und ineffiziente Korrekturen während der Realisierung, Verzögerungen im Einsatz oder erhebliche Störungen im Betrieb als Folge haben.
- Die fehlende Mandantenfähigkeit der gewählten Speicherlösung kann unter Umständen ebenfalls eine Gefährdung für die Institution darstellen. In vielen Institutionen ist die IT heute Dienstleister und stellt (internen) Kunden Speicherplatz zur Verfügung. Damit besteht insbesondere auch die

Notwendigkeit zur Berücksichtigung des unterschiedlichen Schutzbedarfes für die zu speichernden Daten dieser (internen) Kunden, also beispielsweise für einzelne Unternehmensbereiche.

- Eine fehlende oder unzureichende Sicherheitskonzeption sowie die fehlende oder unzureichende Dokumentation können ebenfalls Folgen mangelnder Planung sein.

# G 2.110 Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken

Alle organisatorischen Schritte vor und während eines Versionswechsels des Datenbankmanagementsystems (DBMS) oder einer Datenbankmigration werden in Migrations- und Versionskonzepten festgehalten. Das Fehlen solcher Konzepte kann die Aufgabenerledigung erheblich beeinträchtigen, wenn bei einer Datenbankmigration oder einem DBMS-Upgrade Probleme auftreten und das DBMS oder einzelne Datenbanken unvorhergesehen nicht zur Verfügung stehen.

Werden neben der Planung der physischen und semantischen Datenmigration keine sicheren Rückfallpositionen festgelegt, kann die Arbeitsfähigkeit der Datenbank bzw. des DBMS für Benutzer und Anwendungen gefährdet werden.

Bei einem DBMS-Versionswechsel bleiben die im DBMS abgelegten Datenbanken unverändert. Sicherheitsprobleme können hier weniger in der Datenbank selbst als im Zusammenspiel der Datenbanken mit dem neuen DBMS entstehen.

**Beispiele:**
- Durch ein Datenbank-Upgrade wurden Grunddefinitionen in den Typen geändert.
- Zugriffsberechtigungen für standardmäßig vom DBMS bereitgestellte Benutzergruppen sind geändert und beeinflussen damit die Rechte daraus abgeleiteter Benutzergruppen.

Bei einer Datenmigration werden Daten aus einer Datenbank in eine andere Datenbank überspielt. Dabei können die Daten in jeglicher Art konvertiert und in neue Strukturen einer Datenbank auf einem eventuell völlig anderen DBMS übertragen werden. Hier ist zu beachten, dass Datenbanken zur Sicherstellung der Datenkonsistenz unterschiedliche Konstrukte (Trigger, Constraints, etc.) benutzen können. Über solche Konstrukte werden Reihenfolgen und Abhängigkeiten innerhalb der Daten implementiert, die bei Datenmigrationen berücksichtigt und entsprechend nachgebildet werden müssen. Die Analyse und Nachbildung aller einzuhaltenden Bedingungen kann sehr aufwendig und umfangreich sein. Dadurch besteht die Gefahr, dass sich Fehler einschleichen, die die Datenkonsistenz und die Funktionalität nach der Migration gefährden.

**Beispiele:**
- Bei einer Datenbank-Migration von Microsoft Access auf den Microsoft SQL-Server müssen in Access vorhandene Spalten vom Typ *AutoWert* gesondert beachtet werden, da dieser Typ auf verschiedenen DBMS unterschiedlich implementiert ist.
- In der zu migrierenden Datenbank existieren die zwei Tabellen MITARBEITER und FIRMA. Um sicherzustellen, dass neue Mitarbeiter nur existierenden Firmen zugeordnet werden können, wird der Tabelle MITARBEITER ein UPDATE/INSERT-Trigger zugeordnet, der vor Neueinträgen und/oder Veränderungen in der Tabelle MITARBEITER prüft, ob es in der Tabelle FIRMA einen korrespondierenden Eintrag gibt.

Sollte es keinen entsprechenden Eintrag in der Tabelle FIRMA geben, wird die UPDATE- oder INSERT-Anweisung abgebrochen. Die in dieser DB implementierte Reihenfolge (umgangssprachlich: "Zuerst Firma, dann erst Mitarbeiter") muss bei der Migration der Datenbank beachtet werden. Sollte im

Migrationslauf die Tabelle MITARBEITER vor der Tabelle FIRMA übertragen werden, so wird die Einfügung verweigert, da noch keine korrespondierenden Einträge in der Tabelle FIRMA existieren.

# G 2.111 Kompromittierung von Anmeldedaten bei Dienstleisterwechsel

Wenn ein IT-Dienstleister gewechselt wird, müssen hierfür typischerweise diverse Anmeldedaten geändert werden. Dies führt dann zu vielfältiger Kommunikation von alten und neuen Anmeldedaten. Werden diese Daten unsicher ausgetauscht, besteht das Risiko, dass die Vertraulichkeit der Anmeldedaten und mittelbar die Integrität der IT-Umgebung beeinträchtigt wird.

Bei den vom Dienstleister verwendeten Anmeldekonten handelt es sich meistens um solche mit weitgehenden Berechtigungen im betrachteten Informationsverbund. Normalerweise sollten alle Kennwörter niemandem außer dem zugehörigen Benutzer bekannt sein. Auch alte Kennwörter gelten grundsätzlich als vertrauliche Information. In der Praxis kommt es häufig vor, dass ein aktuelles zentrales Kennwort dem neuen Dienstleister mitgeteilt wird. Bis der neue Dienstleister alle Konsolen und Applikationen mit einem neuen Kennwort versehen hat, könnte das alte Kennwort durch unbefugte Dritte missbraucht werden. Abhängig von der Konfiguration des Systems (z. B. Dienstkonten, Zertifikatsdienste) und Organisation kann es vorkommen, dass das Ändern des Kennwortes nicht in kurzer Zeit mit vertretbarem Aufwand möglich ist.

Oft ist der Auftraggeber selbst nicht in der Lage, Benutzerkonten für externe Dienstleister auf sichere Art und Weise zu administrieren und muss dies gegebenenfalls dem neuen Dienstleister überlassen. Es kommt zu Situationen wie der gemeinsamen Nutzung von Benutzerkonten ("Account Sharing") oder den in G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten* und G 3.43 *Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen* beschriebenen Gefährdungen.

Teilweise besitzt der Auftraggeber selbst entweder keine Kenntnis mehr über Anmeldekonten mit administrativen Berechtigungen oder nur noch aufgrund einer regelmäßigen Unterrichtung durch den Dienstleister über das aktuelle Kennwort ("Account Sharing"). In jedem dieser Fälle liegen Entscheidungs- und Handlungshoheit beim Dienstleister. Der Auftraggeber verfügt über keine nur ihm bekannten Zugangsdaten mehr, mit denen er strategische Entscheidungen umsetzen kann. Diese Situation entspricht einem hohen Grad des Outsourcings. Sie stellt ein hohes Risiko für die Gefährdung der Systemsicherheit dar, wenn die Regelungen und Absicherungen für das Outsourcing nicht den Sicherheitsanforderungen entsprechen und diese nicht unmissverständlich in *Service Level Agreements* (SLA) festgehalten wurden

Insgesamt ergibt sich immer wieder die Situation, dass kritische administrative Konten sogar weniger sorgfältig gehandhabt werden als normale Benutzerkonten, weil etablierte Maßstäbe des Unternehmens oder der Behörde für den Umgang mit Benutzerkonten außer Acht gelassen werden und weil keine Verfahrensweise oder Richtlinie für den Umgang mit administrativen Konten bei Dienstleisterwechsel festgelegt wurde.

**Beispiel:**

Häufig wird in kleinen Unternehmen der zentrale Server von einer externen Person betreut. Diese Person hat dann auch das Kennwort für das zentrale Administratorkonto.

Oft besitzt kein anderer Benutzer innerhalb des Unternehmens ebenfalls ein administratives Konto, auch nicht der Geschäftsführer. Der gängigste Weg ist, dass der Geschäftsführer das Kennwort des zentralen administrativen Kontos in einem Tresor abgelegt hat. Kommt ein neuer Dienstleister, wird ihm dieses Kennwort mitgeteilt. Manchmal kommt es auch vor, dass kein Wartungsvertrag oder eine sonstige dauerhafte Vereinbarung über die Art des Outsourcings und der Verfahrensweisen mit irgendeiner der beteiligten externen Personen besteht. Unter Umständen hat der alte Dienstleister das Kennwort gewechselt und dann sein Engagement unerwartet und kurzfristig beendet. Das System bleibt solange nicht administrierbar, bis das Kennwort durch Nachfrage oder mit technischen Mitteln in Erfahrung gebracht wurde.

# G 2.112 Unzureichende Planung von VoIP

Fehlentscheidungen, die schon in der Planungsphase getroffen werden, können später meist nur mit einem hohen Aufwand korrigiert werden. Um einen stabilen Einsatz von VoIP zu ermöglichen, müssen viele Aspekte beachtet werden.

VoIP setzt ein funktionierendes Datennetz voraus. Dieses Datennetz kann auch für weitere Dienste, wie E-Mail und WWW, genutzt werden. Durch die zusätzlichen IP-Pakete, die für VoIP erforderlich sind, kann das Datennetz schnell überlastet werden. Die Dimensionierung spielt daher für den problemlosen Betrieb eine entscheidende Rolle. Die Folgen einer Fehleinschätzung bezüglich dieses Aspekts können bis zum Ausfall aller technischen Kommunikationsmöglichkeiten reichen. Zur Kommunikation über VoIP werden Signalisierungs- und Medientransportprotokolle benötigt. Bei den Signalisierungsprotokollen, in denen hauptsächlich Steuerungsanweisungen übermittelt werden, hat sich bisher kein Standardprotokoll durchgesetzt. Neben vielen proprietären Lösungen sind die Signalisierungsprotokolle SIP und H.323 zu nennen. Viele VoIP-Geräte unterstützen nur ein Protokoll, wodurch die Planung entscheidend beeinflusst wird.

Die Auswahl eines Medientransportprotokolls ist weniger kritisch, da sich bisher nur das Realtime Transport Protocol (RTP) durchgesetzt hat. Unterstützen beide Kommunikationspartner das verschlüsselte SRTP kann die Kommunikation geschützt stattfinden.

Für die eigentliche Übertragung der Sprache wird ein Codec benötigt, der die Umwandlung von Sprache in digitale Informationen ermöglicht. Obwohl zahlreiche Codecs existieren, spielt die Auswahl bei der Planung nur eine untergeordnete Rolle. In der Regel unterstützen die Endgeräte zahlreiche Codecs. Beim Verbindungsaufbau wird deren Verwendung mit dem Kommunikationspartner ausgehandelt. Unterstützen beide Kommunikationspartner nur wenige gemeinsame Codecs, so kann es passieren, dass ein Codec gewählt wird, der für die Rahmenbedingungen nicht optimal ist. Dies kann auf der einen Seite eine hohe Auslastung des Netzes und auf der anderen Seite eine zu schlechte Sprachqualität zur Folge haben.

Neben der technischen Grundfunktionalität spielt bei der Planung und Anschaffung von VoIP-Geräten eine mögliche Verschlüsselung zwischen den Geräten eine wichtige Rolle. In einigen Anwendungsfällen kann beispielsweise ein mit IPSec oder SSL verschlüsseltes VPN genutzt werden. Die Installation eines VPN-Clienten ist aber bei dedizierten VoIP-Hardphones meist nicht möglich. Wird auch die Verschlüsselung des Medientransportsprotokolls, beispielsweise durch SRTP, nicht unterstützt, so könnte ein Angreifer diese Telefongespräche unter Umständen abhören.

# G 2.113 Unzureichende Planung der Netzkapazität beim Einsatz von VoIP

Für den Einsatz von Voice over Internet Protocol (VoIP) wird ein Datennetz benötigt. Dabei können schon vorhandene Datennetze, an denen die Arbeitsplatzrechner und Server angeschlossen sind, oder hiervon unabhängige Datennetze verwendet werden. Ein Hauptargument für die Umstellung von leitungsvermittelnden Telefonlösungen zu VoIP sind aber die geringeren Wartungskosten von nur einer Kommunikationsinfrastruktur, wenn ein bestehendes Datennetz genutzt wird.

Für VoIP sind bisher nur sehr wenig Erfahrungswerte vorhanden, da es sich hierbei um eine relativ neue Technologie handelt. Wenn VoIP eine leitungsvermittelnde TK-Anlage ersetzen soll, kann in der Regel nicht auf die hier gewonnenen Erfahrungswerte zurückgegriffen werden. Dies betrifft besonders das Verhalten der VoIP-TK-Anlage bei einem großen Benutzerkreis.

Die Anbieter der VoIP-TK-Anlagen versuchen, Aussagen zu treffen, wie viele Benutzer mit ihrem Produkt verwaltet werden können. Diese Aussagen sind aber nicht sehr aussagekräftig, wenn ein bestehendes Datennetz genutzt werden soll. Treten hohe Datenmengen von den Arbeitsplatzrechner auf, kann durch die gleichzeitige Nutzung von VoIP das Netz schnell überlastet werden. Bei leitungsvermittelnden TK-Anlagen bestimmt die maximale Anzahl der Ports, an denen Telefone angeschlossen werden können, die Benutzeranzahl.

Je nach der Konfiguration der aktiven Netzkomponenten können bei einer Überlastung bestimmte IP-Pakete bevorzugt weitergeleitet werden. Werden bei einer hohen Netzlast VoIP-Pakete bevorzugt weitergeleitet, kann an den Arbeitsplatzrechnern unter Umständen nicht mehr effizient gearbeitet werden. Werden alle IP-Pakete mit einer gleich großen Priorität versendet, kann die störungsfreie Nutzung von VoIP nicht mehr garantiert werden.

Auch wenn bei der Umstellung auf VoIP das bestehende Netz für die parallele Nutzung von VoIP und regulären Informationen ausreichend dimensioniert wurde, muss dies für zukünftige Konstellationen nicht mehr genügen. Werden neue Mitarbeiter eingestellt, so müssen sie sowohl an ihren Arbeitsplatzrechnern über das Datennetz arbeiten als auch über VoIP telefonieren können. Damit steigt die Belastung des Netzes stärker an und die freien Ressourcen sind schneller aufgebraucht.

# G 2.114 Uneinheitliche Windows-Server-Sicherheitseinstellungen bei SMB, RPC und LDAP

Die an sich unsicheren Kommunikations-Protokolle SMB/CIFS und LDAP wurden bei Windows Servern mit erweiterten Signierungs- und Verschlüsselungsmechanismen ausgestattet. Ab Windows Server 2003 sind einige der Mechanismen schon in den Einstellungen der lokalen Sicherheitsrichtlinie vorkonfiguriert. Der Einsatz dieser Mechanismen betrifft die Kommunikation mit allen beteiligten Windows-Servern im Netz sowie viele Basisdienste von Windows und hat Auswirkungen auf den gesamten Netzbereich. Wenn diese Einstellungen nicht flächendeckend ordnungsgemäß und konsistent eingestellt werden, sind schwer nachvollziehbare Seiteneffekte bis hin zu Fehlfunktionen einzelner Windows-Server und -Clients die Folge.

Durch Fehlkonfiguration, falsches Vorgehen und falsche Aktivierungsreihenfolge beim Vornehmen der Signierungs- und Verschlüsselungseinstellungen zu SMB/CIFS und LDAP kann die Verfügbarkeit für weite Teile des Windows-Netzes stark beeinträchtigt werden. Bei größeren Umgebungen kann das Zurückversetzen des Windows-Netzes in einen funktionstüchtigen Zustand sehr hohen Aufwand verursachen, da in einer solchen Situation viele netzbasierte Verwaltungs- und Steuerungsfunktionen gestört sind.

Insbesondere für Domänen-Controller stellen inkonsistente Einstellungen innerhalb der Domäne eine große Gefahr dar, weil sich Symptome (Störung von Verwaltungsfunktionen wie der Gruppenrichtlinien) unter Umständen erst nach einer gewissen Zeit bemerkbar machen.

Ältere Windows-Versionen sind nicht ohne weiteres kompatibel zu den erhöhten Sicherheitseinstellungen für SMB/CIFS, RPC und LDAP. Zum Beispiel sind Vertrauensstellungen ohne Kerberos-Authentisierung, wie sie in großen, standortübergreifenden Informationsverbünden genutzt werden, nicht ohne weiteres zu den erhöhten Sicherheitseinstellungen kompatibel. Durch unzureichende Analyse aller betroffenen IT-Systeme und eine unzureichende Planung des Einsatzes können unerwartete Kommunikationsstörungen in allen Bereichen die Verfügbarkeit insgesamt stark einschränken. Eine unzureichende Planung kann hohe Folgekosten bei der Realisierung nach sich ziehen.

**Beispiel:**

In großen Umgebungen kann es zu Schwierigkeiten beim Domänenbeitritt eines Servers sowie zu Problemen mit Vertrauensstellungen kommen, wenn keine durchgehende Vertrauensstellung auf Kerberos Basis verwendet wird. Anmeldeversuche schlagen sporadisch fehl, obwohl das richtige Kennwort eingegeben wurde, je nachdem welcher Domänencontroller zufällig für Authentisierungsversuche ausgewählt wird. Auch Applikationen können in ihrer Funktionsweise beeinträchtigt werden.

# G 2.115 Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen ab Windows Server 2003

Im Betriebssystem Windows Server ab Version 2003 sind zu den aus Windows 2000 Server bekannten eingebauten Sicherheitsgruppen weitere Standardgruppen hinzugekommen. Die Rechte dieser Gruppen können zum Teil nicht eingeschränkt werden und die Berechtigungen sind vom Hersteller nicht im Einzelnen dokumentiert. Bestimmte Berechtigungen werden nicht angezeigt und sind nicht administrierbar, so zum Beispiel bei der Gruppe Netzwerkkonfigurations-Operatoren.

Die Gruppen stellen nicht prinzipiell eine Gefährdung dar. Die Unkenntnis über die Funktionsweise dieser Gruppen sowie deren ungeeignete Verwendung können jedoch zu vorsätzlichem oder versehentlichem Missbrauch von Administratorrechten und zur Fehlkonfiguration des Systems führen.

Neue Gruppen ab Windows Server 2003 sind:

- Hilfedienstgruppe
  Diese Gruppe für das Hilfe- und Supportcenter wird für die Administration und den Betrieb des Servers nicht benötigt, birgt jedoch Möglichkeiten für Missbrauch oder Fehlkonfiguration, weil der Gruppe umfangreiche Berechtigungen für Administrationswerkzeuge zugeordnet werden können.
- Netzwerkkonfigurations-Operatoren
  Mitglieder dieser Gruppe können die Parameter des TCP/IP-Stacks einstellen und manipulieren und somit den Server unerreichbar machen oder für Angriffe öffnen.
- Systemmonitorbenutzer und Leistungsprotokollbenutzer
  Systemmonitorbenutzer dürfen das Programm für den Systemmonitor (*perfmon.exe*) ausführen und benutzen, ohne dass sie besondere Berechtigungen benötigen. Mitglieder der Gruppe Leistungsprotokollbenutzer können Protokolle des Systemmonitors anschauen, verwalten und die Aufzeichnung von Überwachungsdaten konfigurieren. Sie haben direkten Zugriff auf einen Teil der Windows Management Instrumentation (WMI) Datenbank. Leistungs- und Nutzungsprofile sind sicherheitskritische Informationen, genauso wie Informationen über Ausfälle und Fehlfunktionen, die Anlass für einen Angriffsversuch sein könnten. Es stellt eine Gefahr dar, wenn Benutzerkonten unabsichtlich zusätzliche Berechtigungen mittels dieser Gruppen erlangen.
- Remotedesktopbenutzer
  Mitglieder dieser Gruppe können sich von einem anderen Computer aus mittels Remote Desktop Protocol (RDP) auf einem Mitgliedsserver oder allein stehenden Server anmelden und mit ihm arbeiten, als würden sie direkt vor dem physikalischen System sitzen. Dies stellt ein Risiko dar, denn jeder normale Benutzer kann sich auf diese Weise anmelden, ohne dass er besondere zusätzliche Berechtigungen benötigt.
- Distributed COM-Benutzer
  Ab Windows Server 2003 mit Service Pack 1 stehen detailliertere Berechtigungsstrukturen für Distributed-COM-Objekte (DCOM) zur Verfügung, um die Ausführung von COM-Modulen und die Aktivierung von COM-Objekten besser kontrollieren zu können. Insbesondere die Ausführung mittels Remote Procedure Calls (RPC) von anderen Clients aus kann damit besser kontrolliert werden. Viele Windows-Funktionen können über COM-Objekte gesteuert werden, darunter Windows Update, Richtlinienergebnissatz und Zertifikatsdienste. Die Berechtigungen werden in der Konsole "Komponen-

tendienste" konfiguriert. Standardmäßig haben die Distributed-COM-Benutzer das höchste Berechtigungslimit, es geht sogar über das von normalen Administratoren hinaus. Der falsche Umgang mit dieser Gruppe kann die verbesserten DCOM-Sicherheitsfunktionen unwirksam machen oder sogar zu einer erhöhten Angreifbarkeit des Systems führen.

- Erstellungen eingehender Gesamtstrukturvertrauensstellung
  Diese Gruppe ist seit Windows 2003 neu auf Domänencontrollern. Mitglieder dieser Gruppe können eingehende unidirektionale Vertrauensstellungen zur Active Directory-Gesamtstruktur eines Informationsverbundes erstellen. Durch Vertrauensstellungen können Rechte in der jeweils anderen Domänenumgebung ausgeübt werden, daher kann der Missbrauch oder fahrlässige Umgang mit dieser Gruppe Angreifern vielfältige Einflussmöglichkeiten auf den gesamten Informationsverbund verschaffen.

Unter Windows Server 2008 sind nach der Installation weitere Gruppen vorhanden. Dies gilt sowohl für sogenannte Stand-Alone-Systeme, als auch für Server innerhalb einer Domäne.

# G 2.116 Datenverlust beim Kopieren oder Verschieben von Daten ab Windows Server 2003

Das Verschieben und Kopieren von Objekten oder ganzer Teilbäume aus oder in Verzeichnisse umfasst mehrere zum Teil versteckte Vorgänge, welche die bewegten Datenobjekte und Verzeichnisstrukturen unbrauchbar machen können. Die Gefährdung geht weniger von einzelnen Benutzern als von Administratoren aus, da sie zum Teil große oder systemkritische Datenbestände bewegen müssen.

Die klassische Gefahr, die oft bei Migrationsszenarien anzutreffen ist, stellt das Verschieben von Objekten des Dateisystems über Medien- oder Systemgrenzen hinweg dar. Vor dem Entfernen der Daten von ihrem Ursprungsort findet keine Kontrolle dieser Daten am Zielort statt. Die von der Verschiebung betroffenen Daten sind gegebenenfalls verloren.

Weniger offensichtlich ist das Verhalten der Meta-Informationen von Objekten, wie Zugriffsberechtigungen oder andere Attribute, die für mehrere Objekte gleichzeitig gelten. Oft sind komplexe Berechtigungsstrukturen mit automatischen Vererbungsmechanismen in der Verzeichnisstruktur aktiv, die an Ursprungs- und Zielort unterschiedlich wirken. Bei Microsoft Windows bewirkt beispielsweise das Verschieben einer Datei die Mitnahme der vorhandenen Dateiberechtigungen zum Zielort, das Kopieren hingegen setzt die Dateiberechtigungen neu gemäß den Vorgaben am Zielort. Voraussetzung ist immer, dass Berechtigungen und andere Meta-Informationen am Zielort überhaupt korrekt interpretiert werden können. Sonst könnten gewachsene Berechtigungsstrukturen auf einen Schlag verloren gehen.

In Bezug auf die Wirkung von Kopier- und Verschiebemechanismen können Unterschiede bei einzelnen Komponenten auftreten, in Windows Server 2003 beispielsweise zwischen dem Dateisystem, den Komponentendiensten, den Internet Information Services (IIS) und dem Active Directory. Unkenntnis der Mechanismen hinter den Bedienkonzepten und mangelnde Sorgfalt können schnell zu Datenverlust und zur Fehlkonfiguration des Systems führen.

Unerwartete Effekte beim Kopieren und Verschieben sind nicht zuletzt auf darunterliegende Systemkomponenten zurückzuführen, die zur Speicherung und Erzeugung von Objekten und Verzeichnissen verwendet werden. Beispiele aus Windows Server 2003 sind Distributed File System (DFS), Active Directory oder das Encrypting File System (EFS). So enthalten die Lese- und Schreibprozesse beim Kopieren/Verschieben im EFS Schritte zur Zwischenspeicherung und Kryptographie, greifen auf Zertifikatsdienste zurück und speichern öffentliche Schlüssel als Meta-Information ab. Unbedarftes Kopieren und Verschieben von Dateien und Verzeichnisbäumen kann schnell dazu führen, dass die Daten nicht mehr verfügbar oder nicht vollständig sind oder deren Vertraulichkeit nicht mehr gewährleistet ist.

Speziell beim Dateisystem NTFS können unerwartete Effekte durch Alternate Data Streams (ADS) in Dateien auftreten. ADS sind unsichtbare Bereiche innerhalb einer Datei, in denen Windows Server 2003 Zusatzinformationen wie Zoneninformationen oder Piktogramme abspeichern kann.

Die Kommandozeile und der Windows Explorer weisen ein unterschiedliches Verhalten im Umgang mit ADS auf. Durch Verschiebe- und Kopiervorgänge können ADS versehentlich oder missbräuchlich verändert werden, verloren

gehen oder ungewollt mit Inhalt gefüllt werden. Besteht kein ausreichender Schutz durch geeignete Dateiberechtigungen, können ADS zu sehr gefährlichen Angriffspunkten werden.

**Beispiel:**

Auf einem Domänencontroller wird unter Verwendung des Windows-Befehls *xcopy* der Inhalt vom Systemlaufwerk auf eine andere Festplattenpartition kopiert. Der Befehl wird mit bestimmten Parametern aufgerufen, mit denen auch der *SysVol*-Ordner kopiert wird. Nach dem Kopiervorgang werden die Daten auf dem Systemlaufwerk nicht mehr benötigt und rekursiv gelöscht (zum Beispiel mit *rd /s*). Danach sind jedoch alle Informationen, die normalerweise über den *SysVol*-Ordner repliziert werden, auf diesem Domänencontroller nicht mehr verfügbar (z. B. Gruppenrichtlinienobjekte, Anmeldeskripte). Die Ursache liegt in der Struktur der *SysVol*-Ordner, welche Verbindungspunkte (*Junction-Points*) zu DFS-Freigaben enthalten, die mit File Replication Service (FRS) repliziert werden. *Xcopy* sichert in diesem Fall nicht den gesamten Inhalt, sondern nur die Verbindungspunkte. Der spätere rekursive Löschvorgang erreicht über die kopierten Verbindungspunkte die originalen DFS-Freigaben und löscht Teile von deren Inhalt, sofern die Berechtigungen dies zulassen. Unter Umständen wird die Löschung noch auf andere Domänencontroller repliziert und somit der gesamte Domänenbetrieb gestört. Das Problem kann nur durch eine Wiederherstellung des kompletten Systemstatus aus der Datensicherung beseitigt werden.

# G 2.117 Fehlende oder unzureichende Planung des WLAN-Einsatzes

Ein WLAN muss sorgfältig geplant und aufgebaut werden, damit nicht einzelne Sicherheitslücken alle hiermit vernetzten IT-Systeme beeinträchtigen kann. Dies kann sogar dazu führen, dass über ein unzureichend gesichertes WLAN ein damit gekoppeltes Behörden- oder Unternehmensnetz kompromittiert wird. Falls Sicherheitsmechanismen zwischen LAN und WLAN nicht abgestimmt sind, kann es dadurch auch zu Sicherheitslücken kommen, beispielsweise durch Mängel bei der Planung zur Trennung von Benutzergruppen.

Bei fehlender oder unzureichender Planung können sich eine Vielzahl von Problemen ergeben, wie beispielsweise die folgenden:

- Sensitive Daten könnten mitgelesen werden, wenn keine oder nur unzureichende Sicherheitsmaßnahmen im WLAN umgesetzt wurden.
- Die Leistungsfähigkeit eines Funknetzes könnte durch nicht beachtete andere WLAN-Installationen oder andere Funk-Systeme gemindert werden, wenn diese in den Nutzungsbereichs des Funknetzes hineinstrahlen.
- Falls bei der Planung eines WLANs die Gebäudedämpfung oder die Dämpfung durch absorbierende Ausbaumaterialien (beispielsweise Stahlschränke, Nasszellen, Versorgungsleitungen, Stahlbetonbauweise) nicht berücksichtigt wurde, kann dessen Leistungsfähigkeit ebenfalls reduziert werden.
- Gleichkanalstörungen aus einer benachbarten Funkzelle des eigenen WLAN sind eine weitere häufige Ursache für Störungen in einem WLAN. Hierdurch können sich zwei Teilnehmer benachbarter Zellen gegenseitig behindern, da sich deren Funkwellen im Raum überlagern und gegenseitig stören würden.
- Durch Funklöcher kann die Leistungsfähigkeit stark beeinträchtigt werden. Um Funklöcher zu vermeiden, wird bei unzureichender Planung des WLANs häufig einfach die Sendeleistung erhöht werden. Dadurch strahlt das WLAN eventuell in Bereiche hinein, in denen es nicht benötigt wird und in denen es unter Umständen abgehört werden kann.
- Eine Auswirkung mangelhafter Planung kann z. B. unzureichende Übertragungskapazität sein, durch die die Nutzung von bandbreitenintensiven Anwendungen eingeschränkt oder sogar verhindert werden kann.

Eine zusätzliche Gefährdung für das LAN entsteht dadurch, wenn nur eine unzureichende Absicherung der Verbindung zwischen den Access Points bzw. dem Distribution System und der kabelgebundenen Infrastruktur besteht. Erfolgt keine physikalische oder logische Absicherung auf der Ebene des Distribution System, so kann nach einer Kompromittierung der Absicherung der Luftschnittstelle bzw. der Sicherheitseinstellungen auf dem Access Point die gesamte Broadcast-Domäne, in der sich der Access Point befindet, abgehört werden. Die daraus gewonnenen Informationen könnten für einen Angriff auf das gesamte LAN genutzt werden.

**Beispiel:**

Werden für den Sicherheitsgateway am Übergabepunkt zwischen Distribution System und LAN die Filterregeln zu großzügig ausgelegt, kann ein Angreifer durch geschickte Manipulation der Kommunikationsdaten diesen Übergabepunkt durch einen Man-in-the-Middle-Angriff tunneln und somit Zugriff auf die interne LAN-Infrastruktur erlangen. Voraussetzung ist, dass entweder die Sicherheitsmechanismen auf der Luftschnittstelle kompromittiert wurden oder ein direkter Zugang zum Distribution System besteht. Außerdem könnten

Schwachstellen auf Betriebssystemebene ebenfalls zur Tunnelung genutzt werden, falls diese die Systeme des Übergabepunktes nicht ausreichend gehärtet wurden.

# G 2.118 Unzureichende Regelungen zum WLAN-Einsatz

Bei einem Access Point sind in der Regel in der Standard-Einstellung keine Sicherheitsmechanismen aktiviert. Werden WLAN-Komponenten wegen fehlender Vorgaben ungesichert in den Produktivbetrieb übernommen, stellt dies eine massive Gefährdung für das WLAN und daran angeschlossene IT-Systeme dar. Das ist vergleichbar mit der Gefährdung durch einen ungesicherten Internet-Anschluss. Sofern also ein Mitarbeiter, aufgrund fehlender Regelungen zum WLAN-Einsatz, einen ungenehmigten bzw. ungesicherten Access Point an ein internes Netz einer Institution anschließt, untergräbt er praktisch sämtliche im LAN ergriffenen Sicherheitsmaßnahmen, wie z. B. die Firewall zum Schutz gegen unberechtigte externe Zugriffe aus dem Internet.

**Unklare Zuständigkeiten**

Falls Zuständigkeiten nicht klar geregelt sind, kann es z. B. aufgrund fehlender Regelungen zur Administration der WLAN-Infrastruktur zu Fehlkonfigurationen der WLAN-Komponenten kommen. Bei fehlenden Vorgaben zum Konfigurationsmanagement kann es durch nur einen nicht gemäß vorgegebenem Standard-Profil konfigurierten Access Point oder WLAN-Client zu einer Kompromittierung des gesamten Netzes der Institution kommen.

Bei unzureichender Abstimmung der unterschiedlichen Zuständigkeiten innerhalb einer Institution sowie mit externen Dienstleistern kann es in der Praxis immer wieder zu Problemen kommen. Bezogen auf das WLAN ergeben sich Gefährdungen insbesondere dann, wenn für die Betreuung der physikalischen (passiven) Infrastruktur, der aktiven Netztechnik und der Sicherheitssysteme unterschiedliche Gruppen zuständig sind, die organisatorisch weit voneinander entfernt liegen und erst von einer entsprechend hohen Führungsebene koordiniert werden.

Probleme können sich auch ergeben, wenn keine einheitliche Regeln zur Dokumentation von Systemänderungen, wie beispielsweise Austausch von WLAN-Komponenten, Änderungen an Konfigurationen, Austausch der WLAN-Schlüsselinformationen, definiert sind.

**Keine Regelungen für die Überwachung**

Wurden auch zur Überwachung der WLAN-Infrastruktur keine Festlegungen getroffen und die entsprechenden finanziellen und personellen Ressourcen nicht bereitgestellt, werden Angriffe auf das WLAN eventuell nicht rechtzeitig erkannt. Hierzu zählen beispielsweise:

- Ohne regelmäßige Kontrollen wird unter Umständen übersehen, dass fremde Access Points (inklusive privater Access Points) an das Distribution System bzw. unmittelbar an das LAN angeschlossen wurden.
- Wenn die WLAN-Protokolle nicht regelmäßig ausgewertet werden, werden Sicherheitsvorfälle nicht rechtzeitig erkannt. So kann eine plötzliche Häufung fehlgeschlagener Anmeldevorgänge am Access Point auf Angriffsversuche hindeuten.

Werden dringend erforderliche Updates der Virenschutzsoftware oder sicherheitsrelevanter Patches nicht zeitgerecht eingespielt, kann es zur Kompromittierung einer WLAN-Komponente kommen. Besonders gefährdet sind hier WLAN-Komponenten mit direktem Zugriff auf das Internet oder bei der Verwendung in öffentlichen WLANs. Je nach Art der Schadsoftware kann diese

beim nächsten Verbinden mit dem Heimat-WLAN zur Kompromittierung der gesamten WLAN-Infrastruktur und darüber hinaus führen.

**Fehlende Regelungen zur Reaktion auf Sicherheitsvorfälle im WLAN**

Sofern es für den Betrieb eines WLANs keine Überlegungen gibt, wie im Notfall auf Vorfälle reagiert werden soll, kann dies dazu führen, dass es lange dauert, bis Sicherheitsprobleme erkannt und bereinigt werden. In der Zwischenzeit könnte es beispielsweise zu Datenabfluss oder zu Wurmattacken kommen. Sogar wenn Attacken bemerkt werden, werden eventuell aber Gegenmaßnahmen nicht zeitnah (innerhalb von Minuten) eingeleitet, wenn nicht auf entsprechend vorbereitete Maßnahmenkataloge, geregelte Abläufe und Befugnisse zu notwendigen Eingriffen zurückgegriffen werden kann.

**Beispiel:**

- Ein Unternehmen hatte Zugangsinformationen zu einem internen WLAN im Internet veröffentlicht, um mobilen Mitarbeitern den Zugriff von unterwegs zu vereinfachen. Jeder, der diese Informationen kennt, kann sich somit gegenüber dem WLAN authentisieren und erlangt Zugang zu eventuell schutzbedürftigen Daten. Obwohl das WLAN selber nur Informationen mit geringem Schutzbedarf enthielt, konnte über die Anbindung an ein LAN auf Produktivsysteme zugegriffen werden. Die dadurch erlangten Daten, beispielsweise geheime Konstruktionszeichnungen von einem Prototypen, wurden teilweise im Internet veröffentlicht. Andere wurden an einen Mitbewerber weitergegeben. Dieser hätte somit feststellen können, welche Neuentwicklungen geplant sind und schneller durch Eigenentwicklungen darauf reagieren können. Glücklicherweise hat er aber hierüber die Polizei informiert.

# G 2.119 Ungeeignete Auswahl von WLAN-Authentikationsverfahren

Die Auswahl der zu verwendenden Authentikationsverfahren muss sich am Schutzbedarf der in einem WLAN transportierten Daten orientieren. Zunächst ist WEP als unsicher einzustufen und bietet eine Vielzahl von Angriffsmöglichkeiten, wie beispielsweise das Extrahieren der Schlüssel aus den Datenpaketen. Diese könnten dann zu einem erfolgreichen Zugriff auf ein WLAN benutzt werden.

Wird das Schlüsselmaterial, das für die Authentikation bzw. Verschlüsselung im WLAN verwendet wird, nicht sorgfältig verteilt oder ausreichend sicher gespeichert, so sind darauf aufbauende Methoden, um ein entsprechendes Sicherheitsniveau zu erreichen, eventuell vollkommen wertlos. Zu einfache Passwörter oder unzureichend geschützte Zertifikate bieten jedem Angreifer einen gültigen Zugang zu einem WLAN. Bei einem WPA-gesicherten WLAN stellen beispielsweise Pre-Shared Keys eine Sicherheitslücke dar, wenn diese nicht geeignet ausgewählt wurden, also nicht kompliziert genug sind.

Es gibt aber auch EAP-Methoden, die aufgrund einiger Schwachstellen eine Bedrohung darstellen. Beispielsweise wird bei EAP-MD5 CHAP als Authentisierungsmethode verwendet, das unter anderem die beidseitige Kenntnis eines unverschlüsselten Passworts erfordert. Weiterhin unterstützt EAP-MD5 keine Schlüsselerzeugung und kann daher nicht unmittelbar mit IEEE 802.11i benutzt werden. Darüber hinaus sind inzwischen auch kryptographische Schwächen von MD5 bekannt, sodass dieses Hash-Verfahren heute nicht mehr als sicher gilt.

Bei EAP-PEAP ist aus kryptographischer Sicht zu beanstanden, dass PEAP zur Sicherung des äußeren Tunnels nur die Identität des Servers prüft, nicht aber die des Clients.

Einige Implementationen von EAP-Methoden enthalten auch Schwachstellen. So ist das proprietäre EAP-LEAP von Cisco anfällig für sogenannte Wörterbuch-Attacken und es gibt Tools, die diese Schwachstelle bereits gezielt ausnutzen und selbst starke Passwörter wirkungslos sind.

Ebenso ist es von Nachteil, dass EAP-LEAP explizit von allen WLAN-Komponenten unterstützt werden muss und es keine Interoperabilität zwischen EAP-LEAP und anderen EAP-Methoden besteht, wie es in IEEE 802.1X gefordert ist.

# G 2.120 Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen

Werden sicherheitsrelevante IT-Systeme, auf denen Authentikationsdaten vorgehalten werden, an leicht zugänglichen Orten aufgestellt, kann dies zu einer massiven Gefährdung der Gesamtsicherheit eines Netzes führen. Zu den sicherheitsrelevanten IT-Systemen gehören z. B. Sicherheitsgateways, Directory Server, die einen Verzeichnisdienst für Benutzeridentitätsdaten bereitstellen oder IT-Systeme, auf denen Authentikationsdaten vorgehalten werden. Nicht geeignete Orte für deren Aufstellung sind beispielsweise öffentliche Besprechungsräume, Flure oder normale Büroräume. Auch kleinere, aber trotzdem sicherheitsrelevante Netzkoppelelemente wie Router, Switches oder Access Points dürfen nicht ungesichert in Durchgangswegen untergebracht werden. Ein Access Point sollte z. B. nicht ungeschützt direkt unter der Decke installiert werden. Hierdurch ist ein einfacher physischer Zugriff gegeben, durch den Zugriffsinformationen auf das zugehörige WLAN sehr einfach ausgelesen werden könnten. Falls ein direkter Zugriff auf sicherheitsrelevante IT-Systeme möglich ist, können dabei auch andere Sicherheitsmechanismen außer Kraft gesetzt werden.

**Beispiel:**

Ein Access Point wird in einem öffentlichen Besprechungsraum aufgestellt, um einen drahtlosen Zugriff auf das Internet zu gewährleisten. Access Points stellen einen gewissen Wert dar, der zum Diebstahl verleiten kann. Bei einer Besprechung fällt auf, dass dieser Access Point nicht mehr vorhanden ist und es stellt sich heraus, dass er vor mehreren Wochen gestohlen wurde. Da ein Access Point in der Regel wichtige Informationen für den Zugriff auf das WLAN enthält, kann der Dieb unbehindert und unbemerkt Informationen für eine weitere Kompromittierung erlangen. Mit ihm sind z. B. wichtige Zertifikate für die Authentikation am WLAN entwendet worden. Bis zu deren Sperrung und Änderung war das Netz angreifbar.

Auch durch ungünstige Umgebungseinflüsse (z. B. Erschütterungen, unzulängliche klimatische Bedingungen oder eine hohe Staubbelastung) können Schäden an sicherheitsrelevanten IT-Systemen hervorgerufen werden.

# G 2.121 Unzureichende Kontrolle von WLANs

Ein WLAN ist ein potentielles Ziel von Angriffen, sei es, um dieses unberechtigt nutzen zu können oder um dessen Verfügbarkeit zu stören (DoS-Angriffe). Diese könnten eine Kompromittierung der mit dem WLAN verbundenen Infrastruktur nach sich ziehen. Wenn keine ausreichende Kontrolle des WLANs stattfindet, werden Angriffe meistens überhaupt nicht oder nicht zeitnah erkannt.

**Falsch konfigurierte Intrusion Detection Systeme**

Werden bei der Planung für ein Intrusion Detection System die Kommunikationsmuster zum WLAN nicht mit betrachtet, so führt dies entweder dazu, dass Angriffe vom Intrusion Detection System nicht erkannt werden können, oder dass zulässige Kommunikation zu einem Alarm führt.

Eine akute Gefährdung kann auch bei der Protokollierung von IDS-relevanten Ereignissen entstehen:

- Wenn zu viele Informationen protokolliert bzw. zu lange gespeichert werden, besteht die Gefahr, dass die Datenbanken des Intrusion Detection Systems überlaufen.
- Werden bei der Protokollierung zu wenige oder die falschen Daten aufgezeichnet, wird eventuell ein Angriff nicht erkannt und es kann keine sinnvolle post-mortem-Analyse durchgeführt werden.

**Unerlaubte Mitnutzung des WLANs**

Sofern keine ausreichend starken Authentisierungsmechanismen für den Zugang zu einem WLAN implementiert sind, könnte ein Angreifer über eine WLAN-Installation beispielsweise auf das Internet zugreifen. Dadurch könnte die zur Verfügung stehende Bandbreite reduziert und die Antwortzeit für autorisierte WLAN-Nutzer erhöht werden. Ebenso könnte der so erlangte Internet-Zugang dazu verwendet werden,

- Angriffe auf andere Systeme im Internet durchzuführen,
- Spam-Mails zu verbreiten,
- strafrechtlich relevante Inhalte aus dem Internet herunterzuladen oder
- Internet-Tauschbörsen zu benutzen.

**Keine Auswertung der Log-Dateien**

Wenn Angreifer versuchen, sich an einem WLAN anzumelden, müssen sie zunächst die Authentisierung überwinden. Falls sie hierbei Wörterbuch- oder Brute-Force-Methoden anwenden, kommt es zu Fehlermeldungen bei den Authentisierungskomponenten, die diese in ihren Log-Dateien verzeichnen. Werden diese Protokoll-Dateien nicht regelmäßig ausgewertet, so können solche Angriffe nicht erkannt und entsprechende Gegenmaßnahmen ergriffen werden. Werden darüber hinaus erfolgreiche Anmeldungen nicht auf ihre Gültigkeit überprüft, so könnten Angreifer unbemerkt das WLAN mit gültigen ausgespähten Zugangsinformationen benutzen, sogar während die Mitarbeiter abwesend sind.

**Beispiel:**

Der Mitarbeiter Herr Müller ist für drei Wochen in Urlaub. Während dieser Zeit wurden seine Zugangsinformationen für das WLAN von einem Angreifer erfolgreich entschlüsselt. Dieser kann sich nun mit diesen Informationen erfolgreich und unbemerkt mit dem WLAN der Institution verbinden und auf alle Be-

reiche zugreifen, zu denen der Mitarbeiter zugelassen ist. Hierdurch könnten sogar sensible Daten erspäht werden. Bei einer regelmäßigen Analyse der Protokoll-Dateien des Authentisierungsservers hätte den Administratoren auffallen können, dass Herr Müller gar nicht anwesend ist und sich somit auch nicht mit dem WLAN verbinden kann. Ebenso hätte eine Urlaubssperre des WLAN-Accounts von Herrn Müller diesen Angriff verhindern können.

# G 2.122 Ungeeigneter Einsatz von Multifunktionsgeräten

Multifunktionsgeräte sind eine Platz sparende und kostengünstige Lösung, um den Benutzern die Funktionen Scannen, Drucken, Kopieren und oft auch Faxen zur Verfügung zu stellen. Oft enthalten Multifunktionsgeräte auch einen integrierten Kommunikationsanschluss für Datenverbindungen und sind ans Telefonnetz angeschlossen. Es werden sowohl netzfähige Geräte, die einer größeren Benutzergruppe zur Verfügung stehen, als auch Einzelplatzlösungen, beispielsweise mit einer USB-Schnittstelle, angeboten.

Durch die Integration der Funktionen Scannen, Drucken und Kopieren in einem Gerät steigen die Sicherheitsanforderungen im Vergleich zu einzelnen Systemen, da solche Geräte zusätzlich einen "Single Point of Failure" darstellen. Beispielweise muss beim Ausfall einer Funktionalität das gesamte Gerät repariert werden, so dass auch die nicht betroffenen Funktionalitäten während dieser Zeit ebenfalls nicht mehr genutzt werden können.

Ist in einem Multifunktionsgerät eine Kommunikationsschnittstelle zum Telefonnetz (z. B. Fax-Modem) oder Internet integriert, könnten auf diese Weise zentrale Schutzmechanismen, wie ein vorhandenes Sicherheitsgateway, überbrückt werden. Dies hätte möglicherweise zur Folge, dass dadurch im LAN ein ungeschützter Zugang zum Internet entsteht.

Vorhandene, aber nicht dokumentierte Wartungszugänge vom Hersteller ermöglichen unter Umständen ebenfalls den Zugriff auf das LAN.

# G 2.123 Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

Die Sicherheit eines Gesamtsystems hängt maßgeblich von der Sicherheit jedes einzelnen Teilsystems ab. Somit stützt sich die Sicherheit von Verzeichnisdiensten auf die Sicherheit des Basisbetriebssystems und hierbei vor allem auf die Dateisystemsicherheit.

Verzeichnisdienste lassen sich auf einer Vielzahl von Betriebssystemen installieren und betreiben, wodurch sich eine große Vielfalt der bei den eingesetzten Betriebssystemen jeweils vorzunehmenden Sicherheitseinstellungen ergeben kann. Diese Vielfalt erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse sämtlicher als Basis dienender Betriebssysteme voraus. Sollte die Gesamtlösung sehr heterogen sein, besteht daher die Gefahr, dass der Einsatz von Verzeichnisdiensten nicht detailliert und tief genug geplant wird.

Speziell für den Einsatz eines Verzeichnisdienstes im Intranet ist die Planung der Baumstruktur sowie die Abbildung der Organisationsstruktur einer Institution von großer Bedeutung. Wenn die organisatorische Struktur bis ins Kleinste nachgebildet wird, kann dies zu Problemen in der Administration führen. Bei einer fehlerhaften Planung besteht die Gefahr von Inkonsistenzen und übermäßiger Komplexität im Aufbau des Verzeichnisdienstes, woraus Fehlkonfigurationen sowie ein falscher oder unzulänglicher Betrieb des Systems resultieren könnten.

Die globale Baumstruktur eines Verzeichnisdienstes hat weitreichende Auswirkungen auf die Sicherheit einer Installation. Wenn beispielsweise verschiedene Teilbäume unterschiedliche Sicherheitsanforderungen haben oder zu verschiedenen Organisationsbereichen gehören, könnten sich hieraus problematische Aspekte ergeben. Durch die impliziten Vererbungsmechanismen sowie durch die Komplexität der Regeln für die Berechnung der tatsächlich wirksamen, effektiven Rechte einzelner Objekte ergeben sich hohe Anforderungen an die Planung des Systems.

Falls eine Zertifizierungsstelle (englisch: Certificate Authority, CA) eingesetzt wird, stellt diese einen wesentlichen Sicherheitsbestandteil des Verzeichnisdienstes dar. Auch hierbei kann eine fehlerhafte Planung die Sicherheit des Verzeichnisdienstes erheblich beeinträchtigen.

Da ein Verzeichnisdienst eine rollenbasierte Administration der Verzeichnisdatenbank sowie die Delegation einzelner Administrationsaufgaben erlaubt, besteht bei fehlerhafter Planung der Administrationsaufgaben die Gefahr, dass das System unsicher oder unzulänglich administriert wird.

Ferner könnte der Einsatz eines Administrationstools fehlerhaft geplant sein und dadurch unautorisierten Benutzern den Zugang zu Interna der Verzeichnisdienst-Installation erlauben.

Bei der Synchronisation von Verzeichnisdaten mit weiteren Verzeichnisdiensten beispielsweise mittels *DirXML* bei *eDirectory* von Novell können sich weitere Gefahren ergeben. Bei entsprechenden Rechten, die vom jeweils betrachteten Zielsystem abhängen, werden Änderungen infolge der Synchronisation dann auch im Verzeichnisdienst aktiv.

Externe Verzeichnisse könnten sich umgekehrt beim eigenen Verzeichnisdienst einschreiben, um Änderungen des Informationsstandes zu erfahren und ihr Verzeichnis daraufhin abzugleichen. Eine solche Art der Synchronisation bedarf einer detaillierten Planung, da anderenfalls sensitive Daten unter Umständen ungewollt automatisiert nach außen vervielfältigt werden. Umgekehrt könnten beispielsweise ungewollt bestehende Daten auf diesem Weg überschrieben werden. Hierbei könnten Planungsfehler den Verlust von Integrität und Vertraulichkeit von Verzeichnisdaten hervorrufen.

Bei Verwendung von Login-Skripten für Benutzer bzw. Benutzergruppen könnten durch fehlende oder unzulängliche Planung Inkonsistenzen zur festgelegten Sicherheitsrichtlinie auftreten. Ferner können sich bei fehlender oder unzureichender Planung auch zusätzlich noch folgende Probleme ergeben:

- Sofern Replikation und Backup nicht ausreichend berücksichtigt wurden, könnte es zu Datenverlusten kommen.
- Der Betrieb der Public-Key-Infrastruktur (PKI) könnte inadäquat sein.
- Die Systemleistung könnte zu gering sein.

# G 2.124 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

Ein wesentlicher Aspekt bei der Planung des Einsatzes eines Verzeichnisdienstes ist die Partitionierung und die Replizierung. Bei der Partitionierung handelt es sich um eine Aufteilung der Verzeichnisdaten eines Verzeichnisdienstes in einzelne Teilbereiche (Partitionen). Eine solche Partitionierung kann nicht beliebig erfolgen, sondern muss gewissen Regeln entsprechen, welche sich aus der Logik der hierarchischen Baumstruktur ergeben.

Die Replizierung von Partitionen des Verzeichnisdienstes dient in erster Linie der Erhöhung der Verfügbarkeit und der Lastverteilung des Verzeichnissystems. Weiter wird durch die Redundanz in der Datenhaltung die Ausfallsicherheit verbessert. Von entscheidender Bedeutung ist deshalb auch die Planung, da nachträgliche Änderungen an den Partitions- und Replikationseinstellungen zwar möglich sind, aber unter Umständen Inkonsistenzen nach sich ziehen können.

Bei Änderungen am Verzeichnisdienst dauert es eine gewisse Zeit, bedingt durch die Verteilung auf mehrere Systeme, bis alle neuen Einstellungen überall eingespielt sind. Hieraus kann sich ein Zeitfenster ergeben, innerhalb dessen der Verzeichnisdienst inkonsistent ist. Vor allem bei der Definition der Authentisierungsdaten oder auch der Zugriffsrechte auf Verzeichnisdienst-Objekte können solche Inkonsistenzen ein Problem darstellen.

Die Partitionierungsfestlegungen des Verzeichnisdienstes können direkte Auswirkungen auf die Replizierungsaktivitäten des Gesamtsystems haben. Ist die Planung inadäquat, so werden hier beispielsweise bei zu flacher Baumstruktur sehr umfassende Replizierungsringe erzeugt. Wird beispielsweise ein Replizierungsring sehr groß, so besteht eine gewisse Gefahr, dass zumindest ein Server des Ringes zeitweise nicht erreichbar ist, wodurch Fehler- und Statusmeldungen auf jedem weiteren Verzeichnisdienst-Server des Replizierungsrings hervorgerufen werden. Solche Fehler- und Statusmeldungen können zu einem erhöhten Administrationsaufwand führen, der sich über große Teile des Verzeichnisbaums erstrecken kann.

Ferner kann eine fehlerhafte oder unzureichende Planung der Partitionierung und der Replizierung des Verzeichnisdienstes auch zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Systemausfällen führen.

# G 2.125 Fehlerhafte oder unzureichende Planung des Zugriffs auf den Verzeichnisdienst

Ist die Vergabe von Zugangs- und Zugriffsrechten zum bzw. auf dem Verzeichnisdienst unzulänglich oder mit unpassenden Tools geregelt, kann dieses schnell zu gravierenden Sicherheitslücken, beispielsweise durch Wildwuchs in der Rechtevergabe führen. Die Verwaltung von Zugangs- und Zugriffsrechten ist eine äußerst arbeitsintensive Aufgabe, bei der im Extremfall viele manuelle Arbeitsschritte erforderlich sind, die zu Fehlern und Mängeln im Überblick über durchgeführte Arbeiten führen können.

In Organisationen, in denen kein Überblick über alle auf den verschiedenen IT-Systemen eingerichteten Benutzer und deren Rechteprofil vorhanden ist, führt das typischerweise dazu, dass sich Accounts von Benutzern finden, die die Institution längst verlassen haben oder die durch wechselnde Tätigkeiten zu viele Rechte aufgehäuft haben.

Wenn die Tools zur Verwaltung von Zugangs- und Zugriffsrechten schlecht ausgewählt wurden, sind diese oft nicht flexibel genug, um auf Änderungen in der Organisationsstruktur oder auf Wechsel der IT-Systeme angepasst zu werden.

Die Rollentrennung von Benutzern kann falsch vorgenommen worden sein, so dass Sicherheitslücken entstehen, beispielsweise durch falsche Zuordnung von Benutzern in Gruppen oder zu großzügige Rechtevergabe. Benutzer könnten Rollen zugeordnet worden sein, die nicht ihren Aufgaben entsprechen (zu viel oder zu wenig Rechte) oder die sie aufgrund ihrer Aufgaben nicht haben dürfen (Rollenkonflikte).

Der Zugriff durch die Benutzer auf den Verzeichnisdienst erfolgt oft per LDAP-Schnittstelle, welche einen weit verbreiteten Internet-Standard darstellt. Dieser Zugriff bedarf einer eingehenden Planung, insbesondere auch in Bezug auf die für den sinnvollen Einsatz der Anwendungen benötigten Verzeichnisdienst-Rechte. Somit hängt die Planung des LDAP-Zugriffs wesentlich vom Einsatzszenario des Verzeichnisdienstes ab.

Eine unzureichende Planung, ob und welche Daten, beispielsweise Benutzerpasswörter, im Klartext übertragen werden dürfen, kann Inkonsistenzen oder Widersprüche zu organisationsinternen Sicherheitsrichtlinien hervorrufen. Auch kann eine fehlerhafte Planung der Sicherheitsmaßnahmen und -techniken des Verzeichnisdienstes zum Schutz vertraulicher Daten zu Inkompatibilitäten bis hin zum Ausfall einer Verschlüsselung führen.

Das Fehlen eines Wurzelzertifikats im Verzeichnisdienst oder eine nicht nachprüfbare Zertifikatskette wird eine gegenseitige Authentisierung zur Nutzung des Verzeichnisdienstes verhindern.

Aufgrund der Vielfalt an Konfigurationsoptionen für den LDAP-Zugriff auf den Verzeichnisdienst können sich schnell Fehlkonfigurationen mit den nachfolgend aufgezeigten Gefährdungen ergeben:

- Unautorisierte Zugriffsmöglichkeiten auf den Verzeichnisdienst,
- falsche Vergabe von Zugriffsrechten,
- Ausspähen von Informationen im Klartext,
- Übermittlung von unverschlüsselten Benutzerpasswörtern,
- unzureichende Verfügbarkeit des Gesamtsystems sowie

- Fehler beim LDAP-Zugriff, insbesondere für netzbasierte Anwendungen.

# G 2.126 Unzureichende Protokollierung von Änderungen am Active Directory

Das Active Directory stellt in einer Institution üblicherweise einen zentralen Punkt zur Authentisierung und Autorisierung beim Zugriff auf Netzressourcen dar. Änderungen an der Active-Directory-Struktur oder auch an einzelnen Domänen-Controllern können sich daher auf einen Großteil der IT einer Institution auswirken. Dies gilt sowohl für autorisierte als auch für unautorisierte Änderungen.

Werden sicherheitsrelevante Änderungen an der Konfiguration des Active Directory oder eines Domänen-Controllers, z. B. die Heraufstufung eines Servers zum Domänen-Controller, nicht dokumentiert oder protokolliert, so besteht die Möglichkeit, dass solche Änderungen nicht oder erst spät erkannt werden.

Die alleinige Protokollierung von sicherheitskritischen Vorfällen bzw. Änderungen ist jedoch nicht ausreichend. Damit sicherheitskritische Probleme erkannt werden können, muss zusätzlich auch eine regelmäßige Auswertung der Protokolle durchgeführt werden (siehe G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*).

**Beispiele:**

- Wird eine versehentlich oder vorsätzlich eingerichtete Vertrauensbeziehung zu einer externen Domäne aufgrund fehlender Protokollierung nicht erkannt, so können die Benutzer der externen Domäne unter Umständen unbemerkt auf die Systeme der betroffenen Institution zugreifen.
- Werden die Protokolldaten eines Domänen-Controllers nicht regelmäßig ausgewertet, so wird unter Umständen nicht bemerkt, dass alle Benutzer dieser Domäne in die Gruppe der "Domänen-Admins" aufgenommen wurden. Die unerkannte Fehlkonfiguration kann beispielsweise dazu führen, dass Domänen-Mitglieder Vollzugriff auf die Systeme der Domäne erlangen und Schadsoftware (z. B. Backdoors oder Trojanische Pferde) auf den Rechnern der Domäne installieren. Eine solche Hintertür kann beispielsweise durch ein fehlerhaftes Skript im Rahmen der administrativen Tätigkeiten entstehen.

# G 2.127 Unzureichende Planung von Datensicherungsmethoden für Domänen-Controller

Werden für die Sicherung von Domänen-Controllern in einem Active Directory falsche Datensicherungsmethoden angewendet, so kann dies den Betrieb innerhalb der betroffenen Domäne beeinträchtigen. Daher können sich folgende Probleme ergeben, wenn die besondere Stellung, so wie die technischen Gegebenheiten von Domänen-Controllern bei der Datensicherung nicht berücksichtigt werden:

Durch die Nutzung inkompatibler Software zur Datensicherung der Domänen-Controller können auf den betroffenen Systemen unnötige Replizierungen ausgelöst werden und damit zugleich Störungen des Active Directory (siehe G 4.68 *Störungen des Active Directory durch unnötige Dateireplizierung*).

Darüber hinaus ist bei fehlender Planung der Datensicherungsmethoden nicht sichergestellt, dass die Berechtigungen der "Sicherungsoperatoren" für die Mitglied-Server der Domäne ausreichend restriktiv gesetzt werden. Werden die Rechte nur unzureichend oder uneingeschränkt gesetzt, so können die "Sicherungsoperatoren" unter Umständen administrative Berechtigungen für die Domäne erhalten und somit gegebenenfalls Rollenkonzepte unterwandert werden.

Insbesondere bei Institutionen mit mehreren Standorten kann eine fehlende Planung der Datensicherung dazu führen, dass Niederlassungen unberücksichtigt bleiben oder eventuell gewählte Lösungen zur Remote-Sicherung keinen ausreichenden Schutz der zu sichernden Daten bieten und somit sicherheitsrelevante Active Directory-Daten bei der Übertragung mitgelesen werden können.

Wird das Intervall zwischen zwei Datensicherungen zu groß gewählt, so werden bei der Wiederherstellung eines Domänen-Controllers unter Umständen zur Löschung markierte Active-Directory-Objekte eingespielt, deren Lebensdauer bereits überschritten ist. Dies kann zu Problemen bei der Replizierung zwischen Domänen-Controllern und damit zu Inkonsistenzen führen.

# G 2.128 Fehlende oder unzureichende Planung des VPN-Einsatzes

Wird ein Virtuelles Privates Netz (VPN) nicht sorgfältig geplant und aufgebaut, können einzelne Sicherheitslücken des VPNs die Sicherheit aller hiermit vernetzten IT-Systeme beeinträchtigen. Dies kann sogar dazu führen, dass über eine unzureichend gesicherte VPN-Verbindung ein damit gekoppeltes Behörden- oder Unternehmensnetz kompromittiert wird.

Bei fehlender oder unzureichender Planung können sich eine Vielzahl von Problemen ergeben:

- Aufgrund der Auswahl eines ungeeigneten Verschlüsselungsalgorithmus der VPN-Verbindung können Angreifer oder Konkurrenten unter Umständen geschäftskritische Informationen einer Institution erlangen.
- Die Anwendung starker kryptographischer Verfahren muss in bestimmten Ländern genehmigt werden. Dies kann bei Nichtbeachtung zu rechtlichen Konsequenzen führen.
- Bei Internet-basierten VPNs gibt es keine garantierten Laufzeiten. Bei zeitkritischen Anwendungen (zum Beispiel Echtzeit-Maschinensteuerungen) kann dies zu Problemen führen.
- Wenn in der Planung die benötigte Bandbreite nicht richtig eingeschätzt wurde, kann beispielsweise die Übertragungskapazität des VPNs unzureichend sein. Dadurch kann die Nutzung von Anwendungen, die den VPN-Kanal benötigen, eingeschränkt oder sogar verhindert werden.
- Ausbaustufen können unter Umständen nicht umgesetzt werden, wenn bei der Planung und Konzeption des VPNs auf mögliche Erweiterungen keine Rücksicht genommen wurde.
- Es können Komplikationen beim Integrieren der VPN-Endpunkte in bereits vorhandene Sicherheitsgateways entstehen. Diese sind oft darauf zurückzuführen, dass komplexe Einstellungen am Sicherheitsgateway vorgenommen werden müssen.

# G 2.129 Fehlende oder unzureichende Regelungen zum VPN-Einsatz

Die durch Virtuelle Private Netze (VPNs) verbundenen Rechner und Netze können nicht grundsätzlich als vertrauenswürdig eingestuft werden. Dies trifft insbesondere dann zu, wenn die angebundenen Rechner und Netze Fremdnetze sind und nicht selbst administriert werden. Unter diese Kategorie fallen beispielsweise Extranet-VPNs. Hierbei wird das eigene Netz mit Netzen anderer Firmen, unter Berücksichtigung funktionaler Einschränkungen und Sicherheitsanforderungen, verbunden. Für Unternehmen und Behörden kann ein großer Schaden entstehen, wenn sich Sicherheitslücken in einem externen Netz über VPN auf das eigene Netz auswirken.

Extranet-VPNs werden häufig in der Automobilindustrie bzw. in Branchen, die eine intensive Zusammenarbeit zwischen Hersteller und Zulieferer erfordern, angewendet.

Aufgrund fehlender oder unzureichender Regelungen zum VPN-Einsatz können unter anderem folgende Sicherheitsprobleme entstehen:

- Ein VPN sollte nicht "organisch wachsen". Vielmehr sollte vor dem Aufbau eines VPN-Zuganges eine Planung erfolgen. Die Erfahrung zeigt, dass insbesondere beim stetigen Ausbau von VPN-Zugängen komplexe Hard- und Software-Szenarien entstehen können, die schwer zu administrieren sind. Als Folge kann das dazu führen, dass Sicherheitseinstellungen falsch gewählt werden, inkompatibel zueinander sind oder sich gegenseitig aufheben.
- Ohne durchgängiges und verbindliches Sicherheitskonzept bleibt es in der Regel einzelnen Administratoren und VPN-Benutzern überlassen, die Sicherheitseinstellungen nach Gutdünken vorzunehmen. Dies kann zu ungeeigneten Sicherheitseinstellungen führen, die beispielsweise die Verbindungsaufnahme verhindern oder den Aufbau ungesicherter Verbindungen ermöglichen. Da mittels VPN angebundene IT-Systeme in vielen Fällen die gleichen Zugriffsmöglichkeiten wie direkt im LAN befindliche IT-Systeme haben, wird dadurch unter Umständen die Sicherheit des LANs beeinträchtigt.
- Die Sicherheit eines VPNs basiert auf dem Zusammenspiel der physikalischen Komponenten (Rechner, Netzkoppelelemente), deren Verbindungsstruktur (Netzaufteilung, Verbindungstopologie) und den Konfigurationen der jeweiligen Software-Komponenten. Die im Rahmen des VPN-Sicherheitskonzeptes festgelegten Regelungen und deren Umsetzung durch entsprechende Konfigurationseinstellungen können die gewünschte Sicherheit jedoch nur dann erbringen, wenn das tatsächlich installierte System mit dem geplanten System übereinstimmt. Oft ergeben sich jedoch, z. B. aufgrund von fehlenden Detailinformationen während der Planungsphase, nachträgliche Änderungen im physikalischen Aufbau. Werden die Änderungen nicht erfasst, dokumentiert und auf Auswirkungen auf die Informationssicherheit analysiert, so kann die Sicherheit der damit verbundenen Rechner und Netze gefährdet sein.
- VPN-Benutzer sind während der Nutzung in der Regel auf sich alleine gestellt. Existieren für den VPN-Einsatz keine dedizierten Regeln oder sind diese den Benutzern nicht bekannt, so können durch die Benutzer unbewusst Sicherheitslücken geschaffen werden.
- Werden datenschutzrechtlicher Belange bei der Übertragung personenbezogener Daten zwischen den Komponenten des VPNs nicht ausreichend beachtet, kann es zu Gesetzesverstößen kommen. Auch bei anderen Da-

ten können durch gesetzliche Vorgaben bestimmte Sicherheitsmaßnahmen vorgeschrieben sein.

**Beispiele:**

- Aufgrund fehlender Regelungen zum VPN-Einsatz erhielt ein Zulieferer weit reichende Zugriffsberechtigungen auf das Netz und dadurch auch Zugriff auf vertrauliche Dokumente eines Herstellers. Diese gelangten an die Öffentlichkeit, und es entstanden für den Hersteller erhebliche finanzielle Schäden.
- Ein Halbleiterhersteller ist mittels eines Extranet-VPNs an seine Zulieferer angebunden. Durch mangelhafte Virenschutzmaßnahmen seitens eines Zulieferers gelangte Schadsoftware über das VPN in das lokale Firmennetz des Halbleiterherstellers und verursachte massive Störungen.
- Der Administrator des VPNs einer Behörde ließ nur mit Triple-DES-Verfahren verschlüsselte Verbindungen zu, ein Benutzer hatte jedoch für den VPN-Client keine Verschlüsselung konfiguriert. Aufgrund von inkompatiblen Sicherheitseinstellungen konnte daher keine Verbindung aufgebaut werden.
- Bei der Einrichtung des VPNs in einem Unternehmen wurde aufgrund ungünstiger Leitungsführung eine zusätzliche kleine ISDN-Anlage installiert. Da dieses zusätzliche Gerät in der Planung nicht erfasst wurde, wurde versäumt, es im VPN-Sicherheitskonzept zu berücksichtigen. Als Folge bestand über lange Zeit bei aufgebauter VPN-Verbindung nun beispielsweise die Möglichkeit, über den mit einem Standardpasswort gesicherten Fernwartungszugang auf das Gerät zuzugreifen.

# G 2.130 Ungeeignete Auswahl von VPN-Verschlüsselungsverfahren

Die Bedeutung eines geeigneten VPN-Verschlüsselungsverfahrens nimmt mit dem Datendurchsatz im VPN, aber auch mit dem Schutzbedarf der verarbeiteten Informationen zu. Wenn ein ungeeignetes Verschlüsselungsverfahren ausgewählt wurde, werden schützenswerte Informationen bei der Übertragung über unsichere Netze vielen Gefahren ausgesetzt.

Insbesondere statische kryptographische Schlüssel und Pre-Shared Keys ("vorher vereinbarte Schlüssel" oder kurz PSK) sind hierbei anfällig gegenüber Angriffen mittels Kryptoanalyse. Ferner kann die Wahl eines PSKs Einfluss auf die Sicherheit haben, beispielsweise in Bezug auf Wörterbuch- und Brute-Force-Attacken.

Fällt eine Authentisierungskomponente aus, kann es bei einer mangelhaften Notfallplanung (z. B. fehlende Redundanz) zu empfindlichen Betriebsstörungen kommen, wenn sich Benutzer dadurch nicht anmelden und das VPN nutzen können.

**Beispiele:**

- Die Verwendung statischer kryptographischer Schlüssel birgt große Sicherheitsnachteile. Da die Schlüssel häufig für lange Zeiträume unverändert bleiben, werden hiermit in vielen Fällen große Datenmengen verschlüsselt. Dies erleichtert eine Kryptoanalyse der verschlüsselten Daten erheblich und steigert gleichzeitig den Nutzen ihrer Ergebnisse.
- In einem Unternehmen wird ein einziger PSK für die gesamte VPN-Infrastruktur verwendet. Dies führt im Falle einer Kompromittierung zu einer erheblichen Beeinträchtigung der Sicherheit.

# G 2.131 Unzureichende Kontrolle von VPNs

Ein Virtuelles Privates Netz (VPN) ist ein potentielles Ziel von Angriffen, sei es, um dieses unberechtigt nutzen zu können, um die darüber laufende Kommunikation abzuhören oder um dessen Verfügbarkeit zu stören (DoS-Angriffe). Solche Angriffe können eine empfindliche Störung sowohl der mit dem VPN verbundenen Infrastruktur als auch aller verbundenen Applikationen nach sich ziehen.

Wenn ein VPN und dessen Komponenten nicht ausreichend kontrolliert werden, ist es schwer, Angriffe überhaupt und zeitnah zu erkennen. Je länger ein potentieller Angreifer unbemerkt auf ein VPN zugreifen kann, desto größer ist die Gefahr für das Unternehmen oder die Behörde, dass beispielsweise vertrauliche Daten mitgelesen werden. Um solchen Gefahren entgegen zu wirken, werden meist Protokollierungsfunktionen eingesetzt. Oft wird jedoch nicht berücksichtigt, dass ohne Auswertung der Protokolldaten kein Sicherheitsgewinn zum Tragen kommt.

**Beispiel:**

- Ein Angreifer umgeht die Authentisierung eines Unternehmens-VPNs mittels einer Brute-Force-Attacke. Der Angriff wird vom VPN-Gateway protokolliert. Da der zuständige Administrator aber wegen Überlastung die Protokolle nur sporadisch kontrolliert, wird der Angriff nicht zeitnah erkannt. Dem Angreifer ist es somit möglich, über einen längeren Zeitraum sowohl auf das interne Netz des Unternehmens als auch auf die angebundenen Netze von Zulieferern zuzugreifen.

# G 2.132 Mangelnde Berücksichtigung von Geschäftsprozessen beim Patch- und Änderungsmanagement

In Behörden und Unternehmen sollten sich die Informationssicherheitsprozesse ebenso wie die Sicherheitsmaßnahmen an den Geschäftszielen und Geschäftsprozessen der Institution orientieren. Die im Rahmen des Patch- und Änderungsmanagements durchgeführten Veränderungen an IT-Systemen können die Effizienz von einzelnen Sicherheitsmaßnahmen verringern und damit zu einer Gefährdung der Gesamtsicherheit führen. Ungeeignete Patches und Änderungen können unter anderem den reibungslosen Ablauf der Geschäftsprozesse beeinträchtigen oder gar den kompletten Ausfall der beteiligten IT-Systeme verursachen. Auch ein noch so umfangreiches Testverfahren kann nicht vollkommen ausschließen, dass sich ein Patch oder eine Änderung im späteren Produktivbetrieb in speziellen Konstellationen als fehlerbehaftet erweist.

Wird im Laufe des Patch- und Änderungsprozesses die Auswirkung, Kategorie oder Priorität einer eingereichten Änderungsanforderung (RfC, Request for Change) in Bezug auf die Geschäftsprozesse falsch eingeschätzt, kann sich das angestrebte Sicherheitsniveau verringern. Solche Fehleinschätzungen sind überwiegend das Resultat mangelnder Abstimmung zwischen den IT-Verantwortlichen und den zuständigen Fachabteilungen.

Indem Änderungen und Patches eingespielt werden, können zwar Sicherheitslücken geschlossen, aber auch unbeabsichtigt ein großer Schaden angerichtet werden. Beispielsweise könnte durch einen fehlerhaften Patch eine größere Sicherheitslücke entstehen oder die Verfügbarkeit einer Applikation beziehungsweise eines Geschäftsprozesses reduziert werden.

**Beispiele:**

- In einem Unternehmen der Finanzwirtschaft kommt es durch zeitnahes, aber nicht mit den Fachabteilungen abgestimmtes Verteilen ("Rollout") von Sicherheitspatches immer wieder zu Einschränkungen in der Verfügbarkeit einer geschäftskritischen Reporting-Anwendung. In Folge kann ein wichtiger Berichtstermin bei der Aufsichtsbehörde nicht eingehalten werden und das Unternehmen wird mit einem Bußgeld belegt.
- In einem Unternehmen wird eine neue Version einer Handelssoftware zur Kommunikation mit externen Partnern entwickelt und aktualisiert. Da die serverseitige Komponente nun viel umfangreicher ist und mit mehr Clients kommunizieren muss, wurde in der neuen Version auf die bisher eingesetzte SSL-Verschlüsselung verzichtet, ohne dass dies mitgeteilt wurde. Da die Handelspartner vertraglich die Software einsetzen müssen, erfolgt die für die Geschäftsprozesse wichtige Kommunikation unverschlüsselt.

# G 2.133 Mangelhaft festgelegte Verantwortlichkeiten beim Patch- und Änderungsmanagement

Auch im Rahmen des Patch- und Änderungsmanagements sollten eindeutige Verantwortlichkeiten festgelegt werden. Treten Situationen ein, in denen die Verantwortlichkeiten nicht oder fehlerhaft geregelt sind, können erhebliche Nachteile entstehen. Beispielsweise könnten ungeregelte Zuständigkeiten dazu führen, dass gravierende Sicherheitslücken nicht zeitnah geschlossen werden, da niemand die Verantwortung für einen Notfallpatch tragen will.

Mangelhaft festgelegte, sich überschneidende oder ungeklärte Verantwortlichkeiten im Patch- und Änderungsmanagement verlangsamen das Einordnen der Änderungsanforderungen (Requests for Change) in Kategorien und die Vergabe von Prioritäten und damit das gewünschte Verteilen der Patches und Änderungen ("Rollout"). Auch die vorschnelle Freigabe einer Änderung oder eines Patches, ohne Testlauf und Berücksichtigung aller (fachlichen) Aspekte, kann gravierende Auswirkungen auf die Sicherheit haben.

Im Extremfall können mangelhaft festgelegte Verantwortlichkeiten die gesamte Institution komplett oder in großem Umfang beeinträchtigen. Störungen im Betrieb wirken sich auf die Verfügbarkeit aus, die nicht erfolgte Verteilung von sicherheitsrelevanten Patches auf die Vertraulichkeit bzw. Integrität.

**Beispiele:**

- In einem Unternehmen sind für das Patch- und Änderungsmanagement in den Fachabteilungen keine Ansprechpartner festgelegt. Daher kommt es immer wieder zu Verzögerungen bei der Festlegung von Prioritäten der Änderungsanforderungen. Außerdem ist es nur schwer möglich, die Auswirkungen von Änderungen auf die Geschäftsprozesse abzuschätzen. Als Sicherheitslücken in einer Software bekannt wurden, konnten zeitkritische Notfall-Patches nicht rechtzeitig eingebracht werden, so dass sie unbemerkt als Einfallstor für ein Trojanisches Pferd dienten.
- In einer Behörde wurde die Änderung eines IT-Systems ohne vorherigen Kontakt zur Fachabteilung durchgeführt. Die Abteilung konnte sich weder darauf einstellen noch der Änderung zustimmen. Zusätzlich fielen durch das Einspielen einige IT-Systeme der Anwender aus, ohne die wichtige Aufgaben nicht durchgeführt werden konnten.

# G 2.134 Unzureichende Ressourcen beim Patch- und Änderungsmanagement

Um ein wirkungsvolles Patch- und Änderungsmanagement einführen und betreiben zu können, sind angemessene personelle, zeitliche und finanzielle Ressourcen erforderlich. Werden diese nicht zur Verfügung gestellt, kann das vielfältige negative Auswirkungen haben. Es kann beispielsweise dazu führen, dass

- die notwendigen Rollen nicht mit geeigneten Personen besetzt werden,
- die Schnittstellen für bestimmte Informationen, beispielsweise entsprechende Ansprechpartner in den Fachbereichen, nicht geschaffen werden oder
- die erforderlichen Kapazitäten für die Infrastruktur der Test- und Verteilungsumgebungen nicht bereitgestellt werden.

Können die personellen, zeitlichen und finanziellen Mängel im Regelbetrieb häufig noch ausgeglichen werden, werden sie unter hohem Zeitdruck, beispielsweise wenn Notfall-Patches eingespielt werden, um so deutlicher.

**Beispiele:**

- Der Mangel an personellen Ressourcen innerhalb des Patch- und Änderungsmanagements kann zu einer Überlastung der zuständigen Mitarbeiter führen. Die alltägliche Arbeit an geplanten Patches und Änderungen verläuft weitgehend reibungslos, jedoch ist proaktives oder zeitnahes, reaktives Verteilen von aktuellen Sicherheitspatches nicht mehr möglich. Die Institution ist damit kaum in der Lage; schnell auf neue Bedrohungen der Sicherheit zu reagieren.
- Steht nicht genug Zeit zum Testen eines Patches oder einer Änderung zur Verfügung, oder besteht kein beziehungsweise nur eingeschränkter Zugriff auf eine dem Produktivsystem analoge Testumgebung, werden unzureichend getestete Patches und Änderungen in eine komplexe Umgebung verteilt. Die Folge können Probleme mit der Stabilität oder dem reibungslosen Zusammenarbeiten der beteiligten Betriebssysteme, Anwendungen und Datenbankmanagementsysteme sein.

# G 2.135 Mangelhafte Kommunikation beim Patch- und Änderungsmanagement

Die am Patch- und Änderungsmanagement beteiligten Personen sollten sich im Rahmen des Änderungsprozesses regelmäßig austauschen, um unter anderem die Kategorie und die Priorität einer Änderungsanforderung abzustimmen und um einen geeigneten Zeitpunkt für die Verteilung (Rollout) einer Änderung zu finden.

Wenn die am Patch- und Änderungsmanagement beteiligten Personen mangelhaft kommunizieren oder wenn das Patch- und Änderungsmanagement innerhalb der Institution wenig akzeptiert wird, kann dies dazu führen,

- dass Änderungsanforderungen verzögert bearbeitet werden, oder
- über die Annahme einer Änderungsanforderung falsch entschieden wird.

Damit einhergehend kann das Sicherheitsniveau verringert werden und es kann weiter zu ernsthaften Störungen im IT-Betrieb führen. In jedem Fall wird bei mangelhafter Kommunikation der Patch- und Änderungsprozess ineffizient, da er oft mit zu viel Zeit- und Ressourcenaufwand durchgeführt wird.

Ein ineffizienter Patch- und Änderungsprozess wirkt sich negativ auf die Reaktionsfähigkeit der Institution aus, und kann im Extremfall dazu führen, dass Sicherheitslücken entstehen oder wichtige Geschäftsziele nicht erreicht werden.

**Beispiel:**

- In einem Unternehmen wurde die Bedeutung und Vorgehensweise des Patch- und Änderungsmanagements für die Institution den beteiligten Abteilungen, wie beispielsweise der umsetzenden IT-Abteilung und den beauftragenden Fachabteilungen, nicht ausreichend erläutert. Daher wurden Anfragen an Fachabteilungen zu anstehenden Änderungen von diesen nur langsam beantwortet. Außerdem wurde von der IT-Leitung zu wenig Zeit und personelle Ressourcen für die Planung und Durchführung eines Patches oder einer Änderung zur Verfügung gestellt. Durch diese Mängel konnten sich bei der Umsetzung von Änderungen immer wieder Fehler einschleichen, die verschiedene Sicherheitslücken verursachten.

# G 2.136 Fehlende Übersicht über den Informationsverbund

Ohne Überblick über die wesentlichen schützenswerten Informationen, Geschäftsprozesse und IT-Strukturen einer Institution ist weder ein umfassendes Sicherheitsmanagement noch ein funktionierender IT-Betrieb möglich. Dabei müssen nicht nur die technischen Komponenten, sondern auch deren Vernetzung und die räumliche Infrastruktur sowie die Abhängigkeiten der verschiedenen Komponenten untereinander erfasst werden.

Ohne detaillierte Informationen darüber, wo in einer Institution welche IT-Systeme und Anwendungen eingesetzt und welche Geschäftsprozesse und Fachaufgaben damit unterstützt werden, ist z. B. auch kein wirkungsvolles Patch- und Änderungsmanagement möglich. Aus diesem Grund wird eine stets aktuelle und vollständige Bestandsaufnahme aller servicerelevanten Elemente, beispielsweise Netzkomponenten, Server, Clients, Anwendungen und deren Beziehung zueinander benötigt. Dabei ist der Detaillierungsgrad sehr wichtig. Eine zu große Detailtiefe führt zu Unübersichtlichkeit sowie zu gesteigertem Pflegeaufwand. Eine oberflächliche oder unvollständige Bestandsaufnahme der relevanten Elemente kann beispielsweise zur Folge haben, dass diese vom Patch- und Änderungsprozess nicht oder unzureichend erfasst und versorgt werden. Eine Verletzung der Sicherheitsziele der Institution ist in einem solchen Fall nur noch eine Frage der Zeit.

**Beispiele:**

- Ein Unternehmen verwaltet in einer Datenbank zahlreiche Informationen für das Patch- und Änderungsmanagement. Als eine neue Softwareversion der verwalteten IT-Systeme installiert werden soll, initiiert der Änderungsmanager die Aktualisierung, indem die installierte Version mit der neuen, verfügbaren Version verglichen wird. Aufgrund von mangelnden personellen Ressourcen wurde allerdings versäumt, die Datensätze zur installierten Softwareversionen aktuell zu halten. Als Folge dieses Versäumnisses wurden Softwareversionen mit gravierenden Sicherheitsschwachstellen übersehen und nicht aktualisiert. Diese Schwachstellen konnten von einem Angreifer ausgenutzt und vertrauliche Informationen ausgelesen werden.
- In einem Unternehmen werden die Softwarestände und Lizenzen nicht angemessen verwaltet. Dadurch wird bei einigen wichtigen Anwendungen nicht bemerkt, dass der Hersteller für die in der Institution verwendeten Versionen keine Sicherheitspatches mehr zur Verfügung stellt. Auftretende Sicherheitslücken konnten daher nicht zeitnah geschlossen werden.

# G 2.137 Fehlende und unzureichende Planung bei der Verteilung von Patches und Änderungen

Damit Patches und Änderungen in der vorgesehenen Zeitspanne in einer Institution verteilt werden können, müssen im Rahmen des Patch- und Änderungsmanagements die hierfür nötigen technischen und personellen Ressourcen eingeplant werden. Stehen keine ausreichenden Ressourcen zur Verfügung, besteht die Gefahr, dass die Verteilung von Änderungen länger dauert als geplant oder sogar fehlschlägt. Dadurch könnten Geschäftsprozesse mit hohen Verfügbarkeitsanforderungen beeinträchtigt werden, wenn z. B. hierfür benötigte Server oder Datenbanken ausfallen.

Patches und Änderungen können auch softwarebasiert verteilt werden. Wenn die hierfür benutzte Software sich allerdings nicht an die wachsende und komplexer werdende IT-Landschaft anpassen lässt, wird die Verteilung letztendlich zeitintensiver. Dadurch können Sicherheitsupdates nicht mehr zeitnah verteilt werden.

Teilweise ist die Reihenfolge, in der Patches und Änderungen verteilt werden müssen, für die Konsistenz und Sicherheit des gesamten Systems relevant. Beispielsweise könnte eine neue Version einer Sicherheitssoftware ein Betriebssystem erfordern, bei dem alle aktuellen Patches eingespielt sind. In diesem Fall sind zuerst die Betriebssysteme im Informationsverbund zu aktualisieren, gegebenenfalls neu zu starten und dann kann erst die neue Sicherheitssoftware aufgespielt werden. Eine Verteil-Software, die nicht die schon vorhandenen Patches und Änderungen prüft, könnte versuchen, die Sicherheitssoftware vor dem gelungenen Betriebssystemupdate zu installieren. Dadurch würde sie ein inkonsistentes oder sogar ungepatchtes System hinterlassen.

Wird Software auf IT-Systemen aktualisiert, muss anschließend oft die Anwendung oder das Betriebssystem neu gestartet werden. Komplexe Anwendungen wie Datenbanken benötigen einige Zeit, um nach einem Update ihre Daten wieder zur Verfügung zu stellen. In dieser Zeit sind die Anwendungen und Daten der Systeme nicht verfügbar. Bei Systemen mit hohen Anforderungen an die Verfügbarkeit kann das negative Auswirkungen für die Institution haben. Dies ist besonders der Fall, wenn die Systeme auf Grund von Fehlern während des Änderungsvorganges länger als geplant nicht verfügbar sind. Solche Ausfälle können dazu führen, dass Mitarbeiter oder Kunden bei ihrer Arbeit beeinträchtigt werden.

**Beispiele:**

- In einer Institution wird ein Sicherheitspatch für einen Windows Server eingespielt. Dieser muss anschließend neu gestartet werden. Das System ist in dieser Zeit nicht verfügbar. Da auf diesem Server der Anmeldeprozess an das interne LAN läuft, können sich die Benutzer während dieser Zeit nicht anmelden und nur eingeschränkt arbeiten. Die Institution hat mit ihren Kunden ein hohes Verfügbarkeitsniveau durch Service Level Agreements vereinbart und verstößt auf diese Weise gegen bestehende Verträge.
- Die IT-Abteilung eines Unternehmens installiert einen Sicherheitspatch auf einem Voice-over-IP-Server. Beim Neustart des Systems muss zusätzlich noch die Konfigurationsdatei des VoIP-Dienstes angepasst werden. In dieser Zeit können keine externen Anrufe entgegen genommen werden. Die mangelnde Erreichbarkeit des Unternehmens wirkt sich negativ auf die Außenwahrnehmung bei Kunden aus.

# G 2.138 Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement

Der Vorgang, mit dem gelöschte oder beschädigte Daten, Anwendungen oder bestimmte Konfigurationen rekonstruiert werden, zum Beispiel dadurch, dass Daten aus einer Datensicherung wieder eingespielt werden, wird Wiederherstellung genannt. Da es immer wieder zu unvorhersehbaren Komplikationen kommen kann, nachdem komplexe Patches und Änderungen verteilt wurden, sollte vorher stets ein Wiederherstellungspunkt bestimmt werden. Zu diesem kann im Notfall zurückgekehrt und der produktive Betrieb sichergestellt werden.

Sind bei der Verteilung von Änderungen keine Optionen zur Wiederherstellung vorgesehen oder die Wiederherstellungsroutinen der eingesetzten Software nicht oder nicht angemessen wirksam, können die negativen Auswirkungen einer fehlerhaft aktualisierten Software nicht zeitnah korrigiert werden. Der damit verbundene Ausfall der IT-Infrastruktur kann für die Institution erhebliche Schäden verursachen.

In der Regel müssen die betroffenen Systeme zur Schadensbegrenzung zeitnah wiederhergestellt werden. Unangemessene oder gar fehlende Optionen zur zeitnahen Wiederherstellung können in diesem Fall besonders hohe Folgeschäden verursachen.

**Beispiel:**

- Beim Aktualisieren einer Datenbank-Applikation während des Patch- und Änderungsprozess wird deren Konfigurationsdatei überschrieben. Im Verlauf des Updates stellt heraus, dass die aktualisierte Datenbank-Applikation zu Webapplikationen inkompatibel ist, die auf die Datenbank zugreifen sollen. Dieses Problem lässt sich nicht zeitnah beheben. Da die alte Softwareversion nebst ihrer Konfiguration nicht für die Wiederherstellung gespeichert wurde und eine neue Konfiguration mühsam erstellt werden muss, fallen die Datenbank und auch die wichtigen Webapplikationen für einen längeren Zeitraum aus.

# G 2.139 Mangelhafte Berücksichtigung von mobilen Endgeräten beim Patch- und Änderungsmanagement

Die wachsende Mobilität von Endgeräten ist eine der besonderen Herausforderungen für das Patch- und Änderungsmanagement. Mobile Systeme sind durch ihren wechselnden Einsatzort und ihre Anbindung an bestehenden Netze durch Funktechnologien nicht immer in die automatisierte Verteilung von Patches und Änderungen eingebunden.

Zusätzlich ist bei mobilen Endgeräten üblicherweise nicht die gleiche Bandbreite und Stabilität bei der Datenübertragung wie bei stationären Systemen in einem LAN gewährleistet. Das Anlegen von Sicherheitskopien sowie Wiederherstellungspunkten dauert im Vergleich länger und funktioniert weniger zuverlässig.

Werden mobile Systeme bei der Planung von Patches und Änderungen nicht gesondert berücksichtigt, kann die Verteilung nur unvollständig durchgeführt werden, nimmt mehr Zeit in Anspruch als geplant und bedeutet auch immer ein Sicherheitsrisiko.

**Beispiel:**

- Die von einem Unternehmen beschafften Mobiltelefone lassen sich nur via Verbindung an einen Rechner aktualisieren. Dazu müssen die Benutzer die mobilen Geräte an die IT-Abteilung des Unternehmens übergeben. Nachdem eine gravierende Schwachstelle in der Bluetooth-Implementierung entdeckt und ein Sicherheitspatch veröffentlich wurde, konnten Angreifer von einigen Geräten wichtige Informationen auslesen, da die entsprechenden Mitarbeiter ihre Geräte nicht zeitnah zur Aktualisierung abgegeben hatten.

# G 2.140 Unzureichendes Notfallvorsorgekonzept für das Patch- und Änderungsmanagement

Das Patch- und Änderungsmanagement trägt zur technischen Umsetzung von Informationssicherheit in einer Institution bei. Die von diesem Prozess verwendeten IT-Systeme sind in der Regel als kritisch für den IT-Betrieb anzusehen. Dazu gehören beispielsweise die zentralen Server für die Verteilung der Patches und Änderungen, die Datenbanken mit den aktuellen Konfigurationen der IT-Systeme sowie die Backupserver für das Anlegen von Wiederherstellungspunkten. Fällt zum Beispiel der Server aus, der die Patches und Änderungen verteilt, können eventuell neu erscheinende kritische Updates nicht mehr zeitnah eingespielt werden.

Des Weiteren können fehlende Datensicherungen der aktuellen Konfigurationen der IT-Systeme dazu führen, dass in einem Notfall nicht mehr sichergestellt ist, dass wichtige IT-Komponenten möglichst schnell wieder in den ursprünglichen Zustand versetzt werden können.

**Beispiel:**

- Zur Unterstützung des Patch- und Änderungsmanagements wird in einem Unternehmen eine Applikation eingesetzt, die in regelmäßigen Abständen Wiederherstellungspunkte auf einen Backupserver ablegt. Als bei einem Notfall ein System vom Backupserver wiederhergestellt werden soll, stellt sich heraus, dass das System seit einiger Zeit keine Backups mehr aufnehmen konnte, da die Platte über keinen freien Speicherplatz mehr verfügte, aber niemand auf die entsprechenden Fehlermeldungen des Systems reagiert hat. Dadurch konnte die Wiederherstellung zunächst nur mit einem veralteten Softwarestand durchgeführt werden, auf den einige weitere Sicherheitspatches aufgespielt werden mussten.

# G 2.141 Nicht erkannte Sicherheitsvorfälle

Im täglichen IT-Betrieb einer Behörde oder eines Unternehmens können eine hohe Anzahl von Störungen und Fehlern auftreten. Dabei besteht die Gefahr, dass Sicherheitsvorfälle durch das Personal nicht als solche identifiziert werden und ein Angriff bzw. Angriffsversuch unerkannt bleibt. Auch wenn die Benutzer und Administratoren ausreichend für die Belange der Informationssicherheit sensibilisiert bzw. geschult sind, kann es dazu kommen, dass sie Sicherheitsvorfälle nicht erkennen.

Beispiele hierfür sind:

- Die Beeinträchtigung der Kapazität der Internetanbindung wird auf die mangelnde Leistung des Internet Service Providers geschoben, ohne eine genaue Verkehrsanalyse durchzuführen. Die wirkliche Ursache für die Kapazitätseinbußen ist aber ein kompromittierter Server im LAN, der als illegaler Dateiserver benutzt wird und dadurch Bandbreite konsumiert.
- Ein Benutzer bekommt bei der Anmeldung an einer IT-Anwendung den Hinweis, dass er das letzte Mal am Sonntagmorgen angemeldet war, obwohl er am Wochenende nicht gearbeitet hat. Der Benutzer schöpft keinen Verdacht und meldet diesen Vorfall nicht dem Sicherheitsverantwortlichen. Dadurch bleibt die Tatsache verborgen, dass ein Angreifer Zugang zum Benutzerprofil des Benutzers oder dessen Passwort ermittelt hat.
- Ein Notebook-Benutzer, der seit längerer Zeit nicht im lokalen Netz seiner Firma oder Behörde angemeldet war, hält die seit einer Woche auftretende extreme Verlangsamung seines Notebooks während des Internetzugangs für normales Verhalten und bemerkt nicht, dass ein trojanisches Pferd aktiv ist. Er wurde nicht geschult, bei verdächtigen Auffälligkeiten den Sicherheitsverantwortlichen zu informieren.
- Ein Geschäftsreisender bemerkt nicht, dass die Daten seines Notebooks während eines Auslandsaufenthalts heimlich ausgespäht wurden. Er schöpft keinen Verdacht, als sein Notebook in seinem Hotelzimmer für kurze Zeit verschwunden ist und plötzlich wieder auftaucht.
- Ein Einbruchsdiebstahl in einer Filiale wird für einen Fall von Beschaffungskriminalität gehalten, da Notebooks und Flachbildschirme entwendet wurden. Der Tatsache, dass sich auf den Notebooks vertrauliche Informationen und Zugangsdaten für Systeme im Intranet befunden haben, wird keine größere Bedeutung beigemessen und der Sicherheitsverantwortliche nicht informiert. Auf die nachfolgenden Angriffe auf die IT-Systeme anderer Standorte und der Firmenzentrale ist das Unternehmen daher nicht vorbereitet. Für die Planung und Durchführung des Angriffs werden die auf den gestohlenen Notebooks gefundenen Daten verwendet.

# G 2.142 Zerstörung von Beweisspuren bei der Behandlung von Sicherheitsvorfällen

Wenn bei der Behandlung von Sicherheitsvorfällen unvorsichtig oder nicht nach Vorgaben agiert wird, kann es dazu führen, dass wichtige Beweisspuren für die Aufklärung oder spätere juristische Verfolgung unbeabsichtigt zerstört werden.

Beispiele hierfür sind:

- Ein Administrator stellt auf seinem System fest, dass der zur Verfügung stehende Speicherplatz schlagartig kleiner wird und keine Daten mehr gespeichert werden können. Um schnell Speicherplatz freizumachen, löscht er sofort alle Protokolldateien. Diese Protokolldateien hätten jedoch bei einer späteren Untersuchung eventuell enthüllt, dass der Server angegriffen wurde und die möglichen Quellen gezeigt.
- Auf einem PC hat ein Angreifer einen Computer-Virus oder ein trojanisches Pferd hinterlassen, dessen Arbeitsweise und Ziel nur im laufenden Zustand analysiert werden kann. Dafür müssten Informationen über die aktiven Prozesse und der Hauptspeicherinhalt gesichert werden. Wird das betroffene System voreilig ausgeschaltet, können diese Informationen nicht mehr für die Analyse und Aufklärung des Sicherheitsvorfalls herangezogen werden.
- Auf einem Server wird durch einen Administrator ein laufender Prozess gefunden, der in den letzten Tagen sehr viel Rechenzeit verbraucht hat. Zusätzlich schreibt dieser Prozess viele temporäre Dateien auf die Festplatten und versendet unbekannte Informationen über das Internet. Wird der Prozess voreilig beendet und die unbekannten Dateien gelöscht, kann eventuell nicht herausgefunden werden, ob es sich um ein Angriffswerkzeug handelte und ob vertrauliche Daten versendet wurden.
- Ein wichtiger Server wird kompromittiert, weil der Administrator durch die starke Arbeitsbelastung und ein fehlendes Wartungsfenster die letzten Sicherheitsupdates nicht einspielen konnte. Um möglichen disziplinarischen Konsequenzen zu entgehen, spielt der Administrator die fehlenden Updates ein, bevor ein Sicherheitsteam die Einbruchsursache und den entstandenen Schaden analysieren kann. Mangelnde Fehlerkultur hat somit eine Analyse des Problems verhindert.

# G 2.143 Informationsverlust beim Kopieren oder Verschieben von Daten auf Samba-Freigaben

In vielen Fällen wird Samba als Dateiserver für Windows-Systeme genutzt. Windows (ab Windows NT) setzt standardmäßig das New Technology File System (NTFS) als Dateisystem ein. Samba wiederum nutzt das Dateisystem des darunterliegenden Unix Betriebssystems um die Daten zu verwalten. Die Dateisysteme, die von Windows und Unix eingesetzt werden, unterscheiden sich teilweise sehr stark.

Dateisysteme die von Unix-artigen Betriebssystemen verwendet werden, wie third extended file system (ext3) oder Journaled File System (JFS), können bestimmte Eigenschaften von NTFS nicht vollständig abbilden. Samba kann diese Unterschiede in der Regel ausgleichen, in einigen Fällen kann Samba Eigenschaften von NTFS-Dateisystemobjekten aber nicht direkt berücksichtigen. Beim Kopieren oder Verschieben von Dateisystemobjekten über Systemgrenzen hinweg (beispielsweise von einem Windows XP System auf eine Dateifreigabe eines Samba-Servers) können unter Umständen Informationen verloren gehen, wenn sich Administratoren solcher Effekte nicht bewusst sind.

Folgende Informationen können vom Verlust betroffen sein:

- Access Control Lists (ACLs)
- Alternate Data Streams (ADS)
- DOS-Attribute

**Beispiel 1: Access Control Lists (ACLs)**

Beim Verschieben von Dateisystemobjekten von einer NTFS-Partition eines Windows-Systems auf eine Samba Dateifreigabe können ACL-Einträge verloren gehen. Vor dem Kopiervorgang hat der Besitzer der Datei die NT-Berechtigung "Vollzugriff" und die Gruppe "Jeder" hat die NT-Berechtigung "Lesen, Ausführen". Nachdem die Datei verschoben wurde, hat der Besitzer der Datei die NT-Berechtigung "Vollzugriff", die Gruppe "Jeder" hat keinerlei Berechtigungen mehr.

**Beispiel 2: Alternate Data Streams (ADS)**

Windows XP legt (ab Service Pack 2) sogenannte "Zone Identifier" in den ADS von Dateien ab. Diese "Zone Identifier" ermöglichen es auch im Nachhinein, Dateien zu erkennen, die aus dem Internet heruntergeladen wurden (beim Herunterladen fügt der Internet Explorer die entsprechenden "Zone Identifier" hinzu). Programme wie der Windows Explorer nutzen diese Informationen um Benutzer zu warnen, wenn diese eine aus dem Internet herunter geladene Datei ausführen wollen. Speichert der Internet Explorer die herunter geladene Datei auf einer Samba Dateifreigabe, die ADS nicht berücksichtigt, so gehen diese Informationen verloren. Ein Benutzer wird in Folge dessen nicht mehr gewarnt, bevor er diese potentiell gefährliche Datei ausführt.

**Beispiel 3: DOS-Attribute**

Das DOS-Attribut "Archiv" wird unter Windows bei jedem Schreibzugriff neu gesetzt. Sicherungsprogramme können diese Information für eine inkrementelle Sicherung nutzen. Berücksichtigt eine Samba Dateifreigabe dieses DOS-Attribut nicht, so kann es sein, dass ein Sicherungsprogramm keine neue Sicherung einer geänderten Datei erstellt.

# G 2.144 Unzureichende Notfall-Planung bei einem Samba-Server

Versäumnisse bei der Notfallvorsorge können den Betrieb von Samba stören oder zu längeren Ausfallzeiten führen. Zusätzlich zu allgemeinen Fehlern, die oft im Bereich Notfallvorsorge gemacht werden, können bei einem Samba-Server einige spezielle Fehler passieren, die eine schnelle Reaktion auf Zwischenfälle sehr erschweren oder gar unmöglich machen. Einige dieser Fehler werden im Folgenden beschrieben:

- Muss nach einem Notfall (etwa einem Angriff) der Samba-Servers neu installiert werden, sind dazu die bei der Installation verwendeten Installationspakete (Quelltextpakete oder Binärpakete) nötig. Daher kann es zu erheblichen Verzögerungen führen, wenn diese Pakete nicht mehr verfügbar sind weil sie beispielsweise auf dem kompromittierten System selbst gespeichert wurden. In diesem Fall ist es möglich, dass die Installationspakete ebenfalls manipuliert wurden. Die Neuinstallation des Samba-Servers aus den manipulierten Paketen könnte zu großen Sicherheitsproblemen führen.
- Sind die Kompilierungs- und / oder Installationsoptionen der Samba-Server nicht bekannt, kann es sehr schwierig sein, eine funktionell gleichwertige Installation wiederherzustellen. Ist es nicht möglich diese Installation wiederherzustellen, könnten optionale, für den Informationsverbund wichtige Funktionen, nicht von Samba bereitgestellt werden.
- Bei der Systemwiederherstellung nach einem Notfall kann es wünschenswert sein, einen älteren Stand der Konfiguration wieder herzustellen. Wird für die Konfigurationsdateien (insbesondere die Datei smb.conf) keine Versionsverwaltung verwendet, so kann dies schwierig oder gar unmöglich sein.
- Existiert keine oder nur eine unzureichende Dokumentation der Konfiguration, so kann es sehr schwierig sein, nach einem Notfall überhaupt wieder eine funktionierende Konfiguration herzustellen. Eine schlechte oder unzureichende Dokumentation kann auch dazu führen, dass Konfigurationsfehler zunächst nicht entdeckt werden und bei auftretenden Problemen eine aufwendige Fehlersuche erforderlich ist.

# G 2.145 Unzureichende Sicherung von Trivial Database Dateien unter Samba

Um die Konfiguration eines Samba-Servers ohne Verluste wiederherstellen zu können, ist je nach Funktion des Samba-Servers die Sicherung unterschiedlicher Systemkomponenten notwendig. Für eine konsistente Sicherung dieser Systemkomponenten müssen in der Regel keine speziellen Aspekte berücksichtigt werden.

Eine Ausnahme bilden die Trivial Database (TDB)-Dateien, die von Samba genutzt werden, um verschiedene Informationen abzuspeichern. Die Inhalte dieser Datenbanken werden vom Samba-Dienst oft länger im Hauptspeicher vorgehalten (gecacht). Daher sind die Inhalte auf der Festplatte nicht immer aktuell und die Größen und Zeitstempel der TDB-Dateien sind oft über lange Zeit unverändert. Werden diese Besonderheiten beim Erstellen einer Sicherung zur Laufzeit des Samba-Dienstes nicht berücksichtigt, droht der Verlust von Daten.

**Beispiele:**

- Während einer Dateisicherung wurde die Datei "winbindd_idmap.tdb" nicht korrekt gesichert. In dieser Datei werden Windows-Benutzern Unix Benutzer-IDs zugeordnet. Nach dem Wiederherstellen dieser Datei fehlen zehn der zuletzt von Winbind angelegten Zuordnungen. Es kann nicht mehr festgestellt werden, wie die fehlenden Benutzernamen zu den Unix Benutzer-IDs 1005621-105630 lauten. Vorhandene Dateien mit diesen Benutzer-IDs können somit keinem Besitzer mehr zugeordnet werden.
- Auf einem Samba-Server in einem Informationsverbund wird "tdbsam" zur Verwaltung von Kontoinformationen genutzt. Die Passwörter werden hierfür in der Datei "passdb.tdb" abgelegt. Eine Sicherung wurde nicht korrekt durchgeführt, weil der Administrator bei laufendem Samba-Server das Standard-Unix-Programm "cp" verwendet hat. Nach dem Wiederherstellen dieser Datei fehlen zwei, der zuletzt vom Administrator angelegten Benutzer.

# G 2.146 Verlust der Arbeitsfähigkeit von Vista-Clients durch fehlende Reaktivierung vor SP1

Für einen arbeitsfähigen Windows Vista Client müssen das Betriebssystem Windows Vista installiert und eine Windows Vista Lizenz aktiviert sein. Lizenzen für Windows Vista Enterprise können nur im Rahmen eines Volumenlizenzvertrags erworben werden. Die mit dieser Betriebssystemversion erstmals bestehende Notwendigkeit der Aktivierung von Windows Vista Lizenzen aus einem Volumenlizenzvertrag wird auch als Windows Vista Volume Activation 2.0 bezeichnet (Stand Herbst 2007). Windows Vista Volume Activation 2.0 unterscheidet die Aktivierungsformen:

- MAK-Proxyaktivierung (Multi Activation Key, Mehrfachaktivierungsschlüssel),
- MAK-unabhängige Aktivierung und
- KMS-Aktivierung (Key Management Server, Schlüsselverwaltungsserver).

Innerhalb dieser Aktivierungsformen gibt es weitere Unterschiede, die durch die unterstützten Kommunikationswege zum Austausch der Lizenzinformationen mit Microsoft begründet sind. Unterstützt werden Internet und Telefon.

An die Aktivierung einer Windows Vista Lizenz sind bestimmte Vorgaben verknüpft. Wird gegen diese verstoßen, fällt der Windows Vista Client automatisch in den so genannten RFM (Modus mit reduzierter Funktionalität, Reduced Functionality Mode). Im RFM ist der Vista Client solange nicht arbeitsfähig bis erfolgreich eine Windows Vista Lizenz für den Vista Client aktiviert wurde. Mit dem Erscheinen des Windows Vista Service Pack SP1 hat der Hersteller Microsoft den RFM zurückgenommen. Anstelle des RFM zeigt Windows Vista nun entsprechende Warnmeldungen an.

Folgende Vorgabenverstöße mit genau bekannten Kriterien lassen einen Windows Vista Client in den RFM fallen:

- keine Aktivierung innerhalb einer Kulanzfrist (Grace Period) von 30 Tagen nach der Installation von Windows Vista.
- keine erneute Aktivierung innerhalb von 210 Tagen nach der zuletzt erfolgten Aktivierung im Fall einer KMS-Aktivierung.

Folgende Vorgabenverstöße mit öffentlich nur vage bekannten Kriterien lassen einen Windows Vista Client ebenfalls in den RFM fallen:

- keine Reaktivierung innerhalb von 30 Tagen nach signifikanten Hardwaremodifikationen, wie einem Festplattentausch im Fall einer KMS-Aktivierung. Weitere öffentliche Details zu signifikanten Hardwareänderungen finden sich in dem Technical Market Bulletin *Product Activation for Windows Vista and Windows Server 2008* des Herstellers Microsoft vom September 2007.
- Manipulation des Aktivierungsprozesses oder von Lizenzdateien, genauere Angaben sind nicht bekannt.
- Kompromittierter Product Key.
  Der Ausdruck Product Key kann sich auf den MAK-Schlüssel und auf den KMS-Schlüssel beziehen. Kompromittiert kann verloren, gestohlen, missbraucht, illegal kopiert, defekt aufgrund Herstellungsfehler oder nicht mehr gültig da Beta- oder Testschlüssel bedeuten. Genauere Angaben sind nicht bekannt.

Die vagen Kriterien lassen einen Spielraum für so genannte False Positives. False Positive bedeutet im Zusammenhang der Aktivierung, dass sich ein Vi-

sta Client irrtümlich in den RFM versetzt. Dem kann beispielsweise die falsche Annahme zugrunde liegen, dass ein Product Key kompromittiert ist oder für die Lizenzierung relevante Dateien manipuliert sind.

Die vagen Kriterien begünstigen auch mögliche Kontrollverluste bei der Wartung von Vista Clients, weil nicht bekannt ist, welche Hardwaremodifikationen eine Reaktivierung erfordern. Liegen nicht rechtzeitig gültige Lizenzinformationen für eine Reaktivierung vor, dann droht der RFM.

Es besteht die Gefahr, dass die herstellerseitige, restriktive Gestaltung der Windows Vista Volume Activation auch durch den Administrator unverschuldet zum Verlust der Arbeitsfähigkeit der Vista Clients führen kann. Dann können Vista Clients und die auf ihnen laufenden Anwendungen nicht benutzt werden.

Der Verlust der Arbeitsfähigkeit eines Vista Clients kann den Verlust der Arbeitsfähigkeit einer Anwendung nach sich ziehen, die für die Erledigung einer Aufgabenstellung in einem Fachverfahren oder einem Geschäftsprozess unerlässlich ist.

# G 2.147 Fehlende Zentralisierung durch Peer-to-Peer

In vielen IT-Umgebungen werden zentrale Server eingesetzt, um Informationen auszutauschen. E-Mails werden von Clients zu E-Mail-Servern übermittelt und den Clients zum Empfang bereitgestellt. Dateien werden zentral auf einem Dateiserver den berechtigten Benutzern bereitgestellt und Druckserver ermöglichen den Zugriff auf zentrale Drucker.

Für Peer-to-Peer-Dienste werden für den Datenaustausch keine separaten Server benötigt, sondern die Clients ("Peers") stellen sich vorher freigegebene Ressourcen gegenseitig zur Verfügung. Dabei müssen sich die Peers nicht innerhalb eines LANs befinden, sondern können über öffentliche Netze, wie dem Internet, weltweit verteilt sein.

Durch die fehlende Zentralisierung können sich folgende Probleme ergeben:

**Fehlende Kontrolle durch Sicherheitsgateway (Firewall) und lokale Paketfilter**

Eine Peer-to-Peer-Kommunikation mit externen Kommunikationspartnern außerhalb des LANs setzt voraus, dass der interne Peer eine Verbindung zu den Externen oder dass der externe Peer eine Verbindung zu dem Peer im LAN aufbauen darf. Wenn dadurch aber jede Art von Kommunikationsverbindung aufgebaut werden darf, nimmt dies dem Paketfilter im Sicherheitsgateway die Möglichkeit, unerwünschte Pakete von vornherein abzuweisen. Da Port-Nummern oft dynamisch ausgehandelt werden, würde eine Begrenzung auf wenige offene Ports die Peer-to-Peer-Kommunikation behindern. Schutzmechanismen, wie beispielsweise, dass die Peers keine direkte Verbindung ins Internet aufbauen dürfen und einen Proxy nutzen müssen, wären wirkungslos. Wenn externe Kommunikationspartner direkt eine Verbindung zu IT-Systemen im LAN aufbauen dürfen, könnten sie zum Beispiel auch Denial-of-Service-Angriffe auf Clients durchführen oder nach Schwachstellen suchen, zum Beispiel mit Port-Scanning.

**Fehlende Filterung von Schadsoftware**

In einen Informationsaustausch mit anderen Benutzern muss bei Peer-to-Peer-Diensten eine direkte Datenverbindung zwischen den beteiligten Clients aufgebaut werden. Auf diese Weise können sich beispielsweise verschiedene Benutzer Dateien zusenden. Bei Verwendung eines Servers, beispielsweise für den Informationsaustausch über E-Mail, könnte dieser die empfangenen E-Mails auf Schadsoftware untersuchen, bevor er die E-Mail weiterleitet. Diese zusätzliche Instanz ist bei Peer-to-Peer-Diensten nicht vorhanden. Wird Schadsoftware über Peer-to-Peer-Dienste direkt von einem Peer im Internet zu einen Peer im LAN übertragen und ist der Virenschutz nicht ausreichend, kann auf diesen Weg Schadsoftware auf interne Clients gelangen und weitere IT-Systeme im LAN infizieren.

**Unkontrollierter Informationsabfluss**

Bei Peer-to-Peer-Diensten können Informationen ohne eine zentrale Filterung durch einen Server übertragen werden. Wurde beispielsweise ein E-Mail-Server so konfiguriert, dass E-Mails, die mit "Vertraulich" gekennzeichnet sind, nicht an Externe versendet werden, kann diese Hürde mit Peer-to-Peer-Diensten überwunden werden.

Um Peer-to-Peer-Dienste nutzen zu können, muss auf dem Client eine geeignete Peer-to-Peer-Applikation installiert werden. Solche Applikationen werden beispielsweise zum File-Sharing im Internet zur Verfügung gestellt. Dabei könnte eine Peer-to-Peer-Applikation mit einem Trojanischen Pferd infiziert sein, das beispielsweise alle Tastatureingaben des Benutzers protokolliert und diese direkt über den Peer-to-Peer-Dienst ins Internet überträgt. Wenn der Peer-to-Peer-Dienst zusätzlich SSL-verschlüsselt ist, würde ein solches Trojanisches Pferd nur schwer entdeckt werden können, da der Informationsfluss zwischen dem Angreifer und dem Peer nicht eingesehen werden kann.

**Unzureichende Protokollierungsmöglichkeiten**

Eine Protokollierung, mit wem kommuniziert und welche Informationen ausgetauscht wurden, kann bei Peer-to-Peer-Diensten nur mit erheblichen Aufwand auf dem Peer erfolgen. Die Protokolldaten könnten auch im Gegensatz zu einem zentralen Server einfacher an einem Peer manipuliert werden.

**Verschlüsselung**

Für einen verschlüsselten Informationsaustausch müssen mit jedem Benutzer, mit dem kommuniziert werden soll, zusätzliche Informationen ausgetauscht werden. Bei einer symmetrischen Verschlüsselung müssen beide Kommunikationspartner den gemeinsamen geheimen Schlüssel kennen. Auch bei einer asymmetrischer Verschlüsselung, bei der mit einem öffentlichen Schlüssel verschlüsselt und mit einem privaten Schlüssel entschlüsselt wird, kann der Sender sich nicht immer sicher sein, dass der öffentliche Schlüssel von dem Empfänger stammt.

Werden Zertifikate nicht überprüft, könnte ein Angreifer sie fälschen und sich direkt zwischen den Peers positionieren (Man-in-the-Middle-Angriff). Da bei Peer-to-Peer-Diensten oft keine zentrale Instanz vorhanden ist, die für die Verteilung der Schlüssel zuständig ist und deren Authentizität gewährleistet, werden die Zertifikate häufig nicht überprüft.

**Aufwändige Benutzerverwaltung**

Sowohl bei internen als auch öffentlichen Peer-to-Peer-Diensten müssen die Peers Ressourcen, auf die andere Peers zugreifen dürfen, freischalten. Um diese Informationen vor Unberechtigten zu schützen, können Freigaben beispielsweise mit Passwörtern und Benutzernamen geschützt werden.

Sollen zahlreiche Informationen an verschiedene Benutzer freigegeben werden, wird die Zuordnung, wer auf was zugreifen darf, schnell unübersichtlich. Oft kann auch nicht auf zentrale Authentisierungsdienste ("Single-Sign-On") zurückgegriffen werden, wenn sie zum Beispiel von zusätzlich installierten Peer-to-Peer-Applikationen nicht unterstützt werden.

**Suche und Versionspflege**

Im Gegensatz zu einem servergestützten Netz sind bei Peer-to-Peer-Netzen die Ressourcen auf zahlreiche IT-Systeme verteilt. Die Suche nach einer bestimmten Information, beispielsweise einer Datei, kann sehr aufwändig werden, wenn nicht bekannt ist, auf welchem IT-System sie sich befindet.

Oft sind von einer Datei auch mehrere Versionen vorhanden. Typischerweise kopiert sich ein Anwender die Datei, die er bearbeiten möchte, auf sein lokales IT-System und stellt die geänderte Datei auf einer seiner Freigaben wieder zur Verfügung. Auf dieser Weise pflegt jeder Benutzer höchstens auf seinem

IT-System die Versionsstände, aber im gesamten Netz ist nicht unmittelbar ersichtlich, welche Version aktuell ist.

**Fehlende Bandbreite der Peers**

In einem servergestützten Netz wird in der Regel die Netzanbindung zu den Servern so dimensioniert, dass sie die Anfragen der Clients bewältigen kann. Unter Berücksichtigung der benötigten Dienste, die die Clients nutzen können, kann bei einem servergestützten Netz die benötigte Bandbreite geplant und das Netz entsprechend dimensioniert werden.

Bei Peer-to-Peer kann die benötigte Bandbreite nur sehr schwer geplant werden. In der Regel wird auf die Peers, die zur Zeit die meisten und umfangreichsten Informationen bereitstellen, am häufigsten zugegriffen. Die Anbindung dieser Systeme wird überlastet und für essentielle Dienste reicht die vorhandene Bandbreite nicht mehr aus. Stellt ein anderer Peer aktuellere oder öfter benötigte Informationen zur Verfügung, wird innerhalb kürzester Zeit der vorige Peer entlastet und bei dem beliebteren Peer ist die Anbindung an das LAN nicht mehr ausreichend. Im Gegensatz zu einem Server, bei dem die benötigte Bandbreite schon im Voraus errechnet werden kann, ist dies bei den regelmäßig wechselnden, stark beanspruchten Peers nicht möglich.

**Fehlende Spezialisierung der IT-Systeme**

Die Anforderungen an einen Server werden vorher festgelegt, er wird hiernach beschafft und in der Regel nur für die vorgesehene Aufgabe eingesetzt. Server werden außerdem typischerweise in klimatisierten Serverräumen aufgestellt, im Unterschied zu Standard-IT-Systemen, die in einer Büroumgebung betrieben werden. Nur durch den hohen Spezialisierungsgrad der Server können diese die vorgesehenen Aufgaben effizient erfüllen.

Peers, an denen parallel mehrere Benutzer arbeiten können, sind in der Regel nicht für höhere Belastungen ausgelegt. Werden beispielsweise die Informationen statt auf speziellen Serverfestplatten auf Standard-Festplatten abgelegt, kann durch die hohe Belastung die Lebenszeit der Festplatten stark verkürzt werden.

In der Regel werden auf Servern zusätzliche Maßnahmen ergriffen und eine sicherheitskritische Konfiguration steht oft besonders im Vordergrund. Beispielsweise werden erhöhte Anforderungen bezüglich der Verfügbarkeit durch redundante Festplatten erfüllt. Diese Sicherheitsaspekte sind in der Regel an Standard-IT-Systemen nicht vorzufinden.

**Anonymität**

Bei externen Peer-to-Peer-Diensten ist nicht immer sofort auf den ersten Blick ersichtlich, mit wem Informationen ausgetauscht werden. Ein Peer, der am vorigen Tag über eine bestimmte IP-Adresse erreichbar war, kann am nächsten Tag über eine andere IP-Adresse adressiert werden.

Daher ist es nicht auszuschließen, dass hinter einer IP-Adresse von einem Peer, mit dem vor kurzem Textnachrichten ("Messaging") und Informationen ("Filesharing") ausgetauscht wurden, nun ein anderer Peer steht.

Sendet nun ein Benutzer Informationen an einem vermeintlich bekannten Benutzer, könnten diese auch unberechtigte Personen erhalten.

**Rechtliche Aspekte**

Öffentliche Peer-to-Peer-Dienste wurden entwickelt, um Dokumente effizient anderen Benutzern für Diskussionen zur Verfügung zu stellen. Peer-to-Peer-Dienste werden aber auch oft genutzt, um urheberrechtlich geschützte Inhalte in Tauschbörsen zu verteilen. Werden illegale oder urheberrechtlich geschützte Informationen aus einem LAN einer Behörde oder eines Unternehmens über Peer-to-Peer-Dienste bezogen, kann dies neben juristischen Folgen auch dem Ansehen der Institution in der Öffentlichkeit schaden.

# G 2.148 Fehlerhafte Planung der Virtualisierung

Die Einführung von Virtualisierungservern in ein Rechenzentrum bedeutet, dass eine neue Klasse von IT-Systemen in Betrieb genommen werden muss. Ein Virtualisierungsserver ist meist nicht nur ein Server, der den Betrieb virtueller IT-Systeme ermöglicht. Vielmehr integriert er die virtuellen IT-Systeme in das Rechenzentrum und steuert dabei deren Anbindung an weitere Infrastrukturelemente wie z. B. Netze und Speichernetze. Aus Sicht der virtuellen IT-Systeme stellt der Virtualisierungsserver also einen Bestandteil der Rechenzentrumsinfrastruktur dar.

In einer klassischen IT-Infrastruktur werden die (physischen) IT-Systeme häufig in einem arbeitsteiligen Prozess verwaltet. Die einzelnen Strukturelemente der IT-Infrastruktur werden von Administratoren betrieben, die sich auf die von ihnen betreuten IT-Systeme spezialisiert und konzentriert haben. In einer virtualisierten IT-Infrastruktur hingegen sind einzelne Strukturelemente der vorher getrennten Infrastruktur in einem Virtualisierungsserver zusammengefasst. Hierdurch verlagert sich möglicherweise ein Teil der Betriebsverantwortung für diese Rechenzentrumsressourcen von den spezialisierten Administratoren auf die Administratoren der Virtualisierungsserver.

Es verändert sich durch die Einführung der Virtualisierung auch die Sichtweise auf einen Informationsverbund insgesamt. Werden Infrastrukturkomponenten sowie eine Vielzahl von (virtuellen) Servern und (virtuellen) Arbeitsstationen innerhalb eines Virtualisierungsservers abgebildet, können die Unterschiede zwischen einem physischen und einem logischen Informationsverbund nicht wahrgenommen werden. Damit ist die logische Struktur nicht mehr klar erkennbar.

**Fehlende oder mangelhafte Planung der Rollen und Verantwortlichkeiten**

Virtualisierungsserver beinhalten meist auch einen großen Teil der für den Betrieb eines virtuellen IT-Systems notwendigen Infrastrukturkomponenten in virtueller Form. Diese Infrastrukturkomponenten, wie beispielsweise Switches oder Network-Attached-Storage-Systeme, werden sonst durch dedizierte Komponenten bereitgehalten. Dies bedeutet, dass Netzverbindungen eines virtualisierten IT-Systems nicht wie sonst üblich durch einen Switch, sondern in der Regel durch den Virtualisierungsserver bereitgestellt, verwaltet und überwacht werden. Ähnliches gilt für Speicherplatz in Speichernetzen und andere Ressourcen.

Wird beim Einsatz der Virtualisierungsserver nicht geplant, auf welche Weise die Server technisch und organisatorisch in das Rechenzentrum zu integrieren sind, besteht die Gefahr, dass

- die Verantwortlichkeiten für unterschiedliche Bereiche wie z. B. Anwendungen, Betriebssysteme und Netzkomponenten nicht klar definiert sind,
- sich die Zuständigkeiten für unterschiedliche Bereiche überschneiden oder
- eine passende Rechtestruktur, um administrative Zugriffsmöglichkeiten für die unterschiedlichen Bereiche zu trennen, nicht vorhanden ist.

Für Infrastrukturelemente, wie z. B. Switches oder Speichernetze, sind im klassischen Rechenzentrumsbetrieb häufig verschiedene Personen mit voneinander getrennten Rollen verantwortlich. Durch eine nicht ausreichend konzeptionierte Virtualisierung können jedoch diese Rollenkonzepte zur Administration

unterlaufen werden. So haben die Administratoren der virtuellen Infrastruktur weitreichenden Zugriff auf die Gastsysteme, auf deren Kommunikationsverbindungen und die durch sie verarbeiteten und bereitgestellten Informationen. Werden hier unklare oder womöglich keine Regelungen zur Verteilung und Delegation der Aufgaben zwischen den Administratoren getroffen oder wichtige Aspekte in der Planung übersehen und nicht berücksichtigt, können verantwortlichen Personen notwendige Informationen fehlen. In der Folge können durch Fehler, wie z. B.

- unzureichende Bestimmung der Ressourcenanforderungen für die Virtualisierungsinfrastruktur,
- nicht ausreichende Analyse der Performanceanforderungen der zu virtualisierenden Systeme,
- ungenügende Planung und Beschaffung von Infrastrukturkomponenten für Netze und Speichernetze,
- unzureichende Abstimmung der Infrastrukturkomponenten auf die virtuelle Infrastruktur und
- fehlende Integration der Virtualisierungsserver sowie ihrer virtuellen Infrastrukturkomponenten und der virtuellen IT-Systeme in vorhandene Monitoringsysteme weitreichende, negative Folgen für den gesamten Informationsverbund entstehen.

**Fehlende Einsatzplanung für Virtualisierungsserver**

Wird für den Einsatz der Virtualisierungsserver nicht sichergestellt, dass die virtuellen IT-Systeme auf einheitlich konfigurierten Virtualisierungsservern betrieben werden und damit eine einheitliche Infrastruktur vorfinden, können beim Betrieb der virtuellen IT-Systeme Probleme auftreten. Als Beispiel sei hier die Virtualisierungsechnik *Live Migration* genannt. Sie erlaubt es, ein virtuelles IT-System von einem Virtualisierungsserver auf einen anderen zu verschieben:

- Wird ein virtuelles IT-System in der Virtualisierungsinfrastruktur verschoben, kann es möglicherweise auf eine Ressource zugreifen, auf die ein Zugriff aus Gründen der Vertraulichkeit und Integrität nicht möglich sein sollte.
- Zum Anderen könnte bedingt durch eine fehlerhaft geplante Virtualisierungsinfrastruktur der Zugriff eines virtuellen IT-Systems auf eine benötigte Ressource wie z. B. Namensauflösung (DNS) nach einer *Live Migration* nicht mehr möglich sein. Dies kann unmittelbare Folgen für die Verfügbarkeit eines virtuellen IT-Systems haben.

Werden die Hardwareaustattung der Virtualisierungsserver nicht detailliert geplant und keine Vorgaben für die Beschaffung der notwendigen Hardwarekomponenten gemacht, könnten für das gewählte Virtualisierungsprodukt inkompatible Komponenten beschafft werden. Dies kann Nachteile für die Herstellerunterstützung für das gewählte Produkt haben. Weiterhin ist es möglich, dass z. B. bestimmte Prozessoreigenschaften, wie Intel VT und AMD-V fehlen, die für den Betrieb der Virtualisierungslösung zwingend notwendig sind.

Sind die Hardwarekomponenten, die für eine Farm von Virtualisierungsservern beschafft werden, nicht einheitlich ausgestattet, können die Verfügbarkeit und Integrität der virtuellen IT-Systeme gefährdet sein. Beispielsweise kann eine unterschiedliche Prozessorausstattung der Virtualisierungsserver zu Stabilitätsproblemen der virtuellen IT-Systeme führen. Stehen bestimmte Prozessoreigenschaften auf einem Virtualisierungsserver nicht zur Verfügung, wenn ein virtuelles IT-System mittels *Live Migration* dorthin verschoben wird, kann das virtuelle IT-System abstürzen.

**Fehlerhafte Netzintegration**

Im Rechenzentrumsbetrieb haben sich bestimmte Verfahren zur Integration von Servern und ähnlichen Systemen in die Netzinfrastruktur herausgebildet. Diese Verfahren, wie beispielsweise MAC-Filter, dienen dazu, die Verfügbarkeit sowie Integrität und Vertraulichkeit der Netzverbindungen zu schützen. Werden diese Verfahrensweisen nicht beachtet und geeignet angepasst, ist es möglich, dass Maßnahmen, die für physische Systeme geeignet sind, für den Betrieb virtueller Systeme negative Folgen haben. Werden MAC-Filter auf den Switchports der Virtualisierungsserver ungeeignet eingerichtet, können einige Virtualisierungsfunktionen wie die *Live Migration*, also das Verschieben laufender virtueller IT-Systeme zwischen Virtualisierungsservern, nicht funktionieren. In einem solchen Fall verliert die verschobene virtuelle Maschine ihre Netzverbindung, da ihre (virtuelle) MAC-Adresse auf dem Switch-Port des neuen Virtualisierungsservers abgewiesen wird.

**Fehlerhafte Integration in Speichernetze**

Die Besonderheiten der Virtualisierungsserver beim Zugriff auf Speichernetze müssen schon bei der Planung geeignet berücksichtigt werden. Virtualisierungsserver benötigen Zugriff auf alle *iSCSI*- und *Fibre Channel*-Ressourcen eines Speichernetzes, die für den Betrieb der virtuellen IT-Systeme notwendig sind. Virtuelle IT-Systeme greifen in der Regel nicht mit eigenen *iSCSI*- oder *Fibre Channel*-Schnittstellen auf solche Ressourcen zu, sondern nutzen dazu die entsprechenden Schnittstellen der Virtualisierungsserver. Daher benötigen die Virtualisierungsserver auch den Zugriff auf Ressourcen, die eigentlich nur durch die virtuellen IT-Systeme genutzt werden sollen, da die Virtualisierungsserver diese Ressourcen den virtuellen Systemen sonst nicht zur Verfügung stellen können. Werden also im Vorfeld der Inbetriebnahme unklare Regelungen getroffen oder bleiben funktionale sowie zeitliche Anforderungen bei der Planung unbeantwortet, sind Störungen der Verfügbarkeit, Vertraulichkeit und Integrität im weiteren Lebenszyklus der Virtualisierungsumgebung möglich.

Wenn Virtualisierungsserver im Rechenzentrum eingesetzt werden sollen, besteht die Gefahr, dass durch eine nicht an die Virtualisierung angepasste Segmentierung des Speichernetzes (SAN) Gefährdungen entstehen. Es kann beispielsweise dazu kommen, dass virtuelle IT-Systeme den Zugriff auf von ihnen benötigte Ressourcen verlieren, wenn sie zwischen Virtualisierungsservern verschoben werden. Die Verfügbarkeit der von ihnen bereitgestellten Dienste ist damit gefährdet. Andererseits kann eine ungeeignete Planung der Speichernetzintegration dazu führen, dass zu weitreichende Zugriffsmöglichkeiten auf die Speichernetze eingeräumt werden. Dies kann die Vertraulichkeit von in diesen Speichernetzen abgelegten Informationen gefährden.

**Fehlende Einsatzplanung für virtuelle IT-Systeme**

Planungsfehler können auch in anderen Bereichen entstehen, in denen bestehende Verfahrensweisen nicht überprüft werden, wenn Virtualisierung eingesetzt werden soll. Werden in den Bereichen Serverbeschaffung und -bereitstellung sowie Betriebssysteminstallation die im Rechenzentrum üblichen Verfahrensweisen nicht angepasst, kann es zu einem oder mehreren der folgenden Probleme kommen:

- Die fehlende Eignung einzelner Betriebssysteme, Dienste oder Anwendungen für die gewählte Virtualisierungsumgebung ist nie ganz auszuschließen. Weiterhin können Anpassungen der Virtualisierungsserver an die auf ihnen betriebenen virtuelle IT-Systeme bzw. deren Betriebssysteme und Anwendungen notwendig sein. Dies kann bei einer unzurei-

chenden Überprüfung durch qualifiziertes Fachpersonal sowie einer unangemessenen Synchronisation der Projektbeteiligten untereinander möglicherweise unentdeckt bleiben. In der Folge können beim weiteren Betrieb der Virtualisierungsserver bzw. der virtuellen IT-Systeme Performanceprobleme oder Verarbeitungsfehler auf Grund von Inkompatibilitäten der eingesetzten Applikationen mit der eingesetzten Virtualisierungslösung auftreten. Hierdurch ist sind besonders die Integrität und Verfügbarkeit von Informationen gefährdet, die auf den virtuellen IT-Systemen verarbeitet werden.

- Wird nicht geprüft, ob für die Applikationen, die auf virtuellen IT-Systemen betrieben werden sollen, bestimmte Hardwarekomponenten (wie z. B. Softwareschutzmodule (*Dongles*) oder ISDN-Karten), benötigt werden, die mit der gewählten Virtualisierungslösung genutzt werden können, kann es zu erheblichen Verzögerungen bei der Installation dieser IT-Systeme kommen. Möglicherweise kann ein solches System gar nicht virtualisiert werden, oder es muss erst eine mit der Virtualisierungslösung kompatible Komponente beschafft werden.
- Werden virtuelle IT-Systeme (virtuelle Server, Arbeitsstationen und Switches) nicht vollständig inventarisiert, fehlt der Überblick über die im Rechenzentrum überhaupt betriebenen IT-Systeme. Dies kann dazu führen, dass

  - beispielsweise zu wenige Betriebssystem- oder Anwendungslizenzen vorhanden sind, und die Institution somit unterlizenziert ist,
  - IT-Systeme betrieben werden, für die keine Betriebsdokumentation besteht oder die nicht durch die Sicherheitskonzepte der Organisation erfasst werden,
  - IT-Systeme betrieben werden, deren Einsatzzweck unbekannt ist (siehe hierzu auch G 5.66 *Unberechtigter Anschluss von IT-Systemen an ein Netz*),
  - IT-Systeme ohne die notwendige Planungs- und Betriebsvorbereitungen in Betrieb genommen werden,
  - IT-Systeme nicht nach den allgemeinen Regeln der Institution ausgesondert und aus den Inventarlisten gestrichen werden.

# G 2.149 Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme

Virtualisierungsserver benötigen für den Betrieb der virtuellen IT-Systeme Speicherplatz, der entweder lokal im Virtualisierungsserver selbst oder in einem Speichernetz bereitgestellt wird. Werden die hierfür benötigten Speicherkapazitäten nicht ausreichend groß geplant, bestehen weitreichende Risiken für die Verfügbarkeit der virtuellen IT-Systeme und die Integrität der in ihnen verarbeiteten Informationen. Dies gilt insbesondere dann, wenn spezielle Virtualisierungsfunktionen, wie Snapshots oder die Überbuchung von Speicherplatz, genutzt werden. Engpässe können nicht nur den Speicherplatz auf Festplatten oder in Speichernetzen betreffen, sondern auch den Arbeitsspeicher (RAM).

**Virtualisierungsfunktionen wie Snapshots belegen zusätzlichen Speicherplatz**

Das Einfrieren und Speichern von Betriebszuständen virtueller IT-Systeme (*Snapshots*), erfordert ausreichenden Speicherplatz. So werden der Inhalt der virtuellen Massenspeicher und unter Umständen auch die Zustände von Hauptspeicher und Prozessor auf die Festplatte geschrieben, wenn ein Snapshot erzeugt wird. Zusätzlich wird bei einigen Virtualisierungslösungen während der Laufzeit des Gastsystems eine Differenzdatei erzeugt. Diese Differenzdatei bildet zusammen mit dem Urzustand der Daten, der vor der Erstellung des Snapshots auf dem virtuellen Datenträger vorlag, den aktuellen Inhalt der virtuellen Festplatte. Auch Standby-Funktionen, die es ermöglichen, virtuelle Maschinen im laufenden Betrieb anzuhalten, verwenden eine ähnliche Technik und belegen somit Speicherressourcen bis der Betrieb fortgesetzt wird.

**Überbuchung von Speicherplatz**

Eine weitere Besonderheit virtueller Umgebungen ist, dass Speicherplatz überbucht werden kann. Das heißt, es wird kein fester Speicherplatz reserviert, wenn einem virtuellen IT-System eine bestimmte Speicherkapazität zugeordnet wird. Stattdessen wird der Speicherplatz dem virtuellen IT-System in den physisch vorhandenen Ressourcen erst dann zugeteilt, wenn er durch das virtuelle IT-System tatsächlich genutzt wird. Für das virtuelle System sind dann beispielsweise einhundert Gigabyte sichtbar, tatsächlich verbraucht dieses jedoch nur den aktuell genutzten Speicherplatz.

Der überbuchte Speicherplatz kann zum Beispiel durch einen anwachsenden Dateicontainer realisiert werden, der auf einer physisch im Virtualisierungsserver installierten Festplatte oder in einem Speichernetz abgelegt wird. Dieser Container wird immer größer, je stärker er genutzt wird. Werden innerhalb des virtuellen IT-Systems, das diesen Container nutzt, Daten gelöscht, wird der Container in der Regel jedoch nicht automatisch wieder kleiner.

Unabhängig davon, ob der Datenträger, auf dem der Container des virtuellen IT-Systems abgelegt wurde, lokal oder im Netz vorliegt, ist dessen Größe durch den physisch zur Verfügung stehenden Speicherplatz begrenzt. Ohne eine umsichtige Planung der erforderlichen maximalen Kapazitäten führt dies leicht zu Problemen. Ist der Speicher zu stark überbucht worden, steht möglicherweise vorzeitig kein freier Platz mehr zur Verfügung. Der Speicherbedarf des virtuellen IT-Systems kann dann im physischen Medium nicht gedeckt

werden und es kommt für die hiervon betroffene virtuelle Maschine zu einer Fehlersituation. Denn obwohl aus Sicht des virtualisierten IT-Systems freier Speicher nutzbar scheint, kann durch den Virtualisierungsserver kein weiterer Speicher für das Gastsystem bereitgestellt werden. Viele Virtualisierungsprodukte behelfen sich in einer solchen Situation damit, auf die von der Überbuchung betroffenen virtuellen Festplatten nur noch lesenden Zugriff zu gestatten, um die bis dahin vorhandenen Daten zu schützen. Hierdurch kann es dazu kommen, dass Daten auf diesen virtuellen Festplatten inkonsistent werden. Möglicherweise fällt das virtuelle IT-System sogar komplett aus, wenn z. B. das Betriebssystem des virtuellen IT-Systems die auftretenden Fehler nicht ausgleichen kann. Andere Virtualisierungslösungen legen automatisch einen Snapshot der betroffenen Systeme an und schalten diese Systeme danach aus, wenn der physische Speicher nicht mehr ausreicht.

Durch dieses Vorgehen ist die Verfügbarkeit der Dienste dieser virtuellen IT-Systeme gestört. Überdies wird der Betrieb aller durch den Virtualisierungsserver ausgeführten Gastsysteme in gleicher Weise behindert, wenn alle disponierbaren physischen Ressourcen des Virtualisierungsservers erschöpft sind.

**Beispiel:**

Ein international aktives Handelsunternehmen nutzt ein ERP-System *(Enterprise Resource Planning)*, um verschiedene Prozesse, unter anderem im Einkauf, zu automatisieren und zu unterstützen. Um den im Außendienst tätigen Handelsagenten des Unternehmens den Zugriff auf das ERP-System zu ermöglichen, stellt das Unternehmen eine Terminalserverfarm bereit, die von den Handelsagenten verwendet wird, um ihre Einkäufe zu verbuchen und an der Unternehmenskommunikation (Intranet und E-Mail) teilzunehmen. Die Plattform muss ständig zur Verfügung stehen, da die Handelsagenten im Warentermingeschäft tätig sind und es daher auf den genauen Zeitpunkt der Einkäufe ankommt, um einen guten Preis zu erzielen.

Aus Kostengründen entscheidet sich die Unternehmensleitung, die Terminalserverfarm und die ERP-Systeme künftig als virtuelle IT-Systeme zu betreiben. Bei der Analyse der bestehenden physischen Systeme stellt das Planungsteam fest, dass die Festplatten der bestehenden Systeme nur zu einem kleinen Teil ausgelastet sind. Bei einigen Datenbanksystemen tritt allerdings gelegentlich ein erhöhter Platzbedarf auf, wenn die monatliche Auswertung der Einkaufskennzahlen durchgeführt wird. Dieser Speicherplatz wird allerdings sofort wieder freigegeben, wenn die Auswertung beendet ist.

Des Weiteren wird geplant, bei einem Versionswechsel im ERP-System die Snapshot-Funktion der Virtualisierungsserver einzusetzen. Da es bei den Aktualisierungen gelegentlich zu Fehlern kommt, soll diese Funktion genutzt werden, um die Änderungen schnell wieder rückgängig machen zu können. Eine zeitraubende Wiederherstellung des Zustands vor der Aktualisierung kann sich im Warentermingeschäft schnell negativ auf den Geschäftserfolg auswirken. Aus diesem Grunde sind die Snapshot-Funktionen der Virtualisierungsserver ein wichtiger Faktor für die Einführung der Virtualisierungstechnik in diesem Unternehmen.

Da der Festplattenplatz der physischen Systeme nur gering ausgelastet ist, wird davon ausgegangen, dass dieser als Reserve für die Snapshots ausreichend groß ist. Daher wird beschlossen, in dem für die virtuellen IT-Systeme aufgebauten Speichernetz nur soviel Speicher vorzusehen, wie aktuell insgesamt in den physischen Systemen vorhanden ist. Dies wurde als ausreichend angesehen, da bei einer Aktualisierung der physischen Systeme auch nicht

mehr Speicher verbraucht werden könnte, als tatsächlich physisch vorhanden ist.

Kurz vor dem Monatsende wird eine Aktualisierung der ERP-Software durchgeführt. Hierbei müssen die ERP-Systeme selbst sowie die Terminalserver aktualisiert werden, da die neuen und dringend benötigten Funktionen nur dann genutzt werden können, wenn auch die Client-Software auf den Terminalservern ausgetauscht wird. Um möglichen Fehlfunktionen vorzubeugen, ist vor der Aktualisierung ein Snapshot aller Systeme, der ERP-Systeme und der Terminalserver, erzeugt worden. Der Snapshot wurde nach der Erzeugung der monatlichen Kennzahlen erzeugt, um bei einem Fehlschlag der Aktualisierung die Kennzahlen auf der Basis der alten Software schnell zur Verfügung zu haben.

Ab diesem Zeitpunkt werden alle Veränderungen an den Festplattencontainern der virtuellen IT-Systeme in eine Differenzdatei geschrieben und der Speicherverbrauch im Speichernetz steigt sprunghaft an. Es ist nicht bedacht worden, dass durch den Snapshot die bei der Aktualisierung der Software ersetzten Dateien nicht wie vorher physisch überschrieben werden, sondern im Snapshot weiterhin vorhanden sind. Der Speicherbedarf für die Aktualisierung der virtuellen IT-Systeme hat sich dadurch verdoppelt.

Als nun die monatliche Auswertung durchgeführt wird, geht der Speicherplatz im Speichernetz gänzlich zur Neige und es können keine weiteren Daten mehr geschrieben werden. Auch hier ist wiederum nicht beachtet worden, dass der Platz für die Auswertung in der Differenzdatei neu belegt werden muss. Der für die Auswertung zuständige Administrator des virtuellen IT-Systems hat die Speicherknappheit innerhalb der virtuellen Festplatte bemerkt und deshalb die alte Auswertung vor Erzeugung der neuen gelöscht. Allerdings hat dieses Vorgehen keine Auswirkung auf den physisch belegten Speicherplatz, da der für die Auswertung der Alt-Daten verwendete physische Speicherplatz jetzt Bestandteil des Snapshots ist.

Die Virtualisierungssoftware schützt die virtuellen IT-Systeme automatisch vor Datenverlust und -inkonsistenz, indem die virtuellen IT-Systeme angehalten werden. Dadurch fallen alle Terminalserver und alle ERP-Systeme vollständig und gleichzeitig aus. Die Handelsagenten sind von der Unternehmenskommunikation abgeschnitten und können über den Ausfall nicht informiert werden. Hierdurch verzögern sich die auf dem Warenterminmarkt getätigten Geschäfte und das Unternehmen muss wesentlich höhere Preise für die eingekauften Waren bezahlen.

Bevor die ausgefallenen Systeme wieder in Gang gebracht werden konnten, musste freier Speicherplatz für die virtuellen IT-Systeme geschaffen werden. Die Administratoren standen vor der Wahl, die virtuellen IT-Systeme wieder auf den Snapshot zurückzusetzen oder eine Speichererweiterung im Speichernetz vorzunehmen. Da die Terminalserverfarm und das ERP-System schnell wieder verfügbar sein mussten, wurde entschieden, die Systeme auf den Snapshot zurückzusetzen. Die Personalkosten für die Aktualisierung der Systeme mussten daher abgeschrieben werden.

Nachdem der für eine Aktualisierung der ERP-Software unter Verwendung von Snapshots tatsächlich benötigte Speicherplatz korrekt ermittelt worden ist, wurde eine Speichererweiterung des Speichernetzes vorgenommen. Die dringend benötigten Funktionserweiterungen der aktualisierten Software konnten erst genutzt werden, nachdem diese Erweiterung erfolgt war.

# G 2.150 Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen

Mittels Gastwerkzeugen, wie z. B. den *Citrix XenTools* oder den *VMware Tools*, können die virtuellen IT-Systeme in der Virtualisierungsinfrastruktur durch den Administrator vom Virtualisierungsserver aus gesteuert und verwaltet werden. Des Weiteren integrieren diese Programme Treiber und Dienste zur Kommunikation der virtualisierten Betriebssysteme mit dem Host.

Über die Gastwerkzeuge werden verschiedene Funktionen verwirklicht, wie z.B.:

- Synchronisation der Systemzeit einer virtuellen Maschine mit dem Host,
- Anforderung von Hauptspeicher im virtuellen IT-System und Freigabe dieses Speichers für andere Gäste auf dem Virtualisierungsserver (Ballooning),
- Herunterfahren des Betriebssystems des virtuellen IT-Systems ohne Anmeldung,
- Optimierung virtueller Festplatten (Thin Provisioning).

Die Gastwerkzeuge verfügen im Kontext der virtuellen Maschine über weitreichende Berechtigungen auf Systemdateien und -dienste um die beschriebenen Funktionen zu ermöglichen. Diese Funktionen können einem etablierten Berechtigungskonzept sowie weiteren Anforderungen an die virtuelle Umgebung widersprechen, wenn die vorhandenen Konzepte und Anforderungen bei der Planung der Installation der Gastwerkzeuge nicht beachtet und umgesetzt werden. Dadurch können eventuell Funktionen genutzt werden, die mit den Richtlinien der Organisation nicht vereinbar sind.

**Herunterfahren eines virtuellen IT-Systems ohne erforderliche Berechtigung**

Wurde beispielsweise in einer Organisation festgelegt, dass virtuelle und physische Server grundsätzlich nur nach der Anmeldung eines zuständigen Administrators und unter Angabe einer Begründung heruntergefahren werden dürfen, können die Gastwerkzeuge dazu genutzt werden, diese Vorgaben zu umgehen. Mittels der Gastwerkzeuge ist es dem Administrator eines Virtualisierungsservers möglich, ein beliebiges, anderes virtuelles IT-System herunterzufahren. Dazu muss er selbst nicht notwendigerweise ein berechtigter Administrator des betreffenden virtuellen IT-Systems sein. Die Administratoren der Virtualisierungsserver können damit die für die virtuellen IT-Systeme bestehenden Richtlinien und Regelungen zur Nutzung von Systemen unterlaufen und somit die Verfügbarkeit, Integrität und Vertraulichkeit der virtuellen IT-Systeme gefährden.

Es gibt weiterhin Virtualisierungsprodukte (wie z.B. *VMware Workstation, VMware Server*), die umfangreiche Funktionen besitzen, um in eine Entwicklungsumgebung integriert zu werden. Hier gibt es für die Gastwerkzeuge in virtuellen IT-Systemen über die oben angegebenen Möglichkeiten hinaus zusätzliche Funktionen. So können Skripte für Testzwecke in einem virtuellen IT-System hinterlegt und durch Gastwerkzeuge von außen gesteuert werden. Dazu ist keine Interaktion mit und auch keine Authentisierung an dem virtuellen IT-System selbst notwendig. Die Aktionen werden nur durch die Virtualisierungssoftware bzw. den Hypervisor und die Gastwerkzeuge initiiert. Werden nun virtuelle IT-Systeme aus Entwicklungsumgebungen in die virtuelle Infrastruktur für den Produktivbetrieb übernommen, können Sicherheitslücken in der Pro-

duktivumgebung entstehen, da die speziellen für die Entwicklungsumgebung vorgesehenen Werkzeuge und Schnittstellen in der Produktivumgebung weiterhin wirksam sind.

**Beispiel:**

Eine Behörde plant die Aktualisierung einer komplexen Client-/Serveranwendung. Mit der Aktualisierung wird ein externes Beratungsunternehmen beauftragt. Die Entwicklung und der Test der Aktualisierungsschritte erfolgt in einer virtuellen Umgebung, die ein vollständiges Abbild der Produktivumgebung darstellt. Die Testsysteme sind Kopien der Produktivsysteme, die in einem abgeschotteten Netz bereitgestellt wurden.

Einer der externen Berater ist für die Aktualisierung der Clientanwendung zuständig. Die Installation der Anwendung ist auf dem Client recht komplex. Zudem müssen bei jeder Neuinstallation bestimmte festgelegte Konfigurationsschritte auf dem Server durchgeführt werden, damit die neue Clientversion funktionieren kann. Sind die Daten auf dem Server migriert, können Clients mit einer alten Softwareversion nicht mehr auf den Server zugreifen.

Um die immer gleichen Konfigurationsschritte nicht immer wieder manuell durchführen zu müssen, hat der externe Berater Skripte erstellt. Diese sollen zum einen den Client bei jedem Neustart neu konfigurieren und zum anderen über die Gastwerkzeuge Skripte auf dem Server installieren und ausführen.

Der zuständige Referatsleiter möchte sich über den Projektfortschritt informieren und bittet einen seiner Mitarbeiter darum, ihm den Client vorzuführen. Da noch keine Installationspakete für die Clientsoftware in der Produktivumgebung existieren, entscheidet sich der Mitarbeiter, das virtuelle Arbeitsplatzsystem des externen Beraters zu kopieren. Er transferiert es in das Produktivnetz und startet es, um es seinem Vorgesetzten zu demonstrieren.

Im Hintergrund werden jetzt die im Client integrierten Skripte des externen Beraters aktiviert und der Produktivserver der Behörde wird damit auf die neue Version aktualisiert. Die Mitarbeiter können nicht mehr auf den Server zugreifen und es kommt zu einem mehrstündigen Produktionsausfall, da eine Datenwiederherstellung durchgeführt werden muss.

# G 2.151 Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen

Die Virtualisierungstechnik nimmt erst seit wenigen Jahren außerhalb der Mainframe-Welt (*IBM Z-Series, Siemens BS2000, SUN Enterprise 25000*) stärkeren Einfluss auf das Design von Rechenzentren und erst seit ca. 2005 werden vermehrt auch produktive IT-Systeme virtualisiert. Vorher wurden virtuelle IT-Systeme hauptsächlich in Entwicklungs- und Testumgebungen eingesetzt. Es existiert eine große Anzahl unterschiedlicher Virtualisierungsprodukte, die zudem auf unterschiedlichen technischen Ansätzen (Server- und Betriebssystemvirtualisierung) beruhen. Daher ist bisher noch keine Standardisierung eines virtuellen IT-Systems erfolgt, wie dies beispielsweise für IT-Systeme möglich ist, die auf x86- oder x64-Hardware beruhen.

Anwendungen werden durch ihren Hersteller in der Regel für eine bestimmte Kombination aus Betriebssystem und Hardwareplattform freigegeben. d. h., sie unterstützen den Benutzer der Anwendung beispielsweise bei der Fehlersuche, wenn die Anwendung auf der freigegebenen Hardwareplattform mit dem entsprechenden Betriebssystem betrieben wird. Da jedoch noch keine Standardisierung der Hardwareplattform "virtuelles IT-System" erfolgt ist, können keine allgemeinen Aussagen der Anwendungshersteller dazu gemacht werden, inwieweit die Installation ihrer Anwendung auf einem beliebigen virtuellen IT-System unterstützt wird.

Virtuelle IT-Systeme können auf der Basis von völlig unterschiedlichen Virtualisierungstechniken (Server- oder Betriebssystemvirtualisierung) betrieben werden und daher stark unterschiedliche Eigenschaften haben. In virtuellen IT-Systemen, die auf Betriebssystemvirtualisierung (*SUN Solaris Zones, Parallels Virtuozzo*) basieren, also multiple Instanzen eines einzigen Betriebssystems darstellen, können beispielsweise unterschiedliche, betriebssystemnahe Softwarebibliotheken oder unterschiedliche Betriebssystemkerne nicht oder nur sehr eingeschränkt verwendet werden. Eine solche Einschränkung existiert bei virtuellen Systemen, die auf einer vollständigen Servervirtualisierung (z. B. *Citrix XenServer, Microsoft HyperV, QEMU*, *Sun VirtualBox*, *VMware ESX*) beruhen, in der Regel nicht, sodass eine allgemeingültige Aussage für alle denkbaren virtuellen IT-Systeme gleich welcher Virtualisierungstechnik nicht möglich ist.

Aus den vorgenannten Gründen geben Hersteller den Betrieb ihrer Anwendungen auf virtuellen IT-Systemen nicht generell frei, sondern erteilen diese Freigaben gegebenenfalls nur für bestimmte Kombinationen aus Betriebssystem und konkreten Virtualisierungsprodukten. Wird nicht geprüft, ob eine solche Freigabe existiert, besteht die Gefahr, dass Begleitung und Hilfe ("Support") bei aufgetretenen Schwierigkeiten abgelehnt oder eingeschränkt werden.

**Beispiel:**

Ein großes Unternehmen betreibt ein umfangreiches ERP-System, das aus einer Vielzahl von Servern besteht. Das ERP-System besteht aus mehreren Datenbanksystemen und circa 30 Anwendungs- und 80 Webservern. Mit dem Hersteller des ERP-Systems hat das Unternehmen einen Pflege- und Supportvertrag geschlossen, in dem der Hersteller seine Unterstützung bei auftre-

tenden Problemen zusichert. An den Supportvertrag ist die Bedingung gebunden, dass die ERP-Systeme mit dem Betriebssystem Windows Server 2003 auf physischer Hardware betrieben werden müssen. Für virtuelle Systeme behält sich der Hersteller eine Einzelfallprüfung vor und erteilt keine generelle Freigabe.

Das Unternehmen möchte die Serversysteme, auf denen das ERP-System betrieben wird, durch neue Systeme ersetzen, da die bestehenden Systeme mittlerweile recht alt geworden sind und sich Hardwarestörungen häufen. Die zuständigen Administratoren berichten, dass die einzelnen Server, vor allem die Anwendungs- und Webserver, nicht sehr stark ausgelastet sind und Lastspitzen nicht auf allen Systemen gleichzeitig auftreten, sondern sich auf die Systeme über den Tag verteilen. Aus diesen Gründen wird entschieden, die Anwendungs- und Webserver zu virtualisieren und in einer virtuellen Infrastruktur aus mehreren Virtualisierungsservern zu betreiben. Das Unternehmen wählt für die Anwendungsserver eine Servervirtualisierungslösung und für die Webserver ein Produkt, das auf Betriebssystemvirtualisierung basiert. Gerade die Betriebssystemvirtualisierung wird für die Bereitstellung einer großen Menge von Webservern als besonders geeignet angesehen, da hier sehr große Konsolidierungseffekte erzielt werden können, also sehr viele virtuelle Instanzen auf einem Virtualisierungsserver betrieben werden können. Die Administratoren erwarten mit der Virtualisierung der Server keine Probleme, die mit der Virtualisierungssoftware zusammen hängen könnten, und gehen davon aus, dass keine virtualisierungsbedingten Störungen auftreten werden.

Nachdem die ERP-Systeme ohne Rückfrage bei dem Hersteller der ERP-Software virtualisiert worden sind, läuft die ERP-Anwendung eine Zeit lang störungsfrei. Nach einigen Monaten bemerkt allerdings ein Mitarbeiter, dass Fehler im Lagerhaltungsmodul der ERP-Software auftreten. Es wird festgestellt, dass die über einen Webserver von den Lagerarbeitern eingegebenen Zu- und Abgänge im Lager falsch verarbeitet werden. Das ERP-System löst nun automatisch Bestellungen aus, obwohl noch genügend Ware im Lager vorhanden ist. Bei anderen Waren, die für die Produktion dringend benötigt werden, weist das ERP-System aber zu hohe Lagerbestände aus, was dazu führt, das keine Nachbestellungen ausgelöst werden und die Produktion stillsteht. Hierdurch entsteht dem Unternehmen durch den Produktionsausfall ein Schaden in großer Höhe.

Die Administratoren des ERP-Systems befassen sich mit dem Problem und vermuten im Zusammenspiel von Webserver und Anwendungsserver ein Übertragungsproblem, das zu der fehlerhaften Verarbeitung führt. Sie können allerdings keine Lösung dafür finden und wenden sich an den Hersteller. Der Hersteller lässt sich die Konfiguration der ERP-Server und automatisch erzeugte Reports zusenden, die er prüft, um den Fehler eingrenzen und beheben zu können.

Nachdem der Hersteller des ERP-Systems festgestellt hat, dass die Server auf virtuellen Plattformen betrieben werden, teilt er dem Unternehmen mit, dass das ERP-System auf einer nicht freigegebenen und damit unterstützten Plattform läuft. Der Hersteller hat ein Timing-Problem als Ursache ermittelt und lehnt die weitere Bearbeitung ab, da er vermutet, dass das Problem mit der Virtualisierung der Systeme zusammenhängt. Er fordert das Unternehmen auf, das Einsatzszenario auf nicht virtualisierter Hardware nachzustellen, um die Virtualisierung als Problemursache auszuschließen.

Das Unternehmen ist nun gezwungen, leihweise eine große Anzahl an physischen Servern für den Nachbau des Einsatzszenarios zu beschaffen. Dieser

Nachbau ist sehr komplex und zeitaufwendig. Die Fehlerbehebung wird dadurch zudem erheblich verzögert.

Es stellt sich heraus, dass der Fehler auch auf den physischen Servern auftritt und es damit weitgehend ausgeschlossen ist, dass die Virtualisierung der Server ursächlich für den Fehler war. Daraufhin setzt der ERP-Hersteller seine Bemühungen fort und das Problem wird nach eingehender Analyse auch vollständig gelöst.

Das Unternehmen, das das ERP-System nutzt, fordert nun Schadensersatz vom Hersteller der Software für die Kosten, die durch die Reproduktion des Fehlers auf physischen Servern entstanden ist, sowie die verlorene Arbeitszeit und den Produktionsausfall in der Zeit, die während des Aufbaus der Parallelumgebung aufgetreten ist. Das Unternehmen steht auf dem Standpunkt, dass die Problemlösung durch den Softwarehersteller unnötig verzögert worden ist, da die Virtualisierung sich nicht als problemverursachend herausgestellt hat. Der Hersteller wiederum verweist dagegen auf den Wortlaut des Pflege- und Supportvertrages und lehnt eine Haftung ab. Weiterhin betont er, dass er das Timing-Problem, das zu der Vermutung führte, das aufgetretene Problem hänge mit der Virtualisierung zusammen, nur aus Kulanz ermittelt hat, er hätte die Problembearbeitung auch vollständig ablehnen können. Es kommt zu einem Gerichtsverfahren, das der Hersteller der ERP-Software gewinnt.

# G 2.152 Fehlende oder unzureichende Planung des DNS-Einsatzes

Wird die Planung des DNS-Einsatzes vernachlässigt, kann dies zu Problemen und Sicherheitslücken im laufenden Betrieb führen. Zahlreiche Netzdienste und -anwendungen benötigen DNS, um zu funktionieren. So wird DNS von Kommunikationspartnern benötigt, um die IP-Adresse herauszufinden, die der E-Mail-Server des Empfängers hat. Sind die DNS-Server nicht erreichbar, können diese Dienste nicht bzw. nur noch eingeschränkt genutzt werden. Im schlechtesten Fall kann eine, durch schlechte Planung verursachte Sicherheitslücke, zur Kompromittierung der DNS-Server führen.

**DNS-Server-Infrastruktur**

Die Verfügbarkeit und die Leistungsfähigkeit von DNS-Servern hängen unter anderem von der Verteilung im Netz ab. Probleme, die durch unzureichende Planung der Infrastruktur entstehen können, sind:

- Fehlerhafte Anordnung von DNS-Servern:
  Bei der Registrierung eines Domainnamens werden in der Regel mindestens zwei Server angegeben, die als Advertising DNS-Server (siehe M 2.450 *Einführung in DNS-Grundbegriffe*) für diese Domain genutzt werden. Befinden sich diese beiden Advertising DNS-Server innerhalb desselben Netzsegments, kann durch den Ausfall des Gateways, dass dieses Segment mit dem Rest des Netzes verbindet, die Namensauflösung der gesamten Domain ausfallen. Dies führt letztlich dazu, dass nicht mehr auf Dienste wie Webserver, E-Mail aber auch auf Remoteadministrationszugänge zugegriffen werden kann.
- Lange Antwortzeiten:
  Ist die Leistungskapazität der Advertising bzw. Resolving (siehe M 2.450 *Einführung in DNS-Grundbegriffe*) DNS-Server oder die Bandbreite des Netzes nicht ausreichend dimensioniert, führt dies oft zu langen Antwortzeiten oder Time-outs. Wenn keine Priorisierung des Netzverkehrs vorgenommen wird, kann es passieren, dass unwichtigerer und zeitunkritischer Netzverkehr die Bandbreite zu sehr beansprucht.
- Entfernung:
  Je mehr Netzkomponenten sich zwischen einem DNS-Server und den anfragenden Hosts befinden, desto öfter müssen die Pakete bearbeitet werden. Dadurch erhöht sich die Antwortzeit und das Netz wird unnötig belastet.

**Ungeeignete DNS-Server-Software**

Veraltete bzw. wenig getestete Software enthält oft bekannte Softwareschwachstellen, die von Schadsoftware ausgenutzt werden kann. Dies erhöht die Gefahr erfolgreicher Angriffe deutlich.

Des Weiteren kann es zu Problemen kommen, wenn für alle DNS-Server dieselbe Software verwendet wird. Wird in diesem Fall ein DNS-Server aufgrund einer Softwareschwachstelle kompromittiert, kann die Lücke auf jedem weiteren DNS-Server ausgenutzt werden. Plant hingegen ein Informationsverbund, unterschiedliche DNS-Server-Software einzusetzen, besteht die Gefahr, dass diese nur eingeschränkt kompatibel sind. Zusätzlich wird sich dadurch auch der Administrationsaufwand erhöhen.

**DNS-Server und Sicherheitsgateways**

Die Planung der DNS-Server hat Auswirkung auf die Konfiguration von Sicherheitsgateways und Paketfiltern. Sind die Regeln, um DNS-Verkehr im Netz zu ermöglichen, zu freizügig definiert, kann dies unter Umständen einen Angriff ermöglichen. Sind die Regeln jedoch zu restriktiv formuliert, können legitime Clients keine Anfragen an die DNS-Server stellen und werden bei der Benutzung von Diensten wie E-Mail, FTP oder Ähnlichem beeinträchtigt.

**Aufteilung des Namensraums**

Die Domain-Informationen über den Namensraum eines Informationsverbundes enthalten sämtliche Informationen über den Aufbau des internen Netzes. Oft ist es nicht erwünscht, die gesamten Informationen für die Öffentlichkeit zugänglich zu machen. Dazu kann der Namensraum in einen internen (Resolving DNS-Server) und einen öffentlich zugänglichen (Advertising DNS-Server) Bereich geteilt werden. Wird eine Trennung bei der Planung nicht berücksichtigt, kann dies Probleme wie in G 5.154 *DNS Information Leakage* beschrieben, zur Folge haben.

**Kryptografie**

DNS kann über kryptografische Mechanismen abgesichert werden, beispielsweise über TSIG (Trusted Security Transaction Group) und DNSSEC (DNS Security). Wie bei allen kryptografischen Anwendungen sind die kryptografischen Schlüssel geheimes Material. Werden diese Schlüssel veröffentlicht, ist kein Schutz durch diese kryptografischen Mechanismen mehr gegeben. Kommt es in der Planung zu unklaren Regelungen, inwieweit Kryptografie eingesetzt werden soll, kann dies unter anderem zu folgenden Problemen führen:

- Der Einsatzbereich der einzelnen Mechanismen, wie TSIG und DNSSEC, wurde nicht festgelegt. Dadurch herrscht Unklarheit ob und wenn ja zwischen welchen Partnern unverschlüsselte E-Mail Kommunikation erlaubt ist.
- Die Zugriffsrechte auf die Dateien, die die kryptografischen Schlüssel beinhalten, sind zu freizügig definiert. Dadurch kann jeder Benutzer, der sich auf dem Rechner einloggt, die Dateien lesen und verändern.
- Der Austausch der Schlüssel wurde nicht geplant, dadurch werden diese über ungesicherte Netzverbindungen übertragen.

**Beispiele:**

- Im Jahr 2001 wurde die Domain eines großen Softwarehauses für mehrere Stunden praktisch lahmgelegt. Ursache war ein Distributed-Denial-of-Service-Angriff auf den Router, der die DNS-Server für die Domain mit dem Internet verband. Jegliche auf DNS basierende Kommunikation war unterbunden. Lediglich Rechner, deren Resolver die benötigten Domain-Informationen zwischengespeichert hatten, konnten eine Verbindung herstellen.

# G 2.153 Ungeeignete Sicherung des Übertragungsweges in einer Terminalserver Umgebung

Terminalserver ermöglichen physisch entfernten Clients, zentral Applikationen auf einen IT-System auszuführen. Je nach Anforderungen können die Clients über ein LAN oder sogar über öffentliche Netze, wie dem Internet, auf den Terminalserver zugreifen. Werden die hierfür benötigten Informationen zwischen den Clients und den Servern ungeschützt übertragen, können insbesondere bei öffentlichen Netzen sensible Informationen abgehört oder ganze Sitzungen auf dem Terminalserver übernommen werden. Wird eine Sitzung übernommen, könnte ein Angreifer unter Umständen alle Benutzerrechte des Anwenders erhalten, ohne die Sicherheitsbarrieren jedes einzelnen Dienstes überwinden zu müssen.

Folgende Informationen, die zwischen dem Terminalserver und den Clients übertragen werden, können unter Umständen abgehört oder verändert werden:

- Authentisierungsinformationen,
- Benutzereingaben, die von den Clients zu den Terminalservern gesendet werden,
- Bildschirminformationen, die auf den Clients ausgegeben werden,
- Daten aus der Zwischenablage und
- Dateitransfers zwischen den lokalen Laufwerken des Clients und dem Server.

Des weiteren werden Informationen auch auf den Server umgeleitete Geräte des Terminals übermittelt, wie

- Audiogeräte,
- serielle- oder parallele Schnittstellen,
- USB-Geräte und
- Drucker.

Ältere Terminalserver-Dienste, wie z. B. der Microsoft Windows Terminalserver 2000, setzen in ihrer Standardkonfiguration nur eine unidirektionale, protokollinterne Verschlüsselung für den sicheren Transport der Benutzereingaben ein. Diese Informationen werden jedoch vom Terminalserver empfangen und in grafischer Form unverschlüsselt zur Anzeige auf das Terminal zurückgesandt.

Ab dem Windows Server 2003 verwendet Microsoft in der Grundeinstellung bidirektionale Verschlüsselung. Hierfür muss im Vorfeld eine Verschlüsselungsmethode zwischen dem Client und dem Server ausgehandelt werden. Beim "client compatible mode" bestimmt beispielsweise der Client die auszuwählende Methode. Wird eine unzureichende Methode mit nicht als sicher geltende Verschlüsselungsverfahren oder zu kurzen Schlüsseln gewählt, kann ebenfalls die Kommunikation zwischen Client und Server mitgelesen oder verändert werden.

X-Window sieht keine Verschlüsselung zwischen dem Server und Client vor. Ohne zusätzliche Mechanismen, wie SSH-Tunnel oder VPN, kann der Datenstrom ebenfalls manipuliert und eingesehen werden.

**Beispiel:**

Ein Mitarbeiter verwendet an seinem Telearbeitsplatz das Warenwirtschaftssystem des Unternehmens über einen Terminalserver-Client. Der Systemadministrator hat diesen mit einer bidirektionalen Verschlüsselung konfiguriert, der Terminalserver lässt jedoch auch Verbindungen mit einer einseitigen kryptografischen Sicherung zu. Durch einen Bedienungsfehler löscht der Mitarbeiter die Konfiguration seines Clients, kann jedoch durch Kenntnis der Zugangsdaten die Verbindung selbst wiederherstellen. Aufgrund fehlender Sachkenntnis übersieht er dabei die unsichere Konfiguration des Rückkanals. Einem Wirtschaftsspion gelingt es, die Sitzung über das Internet zu belauschen und gelangt so an vertrauliche Kennzahlen der Unternehmensbilanz.

# G 2.154 Ungeeignete Anwendungen für den Einsatz auf Terminalservern

Applikationen, die nicht auf einem Terminalserver installiert und betrieben werden können, werden zunehmend seltener. Dennoch kann es vorkommen, dass einzelne Anwendungen in einer komplexen Softwarelandschaft nicht auf Terminalservern installiert werden können. Wurde im Vorfeld nicht geprüft, ob die Anwendungen für eine Mehrbenutzerumgebung entwickelt worden ist, kann es passieren, dass die Applikationen ihren Dienst versagen, instabil werden, oder schlimmer, unvorhersehbare Inkonsistenzen im Datenbestand auftreten.

Multimediale Inhalten zu übertragen, stellt oft eine besondere Herausforderung an eine Terminalserver-Umgebung dar. Werden Audio- und Videodaten, oder sogar Echtzeit 3D-Grafiken (z. B. im CAD-Bereich) übermittelt, steigt der an die Terminals zu übertragende Datenstrom stark an. Sollen Multimedia-Inhalte übertragen werden, können Benutzer bei mangelhafter Planung und Konzeption der vorhandenen Ressourcen in ihrer Arbeit mit dem IT-System erheblich beeinträchtigt werden. Dies kann dazu führen, dass alle Sitzungen auf dem überlasteten Terminalserver einfrieren oder Datenverbindungen abbrechen. Auch wenn derart aufwändige Anwendungen nicht vorgesehen waren, aber durch eine Fehlkonfiguration der Zugriff darauf (z. B. über ein Browser-Plugin) dennoch möglich ist, können diese Probleme auftreten.

**Beispiel**

Ein Unternehmen möchte von einer Client-Server-Architektur auf eine Terminalserver-Umgebung migrieren. Erst nach dem das Produktivsystem ausgerollt wurde, stellen die Verantwortlichen fest, dass die individuell entwickelte Warenwirtschaft sporadisch abstürzt. Hinzu kommt, dass die von dem Lagerverwaltungsmodul genutzte Datenbank zunehmend fehlerhafte oder veraltete Einträge beinhaltet.

Diese fehlerhaften und veralteten Einträge entstanden, weil das Lagerverwaltungsmodul eine zentrale Datei auf der Client-Seite nutzt, um Schreibzugriffe in die Datenbank zwischenzupuffern. Da bei der Implementierung der Software nicht vorgesehen war, dass mehrere Benutzer gleichzeitig die selbe Client-Applikation auf ein und dem selben Rechner ausführen, werden die zwischengespeicherten Datenbankzugriffe teilweise überschrieben, bevor diese auf die Datenbank übertragen werden. Hinzu kommt, dass gleichzeitige und konkurrierende Zugriffe auf die Datei regelmäßig den Datenbank-Client, der nun auf dem Server ausgeführt wird, abstürzen lassen.

# G 2.155 Fehlende oder unzureichende Planung von OpenLDAP

OpenLDAP ist eine komplexe Anwendung mit einem modularen Aufbau und zudem mit zahlreichen anderen Anwendungen nutzbar. Daraus ergibt sich eine große Komplexität, die eine systematische Planung des OpenLDAP-Einsatzes erfordert.

Bei fehlender oder unzureichender Planung können sich beispielsweise folgende Probleme ergeben:

- **Backends**
  Der Zugriff auf die von OpenLDAP verwendete Datenbank erfolgt nicht direkt durch den slapd-Server, sondern wird von einem oder mehreren sogenannten Backends übernommen. Die Auswahl des oder der Backends und die Wahl der zugehörigen Direktiven und Parameter haben unmittelbaren Einfluss auf die Funktionen, die OpenLDAP anbieten kann. Wird beispielsweise das Backend back-ldif zur Datenspeicherung verwendet, um die Installation einer zusätzlichen Datenbank zu umgehen, stehen nur rudimentäre Funktionen des Verzeichnisdienstes zur Verfügung. Die Unterstützung einer großen Menge von Benutzern oder anderen Objekten ist dann nicht sinnvoll möglich.
- **Overlays**
  Die Anpassbarkeit von OpenLDAP ergibt sich zu einem großen Teil aus sogenannten Overlays. Diese steuern den Datenfluss von und zu den Backends und ermöglichen so zusätzliche Funktionen, ohne Backends anpassen oder neu programmieren zu müssen. Die mangelnde Planung des Overlay-Einsatzes kann zur Verwendung von Overlays führen, die die gewünschte Funktion nicht oder nicht hinreichend erfüllen, die OpenLDAP nicht benötigte Operationen ausführen lassen oder die OpenLDAP in seiner Funktion beeinträchtigen. Beispielsweise kann eine notwendige Protokollierung von Zugriffen auf den Verzeichnisdienst fehlschlagen oder ineffizient sein, wenn die Debug-Funktion des slapd-Servers selbst und die Overlays auditlog und accesslog nicht korrekt geplant werden. Ein anderes Beispiel ist das Overlay unique, wenn es auf interne Betriebsparameter angewandt wird. Dadurch kann OpenLDAP in nicht definierte Systemzustände geraten. Werden mehrere Overlays zusammen verwendet (gestapelt), so hängt ihre Wirkung auch von der Reihenfolge ihres Aufrufs ab, weshalb eine fehlende Planung Fehler verursachen kann.
- **Anwendungen**
  OpenLDAP arbeitet eng mit anderen Anwendungen zusammen und stellt diesen Funktionen zur Verfügung. Beispielsweise kann OpenLDAP die Benutzerverwaltung und Adressbuchfunktion für E-Mail-Programme, Internet-Server und weitere Anwendungen übernehmen. Ohne andere Anwendungen ist OpenLDAP auch nicht in der Lage, die Spezifikationen des Protokolls LDAPv3 zu erfüllen. So wird eine Datenbank (in der Regel BerkeleyDB von Oracle) benötigt, um Verzeichnisdienstobjekte für OpenLDAP zu speichern. Ferner benötigt OpenLDAP Hilfsprogramme zur sicheren Authentisierung (beispielsweise Cyrus-SASL) und zur verschlüsselten Kommunikation (SSL/TLS). Bei der Verbindung mit anderen Anwendungen können aufgrund fehlender oder unzureichender Planung zahlreiche Fehler entstehen. So könnten falsche Versionen eines oder mehrerer Programme eingesetzt werden, deren Kompatibilität nicht gegeben ist. Sehr oft wird auch vergessen, die Schnittstellen zwischen den Anwendungen abzusichern, so dass Daten unverschlüsselt über Netzverbindungen ausgetauscht werden.

- **Systemumgebung**
  Bei fehlender oder unzureichender Planung wird OpenLDAP gegebenenfalls in einer unzureichenden Systemumgebung ausgeführt. Wird für die Datenhaltung von OpenLDAP beispielsweise ein verteiltes Dateisystem wie NFS (Network File System) verwendet, so stehen Dateifunktionen, die OpenLDAP bzw. BerkeleyDB verwenden, nicht zur Verfügung. Das trifft unter anderem auf die Locking-Funktion zu, mit der die Datenbank des Verzeichnisdienstes während der Nutzung für den parallelen Zugriff durch einen anderen Benutzer sicher gesperrt werden kann.

# G 2.156 Kompatibilitätsprobleme beim Anheben der Active Directory-Funktionsebene

Das Active Directory, beziehungsweise seit Windows Server 2008 die Active Directory Domänenservices (AD DS), unterstützen verschiedene Funktionsebenen ("AD functional level") für Domäne und Gesamtstruktur ("Forest").

Die Funktionsebenen entsprechen dem Funktionsumfang der jeweiligen Betriebssystemversionen und ermöglichen "gemischte" Domänen, beispielsweise mit Windows Server 2003- und 2008-Domänencontroller.

Der Wechsel auf eine höhere Funktionsebene wird für Windows Server 2008 in zwei Schritten durchgeführt:

- Erweiterung des AD-Schemas vor der Aufnahme eines Windows Server 2008 als Domänencontroller (mit Hilfe von *adprep*)
- Heraufstufen der Domänenfunktionsebene beziehungsweise der Gesamtstrukturfunktionsebene ("forest functional level") nach Umstellung aller Domänencontroller (mit Hilfe von *domprep*).

Kompatibilitätsprobleme können bei beiden Schritten auftreten, vor allem aber beim zweiten Schritt. Beide Schritte können nicht rückgängig gemacht werden, es ist kein Rollback möglich. Das Wiedereinspielen einer Datensicherung ist ebenfalls nicht zu empfehlen, da alle Domänencontroller betroffen sind (siehe auch M 6.108 *Datensicherung für Domänen-Controller*).

Oft tauchen Probleme erst im Produktivbetrieb auf, da Testumgebungen meist nicht die volle Komplexität einer gewachsenen AD-Struktur abbilden können.

Kompatibilitätsprobleme betreffen häufig auch Nicht-Windows-Systeme und Anwendungen, die an den AD-Service angebunden sind. Das können LDAP-Schnittstellen mit eigenen Schema-Erweiterungen sein, z. B.

- Telefonanlagen, CTI- oder UM-Dienste,
- Samba-Server und eingebettete Samba-Server in NAS oder SAN-Systemen und
- Schnittstellen auf Unix/Linux-basierten Web-Services.

Als Folge können bei der AD-Integration Fehlfunktionen auftreten, die diese Services dauerhaft stören können.

# G 2.157 Mangelhafte Auswahl oder Konzeption von Webanwendungen

Eine Webanwendung nutzt in der Regel ein verteiltes, komplexes System bestehend aus unterschiedlichen Komponenten (z. B. Webserver, Applikationsserver, Hintergrundsysteme) und zugehörigen Schnittstellen. Oft sind diese in einer bestehenden Infrastruktur integriert, wobei der Schutz der Daten über alle Komponenten und Schnittstellen hinweg zu gewährleisten ist.

Individuell entwickelte Webanwendungen werden üblicherweise auf der Grundlage von Frameworks entworfen, die Basis-Funktionen zur Verfügung stellen und einsatzspezifisch konfiguriert bzw. abgesichert werden müssen. Im Rahmen der Konzeption sind Frameworks, Komponenten und Schnittstellen auszuwählen und deren Einbindung und Absicherung zu betrachten.

Im Gegensatz dazu ist bei der Konzeption von Webanwendungen auf Basis von Standardsoftware (z. B. Content Management Systeme) insbesondere auf die Auswahl der Software und die Konfiguration der Teilkomponenten zu achten. Dabei ist in diesem Zusammenhang unter Standardsoftware sowohl Free/Libre Open Source Software (FOSS/FLOSS) als auch kommerzielle Software zu verstehen.

Unabhängig davon, ob die Webanwendung als Individualentwicklung oder Standardsoftware umgesetzt wird, kann eine unzureichende Berücksichtigung deren Komplexität (z. B. von Frameworks, Komponenten und Schnittstellen) bei der Auswahl und Konzeption von Webanwendungen den Schutz der Daten gefährden.

Durch grundlegende Fehlentscheidungen in der Planungsphase können Schwachstellen entstehen, die möglicherweise nicht oder nur durch kostenintensive Nachbesserungen behoben werden können.

**Beispiele:**

**Auswahl von Webanwendungen auf Basis von Standardsoftware**

- Die Einsatzumgebung erfüllt nicht die Mindestanforderungen der Webanwendungen an die Hard- und Software. Somit ist die Integration in die bestehende Infrastruktur (z. B. Anbindung an eine Datenbank oder einen Identitätsspeicher) nicht möglich.
- Das ausgewählte Produkt verfügt nicht über eine ausreichende Sicherheitsfunktionalität, um schützenswerte Daten vor unbefugten Zugriffen zu schützen. Daher müssen die notwendigen Schutzmechanismen nachträglich hinzugefügt werden. Sollte das Produkt nicht um Schutzmechanismen erweiterbar sein, muss der Schutz perimetrisch (z. B. Web Application Firewall) realisiert werden. Hierdurch entstehen zusätzliche Aufwände.

**Entwurf der Software-Architektur der Webanwendung**

- Eine Sicherheitsfunktion (z. B. Authentisierung, Autorisierung) wird nicht nur an einer Stelle umgesetzt und verwendet, sondern ist mehrfach in der Webanwendung realisiert. Wird diese Sicherheitsfunktion an den verschiedenen Stellen unterschiedlich umgesetzt, führt dies zu einem uneinheitlichen Sicherheitsniveau. Darüber hinaus erhöht sich der Entwicklungs- und Wartungsaufwand bei redundant umgesetzten Funktionen.
- Die Sicherheitsfunktion wird ausschließlich clientseitig (z. B. im Web-Browser) umgesetzt. Wird die Konfiguration des Web-Browsers durch

einen Angreifer manipuliert, können die clientseitig umgesetzten Sicherheitsfunktionen umgangen werden. Somit kann der Angreifer unbefugt auf schützenswerte Daten und Funktionen zugreifen.

**Integration und Betrieb der Webanwendung**

- Die Hintergrundsysteme werden unzureichend abgesichert und dadurch ist die Datenbank der Webanwendung aus dem Internet erreichbar. Somit kann ein Angreifer direkt auf die Datenbank und die dort hinterlegten Daten zugreifen, ohne die Funktionen der Webanwendung zu nutzen. Die Sicherheitsmechanismen der Webanwendung werden demnach umgangen und können den unbefugten Zugriff auf die gespeicherten Daten in Hintergrundsystemen nicht verhindern.
- Es werden Anwendungskomponenten oder Frameworks zum Session-Management in einer unsicheren Konfiguration eingesetzt. Infolgedessen werden kurze SessionIDs mit einer langen Laufzeit verwendet. Somit kann ein Angreifer die SessionID eines authentisierten Benutzers erraten und die zugeordnete Sitzung übernehmen (siehe G 5.169 *Unzureichendes Session-Management von Webanwendungen und Web-Services*).

**Erweiterung der Webanwendung**

- Bestehende Sicherheitsfunktionen der Webanwendung werden durch falsch umgesetzte Funktionserweiterungen außer Kraft gesetzt. Wird die Webanwendung um ein Formular ergänzt, bei dem die Eingabedaten nicht validiert werden, kann dies von einem Angreifer für den unbefugten Zugriff auf schützenswerte Daten genutzt werden (z. B. bei einem SQL-Injection-Angriff; siehe G 5.131 *SQL-Injection*).

# G 2.158 Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services

Wird eine Webanwendung oder ein Web-Service mit fehlenden oder unzureichenden Vorgaben und Standards entwickelt beziehungsweise erweitert, so kann dies zu Fehlern, Qualitätseinbußen oder einer unvollständig umgesetzten Funktionalität führen. Fehler, die in frühen Entwicklungsphasen der Anwendung gemacht werden, werden häufig erst in einem fortgeschrittenen Entwicklungsstadium entdeckt. Um diese Fehler nachträglich zu beheben, müssen oft aufwendige Änderungen vorgenommen werden. Dadurch können die Entwicklungskosten deutlich zunehmen. Im Fall von grundlegenden, architektonischen Fehlern ist die Webanwendung oder der Web-Service gegebenenfalls sogar komplett neu zu entwickeln.

Gibt es darüber hinaus keine Vorgaben für die Umsetzung von Sicherheitsmechanismen, wird der erforderliche Schutzbedarf (zum Beispiel hoher Schutzbedarf bezüglich Verfügbarkeit) der zu verarbeitenden Daten möglicherweise nicht erfüllt.

Nachfolgend werden Auswirkungen von fehlenden Vorgaben bei der Entwicklung und Erweiterung von Webanwendungen und Web-Services beispielhaft aufgeführt.

- Aufgrund eines fehlenden Vorgehensmodells bei der Softwareentwicklung (Software Development Lifecycle) werden nicht alle Entwicklungsphasen strukturiert durchlaufen, sodass Sicherheitsaspekte gar nicht oder erst in einer späten Entwicklungsphase berücksichtigt werden. In der Folge sinkt die Qualität der Sicherheitsfunktionen, wodurch das angestrebte Sicherheitsniveau nicht erreicht wird oder die Entwicklungskosten aufgrund notwendiger Nachbesserungen steigen.
- Fehlende Programmierrichtlinien (Coding Guidelines) führen zu einer uneinheitlichen Struktur und unterschiedlichen Ausprägungen von Programmierstilen und Sicherheitsmechanismen. Die Einarbeitung in den Programmcode bei der Erweiterung oder Wartung der Webanwendung oder des Web-Service wird dadurch erschwert. Demzufolge sind nachträgliche Änderungen und Erweiterungen nur mit hohem Aufwand umzusetzen und mit steigender Komplexität auch fehleranfälliger.
- Durch die falsche Spezifikation von (sicherheitsrelevanten) Testfällen und die unvollständige Auswahl von Testdaten werden nicht alle denkbaren Anwendungsfälle abgedeckt, sodass Fehler unerkannt bleiben. Wird zum Beispiel die Komponente einer Webanwendung oder eines Web-Service zur Filterung von Eingabedaten auf Basis unzureichender Testfälle und Testdaten geprüft, so werden unvollständig umgesetzte Filtermechanismen nicht erkannt.
- Falls funktionale und rechtliche Anforderungen an die Barrierefreiheit nicht erfüllt werden, ist die Webanwendung nur eingeschränkt von Menschen mit Behinderung nutzbar.

# G 2.159 Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services

Das Benutzerverhalten bei der Bedienung einer Anwendung kann durch das sogenannte *User Tracking* (üblicherweise ohne explizite Zustimmung des Benutzers) aufgezeichnet werden. Da häufig nicht der Betreiber der Webanwendung oder der von der Anwendung genutzten Web-Services die Datenauswertung durchführt, sondern diese als Dienstleistung integriert, werden die erhobenen Daten in der Regel auf Systemen von Drittanbietern gespeichert. Aus den aufgezeichneten Daten können mittels *User Profiling* Personenprofile erstellt werden, die nicht konform mit den Datenschutzbestimmungen sind. Damit besteht die Gefahr, gegen gesetzliche Vorschriften zu verstoßen.

Im Folgenden sind Beispiele für die unbefugte Sammlung personenbezogener Daten aufgeführt:

- Detaillierte Informationen zu Seitenaufrufen und Eingaben bei Webanwendungen und Web-Services werden Benutzern zugeordnet (zum Beispiel mittels Cookies) und über einen längeren Zeitraum protokolliert. Auf der Grundlage dieser Datensammlung können Personenprofile von den Benutzern der Webanwendung oder des Web-Service ohne ihr Wissen erstellt und zum Beispiel unbefugt für Werbezwecke verwendet werden.
- In den Webseiten der Webanwendung werden Bilder von fremden Servern eingebettet und somit von den Clients der Benutzer geladen. Anhand der angeforderten Bilder können die Betreiber der fremden Server Abrufstatistiken über die Webseiten der Webanwendung führen. Werden darüber hinaus IP-Adressen auf dem fremden Server protokolliert, können den Webseiten-Aufrufen IP-Adressen (und somit eventuell Benutzer) zugeordnet werden. Zusätzlich kann der fremde Server mittels Cookies (engl. *Third Party Cookies*) das Verhalten des Benutzers detailliert nachverfolgen.
- In den HTML-Seiten der Webanwendung ist JavaScript-Code eingebettet, der Anweisungen zur Sammlung von Daten über den Client (zum Beispiel installierte Plugins, grafische Auflösung) enthält. Bei dem Aufruf der Webseite werden diese Anweisungen unbemerkt vom Client ausgeführt. Die gesammelten Daten können demnach ohne Kenntnis und Zustimmung des Benutzers als Identifikationsmerkmale zur Erstellung von Benutzerprofilen verwendet werden.
- Es werden von der Webanwendung oder vom Web-Service personenbezogene Daten zwar rechtskräftig erhoben, jedoch nicht angemessen gespeichert, sodass sie von Dritten unbefugt ausgelesen werden können.
- Ein Web-Service überträgt personenbezogene Daten zur aufrufenden Anwendung oder zu anderen Web-Services mit ungesicherten Klartext-Protokollen über unsichere Netze.

# G 2.160 Fehlende oder unzureichende Protokollierung

Mit Hilfe von Protokolldaten kann beispielsweise festgestellt werden, ob Sicherheitsvorgaben verletzt oder ob Angriffsversuche unternommen wurden. Zusätzlich lassen sich die Protokollinformationen für eine Fehleranalyse im Schadensfall und zur Ursachenermittlung oder Integritätsprüfung nutzen.

In einem Informationsverbund gibt es häufig IT-Systeme oder Anwendungen, bei denen die Protokollierung in der Grundeinstellung nicht aktiviert wurde. Solche Systeme und Anwendungen müssen zuvor entsprechend konfiguriert werden. Unter Umständen ist die Protokollierung bei Systemen und Anwendungen nicht möglich. Auch ein unzureichendes Planungskonzept kann ein Grund für eine fehlende Protokollierung sein.

Selbst wenn die Protokollierung bei einzelnen Systemen genutzt wird, können Informationen und daraus resultierende Erkenntnisse verloren gehen, weil sie nicht an einer zentralen Stelle zusammengeführt werden. In Informationsverbünden ohne zentrale Protokollierung ist es schwierig sicherzustellen, dass die relevanten Protokollinformationen aller IT-Systeme erhalten und ausgewertet werden.

Ist es den Benutzern der IT-Systeme und Anwendungen möglich, die Protokollierung selbstständig zu deaktivieren, kann dies ebenfalls zu Problemen führen. Beispielsweise könnte ein Benutzer gegen Richtlinien verstoßen, ohne dass dies Konsequenzen für ihn hätte. Können die Benutzer vorhandene Protokolldateien verändern oder löschen, besteht die Gefahr, dass Sicherheitsverletzungen nicht erkannt werden.

**Beispiel:**

- Ein nicht autorisierter Benutzer versucht, Passwörter für den Web-Mail-Account anderer Benutzer zu erraten. Da mit dem Passwort meist auch andere Dienste genutzt werden können (Single-Sign-on), ist dies für den Angreifer besonders interessant. Durch eine fehlende Protokollierung auf dem Mail-Server wird dieser Angriff nicht erkannt. Der Angreifer hat die Möglichkeit, die Passwörter der Benutzer unbemerkt durch Brute-Force-Methoden herauszufinden.

# G 2.161 Vertraulichkeits- und Integritätsverlust von Protokolldaten

Einige IT-Systeme generieren Protokollinformationen wie Benutzername, IP-Adresse, E-Mail-Adresse und Rechnername, die konkreten Personen zugeordnet werden können. Solche Informationen lassen sich abhören und manipulieren, wenn sie ungesichert und nicht verschlüsselt übertragen werden. Diese Gefahr besteht besonders dann, wenn eine zentrale Protokollierung genutzt wird. Solche Informationen verbessern die Angriffsmöglichkeiten. Wenn ein Angreifer beispielsweise den Benutzernamen kennt, kann er versuchen, die zugehörigen Passwörter zu erraten oder diese über Wörterbuchattacken herauszufinden (siehe auch G 5.18 *Systematisches Ausprobieren von Passwörtern*).

Auch die Integrität der Protokollinformationen kann durch eine ungesicherte und nicht verschlüsselte Übertragung ebenso wie durch Fehlverhalten von Administratoren beeinträchtigt werden. Wenn ein Administrator beispielsweise die Protokolldaten ändert oder diese löscht, um einen Konfigurationsfehler zu vertuschen, so lassen sich die Informationen vielleicht nicht mehr weiterverarbeiten. Des Weiteren können Übertragungsfehler während der Übermittlung zu einem zentralen Protokollierungsserver zu einem Integritätsverlust bei Protokolldaten führen. Unter Umständen werden Daten aber auch vorsätzlich verfälscht, um falsche Informationen weiterzugeben.

**Beispiele:**

- Durch eine Man-in-the-Middle-Attacke kann der Angreifer die übertragenen und nicht verschlüsselten Protokolldaten mitlesen. Somit erhält er konkrete Informationen zum Informationsverbund, wie die IP-Adressen der einzelnen IT-Systeme. Der Angreifer hat nun die Möglichkeit, IP-Adressen zu fälschen und sich für ein anderes IT-System auszugeben ("IP-Spoofing"). In manchen Informationsverbünden ist es üblich, dass sich interne Systeme gegenseitig vertrauen, sodass sich ein Benutzer ohne Benutzername und Passwort einloggen kann. Der Angreifer kann den Zielrechner nun mithilfe der gefälschten IP-Adresse angreifen, ohne sich zu authentisieren.
- Bei der Übertragung der Protokollmeldungen vom Dateiserver zum zentralen Protokollierungsserver kommt es durch physikalische Störungen im Übertragungskanal zu Übertragungsfehlern. Aus diesem Grund wird von den Administratoren nicht bemerkt, dass der Dateiserver in den letzten Stunden immer wieder ausgefallen ist.

# G 2.162 Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Es besteht die Gefahr, dass personenbezogene Daten rechtswidrig verarbeitet werden, wenn keine ausreichende Rechtsgrundlage (Einwilligung oder gesetzliche Erlaubnis, z. B. durch Datenschutzgesetze, Sozialgesetzbuch, Schulgesetze, Polizeigesetze, Krankenhausgesetze) gegeben ist. Ergänzend wird auch auf die Gefährdung G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen* verwiesen.

Eine Verarbeitung personenbezogene Daten ohne ausreichende Rechtsgrundlage kann eine Geldbuße oder Freiheitsstrafe zur Folge haben bzw. zu dienst- oder arbeitsrechtlichen Konsequenzen führen. Der Betroffene kann ein Recht auf Schadensersatz geltend machen.

# G 2.163 Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten

Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder erstmals gespeichert worden sind. Es besteht die Gefahr, dass diese Daten auch für andere Zwecke verarbeitet werden, da damit der Aufwand für eine erneute Erhebung und Information der Betroffenen erspart werden kann.

Werden personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Informationssicherheit oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert wurden, zu anderen Zwecken genutzt, so ist dies unzulässig.

Eine Gefahr, dass die Zweckbindung missachtet wird, besteht insbesondere bei automatisierten Abrufverfahren und sonstigen Übermittlungen sowie bei Verknüpfungen bzw. Auswertungen von Datenbeständen.

Eine Verarbeitung personenbezogene Daten unter Missachtung der Zweckbindung kann eine Geldbuße oder Freiheitsstrafe zur Folge haben bzw. zu dienst- oder arbeitsrechtlichen Konsequenzen führen. Der Betroffene kann ein Recht auf Schadensersatz geltend machen.

**Beispiele:**

- Die Zweckbindung wird verletzt, wenn eine Betriebsleitung Protokolldateien, in denen die An- und Abmeldung von Benutzern an IT-Systemen aus Gründen der Informationssicherheit und des Datenschutzes festgehalten werden, zur Anwesenheits- und Verhaltenskontrolle nutzt.
- In einem Schreibbüro wird die Anzahl der Anschläge bei der Erstellung von Dokumenten für Zwecke der Kostenrechnung protokolliert. Zusätzlich soll dies unzulässigerweise dazu genutzt werden, die Anschlagsleistung der Mitarbeiter festzustellen.
- In der Kantine eines Unternehmens wird das Essen über eine kombinierte Mitarbeiter- und Kantinenkarte bezahlt. Die Kantinen-Abrechnungsdaten werden zur Erarbeitung individueller Gesundheitsvorsorgeprogramme genutzt, ohne dass die Mitarbeiter hierzu ihre Zustimmung gegeben haben.

# G 2.164 Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten

Personenbezogene Daten dürfen nur verarbeitet werden, wenn dies zur Erfüllung der rechtmäßigen Aufgaben der dafür zuständigen datenverarbeitenden Stelle erforderlich ist.

Bei der Datenverarbeitung muss im Interesse des Betroffenen die sein Persönlichkeitsrecht am wenigsten beeinträchtigende Verarbeitung gewählt werden (Verhältnismäßigkeit).

Der Erforderlichkeitsgrundsatz ist immer dann verletzt, wenn Bearbeiter Zugriffsbefugnisse auf komplette Datenbestände erhalten, obwohl sie diese weit reichenden Zugriffsmöglichkeiten für ihre Aufgabenerfüllung nicht brauchen.

Ein sehr kritischer Punkt sind auch die weit reichenden Zugriffsrechte der Systemverwalter und Netzadministratoren. Gängige Betriebssysteme, insbesondere PC- und Netz-Betriebssysteme lassen noch immer allumfassende Zugriffsberechtigungen zu, die es erlauben, beliebige Dateien zu lesen, zu schreiben und insbesondere Protokolldateien, die eigentlich zur datenschutzrechtlichen Kontrolle und Revision der Datenverarbeitung gedacht sind, zu manipulieren oder sogar zu löschen. Somit können mögliche Spuren unerkannt beseitigt werden.

Auch eine fehlende Funktionstrennung zwischen Systemtechnik, Programmierung, Anwendung und Kontrolle und eine fehlende Abschottung von Programmen und Datenbeständen kann eine Überschreitung des Erforderlichkeitsgrundsatzes begünstigen.

**Beispiele:**
- Ein Versicherungssachbearbeiter ist ausschließlich zuständig für Versicherte mit den Anfangsbuchstaben A bis G, kann aber auf die Daten aller Versicherten zugreifen.
- Zugriffsrechte werden entsprechend der Hierarchie der datenverarbeitenden Stelle nach oben durchgereicht, so dass letztendlich der Leiter der Stelle Kraft seines Amtes alle Daten lesen und verändern kann.

# G 2.165 Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten

Datenvermeidung und Datensparsamkeit sind Grundanforderungen, die bei der Bestimmung der zu erhebenden, verarbeitenden oder zu nutzenden Daten nach Art, Umfang und Dauer zu beachten sind. Sie sind gleichzeitig auch Vorgaben für die technische Gestaltung und ihre Auswahl. Eine Verletzung diese Grundsatzes kann unter Anderem eintreten durch:

- Erhebung von mehr Daten, als für den Verarbeitungszweck benötigt werden (z. B. mehr als zwei Kommunikationsadressen wie postalische Adresse, Telefonnummer und E-Mailadresse für Vertragszwecke).
- Verarbeitung von Daten in größerer Detaillierung als benötigt (z. B. Verarbeitung von Geburtsdatum oder Kreditkartennummer, wenn nur die Bestätigung eines Alters von mehr als 18 Jahren benötigt wird).
- Verarbeitung und Speicherung von personenbezogenen Daten über einen längeren Zeitraum als dies für den Verwendungszweck notwendig ist (z. B. Sicherheitsanalysen von Protokolldateien einer Firewall).

Von den Möglichkeiten der Anonymisierung und Pseudonymisierung ist wann immer möglich Gebrauch zu machen.

# G 2.166 Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten

Das Datengeheimnis, d. h. der Schutz personenbezogener Daten, wird verletzt, wenn Personen, die Zugriff auf personenbezogene Daten haben, solche Daten unbefugt verarbeiten. Die Pflicht zur Wahrung des Datengeheimnisses gilt auch nach Beendigung der Tätigkeit. Ursache für solche Verletzungen sind oft eine Unkenntnis der Bearbeiter über die geltenden datenschutzrechtlichen Bestimmungen, die bei Aufnahme ihrer Tätigkeiten nicht entsprechend unterrichtet oder nicht auf den Datenschutz verpflichtet wurden.

Das Datengeheimnis kann verletzt werden durch das Nichtlöschen oder Verfälschen von gespeicherten personenbezogenen Daten, die Weitergabe von Adressdateien an Werbeunternehmen, die Weitergabe von personenbezogenen Daten innerhalb der Behörde oder des Unternehmens ohne dienstlichen Anlass, die unbefugte Einsichtnahme in Personaldaten, das Erstellen unzulässiger Auswertungen, die Nutzung dienstlicher Daten für private Zwecke (z. B. Weitergabe von Bonitätsdaten eines Nachbarn durch einen Mitarbeiter einer Bank im privaten Kreis).

**Beispiele:**

- Ein Mitarbeiter eines TK-Unternehmens benutzt seine dienstliche Berechtigung zur Abklärung der Bonität von Kunden dazu, Daten der Schufa oder anderer Wirtschaftsauskunfteien über einen missliebigen Nachbarn abzurufen und diese an Verwandte oder Bekannte weiterzugeben.
- Ein Mitarbeiter am Empfang eines Hotels gibt Anmeldedaten berühmter Gäste an die Presse, um sich damit ein Zubrot zu verdienen.
- Ein Administrator einer Stadtverwaltung hat bei seinen Arbeiten mit den Melderegister-Dateien zufällig die geheimgehaltene Anschrift einer alleinerziehenden Mutter gesehen und gibt diese an einen Bekannten im Sportverband weiter, dem das Sorgerecht wegen Bedrohung der Mutter und des Kindes entzogen und eine Kontaktaufnahme verboten worden war.

# G 2.167 Fehlende oder nicht ausreichende Vorabkontrolle

Weist eine Verarbeitung personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen auf wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG). Dies gilt allerdings nicht, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. In manchen Landesdatenschutzgesetzen ist eine Vorabkontrolle generell bei allen Verfahren vorgeschrieben, mit denen personenbezogene Daten durch öffentliche Stellen verarbeitet werden. Die Voraussetzungen hierfür können von den beim Bund geltenden Regelungen abweichen.

Wird eine vorgeschriebene Vorabkontrolle nicht oder nur unzureichend durchgeführt, können sich Gefahren für das informationelle Selbstbestimmungsrecht ergeben.

**Beispiele:**

- Wenn Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, von Unbefugten genutzt werden können, beispielsweise weil sie sich auf Grund unzureichender Sicherungsmaßnahmen Zutritt oder Zugang verschaffen können und dabei Kenntnis von Daten erhalten, kann dies besondere Risiken für die Rechte und Freiheiten der Betroffenen zur Folge haben.
- Die Vertraulichkeit und Integrität der Daten kann bei der Verarbeitung bzw. während einer Datenübermittlung verletzt werden, wenn diese nicht ausreichend geschützt werden (z. B. durch Verschlüsselung).
- Personenbezogene Daten, die im Auftrag verarbeitet werden, können durch den Auftragnehmer weit reichender als vertraglich geregelt zum Schaden der Betroffenen verarbeitet werden.
- Personenbezogene Daten können unter Umgehung der Zweckbindung verarbeitet und unzulässigerweise miteinander zum Nachteil der Betroffenen verknüpft werden.

# G 2.168 Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten

Die Ausübung der aus dem Datenschutz herrührenden Rechte der Betroffenen (z. B. das Recht auf Auskunft, Berichtigung, Sperrung, Löschung) können diesen von der datenverarbeitenden Stelle aus technischen oder organisatorischen Gründen in unzulässiger Weise verwehrt werden. Die Betroffenen können ihre Rechte auch nicht ausüben, wenn Informationen unvollständig angegeben werden.

**Beispiele:**

- Ein Kunde wünscht Berichtigung der über ihn gespeicherten Daten. Die zuständige Stelle gibt vor, der Aufwand sei zu groß oder die technischen Möglichkeiten fehlten.
- Die Stelle erteilt eine unvollständige oder nicht aktuelle Auskunft über die gespeicherten Daten des Betroffenen.

# G 2.169 Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten

Die Vergabe von Tätigkeiten der Datenverarbeitung nach Außen im Wege einer Auftragsdatenverarbeitung ist unter der Voraussetzung zulässig, dass der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist. Die Vergabe des Auftrags hat unter besonderer Berücksichtigung der technischen und organisatorischen Eignung des Auftragnehmers zu erfolgen. Der Auftrag hat schriftlich zu erfolgen, wobei die Datenverarbeitung selber sowie die zugehörigen technischen und organisatorischen Maßnahmen zu beschreiben sind. Zu diesen Maßnahmen gehört insbesondere auch die Gewährleistung der Auftragskontrolle. Der Auftragnehmer bleibt bezogen auf die Datenverarbeitung weisungsgebunden.

Diese Bestimmungen gelten auch für die Prüfung und Wartung von technischen Anlagen, die der automatisierten Verarbeitung personenbezogener Daten dienen (Fernwartung).

**Beispiele:**

- Ein Unternehmen möchte die technische Abwicklung der Lohnbuchhaltung im Rahmen eines Application-Services an einen Dienstleister auslagern. Die Datenverarbeitung findet so statt, dass Mitarbeiter des Dienstleisters im Zuge der Administration und Datensicherung auch Zugriff auf die Lohndaten nehmen können. Die vertraglichen Vereinbarungen regeln lediglich die Verfügbarkeit und das Wiederanlaufen des Dienstes der Lohnbuchhaltung. Aus ungeklärter Ursache kommen Lohndaten von Mitarbeitern des Auftraggebers in die Öffentlichkeit. Sie werden zur Anprangerung der Einkommen der Mitarbeiter benutzt. Konkurrierende Unternehmen versuchen Mitarbeiter mit besseren Angeboten abzuwerben und den Konkurrenten damit zu schädigen. Betroffene Mitarbeiter beschweren sich bei der zuständigen Aufsichtsbehörde.
- Im Zuge der Überprüfung der Datenverarbeitung des Auftraggebers stellt die Aufsichtsbehörde fehlende Regelungen der Auftragsdatenverarbeitung fest, da wesentliche vertragliche Vereinbarungen zur Sicherstellung der datenschutzrechtlichen Bestimmungen (hier insbesondere bezogen auf die Umsetzung der Sicherheitsziele des Datenschutzrechtes, Überprüfung der Umsetzung beim Dienstleister und Vereinbarungen für den Fall der mangelhaften Umsetzung) fehlen. Die Aufsichtsbehörde muss dies beanstanden und fordert dazu auf, die Mängel kurzfristig abzustellen.

# G 2.170 Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen

Werden personenbezogene Daten erhoben, ohne dass der Betroffene über die vorgesehene Verarbeitung und die Rechtsgrundlage unterrichtet wird, ist die Transparenz in Frage gestellt.

Sie ist auch in Frage gestellt, wenn ihm Angaben über die Herkunft und den Empfänger dieser Daten sowie Löschungsfristen vorenthalten werden.

Werden die Datenschutz-Kontrollinstanzen nicht rechtzeitig vor

- der Einführung neuer Verfahren,
- der Freigabe von Verfahren,
- dem Erlass von Verwaltungsvorschriften,
- der Einrichtung von automatisierten Abrufverfahren oder
- einer Vergabe von Datenverarbeitung im Auftrag

informiert, werden sie daran gehindert, Vorschläge zur Verbesserung des Datenschutzes so rechtzeitig zu unterbreiten, dass noch eine Berücksichtigung bei der Verfahrensentwicklung möglich ist. Die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen verbleibt auch bei Einbeziehung der Datenschutz-Kontrollinstanzen bei der datenverarbeitenden Stelle.

Durch fehlende oder mangelhafte Protokollierung und Dokumentation bei der Verarbeitung personenbezogener Daten und durch fehlende Aktualisierung bei Verfahrensänderungen wird die Arbeit der Kontrollinstanzen beeinträchtigt. Eine effektive Kontrolle kann auch durch unvollständige oder nicht aktualisierte Verzeichnisse der eingesetzten IT-Systeme, mangelhafte Konfigurationsübersichten und fehlende Verkabelungspläne gefährdet sein.

Fehlende oder unvollständige Meldungen zu den internen Verzeichnissen und, soweit gesetzlich vorgeschrieben, zu den öffentlichen Verzeichnissen gefährden die Transparenz der Datenverarbeitung für den Betroffenen und die Kontrollinstanzen.

**Beispiele:**

- Einem Betroffenen ist durch eine unzulässige automatisierte Datenverarbeitung einer öffentlichen Stelle Schaden entstanden. Ein Versuch, durch Einsicht in das Verfahrensverzeichnis (soweit ein solches vorhanden ist) beim zuständigen Landesbeauftragten für den Datenschutz nähere Informationen zu erhalten, kann daran scheitern, dass dort keine Meldungen vorliegen oder dass in der Meldung, obwohl vorgeschrieben, die Partner durchgeführter Übermittlungen nicht genannt sind.
- Wegen fehlender Verfahrensbeschreibungen weiß niemand in einer öffentlichen Stelle, welche Dateien von welchen Ämtern über welchen Bediensteten geführt werden.

# G 2.171 Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten

Durch unzureichende technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten besteht vor allem die Gefahr, dass

- Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten können,
- Datenverarbeitungssysteme durch Unbefugte benutzt werden können,
- Berechtigte auf Daten außerhalb ihrer Zugriffsberechtigungen zugreifen können,
- personenbezogene Daten unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- nicht überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,
- nicht nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,
- personenbezogene Daten, die im Auftrag verarbeitet werden, entgegen den Weisungen des Auftraggebers verarbeitet werden können,
- personenbezogene Daten nicht gegen zufällige Zerstörung oder Verlust geschützt sind,
- das nicht gewährleistet ist, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

**Beispiele:**

- Beispielsweise glauben viele IT-Betreuer, dass es bei einzelstehenden PCs, die auch nur durch eine Person mit einer Anwendung genutzt werden, ausreichen würde, den PC durch ein individuelles BIOS-Passwort zu schützen. Dabei wird übersehen, dass der BIOS-Passwortschutz in vielen Fällen mit einfachen Mitteln und in kurzer Zeit zu umgehen ist, so dass personenbezogene Daten unbemerkt zur Kenntnis genommen oder gar verfälscht werden können. Dazu gehört auch, dass PCs, insbesondere tragbare Geräte, sehr leicht gestohlen werden können und dann die Daten, wenn sie nicht verschlüsselt sind, mit Programmen des Betriebssystems von jedem Kundigen ausgelesen und missbräuchlich verwendet werden können.
- Ein bei Kontrollen immer wieder aufgedecktes Problem besteht darin, dass bei IT-Systemen zwar der Zugriff auf die Programme und Datenbestände durch eine Benutzeridentifikation (Benutzerkennung und Passwort) und eine gezielte Benutzerführung (Menüsystem, benutzerspezifische Oberfläche) abgesichert ist, aber es z. B., obwohl gesetzlich vorgeschrieben, nachträglich nicht mehr feststellbar ist, welche Daten in Datenverarbeitungssysteme eingegeben wurden, da man es bei der Konzipierung der Systeme versäumt hat, auch eine ausreichende Protokollierung zu integrieren.
- Ausgelöst durch Diskussionen um eine Reduzierung der Personalkosten und der Kosten der Datenverarbeitung glauben viele Anwender, die vorhandenen Probleme durch eine Verlagerung der Datenverarbeitung außer Haus zu lösen und damit die Verpflichtung zum Datenschutz auf den

Auftragnehmer verlagern zu können. Dabei werden oft die in den Datenschutzgesetzen enthaltenen Bestimmungen im Rahmen der Datenverarbeitung im Auftrag übersehen, die eine klare vertragliche Regelung verlangen und die Verantwortung einschließlich einer Kontrolle der technischen und organisatorischen Maßnahmen weiterhin beim Auftraggeber belassen.

# G 2.172 Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland

Bei der Übermittlung personenbezogener Daten ins Ausland sind besondere gesetzliche Bestimmungen zu beachten. Personenbezogene Daten dürfen in die Mitgliedstaaten der Europäischen Union unter den gleichen Voraussetzungen übermittelt werden wie innerhalb der Bundesrepublik Deutschland. An Stellen in so genannte Drittländer dürfen personenbezogene Daten nur übermittelt werden, wenn dort ein angemessenes Datenschutzniveau (vergleiche § 4b Abs. 3 BDSG) gewährleistet ist, die im Gesetz genannten Ausnahmen vorliegen (§ 4c Abs. 1 BDSG) oder die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist (§ 4 c Abs. 2 BDSG). Im letzteren Fall bedürfen die Übermittlungen einer Genehmigung durch die Aufsichtsbehörden.

**Beispiel:**

- Ein deutsches Unternehmen, das zu einem international agierenden Konzern gehört, möchte seine bisherige nationale Zugangs- und Zugriffsverwaltung auf einen Verzeichnisdienst (Directory Service) umstellen, der in Japan durch eine andere Konzerntochter zentral betrieben werden soll.
- Japan hat (noch) kein angemessenes Datenschutzniveau. Die Weitergabe von personenbezogenen Daten an einen japanischen Auftraggeber ist daher nur zulässig, wenn durch geeignete Maßnahmen ein angemessenes Datenschutzniveau gewährleistet wird. Dies kann durch Unterzeichnung der so genannten Standardvertragklauseln zwischen dem deutschen Auftraggeber und dem japanischen Auftragnehmer erfolgen.

# G 2.173 Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten

Niemand darf einer automatisierten Entscheidung unterworfen werden, die für ihn eine negative rechtliche Folge nach sich zieht oder ihn erheblich beeinträchtigt. Voraussetzung dieses Verbotes ist, dass sich die Entscheidung ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten stützt, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Das Verbot gilt nicht, wenn dem Begehren des Betroffenen stattgegeben wurde. Eine Ausnahme gilt auch, wenn der Betroffene über die automatisierte Einzelfallentscheidung unterrichtet wurde und seine schutzwürdigen Interessen durch geeignete Maßnahmen gewährleistet werden. Hierzu zählt die Möglichkeit, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist dann verpflichtet, ihre Entscheidung erneut zu überprüfen.

Der Betroffene ist in jedem Fall über die Verarbeitung seiner Daten, die der automatisierten Einzelfallentscheidung zugrunde gelegt werden, den Verwendungszweck und die Kategorien der Empfänger zu unterrichten. Um seinen Standpunkt geltend machen zu können, muss er zudem über die Folgen der Verarbeitung und über die Funktionsweise des konkreten Verfahrens (logischer Aufbau) informiert werden.

**Beispiele:**

- Eine Stelle prognostiziert mit Hilfe eines Scoringsystems die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder das zukünftige Verhalten einer Person. Unabhängig vom Ergebnis des Verfahrens hat die verantwortliche Stelle gegenüber dem Betroffenen Informationspflichten. Werden diese vernachlässigt, wird gegen geltende Gesetze verstoßen.
- Wird mit Hilfe des Scoringsystems eine für den Betroffenen nachteilige Entscheidung gefällt, so muss die Daten verarbeitende Stelle durch geeignete Maßnahmen dafür Sorge tragen, dass die berechtigten Interessen der Betroffenen gewahrt bleiben. Hierzu bedarf es nicht nur der Transparenz gegenüber dem Betroffenen, sondern insbesondere auch der Möglichkeit, seinen Standpunkt gegenüber der Stelle geltend zu machen, so dass die Entscheidung einer erneuten Überprüfung unterzogen wird. Werden die Interessen des Betroffenen verletzt oder eine erneute Überprüfung unterlassen, kann sich der Betroffene an die zuständige Datenschutzaufsicht wenden.

# G 2.174 Fehlende oder unzureichende Datenschutzkontrolle

Die Kontrolle der Einhaltung der geltenden Datenschutz-Bestimmungen, vor allem die Kontrolle der technischen und organisatorischen Maßnahmen wird oft unzureichend bleiben, wenn in ihr zu Unrecht nur ein unproduktiver Kostenfaktor gesehen wird. Die datenschutzrechtliche Kontrolle kann auch dadurch sehr erschwert werden, wenn versäumt wird, ihre Anforderungen schon bei der Entwicklung und Erprobung von Verfahren einzubeziehen.

Eine effektive Arbeit für eine Datenschutzkontrolle ist in aller Regel nicht gesichert, wenn in einem Unternehmen oder einer Behörde kein Datenschutzbeauftragter bestellt ist oder wenn der vorhandene Datenschutzbeauftragte nicht ausreichend qualifiziert oder geschult ist, oder wenn er nicht ausreichend unterstützt und nicht rechtzeitig informiert wird (unzureichende Personal- und Sachmittel).

**Beispiele:**

- Der Leiter des Rechenzentrums wird zum internen Datenschutzbeauftragten bestellt, da dieser für das Amt die besten Fachkenntnisse mitbringt. Dabei wird die entstehende Interessenkollision übersehen. Dazu gehört beispielsweise, dass er Sicherheitsvorgaben, die er für den Betrieb von IT-Verfahren gemacht hat oder Protokolldaten, die zur Missbraucherkennung gespeichert wurden, als Datenschutzbeauftragter kontrollieren müsste.
- Es wird eine interne Datenschutzrichtlinie erlassen, nach der jährlich ein Bericht des Datenschutzbeauftragten vorzulegen ist. Der bestellte Datenschutzbeauftragte ist aber schon seit 2 Jahren dauerhaft krank und ein Vertreter wurde nicht ernannt, so dass kein Bericht erstellt wird.

# G 2.175 Unzureichende Isolation und Trennung von Cloud-Ressourcen

Die Bereitstellung von Cloud-Diensten für verschiedene Cloud-Anwender (Mandanten) aus einer gemeinsamen und verteilten Cloud-Infrastruktur ist ein wesentliches Merkmal von Cloud Computing. Durch die gemeinsam genutzte Cloud-Infrastruktur entsteht die Gefährdung, dass ein Cloud-Mandant unberechtigt auf die Informationen eines anderen zugreifen und diese manipulieren oder löschen kann. Dadurch können Schäden sowohl für Cloud-Anwender als auch für Cloud-Diensteanbieter entstehen.

Bei der Zusammenlegung von Ressourcen können verschiedenste Gefährdungen entstehen, wie die folgenden Beispiele zeigen:

- Gefährdungen innerhalb eines Virtualisierungsservers: Wenn ein Mandant von einer virtuellen Maschine, auf die er vollen Zugriff hat (z. B. bei IaaS), unerlaubt Zugriff auf eine fremde virtuelle Maschine bekommt.
- Gefährdungen durch Remote-Angriffe über das Netz, wie beispielsweise Man-In-The-Middle-Angriffe, mit dem Ziel, unerlaubt den Netzwerkverkehr von einer fremden virtuellen Maschine abzufangen.
- Gefährdungen durch Zugriff auf fremde Storage-Ressourcen, wie z. B. das Vortäuschen von fremden Identitäten mit dem Ziel Zugriff auf die Daten eines anderen Mandanten zu erlangen.
- Gefährdungen durch Injection-Angriffe: Bei SaaS werden Kundendaten meist in einer gemeinsamen Datenbank gespeichert. Die Unterscheidung der Kunden untereinander erfolgt dann anhand einer sogenannten Tenant-ID. Ist die geteilte Applikation unsicher programmiert, dann könnte ein Kunde z. B. über eine SQL-Injection unerlaubt auf die Daten eines anderen Kunden zugreifen.

# G 2.176 Mangelnde Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender

Die Nutzung von Cloud-Diensten erfordert eine umfassende Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender. Dadurch, dass der Cloud-Anwender eine externe Dienstleistung bezieht und darüber hinaus gegebenenfalls diesbezügliche Sicherheitsmanagement-Tätigkeiten ausgelagert werden, ist eine enge Koordination zwischen den beiden Parteien notwendig.

Eine mangelnde Kommunikation zum Cloud-Anwender kann in verschiedensten Phasen und Prozessen auftreten und unterschiedliche negative Auswirkungen haben, wie die nachfolgenden Beispiele zeigen.

**Beispiele:**

- **Mangelnde Kommunikation während Planung und Beauftragung**
  Insbesondere bei der Planung und Beauftragung der Cloud-Dienste können mangelnde Kommunikation und Abstimmung zwischen den Beteiligten sehr starke negative Auswirkungen auf die Leistungserbringung haben. Sofern in dieser Phase die verschiedenen Anforderungen nicht kommuniziert und berücksichtigt werden, wird dies im weiteren Verlauf der Leistungserbringung zu unterschiedlichsten Problemen führen. Hieraus können sich erhebliche Mehrkosten auf beiden Seiten ergeben, beispielsweise durch Vertragsänderungen, zusätzliche Sicherheitsmaßnahmen, zusätzliche Audits oder möglicherweise sogar juristische Folgen.
- **Mangelnde Kommunikation über die Einhaltung der Dienstgüte**
  Sofern der Nachweis der Dienstgüte gegenüber dem Cloud-Anwender aufgrund von mangelnder Kommunikation oder undefinierten Kommunikationsschnittstellen nicht erbracht werden kann, ist die korrekte Leistungserbringung bei Unstimmigkeiten nicht zweifelsfrei belegbar, und die Rechnungsstellung wird gefährdet. Mangelhafte oder nicht kommunizierte Kennzahlen hinsichtlich der Dienstgüte können dazu führen, dass der Cloud-Diensteanbieter die vereinbarten Anforderungen unbemerkt über- oder untererfüllt. Somit kann eine ineffiziente Ressourceneinteilung sowohl vom Cloud-Anwender als auch vom Cloud-Diensteanbieter unbemerkt bleiben.
- **Mangelnde Kommunikation im Sicherheitsvorfallmanagement**
  Durch eine ungenügende Kommunikation im Rahmen des Störungsmanagements oder Sicherheitsvorfallmanagements können Schnittstellen nicht bekannt oder Ansprechpartner außerhalb von Betriebszeiten nicht erreichbar sein. Daraus ergeben sich gegebenenfalls erhebliche Verzögerungen bei der Bearbeitung von Störungen und Vorfällen.

# G 2.177 Fehlplanung von Cloud-Diensteprofilen

Cloud-Diensteprofile bestehen aus einem Informationssatz, der die Cloud-Ressourcen (z. B. Arbeitsspeicher, CPU, Storage) und die zugrunde liegende Konfiguration beschreibt. Anhand dieser Informationen wird der Cloud-Dienst provisioniert.

Eine Fehlplanung von Cloud-Diensteprofilen führt dazu, dass die zugesagte Leistung eines Cloud-Dienstes nicht ermöglicht bzw. verhindert wird. Eine Fehlplanung von Cloud-Dienstprofilen liegt dann vor, wenn die Konfiguration der Profile oder die zugeordneten Cloud-Ressourcen die zugesagte Leistung eines Cloud-Dienstes nicht ermöglichen bzw. verhindern. Den gleichen Effekt können ungeprüfte Cloud-Diensteprofile hervorrufen.

**Beispiele:**

- In der Konfiguration eines Cloud-Diensteprofils wird mithilfe eines statischen Pfades auf ein Speicher-System verwiesen. Der Zugriff auf diesen Speicherbereich ist auf Basis von Quell-Adressen eingeschränkt. Bei einer Reproduktion des Cloud-Dienstes wird eine andere Quell-Adresse erzeugt, wodurch kein Zugriff mehr auf den Cloud-Storage besteht. In diesem Beispiel sind die Konfiguration und das Datenmodell der Cloud-Anwendung fehlerhaft und nicht für eine skalierbare Automatisierung eines Cloud-Dienstes ausgelegt.
- Cloud-Diensteprofile werden nicht ausreichend getestet. In der Folge werden Cloud-Dienste nicht korrekt oder nicht in vereinbarter Güte bereitgestellt.

# G 2.178 Unzureichendes Notfallmanagement beim Cloud-Diensteanbieter

Im Rahmen eines IT-Betriebs können Störungen und Unglücke, auch größere, erfahrungsgemäß nicht vollständig verhindert werden. Aufgrund der Konzentration der Ressourcen in zentralen Rechenzentren können Versäumnisse im Notfallmanagement beim Cloud Computing schnell gravierende Folgen nach sich ziehen. Ein unzureichendes Notfallmanagement kann Probleme, die bei Störungen und Unglücken in einer Cloud-Infrastruktur auftreten, wesentlich verschlimmern, Ausfallzeiten verlängern und so die Produktivitätseinbußen, die der Cloud-Diensteanbieter bei einem Notfall erleidet, noch verstärken.

Über den eigentlichen Notfall hinaus kann unzureichendes Notfallmanagement das Vertrauensverhältnis zwischen Cloud-Anwender und Cloud-Diensteanbieter aushöhlen, bis hin zur Kündigung der Dienstleistungsvereinbarung.

Unzureichendes Notfallmanagement äußert sich in unzureichender Koordination und unstrukturiertem Vorgehen bei der Behebung aufgetretener Probleme.

Unzureichendes Notfallmanagement kann sich in der **Notfallwiederherstellung** (engl. Disaster Recovery) oder im **Betriebskontinuitätsmanagement** (**betriebliches Kontinuitätsmanagement**, engl. Business Continuity Management) oder in beidem zeigen.

**Beispiele:**

- Fehlende Festlegungen von Grundgrößen für das Notfallmanagement, insbesondere von maximal tolerierbarer Ausfallzeit (MTA, engl. MTO: Maximum Tolerable Outage), maximaler Wiederanlaufzeit (engl. RTO: Recovery Time Objective), maximal tolerierbarem Datenverlust (engl. RPO: Recovery Point Objective) für Cloud-Infrastruktur oder Cloud-Dienste. Somit ist keine verlässliche Planung für ein effektives und sachgerechtes Vorgehen bei Notfällen möglich.
- Fehlende, unzureichende oder veraltete Notfallpläne für die Cloud-Infrastruktur oder für Cloud-Dienste.
- Nicht getestete Notfallpläne (z. B. fehlende oder unzureichende Sofortmaßnahmen und Disatser-Recovery-Skripte) für Cloud-Infrastruktur oder Cloud-Dienste.
- Nicht oder unzureichend geregelte Zuständigkeiten für Notfallbehandlung für die Cloud-Infrastruktur oder die Cloud-Dienste.
- Nicht definierte Kommunikations-, Eskalations- und Entscheidungswege für Notfallbehandlung für die Cloud-Infrastruktur oder die Cloud-Dienste bzw. deren Nicht-Einhaltung.
- Ein Notbetrieb für die Cloud-Infrastruktur oder die Cloud-Dienste ist nicht oder nur unzureichend vorgesehen.
- Fehlende, unvollständige oder falsch festgelegte Planung für die Nutzung von Ausweichkapazitäten für die Cloud-Infrastruktur, insbesondere die Umschaltung auf ein Ausweich-Rechenzentrum. Dies kann insbesondere eintreten, wenn keine oder eine falsche Priorisierung von Cloud-Diensten für eine Umschaltung vorgenommen wurde, oder wenn Abhängigkeiten, die eine bestimmte Reihenfolge erfordern, nicht festgelegt wurden oder nicht beachtet werden.

- Der Ausfall von Cloud-Administratoren kann nicht kompensiert werden, weil Handlungsanweisungen nicht dokumentiert wurden. Dies kann insbesondere eintreten, wenn die Administratoren "alles im Kopf" haben und an eine mögliche Nicht-Verfügbarkeit nicht gedacht wurde.
- Nicht aktuelle oder unvollständige Datensicherungen der Cloud-Dienste oder der unterliegenden Infrastruktur. Dies kann insbesondere eintreten, wenn Sicherungszyklen oder Aufbewahrungsfristen nicht oder falsch festgelegt wurden bzw. nicht geprüft wurde, ob Datensicherungen erfolgreich waren.
- Nicht funktionierende Wiederherstellung von Cloud-Diensten aus Datensicherungen.
- Fehlende, unvollständige oder fehlerhafte Wiederanlaufpläne für Cloud-Infrastruktur oder für Cloud-Dienste.
- Fehlende, unvollständige oder falsch festgelegte Priorisierung von Cloud-Diensten für einen Wiederanlauf.
- Nicht, unvollständig oder falsch festgelegte Reihenfolge für einen Wiederanlauf der Cloud-Infrastruktur oder der Cloud-Dienste.

# G 2.179 Fehlende Herstellerunterstützung bei der Bereitstellung von Cloud-Diensten

Es kommt selten vor, dass alle Anwendungen, Produkte oder Plattformen aus der Cloud vom Cloud-Diensteanbieter selbst verantwortet oder entwickelt werden. Oft besteht die Konstellation, dass der Cloud-Diensteanbieter zur Bereitstellung der Cloud Services auch Drittdienstleister hinzuzieht, In solchen Fällen entstehen Abhängigkeiten, die dazu führen können, dass die Cloud-Dienste beeinträchtigt werden.

Für die Cloud-Dienste ergeben sich verschiedene Gefährdungsszenarien, die vor allem mit fehlender Herstellerunterstützung (d. h. Unterstützung der beteiligten Dritten) zu tun haben.

**Fehlerhaftes Vornehmen von Sicherheitseinstellungen durch Dritthersteller**

Für Cloud-Dienste, die auf Anwendungen von Drittherstellern basieren, übernimmt der Cloud-Diensteanbieter die notwendigen Konfigurationen, die auch Sicherheitseinstellungen enthalten. Es besteht die Gefährdung, dass der Dritthersteller nicht auf die notwendigen Sicherheitskonfigurationen hinweist oder den Cloud-Diensteanbieter nicht ausreichend für die Umsetzung der Sicherheitseinstellungen unterstützt.

Wenn aus Gewährleistungsgründen Sicherheitseinstellungen ausschließlich durch den Dritthersteller vorgenommen werden dürfen, besteht für den Cloud-Dienstanbieter die Gefährdung, dass der Dritthersteller fehlerhaft konfiguriert. Dies ist zum Beispiel der Fall, wenn eine Anwendung vom Cloud-Diensteanbieter eingekauft wird und sicherheitsrelevante Konfigurationen (wie z. B. die Auswahl eines hinreichend sicheren Verschlüsselungsalgorithmus) nur mit der Unterstützung eines Software-Herstellers möglich sind.

**Beschränkte Kompatibilität der eingesetzten Cloud-Komponenten von Dritten**

Es kann vorkommen, dass Cloud-Dienste, die auf Anwendungen von Drittherstellern basieren, inkompatibel mit der zugrunde liegenden Cloud-Infrastruktur sind. Anwendungen werden häufig durch ihren Hersteller für eine bestimmte Kombination aus Betriebssystem und Hardwareplattform freigegeben. Zum Beispiel kann eine Cloud-Anwendung von einem Dritthersteller nur für ein Windows Betriebssystem in der bestimmten Version freigegeben worden sein und eine Herstellerunterstützung nur bei Einhaltung dieser Vorgaben zu Kompatibilität vorgesehen worden sein. Hieraus entsteht die Gefährdung, dass im Falle einer Schwachstelle oder eines Anwendungsfehlers der Hersteller nicht unterstützt oder eine Fehlerbehebung nur unter Änderung der zugrunde liegenden Plattform möglich ist. Dies kann dazu führen, dass die Dienste-Qualität beeinträchtigt und im schlimmsten Fall eine Beseitigung von Schwachstellen verhindert wird.

**Fehleranfälligkeit durch fehlende Nutzung von standardisierten Formaten**

Bei Angeboten der form IaaS kann die Portabilität von virtuelle Maschinen dadurch erreicht werden, dass OVF (Open Virtualization Format) eingesetzt

wird. OVF ist ein plattformunabhängiger Standard, der dazu eingesetzt werden kann, virtuelle Appliances zu verpacken und zu verteilen. Oft nutzen allerdings Anbieter von virtuellen Maschinen eigene Formate.

Dadurch wird eine Verpackung und Verteilung von virtuellen Maschinen erschwert. Entsprechend muss der Cloud-Diensteanbieter viele Konfigurationen und Operationen im Cloud Management für die Verteilung von Cloud-Diensten vornehmen, wodurch der Cloud Management Prozess /(Cloud-Konfiguration) fehleranfälliger wird.

# G 2.180 Fehlerhafte Provisionierung und De-Provisionierung von Cloud-Diensten

Das Cloud Management sorgt im Betrieb der Cloud-Dienste für die korrekte und leistungsfähige Konfiguration der Cloud-Infrastruktur und der Dienste. Ein wichtiger Bestandteil ist hier die geregelte Orchestrierung, also die Provisionierung und De-Provisionierung von Cloud-Ressourcen (Arbeitsspeicher, CPU, Storage, virtuelle Netze usw.) und deren Konfiguration (Einrichtung der virtuellen Maschinen usw.). Die Informationen hierfür werden in Cloud-Diensteprofilen hinterlegt.

Gefährdungen im Rahmen der Provisionierung und De-Provisionierung von Cloud-Diensten gehen auf Fehler in der Planung und Konzeption zurück. Eine unzureichende Provisionierung und De-Provisionierung liegt vor, wenn die vorliegenden Leistungsmerkmale von Cloud-Diensten von den zugesagten abweichen. Eine unzureichende Provisionierung und De-Provisionierung äußert sich in der falschen Zuweisung von Cloud-Ressourcen und in der falschen Zuweisung von Cloud-Diensteprofilen.

**Beispiele:**

- Es besteht eine Gefährdung für den Betrieb der Cloud-Infrastruktur, wenn die Planung der benötigten Ressourcen für die Cloud-Diensteprofile nicht ausreichend erfolgt. Dies kann auf Schwächen im Anforderungsmanagement zurückgeführt werden. Die falsche oder nicht ausreichende Aufnahme von Cloud-Diensteanforderungen kann dazu führen, dass Cloud-Dienste nicht korrekt bereitgestellt werden und damit verbundene Provisionierungen von Cloud-Ressourcen nicht korrekt funktionieren können.
- Die Umsetzung des Provisionierungsprozesses wird in den Komponenten zur Bereitstellung der Cloud-Ressourcen (sogenannte *Cloud Element Manager* oder kürzer *Element Manager*) nicht kontrolliert. Die Provisionierung ist damit nicht ausreichend getestet.
- Durch falsche Priorisierung der Cloud-Ressourcen ergibt sich in "Stoßzeiten" eine Überlastung der Cloud-Infrastruktur, z. B. bei Monatsabschlüssen.
- Ein virtuelles System für einen Cloud-Dienst wird mit ausreichend Arbeitsspeicher und CPU ausgestattet, die externe Anbindung an die Cloud-Anwender wird jedoch nicht hinreichend dimensioniert.

# G 2.181 Mangelhafte Planung und Konzeption des Einsatzes von Web-Services

Web-Services weisen oft einen hohen Komplexitätsgrad auf. Gerade in Bezug auf die flexible Interaktion verschiedener Web-Services ist es daher erforderlich, sorgfältig zu planen. Typische Planungsfehler umfassen:

- Standards werden nicht berücksichtigt: Gerade für Web-Services existiert eine sehr hohe Anzahl an Standards zu vielfältigen Aspekten. Einige sicherheitsrelevante Standards werden in der Maßnahme M 4.451 *Aktuelle Web-Service Standards* vorgestellt. Werden die einschlägigen Standards nicht berücksichtigt, kann die Interoperabilität mit anderen Web-Services erschwert oder verhindert werden.
- Veraltete, noch nicht ausgereifte oder ungeeignete Standards oder Protokolle werden ausgewählt: Nicht alle Standards haben sich durchgesetzt. Einige publizierte Standards wurden zwischenzeitlich durch neuere Konzepte ergänzt. Veraltete Kommunikationsprotokolle verfügen oft nicht über ausreichende Sicherheitseigenschaften.
- Die geforderte Funktionalität wird falsch umgesetzt: Wenn die Anforderungen aus dem zu unterstützenden Geschäftsprozess nicht korrekt erfasst, dokumentiert oder verstanden wurden, besteht die Gefahr, dass der Web-Service (oder mehrere Web-Services in ihrem Zusammenwirken) an den Anforderungen "vorbei" entwickelt werden und die eigentlich vorgesehene Aufgabe nicht oder nur unzureichend erfüllen.
- Die Anwendungsarchitektur wird unpassend gewählt: Wenn bei der Gestaltung der Architektur nicht alle relevanten Anforderungen geeignet berücksichtigt werden, kann es sein, dass die Funktionalität, Sicherheit oder Verteilbarkeit der Web-Services nicht oder nur mit erhöhtem Aufwand realisiert werden kann. Weiterhin besteht die Gefahr, dass die zur Realisierung der Architektur ausgewählten Komponenten nicht alle erforderlichen Funktionen und Standards unterstützen.
- Verfügbarkeits- und Leistungsanforderungen werden nicht berücksichtigt: Die Architektur und Realisierung der Web-Services muss die vorhandenen Anforderungen an die Verfügbarkeit und Leistungsfähigkeit geeignet berücksichtigen. Dies gilt auch für die Skalierbarkeit der Dienste und Systeme.
- Schnittstellen und XML-Schemata werden ungeeignet ausgestaltet: Das korrekte Zusammenwirken verschiedener Web-Services setzt voraus, dass die Schnittstellen und Nachrichtenformate sorgfältig geplant werden, insbesondere über Anbietergrenzen hinweg.
- Persistente Daten werden ungeeignet gespeichert: Durch das Konzept der Zustandslosigkeit müssen auch für Zwischenergebnisse geeignete Lösungen zur Speicherung vorgesehen werden. Die Datenhaltung muss insgesamt den Anforderungen an Leistungsfähigkeit, Zuverlässigkeit und Parallelverarbeitung gerecht werden. Sofern die Web-Services durch verschiedene Dienstnehmer unabhängig voneinander genutzt werden, müssen auch die Datenbestände entsprechend getrennt werden.
- Sicherheitsfunktionen werden vernachlässigt: Die Entwicklung von Web-Services ist in der Regel fachlich getrieben. Werden in der Entwurfsphase erforderliche Sicherheitsfunktionen wie Authentisierung, Verschlüsselung oder Berechtigungsprüfungen nicht hinreichend berücksichtigt, kann dies dazu führen, dass die realisierten Web-Services dem Schutzbedarf

der verarbeiteten Informationen nicht gerecht werden. Die nachträgliche Realisierung von Sicherheit ist oft umständlich und aufwändig.
- Soweit personenbezogene Daten verarbeitet werden, stellt auch die externe Bereitstellung von Web-Services eine Auftragsdatenverarbeitung im Sinne der Datenschutzgesetze dar. Dies erfordert, dass die daraus resultierenden gesetzlichen Anforderungen berücksichtigt und die für den Datenschutz verantwortlichen Stellen in der Organisation einbezogen werden.
- Je nach Einsatzbereich sind neben dem Datenschutz weitere gesetzliche oder sonstige regulatorische Anforderungen zu beachten. Sind diese Vorgaben oder ihre Inhalte nicht ausreichend bekannt, oder werden sie bei der Konzeption der Web-Services nicht berücksichtigt, so kann später die Einsetzbarkeit oder Nutzbarkeit der Web-Services gefährdet sein.
- Testmöglichkeiten werden nicht vorgesehen: Um die Weiterentwicklung der Web-Services, aber auch das Update eingesetzter Komponenten sowie das Einspielen von Patches in einem geeigneten Prozess abbilden zu können, muss eine Testmöglichkeit vorhanden sein, die auch im laufenden Betrieb die Durchführung von Tests ohne Beeinträchtigung der Produktionsumgebung ermöglicht.

Je nach Art und Umfeld der Web-Services können weitere Aspekte für die Planung relevant sein, eine abschließende Aufzählung ist hier wegen der Verschiedenartigkeit der denkbaren Szenarien nicht möglich.

Neben der fehlenden Berücksichtigung der genannten Planungsaspekte besteht auch die Gefahr, dass entsprechende Überlegungen zwar getätigt, aber nicht nachvollziehbar dokumentiert werden. Wechseln später die Verantwortlichkeiten oder wird der Betrieb erweitert, so können dann wesentliche Informationen oder Entscheidungsgrundlagen fehlen.

# G 2.182 Fehlendes oder unzureichendes Betreiberkonzept für Speicherlösungen

Die Planung, Beschaffung und der Betrieb von Speicherlösungen hinsichtlich deren Dimensionierung sowie der Anforderungen an Verfügbarkeit und Performance gestalten sich für Institutionen zunehmend komplex und sind sehr anspruchsvoll. Dies bedingt, dass auf strategischer Ebene die Betriebsart einer Speicherlösung geplant und festgelegt werden muss.

Dabei sind sowohl unterschiedliche Ausprägungen einer Betriebsart (z. B. Betrieb durch eigenes Personal oder Betrieb durch Dritte mit bzw. ohne Übergabe der Betriebsverantwortung) als auch die Möglichkeit zur Unterbringung der Speicherlösung in den eigenen Räumen bzw. bei einem Dienstleister zu unterscheiden.

Liegen keine Regelungen zur festgelegten Betriebsart, etwa in Form eines Betreiberkonzeptes vor, kann dies weitreichende Störungen im Betrieb zur Folge haben, die sich mittelbar auf die Vertraulichkeit, Verfügbarkeit und Integrität der gespeicherten Daten auswirken können. Unklare Zuständigkeiten im Falle einer Systemstörung sind nur ein Beispiel für mögliche Probleme.

Der Betrieb einer Speicherlösung basiert in der Regel auf der Erstellung eines Servicekatalogs, mit dessen Hilfe angebotene Services bzw. feste Vereinbarungen zu Serviceleistungen, sogenannte Service Level Agreements (SLAs) bzw. Operational Level Agreements (OLAs) bei internen Kunden, beschrieben werden.

Ein fehlender Servicekatalog bringt sowohl für den Anbieter einer Speicherlösung als auch für den Anwender erhebliche Nachteile mit sich, da getroffene Vereinbarungen nicht nachvollzogen werden können und Unsicherheit bezüglich der Rechte und Pflichten entsteht. Ist nicht festgelegt, welchen Kriterien ein Service üblicherweise genügen muss, kann die Servicequalität nicht gemessen und die Serviceerbringung nicht sichergestellt werden.

# G 2.183 Fehlendes oder unzureichendes Zonenkonzept

Ein Zonenkonzept dient dazu, ein oder mehrere Sicherheitsniveaus einzelner Systeme innerhalb einer Institution herzustellen und aufrechtzuerhalten. Ziel eines Zonenkonzeptes ist dabei nicht die Trennung unterschiedlicher Mandanten, sondern die Trennung von Zonen, denen ein unterschiedlicher Schutzbedarf zugesprochen wurde. Mit der Einführung eines Zonenkonzeptes können bestehende Systeme, basierend auf ihrem Schutzbedarf, standardisiert einem Sicherheitsniveau zugeordnet werden.

Ein Zonenkonzept kann unterschiedliche Ausprägungen annehmen. Häufig ist dabei eine Unterteilung in Netzzonen und Storagezonen anzutreffen, die in der Praxis jedoch unterschiedlich restriktiv umgesetzt ist.

Es gilt zu beachten, dass der Begriff Zoning innerhalb eines SAN-Speichernetzes die möglichen Verbindungen zwischen einem Speichersystem und den Servern beschreibt und mit einem Zonenkonzept nur namentlich verwandt ist.

Ein fehlendes oder unzureichendes Zonenkonzept kann zur Folge haben, dass unterschiedliche Anforderungen an das Sicherheitsniveau von Systemen hinsichtlich Verfügbarkeit, Vertraulichkeit oder Integrität nicht oder nur teilweise erfüllt werden können.

Des Weiteren können Mängel in der Umsetzung des Zonenkonzeptes dazu führen, dass der einzig vorgesehene und erlaubte Zugriffsweg auf Systeme mit unterschiedlichem Sicherheitsniveau umgangen werden kann. Ein Beispiel hierfür ist die Verletzung von Regelungen zur Kommunikationsmatrix, die Aufschluss darüber geben, welche Systeme ohne zusätzliche Authentisierungs- oder Autorisierungsmaßnahmen auf Systeme außerhalb ihrer eigenen Zone zugreifen dürfen.

Die Umsetzung eines bestehenden Zonenkonzeptes basiert auf der geeigneten Dokumentation der festgelegten Regeln hinsichtlich der erlaubten Zugriffswege. Fehlende oder unzureichende Dokumentation kann dazu führen, dass Verstöße gegen die bestehende Kommunikationsmatrix und damit die Vermischung von Systemen mit unterschiedlichem Schutzbedarf nicht oder nur verspätet erkannt und beseitigt werden können.

# G 2.184 Fehlendes oder unzureichendes Rechte- und Rollenkonzept in Cloud-Infrastrukturen

Im Cloud-Umfeld ist die gemeinschaftliche Nutzung von IT-Systemen durch mehrere Institutionen weit verbreitet. Wird in einem solchen Umfeld gänzlich auf die Durchsetzung eines Rollen- und Rechtekonzeptes verzichtet oder ist dieses unzureichend umgesetzt, stellt dies eine Gefährdung für die Institution dar. Der unberechtigte Zugriff auf Anwendungsdaten oder auf die Komponenten einer Speicherlösung können die Folge sein.

Die Gefahr solcher unberechtigten Zugriffe besteht dabei immer innerhalb eines Mandanten oder auch über mehrere Mandanten hinweg (mandantenübergreifend). Es ist daher notwendig, ein ausreichendes Rechte- und Rollenkonzept einzusetzen.

Folgende Ausprägungen für unberechtigte Zugriffe in Cloud-Infrastrukturen sind zu unterscheiden:

- Ein Benutzer kann auf die Infrastruktur des Providers zugreifen und innerhalb dieser gegebenenfalls Manipulationen durchführen oder Daten löschen.
- Ein Benutzer kann auf die Daten eines anderen Anwenders zugreifen und diese manipulieren oder löschen.

Je nach Ausprägung des Zugriffs können alle drei Sicherheitsziele (Vertraulichkeit, Verfügbarkeit und Integrität der Informationen) gefährdet sein.

**Beispiel:**

- Eine Institution nutzt Cloud-Services, um ihre verfügbare Speicherkapazität flexibel zu erweitern. Um die Dienste zu verwalten bzw. zu steuern, ist aufseiten der Institution die Rolle eines Cloud-Administrators vorgesehen. Diese Rolle und die damit verbundenen Rechte sind unzureichend definiert. In der Folge administriert der Mitarbeiter durch Vererbung aus der Cloud-Administrationskonsole heraus die eingesetzte Speicherlösung (unbeabsichtigt) mit und verändert dabei beispielsweise die Einstellungen zum LUN-Masking bzw. LUN-Mapping. Durch diese fehlerhaften Einstellungen erhält ein Benutzer unberechtigt Zugriff auf Daten.

# G 2.185 Fehlende oder unzureichende Softwarewartung (Maintenance) und fehlendes oder unzureichendes Patchlevel-Management

Softwarewartung ist auch unter dem englischen Begriff *Software Maintenance* bekannt. Hersteller verfolgen mit der Bereitstellung von Softwareaktualisierungen (Patches) das Ziel, Änderungen und Verbesserungen an implementierten Softwarelösungen auch dann noch vorzunehmen, nachdem diese bereits ausgeliefert sind. Auf diesem Weg werden bekannte Fehler behoben, die Leistungsfähigkeit verbessert und dem Einsatz neuer Technik wie z. B. der Nutzung neuer Festplattengenerationen (SSD, Flash etc.) Rechnung getragen.

Werden Systeme nicht oder lediglich unzureichend gewartet, indem beispielsweise verfügbare Sicherheitspatches nicht eingespielt werden oder auf die Aktualisierung der Firmware verzichtet wird, kann dies zur Instabilität der Systeme und damit zum Ausfall der Speicherlösung führen.

In einigen Fällen ist der reibungslose Betrieb einer Speicherlösung von der Einhaltung einer sogenannten Kompatibilitätsmatrix, bereitgestellt durch den Hersteller, abhängig. In der Kompatibilitätsmatrix werden die in einer Speicherlösung einsetzbaren Hard- und Softwarestände in ihrer wechselseitigen Abhängigkeit beschrieben. Weicht der Firmwarestand einzelner Komponenten von dieser Matrix ab, können Ausfälle oder Performance-Einbußen die Folge sein.

Die Durchführung von Wartungsarbeiten sowie das Patchlevel-Management sind eng mit einem etablierten Verfahren zum Änderungsmanagement verbunden. Fehlt dieses, können vorgenommene Änderungen und damit in Zusammenhang stehende Fehler nur schwer nachvollzogen werden. Aktuelle Versionen eingesetzter Soft- oder Firmware sind im Falle eines fehlenden Änderungsmanagements nur mit erhöhten Aufwänden zu ermitteln.

Der langfristige sichere Betrieb einer Speicherlösung kann durch einen fehlenden Wartungsvertrag ebenfalls gefährdet werden, da die Kompatibilität zu aktuellen Komponenten unter Umständen ein vorheriges Upgrade auf die aktuellste Firmware voraussetzt. Ohne Wartungsvertrag ist ein solches Upgrade unter Umständen gar nicht möglich oder mit erheblichen Kosten verbunden.

Weitere Hinweise für bestehende Gefährdungen im Zusammenhang mit der Wartung von Hardware können der G 2.5 *Fehlende oder unzureichende Wartung* entnommen werden.

# G 2.186 Fehlende oder unzureichende Regelungen / keine klare Abgrenzung von Verantwortlichkeiten bei Speicherlösungen

Der Einsatz zentraler Speicherlösungen bringt steigende Anforderungen an die Administration mit sich. Diese begründen sich sowohl durch eine erhöhte Komplexität moderner Speicherlösungen als auch dadurch, dass zunehmend IP-Netze und Fibre-Channel-Netze innerhalb einer Speicherlösung miteinander verschmelzen.

Hinzu kommt, dass vermehrt Storage-Virtualisierung sowie Storage-Automation eingesetzt werden. Ferner verändert sich die Architektur von Speicherlösungen, was sich auch auf die Administration und damit auf die Anforderungen an die Administratoren auswirkt.

Existieren in diesem Zusammenhang keine oder nur unzureichende Regelungen hinsichtlich der Abgrenzung von Verantwortlichkeiten, besteht die Gefahr von Fehlkonfigurationen durch unzureichende Kenntnisse. Folgende Ausprägungen sind hier häufig zu beobachten:

- Administriert ein Netzadministrator FCoE-Switche, so erhält er möglicherweise Zugriff auf Komponenten, für deren Administration er nicht ausgebildet ist. Ein solcher Vorgang kann Fehlfunktionen oder Fehlkonfigurationen generieren, die bis hin zum Ausfall des Gesamtsystems führen können.
- Oftmals herrscht ein Silodenken zwischen Netzadministratoren und Administratoren der Speicherlösungen. Jeder Bereich beansprucht dabei erweiterte Zugriffsrechte zunächst einmal für sich, ohne dem Kenntnisstand der jeweils anderen Mitarbeiter Beachtung zu schenken. Durch die zunehmende Verschmelzung der IP- und FC-SAN-Welten zu einem vereinten Netz (*unified network*) birgt dieses Silodenken jedoch Gefahren, da technische Abhängigkeiten eine engere Zusammenarbeit und Abstimmung der Administratoren untereinander bedingen.

# G 2.187 Fehlendes oder unzureichendes mandantenfähiges Administrationskonzept für Speicherlösungen

Bei der gemeinsamen Nutzung von IT-Systemen durch unterschiedliche Institutionen, wie sie im Cloud Umfeld weit verbreitet ist, existiert, bedingt durch ein fehlendes oder unzureichendes Rollenkonzept, die Gefahr eines mandantenübergreifenden administrativen Zugriffs. Da Administratoren in der Regel über sehr weitreichende Berechtigungen verfügen, stellt dies eine erhebliche Bedrohung aller Sicherheitsziele einer Institution dar.

Insbesondere im Zusammenhang mit dem Servicemodell Infrastructure as a Service (IaaS), das häufig in Verbindung mit Cloud Storage zur Anwendung kommt, besteht daher die Notwendigkeit zum Einsatz eines mandantenfähigen Administrationskonzeptes.

Aus Sicherheitssicht sind folgende mögliche Ausprägungen eines mandantenfähigen Administrationskonzeptes zu unterscheiden:

- Der Betreiber einer Speicherlösung trennt seine Administratoren entsprechend seiner Mandanten. Existiert für dieses Vorgehen kein Konzept oder ist dieses unzureichend umgesetzt, besteht die Gefahr, dass der Administrator für Mandant A auf die Daten von Mandant B zugreift.
- Die Mandanten erhalten selbst administrative Rechte für ihren jeweiligen Bereich. Bei nicht vorhandenem oder unzureichend umgesetztem Konzept besteht die Gefahr, dass Mitarbeiter von Mandant A direkt auf die Daten von Mandant B zugreifen können.

Kommen bei einer Institution Speichersysteme zum Einsatz, die mehreren Mandanten unabhängig voneinander Speicher zur Verfügung stellen (z. B. virtuelle Fileserver in einer NAS-Umgebung) so kann durch ein fehlendes Rollenkonzept die Gefahr eines mandatenübergreifenden administrativen Zugriffs gegeben sein.

# G 2.188 Unzureichende Vorgaben zum Lizenzmanagement bei Cloud-Nutzung

Im Zusammenhang mit dem Lizenzmanagement besteht für eine Institution, auch bei der Nutzung von Cloud Services, die Notwendigkeit zur Definition von klaren Verantwortlichkeiten. Gerade die Thematik der Lizenzen wird jedoch bei Cloud-Nutzung häufig nicht ausreichend betrachtet.

Ohne eindeutige Regelung, für welche Lizenzen die nutzende Institution und für welche der Cloud-Diensteanbieter verantwortlich zeichnet, drohen rechtliche Konsequenzen. Bei Lizenzprüfungen kann unter Umständen kein valider Nachweis über die rechtmäßige Nutzung der eingesetzten Lizenzen erbracht werden. Um finanzielle Nachforderungen oder anderweitige Konsequenzen zu vermeiden, sollte die Institution darüber auskunftsfähig sein, welche Lizenzen sie in den Cloud Service eingebracht hat und welche Lizenzen vom Cloud-Diensteanbieter bezogen werden beziehungsweise in seinem Verantwortungsbereich liegen.

**Beispiele:**

- Eine Institution benötigt insgesamt 500 Windows-Server. 300 dieser Server werden mit Lizenzen betrieben, die direkt durch die Institution erworben wurden. Die restlichen 200 Lizenzen für den Betrieb der Server werden vom Cloud-Diensteanbieter bezogen.
- Für die Verwendung einer Office-Web-Applikation lässt sich die benötigte Anzahl der Lizenzen für interne Anwender einfach ermitteln. Die Zahl der extern benötigten Lizenzen ist jedoch für die Institution unklar. In der Folge dürfen Mitarbeiter die Office-Web-Applikation nur für interne Zwecke einsetzen.

# G 2.189 Fehlende oder unzureichende Strategie für die Cloud-Nutzung

Die Entscheidung für den Einsatz von Cloud Services in einer Institution ist eine strategische Entscheidung. Durch diese begibt sich eine Institution in ein enges Abhängigkeitsverhältnis zum Cloud-Diensteanbieter.

Fehlentscheidungen hinsichtlich der Strategie zur Cloud-Nutzung können organisatorische, technische oder auch gravierende finanzielle Auswirkungen nach sich ziehen, die unter Umständen auch langfristig und schwerwiegend ausfallen können.

Bedingt durch eine unzureichende oder fehlerhafte Strategie für die Cloud-Nutzung sind in der Praxis folgende Auswirkungen zu beobachten:

- Weitverbreitet sind Fehleinschätzungen bei der Einführung und beim Management der Cloud-Nutzung. Der Aufwand für die sichere Einführung eines Cloud Services (zum Beispiel Erstellung von Dokumentationen, Tests, Absicherung von Systemen) wird häufig unterschätzt. Die daraus resultierenden zeitlichen Verzögerungen verleiten Institutionen oft zu einer Reduktion geplanter Testaufwände, was zu Abstrichen bei der Sicherheit führen kann.
- Es entsteht eine Abhängigkeit vom Cloud-Diensteanbieter, die in der Folge die Institution der Gefahr unangemessener Preiserhöhungen oder sinkender Dienstleistungsqualität aussetzt.
- Durch den Einsatz von Cloud Services besteht die Gefahr, dass der IT-Einsatz nicht mehr ordnungsgemäß gesteuert werden kann (Verlust der Governance). Mögliche Ursachen hierfür liegen in unklaren Service-, Prozess- oder Schnittstellendefinitionen.
- Wird in der Planung weder ein späterer Wechsel zu einem anderen Cloud-Diensteanbieter noch die Rückholung vom Cloud-Diensteanbieter in die eigene IT berücksichtigt, kann dies zu hohen Kosten führen.
- Eine unzureichende Planung der Datenlöschung bei der Beendigung der Nutzung eines Cloud Services birgt das Risiko, dass unberechtigt auf die Daten zugegriffen werden kann.

# G 2.190 Unzureichendes Administrationsmodell für die Cloud-Nutzung

Die Entscheidung Cloud Services in einer Institution zu nutzen, bedingt eine Anpassung des bestehenden Administrationsmodells. In der Praxis ist häufig zu beobachten, dass innerhalb einer nutzenden Institution keine Vorgaben zur Service-Administration eines Cloud-Dienstes existieren. So fehlen auch Rollendefinitionen für diese administrativen Tätigkeiten. Verzögerungen bei der Service-Erbringung oder Ausfälle eines Services können die Folge sein.

Werden Cloud Services genutzt führt dies in der Regel dazu, dass sich das Rollenverständnis innerhalb der Administration verändert. Die unterschiedlichen Aspekte beim Einsatz von Cloud Services bedingen dabei die Entwicklung weg vom klassischen System-Administrator hin zum Service-Administrator. Wird diesem Prozess nicht ausreichend Rechnung getragen, kann dies negative Auswirkungen haben. Beispielsweise bringen die Administratoren unter Umständen nicht das nötige Verständnis für die notwendigen Umstellungen mit oder sind für ihre neue Aufgabe nicht oder nur unzureichend geschult.

Ein unzureichend angepasstes Administrationsmodell für die veränderte Form der Service-Erbringung kann in der Folge zum Verlust der Service-Verfügbarkeit führen. Gegenüber den internen Benutzern einer Institution bleibt die IT auch bei Cloud-Nutzung weiterhin der Dienstleister. Um einen vereinbarten Service für ihre internen Benutzer erbringen zu können, müssen die IT-Mitarbeiter beim Einsatz von Cloud Services allerdings selbst einen oder mehrere Services eines Cloud-Diensteanbieters in Anspruch nehmen. Diese neu gestaltete Service-Erbringung bedingt zwangsläufig ein verändertes Administrationsmodell.

Die Änderungen im Administrationsmodell müssen auch in der Ressourcenplanung berücksichtigt werden, da sonst die Verfügbarkeit von Services aufgrund nicht reibungslos funktionierender Administrationsprozesse beeinträchtigt werden kann.

# G 2.191 Unzureichendes Rollen- und Berechtigungskonzept

Die sorgfältige Definition eines Berechtigungskonzeptes verhindert den unrechtmäßigen Zugriff auf Informationssysteme und schützt damit auch die Integrität, Verfügbarkeit und Authentizität der zugehörigen Daten. Berechtigungskonzepte besitzen dabei Relevanz sowohl für Anwender als auch für Administratoren von IT-Systemen.

In der Regel sind Berechtigungskonzepte an die Definition von Rollen gekoppelt, denen in der Folge gewisse Berechtigungen zugesprochen oder entzogen werden können. Sind die relevanten Rollen unzureichend definiert, kann dies die Wirksamkeit des Berechtigungskonzeptes verringern. Mitarbeiter erhalten unter Umständen Zugriff auf Systeme und Daten, zu denen sie keine Berechtigung haben dürften, wodurch die Vertraulichkeit und Integrität der Daten verletzt wird.

Bestehende Rollen- und Berechtigungskonzepte müssen regelmäßig überprüft werden, da die Mitarbeiter- und Organisationsstruktur einer Institution einem stetigen Wandel unterliegt. Der Entzug beziehungsweise die Erteilung von Berechtigungen für Mitarbeiter beim Wechsel des Arbeitsbereiches und damit Übernahme einer neuen Rolle oder bei Beendigung des Arbeitsverhältnisses muss sichergestellt sein. Sind diese Voraussetzungen nicht erfüllt, können Mitarbeiter unberechtigt auf (vertrauliche) Informationen zugreifen und diese unter Umständen verändern, vernichten oder zu ihrem Vorteil missbrauchen. Finanzielle Einbußen und Schädigung des Images einer Institution sind mögliche Folgen.

Detaillierte Rollenkonzepte bringen eine hohe Komplexität und eine damit einhergehende erhöhte Fehleranfälligkeit mit sich. Unter Umständen sieht sich eine Institution hier einem Konflikt zwischen der Qualität eines Rollenkonzeptes und der Möglichkeit, dieses angemessen zu verwalten, gegenüber.

Die fehlende Überprüfung des Rollenkonzeptes beim Cloud-Diensteanbieter im Verhältnis zum Rollenkonzept in der eigenen Institution erzeugt einen Bruch in der rollenbasierten Ende-zu-Ende-Administration und kann zu einem Verlust der Service-Verfügbarkeit und Datenintegrität führen.

# G 2.192 Unzureichende Verfügbarkeit der erforderlichen personellen Ressourcen mit ausreichender Qualifikation

Die reibungslose Nutzung von Cloud-Diensten erfordert eine ausreichende Verfügbarkeit von qualifizierten IT-Administratoren. Fehlen ausreichend geschulte und erfahrene Administratoren, kann dies für die Institution unter anderem Beeinträchtigungen bei der Service-Verfügbarkeit nach sich ziehen.

Bei mangelnder Planung lässt sich die unzureichende Verfügbarkeit der personellen Ressourcen in der Praxis häufig nicht kurzfristig beheben, da qualifiziertes beziehungsweise in der Administration von Cloud Services erfahrenes Personal häufig nur schwer oder gar nicht verfügbar ist.

Administratoren, die bereits in der Institution beschäftigt sind, wissen unter Umständen nicht, welche Aufgaben ihnen im Zusammenhang mit der Einführung von Cloud Services übertragen werden. In der Regel setzt der Umstieg auf Cloud-Nutzung eine Entwicklung vom System-Administrator hin zum Service-Administrator voraus. Eine solche Umstellung bringt zusätzlichen Schulungsbedarf mit sich, da ungeschulte Mitarbeiter im Administrationsumfeld ein erhebliches Gefahrenpotenzial darstellen (siehe hierzu auch G 2.103 *Unzureichende Schulung der Mitarbeiter*).

# G 2.193 Fehlende Anpassung der Institution an die Nutzung von Cloud Services

Die Nutzung von Cloud Services bedingt eine Anpassung der Institution in unterschiedlichen Bereichen. Unterbleibt diese Anpassung an die neuen Gegebenheiten oder wird diese nur unzureichend umgesetzt, wirkt sich dies negativ auf die Institution aus.

In folgenden Bereichen sind bei der Anpassung der Institution an die Nutzung von Cloud Services häufig Fehler zu beobachten:

**Anpassung der Service-Management-Prozesse**

Werden die Service-Management-Prozesse nicht oder nur unzureichend angepasst, kann dies dazu führen, dass die Dynamik und die Schnelligkeit, die mit der Nutzung von Cloud Services einhergehen, nicht zu den bestehenden Prozessen passen. Dies führt oftmals zu einer Abweichung zwischen der Erwartungshaltung des Anwenders und den bestehenden Prozessen.

**Berücksichtigung der Mitarbeiter**

Häufig geht mit der Nutzung von Cloud Services eine Reduktion des IT-Personals aufseiten der nutzenden Institution einher, die sich durch den sinkenden Bedarf an Fachpersonal begründet. Dies kann zu einem Verlust des Knowhows führen, das mit diesen Mitarbeitern verbunden ist.

Die verbleibenden IT-Mitarbeiter müssen häufig neue Aufgaben wahrnehmen, nachdem sich eine Institution zur Nutzung eines Cloud Services entschieden hat. In der Praxis ist dabei häufig eine fehlende Bereitschaft der Mitarbeiter zur Weiterentwicklung beziehungsweise zur Akzeptanz des neuen Aufgabenbereiches zu erkennen. Die Mitarbeiter sind in der Folge gegebenenfalls weniger motiviert, arbeiten weniger engagiert und sorgfältig, fühlen sich nicht wertgeschätzt beziehungsweise über- oder unterfordert.

Die Cloud-Administration bedeutet in der Regel zusätzlichen Arbeitsaufwand für die IT, da kurzfristig die klassischen IT-Systeme zumeist nicht abgeschafft werden, während die Cloud-Dienste bereits genutzt werden.

Dies alles kann auch zu einer erkennbaren Störung des Betriebsklimas führen mit negativen Folgen wie einer erhöhten Zahl von Krankheitsfällen oder dem Abwerben von Personal. Weitere Hinweise hierzu finden sich in G 2.88 *Störung des Betriebsklimas durch ein Outsourcing-Vorhaben*.

**Kultureller Wandel**

Die Nutzung von Cloud Services bringt in der Regel einen sogenannten kulturellen Wandel innerhalb der Institution mit sich. Dies betrifft nicht nur, wie bereits beschrieben, die Entwicklung des System-Administrators hin zum Service-Administrator, bei den Benutzern ist auch eine veränderte Erwartungshaltung zu beobachten.

Verwenden Benutzer für dienstliche Zwecke Werkzeuge, die jenen aus dem privaten Nutzungsumfeld sehr ähnlich sind, wird der Trend zur Vermischung von dienstlichen und privaten Aspekten verstärkt. Durch die sogenannte "Überall- und Immer-Verfügbarkeit" von Cloud-Diensten verändern sich dabei zunehmend auch die Erwartungen an die Gestaltung der Arbeit. Mitarbeiter

sehen in der Folge beispielsweise keine Notwendigkeit zur ortsgebundenen Arbeit mehr, da sie viele Tätigkeiten auch von einem anderen Ort als ihrer Arbeitsstätte aus erledigen können. Häufig ist zudem erkennbar, dass klassische IT-Services abgelehnt werden, da diese beispielsweise als zu langsam oder wenig intuitiv wahrgenommen werden.

Cloud Computing birgt das Potenzial, erheblichen Einfluss auf die Arbeitswelt vieler Institutionen zu nehmen. Als eine der weitreichenden Folgen können sich Mitarbeiter, die bislang ausschließlich klassische IT-Services genutzt haben und die Veränderungen ablehnend gegenüberstehen, durch den Wechsel zu Cloud Services übergangen und überfordert fühlen.

Sind den Verantwortlichen innerhalb der Institution die notwendigen Weiterentwicklungen beziehungsweise Anpassungen der Unternehmenskultur nicht bewusst, kann es zu Störungen der Service-Erbringung durch die IT kommen.

**Kommunikation der Veränderungen**

Die Veränderungen müssen sowohl den Benutzern als auch den Administratoren klar und zielgruppengerecht kommuniziert werden. Darüber hinaus sollten auch der Betriebs- beziehungsweise Personalrat sowie der Datenschutzbeauftragte frühzeitig in die Veränderungen eingebunden sein, um mögliche Konflikte schon im Vorfeld auszuräumen.

**Beispiel:**

- Das Gremium zur Bewertung und Genehmigung von Änderungsanträgen (Change Advisory Board, CAB) tritt im Wochenrhythmus zusammen. Geplante Änderungen müssen dabei mit einer Vorlaufzeit von drei Werktagen beantragt werden. Cloud Services, zum Beispiel ein neuer Server, können aber oft schon in wenigen Minuten bereitgestellt werden, und so kann der Änderungsmanagementprozess unterlaufen werden.

# G 2.194 Mangelhaftes Anforderungsmanagement bei Cloud-Nutzung

An die Entscheidung einer Institution zur Nutzung von Cloud Services sind in der Regel eine Vielzahl von Erwartungen geknüpft. Anwender erwarten beispielsweise eine höhere Leistungsfähigkeit, einen größeren Funktionsumfang und/oder geringere Kosten.

Mangelndes Anforderungsmanagement bei der Nutzung von Cloud-Diensten kann die Erreichung der gesteckten Ziele gefährden und der Service kann nicht den gewünschten und benötigten Mehrwert liefern.

In der Regel ist das Anforderungsmanagement nicht durch die IT getrieben, sondern durch das Management. Die IT muss in der Folge die gestellten Anforderungen aufnehmen und in jene Service-Leistungen übersetzen, die erforderlich sind, um die Anforderungen zu erfüllen.

Mangelhaftes Anforderungsmanagement kann beispielsweise die folgenden Ausprägungen annehmen:

- Die Anforderungen an den Cloud Service sind unklar definiert. Die Gründe hierfür können darin liegen, dass keine Anforderungsanalyse durchgeführt, aber auch darin dass darauf verzichtet wurde ein Lastenheft zu erstellen. Damit fehlt die Service-Beschreibung für Cloud Services, die in der Institution als IT-Service bereitgestellt werden.
- Die Anforderungen an Cloud Services werden schwächer formuliert beziehungsweise definiert, als dies in vergleichbaren Situationen bei klassischer IT der Fall ist. Dies kann zur Folge haben, dass wichtige Funktionen eines Services nach einem Wechsel hin zur Cloud-Nutzung nicht mehr zur Verfügung stehen, die Zugriffszeiten auf Anwendungen steigen oder die Ausführung von Aufträgen im Vergleich zur Nutzung klassischer IT-Lösungen verzögert erfolgt.
- Die Anforderungen an die IT-Infrastruktur, die durch die Nutzung von Cloud Services entstehen, werden nicht ausreichend betrachtet.
- Es existieren keine Vorgaben hinsichtlich der benötigten Leistungsfähigkeit der Netz- und Internetanbindung.
- Der möglicherweise notwendige Ausbau von Datennetzen oder weiteren Infrastrukturbereichen (zum Beispiel Firewalls, Intrusion-Prevention-Systeme oder Loadbalancer) ist nicht vorgesehen.

# G 2.195 Mangelnde Überwachung der Service-Erbringung

Zwischen einer Institution als Cloud-Anwender und einem Cloud-Diensteanbieter existieren vertragliche Regelungen hinsichtlich der Ausgestaltung der angebotenen Services. Die Beschreibung der Dienste und ihrer Dienstgüten findet sich in Dienstgütevereinbarungen (SLAs - Service Level Agreements bei externen Dienstleistern oder OLAs - Operational Level Agreements bei interner Service-Erbringung). Bei Public Cloud Services sind diese häufig in Form von AGBs oder Nutzungsbedingungen gestaltet.

Weicht die tatsächlich erbrachte Service-Leistung von den vereinbarten Parametern ab, kann dies negative Auswirkungen auf die nutzende Institution haben. Die Überwachung der Service-Erbringung des Cloud-Diensteanbieters durch die nutzende Institution ist daher essenziell, um mögliche Servicemängel erkennen zu können und diesen entgegenzuwirken.

Häufig wird die Überwachung der Service-Erbringung jedoch vernachlässigt. Vertragsverletzungen oder Abweichungen vom vereinbarten Sicherheitsniveau werden dadurch nicht oder erst spät identifiziert. Dies gilt auch bei Nutzung einer Private Cloud, die durch die eigene IT betrieben wird. Hier ist einerseits auf die Überwachung der Service-Erbringung zu achten. Andererseits sollten auch hier die Service-Vereinbarungen die Services ausreichend detailliert und verständlich beschreiben. Bei der Überwachung ist hier insbesondere darauf zu achten, dass die Verantwortlichkeiten festgeschrieben sind und es nicht zu einer "Selbstprüfung" kommt, die keine sinnvollen Ergebnisse liefert.

In der Praxis sind folgende Ausprägungen mangelnder Überwachung der Service-Erbringung zu beobachten:

- Der Cloud-Diensteanbieter stellt der nutzenden Institution in regelmäßigen Abständen Reports zur Verfügung. Aufseiten der Institution werden diese jedoch nicht oder lediglich zeitlich verzögert ausgewertet. Sind solche Reports vertraglich vereinbart, werden vom Anwender aber nicht eingefordert, fällt dies ebenfalls unter mangelnde Überwachung der Service-Erbringung.
- Die Einhaltung der Sicherheitsmaßnahmen aufseiten des Cloud-Diensteanbieters wird durch den Anwender nicht in ausreichendem Maß überwacht. Beispielsweise werden keine unabhängigen Sicherheitsrevisionen oder Penetrationstests durchgeführt oder externe Dienstleister damit beauftragt. Dies kann zu einem erhöhten Aufkommen von Sicherheitsvorfällen und einem sinkenden oder zu niedrigen Sicherheitsniveau aufseiten des Cloud-Diensteanbieters führen. Für den Anwender ist damit die Einhaltung des erforderlichen Sicherheitsniveaus nicht mehr gewährleistet.
- Im SLA mit dem Cloud-Diensteanbieter ist vereinbart, dass er nachweisen muss, dass die Services in der erforderlichen Güte geliefert wurden, aber die nutzende Institution fordert sie nicht ein. Der Cloud-Anwender erlangt damit keine Kenntnis über die Nichterbringung der SLAs und läuft daraufhin seinerseits Gefahr, eigene Services nicht oder lediglich ungenügend erbringen zu können.
- Die Inanspruchnahme von Subunternehmern durch den Cloud-Diensteanbieter stellt möglicherweise ebenfalls eine Gefährdung dar, wenn nicht geregelt ist, in welcher Form dessen Service-Erbringung überwacht wird.

# G 2.196 Fehlende Kosten-Nutzen-Betrachtung der Cloud-Nutzung über den gesamten Lebenszyklus

In der Praxis lässt sich, aufgrund der großen Popularität und Vielfalt von Cloud Services, beobachten, dass nutzende Institutionen die zu erwartenden Kosten kleinrechnen, häufig verbunden mit dem Großrechnen des erhofften Nutzens.

Der Verzicht auf eine realistische Kosten-Nutzen-Betrachtung der Cloud-Nutzung über den gesamten Lebenszyklus zieht häufig finanzielle Einbußen für die nutzende Institution nach sich. Bei der Kosten-Betrachtung ist zwischen Investitionskosten (Capex - capital expenditure) und Kosten für den operativen Geschäftsbetrieb (Opex - operational expenditure) zu unterscheiden. Cloud-Angebote werben oft damit, dass die Investitionskosten durch operative Kosten abgelöst werden, die weniger langfristig und besser mit dem tatsächlichen Bedarf skalieren.

Beim Umstieg auf Cloud Services entstehen zunächst zusätzliche Kosten, da vorhandene Dienste und die dafür benötigte Infrastruktur nicht sofort abgelöst werden können.

In vielen Institutionen ist zu beobachten, dass bei einer Kosten-Nutzen-Betrachtung jedoch lediglich die Kosten für den operativen Geschäftsbetrieb herangezogen werden, da Cloud Services in der Regel nach Verbrauch abgerechnet und somit klassisch als Opex angesehen werden.

Bei der Entscheidung für die Nutzung von Cloud Services wird eine Reihe von Kosten häufig nicht oder unzureichend in eine Kosten-Nutzen-Betrachtung einbezogen, wie zum Beispiel:

- Kosten für die notwendige Anpassung der Prozesse beziehungsweise der vorhandenen Infrastruktur an die Cloud-Nutzung
- Kosten für Fallback-Szenarien im Falle etwaiger Probleme
- Kosten, die im Zusammenhang mit einem möglichen Vendor-Lock-In, also der Abhängigkeit von einem spezifischen Cloud-Diensteanbieter, stehen
- Kosten für die Durchführung von Schulungen, sowohl für Administratoren als auch für Benutzer
- Kosten für die Durchführung von Audits beim Cloud-Diensteanbieter
- Kosten, die durch eine notwendige Anpassung anderer Services in Folge der Cloud-Nutzung entstehen, wie zum Beispiel Backup oder Rechnungslegung in der Buchhaltung

Als Folge einer fehlenden oder unzureichenden Kosten-Nutzen-Betrachtung über den kompletten Lebenszyklus erweisen sich Services, die durch Cloud-Nutzung erbracht werden, unter Umständen als unrentabel. Zudem ist der Nutzen den Kosten gegenüberzustellen. Es kann vorkommen, dass Cloud-Dienste im Produktivbetrieb keinen signifikanten Nutzwert erzielen. Werden solche Cloud-Dienste in die interne IT zurückgeführt, entstehen für die Institution sowohl Kosten für die Auslagerung des Services in die Cloud, als auch für die spätere Wiedereingliederung.

Darüber hinaus existieren weitere Aspekte, die im Zusammenhang mit der Nutzung von Cloud Services als Gefährdung angesehen werden können und

die sowohl finanzielle Risiken als auch Risiken für die Verfügbarkeit des Services nach sich ziehen:

- Die Abschätzung der zu erwartenden Pay-per-Use-Kosten ist falsch beziehungsweise lückenhaft. Grund hierfür ist beispielsweise das Zugrundelegen eines typischen Nutzverhaltens und die Nichtberücksichtigung saisonaler Schwankungen. Dies ist insbesondere dann problematisch, wenn die betroffenen Cloud Services durch externe Benutzer angestoßen werden und die Institution damit nur schwer Einfluss auf den tatsächlichen Verbrauch nehmen kann.
- Bei Risikobewertungen, wie sie beispielsweise hinsichtlich IT -Ausfällen vorgenommen werden, erfolgt keine Anpassung an das Cloud-Nutzungsmodell oder diese Risiken werden schöngerechnet. Zwar werden einige Risiken an den Cloud-Diensteanbieter übertragen, jedoch wird dabei häufig übersehen, dass dadurch neue Risiken für die Institution entstehen können.

# G 2.197 Unzureichende Einbindung von Cloud Services in die eigene IT

Die Entscheidung einer Institution zum Einsatz von Cloud Services bedingt in der Folge, dass diese Services auch angemessen in die eigene IT eingebunden werden. Erfolgt diese notwendige Einbindung nur unzureichend, kann in der Folge nicht sichergestellt werden, dass die beauftragten Cloud-Service-Leistungen durch den Anwender auch in vollem Umfang abgerufen werden können. Beauftragte Cloud Services liefern demnach unter Umständen nicht die erforderliche und vereinbarte Performance oder der Zugriff auf Services ist gar nicht beziehungsweise lediglich verzögert möglich. Beeinträchtigungen der Service-Verfügbarkeit sind die Folge.

Wird ein Cloud Service nur unzureichend in die eigene IT eingebunden, und sind die Mitarbeiter aber grundsätzlich zur Nutzung dieses Services berechtigt, ist häufig zu beobachten, dass diese den Service auch ohne offizielle IT-Unterstützung nutzen. So kann in der Institution eine Schatten-IT und damit ein potenzieller Kontrollverlust über Unternehmensinformationen entstehen.

Eine optimale Einbindung von Cloud Services in die IT einer Institution wird häufig vor allem durch folgende Aspekte beeinträchtigt:

- Die **Performance der Netzanbindung** ist unterdimensioniert. Der Datentransport kann daher nur eingeschränkt erfolgen, was zum verzögerten Kopieren von Daten, verlängerten Zugriffszeiten und erkennbaren Leistungseinbußen führt. Mögliche Gründe hierfür liegen beispielsweise in einer unzureichend gewählten Bandbreite, einer nicht den Anforderungen entsprechenden Priorisierung der Dienste (Quality of Service), konzeptionellen Schwächen des Netzes (siehe hierzu G 2.45 *Konzeptionelle Schwächen des Netzes*) oder in Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Diensteanbieter (siehe hierzu G 4.97 *Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister*).
- Die **Verfügbarkeit der Schnittstellensysteme** ist unzureichend, da notwendige Änderungen in den Verfügbarkeitsanforderungen nicht ausreichend berücksichtigt wurden. Eine mögliche Ausprägung in diesem Zusammenhang zeigt sich in einer unzureichenden Verfügbarkeit in Bezug auf die Anbindung an den Cloud-Diensteanbieter. Der bestehende Internetzugang einer Institution wurde bislang beispielsweise als unkritisch angesehen. Durch die Verlagerung geschäftskritischer Services in die Cloud steigen auch die Anforderungen an den Internetzugang, der in der Folge als sehr kritisch eingestuft wird. Die unzureichende Verfügbarkeit der Schnittstellensysteme ist eine zweite mögliche Ausprägung. Der eingesetzte Proxy innerhalb einer Institution wurde hinsichtlich seiner Verfügbarkeit beispielsweise als unkritisch angesehen. Durch die Verlagerung von Services in die Cloud wird er jedoch zu einem (hoch-)kritischen System.
- Die **Performance der Schnittstellensysteme** ist nicht ausreichend gewählt. Institutionen sollten in diesem Zusammenhang insbesondere jene Systeme beachten, die sich an der Schnittstelle zum Cloud-Diensteanbieter finden. Beispiele hierfür sind Loadbalancer, Proxys, Router, Sicherheitsgateways oder Federation-Systeme.
- Die **Performance interner Systeme** reicht für eine vorgesehene API-Kopplung zum Datenaustausch zwischen Cloud Service und internen Systemen nicht aus. Ein typisches Beispiel hierfür ist der Stammdatenaustausch zwischen dem lokalen ERP-System (Enterprise Resource Plan-

ning) und einem CRM-System (Customer Relationship Management) als Cloud Service.

**Beispiel:**

- Eine Institution entschließt sich zur Nutzung einer Online-Kommunikationsplattform zur Förderung der Zusammenarbeit innerhalb verteilter Teams. Der beauftragte Service wird jedoch nicht vollständig in die IT eingebunden. Einzelne Funktionen, wie beispielsweise die Dateifreigabe für definierte Teammitglieder, funktionieren in der Folge nicht, wie von den Mitarbeitern erwartet. Der Zugriff auf eine freigegebene Datei kann lediglich stark verzögert oder gar nicht erfolgen.

# G 2.198 Mangelnde Planung der Migration zu Cloud Services

In Abhängigkeit des Leistungsumfangs und der Kritikalität der genutzten Cloud Services kann deren Einsatz erhebliche finanzielle und organisatorische Risiken für die Institution mit sich bringen. Insbesondere die Phase der Migration hin zur Nutzung von Cloud Services ist anfällig für Fehler, die sich möglicherweise auf die Informationssicherheit innerhalb der Institution auswirken.

Unter Migration ist in diesem Zusammenhang sowohl der Umstieg von der Nutzung klassischer IT auf die Nutzung von Cloud Services zu verstehen als auch der Wechsel von einem Cloud-Diensteanbieter zu einem anderen. In der Praxis werden häufig die Begriffe Migration und Transition oder auch Transformation synonym verwendet.

Mängel in der Planung der Migration zu Cloud Services beruhen oftmals darauf, dass die diesbezüglichen Besonderheiten gegenüber Migrationen, wie sie beispielsweise bei klassischer IT oder im Zusammenhang mit Outsourcing-Vorhaben anzutreffen sind, nicht oder nur unzureichend berücksichtigt werden.

Eine Migration im Cloud-Umfeld erfordert in der Regel kein hartes Umschalten zwischen klassischer IT und der Nutzung von Cloud Services. In der Praxis ist häufig zu beobachten, dass der alte Service und der neue, über den Cloud-Diensteanbieter bezogene Service über längere Zeit parallel eingesetzt werden. Der Wegfall beziehungsweise die Abschaltung des alten Services und die Nutzung des Cloud Services überschneiden sich an dieser Stelle. Für eine Institution können sich aus einem solchen Parallelbetrieb zusätzliche Herausforderungen und Gefährdungen, zum Beispiel hinsichtlich der Datenkonsistenz, ergeben.

Im Cloud-Umfeld sind Migrationen von einem Diensteanbieter zum anderen in der Regel kurzfristiger und flexibler möglich als beispielsweise im Rahmen von Outsourcing-Vorhaben. Die vertraglichen Vereinbarungen sehen häufig keine langfristigen Bindungen vor. Die technische Umsetzung der Migration von einem Diensteanbieter zu einem anderen kann sich jedoch als problematisch erweisen und ist abhängig vom gewählten Servicemodell. So ist beispielsweise die Migration eines Infrastructure-as-a-Service-Dienstes in der Regel unproblematisch umzusetzen, während bei einem Cloud-Dienst, der als Software as a Service erbracht wird, häufig Schwierigkeiten im Zusammenhang mit dem erforderlichen Datenformat anzutreffen sind.

Verzichtet eine Institution im Rahmen der Planungsphase auf die Betrachtung einer stufenweisen Migration, können in der Praxis zusätzliche Probleme auftreten. Der Verzicht auf das Ausdehnen der Migration über mehrere Stufen, die Auswahl von Pilot-Benutzern oder den Parallelbetrieb von bestehender Infrastruktur und Cloud Services, birgt die Gefahr von Datenverlusten oder kompletten Serviceausfällen, sofern die Migration nicht erwartungsgemäß verläuft.

# G 2.199 Unzureichende Auswahl des Cloud-Diensteanbieters

Hat eine Institution die strategische Entscheidung zur Nutzung von Cloud Services getroffen, begibt sie sich damit immer in ein Abhängigkeitsverhältnis vom gewählten Cloud-Diensteanbieter. Erfolgt die Auswahl des Diensteanbieters nicht mit besonderer Sorgfalt und unter Beachtung der festgelegten Cloud-Nutzungs-Strategie, kann dies über einen langen Zeitraum hinweg negative Auswirkungen für die Institution nach sich ziehen.

Häufig werden bei der Auswahl des Cloud-Diensteanbieters wichtige Faktoren wie beispielsweise dessen Reputation, Anbieter-Rankings, öffentlich zugängliche Pflichtenhefte der Diensteanbieter, Verpflichtungen zur Einhaltung von Gesetzen und Richtlinien oder erworbene Zertifizierungen nicht oder nur unzureichend berücksichtigt. Der Cloud-Markt ist für Auftraggeber wenig transparent, es fehlen standardisierte Angebote der Cloud-Diensteanbieter.

Daraus können Sicherheitsprobleme beim Cloud-Diensteanbieter (zum Beispiel bei mangelhafter Verfügbarkeit) resultieren. Diese sind häufig mit finanziellen Einbußen für die nutzende Institution verbunden, wenn diese auf die Verfügbarkeit des Services angewiesen ist, um ihrerseits einen Service erbringen zu können.

# G 2.200 Unzureichende Planung bei der Anschaffung von Mobiltelefonen, Smartphones, Tablets oder PDAs

Durch Mobiltelefone, Smartphones, Tablets und PDAs treten Probleme für die Informationssicherheit auf, wenn

- relevante Eigenschaften der anzuschaffenden Geräte nicht während der Planungsphase erhoben werden,
- der Funktionsumfang der Geräte nicht dem Einsatzzweck entspricht oder
- sonstige Randbedingungen zum sicheren Betrieb der Geräte nicht berücksichtigt wurden.

Zwar ist der Funktionsumfang von Mobiltelefonen, Smartphones, Tablets und PDAs verschiedener Anbieter sehr ähnlich, an mitunter relevanten Stellen, wie beispielsweise dem Gerätemanagement, gibt es jedoch große Unterschiede. So kann es sein, dass

- ein Smartphone sich nicht auf gewünschte Weise (zum Beispiel mit IPSec) mit dem Netz der Institution verbinden lässt,
- das Gerät keine vollständige Verschlüsselung aller gespeicherten Daten unterstützt,
- auf dem Gerät keine selbst erstellten oder angepassten Applikationen verwendet werden können sollte dies notwendig sein,
- der auf dem Gerät befindliche E-Mail-Client Zugangspasswörter nur im Klartext speichert,
- die eingesetzte Software zum Management für mobile Endgeräte nicht mit der Betriebssystemversion des Smartphones kompatibel ist und deswegen relevante Anforderungen aus dem Sicherheitskonzept (zum Beispiel Erzwingen eines langen Passwortes) nicht umsetzbar sind oder
- ein Mitarbeiter hauptsächlich außerhalb geschlossener Räume arbeitet und daher statt eines handelsüblichen Smartphones ein witterungsbeständiges und stoßfestes Gerät mit längerer Akkukapazität benötigt.

Werden diese und ähnliche Aspekte in der Planungsphase nicht ausreichend berücksichtigt, können Gefährdungen für die Informationssicherheit der Institution entstehen.

# G 2.201 Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern

Institutionen müssen sich regelmäßig an veränderte Anforderungen und Rahmenbedingungen anpassen, um ihre Geschäftsziele zu erreichen und ihre Wettbewerbsfähigkeit zu behaupten. Damit unterliegen auch ihre Prozesse und eingesetzten IT-Systeme einem ständigen organisatorischen und technischen Wandel.

Eine vergleichbare Situation liegt auch für die Mitarbeiter vor: Sie erleben als Teil der Institution diesen Wandel mit und müssen sich an Veränderungen in den Arbeitsaufgaben, in den bekleideten Positionen sowie an Arbeiten mit unterschiedlichen technischen Systemen anpassen. Dies kann für Mitarbeiter eine Chance sein sich weiterzuentwickeln, aber auch demotivierend wirken. Dadurch können Veränderungen dazu führen, dass Sicherheitsvorgaben nicht wie vorgesehen beachtet werden.

Veränderungen für die Mitarbeiter ergeben sich vor allem aus folgenden Ereignissen:

- persönliche Entwicklung der Mitarbeiter innerhalb der Institution (Versetzung, Beförderung, Weggang etc.),
- Änderungen in der oder für die Institution (Umstrukturierungen, Übernahmen etc.),
- Einführung neuer oder geänderter Geschäftsprozesse oder IT-Verfahren.

Damit sich dabei der Umgang der Mitarbeiter mit Informationen und mit der Informationssicherheit verändern kann, müssen diese Ereignisse zielgruppenspezifisch in institutionsweite Sensibilisierungs- und Schulungsmaßnahmen eingebunden werden.

**Beispiele:**

- Ein Praktikant wird nach Abschluss des Studiums in die Institution übernommen und einer Fachabteilung zugewiesen. Seine IT-Berechtigungen sind aber auch jetzt noch sehr weitreichend, da er im Rahmen seines Praktikums in verschiedenen Abteilungen der Institution eingesetzt wurde. So kann er weiterhin auf Informationen aus der Personalabteilung zugreifen, obwohl dies nicht für die Erfüllung seiner neuen Aufgabe erforderlich ist.
- In einer Abrechnungsabteilung wird das Abrechnungssystem durch das Produkt eines neuen Herstellers ersetzt. Die Administratoren werden zwar zum neuen Abrechnungssystem geschult, aber nur zu allgemeinen Grundlagen, nicht zu Sicherheitsaspekten. Dadurch werden wichtige Sicherheitseinstellungen nicht vorgenommen.
- Ein Mitarbeiter wird in den Ruhestand verabschiedet. Die im Laufe seiner Organisationszugehörigkeit unterzeichneten Richtlinien und Vereinbarungen zur Informationssicherheit werden als bekannt und präsent vorausgesetzt. Der Mitarbeiter wird bei seinem Weggang nicht explizit auf weiterhin noch bestehende Verschwiegenheitspflichten hingewiesen. Daher nutzt er die gewonnene Freizeit, um sich in Internetforen und bei persönlichen Treffen mit anderen Personen über das Arbeitsleben auszutauschen und dabei vertrauliche Informationen über die Institution preiszugeben.

# G 2.202 Lock-in-Effekt

Die ursprünglich aus dem Bereich der Wirtschaftswissenschaften stammende Bezeichnung Lock-in-Effekt beschreibt einen Zustand, dessen Veränderung nur durch einen sehr hohen Aufwand erreicht werden kann.

Aus der Sicht einer Institution äußert sich dieser Aufwand in der Regel in Form sogenannter Wechselkosten. Diese Kosten beschreiben u. a. die notwendigen finanziellen Aufwände, die zum Beispiel für den Wechsel eines Betriebssystems aufzubringen sind. Stellen sich diese Kosten als sehr hoch heraus, so wird gegebenenfalls auf einen aus IT-Sicht sinnvollen Wechsel auf eine alternative Betriebssystemumgebung verzichtet.

Im IT-Umfeld traten von je her diese Lock-in-Effekte auf. Einige Beispiele sind im Folgenden dargestellt:

**Drucker**

Herstellerabhängigkeiten, englisch *Vendor Lock*, treten hier bedingt durch die Komplexität im Zusammenspiel von Hardware (Drucker) und weiteren Komponenten (z.B. Patronen für Toner oder Tinte) auf.

Wesentliche Funktionen des Druckers und die dazugehörige Elektronik wurden durch die Hersteller in die dazugehörigen Patronen oder Kartuschen verlagert. Diese sind in der Regel durch Patente oder technische Maßnahmen davor geschützt, durch alternative Anbieter nachgebaut oder wiederbefüllt zu werden. Die Anwender sind dadurch auf den Druckerhersteller als Lieferant für Verbrauchsmaterial beschränkt.

**Dateiformate**

Anwendungsprogramme speichern Daten häufig in proprietären, nicht offengelegten Dateiformaten. Ein späteres Einlesen oder eine Weiterverarbeitung der Daten ist dann nur mit den Programmen des jeweiligen Herstellers möglich. Die Entwicklung alternativer Software wird durch fehlendes Wissen über die Dateiformate erschwert oder durch mit den proprietären Datenformaten verbundene Schutzrechtsansprüche ausgeschlossen.

**Trusted Platform Module (TPM), digitales Rechtemanagement (DRM)**

Mit dem in Computersysteme integrierten Kryptochip TPM können nicht nur Sicherheitsfunktionen umgesetzt oder unterstützt werden. Mit Hilfe eines TPM kann auch verhindert werden, dass unerwünschte Software gestartet oder dass Daten durch andere Anwendungen entschlüsselt werden. Diese Kontrolle darüber liegt dann immer bei derjenigen Komponente (Software oder Betriebssystem), die das TPM erstmalig initialisiert hat. Techniken des digitalen Rechtemanagements (DRM) können ebenfalls einschränken, wie die Systembenutzer auf Daten zugreifen dürfen, indem sie etwa das Abspielen von Mediendaten in einer anderen Anwendung oder geografischen Region unterbinden.

Beim Einsatz dieser Techniken kann eine Migration auf Produkte anderer Hersteller erschwert bis ausgeschlossen werden.

**Cloud-Dienste**

Häufig bieten Apps die Möglichkeit an, Daten direkt in der Cloud zu speichern. Der Zugriff auf diese Daten innerhalb der Cloud ist jedoch meist nur durch Ein-

satz einer speziellen Software oder App des jeweiligen Cloudanbieters möglich. Sollte für relevante Plattformen der Organisation ein Zugriff auf diese Daten notwendig sein, aber eine App oder dedizierte Software für die Plattform nicht verfügbar sein, so müssen Daten auf andere Speicher transferiert werden und ggf. redundant vorgehalten werden.

**BitLocker unter Windows**

Die mit Windows Vista eingeführte Verschlüsselungssoftware BitLocker bietet die Möglichkeit, auch externe Laufwerke zu verschlüsseln. Wird BitLocker als Verschlüsselungssoftware eingesetzt, so besteht die Gefahr, dass relevante andere Betriebssysteme der Institution nicht in der Lage sind, die so verschlüsselten Daten zu nutzen. Gegebenenfalls müssen die Daten dann mit einem alternativen Produkt zeit- und arbeitsaufwändig entschlüsselt und neu verschlüsselt werden.

**Apps**

Integraler Bestandteil des Windows-8-Betriebssystems sind sogenannte Apps. Diese für die Bedienung per Berührung optimierten Anwendungen werden sowohl durch Microsoft als auch weitere Anbieter bereitgestellt. Werden Spezial-Anwendungen einer Institution in Form von Apps bereitgestellt, so ist gegebenenfalls der Zugriff von alternativen Plattformen nicht möglich, da diese Apps dafür nicht verfügbar sind.

# G 2.203 Integrierte Cloud-Funktionalität

Neuere Betriebssysteme und Anwendungen bringen oft Funktionen mit, mit denen Daten unter Nutzung der Dienste von Dritten abgelegt und synchronisiert werden ("Cloud-Computing"). Dies gilt in besonderem Maße bei Anwendungen, die vornehmlich auf die Nutzung von mobilen Geräten aus abzielen ("Apps"). Die Anwendungsdaten werden dabei oft in Cloud-Diensten großer, internationaler Anbieter abgespeichert.

Dadurch besteht die Gefahr, Cloud-Diensten unbewusst (oder zumindest unbedacht) auch für möglicherweise sensible oder personenbezogene Daten zu nutzen. Gleichzeitig können sich Verstöße gegen die Datenschutzgesetze ergeben, wenn Daten bei Dritten, gespeichert werden.

Problematisch sind dabei vor allem:

- Daten werden außerhalb der Grenzen der EU in Staaten ohne ausreichenden Datenschutz gespeichert.
- Anbieter von Cloud-Diensten unterliegen unter Umständen einer für die Wahrung kritischer Geschäftsgeheimnisse problematischen Jurisdiktion.
- Verträge kommen meist implizit über Allgemeine Geschäftsbedingungen der Cloud-Anbieter zustande und genügen deutschen Datenschutzanforderungen nicht.
- Die Anforderungen aus dem Bundesdatenschutzgesetz an eine Auftragsdatenverarbeitung werden hinsichtlich Auswahl, Prüfung und Kontrolle des Dienstleisters nicht erfüllt.
- Unter Umständen erfolgt eine Synchronisation der Daten mit privaten Geräten, die mit demselben Account betrieben werden.

Gefährdet sind dabei nicht nur vorhandene, im Cloud-Dienst abgelegte Daten, sondern auch Meta-Daten, die erst durch die Nutzung des Cloud-Dienstes anfallen. Dazu gehören z. B.

- Nutzungszeiten der Apps und des Systems, die durch die Protokollierung von An- und Abmeldungen anfallen,
- Verknüpfungen zu anderen Personen,
- Beziehungsnetzwerke, die von Dritten erstellt werden können, z. B. über das Tracking gemeinsam genutzter Dateien, besuchte Webseiten oder genutzte E-Mail- und Chat-Adressen,
- Ortsdaten mobiler Geräte, auch bei abgeschalteter Geolokation, indem z. B. die dem Gerät zugeordneten dynamischen IP-Adressen der Internetprovider über Geo-IP-Datenbanken referenziert werden,
- Konfigurations- und sonstige Daten, die die genutzten Apps an die jeweiligen Herausgeber übertragen,
- Verknüpfung mehrerer solcher Möglichkeiten über gemeinsam genutzte Authentifsierungsinformationen (z. B. Windows Live-ID).

Konkrete Beispiele sind:

- Ab Windows 8.1 ist Microsofts Cloud-Speicherlösung OneDrive fester Bestandteil des Betriebssystems. Es ist nicht möglich, OneDrive über die graphische Benutzeroberfläche zu deaktivieren.
- Windows 8 bietet als Standardeinstellung die Möglichkeit, den Bitlocker-Recovery-Schlüssel direkt über den Microsoft-Account in der Cloud zu sichern und damit kritische kryptographische Geheimnisse in die Hände Dritter zu geben.
- Meldet sich ein Nutzer mit bereits aktiviertem Microsoft-Account an einem neuen Gerät an, werden dort automatisch die von ihm genutzten Microsoft-Cloud-Dienste eingerichtet. Außerdem könnten Daten des Unterneh-

mens oder der Behörde ungewollt auf die privaten Geräte der Mitarbeiter übertragen werden, wenn diese mit demselben Microsoft-Account auch private IT-Systeme nutzen.

# G 2.204 TPM-Nutzung

Das Trusted Platform Module (TPM) ist ein Hardware-Chip, der ein IT-System um grundlegende Sicherheitsfunktionen erweitert:

- Erzeugung und sichere Verwahrung kryptographischer Schlüssel,
- Hardware-basierte kryptographische Funktionen,
- Überwachung der Plattformintegrität,
- Plattformauthentisierung,
- Zufallszahlengenerator.

Das TPM ist dabei nicht an einen Benutzer gebunden, sondern an eine Hardware-Instanz, die vom Hersteller überprüft und mit den initialen Schlüsseln, den sogenannten Endorsement-Keys, versehen wird. Diese bilden die Basis für die Erstellung weiterer Schlüssel und verlassen niemals das TPM. Auch der Besitzer eines IT-Systems kann diese Schlüssel nicht einsehen oder ändern.

In Clients ab Windows Vista oder Servern ab Windows Server 2008 wird das TPM des Computers beispielsweise für die Festplattenverschlüsselung mit Bitlocker genutzt. In Clients ab Windows 8 ist das TPM des Computers im Auslieferungszustand aktiviert.

Mit aktiviertem TPM übernimmt das Betriebssystem auf Basis des eingebauten Chips während der Initialisierung die Oberhoheit über alle Sicherheitsfunktionen des IT-Systems. Durch die Einbindung eines Hardware-Chips besteht dabei die grundsätzliche Gefahr, dass Schwachstellen im Betriebssystem auch Auswirkungen auf Funktionen des TPM oder darin gespeicherte Daten haben können. In einem solchen Fall könnte das IT-System dauerhaft unbenutzbar werden. Durch die unzureichende Verfügungsgewalt des Eigentümers beziehungsweise der Institution über eigene Schlüssel kann der Zugriff auf mit diesem System geschützte Daten in einem solchen Fall permanent verhindert werden.

In vielen Konfigurationen kann das Betriebssystem ein zuvor ausgeschaltetes TPM selbst wieder einschalten. Dies kann auch erfolgen, ohne dass der Eigentümer oder Administrator dies bemerkt.

Das TPM kann auch von Herstellern genutzt werden, um Kopierschutzmechanismen zu realisieren. So können darüber die Hersteller von Betriebssystemen und Anwendungssoftware die Identität eines Endgerätes verifizieren und die Lauffähigkeit von Software, aber auch die Lesbarkeit kryptographisch gesicherter Daten, von Schlüsseln im TPM abhängig machen.

Es besteht hierbei für die Benutzer die Gefahr, dass Software durch den Hersteller nachträglich unbrauchbar gemacht wird, oder eine eingesetzte Software auf einem PC mit aktiviertem TPM ab einem bestimmten Zeitpunkt nicht mehr nutzbar ist. Durch eine von der anwendenden Institutionen nicht kontrollierbare Verschlüsselung von Daten kann erreicht werden, dass eine Rückgewinnung der Daten ohne Mitwirkung des Software-Herstellers, z. B. mit Methoden des Reverse Engineering, nicht mehr möglich ist. Auf diese Art kann z. B. eine Insolvenz des Softwareherstellers zu Datenverlusten bei allen Stellen führen, die die entsprechende Software einsetzen. Die Migration zu alternativen Softwareprodukten wird in solchen Szenarien ebenfalls erschwert ("Lock-In-Effekt").

**Beispiele:**

- Durch einen Defekt auf dem Motherboard oder im TPM-Chip kann das System nicht mehr gestartet oder nicht mehr auf verschlüsselte Daten zugegriffen werden.
- Wird Bitlocker mit PIN-Eingabe konfiguriert, so bootet ein betroffenes IT-System nicht mehr, falls der Benutzer die PIN vergessen hat und es keinen Recovery-Schlüssel gibt.
- Die Gültigkeit einer Software-Lizenz wird vom Hersteller zurückgenommen. Dadurch lässt sich das eingesetzte Programm nicht mehr ausführen.
- Nach der Insolvenz eines Herstellers ist die Migration von Anwendungsdaten auf eine Alternativ-Lösung nicht mehr möglich, weil die Daten in der Anwendung mit einem TPM-Schlüssel unter Kontrolle des Herstellers geschützt sind.
- Software- oder Betriebssystemhersteller nutzen TPM-Funktionen, um die Zusammenarbeit ihrer Lösungen mit freien Alternativen einzuschränken.

# G 2.205 Fehlendes Notfallvorsorgekonzept für serviceorientierte Architekturen

Fallen in einer serviceorientierten Architektur (SOA) Service-Provider aus und sind keine alternativen Provider verfügbar, droht der Betrieb unterbrochen zu werden, was sich möglicherweise schwerwiegend auf die Geschäftsprozesse auswirkt. Die Informationssicherheit kann stark gefährdet sein, weil zum Beispiel wichtige Sicherheitskomponenten betroffen sind. Fehlt in diesem Fall ein Sicherheits- bzw. Notfallvorsorgekonzept, welches die Besonderheiten einer SOA berücksichtigt, können geeignete Sicherheitsmaßnahmen möglicherweise nicht zeitnah durchgeführt werden und es droht ein erheblicher Schaden für die Institution.

# G 2.206 Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen

Aus Kostengründen wird der Informationssicherheit bei der Entwicklung von eingebetteten Systemen häufig eine geringere Wertigkeit zugeordnet als z. B. Performance- oder Zuverlässigkeitsanforderungen.

Falls Sicherheitsanforderungen in einem oder mehreren der Entwicklungsteilprozesse

- Anforderungsmanagement
- System- und Schnittstellenentwurf
- Feinentwurf
- Implementierung
- Virtuelle und reale Teststufen
- Integrationsstufen mit Gesamtintegration

nicht ausreichend berücksichtigt werden, können in dem eingebetteten System schwerwiegende Schwachstellen entstehen. Diese sind nachträglich oft nur mit großem Aufwand identifizierbar, da die einzelnen Spezifikationen und Dokumente aufeinander aufbauen und es somit keinen Ansatzpunkt gibt, um Abweichungen festzustellen. Konstruktive oder methodische Mängel der Sicherheitsfunktionalität von Software eingebetteter Systeme werden nicht erkannt, wenn sich der Verifikationsprozess auf die spezifizierten Funktionen beschränkt.

Eingebettete Systeme können verwundet werden, wenn Erkenntnisse aus Sicherheitsvorfällen nicht in den Entwicklungsprozess aufgenommen werden, die Sicherheitsfunktion nicht nachgewiesen werden kann und die verwendeten Entwicklungswerkzeuge es nicht erlauben, Sicherheitsmechanismen sinnvoll zu modellieren und zu implementieren.

**Beispiele:**

- Der Speicherbelegungsplan eines eingebetteten Systems berücksichtigt nicht restliche unbelegte Speicherbereiche. In diese Bereiche eingebrachte Schadsoftware bleibt bis zu ihrer Aktivierung unerkannt. Ein eingebettetes System kann einen mehreren Megabyte großen Flash-ROM haben, von dem es seine Applikationssoftware nach dem Einschalten bootet. Diese Speicher werden nicht als Arbeitsspeicher genutzt, deshalb verändern sich die Software und die Speicherbelegung nicht. Die Speicher werden selten vollständig genutzt, so dass durchaus auch größere statische Speicherbereiche mit Schadsoftware belegt werden könnten. Da solche Bereiche als leer gekennzeichnet sind, sind Programme in diesen Bereichen durch die Software nicht sichtbar. Software in diesen Speicherbereichen ist immun gegen einen Systemneustart und oft auch gegen die Neuinstallation der Betriebssoftware, da nur die durch die Betriebssoftware belegten Bereiche überschrieben werden. Die "leeren" Speicherbereiche können nur mit speziellen Werkzeugen geprüft werden. Schäden können entstehen, wenn z. B. eine Schadsoftware mit Zugriff auf das Bussystem aktiviert wird und danach Daten verändert oder ein System dazu bringt, bestimmte Daten zu ignorieren. Erhebliche Schäden können entstehen, wenn das übergreifende System hochschutzbedürftig ist, wie etwa ein eingebettetes System zum Ver- und Entschlüsseln.

- In einem eingebetteten System werden bei Spannungsschwankungen oder schweren Fehlermeldungen im Rahmen des Neustarts die Ressourcen reorganisiert oder rekonfiguriert. Während dieses kurzen Zeitraums kann es verwundbar sein, z. B. wenn auf die I/O-Ports zugegriffen oder Sicherheitsmechanismen zur Authentikation umgangen werden können. Im Normalbetrieb hätten die Sicherheitsfunktionen dies verhindert. Sofern sich die Tests des Herstellers nur auf die spezifizierte Funktionalität unter den normalen Betriebsbedingungen beschränken, würde die Schwachstelle unerkannt bleiben.

# G 2.207 Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen

Die Schnittstellen eines eingebetteten Systems sind potenzielle Angriffspunkte für Eindringversuche. Dies umfasst Schnittstellen auf allen Ebenen des ISO/OSI-Schichtenmodells und alle eingesetzten Übertragungsmedien. Wird der Zugang über die Schnittstellen nicht kontrolliert oder sind die Kontrollmechanismen zu schwach, kann ein Angreifer in das System eindringen, unbefugt Daten lesen und schreiben und zu Folgeangriffen ansetzen. Er könnte unbemerkt Spionage- oder Sabotagegeräte wie miniaturisierte Steuerungen oder Datenlogger anschließen.

Auf Mikrocontrollerebene könnten bei Anschluss an die I/O-Ports über die I/O-Leitungen Signale in die I/O-Register eingespielt werden oder es könnten Ausgangssignale aufgezeichnet werden. Falls ein Reset-Eingang vorhanden ist, könnte ein Angreifer diesen ansteuern und temporär das System außer Betrieb nehmen.

Kommuniziert das eingebettete System über Ethernet und TCP/IP, kann ein Angreifer versuchen, sich in die Kommunikation einzuschalten, Datenpakete abfangen, einspielen und fälschen. Er kann nach offenen TCP-/UDP-Ports scannen und über diese einen Angriff durchführen.

Falls das eingebettete System über Funk mit anderen Systemen kommuniziert, ist es den üblicherweise in diesem Bereich vorliegenden Gefahren ausgesetzt und ein Angreifer könnte unter Umständen ohne direkten physischen Zugang eindringen. Beispiele hierfür sind WLAN oder Bluetooth, aber auch andere Kommunikationsmittel sind denkbar.

Wartungs- und Debugging-Schnittstellen können vielfältige Zugangs- und Zugriffsmöglichkeiten bieten, da sie häufig mittels sehr einfachen Protokollen ohne Authentisierungs- oder Protokollierungsmechanismen realisiert sind.

# G 2.208 Unzureichende physische Absicherung der elektronischen Komponenten bei eingebetteten Systemen

Ist ein eingebettetes System physisch leicht zugänglich, kann dies einem Täter den Einstiegspunkt für verschiedenste Angriffe bieten. Ein System kann physisch zerstört oder beschädigt werden, z. B. durch mechanische Gewalt, Kurzschlüsse oder Überspannungen. Es kann nach mechanischen, chemischen und physikalischen Vorarbeiten logisch analysiert werden. Sobald ein Täter physikalischen Zugang auf die elektronischen Komponenten hat, z. B. IC-Pins, Kontaktierungen, etc., kann er die elektrischen Signale direkt mit entsprechenden Mess- und Analysewerkzeugen unbemerkt aufnehmen und selbst Signale einspeisen.

# G 2.209 Auswahl einer ungeeigneten Entwicklungsumgebung für Software

Wird für die Entwicklung einer Software eine ungeeignete Entwicklungsumgebung ausgewählt, können vielfältige Probleme entstehen. Werden beispielsweise verschiedene Programmiersprachen bei der Software-Entwicklung benutzt, ist die gewählte Entwicklungsumgebung möglicherweise mit einer oder mehreren Programmiersprachen nicht kompatibel. Wenn keine bestimmte Entwicklungsumgebung aktiv ausgewählt wird, arbeiten verschiedene Entwickler möglicherweise mit unterschiedlichen selbst gewählten Werkzeugen an der Software und können dadurch Kompatibilitätsprobleme verursachen.

Wird eine Entwicklungsumgebung ungeeignet oder unkontrolliert ausgewählt, können dringend benötigte Funktionen fehlen oder nicht in ausreichender Form implementiert sein.

Weiterhin kann eine ungeeignete Entwicklungsumgebung auch Fehler oder Schwachstellen aufweisen, die erhebliche Störungen im Verlauf der Software-Entwicklung verursachen können.

**Beispiele:**

- Ein Java-Projekt muss mehrfach so geändert werden, dass Variablen und Klassen umbenannt werden müssen. Wird eine Entwicklungsumgebung ohne Funktionen zur automatischen Umformatierung von Quellcode und Strukturen (Refactoring) verwendet, stellen bereits diese minimalen Änderungen einen erheblichen Arbeitsaufwand und eine potentielle Fehlerquelle dar.
- Im September 2015 gelang es Angreifern, Schadcode in iOS-Apps zu integrieren, indem sie für Entwickler eine manipulierte Version der Entwicklungsumgebung Xcode bereitstellten. Verschiedene mit dem sogenannten XcodeGhost erstellte Apps wurden veröffentlicht und gelangten auf mehrere Millionen Geräte.

# G 2.210 Unzureichend gesicherter Einsatz von Entwicklungsumgebungen

Wenn die Entwicklungsumgebung unzureichend gesichert eingesetzt wird, kann nicht gewährleistet werden, dass die produzierte Software sicher implementiert wird, da sie möglicherweise manipuliert ist und dies nicht nachträglich entdeckt werden kann.

Wird die Entwicklungsumgebung nicht mit eingeschränktem Zugriff betrieben, wird die Software unkontrolliert entwickelt. Wenn nicht bekannt ist, welche Benutzer zu welchem Zeitpunkt auf die Entwicklungsumgebung zugreifen können und konnten, kann die Software anonym manipuliert werden. Sofern die manipulierten Teile der Software entdeckt werden, kann aufgrund der fehlenden Zugriffsbeschränkungen nicht nachvollzogen werden, welcher Mitarbeiter manipuliert hat.

Bei einer fehlenden oder unzureichenden Versionsverwaltung des Quellcodes ist es nicht möglich, vorherige und bereits funktionierende Versionen der Software wiederherzustellen.

Wenn Quellcodes unzureichend dagegen gesichert werden, dass sie versehentlich oder absichtlich verfälscht werden, besteht die Gefahr, dass Teile eines Projekts oder sogar das gesamte Projekt beschädigt werden und die bereits eingebrachte Arbeitsleistung verloren geht. Dies verzögert den Projektablauf und führt schlimmstenfalls zum Scheitern des Projekts.

**Beispiele:**

- Ein Entwickler möchte spontan eine Software optimieren und verändert dabei wesentliche Kernkomponenten des komplexen Projekts. Die Optimierung erzielt nicht die gewünschten Resultate und der Entwickler entscheidet sich, die ursprüngliche Version wiederherzustellen. Nachdem der Quellcode wiederhergestellt wurde, stellt er fest, dass die nun vorhandene Version nicht dem vorher aktuellen Versionsstand entspricht und auch keine weitere Sicherung mehr zur Verfügung steht.
- Im Jahr 2009 wurde ein Virus entdeckt, der gezielt die Entwicklungsumgebung Delphi befiel. Mit der infizierten Delphi-Entwicklungsumgebung erstellte Programme wurden dadurch automatisch mit Schadcode versehen.

# G 2.211 Auswahl eines ungeeigneten Vorgehensmodells zur Software-Entwicklung

Vorgehensmodelle strukturieren und planen den Projektablauf, indem bestimmte Handlungsschritte und deren Abfolge vorgegeben werden. Wird ein ungeeignetes Ablaufmodell für die Vorgehensweise bei der Software-Entwicklung ausgewählt, kann der Projektverlauf erheblich beeinflusst werden. Je nach Ausprägung des gewählten Modells und Umfang des Projekts werden entweder wichtige Aspekte vernachlässigt oder es werden irrelevante Aspekte übermäßig fokussiert. Beide genannten Probleme erhöhen den Arbeitsaufwand im Projektmanagement und schränken die produktive Arbeit ein.

Ist das gewählte Vorgehensmodell zu starr, können nachträgliche Änderungen nur mit sehr hohem Aufwand eingebracht werden, da sie bei der vorherigen Planung nicht berücksichtigt wurden.

Bei einem zu flexiblen Modell kann der Ablauf der Software-Entwicklung durch übermäßig viele Iterationen verzögert werden, die durch eine nicht ausreichend detaillierte Vorplanung oder durch wiederholte Änderungswünsche entstehen.

Ebenso kann der Personalaufwand zur Realisierung eines Projekts falsch eingeschätzt werden, wenn hierbei ein ungeeignetes Vorgehensmodell zugrunde gelegt wird.

**Beispiel:**

- Das Wasserfallmodell beschreibt einen linearen Ablauf der Software-Entwicklung und sieht nach Abschluss einer Phase keine weitere Iteration dieser Phase vor. Wird die Vorgehensweise nach dem Wasserfallmodell streng eingehalten, können beispielsweise in der Implementierungsphase keine nachträglich geänderten Anforderungen mehr berücksichtigt werden, die zur Verbesserung der Sicherheit sinnvoll wären.

# G 2.212 Unzureichende Berücksichtigung von Konfigurationsoptionen bei der Software-Entwicklung

Werden bei der Software-Entwicklung keine dynamischen Konfigurationsoptionen berücksichtigt, können im produktiven Betrieb Probleme auftreten, weil die Software nicht für geänderte Einsatzbedingungen anpassbar ist.

Wenn die Software zu stark am Entwicklungs-System ausgerichtet ist, besteht die Möglichkeit, dass sie mit dem Produktiv-System nicht mehr kompatibel ist, weil dort beispielsweise unterschiedliche Zugangsdaten für eine Datenbank benötigt werden, diese Information aber im Quellcode der Software fest kodiert wurde. Fehlen dann Konfigurationsoptionen zur Anpassung an unterschiedliche Systemvoraussetzungen, wird der Einsatz der Software erschwert oder verhindert.

Werden Verweise auf Systemdateien als feste Pfadangaben im Quellcode integriert, können Inkompatibilitäten auftreten, wenn die Software auf einem anderen Computer ausgeführt wird.

Sind Ablageorte für dynamisch wachsende Datenmengen, z.B. Protokolldateien, durch die Software festgelegt und können nicht vom Anwender frei gewählt werden, droht ein Mangel an Speicherplatz.

**Beispiele:**

- Im Quellcode einer Anwendungen sind feste Pfadangaben enthalten, die auf Windows-Systemdateien verweisen. Mit anderen Versionen von Windows kann die Anwendung deshalb nicht ausgeführt werden.
- In einer Anwendung kann der Speicherort für Protokolldaten nicht vom Benutzer konfiguriert werden. Während die Anwendung ausgeführt wird, entstehen deshalb regelmäßig Engpässe beim verfügbaren Speicherplatz.

# G 2.213 Fehlende oder unzureichende Qualitätssicherung des Softwareentwicklungsprozesses

Eine fehlende oder unzureichende Qualitätssicherung während der Software-Entwicklung kann dazu führen, dass das Projekt verzögert wird oder scheitert. Insbesondere wenn die sichere Implementierung nicht ausreichend geprüft wird, drohen Sicherheitslücken durch Schwachstellen in der ausgelieferten Software.

Ist die Qualitätssicherung nicht fest im Entwicklungsprozess verankert, kann dem Risiko, welches von Implementierungsfehlern, Konzeptionsfehlern oder gar bewusster Manipulation ausgeht, nicht angemessen begegnet werden. Dabei sollte die Aufmerksamkeit nicht nur selbst entwickelten Bestandteilen, sondern gerade auch externen Beiträgen Dritter oder übernommener Bestandteile z.B. aus externen Bibliotheken gelten. Die Offenlegung des Quellcodes, nach dem Open Source-Prinzip, und die damit prinzipiell verbundene, oft aber nicht genutzte, Möglichkeit zur Untersuchung durch externe Experten kann eine eigene systematische Qualitätssicherung nicht ersetzen.

**Beispiele:**

- Ein Praktikant erhält in einem Software-Unternehmen Vollzugriff auf alle Quellcode-Ressourcen. Er lässt sich von einem Konkurrenten des Unternehmens für das Einschleusen von Schadcode in zentrale Software-Komponenten engagieren. Diese Manipulation wird wegen fehlender Qualitätssicherung erst Monate später entdeckt und zu diesem Zeitpunkt bereits in Produktivsystemen eingesetzt.
- Es ist durchaus nicht ungewöhnlich, dass dieselben über Bibliotheken eingebundenen, in OEM-Firmware enthaltenen oder einfach nur kopierten Standard-Codebausteine in den Produkten verschiedener Hersteller Anwendung finden. Häufig werden innerhalb der Entwicklungsumgebung aus praktischen Gründen auch Daten verwendet, die nicht zur Veröffentlichung bestimmt sind. Was passieren kann, wenn dabei notwendige Anpassungen bzw. Bereinigungsschritte unterbleiben, zeigt das Ergebnis einer 2015 veröffentlichten Sicherheitsstudie. Die Forscher fanden zahlreiche private Schlüssel für SSL-Zertifikate und SSH-Zugänge in der veröffentlichten Firmware verschiedenster Produkte. Unter anderem fanden sich Zertifikate aus den SDKs von OEM-Lieferanten in den eigens erstellten Firmware-Versionen zahlreicher Kunden wieder. Da deren veröffentlichte Firmware auch jederzeit von Angreifern analysiert werden konnte wurde so eine enorm große Anzahl von Anwendern dieser Produkte der potentiellen Gefahr unberechtigter Zugriffe ausgesetzt.
- 2014 ging ein simpler Programmierfehler in einem Zusatzmodul der Open-Source-Bibliothek OpenSSL als Heartbleed-Bug in die Geschichte ein. Durch eine fehlende Längenprüfung war es Angreifern möglich, zufällige Speicherinhalte, welche auch geheime kryptographische Schlüssel oder Kennwörter enthalten konnten, von Gegenstellen abzurufen, welche die Bibliothek zur Implementierung von TLS nutzen. Der unbeabsichtigt fehlerhafte Programmcode war drei Jahre zuvor durch einen externen Entwickler eingereicht worden und wurde im Jahr darauf durch das interne Entwicklerteam in den produktiven Sourcecode übernommen. Die enorme Popularität der OpenSSL-Bibliothek führte schließlich dazu, dass der fehlerhafte Code weltweit in einer Vielzahl von Produkten und Systemen Verbreitung fand.

- Vermutlich seit der ersten Version aus dem Jahre 1989 enthielt der Sourcecode des Kommandozeileninterpreters Bash eine schwerwiegende Schwachstelle, die 2014 als Shellshock bekannt wurde. Sie ermöglichte es entfernten Angreifern unter bestimmten Umständen Code zur Ausführung auf betroffene Systeme wie z.B. Webserver, DHCP-Clients etc. einzuschleusen. Zwar wurde dank der umsichtigen Vorgehensweise des Entdeckers bereits bei Bekanntwerden ein erster Patch veröffentlicht, dieser behob das Problem selbst aber auch nicht vollständig. Folgende Analysen durch Sicherheitsforscher förderten schnell weitere Lücken zu Tage, die durch weitere Patches geschlossen werden mussten. Damit zeigt sich zwar, dass die öffentliche Verfügbarkeit des Quellcodes bei Eintreten des schlimmsten Falles die Analyse des Quellcodes durch interessierte Experten erleichtert und zur raschen Behebung von Schwachstellen beitragen kann. Der Umstand eines seit 25 Jahren unentdeckt bestehenden Fehlers zeigt aber deutlich, dass diese Form der fallweisen externen Qualitätssicherung eigene Prozesse keinesfalls ersetzen kann.

# G 2.214 Fehlende oder unzureichende Konzeption des Identitäts- und Berechtigungsmanagements

Voraussetzung für einen sicheren Einsatz eines Identitäts- und Berechtigungsmanagements ist eine umfassende Planung und Konzeption, wie Benutzerkennungen und deren Berechtigungen anzulegen, zu ändern und zu löschen sind.

Dazu ist der Lebenszyklus einer Identität zu organisieren und konzeptionell sicherzustellen, dass nur zugelassene Berechtigungen der Identität zugeordnet werden. Darüber hinaus müssen die Zuständigkeiten, Aufgaben und Informationswege als Prozesse definiert sein.

Dass Defizite bei einer fehlenden oder unzureichenden Konzeption zu Schäden führen können, machen folgende **Beispiele** deutlich:

- Bei einer fehlenden oder unzureichenden Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement kann es passieren, dass der zuständige Administrator keine Informationen über personelle Veränderungen erhält. So kann es passieren, dass ein Benutzerkonto eines ausgeschiedenen Mitarbeiters nicht gelöscht wird.
- Auch besteht die Gefahr, dass Mitarbeiter, die in eine neue Abteilung versetzt werden, ihre alten und nun nicht mehr benötigten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamt-Berechtigungen ansammeln.

# G 3 Gefährdungskatalog Menschliche Fehlhandlungen

| | |
|---|---|
| G 3.29 | Fehlende oder ungeeignete Segmentierung |
| G 3.30 | Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners |
| G 3.31 | Unstrukturierte Datenhaltung |
| G 3.32 | Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren |
| G 3.33 | Fehlbedienung von Kryptomodulen |
| G 3.34 | Ungeeignete Konfiguration des Managementsystems |
| G 3.35 | Server im laufenden Betrieb ausschalten |
| G 3.36 | Fehlinterpretation von Ereignissen |
| G 3.37 | Unproduktive Suchzeiten |
| G 3.38 | Konfigurations- und Bedienungsfehler |
| G 3.39 | Fehlerhafte Administration des RAS-Systems **- entfallen** |
| G 3.40 | Ungeeignete Nutzung von Authentisierungsdiensten bei VPNs |
| G 3.41 | Fehlverhalten bei der Nutzung von VPN-Diensten |
| G 3.42 | Unsichere Konfiguration der VPN-Clients für den Fernzugriff |
| G 3.43 | Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen |
| G 3.44 | Sorglosigkeit im Umgang mit Informationen |
| G 3.45 | Unzureichende Identifikationsprüfung von Kommunikationspartnern |
| G 3.46 | Fehlerhafte Konfiguration eines Lotus Domino Servers |
| G 3.47 | Fehlerhafte Konfiguration des Browser-Zugriffs auf Lotus Notes **- entfallen** |
| G 3.48 | Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen |
| G 3.49 | Fehlerhafte Konfiguration des Active Directory |
| G 3.50 | Fehlerhafte Konfiguration von Novell eDirectory |
| G 3.51 | Falsche Vergabe von Zugriffsrechten im Novell eDirectory |
| G 3.52 | Fehlerhafte Konfiguration des Intranet-Clientzugriffs auf Novell eDirectory |
| G 3.53 | Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory |
| G 3.54 | Verwendung ungeeigneter Datenträger bei der Archivierung |

G 3.55 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen

G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung

G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS **- entfallen**

G 3.58 Fehlerhafte Konfiguration eines IIS **- entfallen**

G 3.59 Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS **- entfallen**

G 3.60 Fehlerhafte Konfiguration von Exchange

G 3.61 Fehlerhafte Konfiguration von Outlook

G 3.62 Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver **- entfallen**

G 3.63 Fehlerhafte Konfiguration eines Apache-Webservers **- entfallen**

G 3.64 Fehlerhafte Konfiguration von Routern und Switches

G 3.65 Fehlerhafte Administration von Routern und Switches

G 3.66 Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS

G 3.67 Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems

G 3.68 Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers

G 3.69 Fehlerhafte Konfiguration der Unix System Services unter z/OS

G 3.70 Unzureichender Dateischutz des z/OS-Systems

G 3.71 Fehlerhafte Systemzeit bei z/OS-Systemen

G 3.72 Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF

G 3.73 Fehlbedienung der z/OS-Systemfunktionen

G 3.74 Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen

G 3.75 Mangelhafte Kontrolle der Batch-Jobs bei z/OS

G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

G 3.77 Mangelhafte Akzeptanz von Informationssicherheit

G 3.78 Fliegende Verkabelung

G 3.79 Fehlerhafte Zuordnung von Ressourcen des SAN

G 3.80 Fehler bei der Synchronisation von Datenbanken

G 3.81 Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003
G 3.82 Fehlerhafte Konfiguration der VoIP-Middleware
G 3.83 Fehlerhafte Konfiguration von VoIP-Komponenten
G 3.84 Fehlerhafte Konfiguration der WLAN-Infrastruktur
G 3.85 Verletzung von Brandschottungen
G 3.86 Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten
G 3.87 Fehlerhafte Konfiguration von Verzeichnisdiensten
G 3.88 Falsche Vergabe von Zugriffsrechten
G 3.89 Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste
G 3.90 Fehlerhafte Administration von VPNs
G 3.91 Ausfall von VPN-Verbindungen durch Fehlbedienung
G 3.92 Fehleinschätzung der Relevanz von Patches und Änderungen
G 3.93 Falscher Umgang mit defekten Datenträgern
G 3.94 Fehlkonfiguration der Samba-Kommunikationsprotokolle
G 3.95 Fehlerhafte Konfiguration des Betriebssystems für einen Samba-Server
G 3.96 Fehlerhafte Konfiguration eines Samba-Servers
G 3.97 Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista
G 3.98 Verlust von BitLocker-verschlüsselten Daten
G 3.99 Fehlerhafte Netzanbindungen eines Virtualisierungsservers
G 3.100 Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme
G 3.101 Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen
G 3.102 Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen
G 3.103 Fehlerhafte Domain-Informationen
G 3.104 Fehlerhafte Konfiguration eines DNS-Servers
G 3.105 Ungenehmigte Nutzung von externen Dienstleistungen
G 3.106 Ungeeignetes Verhalten bei der Internet-Nutzung
G 3.107 Rufschädigung

# G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten

Durch Fehlverhalten von Personen aller Art kann der Vertraulichkeits- bzw. Integritätsverlust von Informationen und Daten herbeiführt bzw. ermöglicht werden. Die Folgeschäden ergeben sich aus der Schutzbedürftigkeit der Daten. Beispiele für ein solches Fehlverhalten sind:

- Mitarbeiter holen versehentlich Ausdrucke mit personenbezogenen Daten wqnicht am Netzdrucker ab.
- Vertrauliche Informationen werden in Hörweite fremder Personen diskutiert, beispielsweise in Pausengesprächen von Besprechungen oder über Mobiltelefonate in öffentlichen Umgebungen.
- Es werden Datenträger versandt, ohne dass die vorher darauf gespeicherten Daten in geeigneter Weise gelöscht wurden.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben sind.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten vermag ein Mitarbeiter Daten zu ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.
- Neue Software wird mit nicht anonymisierten Daten getestet. Nicht befugte Mitarbeiter erhalten somit Einblick in geschützte Dateien bzw. vertrauliche Informationen. Möglicherweise erlangen überdies auch Dritte Kenntnis von diesen Informationen, weil die Entsorgung von "Testausdrucken" nicht entsprechend geregelt ist.
- Beim Ausbau, Verleih, Einsendung zur Reparatur oder Ausmusterung von Festplatten können Daten auf zum Teil noch intakten Dateisystemen in unbefugte Hände gelangen, wenn diese zuvor nicht irreversibel gelöscht wurden.
- Betreut ein Outsourcing-Dienstleister mehrere Mandanten, so können Daten einer auslagernden Organisation durch menschliches Versagen anderen Mandanten des Outsourcing-Dienstleisters zugänglich werden. Mögliche Ursachen können beispielsweise folgende sein:
  - Auswahl einer falschen E-Mail-Adresse aus dem Adressbuch.
  - Unbedachtes "copy - paste" (z. B. von Konfigurationsdateien von Systemen verschiedener Auftraggeber).
  - Postversand (z. B. von Backup-Medien, Verträgen) an die falsche Adresse.

# G 3.2 Fahrlässige Zerstörung von Gerät oder Daten

Durch Fahrlässigkeit, aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Daten kommen, die den Betrieb des IT-Systems empfindlich stören können. Dies ist auch durch die unsachgemäße Verwendung von IT-Anwendungen möglich, wodurch fehlerhafte Ergebnisse entstehen oder Daten unabsichtlich verändert oder zerstört werden. Durch unachtsames Benutzen eines einzigen Löschbefehls können ganze Dateistrukturen gelöscht werden.

**Beispiele:**

- Benutzer, die aufgrund von Fehlermeldungen den Rechner ausschalten, statt ordnungsgemäß alle laufenden Anwendungen zu beenden bzw. einen Sachkundigen zu Rate zu ziehen, können hierdurch schwerwiegende Integritätsfehler in Datenbeständen hervorrufen.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen werden.
- In einem z/OS-System verfügte ein Systemprogrammierer über die Berechtigung, das Programm *ICKDSF* zum Formatieren von Festplatten aufzurufen. Als er zur Ausübung seiner Tätigkeit dringend eine Festplatte benötigte, wählte er aus dem vorhandenen Pool eine freie Festplatte aus, gab jedoch aufgrund eines Tippfehlers eine falsche Adresse an. Den im System-Log anstehenden Reply las er nur flüchtig und beantwortete ihn sofort. Die Formatierung einer bereits belegten Festplatte wurde dadurch freigegeben und wichtige Produktionsdaten zerstört.
- Ein Benutzer, der es sich zur Gewohnheit gemacht hat, unter Unix den Löschbefehl *rm* grundsätzlich ohne den Parameter für die Sicherheitsabfragen (*-i*) durchzuführen oder gar mit *-f* die Sicherheitsabfragen grundsätzlich ausschaltet, riskiert in hohem Maße das versehentliche Löschen von Dateien.

# G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen

Aufgrund von Nachlässigkeit und fehlenden Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten Sicherheitsmaßnahmen nicht oder nicht im vollen Umfang durchführen. Es können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären. Je nach der Funktion der Person und der Bedeutung der missachteten Maßnahme können sogar gravierende Schäden eintreten. Vielfach werden Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewusstsein heraus nicht beachtet. Ein typisches Indiz dafür ist, dass wiederkehrende Fehlermeldungen nach einer gewissen Gewöhnungszeit ignoriert werden.

- Ein verschlossener Schreibtisch bietet zur Aufbewahrung von Dokumenten, DVDs, USB-Sticks oder anderen Informationsträgern keinen hinreichenden Schutz gegen unbefugten Zugriff, wenn der Schlüssel im selbern Büro aufbewahrt wird, z. B. auf dem Schrank oder unter der Tastatur.
- Obwohl die schadensmindernde Eigenschaft von Datensicherungen hinreichend bekannt ist, treten immer wieder Schäden auf, wenn Daten unvorhergesehen gelöscht werden und aufgrund fehlender Datensicherung die Wiederherstellung unmöglich ist. Dies zeigen insbesondere die dem BSI gemeldeten Schäden, die z. B. aufgrund von Schadsoftware entstehen.
- Der Zutritt zu einem Rechenzentrum sollte ausschließlich durch die mit einem Zutrittskontrollsystem (z. B. Authentikation über Chipkartenleser, PIN-Eingabe oder biometrische Verfahren) gesicherte Tür erfolgen. Die Fluchttür wird jedoch, obwohl sie nur im Notfall geöffnet werden darf, als zusätzlicher Ein- und Ausgang ohne besondere Sicherheitsvorrichtungen genutzt.
- In einem z/OS-System liefen täglich Batch-Jobs für die RACF-Datenbank-Sicherungen. Die korrekte Ausführung dieser Abläufe sollte täglich von den zuständigen Administratoren geprüft werden. Da die Sicherungen jedoch über mehrere Monate ohne Probleme durchgeführt wurden, kontrollierte niemand mehr den Ablauf. Erst nachdem die RACF-Datenbanken des Produktionssyfstems defekt waren und die Sicherungen zurückgespielt werden sollten, wurde festgestellt, dass die Batch-Jobs seit mehreren Tagen nicht mehr gelaufen waren. Dies führte dazu, dass keine aktuellen Sicherungen vorhanden waren und die Änderungen der letzten Tage von Hand nachgetragen werden mussten. Neben einem erheblichen zusätzlichen Administrationsaufwand ergab sich dadurch ein Unsicherheitsfaktor, da nicht alle Definitionen sicher rekonstruiert werden konnten.
- In einer Institution ist es verboten, fremde USB-Geräte an die IT-Infrastruktur der Institution anzuschließen. Ein Mitarbeiter findet gerade keinen dienstlichen USB-Stick und verbindet stattdessen sein Smartphone mit dem PC. Diese mobile IT war jedoch mit einer Schadsoftware infiziert, wodurch es zu einem unberechtigten Datenabfluss kam.

# G 3.4 Unzulässige Kabelverbindungen

Wenn zwischen IT-Systemen oder anderen technischen Komponenten Kabelverbindungen hergestellt werden, die nicht vorgesehen sind, besteht die Gefahr, dass dadurch Sicherheitsprobleme oder Betriebsstörungen entstehen. Beispielsweise kann es aufgrund solcher unzulässiger Kabelverbindungen passieren, dass unerlaubt auf Netze, Systeme, Informationen oder Anwendungen zugegriffen werden kann. Durch unzulässige Kabelverbindungen können Informationen zusätzlich oder ausschließlich zu falschen Empfängern übertragen werden. Die normale Verbindung kann gestört werden.

Unzulässige Kabelverbindungen können unterschiedliche Ursachen und Ausprägungen haben, zum **Beispiel**:

- Technische Defekte
- Fehlerhafte Verkabelung von Patchfeldern, Rangier- oder Spleißverteilern
- Fehlerhafte Verkabelung von aktiven Netzkomponenten
- Unerlaubter Anschluss von fremden IT-Systemen an Netzdosen im LAN

Ungenaue Dokumentation und unzureichende Kabelkennzeichnung führen häufig zu versehentlichen Fehlbelegungen und erschweren das Erkennen von absichtlichen Fehlbelegungen.

# G 3.5 Unbeabsichtigte Leitungsbeschädigung

Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr einer unbeabsichtigten Beschädigung. Eine Beschädigung führt nicht unbedingt sofort zu einem Ausfall von Verbindungen. Auch die zufällige Entstehung unzulässiger Verbindungen ist möglich, wenn beispielsweise Kabelmäntel beziehungsweise Isolierungen nicht mehr vollständig intakt sind. Die folgenden Beispiele sind typisch für solche Beschädigungen im Innenbereich:

- Bei "fliegender" Verlegung können Geräteanschlussleitungen herausgerissen werden, wenn Mitarbeiter oder Besucher darüber stolpern.
- In einer Geräteanschlussleitung kann es zu einem Kabelbruch kommen, wenn mobile Büromöbel über die Leitung gerollt werden.
- Unter Putz verlegte Leitungen können durch Bohren oder Nageln an der falschen Stelle beschädigt werden.
- Wasser kann Beschädigungen verursachen, beispielsweise wenn Wasser in Fensterbank-Kabelkanäle oder in Fußboden-Kabelkanäle eindringt, durch bei Regen offenstehende Fenster oder bei der Gebäudereinigung.
- Auf Putz oder Estrich verlegte Leitungen können beim Transport sperriger und schwerer Gegenstände ramponiert werden.
- Kabel können bereits dann beschädigt werden, wenn sie nicht am Stecker, sondern am Kabel aus der Steckdose gezogen werden.
- Betriebsmittel können überlastet werden, wenn z. B. Geräte mit einer unzulässig hohen Gesamtleistung an einen Steckdosenverteiler angeschlossen werden.

Im Außenbereich können Leitungsbeschädigung beispielsweise durch folgende Ereignisse entstehen:

- Kabel können bei Tiefbauarbeiten beschädigt werden, sowohl bei Handausschachtung als auch bei Baggernutzung.
- Wasser kann in Erdtrassen oder Erdkabel eindringen.
- Kabel können durch Nagetiere angeknabbert werden.
- Trassen und Kabel können durch Wurzeln beschädigt werden (Baumwurzeln besitzen genug Kraft, um Kabel abzuquetschen).
- Die zulässigen Verkehrslasten können überschritten werden (Rohre können dadurch brechen, Kabel können abscheren).
- Steckerkombinationen temporär verlegter Leitungen für Werkzeuge und Maschinen können überfahren werden.

**Beispiel:**

In einer Fußgängerzone hatte es sich die Reinigungskraft eines kleinen Geschäftes zur Angewohnheit gemacht, das gebrauchte Putzwasser in den direkt vor der Ladentür befindlichen Revisionsschacht einer Kabeltrasse zu schütten. Das Wasser verdunstete zwar mit der Zeit immer wieder, der Schmutz- und Seifenanteil jedoch lagerte sich auf den Kabeln ab und musste für Arbeiten daran erst mühsam und zeitaufwendig entfernt werden.

# G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Es ist bereits nicht immer ganz einfach, eigene Mitarbeiter ausreichend zum richtigen Umgang mit geschäftskritischen Informationen und mit IT-Systemen zu schulen. Bei Betriebsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese in den seltensten Fällen kennen.

Besucher, Reinigungs- und Fremdpersonal können interne Informationen, Geschäftsprozesse und IT-Systeme auf verschiedene Art und Weise gefährden, angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des "Spielens" an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten.

**Beispiele:**

- Besucher können, wenn sie unbegleitet sind, Zugriff auf Unterlagen, Datenträger oder Geräte haben, diese beschädigen oder unbefugt Kenntnis von schützenswerten Informationen erlangen.
- Durch Reinigungspersonal kann versehentlich eine Steckverbindung gelöst werden, Wasser kann in Geräte gelangen, Unterlagen können verlegt oder sogar mit dem Abfall entfernt werden.
- Ein externer Mitarbeiter hatte auf seinem Laptop Unterlagen gespeichert, die vor einer Besprechung in einer Behörde noch ausgedruckt werden sollten. Dafür wurden diese schnell per USB-Stick auf einen Rechner im LAN der Behörde kopiert. Dabei wurde allerdings auch Schadsoftware mitübertragen.
- In einem Rechenzentrum sollten in den Maschinenräumen Malerarbeiten durchgeführt werden. Der Maler stieß mit der Leiter versehentlich an den zentralen Notausschalter der Stromversorgung und löste diesen aus. Die gesamte Stromversorgung der z/OSin diesem Rechenzentrum war sofort unterbrochen. Durch den Stromausfall waren mehrere Platten (DASD - Direct Access Storage Device) nicht sofort verfügbar. Der hinzugezogene Techniker benötigte mehrere Stunden, bis die Produktion wieder anlaufen konnte.

# G 3.7 Ausfall der TK-Anlage durch Fehlbedienung

Neben dem technischen Versagen durch defekte Bauteile, Stromausfall oder Sabotage gibt es eine Reihe weiterer Umstände, die zum Ausfall einer TK-Anlage oder anderer Telekommunikationseinrichtungen führen können. So kann es aufgrund des im Allgemeinen großen Funktionsumfangs einer TK-Anlage passieren, dass ungewollte Funktionen ausgelöst werden, wenn sie falsch bedient wird. Ein Ausfall kann beispielsweise durch unzureichend ausgebildetes Wartungspersonal verursacht werden, wenn dieses die TK-Anlagen unsachgemäß konfiguriert. Werden Alarmsignale missachtet oder ein abnormes Betriebsverhalten nicht erkannt, kann es zu Betriebsstörungen kommen. Unsachgemäßes oder unüberlegtes Handeln bei eigentlich einfachen Routinereparaturen kann auch ein Grund für den Ausfall einer TK-Anlage sein.

Da weitgehende konzeptionelle und technologische Unterschiede zwischen klassischen TK-Anlagen und VoIP-Lösungen bestehen, erfordert ein Wechsel auf VoIP oft eine umfangreiche Neuschulung des Personals. Zusätzlich werden weitgehende Kenntnisse in der IP-Netztechnik benötigt. Wird die TK-Anlage als Folge unzureichender Kenntnisse fehlbedient, kann das bei der Anbindung an IP-Netze mehr als nur Ausfälle der Telekommunikationsinfrastruktur verursachen. Soll der VoIP-Medienstrom über ein Datennetz übertragen werden, an dem auch die Arbeitsplatzrechner und Server angeschlossen sind, kann eine Fehlkonfiguration zu einem Ausfall des gesamten Datennetzes führen.

**Beispiele:**

- Bei der Konfiguration der VoIP-Anlage wird ein unzureichender Kompressionsalgorithmus für die Übermittlung der Sprachdaten gewählt, die dadurch zuviel Bandbreite verbrauchen und so zu einer Überlastung des Datennetzes führen. Als Folge ist weder produktives Arbeiten an den Arbeitsplatzrechnern noch die Fernkonfiguration der VoIP-Anlage möglich. Der für die VoIP-TK-Anlage zuständige Administrator vermutet das Problem bei einer fehlerhaften Konfiguration des Netzes, wofür ein anderer Administrator zuständig ist, und wird daher nicht aktiv. Erst nach einer Analyse der Netzaktivität wird das Problem entdeckt und behoben. Obwohl die eigentliche Korrektur des Konfigurationsfehlers nur wenige Minuten dauerte, wurde der gesamte Betrieb für über eine Stunde erheblich gestört.
- Durch die absichtliche oder unabsichtliche Fehlkonfiguration einer TK-Anlage können zum Beispiel einzelne Anschlüsse durch eine Veränderung der Durchwahl so konfiguriert werden, dass sie von außen nicht mehr erreichbar sind. Wenn nach außen bei einer solchen Störung ein Freizeichen signalisiert wird, kann es einige Zeit dauern, bis eine solche Funktionsstörung bemerkt wird.

# G 3.8 Fehlerhafte Nutzung von IT-Systemen

Eine fehlerhafte oder nicht ordnungsgemäße Nutzung von IT-Systemen kann deren Sicherheit beeinträchtigen, wenn dadurch Sicherheitsmaßnahmen missachtet oder umgangen werden.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu Sicherheitsvorfällen führen.

Gleichermaßen können durch die fehlerhafte Bedienung von IT-Systemen oder Anwendungen Daten versehentlich gelöscht oder verändert werden. Dadurch könnten aber auch vertrauliche Informationen an die Öffentlichkeit gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

# G 3.9 Fehlerhafte Administration von IT-Systemen

Eine Administration beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch Sicherheitsmaßnahmen missachtet oder umgangen werden. Jede Modifikation von Sicherheitseinstellungen und die Erweiterung von Zugriffsrechten stellt eine potenzielle Gefährdung der Gesamtsicherheit dar.

Durch die fehlerhafte Installation von Software können Sicherheitsprobleme entstehen. Standard-Installationen von Betriebssystemen oder Systemprogrammen weisen in den seltensten Fällen alle Merkmale einer sicheren Konfiguration auf. Mangelnde Anpassungen an die konkreten Sicherheitsbedürfnisse können hier ein erhebliches Risiko darstellen. Die Gefahr von Fehlkonfigurationen besteht insbesondere bei komplexen Sicherheitssystemen, bei denen sich Systemfunktionen oft gegenseitig beeinflussen.

Die Ursachen für fehlerhaft ausgeführte Administrationstätigkeiten können vielfältigen Ursprungs sein. Denkbar sind hier beispielsweise Fehlbedienungen, die durch nachfolgende Aspekte hervorgerufen werden.

- Die Prozessdokumentation fehlt oder ist nicht aktualisiert. Sie gibt dem Administrator keinen Aufschluss über die Handhabung notwendiger Sicherheitseinstellungen.
- Die hohe technische Komplexität des IT-Systems führt dazu, dass der Administrator die Auswirkungen seiner Tätigkeiten in ihrer Gesamtheit nicht mehr überschauen kann. Durch die Anpassung eines Systemparameters werden weitere Parameter beeinflusst, die unter Umständen ursprünglich nicht im Zusammenhang standen.
- Die fehlende Standardisierung eines IT-Systems oder seiner Komponenten führt dazu, dass dieses auf die Einstellungen eines Administrators anders reagiert als gewünscht.
- Bedingt durch die fehlende Umsetzung des 4-Augen-Prinzips bleibt der Bedienungsfehler eines Administrators zunächst unentdeckt.
- Die eingesetzten Administratoren verfügen über unzureichende Kenntnisse im Zusammenhang mit der Bedienung der eingesetzten IT-Systeme.
- Die falsche Interpretation von aufgezeichneten Ereignissen führt zur Ausführung administrativer Arbeiten, die sich in der Folge als fehlerhaft erweisen. Die tatsächliche Ursache für das Ereignis wird dadurch zunächst nicht untersucht.

Die Durchführung von Wartungs- bzw. Betriebsarbeiten erfolgt in der Regel auf Basis administrativer Berechtigungen. Mögliche Gefährdungen für die Institution ergeben sich hierbei beispielsweise durch:

- die Nichteinhaltung von Standard-Arbeitsanweisungen (*Standard Operating Procedures,*SOP),
- eine falsche Patch-Reihenfolge,
- das Einspielen von Patches ohne das Durchlaufen eines vorherigen Test- und Freigabeverfahrens,
- die Nichtbeachtung der Kompatibilitätsmatrix des Herstellers.

Die Erstellung und Pflege eines entsprechenden Betriebshandbuchs ist die Voraussetzung für die Nachvollziehbarkeit der Konfiguration und Funktionsweise der eingesetzten IT-Systeme. Fehlt dieses, können Fehler unter Umständen verzögert nachvollzogen und beseitigt werden.

# G 3.10 Falsches Exportieren von Dateisystemen unter Unix

Exportierte Platten können von jedem Rechner, der sich mit dem in der Datei */etc/exports* bzw. */etc/dfs/dfstab* angegebenen Namen meldet, gemountet werden. Der Benutzer dieses Rechners kann jede UID und GID annehmen. Solange Verzeichnisse nicht mit der Option *root=* exportiert wurden, stellt die UID 0 (*root*) eine Ausnahme dar, die beim Zugriff auf einen NFS-Server üblicherweise auf eine andere UID (z. B. die des Benutzers *nobody* oder *anonymous*) abgebildet wird. Es lassen sich daher nur Dateien schützen, die *root* gehören.

Für die Verwendung der Protokolle NFS für den Export von Dateisystemen und die Verteilung von Systemdateien mittels NIS sind keine ausreichenden Schutzmaßnahmen in geschützten Umgebungen verfügbar. Der Einsatz stellt somit eine Gefährdung der Integrität der Systeme dar.

# G 3.11 Fehlerhafte Konfiguration von sendmail

Fehler in der Konfiguration oder Software von *sendmail* haben in der Vergangenheit schon mehrmals zu Sicherheitslücken auf den betroffenen IT-Systemen geführt (Stichwort Internet-Wurm).

**Beispiel:**

Es ist durch verschiedene Veröffentlichungen bekannt, dass es möglich ist, die Benutzer- und Gruppenkennung, die mit den Optionen *u* und *g* eingestellt sind (normalerweise *daemon*) zu erlangen. Dazu muss im Absenderfeld (*From:*) eine Pipe angegeben werden, durch die eine fehlerhafte Mail zurückgeschickt wird, und in der Mail selber muss ein Fehler erzeugt werden. Schickt man also z. B. eine Mail mit dem Inhalt

*cp /bin/sh /tmp/sh*
*chmod oug+rsx /tmp/sh*

an einen unbekannten Empfänger und benutzt als Absender ' */bin/sh* ', so wird die Mail als unzustellbar zurückgeschickt, was in diesem Falle einer Ausführung des kurzen Shellskripts gleichkommt. Durch dieses Skript wird dann eine Shell mit gesetztem *suid*-Bit erzeugt, die die im *sendmail.cf* gesetzte Benutzer- und Gruppenkennung hat.

# G 3.12 Verlust der Datenträger beim Versand

Werden Datenträger in nicht sonderlich stabilen Behältnissen (Briefumschlägen oder sonstigen Verpackungen) versandt, besteht die Gefahr, dass die Datenträger bei Beschädigung der Verpackung verloren gehen, insbesondere wenn nur einzelne CDs oder ähnliche Datenträger versandt werden. Auch besteht die Gefahr des Verlustes beim Empfänger, auf dem Postweg oder durch Unachtsamkeit eines Boten. Falls beispielsweise eine CD zusammen mit einem Anschreiben in einem Umschlag verschickt wird, der wesentlich größer als die CD ist, so kann beim Empfang des Umschlages die innenliegende CD übersehen und zusammen mit dem scheinbar leeren Umschlag versehentlich entsorgt werden. Auch wenn nur ein kurzes Anschreiben auf dem Postweg verloren geht, kann dadurch bereits ein wichtiger Termin gefährdet sein.

Wenn die Informationen auf den Datenträgern nicht verschlüsselt sind, können sie außerdem bei einem Verlust in die falschen Hände geraten.

# G 3.13 Weitergabe falscher oder interner Informationen

Bei der Weitergabe von Informationen kommt es immer wieder vor, dass neben den gewünschten Informationen auch andere Informationen übermittelt werden. Dadurch geraten immer wieder vertrauliche oder nicht für die Veröffentlichung geeignete Informationen in die falschen Hände. Dies kann sowohl beim Versand oder der Übergabe von Datenträgern passieren als auch beim persönlichen oder telefonischen Informationsaustausch oder bei jeder anderen Form von Datenübertragung. Eine weitere Möglichkeit ist die unbeabsichtigte Weitergabe von Daten bei der Weitergabe, dem Verkauf oder der Aussonderung von vermeintlich gelöschten Datenträgern.

Es ist denkbar, dass ein für den Versand oder sonstige Weitergabe vorgesehener Datenträger bereits Daten früherer Arbeitsgänge enthält, die dem Empfänger nicht zur Kenntnis gelangen sollen. Diese Daten können vom Empfänger gelesen werden, wenn sie vorher nicht gezielt vom Absender physikalisch gelöscht werden.

Befinden sich darüber hinaus die zu übertragenden Daten in einem Verzeichnis mit weiteren Daten, die ebenfalls schutzbedürftig sind, besteht die Gefahr, dass diese versehentlich mit auf den Datenträger übertragen werden (z. B. weil der Einfachheit halber das komplette Verzeichnis kopiert wurde) und dem Empfänger unnötig (unberechtigt) zur Kenntnis gelangen.

Häufig sollen Datensätze nicht über einen physischen Datenträger ausgetauscht, sondern über Datennetze direkt versandt werden, beispielsweise über E-Mail im Internet, Modem-Verbindung, interne Firmennetze oder einen X.400-Dienst. Hierbei bieten viele Kommunikationsprogramme die Möglichkeit der Verwendung von Kurzbezeichnungen für komplexe Adressstrukturen und Verteilerlisten für die Mehrfachversendung. Werden solche Verteilerlisten nicht zentral geführt oder nicht in regelmäßigen Abständen aktualisiert, können Datensätze an Adressen versendet werden, die zu nicht mehr autorisierten Personen gehören.

Immer wieder kommt es vor, dass Informationen auf Datenträgern, die weitergegeben, verkauft oder ausgemustert werden sollen, nicht vollständig gelöscht wurden. Die einfachen Löschbefehle der meisten Betriebssysteme können rückgängig gemacht oder die Daten mit frei verfügbaren Softwarewerkzeugen wieder hergestellt werden. Vermeintlich vernichtete Daten können ausgelesen und unberechtigt verwendet werden.

Auch beim klassischen Postversand kommt es immer wieder vor, dass vertrauliche Unterlagen versehentlich an den falschen Empfänger versandt werden oder dass Briefe zusammen mit internen Kommentaren ausgedruckt und unbemerkt kuvertiert werden. Häufig sollen auch Unterlagen weitergegeben werden, aus denen nur einige vertrauliche Teilinformationen wie Namensnennungen entfernt werden müssen. Dabei kann es passieren, dass dies nicht oder nur unzulänglich erfolgt, z. B. weil Passagen übersehen wurden oder die falsche Methode gewählt wurde.

**Beispiele:**

- In einer Behörde wurden bei der Ausmusterung von Datenträgern die darauf gespeicherten Daten nicht vollständig und unumkehrbar gelöscht, da ein ungeeignetes Tool dafür genutzt wurde. Die Rekonstruktion mit frei verfügbaren Softwarewerkzeugen war daher möglich. Nach dem Verkauf

von IT-Systemen und Datenträgern war es Käufern möglich, vertrauliche Daten einzusehen und weiterzuverbreiten.

- Eine häufig benutzte Methode, um in Dokumenten Teilinformationen unkenntlich zu machen, ist das Schwärzen. Hierbei kann allerdings vieles schief gehen:
  - Bei Schriftstücken auf Papier werden vertrauliche Passagen oft mit schwarzen Filzstiften übermalt. Die Originalinformation kann dabei oft schon wieder sichtbar gemacht werden, indem das Schriftstück gegen das Licht gehalten wird.
  - Das Pentagon hat im Mai 2005 einen Untersuchungsbericht im Internet veröffentlicht, in dem Personennamen und Informationen zur militärischen Lage im Irak unkenntlich gemacht worden waren. Aus der PDF-Datei ließen sich die geschwärzten Daten jedoch durch einfaches Kopieren und Einfügen über die Zwischenablage wieder sichtbar machen. Im ursprünglichen Word-Dokument hatte das Pentagon die Passagen nur mit einem schwarzen Hintergrund versehen. Beim PDF-Export blieb der darunterliegende Text jedoch erhalten.

# G 3.14 Fehleinschätzung der Rechtsverbindlichkeit eines Fax

Häufig wird versucht, bei eiligen Entscheidungen den Postweg einzusparen, indem wichtige Unterlagen oder Informationen an den Geschäftspartner per Fax übermittelt werden. Dabei wird oft außer Acht gelassen, dass so übermittelte Unterlagen in einem Streitfall nicht immer als rechtsverbindlich angesehen werden. Bestellungen müssen dann nicht vom Kunden angenommen, Zusagen nicht eingehalten werden. Eine Rechtsmittelfrist kann trotz rechtzeitigen Absendens eines Fax ablaufen.

# G 3.15 Fehlbedienung eines Anrufbeantworters

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind. Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu Sicherheitslücken, falls über die notwendigen Rechte hinaus weitere vergeben werden.

**Beispiel:**

Durch eine fehlerhafte Administration der Zugriffsrechte hat ein Sachbearbeiter die Möglichkeit, auf die Protokolldaten zuzugreifen. Durch gezieltes Löschen einzelner Einträge ist es ihm daher möglich, seine Manipulationsversuche am Rechner zu verschleiern, da sie in der Protokolldatei nicht mehr erscheinen.

# G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Arbeiten mehrere Benutzer an einem PC, so kann es aufgrund von Nachlässigkeit oder Bequemlichkeit dazu kommen, dass sich bei einem Wechsel der vorhergehende Benutzer nicht abmeldet und der neue sich nicht ordnungsgemäß anmeldet. Dies wird von den Betroffenen meist damit begründet, dass die Zeit, die das IT-System zum Neustarten benötigt, sehr lang ist und als nicht akzeptabel empfunden wird.

Dieses Fehlverhalten führt jedoch dazu, dass die Protokollierung von An- und Abmeldevorgängen und damit ein Teil der Beweissicherung unwirksam wird. Es lässt sich anhand der Protokolle nicht mehr zuverlässig feststellen, wer den Rechner zu einem bestimmten Zeitpunkt genutzt hat.

**Beispiele:**

- Ein PC wird abwechselnd von drei Benutzern eingesetzt, um Reisekostenabrechnungen durchzuführen. Nachdem der erste Benutzer den Anmeldevorgang durchgeführt hat, erfolgt kein ordnungsgemäßer PC-Benutzerwechsel mehr, weil die damit verbundenen Ab- und Anmeldevorgänge aus Bequemlichkeit nicht durchgeführt werden.
- Aufgrund von Unregelmäßigkeiten wird geprüft, wer welchen Vorgang am Rechner bearbeitet hat. Da nach Protokollierung nur ein Benutzer am PC gearbeitet hat, kann der Verursacher im Nachhinein nicht mehr festgestellt werden bzw. der einzige angemeldete Benutzer muss die Konsequenzen tragen.

# G 3.18 Freigabe von Verzeichnissen, Druckern oder der Ablagemappe

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 3.19 Speichern von Passwörtern unter WfW und Windows 95

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 3.20 Ungewollte Freigabe des Leserechtes bei Schedule+

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 3.21 Fehlbedienung von Codeschlössern

Erfahrungsgemäß führen Fehler in der Bedienung von mechanischen Codeschlössern verhältnismäßig oft dazu, dass der Schrank nicht mehr ordnungsgemäß geöffnet werden kann. Die Fehlbedienungen treten bei der Eingabe und besonders häufig bei der Änderung des Codes auf. Um die aufbewahrten Datenträger oder informationstechnischen Geräte wieder zugänglich zu machen, muss dann ein spezialisierter Schlüsseldienst beauftragt werden, so dass neben dem Schaden, der aus der fehlenden Verfügbarkeit der Datenträger oder Geräte entsteht, auch erhebliche Reparaturkosten anfallen können. Im ungünstigsten Falle muss ein neuer Schutzschrank beschafft werden.

# G 3.22 Fehlerhafte Änderung der Registrierung

Windows-Betriebssysteme bieten die Möglichkeit, die Benutzerumgebung eines IT-Systems global oder für jeden Benutzer individuell einzuschränken. Dies geschieht in der Regel unter Verwendung des Systemrichtlinieneditors *gpedit.msc* oder der Registrierungseditoren. Unter NT-basierten Windows-Versionen werden die Registrierungseditoren *regedt32.exe*, *regedit.exe, regini.exe* sowie die kommandozeilen-orientierten Werkzeuge *reg.exe* und seit Windows 7 die *PowerShell* eingesetzt, um die Registrierung zu bearbeiten.

Die Benutzung dieser Programme sollte mit Bedacht ausschließlich durch geschultes Personal erfolgen. Jede Änderung der Registrierung muss mit äußerster Sorgfalt durchgeführt werden, weil sehr schnell ein Systemzustand hergestellt werden kann, der ein Arbeiten mit dem IT-System nicht mehr erlaubt. Im ungünstigsten Fall müssen dann das Betriebssystem neu installiert oder bestimmte Hardware-Komponenten erneut initialisiert werden (durch Laden der entsprechenden Treiber).

Unter NT-basierten Windows-Versionen sind Registrierungseinträge durch Zugriffsrechte geschützt. Trotzdem kann ein Benutzer durch falsche Konfiguration der Zugriffsrechte die Registrierung wissentlich oder unwissentlich auf unerlaubte Weise modifizieren. Unsachgemäße Änderungen können zu Systemschäden führen, so dass die Sicherheit und/oder die Arbeitsfähigkeit des IT-Systems und im Extremfall des gesamten Netzes gefährdet ist.

# G 3.23 Fehlerhafte Administration eines DBMS

Wird ein Datenbankmanagementsystem (DBMS) nachlässig oder fehlerhaft administriert, kann dies folgende Gefährdungen nach sich ziehen:

- Verlust von Daten,
- (gezielte oder unbeabsichtigte) Datenmanipulation,
- unberechtigter Zugang zu vertraulichen Daten,
- Verlust der Datenbankintegrität,
- Crash der Datenbank und
- Zerstörung der Datenbank.

Die oben aufgeführten Gefährdungen können durch zu großzügig vergebene Rechte für die Benutzer, durch eine unregelmäßige oder gar keine Datenbank-überwachung, durch mangelhafte Datensicherungen, durch ungültige, aber noch nicht gesperrte Kennungen usw. hervorgerufen werden.

# G 3.24 Unbeabsichtigte Datenmanipulation

Je umfangreichere Zugriffsberechtigungen auf eine Datenbank für die Anwender bestehen, um so größer ist auch das Risiko einer unbeabsichtigten Datenmanipulation. Dies kann prinzipiell von keiner Anwendung verhindert werden. Die grundsätzlichen Ursachen für unbeabsichtigte Datenmanipulationen können z. B. sein:

- mangelhafte oder fehlende Fachkenntnisse,
- mangelhafte oder fehlende Kenntnisse der Anwendung,
- zu umfangreiche Zugriffsberechtigungen und
- Fahrlässigkeit (z. B. das Verlassen des Arbeitsplatzes ohne korrekte Beendigung der Anwendung).

# G 3.25 Fahrlässiges Löschen von Objekten

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 3.26 Ungewollte Freigabe des Dateisystems

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 3.27 Fehlerhafte Zeitsynchronisation

Wenn die Systemzeit auf IT-Systemen nicht korrekt synchronisiert wird, arbeitet jedes System mit einer anderen Uhrzeit. Dies kann zu Problemen für die korrekte Funktion oder die Verfügbarkeit von Systemen führen.

Dabei können die folgenden Probleme auftreten:

- Signifikante Zeitabweichungen zwischen IT-Systemen können dazu führen, dass die Kommunikation zwischen den Systemen aufgrund der abweichenden Zeitangaben in den Nachrichten des jeweils anderen Systems gestört, verzögert oder unmöglich gemacht wird.
- Ein übergreifendes Ereignis, wie die Ausbreitung von Schadsoftware über das Netz oder ein im Netz durchgeführter Portscan, hinterlässt auf den einzelnen Systemen Spuren (Protokolleinträge, Dateizugriffe) mit stark abweichenden Zeitangaben. Dadurch wird eine Aufklärung des Vorfalls massiv erschwert, weil die einzelnen Spuren nicht sicher zusammengeführt werden können.
- Bei der Aufklärung von Computerstraftaten kann der Beweiswert computerforensischer Spuren stark eingeschränkt werden, wenn die Korrektheit der Systemzeit nicht nachgewiesen werden kann.
- Bei zeitabhängigen Diensten wie Lizenzservern oder OCSP (Online Certificate Status Protocol)-Respondern kann eine falsche Systemzeit zu Fehlfunktionen des Dienstes führen, weil beispielsweise Lizenzen oder Zertifikate fälschlich als abgelaufen betrachtet werden.
- Kommt es in einem Netz, welches das Einzelreferenz-Verfahren zur Zeitsynchronisation nutzt, zum Ausfall der Zeitquelle, so ist keine Ersatzzeit mehr verfügbar. Dadurch können Datei- und Objektrechte unkontrolliert verändert werden.

# G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten

Durch eine ungeeignete Konfiguration aktiver Netzkomponenten kann es zu einem Verlust der Verfügbarkeit von Teilnetzen oder sogar des gesamten Netzes kommen. Des Weiteren können Konfigurationsfehler zu einem Verlust der Vertraulichkeit und Integrität der übertragenen Informationen führen. Dabei können insbesondere die folgenden Fehlkonfigurationen unterschieden werden:

- Aktive Netzkomponenten, die zur Bildung von VLANs (Virtual LANs) eingesetzt werden, segmentieren das Netz logisch. Im Fall einer Fehlkonfiguration kann unter Umständen die Kommunikation innerhalb eines VLANs, zwischen einzelnen oder zwischen allen VLANs zum Erliegen kommen.
  **Beispiel**: Ein Fileserver und ein Drucker befinden sich in demselben VLAN. Arbeitsplatzsysteme befinden sich in einem anderen VLAN. Damit die Arbeitsplatzsysteme mit dem Fileserver bzw. dem Drucker kommunizieren können, ist ein Schicht-3-Gerät (Router oder Multilayer Switch) erforderlich. Ist ein solches Gerät nicht vorhanden oder falsch konfiguriert, können die Arbeitsplatzsysteme weder auf Datei- noch auf Druckerdienste zugreifen.
- Ein Netz kann durch den Einsatz von Routern mittels Teilnetzbildung strukturiert werden. Für eine Kommunikation zwischen den Teilnetzen ist eine entsprechende Konfiguration der Router erforderlich, die hierzu die Leitwege zwischen den verschiedenen Teilnetzen in Routing-Tabellen vorhalten müssen. Routing-Tabellen können statisch oder dynamisch verwaltet werden. In beiden Fällen ist eine Kommunikation zwischen unterschiedlichen Teilnetzen nicht möglich, wenn die Routing-Tabellen keinen Leitweg zwischen den betreffenden Teilnetzen enthalten. Zu einer Fehlkonfiguration kann es dementsprechend durch eine fehlerhafte Definition statischer Routing-Tabellen oder durch eine fehlerhafte Konfiguration der Routing-Protokolle (wie z. B. RIP oder OSPF) kommen, die zum automatischen Abgleich dynamischer Routing-Tabellen verwendet werden.
  **Beispiel**: Eine Router-zu-Router-Verbindung ist durch einen statischen Eintrag der entsprechenden IP-Adressen konfiguriert. Bei einer Änderung der IP-Adresse einer der Router oder durch das Zwischenschalten eines weiteren Routers ist diese Kommunikationsstrecke nicht mehr verfügbar.
- Aktive Netzkomponenten können, wenn sie entsprechend konfiguriert sind, bestimmte Protokolle sperren oder eine Kommunikation zwischen IT-Systemen mit bestimmten Netzadressen verhindern. Eine Fehlkonfiguration der betreffenden Filter kann entsprechend zu einer unerwünschten Unterbindung der Kommunikation führen.
  Ebenso können fehlkonfigurierte Filter dazu führen, dass Verbindungen aufgebaut werden, die Unbefugten die Möglichkeit bieten, Angriffe gegen IT-Systeme im geschützten Netz durchzuführen. Je nach Art des Angriffs kann daraus ein Verlust der Verfügbarkeit einzelner Netzkomponenten oder sogar des ganzen Netzes resultieren. Weiterhin können Datenpakete umgeleitet, verändert oder mitgelesen werden, wenn die Verbindundungswege manipuliert werden.
  **Beispiel:**Durch eine ungeeignete Konfiguration von aktiven Netzkomponenten (insbesondere von VLANs oder Filterregeln) können Broadcast-Domänen unnötig groß werden oder es können unnötige Kommunikationsverbindungen entstehen. Dadurch kann es Unbefugten möglich sein, vertrauliche Daten zu lesen.

# G 3.29 Fehlende oder ungeeignete Segmentierung

Lokale Netze können physisch durch aktive Netzkomponenten oder logisch durch eine entsprechende VLAN-Konfiguration segmentiert werden. Dabei werden die angeschlossenen IT-Systeme eines Netzes auf verschiedene Segmente verteilt. Dies verbessert die Lastverteilung innerhalb des Netzes und erhöht dessen Administrierbarkeit.

Dabei kann es zu folgenden konkreten Gefährdungen kommen:

- Verlust der Verfügbarkeit
  Eine hohe Anzahl von IT-Systemen innerhalb eines Schicht-2-Segments bringt auch eine hohe Netzlast in dem entsprechenden Segment mit sich. Dies kann dessen Verfügbarkeit stark beeinträchtigen und sogar zu dessen Überlastung bzw. Ausfall führen. Eine ungeeignete Segmentierung kann auch dann vorliegen, wenn Systeme durch aktive Netzkomponenten der Schicht 2 oder 3 getrennt werden, die sehr viel miteinander kommunizieren.
- Kein ausreichender Schutz der Vertraulichkeit
  Um vertrauliche Informationen zu schützen, sollten nur die berechtigten Benutzer darauf zugreifen dürfen. Broadcast-Domänen sind daher auf das unbedingt notwendige Maß zu beschränken. Wurden die einzelnen Segmente jedoch ungeeignet konfiguriert, können Unbefugte die übertragenen vertraulichen Informationen mitlesen und auswerten.

**Beispiel:**

- Zwei IT-Systeme, die große Datenmengen austauschen, sind durch einen Router getrennt. Handelt es sich hierbei um einen langsamen Router, kann dies eine ungeeignete Segmentierung darstellen, da der Datenverkehr durch einen relativ langsamen Router geführt werden muss.

# G 3.30 Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im häuslichen Bereich ist es einfacher, den dienstlichen Telearbeitsrechner privat zu nutzen, weil Kontrollen durch den Arbeitgeber nur bedingt möglich sind. Es besteht die Gefahr, dass nicht geprüfte und freigegebene Software eingesetzt wird und durch unbedachtes Handeln Computer-Viren und andere Schadsoftware auf den Telearbeitsrechner gelangen. Dadurch könnten beispielsweise vertrauliche Daten kompromittiert werden. Diese unsachgemäße Nutzung des Telearbeitsrechners kann nicht nur durch den Telearbeiter selbst, sondern auch durch Angehörige oder Besucher erfolgen. Insbesondere Kinder und Jugendliche können versucht sein, den Telearbeitsrechner zu Spielzwecken zu verwenden, teilweise sogar, ohne dass der Telearbeiter davon Kenntnis hat. Mögliche Schäden sind beispielsweise: gelöschte Festplatten mit Totalverlust der Daten, Reinstallationskosten oder Nacherfassungsarbeiten.

Ebenso besteht die Möglichkeit über den Telearbeitsplatzrechner auf die vielfältigen Ressourcen des LANs der Institution zuzugreifen. Wenn Unbefugte den Telearbeitsrechner nutzen, könnten dadurch auch im LAN angebotene Dienste wie beispielsweise Fax-Gateway, Internet-Anbindung usw. missbraucht werden. Außerdem besteht dabei immer auch das Risiko des Daten- und Programmdiebstahls.

# G 3.31 Unstrukturierte Datenhaltung

Durch unzureichende Vorgaben und/oder fehlende Schulung der Mitarbeiter kann es zu einer unübersichtlichen Speicherung der Daten auf den benutzten Datenträgern kommen. Dadurch kann es zu verschiedenen Problemen kommen wie:

- Speicherplatzverschwendung durch mehrfache Speicherung von Dateien,
- vorschnelle Löschung oder nicht erfolgte Löschung von Daten, da keiner mehr weiß, was in welchen Dateien gespeichert ist,
- unbefugte Zugriffe, wenn sich Dateien in Verzeichnisse oder auf Datenträgern befinden, die Dritten zugänglich gemacht werden, oder
- nicht konsistente Versionsstände in verschiedenen Verzeichnen und IT-Systemen.

**Beispiel:**

Es wurde unterlassen, einen neuen Mitarbeiter mit wenig IT-Erfahrung in die strukturierte Datenhaltung einzuweisen. Bereits nach kurzer Zeit traten Probleme auf, weil der Benutzer alle Dateien im Hauptverzeichnis gespeichert hatte, ohne auch nur ein Unterverzeichnis anzulegen.

# G 3.32 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Dies kann dazu führen, dass bei der Übermittlung verschlüsselter Datensätze in solche Länder die Empfänger diese nicht lesen können, da sie die benötigten Kryptomodule nicht einsetzen können, oder sich vielleicht sogar strafbar machen.

Außerdem ist in sehr vielen Ländern auch der Export von Produkten mit starker Kryptographie erheblich eingeschränkt. Hier sind insbesondere die USA zu nennen. Bei Exportrestriktionen wird häufig die Stärke von an sich starken Verschlüsselungsprodukten künstlich (durch Reduzierung der Schlüsselmannigfaltigkeit) herabgesetzt. Solche künstlich geschwächten Verfahren bieten teilweise nicht einmal für mittleren Schutzbedarf ausreichenden Schutz. Dies gilt z. B. für aus den USA stammende PC-Standardsoftware wie Internet-Browser (SSL), in denen nur eine reduzierte Schlüssellänge von 40 Bit eingesetzt wird. Teilweise erfordern die Exportregelungen aber auch, dass Teile der Schlüssel hinterlegt werden, so dass die Kryptomodule zwar im Prinzip uneingeschränkt nutzbar sind, aber für die ausländischen Nachrichtendienste eine Zugriffsmöglichkeit im Bedarfsfall bleibt.

Auf der anderen Seite können solche Einschränkungen, die beim Einsatz innerhalb mancher Länder bzw. beim Export gelten, dazu verleiten, schützenswerte Daten unverschlüsselt zu lassen oder mit minderwertigen Kryptoprodukten zu schützen. Dies kann zum einen Angreifern Tür und Tor öffnen und zum anderen auch zum Verstoß gegen nationales Recht führen. So kann durch Datenschutzgesetze der Einsatz adäquater kryptographischer Verfahren zum Schutz personenbezogener Daten vorgeschrieben sein.

# G 3.33 Fehlbedienung von Kryptomodulen

Die Fehlbedienung von Kryptomodulen hat in der Praxis schon öfter zu Schäden geführt. Diese Fehlbedienung kann verschiedene Auswirkungen haben:

- Daten werden unverschlüsselt übertragen, weil versehentlich der Klartext-Modus im Kryptomodul aktiviert wurde.
- Bei der Eingabe von kryptographischen Schlüsseln werden Schlüsselteile falsch eingegeben. Die Folge ist, dass weder der Sender (dem die Falscheingabe nicht aufgefallen ist) noch der Empfänger (der den wirklich verwendeten Schlüssel nicht kennen kann) die mit dem falsch eingegebenen Schlüssel chiffrierten Daten korrekt entschlüsseln können.
- Während des Verschlüsselungsvorgangs wird die Stromzufuhr des Kryptomoduls versehentlich ausgeschaltet. Dies hat zur Folge, dass nur Teile der Daten verschlüsselt vorliegen, andere Teile unverschlüsselt. In einem solchen Fall ist es möglich, dass eine Entschlüsselung nicht mehr möglich ist, weil der Vorgang unkontrolliert abgebrochen wurde.
- Bei Eingabe von Verschlüsselungsparametern werden falsche Parameter eingegeben. Dies kann zur Folge haben, dass nicht ausreichend sichere Kryptoalgorithmen oder unsichere kryptographische Schlüssel verwendet werden.
- Wird der Anwender bei der Schlüsselerzeugung beteiligt, in dem er bei der Generierung des Schlüssels zur Eingabe von zufälligen Zeichen aufgefordert wird, besteht eine Fehlbedienung auch darin, an dieser Stelle keine zufälligen Zeichen, sondern bekannte oder leicht erratbare Zeichenketten (Worte) zu verwenden.

Derlei Fehlbedienungen eines Kryptomoduls können dazu führen, dass die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten beeinträchtigt wird. Als Beispiele seien genannt:

- Daten werden nicht oder nicht mehr verschlüsselt, obwohl die Verschlüsselung zur Wahrung der Vertraulichkeit erforderlich wäre.
- Verschlüsselte Daten können nicht mehr entschlüsselt werden, weil durch die Fehlbedienung eine ordnungsgemäße Nutzung des Kryptomoduls nicht mehr möglich ist.
- Daten werden ungewollt oder absichtlich in einer Weise verschlüsselt, die nicht mehr rekonstruierbar ist, weil der notwendige kryptographische Schlüssel unbekannt ist.
- Korrekt verschlüsselte Daten werden verändert, so dass die Daten dann nicht mehr entschlüsselbar sind.

# G 3.34 Ungeeignete Konfiguration des Managementsystems

Für den sicheren Einsatz eines Netz- und/oder Systemmanagement-Systems ist eine konsistente Konfiguration aller beteiligten Komponenten nötig. Zwar werden die einzelnen Komponenten in der Regel von einer zentralen Instanz aus verwaltet (Manager), das Managementsystem besteht jedoch aus vielen Einzelkomponenten, die auf die zu verwaltenden Netz- und Systemkomponenten verteilt sind (Agenten). Eine konsistente Konfiguration eines solchen Systems lässt sich in zwei Bereiche unterteilen:

- Einerseits müssen die mit Hilfe des Managementsystems eingestellten Konfigurationen der Netz- und Systemkomponenten (z. B. Server, Router) insgesamt konsistent sein.
- Andererseits muss auch die Managementsoftware selbst konsistent konfiguriert werden.

Wird beabsichtigt oder unbeabsichtigt die Konsistenz der Konfigurationen verletzt, so arbeiten die Komponenten nicht mehr reibungslos zusammen, was zu Sicherheitsproblemen führen kann. Beispielsweise könnte ein Server oder Router nicht mehr zugreifbar oder Zugriffsrechte zu offen gesetzt sein (siehe auch G 3.38 *Konfigurations- und Bedienungsfehler*).

# G 3.35 Server im laufenden Betrieb ausschalten

Wird ein Netz durch ein Managementsystem verwaltet, so existieren (insbesondere im Bereich Systemmanagement) Server mit Sonderaufgaben. Auf den so genannten Managementservern werden in der Regel Datenbanken mit Managementinformationen gehalten. Werden solche Server im laufenden Betrieb einfach ausgeschaltet, so werden z. B. die im Speicher des Rechners gehaltenen Daten nicht mehr auf das Dateisystem geschrieben. Dies hat zur Folge, dass beim nächsten Start der Maschine Inkonsistenzen auch in den Managementdaten existieren können. Große Managementsysteme benutzen deshalb in der Regel Datenbanken, die durch den Einsatz so genannter Transaktionsmechanismen dafür sorgen, dass die Informationen in einen (alten) konsistenten Zustand zurückversetzt werden können. Dies verringert die Gefahr, kann sie jedoch nicht vollständig beseitigen und kann sogar zum Angriff genutzt werden (Ausnutzen einer alten Konfiguration mit weniger restriktiven Zugriffsrechten).

Auch bei der elektronischen Archivierung kann es zu Fehlern kommen, wenn das Archivsystem vollständig oder in Teilen im laufenden Betrieb abgeschaltet wird. Ein Abschalten kann dazu führen, dass Dokumente als archiviert gelten, tatsächlich aber nur unvollständig oder gar nicht auf das Speichermedium geschrieben worden sind und daher nicht mehr reproduziert werden können.

# G 3.36 Fehlinterpretation von Ereignissen

Beim Einsatz eines Managementsystems ist es eine Aufgabe des jeweils verantwortlichen Systemadministrators, die Meldungen des Managementsystems zu analysieren und zu interpretieren, um dann geeignete Maßnahmen einzuleiten. In der Regel basieren die Meldungen des Managementsystems auf Überwachungsmechanismen, die Systemprotokolle unterschiedlichster Art automatisch nach gewissen Regeln durchsuchen. Es ist dabei nicht einfach, aus der Fülle der anfallenden Protokolldaten automatisiert Anomalien, die auf Systemfehler hindeuten, zu erkennen und entsprechende Meldungen an den Systemadministrator zu erzeugen. Darüber hinaus kann ein Fehler hier sogar unentdeckt bleiben. Die eingehenden Meldungen müssen daher immer vom Systemadministrator gesichtet und interpretiert werden, da die Meldungen (im Fehlerfall) auf Fehlersymptome und deren (automatischer) Interpretation beruhen. Ein Systemadministrator muss hier auch Fehlalarme und Falschmeldungen erkennen können. Werden Systemmeldungen vom Administrator falsch interpretiert, so führen vermeintlich korrigierende Gegenmaßnahmen u. U. zu einer Verschlimmerung der Situation.

# G 3.37 Unproduktive Suchzeiten

Im Internet werden Millionen von Informationsseiten, Dokumenten und Dateien angeboten. Zum Navigieren in diesem riesigen Informationsangebot wird eine durch einfachen Mausklick zu bedienende Querverweistechnik verwendet. Sie erlaubt den schnellen Wechsel auf weiterführende Informationsseiten, die ihrerseits wieder neue Querverweise auf weitere Seiten beinhalten. Das Springen über Querverweise von einer Informationsseite zu weiteren wird als "Surfen" bezeichnet und kann zu sehr langen Suchzeiten führen.

In vielen Organisationen wurden Internet-Dienste eingeführt, ohne die damit verbundenen Ziele und erwarteten Auswirkungen vorher konkret zu untersuchen. Die Schulungen und Hilfen für die Benutzer sind häufig nicht ausreichend, so dass es zu unproduktiven Suchzeiten im vielfältigen Angebot des Internets kommt. Die Kosten für diese Abfragen sind oft weder den Benutzern noch den Verantwortlichen bekannt. Nach Schätzung einer Unternehmensberatung entstehen durch Surfen sowie unnötige und langatmige Recherchen im Internet vermeidbare Personal- und Kommunikationskosten in mehrstelliger Millionenhöhe je Jahr.

# G 3.38 Konfigurations- und Bedienungsfehler

Konfigurationsfehler entstehen durch eine falsche oder nicht vollständige Einstellung von Parametern und Optionen, mit denen ein Programm gestartet wird. In diese Gruppe fallen unter anderem falsch gesetzte Zugriffsrechte für Dateien. Bei Bedienungsfehlern sind nicht einzelne Einstellungen falsch, sondern die IT-Systeme oder IT-Anwendungen werden falsch behandelt. Ein Beispiel hierfür ist das Starten von Programmen, die für den Einsatzzweck des Rechners nicht notwendig sind, aber von einem Angreifer missbraucht werden können.

Beispiele für aktuelle Konfigurations- bzw. Bedienungsfehler sind das Speichern von Passwörtern auf einem PC, auf dem ungeprüfte Software aus dem Internet ausgeführt wird, oder das Laden und Ausführen von schadhaften ActiveX-Controls. Diese Programme, die unter anderem, die Aufgabe haben, Webseiten durch dynamische Inhalte attraktiver zu machen, werden mit den gleichen Rechten ausgeführt, die auch der Benutzer hat. Sie können beliebig Daten löschen, verändern oder versenden.

Viele Programme, die für die ungehinderte Weitergabe von Informationen in einem offenen Umfeld gedacht waren, können bei falscher Konfiguration potenziellen Angreifern Daten zu Missbrauchszwecken liefern. So kann beispielsweise der *finger*-Dienst darüber informieren, wie lange ein Benutzer bereits am Rechner sitzt. Aber auch Browser übermitteln bei jeder Abfrage einer Datei eine Reihe von Informationen an den Webserver (z. B. die Version des Browsers und des verwendeten Betriebssystems, den Namen und die Internet-Adresse des PCs). In diesem Zusammenhang sind auch die Cookies zu nennen. Hierbei handelt es sich um Dateien, in denen Webserver-Betreiber Daten über den Benutzer auf dessen Rechner speichern. Diese Daten können beim nächsten Besuch des Servers abgerufen und vom Server-Betreiber für eine Analyse, der vom Benutzer vorher auf dem Server besuchten Webseiten, verwendet werden.

Der Einsatz eines Domain Name Systems stellt eine weitere Gefahrenquelle dar. Zum einen ermöglicht ein falsch konfigurierter DNS-Server die Abfrage von vielen Informationen über ein lokales Netz. Zum anderen hat ein Angreifer durch die Übernahme dieses Servers die Möglichkeit, gefälschte IP-Adressen zu verschicken, sodass jeglicher Verkehr von ihm kontrolliert werden kann.

Eine große Bedrohung geht auch von den automatisch ausführbaren Inhalten (*Executable Content*) in E-Mails oder HTML-Seiten aus. Dies ist unter dem Stichwort Content-Security-Problem bekannt. Dateien, die aus dem Internet geholt werden, können Code enthalten, der bereits beim "Betrachten" und ohne Rückfrage beim Benutzer ausgeführt wird. Dies ist z. B. bei Makros in Office-Dateien der Fall und wurde zum Erstellen von sogenannten Makro-Viren ausgenutzt. Auch Programmiersprachen und -schnittstellen wie ActiveX, Javascript oder Java, die für Anwendungen im Internet entwickelt worden sind, besitzen bei falscher Implementierung der Kontrollfunktionen ein Schadpotenzial.

Die Verfügbarkeit des Sicherheitssystems RACF ist bei z/OS-Betriebssystemen von zentraler Bedeutung für die Verfügbarkeit des gesamten Systems. Durch unsachgemäßen Einsatz von z/OS-Utilities bei der RACF-Datenbanksicherung oder fehlerhafte Bedienung der RACF-Kommandos kann diese eingeschränkt werden.

# G 3.39 Fehlerhafte Administration des RAS-Systems

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in G 3.90 *Fehlerhafte Administration von VPNs* integriert.

# G 3.40 Ungeeignete Nutzung von Authentisierungsdiensten bei VPNs

Die Identität der VPN-Benutzer, die sich über ein Remote-Access-VPN ins LAN einwählen möchten, muss beim Verbindungsaufbau festgestellt werden. Dazu werden typischerweise Authentisierungsmechanismen verwendet, die auf einer Benutzerverwaltung mit gespeicherten Authentisierungsdaten beruhen. Virtuelle Private Netze (VPNs) bieten für die Speicherung der Benutzerdaten meist mehrere Möglichkeiten an: eine eigene Benutzerverwaltung, die Verwendung der Benutzerverwaltung des Betriebssystems und die Verwendung von Authentisierungsservern (mit eigener Benutzerverwaltung). Werden getrennte Benutzerverwaltungen für VPN und Betriebssystem verwendet, so kann es zum Beispiel aufgrund von organisatorischen Mängeln zu Inkonsistenzen in den beiden Datenbeständen kommen. Als Folge kann dies zu unerlaubten Verbindungsaufnahmen und unberechtigten Zugriffen auf Daten führen.

Viele VPN-Clients für den Remote Access erlauben es, die zur Authentisierung notwendigen Daten nach einmaliger Eingabe lokal zu speichern, so dass beim erneuten Verbindungsaufbau die Eingabe der Daten durch den Benutzer nicht mehr erforderlich ist. Dies birgt jedoch ein hohes Gefahrenpotential für den Fall, dass der VPN-Client einem unberechtigten Zugriff ausgesetzt ist. Der Authentisierungsmechanismus kann seine Aufgabe dann nicht mehr erfüllen. Dadurch können Unbefugte unter Umständen auf die lokalen Netze zugreifen, die über eine VPN-Verbindung von dem entsprechenden Client aus erreichbar sind. Die Sicherheit dieser lokalen Netze ist somit gefährdet.

**Beispiel:**

- Beim Weggang eines Mitarbeiters wird das Benutzerkonto in der VPN-Benutzerverwaltung nicht gelöscht. Der ehemalige Mitarbeiter kann sich daher immer noch über den VPN-Zugang einwählen und auf allgemein zugängliche Daten zugreifen. Der Zugang könnte nun auch dazu benutzt werden, schwerwiegende Angriffe durchzuführen.

# G 3.41 Fehlverhalten bei der Nutzung von VPN-Diensten

Durch Unkenntnis oder (meist unbewusstes) Fehlverhalten kann es bei der VPN-Nutzung bzw. im Umfeld der VPN-Nutzung zu Sicherheitsproblemen kommen, beispielsweise zu Verstößen gegen die Sicherheitsrichtlinien oder zu sicherheitsrelevanten Fehlkonfigurationen. Diese Gefahr besteht besonders, wenn die Anwender nicht ausreichend geschult sind.

Oftmals werden stationäre und mobile IT-Systeme, auf denen VPN-Client-Software installiert ist, nicht nur zum Zugriff auf ein LAN benutzt. Insbesondere wenn die VPN-Verbindung über das Internet aufgebaut wird, erfolgt oft auch die Internet- und E-Mail-Nutzung über diese IT-Systeme. In manchen Fällen wird auf fremde Netze zugegriffen, beispielsweise wenn Außendienstmitarbeiter mit mobilen VPN-Clients spezielle Verbindungen zu Kundennetzen aufbauen. Dadurch können sich folgende Sicherheitsprobleme ergeben:

- Durch den (versuchten) Aufbau nicht genehmigter Verbindungen wird das System unnötig belastet, da die Zulässigkeit der Verbindung überprüft werden muss. Auf diese Weise werden Systemressourcen belegt. In Kombination mit Fehlkonfigurationen kann es auch dazu kommen, dass unberechtigte Zugriffe erfolgreich durchgeführt werden.
- VPN-Clients können unter anderem für den Internet-Zugang eingesetzt werden. Bei Verbindungen mit dem Internet ohne besondere Sicherheitsvorkehrungen kann unter Umständen auch von außen auf den Client-Rechner zugegriffen werden. Ein Angreifer kann dann versuchen, beispielsweise die Datenverschlüsselung abzuschalten oder andere VPN-Konfigurationsdaten so zu verändern, dass die VPN-Kommunikation nicht mehr sicher ist. Software, die aus dem Internet geladen und auf dem VPN-Client abgespeichert wurde, enthält eventuell schädlichen Code, wie beispielsweise Viren oder Trojanische Pferde.
- In fremden LANs, wie z. B. Kundennetzen oder privaten Heimnetzen, bestehen oftmals weitere Verbindungen zu anderen Netzen, beispielsweise zum Internet. Meldet sich nun ein VPN-Client an einem solchen Netz an, kann je nach Sicherheitsvorgaben der LAN-Verwaltung möglicherweise unkontrolliert auf den VPN-Client zugegriffen werden (siehe auch G 5.39 *Eindringen in Rechnersysteme über Kommunikationskarten*).

**Beispiel:**

- Auf einer Dienstreise verbindet sich ein Mitarbeiter über Internet mit dem Firmennetz. Vor dem VPN-Verbindungsaufbau lädt er eine ausführbare Datei von einem Webserver. Die Datei enthält neben der "offiziellen" Funktionalität auch noch einen schädlichen Programmteil, der versucht, in der VPN-Konfiguration die Sicherheitsmechanismen (z. B. Abschalten der Verschlüsselung) zu beeinflussen. Als Folge kann bei bestehender VPN-Verbindung von Unbefugten auf Daten im Firmennetz zugegriffen werden.

# G 3.42 Unsichere Konfiguration der VPN-Clients für den Fernzugriff

Die Sicherheit eines Virtuellen Privaten Netzes (VPNs) hängt sowohl von der sicheren Konfiguration der VPN-Server und der VPN-Clients, als auch von der korrekten Nutzung der angebotenen Sicherheitsmechanismen ab.

Unterliegt die Konfiguration des Servers noch der vollständigen Kontrolle eines Administrators, so werden besonders bei Remote-Access-VPNs die Clients häufig außerhalb der Behörde bzw. des Unternehmens eingesetzt. Damit kann der Client nur noch lose in administrative Abläufe eingegliedert werden. Insbesondere beim Einsatz mobiler VPN-Clients können Benutzer auch mit gewissen administrativen Rechten ausgestattet sein, um Probleme beim VPN-Zugang durch Ändern von VPN-Konfigurationsparametern selbst oder unter telefonischer Anleitung zu beheben.

Generell ergibt sich durch die eingeschränkten Kontrollmöglichkeiten der Systemadministration die Gefahr, dass VPN-Clients unsicher konfiguriert sind. Beispiele hierfür sind:

- Problematisch ist es, wenn Benutzer nicht zugelassene Software auf dem VPN-Client installieren, da diese Sicherheitslücken aufweisen kann bzw. Computer-Viren oder Trojanische Pferde eingeschleppt werden können.
- Die vorhandenen Sicherheitsmechanismen für den VPN-Zugang werden vom Benutzer in vielen Fällen nicht oder nicht korrekt eingestellt.

In der Regel ist es möglich, ein Virtuelles Privates Netz (VPN) so zu konfigurieren (Client und/oder Server), dass schwache oder keine Sicherheitsmechanismen zum Einsatz kommen. Die zur Datenverschlüsselung eingesetzten Mechanismen zum Verbindungsaufbau werden beispielsweise bei der Nutzung von IPSec oder SSL dynamisch zwischen Client und Server ausgehandelt. Während der Verhandlung bietet der Client dem Server eine Liste von unterstützen Verfahren, den so genannten Cipher-Suites, zur Auswahl an, aus denen sich der Server eines auswählt. Die Liste der verwendbaren Verfahren kann durch entsprechende Konfiguration verändert werden. Meist ist auch die Option "keine Verschlüsselung" möglich.

Wird die unverschlüsselte Verbindungsaufnahme im Rahmen der Konfiguration nicht unterbunden, besteht prinzipiell die Gefahr, dass die Daten bei der Übertragung nicht geschützt werden. Dies betrifft insbesondere VPN-Clients, bei denen die Benutzer die Möglichkeit haben, die Konfiguration des VPNs bei Problemen an die lokalen Gegebenheiten anzupassen.

**Beispiel:**

- Eine Institution hat festgelegt, dass die Absicherung der VPN-Kommunikation mittels IPSec erfolgen soll. Auf dem VPN-Server ist eingestellt, dass die IPSec-Verschlüsselung angefordert, jedoch nicht erzwungen wird. Dadurch können die VPN-Clients auch potenziell ungesicherte Verbindungen aufbauen. Einem VPN-Benutzer erscheinen die mit der Verschlüsselung einhergehenden Leistungseinbußen auf seinem älteren Laptop nicht akzeptabel. Daher schaltet er die IPSec-Verschlüsselung ab. Die VPN-Verbindung wird nun unverschlüsselt aufgebaut.

# G 3.43 Ungeeigneter Umgang mit Passwörtern oder anderen Authentikationsmechanismen

Selbst die Nutzung von durchdachten Authentikationsverfahren hilft wenig, wenn die Benutzer nicht sorgfältig mit den benötigten Zugangsmitteln umgehen. Unabhängig davon, ob Passwörter, PINs oder Authentikationstoken eingesetzt werden, werden diese immer wieder weitergegeben oder unsicher aufbewahrt.

Benutzer geben oft aus Bequemlichkeit Passwörter an andere Benutzer weiter. Häufig werden Passwörter innerhalb von Arbeitsgruppen geteilt, um jedem Mitarbeiter den Zugriff auf gemeinsam zu bearbeitende Dateien zu erleichtern. Der Zwang zur Passwortbenutzung wird oft als lästig empfunden und dadurch unterlaufen, dass Passwörter nie gewechselt werden oder alle Mitarbeiter dasselbe Passwort benutzen.

Immer wieder finden sich IT-Systeme und Anwendungen, bei denen die vom Hersteller voreingestellten Passwörter nicht geändert wurden. Häufig betrifft dies sogar die Administrator-Passwörter, die nicht geändert wurden, um sie nicht vergessen zu können. Standard-Passwörter sind jedoch allgemein bekannt und stellen damit ein hohes Sicherheitsrisiko dar.

Wird zur Benutzer-Authentisierung ein Token-basiertes Verfahren eingesetzt (z. B. Chipkarte oder Einmalpasswortgenerator), so ergibt sich bei Verlust die Gefahr, dass das Token unberechtigt verwendet wird. Ein unberechtigter Benutzer kann mit diesem Token unter Umständen erfolgreich eine Remote-Access-Verbindung aufbauen.

Wegen der Vielzahl verschiedener Passwörter und PINs können sich Benutzer diese oftmals nicht alle merken. Daher werden Passwörter immer wieder vergessen, was teilweise zu hohem Aufwand führt, um mit dem System weiterarbeiten zu können. Authentikationstoken können ebenso verloren werden. Bei sehr sicheren IT-Systemen kann der Verlust von Passwörtern oder Token sogar dazu führen, dass alle Benutzerdaten verloren sind.

Passwörter werden oft notiert, damit sie nicht vergessen werden. Dies ist solange kein Problem, wie sie sorgfältig, also vor unbefugtem Zugriff geschützt, aufbewahrt werden. Dies ist nicht immer der Fall. Ein klassisches Beispiel ist das Passwort unter der Tastatur oder auf einem Klebezettel am Bildschirm. Auch Authentikationstoken finden sich oft unter der Tastatur.

Ein anderer Trick, um Passwörter nicht zu vergessen, ist die "geeignete" Auswahl. Wenn Benutzer Passwörter selber auswählen können und nicht ausreichend für die Probleme hierbei sensibilisiert sind, werden in vielen Fällen Trivialpasswörter wie "4711" oder Namen von Freunden gewählt.

**Beispiele:**

- In einem Unternehmen wurde bei Stichproben festgestellt, dass viele Passwörter zu schlecht gewählt bzw. zu selten gewechselt wurden. Es wurde technisch erzwungen, dass die Passwörter monatlich gewechselt wurden und außerdem Zahlen oder Sonderzeichen enthalten mussten. Es stellte sich heraus, dass ein Administrator seine Passwörter wie folgt auswählte:
  Januar-2008, Februar-2008, Maerz-2008,

Diese Passwörter entsprachen zwar den Vorgaben, waren aber leicht zu erraten.

- In einer Behörde zeigte sich, dass einige der Benutzer, die ihre Büros zur Straßenseite hatten, dasselbe Passwort benutzten: den Namen des gegenüberliegenden Hotels, der in großen Leuchtbuchstaben die Aussicht dominierte.

# G 3.44 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass in Institutionen zwar eine Vielzahl von organisatorischen und technischen Sicherheitsverfahren vorhanden sind, diese jedoch durch den sorglosen Umgang mit den Vorgaben und der Technik wieder ausgehebelt werden. Ein typisches Beispiel hierfür sind die fast schon sprichwörtlichen Zettel am Monitor, auf denen Zugangspasswörter notiert sind. Auch andere Beispiele für Nachlässigkeit, Pflichtvergessenheit oder Leichtsinn im Umgang mit schützenswerten Informationen finden sich in großer Menge.

**Beispiele:**

- In der Bahn oder im Restaurant geben Mitarbeiter oft intimste Unternehmensdetails über ihr Mobiltelefon weiter. Dabei informieren sie jedoch nicht nur den Gesprächspartner, sondern auch die Umgebung. Beispiele für besonders interessante Interna sind,
  - warum der Vertrag mit einer anderen Firma nicht zustande kam oder
  - wie viele Millionen der Planungsfehler in der Strategie-Abteilung gekostet hat und wie das die Aktienkurse des Unternehmens drücken könnte, wenn irgendjemand davon erführe.
- Häufig ist es bei Dienstreisen erforderlich, ein Notebook, einen Organizer oder andere mobile Datenträger mitzunehmen. Immer wieder ist zu beobachten, dass diese während Pausen unbeaufsichtigt im Besprechungsraum, im Zugabteil oder im Auto zurückgelassen werden. Bei mobilen IT-Systemen sind die damit erfassten Daten oftmals nicht an anderer Stelle gesichert. Werden die IT-Systeme gestohlen, sind die Daten ebenfalls verloren. Dazu kommt, dass sich brisante Informationen auch gewinnbringend weiter veräußern lassen, wenn der Dieb aufgrund fehlender Verschlüsselung oder eines nur unzureichenden Zugriffsschutzes einfach darauf zugreifen kann.
- Ein Grund, ein Notebook oder Akten auf Dienstreisen mitzunehmen, ist auch, die Fahrzeiten produktiv nutzen zu können. Hierbei bieten sich Mitreisenden oft interessante Einblicke, da es in der Bahn oder im Flugzeug kaum zu vermeiden ist, dass Sitznachbarn in den Unterlagen oder auf dem Bildschirm mitlesen können.
  Öffentliche Räumlichkeiten, z. B. Hotel-Foyer, Hotel-Business-Center, Zug-Abteil, bieten in der Regel nur wenig Sichtschutz. Gibt der Benutzer Passwörter ein oder muss Veränderungen an den Konfigurationen vornehmen, so kann ein Angreifer ohne größeren Aufwand an diese Informationen gelangen und sie missbräuchlich nutzen.
- In jüngerer Zeit werden E-Mails häufig von einem Mobiltelefon oder Smartphone abgerufen, da die Zeit, um das Notebook zu starten, als zu lang empfunden wird oder weil in einem vollen Zug gerade kein Platz für das Notebook ist. Mobiltelefone und Smartphones besitzen jedoch viel seltener Sichtschutzfolien, sodass vertrauliche E-Mails von Personen in der Umgebung unbemerkt mitgelesen werden können.
- Immer wieder sind in der Presse Artikel über Behörden und Unternehmen zu finden, in deren Hinterhöfen sich hochbrisante Papiere im Altpapiercontainer fanden. Bekannt wurden auf diese Weise beispielsweise die Gehaltszahlen aller Mitarbeiter eines Unternehmens und die geheimen Telefonnummern von Unternehmensvorständen.
- Wenn IT-Systeme Defekte aufweisen, werden diese schnell zur Reparatur gegeben. Meist besteht bei einem Defekt auch keine Möglichkeit mehr, die auf dem betroffenen IT-System gespeicherten Daten zuverlässig zu löschen. Gelegentlich bieten Fachhändler ein funktionsfähiges Austausch-

gerät an. Es hat allerdings diverse Fälle gegeben, bei denen der Kundendienst den Fehler bei einer anschließenden Überprüfung schnell beheben konnte und der nächste Kunde ebenso kulant das jetzt reparierte Gerät erhielt inklusive aller vom ersten Kunden erfassten Daten.

# G 3.45 Unzureichende Identifikationsprüfung von Kommunikationspartnern

In persönlichen Gesprächen, am Telefon oder auch in E-Mails sind viele Personen bereit, weit mehr Informationen preiszugeben, als sie das in schriftlicher Form oder in größerer Runde tun würden. Hierbei wird häufig vom Kommunikationspartner stillschweigend erwartet, dass die Gesprächs- oder E-Mail-Inhalte vertraulich behandelt werden. Darüber hinaus besteht die Neigung, die Identität des Kommunikationspartners nicht zu hinterfragen, da dies als unhöflich empfunden wird. Dies gilt auch für weitere Nachfragen zum Grund des Anrufes oder dem Auftraggeber ("Ich arbeite für die XY-Bank und benötige noch einige detaillierte Angaben zu ihren Einkommensverhältnissen."). Solche Verhaltensweisen werden auch beim "Social Engineering" ausgenutzt (siehe auch G 5.42 *Social Engineering*).

**Beispiel:**

Es sind viele Fälle bekannt, in denen Journalisten Prominente angerufen und sich als andere Prominente ausgegeben haben. Damit gelang es ihnen, den Prominenten Aussagen zu entlocken, die nicht für die Öffentlichkeit bestimmt waren. Dies war besonders brisant bei einigen Direktübertragungen im Radio, bei denen auch die Veröffentlichung nicht mehr rückgängig zu machen war.

# G 3.46 Fehlerhafte Konfiguration eines Lotus Domino Servers

Fehlkonfigurationen eines Software-Systems sind häufig die Ursache für erfolgreiche Angriffe. Aufgrund der Komplexität eines Lotus Domino Servers besteht auch hier die Gefahr, dass die installierte Lotus Notes/Domino-Umgebung durch Fehlkonfiguration nicht den geforderten Sicherheitsansprüchen genügt. Durch die Fülle an Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter können auch viele Gefährdungen entstehen.

Fehlerhafte Konfigurationen können sowohl bei der Grundkonfiguration eines Lotus Domino Servers als auch bei der Konfiguration spezieller Dienste, die von dem Server bereitgestellt werden, vorkommen. Dazu zählen z. B. der integrierte Webserver (HTTP-Task) oder die für iNotes bzw. Domino Web Access genutzten Domino Offline Services (DOLS). Aber auch die fehlerhafte Konfiguration des Datenbankdienstes von Domino ist ein Problem für die Gesamtsicherheit des Servers.

Einige typische Fehlkonfigurationen werden im Folgenden aufgeführt:

- **Fehlende Zugriffseinschränkungen auf einen Server**: In der Grundeinstellung ist es generell jedem erlaubt, auf einen Lotus Domino Server zuzugreifen. Werden keine Zugriffsbeschränkungen auf einen Server definiert, so wird diese erste Hürde nicht genutzt. Insbesondere in der Kombination mit schwachen oder falschen Zugriffsberechtigungen auf Dienste oder Datenbanken können so Sicherheitsprobleme entstehen.
- **Fehlerhafte Zugriffslisten (Access Control Lists, ACLs) oder unsichere Standard-ACLs**: Jede Datenbank erhält bei der Erzeugung eine (durch die jeweilige Datenbankvorlage bestimmte) Zugriffsliste mit Standardeinträgen. Je nach Vorlage bietet diese keinen ausreichenden Schutz für die Datenbank im Normalbetrieb. Dies gilt insbesondere dann, wenn die Datenbank nach der Erzeugung initialisiert oder weiter konfiguriert werden muss. Oft sind dazu zunächst umfangreiche Rechte notwendig, die für den laufenden Betrieb nicht mehr benötigt werden. Werden die Standardzugriffslisten nicht verändert, kann dies dazu führen, dass Unbefugte auf die Datenbank zugreifen können oder Benutzern zu hohe Rechte eingeräumt werden.
- **Es wird keine Verschlüsselung eingesetzt**: Die Verschlüsselung der Netzkommunikation (Port-Verschlüsselung) und die Verschlüsselung von Datenbanken oder Datenbankfeldern sind in der Regel standardmäßig nicht aktiviert. Um die Verschlüsselung zu nutzen, muss diese explizit aktiviert werden. Wird dies vergessen, so sind die Daten sowohl bei der Kommunikation als auch auf den Datenträgern ungeschützt.
- **Unzureichende Berechtigungen für Server oder administrative Prozesse**: Damit eine Notes-Datenbank korrekt funktionieren kann, muss sie von einem dedizierten Server verwaltet und gewartet werden. Zu den Verwaltungs- und Wartungsaufgaben eines Servers gehört unter anderem das Aktualisieren von Datenbank-Kopien (Daten, Zugriffslisten, usw.). Sind dem verantwortlichen Server keine ausreichenden Rechte eingeräumt, so schlagen die Verwaltungsaktionen fehl. Dies kann zu Sicherheitsproblemen führen, dass z. B. Veränderungen an den Zugriffsberechtigungen nicht an die Kopien einer Datenbank weitergegeben werden können.
- **Akzeptieren von Cross-Zertifikaten**: Zwischen verschiedenen Zertifikatshierarchien (ohne gemeinsame Zertifizierungsinstanz) können Ver-

trauensstellungen eingetragen werden, indem eine sogenannte Cross-Zertifizierung erfolgt (Anerkennen fremder Zertifikate). Cross-Zertifikate können meist automatisch erzeugt werden, wenn ein unbekanntes Zertifikat "entdeckt" wird. Dies gilt sowohl für Notes-Zertifikate als auch für X.509-Zertifikate. Dabei können Cross-Zertifikate auch von Benutzern einfach im persönlichen lokalen Adressbuch erzeugt werden. Das Anlegen von Cross-Zertifikaten im NAB (Notes Address Book) kann dagegen nur durch einen berechtigten Administrator erfolgen. Werden Zertifikate leichtfertig als vertrauenswürdig anerkannt, so kann dies zu Sicherheitsproblemen führen, z. B. bei aktiven Inhalten, die mit dem nun als vertrauenswürdig geltenden Zertifikat signiert sind.

Die aufgeführten Problemfelder sind Beispiele für mögliche Gefährdungen durch Fehlkonfigurationen eines Lotus Domino Servers. Abhängig vom jeweiligen Einsatzumfeld können weitere hinzukommen.

**Beispiel:**

Ein Server ist so konfiguriert, dass anonyme Zugriffe nicht gestattet sind. An der Web-Schnittstelle sind nur SSL-Verbindungen erlaubt. Bei der Konfiguration der Datenbank-ACLs wird daher kein *Anonymous*-Eintrag erstellt. Weiterhin wird auf das Erzwingen des SSL-geschützten Web-Zugriffs verzichtet, da der Server nur SSL-Verbindungen an der Web-Schnittstelle annimmt. Die *Default*-Rechte aus den Datenbank-Vorlagen wurden nicht geändert, um den administrativen Aufwand bei Vorlagenänderungen zu minimieren. Durch die Einführung einer neuen Datenbank, die öffentliche Informationen enthält, wird der Server so konfiguriert, dass nun auch normale Web-Zugriffe auf diese Datenbank erlaubt sind (anonym, nicht SSL- geschützt). Ab nun kann auf alle Server-Datenbanken anonym zugegriffen werden, es gelten dabei die *Default*-Rechte, die oft mindestens das Lesen erlauben. Dadurch besteht die Gefahr, dass Unbefugte vertrauliche Daten einsehen oder Informationen manipulieren können.

# G 3.47 Fehlerhafte Konfiguration des Browser-Zugriffs auf Lotus Notes

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in G 3.113 *Fehlerhafte Konfiguration eines Lotus Notes Clients oder eines Fremdclients mit Zugriff auf Lotus Domino* integriert.

# G 3.48 Fehlerhafte Konfiguration von Windows- /basierten IT-Systemen

Windows Client- und Serverbetriebssysteme sind komplexe Systeme, deren Sicherheit im Wesentlichen durch die eingestellten Parameter bestimmt wird. Dadurch ergeben sich insbesondere durch Fehlkonfiguration einzelner oder mehrerer Komponenten Sicherheitsgefahren, die von Fehlfunktionen bis hin zur Kompromittierung eines Windows-Netzes führen können. Die folgenden Beispiele zeigen einige solcher Sicherheitsgefahren:

- Bei der Migration von Windows NT 4.0 zu einer neueren Windows Version bleiben die Zugriffsberechtigungen von Windows NT erhalten, die auch normalen Benutzern weitreichenden Zugriff auf Systemdateien erlauben. Damit ist die Zugriffssicherheit bei migrierten Windows Systemen im Allgemeinen niedriger als bei neu installierten Windows Systemen. Ein direktes Update von Windows NT 4.0 ist nur bis Windows Server 2003 möglich.
- Ist der Authentisierungsmechanismus NTLM unsicher konfiguriert, ist es durch Abhören des Netzverkehrs möglich, Benutzerpassworte zu rekonstruieren. Dies war bisher vor allem bei der Nutzung alter NTLM-Versionen kleiner 2.0 ein Problem, mittlerweile ist auch die Version 2.0 des NTLM Protokolls kompromittiert.
- Ist EFS falsch konfiguriert (etwa bei Verwendung lokaler Benutzerkonten ohne aktiviertes Kennwort für das Programm *syskey*, kann die EFS-Verschlüsselung umgangen werden, wenn ein Angreifer physikalischen Zugriff auf den Rechner hat.
- Ist Bitlocker im Basismodus (Bitlocker mit TPM) konfiguriert, so startet das System bis zum Anmeldefenster von Windows. Da das verschlüsselte Volume zum Laden des Betriebssystems entschlüsselt werden muss, kann ein Angreifer, der physikalischen Zugriff zum Rechner hat, in dieser Konfiguration Zugriff auf vertrauliche Daten erlangen.
- Windows 8 bietet bei der Einrichtung der Bitlocker-Verschlüsselung per Default die Möglichkeit, den Bitlocker Recovery-Schlüssel direkt über den Microsoft-Account zu sichern. Wird diese Konfiguration gewählt, so eröffnen sich neue Angriffswege gegen die Verschlüsselung durch ein Ausspähen der Daten beim Cloud-Dienstleister.
- Durch Fehlkonfiguration des Wechselmedienzugriffs ist es möglich, dass Benutzer Schreibzugriff auf Wechselmedien, wie einen USB-Stick oder einen CD/DVD-Brenner erhalten und auf diesem Weg Informationen den Informationsverbund verlassen.

Neben der reinen Betriebssystemkonfiguration ergeben sich Sicherheitsprobleme auch durch die fehlerhafte Konfiguration systemnaher Dienste wie DNS, WINS, DHCP, RAS oder IPSec. Gelingt es einem Angreifer, diese Komponenten mit Erfolg anzugreifen, so ist die Systemsicherheit des gesamten Netzes gefährdet.

# G 3.49 Fehlerhafte Konfiguration des Active Directory

Die Windows-Server-Betriebssysteme ab Windows 2000 Server gestatten die Delegation einzelner administrativer Rechte - auch für Teilbereiche des Active Directory - an bestimmte Benutzer. Diese Delegation erfolgt durch die Vergabe detaillierter Einzelberechtigungen im Active Directory.

Durch die hohe Komplexität der Rechtevergabe im Active Directory, wie beispielsweise die Vergabe zahlreicher spezifischer Einzelberechtigungen für einzelne Objekttypen oder die Vererbung von Berechtigungen, kann es geschehen, dass

- Administratoren Zugriff auf Bereiche des Active Directory haben, zu deren Administration sie nicht befugt sind, oder
- Bereiche des Active Directory nicht durch Zugriffsrechte geschützt sind, so dass jeder Benutzer auf diese Daten zugreifen kann.

Die Gefahr des unberechtigten Zugriffs bei Fehlkonfiguration der Active-Directory-Zugriffsrechte erhöht sich insbesondere dadurch, dass mehrere Zugriffsschnittstellen auf das Active Directory existieren, z. B. Active Directory Service Interfaces (ADSI) oder Lightweight Directory Access Protocol (LDAP).

Werden Vertrauensstellungen zwischen Domänen eingerichtet, so können Benutzer einer Domäne auf Ressourcen einer anderen Domäne zugreifen. Daher kann eine mangelnde Planung von Vertrauensbeziehungen zwischen Domänen zu unerwünschten Zugriffsrechten auf die Ressourcen einer Domäne führen.

Besonders kritisch können Handlungen sein, die die Datenbankstruktur des Active Directory ändern:

- Änderungen des Active Directory-Schemas können dazu führen, dass das bestehende Windows-System zu Softwarepaketen, die das Active Directory ebenfalls nutzen, inkompatibel wird. Da sich Änderungen des Schemas zum Teil nicht rückgängig machen lassen, kann dies dazu führen, dass das bestehende System komplett neu aufgesetzt werden muss.
- Bei der Aufnahme eines personenbezogenen Attributes in den "Global Catalog" des Active Directory besteht die Gefahr, dass personenbezogene Daten auch jenseits des eigentlichen Adressatenkreises zugänglich sind.
- **Beispiel:** Innerhalb einer Firma werden die internen Telefonnummern der Mitarbeiter im Active Directory abgelegt. Wenn die Rechner der Firma nur eine Domäne im Active-Directory-Baum eines größeren Unternehmensverbundes bilden, würden diese internen Telefonnummern bei Aufnahme in den "Global Catalog" an alle Domänen des Active-Directory-Baumes verteilt.

Damit eine sichere Konfiguration des Active Directory auch im laufenden Betrieb sichergestellt werden kann, müssen sicherheitsrelevante Konfigurationsänderungen nicht nur sorgfältig geplant, sondern auch protokolliert werden. Werden Domänen-Controller ohne ausreichende Protokollierung betrieben, so besteht die Gefahr, dass unautorisierte, sicherheitsrelevante Konfigurationsänderungen nicht erkannt werden und nicht rechtzeitig korrigiert werden können.

# G 3.50 Fehlerhafte Konfiguration von Novell eDirectory

Fehlkonfiguration von Software ist eine der häufigsten Ursachen für erfolgreiche Angriffe. Durch die hohe Komplexität und die große Zahl der verfügbaren Parameter bei eDirectory können durch unbeachtete Seiteneffekte auch zusätzliche Sicherheitsprobleme eintreten.

Mögliche Fehlkonfigurationen betreffen unter anderem

- die Erstellung und Definition der Baumstruktur an sich,
- die Konfiguration des Zertifikatsservers,
- die Einrichtung der abzubildenden Objekte,
- die Konfiguration der Zugriffsmechanismen,
- die Vergabe der Zugriffsrechte (siehe G 3.51 *Falsche Vergabe von Zugriffsrechten im Novell eDirectory*),
- die Konfiguration des Intranet-Clientzugriffs auf den Verzeichnisdienst (siehe G 3.29 *Fehlende oder ungeeignete Segmentierung*),
- den LDAP-Zugriff auf eDirectory (siehe G 3.53 *Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory*),
- die Konfiguration der Partitionierung der Verzeichnisdatenbank,
- die Konfiguration der Replikation des eDirectory,
- die Konfiguration der aufzuzeichnenden eDirectory-Events,
- die Konfiguration des Real-time Alert-Mechanismus,
- die Konfiguration des iMonitor-Tools zur Web-basierten Fernüberwachung sowie
- die Konfiguration eines automatisierten Backup-Mechanismus.

Grundsätzlich muss die Konfiguration des Systems an der Sicherheitsrichtlinie ausgerichtet werden. Bei Fehlkonfiguration besteht die Gefahr, dass diese Richtlinie inkonsistent umgesetzt wird und damit die Zielsetzungen der Sicherheitsvorgaben nicht erreicht werden.

eDirectory ermöglicht die Konfiguration einer rollenbasierten Administration des Verzeichnissystems sowie die Delegation von Administrationsrechten. Bei einer Fehlkonfiguration dieser Funktionalitäten ergeben sich u. U. erhebliche Probleme durch unautorisierte Systemzugriffe. Weiterhin besteht bei fehlerhafter Konfiguration die Gefahr, dass eine geregelte Administration nicht mehr möglich ist.

Folgende Liste gibt einen Überblick über die sicherheitsrelevanten möglichen Konsequenzen einer Fehlkonfiguration des Novell eDirectory:

- Auswahl zu schwacher Authentisierungsmechanismen,
- Falsche Rechtevergabe für den Zugriff auf die Objekte des Verzeichnisdienstes,
- unautorisierte Systemzugriffe über die Administrationsschnittstelle,
- unzureichender Schutz vor Systemangriffen,
- Blockade der Administrationsmöglichkeit des Systems,
- fehlerhafte oder langsame Replikation der Daten zwischen den Verzeichnisdatenbanken sowie
- Inkonsistenzen in der Umsetzung der Sicherheitsrichtlinie.

# G 3.51 Falsche Vergabe von Zugriffsrechten im Novell eDirectory

Da eDirectory eine Reihe sensitiver Daten der Systembenutzer und -Ressourcen enthält und zudem eine enge Beziehung zu dem unterliegenden Betriebssystem besteht, ist die Vergabe von Zugriffsrechten auf das eDirectory besonders wichtig.

Die Zugriffsrechte auf eDirectory-Objekte werden über so genannte Access Control Lists (ACLs) vergeben. Dabei gibt es Zugriffsrechte auf das eDirectory-Objekt an sich sowie auf einzelne Attribute eines Objekts.

Auf Objektebene sind dabei folgende Rechte (Privilegien) zu vergeben: *Browse, Create, Delete, Rename* und *Supervisor*. Auf Attributsebene sind dies: *Compare, Read, Add or Delete Self, Write, Supervisor* sowie *Inheritance Control*. *Compare* wird dabei als Teil des *Read*-Rechtes behandelt, d. h. sofern das *Read*-Recht vergeben ist, so besteht auch automatisch das Recht *Compare*.

Die Access Control Lists selbst sind Attribute (Properties) zu den jeweiligen eDirectory-Objekten. Die Zugriffsrechte auf eDirectory-Objekte vererben sich standardmäßig von Vater- auf Kindobjekte innerhalb der Baumhierarchie. Um zu verhindern, dass Brüche dieses Vererbungsmechanismus durch Partitionierung des eDirectory-Verzeichnisses entstehen, wird an das Wurzelobjekt der Partition eine *inherited ACL* angehängt. Auf die Vererbung kann mit Hilfe so genannter Masken oder *Inherited Rights Filter* Einfluss genommen werden.

Die Zugriffsrechte auf Attributsebene werden standardmäßig nicht entlang der Verzeichnishierarchie weitergeleitet. Dies kann jedoch über das Attributsrecht *Inheritance Control* konfiguriert werden. Damit lässt sich auch das besonders kritische *Self*-Recht kontrollieren.

Die Zugriffsrechte werden explizit mittels so genannter *Trustee-Anweisungen* vergeben. Dabei werden die Zugriffsrechte (Privilegien) auf das Target-Objekt (Ziel) durch andere eDirectory-Objekte (Benutzer, Benutzergruppen, Services, Anwendungen, Server, etc.) direkt in die ACL des Target-Objekts eingetragen.

Weiterhin können Zugriffsrechte indirekt durch so genannte *Security-Äquivalenzen* vergeben werden. Beispiel: Target-Objekt X erhält (mindestens) die gleichen Zugriffsmöglichkeiten wie Target-Objekt Y, d. h. die Trustees von Objekt Y werden automatisch auch Trustees von Objekt X. Dies wird ebenfalls als ACL-Eintrag von Objekt X konfiguriert.

Bei einem konkreten eDirectory-Zugriff werden stets die so genannten *effektiven Rechte* berechnet, d. h. das Endresultat der oben beschriebenen Konfigurationen.

Diese Vielfalt an Konfigurationsmöglichkeiten der eDirectory-Zugriffsrechte beinhaltet die Gefahr, dass inkonsistente oder falsche Zugriffsmöglichkeiten vergeben werden. Sofern die Zugriffsrechte im eDirectory falsch vergeben werden, ist die Sicherheit des Gesamtsystems erheblich gefährdet. Dies betrifft die Vertraulichkeit und die Integrität von Daten sowie mögliche Hintertüren für weitreichende Systemangriffe.

Ein besonders kritischer Punkt ist auch die Vergabe der Administrationsrechte. eDirectory ermöglicht die Umsetzung eines rollenbasierten Administrati-

onskonzeptes sowie die Delegation einzelner Administrationsaufgaben durch die Vergabe entsprechender Zugriffsrechte. Bei einer falschen Vergabe dieser Rechte wird das gesamte Administrationskonzept in Frage gestellt und unter Umständen sogar die Administration des Verzeichnissystems blockiert.

# G 3.52 Fehlerhafte Konfiguration des Intranet-Clientzugriffs auf Novell eDirectory

Beim Einsatz des eDirectory-Verzeichnisdienstes im Intranet einer Organisation werden für den verteilten Benutzerzugriff auf das System entsprechende Clients benötigt. Dabei gibt es für die unterschiedlichen Betriebssysteme jeweils eigene Client-Software:

- den Novell Client für Windows-Betriebssysteme,
- eine Client-Library für Linux,
- eine Client-Library für Sun Solaris.

Der Clientzugriff auf den eDirectory-Verzeichnisdienst erfolgt über das proprietäre NDAP-Protokoll (Novell Directory Access Protocol). Dieses setzt seinerseits auf dem Novell NCP-Protokoll auf, welches über IP oder IPX betrieben werden kann.

Bei einem Zugriff mit Hilfe des Novell Clients für Windows auf den eDirectory-Baum (oder ein eDirectory-Objekt) muss der Benutzername und das Passwort dem Client übermittelt werden. Der Client sucht dann beim eDirectory nach dem entsprechenden Objekt und übermittelt dessen privaten Schlüssel, welcher mit dem Benutzerpasswort verschlüsselt ist. Auf Clientseite wird mittels des Benutzerpasswortes der private Schlüssel entschlüsselt und daraus ein so genanntes *Credential* und eine Signatur berechnet. Der private Schlüssel wird anschließend aus dem Speicher des Clients gelöscht und nur das Credential und die Signatur behalten. Diese können in der Folge für weitere "Hintergrundauthentisierungen" zu anderen Objekten oder Diensten verwendet werden. Der Benutzer muss dafür nicht mehr in Interaktion treten und nutzt somit einen *Single-Sign-On*.

Aus dem Credential und der Signatur wird mittels eines so genannten *Zero-Knowledge-Verfahrens* ein Beweis (*proof*) generiert, welcher dem Zielsystem übermittelt wird. Das Zielsystem kann mit dessen Hilfe die Identität des Clients verifizieren. Der Vorteil dieser Methode ist, dass die Signatur nicht explizit über das Netz übertragen wird und somit weniger Angriffsmöglichkeiten bestehen.

Trotzdem sind gewisse Angriffsszenarien, so genannte *Man-in-the-middle-Attacks*, bekannt geworden, welche jedoch eher theoretischer Natur sind, da zu deren Ausnutzung erheblicher technischer Aufwand betrieben werden muss.

Dessen ungeachtet kann es zu ernsthaften Sicherheitsproblemen kommen, wenn

- die Authentisierungsmechanismen für den Clientzugriff mangelhaft sind,
- ein unautorisierter Zugriff auf das eDirectory-Verzeichnis und dessen Objekte möglich ist oder
- Administratorrechte für den Verzeichnisdienst missbraucht oder unberechtigt erlangt werden können.

# G 3.53 Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory

Der LDAP-Zugriff auf den Verzeichnisdienst von eDirectory eignet sich vor allem für zwei Szenarien:

- den Benutzerzugriff auf den Verzeichnisdienst über das Internet und
- den Zugriff auf den Verzeichnisdienst durch weitere Applikationen.

Prinzipiell gibt es aus Sicht des eDirectory drei Arten des Benutzerzugriffs über LDAP:

- als [Public] Objekt (*Anonymous Bind*),
- als Proxy User (*Proxy User Anonymous Bind*),
- als NDS User (*NDS User Bind*).

Dabei ist zu beachten, dass das [Public] Objekt im eDirectory standardmäßig stets das *Browse*-Recht über den Verzeichnisbaum besitzt, sofern dieses Recht nicht explizit entzogen wurde. Weiterhin ist zu berücksichtigen, dass ohne die Konfiguration geeigneter Authentisierungsmechanismen die Gefahr besteht, dass die Benutzerpasswörter im Klartext übertragen werden. Eine Verschlüsselung der Übertragung ist nur dann gegeben, wenn die Kommunikation zwischen Client und eDirectory-Server über SSL erfolgt.

Bei der SSL-Konfiguration ergeben sich ebenfalls Fehlermöglichkeiten, welche zu einer Herabsetzung des Sicherheitsniveaus oder der Performance führen können.

Weiter ist zu beachten, welche LDAP-Version die Clients unterstützen und welche Konfigurationsmöglichkeiten dort bestehen. Unter Umständen kann es dabei zu Missverständnissen kommen und die Sicherheit des Betriebs beeinträchtigt werden.

Für die Anbindung von Netzapplikationen per LDAP an den eDirectory-Verzeichnisdienst ergeben sich prinzipiell die gleichen Gefährdungen wie beim Zugriff von Clients, nämlich:

- der unautorisierte Zugriff auf das Verzeichnis,
- der Verlust der Integrität und der Vertraulichkeit der im Verzeichnis gehaltenen Daten,
- die ungewollte Einrichtung einer Hintertür für das System.

# G 3.54 Verwendung ungeeigneter Datenträger bei der Archivierung

Für die Speicherung von Daten werden Datenträger eingesetzt, die jeweils einen definierten Einsatzbereich und Einsatzzeitraum aufweisen. Hierbei kann es vorkommen, dass für die Speicherung dauerhaft oder temporär Datenträger verwendet werden, die den Anforderungen nicht gerecht werden.

Typische Ursachen hierfür sind beispielsweise

- Fehler bei der Beschaffung oder Bestellung der Datenträger,
- unzureichende Vorratshaltung, so dass nicht vorgesehene Datenträger eingesetzt werden müssen, um Datenverlust zu vermeiden,
- falsche Kennzeichnung der Datenträger oder
- unzureichende Kenntnisse über den Einsatzbereich des Datenträgers.

Der Einsatz ungeeigneter Datenträger kann zu einem Datenverlust führen, der auch erst nach einer längeren Speicherdauer auftreten kann.

**Beispiel:**

Bei der routinemäßigen Beschaffung neuer Datenträger für ein Archivsystem werden anstatt einmalbeschreibbarer WORM-Medien (Write Once Read Multiple) fälschlicherweise wiederbeschreibbare Medien bestellt und geliefert. In Folge der Verwechslung werden Archivdaten überschrieben. Da die Speicherung der ursprünglichen Daten sehr lange zurückliegt, sind keine Kopien der Originaldaten mehr vorhanden. Dadurch sind die ursprünglich gespeicherten Dokumente unwiederbringlich verloren, da diese nur noch elektronisch archiviert wurden.

# G 3.55 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Vorgaben zu beachten, deren Nichteinhaltung zivil- oder strafrechtliche Konsequenzen haben kann. Hervorzuheben sind hier u. a.

- Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben,
- Vorgaben an die Höchstaufbewahrungsdauer, die sich aus Datenschutzregelungen ableiten,
- Zugriffsrechte, die für Externe - wie z. B. Steuerbehörden - gewährt werden müssen, sowie
- die Rechtslage zur digitalen Signatur.

Einige Quellen für rechtliche Rahmenbedingungen sind in der Maßnahme M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung* aufgeführt.

# G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung

Der IIS wird weltweit in unterschiedlichen Umgebungen eingesetzt. Als Einsatzumgebung wird die Netztopologie (Anordnung von weiteren Hard- und Software-Komponenten, Netzkomponenten) verstanden, in der der IIS betrieben wird. Als wesentlicher Aspekt ist dabei auch der Kommunikationsbedarf des IIS mit anderen Systemen zu berücksichtigen.

Die Absicherung eines öffentlichen, aus dem Internet erreichbaren Servers ist im Vergleich zu einem im Intranet installierten Server in der Regel mit einem viel höheren Aufwand verbunden. Von entscheidender Bedeutung ist dabei der sichere Einsatz geeigneter Trenneinrichtungen.

Eine unzureichend geplante Netzstruktur, z. B. ohne Demilitarisierte Zone (DMZ) oder eine fehlerhaft konfigurierte Trenneinrichtung (Firewall), kann für einen Angriff aus dem Internet bzw. Intranet ausgenutzt werden.

Ein weiteres Risiko entsteht durch nicht ausreichend dimensionierte Systemressourcen (Firewall, Netzanbindung). Wenn diese Systeme nicht den Anforderungen an die Verfügbarkeit und Performance des eigentlichen Web-Servers entsprechen, besteht die Gefahr eines Single-Point-of-Failure (SPOF).

**Beispiel:**

Mit Hilfe eines IIS und eines Datenbank-Servers wird eine E-Business-Anwendung realisiert. Befindet sich der Datenbank-Server im gleichen Segment wie der IIS, auf den aus dem Internet zugegriffen werden darf, besteht die Gefahr, dass ein Unbefugter auch auf die Datenbank zugreifen und die vorhanden Datenbestände auslesen oder manipulieren kann.

# G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 3.58 Fehlerhafte Konfiguration eines IIS

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 3.59 Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 3.60 Fehlerhafte Konfiguration von Exchange

Die Fehlkonfigurationen eines Software-Systems ist häufig die Ursache für erfolgreiche Angriffe. Aufgrund der Komplexität eines Microsoft Exchange-Systems können durch die Fülle an Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter zahlreiche Sicherheitsprobleme entstehen.

Einige typische Fehlkonfigurationen werden im folgenden aufgeführt:

- Die Exchange-Server-Komponenten werden auf ungeeigneten Systemen installiert und betrieben.
  Dies hat erhebliche Konsequenzen für die Administrationsrechte auf dem Server und verhindert eine sinnvolle Rollentrennung der Administration. Weiterhin ergeben sich Nachteile bezüglich der Performance und unter dem Aspekt der Ausfallsicherheit.
- Die Zugriffsbeschränkungen auf einen Exchange-Server sind unzureichend.
  Insbesondere in der Kombination mit schwachen oder falschen Zugriffsberechtigungen auf weitere Dienste oder E-Mail-Datenbanken können so Sicherheitsprobleme entstehen.
- Oft sind für die Erzeugung oder Initialisierung einer Exchange-Datenbank zunächst umfangreiche Rechte notwendig, die für den laufenden Betrieb nicht mehr erforderlich sind. Werden die Standard-Zugriffsrechte nicht verändert, kann dies dazu führen, dass Unbefugte auf die E-Mail-Datenbank zugreifen können oder Benutzern zu weitgehende Rechte eingeräumt werden.
- Es wird keine Verschlüsselung eingesetzt.
  Die Verschlüsselung der Netzkommunikation (Port-Verschlüsselung) sowie der E-Mail-Kommunikation ist bei einer Standardinstallation nicht aktiviert.
  Um die Verschlüsselung zu nutzen, muss diese explizit eingerichtet werden. Anderenfalls sind die E-Mail-Daten während des Zustellprozesses ungeschützt.

Die aufgeführten Aspekte sind Beispiele für mögliche Sicherheitsprobleme durch Fehlkonfigurationen. Abhängig vom jeweiligen Einsatzumfeld können weitere Problemfelder hinzukommen.

# G 3.61 Fehlerhafte Konfiguration von Outlook

Microsoft Outlook ist ein wichtiger Teil des Microsoft Exchange-Systems und bezeichnet die Client-Komponente. Die korrekte Konfiguration des Clients ist wichtig für die Gesamtsicherheit des Systems.

Folgende Aspekte sollten hierbei besonders erwähnt werden:

- Die Auswahl des Kommunikationsprotokolls kann spezielle Sicherheitsprobleme nach sich ziehen. Dabei sei besonders die MAPI-Schnittstelle erwähnt, über die sich in der Vergangenheit eine Reihe von Computer-Viren und Würmern verbreitet haben.
- Wird ein Client-Rechner von mehreren Benutzern verwendet, so wird für jeden Benutzer ein eigenes Profil angelegt und gespeichert. Hierbei kann dieses Profil durch einen Kollegen übernommen werden. Dadurch kann unter Umständen das Benutzerkonto einer Person gegenüber dem System unbefugt übernommen sowie die Vertraulichkeit von Daten beeinträchtigt werden.
- Werden Verschlüsselung und elektronische Signatur auf E-Mail-Ebene eingesetzt, z. B. auf der Basis von S/MIME oder PGP, so kann unter Umständen der private Schlüssel kompromittiert werden, sofern dieser lokal abgespeichert wird. Mögliche Folgen sind, dass die Vertraulichkeit der Daten beeinträchtigt und Rechte von Dritten unbefugt übernommen werden.
- Wird Verschlüsselung auf Netzebene eingesetzt, z. B. durch die Nutzung von IPSec, SSL oder TLS, so kann dieser Mechanismus bei einer fehlerhaften Konfiguration des Clients unwirksam werden.
- Eine fehlerhafte Konfiguration des E-Mail-Clients Outlook kann außerdem zu einem Datenverlust sowie zu einer Blockade des Clients führen. Weiterhin kann es zu einem Überlauf und damit zu einer Überlastung des Exchange Servers kommen.
- Ist im Outlook Client die automatische Ausführung gefährlicher Dateiformate nicht in geeigneter Weise eingeschränkt, so können Viren und andere Schadsoftware eingeschleppt oder verbreitet werden.

Die Terminverwaltung und die Aufgabenliste sind weitere Bestandteile des Exchange/Outlook-Systems, die nicht direkt der Abwicklung des E-Mail-Verkehrs dienen, sondern der Unterstützung des Workflows innerhalb einer Institution.

Diese Bereiche enthalten mitunter jedoch ebenso sensible und schützenswerte Informationen wie die elektronischen Nachrichten. Bei einer Fehlkonfiguration dieser Teilsysteme bestehen somit folgende potentielle Sicherheitsprobleme:

- Verlust der Vertraulichkeit durch unbefugten Zugriff,
- Verlust der Integrität der Informationen durch Datenmanipulation (zufällig oder vorsätzlich),
- unberechtigte Übernahme der Rolle bzw. der Identität eines anderen Benutzers oder
- Verlust von Daten und Informationen durch unsachgemäße Datenhaltung und fehlende Backup-Vorkehrungen.

# G 3.62 Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 3.63 Fehlerhafte Konfiguration eines Apache-Webservers

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 3.64 Fehlerhafte Konfiguration von Routern und Switches

Die Konfiguration aktiver Netzkomponenten hängt stark vom Einsatzzweck der Geräte ab. Nachfolgend sind einige Beispiele aufgeführt, die den sicheren Einsatz der Geräte bedrohen können.

**Betriebssystem**

Oft werden auf Routern und Switches veraltete oder unsichere Versionen von Betriebssystemen verwendet. Für eine Vielzahl von Versionsständen für Betriebssysteme unterschiedlicher Geräte und Hersteller stehen auf einschlägigen Seiten im Internet Exploits zum Angriff auf diese Geräte zum Download bereit.

**Passwortschutz**

Der Zugriff auf aktive Netzkomponenten wird oft nur unzureichend durch Passwörter geschützt.

**Administrationszugänge**

Administrationszugänge sind in der Praxis oft frei zugänglich. Es sind beispielsweise keine Access Control Lists (ACL) eingerichtet.

**Remote-Zugriff**

Aktive Netzkomponenten bieten in der Regel die Möglichkeit mit Hilfe von TELNET remote zuzugreifen. Bei der Nutzung von TELNET werden Benutzername und Passwort im Klartext übertragen.

**Login-Banner**

Login-Banner von aktiven Netzkomponenten verraten häufig die Modell- und Versionsnummer des Geräts.

**Unnötige Netzdienste**

Häufig stehen auf Routern und Switches unnötige Netzdienste bereit, mit deren Hilfe Angreifer die Verfügbarkeit, Integrität oder Vertraulichkeit der Komponenten gefährden können.

**Schnittstellen**

Nicht genutzte Schnittstellen auf Routern sind häufig nicht deaktiviert.

**VLAN**

Trunk-Ports können auf alle konfigurierten VLANs zugreifen. Das heißt, dass der Zugang zu einem Trunk-Port den Zugriff auf alle VLANs ermöglicht. Häufig sind auf Switches die Trunking-Protokolle auf den Endgeräte-Ports nicht deaktiviert. Siehe auch G 5.114 *Missbrauch von Spanning Tree*.

**Routing-Protokolle**

Routing-Protokolle ohne Authentisierungsverfahren können die Vertraulich-keit, Verfügbarkeit und Integrität komplexer Netze bedrohen.

# G 3.65 Fehlerhafte Administration von Routern und Switches

Eine fehlerhafte Administration von Routern und Switches kann die Verfügbarkeit, Vertraulichkeit und Integrität von Netzen bedrohen. Es gibt unterschiedliche Zugriffsmöglichkeiten, um Router und Switches zu administrieren, die bei falscher Anwendung ein Sicherheitsrisiko darstellen können:

**Remote-Administration**

Eine Vielzahl von aktiven Netzkomponenten bieten die Möglichkeit der Remote-Administration mit Hilfe des Dienstes Telnet. Die Nutzung von Telnet bietet allerdings eine Gefahr durch die unbefugte Erlangung von Zugriffsrechten, da der Datenverkehr inklusive des Benutzernamens und Passwortes im Klartext mitgelesen werden kann.

Viele Geräte bieten die Möglichkeit, Administrationsarbeiten mit Hilfe des Dienstes HTTP durchzuführen. Auf dem Router bzw. dem Switch ist in diesem Fall ein HTTP-Server gestartet, der Zugriff erfolgt von beliebigen Clients über Web-Browser. Die Standardeinstellungen für den Zugriff auf das Web-Interface sind nicht bei allen Herstellern einheitlich. So kann der Zugriff deaktiviert sein, es ist aber auch möglich, dass dieser Dienst ungeschützt ohne Eingabe von Benutzerinformationen verwendet werden kann.

Wie bei der Nutzung des Dienstes Telnet werden auch beim HTTP der Benutzername und das Passwort im Klartext übertragen. Zudem sind eine Reihe von Exploits bekannt, die Schwachstellen der HTTP-Server unterschiedlicher Hersteller ausnutzen.

**SNMP**

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten "Community Strings". Als Standardeinstellung bei nahezu allen Herstellern ist der read-Community-String auf den Wert "public" eingestellt, während der write-Community-String auf den Wert "private" gesetzt ist. Die SNMP Community Strings werden im Klartext über das Netz übertragen. Oft wird SNMP über nicht abgesicherte Netze genutzt, so dass ein Angreifer in der Lage ist, durch Mitlesen der Datenpakete (Sniffen) SNMP Community Strings zu erraten. Nach Kenntnisnahme der Community Strings kann ein Angreifer die Kontrolle über die Netzkomponenten übernehmen.

**Protokollierung**

Häufig werden sicherheitsrelevante Ereignisse auf Routern und Switches nur unzureichend protokolliert. Zudem kann sich eine fehlende Alarmierungskomponente negativ auf die Verfügbarkeit, Vertraulichkeit und Integrität der Systeme auswirken.

**Fehlendes Backup und Dokumentation**

Oft werden Konfigurationsänderungen auf Routern und Switches nicht gesichert und nicht dokumentiert. Beim Ausfall der Komponenten stehen die letzten Änderungen beim Wiederanlauf des Ersatzsystems nicht zu Verfügung.

# G 3.66 Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS

EBCDIC *(Extended BinaryCoded Decimals Interchange Code)* und ASCII *(American Standard Code for Information Interchange)* sind Kodierungstabellen, die festlegen, wie Buchstaben, Ziffern und andere Zeichen mit Hilfe von 8 bzw. 7 Bits dargestellt werden.

z/OS-Systeme arbeiten mit EBCDIC-*Code*. Lediglich HFS- und zFS-Dateisysteme (*Hierarchical File Systems*), die unter USS (*Unix System Services*) eingesetzt werden, lassen sowohl ASCII- als auch EBCDIC-Speicherung zu. Beim Datenaustausch zwischen z/OS-Systemen und Systemen, die mit ASCII-Code arbeiten (z. B. auch von USS nach MVS), besteht die Gefahr, dass Informationen verfälscht werden, wenn fehlerhafte Übersetzungstabellen (*Code Page Translation*) zum Einsatz kommen. Besonders häufig betroffen ist dabei die Übersetzung von Sonderzeichen.

**Beispiele:**

- In einem Unternehmen wurden zwischen verschiedenen OS/390- und z/OS-Systemen über einen längeren Zeitraum mittels FTP-Protokoll Daten übertragen, ohne dass es zu Problemen kam. Für ein zusätzliches Unix-System wurde der gleiche FTP-Job eingesetzt und die *EBCDIC-ASCII*-Übersetzung mit der Default-Tabelle durchgeführt. Der Transfer verlief zunächst ohne Probleme, bei der weiteren Verarbeitung der Datensätze im Unix-System zeigte sich jedoch, dass bestimmte Umlaute und Sonderzeichen nicht richtig übersetzt worden waren. Erst nach der Erstellung einer speziellen *Translation Table,* die nur für diesen Transfer zum Einsatz kam, war der Fehler bereinigt.
- Bei der Übertragung einer Datei mittels FTP-Protokoll von einem z/OS-Betriebssystem zu einem Unix-Betriebssystem wurde die Option *Binary* verwendet. Die Daten konnten auf dem Zielsystem nicht weiterverarbeitet werden, da die Option *Binary* die Konvertierung von EBCDIC nach ASCII unterdrückt.

# G 3.67 Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems

Die Konfiguration eines z/OS-Betriebssystem ist sehr komplex und erfordert an vielen Stellen den Eingriff des System-Administrators. Durch falsche oder unzureichende Definitionen entstehen schnell Schwachstellen, die zu entsprechenden Sicherheitsproblemen führen können.

**Autorisierte Programme**

Programme, die von einer autorisierten Bibliothek geladen werden und entsprechend gekennzeichnet sind, können hoch autorisierte Funktionen ausführen. Gelingt es Anwendern eigene Programme unberechtigt zu autorisieren, steht diesen Programmen nahezu die gleiche Funktionalität wie den System-Programmen zur Verfügung. Ein Deaktivieren von Sicherheitssperren in RACF ist so z. B. jederzeit möglich.

**System-Programme**

Bei der Installation des z/OS-Betriebssystems und seiner Komponenten ist es notwendig, bestimmte System-Bibliotheken (*Partitioned Datasets*) so zu definieren, dass das Betriebssystem auszuführende System-Programme über interne Tabellen schnell findet. Die Bibliotheken dieser System-Programme werden in sogenannten *Linklists* zusammengefasst und beinhalten in der Regel hoch autorisierte Programme, die im *Kernel-Mode* laufen. Durch Fehler in der Definition (oder durch Manipulation) können andere User-Bibliotheken zu diesen *Linklists* hinzugefügt werden, die nicht dafür vorgesehen sind. Die Programme dieser Bibliotheken sind dann ebenfalls hoch autorisiert und erlauben das Ausführen von Funktionen, die Sicherheitsmechanismen umgehen können.

**Fehler beim Anlegen von Systembibliotheken**

System-Bibliotheken, die als PDS (*Partitioned Dataset)* mit der Option *SecondarySpace* angelegt wurden, können zu Problemen im Betrieb führen. Während der Initialisierungsphase legt das System für einige System-Bibliotheken die *Directory* aus Geschwindigkeitsgründen in den Hauptspeicher und greift beim Laden des Programms nur über dieses Verzeichnis auf die Bibliothek zu. Wird bei der Erweiterung einer Bibliothek im Rahmen einer Programm-Pflege ein neuer Extent (dynamische Erweiterung des Dateibereiches auf der Festplatte) angelegt, kann es passieren, dass das alte Programm statt des neuen aktiv wird, da die interne Directory noch auf die alte Ladeadresse zeigt. Ferner kann dadurch der Platzbedarf einer Datei permanent anwachsen, ohne dass eine kontrollierte Begrenzung stattfindet.

**Supervisor-Calls**

*Supervisor-Calls* (SVCs) sind Aufrufe zu speziellen z/OS-Dienstprogrammen, die im hochautorisierten Kernel-Modus laufen. Programme für diesen Modus müssen besonders sicher programmiert sein (IBM gibt hierfür entsprechende Richtlinien vor). Unsichere SVC-Programme können unter Umständen benutzt werden, um z/OS-Sicherheitsmechanismen zu umgehen. Ein Angreifer befindet sich nach einer erfolgreichen Attacke im hochautorisierten Kernel-Modus. Vielfach gibt es heute noch sogenannte *Autorisierungs-SVCs* in Gebrauch, die aus wenigen Instruktionen bestehen, über *Modeset* den Kernel-Modus an-

oder ausschalten und es damit auch erlauben, unberechtigt im Kernel-Modus Funktionen auszuführen.

**TSO-Kommandos**

*Time-Sharing-Option*-Kommandos (TSO) laufen normalerweise im Anwendungsmodus ab (mit normalen User-Privilegien), d. h. sie sind nicht besonders privilegiert. z/OS verfügt jedoch über Kommandos, die für die Ausführung bestimmter Funktionen (oder Teilfunktionen) eine hohe Autorisierung benötigen. Kommandos, die nicht über die Autorisierung verfügen, die sie zur Verarbeitung benötigen, können im Betrieb Fehler produzieren. Andererseits führt die unkontrollierte Freigabe von autorisierten Kommandos zu einer Schwächung der Sicherheit.

**Restricted Utilities**

IBM und andere Software-Hersteller liefern, zusammen mit den Betriebssystemkomponenten zusätzliche Dienstprogramme (*Utilities*) aus. Diese Programme führen verschiedene verarbeitende Funktionen aus, wie das Kopieren von Dateien oder das Anlegen von Katalogen (z/OS Dateiverzeichnis zum Verwalten von Dateien). Die Mehrzahl dieser Utilities benötigt zur Ausführung lediglich normale User-Privilegien, einige benötigen jedoch eine hohe System-Autorisierung zur Durchführung ihrer Funktionen. Sind diese Utilities nicht korrekt definiert, dann besteht die Gefahr, dass sie nicht richtig funktionieren. Sind diese Utilities nicht hinreichend geschützt, dann besteht die Gefahr, dass sie von nicht autorisierten Mitarbeitern missbraucht werden können. In der Folge kann die Integrität des z/OS-Systems beeinträchtigt werden.

**z/OS-Kommandos unter SDSF (System Display and Search Facility)**

SDSF erlaubt es dem Anwender in einem JES2-System, sich die Ausgabe von Batch-Jobs, das System-Log und weitere System-Optionen anzuschauen und darüber hinaus MVS- und JES2-Kommandos einzugeben. Falls keine oder nur unzureichende Maßnahmen getroffen wurden, kann der Anwender von SDSF unter Umständen Manipulationen vornehmen, wie z. B. laufende Batch-Jobs beenden, *Initiators* stoppen oder starten oder aber Systemkonfigurationen umdefinieren. Darüber hinaus kann er ggf. alle System-Nachrichten aus dem Syslog und auch alle Job-Logs (u. U. auch Kunden-Daten) einsehen.

**Enhanced MCS-Support**

z/OS unterstützt über die MCS-Konsole (*Multiple Console Support*) hinaus die *Enhanced-MCS-Konsole*. Diese stellt eine Schnittstelle dar, über die Kommandos an MVS (JES2/3) übergeben und Nachrichten von MVS empfangen werden können. Die *Enhanced-MCS-Konsole* steht unter *TSO*, *NetView* und Applikationen - wie z. B. *CICS* - zur Verfügung. Wenn nicht entsprechende Schutzdefinitionen vorgenommen werden, können unter Umständen Kommandos abgesetzt werden, die die Integrität eines Systems stark beeinträchtigen können.

**Beispiele:**

- Auf einem OS/390-System wurde in der Vergangenheit ein *Autorisierungs-SVC* eingesetzt, um unter *TSO/ISPF* bestimmte Funktionen im autorisierten. Modus (*Kernel-Mode*) zu nutzen. Obwohl diese Schwachstelle seit längerem bekannt war, wurde der SVC auch in neueren z/OS-Umgebungen installiert und stand jedem Anwender zur Verfügung.
- Aus historischen Gründen wurde ein z/OS-Betriebssystem mit dem RACF-Attribut *OPERATIONS* betrieben. Viele Benutzer, deren Konto über die-

ses Attribut verfügte, konnten nahezu alle Dateien lesen und modifizieren. Die Integrität der Dateninhalte konnte bei diesem z/OS-System nur noch bedingt gewährleistet werden.

- In einem z/OS-System wurde das *SDSF* für *JES2* ohne jeden Schutz zur Verfügung gestellt. Schon nach kurzer Zeit hatten die Mitarbeiter herausgefunden, wie sie die Priorität des eigenen Benutzerkontos im System erhöhen konnten, um ihre Batch-Jobs im System schneller bearbeiten zu lassen. Eine Kontrolle und effiziente Auslastung des Systems waren nicht mehr möglich.

# G 3.68 Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers

Die Übernahme der Default-Einstellungen oder eine fehlerhafte Konfiguration des z/OS-Webservers kann zu Sicherheitsproblemen führen.

- Bei Verwendung der standardmäßig vorgegebenen Einstellungen (*httpd.conf*-Datei) und falsch eingestellten *Userid*-Regeln können durch die *MVSDS* Funktion des Webservers unter Umständen Dateien angezeigt werden, die dem Anwender normalerweise unter seiner Kennung nicht zur Verfügung stehen sollten, wie z. B. Systemdateien.
- Administrationsfehler können dazu führen, dass Prozesse des z/OS-Webservers unter der *Started-Task*-Kennung laufen. Besitzt diese Kennung hohe Rechte im System (z. B. *Superuser)*, kann dies zu Sicherheitsproblemen führen. Datei-Zugriffe und Kommandos erfolgen dann unter der Autorisierung dieser Kennung. Als Folge sind u. U. Zugriffe auf Dateien mit Kundendaten oder, wie vorher beschrieben, auf Systemdateien über die *MVS-Dataset-Display*-Funktion möglich.
- Der z/OS-Webserver unterstützt verschlüsselte Datenkommunikation über das SSL-Protokoll. Bei falscher Konfiguration der Parameter besteht dabei die Gefahr, dass die Verschlüsselung deaktiviert ist oder die Prozesse unter einer anderen RACF-Kennung laufen.

Weitere Gefährdungen werden im Baustein B 5.4 *Webserver* aufgeführt.

**Beispiel:**

- Die Verwendung der Standarddefinitionen eines z/OS-Webservers ermöglichte es einem externen Angreifer, sich sensitive Dateien anzeigen zu lassen. Darüber hinaus war der Webserver so eingestellt, dass der Dienst mit hohen Rechten unter der eigenen *Started-Task*-Kennung lief. Einem externen Angreifer war es dadurch aus dem Internet möglich, die Dateien *SYS1.PROCLIB* und *SYS1.PARMLIB* anzuzeigen. Aus diesen Angaben konnte der Angreifer Informationen herauslesen, die den Angriff auf das gesamte z/OS-System erleichterten.

# G 3.69 Fehlerhafte Konfiguration der Unix System Services unter z/OS

*Unix System Services (USS)* ist ein z/OS-Subsystem, das vor der Inbetriebnahme angepasst werden muss.

Bei der Anpassung der USS-Parameter gibt es eine Reihe von Problemfeldern, die beachtet werden müssen, damit es nicht zu Sicherheitsproblemen beim z/OS-System bzw. bei Teilen des z/OS-Systems kommt.

Je nach Art der Fehlkonfiguration stehen nach dem Start des z/OS-Systems bestimmte Teilfunktionen der *Unix System Services* nicht zur Verfügung bzw. das *USS-Subsystem* startet nicht:

- Fallen Teilfunktionen der USS aus, können wichtige Subsysteme, wie z. B. TCP/IP, fehlen.
- Startet das gesamte *USS-Subsystem* nicht, steht auch das z/OS-Betriebssystem nicht zur Verfügung.
- Werden *HFS-Dateien* während der Startphase nicht allokiert (*Mount*), können Applikationen, die diese Dateien benötigen, nicht betrieben werden.

Im Folgenden sind einige typische Fehler bei der Konfiguration der USS aufgeführt:

- Der komplexe Aufbau der *BPXPRMxx-Member* kann zu Administrationsfehlern führen. Dies hat während des *Initial Program Load (IPL)* einen fehlerhaften Start des Systems zufolge. Dies ist eine Frage der Reihenfolge, in der die einzelnen Member-Definitionen durchlaufen werden.
- Bestimmte Parameter im *BPXPRM00-Member* müssen auf die Kapazitätsgrenzen des Systems abgestimmt sein. Anderenfalls besteht die Gefahr, dass mehr Unix-Prozesse anlaufen, als es das System verkraften kann.
- Es können Fehler bei den *Sysplex*-Definitionen auftreten, z. B. bei der *VERSION*-Angabe.
- Es sind Fehler bei der Definition der *Mount-Policies* von HFS- und zFS-Files (Type, Mode und Mountpoint) möglich.
- Innerhalb der *BPXPRMxx-Member* können Variablen falsch verwendet worden sein.

**Beispiele:**

- Der Aufruf eines rekursiven Unix-Kommandos erzeugte auf einem z/OS-System fortwährend neue Prozesse, bis die z/OS-Auslagerungsdateien (*Page-Platten*) nicht mehr ausreichten. Trotz vorhandener weiterer *Page-Platten*, war es nicht möglich, das System zu retten, da nur noch wenige Systemeingaben möglich waren. Das Problem konnte nur durch einen Neustart (*IPL*) des Systems gelöst werden.
- Auf einem z/OS-System mit mehreren *BPXPRMxx-Membern* wurde eine Parameteränderung in einem falschen Member vorgenommen. Die Änderung wurde vom System nicht berücksichtigt, weil der Parameter während des *IPL* von einem vorhergehenden Member gelesen wurde.

# G 3.70 Unzureichender Dateischutz des z/OS-Systems

Im z/OS-Betriebssystem steuert und überwacht ein Sicherheitssystem, wie RACF, den Dateizugriff. Eine fehlerhafte Administration des Dateischutzes erlaubt es unter Umständen einem Angreifer, unberechtigt auf wichtige Dateien zuzugreifen, z. B. auf Betriebssystemprogramme, auf Konfigurationsdateien oder auf Anwendungsdaten.

RACF sieht beispielsweise vor, dass Benutzerkonten mittels spezieller Attribute (z. B. *Special* oder *Operations*) mit umfassenden Rechten ausgestattet werden können.

Es sollte beachtet werden, dass Daten, auf die ein Anwender lesenden Zugriff hat, unter z/OS immer auch von ihm kopiert werden können.

In diesem Zusammenhang sollte auch die Gefährdung G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten* beachtet werden.

**Beispiele:**
- Die Dateien mit den Lohndaten wurden als Kopie unter der Kennung eines Mitarbeiters angelegt, dessen Benutzerkonto in RACF mit dem Attribut *Universal Access UPDATE* definiert war. Alle Mitarbeiter hatten dadurch nicht nur lesenden Zugriff, sondern konnten die Daten auch modifizieren.
- Aufgrund eines nachlässigen Umgangs mit dem RACF-Attribut *Operations* verfügte ein Anwender über die Möglichkeit, nahezu alle System- und Kundendaten zu lesen oder zu kopieren.

# G 3.71 Fehlerhafte Systemzeit bei z/OS-Systemen

Die Systemzeit (Datum und Uhrzeit) stellt für eine ganze Reihe von Anwendungen und Systemprogrammen eine wichtige Größe dar, von der die korrekte Ausführung einer Vielzahl von Aktionen und die verlässliche Erstellung von Ergebnissen und Daten abhängig ist.

Durch falsche Datums-/Zeitangaben können unter anderem folgende Sicherheitsprobleme und resultierende Schäden entstehen:

- Anwendungen, die Entscheidungen auf Basis des aktuellen Datums treffen, liefern fehlerhafte Ergebnisse. Die Nacharbeitung ganzer Tagesproduktionen kann die Folge sein. Dies gilt insbesondere für Online-Anwendungen und deren Transaktionsdaten. Korrekturen sind oft nicht mehr möglich, wenn z. B. Kunden online auf das System zugreifen.
- Die Analyse von Sicherheitsvorfällen, die Zeitangaben berücksichtigt, kann deutlich erschwert sein oder zu fehlerhaften Ergebnissen führen.
- Differierende Systemzeiten in miteinander verbundenen Systemen sind problematisch, wenn z. B. Log-Daten zu einer gemeinsamen Auswertung herangezogen werden.
- Anwendungen, die Daten von mehreren Einzelsystemen empfangen und in Abhängigkeit der Zeitstempel verarbeiten, liefern verfälschte Ergebnisse.

**Systemzeit bei z/OS-Systemen**

Werden z/OS-Systeme nicht im *Parallel-Sysplex-Cluster* betrieben, muss die Systemzeit in der Regel während des *IPL* (Initial Program Load) manuell durch den Bediener eingegeben werden. Dabei kann es leicht passieren, dass das Datums- oder Zeitfeld falsch gesetzt wird.

Die Änderung der Systemzeit ist auch während des Betriebes möglich. Hier ist die Gefahr von Fehleingaben durch Unachtsamkeit noch größer als bei einem IPL.

In dem *Member Clock00* wird die Zeitzone bzw. die Abweichung von der Greenwich-Mean-Time (GMT) eingestellt. Eine falsche Einstellung der Zeitzone führt zum gleichen Ergebnis als wäre die Systemzeit selbst falsch eingestellt worden.

**Beispiele:**

Während des Betriebs sollte die Zeiteinstellung eines z/OS-Systems um 5 Minuten korrigiert werden. Ein Tippfehler bei der Eingabe des Kommandos *SET* führte zu einer Systemzeit, die in den Abendstunden lag. Der *Job-Scheduler* startete dementsprechend die abendliche Batch-Produktion bereits während des Tages. Weil die Batch-Jobs exklusiv auf die Datenbanken der Anwendung zugriffen, war online keine Dateneingabe mehr möglich.

# G 3.72 Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF

Im z/OS-Betriebssystem ist für den Zugangs- und Zugriffsschutz auf Ressourcen ein spezielles Sicherheitssystem zuständig. Hierfür kommt häufig RACF (*Resource Access Control Facility*) zum Einsatz. Die Konfiguration von RACF im Auslieferungszustand entspricht in der Regel nicht den Sicherheitsanforderungen im jeweiligen Einsatzszenario.

Im Folgenden werden die am häufigsten vorzufindenden Problemfelder in Bezug auf die RACF-Konfiguration beschrieben.

**Gültigkeitsregeln für Passwörter**

Mit dem Kommando SETROPTS können in RACF systemweit gültige Sicherheitseinstellungen des z/OS-Systems, insbesondere für Passwörter, definiert werden. Zu den Parametern gehören die minimale Passwortlänge, die Anzahl der erlaubten Anmeldeversuche, die maximale Gültigkeitsdauer, die Passwort-Historie, Auditeinstellungen und die Klassenaktivierungen.

**Missbrauch von Standard-Passwörter**

Im Auslieferungszustand von z/OS sind für die Kennung *IBMUSER* und das RACF-Kommando *RVARY* Standard-Passwörter voreingestellt. Noch während des Betriebs sind oft die Systemmonitore mit sicherheitskritischen Funktionen über Standard-Passwörter zugänglich.

Die Kennung *IBMUSER* dient als erste Kennung zum Aufbau eines neuen Systems und besitzt *Special*- und *Operations*-Berechtigung. Da die Kennung *IBMUSER* keinem eindeutigen Anwender zugeordnet ist, lässt sich kaum herausfinden, wer diese Kennung benutzt bzw. benutzt hat.

Mit dem RACF-Kommando *RVARY* kann die RACF-Datenbank aktiviert und deaktiviert, d. h. auch gewechselt werden.

Die Standard-Passwörter sind in der Produktdokumentation aufgeführt und damit allgemein bekannt.

**Warning-Modus**

RACF-Ressourcen können im *Warning-Modus* geschützt werden. Dies bedeutet, dass alle Zugriffe auf die Ressource gewährt werden, auch wenn die RACF-Definitionen einen Zugriff auf die Ressource eigentlich verbieten würden. Durch den Warning-Modus werden unter Umständen sehr viel mehr Nachrichten in das Syslog geschrieben und darüber hinaus mehr SMF-Sätze (*System Management Facility*) erzeugt. Dies kann zu einer starken Erhöhung des Plattenspeicherplatzbedarfs führen.

Eine irrtümliche Freigabe von Ressourcen über den Warning-Modus kann zu einem Verlust der Vertraulichkeit von Daten führen.

**Schutz von z/OS-System-Kommandos**

Die z/OS-System-Kommandos werden über spezielle Klassen im RACF geschützt. Durch unzureichende Definitionen dieser Klassen ist es möglich, dass Anwender System-Befehle absetzen können, die unter Umständen den stabilen Systembetrieb beeinträchtigen. Beispiele hierfür sind das Starten oder Stoppen von *StartedTasks* oder das Online-Setzen von Plattensystemen.

**Global Access Checking Table**

Sind Dateien in der *Global Access Checking Table (GAC)* eingetragen, so erfolgt beim Zugriff keine Prüfung über die RACF-Datenbank. Der Anwender bekommt direkten Zugriff gemäß den in der *GAC* definierten Regeln. Werden in der *GAC* irrtümlich Dateien eingetragen, so sind diese nicht mehr über die RACF-Profile geschützt. Diese Dateien können z. B. von allen Anwendern ausgelesen werden, falls sie in der *GAC* mit *READ* eingetragen sind.

**RACF-Datenbank**

Die RACF-Datenbank enthält in verschlüsselter Form alle Passwörter der Benutzer und muss, wie jede andere Datei des z/OS-Betriebssystems, über entsprechende Definitionen geschützt werden. Ist der Zugriffsschutz auf die Datenbank so definiert, dass jeder Benutzer die Datei lesen (und damit auch kopieren) kann (z. B. über die Definition *Universal Access (UACC) = READ*), ist ein Brute-Force-Angriff auf die Passwörter möglich.

**Beispiele:**

- Über das Kommando *RVARY* kann die RACF-Datenbank gewechselt werden. Ein Systemprogrammierer fand heraus, dass das Passwort des Kommandos *RVARY* noch mit dem ausgelieferten Standardpasswort übereinstimmte. Daraufhin konnte er eine andere speziell vorbereitete RACF-Datenbank in das System bringen und aktivieren und hatte Zugriff auf Daten, die er vorher nicht einsehen konnte.
- Nach dem Aufbau einer neuen RACF-Datenbank vergaß ein Bediener, die Kennung *IBMUSER* zu sperren. Ein Sachbearbeiter entdeckte diese Nachlässigkeit und es gelang ihm, unerlaubt Daten aus dem System zu kopieren.
- Die Sicherungskopie einer RACF-Datenbank war aufgrund eines Administrationsfehlers lediglich über die Definition *UACC(READ)* geschützt. Ein Angreifer nutzte dies aus, um die Datenbank auf seinen PC zu kopieren. Auf dem PC führte er mit frei verfügbaren Programmen einen Brute-Force-Angriff auf die Passwörter der RACF-Datenbank aus und war in mehreren Fällen erfolgreich. Der Angreifer nutzte die ihm bekannten Kennungen und Passwörter von anderen Anwendern aus, um Produktionsdaten zu verändern. Der Verdacht fiel zunächst auf den Besitzer der Kennung, die für den Zugriff in den Protokolldateien registriert wurde, und nicht auf den Verursacher des Schadens.

# G 3.73 Fehlbedienung der z/OS-Systemfunktionen

Während des Betriebs des z/OS-Systems sind von Zeit zu Zeit Eingriffe durch die Bediener (*Operators*), wie Anpassungen von RACF-Einstellungen oder anderen Systemdefinitionen, erforderlich.

Aufgrund der Komplexität des z/OS-Betriebssystems und seiner Komponenten lassen sich Fehlbedienungen durch die Bediener nicht vollständig ausschließen. Je nach Art der Fehlbedienung können in der Folge einzelne Komponenten oder das gesamte System ausfallen. Nachfolgend sind einige typische Beispiele für Fehlbedienungen aufgeführt.

**Unbeabsichtigter Neustart über die Hardware Management Console (HMC)**

Der Neustart eines Systems kann über die HMC angefordert werden. Zur Auswahl des Systems genügt ein einfaches Anklicken des System-Icons, danach muss nur noch die Funktion ausgewählt werden (z. B. *Initial ProgramLoad*). Nach Bestätigung einer entsprechenden Rückfrage führt dieser Vorgang umgehend zum Neustart des ausgewählten Systems. Alle laufenden Prozesse werden unkontrolliert beendet. Eine Verwechselung der Systeme kann hierdurch schwerwiegende Folgen nach sich ziehen.

Da in der *HMC* auch Gruppen von Systemen zusammengefasst werden können, bis hin zu allen z/OS-Systemen eines Rechenzentrums, können weite Bereiche der Informationsverarbeitung betroffen sein.

**Fehler beim JES3 DSI (Dynamic System Interchange)**

Das *Job Entry Subsystem* JES3 gestattet den Betrieb eines Systemverbunds, der aus einem *Global*-Rechner und verschiedenen *Local*-Rechnern bestehen kann. Auf alle Rechner im Verbund (*Global* und *Local*) werden unter der Kontrolle des *Global*-Rechners vor allem Batch-Jobs automatisch verteilt und dann dort ausgeführt (ähnlich wie bei einem *Parallel-Sysplex-Cluster*, jedoch auf JES3 beschränkt). Der *Global*-Rechner übernimmt dabei die zentrale Kontrolle des gesamten Lebenszyklus des Batch-Jobs, wie z. B. Interpretation der Job Control Language, Systemzuordnung, Ressourcenkontrolle, Output-Management usw.

Zur Übernahme der Funktion des *Global*-Rechners auf einen *Local*-Rechner sind eine Reihe von Systemfragen zu beantworten. Falsche Angaben können im Extremfall zu einem IPL (*Initial Program Load*) aller Systeme des Verbunds führen.

**Sperrung von z/OS-Kennungen**

Kennungen mit dem Attribut *Special* erzeugen bei mehrmaliger aufeinander folgender Falscheingabe des Passwortes während der Anmeldung eine Konsol-Nachricht (*Reply*). Das Bedienpersonal (*Operator*) kann entscheiden, ob diese Kennung gesperrt werden soll. Werden im Extremfall, z. B. bei einer DoS-Attacke, alle Kennungen mit dem Attribut *Special* gesperrt (z. B. durch Automatismen), existiert auf diesem System keine Kennung mehr, die RACF bedienen kann. Das Sicherheitssystem ist dann in sich gesperrt.

**Offline-Setzen von Platten**

Ein versehentliches *Offline-Setzen* einer Platte kann gravierende Auswirkungen, bis hin zum Totalausfall des Systems, haben.

**Löschen der Default Program Class in RACF**

Wird versehentlich (z. B. durch Tippfehler) das Stern-Profil der Klasse *Program* gelöscht, kann dies zum Stillstand des Systems führen. Ein IPL hilft nicht weiter, da dadurch die Fehlerursache nicht beseitigt wird. Es muss erst die RACF-Datenbank bereinigt werden. Ein solcher Fehler kann einen stundenlangen Ausfall des kompletten Systems und einen erheblichen Aufwand für die Fehlerbeseitigung bedeuten.

**Weiterleiten von fehlerhaften RACF Kommandos**

Wenn ein System in eine RACF-Kommando-Synchronisierung (z. B. *RACF Remote Sharing Facility* - RRSF) eingebunden ist, kann ein fehlerhaftes RACF-Kommando alle anderen Systeme dieses Verbundes betreffen. Wird beispielsweise das Löschen der *Default Program Class* via RRSF übertragen, kann dies zum Stillstand aller Systeme im jeweiligen RRSF-Verbund führen.

**Fehlbedienung vordefinierter Programm-Funktionstasten**

Auch durch die Benutzung vordefinierter Programm-Funktionstasten kann es unter Umständen zu Sicherheitsproblemen kommen. Besondere Sorgfalt ist z. B. geboten, wenn Funktionstasten mit Kommandos belegt werden, die vor der Ausführung noch um bestimmte Werte ergänzt werden müssen. Hier besteht die Gefahr, dass der Operator die Funktionstaste versehentlich drückt, ohne eine Ergänzung einzugeben. Wenn das entsprechende Kommando auch ohne Ergänzung syntaktisch korrekt ist, wird es ausgeführt und bewirkt unter Umständen unerwünschte Effekte oder sogar enorme Schäden.

**Falscheingaben im Allgemeinen**

Generell besteht immer die Gefahr der Falscheingaben. Soll z. B. eine System-Task (oder ein Batch-Job) gestoppt werden und der Bediener vertippt sich, so kann es vorkommen, dass auf Grund von ähnlichen Jobnamen der falsche Job gestoppt wird. Das Gleiche gilt für den Gebrauch von System Kommandos.

Wird z. B. beim Inaktivieren von SNA-Knoten statt eines einzelnen Terminal-Namens versehentlich der *Cross Domain* Manager-Name eingegeben, so bedeutet dies den Verlust aller *SNA Sessions* dieser Domain. Nach dem Neustart des Knotens müssen sich die Anwender neu einloggen und die *SNA*-Verbindung zum System neu aufbauen.

**Verriegelung von Ressourcen**

Bei einer gegenseitigen Verriegelung von Ressourcen (*Enqueue Contention*) können Funktionen so lange nicht verfügbar sein, bis die Verriegelung wieder gelöst wird. Oft sind eine Reihe von System-Abfragen (*Displays*) und viel Betriebserfahrung notwendig, um gegenseitige Verriegelungen mit Hilfe der richtigen MVS-Kommandos wieder aufzulösen.

**Unbeabsichtigte Eingabe des Befehls "Z EOD"**

Wird an einer MVS-Master-Konsole während des Betriebs der Befehl *Z EOD* eingegeben, wird dieses System kontrolliert heruntergefahren. Alle Prozesse

werden beendet und müssen neu aufgesetzt werden. Dieser Vorgang und der damit verbundene Betriebsausfall dauert in der Regel mindestens 30 Minuten.

# G 3.74 Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen

Viele z/OS-Systemeinstellungen lassen sich während des Betriebs verändern, ohne dass ein IPL durchgeführt werden muss. Nach Veränderung einer vorhandenen oder Erstellung einer neuen Parameterdatei (Member der *Parmlib*) löst ein Aktivierungskommando den Änderungsvorgang aus.

Die Sicherheit von z/OS-Systemen kann beeinträchtigt werden, wenn bestimmte Kommandos fehlerhaft bedient oder von Unbefugten missbraucht werden. Die wichtigsten kritischen Parameterdateien und Systemkommandos, durch die im laufenden Betrieb dynamisch Einstellungen geändert werden können, sind im Folgenden aufgeführt.

**Erweiterung der APF-Dateien**

Dateien, die über das *Authorized Program Facility* (APF) autorisiert werden müssen, können in einem *Definitions Member* festgelegt (*PROGnn*) und anschließend mit dem Kommando *SET PROG=nn* (Kommando *SET* und Parameter *PROG=m*) aktiviert werden. Alternativ lassen sich mit dem Kommando *SETPROG APF* (Kommando *SETPROG* und Parameter *APF*) einzelne Bibliotheken in den APF-Mechanismus einbinden. Sind die *Parmlib*-Definitionen oder die passenden Kommandos nicht richtig geschützt, kann es zu Sicherheitsproblemen kommen, da Dritte hierdurch unter Umständen eigene Programme mit hohen Autorisierungen versehen und während des Betriebs aktivieren können.

**Erweiterung des *LINKLIST*-Mechanismus**

Programme, die ohne *Steplib* oder *JoblibDD Statement* in einem Batch-Job verfügbar sein sollen, können in der *LINKLIST* definiert werden. Diese Definitionen sind in einem *PROGnn-Member* der *Parmlib* abgelegt, wobei Dateien durch das Kommando *SETPROG LNKLST* über ein neu zu definierendes Member dynamisch hinzugefügt werden können. Ist die *LINKLIST* in der Systemdefinition (*IEASYSnn*) mit *LNKAUTH=LNKLST* definiert, sind alle Programme, die über diesen Mechanismus geladen werden, automatisch APF-autorisiert. Auch hier ist die Integrität des Systems gefährdet, wenn das Kommando ungeschützt zur Verfügung steht.

**Deaktivierung und Modifizierung der *User Exits***

Durch das Kommando *SETPROG EXIT* ist es möglich, *Exits* zu deaktivieren oder durch andere zu ersetzen. Ist das Kommando nur unzureichend geschützt, kann ein Angreifer unter Umständen auf dem System eigene *Exits* ausführen. Damit lässt sich z. B. das Schreiben von SMF-Sätzen (*System Management Facility*) unterbinden und die Auditierung des Systems beeinflussen (Verschleierung).

**Veränderung der Message Processing Facility (MPF)**

Viele Programme zur Automation von Vorgängen werten Nachrichten (*Messages*) des Systems aus. Durch Setzen anderer MPF-Versionen (*Message Processing Facility*) mit dem Kommando *T MPF=nn* kann die Automation manipuliert oder vollständig ausgeschaltet werden (*T MPF=NO*).

**Austausch von Parmlibs**

Parameterdateien (*Parmlibs*) sind die zentrale Stelle der z/OS-System-Definitionen. Mit Hilfe des Kommandos *SETLOAD* lassen sich vorhandene *Parmlibs* durch neue ersetzen.

**Weitere kritische z/OS-Kommandos für dynamische Änderungen**

Neben den oben beschriebenen Kommandos sind eine Reihe weiterer Kommandos zum Verändern von z/OS-Systemeinstellungen verfügbar, wie z. B. *SETSSI* zum Hinzufügen oder Löschen von Subsystemen oder *SETSMS* zum Verändern der SMS-Definitionen.

Von allen diesen Kommandos, die dynamisch z/OS-Definitionen ändern, können Sicherheitsprobleme ausgehen, wenn sie unkontrolliert im System zur Verfügung stehen. Durch den Missbrauch dieser Kommandos können ähnliche Probleme entstehen wie durch die Manipulation von kritischen Definitions-Dateien.

**Beispiele:**

- Ein Mitarbeiter eines Unternehmens konnte aufgrund eines unzureichenden Schutzes des Kommandos *SETPROG APF* eine eigene Programmdatei autorisieren. Unter Zuhilfenahme eines weiteren Programms, das von dieser Datei geladen wurde, war es ihm möglich, wichtige Finanzdaten zu verfälschen.
- Ein Bediener schaltete mit dem Kommando *T MPF=NO* (T ist eine Kurzform des SET-Kommandos) das *z/OS-Message-Processing* aus. Dies führte zu einer Überlastung der Konsole (Nachrichtenflut) und zur Sperrung einiger dort definierter *Exits*, so dass die Automation des Systems stark behindert wurde.

# G 3.75 Mangelhafte Kontrolle der Batch-Jobs bei z/OS

z/OS-Betriebssysteme werden noch immer in hohem Maße für die Durchführung von Batch-Jobs eingesetzt. Ein Batch-Job besteht aus einem oder mehreren Einzelschritten (Job-Steps).

Die Eingabe zu einem Batch-Job sind entweder eine/mehrere Datei(en) oder entsprechende Steuerkarten, die über das *Job Entry Subsystem (JES2/3)* zugeführt werden. Die Ausgabeverwaltung erfolgt ebenfalls durch das *Job Entry Subsystem*.

Die Steuerung der Batch-Jobs besteht im wesentlichen aus *Start*, *Überwachung* des Ablaufs und der *Prüfung* des Ergebnisses (meist in Form eines *Returncodes*). Je nach *Returncode* müssen darauf häufig Folge-Batch-Jobs gestartet werden. Je höher die Anzahl der Jobs und die Komplexität der Abläufe ist, umso höher ist die Wahrscheinlichkeit eines Fehlers.

**Manuelle Steuerung**

Bei der manuellen Ausführung von Batch-Jobs besteht immer die Gefahr, dass durch menschliche Fehlhandlungen Probleme in den Batch-Abläufen entstehen. Betroffen sind neben dem zeitlichen Ablauf auch die Abhängigkeiten der Batch-Jobs voneinander. Bei zunehmender Zahl der zu steuernden Batch-Jobs erhöht sich deshalb die Komplexität der gesamten Batch-Kette immer drastischer und führt zu einer immer größeren Anzahl von Fehlern. Einer manuellen Steuerung sind deshalb natürliche Grenzen gesetzt.

Zeitliche Verzögerungen können sich z. B. so auswirken, dass ein nach den Batch-Jobs laufendes Online-Verfahren nicht termingerecht gestartet werden kann oder dass Dateisicherungen mit dem Online-Verfahren kollidieren.

**Maschinelle Steuerung (Job-Scheduler)**

Ist ein maschinelles Verfahren (*Job Scheduler*) eingesetzt, stellt dieses zwar den Ablauf sicher. Es können jedoch Fehler auftreten, wenn die Anweisungen an diesen *Job Scheduler* nicht sachgerecht getestet wurden und sich Fehler bei den Anweisungen eingeschlichen haben. Auch durch falsch definierte Automation im Ablauf der Stapelverarbeitung kann es zu fehlerhaften Reaktionen des *Job Schedulers* kommen.

**Beispiel:**

- Der Abbruch eines Batch-Jobs wurde während der Stapelverarbeitung nicht registriert. Erst die Online-Verarbeitung am nächsten Tag zeigte die Fehler in den Datenbeständen. Zur Korrektur musste die Online-Verarbeitung gestoppt, Datenbestände zurückgeladen und danach die Stapelverarbeitung wiederholt werden. In dieser Zeit stand die Online-Verarbeitung nicht zur Verfügung.

# G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

Daten, die auf mobilen IT-Systemen wie Laptops, Mobiltelefonen und PDAs gespeichert sind, werden häufig mit stationären IT-Systemen synchronisiert.

Dabei können allerdings auch Daten zerstört werden. Im Allgemeinen muss vor einer Synchronisation eingestellt werden, wie mit Konflikten beim Datenabgleich umzugehen ist: ob beispielsweise bei gleichlautenden Dateien die des mobilen Endgerätes oder des anderen Endgerätes ungefragt übernommen werden oder ob eine Abfrage erfolgt. Dies wird häufig bei Inbetriebnahme der Dockingstation einmal konfiguriert und gerät danach wieder in Vergessenheit. Werden dann aber Daten in einer anderen Reihenfolge geändert als ursprünglich einmal gedacht, gehen dabei schnell wichtige Informationen verloren. Dieser unangenehme Nebeneffekt kann auch eintreten, wenn mehrere Benutzer ihre mobilen Endgeräte mit demselben Endgerät synchronisieren, ohne daran zu denken, dass gleichnamige Dateien dabei überschrieben werden können.

# G 3.77 Mangelhafte Akzeptanz von Informationssicherheit

Verschiedene Umstände können dazu führen, dass in einer Institution oder auch in Teilen einer Institution die Informationssicherheit nicht akzeptiert wird und damit auch keine Einsicht in die Notwendigkeit besteht, Sicherheitsmaßnahmen umzusetzen. Dies kann beispielsweise bedingt sein durch

- die Behörden- oder Unternehmenskultur (nach dem Motto: "Das war schon immer so!", "Unseren Mitarbeitern können wir vertrauen, hier muss nichts weggeschlossen werden.", "Was soll hier schon passieren?", "Diese Sicherheitsmaßnahmen stören doch nur die Arbeitsabläufe."),
- fehlende Vorbilder, wenn beispielsweise die Vorgesetzten nicht mit gutem Beispiel vorangehen, oder
- ein anderes soziales Umfeld oder einen anderen kulturellen Hintergrund ("andere Länder, andere Sitten"). Typische Probleme können dadurch entstehen, dass bestimmte Benutzerrechte oder auch die Ausstattung mit Hard- oder Software als Statussymbol gesehen werden. Einschränkungen in diesen Bereichen können auf großen Widerstand stoßen.

**Beispiele:**

- Im militärischen Umfeld gehen Vorgesetzte häufig davon aus, dass die Umsetzung von Sicherheitsmaßnahmen befohlen werden kann. Allerdings zeigt auch hier die Erfahrung, dass Mitarbeiter, die nicht über Sinn und Zweck von Sicherheitsmaßnahmen informiert sind, diese umgehen, wenn sie diese nur als Behinderung ihrer eigentlichen Aufgabe ansehen.
- Ein Befehl, nur sichere Passwörter zu verwenden, führte bei einem militärischen IT-System dazu, dass ein Passwort-Generator implementiert wurde. Dieser erzeugte 16-stellige zufällige Passwörter, die einmalig 10 Sekunden am Bildschirm angezeigt wurden. Diese Zeitspanne reichte aus, um die Passwörter aufzuschreiben. Da es vielen Leuten schwer fällt, sich Passwörter der Form "aN§3bGP?tz1BuH89" zu merken, wurden diese Zettel entgegen der Anweisungen nicht vernichtet, sondern häufig in der Nähe der Rechner aufbewahrt.
- Gerade Smartphones oder Tablets werden als Statussymbol angesehen, wodurch die Bereitschaft sinkt, Anweisungen zur Informationssicherheit zu befolgen, wie beispielsweise die Geräte nicht für private Zwecke zu benutzen. So gibt es Fälle, in denen Mitarbeiter die Sicherungsmaßnahmen der IT-Abteilung durch "rooten" beziehungsweise "jailbreaking" aktiv umgingen, um gesperrte Applikationen zu installieren. Diese hatten dann allerdings das Recht, das Telefonbuch auszulesen, wodurch die dort gespeicherten Kundendaten in unbefugte Hände gerieten.

# G 3.78 Fliegende Verkabelung

In Besprechung-, Veranstaltungs- und Schulungsräumen wechseln häufig sowohl die Benutzer als auch die Nutzungsart. Damit wird mitunter die Geräteausstattung und damit natürlich auch die Verkabelung in solchen Räumen geändert. Je nach Lage der Anschlusspunkte im Raum (Steckdosen der Stromversorgung und des Datennetzes) kann das dazu führen, dass Kabel quer durch den Raum, auch über Verkehrswege hinweg verlegt werden. Solche "fliegenden" Kabel sind nicht nur Stolperfallen für Personen. Wenn jemand daran hängen bleibt, kann das auch zu Schäden an IT-Geräten führen:

- Im einfachsten Fall wird lediglich eine Steckverbindung gelöst und die entsprechende Verbindung unterbrochen.
- Durch den plötzlichen Zug am Kabel kann aber die Steckverbindung beschädigt oder zerstört werden. Darüber hinaus kann aber auch, besonders bei verschraubten Steckern, das angeschlossene Gerät vom Tisch auf den Boden stürzen und dabei beschädigt werden.

# G 3.79 Fehlerhafte Zuordnung von Ressourcen des SAN

Betriebssysteme reagieren unterschiedlich auf sichtbare Speicherressourcen. Wenn keine eindeutige und starke Zuordnung von Servern und Speicherressourcen vorgenommen wird, können unautorisierte Zugriffe auf Speicherressourcen, z. B. durch andere Server, das Schutzkonzept auf Ebene des Betriebssystems oder der Anwendung unterlaufen.

An dieser Stelle ist nicht nur der vorsätzliche Angriff zu betrachten, bei dem ein Angreifer versucht, Lücken der Konfiguration für seine Absichten auszunutzen. Beachtlich ist auch die Eigenart mancher Betriebssysteme, alle erreichbaren Festplatten an sich zu binden und in die eigene Hardwarekonfiguration einzubinden.

Gerade Windows Server neigen dazu, alle sichtbaren Speicherressourcen zu beanspruchen. Bei einem Speichernetz kann es so vorkommen, dass Speicherbereiche, die anderen Systemen zugeordnet sind, diesen entzogen werden oder Daten darauf verfälscht oder zerstört werden.

# G 3.80 Fehler bei der Synchronisation von Datenbanken

Um die Daten einer Datenbank an verschiedenen Standorten oder auf mobilen Endgeräten zu halten, werden oft Datenbanken oder Auszüge davon gespiegelt. Damit diese Daten untereinander abgeglichen werden können, ist eine Datenbanksynchronisation erforderlich.

Bei der Synchronisation kann es zu Konflikten und damit zu einem Datenverlust kommen, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbanken geändert bzw. gelöscht haben. Oft helfen hier auch nicht die im System konfigurierten Regeln, welche Daten unter welchen Bedingungen überschrieben werden, da die Datenänderungen im Normalfall inhaltlich betrachtet werden müssen. Selbst wenn diese Regeln für alle Synchronisationen gelten, sind diese Regeln nicht immer allen Anwendern bekannt und führen dadurch gegebenenfalls zum falschen Ergebnis.

Synchronisationen zwischen Datenbanken an verschiedenen Standorten werden im Normalfall automatisiert durchgeführt. Konflikte werden dabei häufig erst erkannt, wenn ein Datenbank-Administrator die Datenbank öffnet bzw. die Log-Dateien analysiert. Der Datenbank-Administrator kann oft aufgrund mangelnder Befugnisse und Kenntnisse bezüglich der Dateninhalte nicht entscheiden, wie der Konflikt zu lösen ist. Dies trifft auch zu, wenn die Synchronisation manuell angestoßen wurde, aber die Synchronisations-Programme den Anwender nicht über auftretende Konflikte informieren.

Mobile Endgeräte werden meist manuell synchronisiert. Dabei bieten einige Datenbanken die Möglichkeit, die Benutzer über Konflikte zu informieren. Dennoch kann ein Benutzer nicht immer über die Synchronisation der Daten entscheiden, wenn ihm nicht alle Umstände der Datenänderungen bekannt sind.

# G 3.81 Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003

Windows Server ab Version 2003 ermöglicht die Übernahme von Einstellungen aus Vorlagen direkt in die Systemkonfiguration. Dafür existieren drei Vorlagentypen:

- Dateien mit der Erweiterung *.inf*, ab Windows Server 2003 *Sicherheitsvorlagen* genannt, werden im Sicherheitskonfigurations-Editor (SCE) bearbeitet.
- XML-Vorlagen, ab Windows Server 2003 mit Service Pack 1 als *Sicherheitsrichtlinien* bezeichnet, werden mit dem Sicherheitskonfigurations-Assistenten (SCW) bearbeitet.
- Dateien mit der Erweiterung *.pol* (Windows NT 4.0-Vorlagen) können ebenfalls auf Windows Server 2003 angewendet werden.

Alle genannten Typen werden nachfolgend Sicherheitsvorlagen genannt. Sie verändern die Systemkonfiguration, sobald sie angewendet werden.

Neben sogenannten Sicherheitsvorlagen existieren administrative Vorlagen (Erweiterung *.adm*).

Mit Windows Vista wurden die ADM-Dateien durch ADMX-Vorlagedateien ersetzt, die eine neue Syntax auf XML-Basis für die Registry-basierten Richtlinien verwenden. ADMX-Dateien bieten den Vorteil, dass sie, im Gegensatz zu ADM-Dateien, sprachneutral sind und in Verbindung mit sprachspezifischen ADML-Dateien auf beliebige Sprachversionen angewendet werden können.

In Unterschied zu ADM-Dateien werden ADMX-Dateien nicht mehr einzeln in jedes Gruppenrichtlinienobjekt geladen, sondern in einem zentralen Speicher verwaltet. Da sich die Gruppenrichtlinien-Snap-ins *Gruppenrichtlinienverwaltung* und *Gruppenrichtlinienobjekt-Editor* standardmäßig mit dem PDC-Emulator verbinden, wird in einer Active Directory-basierten Umgebung die zentrale Speicherung der ADMX/ADML-Dateien im SYSVOL-Verzeichnis auf diesem Betriebsmaster empfohlen. Die Betriebsmasterrolle PDC-Emulator emuliert einen Primary- oder Backup-Domain-Controller unter Windows NT, um für Abwärtskompatibilität zu sorgen.

Es ist auch möglich, eigene administrative Vorlagen zu definieren. Diese Vorgehensweise empfiehlt sich vor allem, wenn in der Institution reger Gebrauch von direkten Registry-Einstellungen gemacht wird. Durch die einmalige Definition einer administrativen Vorlage können die entsprechenden Registry-Einstellungen komfortabel über den Gruppenrichtlinien-Mechanismus verteilt werden. Dies stellt unter anderem sicher, dass die Registry-Einstellungen tatsächlich auf allen Zielrechnern umgesetzt werden.

Da Sicherheitsvorlagen die Systemkonfiguration tiefgreifend ändern, besteht die Gefahr, dass bestimmte Funktionen oder der ganze Server nicht mehr verfügbar sind, wenn diese nicht getestet wurden. Werden sie mit Hilfe von Gruppenrichtlinien oder Skripten automatisch auf mehrere Server ausgerollt, kann der Betrieb im gesamten Informationsverbund gestört werden und sogar vollständig ausfallen.

Durch unsachgemäßen Umgang mit Sicherheitsvorlagen ergibt sich daher ein hohes Gefährdungspotential.

Mögliche Gefährdungen können ihre Ursache bereits in einem fehlerhaften Verhalten bei der Erstellung von Sicherheitsvorlagen haben. Der Erstellung geht meist die Analyse von Anforderungen voraus. Anschließend wird ein Referenzsystem manuell vom Administrator oder automatisch durch den SCW analysiert. Die Analyseprozesse umfassen viele Komponenten des Servers und betreffen Einstellungen, die tief in das Betriebssystem eingreifen. Die Analyseprozesse können unvollständig bleiben oder unbemerkt aus technischen Gründen fehlschlagen. Die zugrunde liegenden Sicherheitsdatenbanken und Sicherheitskataloge können korrupt oder nicht aktuell sein. Außerdem können Programme von Drittherstellern oder eine spezielle Systemkonfiguration unvorhergesehenen Einfluss auf den Analysevorgang haben.

Der SCW kann Sicherheitsvorlagen des SCE umwandeln und in seine *Sicherheitsrichtlinien*-Dateien mit einbinden. Hieraus können sich Konflikte von bestimmten Parametern ergeben. Sicherheitsvorlagen insgesamt können zwar von den Verteilungsmechanismen von Active Directory und Gruppenrichtlinien profitieren, allerdings müssen dazu alle Vorlagentypen in Gruppenrichtlinienobjekte umgewandelt oder - im Falle von *.pol*-Dateien aus Windows NT 4.0 - migriert werden. Dabei können ebenfalls Konflikte oder Kompatibilitätsprobleme auftreten.

Das Einspielen von Sicherheitsvorlagen auf einen Server kann fehlschlagen, wenn der Server nicht den Voraussetzungen für die jeweilige Vorlage entspricht. Alte Applikationen, die nicht für aktuelle Windows-Versionen entwickelt wurden, führen häufig zu unerwarteten Effekten.

Außerdem können Berechtigungseinstellungen, die in der Vorlage auf *Verweigern* gesetzt sind, unerwartetes Verhalten verursachen, das sehr schwer zu beheben ist.

Bei allen beschriebenen Punkten besteht die Gefahr, dass eine Vorlage nicht die geplante Wirkung erzielt und das System in einen unvorhergesehenen Zustand versetzt wird.

Die Gefahren verschärfen sich erheblich, wenn beim Entwickeln und Ausrollen von Sicherheitsvorlagen auf Tests verzichtet wird oder wenn die im Test verwendeten Referenzsysteme nicht repräsentativ sind.

Schließlich kann auch eine unzureichende technische und organisatorische Durchsetzung und Kontrolle der Verteilungsmechanismen von Sicherheitsvorlagen den Informationsverbund gefährden. Wenn Ausrollvorgänge unbemerkt fehlschlagen, ergeben sich Inkonsistenzen zwischen Servern. Die Konfiguration ist somit entspricht somit nicht flächendeckend den Vorgaben, so dass auch die Sicherheitsziele nicht erreicht werden. Beim Entwickeln und inkrementellen Ausrollen weiterer Vorlagen entsprechen einige Zielsysteme auch nicht mehr den erwarteten Voraussetzungen. Dieser Zusammenhang wird auch als fehlende Richtlinien-Konformität bezeichnet.

Sicherheitsvorlagen aus Windows NT 4.0 (*.pol*-Dateien) bergen verstärkt das Risiko von Konformitätsproblemen und Inkompatibilitäten mit anderen Vorlagentypen. Für *.pol*-Dateien werden ab Windows Server 2003 keine Werkzeuge mehr mitgeliefert und es gibt keine Herstellerunterstützung.

# G 3.82 Fehlerhafte Konfiguration der VoIP-Middleware

Eine VoIP-basierte Telefonanlage kann in ähnlicher Weise von Fehlkonfigurationen betroffen sein wie eine leitungsvermittelnde Telefonlösung. Dies reicht von falschen Zuordnungen von Telefonbenutzern zu Telefonnummern bis hin zu einem Verlust der Verfügbarkeit der Telefoninfrastruktur. Auch eher unkritische Fehler, wie ein falsch geschriebener Name im Telefonbuch, sind natürlich nicht auszuschließen.

Weiterhin können über die Telefonanlage bestimmten Benutzern Privilegien beim Telefonieren zugeordnet oder entzogen werden. Beispiele sind Telefonverbindungen ins Ausland oder der Anruf kostenpflichtiger Service-Rufnummern. Eine Fehleinstellung kann hier einen Missbrauch ermöglichen, wenn beispielsweise ein allgemein zugängliches Telefon Auslandsberechtigung erhält.

Beim Einsatz von VoIP sind in der Regel mehrere Systeme integriert. Wird SIP als Initialisierungsprotokoll eingesetzt, werden meist Systeme wie Registrare, SIP-Proxy-Server und Location-Server für die Kommunikation benötigt. Bei Veränderungen müssen alle Systeme angepasst werden, wodurch Konfigurationsfehler entstehen können. Auch wenn sich alle Dienste auf einem Rechnersystem befinden, müssen häufig alle einzeln konfiguriert werden. Wird eine Änderung nur auf einem System nicht korrekt durchgeführt, kann die gesamte Telefoninfrastruktur möglicherweise nicht mehr genutzt werden.

Bei VoIP wird in der Regel kein klassischer Anrufbeantworter eingesetzt, sondern es wird im Falle der Abwesenheit oder Nichtverfügbarkeit des Benutzers eine Voice-Mail versendet. Dies ist oft eine E-Mail, an die eine Sprachmitteilung als Audio-Datei angefügt ist. Passiert während der Konfiguration ein Tippfehler bei der E-Mail-Adresse, erhält der eigentliche Empfänger die eingegangenen Nachrichten nicht. Es kann sogar passieren, dass sie stattdessen an einen falschen Empfänger zugestellt werden.

Neben den eigentlichen VoIP-Vermittlungssystemen müssen auch die Router und Switches, die auf tieferen Netzschichten operieren, konfiguriert werden. Um Verzögerungen bei der Vermittlung zu vermeiden, kann bei vielen Geräten eingestellt werden, dass VoIP-Nachrichten bevorzugt weitergeleitet werden. Fehler bei der Konfiguration können hier im schlimmsten Fall zu einem Komplettausfall des Netzes führen.

# G 3.83 Fehlerhafte Konfiguration von VoIP-Komponenten

Unabhängig davon, ob es sich bei VoIP-Komponenten um dedizierte Hardware (Appliances) oder softwarebasierte Systeme handelt, spielt die Konfiguration eine entscheidende Rolle. Neben den Einstellungen zur Signalisierung, die im Verlauf der Planung festgelegt wurden, spielt das Übertragungsverfahren für die Medienströme eine wichtige Rolle. Durch ein Kompressionsverfahren kann die Größe der IP-Pakete mit den Sprachinformationen verkleinert werden.

Sehr oft führt der Einsatz eines ungeeigneten Verfahrens, das die Sprachinformationen zu stark komprimiert, zu einer Verschlechterung der Sprachqualität. Wird hingegen ein Verfahren gewählt, das eine zu geringe Kompression vornimmt, wird der Nachrichtenstrom nicht ausreichend vermindert und das IP-Netz kann überlastet werden.

Um die Vertraulichkeit der Telefongespräche zu schützen, kann bei einigen wenigen Protokollen zur Medienübertragung, wie SRTP, eine Verschlüsselung genutzt werden. Um der Protokollierung an eventuell benötigten Vermittlungssystemen entgegenzuwirken, kann bei vielen verschlüsselten Protokollen die Verschlüsselung direkt zwischen den Endgeräten erfolgen. Eine Fehlkonfiguration kann dabei zu einer unverschlüsselten Übertragung führen, möglicherweise sogar ohne dass dies von den Benutzern bemerkt wird. Werden zu schwache Verschlüsselungsverfahren oder zu kurze Schlüssellängen gewählt, kann ein Angreifer die Kommunikation unter Umständen trotz Verschlüsselung mithören.

Nicht nur das Abhören von Gesprächen kann für einen Angreifer interessant sein. Auch die Informationen, die bei der Signalisierung übertragen werden, können von einem Angreifer missbraucht werden. Wird durch eine fehlerhafte Einstellung im Endgerät das Passwort bei der Anmeldung im Klartext übertragen, könnte der Angreifer sich beispielsweise für einen anderen Benutzer ausgeben, obwohl alle beteiligten VoIP-Komponenten sicherere (Challenge-Response-) Verfahren unterstützen. Durch diesen Identitätsdiebstahl könnte der Angreifer auf Kosten des Opfers telefonieren oder weitere Dienste, wie das Abhören vom Anrufbeantworter, missbrauchen.

Sehr oft werden Applikationen, wie Softphones oder softwarebasierte Telefonanlagen, auf einem Standard-PC betrieben. Hierfür muss ein handelsübliches Betriebssystem installiert sein, auf dem die Programme ausgeführt werden. Fehler in der Administration und Konfiguration des Betriebssystems können große Auswirkungen auf den Betrieb und die Sicherheit der VoIP-Applikationen haben.

Unabhängig davon, ob auf dem IT-System ein Endgerät (Softphone) oder eine Vermittlungsanlage (Software-TK-Anlage) betrieben wird, können durch eine fehlerhafte Verteilung von Zugriffsrechten auf der einen Seite bestimmte Funktionalitäten nicht genutzt oder auf der anderen Seite fälschlich vergebene Zugriffsrechte missbraucht werden.

# G 3.84 Fehlerhafte Konfiguration der WLAN-Infrastruktur

Access Points und andere WLAN-Komponenten bieten eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch die Nutzung von Sicherheitsfunktionen betreffen. Werden hier falsche Einstellungen vorgenommen, dann kann es passieren, dass entweder keine Kommunikation über den Access Point möglich ist oder die Kommunikation unzureichend geschützt erfolgt, obwohl die Benutzer von einem vorhandenen Schutz ausgehen. Durch fehlerhafte Konfiguration von WLAN-Komponenten können diverse Sicherheitsprobleme entstehen, beispielsweise:

- Falls ein Access Point ungenügend gegen unbefugten Zugriff abgesichert ist, könnte jemand hieran Konfigurationsänderungen vornehmen, die zu weiteren Sicherheitslücken führen.
- Durch eine uneinheitliche Konfiguration der WLAN-Sicherheitsmechanismen auf den Access Points, können sich Verfügbarkeitsprobleme oder Sicherheitslücken ergeben.
- Sofern über ein WLAN auf das Internet zugegriffen werden kann, ist ohne weitere Filtermechanismen eine Internet-Nutzung durch jeden möglich, der sich mit dem WLAN verbinden kann.
- Eine zu freizügige Freigabe von Verzeichnissen oder anderen Systemressourcen bei einem WLAN-Client kann einem Angreifer einen unbemerkten Zugriff auf den Client ermöglichen.
- Bei einer nicht korrekt konfigurierter oder durch den Benutzer ausgeschalteten Personal Firewall eines WLAN-Clients ist dieser unter Umständen Angriffen auf Betriebssystem-Ebene ausgesetzt. Dies ist besonders in fremden Umgebungen und Hotspots problematisch.

Sicherheitsprobleme bereiten auch immer wieder Remote-Support-Zugänge auf WLANs, wenn sie nicht ausreichend abgesichert sind und über unsichere Netze genutzt werden. Sofern hier Fehlkonfigurationen vorgenommen wurden, kann dies beispielsweise dazu führen, dass es ein WLAN-Client kompromittiert wird und ein Angreifer hierbei Informationen über den Zugriff auf das WLAN erlangt. Diese Informationen können anschließend zum Angriff auf das komplette WLAN und ein eventuell damit verbundenes LAN verwendet werden.

# G 3.85 Verletzung von Brandschottungen

Jedes Gebäude, in dem IT betrieben wird, ist von einer Vielzahl von Leitungen und Kabeln durchzogen. Frisch- und Abwasserleitungen, Heizungsrohre, Energieversorgung und Datenübertragung seien als Beispiele genannt. Es ist dabei unvermeidlich, dass solche Rohr- und Kabel-Trassen Brandschutzwände und Geschossdecken queren müssen. Wenn an solchen Stellen keine geeigneten Brandschottungen eingebaut sind (siehe M 1.9 *Brandabschottung von Trassen*), können sich hierüber unter Umständen Brände und Rauch unkontrolliert ausbreiten.

Im Laufe der Gebäudenutzung ist es meist unumgänglich, Arbeiten an solchen Trassen durchzuführen oder neue Trassen zu verlegen, sei es zu Reparaturzwecken oder um Platz für zusätzlich erforderlich gewordene Leitungen zu schaffen.

Bei solchen Arbeiten müssen unter Umständen Brandschottungen teilweise oder ganz entfernt werden. Zusätzliche Kabel verändern außerdem die Brandlast der Kabeltrasse. Folge daraus ist, dass während und nach den Arbeiten der baulich vorbeugende Brandschutz mitunter massiv beeinträchtigt sein kann.

Leider zeigt die Erfahrung, dass die mit solchen Arbeiten betrauten Personen (in der Planung, in der Ausführung und in der Abnahme) die Tragweite ihrer Arbeiten für den Brandschutz häufig nicht richtig einschätzen und entsprechend handeln:

- Ersatzmaßnahmen für entfernte Brandschottungen werden weder geplant noch realisiert.
- Beschädigte Brandschottungen werden nicht umgehend ordnungsgemäß wiederhergestellt.
- Brandschutzmaßnahmen werden den neuen Gegebenheiten nicht angepasst.

Folge dieser Fehlhandlungen ist ein erhöhtes Risiko der Brandentstehung und der Ausbreitung von Feuer und Rauch. Sofern notwendige Flure, Flucht- und Rettungswege betroffen sind, wird dadurch nicht nur die IT, sondern auch die Gesundheit und das Leben von Personen gefährdet, was massive Haftungsfolgen haben kann.

**Beispiel:**

- In einem mehrgeschossigen Bürogebäude wurden verschiedene Netze über eine gemeinsame Steigetrasse aus dem Keller bis in das oberste Geschoss geführt. Alle Deckendurchbrüche waren mit reichlich Reserve hergestellt, nach Verlegung der Leitungen allerdings nicht wieder verschlossen worden. Im Keller wurden im Bereich des Trassenbeginns große Papier- und Stoffmengen gelagert. Die direkt darüber beginnende Steigetrasse hätte im Brandfall wie ein Kamin gewirkt. Rauch und Feuer hätten sich in kürzester Zeit über alle Etagen ausgebreitet.

# G 3.86 Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten

In jeder Institution sind Informationen zu finden, die nicht für die Öffentlichkeit bestimmt sind. Dies können Ergebnisse aus der Entwicklung, Strategiepapiere oder andere vertrauliche Informationen sein. Die Vervielfältigung dieser Dokumente wird in der Regel kontrolliert, damit diese Informationen nicht an Unbeteiligte weitergegeben werden können.

Beim Bestreben, ein möglichst hohes Sicherheitsniveau für alle mit IT verarbeiteten Informationen zu erreichen, dürfen die analog vorliegenden Informationen nicht vernachlässigt werden. Dies betrifft beispielsweise Ausdrucke, Papierakten oder Mikrofilme. Die stärkste Verschlüsselung ist nutzlos, wenn das verschlüsselte Dokument nach dem Entschlüsseln ausgedruckt wird und von Unberechtigten eingesehen werden kann.

Bei Netzdruckern verbleiben oft die ausgedruckten Dokumente eine längere Zeit im Ausgabefach des Druckers. Insbesondere, wenn sich die Drucker nicht im direkten Umfeld der Benutzer befinden, drucken die Benutzer häufig mehrere Dateien, bevor sie alle zusammen abholen. Da Etagen- oder Abteilungsdrucker von einer Vielzahl von Personen genutzt werden, haben damit auch viele Personen die Möglichkeit, Ausdrucke einzusehen oder zu entwenden.

Wenn Ausdrucke nicht sofort abgeholt werden, erhöht sich die Wahrscheinlichkeit, dass sie eingesehen werden oder ganz verschwinden. Dies muss nicht böswillig geschehen. Wenn Mitarbeiter, die den Drucker ebenfalls nutzen, beispielsweise eine längere Zeitspanne auf ihren Ausdruck am Gerät warten müssen, werden sie eventuell die Wartezeit überbrücken und schauen, was andere Kollegen ausgedruckt und nicht abgeholt haben.

Auch an Kopierern finden sich immer wieder vertrauliche Dokumente, die dort beispielsweise im Einzug vergessen wurden.

Benutzer suchen häufig nicht nach Ursachen, wenn ihre Ausdrucke sich nicht am Drucker finden. Stattdessen vermuten sie IT-Probleme und starten einen neuen Druckauftrag, da sie daran gewöhnt sind, dass mit der Hard- und Software immer wieder Probleme und auch unerklärliche Phänomene auftreten. Die Ausdrucke könnten allerdings auch von anderen mitgenommen worden sein. Ebenso kommt es häufig vor, dass Benutzer an ihrem Arbeitsplatz-Rechner versehentlich einen anderen Drucker ausgewählt haben als den, den sie üblicherweise verwenden. Typischerweise suchen dann die Benutzer ihre Ausdrucke am falschen Drucker, finden sie dort nicht und starten einfach einen neuen Druckauftrag, diesmal an den Standard-Drucker. Dadurch finden sich an vielen Netzdruckern Fehlausdrucke, die nicht abgeholt werden.

**Beispiel:**

- Fehldrucke werden von einem Benutzer schon im Druckerraum bemerkt und dort direkt im Papierkorb entsorgt. Ein weiterer Mitarbeiter, der auf einen Druckauftrag warten muss, benutzt die Rückseite des weggeworfenen Ausdrucks für Notizen. Als diese Notizen im Rahmen einer Besprechung an eine externe Firma weitergegeben werden, gelangt auch der Fehldruck mit internen Informationen an Externe.

# G 3.87 Fehlerhafte Konfiguration von Verzeichnisdiensten

Fehlkonfiguration von Software ist eine der häufigsten Ursachen für erfolgreiche Angriffe. Bei Verzeichnisdiensten können durch die hohe Komplexität und die große Zahl der verfügbaren Parameter durch unbeachtete Seiteneffekte zusätzliche Sicherheitsprobleme eintreten. Fehlkonfigurationen können in folgenden Bereichen besonders schwerwiegende Auswirkungen haben:

- Zertifikatsserver,
- Erstellung und Definition der Baumstruktur an sich,
- Einrichtung der abzubildenden Objekte,
- Zugriffsmechanismen,
- Vergabe der Zugriffsrechte,
- LDAP-Zugriff auf den Verzeichnisdienst,
- Partitionierung der Verzeichnisdatenbank,
- Replikation des Verzeichnisdienstes,
- Intranet-Clientzugriff auf den Verzeichnisdienst,
- Real-time Alert-Mechanismus,
- Festlegung der aufzuzeichnenden Events,
- Zugriffsrechte des Administrator-Werkzeugs sowie
- Einstellung eines automatisierten Backup-Mechanismus.

Die Konfiguration eines Systems muss grundsätzlich an dessen Sicherheitsrichtlinie ausgerichtet werden. Bei Fehlkonfigurationen besteht die Gefahr, dass eine solche Richtlinie unzureichend oder fehlerhaft umgesetzt wird und somit die Zielsetzungen der Sicherheitsvorgaben nicht erreicht werden.

Die Konfiguration einer rollenbasierten Administration des Verzeichnissystems sowie eine Delegation von Administrationsrechten sind in der Regel zentrale Funktionalitäten eines Verzeichnisdienstes Durch eine fehlerhafte Konfiguration dieser Funktionalitäten ergeben sich unter Umständen erhebliche Probleme durch unautorisierte Systemzugriffe. Ferner besteht bei einer fehlerhaften Konfiguration die Gefahr, dass eine geregelte Administration nicht mehr möglich ist.

Nachfolgende Liste zeigt mögliche sicherheitsrelevante Konsequenzen bezüglich einer Fehlkonfiguration des Verzeichnisdienstes auf:

- Fehlerhafte Vergabe von Rechten für den Zugriff auf die Objekte des Verzeichnisdienstes,
- Auswahl zu schwacher kryptographischer Authentisierungsmechanismen,
- unautorisierte Systemzugriffe über Administrationsschnittstellen,
- Blockade der Administrationsmöglichkeit des Systems,
- unzureichender Schutz vor Systemangriffen,
- fehlerhafte oder unperformantes Speichern der Daten in mehreren Verzeichnisdatenbanken (Replikation) sowie
- Unstimmigkeiten in der Umsetzung der Sicherheitsrichtlinie.

# G 3.88 Falsche Vergabe von Zugriffsrechten

Aufgrund der engen Beziehung zwischen dem Verzeichnisdienst und zu dem darunter liegenden Betriebssystem und der Tatsache, dass Verzeichnisdienste eine Reihe kritischer Daten von Systembenutzern und über Ressourcen enthalten, ist die korrekte Vergabe von Zugriffsrechten auf den Verzeichnisdienst besonders sicherheitskritisch.

Die Zugriffskontrolllisten selbst sind so genannte Attribute (Properties) zu den jeweiligen Objekten. Zugriffsrechte existieren auf Objekte an sich, aber auch auf einzelne Attribute eines Objekts. Die Zugriffsrechte auf Objekte vererben sich standardmäßig von Vater- auf Kind-Objekte innerhalb der Baumhierarchie. Durch ungeeignete Partitionierung des Verzeichnisses können dabei Brüche dieses Vererbungsmechanismus entstehen.

Auch besteht die Gefahr, dass durch die Vielfalt an Konfigurationsmöglichkeiten der Zugriffsrechte inkonsistente oder falsche Zugriffsmöglichkeiten vergeben werden könnten. Sofern die Zugriffsrechte im Verzeichnisdienst falsch vergeben werden, ist dadurch die Sicherheit des Gesamtsystems erheblich gefährdet. Es könnten beispielsweise die Vertraulichkeit und die Integrität von Daten beeinträchtigt sowie mögliche Hintertüren (Backdoors) für weitreichende Systemangriffe eröffnet werden.

Ein besonders kritischer Punkt ist auch die Vergabe der Administrationsrechte wie beispielsweise die Umsetzung eines rollenbasierten Administrationskonzeptes oder die Delegation einzelner Administrationsaufgaben durch die Vergabe entsprechender Zugriffsrechte. Werden diese Rechte falsch vergeben, kann das gesamte Administrationskonzept in Frage gestellt und unter Umständen sogar die Verzeichnissystem-Administration blockiert werden.

# G 3.89 Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste

LDAP eignet sich vor allem dann als Protokoll für Zugriffe auf Verzeichnisdienste, wenn die Zugriffe durch weitere Applikationen, wie z. B. Internet- oder Intranet-Anwendungen, erfolgen. Ist der LDAP-Zugriff falsch konfiguriert, kann es jedoch zu folgenden Problemen kommen:

- Falsche Vergabe von Zugriffsrechten und unautorisierte Zugriffsmöglichkeiten auf den Verzeichnisdienst
  Wenn Verzeichnisdienste von unterschiedlichen Herstellern eingesetzt werden, kann es bei LDAP-Einstellungen zu Problemen kommen, die auf Erweiterungen eines bestimmten Verzeichnisdienstes, beispielsweise Active Directory oder Novell eDirectory, basieren. Darüber hinaus kann es passieren, dass Benutzern aufgrund der eventuell inkompatiblen LDAP-Syntax falsche Rechte zugewiesen werden. Hierdurch kann es unter anderem dazu kommen, dass Benutzer ungewollt auf Bereiche zugreifen dürfen, für die sie eigentlich keine Rechte haben sollten.
- Übermittlung von Benutzerpasswörtern im Klartext und Ausspähen von unverschlüsselten Informationen
  Da LDAP ein rein textbasiertes Protokoll ist, werden alle Informationen, auch Benutzerpasswörter, im Klartext übertragen und könnten dabei ausgespäht werden. Deswegen sollte LDAP zusätzlich abgesichert werden, zum Beispiel durch eine SSL-Verschlüsselung. Jedoch ergeben sich bei der SSL-Konfiguration ebenfalls Fehlermöglichkeiten, die zu einer Herabsetzung des Sicherheitsniveaus führen können.
- Fehler beim LDAP-Zugriff, insbesondere für netzbasierte Anwendungen
  Hierbei können Anmeldeversuche sporadisch fehlschlagen, obwohl die richtigen Authentisierungsinformationen verwendet werden. Dies kann beispielsweise durch unterschiedliche LDAP-Konfigurationen auf den einzelnen Verzeichnisdienstkomponenten entstehen.
- Beeinträchtigung der Verfügbarkeit des Verzeichnisdienstes durch die Verschlüsselungseinstellungen von LDAP
  Durch Fehlkonfiguration, falsches Vorgehen und falsche Aktivierungsreihenfolge beim Vornehmen der Signierungs- und Verschlüsselungseinstellungen von LDAP kann die Verfügbarkeit für weite Teile des Verzeichnisdienstes stark beeinträchtigt werden. Bei größeren Umgebungen kann das Zurückversetzen des Verzeichnisdienstes in einen funktionstüchtigen Zustand sehr hohen Aufwand verursachen, da in einer solchen Situation viele netzbasierte Verwaltungs- und Steuerungsfunktionen gestört sind. Die Auswirkungen dieser inkonsistenten Einstellungen machen sich unter Umständen erst nach einer gewissen Zeit bemerkbar.
- Unzureichende Produktivität des Gesamtsystems durch unterschiedliche LDAP-Versionen
  Wenn die Clients unterschiedliche LDAP-Versionen unterstützen, bestehen unter Umständen abweichende Konfigurationsmöglichkeiten. Verwenden beispielsweise Clients eine ältere LDAP-Version, kann es sein, dass neue Befehlssätze nicht unterstützt werden oder noch Schwachstellen in den Funktionen vorhanden sind usw. Auch die Unterstützung der verschiedenen LDAP-Versionen durch die Clients und die damit zusammenhängenden Konfigurationsmöglichkeiten können zu Fehlern führen, die die Sicherheit des Betriebes beeinträchtigen.
- Nicht oder unzureichend eingeschränkte Suchfilter
  Wird ein Verzeichnisdienst via LDAP als öffentlicher Adress- oder Zertifikatsserver eingesetzt, so werden über das Internet gestellte Suchanfra-

gen vom Verzeichnisdienst beantwortet. So wird nach Eingabe einer E-Mail-Adresse das zugehörige Zertifikat für eine mögliche Verschlüsselung übermittelt. Werden die Such- und Rückgabekriterien dabei nicht eingeschränkt, können über diese Anfragen interne Informationen nach außen gelangen. Lässt ein Unternehmen zum Beispiel bei einer Suche Platzhalter (so genannte Wildcards) zu und schränkt auch die Ausgabe für die Antwort nicht ein, kann mit einer Abfrage das komplette Verzeichnis ausgelesen werden. Eine Suche nach dem Zertifikat zur Adresse *@* würde dann als Ausgabe eine vollständige Liste aller E-Mail-Adressen von Mitarbeitern der Institution liefern. Diese Liste kann für den Spam-Versand oder zur Vorbereitung von gezielten Angriffen (siehe G 5.42 *Social Engineering*) genutzt werden.

# G 3.90 Fehlerhafte Administration von VPNs

Die fehlerhafte Administration eines VPN-Endpunktes kann die Verfügbarkeit, Vertraulichkeit und Integrität der beteiligten Netze bedrohen. Dies stellt daher ein nicht zu vernachlässigendes Gefährdungspotential für den sicheren Betrieb dar.

Für VPNs sind hier unter anderem folgende Aspekte zu nennen:

- Sicherheitsrelevante Routineaufgaben auf dem VPN-Client werden häufig vernachlässigt. Dazu gehören zum Beispiel die regelmäßige Datensicherung oder die Prüfung auf Computer-Viren. Insbesondere mobile VPN-Clients werden meistens vom jeweiligen Benutzer mitgeführt und sind daher für die Systemadministration nur schwer erreichbar. Zwar kann auch eine Administration aus der Ferne während einer aufgebauten VPN-Verbindung erfolgen, je nach Nutzungsprofil sind die Verbindungszeiten jedoch zu kurz, um eine geregelte Fernwartung durchzuführen. Werden die administrativen Aufgaben nicht regelmäßig durchgeführt, kann es beispielsweise zu nicht abgestimmten Konfigurationen kommen.
- Die Fernadministration von Rechnern kann mit Hilfe von verbreiteten Software-Produkten erfolgen und wird vielfach schon in Ansätzen durch Mechanismen des Betriebssystems möglich. Die Verwendung unautorisierter Software (durch den Benutzer oder den Administrator) kann dazu führen, dass nicht erlaubte Protokolle über eine VPN-Verbindung verwendet werden und dass Sicherheitslücken durch unsichere Einstellungen entstehen.
- Verschlüsselte Daten können durch Computer-Viren-Schutzprogramme nicht überprüft werden. Wenn die Konzepte zur Verschlüsselung der Daten und zum Schutz vor schädlichem Code nicht aufeinander abgestimmt sind, besteht daher das erhöhte Risiko, dass beispielsweise Computer-Viren, Trojanische Pferde oder Würmer über den VPN-Client eingeschleppt werden und Schäden im Netz verursachen.
- Da VPN-Clients in vielen Fällen in unsicheren Umgebungen betrieben werden und somit beispielsweise der Austausch von Datenträgern praktisch nicht kontrolliert werden kann, stellen Computer-Viren und anderer schädlicher Code eine besonders starke Gefährdung dar. Wenn auf dem VPN-Client kein aktuelles Computer-Viren-Schutzprogramm installiert ist, ist das Risiko groß, dass beispielsweise Computer-Viren, Trojanische Pferde oder Würmer über den VPN-Client in das LAN gelangen.
- Werden bandbreitenintensive Funktionen über VPN-Verbindungen ausgeführt, so besteht die Gefahr, dass der Benutzer die VPN-Verbindung unterbricht und neu aufbaut, weil er davon ausgeht, dass eine Störung vorliegt. In Wirklichkeit ist meist lediglich die Antwortzeit unakzeptabel lang, da die Bandbreite nicht ausreicht. Hierdurch können einerseits Inkonsistenzen in den Anwendungsdaten und andererseits erhöhte Belastungen des VPNs entstehen.
- Da VPNs ab einer gewissen Größe und Struktur sehr komplex sind, kann es durch Fehler bei der Konfiguration zu unsicheren und inkorrekten Einstellungen kommen. Diese Gefahr besteht besonders, wenn die Administratoren nicht ausreichend für die verwendeten Techniken und Produkte geschult sind. Hier reichen die Fehlkonfigurationen von fehlenden Sicherheitseinstellungen bis hin zu inkompatiblen Kommunikationsprotokollen. Ebenso breit gestreut sind auch die daraus resultierenden Konsequenzen. Beispielsweise könnte es passieren, dass benötigte Verbindungen nicht zustande kommen oder dass sich nicht autorisierte Dritte erfolgreich mit dem VPN-Gateway verbinden können.

Jede Modifikation von Sicherheitseinstellungen durch ungeschulte Administratoren sowie die Erweiterung von Zugriffsrechten (siehe G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*) kann die Gesamtsicherheit beeinträchtigen. Oft werden die vorgenommenen Konfigurationsänderungen auf VPN-Endpunkten weder gesichert noch dokumentiert. Beim Ausfall der Komponenten sind dann die letzten Änderungen, welche für ein erfolgreiches Wiederanlaufen des Systems nötig wären, nicht mehr bekannt. Auch ein mangelhaftes Betriebskonzept und unzureichend geplante Wartungsfenster können sich negativ auf die Verfügbarkeit des VPNs auswirken.

**Beispiele:**

- Ein neuer, bislang ungeschulter Administrator ändert unbedacht einen Konfigurationsparameter des VPNs. Dies führt zu einer länger andauernden Unterbrechung der gemeinsamen Verbindung zwischen einem Hersteller und dessen Zulieferer. Als Folge kommt es zu einem kostspieligen Produktionsstillstand, da dringend benötigte Teile nicht geliefert werden.
- Ein Unternehmen setzt ein Software-Managementsystem ein, das regelmäßig neue Software-Updates auf den einzelnen Benutzerrechnern installiert. Aufgrund eines Konfigurationsfehlers werden in dieses Verfahren auch die mobilen VPN-Clients mit einbezogen. Nach erfolgreichem Verbindungsaufbau wird dann die gesamte Bandbreite durch die Management-Software in Anspruch genommen, die ein größeres Update-Paket an den mobilen Client überträgt.

# G 3.91 Ausfall von VPN-Verbindungen durch Fehlbedienung

Neben dem technischen Versagen, beispielsweise durch Defekt von Bauteilen oder durch Stromausfall, gibt es eine Reihe weiterer Umstände, die zum Ausfall einer VPN-Verbindung führen können. Werden Alarmsignale oder abnormes Betriebsverhalten nicht rechtzeitig erkannt, so kann oftmals nicht mehr rechtzeitig gegengesteuert werden. Dies kann ebenso zu Ausfällen führen wie unsachgemäßes oder unüberlegtes Handeln bei einfachen Routinearbeiten oder -reparaturen. Die Hauptursache für Ausfälle durch Fehlbedienung liegt in der unzureichenden Schulung der beteiligten Parteien. Probleme können nicht nur auf der Seite der Administratoren entstehen, oft tragen auch Benutzer durch Fehlverhalten zur Überlastung oder zu einem Ausfall der VPN-Dienste bei.

**Beispiel:**

- Ein auf mehrere Standorte verteiltes Unternehmen nutzt ein VPN, um die Liegenschaften miteinander zu verbinden. Ein Wechsel auf eine aktuellere Softwareversion aller VPN-Komponenten, die nicht zu älteren Versionen kompatibel ist, erforderte eine Neukonfiguration aller VPN-Systeme. Da der Ausfall während der Konfiguration so kurz wie möglich gehalten werden musste und es nur einen VPN-Administrator in dem Unternehmen gibt, mussten auch die System- und "normalen" Netz-Administratoren die VPN-Komponenten konfigurieren. Nachdem ein hierfür ungeschulter Mitarbeiter VPN-Konfigurationsparameter fehlerhaft eingegeben hatte, war ein Standort für eine längere Zeit nicht erreichbar.

# G 3.92 Fehleinschätzung der Relevanz von Patches und Änderungen

Wird die Bedeutung von Patches für den sicheren IT-Betrieb falsch eingeschätzt, kann dies zu einer falschen Priorisierung führen. Werden die Aktualisierungen falsch priorisiert, kann es passieren, dass erst unwichtige Patches installiert werden. Wichtige Patches hingegen werden dann zu spät installiert und Sicherheitslücken bleiben länger unbehoben.

Das Patch- und Änderungsmanagement wird oft durch softwarebasierte Werkzeuge unterstützt. Auch diese Werkzeuge können Softwarefehler enthalten und dadurch unzureichende oder fehlerhafte Angaben über eine Änderung machen. Daher müssen die Angaben, die ein solches Tool über eine Änderung macht, immer überprüft und auf Plausibilität getestet werden.

**Beispiele:**

- Beim Patch- und Änderungsmanagement schätzt ein Mitarbeiter die Relevanz und damit auch die Priorität eines Sicherheitspatches fälschlicherweise als sehr hoch ein und veranlasst, dass ein Emergency-Patch auf alle betroffenen Systeme eingespielt wird. Durch die verkürzten Testphasen wird ein Fehler in diesem Patch übersehen, der eine schwerwiegende Sicherheitsschwachstelle an einer anderen Stelle öffnet.

# G 3.93 Falscher Umgang mit defekten Datenträgern

Beschädigungen, Fehler oder Ausfälle können bei allen Arten von Datenträgern auftreten. Dokumente können verschmiert oder zerrissen worden sein, CDs Bitfehler anzeigen oder ein Festplattencrash aufgetreten sein. Vor allem preisgünstige Datenträger werden dann häufig sofort weggeworfen und durch neue ersetzt. Teurere Datenträger werden zur Reparatur gegeben. In beiden Fällen darf aber nicht sorglos vorgegangen werden, da unter Umständen selbst aus nahezu zerstörten Datenträgern die darauf gespeicherten Informationen wieder rekonstruiert werden können. Professionelle Firmen zur Datenrettung können mit der entsprechenden Ausrüstung je nach Schaden selbst auf verbrannten Festplatten wieder die Daten lesbar machen. Daher muss davon ausgegangen werden, dass bei einer leichtfertigen Entsorgung bzw. Aussonderung von defekten Datenträgern vertrauliche Daten ausgelesen und weiterverwendet werden können.

**Beispiele:**

- In einem Unternehmen ließ sich der Laptop des Geschäftsführers nicht mehr hochfahren. Da dies noch während der Garantiezeit passierte, wurde er zum Hersteller geschickt. Nach der erfolgreichen Reparatur wurde er per Post zurückgeschickt, kam allerdings nie im Unternehmen an. Auf dem Laptop befanden sich nicht nur zeitkritische Projektpläne, sondern auch personenbezogene Daten und brisante Interna.
- Eine Behörde hatte längere Zeit alle entsorgten CDs gesammelt und einer caritativen Organisation für einen guten Zweck übergeben. Diese hat die CDs unter anderem als Grundlage für Bastelarbeiten und ähnliches verwendet. Unter den gespendeten CDs befanden sich viele Werbebeilagen-CDs, aber auch solche mit Datensicherungen. Dadurch fanden sich später an Weihnachtsbäumen in der Innenstadt CDs, bei denen unter einer weihnachtlichen Bemalung die Beschriftung "Personalakten A-D, Firma ABC, vertraulich" zu lesen war. Da die glänzende Datenseite nicht bearbeitet worden war, ließen sich diese Daten sogar teilweise noch ohne Aufwand auslesen.

# G 3.94 Fehlkonfiguration der Samba-Kommunikationsprotokolle

Samba setzt zur netzweiten Kommunikation eine Vielzahl von Protokollen ein:

- Microsoft Remote Procedure Call (MSRPC), eine Sonderform von Distributed Computing Environment Remote Procedure Call (DCE RPC)
- Network Basic Input/Output System (NetBIOS)
- Server Message Block (SMB)
- Transmission Control Protocol (TCP)/Internet Protocol (IP)
- Lightweight Directory Access Protocol (LDAP)

Durch Fehlkonfiguration der Kommunikationsprotokolle kann die Verfügbarkeit und die Sicherheit der Dienste, die von einem Samba-Server zur Verfügung gestellt werden, beeinträchtigt werden.

**Beispiel 1:**

Standardmäßig authentisiert Samba die Benutzer sowohl über die Protokolle NT LAN-Manager (NTLM) (smb.conf Parameter ntlm auth) als auch über NTLMv2. Dies erleichtert einen Angriff, da das NTLM Protokoll in Bezug auf die Sicherheit nicht so robust ist wie das NTLMv2 Protokoll.

**Beispiel 2:**

Standardmäßig benutzt ein Samba-Server kein SMB Message Signing (smb.conf Parameter server signing). Das SMB Protokoll ist daher anfällig für Man-in-the-Middle (MitM)-Attacken.

**Beispiel 3:**

Benutzt Samba in der Rolle als Primary Domain Controller (PDC) die Applikation ldapsam als Backend, werden die Kontoinformationen der einzelnen Benutzer (zum Beispiel LAN Manager (LM) und/oder NTLM-Hashes) in einem LDAP-Verzeichnis abgespeichert.

Ist die Verbindung zwischen Samba und dem LDAP Server nicht über Secure Sockets Layer (SSL) verschlüsselt, kann ein Angreifer durch abhören in den Besitz der Passwort-Hashes der Benutzer kommen und diese unter Umständen mit geringen Aufwand berechnen.

# G 3.95 Fehlerhafte Konfiguration des Betriebssystems für einen Samba-Server

Eine fehlerhafte Konfiguration des Betriebssystems für einen Samba-Server kann den sicheren und fehlerfreien Betrieb des Servers stören oder die Auswirkungen von Störungen verschlimmern. Häufige Fehler bei der Konfiguration des Betriebssystems sind:

- Verwendung eines nicht passenden Dateisystems, beziehungsweise von nicht passenden Dateisystemoptionen in Verbindung mit Samba.
  Wenn das Dateisystem third extended file system (ext3) einer Samba Dateifreigabe ohne die Option "acl" eingebunden wird, kann dies zu einem Informationsverlust führen. Werden beispielsweise Dateiordner von einem Windows-System auf eine Samba Dateifreigabe verschoben, können alle Access Control List (ACL)-Einträge verloren gehen, die nicht über die Standard-Dateisystemberechtigungen von Unix abgebildet werden können.
- Fehlkonfiguration des lokalen Paketfilters.
  Der Samba-Dienst lauscht an verschiedenen TCP- und UDP-Ports, um Netzverbindungen mit den Clients aufbauen zu können. Wird der Zugriff auf diese Ports von Außen mit einem Paketfilter reguliert, kann bei einer fehlerhaften Konfiguration des Paketfilters der Samba-Dienst nicht erreichbar sein.

**Beispiele:**

Bei der Konfiguration des lokalen Paketfilters eines Samba-Servers wird die Kommunikation mit Port 137/User Datagram Protocol (UDP) unterdrückt. Dieser Port wird benötigt, damit das Programm "nmbd" den Network Basic Input/Output System (NetBIOS) Name Service bereitstellen kann. Da der NetBIOS Name Service nun nicht bereit steht, ist die Funktionalität von Samba stark beeinträchtigt. Wird Samba beispielsweise als Primary Domain Controller (PDC) eingesetzt, so ist der Samba-Server für Clients nicht mehr auffindbar.

# G 3.96 Fehlerhafte Konfiguration eines Samba-Servers

Um einige Fähigkeiten des Samba-Servers zu zeigen und um den Administratoren einen schnellen Einstieg zu ermöglichen, wird bei der Installation des Samba-Servers die Konfigurationsdatei "smb.conf" mit Standardeinstellungen erzeugt. Wird diese als Beispiel mitgelieferte Konfigurationsdatei jedoch direkt oder nur mit geringfügigen Änderungen übernommen, kann dies zu erheblichen Sicherheitslücken führen. Bei der Änderung der Konfigurationsdatei können verschiedene Fehler auftreten:

- Werden die beispielhaft vorgenommenen Dateifreigaben nicht auskommentiert, können in diesen unerwünschten Freigaben sensible Informationen eingesehen werden.
- Binärpakete von Samba enthalten oft Funktionen, die nicht benötigt werden. Sind sich Administratoren dieser Funktionen nicht bewusst, kann dies die Sicherheit und Verfügbarkeit der Dienste eines Samba-Servers beeinträchtigen. Ein Beispiel hierfür wäre der Parameter -enable-cups für das Skript configure bei der Kompilierung. Er bestimmt, ob Samba mit oder ohne Common Unix Printing System (CUPS) Unterstützung kompiliert wird.
- Die Samba Konfiguration enthält Vorgabewerte für bestimmte Einstellungen, die Einfluss auf die Performance eines Samba-Servers haben. Werden diese Einstellungen ohne genaue Kenntnis der Auswirkungen geändert, so kann dies die Performance verschlechtern oder sogar die Verfügbarkeit der Dienste des Samba-Servers beeinträchtigen. Oft sind die Auswirkungen einer Änderung nicht sofort sichtbar. Ein Beispiel hierfür ist der Konfigurationsparameter *allocation roundup size*.

# G 3.97 Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista

Die BitLocker-Laufwerksverschlüsselung (engl. BitLocker Drive Encryption, BDE) ist ein Programm zur Verschlüsselung von Partitionen auf Datenträgern. BitLocker erfordert mindestens zwei Partitionen: eine unverschlüsselte Systempartition, typischerweise S:\, die nicht im Explorer erscheint, sowie die eigentliche Windows-Partition, typischerweise C:\, auf der das Betriebssystem installiert ist.

BDE verschlüsselt die Windows-Partition vollständig, mit Ausnahme des Bootsektors und eines Bereichs mit BitLocker-Metadaten. Weitere Partitionen auf internen Festplatten, wie eine Datenpartition, lassen sich durch BDE erst ab Windows Vista mit dem Service Pack 1 verschlüsseln. Bei Windows 7 und Windows Server 2008 R2 enthält BDE die Funktion BitLocker To Go zur Verschlüsselung externer und virtueller Datenträger.

Ein Benutzer von Windows Vista ohne Service Pack 1 kann fälschlicherweise annehmen, dass BDE alle Daten auf einer Festplatte verschlüsselt, einschließlich den Daten in einer zusätzlichen Datenpartition. Dadurch können Vertraulichkeitsverletzungen von Benutzerdaten begünstigt werden, wenn diese entgegen der Annahme des Benutzers unverschlüsselt gespeichert sind.

BDE verhält sich bei einem laufenden Windows-System vollkommen transparent. Während des Startvorgangs entschlüsselt BDE nach Eingabe der korrekten Zugangsdaten oder biometrischen Kennung die Partitionen. Diese bleiben während der gesamten Laufzeit des IT-Systems entschlüsselt. Für diesen Zeitraum besteht kein Schutz der Vertraulichkeit durch BDE. Somit schützt BDE insbesondere nicht gegen Vertraulichkeitsverletzungen durch Schadcode.

Die BDE-Konfiguration lokaler Festplatten erfordert administrative Berechtigungen. Auf mobilen und virtuellen Datenträgern genügen normale Benutzerberechtigungen. Verfügt ein Benutzer oder ein Schadprogramm über administrative Berechtigungen oder Benutzerrechte, so können diese zur unbefugten Deaktivierung von BDE, zum Hinzufügen zusätzlicher, eigener Schlüssel sowie zur Löschung von Schlüsselmaterial verwendet werden.

Die Folge der Deaktivierung oder des unbefugten Hinzufügens eigener Schlüssel ist der Verlust der Vertraulichkeit. Das Löschen von Schlüsselmaterial der Systempartition führt zum Verlust der Verfügbarkeit des Gesamtsystems.

Die Deaktivierung von BDE oder das ungewollte Löschen von Schlüsselmaterial kann, administrative Berechtigungen vorausgesetzt, auch das Ergebnis einer fehlerhaften Bedienung der mit dem System ausgelieferten Wartungswerkzeuge *manage-bde.wsf* oder *manage-bde.exe* sein.

Eine Vertraulichkeitsverletzung trotz BitLocker Drive Encryption droht auch, wenn Unbefugte den Wiederherstellungsschlüssel (Recovery Key) kennen. Mit diesem lässt sich eine BDE-verschlüsselte Partition wieder entschlüsseln. Dies gilt unabhängig von einem Trusted Platform Module (TPM), da der Wie-

derherstellungsschlüssel die Entschlüsselung insbesondere im Fall eines defekten TPM ermöglichen soll.

Die BDE-Konfigurationswerkzeuge erlauben es zu Wartungszwecken, die Verschlüsselung von Festplatten-Partitionen temporär zu deaktivieren, ohne die Daten zu entschlüsseln. Die Daten bleiben dann zwar verschlüsselt, aber es wird ein offener Startschlüssel (engl. *Clear Key*) ungeschützt auf dem Laufwerk gespeichert. Die Integritätsprüfung beim Startvorgang wird ebenfalls ausgeschaltet. Das System kann in diesem Zustand ohne Authentisierung gestartet werden, auch auf anderer Hardware, und erlaubt ungehinderten Datenzugriff. Es kann kopiert und der Clear Key kann ausgelesen werden. Ein Angreifer könnte dies nutzen und versuchen, geschütztes Schlüsselmaterial zu extrahieren, um damit später auch die Datenverschlüsselung zu umgehen.

# G 3.98 Verlust von BitLocker-verschlüsselten Daten

BitLocker Drive Encryption (BDE) ist ein Programm zum Verschlüsseln von Partitionen auf Datenträgern.

Für die Entschlüsselung der Windows-Partition durch BDE während des Startvorgangs des Betriebssystems kann der Administrator unterschiedliche Verfahren zur Authentisierung sowie Kombinationen daraus konfigurieren:

- TPM-Nutzung ohne Benutzer-Authentisierung (setzt ein Trusted Platform Modul, TPM, voraus)
  BDE startet in dieser Konfiguration ohne Interaktion durch den Benutzer, dieser muss sich nicht gegenüber BDE authentisieren. Der Startvorgang wird nur abgebrochen, wenn der Zugriff auf das TPM nicht möglich ist (z. B. wenn das TPM deaktiviert oder defekt ist).
- Authentisierung mittels eines Schlüssels auf einem USB-Stick
  Es besteht die Gefahr, dass der Benutzer den USB-Stick verliert oder das der Stick defekt ist. Als Folge wird der Startvorgang von Windows nicht fortgesetzt.
- Authentisierung mittels einer PIN (setzt den TPM-Chip des IT-Systems voraus)
  Es besteht die Gefahr, dass der Benutzer die PINvergisst. Ohne Eingabe der korrekten PIN setzt das Betriebssystem den Startvorgang nicht fort.
- Authentisierung mittels PIN *und* USB-Stick

Wenn das TPM für die Nutzung durch BitLocker konfiguriert wurde, kann Windows den Startvorgang des IT-Systems aus verschiedenen Gründen abbrechen:

- Bei Veränderungen am BIOS der Hauptplatine
- Bei einer Beschädigung des TPM
- Wenn der Master Boot Record (MBR) der Festplatte modifiziert wurde
- Wenn die frühen Bootkomponenten des Betriebssystems geändert wurden
- Wenn weitere von BitLocker überwachte Dateien modifiziert wurden.

Veränderungen am BIOS treten beispielsweise durch ein Firmwareupdate auf, Dateien können durch Softwareupdates geändert werden. Der Abbruch des Startvorgangs hat in jedem Fall zur Folge, dass der Benutzer das IT-System nicht nutzen kann. Die durch BDE geschützten Daten bleiben verschlüsselt.

Als Absicherung für die geschilderten Fälle dient ein numerisches Wiederherstellungskennwort oder ein Wiederherstellungsschlüssel. Dieser liegt im Binärformat vor, während das Kennwort auch als Papierausdruck aufbewahrt werden kann. Zu den unterstützten digitalen Ablageorten für das Wiederherstellungskennwort und den Wiederherstellungsschlüssel zählen Active Directory und Dateien, die entweder lokal oder auf externen Laufwerken wie USB-Sticks abgelegt sein können.

Insbesondere wenn das Wiederherstellungskennwort auf Papier ausgedruckt oder auf einem USB-Stick gespeichert wird, besteht die Gefahr des Zugangs durch Unbefugte und in der Folge ein Vertraulichkeitsverlust der durch BitLocker verschlüsselten Daten.

Des Weiteren besteht die Gefahr, dass das Wiederherstellungskennwort oder der Wiederherstellungsschlüssel ebenfalls verloren gehen. In diesem Fall

kann der Benutzer das IT-System nicht mehr nutzen. Die verschlüsselten Daten bleiben dauerhaft verschlüsselt.

In der Folge kann auch der Zugang zu den mit EFS (Encrypting File System) verschlüsselten Daten gefährdet sein, wenn der EFS-Schlüssel in einer durch BDE verschlüsselten Partition abgelegt wurde.

Ab Windows 7 und Windows Server 2008 R2 können Benutzer ohne Administrator-Berechtigungen kritische Daten auf internen und externen Laufwerken durch BitLocker To Go verschlüsseln. Zur Authentisierung können die Benutzer standardmäßig ein beliebiges Kennwort oder eine Smartcard nach eigener Wahl verwenden. Wird BitLocker To Go genutzt, sind die Daten auf dem Medium für die Institution nicht mehr verfügbar, falls der Ersteller des verschlüsselten Datenträgers das Kennwort vergisst oder die Herausgabe verweigert.

# G 3.99 Fehlerhafte Netzanbindungen eines Virtualisierungsservers

**Netzverbindungen für virtuelle IT-Systeme**

Ein Virtualisierungsserver sorgt für die Netzzugänge der auf ihm betriebenen virtuellen IT-Systeme. Hierzu stellt er in der Regel den virtuellen IT-Systemen eine emulierte Netzkarte zur Verfügung. Diese wiederum ermöglicht es den virtuellen IT-Systemen, auf Netze oder Speichernetze zu zugreifen. Diese (Speicher-) Netze können entweder physische oder virtuelle Netze sein.

Damit virtuelle IT-Systeme physische Netze nutzen können, muss der Virtualisierungsserver eine Verbindung der virtuellen Netzkomponenten der virtuellen IT-Systeme zu den physischen Netzen ermöglichen. Dies wird dadurch realisiert, dass der Virtualisierungsserver seine physischen Interfaces den virtuellen IT-Systemen zur Verfügung stellt. Die Verfahrensweise ist bei den verschiedenen Virtualisierungsprodukten unterschiedlich. Es gibt jedoch zwei wesentliche Prinzipien, wie der Übergang von virtuellen zu physischen Netzkomponenten realisiert wird:

- durch direkte Zuordnung von virtuellen zu physischen Netzen. Die Netzkarte eines virtuellen IT-Systems wird direkt einer physikalischen Schnittstelle des Virtualisierungsservers zugeordnet.
- durch indirekte Zuordnung. Die (virtuellen) Netzkarten der virtuellen IT-Systeme werden mit einem virtuellen Switch verbunden. Dieser wird vom Virtualisierungsserver in Software nachgebildet. Der virtuelle Switch wiederum kann mittels einer physischen Netzkarte mit dem physischen Netz verbunden sein. Da ein virtueller Switch nicht zwingend einen physischen Netzübergang besitzen muss, kann auf diese Weise ein Netz realisiert werden, in dem die daran angeschlossenen virtuellen IT-Systeme keine Verbindung nach außen besitzen. Eine solche Konfiguration kann zum Beispiel für Testsysteme genutzt werden, die keine Außenverbindungen benötigen.

Innerhalb der Verwaltungssoftware des Virtualisierungsservers werden die Netzschnittstellen der virtuellen IT-Systeme den physikalischen Schnittstellen des Virtualisierungsservers zugeordnet. Wird diese Zuordnung fehlerhaft vorgenommen, kann eine virtuelle Maschine mit einem falschen Netz verbunden werden. Wird beispielsweise ein Intranet-Webserver mit vertraulichen Daten, der nur im internen Netz betrieben werden soll, auf diese Weise versehentlich am Sicherheitsgateway (Firewall) vorbei mit dem Internet verbunden, sind die vertraulichen Daten möglicherweise im Internet sichtbar.

Ein Virtualisierungsserver besitzt häufig eine im Vergleich zu sonstigen Servern große Anzahl an Netzkarten. Diese große Anzahl wird benötigt, um eine möglichst gute Integration des Virtualisierungsservers in das Netz des Rechenzentrums zu erreichen. Es wird dadurch möglich, auf einem Virtualisierungsserver virtuelle IT-Systeme zu betreiben, die in unterschiedlichen Netzsegmenten benötigt werden. Des Weiteren werden weitere Schnittstellen für verschiedene Funktionen der Virtualisierungsserver benötigt, beispielsweise für den Zugriff auf Speichernetze oder die *Live Migration*, die es erlaubt, ein laufendes virtuelles IT-System von einem Virtualisierungsserver auf einen anderen zu verschieben.

Auf Grund der für einen Server untypischen Anzahl an Netzkarten und Kabelverbindungen zu Switchen und ähnlichen IT-Systemen besteht verstärkt die Gefahr, durch eine fehlerhafte Verkabelung unbeabsichtigt Fehler in der Netzinfrastruktur zu erzeugen. Solche Fehler können neben den in G 3.4 *Unzuläs-*

*sige Kabelverbindungen* und G 3.29 *Fehlende oder ungeeignete Segmentierung* schon angeführten beispielsweise sein:

- Mittels zweier physischer Netzkarten des Virtualisierungsservers und einem virtuellen Switch wird fälschlicherweise eine Kopplung von zwei Netzsegmenten geschaltet (*Brücke*). Diese Netze sollten aber getrennt sein. Verbindungen zwischen diesen Netzen sollten nur durch ein Sicherheitsgateway ermöglicht werden. Durch die Falschverkabelung können nun direkte Verbindungen zwischen Systemen aufgebaut werden. Die eigentlich gewünschte Segmentierung des Netzes wird unbeabsichtigt aufgehoben.
- Zwei physische Netzkarten eines Virtualisierungsservers sind einem virtuellen Switch zugeordnet. Sie werden versehentlich mit zwei unterschiedlichen physischen Netzsegmenten verbunden. Der virtuelle Switch ist so konfiguriert, dass er auf der einen Netzschnittstelle empfangene Pakete nicht an die andere Schnittstelle weiterleitet und somit keine Brücke (s. o.) bildet. Auf Grund der zwei Netzschnittstellen, die mit unterschiedlichen Netzsegmenten verbunden sind, ist der virtuelle Switch nicht eindeutig einem physischen Segment zugeordnet. Durch diesen Fehler kommt es durch den Lastverteilungsmechanismus des virtuellen Switches dazu, das Netzpakete eines an diesen Switch angeschlossenen virtuellen IT-Systems mal in das eine, mal in das andere Netzsegment weitergeleitet werden. Hierdurch ist das virtuelle IT-System nur sporadisch im Netz erreichbar und die Verfügbarkeit des Systems gefährdet.
- Einige Virtualisierungsprodukte können eine Falschverkabelung (wie in den vorherigen zwei Fällen beschrieben) erkennen und schalten in einem solchen Fall eine oder mehrere physische Netzkarten ab. Mit welchem physischen Netzsegment der virtuelle Switch dann tatsächlich verbunden ist, kann möglicherweise nicht mehr vorhergesagt werden. Hierdurch kann es zu Verbindungsabbrüchen zu den mit dem betroffenen virtuellen Switch verbundenen IT-Systemen kommen.
- Mit zwei oder mehreren Virtualisierungsservern wird eine virtuelle Infrastruktur aufgebaut. Hierzu sollen diese Server mit mehreren physischen Netzsegmenten verbunden werden, die jeweils virtuellen Switches zugeordnet werden. Diese Switche werden korrespondierend mit dem jeweiligen physischen Segment benannt (Switch A - Segment A, Switch B - Segment B usw.). Durch einen Verkabelungsfehler wird nun auf einem der beiden Virtualisierungsserver das physische Segment A mit dem virtuellen Switch B verbunden. Wird jetzt die Funktion *Live Migration* in dieser virtuellen Infrastruktur genutzt, kommt es durch den Migrationsprozess dazu, dass sich ein virtuelles IT-System am Switch B nach einer Migration in einem anderen physischen Netzsegment befindet als vor der Migration. Der Grund dafür liegt darin, dass der Switch B auf dem einen Virtualisierungsserver mit dem Segment B, auf dem anderen jedoch mit dem Segment A verbunden ist. Die Verfügbarkeit des Systems ist dadurch gefährdet. Es besteht auch die Gefahr, dass auf die von diesem System bereitgehaltenen Daten in Netzen zugegriffen werden kann, in denen dieser Zugriff eigentlich nicht zulässig ist.
- Virtualisierungsserver benötigen zum Betrieb der virtuellen IT-Systeme meist Verbindungen zu Speichernetzen, in denen die Daten (Konfigurationsdateien, Dateicontainer virtueller Festplatten) liegen. Werden die Verbindungen zu diesen Speichernetzen fehlerhaft verkabelt, können Störungen auftreten, wenn die Virtualisierungsserver auf das Speichernetz zu greifen. Dies gefährdet die Verfügbarkeit der virtuellen IT-Systeme, die auf diesen Virtualisierungsservern betrieben werden. Hiervon kann möglicherweise eine große Anzahl virtueller IT-Systeme betroffen sein.
- Auch Fehler in der Verkabelung von Netzkarten, die die Virtualisierungsserver zur Kommunikation untereinander in einer virtuellen Infrastruktur

nutzen, haben weitreichende Folgen für deren Funktion. So basieren die Funktionen *Live Migration* und *Fault Tolerance* auf der Synchronisierung einer Kopie eines virtuellen IT-Systems auf zwei unterschiedlichen Virtualisierungsservern. Mit *Fault Tolerance* wird ein Verfahren bezeichnet, bei dem ein virtuelles IT-System auf zwei Virtualisierungsservern gleichzeitig betrieben wird, wobei nur eine Kopie aktiv, die andere passiv ist. Fällt einer der Virtualisierungsserver aus, übernimmt die auf dem weiterlaufenden Server beheimatete Kopie des virtuellen IT-Systems transparent alle Funktionen des ausgefallenen. Werden nun die Netzverbindungen, die die Virtualisierungsserver zur Synchronisation virtueller IT-Systeme für die *Live Migration* oder *Fault Tolerance* verwenden, fehlerhaft verkabelt, ist es möglich, dass diese Virtualisierungsfunktionen nicht einwandfrei funktionieren. Die Verfügbarkeit der virtuellen IT-Systeme ist aufgrund dessen gefährdet.

**Netzverbindungen für Virtualisierungsserver**

Die Netzverbindungen der Virtualisierungsserver werden häufig redundant ausgelegt, da von den physischen Schnittstellen eine Vielzahl von Funktionen der virtuellen Infrastruktur abhängt. Um die Verfügbarkeit von Netzschnittstellen zu steigern, werden meist mehrere Netzwerkkarten so konfiguriert, dass sie wechselweise oder sogar gleichzeitig die Funktion der jeweils anderen ausführen können. Hierzu existieren verschiedene Verfahren:

- Load Balancing: Die MAC-Adressen der virtuellen IT-Systeme werden auf der Basis eines Algorithmus auf die physischen Schnittstellen verteilt, um eine möglichst gleichmäßige Auslastung der einzelnen physischen Schnittstellen zu erreichen. Fällt eine der Schnittstellen aus, übernimmt eine der verbliebenen die Aufgabe der ausgefallenen. Hierbei wird die Netzverbindung der virtuellen IT-Systeme allerhöchstens unmerklich unterbrochen. Dieses Verfahren arbeitet mit allen gängigen physischen Switches zusammen und erfordert in der Regel keine spezielle Konfiguration dieser Switche. Load Balancing ist zwar nicht virtualisierungsspezifisch, dem Verfahren kommt jedoch beim Einsatz virtueller IT-Systeme eine besondere Bedeutung zu.
- *IEEE 802.3ad (Link Aggregation Control Protocol - LACP)* oder *Etherchannel* (Cisco) sind Protokolle, bei denen mehrere physische Schnittstellen zu einem logischen Kanal zusammengeschaltet werden. Diese Verfahren erfordern in der Regel eine angepasste Konfiguration auf dem verbundenen, physischen Switch.

Es existieren des Weiteren eine Reihe von herstellerspezifischen Bezeichnungen für verschiedene Protokolle und Verfahren zur Verfügbarkeitssteigerung von Netzwerkkarten wie *Bonding* im Linux-Umfeld, *Teaming, Port Aggregation, Link Aggregation* und *Trunking*. Hierbei erfordern einige Protokolle, dass entsprechend angepasste Konfigurationen auf den physischen Switchen vorgenommen werden müssen. Teilweise sind die Verfahren nur eingeschränkt kompatibel. Werden diese Verfahren unzulässig gemischt oder kommt es zu Missverständnissen zwischen den Administratoren der Virtualisierungsserver und denen der physischen Netzinfrastruktursysteme, können Inkompatibilitäten durch Fehlfunktionen auftreten. Die sich dabei ergebenden Verbindungsabbrüche treten häufig nur sporadisch auf und ihre Ursachen sind dementsprechend schwer zu ermitteln.

# G 3.100 Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme

Durch Snapshots kann der Zustand einer virtuellen Maschine zu einem beliebigen Zeitpunkt eingefroren werden. Es ist hierbei nicht von Belang, ob das System in dem Moment der Erzeugung des Snapshots läuft oder nicht. Auf diesem Weg ist es möglich, ohne aufwendigen Prozess zu dem im Snapshot konservierten Zustand des virtuellen IT-Systems zu gelangen. Der Snapshot kann auch auf einen anderen Virtualisierungsserver übertragen werden oder als Datensicherung dienen.

Wird die virtuelle Maschine nach der Erzeugung eines Snapshots weiter betrieben und der konservierte Zustand später geladen, gehen alle seitdem am Gastsystem erfolgten Änderungen verloren. Dies kann bei einer unbedachten Vorgehensweise zu Datenverlusten führen und ist bei Produktivsystemen meist unerwünscht. Auch Änderungen am Betriebssystem, Diensten und Anwendungen des virtuellen IT-Systems können so zurückgesetzt werden. Unzureichende Dateiberechtigungen, Sicherheitslücken und Schwachstellen oder auch gelöschte Benutzerkonten werden auf diese Weise erneut aktiv.

Bei virtuellen Servern, die über offene Dateien oder Datenbanksitzungen verfügen, können inkonsistente Daten entstehen. Dies ist beispielsweise der Fall, wenn Informationen durch einen Client auf den virtualisierten Server geschrieben werden, während der Snapshot erstellt wird. Der zu speichernde Dateiinhalt ist dann nicht vollständig im Snapshot enthalten. Wird der eingefrorene Zustand der virtuellen Maschine nun erneut eingesetzt, befinden sich dort mit hoher Wahrscheinlichkeit defekte Dateien oder in ihrer Integrität gestörte Datenbanken.

Verteilte Systeme wie Datenbank-Cluster oder auch Active Directory Domaincontroller nutzen in der Regel einen Replikationsmechanismus um sicher zustellen, dass ihre Daten synchronisiert werden. Hierbei können erhebliche Probleme auftreten, wenn diese auf einen Snapshot zurückgesetzt werden. Es kann in einem solchen Fall zu Inkonsistenzen in den Datenbanken kommen, die durch den Replikationsmechanismus nicht aufgelöst werden können.

Ist nicht genügend Speicherplatz für umfangreiche oder mehrere Snapshots vorhanden, kann es passieren, dass es zu Speicherplatzengpässen kommt und keine weiteren Informationen abgespeichert werden können.

**Beispiel:**

Ein großes Fotolabor entwickelt Filme für seine Kunden. Dazu sendet der Kunde seinen Film in einer Versandtasche ein und gibt auf dieser Tasche die Rücksendeadresse an. Alle Versandtaschen sind mit einer eindeutigen Nummer versehen. Im Labor wird den Filmen zusätzlich eine interne Bearbeitungsnummer zugeordnet. Diese interne Bearbeitungsnummer dient dazu, die Filme zu anonymisieren. Für das automatische Versandverfahren wird die Bearbeitungsnummer mit der maschinenlesbaren Versandtaschennummer in einer Datenbank abgelegt. Sind die Bilder fertig entwickelt, werden sie mittels der Bearbeitungsnummern automatisch wieder den Versandtaschen zugeordnet. Die Versandtasche wird dann dem Kunden per Post zugeschickt.

Die Geschäftsleitung des Fotolabors hat sich nun entschieden, neben anderen IT-Systemen auch das Datenbanksystem, das für die Zuordbarkeit von Bearbeitungs- und Versandtaschennummer sorgt, zu virtualisieren.

Während die Produktion im Labor läuft, stellt der zuständige Administrator fest, dass es auf dem virtuellen Datenbankserver zu einem Problem gekommen ist. Um dieses schnell zu beheben, setzt er den Server auf einen Snapshot zurück. Er weiß, dass der Server zum dem Zeitpunkt, bei dem der Snapshot erstellt wurde, einwandfrei funktionierte. Nun stimmt aber die Zuordnung von Bearbeitungs- und Versandtaschennummern nicht mehr, da auch die Tabelle mit der Zuordnung der Bearbeitungsnummern zu den Versandtaschennummern auf den Snapshot zurückgesetzt worden ist. Der Fehler bleibt beim Versand unbemerkt. In der Folge werden einigen Kunden die falschen Filme zugestellt. Sehr viele Filme können auch gar nicht mehr den Kunden zugeordnet werden und es kommt zu einem Ansehensverlust des Fotolabors, der zu starken Umsatzeinbußen führt.

# G 3.101 Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen

Bei vielen Virtualisierungsprodukten können in den virtuellen IT-Systemen sogenannte Gastwerkzeuge installiert werden. Mit diesen Gastwerkzeugen können zum Einen die für Betriebssystemvirtualisierung notwendigen Gerätetreiber für virtuelle oder emulierte Geräte wie Netzwerkkarten, Festplatten oder Grafikkarten bereitgestellt werden. Zum Anderen stellen sie für virtuelle Maschinen eine Vielzahl anderer Funktionen bereit. Solche Funktionen sind zum Beispiel:

- Herunterfahren des Betriebssystems eines virtuellen IT-Systems ohne Interaktion im dem virtuellen IT-System direkt über den Virtualisierungsserver,
- Austausch des Inhalts der Zwischenablage zwischen der Konsolen-Emulation der virtuellen Maschine und dem Arbeitsplatzsystem des Benutzers,
- Nahtlose Integration des Mauszeigers des Arbeitsplatzsystems des Nutzers einer virtuellen Maschine mit ihrer Konsolenemulation,
- Vereinfachtes Laden und Entladen von Datenträgern in die virtuellen IT-Systeme. Dies können physische Disketten-, CD- oder DVD-Laufwerke, aber auch Abbilddateien von solchen Datenträgern sein (ISO-Images).

Diese Funktionen steigern die Bedienbarkeit der virtuellen IT-Systeme durch einen Benutzer und ermöglichen weiterhin eine automatisierte Verwaltung des Betriebszustands (Ein-/Ausschalten, Hoch- und Herunterfahren) virtueller IT-Systeme durch den Virtualisierungsserver.

### Herunterfahren des Systems ohne Anmeldung / Interaktion

Wird die Funktion zum Herunterfahren eines IT-Systems durch einen Administrator des Virtualisierungsservers genutzt, werden gegebenenfalls restriktivere Konfigurationseinstellungen innerhalb des virtuellen IT-Systems selbst umgangen oder Richtlinien verletzt, die einen Neustart oder ein Herunterfahren ohne eine korrekte Autorisierung verbieten.

### Zugriff auf CD- / DVD-Laufwerke oder Diskettenlaufwerke

Des Weiteren erlauben die Gastwerkzeuge bei entsprechender Konfiguration den direkten Zugriff auf Laufwerke des Virtualisierungsservers. So kann beispielsweise der Zugriff auf das im Virtualisierungsserver angeschlossene, physische CD-Laufwerk von einem virtuellen IT-System aus möglich sein. Auf eine CD-ROM mit vertraulichen Daten, die in das Laufwerk des Virtualisierungsservers eingelegt wurde, um die darauf enthaltenen Daten auf ein bestimmtes virtuelles IT-System zu übertragen, kann daher auch von anderen virtuellen Instanzen aus zugegriffen werden. Die Vertraulichkeit der Daten ist gefährdet, da möglicherweise die Daten von unberechtigten Personen gelesen wurden.

Bei einigen Virtualisierungsprodukten kann auch die CD- oder DVD-Laufwerksschublade des Virtualisierungsservers über die Gastwerkzeuge von einem virtuellen IT-Systeme aus geöffnet werden, wenn sie entsprechend konfiguriert sind. Das Laufwerk könnte beschädigt werden, wenn es beispielsweise gegen die Tür des Serverschrankes stößt oder von einer Zierblende am Servergehäuse gestoppt wird.

**Beispiele:**

- In einem mittelständischen Unternehmen werden mehrere Virtualisierungsserver eingesetzt. Auf diesen Servern werden mehrere virtuelle IT-Systeme betrieben. Einige davon gehören zu einem ERP-System, auf dem sämtliche kaufmännischen Anwendungen des Unternehmens betrieben werden. Dieses ERP-System wird nicht durch die gleichen Administratoren verwaltet wie die Virtualisierungsserver. Da für die Server, die zum ERP-System gehören, ein hoher Schutzbedarf festgestellt worden ist, dürfen diese Systeme nur heruntergefahren werden, wenn ein Wartungszeitraum mit den Nutzern des ERP-Systems vereinbart worden ist. Weiterhin dürfen die Server nur von dazu besonders berechtigten Administratoren heruntergefahren werden, was durch den jeweiligen Administrator des Weiteren protokolliert und dokumentiert werden muss. Um diese Richtlinie technisch umzusetzen, wurde im Betriebssystem der virtuellen IT-System die Berechtigung, die einzelnen ERP-Systeme zu stoppen, nur an die ERP-Administratoren vergeben. Weiterhin wurde das Betriebssystem so konfiguriert, dass es den Administrator zwingt, vor dem Herunterfahren den Grund dafür anzugeben.
  Bei einem der Virtualisierungsserver fällt nun ein Lüfter aus. Dies ist zwar für die Funktion des Servers nicht direkt kritisch, der defekte Lüfter sollte jedoch unverzüglich ausgetauscht werden. Der Administrator des Virtualisierungsservers vereinbart dazu mit einem Servicetechniker des Serverherstellers einen Termin für die Reparatur. Der Techniker des Herstellers erscheint am nächsten Tag im Laufe des Vormittags. Er hat das benötigte Ersatzteil dabei und möchte sofort mit der Reparatur beginnen, da er noch weitere Termine hat. Für den Austausch des Lüfters muss der Virtualisierungsserver ausgeschaltet werden. Der Administrator des Virtualisierungsservers fährt den Virtualisierungsserver nun über die Verwaltungskonsole herunter. Dabei werden alle virtuellen IT-Systeme ebenfalls über die Gastwerkzeuge automatisch heruntergefahren. Die Gastwerkzeuge fahren die Systeme ohne die erforderliche Protokollierung herunter und überprüfen auch nicht, ob der Administrator überhaupt die Berechtigung dazu hatte. Nach der Reparatur schaltet der Administrator den Virtualisierungsserver wieder ein und fährt alle virtuellen IT-Systeme wieder hoch.
  Während der Reparatur stehen wichtige Teile des ERP-Systems nicht zur Verfügung und es kommt zu einem großen Arbeitszeitverlust, da einige Mitarbeiter ihre Arbeit nicht erledigen können. Die Administratoren des ERP-Systems werden von der Geschäftsleitung des Unternehmens gerügt, da sie die Richtlinien missachtet haben sollen und nicht dafür gesorgt haben, dass die ERP-Systeme ausschließlich von berechtigten Administratoren heruntergefahren werden können, sowie Protokollierungsvorschriften ignoriert wurden.
- Der Administrator eines virtuellen IT-Systems hat Langeweile und erforscht dabei die Funktionen der auf dem virtuellen IT-System installierten Gastwerkzeuge. Er findet dabei die Funktion zum Verbinden und Trennen von physischen CD- oder DVD-Laufwerken des Virtualisierungsservers. Da er nicht weiß, dass das Öffnen der Laufwerksschublade im virtuellen IT-System tatsächlich zum Öffnen der physischen Laufwerkschublade des Virtualisierungsservers führt, spielt er mit der entsprechenden Funktion herum.
  Ein Techniker, der sich zu dieser Zeit im Serverraum befindet und Arbeiten an einem mit dem Virtualisierungsserver benachbarten IT-System durchführt, bemerkt das offene Laufwerk nicht und bleibt mit seinem Ärmel an der Schublade hängen. Dabei wird das Laufwerk beschädigt und muss ausgetauscht werden.

# G 3.102 Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen

Gängige Betriebssysteme verfügen über eine eigene interne Uhr. Die Uhrzeit wird dabei vom Betriebssystem in der Regel durch die Zählung von Prozessorzyklen und den gelegentlichen Abgleich mit einer verlässlichen Zeitquelle, wie einem Zeitserver oder einer internen Hardware-Uhr, ermittelt. Der Zeitpunkt und die Häufigkeit der Synchronisation mit der verlässlichen Zeitquelle hängt dabei vom verwendeten Betriebssystem ab.

Gastbetriebssysteme in virtuellen Umgebungen haben jedoch keine Kontrolle und Kenntnis über die tatsächlich verbrauchte Rechenzeit auf dem physischen IT-System. Die Berechnung der aktuellen Uhrzeit über die abgearbeiteten Rechenschritte als Taktgeber ist daher unzuverlässig. Je nachdem, mit welchem Algorithmus die Uhrzeit aus dem Vergleich von Prozessorzyklen und verlässlicher Zeitquelle ermittelt wird, kann die Uhr eines virtuellen IT-Systems der tatsächlichen Zeit nachlaufen oder vorauseilen. In Extremfällen kann es sogar dazu führen, dass die Uhr des Betriebssystems rückwärts läuft. Dies kann zu unerwünschten Effekten führen, die sich unter ungünstigen Umständen erheblich auf die Sicherheit der virtuellen Infrastruktur auswirken.

Beispielsweise sind Zeitstempel etwa im Dateisystem einer virtuellen Maschine mit einer falsch laufenden Uhr unzuverlässig. In der Folge können Inkonsistenzen in der Datensicherung entstehen, wenn diese über die Zeitstempel des Dateisystems ermittelt, welche Dateien zu sichern sind.

Auch die Fehlersuche bei Problemen wird nachhaltig behindert, da die zeitliche Abfolge der Ereignisse, die zu dem Problem geführt haben, nicht zuverlässig ermittelbar ist. Überdies sind beweiskräftige Aussagen bei Sicherheitsvorfällen mit inkorrekten Zeitstempeln in Ereignisprotokollen schlimmstenfalls unmöglich, da die Korrelation von Ereignissen über die Zeitstempel nicht möglich ist.

Werden in virtuellen IT-Systemen Verfahren zur Authentisierung genutzt, die auf korrekten Zeitstempeln für die Übermittlung von Authentisierungsschlüsseln basieren (z. B. Kerberos), können Anmeldungen fehlschlagen.

Verschiedene verteilte Datenbanksysteme und Verzeichnisdienste wie Active Directory nutzen Zeitstempel zur Konsistenzprüfung bei Replikationsvorgängen. Sind diese Zeitstempel unzuverlässig, können Inkonsistenzen in diesen Systemen auftreten.

**Beispiel:**

Ein Unternehmen hat sich für den Fernzugang für Telearbeiter für eine auf Token basierende Authentisierungsmethode entschieden. Auf den Token werden in bestimmten zeitlichen Abständen regelmäßig neue Passphrasen erzeugt, die zusammen mit dem Benutzernamen und dem Passwort eingegeben werden müssen. Die Token, die von den Benutzern mitgeführt werden, sind mit einer internen Uhr ausgestattet, die mit der Uhrzeit des Authentisierungsservers synchronisiert ist.

Nachdem der Authentisierungsserver virtualisiert wurde, können sich die Benutzer nach kurzer Zeit nicht mehr anmelden, da die angezeigten Einmalpasswörter nicht mehr mit denen auf dem Authentisierungsserver übereinstimmen. Die Ganggenauigkeit der Uhr in der virtuellen Umgebung reicht dazu nicht aus.

# G 3.103 Fehlerhafte Domain-Informationen

Selbst wenn die Planung des DNS-Einsatzes sorgfältig durchgeführt und somit alle sicherheitsrelevanten Punkte berücksichtigt wurden, ist dass nicht ausreichend, wenn fehlerhafte Domain-Informationen erstellt werden. Fehlerhaft bedeutet, dass bei der Erstellung der Domain-Informationen semantische und/oder syntaktische Fehler begangen wurden. Beispielsweise, wenn einem Hostnamen eine falsche IP-Adresse zugeordnet wurde, Daten fehlen oder nicht erlaubte Zeichen verwendet wurden. Enthalten Domain-Informationen Fehler, funktionieren Dienste, die diese Informationen benutzen aufgrund der Falschinformationen nur eingeschränkt. Nachfolgend einige Beispiele für übliche Fehler:

- Für die Vorwärtsauflösung und die Rückwärtsauflösung werden die Daten jeweils in einer eigenen Datenbank gepflegt. Einer der häufigsten Fehler ist, dass neue hinzugekommene Domain-Informationen in die Daten der Vorwärtsauflösung hinzugefügt werden. Es wird jedoch vergessen, die Domain-Informationen auch in die Daten der Rückwärtsauflösung einzupflegen.
- Multi-homed-Hosts, wie beispielsweise Router, haben eine Netzanbindung in mehrere Netzsegmente und somit mehrere IP-Adressen. Wenn bei einem Multi-homed-Host vergessen wird, für alle IP-Adressen die entsprechenden PTR-Records (Kurzform für "Pointer") in die Domain-Informationen einzutragen, wird für IP-Adressen ohne PTR-Records eine Rückwärtsauflösung fehlschlagen. Services, die Rückwärtsauflösungen benötigen, werden somit gestört.
- Das Verwenden von nicht erlaubten Zeichen in Domainnamen führt dazu, dass Informationen falsch bzw. gar nicht interpretiert werden. Erlaubte Zeichen sind ASCII-Buchstaben, Ziffern und der Bindestrich. Auch Namen, die im DNS-Namensraum gültig sind, können von Anwendungen anders interpretiert werden. "0xe" ist zum Beispiel ein gültiger Hostname. Wird versucht sich per *"telnet 0xe*" zu diesem Host zu verbinden, wird Telnet "0xe" als IP-Adresse interpretieren. Es erfolgt keine Namensauflösung, und sofern 0.0.0.14 nicht die richtige IP-Adresse ist, wird die Verbindung fehlschlagen.
- In Domain-Informationen müssen Seriennummern eintragen werden, aus denen auch das Datum hervorgeht, wann die Zone zuletzt aktualisiert wurde. Wird das Datum als Kommazahl geschrieben, kann dies zu unerwarteten Ergebnissen führen, da diese von DNS-Servern intern in eine Ganzzahl umgewandelt werden.
- Resolving DNS-Server sowie Resolver auf reinen Client-IT-Systemen speichern in der Regel erhaltene Antwortdaten im Cache zwischen. Dadurch wird die Anzahl der benötigten Anfragen beim übergeordneten DNS-Server verringert. Die Zeitdauer der Zwischenspeicherung wird als "Time to Live" (TTL) bezeichnet und stellt einen Teil der Domain-Informationen dar. Zu lange TTL-Zeiten, vor allem bei Domain-Informationen die sich häufig ändern, bewirken, dass die zwischengespeicherten Daten veraltet sind. Hingegen erhöht eine zu kurze TTL die Last für DNS-Server.
- "Glue Records" sind in bestimmten Fällen notwendig, um die zuständigen DNS-Server finden zu können. Normalerweise speichert ein DNS-Server nur die Domainnamen der DNS-Server seiner Subdomains. Befindet sich ein DNS-Server einer solchen Subdomain innerhalb der eigenen Subdomain, muss der darüber liegende DNS-Server auch dessen IP-Adresse gespeichert haben, da sonst kein DNS-Server fähig wäre, eine Namensauflösung durchzuführen. Dieser Eintrag wird als Glue Record be-

zeichnet. Es kann passieren, dass bei der Migration oder der Außerbetriebnahme von DNS-Servern vergessen wird, die dazugehörigen "Glue Records" zu adaptieren oder zu löschen. Dann werden bei entsprechenden Anfragen Daten über nicht mehr existente DNS-Server zurück geliefert.

- DNS bietet die Möglichkeit Aliase zu definieren. Ein Alias ist ein frei gewählter Name, der im Regelfall leicht zu merken ist. Ein Beispiel für einen oft verwendeten Alias bei DNS ist "www" für den Webserver. Einem Alias dürfen jedoch keine weiteren Daten zugewiesen werden. Es ist beispielsweise nicht zulässig, für einen Alias eine IP-Adresse zu definieren. Ein weiterer Fehler bezüglich Aliase ist, einen Host zu löschen, den zugehörigen Alias jedoch nicht.
- Da Domain-Informationen wichtige Daten darstellen, werden diese in der Regel von mindestens zwei DNS-Servern, dem Primary DNS-Server und einem oder mehreren Secondary DNS-Servern zur Verfügung gestellt. Die Daten werden auf dem Primary DNS-Server gepflegt und auf den oder die Secondary DNS-Server synchronisiert. DNS-Server verwenden die in den Domain-Informationen vorhandenen Seriennummern als Indikator dafür, ob es Änderungen gegeben hat. Werden Domain-Informationen geändert und die enthaltene Seriennummer nicht erhöht, werden die neuen Domain-Informationen nicht synchronisiert. Die daraus resultierende Inkonsistenz wird zu unterschiedlichen Namensauflösungen führen, je nachdem welcher DNS-Server befragt wird.

Domain-Informationen werden in Textdateien, sogenannten Master Files, gespeichert. Werden diese Textdateien händisch bearbeitet, stellt eine unübersichtliche, uneinheitliche Struktur eine zusätzliche Fehlerquelle dar.

Neben dem Hinzufügen von neuen Informationen stellt vor allem das Löschen, im Falle der Aussonderung eines Hosts, eine große Fehlerquelle dar. Wenn nicht alle Domain-Informationen gelöscht werden, bleiben Informationen über nicht mehr existente Hosts vorhanden.

# G 3.104 Fehlerhafte Konfiguration eines DNS-Servers

Sicherheitskritische Standardeinstellungen, selbst konfigurierte sicherheitskritische Einstellungen oder fehlerhafte Konfigurationen können dazu führen, dass ein DNS-Server nicht ordnungsgemäß funktioniert und die Verfügbarkeit dadurch eingeschränkt wird. Des Weiteren werden durch fehlerhafte Konfigurationen Angriffe auf die Verfügbarkeit und Integrität des DNS-Servers erleichtert. Bei den sicherheitskritischen Konfigurationen sind vor allem folgende Punkte von Bedeutung:

**DNS-Server mit Superuser-Rechten**

Das Betreiben eines DNS-Servers mit Superuser-Rechten erleichtert wirkungsvolle Angriffe auf das IT-System. Gelingt es einem Angreifer einen DNS-Server-Prozess erfolgreich anzugreifen, kann er mit den Rechten des DNS-Server-Prozesses arbeiten und auf alle weiteren Prozesse dieses Rechners zugreifen sowie weitere Rechner im Netz kompromittieren.

**Rekursive Anfragen**

Es gibt zwei Arten von Anfragen an einen DNS-Server: iterative und rekursive. Bei iterativen Anfragen beantwortet ein DNS-Server nur Anfragen, sofern er die gewünschten Informationen selbst gespeichert hat. Dieses Verhalten entspricht einem Advertising DNS-Server. Ansonsten verweist er auf einen anderen DNS-Server. Bei rekursiven Anfragen beantwortet ein DNS-Server alle Anfragen, dies entspricht einem Resolving DNS-Server. Wenn der Resolving DNS-Server die Informationen nicht selbst gespeichert hat, stellt er selbst Anfragen an andere DNS-Server, um die gewünschten Informationen zu erhalten. Ist ein Resolving DNS-Server so konfiguriert, dass er rekursive Anfragen uneingeschränkt annimmt, kann dies die Verfügbarkeit des Servers aufgrund der erhöhten Last stark beeinträchtigen. Uneingeschränkt bedeutet in diesem Fall, dass der Resolving DNS-Server rekursive Anfragen sowohl aus dem internen LAN als auch aus dem Internet akzeptiert.

Im Weiteren werden dadurch Cache-Poisoning Angriffe, wie beispielsweise in G 5.78 *DNS-Spoofing* beschrieben, erleichtert. Vereinfacht dargestellt funktionieren Cache-Poisoning Angriffe wie folgt: Ein Angreifer sendet eine rekursive Anfrage an einen Resolving DNS-Server betreffend Domain-Informationen, die dieser Resolving DNS-Server nicht gespeichert hat. Danach versucht der Angreifer eine gültige, gefälschte Antwort an den Resolving DNS-Server zu senden. Akzeptiert ein Resolving DNS-Server rekursive Anfragen nur aus dem internen Netz, wird er die Anfrage des Angreifers nicht auflösen, sondern an den nächsten zuständigen DNS-Server verweisen. Damit ist er durch den vorher beschriebenen Angriff nicht gefährdet. Akzeptiert der DNS-Server rekursive Anfragen uneingeschränkt bzw. befindet sich der Angreifer innerhalb des Firmennetzes, ist dieser potenziell stark gefährdet.

**Zonentransfers**

Da DNS von vielen Netzdiensten vorausgesetzt wird, werden bestimmte Teile des Domain-Namensraums nicht von einem einzigen DNS-Server verwaltet, sondern in der Regel von mindestens zwei. Zur Synchronisation dieser Server werden sogenannte Zonentransfers durchgeführt. Sind Zonentransfers nicht auf berechtigte DNS-Server beschränkt, kann jeder Host, der die Möglichkeit hat eine Anfrage an den DNS-Server zu stellen, die gesamten Domain-Informationen dieser Server mithilfe eines Zonentransfers auslesen. Führt jemand

ohne Berechtigung einen Zonentransfer durch, stellt dies für den Informationsverbund zwar keinen unmittelbaren Schaden dar, die gewonnenen Daten können aber spätere Angriffe erleichtern.

**Dynamische Updates**

Dynamische Updates ermöglichen es, Domain-Informationen automatisiert zu aktualisieren. Vor allem im Zusammenhang mit DHCP sind dynamische Updates wichtig. Wird von einem DHCP-Server eine IP-Adresse an einen Host vergeben, müssen diese Informationen auch in den Domain-Namensraum eingepflegt werden. Dies kann über dynamische Updates geschehen. Eine fehlerhafte Konfiguration von dynamischen Updates kann zu folgenden Problemen führen:

- Die Berechtigungen wurden zu restriktiv konfiguriert, sodass der DNS-Server die Updates des internen DHCP-Servers nicht akzeptiert. Dadurch können die Domain-Informationen nicht aktualisiert werden und bei Anfragen werden veraltete, falsche Daten als Antwort geliefert.
- Werden die Berechtigungen zu großzügig konfiguriert, kann dies eine potenzielle Angriffsmöglichkeit, wie in G 5.155 *Ausnutzen dynamischer DNS-Updates* beschrieben, darstellen.

**Kryptografie**

Zur Absicherung von DNS wird oft Kryptografie eingesetzt. Fehler bei der Konfiguration der kryptografischen Schlüssel führen beispielsweise dazu, dass aufgrund falscher Schlüssel Verbindungen abgelehnt oder valide Daten als nicht valide verworfen werden.

# G 3.105 Ungenehmigte Nutzung von externen Dienstleistungen

Es kommt wieder vor, dass Mitarbeiter externe Dienstleistungen in Anspruch zu nehmen, ohne dass dies innerhalb ihrer Institution abgestimmt ist. Dies kann daran liegen, weil sie nicht wussten, welche Schritte dafür intern durchzuführen sind. Es kann aber auch daher kommen, dass

- ihnen die Genehmigungsverfahren bekannt, aber zu aufwändig sind oder zu lange dauern,
- sie diese Dienstleistungen auch privat nutzen und sie diese daher für selbstverständlich halten.

Bei einer dienstlichen Nutzung gelten aber häufig andere Rahmenbedingungen als bei privater. Es kann zu Problemen kommen, wenn

- die Nutzung externer Dienstleistungen nicht vertraglich geregelt ist,
- dadurch neue, dem Informationssicherheitsmanagement unbekannte und damit unkontrollierte Datenflüsse entstehen,
- vertrauliche Daten unautorisiert an Dritte gegeben werden und damit interne Sicherheitsvorgaben oder Datenschutzbestimmungen verletzt werden,
- technische Sicherheitsmaßnahmen wie Virenschutz unterlaufen werden.

**Beispiele:**

- Mitarbeiter greifen auf Web-Mail-Dienste zurück, um flexibler von unterwegs auf E-Mail zugreifen zu können. Bei Abwesenheiten leiten sie automatisch ihre dienstlichen E-Mails an diese Web-Mail-Dienste weiter. Damit können vertrauliche Daten bei Wettbewerbern oder personenbezogene Daten bei ausländischen Providern landen.
- Online-Officeprogramme wie Google Documents oder Microsoft Office 2010 Web Apps ermöglichen einen schnellen Zugriff auf zu bearbeitende Dokumente von jedem Ort aus. Dadurch werden aber nicht nur unter Umständen Zugriffsregeln der eigenen Institution umgangen. Hinzu kommt, dass die genutzten Daten bei einem Dienstleister gespeichert werden, der damit eventuell Zugriff auf vertrauliche Daten oder sogar Nutzungsrechte erhält.

# G 3.106 Ungeeignetes Verhalten bei der Internet-Nutzung

Falsches Verhalten der unterschiedlichsten Art kann bei der Nutzung von Internet-Diensten negative Auswirkungen haben. Typische Beispiele für ein unpassende Handlungsweise und daraus resultierende unerwünschte Wirkungen sind im Folgenden aufgeführt.

**Unzureichende Reaktionsgeschwindigkeit**

Die Erwartung von Kommunikationspartner an die Reaktionsgeschwindigkeit ihrer Ansprechpartner ist bei Internet-Anwendungen und E-Mail hoch. Wenn diese Erwartungen nicht erfüllt werden, z. B. weil kein angepasster Bearbeitungsprozess vorhanden ist, kann das zu Umsatzeinbußen, Frustration von Kunden und Mitarbeitern etc. führen.

**Kontrollverlust**

Durch die Publikation von Informationen in Internet-Diensten oder die Weitergabe per E-Mail ist nicht mehr durch den Verfasser steuerbar, wer diese Informationen erhält und was mit ihnen geschieht. Dadurch kann es zu unerwünschter oder missbräuchlicher Verwendung dieser Informationen kommen.

**Vermischung privater und beruflicher Sphäre**

Da viele IT-Systeme (z. B. Mobiltelefone, PDAs), Anwendungen und Dienste (z. B. soziale Netzwerke, Web-Mail) sowohl beruflich als auch privat genutzt werden, ist es schwierig, die dort verwendeten Informationen sauber zwischen privater und beruflicher Sphäre zu trennen. Dies kann dann problematisch sein, wenn Angreifer so eine Vielzahl von Daten zusammentragen und für gezielte Angriffe auf einzelne Personen oder Institutionen auswerten, wie z. B. beim Social Engineering.

**Vertraulichkeitsverlust**

Häufig wird die Sicherheit von Internet-Anwendungen falsch eingeschätzt oder ungeeignete Maßnahmen zur Absicherung von Informationen benutzt, z. B. wenn Informationen verschleiert statt verschlüsselt werden. Dadurch werden vertrauliche Informationen ungewollt einer breiten Öffentlichkeit zugänglich gemacht.

**Beispiel:**

- Um Daten einfach auszutauschen, hatten zwei Vertragspartner Dateien auf einem Webserver abgelegt. Die URL wurde nur den vertrauenswürdigen Personen der entsprechenden Institutionen per E-Mail mitgeteilt. Die Partner gingen davon aus, dass es nicht möglich ist, diese Dateien über Suchmaschinen zu finden. Doch aufgrund von Webserver-Statistiken, die die meistbesuchten Dateien oder Dateien, die den meisten Datenverkehr (Traffic) verursachten, auflisten, kann es passieren, dass genau diese versteckten Dateien samt genauem Link in der Statistik aufgeführt werden und damit auch für nicht befugte Personen erreichbar sind.

# G 3.107 Rufschädigung

Durch Sicherheitsvorfälle kann es zu einer Rufschädigung der gesamten Institution kommen.

Die verschiedenen Arten von Sicherheitsvorfällen können unterschiedliche direkte Auswirkungen haben, z. B. können dabei sowohl vertrauliche Daten offengelegt als auch finanzrelevante Daten manipuliert werden oder sogar Geschäftsprozesse längere Zeit ausfallen. Wenn Sicherheitsvorfälle publik werden, kann das dazu führen, dass der Ruf der betroffenen Institution geschädigt wird. Je nach Art und Auswirkung eines Sicherheitsvorfalls kann dadurch das Vertrauen der Öffentlichkeit, der Partner, der Kunden, aber auch der Mitarbeiter in die betroffene Institution untergraben werden.

Zu einer Rufschädigung kann es nicht nur durch Sicherheitsvorfälle kommen, die durch höhere Gewalt oder durch Angriffe von Externen verursacht werden, sondern auch durch Fehlverhalten von Mitarbeitern ausgelöst werden, z. B. durch unseriöse Aktivitäten im Internet, Versand von Kettenmails, Sicherheitsvorfälle, die dadurch entstehen, dass Sicherheitsregeln missachtet oder falsch angewandt werden (Laptop mit Kundendaten wird gestohlen, inklusive Kreditkartendaten und Überblick über Bestellungen der letzten Jahre).

**Beispiele:**

- Ein Mitarbeiter einer großen Firma hielt sich bei der Nutzung von Internet-Diensten nicht an die von der Institution aufgestellten Richtlinien, sondern fiel in Diskussionsgruppen immer wieder durch einen unangemessenen Tonfall unangenehm auf. Dies löste nicht nur Aversionen gegenüber dieser Person, sondern gegenüber der gesamten Institution aus, da der Mitarbeiter durch seine elektronischen Visitenkarten als Vertreter seiner Firma wahrgenommen wurde. Dies verschaffte der Firma den Ruf, überheblich zu sein und auch fachlich nicht fundiert zu agieren. Es war eine spezielle Marketingkampagne notwendig, um diesen Ruf wieder zu sanieren.
- Ein Außendienstmitarbeiter verlor bei einer Zugfahrt von ihm unbemerkt einen USB-Stick. Auf diesem Stick befand sich der Überblick über seine Auftragseingänge des letzten Jahres, inklusive Kundenanschriften, Kontodaten und E-Mail-Adressen. Die Daten waren nicht verschlüsselt. Der Finder verkaufte die Daten im Internet. Dies führte bei einigen Kunden zu betrügerischen Abbuchungen. Bei den anschließenden polizeilichen Ermittlungen konnten diese auf den USB-Stick-Verlust zurückgeführt werden, was zu negativen Pressemeldungen und großen Vertrauensverlusten bei Partnern und Kunden führte.
- Mitte Dezember 2008 erhielt der Chefredakteur einer großen deutschen Zeitung anonym ein Paket, das vertrauliche Daten von 130.000 Kunden einer Bank enthielt. Dazu gehörten Buchungsübersichten von Kreditkartenkunden, Geheimnummern für Bank- und Kreditkarten, Listen von Zahlungsströmen, Auslandsabbuchungen und Rücküberweisungen. Im Paket fand sich außerdem eine Rechnung einer Finanzdienstleistungsfirma an die Bank. Die Zeitung vermutete, dass ein Insider auf Datenschutzprobleme aufmerksam machen wollte und veröffentlichte entsprechende Berichte. Der Vorfall wurde als Datenskandal von anderen Medien aufgegriffen und die betroffene Bank sowie die Finanzdienstleistungsfirma an den Pranger gestellt.
  Nach einer Woche stellte sich heraus, dass der Vorfall auf den Heißhunger zweier Kurierfahrer zurückging. In deren Lieferwagen befand sich neben vielen anderen Paketen eines mit einem Weihnachtsstollen, der als

Geschenk für den Chefredakteur gedacht war. Die Kurierfahrer vernaschten den Stollen und versuchten anschließend, dies zu vertuschen, indem sie den zugehörigen Adressaufkleber auf ein anderes Päckchen klebten. Dies war zufällig das Paket mit den Bankkundendaten. Die Kuriere erhielten eine geringe Strafe, der Imageschaden für die Bank war enorm.

# G 3.108 Fehlerhafte Konfiguration von Mac OS X

Um die Systemkonfiguration unter Mac OS X zu verändern, können die Konfigurationsdateien mit einem Texteditor, per Kommandozeilenaufrufe oder mittels einer grafischen Benutzeroberfläche angepasst werden. Werden verschiedene Methoden eingesetzt, um Änderungen am System vorzunehmen, können Inkonsistenzen entstehen, da die Anpassungen in unterschiedlichen Konfigurationsdateien gespeichert werden und keine Synchronisation zwischen diesen erfolgt. Weiterhin können sich Sicherheitseinstellungen gegenseitig aufheben oder die Verwaltung des Clients unter Mac OS X komplizieren.

So ist es zum Beispiel bei der SSH-Konfiguration möglich, die Datei "*/etc/sshd_config*" sowohl direkt anzupassen als auch die grafische Benutzeroberfläche in den "Systemeinstellungen" unter "Freigaben" zu verwenden. Die getroffenen Einstellungen werden in unterschiedlichen Konfigurationsdateien abgelegt und nicht synchronisiert. Dadurch ist es zum Beispiel möglich, dass trotz korrekter SSH-Konfigurationsdateien keine Einwahl per SSH möglich ist, weil sich die Inhalte der Konfigurationsdateien widersprechen.

**Beispiel:**

- In einem kleinen Unternehmen arbeiten zwei Administratoren. Einer der Administratoren nutzt bei der Konfiguration eines Systems grundsätzlich die Kommandozeile beziehungsweise einen Texteditor. Der andere Administrator bevorzugt die grafische Benutzeroberfläche. Um die personelle Ausfallsicherheit zu erhöhen, werden beide Administratoren damit beauftragt, die Fernzugriffe zu pflegen. In der Datei "*/etc/sshd_conf*" befinden sich bereits mehrere Benutzer, die für den Fernzugriff per SSH freigeschaltet sind. Als ein neuer Mitarbeiter eingestellt wird, erstellt der Administrator, der die grafische Benutzeroberfläche bevorzugt, einen Eintrag für den neuen Mitarbeiter. Weil die beiden Listen nicht konsistent sind, kann sich niemand mehr per SSH anmelden.

# G 3.109 Unsachgemäßer Umgang mit FileVault-Verschlüsselung

Unter Mac OS X können die Benutzerverzeichnisse mit dem Programm "FileVault" verschlüsselt werden. Dabei wird der Algorithmus AES-128 eingesetzt. Benutzer können nur mit einem korrekten Passwort auf die mit FileVault-verschlüsselten Daten zugreifen. Das Passwort sollte daher entsprechend stark gewählt sein.

Passwörter können vergessen werden oder in einem Vertretungsfall nicht verfügbar sein.

Um die Daten in diesem Fall trotzdem lesen zu können, ist das Haupt-FileVault-Kennwort vorgesehen. Durch das lokal festgelegte Haupt-FileVault-Kennwort ist es möglich, jeden Benutzerordner des zugehörigen IT-Systems zu entschlüsseln oder das zugehörige Passwort zurückzusetzen. Wird das Haupt-FileVault-Kennwort an einem unsicheren Ort aufbewahrt, können allerdings unter Umständen Unbefugte auf die verschlüsselten Informationen zugreifen.

Gehen sowohl das Benutzer-Passwort als auch das Haupt-FileVault-Kennwort, zum Beispiel wegen eines Feuers oder Diebstahls, verloren, kann dauerhaft nicht mehr auf die mit FileVault-verschlüsselten Daten zugegriffen werden. Das Haupt-FileVault-Kennwort ist mit einem schwächeren Algorithmus (RSA-1024) geschützt, es ist daher einem höheren Risiko ausgesetzt als die Benutzer-Passwörter.

Mit FileVault ist es nicht möglich, die gesamte Festplatte zu verschlüsseln. Somit kann ein Angreifer, der physikalischen Zugriff auf die Festplatte oder ein Benutzerkonto hat, auf sensible Konfigurationsdateien bzw. -ordner zugreifen. Dazu gehören zum Beispiel:

- Protokolldateien in */Library/Logs* und */var/log*,
- Cache- und temporäre Dateien in */Library/Caches* und */tmp*,
- systemweite Einstellungen in */Library/Preferences*,
- eigener Quelltext in */Developer* oder
- jegliche zusätzlichen Programme, die außerhalb des Benutzerordners abgelegt wurden.

Unbefugte könnten auch dann Zugriff auf die Informationen erlangen, wenn sich Benutzer am Client ohne Authentisierung anmelden dürfen ("Automatische Anmeldung"). Die mit FileVault geschützten Informationen werden dann ohne Passwortabfrage beim Start des Computers entschlüsselt.

Ein weiteres Problem kann vom Programm "*Time Machine*" ausgehen. "*Time Machine*" dient zur Datensicherung unter Mac OS X und kann Kopien von kompletten Festplatten, einzelnen Verzeichnissen oder von FileVault-verschlüsselten Benutzerordnern erzeugen. Die Informationen werden jedoch immer unverschlüsselt auf dem Datensicherungsmedium abgelegt, die Art des Mediums spielt dabei keine Rolle. Es ist darauf zu achten, dass die Sicherungsmedien an einem Ort aufbewahrt werden, zu dem unberechtigte Personen keinen Zugang haben.

Zu beachten ist auch, dass eine Datensicherung mit "*Time Machine*" bei aktiviertem FileVault erst durchgeführt werden kann, nachdem sich der Benutzer vom System abgemeldet hat. Ist der Client unter Mac OS X gesperrt oder

befindet er sich im Ruhezustand, kann keine Datensicherungen durchgeführt werden.

**Beispiele:**

- In einem Unternehmen werden die Benutzerordner grundsätzlich mit FileVault verschlüsselt. Da die Mitarbeiter davon ausgehen, dass die Daten durch FileVault ausreichend geschützt sind, bitten sie den zuständigen Administrator darum, die automatische Anmeldung am System zu aktivieren, um Zeit zu sparen. Der Administrator befindet sich ebenfalls in dem Irrglauben, dass die Informationen noch durch FileVault geschützt sind. Indem er die automatische Anmeldung am System aktiviert, wird der mit FileVault geschützte Benutzerordner entschlüsselt und Unbefugte können auf die Informationen zugreifen.
- In einem Unternehmen wird FileVault zur Verschlüsselung und "*Time Machine*" zur Datensicherung eingesetzt. Die Mitarbeiter schalten den Computer während der Mittagspause und am Abend nicht aus, sondern versetzen ihn nur in den Ruhezustand. Nach mehrtägiger Arbeit am System ohne zwischenzeitliches Ausschalten tritt ein Hardware-Fehler auf, der zu einem Datenverlust führt. Weil der Computer nie ausgeschaltet wurde, ließ FileVault kein Backup durch "*Time Machine*" zu. Die Arbeit aus den Tagen seit der letzten Sicherung ist dadurch verloren.
- Auf einem Client unter Mac OS X werden die Benutzerordner mit FileVault verschlüsselt, um ein angemessenes Schutzniveau zu erreichen. Die anschließende Datensicherung wird mit "*Time Machine*" auf einem entfernten Server abgelegt. Die kopierten Informationen können jedoch von allen Personen eingesehen werden, die Zugriffsrechte auf das jeweilige Verzeichnis haben, da die Informationen von "*Time Machine*" unverschlüsselt gespeichert wurden. Ein weiteres Problem entsteht beim Verlust des Datenträgers, da die Informationen unverschlüsselt auf dem Datenträger abgelegt sind.

# G 3.110 Fehlerhafte Konfiguration von OpenLDAP

OpenLDAP ist ein Verzeichnisdienst mit umfangreichen Funktionen. Die Funktionsvielfalt wird durch den modularen Aufbau der Anwendung und die umfassende Anpassbarkeit als Open Source Software erreicht. Darüber hinaus handelt es sich um eine Client-Server-Architektur, bei der sowohl auf Server- als auch auf Client-Seite Konfigurationen vorzunehmen sind. Insgesamt ist OpenLDAP eine hochgradig komplexe Anwendung.

Bei einer fehlerhaften Konfiguration können sich beispielsweise folgende Gefährdungen ergeben:

- Administratoren könnten Anpassungen an der Konfiguration von OpenLDAP vornehmen, die technisch möglich, aber fachlich nicht zulässig sind. Zum Beispiel könnte ein Administrator ein Standard-Schema von OpenLDAP verändern, um zusätzliche Attribute für Verzeichnisdienstobjekte zu gewinnen. Dies führt beim Einsatz von weltweit einheitlichen Standard-Schemas zu Inkompatibilitäten mit anderen Verzeichnisdiensten und kann Probleme bei Updates von OpenLDAP oder bei der Migration auf einen anderen Verzeichnisdienst verursachen. Durch falsche Implementierung kann auch der LDAP-Standards verletzt werden.
- Fehlerhafte Einträge in den zentralen Konfigurationsdateien des slapd-Servers können zu unerwünschtem Verhalten des Servers führen oder diesen unbrauchbar machen, zum Beispiel wenn eine Datenbank versehentlich in einen Nur-Lese-Zustand versetzt wird. Bei fehlerhaften Anweisungen an Backends ist denkbar, dass es zu Datenverlusten kommt, wenn diese Anweisungen beispielsweise nicht zur verwendeten Datenbank passen.
- OpenLDAP kann aus den für eine Betriebssystemdistribution bereitgestellten Binärpaketen installiert werden. Bei einigen Distributionen wird der slapd-Server nach Installation automatisch mit einer Standardkonfiguration gestartet. Eine solche Standardkonfiguration ist häufig unzureichend, insbesondere werden dabei in der Regel keine Maßnahmen wie die Verschlüsselung von Kommunikationsverbindungen konfiguriert.
- Konfigurationseinstellungen können in einer falschen Datei vorgenommen werden. Werden zum Beispiel Benutzer-Einstellungen statt in der korrekten Datei (in der Regel ~/.ldaprc) in der Datei für globale Client-Einstellungen (in der Regel ldap.conf) eingetragen, bleiben sie meist wirkungslos. Werden Client-Einstellungen in die Konfiguration des Servers (in der Regel slapd.conf) eingefügt, können sie die Funktionsfähigkeit des gesamten Systems beeinträchtigen. Das gilt beispielsweise, wenn die für Clients sinnvolle Einstellung, dass sich ein Kommunikationspartner mit einem Zertifikat authentisieren muss, auf Server angewandt wird. Die meisten Clients verfügen nicht über ein geeignetes Zertifikat.
- Zugriffskontrolllisten (Access Control Lists, ACLs) stellen einen grundlegenden Sicherheitsmechanismus von OpenLDAP dar. Die Wirksamkeit der Zugriffsrechteverwaltung hängt entscheidend von der korrekten Konfiguration der ACLs ab. Soll beispielsweise einem bestimmten Benutzer ein Zugriff auf den Verzeichnisdienst untersagt werden, kann ein Administrator, dies durch eine entsprechende Zugriffsregel am Ende des bestehenden Regelwerkes umsetzen. Eine solche Regel wird aber oft nicht wirken, da die Prüfung des Regelwerks nach dem ersten zutreffenden Kriterium abgebrochen wird.

# G 3.111 Unzureichende Trennung von Offline- und Online-Zugriffen auf OpenLDAP

Für den Zugriff auf die durch OpenLDAP verwalteten Daten, das heißt Objekte im Verzeichnisdienst ebenso wie Konfigurationseinstellungen, bestehen verschiedene Zugriffsmöglichkeiten, nämlich

- über das Protokoll LDAP mittels der ldap*-Werkzeuge bei laufendem slapd-Server (auch als Online-Zugriff bezeichnet),
- per Direktzugriff auf die Datenbankdateien der BerkeleyDB mittels der slap*-Werkzeuge von OpenLDAP, unabhängig vom slapd-Server (auch als Offline-Zugriff bezeichnet),
- per Datenbankmanipulation mittels der BerkeleyDB-Werkzeuge von Oracle und
- durch die direkte Manipulation von Konfigurationsdateien im Dateisystem.

Die verschiedenen Zugriffsmöglichkeiten und Werkzeuge erfüllen dabei ganz oder teilweise identische Funktionen. Werden die Zugriffsmöglichkeiten vermischt oder wird die jeweilige Wirkungsweise nicht verstanden, können zahlreiche Fehlersituationen auftreten.

**Beispiele:**

- In einem Unternehmen werden die von OpenLDAP gespeicherten Datensätze mithilfe des Werkzeugs slapcat offline im Format LDIF gesichert. Bei einer Rücksicherung versucht der Administrator, die Datensicherung über die Applikation ldapadd in die leere Datenbank einer laufenden OpenLDAP-Instanz zu laden. Dabei wird übersehen, dass der Export mittels slapcat die Datensätze in der Reihenfolge gesichert hat, wie sie physisch in der Datenbank vorgefunden wurden. Das ldap*-Werkzeug ldapadd erwartet die Datensätze aber gemäß der hierarchischen Verzeichnisstruktur. Der Import führt zu einer inkonsistenten Datenbank, da "ldapadd" versucht, Datensätze einzufügen, deren übergeordnete Einträge noch nicht importiert wurden.
- Ein Anwender von OpenLDAP führt Datensicherung und Rücksicherung der Datenbestände über die BerkeleyDB-Werkzeuge durch. Er umgeht OpenLDAP und sichert die Datenbank mittels des Programms "db_dump" und spielt die Daten mittels "db_load" wieder ein. Da bei dieser Sicherung anwendungsspezifische Zeitstempel nicht korrekt wiederhergestellt werden, ist die wiederhergestellte Datenbank für OpenLDAP inkonsistent und nicht nutzbar.

# G 3.112 Unautorisierte oder falsche Nutzung von Images bei der Nutzung von Windows DISM

DISM (*Deployment Image Servicing and Management*) ist ein Kommandozeilenwerkzeug ab Windows Vista Service Pack 2. Mit ihm können weitreichende Konfigurationsänderungen an Windows-Installationen in Abbilddateien von Festplatten durchgeführt werden DISM ist sowohl auf *Windows Image Format*-Dateien (*WIM*) als auch auf virtuelle Festplatten (*Virtual Hard Disk*, *VHD*) anwendbar. Beide werden bei der angepassten Bereitstellung eines Windows-Systems eingesetzt. DISM kann teilweise auch auf laufende Systeme angewendet werden.

Unautorisierte Änderungen könnten an Installationsquellen oder IT-Systemen unbemerkt durchgeführt werden, entweder unabsichtlich oder durch einen Angreifer. In beiden Fällen kann der Bereitstellungsprozess gestört, die Sicherheitskonfiguration der Installationen beschädigt und auch Schadcode in Umlauf gebracht werden.

Das Windows Image Format ist ein datenbasiertes Imageformat (WIM), das Installationsquellen für Windows ab den Versionen Vista bzw. Server 2008 enthalten kann. Eine WIM-Datei kann mehrere Windows-Editionen enthalten.

Wesentliche Funktionen von DISM sind:

- *Windows Edition Servicing Commands*, um das Windows Image zu ändern
- *Unattended Servicing Commands*, um Änderungen ohne Benutzerinteraktion auszuführen
- *Driver Servicing Commands*, um Gerätetreiber in ein Image zu integrieren
- *International Servicing Commands*, um Sprachpakete anzupassen
- *Application Servicing Commands*, um Anwendungen in Images zu integrieren
- *Package Servicing Commands*, um Pakete in Images oder ein laufendes System zu integrieren

Bei den *Unattended Service Commands* kann insbesondere der Befehl */Apply-Unattended* dazu genutzt werden, einzelne schadcodebehaftete Dateien in ein vorhandenes Image einzuspielen, ohne dass dies vom verantwortlichen Administrator bemerkt wird. Dieses Feature ist insbesondere im Zusammenhang mit der optionalen Angabe einer Steuerdatei im XML-Format kritisch, da hierdurch mehrere Dateien automatisiert installiert werden können.

Die *Application Servicing Commands* können benutzt werden, um zu identifizieren, ob eine bestimmte Anwendung in einem Image enthalten ist. Hierzu wird beispielsweise der Befehl */Get-AppInfo* verwendet. Alternativ können alle in einem Image enthaltenen Applikationen mit dem Befehl */Get-Apps* gelistet werden. Die Anzeige der im Image befindlichen Dateien bietet die Möglichkeit, Angriffsversuche gegen bestimmte Versionen von Software auszuführen.

Die Befehle */Add-Package* und */Remove-Package* aus den *Package Servicing Commands* erlauben es, ganze Pakete (englisch: packages) unter Windows 7 mittels DISM zu ersetzen. Dies vereinfacht das Ersetzen von Dateien für einen potenziellen Angreifer, da mit einem Kommando mehrere Dateien auf einmal ausgetauscht werden können.

Große Sammel-Images bieten viel Spielraum für unkontrollierte Änderungen mit möglicherweise schädlichen Auswirkungen auf die spätere Installation.

Einzelne Softwarekomponenten in einem Sammel-Image könnten mit */Enable-Feature* und */Disable-Feature* aktiviert werden. Ein Manifest oder eine zentrale Definition existiert nicht. So besteht die Gefahr, dass sich, böswillig oder fahrlässig, nicht freigegebene Änderungen in den Bereitstellungsprozess einschleichen, wodurch die Angriffsfläche der bereitgestellten Windows-Systeme unnötig vergrößert wird und die Systeme die erwartete Konformität nicht erfüllen.

# G 3.113 Fehlerhafte Konfiguration eines Lotus Notes Clients oder eines Fremdclients mit Zugriff auf Lotus Domino

Für die betrachteten Lotus Domino Versionen 8.x können verschiedene Clientkomponenten eingesetzt werden. Dazu zählen die Lotus Notes Clients (Standard Client, Basic Client, Entwickler-Client und administrativer Client), Browser (über iNotes), spezielle Clients für PDAs (und andere mobile Endgeräte) und fremde E-Mail-Clients mit Domino-Zugriff über POP3 und/oder IMAP-Schnittstellen. Die fehlerhafte Konfiguration einer Clientkomponente kann die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten der Lotus Notes/Domino-Plattform beeinträchtigen und erfolgreiche Angriffe auf die Plattform ermöglichen.

Beide Lotus Notes Fat Clients der Versionen ab 8.x sind komplexer als die der Vorgängerversionen. Der Standard Client erbt die Komplexität des Eclipse-Frameworks und der Basic Client ist durch die zunehmende Komplexität der Lotus Notes Dienste geprägt. Dies erhöht die Wahrscheinlichkeit fehlerhafter Konfigurationen.

Einige typische fehlerhafte Konfigurationen eines Lotus Notes Clients werden im Folgenden aufgeführt:

- **Fehlende oder unzureichende clientseitige Verschlüsselung von vertraulichen Informationen des Lotus Notes Clients (z. B. der Notes-ID) und clientseitigen Datenbanken (einschließlich Repliken):** Damit bei Verlust oder Diebstahl eines Endgeräts mit einem Lotus Notes Client keine Unbefugten auf vertrauliche Daten zugreifen können, muss entweder das Endgerät oder zumindest die auf dem Notes Client vorhandenen vertraulichen Informationen (einschließlich der ID und vorhandener Zertifikate) ausreichend sicher verschlüsselt sein.
- **Falsche clientseitige Einstellungen zur Replikation:** Dadurch können z. B.serverseitig Daten gelöscht werden, die bei später Entdeckung des Löschvorgangs nur aufwendig wiederherstellbar sind.
- **Falsche clientseitige Einstellungen zum E-Mail-Rückruf:** Diese Einstellungen müssen konsistent sein zur entsprechenden Richtlinie der Institution bezüglich des Umgangs mit E-Mail-Rückruf im Kontext der Verbindlichkeit von E-Mails.
- **Falsch konfigurierte Execution Control List (ECL):** Welche aktiven Inhalte in einem Lotus Notes Client ausgeführt werden können und welche Berechtigungen ihnen zugestanden werden, wird über die Execution Control List (ECL) gesteuert. Ist die ECL fehlkonfiguriert, so können die aktiven Inhalte auch zum Angriff auf den Lotus Notes Client genutzt werden. Bei falsch konfigurierter ECL könnten über aktive Inhalte beispielsweise:
  - Zugriff auf lokale Datenbestände des Client-Rechners (Datenbanken, Dateien, usw.) genommen und Daten "geraubt" werden,
  - auf den Clients lokale Daten verändert oder gelöscht werden und
  - schädliche Programme, beispielsweise Computer-Viren oder trojanische Pferde installiert werden.
- **Weitreichender Zugriff auf die Konfigurationseinstellungen des Lotus Notes Clients durch die Benutzer:** Die Konfigurationseinstellungen eines Lotus Notes Clients können erhebliche Auswirkungen auf die Sicherheit des Clients (wie auch der Lotus Notes/Domino-Plattform) haben. Da-

her ist es gefährlich, wenn Benutzer sicherheitsrelevante Konfigurationen des Clients ändern können.

Die aufgeführten Problemfelder sind Beispiele für mögliche Gefährdungen durch clientseitigen Fehlkonfigurationen. Abhängig vom jeweiligen Einsatzumfeld können weitere Gefährdungen hinzukommen.

Auch bei der Nutzung von Browsern als Notes Clients (über iNotes oder den Domino-Webserver) und bei speziellen Clients für PDAs und vergleichbare mobile Endgeräte wie auch bei der Nutzung von "fremden" E-Mail-Clients über POP3- und/oder IMAP-Schnittstellen kann eine fehlerhafte Konfiguration zu Sicherheitsproblemen führen. Dies ist abhängig von den Konfigurationseinstellungen des verwendeten Browsers oder der fremden Clients und kann z. B. die Ausführung aktiver Inhalte im Browser bzw. Client oder die Kommunikation zum Domino-Server betreffen.

**Beispiel:**

Von einem gestohlenen Laptop ohne Festplattenverschlüsselung mit Lotus Notes Client werden aus der unverschlüsselten lokalen Replik der E-Mail-Datenbank E-Mails mit vertraulichen Inhalten kopiert und deren Inhalt Wettbewerbern oder der Presse zugespielt.

# G 3.114 Fehlerhafte Administration bei der Protokollierung

Werden Protokollierungsserver fehlerhaft administriert und dadurch Sicherheitsvorfälle missachtet oder nicht entdeckt, kann die Sicherheit des gesamten Informationsverbundes beeinträchtigt sein. Als Gründe kommen Konfigurations- oder Bedienungsfehler infrage. Unter Umständen führen solche Administrationsfehler zusätzlich zu einem Vertraulichkeitsverlust von schutzbedürftigen Daten.

Zu den Konfigurationsfehlern zählen falsch oder nicht vollständig eingestellte Parameter und Optionen. Das kann ein zu hoher Grenzwert sein, ab dem eine Alarmierung erfolgt oder zu tolerante Einstellungen der Filter. Solche Fehlkonfigurationen können häufige Fehlalarme auslösen, die eine Frühwarnung erschweren.

Bedienungsfehler bei der zentralen Protokollierung können auftreten, wenn unzureichend oder nicht geschult wird. Das kann dazu führen, dass die Administratoren Analyseergebnisse von Protokolldaten falsch deuten und dadurch einen Sicherheitsvorfall übersehen. Die fehlerhafte Bedienung kann auch dazu führen, dass Protokolldaten versehentlich gelöscht oder verändert werden. Eine weitere potenzielle Gefahr für die Gesamtsicherheit geht von modifizierten Sicherheitseinstellungen und erweiterten Zugriffsrechten für das Protokollierungssystem aus. Diese könnten durch unbefugte Benutzer ausgenutzt werden, um Zugang zu den überwachten IT-Systemen zu erhalten.

**Beispiele:**

- In einer Institution wurden die Grenzwerte für die Auslastung im Frühwarnsystem zu niedrig eingestellt. Aus diesem Grund wird schon bei geringer Auslastung eines Servers ein Fehlalarm ausgelöst. Mit der Zeit werden die Alarme immer mehr vernachlässigt und letztendlich nicht mehr beachtet. Dies führt zu einem hohen Sicherheitsrisiko, da nun auch echte Alarme, bei denen ein Server wirklich stark überlastet ist, ignoriert werden. Wegen der Überlast fällt ein Server für längere Zeit aus und verursacht großen finanziellen Schaden.
- Ein Administrator verändert in einer der Protokolldateien unabsichtlich die Uhrzeit eines Login-Ereignisses von 07:13 auf 77:13, indem er im ausschließlich durch die Tastatur steuerbaren Texteditor einen falschen Befehl eingibt. Diese Protokolldatei wird später benötigt, um zu beweisen, dass sich ein Mitarbeiter am 14. April 2009 um 07:13 Uhr mit seinem Benutzernamen an seinem Rechner angemeldet hat. Durch die ungültige Uhrzeit kann der Eintrag in dieser Protokolldatei nicht verwendet werden. Da das Ereignis auch in keiner anderen Protokolldatei vorhanden ist, lässt sich nicht beweisen, dass der Mitarbeiter an diesem Tag um diese Zeit an seinem Arbeitsplatz war.

# G 3.115 Fehlerhafte Auswahl von relevanten Protokolldaten

Protokolldaten liefern einem IT-Frühwarnsystem oft wichtige Informationen, um IT-Sicherheitsvorfälle zu erkennen. Die relevanten Meldungen aus der großen Menge der verschiedenen Protokollereignisse auszuwählen, ist eine besondere Herausforderung.

Zahlreiche Meldungen haben nur informativen Charakter und lenken von den wirklich wichtigen Meldungen ab. Dies gilt insbesondere, wenn eine zentrale Protokollierung genutzt wird, da dann zahlreiche IT-Systeme ihre Meldungen zum zentralen Protokollierungsserver senden.

Werden zu viele Protokollmeldungen ausgewählt, lässt sich die Fülle von Informationen nur schwer und mit hohem Zeitaufwand auswerten. Des Weiteren besteht die Gefahr, dass Protokolldaten verworfen oder überschrieben werden, wenn Arbeitsspeicher oder Festplattenkapazität des Protokollierungsservers zu klein gewählt wurden. Für den Fall, dass zu wenige oder nicht genug relevante Protokollmeldungen aufgezeichnet werden, könnten sicherheitskritische Vorfälle unerkannt bleiben. Dieses Problem entsteht oft durch falsch konfigurierte Filterfunktionen eines IT-Frühwarnsystems.

**Unterschiedliche Formate**

Protokolldateien werden in verschiedenen Formaten gespeichert und in einer unterschiedlichen Reihenfolge sortiert. Dies ist von den verschiedenen Herstellern der Applikationen und Prozesse abhängig, aus denen die gesammelten Informationen stammen. Beispielsweise stehen in einer Betriebssystemprotokolldatei die Datums- und Uhrzeiteinträge an einer anderen Stelle als bei einer Protokolldatei eines Webservers.

Die Protokollierung von Systemmeldungen wird zur Fehlersuche eingesetzt und verwendet, um Sicherheitsvorfälle aufzuklären. Die Meldungen lassen sich auch zusammen mit einem IT-Frühwarnsystem einsetzen. Um einen Überblick über die auflaufenden Daten zu erhalten, müssen diese korreliert werden. Dazu werden die Protokolldaten normalisiert, also in ein einheitliches Format gewandelt.

**Probleme bei Applikationen und IT-Systemen**

Neben allgemeinen Aspekten bei der Protokollierung können auch Probleme bei den Applikationen und IT-Systemen auftreten, die überwacht werden sollen. So könnte der Fokus bei einem Sicherheitsgateway (Firewall) oder anderen Netz-Komponenten fälschlicherweise auf unterbundene Aktionen wie abgelehnte Verbindungen gelegt werden. Die Auswertung von erlaubten Aktionen, beispielsweise eine korrekt aufgebaute Verbindung, wird vernachlässigt. Dabei könnten genau diese Informationen ein Indiz für einen erfolgreichen Angriffsversuch liefern, zum Beispiel wenn ein Angreifer durch mehrmaliges Ausprobieren das richtige Passwort eines Benutzers errät.

**Beispiele:**

In einem Informationsverbund wird der zentrale Protokollierungsserver immer wieder überlastet. Der Grund hierfür ist, dass die Windows-Ereignismeldungen redundant an den Protokollierungsserver übertragen und abgespeichert werden. Beispielsweise werden bei einer An- und Abmeldung Protokolleinträge sowohl am jeweiligen Client als auch am Domänen-Controller generiert und

an den Protokollierungsserver übertragen. Durch diese Überlastungen könnten andere Protokollinformationen, die relevante Ereignisse, wie Informationen über einen Angriff enthalten, verworfen werden. Die Folge sind Lücken in der Überwachung des Informationsverbundes.

- Der Exchange Server eines Unternehmens soll in das IT-Frühwarnsystem eingebunden und überwacht werden. Hauptaufgabe des Frühwarnsystems ist es, sämtliche E-Mails, die über den Exchange Server übertragen werden, aufzuzeichnen. Der Administrator muss hierfür SMTP-Transaktionen am Exchange Server protokollieren. Weil aber irrtümlich das Exchange Message Tracking am Server nicht aktiviert wurde, kann der Exchange Server nicht sinnvoll überwacht werden.

# G 3.116 Fehlende Zeitsynchronisation bei der Protokolldatenauswertung

Wenn in einem Informationsverbund die Zeit nicht auf allen IT-Systemen synchronisiert wird, können die Protokolldaten unter Umständen nicht miteinander verglichen werden, da die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. So kann beispielsweise die Korrelation einer Regelverletzung bei einem Sicherheitsgateway (Firewall) mit fehlgeschlagenen Anmeldeversuchen missglücken. Diese Gefahr besteht besonders, wenn eine zentrale Protokollierung eingesetzt wird. Ohne gemeinsame Zeitbasis sind Meldungen von unterschiedlichen IT-Systemen nicht miteinander korrelierbar.

Die Zeit- und Datumseinstellungen bei einer Zeitstempelfunktion hängen sehr oft von der regionalen Einstellung ab. So wird beispielsweise im angelsächsischen Raum das Datum in der Schreibweise MM/DD/YYYY (Monat/Tag/Jahr, z. B. (05/09/2009) angegeben. Dies kann bei einer automatischen Auswertung, wie beispielsweise durch ein IT-Frühwarnsystem, zu Fehlinterpretationen führen.

Des Weiteren fehlt, vor allem bei Unix-Systemen, oft die Angabe einer Jahreszahl in den Protokolldateien. Dies ist besonders problematisch im Bezug auf die Beweiskraft der Daten, wenn weiter zurückliegende Ereignisse betrachtet werden müssen und diese zeitlich nicht eingeordnet werden können.

**Beispiele**

- In einem Informationsverbund wird ein zentraler Protokollierungsserver in Betrieb genommen. Das gesamte Netz erhält seinen Zeittakt von einem internen NNTP-Server im LAN. Der Informationsverbund wird mehrfach Ziel von Angriffen, bei denen der NTP-Server kompromittiert wird. Auf diese Weise wird die Uhrzeit, die der NTP-Server verteilt, geändert, sodass die restlichen IT-Systeme über eine unterschiedliche Uhrzeit als der Protokollierungsserver verfügen. Dies hat zur Folge, dass die Protokolldaten der IT-Systeme inkonsistent sind und sich nicht mehr untereinander vergleichen lassen.
- Ein deutsches Unternehmen integriert ein neues Sicherheitsgateway (Firewall), das im außereuropäischen Ausland entwickelt und hergestellt wurde, in seinen Informationsverbund. Da im Unternehmen alle IT-Systeme und Anwendungen mithilfe eines IT-Frühwarnsystems überwacht werden, wird auch dieses Sicherheitsgateway eingebunden. Am IT-Frühwarnsystem ist die Einstellung aktiv, dass alle Protokolldaten, die ein anderes Datum enthalten als das Tagesdatum, einen Alarm auslösen. Dadurch sollen mögliche Manipulationen der Protokolldaten aufgedeckt werden. Das Datum wird am Frühwarnsystem in der Form DD/MM/YY (Tag/Monat/Jahr) interpretiert. Die Protokolldateien des neuen Sicherheitsgateways liefert Datumseinträge allerdings im Format MM/DD/YY (Monat/Tag/Jahr). Dies führt dazu, dass das Sicherheitsgateway bereits am ersten Tag, an dem es in das IT-Frühwarnsystem integriert ist, eine große Menge an Fehlalarmen produziert.

# G 3.117 Fehlerhafte Automatisierung beim Cloud Management

Um die potenziellen Vorteile des Cloud-Computings zu nutzen, ist eine Automatisierung der Routineaufgaben und der Bereitstellung der Cloud-Ressourcen erforderlich. Die Automatisierung von Prozessen bringt auch eine Reihe von Herausforderungen mit sich.

Eine Automatisierung ist dann fehlerhaft, wenn bei der Reproduktion eines Cloud-Dienstes die automatisierte Bereitstellung der dafür benötigten Cloud-Ressourcen (virtuelle Maschine, Arbeitsspeicher, CPU, Festplattenkapazität) nicht hinreichend erfolgt, um den Cloud-Dienst in den versprochenen Eigenschaften bereitzustellen.

Eine fehlerhafte Automatisierung kann auch durch technische Ursachen begründet sein. Dies ist dann beispielsweise der Fall, wenn Konfigurationen für die automatisierte Provisionierung und De-Provisionierung nicht an den technischen Cloud-Komponenten umgesetzt werden.

Durch eine fehlerhafte Automatisierung können größere Auswirkungen entstehen als durch einzelne manuelle Konfigurationen.

Eine fehlerhafte Automatisierung ist mit großen Schäden verbunden, wenn die Nutzung und Zuweisung von Ressourcen über automatisierte Prozesse nicht durch Richtlinien beschränkt ist. Wenn für Cloud-Ressourcen keine Priorisierungen und Grenzen für die verschiedenen Cloud-Dienste definiert wurden, kann es zu Ressourcen-Engpässen oder Ressourcen-Verschwendung kommen.

**Beispiele:**

- Für eine Cloud-Anwendung wären 4 GB Speicherplatz je Mandant vorzusehen. In der Richtlinie zur automatisierten Bereitstellung der Cloud-Anwendung wird versehentlich ein Wert von 400 GB je Mandant hinterlegt. Entsprechend kann bei einer automatisierten Bereitstellung dieser Cloud-Anwendung bei einer Vielzahl von Mandanten bald der Speicherplatz nicht mehr bereitgestellt werden.
- Bei der automatisierten Provisionierung von Cloud-Ressourcen wird ein Verwaltungssystem für Speicher konfiguriert. Dieses Verwaltungssystem ist jedoch nicht verfügbar und es erfolgt weder eine Umsetzung der Konfiguration noch eine Fehlermeldung.

# G 3.118 Ungeeignete Konfiguration von Cloud-Diensten und Cloud-Verwaltungssystemen

Die Cloud-Administration umfasst die Einstellungen an den Verwaltungssystemen für Virtualisierung und für die Cloud. Die Vielzahl der zu verwaltenden Cloud-Komponenten macht Änderungen, die durchgängig an allen Systemen umgesetzt werden müssen, für die Administration im Cloud Management komplex und fehleranfällig. Insbesondere menschliche Fehlhandlungen bei der Cloud-Administration können enorme Sicherheitsprobleme nach sich ziehen, denn Fehleingaben in den Verwaltungssystemen führen zu ungeeigneten Konfigurationen.

**Ungeeignete Konfiguration von Cloud-Diensten**

Menschliche Fehlhandlungen können dazu führen, dass die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Informationen der Cloud-Dienste durch deren ungeeignete Konfiguration gefährdet wird. Diese kann in der Zuweisung von Cloud-Ressourcen zu einem Cloud-Dienst bestehen, oder in einer falschen Vergabe von Berechtigungen.

Bei der Verwendung von fehlerhaften Cloud-Diensteprofilen wirken sich solche ungeeigneten Konfigurationen auf alle darauf basierenden Cloud-Dienste aus.

**Ungeeignete Konfigurationen der Cloud-Verwaltungssysteme**

Bei automatisierten Konfigurationen von Cloud-Diensten über die Cloud-Verwaltungssoftware kann es vorkommen, dass Konfigurationen nicht oder nicht korrekt an den einzelnen Verwaltungskomponenten (die sogenannten *Element Manager*) der Cloud-Infrastruktur umgesetzt werden. Dies kann durch Fehler in den umzusetzenden Konfigurationsdatensätzen oder durch fehlerhafte Übermittlung oder Umsetzung der Änderungen durch die Element Manager begründet sein.

**Beispiele:**

- Eine virtuelle Maschine (als Teil einer Cloud-Infrastruktur) wird einer falschen Sicherheitszone zugeordnet.
- Eine virtuelle Maschine (als Teil einer Cloud-Infrastruktur) wird einem falschen Mandanten zugeordnet.
- Bei der Cloud-Administration erfolgt eine Fehlkonfiguration bei der Zuweisung von Verwaltungsservern zu virtuellen Speichernetzen (sogenannten VSANs). Als Folge stehen den virtuellen Maschinen der verwalteten Cloud-Dienste keine Speicherressourcen zur Verfügung.

# G 3.119 Fehlerhafte Anwendung von Standards

Für die Realisierung von Web-Services sind zahlreiche Standards verfügbar (siehe M 4.451 *Aktuelle Web-Service Standards*), die insbesondere in ihrem Zusammenwirken und ihren Abhängigkeiten untereinander eine hohe Komplexität erreichen.

Als Konsequenz dieser Komplexität sind Fehler in der Anwendung der Standards naheliegend. Solche Fehler können vielfältige Konsequenzen haben:

- Der Standard wird nicht wirksam umgesetzt. Insbesondere kann dies dazu führen, dass vorgesehene Sicherheitsfunktionen nicht wirksam realisiert werden, indem zum Beispiel Berechtigungsprüfungen nicht durchgeführt werden oder eine Verschlüsselung nicht erfolgt.
  Beispiel: In einem sicherheitsrelevanten SOAP-Header wurde ein Tippfehler gemacht, gleichzeitig fehlt das Attribut env:mustUnderstand=true. Der SOAP-Knoten kann den Header aufgrund des Tippfehlers nicht interpretieren und ignoriert ihn.
- Die Anwendung des Standards erfolgt nicht in der vorgesehenen Art beziehungsweise nicht im vorgesehenen Umfang. So ist es denkbar, dass zum Beispiel XML-Signaturen nicht alle relevanten Bestandteile einer Nachricht umfassen, oder dass nicht mit ausreichend sicheren Algorithmen verschlüsselt wird.
  Beispiel: Eine XML-Signatur wird über ein XML-Element erzeugt, das in der verwendeten XML-Struktur mehrfach vorkommen kann, sodass ein Angreifer mit *XML Signature Wrapping* die Inhalte der Nachricht semantisch verändern kann, ohne dass die Signatur ihre Gültigkeit verliert.
- Die Implementierung erzeugt Fehler im Betrieb, die unter Umständen nur in besonderen Situationen auftreten und die Verfügbarkeit des Web-Service einschränken.
  Beispiel: Berechtigungsprüfungen werden mit einem Fehler abgebrochen, wenn der aufrufende Benutzer einer bestimmten Kombination aus Rolle und Organisationseinheit zuzuordnen ist.
- Die Implementierung umfasst zusätzliche, vom jeweiligen Standard umfasste Funktionen, die für den konkreten Web-Service nicht erforderlich sind. Solche ungenutzten Funktionen bieten dem Angreifer eine höhere Angriffsfläche und können insbesondere für Angriffe auf die Verfügbarkeit des Web-Service missbraucht werden.
  Beispiel: Beim Parsen einer Nachricht werden externe XML-Referenzen aufgelöst, obwohl dies für den betroffenen Web-Service nicht erforderlich ist.

Aus Implementierungsfehlern kann sich einerseits eine unbeabsichtigte Beeinträchtigung der Verfügbarkeit, Offenlegung oder Verfälschung von Informationen oder Metadaten ergeben, indem die implementierten Dienste nicht oder falsch funktionieren. Andererseits können Angreifer solche Implementierungsfehler auch gezielt ausforschen (siehe G 5.184 *Informationsgewinnung über Web-Services*) und ausnutzen, um die Verfügbarkeit, Vertraulichkeit oder Integrität des Web-Service anzugreifen.

Wegen der hohen Abhängigkeiten der relevanten Standards untereinander besteht zudem die Gefahr, dass Fehler in der Anwendung eines Standards ihre Auswirkungen erst im Kontext davon unmittelbar oder mittelbar abhängiger Standards und Komponenten zeigen, sodass der Fehler nur mit hohem Aufwand eingegrenzt und behoben werden kann.

# G 3.120 Fehler bei der Orchestrierung

Wenn verschiedene Web-Services zusammengefügt werden, um übergreifende Aufgaben zu realisieren, so spricht man von *Orchestrierung*. Die Orchestrierung kann statisch erfolgen, indem auf der Grundlage von WSDL und UDDI geeignete Dienste ausgewählt und zusammengefügt werden. In Service-orientierten Architekturen kann eine Orchestrierung aber auch dynamisch erfolgen, das heißt, für die zu erledigenden Aufgaben werden erst zur Laufzeit geeignete Dienste identifiziert und ausgewählt. In der Praxis ist die dynamische Orchestrierung wenig verbreitet.

Die Orchestrierung oder, im Falle einer dynamischen Orchestrierung, ihre Implementierung erfordern besondere Sorgfalt, um Fehler unterschiedlichster Art zu vermeiden:

- Fachaufgaben werden fehlerhaft abgebildet oder Dienste werden fehlerhaft zusammengestellt: Aus dem Zusammenwirken der einzelnen Dienste kann sich eine hohe Komplexität ergeben, die hohe Anforderungen an die Planung der Orchestrierung stellt. Fehlendes Verständnis der zu realisierenden Fachaufgabe, aber auch der Funktionalität und Interaktion der beteiligten Services kann dazu führen, dass die Orchestrierung nicht korrekt erfolgt und die resultierende Funktionalität nicht den Anforderungen entspricht.
- Dienste oder Schnittstellen werden fehlerhaft beschrieben oder implementiert: Wenn die Beschreibung eines Dienstes und seine Implementierung voneinander abweichen, kann daraus resultieren, dass ein ausgewählter Dienst die ihm zugedachte Aufgabe nicht oder nur unzureichend erfüllt. Dies kann einerseits die Abbildung der fachlichen Funktionalität beeinträchtigen, aber auch unmittelbare Auswirkungen auf die Sicherheit haben, wenn der ausgewählte Dienst eine Sicherheitsfunktion erfüllen sollte (zum Beispiel Autorisierung).
- Eine Transaktionssicherheit fehlt, oder parallele Prozesse haben ungewollte Auswirkungen: Web-Services werden typischerweise von mehreren Anwendungen oder Prozessen gleichzeitig benutzt. Dieser Umstand muss bei der Orchestrierung berücksichtigt werden. Insbesondere dürfen die beteiligten Web-Services keine Annahmen über den Zustand von Daten oder Systemen zwischen zwei Aufrufen oder vor und nach dem Aufruf eines weiteren Services machen.
- Der Schutzbedarf wird nicht ausreichend berücksichtigt: Wenn Dienste im Rahmen der Orchestrierung zusammengestellt werden, ist neben funktionalen Aspekten auch das vom jeweiligen Dienst realisierte Sicherheitsniveau zu berücksichtigen (zum Beispiel Qualität der Authentisierung, Verschlüsselung, aber auch Verfügbarkeiten). Andernfalls besteht die Gefahr, dass Dienste in eine Fachaufgabe eingebunden werden, die dem Schutzbedarf dieser Aufgabe nicht gerecht werden. Dieser Aspekt gewinnt besondere Bedeutung, wenn die Orchestrierung Dienste verschiedener Diensteanbieter umfasst.

Gerade in komplexen Szenarien mit vielen zusammenwirkenden Diensten oder mit dynamischer Orchestrierung bestehen oft nur eingeschränkte Möglichkeiten, Dienste in ihrem Zusammenspiel zu testen, sodass die oben beschriebenen Fehler gegebenenfalls erst im laufenden Betrieb erkannt werden.

# G 3.121 Konfigurations- und Administrationsfehler bei Web-Services

Beim Einsatz von Web-Services können Konfigurations- und Administrationsfehler nicht nur bei den zugrunde liegenden Plattformen (Betriebssysteme, Web- und Applikationsserver, Datenbanken) auftreten, sondern auch in Verbindung mit den Web-Services selbst oder den dazugehörigen Komponenten, zum Beispiel einem Enterprise Service Bus oder einem Security Token Service.

Je nach Art des Dienstes beziehungsweise der Komponenten können Konfigurationseinstellungen und Parameter in unterschiedlichster Form gepflegt werden, von (gegebenenfalls XML-basierten) Konfigurationsdateien über Datenbankinhalte bis hin zu eigenen Administrationswerkzeugen und -oberflächen. Entsprechend unterschiedlich stark ausgeprägt ist die Gefahr von Fehlern: Wenn XML-Dateien manuell bearbeitet werden, ist die Fehlergefahr sicherlich gegenüber einer Administrationsoberfläche mit Plausibilitätsprüfungen und Sicherheitsabfragen deutlich erhöht.

Administrationsfehler werden weiter begünstigt, wenn die Dokumentation der Konfigurationsmöglichkeiten, ihrer Auswirkungen und der gewählten Einstellungen fehlt, veraltet oder unvollständig ist, und wenn das administrative Personal nicht ausreichend geschult oder eingewiesen wurde.

Die Konsequenzen solcher Konfigurations- und Administrationsfehler können ganz unterschiedlich ausfallen:

- Web-Services funktionieren nicht oder erfüllen nicht die ihnen zugedachte Aufgabe. Besonders problematisch sind hier Fehler, die sich auf den Web-Service erst verzögert oder nur unter bestimmten Randbedingungen auswirken, sodass eine Zuordnung des Problems zur Ursache erschwert wird.
- Benutzer oder Berechtigungen werden falsch administriert. Dadurch können entweder berechtigte Benutzer die ihnen zugedachten Dienste nicht nutzen (Beeinträchtigung der Verfügbarkeit), oder unberechtigte Benutzer haben Zugriff auf Dienste oder Informationen, die nicht für sie bestimmt sind (Beeinträchtigung der Vertraulichkeit, bei Schreibzugriff auch der Integrität).
- Vorgesehene Sicherheitsmechanismen werden versehentlich deaktiviert, funktionieren falsch oder verfügen nicht über eine angemessene Stärke (zum Beispiel wenn kryptographische Algorithmen und Parameter falsch gewählt werden).
- Die Kommunikation zwischen verschiedenen Diensten oder der Austausch von Nachrichten, gegebenenfalls über einen Enterprise Service Bus, werden gestört, verzögert oder unterbunden.
- Die Orchestrierung verschiedener Web-Services wird beeinträchtigt, weil Dienste- oder Schnittstellenbeschreibungen falsch sind oder Repositories nicht richtig konfiguriert sind. Insbesondere bei einer dynamischen Orchestrierung können die Folgen erheblich sein (siehe hierzu auch G 3.120 *Fehler bei der Orchestrierung*).
- Die Nachvollziehbarkeit der Informationsverarbeitung und die Erkennbarkeit oder Aufklärungsmöglichkeiten von Angriffen werden beeinträchtigt, wenn Fehler in der Konfiguration von Protokollierungsmechanismen oder -komponenten gemacht werden, indem zum Beispiel Protokollierungs-

funktionen ausgeschaltet oder Protokollierungsinhalte ungeeignet definiert werden.
- Die Angriffsfläche kann sich unnötig erhöhen, wenn in produktiven Umgebungen Funktionen für die Fehlersuche (Debugging) und die Softwareentwicklung oder andere ungenutzte Funktionen aktiv bleiben.
- Durch die unnötige Preisgabe von Informationen können Angriffe ermöglicht oder erleichtert werden (siehe hierzu auch G 5.184 *Informationsgewinnung über Web-Services*).

In verteilten Umgebungen, bei denen die beteiligten Web-Services von verschiedenen Anbietern betrieben werden, erhöht sich die Fehlergefahr durch die mangelhafte Abstimmung oder Kommunikation der beteiligten Anbieter untereinander.

# G 3.122 Fehlerhafte Nutzung eines Cloud Services

Werden Cloud Services innerhalb einer Institution abweichend zu den Vorgaben aus der Planungs- und Konzeptionsphase eingesetzt, liegt eine fehlerhafte Nutzung vor, aus der sich unterschiedliche Gefährdungen, insbesondere der Vertraulichkeit, ergeben können.

In der Praxis sind folgende Ausprägungen fehlerhafter Nutzung relevant:

- Cloud Services werden von Benutzern für Informationen eingesetzt, deren Schutzbedarf höher klassifiziert ist als der Schutzbedarf, für den der verwendete Cloud Service ursprünglich definiert wurde.
- Der Zugriff auf einen Cloud Service erfolgt über nicht autorisierte Kanäle oder Schnittstellen. In der Folge kann es zum Aufbau unerwünschter und nicht kontrollierter Kommunikationsverbindungen kommen. Die entstandenen Verbindungen können sowohl vom Cloud-Diensteanbieter zum Cloud-Anwender als auch von der Cloud nach außen aufgebaut werden. Gerade ein solcher Verbindungsaufbau kann durch nachfolgende Verkettung zu weiteren unerwünschten Kommunikationsverbindungen führen (Chaining).
- Durch die Nutzung spezieller Funktionen, wie beispielsweise die Freigabe von Dateien oder Ordnern für andere Benutzer, kommt es zu einer ungewollten Erteilung von Zugriffsrechten. In der Folge haben Unberechtigte Zugriff auf Informationen der Institution. Die Vertraulichkeit und Integrität der Daten ist damit nicht mehr gewährleistet.

**Beispiel:**

- Ein Mitarbeiter verwendet einen Online-Speicher-Dienst. Mithilfe der zur Verfügung stehenden Optionen gibt er einen Teil seines Laufwerks für andere Benutzer frei. Auf diesem Laufwerk befinden sich neben den Daten, die für die Freigabe vorgesehen waren, auch schützenswerte Daten, deren Veröffentlichung nicht vorgesehen war. Durch die erfolgte Freigabe des Laufwerks können auch Unberechtigte Zugriff auf diese Daten erlangen.

# G 3.123 Unerlaubte private Nutzung des dienstlichen Mobiltelefons, Smartphones, Tablets oder PDAs

Wird ein dienstliches Mobiltelefon, Smartphone, Tablet oder ein PDA unerlaubt privat benutzt, kann dies zu folgenden Problemen führen. Beispiele sind:

- Durch private Anrufe oder Nutzung von Datendiensten entstehen Kosten für die Institution.
- Nutzt der Anwender eine grafisch aufwendige Applikation (z. B. ein Spiel), entleert sich der Akku schneller. Dadurch kann das Gerät für die nachfolgende dienstliche Nutzung gegebenenfalls nicht mehr zur Verfügung stehen.
- Verbietet die Institution die private Nutzung von Mobiltelefonen, Smartphones, Tablets und PDAs nicht explizit bzw. kontrolliert ein solches Verbot nicht wirksam, kann dies z. B. datenschutzrechtliche Folgen haben, was das Informationssicherheitsmanagementsystem der Institution behindern kann.
- Werden auf dem Gerät auch private personenbezogene Daten gespeichert, erhöht sich dadurch die Gefahr, dass die Institution Datenschutzgesetze verletzt, beispielsweise wenn die Daten vom Telefon automatisiert durch die Institution gesichert werden.
- Wird auf einem dienstlichen Mobiltelefon, Smartphone, Tablets oder PDA eine private und nicht von der Institution freigegebene Anwendung installiert und betrieben, kann dadurch Schadsoftware auf das Gerät gelangen, Daten, wie z. B. das dienstliche Telefonbuch, können an unbefugte Stellen abfließen oder die Integrität der Daten auf dem Gerät kann durch Fehler in der Anwendung beeinträchtigt werden.

# G 3.124 Fehlende und ungenügende Implementierungen bzw. Konfigurationen in einer SOA

Durch aktuelle Authentisierungs-, Integritäts- und Verschlüsselungsmechanismen lässt sich das Sicherheitsniveau in einer serviceorientierten Architektur (SOA) wesentlich verbessern. Allerdings müssen diese Maßnahmen korrekt eingesetzt bzw. konfiguriert werden. Beispielsweise erhöhen XML-Signaturen nur dann die Informationssicherheit hinsichtlich der Integrität, wenn sie auf alle Elemente innerhalb der XML-Datei angewendet werden und die Signatur bei der Verarbeitung der Nachrichten korrekt geprüft wird.

Eine Signatur für einzelne Elemente ist syntaktisch zwar möglich, aber unter Umständen nicht hilfreich. Denn so ist es für Empfänger eines XML-Objektes nicht immer erkennbar, dass alle anderen, nicht-signierten Elemente weiterhin manipuliert sein könnten. Außerdem besteht die Gefahr, dass signierte Elemente durch einen Replay-Angriff ausgetauscht und so als vollkommen valide erkannt werden.

# G 4 Gefährdungskatalog Technisches Versagen

G 4.27 Unterlaufen von Zugriffskontrollen über ODBC

G 4.28 Verlust von Daten einer Datenbank

G 4.29 Datenverlust einer Datenbank bei erschöpftem Speichermedium **- entfallen**

G 4.30 Verlust der Datenbankintegrität/-konsistenz

G 4.31 Ausfall oder Störung von Netzkomponenten

G 4.32 Nichtzustellung einer Nachricht

G 4.33 Schlechte oder fehlende Authentikationsverfahren und -mechanismen

G 4.34 Ausfall eines Kryptomoduls

G 4.35 Unsichere kryptographische Algorithmen

G 4.36 Fehler in verschlüsselten Daten

G 4.37 Mangelnde Verlässlichkeit von Groupware

G 4.38 Ausfall von Komponenten eines Netz- und Systemmanagementsystems

G 4.39 Software-Konzeptionsfehler

G 4.40 Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients **- entfallen**

G 4.41 Nicht-Verfügbarkeit des Mobilfunknetzes

G 4.42 Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs

G 4.43 Undokumentierte Funktionen

G 4.44 Ausfall von Novell eDirectory

G 4.45 Verzögerte Archivauskunft

G 4.46 Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung

G 4.47 Veralten von Kryptoverfahren

G 4.48 Ausfall der Systeme eines Outsourcing-Dienstleisters

G 4.49 Unsichere Default-Einstellungen auf Routern und Switches

G 4.50 Überlastung des z/OS-Betriebssystems

G 4.51 Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs

G 4.52 Datenverlust bei mobilem Einsatz

G 4.53 Unsichere Default-Einstellungen bei Speicherkomponenten

| | |
|---|---|
| G 4.54 | Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS |
| G 4.55 | Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP |
| G 4.56 | Ausfall der VoIP-Architektur |
| G 4.57 | Störungen beim Einsatz von VoIP über VPNs |
| G 4.58 | Schwachstellen beim Einsatz von VoIP-Endgeräten |
| G 4.59 | Nicht-Erreichbarkeit bei VoIP durch NAT |
| G 4.60 | Unkontrollierte Ausbreitung der Funkwellen |
| G 4.61 | Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen |
| G 4.62 | Verwendung unzureichender Steckdosenleisten |
| G 4.63 | Verstaubte Lüfter |
| G 4.64 | Komplexität von Druckern, Kopierern und Multifunktionsgeräten |
| G 4.65 | Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten |
| G 4.66 | Beeinträchtigung von Gesundheit und Umwelt durch Drucker, Kopierer und Multifunktionsgeräte |
| G 4.67 | Ausfall von Verzeichnisdiensten |
| G 4.68 | Störungen des Active Directory durch unnötige Dateireplizierung |
| G 4.69 | Probleme bei der IPSec-Konfiguration |
| G 4.70 | Unsichere Standard-Einstellungen auf VPN-Komponenten |
| G 4.71 | Probleme bei der automatisierten Verteilung von Patches und Änderungen |
| G 4.72 | Inkonsistenzen von Datenbanken im Trivial Database Format unter Samba |
| G 4.73 | Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme von Windows-Versionen |
| G 4.74 | Ausfall von IT-Komponenten in einer virtualisierten Umgebung |
| G 4.75 | Störung der Netzinfrastruktur von Virtualisierungsumgebungen |
| G 4.76 | Ausfall von Verwaltungsservern für Virtualisierungssysteme |
| G 4.77 | Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen |

G 4.78 Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse

G 4.79 Schwachstellen in der Bluetooth-Implementierung

G 4.80 Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen

G 4.81 Erweiterte Rechte durch Programmdialoge auf Terminalservern

G 4.82 Ausfall und Nichterreichbarkeit von Terminalservern

G 4.83 Fehlfunktionen selbstentwickelter Makros unter Outlook

G 4.84 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services

G 4.85 Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services

G 4.86 Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen

G 4.87 Offenlegung vertraulicher Informationen bei Webanwendungen

G 4.88 EMV-untaugliche Stromversorgung

G 4.89 Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung

G 4.90 Ungewollte Preisgabe von Informationen durch Cloud Cartography

G 4.91 Unberechtigtes Wiedereinspielen von Snapshots

G 4.92 Inkompatibilität zwischen der Cloud-Administration und der Administration der Cloud-Elemente

G 4.93 Ausfall von Verwaltungsservern und Verwaltungssoftware

G 4.94 Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services

G 4.95 Ausfall von Komponenten einer Speicherlösung

G 4.96 Fehlfunktion von Komponenten einer Speicherlösung

G 4.97 Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister

G 4.98 Ausfall von Tools zur Administration von Cloud Services bei Cloud-Nutzung

G 4.99 Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen

G 4.100 Hardwareausfall und Hardwarefehler bei eingebetteten Systemen

G 4.101 Ausfall eines zentralen Identitäts- und Berechtigungsmanagement-Systems

# G 4.1 Ausfall der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Bei einer Messung mit circa 60 Messstellen wurden 1983 in Deutschland rund 100 solcher Netzeinbrüche registriert. Davon dauerten fünf Ausfälle bis zu einer Stunde und einer länger als eine Stunde. Diese Unterbrechungen beruhten einzig auf Störungen im Versorgungsnetz. Dazu kommen Unterbrechungen durch Abschaltungen bei nicht angekündigten Arbeiten oder durch Kabelbeschädigungen bei Tiefbauarbeiten.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Rohrpostanlagen, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen, Sprinkleranlagen, Telefonnebenstellenanlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druckerzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig.

Die Liberalisierung des Strommarktes führte in einigen Industrieländern zu einer Verschlechterung des Versorgungsniveaus. Auch in Deutschland könnte daher die Gefahr wachsen, dass Probleme durch Ausfälle der Stromversorgung oder durch Schaltvorgänge an nationalen Versorgungsübergängen entstehen.

**Beispiele:**

- In einem großen süddeutschen Industriebetrieb war die gesamte Stromversorgung für mehrere Stunden unterbrochen, da technische Probleme beim Stromversorgungsunternehmen aufgetreten waren. Infolgedessen fielen sowohl die Produktion als auch sämtliche Rechner der Entwicklungsabteilungen aus, die über keine Ersatz-Stromversorgung verfügten.
- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien nach etwa 40 Minuten fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die Energieversorger ihre Abschaltpläne geheim.
- Im November 2005 waren nach heftigen Schneefällen in Niedersachsen und Nordrhein-Westfalen viele Gemeinden tagelang ohne Stromversorgung, weil viele Hochspannungsmasten unter der Schnee- und Eislast umgestürzt waren. Die Wiederherstellung der Stromversorgung dauerte einige Tage.

# G 4.2 Ausfall interner Versorgungsnetze

Es gibt in einem Gebäude eine Vielzahl von Netzen, die der Ver- und Entsorgung und somit als Basis für alle Geschäftsprozesse einer Institution einschließlich der IT dienen. Der Ausfall von Versorgungsnetzen wie:

- Strom,
- Telefon und
- Kühlung

kann eine Vielzahl von Aufgaben beeinträchtigen. Ein solcher Ausfall kann aber auch zu einer sofortigen Störung des IT-Betriebs führen. Demgegenüber kann es bei Ausfall in den Bereichen:

- Heizung bzw. Lüftung,
- Wasser,
- Löschwasserspeisungen,
- Abwasser,
- Rohrpost,
- Gas,
- Melde- und Steueranlagen (Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen

unter Umständen zu zeitverzögerten Störungen kommen.

Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

**Beispiele:**

- Der Ausfall der Stromversorgung wirkt nicht nur auf die IT direkt, sondern auch auf alle anderen Netze, die mit elektrisch betriebener Steuer- und Regeltechnik ausgestattet sind. Selbst in Abwasserleitungen sind unter Umständen elektrische Hebepumpen vorhanden.
- Der Ausfall der Wasserversorgung beeinträchtigt eventuell die Funktion von Klimaanlagen.
- Ein länger anhaltender Stromausfall führte im Backup-Rechenzentrum eines Hosting-Dienstleisters zum Totalausfall mehrerer Speichersysteme. Ursache war, dass die Klimatechnik nicht an die Netzersatzversorgung (NEA) angeschlossen war und keine adäquate Fernüberwachung der versorgenden Technik des RZ aufgebaut war. So liefen die IT-Systeme über NEA-Versorgung ohne Kühlluftkreislauf weiter. Mehrere hundert Festplatten mussten so als Totalschaden ausgetauscht werden.

# G 4.3 Ausfall vorhandener Sicherungseinrichtungen

Durch technische Defekte oder äußere Einflüsse (z. B. aufgrund von Alterung, Fehlbedienung, mangelhafter Wartung, Manipulation, Stromausfall) kann es zum Ausfall von Sicherungseinrichtungen kommen, so dass ihre Schutzwirkung stark herabgesetzt ist oder gänzlich ausfällt. Weiterhin kommt es vor, dass in Problembereichen, z. B. durch starke Umwelteinflüsse oder besonders hohe Nutzungsfrequenzen, Kontrollen und Wartungsintervalle nicht entsprechend angepasst werden. Auch hierdurch können Sicherungseinrichtungen ausfallen.

**Beispiele:**

- Türschlösser können durch Alterung oder Fehlbedienung beschädigt werden.
- Feuerlöscher, die nicht ordnungsgemäß gewartet werden, funktionieren u. U. unzureichend.
- Verschmutzte Brandmelder erkennen u. U. Brände nicht ordnungsgemäß oder geben Fehlalarm.
- Schlüssel oder Ausweiskarten können durch unsachgemäße Aufbewahrung oder durch Abnutzung beschädigt werden.
- Riegelkontakte in Türen können festgeklemmt sein.
- Standbilder in Überwachungsmonitoren können sich einbrennen.
- Brandschutztüren werden oft unzulässigerweise durch Holzkeile aufgehalten.
- Es kommt vor, dass Rauchmelder in Nichtraucherzonen manipuliert werden.

# G 4.4 Leitungsbeeinträchtigung durch Umfeldfaktoren

Die Übertragungseigenschaften von Kabeln mit elektrischer Signalübertragung können durch elektrische und magnetische Felder negativ beeinflusst werden. Ob dies zu einer tatsächlichen Störung der Signalübertragung führt, hängt im wesentlichen von folgenden Faktoren ab:

- Frequenzbereich, Stärke und Dauer der Einwirkung,
- Abschirmung des Kabels und
- Schutzmaßnahmen bei der Datenübertragung (Redundanz, Fehlerkorrektur).

Viele Beeinträchtigungen lassen sich im Vorfeld erkennen:

- Entlang von Starkstromtrassen und im Bereich großer Motoren entstehen starke induktive Felder (Eisenbahn, Produktionsbetrieb, Aufzug).
- Im Bereich von Sendeeinrichtungen existieren starke elektromagnetische Felder (Rundfunk, Polizei- bzw. Feuerwehrfunk, Betriebsfunk, Personensuchanlagen, Funknetze).
- Mobiltelefone überschreiten durch ihre Sendeleistung in bestimmten Fällen die Störempfindlichkeit von IT-Systemen.
- Kabel beeinflussen sich gegenseitig durch wechselseitige Induktion.

Unabhängig von den rein elektrischen oder magnetischen Einflüssen können weitere Umfeldfaktoren auf ein Kabel wirken:

- hohe Temperaturen (beispielsweise in industriellen Fertigungsbereichen),
- aggressive Gase und
- hohe mechanische Belastungen (z. B. bei provisorischer Verlegung auf dem Fußboden oder bei Leitungen zu beweglichen Geräten).

# G 4.5 Übersprechen

Übersprechen ist eine spezielle Form der Leitungsbeeinträchtigung. Dabei wird die Störung nicht allgemein im Umfeld, sondern durch Ströme und Spannungen von Signalen erzeugt, die auf eine benachbarte Leitung übertragen werden. Die Stärke dieses Effektes ist vom Kabelaufbau (Abschirmung, Kabelkapazität, Isolationsgüte) und von den elektrischen Parametern bei der Informationsübertragung (Strom, Spannung, Frequenz) abhängig.

Nicht jede Leitung, die durch Übersprechen beeinflusst wird, muss ihrerseits auch andere beeinflussen. Das Prüfen eigener Leitungen auf eingekoppelte Fremdsignale gibt keine Auskunft darüber, ob die eigenen Signale auf andere Leitungen übersprechen und somit dort abhörbar sind.

Der wesentliche Unterschied zu anderen Leitungsstörungen ist der, dass neben der Störung der Signalübertragung auf benachbarten Leitungen durch Übersprechen eventuell auswertbare Informationen auf fremden Leitungen zur Verfügung stehen können.

# G 4.6 Spannungsschwankungen/ Überspannung/Unterspannung

Durch Schwankungen der Versorgungsspannung kann es zu Funktionsstörungen und Beschädigungen der IT kommen. Die Schwankungen reichen von extrem kurzen und kleinen Ereignissen, die sich kaum oder gar nicht auf die IT auswirken, bis zu Totalausfällen oder zerstörerischen Überspannungen. Die Ursache dafür kann in allen Bereichen des Stromversorgungsnetzes entstehen, vom Netz des Energieversorgungsunternehmens bis zum Stromkreis, an dem die jeweiligen Geräte angeschlossen sind.

Außerhalb des Energieversorgungsnetzes ist auch auf allen anderen elektrisch leitenden Netzen (wie Telefonanbindung, Gebäudeleittechnik, Wasser- oder Gasleitungen etc.) mit Einkopplungen von Überspannungen zu rechnen.

# G 4.7 Defekte Datenträger

Beschädigungen, Fehler oder Ausfälle können bei allen Arten von Datenträgern auftreten. Zum Problem werden sie dann, wenn die auf den Datenträgern gespeicherten Informationen an keiner anderen Stelle gespeichert sind und sich nicht schnell und einfach rekonstruieren lassen. Dabei kommen Totalverluste bei der Beschädigung von analogen Datenträgern seltener vor als bei digitalen. Menschen sind anders als Computer in der Lage, selbst aus halbverbrannten oder zerrissenen Papierdokumenten Informationen ohne aufwändige Hilfsmittel auszulesen.

Leider ist der Ausfall bzw. der Defekt einzelner digitaler Datenträger durch technische Mängel oder Beschädigung kein Einzelfall. Betroffen sind Massenspeicher wie Festplatten, Bänder oder Kassettensysteme. Festplatten können durch den "Headcrash" des Schreib-/Lesekopfes, Bänder oder Kassetten durch direkte mechanische Einwirkung zerstört werden. CD-ROMs oder DVDs können durch Verkratzen der Oberfläche unbrauchbar werden.

**Beispiele:**

- In einem mittelständischen Unternehmen kam es aufgrund von Bauarbeiten zu einer starken Staubentwicklung. Dadurch gelangten Staubpartikel sogar in den Rechnerraum und dort in die Festplatte eines Servers. Als Folge kam es zu einem "Headcrash" und zur Zerstörung von Daten.
- Beim Laptop eines Außendienstmitarbeiters kam es zu unerklärlichen Ausfallerscheinungen, obwohl der Laptop immer sorgfältig verpackt transportiert wurde. Es stellte sich heraus, dass die Festplatte des Laptops durch einen Magneten beschädigt worden war, der zur Befestigung eines Klapptisches im Zug diente.
- Während der Datensicherung eines Multimedia-PCs wurden ZIP-Disketten auf dessen Lautsprecher zwischengestapelt. Durch die Magnete in den Lautsprechern wurden Teile der Datenträger gelöscht.
- Aufgrund von Bit-Fehlern auf Archivdatenträgern konnten verschlüsselte Dokumente nicht mehr entschlüsselt werden. Ebenso konnten elektronische Signaturen nicht mehr verifiziert werden.

# G 4.8 Bekanntwerden von Softwareschwachstellen

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 4.9 Ausfall der internen Stromversorgung

Der Einsatz eines mobilen IT-Systems, z. B. eines Laptops, setzt voraus, dass das System über eine vom Versorgungsnetz unabhängige Stromversorgung verfügt. Diese meist mit wiederaufladbaren Batterien konzipierte Stromversorgung reicht üblicherweise für eine mehrstündige Betriebsdauer. Nach dieser Zeit ist die ausreichende Stromversorgung nicht mehr gesichert, so dass das IT-System außer Betrieb genommen bzw. an das Stromnetz angeschlossen werden muss. Die überwiegende Zahl der mobilen Systeme überprüft kontinuierlich die Versorgungsspannung und zeigt einen kritischen Spannungsabfall an. Wird diese Anzeige ignoriert, kann es passieren, dass das System plötzlich seinen Dienst versagt und die letzten Arbeitsergebnisse im Hauptspeicher verloren gehen.

# G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen

Im Gegensatz zu Stand-alone-Systemen, bei denen im Wesentlichen der Login-Prozess für die Zugangskontrolle verantwortlich ist und die somit nur durch schlechte oder fehlende Passwörter korrumpiert werden können, gibt es auf Netzrechnern sehr viele komplexe Prozesse, die die verschiedensten Arten von Zugängen erlauben. So ermöglicht zum Beispiel unter Unix der *sendmail*-Daemon das Einbringen von Texten (E-Mails) in den Netzrechner, der FTP-Daemon einen, wenn auch etwas eingeschränkten Login, der unter Umständen (*anonymous FTP*) nicht einmal durch ein Passwort geschützt ist, der TELNET-Daemon einen kompletten Login.

Moderne Server-Systeme vermeiden aus Sicherheitsgründen die Übertragung von Klartext-Passwörtern. Dieser Schutzmechanismus wird jedoch durch den Einsatz von Diensten wie FTP oder Telnet unterlaufen, da hier wieder Klartext-Passwörter Verwendung finden.

Abgesehen davon, dass alle diese Prozesse durch eine falsche oder fehlerhafte Konfiguration eine Sicherheitslücke darstellen können, ist aufgrund ihres Umfangs natürlich auch die Wahrscheinlichkeit, dass in einem dieser Prozesse ein sicherheitsrelevanter Programmierfehler ist, wesentlich größer.

Es gibt zahlreiche verschiedene Möglichkeiten, ein z/OS-System an interne und öffentliche Netze anzubinden. Es sind Zugriffe über SNA und TCP/IP, zum Beispiel FTP, Telnet oder Browser, möglich. Viele der von Unix-Installationen bekannten Netzfunktionen können unter den *Unix System Services* von z/OS verwendet werden. Diese Vielfalt der Anschlussmöglichkeiten macht eine sichere Netzkonfiguration der z/OS-Systeme sehr komplex.

Auch Cloud Services bieten häufig eine Vielzahl unterschiedlicher Zugriffswege (beispielsweise Zugriff über einen Browser oder über dedizierte Tools) und unterschiedlicher Authentisierungsmöglichkeiten (zum Beispiel Single Login oder Federation Services). Die Zugriffswege und Funktionen sind für den Anwender häufig nicht transparent und bergen die Gefahr, unentdeckte Schwachstellen zu enthalten.

**Beispiel:**

- Einem externen Angreifer gelang es, die Benutzerkennung und das Passwort für eine hoch autorisierte Anwendung unter z/OS zu ermitteln. Obwohl die Kennung über kein *TSO-Segment* verfügte, konnte der Angreifer einen Batch-Job über FTP direkt in das *JES2* einbringen und ausführen lassen. Da der Job-Output ebenfalls über FTP ausgelesen werden konnte, war dadurch der Zugriff auf vertrauliche Daten möglich.
- Der Client, der für die Nutzung eines Cloud Services benötigt wird, verwendet ein Authentisierungstoken, das vom Cloud Service für unterschiedliche Clients bereitgestellt wird. Eine neue Anwendung erhält aufgrund eines Fehlers in der Konfiguration die Berechtigung, dieses Token ebenfalls zu nutzen. Somit kann mithilfe der Anwendung unberechtigt auf den Cloud Service zugegriffen werden.

# G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client

Kennt man den NIS-Domain-Namen, lässt sich jeder Rechner als Client anmelden, und es lassen sich alle NIS-Maps, insbesondere also auch die *passwd*-Map, abrufen.

Ist es möglich, Administrationsrechte auf einem Rechner zu bekommen, lässt sich auf diesem ein NIS-Server-Prozess (*ypserv*) an einem privilegierten Port starten. Startet man nun den Client-Prozess *ypbind* auf dem zu infiltrierenden Rechner neu und sorgt dafür, dass der eigene Server-Prozess vor dem korrekten NIS-Server antwortet, lässt sich jede beliebige Information an den Client überspielen.

# G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client

Für das X-Window-System gilt im besonderen Maße, dass es ohne geeignete Sicherheitsmechanismen, wie z. B. "Magic Cookies" oder Verwendung von Secure Shell, nur in einer vertrauenswürdigen Umgebung eingesetzt werden sollte. Ohne Sicherheitsfunktionen besteht für alle beteiligten Benutzer die Möglichkeit, sowohl den X-Client als auch den X-Server zu korrumpieren. Der X-Server-Prozess, der auf einem Rechner für die Ein- und Ausgabe zuständig ist, kann nicht erkennen, wem der X-Client-Prozess gehört, der mit ihm kommuniziert. Alle X-Clients können also auf alle Daten, die auf einem X-Server eingegeben werden, zugreifen, und der X-Server hat keine Möglichkeit festzustellen, von welchem X-Client er Daten erhält. So simuliert z. B. das Programm *meltdown* das optische "Schmelzen" des Bildschirms eines beliebigen X-Servers. Genauso ist es möglich, Daten von einem *xterm*-Client zu lesen oder ihm eigene Daten zu schicken, also z. B. Bildschirmabzüge von einem anderen, mit X-Window arbeitenden Rechner zu machen.

**Beispiele:**

- Mit dem Tool *xspy* lassen sich automatisiert Tastatureingaben auf einem Xterm remote protokollieren.
- Fenster, die von einem Angreifer auf einem X-Server dargestellt werden, sind optisch nicht von denen des eigentlich gewünschten X-Clients zu unterscheiden. Ein Angreifer kann auf diese Weise falsche Informationen einschleusen oder mit Hilfe von gefälschten Fenstern die Eingabe von sensitiven Informationen provozieren.

# G 4.13 Verlust gespeicherter Daten

Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben. Sind die Anwendungsdaten oder die Kundenstammdaten verloren oder verfälscht, so können privatwirtschaftliche Betriebe in ihrer Existenz bedroht sein. Der Verlust oder die Verfälschung wichtiger Dateien kann in Behörden Verwaltungs- und Fachaufgaben verzögern oder sogar ausschließen.

Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf Geschäftsprozesse und damit auf die gesamte Institution haben. Wenn geschäftsrelevante Informationen, egal welcher Art, zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar deren Ausführung verhindert werden. Insgesamt kann der Verlust gespeicherter Daten, neben dem Produktionsausfall und den Kosten für die Wiederbeschaffung der Daten, vor allem zu langfristigen Konsequenzen, wie Vertrauenseinbußen bei Kunden und Partnern sowie einem negativen Eindruck in der Öffentlichkeit, führen. Von den durch Datenverluste verursachten direkten und indirekten Schäden können Institutionen sogar in ihrer Existenz bedroht sein.

Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein:

- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- vorsätzliches oder versehentliches Setzen von Löschmarkierungen in Archivsystemen (siehe auch G 5.106 *Unberechtigtes Überschreiben oder Löschen von Archivmedien*),
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust) und
- Datenzerstörung durch Schadprogramme.

# G 4.14 Verblassen spezieller Faxpapiere

Bei Faxgeräten, die im Thermodruckverfahren arbeiten, muss Spezialpapier eingesetzt werden, auf dem oft bereits nach relativ kurzer Zeit die Schrift bis zur Unlesbarkeit verblasst oder durch Schwärzung des Papieres unlesbar wird. Außerdem können sich diese Papiere bei Kontakt mit Textmarkern oder Klebstoffen so verfärben, dass der Text nicht mehr lesbar ist.

# G 4.15 Fehlerhafte Faxübertragung

Beim Faxversand können Störungen auf dem Übertragungsweg oder an den beteiligten Geräten auftreten. Dadurch können Faxsendungen unvollständig, unlesbar oder gar nicht beim Empfänger ankommen. Entscheidungen, die von diesen Informationen abhängig sind, können fehlerhaft sein und somit Schäden verursachen.

Weiterhin besteht die Gefahr, dass ein Fax an einen falschen Empfänger übermittelt wird. Ursache kann eine Fehlschaltung im öffentlichen Telekommunikationsnetz sein. Ebenso ist denkbar, dass bei herkömmlichen Faxgeräten Rufnummern falsch gewählt oder Zielwahltasten falsch programmiert werden. Bei der Verwendung von Faxservern kann eine Empfänger-Rufnummer falsch eingegeben oder im Adressbuch falsch abgespeichert werden. Dadurch können unter Umständen vertrauliche Informationen unbefugten Personen bekannt werden. Der mögliche Schaden ist von der Vertraulichkeit der Informationen abhängig. Darüber hinaus wird der Absender im Glauben bleiben, dass das Fax ordnungsgemäß an den gewünschten Adressaten übermittelt wurde. Hierdurch auftretende Zeitverzögerungen können zu Schäden führen.

**Beispiel:**

Eine bekannte deutsche Firma verlor einen Großauftrag, weil das Angebot versehentlich an einen falschen Empfänger versandt wurde.

# G 4.16 Übertragungsfehler bei Faxversand

Die Gefährdung G 4.16 *Übertragungsfehler bei Faxversand* wurde in die Gefährdung G 4.15 *Fehlerhafte Faxübertragung* integriert.

# G 4.17 Technischer Defekt des Faxgerätes

Die Gefährdung G 4.17 *Technischer Defekt des Faxgerätes* wurde in die Gefährdung G 4.15 *Fehlerhafte Faxübertragung* integriert.

# G 4.18 Entladene oder überalterte Notstromversorgung im Anrufbeantworter

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 4.19 Informationsverlust bei erschöpftem Speichermedium

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 4.20 Überlastung von Informationssystemen

Wenn Informations- oder Kommunikationssysteme wie Hardware, Software oder Netze nicht ausreichend dimensioniert sind, ist irgendwann der Punkt erreicht, wo sie den Anforderungen der Benutzer nicht mehr gerecht werden. Je nach Art der betroffenen Systeme kann dies eine Vielzahl von negativen Auswirkungen haben.

Auslöser für die Überlastung von Informationssystemen können sein, dass

- vorhandene Speicherplatzkapazitäten überschritten werden, beispielsweise wenn die Mailbox bei längerer Abwesenheit des Inhabers überläuft,
- zahlreiche Anfragen zur gleichen Zeit ein System überbeanspruchen und dadurch die Prozessoren überlastet werden,
- zu viel Rechenleistung von den Anwendungen beansprucht wird, z. B. wenn die Prozessleistung nicht für intensive Grafikanwendungen ausreicht,
- eine große Anzahl Nachrichten als Newsletter zur gleichen Zeit versendet werden.

Mögliche Konsequenzen können beispielsweise sein, dass IT-Systeme oder Dienste vorübergehend nicht verfügbar sind oder dass es zu Datenverlusten kommt.

Jedes Speichermedium kann nur begrenzt viele Daten aufnehmen. Wenn diese Grenze erreicht ist, kann das zu Datenverlusten führen, aber auch dazu, dass Dienste nicht mehr verfügbar sind, wie z. B. dass

- Benutzer keine Daten mehr abspeichern können,
- eingehende E-Mails abgewiesen werden und eventuell außerdem keine E-Mails mehr versandt werden können,
- eingehende und gegebenenfalls ausgehende Faxsendungen abgewiesen werden,
- keine Protokollierung mehr möglich ist bzw. noch nicht ausgewertete Protokolldaten überschrieben werden oder
- Dokumente nicht mehr elektronisch archiviert werden können.

Die Kapazität des Speichermediums kann aus verschiedenen Gründen plötzlich erschöpft sein, z. B. durch Fehler in Anwendungsprogrammen, erhöhten Speicherbedarf der Benutzer oder auch durch einen gezielten Angriff, bei dem vorsätzlich der vorhandene Speicherplatz reduziert wird, um eine Protokollierung zu verhindern.

Bei der elektronischen Archivierung sind meist große Datenmengen zu sichern. Die Datenmengen entstehen einerseits durch die große Anzahl von Dokumenten, die bei bestimmten Vorgängen zu archivieren sind. Hinzu kommt andererseits, dass jede neu erstellte Version eines Dokuments unter Vergabe einer neuen Versionsnummer neu gespeichert wird.

Ressourcen können auch absichtlich überlastet werden, wenn jemand einen intensiven Bedarf an einem Betriebsmittel vorsätzlich generiert und dadurch eine intensive und dauerhafte Störung des Betriebsmittels provoziert, siehe auch G 5.28 *Verhinderung von Diensten*.

# G 4.21 Ausgleichsströme auf Schirmungen

Werden IT-Geräte, die über ein TN-C-Netz elektrisch versorgt werden, durch Datenleitungen mit beidseitig aufgelegtem Schirm miteinander verbunden, kann es zu Ausgleichsströmen auf dem Schirm kommen (eine erläuternde Zeichnung enthält M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen*).

Ursache dafür ist die Eigenart des TN-C-Netzes, dass bei ihm Schutz- (PE-) und Neutral- (N-) Leiter bis zu den einzelnen Verteilungen gemeinsam als PEN-Leiter geführt werden. Erst in der Verteilung erfolgt die Aufteilung in N-Leiter und PE-Leiter. Diese Installation ist gemäß VDE 0100 "Bestimmungen für das Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V" zulässig!

Werden die mit PE verbundenen Schnittstellen-Schirmungen von Geräten, die an verschiedenen Verteilungen angeschlossen sind, durch geschirmte Datenleitungen miteinander verbunden, kommt es zu einer Parallelschaltung des PEN-Leiters zwischen den Verteilungen und der Schirmung zwischen den Schnittstellen. Der dadurch über die Schirmung fließende Ausgleichsstrom kann zu Schäden an den Schnittstellen und zu Personengefährdungen bei Arbeiten an den Datenleitungen führen.

Zwischen Geräten, die in einem TN-C-Netz an der gleichen Verteilung oder zwischen Geräten, die in einem TN-S-Netz - auch an verschiedenen Verteilungen - angeschlossen sind, fließen keine Ausgleichsströme über die Schirmung von Datenleitungen.

Bei TN-CS-Netzen sind einige Teilbereiche als TN-C-Netz, andere als TN-S-Netz ausgeführt. Solange Datenleitungen mit beidseitig aufgelegtem Schirm nur jeweils innerhalb gleichartiger Teilbereiche geführt werden, gelten dort die gleichen Verhältnisse wie in den jeweiligen Netzen. Werden jedoch IT-Geräte aus unterschiedlichen Bereichen über Datenleitungen mit beidseitig aufgelegter Schirmung verbunden, können auch im TN-S-Bereich Ausgleichsströme fließen!

# G 4.22 Software-Schwachstellen oder -Fehler

Für jede Art von Software gilt: je komplexer sie ist, desto häufiger treten Programmier- oder Designfehler auf. Unter Software-Schwachstellen sollen unbeabsichtigte Programmfehler verstanden werden, die dem Anwender nicht oder noch nicht bekannt sind und ein Sicherheitsrisiko für das IT-System darstellen. Es werden ständig neue Sicherheitslücken in vorhandener, auch in weitverbreiteter oder ganz neuer Software gefunden.

Zu Fehlern oder Schwachstellen in Software kann es durch eine Vielzahl von Gründen kommen. Dazu gehören beispielsweise Kommunikationsfehler zwischen Kunden und Entwicklern, unzureichende Ausbildung der Programmierer oder ungenügende Tests. Auch zu hohe Erwartungen der Anwender und zeitlich zu knapp bemessene Fertigstellungstermine können dazu führen, dass die Hersteller ihre Produkte teilweise unausgereift oder nicht fehlerfrei anbieten.

Werden Softwarefehler nicht erkannt, können die bei der Anwendung entstehenden Fehler zu weitreichenden Folgen führen. Bei weitverbreiteter Standardsoftware können Software-Schwachstellen schnell dazu führen, dass weltweit schwerwiegende Sicherheitsprobleme für alle Arten von Institutionen entstehen können.

**Beispiele:**

- Ein Software-Fehler in der Sicherheitssoftware RACF des z/OS-Betriebssystems kann bedeuten, dass nicht nur RACF den Dienst einstellt, sondern dadurch das ganze System nicht mehr funktionsfähig ist und neu gestartet werden muss.
- Die Stärke der in Standardsoftware implementierten Sicherheitsfunktionalitäten (wie Passwörter oder Verschlüsselungsalgorithmen) wird vom Anwender häufig zu hoch eingeschätzt. Häufig können diese Sicherheitsfunktionalitäten einem sachkundigen Angriff nicht dauerhaft standhalten. Dies gilt z. B. für die Verschlüsselungsfunktionen, die in vielen Textverarbeitungsprogrammen integriert sind. Für fast alle davon gibt es im Internet zahlreiche Tools, um diese Verschlüsselung zu überwinden.
- Nachweislich führte das Auftreten eines bestimmten Wortes in der Rechtschreibprüfung eines Textverarbeitungsprogrammes immer zu dessen Absturz.
- Vielfach enthält Standardsoftware nicht dokumentierte Funktionen, wie sog. "Ostereier" oder "Gagscreens", mit denen sich die Entwickler des Produktes verewigt haben. Zum einen werden hierdurch zusätzliche IT-Ressourcen verbraucht, zum anderen wird dadurch auch deutlich, dass im Softwaretest die gesamte Funktionalität des Produktes nicht bis ins Letzte geklärt werden kann.
- Die meisten Warnmeldungen der Computer Emergency Response Teams in den letzten Jahren bezogen sich auf sicherheitsrelevante Programmierfehler. Dies sind Fehler, die bei der Erstellung von Software entstehen und dazu führen, dass diese Software von Angreifern missbraucht werden kann. Der größte Teil dieser Fehler wurde durch Speicherüberläufe (Buffer Overflow) hervorgerufen. Hierbei handelt es um Fehler, bei denen eine Routine zum Einlesen von Zeichen nicht prüft, ob die Länge der eingegebenen Zeichenkette mit der Länge des dafür vorgesehenen Speicherbereiches übereinstimmt. Dadurch ist es Angreifern möglich, eine überlange Zeichenfolge zu übertragen, so dass hinter dem für die Eingabe reservierten Speicherbereich zusätzliche Befehle gespeichert werden können, die

zur Ausführung gebracht werden. Diese Befehle können zum Beispiel beliebige Programme sein.

- Eine weitere große Anzahl von Warnmeldungen wurde durch Verfügbarkeitsangriffe (Denial of Service, DoS ) verursacht, bei denen durch Fehler in einzelnen Routinen, die für die Netzdatenverarbeitung eingesetzt werden, der gesamte Rechner zum Absturz gebracht werden kann.
- Die unzureichende Absicherung der Registrierung zur Nutzung eines Cloud Services führt dazu, dass ein Benutzer den Service in der Folge unter einem falschen Namen missbrauchen kann. Der Benutzer registriert sich dabei beim Cloud Service im Namen eines anderen Cloud-Service-Benutzers. Bei der Registrierung wird auf eine ausreichende Absicherung, beispielsweise mithilfe eines Aktivierungs-Links unter der angegebenen E-Mail-Adresse, verzichtet.

# G 4.23 Automatische Erkennung von Wechseldatenträgern

Bei vielen Betriebssystemen wie z. B. Windows können CD-ROMs, DVD-ROMs, aber auch andere auswechselbare Datenträger automatisch erkannt und Applikationen hierauf ausgeführt werden. Oft wird z. B. direkt ein Film abgespielt, wenn eine Video-DVD eingelegt wird. Ein Wechseldatenträger könnte so manipuliert werden, dass Schadsoftware ausgeführt und installiert wird, wenn der Wechseldatenträger eingelegt oder angeschlossen wird.

**Automatische Erkennung unter Windows**

Die unter Windows so genannte Autorun-Funktion erkennt automatisch, wenn ein Datenträger eingebunden wird und versucht auf dem Datenträger gespeicherte Programme aufzurufen. Medien mit Filmen oder Musik werden unter Windows oft mit der so genannten Autoplay-Funktion automatisch abgespielt.

Windows-Betriebssysteme werten hierzu die Inhalte der Datei *AUTORUN.INF* im Wurzelverzeichnis des Datenträgers aus, denn diese enthält die Informationen, die zum Start der Programme notwendig sind. Diese Datei kann beliebige auf der CD-, beziehungsweise DVD-ROM, gespeicherte Programme (z. B. mit Schadfunktion) automatisch ausführen.

Der mittlerweile unter Windows übliche Autorun-Dialog, bei dem der Benutzer die Möglichkeit hat, auszuwählen, in welcher Art und Weise Inhalte auf den Wechseldatenträgern gestartet werden sollen, bietet hier keinen Schutz, da moderne Schadprogramme bis dahin die zur Infizierung notwendigen Aktionen bereits durchgeführt haben.

**Automatische Erkennung unter anderen Betriebssystemen**

Auch unter Unix-Betriebssystemen, wie Linux oder Mac OS X, gibt es Funktionen, um Wechseldatenträger automatisch zu mounten und auf dem Datenträger abgelegte Skripte oder Anwendungen zu starten. Je nach Betriebssystem-Umgebung können z. B. die um zusätzliche Parameter ergänzten Inhalte und aus Windows bekannte *AUTORUN.INF*-Datei ausgeführt werden.

**Beispiel:**

- Der Computerwurm Conficker nutzt unter anderem gezielt die Autostart-Funktion von Windows aus, um sich von USB-Medien weiter zu verbreiten. Alle Aktionen laufen für den Benutzer nicht sichtbar im Hintergrund und er hat keine Möglichkeit, dies bei aktivierter Autostart-Funktion zu umgehen. Selbst der Abbruch der Autostart-Funktion und des Autostart-Dialogs bietet keinen Schutz.

# G 4.24 Dateinamenkonvertierung bei Datensicherungen unter Windows 95

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen.

# G 4.25 Nicht getrennte Verbindungen

Bei der Verwendung von ISDN-Kommunikationskarten kann es vorkommen, dass eine über die Kommunikationssoftware ausgelöste Verbindung nicht tatsächlich durch die ISDN-Karte getrennt wird. Besteht der Verdacht eines solchen Defekts, lässt sich dieser durch einen Anrufversuch bei der betreffenden ISDN-Rufnummer leicht verifizieren.

**Beispiel:**

Ein Netzadministrator hat vor seinem 14-tägigen Urlaub eine ISDN-Datenverbindung zu seinem Internet-Provider aufgebaut. Bei Beendigung der Sitzung wurde die ISDN-Verbindung nicht korrekt ausgelöst. Nach Beendigung des Urlaubs wunderte sich der Administrator über die recht hohe Rechnung für Verbindungsentgelte von Seiten des ISDN-Carriers.

# G 4.26 Ausfall einer Datenbank

Der Ausfall einer Datenbank zeigt sich dem Benutzer zumeist durch fehlende Reaktion des Datenbankmanagementsystems (DBMS), welches die Daten der Datenbank darstellen soll. Der Ausfall kann durch geplante Ereignisse, wie z. B. Wartungsarbeiten, ausgelöst worden sein oder auf unvorhersehbare Ereignisse zurückgeführt werden. Zum letzteren Bereich gehören z. B. Hardware-, Software- oder Netzprobleme. Produktfehler, höhere Gewalt, Fahrlässigkeit oder Sabotage können beispielsweise Ursachen für solche Datenbankausfälle sein.

Steht eine Datenbank für einen Benutzer oder eine Anwendung nicht mehr zur Verfügung, kann dies je nach Einsatzzweck und Bedeutung der Datenbank weitreichende Folgen haben. Sämtliche Anwendungen, die auf die Daten der Datenbank angewiesen sind, können nur noch eingeschränkt oder gar nicht mehr benutzt werden. Die Benutzer solcher Anwendungen können ihre Aufgaben nur noch teilweise oder gar nicht mehr wahrnehmen, falls sie diese nicht mit anderen Mitteln erfüllen können. Je nach Art der Aufgaben, die nur mittels IT-Unterstützung unter Benutzung der Datenbank ausgeführt werden können, sind unter anderem folgende Konsequenzen möglich:

- wirtschaftlicher Schaden,
- gesundheitlicher Schaden,
- Vertrauensverlust bei Kunden oder Partnern durch die Nichterbringung vereinbarter Leistungen oder
- eingeschränkte oder vollständige Handlungsunfähigkeit.

**Beispiele:**

- Elektronische Archive basieren auf einer Datenbank, in der alle archivierten Dokumente indiziert sind. Bei einem Ausfall dieser Index-Datenbank können archivierte Dokumente nicht wiedergefunden bzw. nicht gesucht werden. Dadurch ist, wenn überhaupt, nur ein stark eingeschränkter Betrieb des Archivs möglich.
- Die Inhalte sowie alle Zusatzinformationen einer regelmäßig erscheinenden Publikation wurden vollständig in eine Datenbank verlagert. Da für alle Arbeiten im zuständigen Referat zumindest ein lesender Zugriff auf diese Datenbank erforderlich ist, sind ohne das korrekte Funktionieren dieser Datenbank keine inhaltlichen Arbeiten mehr möglich. Nachdem die Datenbank aufgrund von planmäßigen Wartungsarbeiten heruntergefahren wurde, kam es im weiteren Verlauf zu unvorhergesehenen Verzögerungen, wodurch die Datenbank länger als geplant nicht zur Verfügung stand. Das Referat konnte, da keine Ersatzdatenbank existierte, insgesamt eine Woche inhaltlich nur sehr eingeschränkt arbeiten.
- Eine öffentlich zur Verfügung stehende Datenbank wird durch eine immense Menge zeitgleich eintreffender Anfragen so überlastet, dass ein geregelter Zugriff auf die Datenbank fast unmöglich wird.

# G 4.27 Unterlaufen von Zugriffskontrollen über ODBC

Datenbankschnittstellen stellen dem Benutzer eine Verbindung (Application Programming Interface, API) von Anwendungsprogrammen zu anderen Datenbanken in Form von Treibern zur Verfügung.

Beispiele für Datenbankschnittstellen sind:

- ODBC: Open Database Connectivity
- IDAPI: Integrated Database Application Programming Interface
- JDBC: Java Database Connectivity

Dabei werden die Anweisungen des Anwendungsprogramms durch die Datenbankschnittstelle in für die jeweilige Datenbank spezifische Befehle übersetzt, der Datenbank übermittelt und die Ergebnisse an das Anwendungsprogramm zurück übertragen.

Bestandteil der Kommunikation über die Schnittstelle zwischen Anwendungsprogramm und Datenbank ist die Identifizierung der Anwendung als registrierter Datenbanknutzer.

Existierende Zugangs- oder Zugriffskontrollen einer Datenbank können unterlaufen werden, wenn auf die Datenbank über Datenbankschnittstellen zugegriffen wird und bei der Installation, Konfiguration oder Nutzung der zugehörigen Treiber Fehler gemacht wurden. In diesem Fall kann ein Schutz vertraulicher Daten nicht gewährleistet werden und die Manipulation von Daten ist möglich.

**Beispiel:**

Eine ODBC-Datenquelle kann in Microsoft Excel oder Word genutzt werden, um Informationen aus einer Datenbank in ein Dokument einzubinden. Um auch später wieder einfach auf diese Informationen zugreifen zu können, ist es möglich, zu der Abfrage auch den Benutzernamen und das Passwort zu speichern. Benutzername und Passwort werden dabei im Klartext in der Datei gespeichert. Wird das betroffene Excel- oder Word-Dokument nun an einen Dritten weitergegeben, kann dieser mit einem Editor den Benutzernamen und das Passwort lesen und so möglicherweise Zugriff auf die Datenbank erhalten.

# G 4.28 Verlust von Daten einer Datenbank

Ein Verlust von Daten einer Datenbank kann auf vielfältige Art und Weise verursacht werden. Dies kann sich von ungewollten Datenmanipulationen (z. B. durch das versehentliche Löschen von Daten) über einen Verlust durch einen Zusammenbruch der Datenbank, z. B. als Ergebnis der Erschöpfung eines Speichermediums, bis hin zu gezielten Angriffen erstrecken.

Jedes Speichermedium kann nur begrenzt viele Daten aufnehmen. Dies gilt auch für eine Datenbank, die für die dauerhafte Speicherung ihrer Daten auf ein physikalisches Speichermedium zurückgreifen muss. Ist dieses erschöpft, kann es zu einem Zusammenbruch der Datenbank und einem Verlust von Daten kommen.

Die Kapazität des Speichermediums kann aus verschiedenen Gründen erschöpft sein. Beispiele hierfür sind Fehler in Anwendungsprogrammen, erhöhter Speicherbedarf der Benutzer oder auch gezielte Angriffe, bei denen vorsätzlich der vorhandene Speicherplatz reduziert wird, um z. B. eine Protokollierung zu verhindern.

Unabhängig von der Ursache ist als Folge die Verfügbarkeit und die Vollständigkeit der Daten nicht mehr gewährleistet, und es kann zu folgenden Konsequenzen kommen:

- Bestimmte Anwendungen, die auf die Daten der Datenbank angewiesen sind, können gegebenenfalls nicht oder nicht mehr in vollem Umfang ausgeführt werden.
- Der Informationsgehalt der Daten in ihrer Gesamtheit geht verloren.
- Es entsteht ein hoher Aufwand, um zerstörte Daten wiederzubeschaffen.

Je nach Ursache des Datenverlustes kann es schwer bis unmöglich sein festzustellen, welche Daten nicht mehr vorhanden sind. Dies kann weitere wirtschaftliche Schäden oder Sicherheitsrisiken nach sich ziehen.

**Beispiel:**

Bei Änderungen des Datenmodells müssen im Rahmen eines Migrationskonzeptes unter anderem zunächst die alten Tabellen und Strukturen gesichert werden und können erst danach gelöscht werden. Anschließend werden die neuen Tabellen angelegt. Danach müssen die alten Datenbestände konvertiert und in die geänderten Tabellen eingespielt werden. Durch Fehler bei diesen Abläufen kann es schnell passieren, dass Daten verloren gehen oder sich nicht mehr einspielen lassen.

# G 4.29 Datenverlust einer Datenbank bei erschöpftem Speichermedium

Diese Gefährdung ist mit der Version 2006 entfallen. Alle relevanten Inhalte werden G 4.28 *Verlust von Daten einer Datenbank* integriert.

# G 4.30 Verlust der Datenbankintegrität/-konsistenz

Ein Verlust der Datenbankintegrität/-konsistenz bedeutet, dass die Daten in der Datenbank zwar noch vorhanden sind, sich aber in einem fehlerhaften Zustand befinden. Dadurch kann auf die Daten nicht mehr korrekt zugegriffen werden oder die Daten können im Weiteren nicht mehr korrekt verarbeitet werden. Eine Datenbankinkonsistenz kann auf vielfältige Art und Weise verursacht werden, von ungewollten Datenmanipulationen (z. B. durch das unbeabsichtigte Ändern von Daten) über eine fehlerhafte Synchronisationskontrolle der Transaktionen bis hin zu gezielten Angriffen.

Dadurch kann es unter anderem zu folgenden Konsequenzen kommen:

- Bestimmte Aufgaben, die auf die korrekten Daten der Datenbank angewiesen sind, können nicht oder nicht mehr in vollem Umfang durchgeführt werden.
- Der Informationsgehalt der Daten in ihrer Gesamtheit wird verfälscht.
- Es entsteht ein hoher Aufwand, um Datenintegrität und Datenkonsistenz der Datenbank wiederherzustellen.

Je nach Ursache der Verletzung der Datenbankintegrität/-konsistenz kann es schwer bis unmöglich sein festzustellen, welche Daten verändert wurden (siehe auch G 2.22 *Fehlende oder unzureichende Auswertung von Protokolldaten*). Dies kann weitere wirtschaftliche Schäden oder Sicherheitsrisiken nach sich ziehen.

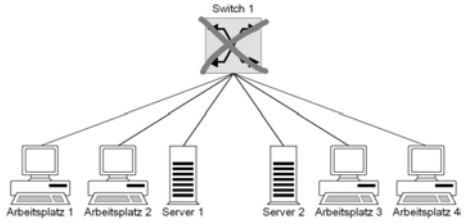
**Beispiele:**

- Aus Platzmangel und Zeitdruck wurde auf einem Unix-Server eine Datei einer Datenbank im */tmp*-Dateisystem angelegt. Dieses Dateisystem wurde über Nacht automatisch gelöscht, so dass daraufhin die gesamte Datenbank nicht mehr nutzbar war.
- Elektronische Archive basieren auf einer Datenbank, in der alle archivierten Dokumente indiziert sind. Bei Verlust der Indizierung oder der Referenz auf einzelne Dokumente können diese unter Umständen nicht mehr mit vertretbarem Aufwand gefunden werden. Aus einem solchen Verlust der Datenbankintegrität kann zu einem späteren Zeitpunkt ein erheblicher wirtschaftlicher oder juristischer Schaden entstehen.

# G 4.31 Ausfall oder Störung von Netzkomponenten

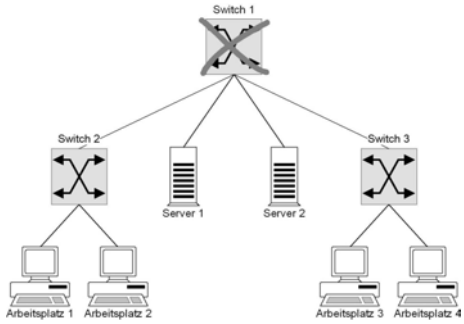
Durch einen Ausfall oder eine Störung von aktiven Netzkomponenten kann es zu einem Verlust der Verfügbarkeit des Netzes oder von Teilbereichen davon kommen. Hier sind prinzipiell folgende Varianten denkbar:

- Totalausfall einer aktiven Netzkomponente
  Der Totalausfall einer aktiven Netzkomponente kann dazu führen, dass alle direkt angeschlossenen IT-Systeme (Clients, Server etc.) nicht mehr mieinander kommunizieren können.
  **Beispiel**: Fällt, wie in der folgenden Abbildung dargestellt, der zentrale Switch 1 völlig aus, ist keinerlei Kommunikation zwischen den angeschlossenen Endgeräten mehr möglich.




Ausfall eines zentralen Switchs

- Es handelt sich um aktive Netzkomponenten, die zwar nicht direkt an den Netzsegmenten von miteinander kommunizierenden Arbeitsplatz- und Serversystemen angeschlossen sind, jedoch im Signalpfad zwischen Arbeitsplatz- und Serversystemen liegen. Falls keine redundanten Signalpfade zwischen den betreffenden Arbeitsplatz- und Serversystemen zur Verfügung stehen, kann bei Ausfall oder Störung einer oder mehrerer dieser Komponenten keine oder nur eingeschränkte Kommunikation zwischen Arbeitsplatz- und Serversystemen mehr stattfinden.
  **Beispiel:** Fällt, wie in der folgenden Abbildung dargestellt, Switch 1 völlig aus, ist zwar von den Arbeitsplätzen 1 und 2 eine lokale Kommunikation mit Server 1 möglich,. Zentrale Services, die beispielsweise auf Server 2 angeboten werden, sind jedoch für diese Arbeitsplätze nicht mehr erreichbar.




Ausfall eines Switchs

- Teilausfall einer aktiven Netzkomponente
  Fällt ein Port einer aktiven Netzkomponente aus oder wird dieses gestört, dann ist nur für das dort angeschlossene Endgerät das Netz nicht verfügbar.

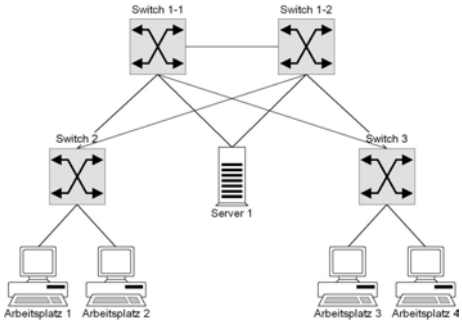



Abbildung: Ausfall eines redundanten Switchs

Auch der Ausfall einer passiven Netzkomponente kann den Verlust der Verfügbarkeit eines Netzes bedingen. Dies trifft beispielsweise für Kabel und Steckverbinder zu, die Segmente miteinander verbinden. Diese Gefährdung kann z. B. bei nicht sachgemäßer Installation der Kabel (z. B. Nichtbeachtung des maximalen Biegeradiuses), fehlerhafter Konfektion der Kabel mit Steckverbindern (insbesondere bei LWL) oder Störungen durch elektromagnetische Unverträglichkeit eintreten.

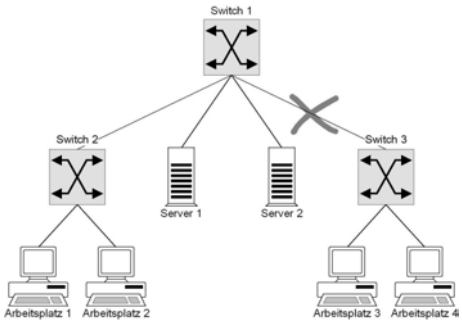



Abbildung: Ausfall einer Kommunikationsstrecke

# G 4.32 Nichtzustellung einer Nachricht

Der Datenaustausch über E-Mail ist schnell und komfortabel, aber nicht immer zuverlässig. Aufgrund von Hardware- oder Softwarefehlern bei den beteiligten IT-Systemen oder durch Störungen auf dem Übertragungsweg kommt es immer wieder zum Nachrichtenverlust. Die technischen Probleme können vielfältige Ursachen haben, z. B. können Leitungen beschädigt sein, Netzkopplungselemente ausfallen oder die Kommunikationssoftware falsch konfiguriert sein. E- Mails können auch verloren gehen, wenn die Empfängeradresse nicht korrekt angegeben ist. Dabei ist das größte Problem, dass die Benutzer häufig nicht informiert werden, wenn eine E-Mail nicht zugestellt werden konnte. Es kann also nicht darauf vertraut werden, dass eine Nachricht den Empfänger erreicht hat, sofern keine Probleme angezeigt werden.

Viele E-Mailprogramme bieten Optionen wie "Zustellung bestätigen" oder "Empfang bestätigen". Entsprechende Rückmeldungen sollten aber nicht überbewertet werden. Zum einen werden die Zustellbestätigungen häufig nicht durch die Ankunft einer E-Mail am Bildschirmarbeitsplatz des Empfängers ausgelöst, sondern durch die Ankunft bei einem Mailserver. Ob der Mailserver die E-Mail erfolgreich an den Adressaten weitergeleitet hat, wird dann nicht mehr mitgeteilt. Zum anderen erfolgt auch häufig keine Zustellbestätigung, obwohl die E-Mail korrekt übertragen wurde, wenn diese Option durch die Empfängerseite nicht unterstützt wird.

Das Problem, dass Nachrichten nicht zugestellt werden, tritt auch bei Kurznachrichten von Mobiltelefonen auf. Ist der Empfänger nicht erreichbar, weil er sich in einem Funkloch befindet oder sich ohne Roaming im Ausland aufhält, wird die Kurzmitteilung nicht zugestellt. Eine Zeit lang versucht der Dienst dann die SMS erneut zu senden. Sobald jedoch die vom Netzbetreiber voreingestellte Lebensdauer der Kurzmitteilung erreicht ist, wird sie sogar vollständig gelöscht und kann den Empfänger auch dann nicht mehr erreichen, wenn er wieder empfangsbereit ist.

# G 4.33 Schlechte oder fehlende Authentikationsverfahren und -mechanismen

Authentikationsverfahren und -mechanismen können zur Authentikation von Benutzern oder IT-Komponentenb oder zur Bestimmung des Datenursprungs eingesetzt werden. Wenn Authentikationsverfahren und -mechanismen fehlen oder zu schlecht sind, besteht die Gefahr, dass

- Unbefugte auf IT-Systeme oder Daten zugreifen können,
- die Verursacher von Problemen nicht identifiziert werden können oder
- die Herkunft von Daten nicht bestimmt werden kann.

Sicherheitslücken können beispielsweise entstehen

- bei der Benutzerauthentikation, wenn Benutzer Passwörter wählen, die einfach zu erraten sind, oder wenn sie die Passwörter nie wechseln,
- bei der Komponentenauthentikation, wenn nach Inbetriebnahme eines IT-Systems Default-Passwörter nicht durch individuell gewählte ersetzt werden, wenn die Passwörter, die bei vielen IT-¿Systemen fest eingegeben werden, nie wieder geändert werden oder wenn die Passwörter nicht sicher hinterlegt werden und sich nach einem Systemabsturz herausstellt, dass das jetzt dringend benötigte Passwort vergessen wurde,
- bei der Wahl der Verfahren, wenn diese völlig untauglich sind oder Sicherheitslücken bekannt werden, auf die im laufenden Betrieb aber nicht reagiert wird.

Authentikationsverfahren können beispielsweise unzureichend sein, wenn

- sie nicht zulassen, dass ausreichend lange Passwörter ausgewählt werden können,
- die Authentikationsdaten unverschlüsselt und ohne Zugriffsschutz auf Servern oder Clients gespeichert werden,
- die Authentikationsdaten unverschlüsselt übertragen werden,
- sie keinen Schutz gegen das Wiedereinspielen von Nachrichten bieten und sich dadurch Angreifer unter Vortäuschen einer falschen Identität Zugang zu einem System verschaffen können (siehe auch G 5.24 *Wiedereinspielen von Nachrichten*),
- sie nicht ausreichend widerstandsfähig gegen sogenannte Man-in-the-Middle-Angriffe oder Session Hijacking sind (siehe G 5.89 *Hijacking von Netz-Verbindungen*). Hierbei hängt sich ein Angreifer in eine laufende Verbindung, beispielsweise indem er eine Anmeldenachricht vom Client blockiert und sie stattdessen benutzt, um sich unter fremdem Namen anzumelden.

**Beispiele:**

- Bei SNMP (Simple Network Management Protocol) unterstützten die ersten beiden Versionen, SNMPv1 und SNMPv2, nur einfache Authentikationsverfahren, bei denen Authentikationsparametern (sogenannte Community Strings) im Klartext übertragen wurden. Erst ab SNMPv3 wurden die Sicherheitsmechanismen verbessert. Dort, wo noch mit den alten Versionen gearbeitet wird, könnten Angreifer die Klartext-Authentikationsparameter abhören und sich damit unberechtigt anmelden.
- In dem WLAN-Standard IEEE 802.11 (Wireless LAN, Wi-Fi) wurde mit Wired Equivalent Privacy (WEP) zunächst ein Verfahren zur Authentikation spezifiziert, das viele Angriffsmöglichkeiten bot. Mit WPA (Wi-Fi Protected Access) bzw. WPA2 (Wi-Fi Protected Access 2) wurden diese Schwächen

beseitigt. Es finden sich aber immer noch WLAN-Netze, die mit WEP arbeiten und daher unzureichend gegen unbefugten Zugriff geschützt sind.

- Im Standard IEEE 802.1X Port Based Network Access Control ist das EAP (Extensible Authentication Protocol) definiert. In einigen der beschriebenen EAP-Methoden sind Schwachstellen enthalten, z. B. sollte CHAP bei EAD-MD5 nicht als Authentikationsmethode eingesetzt werden, da es auf der Kenntnis eines unverschlüsselten Passwortes sowohl bei Sender wie auch Empfänger basiert.

# G 4.34 Ausfall eines Kryptomoduls

Wird ein Kryptomodul zur Sicherung der Vertraulichkeit schützenswerter Daten eingesetzt, kommt dem fehlerfreien Funktionieren des Kryptomoduls eine besondere Bedeutung zu. Der Ausfall eines solchen im Einsatz befindlichen Kryptomoduls kann auf verschiedene Ursachen zurückzuführen sein:

- technischer Defekt, der die Funktionsfähigkeit beeinträchtigt,
- Stromausfall, in dessen Folge die flüchtig gespeicherten kryptographischen Schlüssel gelöscht werden, so dass das Kryptomodul infolgedessen nicht mehr ordnungsgemäß verschlüsseln kann,
- unabsichtliche oder absichtliche Zerstörung durch mechanische Einwirkung, Fehlbedienung oder ähnliches.

Die Folgeschäden aufgrund des Ausfalls eines Kryptomoduls können ebenfalls vielseitig sein. Hier sind insbesondere zu nennen:

- Die kryptographische Absicherung einer Datenübertragungsstrecke ist nicht mehr möglich, so dass die Vertraulichkeit temporär nicht mehr gewahrt werden kann. Dies ist insbesondere dann kritisch, wenn der Ausfall nicht bemerkt wird und durch die Fehlfunktion keine Verschlüsselung mehr stattfindet, obwohl die Anwender auf die Sicherstellung der Vertraulichkeit der Daten durch das Kryptomodul bauen.
- Verschlüsselte Daten können nicht mehr entschlüsselt werden, solange das erforderliche Kryptomodul nicht mehr verfügbar ist. Daraus können sich Verfügbarkeitsprobleme für IT-Anwendungen ergeben, die die entschlüsselten Daten weiterverarbeiten.
- Arbeitet das Kryptomodul fehlerhaft, ohne dass ein vollständiger Ausfall eintritt, werden Daten unvollständig oder inkorrekt verschlüsselt. In beiden Fällen kann es bedeuten, dass im Falle der Datenübertragung der Empfänger der Daten bzw. bei lokaler Speicherung der Daten der Anwender die Daten nicht mehr korrekt entschlüsseln kann. Ohne entsprechende Datensicherungen bedeutet dies ggf. einen Totalverlust der Daten.

# G 4.35 Unsichere kryptographische Algorithmen

Der Sicherheitszugewinn durch Einsatz kryptographischer Verfahren ist grundsätzlich von zwei Parametern abhängig: es müssen sichere kryptographische Algorithmen eingesetzt werden und die geheimen Schlüssel müssen vertraulich gehandhabt werden (zur Kompromittierung kryptographischer Schlüssel siehe G 5.83 *Kompromittierung kryptographischer Schlüssel*).

Unsichere kryptographische Algorithmen sind dadurch gekennzeichnet, dass es einem potentiellen Angreifer mit vertretbaren Ressourcen gelingt, das eingesetzte kryptographische Verfahren zu brechen. Bei Verschlüsselungsalgorithmen bedeutet dies, dass es gelingt, aus dem verschlüsselten Text den ursprünglichen Klartext zu ermitteln, ohne dass zusätzliche Informationen bekannt sind. Dabei sind als relevante Ressourcen auf Angreiferseite z. B. die verfügbare Rechenleistung, Hilfsmittel wie Analysetools, vorhandene Kenntnisse, verfügbare Arbeitszeit, Kenntnisse über Schwachstellen etc. zu berücksichtigen. Werden also unsichere kryptographische Algorithmen eingesetzt, besteht für Angreifer die Möglichkeit, den kryptographischen Schutz zu unterlaufen.

Ob jedoch ein kryptographischer Algorithmus unsicher ist, muss jeweils im Einzelfall untersucht werden. Es gibt jedoch einige Kriterien, die auf Unsicherheiten schließen lassen:

- Werden bei symmetrischen Verschlüsselungsverfahren geheime Schlüssel benutzt, deren effektive Länge geringer als 100 Bit ist, so können sie heute mit moderatem Rechnereinsatz durch Ausprobieren aller potentiell möglichen Schlüssel gebrochen werden. Mit steigender Rechnerleistung ist anzunehmen, dass diese Grenze in Zukunft über 100 Bit steigen wird.
- Werden bei asymmetrischen Verschlüsselungs- und Signaturverfahren Algorithmen eingesetzt, deren Sicherheit auf dem Problem des Faktorisierens großer Zahlen basiert, so wird heute angenommen, dass Schlüssellängen von weniger als 2000 Bit als unsicher zu betrachten sind. Dies begründet sich in den Fortschritten bei der Entwicklung effizienter Faktorisierungsalgorithmen, die heute unter massivem Rechnereinsatz Faktorisierungen von Zahlen mit rund 800-900 Bit Länge erlauben.
- Hashfunktionen, die eine beliebig lange Zeichenkette auf einen Hashwert mit konstanter Bitlänge abbilden, können als unsicher betrachtet werden, wenn die konstante Länge des Hashwertes geringer ist als 200 Bit, da sonst zwei Zeichenketten ermittelt werden können, die den gleichen Hashwert ergeben.
- Kryptographische Algorithmen, die von unerfahrenen Entwicklern entworfen wurden und nicht in der wissenschaftlichen Szene untersucht wurden, sollten als potentiell unsicher betrachtet werden, da die Entwicklung sicherer kryptographischer Algorithmen langjährige Erfahrung voraussetzt.
- Nicht veröffentlichte kryptographische Algorithmen, die auffällig schnell in Software ablaufen, sollten ebenfalls als potentiell unsicher betrachtet werden. Die Erfahrung zeigt, dass sichere Algorithmen meist auf komplexen mathematischen Funktionen beruhen müssen.
- Bei der Anwendung kryptographischer Verfahren werden häufig Zufallszahlen benötigt. Schlechte Zufallszahlengeneratoren können dazu führen, dass die damit erzeugten Werte vorhersagbar sind. Dadurch können z. B. kryptographische Checksummen, die die Nachrichtenintegrität sicherstellen sollen, wertlos werden.

Von diesen Kriterien betroffen ist beispielsweise der weltweit sehr häufig eingesetzte DES-Algorithmus zur symmetrischen Verschlüsselung. Dieser benutzt eine effektive Schlüssellänge von 56 Bit. Der so genannte Triple-DES-Algorithmus als dreifache Hintereinanderausführung mit zwei Schlüsseln hat eine effektive Schlüssellänge von 112 Bit und kann zurzeit noch als ausreichend sicher betrachtet werden. Auch betroffen ist der RSA-Algorithmus, der als asymmetrisches Verfahren auf dem Faktorisierungsproblem basiert. Wird RSAmit einer Schlüssellänge unter 1024 Bit betrieben, muss davon ausgegangen werden, dass dies keine ausreichende Sicherheit bietet. Für die nächsten Jahre kann eine Schlüssellänge von mindestens 2000 Bit noch als ausreichend sicher angesehen werden.

Der Hash-Algorithmus MD5 ist veraltet und weist bekannte Schwächen auf, die auch bereits anhand praktischer Beispiele demonstriert werden konnten. Auch der Hash-Algorithmus SHA-1 ist nicht mehr für alle Einsatzzwecke geeignet.

Ein häufiges Beispiel unsicherer, aber sehr schneller Algorithmen ist die so genannte XOR-Funktion, bei der konstante Werte mit dem ursprünglichen Klartext auf einfache Weise verknüpft werden. Dies ist ein hochperformanter Algorithmus, der jedoch sehr schnell gebrochen werden kann. Die XOR-Funktion kann andererseits aber der sicherste Verschlüsselungsalgorithmus überhaupt sein, wenn die zu verschlüsselnden Daten mit nicht vorhersagbaren Zufallswerten XOR-iert werden (One-Time-Pad).

Für den Laien ist es praktisch unmöglich, festzustellen, ob ein kryptographischer Algorithmus ausreichend sicher ist. Daher sollten nur solche Algorithmen eingesetzt werden, die bekanntermaßen von Experten entwickelt wurden oder die einer langjährigen Untersuchung durch die wissenschaftliche Szene unterzogen wurden.

# G 4.36 Fehler in verschlüsselten Daten

Liegen Daten in verschlüsselter Form vor und werden diese verändert, kann es bei der Entschlüsselung der Daten dazu kommen, dass die Daten nicht mehr korrekt entschlüsselt werden können. Je nach Betriebsart der Verschlüsselungsroutinen kann dies bedeuten, dass nur wenige Bytes falsch entschlüsselt werden oder dass sämtliche Daten ab dem Fehler falsch entschlüsselt werden. Gibt es keine Datensicherung, kann dies einen Totalverlust der Daten bedeuten.

Die genannten Fehler in den verschlüsselten Daten können auf verschiedene Weise entstehen:

- Bei der Datenübertragung der verschlüsselten Daten kommt es zu einem Übertragungsfehler, der nicht behoben werden kann.
- Auf dem Speichermedium (Diskette, Festplatte) kommt es zu einem irreparablen Fehler.
- Ein Computer-Virus führt an den Daten Manipulationen durch.
- Ein Dritter führt absichtlich Manipulationen an den Daten durch, beispielsweise indem die verschlüsselten Daten mit einem Editorprogramm an wenigen Stellen manipuliert werden.

In ungünstigen Fällen, wenn z. B. ein Bitverlust auftritt oder zu große Datenmengen verändert werden und eine Fehlerfortpflanzung stattfindet, können die Daten selbst bei Kenntnis des kryptographischen Verfahrens und der zur Verschlüsselung benutzten Schlüssel nicht mehr rekonstruiert werden.

Noch kritischer kann sich ein Fehler in den verwendeten kryptographischen Schlüsseln auswirken. Schon die Änderung eines einzigen Bits eines kryptographischen Schlüssels führt dazu, dass sämtliche damit verschlüsselten Daten nicht mehr entschlüsselt werden können. Ohne eine Datensicherung des kryptographischen Schlüssels sind diese Daten verloren.

# G 4.37 Mangelnde Verlässlichkeit von Groupware

Groupware-Dienste ersetzen an vielen Stellen die herkömmliche Verfahrensweise, so ersetzt E-Mail die traditionelle Kommunikation per Post, Kalender oder Adressbücher werden online gepflegt. Dabei wird jedoch häufig nicht beachtet, dass diese Dienste ohne zusätzliche Sicherungsmaßnahmen nicht ausreichend verlässlich sind. Dies betrifft sowohl Vertraulichkeit als auch Integrität und Verfügbarkeit dieser Dienste und der damit verarbeiteten Informationen.

**Ausfälle und Nachrichtenverluste**

Der Datenaustausch über Groupware-Dienste wie E-Mail ist schnell und komfortabel, aber nicht immer sehr zuverlässig. Aufgrund von Hardware- oder Softwarefehlern bei den beteiligten IT-Systemen oder durch Störungen auf dem Übertragungsweg kommt es immer wieder zum Nachrichtenverlust. Die technischen Probleme können vielfältige Ursachen haben, z. B. können Leitungen beschädigt sein, Netzkopplungselemente ausfallen oder die Kommunikationssoftware falsch konfiguriert sein. E-Mails können auch verloren gehen, weil die Empfänger-adresse nicht korrekt angegeben war. Dabei ist das größte Problem, dass die Benutzer häufig nicht über die unterbliebene Zustellung der E-Mail informiert werden. Auf eine automatisierte Unterrichtung bei einer unterbliebenen Zustellung kann nicht vertraut werden.

**Beispiel:**

- Viele E-Mailprogramme bieten Optionen wie "Zustellung bestätigen" oder "Empfang bestätigen". Entsprechende Rückmeldungen sollten aber nicht überbewertet werden. Zum einen werden die Zustellbestätigungen häufig nicht durch die Ankunft einer E-Mail am Bildschirmarbeitsplatz des Empfängers ausgelöst wird, sondern durch die Ankunft bei einem Mailserver. Ob der Mailserver die E-Mail erfolgreich an den Adressaten weitergeleitet hat, wird dann nicht mehr mitgeteilt. Zum anderen erfolgt auch häufig keine Zustellbestätigung, obwohl die E-Mail korrekt übertragen wurde, wenn diese Option durch die Empfängerseite nicht unterstützt wird.

**Mangelnde Authentizität und Vertraulichkeit von Nachrichten**

Groupware-Dienste werden meistens in der Grundeinstellung ohne kryptographische Absicherung angeboten. Dadurch können über Kalenderdienste unter Umständen auch Unbefugte Einsicht in die Zeitplanung von Gruppen oder einzelnen Personen nehmen. Dies kann der gezielten Vorbereitung für verschiedene Formen von Angriffen dienen, z. B. Einbrüchen, Social Engineering oder Wirtschaftsspionage.

Bei unverschlüsselten E-Mails können alle Informationen auf jedem IT-System gelesen werden, auf dem die Nachricht auf ihrem Weg durchs Netz bearbeitet wird. Da der genaue Transportweg im Allgemeinen nicht vorhersagbar ist, kann eine E-Mail sehr viele verschiedene Systeme passieren.

Informationen, die nicht durch digitale Signaturen geschützt sind, können auch auf jedem beteiligten System verändert oder gelöscht werden, ohne dass dies vom Empfänger bemerkt werden kann. Abgesehen von Veränderungen am Text oder an etwaigen Dateianhängen einer E-Mail können auch Informationen wie Absende- und Weiterleitungsdaten oder die Absenderadresse selbst verändert werden, siehe auch G 5.73 *Vortäuschen eines falschen Absenders*.

Daher ist es falsch, E-Mails mit klassischen Briefen zu vergleichen. Ein Vergleich mit Postkarten wäre zutreffender.

**Beispiele:**

- Ein Angestellter verschickte mit der Absenderangabe seines Chefs E-Mails mit Arbeitsaufträgen an verschiedene Kollegen.
- Praktisch alle der vielen Spam-E-Mails, die täglich die E-Mail-Postfächer füllen, tragen eine gefälschte Absenderadresse.
- Als Absendedatum einer E-Mail wird meist die lokale Systemzeit auf dem Rechner des Absenders eingetragen. Da diese oft selbst von normalen Anwendern verstellt werden kann, stellt ein bestimmtes Absendedatum in einer E-Mail keinen Beweis dafür dar, dass diese wirklich zu einem bestimmten Zeitpunkt verschickt wurde.

# G 4.38 Ausfall von Komponenten eines Netz- und Systemmanagementsystems

Bei einem Netz- und Systemmanagementsystem kann es zu einem Ausfall verschiedener Komponenten kommen. Einige der dadurch entstehenden Probleme und Gefährdungen sind im folgenden beschrieben.

**Ausfall von verwalteten Komponenten**

Fallen beim Einsatz eines Netz- und Systemmanagementsystems damit verwaltete Komponenten aus, so kann es je nach Managementsystem vorkommen, dass die Managementinformationen nicht automatisch aufgrund dieses Ereignisses aktualisiert werden. In der Regel wird dem Systemadministrator z. B. bei Netzmanagement-Systemen nur das Ausfallen der Komponente angezeigt. Wird z. B. der Ausfall der Komponente von einem Angreifer beobachtet oder bewusst herbeigeführt, so kann dieser u. U. außerhalb des LANs einen eigenen Rechner in das System einbringen und als die ausgefallene Komponente ausgeben (IP-Spoofing). Dieser Rechner kann dann zu weiteren Angriffen genutzt werden, bei denen er dann mit den Rechten eines internen Rechners ausgestattet ist (z. B. Einbringen falscher Managementinformationen).

**Ausfall von Überwachungskomponenten**

Fallen beim Einsatz eines Managementsystems Teile des Systems (auch unbemerkt) aus, so sind die durch die Komponente überwachten oder verwalteten Systemkomponenten nicht mehr an das Managementsystem angeschlossen. Neue eingehende Managementanweisungen werden dadurch nicht mehr auf diesen Rechnern umgesetzt. Dies hat zur Folge, dass inkonsistente Systemkonfigurationen entstehen, die wiederum zu Sicherheitsproblemen führen können.

**Nicht-Verfügbarkeit der zentralen Managementstation**

Fällt in einem durch ein Managementsystem verwalteten Netz die zentrale Managementstation aus, so kann das System nicht mehr zentral verwaltet werden. Dauert die Nicht-Verfügbarkeit länger an, weil z. B. die Hardware aufgrund fehlender Wartungsverträge nicht kurzfristig ersetzt werden kann, so werden unter Umständen Routinefunktionen wie etwa Datensicherungen nicht mehr angestoßen. Werden nun "von Hand" Änderungen an den einzelnen verwalteten Systemen unkoordiniert durchgeführt, so entstehen Inkonsistenzen und möglicherweise Sicherheitsprobleme.

**Ausfall von Netzkoppelelementen während der Übertragung von Managementinformationen**

Beim Einsatz eines Managementsystems zur Verwaltung eines Rechnernetzes ist der Austausch von so genannter Managementinformation zwischen den einzelnen Komponenten des Managementsystems nötig. Die Information wird über das lokale Netz übertragen. Lokale Netze bestehen in der Regel (je nach verwendeter Netztechnik) aus mehreren Teilnetzen, die über Netzkoppelelemente wie Router miteinander verbunden sind. Die Netzkoppelelemente reichen dabei Daten aus einem Teilnetz in ein anderes Teilnetz weiter. Fallen die Koppelelemente aus, so ist dies gleichbedeutend mit der physikalischen Trennung der betroffenen Teilnetze. Managementinformationen können dann nicht mehr ausgetauscht werden. Dabei existiert in der Regel ein Teilnetz, das noch von der jeweiligen Managementstation verwaltet werden kann, und ein

Teilnetz, das nicht mehr verwaltet werden kann. Je nach Dauer der Nichterreichbarkeit führt dies zu Inkonsistenzen und Sicherheitsproblemen.

# G 4.39 Software-Konzeptionsfehler

Bei der Planung von Programmen und Protokollen können sicherheitsrelevante Konzeptionsfehler entstehen. Häufig sind diese Fehler historisch gesehen durchaus verständlich. So ist sicherlich keiner der Entwickler der im Internet verwendeten Protokolle Ende der 60er-Jahre davon ausgegangen, dass diese Protokolle einmal die Grundlage für ein weltumspannendes und kommerziell höchst bedeutendes Computer-Netz werden würden.

**Beispiele:**

- Beispiele für Konzeptionsfehler sind die offene Übertragung der Daten im Internet, so dass Daten (z. B. Passwörter) mitgelesen oder verändert werden können, oder die Möglichkeit, Pakete mit Internet-Adressen zu versenden, die einem anderen Rechner zugeteilt worden sind. Ein Spezialfall hiervon ist die so genannte FTP-Bounce-Attacke, bei der ausgenutzt wird, dass die Verbindung, die beim FTP-Protokoll für die Datenübertragung eingesetzt wird, zu einem beliebigen Rechner aufgebaut werden kann. Im ungünstigen Fall können auf diese Weise sogar Firewalls mit dynamischen Paketfiltern überwunden werden (siehe CERT Advisory 97-27). Weitere Fehler in den Internet-Protokollen sind sicherlich vorhanden und werden zukünftig publiziert werden.
- Ein weiteres Beispiel für einen Konzeptionsfehler ist das so genannte DNS-Spoofing (siehe auch G 5.78 *DNS-Spoofing*). Das Domain Name System ist der zentrale Auskunftsdienst im Internet, der die Übersetzung der leicht merkbaren Rechnernamen wie www.preiswert.de in die zugehörige Internet-Adresse ermöglicht. Bei DNS-Spoofing versucht ein Angreifer, einem Rechnernamen einen falschen Rechner zuzuweisen, so dass Auskunftsuchende fehlgeleitet werden.
- Ein weiteres Beispiel für einen Konzeptionsfehler ist die Möglichkeit, anonym sehr viele Werbe-E-Mails zu versenden (Mail-Spamming). Hierbei werden häufig fremde Mailserver als so genannte Remailer eingesetzt, so dass Gegenaktionen durch den Empfänger ins Leere laufen. Die Ursache für diese Angriffe liegt eindeutig in den mangelhaften Authentisierungsmöglichkeiten, die das Internet zur Zeit bietet.

# G 4.40 Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen.

# G 4.41 Nicht-Verfügbarkeit des Mobilfunknetzes

Wie alle Systeme, die keine hundertprozentige Verfügbarkeit gewährleisten, stehen auch Mobilfunknetze nicht immer an den Orten und zu den Zeiten zur Verfügung, zu denen sie am dringendsten benötigt werden.

Häufigste Ursache sind Funklöcher, also Bereiche, die nicht vom eigenen Netzbetreiber versorgt werden. Bei einer sehr großen Nachfrage können aber auch Teile des Netzes überlastet sein. Dies kann dazu führen, dass Nachrichten nicht bzw. verzögert empfangen oder gesendet werden.

Werden Datendienste über das Mobilfunknetz genutzt, können die Übertragungsraten zu niedrig sein. Es gibt bei den Mobilfunkanbietern verschiedene Funknetzstandards mit unterschiedlichen Datenübertragungsraten (z. B. GPRS, HSDPA, LTE). So kann es sein, dass zwar das Mobilfunknetz des jeweiligen Anbieters verfügbar ist, aber der schnelle Datendienst über LTE oder HSDPA nicht funktioniert. Dann werden Informationen aus dem Internet nur sehr langsam abgerufen. Anders als bei der Telefonie, wo der Unterschied zwischen einer GSM- oder UMTS-Verbindung kaum auffällt, ist der Qualitätsunterschied bei den Datendiensten erheblich.

Weiterhin kann es Störsender geben, die in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist. Es gibt auch Geräte, die genau für diesen Zweck verkauft werden. Allerdings ist der Betrieb solcher Geräte in Deutschland nicht zulässig.

Defekte elektrische Geräte können Funkverbindungen ebenfalls stören.

**Beispiele:**

Die Funkkapazität einer Sendestation reicht nicht, wenn nach einem großen Unfall sehr viele Personen gleichzeitig ein Mobiltelefonat führen wollen, um Rettungsdienste zu benachrichtigen oder ihre Angehörigen zu informieren.

# G 4.42 Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs

Die Benutzung eines Mobiltelefons, Smartphones, Tablets oder PDAs kann durch verschiedene Faktoren negativ beeinträchtigt werden:

- Der Akku kann leer sein, weil vergessen wurde, ihn aufzuladen oder weil das Gerät stark genutzt wurde. Der Akku kann leer sein, weil vergessen wurde, ihn aufzuladen.
- Der Akku kann seine Fähigkeit, Energie zu speichern, verloren haben.
- Der Benutzer hat das Zugangspasswort bzw. die PIN vergessen und kann deswegen das Gerät nicht mehr benutzen oder es wird gelöscht, nachdem das Zugangspasswort bzw. die PIN wiederholt falsch eingegeben wurde.
- Komponenten wie Display, Tasten oder SIM-Karte können defekt sein.

Wenn ein Mobiltelefon, Smartphone, Tablet oder PDA schädigenden Umwelteinflüssen ausgesetzt wird, kann seine Funktionsfähigkeit beeinträchtigt werden. So können die Geräte beispielsweise sowohl unter zu hohen als auch zu niedrigen Temperaturen leiden, ebenso unter Staub oder Feuchtigkeit. Wenn ein Mobiltelefon oder PDA schädigenden Umwelteinflüssen ausgesetzt wird, kann seine Funktionsfähigkeit beeinträchtigt werden. Mobiltelefone und PDAs können sowohl unter zu hohen als auch zu niedrigen Temperaturen leiden, ebenso unter Staub oder Feuchtigkeit.

**Beispiele:**

- Auf einer längeren Zugfahrt bearbeitete ein Mitarbeiter auf seinem Smartphone eine Präsentation. Um inhaltliche Details zu klären, wurde diese zwischen ihm und einem Kollegen in der Firma mehrmals per E-Mail hin und her geschickt. Da jedoch die Akkulaufzeit stark von der Nutzung abhängig ist und insbesondere Datendienste viel Akkuleistung benötigen, war der Akku unbemerkt nahezu leer geworden. Bei einem späteren wichtigen Telefonat schaltete sich das Gerät automatisch ab und konnte erst Stunden später im Hotelzimmer wieder in Betrieb genommen werden.
- Ein Tablet wird in einem geparkten Auto zurückgelassen. Dies erhöht nicht nur die Diebstahlgefahr, sondern es wird auch eventuell schädigenden Umwelteinflüssen ausgesetzt. Durch direkte Sonneneinstrahlung können im Sommer hinter einer Glasscheibe Temperaturen von über 60°C entstehen. Ein ähnliches Problem besteht im Winter, wo im geparkten Auto Temperaturen deutlich unter dem Gefrierpunkt herrschen können. Durch solche extremen Temperaturen kann der Akku oder auch das Display beschädigt werden.
- Auf einer Dienstreise ist einem älteren PDA zwischendurch der Strom ausgegangen, weil die Ersatzbatterien zu spät eingesetzt wurden. Nach dem Wiedereinschalten sind allerdings viele Konfigurationseinstellungen verloren gegangen, da diese vom Betriebssystem nicht automatisch gesichert wurden. Dadurch laufen anschließend einige Anwendungen wie E-Mail und Internetzugriff nicht mehr korrekt. Auf einer Dienstreise ist dem PDA zwischendurch der Strom ausgegangen, weil die Ersatzbatterien zu spät eingesetzt wurden. Nach dem Wiedereinschalten sind allerdings viele Konfigurationseinstellungen verloren gegangen, da diese vom Betriebssystem nicht automatisch gesichert wurden. Dadurch laufen anschließend einige Anwendungen wie E-Mail und Internetzugriff nicht mehr korrekt.

# G 4.43 Undokumentierte Funktionen

Viele Anwendungsprogramme enthalten undokumentierte Funktionen, also Funktionen, die nicht in der Dokumentation beschrieben sind und die den Benutzern nicht bekannt sind. Bei einigen Betriebssystemen beziehungsweise Anwendungsprogrammen gibt es mittlerweile Literatur, die einen Großteil der bekannt gewordenen, bis dato undokumentierten Funktionen beschreibt und die im Allgemeinen umfassender ist als die mitgelieferten Handbücher. Undokumentierte Funktionen müssen sich allerdings nicht nur auf Hilfsmittel mit nützlichen Effekten beschränken. Solange diese Funktionen nicht offengelegt sind, kann nicht ausgeschlossen werden, dass mit ihnen auch viel Schaden angerichtet werden kann.

Dies ist insbesondere dann problematisch, wenn die undokumentierten Funktionen Sicherheitsmechanismen des Produktes betreffen, beispielsweise den Zugriffsschutz. Solche Funktionen dienen oft als "Hintertüren" (engl. Backdoor) während der Entwicklung oder der Verteilung von Anwendungsprogrammen.

**Beispiele:**

- Bei verschiedenen IT-Systemen fanden sich von den Entwicklern eingebaute (und vergessene) Hintertüren, um die Wartung zu erleichtern, die es allerdings auch ermöglichten, mit einem trivialen Passwort Administrator-Rechte zu erlangen.
- Viele Programme können (oder müssen sogar) online beim Hersteller registriert werden. Bei einigen dieser Programme wurde bei der Online-Registrierung der Software gleichzeitig ein Überblick über alle auf der Festplatte gespeicherten Programme mitgeliefert.
- Eine Software, deren Einsatz für die Nutzung eines Cloud Services vorausgesetzt wird, enthält eine bewusst eingebaute beziehungsweise nicht verschlossene Backdoor. Mit deren Hilfe können sich Angreifer Zugriff auf die Systeme des Cloud-Benutzers verschaffen.

# G 4.44 Ausfall von Novell eDirectory

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen kann es zum Ausfall eines eDirectory-Systems oder Teilen davon kommen. Als Konsequenz davon können die im Verzeichnis gehaltenen Daten temporär nicht mehr zugänglich sein, und zwar weder für eDirectory-Benutzer noch für etwaige Netzapplikationen, die auf das eDirectory zugreifen. Im Extremfall kann es auch zu Datenverlusten kommen.

Dadurch können Geschäftsprozesse gestört und der interne Workflow behindert werden, durch die vielfältigen Funktionen von eDirectory und die starke Einbindung in die Organisation kann es damit auch zu Produktivitätsausfällen kommen.

Sind Repliken der ausgefallenen Systemteile funktionsfähig vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch unter Umständen - abhängig von der Netztopologie - mit reduzierter Performance.

# G 4.45 Verzögerte Archivauskunft

Verzögerungen bei der Wiederbeschaffung archivierter Dokumente können Geschäftsprozesse, in deren Kontext eine Archivanfrage erfolgt, stören oder behindern. Für derartige Verzögerungen kommen viele Ursachen in Betracht, beispielsweise:

- veraltete Archivserver-Software,
- ungünstige Wahl von Index- und Suchkriterien bei Ablage oder Suche von archivierten Daten,
- überlastete Hardware des Archivservers oder beteiligter Datenbankserver,
- Verzögerungen im Netz sowie
- unausgewogenes Verhältnis von Speichermedien zu Laufwerken.

Bei dem letztgenannten Punkt sind zwei Fälle zu unterscheiden:

- Wird für die Archivierung ein Laufwerk mit einem einzelnen Speichermedium genutzt, das eine sehr große Kapazität hat, können die Antwortzeiten sehr groß werden, da nur jeweils ein Benutzer gleichzeitig auf das Archiv zugreifen kann. Alle anderen Anfragen werden zwischengespeichert und dann der Reihe nach abgearbeitet.
- Bei einer großen Anzahl kleiner Speichermedien sind im Verhältnis dazu nur wenige Laufwerke verfügbar. Daher müssen die Datenträger bei Anfragen entsprechend oft gewechselt werden, was zu längeren Antwortzeiten führt. Kleine Speichermedien sind darüber hinaus schneller in ihrem Speicherplatz erschöpft (siehe G 4.20 *Überlastung von Informationssystemen*).

Verzögerungen können sich auch bei der Einstellung von Dokumenten ins Archiv ergeben, etwa wenn die Bestätigung des Archivierungsvorgangs durch lange Übertragungszeiten im LAN verzögert wird.

# G 4.46 Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung

Bei der Archivierung werden sehr große Datenvolumen gespeichert. Auf alle archivierten Daten muss zu einem späteren Zeitpunkt in annehmbarer Zeit jederzeit kontrolliert und eindeutig zugegriffen werden können. Diese Funktionalität wird durch das Archivsystem gewährleistet, das hierzu einen Index der gespeicherten Dateien erzeugt.

Archivsysteme realisieren jedoch meist nur einfache Dateizugriffe. Um mehr Komfort beim Zugriff zu erreichen, wird daher sehr oft ein übergeordnetes Dokumentenmanagementsystem (DMS) eingesetzt, über das der Zugriff auf das Archiv gesteuert und weitergehende Funktionalitäten, z. B. komplexe Suchanfragen, realisiert werden.

Das DMS erzeugt bei der Archivierung die Referenzierung der Daten, kontrolliert deren Version und legt gegebenenfalls einen Volltextindex an, so dass alle auf dem Speichermedium archivierten Daten zu einem späteren Zeitpunkt eindeutig identifiziert werden können.

Letztlich gibt es daher zwei Indexdatenbanken (im Archivsystem und im DMS), die beide synchronisiert werden müssen. Kommt es einseitig zu Veränderungen in den im DMS gespeicherten Indexdaten oder zu Fehlern auf dem Speichermedium, ohne dass die Veränderungen im anderen Teil berücksichtigt werden, können archivierte Daten nicht mehr den Referenzen im DMS zugeordnet werden.

# G 4.47 Veralten von Kryptoverfahren

Die Zuverlässigkeit von Kryptosystemen ist direkt mit der fortschreitenden Entwicklung der Rechenleistung von IT-Systemen, der Entwicklung neuerer Algorithmen sowie der Forschung auf dem Gebiet der Kryptoanalyse verknüpft. Durch die Steigerung der Leistungsfähigkeit von IT-Systemen können als sicher geltende Kryptoalgorithmen bzw. Schlüssellängen zukünftig möglicherweise kompromittiert werden.

Hierdurch besteht die Gefahr, dass im Falle der Kompromittierung von Kryptoverfahren oder Kryptoschlüsseln

- verschlüsselte Daten unbefugt entschlüsselt werden können,
- von Unbefugten Dokumente mit einer technisch gültigen Signatur versehen werden können, so dass dann
- authentische, signierte Dokumente nicht mehr von gefälschten unterschieden werden können.

**Beispiel:**

Krankenhäuser müssen die Akten ihrer Patienten auch nach Abschluss der Behandlung für einen langen Zeitraum sicher aufbewahren. Ein deutsches Krankenhaus hat dementsprechend 1980 angefangen, die elektronisch gespeicherten Krankendaten zu verschlüsseln. Das dazu verwendete Verfahren basierte auf DES mit 40 Bit langen Schlüsseln. Da sich im Krankenhaus niemand mit Verschlüsselung auskannte, wurde dieses Verfahren auch im Jahr 2001 noch eingesetzt, obwohl mittlerweile bereits im Internet Programme verfügbar waren, um die damit verschlüsselten Daten auszulesen. Dies fiel erst bei einer Datenschutzkontrolle auf.

# G 4.48 Ausfall der Systeme eines Outsourcing-Dienstleisters

Bei einem Outsourcing-Dienstleisters können die IT-Systeme teilweise oder ganz ausfallen, wodurch auch der Auftraggeber betroffen ist.

Auch wenn der IT-Ausfall nur einige Systeme oder Applikationen betrifft, kann dies dazu führen, dass die Datenverarbeitung inkonsistent oder fehlerhaft ausgeführt wird.

Außerdem ist zu berücksichtigen, dass bei unzureichender Strukturierung oder Isolation der IT-Systeme des Dienstleisters bereits der Ausfall eines Systems, das nicht dem Auftraggeber zugeordnet ist, trotzdem dazu führen kann, dass der IT-Betrieb des Auftraggebers beeinträchtigt wird. Dies kann immer dann ein Problem sein, wenn einzelne IT-Komponenten (z. B. Host-Rechner, Firewalls) für verschiedene Auftraggeber des Dienstleisters gemeinsam genutzt werden. Dann kann unter Umständen ein Fehler im Datenbestand eines beliebigen Kunden des Outsourcing-Dienstleisters dazu führen, dass beispielsweise bei der Host-Verarbeitung die Batch-Verarbeitung mehrerer Kunden eingestellt werden muss, wenn diese schlecht oder fehlerhaft konfiguriert ist.

Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen auslagernder Organisation und Outsourcing-Dienstleister ausfällt.

# G 4.49 Unsichere Default-Einstellungen auf Routern und Switches

Aktive Netzkomponenten werden von Herstellern oft mit unsicheren Default-Konfigurationen ausgeliefert, die den sicheren Einsatz gefährden. Bei einigen Geräten zeigen außerdem die Systembefehle zur Anzeige einer Konfiguration nicht alle Parameter an.

Folgende Aspekte sind häufig problematisch:

**Betriebssystem**

Aktive Netzkomponenten werden oft mit einem veralteten Versionsstand des Betriebssystems ausgeliefert.

**Hostname**

Werkmäßig eingestellte Hostnamen verraten oft den Hersteller der Geräte.

**Dienste**

Werkseitig werden Geräte mit Standardkonfigurationen ausgeliefert, auf denen eine Vielzahl von Diensten aktiviert sind. Beispielsweise können dies HTTP, Telnet, FINGER oder sonstige Dienste sein.

**Benutzerkonten und Passworte**

Werksmäßig eingerichtete Benutzerkonten haben dokumentierte und damit allgemein bekannte Standardnamen und -Passworte. Auf einschlägigen Internet-Seiten stehen Listen mit herstellerspezifischen Standard-Accounts und Passworten zum Download bereit.

**Unsichere SNMP-Versionen**

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten sogenannten Community Strings. Als Standardeinstellung bei nahezu allen Herstellern ist der Read-Community-String auf den Wert "public" eingestellt, während der Write-Community-String auf den Wert "private" gesetzt ist. Wenn die unsicheren SNMP-Versionen genutzt werden und für die Administration kein eigenes Administrationsnetz eingerichtet wurde, kann ein Angreifer leicht die Kontrolle über Netzkomponenten erlangen, wenn diese Default-Einstellungen beibehalten werden.

**Routing-Protokolle**

Auf Routern und Switches verschiedener Hersteller sind standardmäßig Routing-Protokolle aktiviert.

**Login-Banner**

Werksmäßig verraten Login-Banner unterschiedlicher Geräte beispielsweise die Modell- und Versionsnummer des Gerätes. Diese Angaben können für die gezielte Auswahl bekannter Exploits verwendet werden und erleichtern Angreifern so die Durchführung von Angriffen.

# G 4.50 Überlastung des z/OS-Betriebssystems

Auch wenn durch den *Workload Manager* ein z/OS-Betriebssystem so verwaltet wird, dass eine Überlastung eigentlich nicht vorkommen sollte, gibt es eine Reihe von Gefährdungen, die zu einer Überlastung führen können. Eine Überlastung muss nicht zwangsläufig zu einem kompletten System-Stillstand führen. Es können auch nur verschiedene System-Ressourcen nicht mehr verfügbar sein, obwohl das System selbst noch reagiert. Die nachfolgenden Situationen sind typisch, aber nicht die einzigen Gefährdungen dieser Art.

### *Spool-Full*-Situation

Die Spool-Datei eines *Job Entry Subsystem* (JESx) ist nur für eine bestimmte Menge von Ausgabedaten vorgesehen. Es kann vorkommen, dass z. B. durch eine Programmschleife unbegrenzt Daten auf die Spool-Datei des JESx geschrieben werden. Dies kann zu einer *Spool-Full*-Situation führen, neue Batch-Jobs können nicht mehr gestartet werden. Nur die laufenden Online-Verfahren sind u. U. noch aktiv, sofern keine Ausgabedateien auf die Spool-Datei geschrieben werden. Da viele JES-Kommandos bei der Ausführung eine benutzbare Spool-Datei voraussetzen, kann dies bedeuten, dass umfangreiche (und zeitintensive) Recovery-Maßnahmen notwendig sind, um dieses Problem zu bereinigen.

### Vollständiger System-Stillstand

Unix-Prozesse im USS-Subsystem (*Unix System Services*) werden in z/OS auf Adressräume abgebildet. Steht nicht mehr genügend Hauptspeicher zur Verfügung, müssen diese Adressräume über den *AuxiliaryStorage Manager* (ASM) auf die Page-Platten ausgelagert werden. Reichen auch diese nicht aus, kann kein Adressraum mehr angelegt werden.

Wenn die Anzahl der Unix-Prozesse im USS nicht beschränkt ist und nicht genügend Platz auf den Page-Platten zur Verfügung steht, können sich deshalb Sicherheitsprobleme durch den Start von zu vielen Unix-Prozessen ergeben. Ursache kann beispielsweise eine rekursive Funktion sein, die unentwegt neue Unix-Prozesse startet. Als Folge kann es passieren, dass das System praktisch stillsteht.

Von diesem Problem ist z/OS (mit 64 Bit-Adressierung) im Vergleich zu seinem Vorgänger OS/390 (mit 31 Bit-Adressierung) durch die höhere Adressierbarkeit deutlich weniger betroffen. Durch die höhere Adressierbarkeit kann dem z/OS-System ein größerer Hauptspeicher zur Verfügung gestellt werden. Dies hat zur Folge, dass die Page-Platten erst viel später benötigt werden.

Generell können Kommandos oder Programmteile, die ständig neue Prozesse starten, sehr schnell das System überlasten. Dies kann letztendlich einen Initial Program Load (IPL) erforderlich machen.

### Systemüberlastung durch zu viele JESx Initiators

Über die Anzahl der gestarteten *Initiators* steuert der Administrator die Batch-Verarbeitung und deren Prioritäten. Sind zu wenig *Initiators* gestartet, können Staus bei der Batch-Verarbeitung entstehen. Sind zu viele *Initiators* gestartet, kann dies zur Überlastung von Ressourcen führen.

Werden zu viele Batch-Jobs gestartet, so besteht die Gefahr, dass die *Page Datasets* nicht ausreichen. Dies erfordert ein manuelles Eingreifen in die Systemsteuerung durch das Bedienpersonal.

Ist das *Job Entry Subsystem* mit einer sehr großen Anzahl von *Initiators* definiert worden, die jedoch nicht sofort aktiviert werden, kann es vorkommen, dass bei der Eingabe des JES2-Kommandos *$SI* (statt z. B. *$SI1-10*) alle möglichen *Initiators* gestartet werden. Dadurch laufen unter Umständen mehr Batch-Jobs an als geplant. Dies führt zwar in der Regel nicht zu einem System-Stillstand, die Antwortzeiten können sich jedoch erheblich verlängern.

**Verzögerte Bandverarbeitung**

Wenn gleichzeitig mehr Bandeinheiten angefordert werden, als Stationen vorhanden sind, verzögert sich die Sicherung der Daten auf Bänder. Die Sicherungs-Jobs gehen in den *Wait*-Status und warten auf freie Bandstationen.

**Beispiele**

- In einer z/OS-Installation wurden zu viele *Initiators* gestartet. Dies hatte zur Folge, dass während der Batch-Verarbeitung zu viele Batch-Jobs gleichzeitig aktiviert wurden, wodurch die CPU des Systems stark belastet wurde. Obwohl das System die Last bewältigt hat, führte die Situation zu langen Antwortzeiten bei der *Time Sharing Option* (TSO).
- Bei der USS-Basisdefinition eines z/OS-Betriebssystems wurden die Werte von *MAXPROCSYS* und *MAXFILEPROC* auf sehr hohe Werte gesetzt. Als ein Mitarbeiter einen rekursiven Funktionsaufruf, den er auf einer Unix-Schulung kennen gelernt hatte, unter *Unix System Services* ausprobierte, blieb das System nach kurzer Zeit wegen *Auxiliary Storage Shortage* stehen.

# G 4.51 Unzureichende Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs

Ein IT-System, das sich im mobilen Einsatz befindet, kann über ein VPN an ein LAN angeschlossen sein, so dass die Kommunikationsverbindung sehr gut geschützt ist. Wenn allerdings dieses IT-System selber ungenügend gegen unbefugten Zugriff geschützt ist, besteht die Gefahr, dass ein Unbefugter dieses als "Gateway" missbraucht, um auf das interne Netz zuzugreifen.

Typische Endgeräte für den mobilen Einsatz sind Handys oder PDAs, bei denen meistens keine Benutzertrennung möglich ist. Dadurch kann jeder, der Zugriff auf das IT-System hat, auf alle Daten und Programme zugreifen, auch auf interne Daten der Organisation oder sehr persönliche Daten des Eigentümers.

Andere leider sehr typische Schwachstellen bei mobilen Komponenten wie PDAs sind:

- unzureichende Zugriffschutz- und Authentisierungsmechanismen
- keine oder unzureichende Möglichkeiten zur Verschlüsselung von Daten
- ungesicherte Synchronisation
- keine oder unzureichende Protokollierungsmöglichkeiten

Es gibt eine Vielzahl verschiedener PDA-Modelle mit den unterschiedlichsten Betriebssystemen. Die Sicherheitseigenschaften der verschiedenen PDA-Plattformen sind unterschiedlich, einen sicheren Schutz gegen Manipulationen bietet aber derzeit keines der kommerziell gebräuchlichen Systeme.

**Beispiel:**

Bei Palm OS 3.5.2 und allen Vorgängerversionen kann über eine Tastenkombination wahlweise in den sogenannten "Console Mode" oder den "Debug Mode" gewechselt werden. Beide Modi erlauben, an allen Sicherheitsmechanismen des Betriebssystems vorbei, den direkten Zugriff auf Systemdaten. Dabei ist es völlig gleichgültig, ob der PDA-Zugriff über ein Passwort geschützt ist oder nicht: beide Modi können unter Umgehung des Zugriffsschutzes aktiviert werden.

# G 4.52 Datenverlust bei mobilem Einsatz

Bei mobilen Endgeräten und mobilen Datenträgern ist das Risiko von Datenverlusten höher als bei stationären Systemen. Ursache können Diebstahl oder Geräteverlust sein, aber auch technische Probleme oder schlichter Strommangel.

Mobile Datenträger und Geräte werden oft gestohlen, da sie klein und universell einsetzbar sind. Teilweise haben es die Täter auf die Geräte abgesehen, teilweise aber auch auf die dort gespeicherten Informationen.

Noch häufiger sind Datenverluste ohne kriminelle Absichten von Außenstehenden. In Umfragen hat sich gezeigt, dass jeder zweite Befragte schon einmal einen USB-Stick, eine Speicherkarte oder einen anderen mobilen Datenträger verlegt, vergessen oder verloren hat. Dadurch können schützenswerte Daten in fremde Hände gelangen.

Mobile IT-Endgeräte sind nicht immer online. Daher befinden sich die auf diesen Systemen gespeicherten Daten nicht immer auf dem aktuellsten Stand. Dies betrifft sowohl Kalendereinträge als auch allgemeine Informationen, kann aber unter Umständen auch sicherheitsrelevante Auswirkungen haben. Während der Zeit, in der keine Verbindung zu den organisationseigenen IT-Systemen und Informationsquellen besteht, können beispielsweise keine Informationen über aktuelle Sicherheitsprobleme eingeholt und Virenscanner nicht aktualisiert werden.

Beispiele:

- Das neue Smartphone fällt aus der Hemdtasche und zerschellt oder ein Handheld wird statt der Zeitung vom Hund apportiert. Vor allem Transportschäden führen häufig zu Datenverlusten und Geräte- oder Komponentenausfällen. Staub, Verschmutzung, Feuchtigkeit und Stürze, kurz "unsachgemäße Behandlung", sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Die Daten eines mobilen Gerätes können temporär nicht verfügbar sein, weil der Akku leer ist, da vergessen wurde, ihn aufzuladen. Sie können unter Umständen, wie z.B. bei älteren Geräten, aber auch vollständig vernichtet sein, wenn neben dem Akku auch die eventuell vorhandene Sicherungsbatterie leer ist und damit alle nicht bereits synchronisierten Daten verloren sind.
- Auch bei der Synchronisation von mobilen Datenträgern und Geräten mit anderen IT-Systemen können Daten zerstört werden. Im Allgemeinen muss vor einer Synchronisation eingestellt werden, wie mit Konflikten beim Datenabgleich umzugehen ist: ob beispielsweise bei gleichlautenden Dateien
  - die des mobilen Endgerätes oder des anderen Endgerätes ungefragt übernommen werden,
  - die neueste Datei übernommen wird oder ob
  - eine Abfrage erfolgt.

Dies wurde häufig bei Inbetriebnahme der Dockingstation einmal konfiguriert und gerät danach wieder in Vergessenheit. Werden dann aber Daten in einer anderen Reihenfolge geändert als ursprünglich einmal gedacht, gehen dabei schnell wichtige Informationen verloren. Zu diesem unangenehmen Nebeneffekt kann es auch kommen, wenn mehrere Benutzer ihre mobilen Endgeräte

mit demselben Endgerät synchronisieren, ohne daran zu denken, dass gleichnamige Dateien dabei überschrieben werden können.

# G 4.53 Unsichere Default-Einstellungen bei Speicherkomponenten

Speicherkomponenten werden von Herstellern oft mit unsicheren Default-Konfigurationen ausgeliefert, die den sicheren Einsatz gefährden.

Folgende Aspekte sind häufig problematisch:

**Betriebssystem**

Speichersysteme werden oft mit einem veralteten Versionsstand des Betriebssystems ausgeliefert. Dieser entspricht oft nicht dem aktuellen Sicherheitsstand.

**Hostname**

Voreingestellte Hostnamen verraten oft den Hersteller der Geräte. Dadurch könnten gezielte Angriffe auf bekannte Sicherheitslücken dieser Geräte gestartet werden.

**Dienste**

Werkseitig werden Geräte mit Standardkonfigurationen ausgeliefert, auf denen eine Vielzahl von Diensten aktiviert sind. Beispielsweise können dies HTTP, Telnet, FINGER oder sonstige Dienste sein, die aus Sicherheitsgründen bei Speichersystemen nicht aktiviert sein sollten.

**Benutzerkonten und Passwörter**

Vom Hersteller eingerichtete Benutzerkonten haben oft dokumentierte und damit allgemein bekannte Standardnamen und -passwörter. Auf einschlägigen Internet-Seiten stehen Listen mit herstellerspezifischen Standard-Accounts und Passwörtern zum Download bereit, so dass hierüber ein einfacher Zugriff auf die Systeme für Unbefugte möglich ist.

**Unsichere SNMP-Versionen**

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten sogenannten Community Strings. Als Standardeinstellung bei nahezu allen Herstellern ist der Read-Community-String auf den Wert "public" eingestellt, während der Write-Community-String auf den Wert "private" gesetzt ist. Wenn die unsicheren SNMP-Versionen genutzt werden und für die Administration kein eigenes Administrationsnetz eingerichtet wurde, kann ein Angreifer leicht die Kontrolle über Netzkomponenten erlangen, wenn diese Default-Einstellungen beibehalten werden.

# G 4.54 Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS

Das verschlüsselnde Dateisystem (*Encrypting File System,* EFS) ab Windows Server 2003/XP ist ein für Benutzer einfach zu bedienendes Mittel, damit Anwendungen transparent mit verschlüsselten Dateien arbeiten können. Es eignet sich am besten für einzelne Benutzer und exponierte Client-Computer, die zeitweise außerhalb der geschützten IT-Umgebung zum Einsatz kommen. Die Hauptintention bei EFS ist es, die Vertraulichkeit von dedizierten lokalen Daten zu schützen.

Die in G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung* genannten Gefährdungen können in vielfältiger Art und Weise dazu führen, dass EFS-Zertifikate, welche zur Ver- und Entschlüsselung verwendet werden, offen gelegt werden oder abhanden kommen. Auf einem Dateiserver wären dann große Datenmengen nicht mehr vertraulich oder nicht mehr verfügbar, was im Vergleich zu einem einzelnen Client fatal sein kann. Auf einem Server spielt auch Datenverlust beim Kopieren oder Verschieben von Daten eine erhebliche Rolle und kann zum Verlust oder zur Beschädigung größerer Datenmengen führen. Wenn sich Administratoren solcher Effekte und den komplexen Anforderungen nicht ausreichend bewusst sind, kann die durch ein aktiviertes EFS beabsichtigte höhere Sicherheit leicht verloren gehen. Kommt aufgrund der vermeintlichen Sicherheit noch Fahrlässigkeit bei Benutzern und Administratoren hinzu, sind kritische Daten sogar stärker bedroht als ohne aktiviertes EFS. Im Folgenden werden einige Teilaspekte genauer erläutert.

Mit EFS ist es nicht möglich, die Vertraulichkeit von verschlüsselten Daten auf Remote-Servern gegenüber Administratoren zu garantieren. Ein Administrator kann sich jederzeit die Möglichkeit verschaffen, mittels Berechtigungen und dem integrierten Wiederherstellungsverfahren auf verschlüsselte Daten zuzugreifen.

EFS ist vollständig transparent für Benutzer und Anwendungen. Das bedeutet, dass jeder Prozess und jede Anwendung, die im Kontext des Benutzers ausgeführt wird, Zugriff auf die verschlüsselten Dateien hat. EFS stellt somit keinen Schutz vor Schadsoftware wie Trojanischen Pferden und Viren dar. EFS ersetzt nicht die sorgfältige Administration der Zugriffsberechtigungen (*Access Control Lists*, ACL) des NTFS. Verschlüsselte Dateien können von Benutzern oder Anwendungen unabhängig vom Schutz durch EFS gelöscht werden, wenn sie über ausreichende NTFS-Berechtigungen verfügen.

Die Transparenz geht soweit, dass Benutzer im Allgemeinen nicht wissen, ob Daten ver- oder entschlüsselt sind. Eine Verschlüsselung liegt aber nur auf NTFS-formatierten Datenträgern vor. Beim Kopieren und Verschieben auf Speichermedien mit anderen Dateisystemen werden die Dateien unverschlüsselt abgespeichert.

**Fehlende Kontrolle über EFS-Zertifikate**

EFS erfordert ein definiertes zentrales Schlüsselmanagement. Ohne den Einsatz einer *Public Key Infrastructure* (PKI) werden selbstsignierte Zertifikate des lokalen Computers (Client oder Server) benutzt. Damit stellt EFS ein nicht unerhebliches Risiko dar, durch Schlüsselverlust den Zugriff auf die verschlüsselten Dateien zu verlieren.

Werden von einem Client aus Daten mittels EFS auf einem Server verschlüsselt, der Mitglied in einer Domäne ist, muss dieser Server im Namen des Client-Benutzers ein EFS-Zertifikat anfordern. Das ist nur möglich, wenn dem Domänenkonto des Servers erweiterte Berechtigungen eingeräumt werden. Dem Serverobjekt innerhalb der Domäne wird für Delegierungszwecke vertraut. Diese "Stellvertretung" und das "Vertrauen" lassen sich mit dem Kerberos-Protokoll realisieren, designbedingt wird dadurch allerdings die Sicherheit der Kerberos-Umgebung verringert. Im Falle einer Kompromittierung des vertrauten Servers kann der Angreifer Einfluss auf benutzerspezifische Daten nehmen. Sind die Einstellungen zum Vertrauen nicht korrekt konfiguriert und auf EFS-relevante Dienste beschränkt, ergeben sich auch Manipulationsmöglichkeiten in anderen Bereichen des Servers oder der Domäne.

Werden EFS-Zertifikate auf dem Remote-Server oder im Active Directory erzeugt, ist es außerdem schwieriger, das Schlüsselmaterial zu verwalten und zu schützen.

**Nutzung des EFS-API**

Greift eine Anwendung auf verschlüsselte Dateien zu, welche für mehrere Benutzer verschlüsselt wurden, muss die Anwendung das entsprechende Application Programming Interface (API), das ab Windows Server 2003/Windows XP verfügbar ist, unterstützen. Anderenfalls werden die Schlüssel der zusätzlichen Benutzer von den Dateien entfernt. Kein Benutzer außer dem ursprünglichen Erzeuger hat dann noch Zugriff auf die jeweilige Datei. Sicherungs-, Archiv- und Synchronisierungs-Tools von Drittherstellern bergen ähnliche Risiken, sobald sie zur Verarbeitung verschlüsselter Dateien zum Einsatz kommen.

# G 4.55 Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP

Windows-Betriebssysteme ab Server 2003 und Windows XP schützen die privaten Schlüssel lokaler Benutzerkonten vor der Verwendung durch Administratoren. "Lokales Benutzerkonto" bedeutet, dass Benutzername und Kennwort des Kontos nur auf dem jeweiligen Computer existieren und verwendet werden können. In früheren Windows-Versionen konnte ein Administrator das Kennwort eines lokalen Benutzerkontos zurücksetzen und anschließend die privaten Schlüssel des Benutzers verwenden und exportieren. Ab Windows Server 2003/XP löscht das Krypto-API alle für ein solches Benutzerkonto gespeicherten privaten Schlüssel, sobald das Kennwort durch einen Administrator zurückgesetzt wird. Durch dieses Verhalten ist es möglich, höchstvertrauliche Informationen selbst vor Administratoren zu verbergen. Jedoch sind nach dem Zurücksetzen durch einen Administrator alle privaten Schlüssel verloren, wenn keine Sicherungskopie erstellt wurde. Verschlüsselte Daten in E-Mails und Dateien sind dann nicht mehr verfügbar.

Dieses Verhalten kann auch zum Verlust des privaten Schlüssels des Wiederherstellungsagenten für das Encrypting File System (EFS) führen, wenn der Wiederherstellungsagent einem lokalen Benutzerkonto zugewiesen wurde. In diesem Fall ist ein Wiederherstellungsagent konfiguriert. Da aber kein Zugang zu den Schlüsseln des Benutzerkontos möglich ist, kommt dieses Szenario einem nicht vorhandenen Wiederherstellungsagenten gleich. Die Daten der Benutzer, die ihren eigenen Schlüssel nicht mehr nutzen können, wären in diesem Fall verloren.

# G 4.56 Ausfall der VoIP-Architektur

VoIP kann als Alternative zu einer leitungsvermittelnden TK-Anlage eingesetzt werden. Alle Gespräche, also alle eingehenden, ausgehenden und internen Telefonate, können vollständig über VoIP abgewickelt werden. Es kann sowohl das bestehende, als auch ein hierfür separat betriebenes Datennetz für die Kommunikation genutzt werden.

Ein IP-Netz besteht aus aktiver und passiver Netztechnik. Unter passiver Netztechnik wird in erster Linie die strukturierte Verkabelung verstanden. Zur aktiven Netztechnik gehören beispielsweise Hubs, Bridges, Switches und Router. Ein Ausfall einer oder mehrerer Komponenten der aktiven Netztechnik kann zum kompletten Stillstand des gesamten IT-Netzes führen. In einem solchen Fall ist die VoIP-Architektur ebenfalls nicht mehr nutzbar, wenn sie über dasselbe IT-Netz abgewickelt wird.

Hat ein Angreifer direkten Zugang zum LAN, beispielsweise durch Anschluss an einen Switch oder über ein drahtloses Netz, kann er unter Umständen bestehende Verbindungen beenden. Ein Beispiel hierfür ist eine mit dem Session Initiation Protocol (SIP) oder H.323 initiierte TCP-Verbindung, die mit einem IP-Paket mit gesetztem RST-Flag beendet wird.

Durch Techniken wie Flooding könnte ein Angreifer das Datennetz überlasten. Dies betrifft jedoch nicht nur VoIP-Architekturen. Praktisch jeder Nachrichtenstrom kann auf diese Weise gestört werden.

Der Betrieb der VoIP-Architektur erfordert in der Regel den Einsatz von Komponenten für die Vermittlung der Telefonate. Beispiele hierfür sind H.323-Gatekeeper und SIP-Registrare. Diese VoIP-Middleware kann auf separaten IT-Systemen oder dedizierten Hardware-Elementen betrieben werden. Die Integration dieser Geräte in IT-Netze führt zu neuen Bedrohungen, verglichen mit leitungsvermittelnden TK-Anlagen, die eine eigene Kabelinfrastruktur voraussetzen. So könnten VoIP-Komponenten über das IP-Netz beispielsweise durch Würmer kompromittiert werden und dadurch ausfallen.

Um VoIP nutzen zu können, müssen sich die Benutzer in der Regel an einem entsprechenden System, beispielsweise einem Registrar bei SIP oder einem Gatekeeper bei H.323, anmelden. Ohne entsprechende Sicherheitsmechanismen kann ein Angreifer einen Benutzer durch gefälschte Pakete wieder abmelden (De-Registration). Dies hat zur Folge, dass dieser Benutzer nicht mehr telefonisch erreichbar ist.

Die Vermittlungseinheiten sind ein besonders attraktives Ziel für Angriffe, da beim Ausfall eines solchen Systems zahlreiche Benutzer nicht mehr telefonieren können. Hat ein Angreifer beispielsweise physischen Zugriff auf eine Vermittlungseinheit, kann er diese zentrale Architektur manipulieren, beschädigen oder einfach ausschalten. Aber auch durch logische Angriffe auf Vermittlungseinheiten, zum Beispiel durch Zurücksetzen von Netzverbindungen oder Löschen wichtiger Systemdateien, können unter Umständen hohe Schäden entstehen.

Diese erhöhte Gefährdungslage gilt auch für VoIP-Endgeräte. Für Angriffe auf vernetzte IT-Systeme, deren Gefährdungslage den VoIP-Geräten ähnlich ist, wurden viele Werkzeuge entwickelt. Diese Programme können häufig auch von weniger erfahrenen Angreifern eingesetzt werden. Durch eine Auswertung verschiedener Netzparameter, wie die Antwort auf bestimmte IP-Pakete, kann bei einigen Geräten die genaue Typbezeichnung des Endgeräts ermit-

telt werden. Diese Informationen können für zielgerichtete Angriffe verwendet werden.

Sowohl die VoIP-Endgeräte als auch die Middleware besitzen einen hohen Software-Anteil. Es besteht daher das Risiko, dass diese Software Schwachstellen besitzt, die von Angreifern ausgenutzt werden können. VoIP-Geräte können deshalb auch anfällig für Schadsoftware, beispielsweise für Computer-Viren oder -Würmer, sein.

Die Verfügbarkeit kann außerdem durch unvorhergesehene Ereignisse beeinträchtigt werden. Telefone für leitungsvermittelnde Netze erhalten ihre Betriebsspannung häufig direkt über das Telefonnetz. Wird eine TK-Anlage für leitungsvermittelnde Netze mit einer lokalen USV bei einem Stromausfall versorgt, können die Endgeräte weiterhin ihre Betriebsspannung hierüber beziehen. VoIP-Endgeräte beziehen ihre Stromversorgung hingegen in der Regel nicht vom IT-Netz, sondern separat. Auch wenn die VoIP-Anlage über eine USV versorgt wird, können die Endgeräte bei einem Stromausfall nicht verwendet werden. Hinzu kommt, dass auch ein Ausfall der aktiven Netztechnik dazu führt, dass das Datennetz nicht funktionsbereit ist und somit keine VoIP-Telefonate mehr möglich sind.

# G 4.57 Störungen beim Einsatz von VoIP über VPNs

Für ein Telefonat über VoIP werden sowohl die Signalisierungsinformationen als auch der eigentliche Medienstrom über ein Datennetz gesendet. Für die Transportsicherung dieser Daten auf Protokollebene gibt es Schutzmechanismen, die jedoch nicht von allen Herstellern und Geräten unterstützt werden. Das Verfahren zum Schutz der eigentlichen Sprachkommunikation wird in der Regel von den Endgeräten ausgehandelt. Hierfür kann beispielsweise das Secure Realtime Transport Protocol (SRTP) verwendet werden.

Unterstützen nicht alle Geräte verschlüsselte Protokolle und sollen Gespräche über unsichere Netze übertragen werden, können Virtual Private Networks (VPNs) diesen Schutz gewährleisten. VPNs werden in der Praxis zur Einbindung von einzelnen Mitarbeitern oder zum Zusammenschluss ganzer Netze über ein öffentliches Netz genutzt. Beim Einsatz von VPNs werden ausgewählte oder alle Pakete von einem VPN-Gateway verschlüsselt und je nach Routing-Tabelle an ein entferntes VPN-Gateway übermittelt. Dieses entschlüsselt das Paket und übermittelt es an den Empfänger. Dadurch wird außerdem erreicht, dass sich Sender und Empfänger im gleichen Subnetz befinden, obwohl sie mehrere hundert Kilometer voneinander entfernt sein können.

Durch den Einsatz eines VPNs können sowohl der Signalisierungs- und Medienstrom von VoIP als auch alle weiteren Informationen, wie beispielsweise E-Mails, geschützt werden. Einige Hardphones unterstützen VPNs direkt. Wird ein verschlüsseltes Medientransportprotokoll, wie zum Beispiel SRTP, verwendet, ist es ausreichend, wenn nur der Signalisierungsstrom durch das VPN geschützt wird.

Der Einsatz von VPNs in Verbindung mit VoIP führt jedoch häufig zu Problemen.

Bei Netzen, die neben VoIP-Daten auch andere Informationen übertragen, werden an den Routern und Switches oft VoIP-Nachrichten bevorzugt weitergeleitet. Durch dieses Vorgehen sollen Qualitätsstörungen, wie Aussetzer oder Jitter, vermieden werden. Obwohl hierfür bei IPv4 ein eigenes Feld im IP-Header vorgesehen ist (Type of Service), wird es in der Praxis häufig nicht verwendet. Stattdessen priorisieren die Router die Pakete an Hand ihres Inhalts. Bei einer Verschlüsselung des Inhalts ist dies aber nicht mehr möglich. Als Folge kann es bei der Übertragung von VoIP über VPNs vermehrt zu Störungen der Übertragungsqualität kommen, wenn das Netz zu stark ausgelastet ist.

Die Verwendung von Hiding NAT (Network Address Translation oder Masquerading) kann ebenfalls zu Problemen führen. Im Gegensatz zu statischen NAT wird nicht jeder internen IP-Adresse genau eine öffentliche IP-Adresse zugeordnet, sondern mehrere interne Adressen können eine öffentliche IP-Adresse parallel nutzen. Für dieses Verfahren müssen nicht nur die internen IP-Adressen, sondern auch die Portnummern im IP-Paket durch das NAT-Gateway geändert werden. Diese Änderungen führen dazu, dass die vom VPN-Gateway erzeugte Prüfsumme nicht mehr zu dem neuen Paket passt. Wird die gesamte IP-Nutzlast verschlüsselt, kann dies auch zu Problemen führen.

Pakete, die zur Übermittlung von VoIP-Inhalten genutzt werden, sind meist sehr klein. Würde mit der Übermittlung gewartet werden, bis sich eine bestimmte Anzahl von Bytes angesammelt haben, könnte eine zu große Verzögerung bei der Übertragung entstehen. So ist die eigentliche Nutzlast der IP-

Pakete in der Regel zwischen 10 und 40 Bytes groß. Sollen die IP-Pakete durch ein VPN geschützt werden, kommt zusätzlich ein VPN-Header hinzu. Bei IP-Paketen mit einem geringen Umfang stellen die hinzukommenden VPN-Informationen einen signifikanten Overhead dar. Als Folge ergibt sich durch die Aktivierung der VPN-Absicherung eine deutliche Erhöhung des VoIP-Datenaufkommens. Dies kann zu einer Überlastung des LANs oder des WANs führen.

Auch die Ver- und Entschlüsselung der übertragenen Informationen benötigen Ressourcen. Ist das System, dass die Ver- oder Entschlüsselung vornimmt, schwach dimensioniert, kann an dieser Stelle ebenfalls eine Verzögerung in der Übertragung auftreten. Eine solche Erhöhung der Latenzzeit kann zu Aussetzern oder anderen Qualitätsproblemen führen.

Viele Verschlüsselungsarchitekturen für VPN nutzen X.509-Zertifikate oder Pre-Shared-Secrets. Besonders für die zertifikatsbasierte Lösung setzen viele Hersteller derzeit auf proprietäre Ansätze, die untereinander nicht kompatibel sind. Wenn VoIP-Verbindungen zu externen Partnern aufgebaut werden sollen, kann mit diesen daher nicht oder nicht verschlüsselt telefoniert werden.

# G 4.58 Schwachstellen beim Einsatz von VoIP-Endgeräten

Bei VoIP-Endgeräten werden zwei Arten unterschieden: Hardphones und Softphones. Hardphones sind eigenständige Geräte mit meistens proprietären Betriebssystemen, die direkt an das IP-Netz angeschlossen werden. Einige Hardphones laden ihre aktuelle Konfiguration über das TFTP-Protokoll.

Softphones sind auf dem Computer installierte Anwendungsprogramme, deren Funktionalität der eines Hardphones entspricht. Für den Zugang zum IP-Netz benutzen Softphones die Schnittstelle des Computers, die sie mit anderen installierten Anwendungen teilen.

Alle VoIP-Endgeräte bieten im Wesentlichen ähnliche Funktionen an, die von Programmen mit Schadensfunktionen beeinträchtigt werden können. Das Bedrohungsspektrum erstreckt sich dabei von der partiellen Beeinträchtigung des Normalbetriebs bis zu einer vollständigen Übernahme der Kontrolle über das Gerät durch den Angreifer.

Bei mangelhaften Sicherheitsvorkehrungen kann es zur Ausbreitung von Schadsoftware, wie Trojanischen Pferden, kommen. Trojanische Pferde könnten bei der VoIP-Nutzung beispielsweise benutzt werden, um private Informationen eines Teilnehmers oder Gesprächsinhalte während des Gesprächs an einen Angreifer zu übermitteln.

Schadprogramme könnten auch versuchen, Anrufe ohne Wissen des Anwenders zu initiieren oder Informationen über die geführten Telefonate sowie private Telefonnummern aus dem Adressbuch zu ermitteln und weiterzuleiten.

Wird ein Anruf vom Anwender initiiert, so bauen Geräte die Verbindung gemäß der eingestellten Konfiguration und der gewählten Telefonnummer auf. Manipulationen an der Konfiguration oder Firmware des Geräts können zur Störung des Anwahlprozesses oder sogar zur Umleitung des Gesprächs über die Angreiferinfrastruktur führen. Damit kann der Angreifer das darauf folgende Gespräch unter Umständen auch abhören.

Beendet der Anrufer das Gespräch, so könnte ein infiziertes Gerät die Signalisierung des Gesprächsendes vortäuschen, während die Verbindung im Hintergrund aufrecht erhalten wird. Diese Verbindung könnte zum Abhören des Benutzers genutzt werden. Ist ein Gerät von Schadsoftware befallen, so könnte diese möglicherweise auch die Signalisierung von ankommenden Anrufen unterdrücken, ohne dass der Angerufene es merkt. Dies hätte zur Folge, dass der Benutzer nicht mehr angerufen werden kann.

Eine weitere potentielle Angriffsvariante durch Schadsoftware besteht darin, das Mikrofon eines VoIP-Endgerätes unbemerkt zu aktivieren, um die Gespräche im Raum aufzuzeichnen und per VoIP an den Angreifer zu übermitteln. Der Aufwand zur Programmierung einer entsprechenden Schadsoftware mit einer solchen Funktionalität ist dabei relativ gering, weil die benötigte VoIP-Funktionalität (Codec, VoIP-Protokolle) bereits auf den Endgeräten implementiert ist und von der Schadsoftware genutzt werden kann.

In welchem Maße die beschriebenen Risiken tatsächlich bei einem Gerät auftreten, hängt von mehreren Faktoren ab, wie z. B. Art und Einstellungen des Betriebssystems, Verwendung von gemeinsamen Ressourcen mit anderen

Anwendungen (z. B. bei Softphones), und implementierten Schutzmechanismen.

Generell lässt sich sagen, dass Softphones für Angriffe von Programmen mit Schadensfunktionen anfälliger sind als Hardphones, weil Softphones meist auf weit verbreiteten Betriebssystemen basieren und Ressourcen mit anderen installierten Anwendungen teilen, die eigene Sicherheitslücken haben können. Dagegen haben Hardphones eine eigene Netzschnittstelle und basieren meist auf proprietären Betriebssystemen, deren Einstellungen auf die geforderte Funktionalität zugeschnitten sind. Somit können sie in der Regel nur den Angriffen von schädlichen Programmen ausgesetzt werden, die speziell für solche Betriebssysteme entwickelt worden sind.

# G 4.59 Nicht-Erreichbarkeit bei VoIP durch NAT

Über seine IP-Adresse kann ein Rechner im Internet eindeutig angesprochen werden. Bei dem zur Zeit hauptsächlich verwendeten Internet Protocol in der Version 4 (IPv4) setzt sich die IP-Adresse aus vier Zahlen zwischen 0 und 255 zusammen, also zum Beispiel 194.95.176.226. Bei dem neueren Internet Protocol in der Version 6 (IPv6) besteht eine IP-Adresse aus acht vierstelligen hexadezimalen Zahlen, wie FEDC:BA98:7654:3210:FEDC:BA98:7654:3210. Ein großer Nachteil der Version 4 gegenüber der Version 6, die sich bisher noch nicht durchgesetzt hat, ist die geringe Anzahl von verfügbaren öffentlichen IP-Adressen. Nur sehr wenige Institutionen erhalten genug IP-Adressen, um jedem Arbeitsplatzrechner eine eigene, statische IP-Adresse zuweisen zu können. Durch Network Address Translation (NAT) kann dieses Problem behoben werden. Dabei benötigt nur das System, das sich zwischen dem öffentlichen und dem privaten Netz befindet, eine oder wenige öffentliche IP-Adressen. Die eigentlichen Arbeitsplatzrechner erhalten interne IP-Adressen, wobei von einer aktiven Netzkomponente (meistens ein NAT-Gateway) bei der Weiterleitung eines Paketes die interne in eine externe IP-Adresse umgewandelt wird.

Für den Medienstrom, der für die Übertragung der Sprachinformation benötigt wird, muss eine neue UDP- bzw. TCP-Verbindung aufgebaut werden. Die hierfür benötigten IP-Adressen und Portnummern werden in den Signalisierungsnachrichten übertragen. Durch NAT werden im UDP- bzw. TCP-Header des Medienstroms die Quell-IP-Adresse im IP-Header und die Quellportnummer modifiziert. Die Angaben über die Quell-IP-Adresse und die Portnummer im Nachrichtenteil der Signalisierungsnachricht bleiben unverändert.

In Folge können keine Medienströme an das VoIP-Telefon, das sich hinter einem NAT-Gateway befindet, gesendet werden. VoIP-Geräte, die sich im Internet befinden, können keinen Medienstrom zu einem hinter einem NAT-Gateway befindlichen VoIP-Telefon senden, da die private IP-Adresse nicht im Internet geroutet wird. Eine Sprachkommunikation ist somit zu VoIP-Geräten, die sich hinter einem NAT-Gateway befinden, weil eine sicherheitskritische Konfiguration erreicht werden soll, nicht möglich, obwohl bei der Signalisierung keine Fehler aufgetreten sind.

Eine Ausnahme bilden Protokolle wie beispielsweise IAX (InterAsterisk eXchange) oder Skype. Bei diesen Protokollen findet sowohl die Signalisierung als auch der Medientransport über eine bestehende Verbindung statt. Da keine zusätzlichen Verbindungen zu den Rechnern im privaten Netz aufgebaut werden müssen, treten die beschriebenen Probleme mit NAT bei dem Einsatz dieser Protokolle nicht auf. Da hiermit aber auch keine Kontrolle am Netzübergang mehr stattfindet, können dadurch andere Sicherheitsprobleme entstehen.

Um eine VoIP-Kommunikation über ein NAT-Gateway hinweg zu ermöglichen, kann der Medienstrom des NAT-Gateways zu den VoIP-Geräten statisch weitergeleitet werden. Dieser Lösungsansatz ist oft bei der Anbindung privater Kunden an SIP-Providern zu finden. Dies kann allerdings zu Problemen führen. Hier baut der Sender, der sich außerhalb des LANs befindet, eine Verbindung zu dem NAT-Gateway über eine reservierte Portnummer auf. Das NAT-Gateway leitet diese zu einem Endgerät, das der Portnummer zugeordnet ist, weiter. Dies setzt voraus, dass die Gesprächsteilnehmer die reservierten Portnummern kennen. Gravierender ist der Nachteil, dass auf die weitergeleiteten

Ports der VoIP-Systeme hinter dem NAT-Gateway aus dem öffentlichen Datennetz zugegriffen werden kann.

# G 4.60 Unkontrollierte Ausbreitung der Funkwellen

Funknetze bzw. die ausgesendeten Funkwellen überschreiten nicht selten die Grenzen der selbstgenutzten Räumlichkeiten, so dass Daten auch noch in Bereiche übertragen werden, die nicht vom Benutzer oder einer Institution kontrolliert und gesichert werden können. Eine Aufzeichnung ist somit ohne viel Aufwand möglich und die Entdeckung solcher Lauschangriffe wird nur bei einem Bruchteil der Fälle erfolgen. Ziel solcher Angriffe kann es sein, sensitive Informationen zu erlangen oder zu manipulieren. Selbst wenn die Daten verschlüsselt übertragen werden, reicht es durch den unzureichenden Schutz vieler drahtloser Netze häufig aus, eine Zeitlang den Funkverkehr aufzuzeichnen und auszuwerten, um anschließend mit den gesammelten Daten die kryptographischen Schlüssel berechnen zu können und so die übertragenen Daten zu entschlüsseln. Durch den Einsatz von Richtantennen könnten zudem auch außerhalb der eigentlichen Nutzreichweite des Funknetzes Daten empfangen und abgehört werden.

**Beispiel:**

Ein Laptop mit WLAN-Karte zusammen mit einigen frei verfügbaren WLAN-Applikationen reicht aus, um nach schlecht gesicherten WLANs zu suchen. Beim Wardriving wird beispielsweise mit einem WLAN-Client eine bestimmte Region, ein Stadtviertel oder typische Büroumgebung abgefahren und dabei aufgezeichnet, wo sich welche WLANs melden und wie schlecht diese gesichert sind. Dabei können diese Daten auch direkt mit GPS-Daten verknüpft werden, um die geographische Position der gefundenen WLANs festhalten zu können. Anschließend können schlecht gesicherte WLANs gezielt angegriffen werden, z. B. um darüber kostenlos auf das Internet zugreifen zu können.

# G 4.61 Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen

Im Auslieferungszustand sind die WLAN-Komponenten häufig so konfiguriert, dass keine oder nur einige Sicherheitsmechanismen aktiviert sind. Einige der Mechanismen sind darüber hinaus unzuverlässig und bieten keinen ausreichenden Schutz. Auch heute noch sind diverse WLAN-Komponenten im Einsatz bzw. als Neugeräte am Markt verfügbar, die lediglich unzureichende Sicherheitsmechanismen wie z. B. WEP unterstützen. Teilweise können diese Geräte nicht einmal auf stärkere Sicherheitsmechanismen aufgerüstet werden.

Können keine oder nur schwache Mechanismen genutzt werden, mit denen sich die Funkschnittstelle bzw. die über das WLAN genutzten Dienste angemessen absichern lassen, ist keine sichere Kommunikation im WLAN möglich. Hierdurch ergeben sich weitere Gefahren für alle damit gekoppelten Komponenten, also z. B. alle auf einem WLAN-Client gespeicherten Daten oder ein LAN, was die gesamte IT-Infrastruktur einer Behörde oder eines Unternehmens beeinträchtigen kann. Im Folgenden werden mögliche Sicherheitsprobleme exemplarisch aufgeführt.

**WEP**

Wird die Funkübertragung im WLAN gar nicht oder nur mit WEP geschützt, kann ein Angreifer leicht die gesamte WLAN-Kommunikation abhören und damit nicht selten in den Besitz vertraulicher Informationen gelangen. Beim Einsatz einiger Geräte wie WLAN-fähigen Druckern wird vielfach nicht wahrgenommen, dass hiermit ein WLAN aufgebaut wird und dieses somit auch nicht adäquat abgesichert. Ein Angreifer könnte aber eventuell nicht nur die gedruckten Daten abhören, sondern über die WLAN-Komponente auf Hintergrundsysteme zugreifen.

**SSID Broadcast**

Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID (Service Set Identifier oder Netzname) dazu, den nächsten Access Point zu finden. Einige Access Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das WLAN vor Unbefugten zu verstecken (so genanntes "Closed System"). Allerdings kann mittels WLAN-Analysatoren auch in diesem Falle die SSID aus anderen Management- und Steuersignalen ermittelt werden.

**Manipulierbare MAC-Adressen**

Jede Netzkarte verfügt über eine eindeutige Hardware-Adresse, die sogenannte MAC-Adresse (Media Access Control-Adresse). Die MAC-Adressen der WLAN-Clients können relativ einfach abgehört und manipuliert werden, somit sind die in den Access Points zum Zweck des Zugriffsschutzes häufig eingebauten MAC-Adressfilter überwindbar.

**Fehlendes Schlüsselmanagement**

Kryptographische Schlüssel müssen in vielen WLANs manuell verteilt werden, d. h. in jedem WLAN-Client und Access Point muss der gleiche statische Schlüssel eingetragen werden. Dies erfordert physischen Zugriff auf die Komponenten. Diese Art des Schlüsselmanagements führt in der Praxis oft dazu, dass die kryptographischen Schlüssel sehr selten oder überhaupt nicht ge-

wechselt werden. Wenn dann ein WLAN-Schlüssel offengelegt wird, wird das gesamte WLAN kompromittiert.

**Schwachstellen beim administrativen Zugriff auf Access Points**

Viele Access Points bieten unterschiedliche Schnittstellen und Protokolle zur Administration an und erlauben es, diese sowohl über die LAN-, als auch über die Funkschnittstelle zu verwenden. Erfolgt die Administration über die Funkschnittstelle über Klartext-Protokolle, wie Telnet, HTTP oder SNMP, können die über das WLAN übertragenen Administrationspasswörter mitgelesen werden. Angreifer könnten diese Informationen zum Umkonfigurieren des Access Points nutzen.

Verschlüsselte Varianten der genannten Zugriffsprotokolle werden häufig auf der Access-Point-Seite nicht unterstützt bzw. nicht erzwungen.

# G 4.62 Verwendung unzureichender Steckdosenleisten

Oft reicht die Zahl fest installierter Steckdosen für die Menge der zu betreibenden Geräte nicht aus. Um diesen Mangel auszugleichen, werden dann typischerweise Steckdosenleisten verwendet. Solche Steckdosenleisten stellen, wenn sie von unzureichender Qualität sind, auf Grund

- mangelhafter Kontaktierung,
- zu schwacher Kontaktfedern,
- fehlender Zugentlastung,
- eines zu geringem Leitungsquerschnitts,
- von Überlastung

eine gefährliche Zündquelle und damit eine große Brandgefahr dar.

Werden zusätzlich mehrere kleinere Steckdosenleisten hintereinander geschaltet, um ausreichende Steckplätze für alle Geräte bereitzustellen, steigt die Gefahr durch zu geringen Leitungsquerschnitt und Überlastung weiter an.

Liegen Steckdosenleisten im Fußraum von Arbeitsplätzen, sind sie häufigen mechanischen Belastungen durch Gegentreten, Staubsaugen etc. ausgesetzt. Dadurch können fehlende Zugentlastungen und schwache Kontakte rasch zu Übergangswiderständen, Überhitzungen und schließlich zum Brand führen. Darüber hinaus sind solche frei ausliegenden Steckdosenleisten gefährliche Fußangeln.

**Beispiel:**

In einer Niederlassung einer Versicherung ereignete sich ein Schwelbrand aufgrund des Defekts einer privat beschafften Steckdosenleiste. Mitarbeiter hatten im Herbst zusätzlich zu PC und Drucker einen Heizlüfter angeschlossen. Als dieses Gerät versehentlich während einer Betriebsversammlung in höchster Stufe weiterlief, verschmorte das Gehäuse der überlasteten Steckdosenleiste.

# G 4.63 Verstaubte Lüfter

IT-Geräte sollen, wie alle anderen elektrischen Geräte auch, nur innerhalb einer vom Hersteller festgelegten Temperaturspanne betrieben werden. Die Einhaltung der Minimaltemperatur stellt in der Regel keine besonderen Anforderungen. Hingegen müssen meist zusätzliche Einrichtungen betrieben werden, um die Maximaltemperatur einhalten zu können. Den meisten dieser Einrichtungen ist gemeinsam, dass die überschüssige Wärme mittels Lüftern abgeführt wird.

Es befindet sich immer ein gewisser Staubanteil in der Umgebungsluft, auch in der Raumluft von normalen Büro- oder Serverräumen. Da sich dieser zum Teil an Lüftern absetzt, bilden sich dort mit der Zeit meist ansehnliche Staubpolster. Diese Staubansammlungen können

- den Luftdurchsatz und damit die Kühlwirkung der Lüfter so weit reduzieren, dass Geräte überhitzen und ausfallen oder (vornehmlich bei Netzteilen) sich entzünden.
- den freien Lauf des Lüfters bremsen oder komplett unterbinden, wodurch der nun blockierte Lüftermotor selbst überhitzt und zur Zündquelle wird.

# G 4.64 Komplexität von Druckern, Kopierern und Multifunktionsgeräten

Netzdrucker, Hochleistungskopierer und Multifunktionsgeräte sind mittlerweile komplexe IT-Systeme. Sie bieten nicht nur eine umfangreiche Ausstattung und einen erweiterten Funktionsumfang, sondern können dadurch auch neue Gefährdungen für andere IT-Systeme oder das LAN mit sich bringen.

**Lokale Administrationsschnittstellen**

Bei einigen Druckern und Multifunktionsgeräten kann der Zugriff auf die Administrationsschnittstelle nicht abgesichert werden, also auch nicht über eine Passwortabfrage vor unbefugtem Zugriff geschützt werden. Mit Administratorrechten könnte ein Angreifer den Drucker manipulieren, beispielsweise so, dass er keine Druckaufträge annimmt oder alle empfangenen Druckaufträge auf einen internen Speicher zur späteren Einsicht schreibt.

**Administration über das LAN**

Netzdrucker und Multifunktionsgeräte können im Allgemeinen auch über das lokale Netz administriert werden. Wenn hierfür kein Zugriffsschutz möglich ist oder gesetzt wurde, können hierüber Daten im Drucker ausgelesen oder manipuliert werden. Dies ist in manchen Fällen nicht nur von Arbeitsplätzen des lokalen Netzes möglich, sondern auch aus dem Internet. Manche Drucker besitzen sogar eine Java-Engine, die es ermöglicht, beliebige Java-Programme und Java-Applets zur Konfiguration auf dem Drucker zu installieren und auszuführen. Damit eröffnet sich neben der Möglichkeit der Manipulation von Druckereinstellungen und Druckaufträgen ein weites Feld von Angriffen über Drucker auf das lokale Netz.

**Integrierte Webserver**

Viele Netzdrucker und Hochleistungskopierer haben mittlerweile eingebaute Webserver, die die Administration erleichtern sollen. Komfort wird hier aber auch mit zusätzlichen Risiken erkauft. So sind z. B. Drucker mit integriertem Webserver in der Vergangenheit durch einen Nebeneffekt eines Wurm-Angriffes ("Code Red") zum Absturz gebracht worden, obwohl sie für den eigentlichen Angriff des Wurms gar nicht empfindlich waren. Manche Hersteller bieten keine Möglichkeit an, den Webzugriff auf die Druckeradministration abzusichern und beispielsweise nur auf autorisierte Personen zu beschränken. Häufig wird aber auch die Webschnittstelle bei der Konfiguration vernachlässigt, so dass interne oder sogar externe Personen die Druckerkonfiguration und -nutzung manipulieren können, je nach Einbindung in vorhandene Netze. Beispielsweise könnten von beliebigen Benutzern des Druckers absichtlich oder unbeabsichtigt Druckaufträge anderer gelöscht oder die Verfügbarkeit des Druckers beeinträchtigt werden. Manche Webserver von Druckern liefern außerdem bei Angabe einer überlangen URL Diagnosedaten zurück, auf deren Basis die Entwicklung von Angriffsprogrammen möglich ist.

**Unverschlüsselte Kommunikation zur Administration**

Als Protokolle für die Konfiguration werden häufig HTTP(S), Telnet oder SNMP (Simple Network Management Protocol) benutzt.

Bei einem Zugriff über HTTP oder Telnet werden die übertragenen Informationen ungeschützt transportiert. In dem Fall könnte ein Angreifer die Kommuni-

kation und somit beispielsweise das Passwort zur Konfiguration mitlesen und dies für eine Vielzahl von Angriffen auf die Vertraulichkeit, Verfügbarkeit und Integrität benutzen, wenn nicht andere Schutzmaßnahmen dagegen getroffen werden.

Neben der Konfiguration durch den Administrator wird oft gewünscht, dass die Benutzer ebenfalls auf den Webserver von Druckern zugreifen können. Beispielsweise könnten damit die Benutzer ihre Druckaufträge stornieren oder überprüfen, ob der Drucker zur Zeit keine anderen Druckaufträge bearbeitet. Allerdings können sie dabei auch sehen, welche Art von Dokumenten andere Mitarbeiter ausdrucken. Meist sind die Dateinamen der gedruckten Dokumente erkennbar, beispielsweise "Bewerbung_Nachbarfirma.doc". Gelingt es einem Angreifer, im Klartext übermittelte Passwörter der anderen Benutzer mitzulesen, könnte er die Druckaufträge der anderen Benutzer stornieren, sie einsehen oder den Ausdruck auf andere Drucker umlenken. Typischerweise wiederholen Benutzer den Druckvorgang so lange, bis an ihrem Lieblingsdrucker der Ausdruck ankommt. So können in sensitiven Bereichen unbemerkt Dokumente in die Hände von Unberechtigten gelangen.

**Spezielle Druckserverdienste und Einsatzumgebungen**

Verschiedene Hersteller haben auf Netzdruckern eine Adressbuchfunktion für den integrierten E-Mail- oder Faxversand implementiert. Bei Nutzung solcher Funktionen ist es schwierig auszuschließen, dass Daten über den Drucker unberechtigt weitergeleitet werden, z. B. ins Internet.

Viele Drucker lassen sich auch über ftp und mit anonymen Zugriffen über LDAP steuern. Dies kann dann möglicherweise auch von jedem Benutzer im lokalen Netz für Manipulationen am Drucker ausgenutzt werden. Manche Hersteller bieten sogar über das Internet kostenfreie Zusatzsoftware an, mit der ein vergebenes Druckerpasswort für die Konfiguration weitestgehend umgangen werden kann. In den meisten Fällen ist der Zugriff auf die Konfiguration des Druckers nach Auslieferung durch den Hersteller nicht beschränkt. Bei einigen Betriebssystemen können Netzdrucker außer über LDAP über eine Domänenzugehörigkeit konfiguriert werden. Hier besteht die Gefahr, dass Unberechtigte auf LAN-Servern Administrator-Rechte für den Drucker erlangen können.

Für manche Zwecke kann es sinnvoll sein, eine Druckeranbindung per Funknetz oder auch direkt über den Einsatz von Wireless-Printern durchzuführen. Auch für solche Funkübertragungen muss ein angemessener Schutz vor Abhören der Funkstrecken, Verfälschung von Daten, Manipulation der Druckerkonfiguration, Störung der Verbindungen und anderen Sicherheitsproblemen gewährleistet sein.

**Software-Fehler**

Fehler in der Implementierung von Druckertreibern können auch Auswirkungen auf die Sicherheit des Arbeitsplatzrechners haben. So sind Sicherheitslücken aufgetreten, bei denen aufgrund eines fehlerhaften Druckertreibers einfache Benutzer Administratorrechte erlangen konnten.

Der unter Unix häufig verwendete Druckerdämon *lpd* ist in verschiedenen Versionen gegen Pufferüberläufe empfindlich. Dadurch sind beispielsweise Denial-of-Service-Angriffe oder der Start von Programmcode mit Root-Rechten von entfernten Rechnern aus möglich. Eine gefährliche Funktionalität in Windows ME war auch die automatische Druckerinstallation aller im Netz freigegebenen Drucker. Hierbei werden vom fremden Drucker bzw. Betriebssystem

automatisch Dateien auf den Rechner mit Windows ME übertragen und installiert. Ein Angriff mittels ausgeführter *VXD*-Dateien auf das Betriebssystem ist so leicht möglich.

**Beispiele:**

- Ein Angreifer leitet einen bestimmten Ausdruck an einen Drucker um, den der Benutzer sonst nicht verwendet. Auf diese Weise kann der Angreifer auch Dokumente mit einem höheren Schutzbedarf bezüglich der Vertraulichkeit einsehen. Der Benutzer findet den gewünschten Ausdruck nicht im Drucker und vermutet technische Probleme. Ohne daran zu denken, dass es sich um einen Angriff handeln könnte, erstellt der Benutzer einen neuen Ausdruck, den er auch dem Ausgabefach entnehmen kann.
- Der Wurm "Bugbear" ist seit Ende September 2002 bekannt. Er verbreitet sich über E-Mail und Netzfreigaben. Ein möglicher Nebeneffekt von "Bugbear" ist, dass an alle freigegebenen Netzdrucker selbstständig Druckaufträge mit unsinnigem Inhalt gesendet und dann eventuell auch gedruckt werden. Als Folge können unter anderem Drucker blockiert oder Verbrauchsmaterial verschwendet werden.

# G 4.65 Unzureichender Schutz der Kommunikation bei Druckern und Multifunktionsgeräten

**Unverschlüsselte Druckerkommunikation**

Netzdrucker werden typischerweise nicht lokal angesteuert, sondern über einen Netzanschluss. Der Druckertreiber des jeweiligen lokalen Rechners sendet dazu alle benötigten Informationen direkt an den Drucker oder an einen zentralen Druckerserver, der diese an einen Drucker weiterleitet. Diese Datenübertragung wird nur selten verschlüsselt.

**Fehlende Netztrennung**

Sicherheitsgateways zwischen LAN und Internet werden häufig so konfiguriert, dass der Internet-Zugriff für ganze Subnetze freigeschaltet ist. Andererseits werden Netzdrucker oft dem gleichen Subnetz zugeordnet wie die Arbeitsplatz-PCs, von denen aus auf diese Geräte gedruckt wird. Dadurch kann es passieren, dass auch die Netzdrucker auf das Internet zugreifen können. Wenn die Verbindungen von und zu den Druckern aus dem Internet nicht von den Sicherheitsgateways abgewiesen werden, können unter Umständen sensible Informationen unerwünscht das Netz verlassen. Das Spektrum der übertragenen Informationen kann von Fehlermeldungen über Statistiken bis hin zu ganzen Dokumenten reichen. Sogar aus Fehlermeldungen und Statistiken, die übertragen werden, können detaillierte Benutzerprofile erstellt werden. Beispielsweise aus den IP-Adressen auf die Netzstruktur rückgeschlossen werden.

Manche Hersteller sind zu statistischen und zu Wartungszwecken dazu übergegangen, Daten direkt vom Drucker an einen Server des Herstellers zu senden. Oft ist nicht dokumentiert oder nachprüfbar, welche Daten hierbei an den Hersteller übermittelt werden.

Neben dem ungewollten Informationsfluss aus dem LAN heraus könnte ein netzfähiger Drucker auch unerwünscht Daten aus dem Internet empfangen und eventuell weiter verteilen. Ein Beispiel ist Schadsoftware, die nicht nur das Gerät in seiner Funktion beschränkt, sondern weitere IT-Systeme im Netz infiziert. Schadsoftware könnte beispielsweise durch kompromittierte Patches aus dem Internet eingespielt worden sein. Ein Netzdrucker kann dadurch unter Umständen zu einem Einfallstor für Angriffe aus dem Internet werden.

# G 4.66 Beeinträchtigung von Gesundheit und Umwelt durch Drucker, Kopierer und Multifunktionsgeräte

Obwohl sehr viele Informationen digital gespeichert sind, kann häufig auf Papierdokumente nicht verzichtet werden. Viele Personen lesen oder bearbeiten Dokumente lieber auf Papier als am Bildschirm. Drucker und Kopierer werden daher noch lange unverzichtbare Arbeitsmittel sein. Bei deren Einsatz kann es aber auch zu gesundheitlichen Beeinträchtigungen kommen.

Laserdrucker und Kopierer nutzen meist Trockentoner, der auf das Papier übertragen wird. Der staubförmige Toner enthält neben dem eigentlichen Farbstoff auch Schwermetalle wie Blei und Cadmium. Dieser Tonerstaub wird nicht komplett auf das Papier übertragen, so dass sich Reste davon im gesamten Raum verteilen können. Auch beim Austausch einer fast leeren Toner-Kartusche gegen eine volle kann Toner austreten. So kann der feine gesundheitsgefährliche Tonerstaub eingeatmet werden und sich in der Lunge ablagern. Zusätzlich wird bei einigen Geräten im Betrieb Ozon freigesetzt. Moderne Geräte besitzen aber Filter, die die Freigabe von Ozon verringern.

Häufig werden zentrale Drucker, Kopierer und Multifunktionsgeräte eingesetzt, die einem großen Benutzerkreis zugänglich sind. Diese Geräte sind oft stark ausgelastet. Obwohl die Betriebslautstärke moderner Geräte nicht zu Gehörschäden führt, ist in der Nähe des Geräts nur selten effizientes Arbeiten möglich. Dies gilt insbesondere für Geräte, die sich neben Arbeitsplätzen und nicht in separaten Zimmern befinden.

# G 4.67 Ausfall von Verzeichnisdiensten

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen kann es zum Ausfall eines Verzeichnisdienstes oder Teilen davon kommen. Als Folge sind die im Verzeichnis gehaltenen Daten temporär nicht mehr zugänglich. Im Extremfall kann es zu Datenverlusten kommen. Dadurch können Geschäftsprozesse und interne Arbeitsabläufe behindert werden. Sind funktionsfähige Kopien der ausgefallenen Systemteile vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch unter Umständen je nach gewählter Netztopologie nur mit eingeschränkter Leistungsfähigkeit.

Auch ein technischer Defekt an einem zentralen kryptographischen Modul kann die Funktionsfähigkeit eines Verzeichnisdienstes erheblich beeinflussen, wenn dadurch kein Zugriff mehr auf die Verzeichnisdienst-Komponenten möglich ist. Hierbei könnten kryptographische Schlüssel, die z. B. für die Absicherung einer Datenübertragungsstrecke eines Verzeichnisdienstes benötigt werden, gelöscht werden, insbesondere sofern sie nur flüchtig gespeichert wurden. Die Folge ist, dass die Vertraulichkeit temporär nicht mehr gewahrt werden kann. Dies ist besonders dann kritisch, wenn der Ausfall nicht bemerkt wird und durch die Fehlfunktion keine Verschlüsselung mehr stattfindet, obwohl der Verzeichnisdienstbetreiber auf die Sicherstellung der Vertraulichkeit der Daten durch das kryptographische Modul baut. Verschlüsselte Daten könnten dann solange nicht entschlüsselt werden, wie das erforderliche kryptographische Modul nicht zur Verfügung steht, woraus sich beispielsweise Verfügbarkeitsprobleme für den Verzeichnisdienst oder weiterer Anwendungen ergeben können, welche die entschlüsselten Daten weiterverarbeiten.

# G 4.68 Störungen des Active Directory durch unnötige Dateireplizierung

Seit der Einführung des Betriebssystems Windows 2000 Server verwenden die Domänen-Controller den Dateireplizierungsdienst (File Replication Service, FRS) zur Replikation von Systemrichtlinien und Anmeldeskripten der Clients im Netz einer Institution.

Darüber hinaus wird FRS verwendet, um Daten von fehlertoleranten Freigaben im Distributed File System (DFS) zwischen Servern ab Windows 2000 Server zu replizieren.

Damit eine Replizierung zum geeigneten Zeitpunkt vom FRS angestoßen wird, überwacht der FRS-Dienst "File Close"-Ereignisse des Dateisystems NTFS für alle Verzeichnisse und Dateien, die per FRS repliziert werden sollen. "File Close"-Ereignisse werden dabei von bestimmten Dateioperationen, wie z. B. Löschen und Erstellen von Dateien oder Änderungen an den Datei- und Verzeichnisberechtigungen, ausgelöst.

Software, die zur Systemverwaltung verwendet wird, z. B. Backup-Programme oder Virenschutzprogramme, und dabei auf Dateien und Verzeichnisse zugreift, die vom FRS-Dienst überwacht werden, kann bei unsachgemäßen Zugriff auf die Dateien und Verzeichnisse eine unnötige Replizierung auslösen. Alle Dateien die zur Replizierung anstehen, werden vor der eigentlichen Replizierung im sogenannten Staging-Ordner zusammengefasst.

Anzeichen für eine unnötige Replizierung könnten sich in der Systemumgebung auf folgende Weise bemerkbar machen:

- Dateien aus DFS-Freigaben werden häufig repliziert ohne dass dabei eine erkennbare Änderung an den Dateien vorgenommen wurden.
- Für die Replizierung wird zwischen den Replikationspartnern im Netz zu viel Bandbreite verwendet.
- Die Anzahl der Dateien im Staging-Ordner erhöht sich ständig. Steigt die Anzahl der Dateien beispielsweise immer dann, wenn ein Virenscanner oder Backup-Programm ausgeführt wird, so ist dies ein deutliches Anzeichen für eine unnötige Replizierung. Häufig ist der Staging-Ordner nach der Ausführung des Virenschutzprogramms oder Backup-Programms mit dem nächsten Replizierungszyklus des FRS wieder geleert.
  Wird der Staging-Ordner nie komplett geleert, so deutet dies darauf hin, dass die Replizierung aufgrund der hohen Anzahl von modifizierten Dateien nicht vollständig durchgeführt werden kann.

**Beispiel:**

In einer Institution wird ein Virenschutzprogramm verwendet, das aufgrund einer fehlerhaften Implementierung bei jedem Dateizugriff das "File Close" Ereignis auslöst. Das Computer-Viren-Schutzkonzept der Institution sieht vor, dass in regelmäßigen Abständen das verwendete Viren-Suchprogramm auf den Servern gestartet wird und ein Suchvorgang über alle Dateien gestartet wird.

Durch den fehlerhaften Umgang mit dem "File Close" Ereignis wird für jede Datei eine Replizierung ausgelöst, die gleichzeitig eine unbeabsichtigte, vollständige Synchronisierung aller Dateien und Verzeichnisse zwischen den Servern und Domänen Controllern einer Institution anstößt.

Der dadurch entstehende Datenverkehr kann den geregelten Zugriff auf die Ressourcen innerhalb einer Institution so weit einschränken, dass der ordnungsgemäße Betrieb nicht mehr gewährleistet werden kann. Dies gilt insbesondere für die Niederlassungen einer Institution, die mit einer verhältnismäßig geringen Bandbreite an die Hauptniederlassung angebunden sind.

# G 4.69 Probleme bei der IPSec-Konfiguration

Internet Protocol Security, kurz IPSec, ist ein weit verbreitetes Verfahren zur Absicherung von IP-basierter Kommunikation und kommt häufig für VPNs zum Einsatz. Unter IPSec versteht man eine Reihe von Protokollen zur Schlüsselverwaltung, Authentisierung und Verschlüsselung. Aufgrund der Komplexität des Standards kann es zu fehlerhaften Konfigurationen kommen, die die Sicherheit und Stabilität der Kommunikationsverbindung, z. B. des VPN-Kanals, gefährden.

Vor der eigentlichen Verschlüsselung müssen sich die Kommunikationspartner über die zu verwendenden Security Associations (SA) einig sein. In vielen IPSec-Implementierungen gibt es die Möglichkeit, mit festen SAs und Schlüsseln zu arbeiten. Dies ist jedoch mit den in G 2.130 *Ungeeignete Auswahl von VPN-Verschlüsselungsverfahren* beschriebenen Nachteilen verbunden.

Wird bei der Schlüsselaushandlung der Aggressive Mode (Modus zum schnelleren Verbindungsaufbau) gewählt, so werden die Identitäten und Signaturen (sowie optional Zertifikate) im Klartext übertragen.

Da der IPSec-Standard bereits 1998 spezifiziert wurde, sind darin einige später entwickelte Verfahren zur Netzkonfiguration nicht berücksichtigt. So hat IPSec in bestimmten Konfigurationen verfahrensbedingte Probleme mit der heute in vielen Netzen eingesetzten Network Address Translation (NAT), weil dabei das IPSec-Paket verändert wird. Aus diesem Grund wurden die ergänzenden RFCs 3947 und 3948 zum Thema NAT-Traversal erarbeitet.

Viele Hersteller von VPN-Software haben außerdem in ihren Produkten eine oder mehrere Versionen der zum Teil untereinander inkompatiblen Lösungsvorschläge zur NAT-Problematik implementiert. Dadurch kommt es vor, dass unterschiedliche VPN-Produkte beim Einsatz von NAT gar nicht, nur eingeschränkt oder nur auf einem niedrigen Sicherheitsniveau miteinander kommunizieren können.

Die häufigsten Konfigurationsprobleme eines IPSec-VPNs sind auf SA-Vorschlagslisten zurückzuführen, bei denen keiner der SA-Vorschläge des Initiators mit den Vorschlägen der Gegenseite, also des Responders, übereinstimmt. Ein weiterer häufig vorkommender Grund für das Scheitern einer IPSec-Verbindung sind ungenügende Freischaltungen auf Sicherheitsgateways.

**Beispiele:**

- Ein Administrator setzt aufgrund des schnelleren Verbindungsaufbaus den Aggressive Mode ein. Die Klartextübertragung beim Aggressive Mode besitzt aber eine Schwachstelle: Das Gateway sendet einen aus dem Verfahren Pre Shared Keying (PSK) abgeleiteten Hashwert zur Authentisierung über das Netz. Da dieser Hashwert nicht verschlüsselt ist, könnte ein Angreifer den Schlüssel über Wörterbuch- bzw. Brute-Force-Angriffe rekonstruieren und auf das Firmennetz zugreifen.
- Bei der Erstinstallation des VPNs eines mittelständischen Unternehmens übermittelt ein unerfahrener Administrator die verwendeten Schlüssel per unverschlüsselter E-Mail an die beteiligte Zweigstelle. Die Übertragung wird abgehört. Der Angreifer kann sich mit Hilfe der abgehörten Informationen ins VPN einwählen, auf vertrauliche Dokumente zugreifen und diese an ein Konkurrenzunternehmen verkaufen.

# G 4.70 Unsichere Standard-Einstellungen auf VPN-Komponenten

Die Standard-Einstellungen von VPN-Komponenten weisen nicht immer alle Merkmale einer sicheren Installation auf. Oft wird mehr auf Benutzerfreundlichkeit und problemlose Integration in bestehende Systeme als auf Sicherheit geachtet. Mangelnde Anpassungen an die konkreten Sicherheitsbedürfnisse können daher zu vermeidbaren Schwachstellen und somit zu gefährlichen Angriffspunkten führen.

Da die Verschlüsselung eines VPN-Kanals bei korrekter Anwendung nur mit hohem Aufwand angreifbar ist, bieten die VPN-Endpunkte einen einfacheren Ansatzpunkt für einen Einbruch in ein Netz. Zur Vorbereitung eines Angriffs sammelt ein Angreifer zunächst alle verfügbaren Informationen über das VPN. Im Internet sind spezielle Tools erhältlich, die solche Analysen erleichtern.

**Beispiel:**

- Ein neu erworbenes VPN-Gateway wird vom Administrator einer Firma in das interne Netz eingebunden. Da es mit den Standard-Einstellungen auf Anhieb zuverlässig seinen Dienst verrichtet, ändert der Administrator nichts an den gewählten Einstellungen. Das Produkt ermöglicht jedoch ab Werk eine Fernadministration mit einem bekannten Standard-Passwort. Da das Standard-Passwort aber vielen Anwendern bekannt ist, ergibt sich hierdurch eine Gefahr für den sicheren Betrieb der internen Standortvernetzung.

# G 4.71 Probleme bei der automatisierten Verteilung von Patches und Änderungen

Häufig werden Patches und Änderungen nicht manuell, sondern zentral softwareunterstützt verteilt. Der Einsatz der softwarebasierten Werkzeuge im Rahmen des Patch- und Änderungsmanagements ist neben einigen Vorteilen auch mit Nachteilen verbunden. Bei komplexen IT-Strukturen einer Institution können einzelne Fehler beim Patchen der IT-Systeme massenhafte Sicherheitsprobleme nach sich ziehen. Besonders gravierend ist dies, wenn auf vielen Systemen gleichzeitig Software installiert wird, die Sicherheitslücken enthält.

Treten nur vereinzelte Fehler auf, lassen sie sich oft per Hand beheben. Problematisch wird es aber, wenn das IT-System dauerhaft nicht im LAN erreichbar ist. Ein Beispiel sind Außendienstmitarbeiter, die ihre Rechner nur selten und unregelmäßig an das LAN anschließen. Wenn beispielsweise das Werkzeug so konfiguriert wird, dass die Aktualisierungen nur innerhalb eines bestimmten Zeitraums verteilt werden und nicht alle IT-Systeme erreichbar sind, können diese IT-Systeme nicht aktualisiert werden.

**Beispiel:**

In einem Unternehmen wurden auf die Sicherheitsgateways (Firewalls) verschärfte Paketfilterregeln aufgespielt. Dies führte dazu, dass kein Zugriff auf das LAN mehr möglich war. Eine automatisierte Behebung war ebenfalls nicht mehr möglich und die manuelle Behebung dauerte sehr lange. Während dieser Zeit standen keine Serverdienste mehr zur Verfügung, was das Unternehmen Zeit und Geld kostete.

# G 4.72 Inkonsistenzen von Datenbanken im Trivial Database Format unter Samba

Samba legt in mehreren Verzeichnissen Datenbanken im Trivial Database (TDB)-Format ab. Die Dateien in diesen Verzeichnissen sind für den einwandfreien Betrieb von Samba sehr wichtig. Die Datenbanken werden beispielsweise von den smbd-Prozessen zur Kommunikation untereinander eingesetzt.

Samba stellt bei diesen Datenbanken sehr hohe Anforderungen an das darunterliegende Dateisystem des Betriebssystems bezüglich Performance und Konsistenz. Diese Anforderungen werden nicht von allen Dateisystem/Betriebssystem-Kombinationen erfüllt. Dies betrifft vor allem ältere Betriebssystem- und Dateisystem-Versionen.

Beispielsweise hatte Solaris in Verbindung mit Samba 3 lange ein schwerwiegendes Skalierungsproblem beim Locking in Dateisystemen. Dieses Problem trat auf, sobald ungefähr 600 Benutzer gleichzeitig auf den Samba-Server zugriffen. Auch Linux ist von ähnlichen Problemen betroffen. Bei einigen älteren Versionen des Dateisystems ReiserFS gab es ebenfalls Schwierigkeiten im Zusammenspiel mit Samba.

Wenn bei der Installation nicht darauf geachtet wird, dass die verwendete Betriebssystem/Dateisystem-Kombination für TDB-Dateien von Samba geeignet ist, kann es zu schwerwiegenden Performance-Problemen oder zu Fehlfunktionen durch Inkonsistenzen in den Datenbanken kommen.

# G 4.73 Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme von Windows-Versionen

Software, die auf Vorgängerversionen eines Betriebssystems erfolgreich betrieben werden konnte, muss nicht auch mit der aktuellen Version des Betriebssystems zusammenarbeiten. Mögliche Ursachen sind neue Sicherheitsmerkmale oder Betriebssystemeigenschaften. In der Folge kann die Software nicht oder nur mit Einschränkungen verwendet werden. Dies kann sich auf bestehende Software und auf neu erworbene Software beziehen.

Laut Microsoft können neue, aktivierte Sicherheitsmerkmale von neuen Windows-Versionen die Ursache möglicher Kompatibilitätsprobleme sein. Dazu zählen:

- Benutzerkontensteuerung (UAC, User Account Control), neu in Clients ab Windows Vista
- Kernel PatchGuard oder Patch Protection, nur bei 64-Bit-Versionen ab Windows Vista und bereits aus vorangegangen 64-Bit-Windows-Versionen bekannt
- Umleitung der Systempfade und Registry-Schlüssel im 32-Bit-Modus WoW64 (Windows-On-Windows 64-Bit) der Windows 64-Bit-Versionen
- Windows Ressourcenschutz (Windows Resource Protection, WRP), neu in Clients ab Windows Vista
- Geschützter Modus des Internet Explorer (Protected Mode), neu in Clients ab Windows Vista
- Notwendigkeit signierter Treiber für die 64-Bit-Versionen von Clients ab Windows Vista
- Veraltete Objekte, die von Windows XP-kompatibler Software häufig verwendet wurden, existieren nicht mehr. Gleiches gilt für GINA und sogenannte Session 0-Prozesse

**Beispiele:**

- Benutzerkontensteuerung (UAC)
  Die Benutzerkontensteuerung kann die Ausführung von gruppenrichtlinieengesteuerten Anmeldeskripten beeinflussen und verhindern. Die Verteilung und korrekte Ausführung von GPO-basierten Anmeldeskripten ist im Einzelfall auf Rechnern ab Windows Vista zu prüfen. Die Benutzerrechte, die zur Ausführung der Skripte erforderlich sind, müssen gegeben sein.
- Kernel Patch Protection in Clients ab Windows Vista
  Kernel Patch Protection soll unbefugte Veränderungen des Kernels durch Programme verhindern (der Begriff "Patch" bezeichnet Korrektur-Software). Mit Kernel Patch Protection können Programme ausschließlich über spezielle Windows Programmierschnittstellen (Application Programming Interface, API) mit Kernel-Komponenten kommunizieren.
  Kernel Patch Protection ist nur für die 64-Bit-Versionen und nicht für die 32-Bit-Versionen von Clients ab Windows Vista verfügbar, sie kann nicht deaktiviert werden.
  Es hat sich gezeigt, dass Programme Dritter, insbesondere Virenschutzprogramme, nicht immer kompatibel zur Kernel Patch Protection waren.
  Die Folge davon kann ein nicht vorhandener oder ein eingeschränkter Virenschutz des IT-Systems sein.

- Fingerabdruckleser, VPN-Lösungen und Schutzsoftware funktionieren nicht mehr richtig, wenn sie alte GINA-Module verwenden oder alte Funktionsaufrufe des Kommunikationsprotokolls IPv4 ansprechen.
- Das für Touch-Oberflächen optimierte Windows 8 führt erstmalig Programme als Apps ein. Diese zeichnen sich vor allem durch eine für Touch-Geräte optimierte Oberfläche aus (Bedienung mit Fingern statt Maus und Tastatur). Bekannte Windows-Programme und deren App-Versionen können sich in ihrer Funktionalität jedoch unterscheiden:
  Beispielsweise ist der Internet Explorer ab Windows 8 in zwei Betriebsmodi verfügbar. Er lässt sich weiterhin in der bisher bekannten Desktop-Version starten und unterstützt zahlreiche Plug-Ins und Erweiterungen. In der App-Version des Internet Explorers ist die Funktionalität von Plug-Ins und Erweiterungen jedoch stark eingeschränkt.

# G 4.74 Ausfall von IT-Komponenten in einer virtualisierten Umgebung

Innerhalb einer klassischen IT-Infrastruktur werden Serverbetriebssysteme und deren Dienste, aber auch die Betriebssysteme der Arbeitsplatzrechner auf physikalischen IT-Systemen ausgeführt. Die zum Betrieb der Serversysteme notwendigen Infrastruktur-Komponenten (Netzkomponenten, Speichernetze und ähnliches) werden ebenfalls verteilt auf verschiedenen physikalischen IT-Systemen bereitgestellt.

In einer virtualisierten Umgebung hingegen werden die Serversysteme sowie Teile der notwendigen Infrastrukturkomponenten als eigene Server-Instanzen zu einem großen Teil durch die Virtualisierungsserver selbst bereitgestellt. Wenn also ein virtueller Server beispielsweise auf das Netz zugreift, so greift er nicht auf ein physikalisches IT-System wie einen Switch zu, sondern auf eine durch den Virtualisierungsserver zur Verfügung gestellte Komponente, die nur als Software, aber nicht als eigene Hardware betrieben wird.

Fällt ein physikalisches IT-System aus, kann oftmals noch mit den restlichen Systemen weiter gearbeitet werden. Zwar sind die Dienste, die durch den ausgefallenen Server bereitgestellt werden, nicht länger verfügbar, dies betrifft jedoch nicht zwingend alle anderen installierten Server. Ist beispielsweise ein Datenbankserver ausgefallen, kann dennoch der Zugriff auf den Dateiserver erfolgen. Nicht alle Geschäftsprozesse, die durch den Informationsverbund unterstützt werden, sind also betroffen.

Im Gegensatz dazu werden in einer virtualisierten IT-Infrastruktur in der Regel zahlreiche und unterschiedliche Instanzen virtualisierter IT-Systeme (Gäste) technisch auf wenigen physikalischen Maschinen zusammengeführt (konsolidiert). Hierdurch erhöhen sich die Auswirkungen auf die Verfügbarkeit bei Störungen eines Virtualisierungsservers erheblich. Bei Beschädigungen von physikalischen Komponenten des Virtualisierungsservers oder einer Fehlfunktion in dessen Betriebssystem werden alle darauf ablaufenden virtuellen IT-Systeme in Mitleidenschaft gezogen.

Beim Ausfall eines IT-Systems können die Daten beschädigt werden, die von diesem System verarbeitet werden. Es entsteht gegebenenfalls ein höherer Aufwand, um das System wieder in Betrieb zu nehmen, da die Daten möglicherweise aus der Datensicherung wieder hergestellt werden müssen. Es können auch Daten unwiederbringlich verloren gegangen sein. Fallen nun mehrere virtuelle IT-Systeme aufgrund eines Fehlers eines Virtualisierungsservers gleichzeitig aus, steigt die Wahrscheinlichkeit, dass mindestens eines der ausgefallenen Systeme von einer solchen Beschädigung betroffen ist. Daher kann es in einem solchen Fall zu einer längeren Betriebsunterbrechung kommen, als es beim Ausfall nur eines IT-Systems der Fall gewesen wäre.

Im Rechenzentrumsbetrieb hängen viele Dienste voneinander ab. Zum Beispiel benötigt ein Mailsystem einen Verzeichnisdienst, um Empfängeradressen den Postfächern zuzuordnen. Ein System zur Auftragsverwaltung benötigt das Mailsystem, um eingehende und ausgehende Aufträge zu verarbeiten. Es erstellt außerdem automatisch Aufträge im Warenwirtschaftssystem, um die Abarbeitung der Kundenaufträge zu unterstützen. Zudem greift das Warenwirtschaftssystem auf die Datenbank der Lagerverwaltung zu, um Lagerbestände zu überwachen.

Der Ausfall von einzelnen Komponenten des Informationsverbundes kann dazu führen, dass ebenso Dienste, die im Rechenzentrum bereitgestellt werden,

teilweise ausfallen. Werden nun mehrere IT-Systeme als virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben, fallen mit dem Virtualisierungsserver zusammen gleich mehrere Komponenten eines Informationsverbundes aus. Hierdurch kann es zu einer stärkeren Beeinträchtigung des IT-Betriebs kommen, als es im klassischen, nicht virtualisierten Rechenzentrumsbetrieb der Fall wäre.

**Beispiel:**

Ein mittelständisches Unternehmen hat sich für die Verwendung einer Virtualisierungslösung entschieden. Es wird geplant, einige sehr leistungsfähige Server zu beschaffen und die Anzahl physikalischer Systeme stark zu reduzieren.

Auf den Virtualisierungsservern wurden IT-Systeme und deren Dienste nach Aspekten wie Prozessorlast und Speicherverbrauch verteilt. Dabei wurde überlegt, wie die virtuellen IT-Systeme auf die Virtualisierungsserver optimal verteilt werden können.

Das Unternehmen nutzt ein Mailsystem, das auf einem Verzeichnisdienst beruht. Dazu wird ein Buchhaltungssystem betrieben, das in einen Anwendungsserver und einen Datenbankserver aufgeteilt ist. Die weiterhin noch genutzten Warenwirtschafts- und Lagerhaltungssysteme verwenden ebenfalls die Buchhaltungsdatenbank für den Austausch von Daten.

Da der Datenbankserver des Buchhaltungssystems und der Mailserver zu den IT-Systemen mit den größten Performanceanforderungen gehören, wurde entschieden, sie auf getrennten Virtualisierungsservern zu betreiben. Dadurch soll erreicht werden, dass diese sich während des Betriebs nicht gegenseitig beeinträchtigen. Die weitere Analyse der Performanceanforderungen der Systeme ergab dabei, dass ein optimaler Konsolidierungsseffekt erreicht werden kann, wenn die virtuellen IT-Systeme wie folgt verteilt werden:

Erster Virtualisierungsserver: Datenbank, Verzeichnisdienst

Zweiter Virtualisierungsserver: Mailsystem, Buchhaltungssystem

Dritter Virtualisierungsserver: Warenwirtschafts-, Lagerhaltungssystem

Durch einen beschädigten Elektrolytkondensator auf der Hauptplatine des ersten Virtualisierungsservers kommt es zum Ausfall dieses Servers. Auf diesem Server befanden sich getrennt in virtuellen Maschinen die Datenbank für das Buchhaltungssystem und der Verzeichnisdienst der Firma.

Der Wegfall dieses einen physikalischen Servers hat insgesamt weitreichende Konsequenzen für den IT-Betrieb. Zwar liegen die Applikationsserver der Buchhaltung sowie der Lager- und Warenwirtschaft auf anderen Virtualisierungsservern, sind jedoch auf einen Datenaustausch mit der Datenbank angewiesen, um ordnungsgemäß zu funktionieren. In dem Unternehmen fielen zentrale Prozesse vollständig aus, sodass es zu einem Stopp der Auslieferung der Kundenaufträge kam und durch den Ausfall des Warenwirtschafts- und Lagerhaltungssystems ein mehrstündiger Produktionsausfall hingenommen werden musste.

Weiterhin konnten die Kunden des Unternehmens nicht sofort wie vertraglich vereinbart per E-Mail über den Produktionsausfall unterrichtet werden, da das Mailsystem ebenfalls ausgefallen war. Dadurch verletzte das Unternehmen wesentliche Pflichten aus seinen Lieferverträgen und musste neben den durch

den Produktionsausfall verursachten Kosten auch noch Vertragsstrafen übernehmen.

# G 4.75 Störung der Netzinfrastruktur von Virtualisierungsumgebungen

Mehrere Virtualisierungsserver können zu einer so genannten virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die virtuellen IT-Systeme beliebig auf die einzelnen Virtualisierungsserver verteilt werden. Weiterhin ist es möglich, die virtuellen Maschinen zwischen den Virtualisierungsservern zu verschieben. Dies kann bei einigen Produkten auch geschehen, wenn das virtuelle IT-Systeme gerade ausgeführt wird (Beispiele: Microsoft Hyper-V Live Migration, VMware VMotion, XEN LiveMigration). Ein solcher Prozess, im Folgenden Live Migration genannt, ist in der Regel transparent für das virtuelle IT-System, d. h. es bemerkt diesen Migrationsprozess nicht. Auf dieser Migrationstechnik bauen weitere Funktionen einer virtuellen Infrastruktur auf. Dies sind Funktionen wie z. B. die dynamische Zuteilung von Prozessor- und Hauptspeicherressourcen. Hierbei wird das virtuelle IT-System immer auf den Virtualisierungsserver migriert, der die benötigten Ressourcen optimal zur Verfügung stellen kann. Ein virtuelles IT-System erhält auf diese Weise immer die bestmögliche Ressourcenzuteilung.

Es gibt des Weiteren Virtualisierungsprodukte, bei denen der Ausfall eines Virtualisierungsservers kompensiert wird, indem die davon mit betroffenen virtuellen IT-Systeme auf einem anderen Virtualisierungsserver automatisch neu gestartet werden.

Um die beschriebenen technischen Möglichkeiten zu realisieren, wird zwischen den beteiligten Virtualisierungsservern ein Kommunikationsnetz zur Koordinierung dieser Funktionen (automatischer Neustart, Live Migration) benötigt. Kommt es zu Störungen in diesem Netz, sind die hierüber koordinierten Funktionen ebenfalls gestört.

Eine Störung in der Kommunikation zwischen Virtualisierungsservern kann eine Live Migration abbrechen lassen. Hierdurch können möglicherweise Mechanismen zur dynamischen Lastverteilung fehlschlagen, wenn eine virtuelle Maschine aufgrund eines Ressourcenengpasses auf einen anderen Zielserver verschoben werden soll. In der Folge führt der nicht behebbare Ressourcenengpass auf dem Quellserver zu einer Einschränkung der Verfügbarkeit des nicht verschiebbaren IT-Systems.

Um die Verfügbarkeit virtueller IT-Systeme zu steigern, können mehrere Virtualisierungsserver zu einem Cluster miteinander verbunden werden. Die Systeme, die an einem solcher Serververbund teilnehmen, benötigen eine reibungslose Kommunikation untereinander. Mittels dieser Kommunikation überwachen sich die Systeme gegenseitig und prüfen z. B., ob die auf ihren Partnern laufenden virtuellen IT-Systeme weiterhin verfügbar sind (Heartbeat). Fällt einer der Partner des Verbundes aus, werden die ebenfalls ausgefallenen IT-Systeme, sofern möglich, auf einem anderen Virtualisierungsserver neu gestartet.

Fällt das Kommunikationsnetz des Clusters, beispielsweise aufgrund eines Hardwarefehlers auf einem Switch, aus, ist die Funktion zur Ausfallkompensation des Clusters gestört. Möglicherweise sind die virtuellen IT-Systeme auf den Virtualisierungsservern, die Mitglieder des Clusters sind, ebenfalls in ihrer Verfügbarkeit gefährdet.

Das Kommunikationsnetz zwischen den am Hochverfügbarkeitsverbund beteiligten Systemen erfüllt im Übrigen neben den vorgenannten weitere wichtige Funktionen: Fällt die Kommunikation zwischen mehreren Systemen eines Verbundes gleichzeitig aus, muss jedes System entscheiden können, ob es selbst oder die anderen Systeme von dem Ausfall betroffen sind (Isolationsproblem). Würden zwei oder mehrere an einem Hochverfügbarkeitsverbund beteiligte Virtualisierungsserver isoliert voneinander ein virtuelles IT-System mehrfach starten, können die Daten, die dieses virtuelle System repräsentieren, beschädigt werden. Dadurch kann das virtuelle IT-System unbenutzbar werden. Es kann auch zu Störungen kommen, wenn ein und dasselbe IT-System mehrfach im Netz vorhanden ist (z. B. durch doppelte IP- oder MAC-Adressen).

**Anbindung von Speichernetzen**

Virtuelle IT-Systeme werden in der Regel durch eine Reihe von Dateien physisch repräsentiert. Diese Dateien enthalten neben der Konfiguration des virtuellen IT-Systems beispielsweise auch die Container für virtuelle Festplatten. Werden Snapshots, also Abbilder eines virtuellen IT-Systems in einem beliebigen, auch laufenden Betriebszustand, erzeugt, speichert der Virtualisierungsserver die hierbei entstehenden Daten ebenfalls in Dateien. Diese Dateien können entweder auf dem Virtualisierungsserver selbst oder in dem dazugehörigen zentralen Speichernetz gespeichert sein.

Virtuelle Serverumgebungen aus mehreren Virtualisierungsservern sind oftmals mit zentralen Speichernetzen verbunden, damit auf die Dateien, die die virtuellen IT-Systeme repräsentieren, von mehreren Stellen aus zugegriffen werden kann. Bricht die Verbindung zu diesen Speicherressourcen ab, wirkt sich dies auf die virtuellen IT-Systeme so aus, als würde einem physischen Server im laufenden Betrieb eine Festplatte entfernt. Da auf Speicherressourcen in einem Speichernetz häufig mehr als ein virtuelles IT-System gespeichert ist, ist bei einem Ausfall die Betriebssicherheit vieler virtueller IT-Systeme gefährdet. In den von dem Ausfall betroffenen virtuellen IT-Systemen und Virtualisierungsservern können bei einem Ausfall Dateisysteminkonsistenzen auftreten, die unter Umständen umfangreiche Wiederherstellungsmaßnahmen erfordern.

# G 4.76 Ausfall von Verwaltungsservern für Virtualisierungssysteme

Mittels mehrerer Virtualisierungsserver kann eine virtuelle Infrastruktur aufgebaut werden. Dabei werden die Virtualisierungsserver in einer Weise miteinander verbunden, dass die auf ihnen laufenden virtuellen IT-Systeme immer auf dem Virtualisierungsserver ausgeführt werden, der die für dieses IT-System optimale Performance bereitstellen kann. Kann ein Virtualisierungsserver einem laufenden virtuellen IT-System mehr Ressourcen zur Verfügung stellen (dynamische Ressourcenzuteilung, z. B. *Citrix XenServer Workload Balancing* oder *VMware Dynamic Resource Scheduling*), ist es sogar möglich dieses IT-System mittels einer Migration (*Live Migration*) auf das IT-System mit den freien Ressourcen zu verschieben.

Zusätzlich kann die Verfügbarkeit der virtuellen IT-Systeme durch Hochverfügbarkeitsmechanismen wie den automatischen Neustart von ausgefallenen virtuellen Maschinen gesteigert werden. Diese Funktionen erfordern bei den meisten Virtualisierungsprodukten einen zentralen Verwaltungsserver, der den Betrieb der einzelnen virtuellen Maschinen und der Virtualisierungsserver koordiniert. Virtualisierungsprodukte, die einen solchen zentralen Verwaltungsserver verwenden können, sind beispielsweise *Citrix XenServer, Microsoft Hyper-V* oder *VMware ESX*. Der Verwaltungsserver (*Citrix XenCenter*, *Microsoft System Center Virtual Machine Manager*, *SUN Management Center* oder *Vmware vCenter*) besitzt in der Regel ebenfalls eine Monitoring-Komponente, mittels derer die Funktion der virtuellen IT-Systeme und der Virtualisierungsserver überwacht werden kann.

Da über den Verwaltungsserver sämtliche Funktionen einer virtuellen Infrastruktur gesteuert und administriert werden, führt ein Ausfall dieses Verwaltungssystems dazu, dass keine Konfigurationsänderungen an der virtuellen Infrastruktur durchgeführt werden können. Die Administratoren können in dieser Zeit weder auf auftretende Probleme wie Ressourcenengpässe oder den Ausfall einzelner Virtualisierungsserver reagieren noch einen neuen Virtualisierungsserver in die Infrastruktur integrieren bzw. neue virtuelle IT-Systeme anlegen.

Auch Funktionen wie *Live Migration* und damit die dynamische Zuteilung von Ressourcen für einzelne Gastsysteme stehen nicht mehr zur Verfügung, da die Instanz, die solche Funktionen koordiniert, nicht mehr betriebsbereit ist. In der Folge kann die virtuelle Infrastruktur nicht mehr automatisch auf Ressourcenengpässe reagieren und sowohl die Performance als auch die Verfügbarkeit einzelner virtueller IT-Systeme werden nachteilig beeinflusst. Dies tritt insbesondere dann auf, wenn die Ressourcen der Virtualisierungsserver überbucht wurden.

Zusätzlich dient der Verwaltungsserver der Überwachung der Virtualisierungsserver und der auf diesen betriebenen virtuellen IT-Systeme. Liefert der Verwaltungsserver oder dessen Monitoring-Komponente falsche oder gar keine Daten, kann die Funktion der virtuellen Infrastruktur durch die Administratoren nicht mehr hinreichend überwacht werden. Es besteht damit die Gefahr, dass Ressourcenengpässe in der virtuellen Infrastruktur unbemerkt bleiben und nicht rechtzeitig für eine Erweiterung der virtuellen Infrastruktur gesorgt wird. Der Ausfall von einzelnen virtuellen IT-Systemen kann möglicherweise ebenfalls nicht rechtzeitig festgestellt werden, wenn die Überwachung der virtuellen Infrastruktur ausgefallen ist.

Weiterhin kann sogar der Ausfall von Virtualisierungsservern unbemerkt bleiben, wenn die auf ihm laufenden virtuellen IT-Systeme zwar auf einen anderen Virtualisierungsserver migriert worden sind und damit keine Dienste im Rechenzentrum ausfallen, der Ausfall aber wegen eines Fehlers in der Verwaltungs- und Überwachungssoftware nicht signalisiert wird. Durch die damit verbundene Herabsetzung der Redundanz kann die Gesamtverfügbarkeit der virtuellen Infrastruktur massiv verringert werden.

**Beispiel:**

- Eine Organisation betreibt mehrere Virtualisierungsserver, die in zwei Farmen zusammengefasst sind. In diesen Farmen werden jeweils mehrere virtuelle IT-Systeme betrieben. Die Virtualisierungsserver sind auf zwei Farmen verteilt worden, da auf Grund unterschiedlicher Schutzbedarfsanforderungen bestimmte virtuelle IT-Systeme nicht mit anderen zusammen betrieben werden dürfen.
  Bei der Planung der beiden Farmen ist die Anzahl der jeweils notwendigen Virtualisierungsserver auf Grund einer Prognose des zukünftigen Performancebedarfs ermittelt worden. Nach einiger Zeit stellt sich jedoch heraus, dass die Prognose unzutreffend war. Es wird festgestellt, dass in der ersten der beiden Farmen ein weiterer Virtualisierungsserver benötigt wird, um die Performanceanforderungen der virtuellen IT-Systeme abzudecken.
  Die Administratoren der Virtualisierungsserver stellen nach einer Auswertung der Performancedaten der zweiten Farm fest, dass deren Auslastung weit hinter der Performanceprognose zurückliegt. Daher wird entschieden, keinen neuen Virtualisierungsserver zu beschaffen, sondern stattdessen einen aus der zweiten Farm in die erste zu verlagern.
  Nun werden die virtuellen IT-Systeme auf dem Virtualisierungsserver, der in die erste Farm verlagert werden soll, auf andere migriert und der Server wird in die erste Farm aufgenommen. In der Folge sind die Ressourcen in der zweiten Farm massiv überbucht und es kommt zu starken Performanceeinbrüchen. Dies war nach den Ergebnissen der Performanceanalyse nicht zu erwarten.
  Die Ursache für die massiven Performanceverluste der virtuellen IT-Systeme in der zweiten Farm lag darin, dass das Verwaltungssystem für diese Farm die Performancedaten der einzelnen Virtualisierungsserver falsch verarbeitet hat und deutlich zu niedrige Werte für den Ressourcenverbrauch angezeigt hat.

# G 4.77 Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen

Bei vielen Virtualisierungsprodukten können so genannte Gastwerkzeuge in den virtuellen IT-Systemen installiert werden. Diese dienen einerseits dazu, spezielle, optimierte Gerätetreiber für die virtuellen Hardwarekomponenten einer virtuellen Maschine bereitzustellen. Andererseits kann der Virtualisierungsserver bei bestimmten Produkten über diese Gastwerkzeuge den Ressourcenverbrauch eines virtuellen IT-Systems steuern. Dies ist insbesondere dann notwendig, wenn das verwendete Virtualisierungsprodukt die Überbuchung von Ressourcen wie Arbeitsspeicher oder Festplattenplatz ermöglicht. Konkurrieren beispielsweise zwei virtuelle IT-Systeme um Arbeitsspeicher, kann das Hostbetriebssystem oder der Hypervisor die Gastwerkzeuge anweisen, virtuelles RAM und damit dessen physische Entsprechung in einem der virtuellen IT-Systeme zu reservieren. Die physische Repräsentation dieses Speichers wird nun durch das virtuelle IT-System nicht genutzt und steht über die Gastwerkzeuge unter der Kontrolle des Hypervisors. Der Hypervisor kann nun diesen physischen Speicher dem anderen virtuellen IT-System als virtuelles RAM zur Verfügung stellen. Andersherum kann ein virtuelles IT-System über die Gastwerkzeuge auch Hauptspeicher anfordern. Eine solche Technik wird zum Beispiel bei dem Produkt *ESX* des Herstellers *VMware* genutzt. Hier wird die Speicherreservierung über einen so genannten *Ballooning-Treiber* realisiert. Dieser ist in den Gastwerkzeugen (*VMware Tools*) enthalten.

Weiterhin kann bei einigen Virtualisierungsprodukten über die Gerätetreiber der Gastwerkzeuge der Zugriff auf Ressourcen eingeschränkt werden. So ist es zum Beispiel möglich, die Bandbreite, mit der ein virtuelles IT-System auf das Netz oder das Speichernetz zugreift, zu begrenzen.

Programmierfehler in den Gastwerkzeugen können daher auf Grund ihrer vielfältigen Funktionen weitreichende Folgen für den Betrieb der davon betroffenen virtuellen IT-Systeme haben, da meist eine Vielzahl von IT-Systemen gleichzeitig davon betroffen ist.

### Gerätetreiber

Der häufigste Anwendungszweck der Gastwerkzeuge ist es, optimierte Gerätetreiber für die vom Virtualisierungsserver bereitgestellte emulierte Hardware (Grafikkarte, Netzkarte, Massenspeicher) der virtuellen IT-Systeme bereitzustellen. Die emulierte Hardware kann vom virtuellen IT-System zwar meist auch mit den im Lieferumfang der gängigsten Betriebssysteme enthaltenen Treibern genutzt werden, jedoch ist eine optimale Nutzung erst mit speziell angepassten Treibern möglich. Da diese in der Regel in allen virtuellen IT-Systemen genutzt werden, sind von einem Fehler in diesen Treibern auch alle virtuellen Maschinen betroffen.

### Überbuchung von Speicherressourcen

Werden der Hauptspeicher des Virtualisierungsservers überbucht und Speicheranforderungen innerhalb eines virtuellen IT-Systems durch die Gastwerkzeuge fehlerhaft verarbeitet, kann es passieren, dass Prozessen zu wenig Speicher zur Verfügung steht.

**Fehler im Bandbreitenmanagement**

Sind die Funktionen zum Bandbreitenmanagement in den Gastwerkzeugen fehlerhaft programmiert, können die hierfür definierten Richtlinien wirkungslos sein. Genauso kann es aber dazu kommen, dass einem virtuellen IT-System viel zu wenig oder gar keine Bandbreite zur Verfügung gestellt wird.

Wenn beispielsweise ein virtuelles System ständig sehr viel Netzverkehr verursacht und dadurch die physikalisch vorhandenen Ressourcen stark ausnutzt, können die Verbindungen anderer virtueller IT-Systeme in Mitleidenschaft gezogen werden, so dass in der Folge Verbindungen dieser IT-Systeme abbrechen und damit deren Verfügbarkeit gefährdet ist.

Über die Gastwerkzeuge könnte nun der Administrator des Virtualisierungsservers entweder die nutzbare Bandbreite des ersten virtuellen IT-Systems beschränken oder den anderen Systemen eine gewisse Mindestbandbreite garantieren. Sind die Richtlinien zur Bandbreitensteuerung beispielsweise nach einer Aktualisierung der Gastwerkzeuge auf Grund eines Programmierfehlers wirkungslos, werden die Ziele, die mit diesen Richtlinien verfolgt wurden, nicht erreicht. Die Verfügbarkeit der Systeme ist also weiterhin eingeschränkt.

Führt der Fehler in den Gastwerkzeugen trotz korrekter Richtlinien im genannten Szenario dazu, dass zu wenig Bandbreite für das erste IT-System zur Verfügung steht, kann dieses System in der Verfügbarkeit eingeschränkt sein, da es nicht mit der erforderlichen Bandbreite auf das Netz zugreifen kann. Gleiches gilt für die anderen IT-Systeme, deren Kommunikation geschützt werden sollte.

**Beispiel:**

Ein mittelständisches Unternehmen betreibt eine Reihe von Virtualisierungsservern, um auf diesen Virtualisierungsservern seine sonstige Server-Infrastruktur effizient bereitstellen zu können. Alle im Unternehmen genutzten Dienste hängen direkt oder indirekt von den virtuellen IT-Systemen in der virtuellen Infrastruktur ab. Dort laufen Systeme wie der Verzeichnisdienst, der zentrale Mailserver sowie das ERP-System. Weiterhin werden Datei- und Druckserver als virtuelle IT-Systeme betrieben.

Die Systeme laufen einige Zeit störungsfrei. Nachdem eine Aktualisierung der Virtualisierungssoftware auf den Virtualisierungsservern durchgeführt wurde, zeigte die zentrale Verwaltungssoftware der Virtualisierungsserver an, dass die Gastwerkzeuge der virtuellen IT-Systeme nicht mehr aktuell seien. Der zuständige Administrator entscheidet sich, die Gastwerkzeuge in den virtuellen IT-Systemen zu aktualisieren. Er hat mit dieser Aktualisierung in der Vergangenheit keine schlechten Erfahrungen gemacht. Da er selbst nicht auf allen virtuellen IT-Systemen Administratorrechte besitzt, benutzt für die Aktualisierung eine Funktion der Virtualisierungsserver, die es ermöglicht, die Werkzeuge auf allen Virtualisierungsservern ohne Interaktion mit den einzelnen virtuellen IT-Systemen zu erneuern. Er beginnt an einem Arbeitstag zwei Stunden vor allgemeinem Arbeitsbeginn mit dem Update. Er beobachtet, wie die Gastwerkzeuge in den virtuellen IT-Systemen neu installiert werden und stellt zunächst keine offensichtlichen Fehler fest, da auf der Konsole der virtuellen Systeme keine Fehlermeldungen protokolliert werden.

Nachdem aber eine gewisse Anzahl virtueller IT-Systeme aktualisiert wurde, bemerkt er, dass diese nicht mehr mit dem Netz verbunden sind. Er untersucht das Problem und stellt fest, dass die Netzkarten-Treiber der virtuellen IT-Systeme als Bestandteil der Gastwerkzeuge ebenfalls aktualisiert worden

sind. Hierbei ist dem Hersteller ein Fehler unterlaufen, der dazu führt, dass die Betriebssysteme der virtuellen IT-Systeme die virtuelle Netzkarte als neue Hardware erkennen. Hierdurch ist die Netzkarte unkonfiguriert. Erst nachdem die anderen Administratoren im Unternehmen eingetroffen sind, können die Netzkarten neu konfiguriert werden. Bis dahin können viele Mitarbeiter in der Verwaltung des Unternehmens zunächst nicht auf ihre Daten zugreifen. Dadurch geht viel Arbeitszeit verloren.

# G 4.78 Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse

Klassische Datensicherungsmethoden basieren auf Agenten, die auf den zu sichernden IT-Systemen installiert werden. Diese Agenten übermitteln die zu sichernden Daten vom IT-System aus an den Datensicherungsserver. Dieser wiederum leitet die Daten an die Datensicherungsgeräte weiter.

Durch die Einführung von Speichernetzen können IT-Systeme und der von ihnen genutzte Massenspeicher entkoppelt werden. Dies bedeutet, dass die Datensicherung nicht mehr vom zu sichernden IT-System selbst, sondern vom Speichernetz an den Datensicherungsserver übermittelt werden kann. Bei einigen Speichernetz-Produkten sind die Datensicherungsgeräte selbst Bestandteile des Speichernetzes und werden nur noch durch den Datensicherungsserver gesteuert. Hierdurch wird das gesicherte IT-System und der Datensicherungsserver vom Transport der Daten der Datensicherung entlastet.

Dieses Konzept wird von einigen Virtualisierungsprodukten nachgebildet und erweitert. So können die Virtualisierungsserver den Massenspeicher virtueller IT-Systeme (virtuelle Festplatten) einem Datensicherungssystem zur Verfügung stellen, damit dieses Datensicherungssystem die auf dem Massenspeicher abgelegten Daten sichern kann. Es ist notwendig, dass diese virtuelle Festplatte sich in einem konsistenten Zustand befindet, damit keine inkonsistenten Daten in die Sicherung gelangen. Um dies zu erreichen, wird der Inhalt der virtuellen Festplatte eingefroren (Snapshot). Dieser Vorgang ist für das gesicherte virtuelle IT-System vollkommen transparent. Da das zu sichernde virtuelle IT-System weiterläuft und weiterhin Änderungen an dieser Festplatte erfolgen, werden diese Änderungen in eine Differenzdatei geschrieben. Hierbei wächst der insgesamt von diesem IT-System benötigte Speicherplatz an. Wie groß diese Differenzdatei wird, hängt davon ab, wie viele Änderungen im Dateisystem des virtuellen IT-Systems während der Dauer der Sicherung geschehen. Ist die Datensicherung beendet, werden die Änderungen, die in der Zwischenzeit erfolgt sind, auf den eingefrorenen Zustand angewendet und die Differenzdatei wird gelöscht.

Wird eine Datensicherung in der Virtualisierungsumgebung etwa aufgrund langer Laufzeit des Datensicherungsprozesses oder durch Kommunikationsprobleme im Netz nicht vollständig ausgeführt, kann die Differenzdatei, die angelegt wurde, als der Snapshot erzeugt wurde, sehr groß werden. Möglicherweise bleibt sie dauerhaft bestehen, wenn der Datensicherungsprozess unvorhergesehen abbricht. Dies kann dazu führen, dass der Speicherplatz, in dem die virtuellen Festplatten der zu sichernden virtuellen Maschinen liegen, vollkommen ausgeschöpft wird, insbesondere dann, wenn mehrere virtuelle IT-Systeme gleichzeitig auf diese Weise gesichert werden.

Ist der Speicherplatz, der für die oben erwähnte Differenzdatei genutzt wird, erschöpft, verweigert der Virtualisierungsserver dem virtuellen IT-System weitere Schreibzugriffe auf die virtuelle Festplatte, und das virtuelle IT-System gerät in eine Fehlersituation. Dies kann zu einem Absturz des virtuellen IT-Systems führen, wenn das Betriebssystem diese Fehlersituation nicht ausgleichen kann.

**Beispiel:**

Der Betreiber eines Rechenzentrums hat eine Vielzahl seiner Serversysteme virtualisiert. Auf diesen Servern werden täglich große Mengen an Daten verarbeitet. Diese Daten müssen täglich gesichert werden.

Die Sicherung der Daten beansprucht die virtuellen IT-Systemen auf Grund der hohen Datenmenge stark und kann nicht mehr ausschließlich während der Nachtstunden erfolgen. Es kommt daher zu Performanceeinbußen während der normalen Arbeitszeit. Daraufhin wurde entschieden, die Datensicherung nicht mehr auf klassische, agentenbasierte Weise auszuführen, sondern Snapshots zu verwenden. Diese werden jeweils abends zu einer bestimmten Zeit angelegt, die Daten werden gesichert und sobald der Sicherungsvorgang abgeschlossen ist, die Snapshots wieder gelöscht.

Diese Lösung läuft einige Zeit störungsfrei, jedoch wächst das Datensicherungsvolumen bald so stark an, dass ein neuer Datensicherungsprozess ausgelöst wird, bevor der vorherige abgeschlossen ist. Kurz darauf kommt es zu einem Ausfall aller virtuellen IT-Systeme auf dem Virtualisierungsserver, da der zur Verfügung stehende Speicherplatz erschöpft ist.

# G 4.79 Schwachstellen in der Bluetooth-Implementierung

Die Bluetooth-Spezifikationen enthalten viele Freiheiten, die dort beschriebenen Funktionen umzusetzen. Bereits in den Bluetooth-Spezifikationen finden sich diverse Schwachstellen, durch die jeweiligen Implementierungen der Bluetooth-Geräte können weitere Schwachstellen hinzukommen.

Um die Schwachstellen der Bluetooth-Implementierungen in Endgeräten bzw. der Bluetooth-Spezifikationen auszunutzen, sind diverse Angriffsverfahren bekannt. Im Folgenden sind einige der wesentlichen Angriffsverfahren dargestellt:

**Bluejacking**

Mit Bluejacking wird ein Übergriff bezeichnet, bei dem von einem Bluetooth-Endgerät, z. B. einem Handy oder PDA, per Bluetooth eine Nachricht auf ein fremdes Bluetooth-fähiges Gerät übertragen wird. Ziel ist es dabei in den meisten Fällen, dadurch beim Empfänger Befremden auszulösen. Als typische Nachrichten finden sich dann solche wie "Deine rote Hose gefällt mir sehr gut.", "Auf der Cebit sollten Sie auf Ihr Handy besser aufpassen." oder einfach "Hello, you've been bluejacked". Hierdurch wird vermittelt, dass einerseits ein tatsächlicher Angriff sehr leicht möglich wäre und dass man andererseits unter Beobachtung steht. Da Bluetooth allerdings nur im Nahbereich funktioniert, ist dies nicht weiter erstaunlich.

Die Nachricht, die hier übertragen wird, ist dabei nicht anderes als der Name des sendenden Bluetooth-Gerätes, der zu einer "Nachricht" ausgebaut wurde. Bei einer Verbindungsanfrage wird der Name des anfragenden Bluetooth-Geräts normalerweise auf dem Display des anderen Gerätes angezeigt. Der Name eines Bluetooth-Geräts ist frei wählbar und kann bis zu 248 Zeichen lang sein. Daher kann dieser auch dazu missbraucht werden, kurze Nachrichten zu übertragen, die den Benutzer verwirren sollen.

**Blueprint**

Mit dem Blueprint-Verfahren ist es möglich, die Kennung (ID) eines Bluetooth-Endgerätes auszulesen. Aufgrund dieser ID ist es möglich zu ermitteln, um welches Modell es sich bei dem Endgerät handelt. Wenn danach frei verfügbare Informationen, welche Schwachstellen bei dem Modell vorherrschen, ausgewertet werden, kann dann ein gezielter Angriff erfolgen.

**Bluesnarfing**

Bluesnarfing bezeichnet das Ausspionieren von Informationen aus Bluetooth-Mobiltelefonen wie Adressbüchern und Kalendereinträgen, ohne dass der Handybenutzer darauf aufmerksam wird. Bluesnarfing nützt eine Sicherheitslücke bei Bluetooth-Handys aus. Bei einigen Modellen besteht freier Zugriff auf gespeicherte Daten, wenn Bluetooth eingeschaltet und das Telefon auf "sichtbar" geschaltet ist.

Bei Bluesnarfing wird, ähnlich wie bei Bluejacking, ein fehlerhaft implementiertes Object Exchange Profil in Endgeräten ausgenutzt. Durch den Angriff ist es möglich, mit einem Bluetooth-Endgerät eine direkte Verbindung aufzubauen und beliebige Daten auszulesen, die auf dem Endgerät gespeichert sind. Dadurch können beispielsweise Informationen wie wie Adressbücher aus Mobiltelefonen ausspioniert werden, ohne dass deren Benutzer dies merken. Bei

Mobiltelefonen und Smartphones ist es dadurch auch möglich, die International Mobile Equipment Identity (IMEI) des Endgerätes auszulesen. Diese IMEI ist für jedes Endgerät eindeutig und ein Angreifer kann beispielsweise eingehende Gespräche auf ein Endgerät unter seiner Kontrolle umleiten, indem er dieses dazu bringt, vorzugeben das angerufene Endgerät zu sein. Mit dem Bluesnarfing++-Verfahren besteht zusätzlich die Möglichkeit, schreibend auf das Endgerät zuzugreifen.

**Bluebugging**

Durch das Bluebugging wird eine fehlerhafte Bluetooth-Implementierung in manchen älteren Endgeräten ausgenutzt, um einen Zugriff auf das Endgerät direkt bzw. die Kontrolle über das Endgerät zu erlangen. Hierbei werden beim Bluetooth-Protokoll RFCOMM (Radio Frequency Communication), welches dazu dient, serielle Schnittstellen zu emulieren, die Kanäle 16 und 17 ausgenutzt, um Daten auszulesen oder Einstellungen an dem Bluetooth-Endgerät vorzunehmen. Darüber hinaus können über Bluebugging ausgehende Telefongespräche initiiert und damit Kosten verursacht bzw. vom Benutzer geführte Telefongespräche überwacht werden. Über Bluebugging können auch andere Dienste beeinträchtigt werden, die das Endgerät anbietet. Bei älteren Endgeräten erhält der Benutzer keinerlei Hinweis darauf, dass sein Endgerät attackiert wird. Bei neueren Endgeräten wird meist eine Sicherheitsabfrage angezeigt, dass ein anderes Endgerät versucht, eine Verbindung zu dem eigenen Endgerät aufzunehmen.

**Bluesniping**

Als Bluesniping werden Angriffe bezeichnet, bei denen über größere Entfernungen mittels Richtfunkantennen gezielt Bluetooth-Geräte angegriffen werden. In Laborumgebungen wurden hierbei bereits Entfernungen von bis zu zwei Kilometern erreicht. Durch Bluesniping können die verschiedenen Bluetooth-Angriffsverfahren auf eine größere Umgebung ausgeweitet werden.

**Denial of Service / BlueSmacking**

Denial-of-Service-Angriffe zielen bei Bluetooth in der Regel darauf ab, durch Kompromittierung der Bluetooth-Schnittstelle entweder das Endgerät nicht nutzbar zu machen, beispielsweise weil ständig Pairing-Anfragen beantwortet werden müssen, oder die Batterie des Endgerätes schnell leer zu bekommen.Ein typischer Denial-of-Service-Angriff im Bluetooth-Umfeld ist BlueSmacking. Hierbei werden L2CAP-Anfragen missbraucht, um alle in Empfangsreichweite befindlichen Bluetooth-Geräte gleichzeitig zu stören. Die L2CAP-Anfrage "Echo Request" dient grundsätzlich dazu, ähnlich wie mit einem Ping-Kommando die Empfangsbereitschaft und die Verbindungsgeschwindigkeit zu testen.

# G 4.80 Unzureichende oder fehlende Bluetooth-Sicherheitsmechanismen

Die in den Bluetooth-Spezifikationen beschriebenen und von Herstellern entsprechend implementierten Sicherheitsmechanismen weisenverschiedene prinzipielle Schwächen auf. Einige von diesen werden im Folgenden kurz benannt.

**Verschlüsselung nicht vorgeschrieben**

Unabhängig vom verwendeten Sicherheitsmodus ist die Verschlüsselung der mit Bluetooth zu übertragenden Daten optional und muss von den Anwendungen explizit beantragt werden.

**Unsichere Voreinstellungen**

Die Voreinstellungen sind von Seiten der Hersteller oft unsicher konfiguriert. Sicherheitsfunktionen wie Authentisierung und Verschlüsselung sind häufig abgeschaltet und Passwörter bzw. PINs auf Standardwerte ("0000", "1234" usw.) eingestellt. Wenn Geräte keine Eingabemöglichkeit besitzen (z. B. Headsets), ist eine Änderung der voreingestellten Werte gar nicht oder nur umständlich möglich.

**Erraten schwacher PINs bei Bluetooth ohne Secure Simple Pairing (SSP)**

Beim Pairing zweier Bluetooth-Geräte wird ein Verbindungsschlüssel erzeugt und dauerhaft in beiden Geräten gespeichert. Dessen Erzeugung basiert unter anderem auf den Geräteadressen und einer PIN. Mit dem Verfahren Secure Simple Pairing (SSP) wird beim Verbindungsaufbau ein sicherer Kanal aufgebaut, ohne SSP werden die Authentisierungsinformationen unverschlüsselt übertragen.

Wird bei der Gerätepaarung eine schwache PIN verwendet, kann ein Angreifer die PIN erraten und damit den aus der Paarung resultierenden Verbindungsschlüssel berechnen. Dazu muss der Angreifer nur die Paarung und die folgende Authentisierung abhören. Ohne SSP kann der Angreifer anhand der Aufzeichnungen der abgehörten Protokolle überprüfen, ob die PIN von ihm korrekt geraten wurde.

Als sicherheitskritisch anzusehen ist, dass die PIN bei Bluetooth ohne SSP als einziger geheimer Parameter in die Erzeugung des Verbindungsschlüssels einfließt. Erfahrungsgemäß lassen sich weit verbreitete Nutzer- bzw. Herstellergewohnheiten zu schwachen Sicherheitseinstellungen nur schwer durchbrechen. In der Tat gibt es kaum Bluetooth-Geräte, die den Benutzern eine Mindestlänge und Komplexität für die PIN vorgeben. Es bleibt im Allgemeinen den Benutzern überlassen, welche PIN sie wählen.

**Re-Initialisierung semipermanenter Verbindungen bei Bluetooth ohne SSP**

Die Bluetooth-Spezifikation sieht die Möglichkeit vor, dass eine erneute Authentisierung durchgeführt werden kann, beispielsweise wenn festgestellt wird, dass der Verbindungsschlüssel in einem der Geräte verloren gegangen ist. Dies bietet einem Angreifer die Möglichkeit, im passenden Moment ein entsprechendes Paket mit der Aufforderung der Reinitalisierung der Verbin-

dung in die laufende Kommunikation zweier Geräte einzubringen. Hierdurch wird eine erneute Paarung provoziert, die dann abgehört werden kann.

**Keine verbindliche Vorgabe einer ausreichenden Schlüssellänge**

Neben Länge und Komplexität der bei der Authentisierung (bei Bluetooth ohne SSP) verwendeten PIN spielt auch die Länge der für die Verschlüsselung der übertragenen Daten verwendeten Schlüssel eine Rolle für die Sicherheit. Während die Bluetooth-Spezifikation für Schlüssel, die zur Authentisierung benutzt werden, eine Schlüssellänge von 128 Bit fest vorschreibt, kann die Länge des für die Verschlüsselung der weiteren Paketinhalte verwendeten Schlüssels variieren. Beide Geräte handeln im Rahmen des Verbindungsaufbaus die tatsächlich genutzte Schlüssellänge aus. Die Bluetooth-Spezifikation sieht hier eine Spannweite von 8 bis 128 Bit vor, d. h. es könnte eine minimale Schlüssellänge von 8 Bit verwendet werden, ohne gegen die Spezifikation zu verstoßen.

In der Spezifikation wird sogar ausdrücklich ausgeschlossen, dass die minimale Schlüssellänge durch den Anwender verändert werden kann. Diese kann nur über die Werkseinstellung des Herstellers definiert werden. Die Güte der erreichbaren Verschlüsselung ist damit allein abhängig von der Herstellerentscheidung.

**Schwache Integritätssicherung**

Zur Integritätssicherung wird ein Cyclic Redundancy Check (CRC, Verfahren zur Erkennung von Übertragungsfehlern anhand einer Prüfsumme) verwendet. Dadurch werden zwar mit hoher Wahrscheinlichkeit zufällige Störungen bei der Übertragung von Datenpaketen erkannt, aber gegen eine absichtliche Manipulation von Datenpaketen bieten CRC-Verfahren keinen Schutz.

**Qualität des Zufallsgenerators**

Zur Zufallserzeugung sehen die Bluetooth-Spezifikationen 1.x und 2.0 + EDR die Verwendung eines sogenannten Pseudozufallszahlen-Generators vor. Es wird jedoch keine Vorgabe für dessen Implementierung gemacht. Es ist daher nicht auszuschließen, dass die verwendeten Zufallszahlen-Generatoren Schwächen aufweisen, die sich für das Überwinden der kryptographischen Verfahren ausnutzen lassen. In der Bluetooth-Spezifikation ab 2.1 + EDR wird hingegen die Verwendung eines Zufallszahlen-Generators gemäß der Norm FIPS 140-2 gefordert.

**Verkürzter Initialisierungsvektor**

Jedes übertragene Datenpaket wird unter Verwendung eines neuen Initialisierungsvektors verschlüsselt. Dieser errechnet sich unter anderem aus dem Zeittakt des Masters. Es wird allerdings das höchstwertige Bit des Zeittaktes "vergessen". Durch diese Schwäche lassen sich selbst bei eingesetzter Verschlüsselung Man-in-the-Middle-Angriffe durchführen, da es immer zwei unterschiedliche Offsets in der Sprungsequenz zu einem Initialisierungsvektor gibt. Ein Man-in-the-Middle-Angriff auf eine verschlüsselte Verbindung erlaubt jedoch nur, den Datenstrom zu manipulieren, nicht jedoch, diesen zu entschlüsseln.

**Manipulation von verschlüsselten Daten**

Aufgrund der Eigenschaften von Stromchiffren im Zusammenwirken mit dem zur Integritätssicherung eingesetzten CRC ist es möglich, Änderungen am Chiffrat vorzunehmen, so dass der Empfänger das Paket nach wie vor als gül-

tig erkennt. So ist es beispielsweise bei Bluetooth ohne SSP im Rahmen eines Man-in-the-Middle-Angriffs möglich, IP-Header gezielt zu manipulieren.

# G 4.81 Erweiterte Rechte durch Programmdialoge auf Terminalservern

Sichere Konfigurationen von Terminalservern sehen zumeist einen restriktiven Zugriff vor. Hierzu dürfen nur bestimmte Anwendungen, die in einer Positivliste (Whitelist) aufgeführt sind, dem Benutzer angeboten und gestartet werden. Der Zugriff auf den gesamten Desktop, der eine Vielzahl von Start- und Interaktionsmöglichkeiten von und mit Anwendungen erlaubt, wird in der Regel unterbunden. Häufig lassen sich jedoch über Programmdialoge in freigegebenen Anwendungen weitere Applikationen starten und Lese- wie Schreibberechtigungen ausdehnen.

**Unerlaubte Dateizugriffe**

Besonders Dialoge, in denen Dateien geöffnet und gespeichert werden können, sind exponierte Angriffspunkte, um auf ungesicherte Verzeichnisse und Laufwerke des Terminalservers zu gelangen. Ohne besondere Vorkehrungen sind beispielsweise die Benutzer bei auf Windows basierenden Lösungen in der Lage, auf das eigentlich verborgene Laufwerk M zuzugreifen, das das Betriebssystem beherbergt. Bei Unix-basierten Lösungen kann ebenfalls ohne ein entsprechendes Rechtekonzepte auf alle Ressourcen innerhalb des Verzeichnisbaums zugegriffen werden. Auch vermeintlich ungefährdete Dialoge, wie Hilfefunktionen, Druckdialoge etc., können Menüpunkte enthalten, die ein Ausspähen des Terminalservers ermöglichen.

**Directory Traversal**

Über den "Verzeichnis übergreifenden Zugriff" (Directory Traversal) kann gegebenenfalls in übergeordnete Dateiordner gewechselt werden. Hierfür können beispielsweise die üblichen Schaltflächen zur Navigation durch die Verzeichnisstruktur genutzt werden. Sind diese durch den Systemadministrator deaktiviert worden, kann der Schutz durch die direkte Eingabe von Zeichenketten, wie z. B. "../" auf Unixsystemen oder "..\" unter Windows, umgangen werden.

**Uniform Ressource Identifier**

Uniform Ressource Identifier (URI) identifizieren virtuelle sowie physische Ressourcen und verknüpfen so lokale oder auf einem Server bereitgestellte Dateien mit lokal installierten Anwendungen. Wird ein URI angeklickt, wird die angegebene Datei mit der vorher festgelegten Anwendung geöffnet. Hierdurch kann der Anwender unter Umständen direkt auf die Datei zugreifen, in deren Verzeichnis er sonst nicht wechseln darf. Das genaue Verzeichnis, in dem sich die festgelegte Applikation befindet, muss der Anwender ebenfalls nicht kennen und kann so eventuell auf Anwendungen zugreifen, auf die er nicht zugreifen darf.

Neben den ursprünglich für Browser definierten URI-Typen http:// und ftp:// existieren inzwischen zahlreiche weitere Typen, deren Verwendung nicht mehr nur auf Dialoge in Internetanwendungen beschränkt ist. Eine aktuelle Übersicht pflegt die Internet Assigned Numbers Authority (IANA) gemäß der RFC4395. Überdies registrieren einige Programme eigene URI, die noch nicht Bestandteil des Standards sind.

Beispiele für weitere häufig registrierte URI sind:

- file://
  Erlaubt den Zugriff auf das lokale Dateisystem
- tftp://
  Trivial File Transfer Protocol, gestattet gegebenenfalls den Dateizugriff eingebettete Systeme wie Router, Drucker etc.
- mailto://
  Startet das im System als Standard registrierte E-Mail-Programm
- telnet://
  Startet eine Telnet-Applikation
- nfs://
  Network File System Protocol, Zugriff auf NFS-Dateiserver
- skype://, callto://
  Verknüpfung mit Voice-Over-IP Anwendungen

# G 4.82 Ausfall und Nichterreichbarkeit von Terminalservern

Bei einer klassischen Client-Server-Architektur werden Applikationen, wie Textverarbeitung, auf den Clients der Benutzer ausgeführt. Besteht gerade kein Kontakt zu einem benötigten Server, kann oftmals, je nach Anwendung, asynchron an den Clients weitergearbeitet werden. So kann beispielsweise bei einem Ausfall des Netzes ein geöffnetes Dokument auch zu einem späteren Zeitpunkt auf dem Dateiserver gespeichert werden. Ist ein Mailserver für kurze Zeit nicht verfügbar, wird die Nachricht üblicherweise von dem Mail-Client zwischengespeichert und verzögert übertragen. Unter Umständen wird ein solcher Zwischenfall überhaupt nicht vom Benutzer bemerkt.

In einer Umgebung mit Terminalservern hingegen werden die Applikationen zentral ausgeführt und deren Ausgabe auf das entsprechende Terminal übertragen. Ist der Terminalserver nicht verfügbar, können keine Benutzereingaben mehr verarbeitet werden und die von dem Server bereitgestellten Anwendungen versagen unmittelbar ihren Dienst. Beziehen die Clients, wie z. B. in einer Thin-Client Umgebung üblich, die gesamte Benutzeroberfläche, einschließlich des Betriebssystems, von dem entfernten Server, fällt aus der Perspektive des Benutzers gesehen, dass IT-System vollständig aus.

Von Ausfällen des Netzes oder des Terminalservers sind in der Regel nicht nur einzelne Benutzer betroffen. In vielen Fällen sind zahlreiche oder sogar alle Clients der Institution auf den Terminalserver angewiesen. Fällt ein Terminalserver aus, sind in diesem Fall eine große Anzahl von Benutzern gleichzeitig betroffen.

**Beispiel:**

Ein kommunaler Dienstleister führt für mehrere seiner Geschäftsbereiche Terminalserver ein. Hierfür werden zwar mehrere Terminalserver beschafft, aber an Stelle einer zentralen Terminalserver-Farm erhält jeder Geschäftsbereich einen eigenen Terminalserver. Hierdurch können Kosten für Loadbalancer gespart und Kommunikationswege zwischen Client und Server verkürzt werden.

Nach einigen Monaten, in denen die Terminalserver stabil arbeiten, fällt ein Server aus und der gesamte Geschäftsbereich kann bis zur Reparatur nicht mehr arbeiten. Nach einigen weiteren Monaten konnte ein anderer Geschäftsbereich expandieren und konnte dadurch zahlreiche zusätzliche Mitarbeiter einstellen. Die damit erhöhte Auslastung des Terminalservers des Geschäftsbereich wurde ausgeglichen, in dem die neuen Mitarbeiter auf die weniger ausgelasteten Terminalserver der anderen Geschäftsbereiche verteilt wurden. Dies führte zu unstrukturiertem "Chaos" auf den Terminalservern und zu einem erheblichen organisatorischen Aufwand .

# G 4.83 Fehlfunktionen selbstentwickelter Makros unter Outlook

Viele Softwarehersteller sehen aus Gründen der Interoperabilität in ihren Tools und Anwendungen Programmierschnittstellen vor, z. B. als Application Programming Interface (API). Diese erlauben es, bestimmte Funktionen auch aus anderen Programmen heraus zu nutzen oder den Funktionsumfang der Anwendung zu erweitern. Dabei können Fehler und falsche Berechnungen in Makros ein erhöhtes Risiko darstellen. Als vorsätzliche Handlung könnte selbstentwickelte Software mit Schadfunktion auch für Angriffe genutzt werden (siehe G 5.164 *Missbrauch von Programmierschnittstellen unter Outlook*).

Für Microsoft Outlook werden Programmierschnittstellen angeboten, mit denen Benutzer eigene Anwendungen oder Funktionserweiterungen (Makros) schreiben können, die über den Client Nachrichten, Termine und Aufgaben verschicken und empfangen können.

**Beispiel:**

- Durch ein Makro werden für eine Statistik bestimmte Schlüsselwörter in E-Mails gesammelt. Das Makro zählt durch einen Indexfehler falsch. Dadurch werden falsche wirtschaftliche Entscheidungen wie Käufe oder Verkäufe ausgelöst.

# G 4.84 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services

Webanwendungen werden im Allgemeinen von generischen Clients (Web-Browsern) verwendet, sodass Benutzer beliebige Eingabedaten an den Server übermitteln können. Auf Web-Services wird dagegen durch andere Anwendungen oder Dienste zugegriffen (beispielsweise Smartphone-Apps). Eingabedaten können aber auch hier oft modifiziert werden, beispielsweise durch den Einsatz eines Proxys oder durch Manipulation der Clients. Werden schadhafte Eingaben eines Angreifers von der Webanwendung beziehungsweise dem Web-Service verarbeitet, können möglicherweise Schutzmechanismen umgangen werden.

Beispiele für Angriffe, die auf einer unzureichenden Validierung von Eingabedaten beruhen, sind SQL-Injection (siehe G 5.131 *SQL-Injection*), Path Traversal (siehe G 5.172 *Umgehung der Autorisierung bei Webanwendungen und Web-Services*) und Remote File Inclusion. Diese Angriffe können Unbefugten Zugriff auf das Betriebssystem oder auf Hintergrundsysteme ermöglichen. Bei einem erfolgreichen Angriff können schützenswerte Daten unautorisiert ausgelesen oder manipuliert werden.

Nachdem die Webanwendung beziehungsweise der Web-Service die Eingabedaten erfolgreich verarbeitet hat, werden üblicherweise wieder Daten ausgegeben. Die Ausgabedaten werden entweder direkt an den Browser des Benutzers (zum Beispiel Statusmeldungen oder ein neuer Eintrag im Gästebuch) oder die aufrufende Anwendung übermittelt oder an nachgelagerte Systeme weitergereicht. Werden die Daten vor der Ausgabe nicht ausreichend validiert, könnten die Ausgaben Schadcode enthalten, der auf den Zielsystemen interpretiert oder ausgeführt wird.

Die folgenden Beispiele beschreiben mögliche Auswirkungen einer unzureichenden Validierung von Ein- und Ausgaben:

- Eine Webanwendung beziehungsweise ein Web-Service verwendet Eingabedaten ungefiltert zur Erzeugung von Datenbankabfragen. Dies kann ein Angreifer ausnutzen und eine Anfrage formulieren, die neben den regulären Eingabedaten zusätzliche Befehle für die Datenbank enthält. Durch das ungefilterte Einbetten der Eingabedaten in die Datenbankabfrage werden die Befehle von der Datenbank ausgeführt. So kann der Angreifer direkten Zugriff auf die Datenbank erhalten.
- Eine Webanwendung bietet eine Funktion zum Datei-Upload an und schränkt diese auf gewisse Dateitypen ein. Zur Bestimmung des Dateityps überprüft die Webanwendung ausschließlich die Dateiendung und berücksichtigt dabei nicht den Inhalt der Datei. Wird eine erlaubte Dateiendung für den Upload verwendet, können so Dateien mit beliebigem Inhalt zum Server übermittelt werden.
- Werden Eingabedaten durch die Filterkomponente automatisiert geändert und angepasst (Sanitizing), können die Daten durch gezielte Eingaben eines Angreifers von der Filterkomponente in einen Angriffsvektor überführt werden.
- Ein- und Ausgabedaten können in verschiedenen Kodierungen (zum Beispiel UTF-8, ISO 8859-1) und Notationen (zum Beispiel bei UTF-8 ist "." = "2E" = "C0 AE") vorliegen. Abhängig vom angewandten Kodierungssche-

ma kann der gleiche Wert unterschiedlich interpretiert werden. Interpretiert die Filterkomponente die Daten anders als die verarbeitenden Komponenten der Webanwendung oder des Web-Service, so kann ein Angreifer schadhafte Daten (zum Beispiel SQL-Anweisungen) derart codieren, dass sie bei der Filterung nicht erkannt werden. Somit werden die vom Angreifer schadhaften Daten an die verarbeitenden Komponenten weitergereicht und aufgrund der unterschiedlichen Interpretation ausgeführt.

- Die Kommentar-Funktion einer Webanwendung erlaubt eine Formatierung der Texte durch HTML. Die Eingaben werden zum Beispiel nicht auf spezielle HTML-Tags eingeschränkt, sodass ein Angreifer über diese Funktion beliebigen HTML-Code auf der Webanwendung platzieren kann. Dies kann ein Angreifer dazu nutzen, um Elemente der Webseite zu manipulieren oder zu überlagern und Benutzereingaben abzufangen (siehe G 5.175 *Clickjacking*). Derselbe Angriff ist übertragbar auf Web-Services, welche HTML-Code als Eingabe erlauben und diesen ungefiltert in ihre Ausgabe übernehmen.

# G 4.85 Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services

Treten Fehler während des Betriebs einer Webanwendung oder eines Web-Service auf, kann dies unvorhersehbare Auswirkungen haben und die Verfügbarkeit der Webanwendung oder des Web-Service bis zur Unerreichbarkeit einschränken. So werden gegebenenfalls Aktionen unvollständig durchgeführt, zwischengespeicherte Zustände und Daten gehen verloren oder Sicherheitsmechanismen fallen aus. Werden Fehler nicht korrekt behandelt, kann sowohl der Betrieb als auch der Schutz der Funktionen und Daten einer Webanwendung oder eines Web-Service nicht mehr gewährleistet werden.

Beispiele:

- Im laufenden Betrieb belegen Webanwendungen und Web-Services üblicherweise Ressourcen, wie offene Netz- oder Datei-Streams, um auf Hintergrundsysteme, zwischengespeicherte Zustände oder sonstige Daten zugreifen zu können. Solange die Webanwendung/der Web-Service auf diese Ressourcen zugreift, sind diese häufig für den exklusiven Zugriff reserviert und können nicht durch andere Prozesse verwendet werden. Werden im Fehlerfall die belegten Ressourcen nicht ordnungsgemäß freigegeben, so bleiben diese gegebenenfalls in einem blockierten Zustand. Dadurch können Daten verloren gehen, da beispielsweise zwischengespeicherte Änderungen nicht ordnungsgemäß geschrieben werden können.
- Treten während der Ausführung der Sicherheitskomponenten (zum Beispiel Authentisierung, Autorisierung) Fehler auf und werden diese unzureichend behandelt, so werden angeforderte Aktionen möglicherweise unkontrolliert ausgeführt. Aktionen, die im normalen Zustand abgelehnt werden, könnten im Fehlerfall zugelassen werden.
- Fehlermeldungen können detaillierte Hinweise zur Fehlerursache beinhalten, die für den Benutzer nicht notwendig sind jedoch gezielte Angriffe ermöglichen. Zu diesen detaillierten Informationen gehören Stacktraces, Debugging-Ausgaben, Fehlermeldungen bei ungültigen SQL-Abfragen, Angaben zu verwendeten Webservern und anderen Anwendungskomponenten. Auch scheinbar unkritische Informationen, wie die Meldung bei einer fehlgeschlagenen Anmeldung mit Benutzernamen und Passwort, dass der Benutzernamen bekannt ist, aber ein ungültiges Passwort eingegeben wurde, können zum Beispiel im Rahmen von Brute-Force-Angriffen ausgenutzt werden. In diesem Fall weiß der Angreifer, dass der Benutzername existiert.
- Wird die Fehlerbehandlung ausschließlich auf dem Client (zum Beispiel Webbrowser oder Anwendung, welche einen Web-Service nutzt) durchgeführt, kann sie manipuliert oder außer Kraft gesetzt werden. Ein Angreifer kann somit die Behandlung der Fehler beeinflussen und steuern.

# G 4.86 Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen

Werden sicherheitsrelevante Ereignisse von der Webanwendung unzureichend protokolliert, können diese zu einem späteren Zeitpunkt nicht nachvollzogen und die Ursache nicht mehr ermittelt werden. Kritische Fehler und Angriffe bleiben gegebenenfalls unbemerkt und die Behebung einer Schwachstelle ist dann nicht oder nur unter erschwerten Bedingungen möglich.

Werden darüber hinaus Ereignisse auf der System- und Netzebene nur eingeschränkt protokolliert, sind sicherheitsrelevante Vorfälle nur noch schwer zu erkennen und nachzuvollziehen.

**Beispiele:**

- Sicherheitsrelevante Ereignisse der Webanwendung werden nicht oder nur eingeschränkt protokolliert. So bleiben unbefugte Konfigurationsänderungen (z. B. durch einen Angreifer) unentdeckt.
- Es werden nicht alle notwendigen Eigenschaften eines Ereignisses protokolliert, sodass Vorgänge nicht vollständig nachvollzogen werden können (z. B. nur das Datum, aber keine Uhrzeit).
- Ist der Schutz der Protokolldaten nicht gewährleistet, können sie unbemerkt manipuliert werden. Somit kann ein Angreifer Hinweise auf durchgeführte Aktionen löschen und der Angriff bleibt unentdeckt oder ist nicht mehr nachvollziehbar.

# G 4.87 Offenlegung vertraulicher Informationen bei Webanwendungen

Webseiten und Daten, die von einer Webanwendung generiert und ausgeliefert werden, können vertrauliche Informationen enthalten, die nicht für die Nutzung der Webanwendung erforderlich sind, zum Beispiel Angaben zu Produkt und Versionsständen von Frameworks. Diese Informationen können einem Angreifer Hinweise zur Durchführung gezielter Angriffe auf die Webanwendung geben. Wenn also Informationen unnötig offengelegt werden, kann dies einen Angriff erleichtern. Hierbei können Informationen auch über weniger offensichtliche Übertragungswege übermittelt werden, zum Beispiel im HTTP- oder SOAP-Header.

**Beispiele:**

- Es werden detaillierte Informationen über Sicherheitsmechanismen oder -attribute ausgegeben, die für einen Benutzer der Webanwendung nicht notwendig sind, aber Hinweise für potenzielle Angriffe geben, zum Beispiel "Geben Sie bitte die 6-stellige, numerische PIN ein" anstelle von "Geben Sie bitte die PIN ein". Aufgrund dieser Information könnte ein Angreifer den möglichen Zeichenraum bei einem Brute-Force-Angriff einschränken und somit schneller eine gültige PIN ermitteln.
- Kommentare, zum Beispiel im HTML-Quelltext, können Informationen zu bekannten Fehlern, Funktionsweisen, eingesetzten Techniken und der angebundenen Infrastruktur beinhalten. Ein Angreifer kann hierdurch gezielt nach Schwachstellen in der Webanwendung und der Infrastruktur suchen und diese ausnutzen. Werden beispielsweise die in der Entwicklungsphase verwendeten Zugangsdaten für eine Datenbank in Kommentaren erwähnt, können Angreifer diese womöglich auch noch im produktiven Betrieb der Webanwendung für den unautorisierten Zugriff benutzen.
- Dateien mit unbekannter Dateiendung, zum Beispiel temporäre Dateien mit .tmp oder Backup-Dateien mit .bak von Skripten der Webanwendung, werden von der Webanwendung im Quelltext ausgeliefert. Auf diese Weise lassen sich vertrauliche Informationen wie fest kodierte Zugangsdaten auslesen. Darüber hinaus können Angreifer Programmabläufe aus offengelegten Code auf Schwachstellen untersuchen.
- Besitzt ein Angreifer die nötigen Informationen, um XML-Nachrichten innerhalb eines Transportcontainers zu erstellen, so kann er testen, ob bestimmte Parameter innerhalb einer Nachricht übermittelt werden, zum Beispiel in REST, SOAP, ZIP. Die zurückkommenden Fehlermeldungen des Service-Providers beinhalten eventuell für einen Angriff nützliche Informationen, zum Beispiel Angaben über das verwendete Framework, Programmbibliotheken oder interne Systemstrukturen. Darüber hinaus kann der Angreifer gegebenenfalls über Fehlercodes feststellen, ob Eingaben geprüft oder bestimmte Aktionen ungefiltert durchgeführt werden. Findet keine Filterung statt, kann er sogenannte Injection-Angriffe durchführen. Diese stellen eine erhebliche Bedrohung für die Backend-Anwendungen dar (siehe G 5.143 *Man-in-the-Middle-Angriff*).

# G 4.88 EMV-untaugliche Stromversorgung

Moderne IT-Systeme zeichnen sich unter anderem zunehmend durch folgende drei Eigenschaften aus:

- extrem hohe Vernetzung
- extrem hohe Taktraten
- sehr kleine Signalpegel

Genau diese drei Eigenschaften machen moderne IT-Netze zunehmend anfällig gegen Störungen aus nicht EMV-tauglichen Stromversorgungsnetzen, also solchen, die nicht elektromagnetisch verträglich sind. Als wesentliche Störquellen sind hierbei zu nennen:

**Aufbau der Stromversorgung in der falschen Netzform (kein TN-S-System)**

Alle anderen Netzformen, außer TN-S-Systemen und TT-Systemen mit guten durchgängigen Erdern, fördern das Auftreten von Strömen auf dem PE-System.

**Unzulässige Ströme auf dem PE-System und unzulässige induktive Kopplung durch nicht EMV-gerechten Schaltschrankaufbau**

Ströme auf dem PE-System beeinträchtigen die Datenübertragung auf kupfergebundenen Datenleitungen und führen zu vorzeitigen Versagen technischer Einrichtungen.

**Zu hohe Pegel von Störfrequenzen ab 150 Hz aufwärts bis in den 100 kHz-Bereich hinein**

Nicht nur die üblicherweise betrachteten Harmonischen bis 1 kHz oder 2 kHz, sondern auch die weit darüber liegenden Störfrequenzen können die Datenübertragung und die Funktion von IT-Geräten massiv beeinträchtigen.

**Elektromagnetische Felder durch unsachgemäße Leitungsverlegung**

Elektromagnetische Felder bewirken Ströme auf elektrisch leitfähigen Systemen, die dort eigentlich gar nicht fließen sollen und können dadurch in allen Bereichen rund um die IT zu Schäden führen.

**Falsche Anpassung an den tatsächlichen Wirkfaktor (kurz auch "cos Phi" oder "Cosinus Phi") der versorgten Verbraucher**

Viele Stromversorgungssysteme inklusive eventuell vorhandener Netzersatzanlagen (NEA) und USV-Anlagen sind noch auf die Versorgung induktiver Lasten ausgelegt, während die überwiegende Mehrheit aller IT-Geräte für ein stark kapazitives Lastverhalten im Netz sorgen. Folge dieser Fehlanpassung sind neben hoher Verlustleistungen auch unkalkulierbare Ausfälle von Stromerzeugern (NEA und USV) und Verbrauchern.

**Nicht vorhandene Information über den aktuellen Betriebszustand des Stromversorgungssystems, insbesondere über die Korrektheit des TN-S-Systems**

Ohne ausreichende Kenntnis aller Betriebszustände des Stromversorgungssystems in Echtzeit können sich anbahnende Probleme nicht erkannt werden.

Ohne eine Aufzeichnung dieser Echtzeitdaten ist es nahezu unmöglich, bei Schadensfällen deren tatsächliche Ursache zu ermitteln und zu beheben.

# G 4.89 Fehlendes oder unzureichendes Alarmierungskonzept bei der Protokollierung

Produkte, die Protokoll- und Monitoringdaten speichern und auswerten, können häufig als optionale Komponenten in ein IT-Frühwarnsystem eingebunden werden. IT-Frühwarnsysteme werden eingesetzt, um bereits während eines Sicherheitsvorfalls zu warnen, noch bevor mögliche Auswirkungen spürbar sind. Dies ist insbesondere bei einer zentralen Protokollierung wirkungsvoll. Durch sinnvoll ausgewertete Protokollereignisse können solche Sicherheitsvorfälle schneller entdeckt werden.

Allerdings muss die Überwachung eine Alarmierungskomponente enthalten. Es wirkt sich sonst negativ auf die Verfügbarkeit, Vertraulichkeit und Integrität der Systeme aus, wenn der gesamte Informationsverbund überwacht wird und auch die Protokolldaten ausgewertet werden, aber nicht alarmiert wird.

**False-Positives und False-Negatives**

Zu niedrig oder zu hoch eingestellte Grenzwerte sind häufige Fehler in Alarmierungskomponenten. Diese Grenzwerte bestimmen den Punkt, ab dem alarmiert wird. Zu niedrig eingestellte Grenzwerte können zu Fehlalarmen (False-Positives) führen. Bei zu hohen Grenzwerten wird kein Alarm trotz eines IT-Sicherheitsvorfalls ausgelöst (False-Negatives).

False-Positives können auch daher rühren, dass die Administratoren bestimmte Systeme, die fälschlicherweise oft als bösartig identifiziert werden, nicht auf die Ausnahmelisten (Whitelists) setzen. Hierzu gehören beispielsweise Schwachstellen-Scanner oder Monitoring-Stationen, die sich sehr häufig zu anderen Systemen und Diensten auf unterschiedlichen Ports verbinden und häufig Grenzwerte überschreiten. Whitelists lassen sich aber auch von Angreifern missbrauchen, um bei einem Angriff auf ein IT-System keinen Alarm auszulösen (False-Negative). Sind zu viele Systeme in den Whitelists eingetragen, können viele False-Negative-Vorfälle entstehen.

**Falsche Reaktion auf Sicherheitsvorfälle**

Ein weiteres Problem stellt eine falsche Reaktion auf eingetretene Sicherheitsvorfälle dar. Es können unter Umständen große Schäden bis hin zu Katastrophen entstehen, beispielsweise wenn angegriffene Dienste abgeschaltet werden oder die Sprinkleranlage bei einem Zutrittsalarm ausgelöst wird. Möglich ist auch, dass das Personal Sicherheitsvorfälle falsch interpretiert und einen Alarm ignoriert, der durch einen Angriff ausgelöst wurde. Solche Gefährdungen werden durch mangelhafte oder falsche Schulungen der Administratoren begünstigt.

**Beispiel:**

- Die zuständigen Administratoren für das IT-Frühwarnsystem entdecken in den Protokolldateien eines Sicherheitsgateways auffällige Einträge. Sie gehen dem Fall aber nicht weiter nach, da die Einträge von einem System stammen, das auf der Whitelist steht. Einen Tag zuvor wurde ein Angriff auf den Protokollierungsserver erkannt, der ausgelöste Alarm jedoch als Fehlalarm interpretiert. Dadurch konnte sich ein Angreifer Zugriff auf den Protokollierungsserver verschaffen und das Sicherheitsgateway auf die Whitelist setzen. Somit konnten die Angreifer nach weiteren Versuchen

die Firewall mit einem erfolgreichen Angriff unbemerkt überwinden und in das interne Netz der Institution eindringen.

# G 4.90 Ungewollte Preisgabe von Informationen durch Cloud Cartography

Das Ziel von Cloud Cartography ist es, die Infrastruktur des Cloud-Diensteanbieters zu kartieren, um zu ermitteln, wo eine bestimmte virtuelle Maschine betrieben wird. Bei erfolgreicher Cloud Cartography erlangt ein Angreifer aus den Informationen über erreichbare Cloud-Elemente ein detailliertes Bild der internen Netzstruktur des Cloud-Diensteanbieters. Diese Informationen können als Grundlage für weiterführende Angriffe dienen.

Durch Abfragen sowohl von außerhalb als auch von innerhalb der Cloud lässt sich das prinzipielle Layout des Netzes ermitteln: Mit Hilfe von Whois-Abfragen werden öffentliche IP-Adressbereiche ermittelt. Über Werkzeuge zum Herunterladen von Webinhalten erfährt man, auf welchen Servern der HTTP-Dienst aktiv ist und per Cloud-interner DNS-Abfrage ermittelt man private IP-Adressen und gegebenenfalls Hostnamen. Ein wertvolles Ergebnis für einen Angreifer kann sein, die geografischen Verfügbarkeitsbereiche und die mietbaren virtuellen Leistungsklassen der Cloud-Dienste oder der damit verbundenen virtuellen Maschinen den internen IP-Adressbereichen zuordnen zu können. Unter Umständen können statische Zuordnungen von virtuellen Instanzen zu physischen Cloud-Ressourcen zu priorisierten Angriffszielen führen. Mithilfe verschiedener Verfahren kann ein Angreifer feststellen, ob eine selbst gestartete virtuelle Instanz in der Cloud mit einer fremden virtuellen Instanz benachbart ist, also auf der gleichen physischen Maschine läuft. Die fremde virtuelle Instanz wird so ein mögliches Angriffsziel.

# G 4.91 Unberechtigtes Wiedereinspielen von Snapshots

Mit Hilfe von Snapshots kann der Status einer virtuellen Maschine zu einem bestimmten Zeitpunkt konserviert werden, ohne dass die Ausführung des virtuellen IT-Systems hierdurch beeinträchtigt wird.

Beim Anlegen eines Snapshots wird die virtuelle Festplatte eingefroren und nachfolgende Schreibzugriffe werden in eine separate Datei umgeleitet. Der aktuelle Zustand ergibt sich bei virtuellen Maschinen mit aktiven Snapshots aus der Überlagerung aller Snapshots mit der Basis-Datei.

Snapshots können mit oder ohne Inhalt des Arbeitsspeichers des virtuellen IT-Systems angelegt werden. Ohne Arbeitsspeicherinhalt spiegeln Snapshots meist den Zustand des virtuellen IT-Systems wieder, das nicht heruntergefahren, sondern im laufenden Betrieb ausgeschaltet wurde. Snapshots mit Arbeitsspeicherinhalt erlauben es, das IT-System exakt in den Zustand zu versetzen, wie es zum Zeitpunkt des Snapshots vorlag, d. h. es ist eine Rückkehr in ein laufendes Betriebssystem mit geöffneten Anwendungen möglich.

Ein Cloud-Administrator kann bei Bedarf (z. B. vor Einspielen eines Patches) einen Snapshot und somit eine Sicherungskopie des Systems erstellen. Mit diesem Snapshot ist jederzeit eine Rücksicherung des Systems möglich, falls beispielsweise ein Patch nicht ordnungsgemäß funktioniert.

Beim Einspielen eines falschen Snapshots könnte eine veraltete Version des Systems eingespielt werden, in dem alte Sicherheitseinstellungen oder Patches enthalten sind, die wiederum zu Schwachstellen im System führen könnten.

Die Snapshots können aber auch auf unberechtigte Art und Weise vom Administrator wieder eingespielt werden. So ist es denkbar, dass ein Administrator unbefugt eine Snapshot-Kopie auf einem Fremdsystem einspielt und somit eine vollständige Spiegelung des IT-Systems in einer Fremdumgebung erstellt. In dieser Fremdumgebung kann er unbemerkt versuchen, Zugriff auf das System zu erlangen.

**Beispiel:**

- Ein Cloud-Administrator erstellt einen Snapshot von einem System, auf dem eine Datenbank mit Personaldaten für eine HR-Anwendung läuft. Er kopiert diesen Snapshot unbemerkt auf eine externe Festplatte und installiert ihn später auf seiner privaten Virtualisierungsplattform. Anschließend konvertiert er das System auf eine bootfähige Festplatte. Mit einem Wiederherstellungs-Tool kann er nun das Betriebssystem dieser Festplatte starten und das lokale Administrator-Passwort des Systems zurücksetzen. Anschließend kann er das System als Administrator starten und sich die notwendigen Datenbank-Berechtigungen vergeben, um auf die Datenbankinhalte zugreifen zu können.

# G 4.92 Inkompatibilität zwischen der Cloud-Administration und der Administration der Cloud-Elemente

Eine Cloud-Infrastruktur setzt sich aus einer Vielzahl von Cloud-Elementen zusammen. Neben den physischen (mit CPU, Arbeitsspeicher und anderer Hardware) und virtuellen Servern (mit den virtuellen Pendants zur Hardware der physischen Server) zählen noch Netze (mit Netzkoppelelementen, Verkabelung) und Speicherlösungen dazu. Die aufgezählten Bereiche verfügen über eine Verwaltungssoftware, wie z. B. Netzmanagement-Werkzeuge. Diese nennt man auch *Element Manager.* Die Cloud-Verwaltungssoftware kommuniziert in der Regel mit den *Element Managern* und nicht direkt mit den zugehörigen Komponenten (z. B. Router).

Eine Gefährdung durch fehlerhafte Kommunikation zwischen Cloud-Verwaltungssoftware und Cloud-Elementen tritt auf, wenn Produkte verschiedener Hersteller (oder auch desselben) zueinander inkompatibel sind und keine gemeinsamen Protokolle unterstützen.

Eine zentrale Verwaltungssoftware kommuniziert mit den Cloud-Elementen über Schnittstellen, um die benötigten Cloud-Ressourcen anzufordern. Erfolgt die Kommunikation zwischen Cloud-Verwaltungssoftware und den Cloud-Elementen nicht korrekt, besteht die Gefahr, dass die Cloud-Elemente (wie Server, Netze, Speicher) die Konfigurationen verwerfen oder die Kommunikation fehlschlägt.

Die Rückmeldung zur Umsetzung von Konfigurationen und Auslastungsinformationen von Cloud-Elementen zur Cloud-Verwaltungssoftware ist für den Orchestrierungsprozess von großer Bedeutung. Falls die Cloud-Elemente diese Konfigurations- und Auslastungsinformationen nicht korrekt an die Cloud-Verwaltungssoftware melden, kann seitens des Cloud Management keine korrekte Bereitstellung von Cloud-Diensten nachvollzogen werden.

**Beispiel:**

- In der Kommunikation zwischen der Cloud-Verwaltungssoftware und den Cloud-Elementen (virtuelle Router und Switches) wird auf eine neue Version des Management-Protokolls (z. B. SNMP) umgestellt. Der Cloud Element Manager der Switches unterstützt jedoch die neue Version nicht, weshalb die Kommunikation fehlschlägt.

# G 4.93 Ausfall von Verwaltungsservern und Verwaltungssoftware

Für eine Cloud-IT-Infrastruktur werden mehrere Virtualisierungsserver und gegebenenfalls auch mehrere Server für die Verwaltung der Cloud eingesetzt. Bei einem Ausfall eines Verwaltungsservers der Cloud muss nicht zwangsläufig die Verfügbarkeit aller Cloud-Dienste direkt betroffen sein, da die virtualisierten Komponenten auch ohne Verwaltung eigenständig weiterlaufen können. Beim Ausfall von Verwaltungsservern für die Cloud sind jedoch nahezu alle Cloud-Management-Prozesse direkt oder indirekt betroffen, sodass viele oder alle Funktionen des Cloud Managements ausfallen.

Es sind keine Konfigurationsänderungen mehr möglich, und automatisierte Orchestrierungsprozesse sind nicht mehr verfügbar.

Genauso wirkt sich der Ausfall auf die Verfügbarkeit der administrativen Schnittstellen aus. Die Cloud-Administratoren können in der Zeit eines Ausfalls von Verwaltungsservern weder auf auftretende Probleme reagieren noch neue Cloud-Ressourcen (physisch und virtuell) in die Cloud-IT-Infrastruktur integrieren.

**Beispiel:**

- Liefert der Verwaltungsserver oder dessen Monitoring-Komponente falsche oder gar keine Daten, kann die Funktion der Cloud-Infrastruktur durch die Administratoren nicht mehr hinreichend überwacht werden. Ressourcenengpässe bleiben in der virtuellen Infrastruktur unbemerkt und eine Erweiterung der virtuellen Infrastruktur kann nicht rechtzeitig durchgeführt werden. Der Ausfall von einzelnen Cloud-Komponenten kann ebenfalls nicht rechtzeitig festgestellt werden, wenn die Überwachungskomponente ausgefallen ist. Daten- oder Arbeitsspeicher sind dann erschöpft und Teile der Systemumgebung nicht mehr arbeitsfähig.

# G 4.94 Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services

Ein zentraler Vorteil bei der Realisierung von IT-Diensten als Web-Services ist die Möglichkeit, identische Dienste auf einer gemeinsamen technischen Infrastruktur für verschiedene Anwender ("Mandanten") anzubieten und so die Betriebskosten pro Mandant zu senken. Die Art der angebotenen Dienste kann dabei vielfältig sein, von Cloud-Speicherdiensten über Online-Zahlungsdienste bis hin zu Business-Anwendungen wie zum Beispiel CRM oder Finanzbuchhaltung.

Sofern die Web-Services dabei auf mandantenspezifische Datenbestände zugreifen, besteht die Gefahr, dass durch Konzeptions- oder Implementierungsfehler Zugriffsmöglichkeiten auf Datenbestände der anderen Mandanten des Dienstes entstehen. Typische Ursachen für solche Fehler sind:

- Benutzer werden einem Mandanten falsch zugeordnet: Wenn bei der Administration der Benutzer und Berechtigungen durch einen Bedien- oder Programmfehler eine falsche Zuordnung vorgenommen wird, kann ein Mitarbeiter eines Mandanten irrtümlich Zugriff auf die Daten eines anderen Mandanten erhalten. Hierbei kann es sich auch um die fehlerhafte automatisierte Abbildung von Benutzern auf technische Dienstkonten in Hintergrund-Systemen handeln.
- Fehler in der Programmlogik: Soweit die Trennung der mandantenspezifischen Daten nur durch Prüfungen im Programmcode realisiert ist, können einfache Programmierfehler zum Zugriff auf falsche Daten führen, die unter Umständen auch zu einem anderen Mandanten gehören.
- Fehlende Prüfungen beim direkten Aufruf von Web-Services: Werden beim direkten Aufruf eines Web-Service Parameter übergeben (oder bei REST-basierten Web-Services URL-Bestandteile geändert), die sich auf Daten eines anderen Mandanten beziehen, so besteht bei fehlerhafter beziehungsweise fehlender Umsetzung von Prüfungen die Möglichkeit, dass Daten des anderen Mandanten angezeigt oder verarbeitet werden.
- Unbefugter Zugriff auf administrative Schnittstellen: Sind administrative Funktionen für die mandantenübergreifende Verwaltung des Dienstes, insbesondere durch den Web-Service-Anbieter selbst, nicht ausreichend gegen unbefugten Zugriff gesichert, so kann auch hierüber ein Zugriff auf mandantenspezifische Daten möglich werden.
- Unnötige Kenntnisnahme von fremden Daten im Rahmen von Ermittlungstätigkeiten: Zur Aufklärung von Sicherheitsvorfällen kann es sein, dass Dienstnutzer oder dritte Stellen (zum Beispiel Ermittlungsbehörden) Einsicht in Protokolldaten oder IT-forensische Untersuchungen an den eingesetzten Systemen verlangen. Fehlen entsprechende Konzepte für die Sicherstellung der Datentrennung in solchen Fällen, so können dabei unbeabsichtigt auch sensible Daten anderer, vom Vorfall nicht betroffener Mandanten erhoben und zum Beispiel in Untersuchungsberichten dokumentiert werden.

Der Zugriff auf Daten fremder Mandanten kann in allen Fällen auch die Daten der eingerichteten Dienstnutzer, darunter insbesondere auch Authentisierungsinformationen (zum Beispiel Passwörter) umfassen. In diesem Fall können die Auswirkungen auch über den betroffenen Dienst hinausgehen, so-

fern die Authentisierungsdaten auch für andere Dienste genutzt werden oder Rückschlüsse auf Passwortmuster der Anwender erlauben.

# G 4.95 Ausfall von Komponenten einer Speicherlösung

Komplexe, netzbasierte Speicherlösungen bestehen in der Regel aus einer Vielzahl von Komponenten. Ausfallpotenzial wird dabei vor allem in diesen Teilbereichen gesehen:

- FC-Switche
- Virtualisierungs-Appliance
- Storage Controller (Block, NAS, NAS-Gateway)
- Leitungen
- Datenträger

Der Ausfall von Komponenten einer Speicherlösung kann weitreichende Folgen für eine Institution haben. Im Anschluss an einen solchen Ausfall arbeiten unter Umständen wichtige Anwendungen nicht mehr korrekt, es drohen Datenverluste und finanzielle Risiken. Häufig ist bei einem Problem gar nicht sofort ersichtlich, welche der oben genannten Komponenten ausgefallen ist und das konkrete Problem mitverursacht hat. So kann ein eigentlich kleiner Ausfall zu größerer Ausfallzeit und erheblichen Aufwänden für die Fehlersuche und Fehlerbeseitigung führen.

# G 4.96 Fehlfunktion von Komponenten einer Speicherlösung

Die Fehlfunktion von Komponenten einer Speicherlösung kann weitreichende Folgen für eine Institution haben. Im Anschluss an eine aufgetretene Fehlfunktion arbeiten unter Umständen wichtige Anwendungen nicht mehr korrekt, es drohen Datenverluste und finanzielle Risiken. Dies gilt beim Einsatz von Speicherlösungen für Cloud Services auch für die Fehlfunktion der Kommunikation zwischen dem sogenannten Cloud Orchestrator und dem Storage-Element-Manager.

Ursachen für solche Fehlfunktionen können unterschiedlicher Natur sein. Ein häufiger Grund liegt darin, dass nicht kompatible Systemkomponenten eingesetzt werden. Viele Hersteller setzen voraus, dass Institutionen sich beim Aufbau und Betrieb komplexer IT-Infrastrukturen an die Kompatibilitätsmatrix der Hersteller halten. Wird von diesem Vorgehen abgewichen, kann es zu einer Fehlfunktion kommen oder die Leistung kann vermindert werden.

Verzeichnet eine Institution beispielsweise aufgrund von mangelndem Quality of Service (QoS) Performanceeinbußen, wenn auf benötigte Speicherressourcen zugegriffen wird, ist dies ebenfalls als Fehlfunktion von Komponenten anzusehen.

Eine besondere Ausprägung der Fehlfunktion von Komponenten ist unter G 4.95 *Ausfall von Komponenten einer Speicherlösung* beschrieben.

# G 4.97 Schwachstellen bei der Anbindung an einen Outsourcing- oder Cloud-Dienstleister

Die Durchführung eines Outsourcing- oder Cloud-Nutzungs-Vorhabens verlangt in aller Regel den Zugriff des Dienstleisters auf interne Ressourcen des Auftraggebers. Dies wird häufig durch eine gegenseitige Anbindung von Teilen der jeweiligen IT-Infrastruktur realisiert. Zum beschleunigten Informationsaustausch zwischen Auftraggeber und Auftragnehmer werden möglicherweise spezielle Informationskanäle (zum Beispiel dedizierte Standleitungen, VPN-Verbindungen, Zugänge für die Remote-Wartung) eingerichtet.

Ist diese Anbindung nicht gesichert oder treten bei der Absicherung Schwachstellen auf, so ergeben sich zwangsläufig eine Reihe von Gefährdungen:

- Die Vertraulichkeit der Kommunikation kann gefährdet sein.
- Die Integrität von übermittelten Datensätzen ist nicht mehr garantiert.
- Der Empfang von übermittelten Informationen und Nachrichten könnte abgestritten werden.
- Es wird Externen ein für die tatsächlichen Bedürfnisse des Dienstleisters zu umfassender Einblick in Interna des Auftraggebers gegeben.
- Es entstehen zusätzliche Zugangsmöglichkeiten für Außenstehende zum Intranet der Institution und damit Gefahrenquellen.
- Bei offenen oder schlecht gesicherten IT-Zugängen ergeben sich Manipulationsmöglichkeiten.
- Es könnten vertrauliche Informationen und geistiges Eigentum an Außenstehende weitergegeben werden.
- Externe Systemzugriffe werden unter Umständen nicht ausreichend kontrolliert.

Der Schutzbedarf von Schnittstellensystemen (zum Beispiel Application Level Gateways, Paketfilter) und Leitungen kann durch die Nutzung von Outsourcing oder Cloud Services steigen. Wird keine neue Analyse des Schutzbedarfs vorgenommen, ergibt sich eine Gefährdung für die Verfügbarkeit der Anbindung.

Die IT-Anbindung zwischen auslagernder Institution und Dienstleister kann auch komplett ausfallen. Dabei können Daten, deren Übertragung vor dem Ausfall noch nicht vollständig abgeschlossen war, zerstört oder inkonsistent werden. In Abhängigkeit von der Dauer und Art des Ausfalls können die Konsequenzen auch existenzbedrohend sein. Diese Gefahr wird verstärkt, wenn kein Notfallvorsorgekonzept (siehe G 2.93 *Unzureichendes Notfallvorsorgekonzept bei Outsourcing oder Cloud-Nutzung*) existiert.

# G 4.98 Ausfall von Tools zur Administration von Cloud Services bei Cloud-Nutzung

Der Ausfall von Management-Tools stellt im Zusammenhang mit der Nutzung von Cloud Services eine Gefährdung für die Institution dar. Mögliche Ursachen für den Ausfall von Management-Tools können beispielsweise Software-Schwachstellen oder -Fehler sein, wie sie in G 4.22 *Software-Schwachstellen oder -Fehler* beschrieben sind.

Grundsätzlich ist zwischen dem Ausfall von Management-Tools, die für die Nutzung von Cloud Services relevant sind, und den Verwaltungsservern beziehungsweise der Verwaltungssoftware aufseiten des Cloud-Diensteanbieters zu unterscheiden.

Beim Ausfall von Verwaltungsservern für die Cloud sind nahezu alle Cloud-Management-Prozesse direkt oder indirekt betroffen, sodass viele oder alle Funktionen des Cloud Managements, wie beispielsweise administrative Schnittstellen, ausfallen. Weitere Informationen hierzu finden sich in G 4.93 *Ausfall von Verwaltungsservern und Verwaltungssoftware* des Bausteins B 5.23 *Cloud Management*.

Im Umfeld der Cloud-Nutzung ist eine Unterscheidung von Management-Tools hinsichtlich deren Bereitstellung vorzunehmen. Häufig werden diese der nutzenden Institution dabei durch den Cloud-Diensteanbieter zur Verfügung gestellt. Darüber hinaus existieren Management-Tools, die von Dritten bereitgestellt werden, sogenannte Third-Party-Management-Tools. In diesem Fall kann der Anwender aus unterschiedlichen, am Markt verfügbaren Produkten auswählen. Third-Party-Management-Tools sind in der Regel abhängig von der API (Schnittstelle), die durch den Cloud-Diensteanbieter definiert wird. Ändert er die API, kann der Zugriff auf das entsprechende Management-Tool gestört werden.

Eine solche Verhinderung des Zugriffs durch Management-Tools stellt eine Gefährdung für die Institution dar. In der Folge können durch den Administrator aufseiten der nutzenden Institution keine Veränderungen an bestehenden Services vorgenommen werden.

**Beispiel:**

- Für einen Dienst, der als Plattform as a Service erbracht wird, muss zusätzliche Speicherkapazität beauftragt werden. Die Institution nutzt zur Administration des Cloud Services die Software eines Drittherstellers. Das eingesetzte Management-Tool kann jedoch nicht auf die entsprechende Schnittstelle des Cloud-Diensteanbieters zugreifen. Die Verfügbarkeit des betroffenen Services kann in der Folge nicht mehr sichergestellt werden.

# G 4.99 Fehlende oder unzureichende Sicherheitsmechanismen in Anwendungen

Hinweis: Ähnliches wird behandelt in G 4.22 *Software-Schwachstellen oder -Fehler* sowie in G 4.39 *Software-Konzeptionsfehler*.

Bei vielen Anwendungen stand bei der Entwicklung nicht die Informationssicherheit im Fokus, sodass häufig die erforderlichen Sicherheitsmechanismen fehlen oder unzureichend sind. Darüber hinaus kann es vorkommen, dass die vorhandenen Sicherheitsmechanismen schlecht konzipiert, implementiert oder unzuverlässig sind und somit keinen ausreichenden Schutz bieten. Nach der Erst-Installation sind außerdem häufig die Anwendungen so vorkonfiguriert, dass keine oder nur einige Sicherheitsmechanismen aktiviert sind.

Je nach Art der Anwendung, deren Einsatzumgebung und dem Schutzbedarf der damit verarbeiteten Daten können verschiedene Sicherheitsfunktionalitäten erforderlich sein und nur unzureichend vorhanden sein. Im Folgenden werden einige leider sehr typische Schwachstellen exemplarisch genannt:

- Keine Benutzertrennung:
  Dadurch kann jeder, der Zugriff auf eine Anwendung hat, auf alle gespeicherten Daten zugreifen.
- Unzureichende Zugriffschutz- und Authentisierungsmechanismen:
  Leider finden sich immer wieder Anwendungen, die überhaupt keine Zugriffsschutz-Mechanismen bieten. Darüber hinaus finden sich bei vorhandenen Authentisierungsmechanismen Schwachstellen, die die Sicherheit negativ beeinflussen (siehe auch G 4.33 *Schlechte oder fehlende Authentikationsverfahren und -mechanismen*). So kann die Mechanismenstärke bei einer Authentisierung unzureichend sein. Beispielsweise kann die Passwort-Auswahl auf vier Stellen eingeschränkt sein.
- Keine oder unzureichende Möglichkeiten zur Verschlüsselung von Daten
- Verwendung unsicherer Kryptoalgorithmen (siehe auch G 4.35 *Unsichere kryptographische Algorithmen*)
- Keine oder unzureichende Protokollierungsmöglichkeiten
- Unsichere Voreinstellungen:
  In Anwendungen häufig vorhandene Sicherheitsfunktionen wie Authentisierung und Verschlüsselung sind abgeschaltet und Passwörter bzw. PINs auf Standardwerte ("0000", "1234" usw.) eingestellt.
- Gegen bekannte und für den geplanten Einsatzzweck einschlägige Angriffe wurde in der Anwendung keine Vorkehrungen getroffen. Beispiele dafür sind Web-Anwendungen mit Datenbankanbindung, die nicht oder nur unzureichend gegen Injection-Angriffe (siehe auch G 5.131 *SQL-Injection*) oder Cross-Site-Request-Forgery / Cross-Site-Scritping abgesichert sind.

# G 4.100 Hardwareausfall und Hardwarefehler bei eingebetteten Systemen

Die Hardware von eingebetteten Systemen kann ausfallen oder fehlerhaft arbeiten. Die Ursachen dafür können in verschiedensten Bereichen liegen, z. B.

- ungünstige Umgebungseinflüsse wie elektromagnetische Interferenz,
- Temperaturschwankungen,
- Feuchtigkeit,
- mechanische Belastung,
- radioaktive Strahlung,
- eine instabile Spannungsversorgung,
- herstellungsbedingte Materialfehler und Fertigungsstreuung und
- normaler oder vorzeitiger Verschleiß.

Zudem führt der generelle Trend zu sinkenden Strukturgrößen, höherer Integrationsdichte und geringeren Versorgungsspannungen bei Halbleitern dazu, dass auftretende Hardwarefehler schwieriger zu erkennen sind. Diese können zunächst nur vorübergehend in unregelmäßigen Abständen auftreten (sporadische Fehler) oder über eine unbegrenzt lange Zeitdauer bestehen bzw. dazu übergehen (permanente Fehler).

Transiente Fehler treten wie sporadische Fehler unregelmäßig auf, münden aber in der Regel nicht in einem permanenten Fehler. Sie werden z. B. durch Partikeleinschläge verursacht und manifestieren sich als Bitkipper. Diese können in Speicherzellen, in Bussystemen oder in Registern der Central Processing Unit (CPU) auftreten. Mögliche Folgen hängen davon ab, wie fehlertolerant ein System ist, sowie der konkreten Situation im Einzelfall. Ein Software-Modul kann falsche Werte liefern, was zu Fehlreaktionen oder zum Absturz des eingebetteten bzw. des übergeordneten Systems führen kann. Nicht erkannte Fehler oder Fehlberechnungen können zu hohen Schäden führen, z. B. wenn ein Sensor einen kritischen Messwert liefert, der eine umgehende Aktion erfordert und dieser oder der Vergleichswert verfälscht ist.

Jeder Fehler kann letztlich zum vollständigen Ausfall des eingebetteten Systems führen und dadurch die umgebenden Systeme stark beeinträchtigen.

# G 4.101 Ausfall eines zentralen Identitäts- und Berechtigungsmanagement-Systems

In einem zentralen Identitäts- und Berechtigungsmanagement-System werden die Identitäten aller Zugriffsberechtigten gesammelt und die jeweiligen Berechtigungen für die institutionsweite Informationsverarbeitung verwaltet.

Wenn das zentrale Identitäts- und Berechtigungsmanagement-System ausfällt, können keine Benutzerprofile mehr geändert, gelöscht oder neu angelegt werden. Mittelfristig sind die verknüpften Prozesse und Anwendungen gegebenenfalls nicht mehr benutzbar, weil die Berechtigungen nicht mehr aktualisiert werden können.

Wenn die Anmeldungen an IT-Komponenten oder Anwendungen zentral verarbeitet werden, kann bei einem Ausfall des Identitäts- und Berechtigungsmanagement-Systems die komplette institutionsweite Informationstechnik nicht mehr genutzt werden, weil sich die Benutzer nicht mehr anmelden können. Dies kann zur Folge haben, dass auch Kernprozesse der Institution nicht mehr funktionieren.

**Beispiel:**

- Das zentrale Identitäts- und Berechtigungsmanagementsystem eines Unternehmens fällt durch einen Denial-of-Service-Angriff aus. Den Mitarbeitern wird so der Zugriff auf die auf einem Server zentral gespeicherten Dateien verwehrt, da das System sie nicht mehr authentisieren kann.

# G 5 Gefährdungskatalog Vorsätzliche Handlungen

G 5.32 Auswertung von Restinformationen in Faxgeräten und Faxservern

G 5.33 Vortäuschen eines falschen Absenders bei Faxsendungen

G 5.34 Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes

G 5.35 Überlastung durch Faxsendungen

G 5.36 Absichtliche Überlastung des Anrufbeantworters **- entfallen**

G 5.37 Ermitteln des Sicherungscodes **- entfallen**

G 5.38 Missbrauch der Fernabfrage **- entfallen**

G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten

G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon und Kamera

G 5.41 Missbräuchliche Nutzung eines Unix-Systems mit Hilfe von UUCP

G 5.42 Social Engineering

G 5.43 Makro-Viren

G 5.44 Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen

G 5.45 Ausprobieren von Passwörtern unter WfW und Windows 95 **- entfallen**

G 5.46 Maskerade unter WfW **- entfallen**

G 5.47 Löschen des Post-Office unter WfW **- entfallen**

G 5.48 IP-Spoofing

G 5.49 Missbrauch des Source-Routing

G 5.50 Missbrauch des ICMP-Protokolls

G 5.51 Missbrauch der Routing-Protokolle

G 5.52 Missbrauch von Administratorrechten bei Windows-Betriebssystemen

G 5.53 Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit

G 5.54 Vorsätzliches Herbeiführen eines Abnormal End **- entfallen**

G 5.55 Login Bypass **- entfallen**

G 5.56 Temporär frei zugängliche Accounts **- entfallen**

G 5.57 Netzanalysetools

G 5.58 Hacking Novell Netware **- entfallen**

G 5.59 Missbrauch von Administratorrechten unter Novell Netware Servern **- entfallen**

G 5.60 Umgehen der Systemrichtlinien **- entfallen**

G 5.61 Missbrauch von Remote-Zugängen für Managementfunktionen von Routern

G 5.62 Missbrauch von Ressourcen über abgesetzte IT-Systeme **- entfallen**

G 5.63 Manipulationen über den ISDN-D-Kanal

G 5.64 Manipulation an Daten oder Software bei Datenbanksystemen

G 5.65 Verhinderung der Dienste eines Datenbanksystems

G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz

G 5.67 Unberechtigte Ausführung von Netzmanagement-Funktionen

G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten

G 5.69 Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

G 5.70 Manipulation durch Familienangehörige und Besucher

G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

G 5.72 Missbräuchliche Groupware-Nutzung

G 5.73 Vortäuschen eines falschen Absenders

G 5.74 Manipulation von Alias-Dateien oder Verteilerlisten **- entfallen**

G 5.75 Überlastung durch eingehende E-Mails

G 5.76 Mailbomben **- entfallen**

G 5.77 Mitlesen von E-Mails

G 5.78 DNS-Spoofing

G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen

G 5.80 Hoax

G 5.81 Unautorisierte Benutzung eines Kryptomoduls

G 5.82 Manipulation eines Kryptomoduls

G 5.83 Kompromittierung kryptographischer Schlüssel

G 5.84 Gefälschte Zertifikate

G 5.85 Integritätsverlust schützenswerter Informationen

G 5.86 Manipulation von Managementparametern

G 5.87 Web-Spoofing

| | |
|---|---|
| G 5.88 | Missbrauch aktiver Inhalte |
| G 5.89 | Hijacking von Netz-Verbindungen |
| G 5.90 | Manipulation von Adressbüchern und Verteillisten |
| G 5.91 | Abschalten von Sicherheitsmechanismen für den RAS-Zugang **- entfallen** |
| G 5.92 | Nutzung des VPN-Clients als VPN-Server |
| G 5.93 | Erlauben von Fremdnutzung von VPN-Komponenten |
| G 5.94 | Missbrauch von SIM-Karten |
| G 5.95 | Abhören von Raumgesprächen über Mobiltelefone |
| G 5.96 | Manipulation von Mobiltelefonen |
| G 5.97 | Unberechtigte Datenweitergabe über Mobiltelefone |
| G 5.98 | Abhören von Mobiltelefonaten |
| G 5.99 | Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen |
| G 5.100 | Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes/Domino |
| G 5.101 | Hacking Lotus Notes/Domino |
| G 5.102 | Sabotage |
| G 5.103 | Missbrauch von Webmail |
| G 5.104 | Ausspähen von Informationen |
| G 5.105 | Verhinderung der Dienste von Archivsystemen |
| G 5.106 | Unberechtigtes Überschreiben oder Löschen von Archivmedien |
| G 5.107 | Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister |
| G 5.108 | Ausnutzen von systemspezifischen Schwachstellen des IIS **- entfallen** |
| G 5.109 | Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver **- entfallen** |
| G 5.110 | Web-Bugs |
| G 5.111 | Missbrauch aktiver Inhalte in E-Mails |
| G 5.112 | Manipulation von ARP-Tabellen |
| G 5.113 | MAC-Spoofing |
| G 5.114 | Missbrauch von Spanning Tree |
| G 5.115 | Überwindung der Grenzen zwischen VLANs |
| G 5.116 | Manipulation der z/OS-Systemsteuerung |

G 5.117 Verschleiern von Manipulationen unter z/OS

G 5.118 Unbefugtes Erlangen höherer Rechte im RACF

G 5.119 Benutzung fremder Kennungen unter z/OS-Systemen

G 5.120 Manipulation der Linux/zSeries Systemsteuerung

G 5.121 Angriffe über TCP/IP auf z/OS-Systeme

G 5.122 Missbrauch von RACF-Attributen unter z/OS

G 5.123 Abhören von Raumgesprächen über mobile Endgeräte

G 5.124 Missbrauch der Informationen von mobilen Endgeräten

G 5.125 Datendiebstahl mithilfe mobiler Endgeräte

G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

G 5.127 Spyware **- entfallen**

G 5.128 Unberechtigter Zugriff auf Daten durch Einbringen von Code in ein SAP System

G 5.129 Manipulation von Daten über das Speichersystem

G 5.130 Manipulation der Konfiguration einer Speicherlösung

G 5.131 SQL-Injection

G 5.132 Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003

G 5.133 Unautorisierte Benutzung web-basierter Administrationswerkzeuge

G 5.134 Fehlende Identifizierung zwischen Gesprächsteilnehmern

G 5.135 SPIT und Vishing

G 5.136 Missbrauch frei zugänglicher Telefonanschlüsse

G 5.137 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

G 5.138 Angriffe auf WLAN-Komponenten

G 5.139 Abhören der WLAN-Kommunikation

G 5.140 Auswertung von Restinformationen in Druckern, Kopierern und Multifunktionsgeräten

G 5.141 Datendiebstahl über mobile Datenträger

G 5.142 Verbreitung von Schadprogrammen über mobile Datenträger

G 5.143 Man-in-the-Middle-Angriff

| | |
|---|---|
| G 5.144 | Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff |
| G 5.145 | Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement |
| G 5.146 | Vertraulichkeitsverlust durch Auslagerungsdateien |
| G 5.147 | Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes |
| G 5.148 | Missbrauch von Virtualisierungsfunktionen |
| G 5.149 | Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen |
| G 5.150 | Kompromittierung des Hypervisor virtueller IT-Systeme |
| G 5.151 | DNS-Flooding - Denial-of-Service |
| G 5.152 | DNS-Hijacking |
| G 5.153 | DNS-Amplification Angriff |
| G 5.154 | DNS Information Leakage |
| G 5.155 | Ausnutzen dynamischer DNS-Updates |
| G 5.156 | Bot-Netze |
| G 5.157 | Phishing und Pharming |
| G 5.158 | Missbrauch sozialer Netzwerke |
| G 5.159 | Erstellung von Bewegungsprofilen unter Bluetooth |
| G 5.160 | Missbrauch der Bluetooth-Profile |
| G 5.161 | Gefälschte Antworten auf XDMCP-Broadcasts bei Terminalservern |
| G 5.162 | Umleiten von X-Window-Sitzungen |
| G 5.163 | Angriffe auf Exchange-Systeme |
| G 5.164 | Missbrauch von Programmierschnittstellen unter Outlook |
| G 5.165 | Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services |
| G 5.166 | Missbrauch einer Webanwendung durch automatisierte Nutzung |
| G 5.167 | Fehler in der Logik von Webanwendungen und Web-Services |
| G 5.168 | Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services |
| G 5.169 | Unzureichendes Session-Management von Webanwendungen und Web-Services |

| | |
|---|---|
| G 5.170 | Cross-Site Scripting (XSS) |
| G 5.171 | Cross-Site Request Forgery (CSRF, XSRF, Session Riding) |
| G 5.172 | Umgehung der Autorisierung bei Webanwendungen und Web-Services |
| G 5.173 | Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services |
| G 5.174 | Injection-Angriffe |
| G 5.175 | Clickjacking |
| G 5.176 | Kompromittierung der Protokolldatenübertragung bei zentraler Protokollierung |
| G 5.177 | Missbrauch von Kurz-URLs oder QR-Codes |
| G 5.178 | Missbrauch von Administratorrechten im Cloud-Management |
| G 5.179 | Angriffe auf Protokolle |
| G 5.180 | Angriffe auf Registries und Repositories |
| G 5.181 | Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services |
| G 5.182 | Manipulation von Routen (Routing Detours) |
| G 5.183 | Angriffe auf XML |
| G 5.184 | Informationsgewinnung über Web-Services |
| G 5.185 | Erlangung physischen Zugangs auf SAN-Switches |
| G 5.186 | Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing |
| G 5.187 | Überwindung der logischen Netzseparierung |
| G 5.188 | Unberechtigter Zugriff auf Daten innerhalb einer Cloud-Storage-Lösung |
| G 5.189 | Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden |
| G 5.190 | Missbrauch von Services |
| G 5.191 | Manipulation der Abrechnungsinformationen |
| G 5.192 | Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender |
| G 5.193 | Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs |
| G 5.194 | Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion |

| | |
|---|---|
| G 5.195 | Ausnutzen von Schwachstellen in Backend-Anwendungen |
| G 5.196 | Unterbinden einer Informations- und Dienstesynchronisation in einer verteilten SOA-Umgebung |
| G 5.197 | Missbrauch von SAML-Token in SOA-Umgebungen |
| G 5.198 | Missbrauch der WS-Notification-Broker in einer SOA |
| G 5.199 | Ungenügende Absicherung der SOAP-Kommunikation |
| G 5.200 | Manipulation von Richtlinien in einer SOA |
| G 5.201 | Einspielen (Flashen) von manipulierten Software-Updates/-Upgrades bei eingebetteten Systemen |
| G 5.202 | Seitenkanalangriffe auf eingebettete Systeme |
| G 5.203 | Physikalischer Eingriff in ein eingebettetes System |
| G 5.204 | Eindringen und Manipulation über die Kommunikationsschnittstelle von eingebetteten Systemen |
| G 5.205 | Einsatz gefälschter Komponenten |
| G 5.206 | Reverse Engineering |

# G 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör

Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, Geräte, Zubehör, Schriftstücke und andere Datenträger zu manipulieren oder zu zerstören. Die Angriffe können umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tief greifender die Folgen für einen Arbeitsvorgang sind. Die Manipulationen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen. Erhebliche Ausfallzeiten können die Folge sein.

**Beispiel:**

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteillüfter mit einem hinter dem Server versteckt aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt und der Server fiel für mehrere Tage aus. Hinterher behauptete der Angreifer, dass es sich um ein Versehen gehandelt habe.
- Ein Mitarbeiter hatte sich über das wiederholte Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Er trat mehrmals gegen den Rechner und beschädigte dabei die Festplatte so stark, dass sie unbrauchbar wurde. Die darauf gespeicherten Daten konnte die IT-Abteilung nur teilweise wieder durch ein Backup vom Vortag rekonstruieren.

# G 5.2 Manipulation an Informationen oder Software

Informationen oder Software können auf vielfältige Weise manipuliert werden: durch falsches Erfassen von Daten, Änderungen von Zugriffsrechten, inhaltliche Änderung von Abrechnungsdaten oder von Schriftverkehr, Änderungen in der Betriebssystem-Software und vieles mehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen und Software-Komponenten manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.

Die Beweggründe der Täter sind vielfältig und reichen von Rache und mutwilliger Zerstörungslust bis zu Bereicherung oder anderen persönlichen Vorteilen.

**Beispiele:**

- In einem Schweizer Finanzunternehmen wurde durch einen Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Damit war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Mitarbeiter, die die Firma verlassen, kopieren vorher Kundendaten, um sie für andere Zwecke gewinnbringend einzusetzen. Solche illegal beschafften Daten von Privatkunden sind beispielsweise benutzt worden, um Vertragsabschlüsse vorzutäuschen. Mitarbeiter, die im Unfrieden eine Behörde oder ein Unternehmen verlassen, könnten auch Informationen oder IT-Systeme mutwillig zerstören oder den Zugriff auf wichtige Informationen oder IT-Systeme verhindern.
- Manipulationen archivierter Dokumente können besonders schwer wiegen, da sie unter Umständen erst nach Jahren bemerkt werden und eine Überprüfung dann oft nicht mehr möglich ist. Archivierte Dokumente stellen meist besonders schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.
- Eine Mitarbeiterin hat sich über die Beförderung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin unerlaubt Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das veröffentlichte Jahresergebnis des Unternehmens genommen.
- Ein Mitarbeiter ärgert sich darüber, dass sein Vorgesetzter ihm keine Gehaltserhöhung bewilligt hat. Aus Wut sendet er an einige seiner Arbeitskollegen per E-Mail ein Dokument, das einen Computer-Virus enthält und als Geschäftsbrief getarnt ist. Beim Öffnen dieses Dokuments werden unterschiedliche Dateien auf den betroffenen Systemen verändert. Ein Mitarbeiter ärgert sich darüber, dass sein Vorgesetzter ihm keine Gehaltserhöhung gegeben hat. Aus Wut sendet er an einige seiner Arbeitskollegen per E-Mail ein Dokument, das einen Computer-Virus enthält und als Geschäftsbrief getarnt ist. Beim Öffnen dieses Dokuments werden unterschiedliche Dateien auf den betroffenen Systemen verändert.
- Ein Mitarbeiter empfindet die Einschränkungen durch Sicherheitsmaßnahmen bei seinem Smartphone als zu restriktiv und "rootet" sein Smartphone. So gelangt nicht freigegebene Software auf das Gerät, die Schad-

software enthält, vertrauliche Informationen der Institution abgreift und an unbefugte Dritte verschickt. Dadurch entsteht ein großer wirtschaftlicher Schaden.

# G 5.3 Unbefugtes Eindringen in ein Gebäude

Wenn Unbefugte in ein Gebäude oder einzelne Räumlichkeiten eindringen, kann dies verschiedene andere Sicherheitsgefährdungen nach sich ziehen. Dazu gehören beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen. Maßnahmen, die dagegen gerichtet sind, wirken dadurch auch gegen die entsprechenden Folgegefährdungen. Bei qualifizierten Angriffen versierter Täter ist die Zeitdauer entscheidend, in der die Täter ungestört ihr Ziel verfolgen können. Ziel eines Einbruchs kann der Diebstahl von IT-Komponenten oder anderer leicht veräußerbarer Ware sein, aber auch das Kopieren oder die Manipulation von Daten oder IT-Systemen. Dabei können nicht offensichtliche Manipulationen weit höhere Schäden als direkte Zerstörungsakte verursachen.

Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.

**Beispiele:**

- Bei einem nächtlichen Einbruch in ein Bürogebäude konnten die Täter keine lohnende Beute machen. Aus Frustration darüber leerten sie die Pulverlöscher in die Büroräume. Der Einbruchschaden war gering, der Vandalismusschaden dagegen durch die Reinigungskosten und Arbeitsunterbrechungen unverhältnismäßig hoch.
- Bei einem Einbruch in ein Unternehmen an einem Wochenende wurde nur Bagatellschaden durch Aufhebeln eines Fensters angerichtet, lediglich eine Kaffeekasse und kleinere Einrichtungsgegenstände wurden entwendet. Bei einer Routinekontrolle wurde jedoch später festgestellt, dass ein zentraler Server genau zum Zeitpunkt des Einbruchs geschickt manipuliert wurde.

# G 5.4 Diebstahl

Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und die daraus resultierenden Konsequenzen entstehen.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht zu transportieren sind. Gerade neue Smartphones oder Tablets sind bei Dieben als teure Statussymbole beliebt. Ihr Verlust ist meist schwerwiegend, weil sie für viele Anwendungen benutzt werden (E-Mails, Internet, Präsentationen erstellen) und große Datenmengen speichern können.

**Beispiele:**

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptografisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war. Bei Sicherheitsuntersuchungen war bereits vor ungenügenden Kontrollen gewarnt worden.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Das auch Akten kopiert oder manipuliert wurden, konnte nicht zweifelsfrei ausgeschlossen werden.
- In Großbritannien gab es eine Reihe von Datenpannen, bei denen vertrauliche Unterlagen offengelegt wurden, weil Datenträger gestohlen wurden. In einem Fall wurden bei der britischen Luftwaffe Computer-Festplatten gestohlen. Sie enthielten auch sehr persönliche Informationen, die zur Sicherheitsüberprüfung von Mitarbeitern erfasst worden waren.
- Ein Mitarbeiter eines Call-Centers erstellte, kurz bevor er das Unternehmen verlassen musste, Kopien einer großen Menge von vertraulichen Kundendaten. Nach seinem Ausscheiden aus dem Unternehmen hat er diese dann an Wettbewerber verkauft. Da anschließend Details hierüber an die Presse gelangten, verlor das Call-Center viele wichtige Kunden.

# G 5.5 Vandalismus

Durch Vandalismus wird fremdes Eigentum zerstört oder beschädigt. Die Auswirkungen sind mit denen eines Anschlags sehr verwandt, nur dass Vandalismus nicht wie dieser gezielt geplant und umgesetzt wird, sondern meist Ausdruck spontaner, blinder Zerstörungswut ist.

Sowohl Außentäter (z. B. enttäuschte Einbrecher, außer Kontrolle geratene Demonstranten) als auch Innentäter (z. B. frustrierte oder psychisch labile Mitarbeiter) kommen als Verursacher in Betracht. Die tatsächliche Gefährdung durch Vandalismus ist schwerer abschätzbar als die eines Anschlages, da ihm in der Regel keine zielgerichtete Motivation zugrunde liegt. Mögliche Auslöser für Vandalismus können unter anderem Meinungsverschiedenheiten, persönliche Probleme, Mobbing oder ein schlechtes Betriebsklima sein.

**Beispiele:**

- Weil ein Kunde bei einem Unternehmen zu lange warten musste, ärgerte er sich so, dass er die Netzkabel beschädigte, die durch einen Kabelkanal im Wartebereich liefen. Dadurch kam es längere Zeit zu Verbindungsstörungen im LAN, da die Fehlerquelle nicht direkt ermittelt werden konnte.
- Vandalismus kann sich auch virtuell ausdrücken. Die missverständliche Produktwerbung eines Unternehmen löste größeren Unmut in bestimmten Bevölkerungsgruppen aus. In der Folge wurden Marketingauftritte dieses Unternehmens im Internet durch Angreifer verunstaltet.

# G 5.6 Anschlag

Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: geworfene Ziegelsteine, Explosion durch Sprengstoff, Schusswaffengebrauch, Brandstiftung. Ob und in welchem Umfang eine Institution der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von ihren Aufgaben und vom politisch-sozialen Klima ab. Unternehmen und Behörden, die in politisch kontrovers diskutierten Bereichen agieren, sind stärker bedroht als andere. Institutionen in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Orten. Für die Einschätzung der Gefährdung oder bei Verdacht auf Bedrohungen durch politisch motivierte Anschläge können in Deutschland die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

Für Archive ist bei dieser Einschätzung als besonderer Umstand zu berücksichtigen, dass darin eine große Anzahl von Dokumenten und Daten auf vergleichsweise kleinem Raum gespeichert wird. Dies können z. B. Krankendaten, Verträge, Urkunden oder Testamente sein. Deren Vernichtung kann weitreichende Auswirkungen haben, nicht nur auf die speichernde Stelle, sondern auch auf andere Benutzer. Beispielsweise kann es in einem solchen Fall notwendig werden, die vernichteten Informationen mit großem Aufwand neu zu ermitteln und zu erfassen. Unter Umständen sind bestimmte Informationen sogar unwiederbringlich verloren. Anschläge auf papiergebundene und elektronische Archive können daher erhebliche Schäden verursachen.

**Beispiele:**

- In den 80er-Jahren wurde ein Sprengstoffanschlag auf das Rechenzentrum einer großen Bundesbehörde in Köln verübt. Durch die große Durchschlagskraft des Sprengkörpers wurden nicht nur Fenster und Wände, sondern auch viele IT-Systeme im Rechenzentrum zerstört.
- Ein Finanzamt im rheinischen Raum wurde praktisch jährlich durch Bombendrohungen für einige Stunden lahm gelegt.
- Bei dem Anschlag auf das World-Trade-Center in New York am 11. September 2001 wurden nicht nur viele Menschen getötet, sondern es wurden auch zahlreiche IT-Einrichtungen zerstört. Als Folge hatten mehrere Unternehmen erhebliche Schwierigkeiten, ihre Geschäftstätigkeiten fortzusetzen.

# G 5.7 Abhören von Leitungen

Abhörangriffe auf Leitungen sind eine Gefahr für die Informationssicherheit, die nicht vernachlässigt werden sollte. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich hinsichtlich des zum Abhören erforderlichen Aufwands unterscheiden sich die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischem Aufwand feststellbar.

Der Entschluss, eine Leitung abzuhören, wird auf Seiten des Angreifers im Wesentlichen durch die Frage bestimmt, ob die Informationen den technischen bzw. den finanziellen Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig. Somit ist eine sichere Festlegung, welche Informationen und damit Leitungen möglicherweise abgehört werden, nicht möglich.

Der Aufwand zum Abhören von Leitungen kann sehr gering sein. Bei manchen Arten von LAN-Verkabelung kann der Zugang zu einer LAN-Dose ausreichen, um den gesamten Netzverkehr des lokalen Netzes abzuhören. Größer ist das Risiko, wenn ein Angreifer Zugriff auf passive oder gar aktive Koppelelemente des IT-Netzes hat. Noch einfacher können drahtlose Netze (Wireless LAN / Funk-LAN, IEEE 802.11) abgehört werden. Hier ist zudem das Risiko der Entdeckung praktisch gleich null.

Besonders kritisch ist die ungeschützte Übertragung von Authentisierungsdaten bei Klartextprotokollen wie HTTP, ftp oder telnet, da sich hier die Position der vom Benutzer eingegebenen Daten in den übertragenen Paketen durch die einfache Struktur der Protokolle leicht bestimmen lässt (siehe G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*). Eine automatische Analyse solcher Verbindungen lässt sich somit mit geringem Aufwand realisieren.

Mittels Password-Sniffing können in einem ersten Schritt beispielsweise Passwörter bei der Übertragung zu einem System abgefangen werden. Dies erlaubt es dem Angreifer anschließend auf das IT-System zu gelangen, um dann weitere Angriffe lokal auf dem Rechner durchzuführen.

Mittels Fingerprint-Techniken kann zudem das verwendete Framework oder Betriebssystem herausgefunden werden. Mit diesen Informationen lassen sich anschließend bereits bekannte Schwachstellen des Systems ausnutzen. Ebenso ist es denkbar, dass Informationen zu Verzeichnisdiensten gewonnen werden, die Angreifern dazu dienen können, Authentisierungsmechanismen zu umgehen.

**Beispiele:**

- Es ist falsch anzunehmen, dass per E-Mail versandte Nachrichten mit klassischen Briefen vergleichbar sind. Da E-Mails während ihres gesamten Weges durch das Netz gelesen werden können, ist ein Vergleich mit Postkarten sehr viel realistischer.
- Einige Hersteller liefern schon zusammen mit den Betriebssystemen Programme (Sniffer) aus, die zum Debuggen der Netze dienen, aber auch zum Abhören benutzt werden können, schon zusammen mit den Betriebssystemen aus.

# G 5.8 Manipulation von Leitungen

Neben dem Abhören von Leitungen (siehe G 5.7 *Abhören von Leitungen*) stellen weitere bewusste Manipulationen oder gar die Zerstörung von IT-Leitungen eine Gefahr für die Institution dar. Vor allem die Primärverkabelung größerer Institutionen und Leitungen, welche die IT- oder TK-Anbindungen an einen Provider realisieren, haben oft einen hohen Schutzbedarf in Bezug auf die Verfügbarkeit.

Fehlfunktionen von Leitungen können bewusst und in manipulativer Absicht herbeigeführt werden. Möglich ist dies beispielsweise durch:

- Vorsätzliches falsches Patchen von Kabeln oder Verbindungen
- Vorsätzliches falsches Stecken von Kabeln
- Bewusst herbeigeführte Fehlbedienung bzw. Zerstörung von Kabeln
- Bewusst herbeigeführte Verletzung vorgegebener Biegeradien bei Glasfaserkabeln
- Bewusste Verunreinigung von Steckverbindungen (z. B. optische Übertragungsmedien, Fibre Channel)

Solche Manipulationen verfolgen oftmals das Ziel, den IT-Betrieb zu stören oder finanzielle Schäden für die Institution zu verursachen.

**Beispiel:**

- Bei Ausbauarbeiten auf dem Gelände eines großen Unternehmens gelang es Angreifern, im schlecht zutrittsgeschützten Baustellenbereich einen Revisionsschacht zu öffnen. Mit einer Astschere wurde ein Glasfaserbündel der Primärverkabelung zerschnitten. Da damit einige Produktionsgebäude vom IT-Netz abgeschnitten waren, war der Betrieb gestört und teilweise unterbrochen, was einen Schaden in Millionenhöhe verursachte.

# G 5.9 Unberechtigte IT-Nutzung

Die Identifikation und Authentisierung von Benutzern soll verhindern, dass Informationstechnik unberechtigt benutzt wird. Aber auch bei IT-Systemen mit einer Identifikations- und Authentisierungsfunktion in Form von Benutzer-ID- und Passwort-Prüfung ist eine unberechtigte Nutzung denkbar, wenn die Zugangsdaten ausgespäht werden.

Um ein geheim gehaltenes Passwort zu erraten, können Unbefugte innerhalb der Login-Funktion ein mögliches Passwort eingeben. Die Reaktion des IT-Systems gibt anschließend Aufschluss darüber, ob das Passwort korrekt war oder nicht. Auf diese Weise können Passwörter durch Ausprobieren erraten werden.

Erfolg versprechender ist jedoch die Attacke, ein sinnvolles Wort als Passwort anzunehmen und alle Benutzereinträge durchzuprobieren. Bei entsprechend großer Benutzeranzahl wird damit oft eine gültige Kombination gefunden.

Falls die Identifikations- und Authentisierungsfunktion missbräuchlich nutzbar ist, so können sogar automatisch Versuche gestartet werden, indem ein Programm erstellt wird, das systematisch alle möglichen Passwörter testet.

Beispiel:

- Eine Schadsoftware nutzte eine Schwachstelle eines Unix-Betriebssystems aus, um gültige Passwörter zu finden, obwohl die Passwörter verschlüsselt gespeichert waren. Dazu probierte ein Programm sämtliche Eintragungen eines Wörterbuches aus, indem es sie mit der zur Verfügung stehenden Chiffrierfunktion verschlüsselte und das Ergebnis jeweils mit den abgespeicherten verschlüsselten Passwörtern verglich. Sobald eine Übereinstimmung gefunden war, war auch ein gültiges Passwort erkannt.

# G 5.10 Missbrauch von Fernwartungszugängen

Fernwartungszugänge ermöglichen es, von außen auf IT-Systeme zuzugreifen. Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, dass Unbefugte unbemerkt Zugang zu diesen IT-Systemen erlangen, unter Umständen sogar mit administrativen Berechtigungen. Beispielsweise könnten Angreifer nach Überwindung von Authentisierungsmechanismen wie der Passworteingabe alle Administrationstätigkeiten ausüben. Bei einem vollständigen Anlagenausfall, schweren Betriebsstörungen, verfälschten Daten oder auch dem Verlust der Vertraulichkeit aller auf dem betroffenen IT-System gespeicherten Daten, können unter Umständen große finanzielle Schäden entstehen.

**Beispiele:**

- Zur Weitergabe von Systemfehlern an den Hersteller wird bei Großrechnern mit dem Betriebssystem z/OS in der Regel das *Remote Support Facility (RSF)* eingesetzt. RSF kann auch verwendet werden, um seitens des Herstellers Patches am sogenannten Microcode vorzunehmen. Ein Missbrauch des RSF-Zugangs von z/OS-Systemen stellt deshalb eine erhebliche Gefahr dar.
- Weil die Passwort-Richtlinie mangelhaft durchgesetzt wurde beziehungsweise weil die Passwort-Richtlinie zu schwach war, konnte das Passwort für einen Wartungs-PC einer TK-Anlage durch systematisches Ausprobieren (durch eine Wörterbuchattacke) ermittelt werden. Nach Überwindung des Anlagenpasswortes konnte der Angreifer die TK-Anlage nach eigenen Vorstellungen administrieren.

# G 5.11 Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten

In TK-Anlagen werden personenbezogene und interne Daten für längere Zeit gespeichert, beispielsweise auf Festplatten oder Speicherkarten. Personenbezogene Daten sind beispielsweise Gebührendaten, Konfigurationsdaten, Berechtigungen und elektronische Telefonbücher, Passwörter und Verrechnungsnummern. Für die Rechnungserstellung können TK-Anlagen oft Verbindungsdatensätze aufzeichnen, die mindestens Informationen über die angerufene Teilnehmernummer, den Anrufzeitpunkt und die Dauer des Gesprächs enthalten. Hieraus lassen sich Kommunikationsprofile für einzelne Endgeräte oder Nutzer ableiten. Verbindungsdaten sind daher für Unbefugte interessant und müssen vor einem unautorisierten Zugriff geschützt werden.

Beim Betrieb von VoIP-TK-Anlagen können auch Sprachinformationen sehr effizient protokolliert werden, da diese schon digital vorliegen. So können beispielsweise auch alle geführten Telefongespräche vollständig auf Festplatten gespeichert und zur Auswertung auf ein anderes System kopiert werden. Es besteht das Risiko, dass eine solche Protokollierung der Telefonate unzulässigerweise aktiviert und für Angriffe auf die Vertraulichkeit missbraucht wird.

Viele TK-Applikationen arbeiten mit personenbezogenen Daten und reichen diese unter Umständen an andere Anwendungen weiter. Besonders hervorzuheben sind Unified Messaging-Systeme, bei denen die Auswirkungen eines Vertraulichkeitsverlustes aufgrund der zentralen Sammlung unterschiedlicher Nachrichtentypen gravierend sein können.

Die gespeicherten Daten könnten durch das TK-Administrationspersonal eingesehen und verändert werden. Art und Umfang dieser Eingriffe sind vom Anlagentyp und, falls vorgesehen, von der Rechtevergabe abhängig. Das Administrationspersonal hat diese Möglichkeit sowohl vor Ort als auch über Fernwartung. Bei einer externen Fernwartung hat der damit Beauftragte (im Regelfall der Hersteller oder ein Dienstleister) jederzeit diese Möglichkeit.

# G 5.12 Abhören von Telefongesprächen und Datenübertragungen

Wenn Telefongespräche oder Daten unverschlüsselt übertragen werden, besteht grundsätzlich die Gefahr, dass Angreifer Informationen mithören oder mitlesen. Angreifer könnten beispielsweise die Telefonkabel direkt anzapfen oder an einer, zwischen den Gesprächsteilnehmern vermittelnden TK-Anlage, lauschen.

Beim Einsatz von VoIP ist das Abhören von Telefongesprächen und Datenübertragungen einfacher als bei klassischen TK-Anlagen. Alle Sprachinformationen werden innerhalb eines IP-Medienstroms, beispielsweise mit dem *Realtime Transport Protocol* (RTP) übertragen. Durch Techniken wie *Spoofing* und *Sniffing* stehen alle Möglichkeiten von Angriffen in IP-Datennetzen zur Verfügung.

Bei vielen TK-Anlagen können Anrufer einem Empfänger Nachrichten hinterlassen, wenn dieser zum Zeitpunkt des Anrufs telefonisch nicht erreichbar ist. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei mittels einer E-Mail. Der Inhalt dieser Mail könnte, wie ein VoIP-Medienstrom, direkt von einem Angreifer abgefangen und angehört werden.

Weiterhin können unter Umständen auch durch die missbräuchliche Verwendung von Leistungsmerkmalen sowohl bei VoIP als auch bei den leitungsvermittelnden TK-Systemen Gespräche im Kollegenkreis mitgehört werden. Ein Beispiel hierfür ist die Dreierkonferenz. Erhält Teilnehmer A einen Anruf für Teilnehmer B, so könnte er, anstatt den Anruf zu übergeben, versuchen, heimlich eine Dreierkonferenz herzustellen. Hat Teilnehmer B ein Telefon ohne Display oder sieht nicht richtig hin, würde er diese Tatsache nicht bemerken.

Des Weiteren könnten Gespräche durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen Leistungsmerkmalen, von Dritten mitgehört werden. Als ein Beispiel sei hier die Zeugenschaltung erwähnt. Eine derartige Aktivierung erfordert genauere Systemkenntnisse, die aber aufgrund vieler frei verfügbarer Hinweise im Internet häufig kein großes Hindernis darstellen.

# G 5.13 Abhören von Räumen über TK-Endgeräte

Über Mikrofone in Endgeräten können grundsätzlich auch Räume abgehört werden. Dabei werden zwei Varianten unterschieden. Bei der ersten Variante geht die Bedrohung von einem Endgerät aus. Hier sind intelligente Endgeräte mit eingebauten Mikrofonen wie Multimedia-PCs, PDAs, Mobiltelefone, aber auch Anrufbeantworter zu nennen. Solche Endgeräte können, wenn entsprechende Funktionalitäten implementiert sind, aus dem öffentlichen Netz oder über das LAN, dazu veranlasst werden, die eingebauten Mikrofone zu aktivieren (siehe auch G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon und Kamera*). Ein bekanntes Beispiel hierfür ist die so genannte "Baby-Watch-Funktion" von Telefonen oder Anrufbeantwortern.

Bei der zweiten Variante wird die Funktionalität einer TK-Anlage in Verbindung mit entsprechend ausgerüsteten Endgeräten ausgenutzt. Diese Gefährdung entsteht durch die missbräuchliche Verwendung des Leistungsmerkmals "direktes Ansprechen" in Kombination mit der Option "Freisprechen". Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden. Im Normalfall wird ein kurzer, einmaliger Warnton bei Aktivierung des Mikrofons abgegeben. Warntöne können aber durch eine entsprechende Konfiguration unterbunden werden. Jeder, der in der Lage ist, eine TK-Anlage zu administrieren, könnte in diesem Fall jeden Raum, in dem ein entsprechend ausgerüstetes Telefon steht, von jedem Endgerät mit Zugriff auf die TK-Anlage oder den Anlagenverbund abhören.

Bei der Nutzung von VoIP-Softphones ergibt sich ein weiteres Gefährdungsszenario. Diese Applikationen ermöglichen die Verwendung eines Multimedia-PCs als Telefon-Endgerät. Der Multimedia-PC wird in der Regel auch für weitere Aufgaben genutzt, beispielsweise um im Internet zu surfen. Da ein Mikrofon für die Sprachübermittlung benötigt wird, könnte es unter Umständen durch Schadsoftware aktiviert und die Umgebung des PCs abgehört werden.

# G 5.14 Gebührenbetrug

Gebührenbetrug im Zusammenhang mit Daten- oder Telekommunikationsdiensten hat das Ziel, die Kosten für geführte Telefonate oder Datenübertragungen auf jemand anderen zu übertragen, beispielsweise durch missbräuchliche Nutzung einer TK-Anlage. Entsprechende Manipulationen sind auf verschiedene Weise durchführbar. Zum einen kann versucht werden, vorhandene Leistungsmerkmale einer TK-Anlage für diese Zwecke zu missbrauchen. Geeignet hierfür sind beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-In-Optionen. Zum anderen können die Berechtigungen so vergeben werden, dass kommende "Amtsleitungen" abgehende "Amtsleitungen" belegen. Auf diese Weise kann der Anrufer bei Anwahl einer bestimmten Rufnummer von außen automatisch wieder mit dem "Amt" verbunden werden, wobei dies auf Kosten des TK-Anlagenbetreibers geschieht.

Neben den technischen Möglichkeiten kann ein Gebührenbetrug auch durch die Benutzer selbst erfolgen. Auf unterschiedliche Arten, wie z. B. durch das Telefonieren von fremden Apparaten, Auslesen fremder Berechtigungscodes (Passwort) oder Verändern der persönlichen Berechtigungen kann versucht werden, auf Kosten des Arbeitgebers oder der anderen Beschäftigten zu telefonieren.

# G 5.15 Missbrauch von Leistungsmerkmalen von TK-Anlagen

Klassische TK-Anlagen verfügen in der Regel über eine Vielzahl von Leistungsmerkmalen, um den Benutzern größtmögliche Bequemlichkeit bei der Kommunikation und eine möglichst weitgehende Anpassung an die jeweilige Arbeitsumgebung zu bieten. Einige Leistungsmerkmale können allerdings auch zu gezielten Angriffen missbraucht werden, insbesondere auf Vertraulichkeit oder Verfügbarkeit.

**Beispiele:**

- Die Funktionalitäten "direktes Ansprechen" und "automatische Rufannahme" können in Verbindung mit einer Freisprechfunktionalität bei Telefonen zum Abhören von Räumen missbraucht werden.
- Bei einer Rufumleitung kann durch versehentliche oder böswillige Fehlnutzung die Nichterreichbarkeit des Telefonanschlusses eines Nutzers die Folge sein.
- Dial-In-Funktionalitäten ermöglichen einen Zugriff von außen für mobile Mitarbeiter, können aber auch für Angriff, beispielsweise zum Gebührenbetrug, missbraucht werden.
- Die Funktion "Konferenzschaltung" könnte zu einem unbemerkten Aufbau einer Verbindung im Hintergrund ausgenutzt werden.
- Funktionen wie beispielsweise die "Zeugenschaltung" oder das "Abhören", die zu in Deutschland untersagten Export-Merkmalen von TK-Anlagen gehören, könnten zum unbemerkten Mithören von Telefongesprächen genutzt werden.

Einige der Leistungsmerkmale von TK-Anlagen können möglicherweise durch Mitarbeiter missbraucht werden, da hierfür keine vertieften Kenntnisse erforderlich sind. Beispielsweise könnten Mitarbeiter versuchen,

- unerlaubt Anrufe für Kollegen auf ihren eigenen Telefonapparat umzuleiten,
- unerlaubt Anrufe für andere anzunehmen,
- mit der Funktion "Freisprechen / Lauthören" Raumgespräche abzuhören,
- unerlaubt fremde Anruf- und Wahlwiederholspeicher auszulesen und
- durch das Aufschalten auf Verbindungen Dritter unerlaubt Telefongespräche mitzuhören.

Hierdurch besteht die Gefahr, dass Mitarbeiter unerlaubt Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

# G 5.16 Gefährdung bei Wartungs-/ Administrierungsarbeiten

Ein IT-System kann bei Wartungsarbeiten auf jedwede Weise manipuliert werden. Die Gefahr besteht in erster Linie darin, dass der Eigentümer oft nicht in der Lage ist, die vorgenommenen Modifikationen sofort zu erkennen und nachzuvollziehen. Darüber hinaus haben externe sowie interne Wartungstechniker üblicherweise auch vollen Zugriff auf alle auf den betreuten IT-Systemen gespeicherten Daten.

Externe Wartungstechniker könnten versuchen, sich unbefugt interne Informationen zu verschaffen oder sich Hintertüren einzubauen, um jederzeit Zugriff auf die IT-Systeme zu haben.

Zum eigenen Vorteil oder aus Gefälligkeit für Kollegen könnte bei Wartungs- oder Administrationsarbeiten durch internes Personal versucht werden, Berechtigungen (z. B. Auslandsberechtigung für Telefongespräche oder Zugriff auf Internetdienste) zu ändern oder weitere Leistungsmerkmale zu aktivieren. Dabei können durch Unkenntnis Systemabstürze verursacht werden oder weitere Sicherheitslücken durch Konfigurationsfehler eröffnet werden.

Das Wartungspersonal hat außerdem häufig vollen Zugriff auf die gespeicherten Daten auf den betreuten IT-Systemen (lesend und schreibend). Selbst wenn der Zugriff auf bestimmte Speicherbereiche oder bestimmte Zeiten eingeschränkt ist, lässt dies Spielraum, auf die gespeicherten Daten zuzugreifen und diese eventuell unbefugt weiterzugeben oder zu manipulieren.

Auch die eigenhändige Steuerung oder zeitweilige Deaktivierung von Regel- oder Alarmtechnik bei der Wartung birgt ein hohes Gefährdungspotential. Dies betrifft auch Gefahrenmeldeanlagen und Leitsysteme.

**Beispiele:**

- Eine kurzfristig eingestellte Aushilfe, die die Aufgabe hatte, nicht mehr genutzte Accounts zu sperren, nutzt ihre umfassende Berechtigung, um sich urheberrechtlich geschützte Software vom zentralen Applikationsserver für private Zwecke herunterzuladen. Um das Programm auch gleich an Freunde verteilen zu können, nutzt er dienstliche CD-ROM-/DVD-Brenner und Datenträger.
- Damit eine Kollegin auch während der Dienstzeit ihre privaten Homebanking-Transaktionen ausführen kann, wird ihr aus Gefälligkeit ein exklusiver Zugang zu ihrem Internet-Provider via ISDN zugänglich gemacht. Als sie sich zu Ostern einen Bildschirmschoner aus dem Internet herunterlädt, infiziert sie ihren PC mit einem Virus. Da der Rechner mit dem Hausnetz verbunden ist, verbreitet sich der Virus sehr schnell. Das Unternehmensnetz ist bis zur Behebung des Problems für mehrere Stunden nicht nutzbar.
- Einbruchmeldeanlagen haben in vielen Fällen einen integrierten Protokollierungsdrucker. Es kommt immer wieder vor, dass die Einbruchmeldeanlage zum Auswechseln des hierzu erforderlichen Druckerpapiers "vorsorglich" abgeschaltet wird. Beim anschließenden Wiedereinschalten besteht die Gefahr, dass das System unsachgemäß gestartet wird und sich dadurch Fehlfunktionen ergeben.

# G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in G 5.16 *Gefährdung bei Wartungs-/Administrierungsarbeiten* integriert.

# G 5.18 Systematisches Ausprobieren von Passwörtern

Zu einfache Passwörter lassen sich durch systematisches Ausprobieren herausfinden. Dabei ist zwischen dem simplen Ausprobieren aller möglichen Zeichenkombinationen bis zu einer bestimmten Länge (sogenannter Brute-Force-Angriff) und dem Ausprobieren anhand einer Liste mit Zeichenkombinationen (sogenannter Wörterbuch-Angriff) zu unterscheiden. Beide Ansätze lassen sich auch kombinieren.

Die meisten Betriebssysteme verfügen über eine Datei oder Datenbank (z. B. passwd- bzw. shadow-Datei bei Unix oder RACF-Datenbank bei z/OS) mit den Kennungen und Passwörtern der Benutzer. Allerdings werden zumindest die Passwörter bei vielen Betriebssystemen nicht im Klartext gespeichert, sondern es kommen kryptographische Mechanismen zum Einsatz. Ist die Datei nur unzureichend gegen unbefugten Zugriff geschützt, kann ein Angreifer diese Datei möglicherweise kopieren und mit Hilfe leistungsfähigerer Rechner und ohne Einschränkungen hinsichtlich der Zugriffszeit einem Brute-Force-Angriff aussetzen.

Die Zeit, die bei einem Brute-Force-Angriff zum Herausfinden eines Passworts benötigt wird, hängt ab von

- der Dauer einer einzelnen Passwortprüfung,
- der Länge des Passworts und
- der Komplexität des Passworts.

Die Dauer einer einzelnen Passwortprüfung hängt stark vom jeweiligen System und dessen Verarbeitungs- bzw. Übertragungsgeschwindigkeit ab. Im Falle eines Angriffs spielen auch die Methode und die Technik des Angreifers eine Rolle.

Die Verwendung von Rainbow Tables kann die benötigte Rechenzeit noch einmal deutlich verringern. In Rainbow Tables werden Passwörter in zusammenhängenden Passwortsequenzen durch eine Hashfunktion und weitere Funktionen verkettet. Wenn keine entsprechenden Gegenmaßnahmen bei der Implementierung der Passwort-Prüfung getroffen wurden, können Rainbow Tables von Angreifern missbraucht werden, um Brute-Force-Angriffe zu beschleunigen.

Länge und Zeichenzusammensetzung des Passworts lassen sich dagegen durch organisatorische Vorgaben oder sogar durch technische Maßnahmen beeinflussen.

Beispiel:

- Bei einem Zeichenvorrat von 26 Zeichen, also zum Beispiel, wenn für Passwörter nur Kleinbuchstaben ohne Sonderzeichen verwendet werden, ergeben sich für ein acht Zeichen langes Passwort circa 209 Milliarden mögliche Kombinationen. Ein moderner PC, der circa 100 Millionen Hashwerte pro Sekunde berechnen kann, hätte nach 35 Minuten alle möglichen Passwörter mit acht Kleinbuchstaben geprüft. Durch die Verwendung von Sonderzeichen, Großbuchstaben und Zahlen steigt die Anzahl der verwendbaren Zeichen auf 72 an. Bei achtstelligen Passwörtern wären damit 722 Billionen Kombinationen möglich. Um mit handelsüblichen PCs alle Hashwerte zu berechnen, würden ca. 83 Tage benötigt.

# G 5.19 Missbrauch von Benutzerrechten

Eine missbräuchliche Nutzung liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten ausnutzt, um dem System oder dessen Benutzern zu schaden.

In nicht wenigen Fällen verfügen Anwender aus systemtechnischen Gründen über höhere oder umfangreichere Zugriffsrechte, als sie für ihre Tätigkeit benötigen. Diese Rechte können zum Ausspähen von Daten verwendet werden, auch wenn Arbeitsanweisungen den Zugriff verbieten.

**Beispiele:**

- Auf vielen Unix-Systemen ist die Datei */etc/passwd* für jeden Benutzer lesbar, so dass er sich Informationen über dort eingetragene persönliche Daten verschaffen kann. Außerdem kann er mit Wörterbuchattacken (siehe G 5.18 *Systematisches Ausprobieren von Passwörtern*) versuchen, die verschlüsselten Passwörter zu erraten. Bei zu großzügiger Vergabe von Gruppenrechten, insbesondere bei den Systemgruppen wie z. B. *root, bin, adm, news* oder *daemon*, ist ein Missbrauch wie z. B. das Verändern oder Löschen fremder Dateien leicht möglich.
- Ein für die Verwaltung der Festplatten in z/OS-Systemen zuständiger Storage-Administrator konnte dank des Attributes *Operations*, das er für die Ausführung seiner Tätigkeit von der RACF-Administration erhalten hatte, Kundendateien einsehen. Er nutzte dieses Zugriffsrecht aus, um unerlaubt Kopien zu erstellen.

# G 5.20 Missbrauch von Administratorrechten

Eine missbräuchliche Administration liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Super-User- (*root*-) Privilegien ausnutzt, um dem System oder dessen Benutzern zu schaden.

**Beispiele:**

- Da *root* auf Unix-Anlagen keinerlei Beschränkungen unterliegt, kann der Administrator unabhängig von Zugriffsrechten jede Datei lesen, verändern oder löschen. Außerdem kann er die Identität jedes Benutzers seines Systems annehmen, ohne dass dies von einem anderen Benutzer bemerkt wird, es ist ihm also z. B. möglich, unter fremden Namen Mails zu verschicken oder fremde Mails zu lesen und zu löschen.
- Es gibt verschiedene Möglichkeiten, missbräuchlich Super-User-Privilegien auszunutzen. Dazu gehören der Missbrauch von falsch administrierten Super-User-Dateien (Dateien mit Eigentümer *root* und gesetztem s-Bit) und des Befehls *su*.
- Die Gefährdung kann auch durch automatisches Mounten von austauschbaren Datenträgern entstehen: Sobald das Medium in das Laufwerk gelegt wird, wird es gemountet. Dann hat jeder Zugriff auf die dortigen Dateien. Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann jeder Benutzer Super-User-Rechte erlangen.
- In Abhängigkeit von der Unix-Variante und der zugrunde liegenden Hardware kann bei Zugangsmöglichkeit zur Konsole der Monitor-Modus aktiviert oder in den Single-User-Modus gebootet werden. Das ermöglicht die Manipulation der Konfiguration.
- Durch Softwarefehler kann es möglich sein, dass eine Anwendung nur eine begrenzt große Menge an Daten verarbeiten kann. Werden dieser Anwendung übergroße Datenmengen oder Parameter übergeben, können Bereiche im Hauptspeicher mit fremdem Code überschrieben werden. Dadurch können Befehle mit den Rechten der Anwendung ausgeführt werden. Dies war unter anderem mit dem Befehl *eject* unter SunOS 5.5 möglich, der mit SetUID-Rechten ausgestattet ist, also bei der Ausführung Super-User-Rechte besitzt.

# G 5.21 Trojanische Pferde

Ein Trojanisches Pferd, oft auch (eigentlich fälschlicherweise) kurz *Trojaner* genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Der Benutzer kann daher auf die Ausführung dieser Funktion keinen Einfluss nehmen - insoweit besteht eine gewisse Verwandtschaft mit Computer-Viren. Es ist jedoch keine Selbstreproduktion vorhanden. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen. Aber auch Scriptsprachen, wie Batch-Dateien, ANSI-Steuersequenzen, *REXX Execs* und *ISPF Command Tables* bei z/OS-Betriebssystemen, Postscript und Ähnliches, die vom jeweiligen Betriebssystem oder Anwenderprogramm interpretiert werden, können für Trojanische Pferde missbraucht werden.

Die Schadwirkung eines Trojanischen Pferdes ist um so wirkungsvoller, je mehr Rechte sein Trägerprogramm besitzt.

**Beispiele:**

- Ein geändertes Login-Programm kann ein Trojanisches Pferd enthalten, das Namen und Passwort des Benutzers über das Netz an den Angreifer übermittelt und dann an das eigentliche Login-Programm weitergibt. Solche Trojanischen Pferde sind z. B. bei Online-Diensten wie AOL oder T-Online aufgetreten.
- Auch Bildschirmschoner, besonders solche, die aus dem Internet herunter geladen werden, können eine versteckte Funktion enthalten, mit der die eingegebenen Passwörter des angemeldeten Benutzers protokolliert und an einen Angreifer übermittelt.
- Bei dem Programm *Back Orifice* handelt es sich um eine Client-Server-Anwendung, die es dem Client erlaubt, einen Windows-PC über das Netz fernzuwarten. Insbesondere können Daten gelesen und geschrieben sowie Programme ausgeführt werden. Eine Gefährdung entsteht dadurch, dass dieses Programm in ein anderes Anwendungsprogramm integriert und somit als Trojanisches Pferd verwendet werden kann. Wird das Trojanische Pferd gestartet und besteht eine Netzverbindung, so kann ein Angreifer die Fernwartungsfunktion von *Back Orifice* für den Benutzer unbemerkt benutzen. In diesem Zusammenhang ist auch das Programm NetBUS zu erwähnen, das ähnliche Funktionen bietet.
- Mit Hilfe von Root-Kits für verschiedene Unix-Varianten, die manipulierte Versionen von Systemprogrammen wie *ps*, *who*, *netstat* etc. enthalten, ist es möglich, längere Zeit unbemerkt Hintertüren (so genannte *Backdoors*) offen zu halten, die einen unbemerkten Einbruch in das System ermöglichen und dabei die Angriffsspuren verstecken. Häufig werden u. a. die Dateien */sbin/in.telnetd, /bin/login, /bin/ps, /bin/who, /bin/netstat* und die C-Libraries ausgetauscht.
- Eine weitere Gefahrenquelle bei Unix-Systemen ist der "." in der Umgebungsvariable *$PATH*. Wenn das jeweils aktuelle Arbeitsverzeichnis (.) als Pfad in der Variable *PATH* enthalten ist, werden zunächst die dort befindlichen Programme ausgeführt. So könnte beim Auflisten des Inhaltes eines Verzeichnisses vom Superuser unbeabsichtigt ein darin enthaltenes modifiziertes "*ls*"-Programm mit root-Rechten ausgeführt werden.
- Eine Möglichkeit, sich im z/OS-Betriebssystem höhere Rechte zu erschleichen, bietet sich dann, wenn für den Angreifer ein *Update*-Zugriff auf Dateien existiert, die entweder beim Logon-Vorgang durchlaufen (z. B. eine *REXX EXEC*) oder während der Verarbeitung allgemein benutzt werden (z. B. *ISPF Command Tables*). Der Angreifer kann dann den vorhandenen Code durch eigene Programmteile ersetzen.

# G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems

Wird ein IT-System mobil genutzt, so ergeben sich neue Gefährdungen, die stationäre IT-Systeme nicht im gleichen Maße bedrohen. Mobile Systeme wie Laptops werden üblicherweise nicht in einem durch Schutzvorkehrungen gesicherten Raum eingesetzt. Sie werden in PKW oder öffentlichen Verkehrsmitteln transportiert, in fremden Büroräumen in Pausen zurück gelassen oder in Hotelzimmern unbewacht aufgestellt.

Aufgrund dieser Umfeldbedingungen sind solche mobil eingesetzten IT-Systeme naturgemäß einem höheren Diebstahlrisiko ausgesetzt. Der im Kofferraum eines PKW eingeschlossene Laptop kann überdies gestohlen werden, ohne dass dies das originäre Ziel des Diebstahls war, denn wenn der Wagen gestohlen wird, gerät auch der Laptop in die falschen Hände.

**Beispiel:**

- Dem Geschäftsführer einer größeren Firma wurde auf einer Dienstreise der Laptop gestohlen. Der materielle Verlust war vernachlässigbar, innerhalb eines Tages konnte ein neues Gerät beschafft werden. Schmerzlicher war der Verlust von wichtigen Kundendaten, die auf dem Laptop gespeichert waren. Von diesen Informationen gab es keine Datensicherung, da sie erst im Verlauf der Geschäftsreise erfasst worden waren.

# G 5.23 Schadprogramme

Ein Schadprogramm ist eine Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Zu den typischen Arten von Schadprogrammen gehören unter anderem Viren, Würmer und Trojanische Pferde. Schadprogramme werden meist heimlich, ohne Wissen und Einwilligung des Benutzers aktiv.

Schadprogramme bieten heutzutage einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können Schadprogramme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren.

Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch der Imageverlust und der finanzielle Schaden, der durch Schadprogramme entstehen kann, ist von großer Bedeutung.

**Beispiele:**

- In der Vergangenheit verbreitete sich das Schadprogramm W32/Bugbear auf zwei Wegen: Es suchte in lokalen Netzen nach Computern mit Freigaben, auf die schreibender Zugriff möglich war, und kopierte sich darauf. Zudem schickte es sich selbst als HTML-E-Mail an Empfänger im E-Mail-Adressbuch von befallenen Computern. Durch einen Fehler in der HTML-Routine bestimmter E-Mail-Programme wurde das Schadprogramm dort beim Öffnen der Nachricht ohne weiteres Zutun des Empfängers ausgeführt.
- Das Schadprogramm W32/Klez verbreitete sich in verschiedenen Varianten. Befallene Computer schickten den Virus an alle Empfänger im E-Mail-Adressbuch des Computers. Hatte dieser Virus einen Computer befallen, verhinderte er durch fortlaufende Manipulationen am Betriebssystem die Installation von Viren-Schutzprogrammen verbreiteter Hersteller und erschwerte so die Desinfektion der befallenen Computer erheblich.
- Auch gewisse Arten von eingebetteten Systemen können von Schadsoftware befallen werden. Prominentester Vertreter ist "Stuxnet", eine auf Prozesssteuerungssysteme spezialisierte Schadsoftware, welche dort unter anderem Prozessdaten manipuliert. Die Schadsoftware "Duqu" ist eine vermutete Weiterentwicklung von Stuxnet und soll vermutlich vor allem dazu dienen, Informationen zur Vorbereitung von Angriffen zu sammeln. Ebenfalls im Verdacht Industrieanlagen anzugreifen steht der Trojaner "Havex Remote Access Trojan". Er versucht Netzwerkverkehr mitzulesen und ein infiziertes System unter administrative Kontrolle zu bringen und fernzusteuern.

# G 5.24 Wiedereinspielen von Nachrichten

Angreifer zeichnen bei dieser Art Angriff Nachricht auf und spielen sie zu einem späteren Zeitpunkt unverändert wieder ein (Replay-Attacken). Dies kann benutzt werden, um IT-Systeme oder Anwendungen durch scheinbar echte Nachrichten dazu zu veranlassen, unautorisierte Zugriffe zuzulassen. Dies ist möglich, weil das System von einer bestehenden und bereits autorisierten Kommunikation ausgeht.

Auch verschlüsselte Nachrichten können wieder eingespielt werden, wenn sie keine dynamischen, also veränderlichen Informationen enthalten, wie beispielsweise Zufallszahlen, Sequenznummern oder Zeitstempel.

**Beispiele:**

- Ein Angreifer zeichnet die Authentisierungsdaten (z. B. Benutzer-ID und Passwort) während des Anmeldevorgangs eines Benutzers auf und verwendet diese Informationen, um sich unter Vortäuschen einer falschen Identität Zugang zu einem System zu verschaffen (siehe auch G 5.21 *Trojanische Pferde*).
- Um finanziellen Schaden beim Arbeitgeber zu verursachen, gibt ein Mitarbeiter eine genehmigte Bestellung mehrmals auf.

# G 5.25 Maskerade

Die Maskerade benutzt ein Angreifer um eine falsche Identität vorzutäuschen. Eine falsche Identität erlangt er z. B. durch das Ausspähen von Benutzer-ID und Passwort (siehe auch G 5.9 *Unberechtigte IT-Nutzung*), die Manipulation des Absenderfeldes einer Nachricht oder durch die Manipulation einer Adresse (siehe beispielsweise auch G 5.48 *IP-Spoofing* oder G 5.87 *Web-Spoofing*) im Netz. Weiterhin kann eine falsche Identität durch die Manipulation der Rufnummernanzeige (Calling Line Identification Presentation) im ISDN oder durch die Manipulation der Absenderkennung eines Faxabsenders (CSID - Call Subscriber ID) erlangt werden.

Ein Benutzer, der über die Identität seines Kommunikationspartners getäuscht wurde, kann leicht dazu gebracht werden, schutzbedürftige Informationen zu offenbaren.

Ein Angreifer kann durch eine Maskerade auch versuchen, sich in eine bereits bestehende Verbindung einzuhängen, ohne sich selber authentisieren zu müssen, da dieser Schritt bereits von den originären Kommunikationsteilnehmern durchlaufen wurde (siehe dazu auch G 5.89 *Hijacking von Netz-Verbindungen*).

# G 5.26 Analyse des Nachrichtenflusses

Über eine Verkehrsflussanalyse versucht ein Angreifer Auskunft darüber zu erhalten, wer wann welche Datenmengen an wen gesendet hat und wie oft. Sogar wenn der Lauscher die Nachrichteninhalte nicht lesen kann, können hierdurch Rückschlüsse auf das Benutzerverhalten gezogen werden. Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adresssammler für Adressverlage nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.

Innerhalb des ISDN (Integrated Services Digital Network) wäre der D-Kanal einer Kommunikationsverbindung, welcher der Signalisierung zwischen Endgerät und Vermittlungsstelle dient, ein geeigneter Angriffspunkt. Die Analyse der dort übertragenen Signalisierung mittels eines Protokollanalysators lässt nicht nur die o. a. Rückschlüsse auf das Benutzerverhalten zu (z. B. wer telefoniert wann mit wem wie lange?), sondern kann auch der Vorbereitung komplexerer Angriffe über den D-Kanal dienen.

# G 5.27 Nichtanerkennung einer Nachricht

Bei jeder Art von Kommunikation kann ein Kommunikationsteilnehmer den Nachrichtenempfang ableugnen (Repudiation of Receipt). Dies ist insbesondere bei finanziellen Transaktionen von Bedeutung. Ein Nachrichtenempfang kann beim Postversand ebenso abgeleugnet werden wie bei Fax-, E Mail- oder SMS-Nutzung.

**Beispiele:**

- Ein dringend benötigtes Ersatzteil wurde elektronisch bestellt. Nach einer Woche Arbeitsausfall wurde das Fehlen der Ware reklamiert. Der Lieferant leugnet, je eine Bestellung erhalten zu haben.
- Ebenso kann es passieren, dass ein Kommunikationsteilnehmer den Nachrichtenversand ableugnet, also beispielsweise eine getätigte Bestellung abstreitet (Repudiation of Origin).
- An einem Feiertag wird der Administrator einer Institution per SMS alarmiert, dass ein Server ausgefallen ist. Der Administrator trifft aber nicht in der Institution ein und streitet hinterher ab, eine solche SMS erhalten zu haben. Durch die Verzögerung fällt der Server längere Zeit aus, wodurch wirtschaftlicher Schaden entsteht.

# G 5.28 Verhinderung von Diensten

Ein solcher Angriff, auch "Denial of Service" genannt, zielt darauf ab, die Benutzer daran zu hindern, Funktionen oder Geräte zu verwenden, die ihnen normalerweise zur Verfügung stehen. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass andere Benutzer an der Arbeit gehindert werden. Es können zum Beispiel die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Plattenplatz, Inodes, Verzeichnisse.

Dies kann zum Beispiel geschehen durch:

- das Starten von beliebig vielen Programmen gleichzeitig,
- das mehrfache Starten von Programmen, die viel CPU-Zeit verbrauchen,
- das Belegen aller freien Inodes in einem Unix-System, sodass keine neuen Dateien mehr angelegt werden können,
- unkoordiniertes Belegen von Bandstationen in z/OS-Systemen, sodass Anwendungen auf freie Bandstationen warten müssen und die Online-Verarbeitung eingeschränkt ist,
- bewusste Falscheingabe von Passwörtern (auch Skript-gesteuert) mit dem Ziel der Sperrung aller Kennungen eines z/OS-Systems,
- das Versenden bestimmter konstruierter Datenpakete, die beim Empfänger aufgrund von Software-Schwachstellen zu Fehlfunktionen oder zu einer Überlastung führen können (zum Beispiel indem exzessiv kryptographische Operationen aufgerufen werden),
- die gezielte Überlastung des Netzes,
- das Kappen von Netzverbindungen
- das gezielte Generieren von XML-Nachrichten mit großen Datenmengen, rekursiven Inhalten, einer großen Anzahl an Verschachtelungen und fehlerhaften DTDs, sodass ein XML-Parser intensiv Speicherressourcen seines Systems belegt.

# G 5.29 Unberechtigtes Kopieren der Datenträger

Werden Datenträger ausgetauscht oder transportiert, so bedeutet dies unter Umständen, dass die zu übermittelnden Informationen aus einer gesicherten Umgebung heraus über einen unsicheren Transportweg in eine unter Umständen unsichere Umgebung beim Empfänger übertragen werden. Unbefugte können sich in solchen Fällen diese Informationen dort durch Kopieren einfacher beschaffen, als es in der ursprünglichen Umgebung der Fall war.

Wegen der großen Konzentration schützenswerter Informationen auf Datenträgern elektronischer Archive (z. B. personenbezogene oder firmenvertrauliche Daten) stellen diese ein besonderes Angriffsziel für Diebstahl oder Kopie durch Unbefugte dar.

**Beispiel:**

- Vertrauliche Entwicklungsergebnisse sollen vom Entwicklungslabor in X-Stadt zur Produktion nach Y-Stadt transportiert werden. Werden die entsprechenden Datenträger unkontrolliert über den Postweg versandt, kann nicht ausgeschlossen werden, dass diese unberechtigterweise kopiert und gegebenenfalls an die Konkurrenz verkauft werden, ohne dass die Bloßstellung der Informationen bemerkt wird.

# G 5.30 Unbefugte Nutzung eines Faxgerätes oder eines Faxservers

Der unberechtigte Zugang zu einem Faxgerät oder unberechtigte Zugriff auf einen Faxserver kann für manipulative Zwecke ausgenutzt werden. Dabei können neben den Kosten für die Faxübertragung (Gebühren und Material) auch Schäden dadurch entstehen, dass ein Unbefugter vorgibt, das Gerät als Berechtigter zu nutzen (Schreiben mit Firmenkopf vom entsprechenden Fax-Anschluss).

Es muss zudem vermieden werden, dass Unbefugte Zugriff auf eingehende Faxsendungen haben.

**Beispiele:**
- Ein Faxgerät ist im Flur aufgestellt, so dass jeder im Vorbeigehen unkontrolliert Faxe lesen oder an sich nehmen kann.
- Bei einem Faxserver sind die Berechtigungen auf die gespeicherten Faxdaten falsch gesetzt, so dass Unbefugte fremde Faxe lesen können.

# G 5.31 Unbefugtes Lesen von Faxsendungen

Beim Einsatz von Faxgeräten besteht dann die Gefahr des unbefugten Lesens eingegangener Faxsendungen, wenn die Geräte in frei zugänglichen Bereichen aufgestellt werden. Zudem können Unbefugte Kenntnis vom Inhalt vertraulicher Faxsendungen erlangen, wenn die Verteilung innerhalb der Organisation fehlerhaft ist.

Beim Einsatz von Faxservern ist eine unbefugte Kenntnisnahme ein- und ausgehender Faxsendungen u. U. möglich, sofern die Zugriffsrechte auf dem Faxserver nicht sorgfältig vergeben werden.

Faxserver verfügen zudem über so genannte Adressbücher. Die Adressbücher erleichtern die Versendung von Faxen, da die Benutzer nur den jeweiligen Empfänger auswählen und nicht bei jedem Fax die Empfängerrufnummer erneut eingeben müssen. Sofern in einem Adressbuch eine falsche Empfängerrufnummer eingetragen ist, wird bei Benutzung dieses Eintrages das Fax an den falschen Empfänger gesendet. Häufig bieten Adressbücher auch die Möglichkeit, mehrere Adressaten zu einer Gruppe zusammenzufassen. Der Benutzer, der ein Fax an die Mitglieder einer solchen Gruppe senden will, braucht als Empfänger nur die Gruppe und nicht jedes Gruppenmitglied anzugeben. Sofern sich in solch einer Gruppe unbefugte Adressaten befinden, können diese Kenntnis von allen Faxsendungen erhalten, die über diese Gruppendefinition versandt werden. Die falsche Zuordnung kann durch Unachtsamkeit oder aufgrund einer gezielten Manipulation erfolgen.

Auf einem Faxserver eingegangene Faxsendungen müssen an die Empfänger verteilt werden. Dies kann entweder dadurch erfolgen, dass Eingangs-Faxsendungen ausgedruckt und manuell an die Empfänger weitergeleitet werden oder dass der Faxserver die Verteilung automatisch über das Netz vornimmt.

Eine unbefugte Kenntnisnahme von eingegangenen Faxsendungen ist u. U. bei der manuellen Verteilung möglich, wenn der Drucker, auf dem der Ausdruck erfolgt, in einem allgemein zugänglichen Bereich aufgestellt wurde oder die Verteilung innerhalb der Organisation fehlerhaft ist.

Bei der automatischen Weiterleitung von Faxsendungen benötigt der Faxserver eine Zuordnungstabelle, in der festgelegt wird, an welchen Benutzer bzw. an welche Benutzergruppe Eingangs-Faxsendungen, die z. B. von einem bestimmten Absender stammen oder über eine bestimmte Rufnummer gesendet wurden, weitergeleitet werden sollen. Sofern ein Unbefugter in einer solchen Zuordnungstabelle - sei es durch Unachtsamkeit oder aufgrund einer gezielten Manipulation - aufgenommen wird, erhält er Faxsendungen, die nicht für ihn bestimmt sind.

# G 5.32 Auswertung von Restinformationen in Faxgeräten und Faxservern

**Faxgeräte**

Abhängig vom technischen Verfahren, mit denen Faxgeräte Informationen speichern, weiterverarbeiten oder drucken, können sich nach dem Faxempfang Restinformationen unterschiedlichen Umfanges im Faxgerät befinden. Sie können wiederhergestellt werden, wenn man in den Besitz des Gerätes oder der entsprechenden Bauteile kommt.

Bei Faxgeräten, die mittels des Thermotransferverfahrens drucken, werden eingehende Faxsendungen zunächst auf eine Zwischenträgerfolie geschrieben, mit deren Hilfe sie dann ausgedruckt werden. Diese Folie ist Verbrauchsmaterial und muss regelmäßig ausgetauscht werden, das Entfernen der Folie ist daher leicht möglich. Gelangt ein Unbefugter in den Besitz dieser Folie (durch Diebstahl oder bei der Entsorgung), kann er den Inhalt mit einfachen technischen Mitteln reproduzieren. Dabei können ihm die Informationen von mehreren hundert Faxseiten bekannt werden.

Die meisten Faxgeräte verfügen über einen Zwischenspeicher (Dokumentenspeicher, Puffer), in den ausgehende Faxe bis zur erfolgreichen Übertragung eingelesen bzw. eingehende Faxe vor dem Ausdrucken zwischengespeichert werden können. Dieser Speicher kann je nach Faxgerät eine größere Anzahl Faxseiten enthalten und kann im Allgemeinen von jedem, der Zugang zum Faxgerät hat, ausgedruckt werden.

**Faxserver**

Faxserver sind Applikationen, die auf IT-Systemen installiert sind, die in aller Regel mit mindestens einer Festplatte ausgestattet sind oder über das Netz auf ein Laufwerk zugreifen können. Hierauf werden Faxsendungen solange gespeichert, bis sie an einen Empfänger zugestellt werden können. Weiterhin arbeiten moderne Betriebssysteme mit Auslagerungsdateien, die auch Restinformationen enthalten können. Hier besteht die Gefahr, dass diese Informationen bei Zugriff auf diesen Faxserver unerlaubt ausgewertet werden. Fällt z. B. eine Festplatte während der Garantiezeit aus, muss diese zur Geltendmachung von Garantieansprüchen an den Händler oder an den Hersteller eingesandt werden. Problematisch ist dabei, dass sich noch Daten auf der Festplatte befinden können, von denen Unbefugte auf diesem Weg Kenntnis erlangen können. Bei defekten Festplatten ist eine Löschung der Daten mit Softwaretools häufig nicht möglich.

Ein unbefugter Zugriff auf Faxdaten im Faxclient ist dann möglich, wenn ein Arbeitsplatzrechner bzw. die dort installierte Fax-Software nicht ausreichend gesichert ist. Auch beim Zugriff auf die Festplatte des Arbeitsplatzrechners können Informationen von Unbefugten ausgelesen werden.

# G 5.33 Vortäuschen eines falschen Absenders bei Faxsendungen

So wie man einen Brief unter falschem Namen und mit falschem Briefkopf schreiben kann, kann man auch ein entsprechend gefälschtes Fax versenden. Dadurch können Schäden entstehen, wenn der Empfänger die darin enthaltenen Informationen als authentisch und ggf. als rechtsverbindlich ansieht (siehe G 3.14 *Fehleinschätzung der Rechtsverbindlichkeit eines Fax*).

**Beispiele:**

- Unterschriften können von anderen Schriftstücken eingescannt und auf die Faxvorlage ausgedruckt bzw. beim Einsatz eines Faxservers als Grafikdatei in das Schriftstück einkopiert werden. Auf dem empfangenen Fax ist kein Unterschied zwischen einer so reproduzierten und einer authentischen handschriftlichen Unterschrift erkennbar.
- Bei der Übertragung wird in der Regel die Rufnummer des sendenden Faxanschlusses übermittelt. Es ist jedoch möglich, eine andere Rufnummer vorzutäuschen. Daher ist auch die Auswertung des Empfangsprotokolls keine verlässliche Bestätigung des Absenders.

# G 5.34 Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes

Um häufig wiederkehrende Empfänger-Faxnummern nicht ständig neu eingeben zu müssen, bieten einige Faxgeräte programmierbare Zielnummerntasten an. Häufig werden die Empfängernummern beim Versenden des Fax nicht einmal mehr kontrolliert. Kann ein Unbefugter die Programmierung der Zieltasten ändern und veranlasst er dann noch, dass die bei der neuen Zieladresse eingehenden Faxsendungen möglichst unverzüglich zum berechtigten Empfänger weitergeleitet werden, kann er bequem den Fax-Verkehr zu diesem Empfänger mitverfolgen, ggf. ohne jemals entdeckt zu werden.

# G 5.35 Überlastung durch Faxsendungen

Eine Überlastung durch eingehende Faxsendungen kann entstehen, wenn nicht genügend Faxanschlüsse oder nicht genügend Telekommunikations-Leitungen bzw. Kanäle vorhanden sind. Darüber hinaus kann ein Faxanschluss absichtlich blockiert werden, indem

- andauernd umfangreiche Faxe (ggf. mit sinnlosem Inhalt) zugesandt werden oder
- absichtlich solange Faxe zugesandt werden, bis der Papiervorrat eines Faxgerätes und der Pufferspeicher aufgebraucht sind.

Ein Faxserver kann ebenfalls überlastet werden, wenn solange Faxe zugesendet werden, bis der zur Verfügung stehende Platz auf der Festplatte ausgeschöpft ist. Zu beachten ist aber, dass eine gefaxte Seite DIN A 4 etwa 70 kB groß ist. Bei heute üblichen Festplattengrößen müssen dazu sehr viele Faxsendungen dieser Art eingehen. Zudem muss berücksichtigt werden, dass nur eine begrenzte Zahl an Leitungen bzw. Kanälen zur Verfügung steht und jede Faxsendung auch für die Abwicklung des Faxprotokolls Zeit benötigt. Eine Überlastung des Faxservers in diesem Sinne kann nur dann auftreten, wenn eine zu klein dimensionierte Festplatte gewählt wurde oder Faxsendungen auf dem Faxserver archiviert werden.

Im Gegensatz zu herkömmlichen Faxgeräten ist die Überlastung eines Faxservers durch ausgehende Faxsendungen durchaus möglich. So kann durch eine sehr große Anzahl von Serien-Faxsendungen ein Faxserver völlig ausgelastet werden und damit auch keine eingehenden Faxsendungen mehr empfangen.

# G 5.36 Absichtliche Überlastung des Anrufbeantworters

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.37 Ermitteln des Sicherungscodes

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.38 Missbrauch der Fernabfrage

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten

Eine Kommunikationskarte (z. B. eine ISDN-Karte oder ein internes Modem, aber auch ein externes Modem) kann eingehende Anrufe automatisch entgegennehmen. Abhängig von der eingesetzten Kommunikationssoftware und deren Konfiguration besteht dann die Möglichkeit, dass ein Anrufer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann.

Über eine Kommunikationskarte kann ein externer Rechner als Terminal an einen Server angeschlossen werden. Falls der Benutzer sich nach einer Terminalsitzung abmeldet, aber die Leitung ansonsten bestehen bleibt, ist vom externen Rechner ein Zugang wie über ein lokales Terminal möglich. Damit haben Dritte, die Zugang zu diesem Rechner haben, die Möglichkeit, Benutzer-Kennungen und Passwörter zu testen. Wesentlich gefährlicher ist der Fall, dass die Verbindung unterbrochen wird, aber der Benutzer nicht automatisch am entfernten System ausgeloggt wird. Dann kann der nächste Anrufer unter dieser Benutzer-Kennung weiterarbeiten, ohne sich anmelden zu müssen. Er hat somit vollen Zugriff auf das IT-System, ohne sich identifiziert und authentisiert zu haben.

# G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon und Kamera

Viele IT-Systeme werden mittlerweile mit Mikrofon und teilweise auch mit Kameras ausgeliefert. Mikrofon oder Kamera eines vernetzten Rechners können von denjenigen benutzt werden, die über Zugriffsrechte auf die entsprechende Gerätedateien verfügen. Unter Unix ist das zum Beispiel /dev/audio für die Soundkarte oder /dev/video für eine Kamera, unter Windows ist es ein Eintrag in der Registrierung. Wenn diese Rechte nicht sorgfältig vergeben sind und dadurch auch andere als die vorgesehenen Benutzer Zugriff haben, können Mikrofon oder Kamera missbraucht werden, um Räume abzuhören oder unbemerkt Besprechungen aufzuzeichnen.

**Beispiel:**

- Im März 2001 hat ein TV-Wirtschaftsmagazin gezeigt, wie über das Mikrofon eines Laptops ein Raum abgehört werden kann, wenn der Rechner mit einer ISDN-Telefonleitung verbunden ist. Dies wurde mit dem Laptop einer deutschen Politikerin demonstriert. Zunächst wurde sie in einer gefälschten Virenwarnung per E-Mail aufgefordert, ein als Anlage mitgeschicktes Schutzprogramm zu öffnen. Dieses Programm enthielt aber ein Trojanisches Pferd, das später über die ISDN-Leitung eine Verbindung nach außen herstellte und die Telefonnummer übermittelte.
  Danach konnte der Rechner von außen angerufen werden, ohne dass der Benutzer darüber optisch oder akustisch informiert wurde. Anschließend wurde über die offene Verbindung das eingebaute Mikrofon im Laptop aktiviert und die Geräusche aus dem Büro nach außen übertragen.

# G 5.41 Missbräuchliche Nutzung eines Unix-Systems mit Hilfe von UUCP

Das Programmpaket UUCP (Unix-to-Unix Copy) erlaubt den Austausch von ASCII- und Binärdateien zwischen IT-Systemen und die Ausführung von Kommandos auf entfernten IT-Systemen. UUCP war ursprünglich auf Unix-Systeme beschränkt, ist aber mittlerweile auch für viele andere Betriebssysteme verfügbar. Bei der Kommunikation über UUCP werden IT-Benutzern auf entfernten Rechnern Rechte auf dem lokalen Rechner eingeräumt. Wenn diese Rechte nicht sorgfältig und auf das Notwendige beschränkt vergeben werden, besteht die Gefahr der missbräuchlichen Nutzung des lokalen Systems. Denkbar ist auch eine Maskerade über UUCP, indem z. B. ein Host - bei Kenntnis des Passworts - vorgetäuscht wird.

# G 5.42 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:

- Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
- Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt,
- Telefonentstörer, der einige technische Details wissen will, z. B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat,
- Externer, der gerne Herrn X sprechen möchte, der aber nicht erreichbar ist. Die Information, dass Herr X drei Tage abwesend ist, sagt ihm auch gleichzeitig, dass der Account von Herrn X in dieser Zeit nicht benutzt wird, also unbeobachtet ist.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich "nur eine Aushilfe" oder eine "wichtige" Persönlichkeit.

Eine weitere Strategie beim systematischen Social Engineering ist der Aufbau einer längeren Beziehung zum Opfer. Durch viele unwichtige Telefonate im Vorfeld kann der Angreifer Wissen sammeln und Vertrauen aufbauen, das er später ausnutzen kann.

Solche Angriffe können auch mehrstufig sein, indem in weiteren Schritten auf Wissen und Techniken aufgebaut wird, die in vorhergehenden Stufen erworben wurden.

**Beispiel:**

- Ein Angreifer hat leichteres Spiel, wenn er das Opfer dazu bringt, ihn von sich aus zu kontaktieren. Beispielsweise kann der Angreifer die Telefonanlage der Ziel-Organisation so manipulieren, dass alle Anrufe an den Administrator an ihn weitergeleitet werden. Dies kann zum Beispiel nach einem erfolgreichen Social-Engineering-Angriff auf den Telefontechniker oder einer erfolgreichen Kompromittierung einer unsicher konfigurierten Telefonanlage von außen geschehen. Gelingt es dem Angreifer dann beispielsweise, einen Denial-of-Service-Angriff durchzuführen, wird das Opfer des Angriffes den Administrator verständigen. Durch die Manipulation der Telefonanlage erreicht das Opfer aber nur den Angreifer. Dass dieser kein "echter" Administrator ist, wird aber normalerweise niemand im normalen Tagesgeschäft hinterfragen.

Viele Anwender wissen, dass sie Passwörter an niemanden weitergeben dürfen. Social Engineers wissen dies und müssen daher über andere Wege an das gewünschte Ziel gelangen. Beispiele hierfür sind:

- Ein Angreifer kann das Opfer bitten, ihm unbekannte Befehle oder Applikationen auszuführen, z. B. weil dies bei einem IT-Problem helfen soll. Dies kann eine versteckte Anweisung für eine Änderung von Zugriffsrechten sein. So kann der Angreifer an sensible Informationen gelangen.
- Viele Benutzer verwenden zwar starke Passwörter, aber dafür werden diese für mehrere Konten genutzt. Wenn ein Angreifer einen nützlichen Netzdienst (wie ein E-Mail-Adressensystem) betreibt, an dem die Anwender

sich authentisieren müssen, kann er an die gewünschten Passwörter und Logins gelangen. Viele Benutzer werden die Anmeldedaten, die sie für diesen Dienst benutzen, auch bei anderen Diensten verwenden.

Beim Social Engineering tritt der Angreifer nicht immer sichtbar auf, es gibt auch diverse Varianten, bei denen er im Hintergrund bleibt. Oft erfährt das Opfer niemals, dass es ausgenutzt wurde. Ist dies erfolgreich, muss der Angreifer nicht mit einer Strafverfolgung rechnen und besitzt außerdem eine Quelle, um später an weitere Informationen zu gelangen.

Die Nutzung von E-Mail und Internet-Diensten bietet viele Möglichkeiten, unter Vorspiegelung falscher Tatsachen an Informationen zu gelangen. Ist erst einmal das Vertrauen des Opfers gewonnen, ist es für den Angreifer leicht, dem Opfer eine E-Mail z. B. mit einem Trojanischen Pferd als Anhang zu übersenden. Da das Opfer den Angreifer kennt und als vertrauenswürdig einstuft, wird es meist auch die E-Mail und den Anhang als vertrauenswürdig einstufen und den Anhang öffnen.

**Soziale Netzwerke**

Soziale Netzwerke im Internet bieten eine gute Ausgangsbasis für Social Engineering. Über diese Plattformen können eine Vielzahl von Hintergrundinformationen über Personen gefunden werden. Die Informationen, die sie über ihr Profil preisgeben, können gesammelt und als Grundlage für die weitere Informationsbeschaffung genutzt werden.

# G 5.43 Makro-Viren

Mit dem Austausch von Dateien (z. B. per Datenträger oder E-Mail) besteht die Gefahr, dass neben der eigentlichen Datei (Textdatei, Tabelle, etc.) weitere, mit dem Dokument verbundene Makros bzw. eingebettete Editorkommandos übersandt werden. Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel, etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.

Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, dass einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z. B. einen Virus).

In der Praxis hat diese Gefährdung insbesondere bei den Dateien der Programme Word für Windows und Excel der Firma Microsoft weltweit beträchtlich zugenommen. Für den Benutzer ist dabei nicht transparent, dass Dateien für Word-Vorlagen (*.DOT), in denen Makros enthalten sein können, durch Umbenennen in *.DOC-Dateien scheinbar zu Datendateien werden, die keine Makros enthalten. Von Microsoft Word werden solche Dateien jedoch ohne Hinweis auf diese Tatsache in nahezu gleicher Weise verarbeitet (Ausnahme: Winword ab Version 7.0a).

Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen. Hervorzuheben ist, dass Makro-Viren auf verschiedenen Betriebssystem-Plattformen auftreten können, nämlich auf allen, auf denen Winword läuft (Windows Versionen 3.1 und 3.11, Windows 95, Windows NT, Apple-Computer).

**Beispiel:**

- Der Winword-Makro-Virus "Winword.Nuclear" wurde im Internet über die Datei WW6ALERT.ZIP verbreitet. Der Makro-Virus bewirkt einerseits, dass an Ausdrucken der Text "STOP ALL FRENCH NUCLEAR TESTING IN PACIFIC!" angehängt wird, andererseits aber auch den Versuch, Systemdateien zu löschen.

# G 5.44 Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen

TK-Anlagen verfügen über Remote-Zugänge für Managementfunktionen. Über diese Zugänge können alle Administrations- und Wartungstätigkeiten sowie sonstige Managementfunktionalitäten wie z. B. Alarmsignalisierung und -bearbeitung abgewickelt werden.

Solche Remote-Zugänge sind besonders in TK-Anlagen-Verbünden (Corporate Networks) nützlich und teilweise unverzichtbar. Bei der Art des Remote Zuganges lässt sich zwischen

- IP-basierter Zugang über Datennetze,
- "Modem"-Zugang über dedizierte Managementports und
- direkte Einwahl über DISA (Direct Inward System Access)

unterscheiden. Desweiteren sind in neueren Protokollierungsverfahren wie QSig und einigen anderen proprietären Protokollen Managementfunktionen bereits im Signalisierungsspektrum enthalten. Hieraus ergeben sich potentielle Missbrauchsmöglichkeiten.

Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, dass Hacker Zugang zu den Managementprogrammen des TK-Systems erlangen. Sie können somit nach Überwindung des Anlagenpasswortes ggf. **alle** Administrationstätigkeiten ausüben. Der entstehende Schaden kann sich vom vollständigen Anlagenausfall, über schwerste Betriebsstörungen, den Verlust der Vertraulichkeit aller auf der Anlage vorhandenen Daten bis hin zum großen direkten finanziellen Schaden z. B. durch Gebührenbetrug erstrecken.

# G 5.45 Ausprobieren von Passwörtern unter WfW und Windows 95

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 5.46 Maskerade unter WfW

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 5.47 Löschen des Post-Office unter WfW

Diese Gefährdung ist 2009 mit der 11. Ergänzungslieferung entfallen.

# G 5.48 IP-Spoofing

IP-Spoofing ist eine Angriffsmethode, bei der falsche IP-Adressen verwendet werden, um dem angegriffenen IT-System eine falsche Identität vorzuspielen.

Bei vielen Protokollen der TCP/IP-Familie erfolgt die Authentisierung der kommunizierenden IT-Systeme nur über die IP-Adresse, die leicht gefälscht werden kann. Wird dazu noch ausgenutzt, dass die, von den Rechnern beim Aufbau einer TCP/IP-Verbindung erzeugten Sequenznummern leicht zu erraten sind, ist es möglich, Pakete mit jeder beliebigen Absenderadresse zu verschicken. Damit können entsprechend konfigurierte Dienste wie *rlogin* benutzt werden. Allerdings muss ein Angreifer dabei u. U. in Kauf nehmen, dass er kein Antwortpaket von dem missbräuchlich benutzten Rechner erhält.

Weitere Dienste, die durch IP-Spoofing bedroht werden, sind *rsh, rexec,* X-Windows*,* RPC-basierende Dienste wie NFS, DNS und der TCP-Wrapper, der ansonsten ein sehr sinnvoller Dienst zur Einrichtung einer Zugangskontrolle für TCP/IP-vernetzte Systeme ist. Leider sind auch die in Schicht 2 des OSI-Modells eingesetzten Adressen wie Ethernet- oder Hardware-Adressen leicht zu fälschen und bieten somit für eine Authentisierung keine zuverlässige Grundlage.

In LANs, in denen das Address Resolution Protocol (ARP) eingesetzt wird, sind sehr viel wirkungsvollere Spoofing-Angriffe möglich. ARP dient dazu, zu einer 32-Bit großen IP-Adresse die zugehörige 48-Bit große Hardware- oder Ethernet-Adresse zu finden. Falls in einer internen Tabelle des Rechners kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der unbekannten IP-Adresse ausgesandt. Der Rechner mit dieser IP-Adresse sendet dann ein ARP-Antwort-Paket mit seiner Hardware-Adresse zurück. Da die ARP-Antwort-Pakete nicht manipulationssicher sind, reicht es dann meist schon, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu kompromittieren.

# G 5.49 Missbrauch des Source-Routing

Der Missbrauch des Routing-Mechanismus und -Protokolls ist eine sehr einfache protokoll-basierte Angriffsmöglichkeit. In einem IP-Paket lässt sich der Weg, auf dem das Paket sein Ziel erreichen soll oder den die Antwortpakete nehmen sollen, vorschreiben. Die Wegbeschreibung kann aber während der Übertragung manipuliert werden, so dass nicht die durch die Routing Einträge vorgesehenen sicheren Wege benutzt werden (z. B. über die Firewall), sondern andere unkontrollierte Wege.

# G 5.50 Missbrauch des ICMP-Protokolls

Das Internet Control Message Protocol (ICMP) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen zu transportieren. Durch Missbrauch von ICMP-Nachrichten kann ein Angreifer sowohl den Netzbetrieb stören als auch Informationen über das interne Netz herausfinden, die ihm bei der Planung eines Angriffs nützen:

- Durch ICMP-*Redirect* Nachrichten können die Routing-Tabellen von Rechnern manipuliert werden.
- ICMP-*Unreachable* Nachrichten können dazu benutzt werden, bestehende Verbindungen zu stören oder ganz zu unterbrechen.
- Die verschiedenen ICMP-*Request* Nachrichtentypen (*Echo Request, Information Request, Timestamp Request, Address Mask Request*) können auf einfache Weise dazu benutzt werden, das interne Netz einer Organisation zu "kartographieren" (*ICMP Sweeps*).
- Auch gefälschte ICMP-*Reply* Nachrichten können dazu benutzt werden, um Informationen über das interne Netz herauszufinden, indem sie die Zielrechner dazu bewegen, auf diese mit einer Fehlermeldung zu antworten.
- Verschiedene Betriebssysteme unterscheiden sich in der Art und Weise, wie sie auf bestimmte ICMP-Nachrichten reagieren. Neben der Information darüber, dass eine bestimmte Adresse aktiv ist können ICMP-Antworten daher auch verraten, unter welchem Betriebssystem der betreffende Rechner läuft (*Fingerprinting*).
- Fehlerhafte Implementierungen von ICMP in einigen Betriebssystemen haben in der Vergangenheit zu Sicherheitsproblemen geführt:
  - Rechner mit Windows 95 konnten durch bestimmte ICMP-Echo Pakete ("Ping of Death") zum Absturz gebracht werden.
  - In ICMP-Antwortpaketen verschiedener Betriebssysteme konnten Ausschnitte aus dem Arbeitsspeicher des betreffenden Rechners enthalten sein. Im Extremfall könnten auf diese Weise Passwörter oder kryptographische Schlüssel an einen externen Rechner übermittelt werden.
- Jede Art von ICMP-Nachrichten kann auch dafür benutzt werden, einen verdeckten Informationskanal zu schaffen, auf dem Daten aus dem internen Netz nach draußen zu transportiert werden können.

# G 5.51 Missbrauch der Routing-Protokolle

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routing-Tabellen zu ermöglichen. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren.

Der Einsatz von dynamischem Routing ermöglicht es, Routing-Informationen an einen Rechner zu schicken, die dieser in der Regel ungeprüft zum Aufbau seiner Routing-Tabellen benutzt. Dies kann ein Angreifer ausnutzen, um gezielt den Übertragungsweg zu verändern.

# G 5.52 Missbrauch von Administratorrechten bei Windows-Betriebssystemen

Eine missbräuchliche Administration liegt vor, wenn vorsätzlich recht- oder unrechtmäßig erworbene Administratorberechtigungen ausgenutzt werden, um dem System oder dessen Benutzern zu schaden.

**Beispiele:**

- Durch missbräuchliche Nutzung des Rechtes zur Besitzübernahme beliebiger Dateien kann sich ein Administrator auf einem Windows NT-basierten System Zugriff auf beliebige Dateien verschaffen, obwohl deren Eigentümer ihm diesen Zugriff explizit durch entsprechende Zugriffskontrollen verwehrt haben. Ein Zugriff kann allerdings vom ursprünglichen Eigentümer der Dateien erkannt werden, da der Administrator sich zum Besitzer der betreffenden Dateien machen muss. Auf Windows NT-basierten Systemen ist keine Funktion verfügbar, um diese Änderung wieder rückgängig zu machen. Allerdings bietet Windows ab Windows Server 2003 bzw. Windows Vista die Möglichkeit, die Besitzübernahme zu verschleiern und den Besitz an einen beliebigen Benutzer zurückzugeben. Ein Administrator kann auch ohne Besitzübernahme unbemerkt auf Benutzerdateien zugreifen, in dem er sich z.B. in die Gruppe Sicherungs-Operatoren einträgt und ein Backup der Dateien durchführt, die er lesen will.
- Es gibt verschiedene Möglichkeiten, missbräuchlich Administratorrechte auszunutzen. Dazu gehören unzulässige Zugriffe auf Dateien sowie Veränderungen der Protokollierungseinstellungen und der Vorgaben für Benutzerkonten. Andere Möglichkeiten des Missbrauchs bestehen in der Fälschung von Protokollinformationen durch Verstellen der Systemzeit oder in der detaillierten Verfolgung der Tätigkeiten einzelner Benutzer.
- In Abhängigkeit von der zugrunde liegenden Hardware kann bei Zugangsmöglichkeit zur Konsole bzw. zum Systemgehäuse das System gebootet werden. Dies ermöglicht gegebenenfalls die Manipulation der Konfiguration, wenn hierbei von einem Fremdmedium gebootet oder ein anderes Betriebssystem ausgewählt werden kann.

# G 5.53 Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit

Eine häufig festzustellende Form der absichtlichen Fehlbedienung von Schutzschränken mit mechanischen Codeschlössern besteht darin, nach Schließen eines Schutzschrankes den Code nicht zu verwerfen, um den Code beim Öffnen nicht wieder eingeben zu müssen. Dieses Fehlverhalten reduziert den Schutzwert des Schrankes gegen unbefugten Zugriff, da hierdurch einem Dritten das Öffnen des Schutzschrankes ohne Kenntnis des Codes ermöglicht wird.

Ebenso häufig anzutreffen ist der Umstand, dass Schutzschränke bei kurzfristigem Verlassen des Raumes nicht verschlossen werden, um sich das Öffnen des Schrankes nach Rückkehr zu ersparen. Dies reduziert ebenfalls den Schutzwert gegen unbefugten Zugriff.

# G 5.54 Vorsätzliches Herbeiführen eines Abnormal End

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen.

# G 5.55 Login Bypass

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 5.56 Temporär frei zugängliche Accounts

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 5.57 Netzanalysetools

Werden die im Netzsegment übertragenen Informationen nicht verschlüsselt, so können diese Informationen mithilfe von Netzanalysetools, sogenannten "Sniffern", im Klartext ausgelesen werden.

Moderne Managementwerkzeuge beinhalten heutzutage Funktionen, mit deren Hilfe Datenpakete gelesen werden können, um Probleme in Netzen zu analysieren. Angreifer können diese Zusatzfunktionen missbrauchen, um vertrauliche Daten auszulesen. Neben IP-Netzen sind auch Fibre-Channel-Verbindungen durch Netzanalysetools gefährdet. Unterschiedliche Hersteller bieten mittlerweile freien Zugang zu physischen FC-Analysern an, mit deren Hilfe Datenverkehr mitgelesen werden kann. So können die gespeicherten Daten aus Speichernetzen abgegriffen werden, ohne dass auf die physischen Datenträger zugegriffen werden muss. An einem nicht gesicherten zentralen Knotenpunkt eingesetzt, entsteht hieraus ein enormes Risiko, die Vertraulichkeit der Daten zu gefährden.

Eine zusätzliche Gefährdung durch den Einsatz von Netzanalysetools stellt der Zugriff von Serviceprovidern auf angemietete Leitungen dar.

# G 5.58 Hacking Novell Netware

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 5.59 Missbrauch von Administratorrechten unter Novell Netware Servern

Diese Gefährdung ist 2013 mit der 13. Ergänzungslieferung entfallen.

# G 5.60 Umgehen der Systemrichtlinien

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen.

# G 5.61 Missbrauch von Remote-Zugängen für Managementfunktionen von Routern

Router verfügen über Remote-Zugänge für Managementfunktionen. Über diese Zugänge können alle Administrations- und Wartungstätigkeiten sowie Signalisierungsfunktionalitäten abgewickelt werden. Solche Remote-Zugänge sind besonders in größeren Netzen mit mehreren Routern bzw. bei der LAN-Kopplung über Weitverkehrsnetze nützlich und teilweise unverzichtbar.

Bei der Art des Remote-Zugangs lässt sich unterscheiden zwischen:

- "Modem"-Zugang über dedizierte Schnittstelle (z. B. V.24) und
- direkter Zugang über reservierte Bandbreiten.

Wird für das Netzmanagement das Protokollverfahren SNMP (Simple Network Management Protocol) eingesetzt, ergeben sich aufgrund fehlender bzw. noch nicht umgesetzter Sicherheitsfunktionalitäten weitere Gefährdungen, die über den direkten Missbrauch der ungeschützten Remote-Schnittstellen hinausgehen:

- Ein nicht autorisierter Benutzer fängt Datenpakete einer SNMP-Management-Station ab und verändert die darin enthaltenen Parameterwerte für seine Zwecke. Nach dieser Manipulation werden die manipulierten Datenpakete zur eigentlichen Zielstation gesendet. Das Empfängergerät hat keine Möglichkeit, diese Datenmanipulation zu erkennen und reagiert deshalb auf die im Paket enthaltenen Informationen so, als ob diese von der Management-Station direkt abgesandt worden wären.
- Erhält der Besitzer einer Netzmanagement-Station Zugang zum mittels SNMP verwalteten Netz, ist das Vorspiegeln einer Community (Verwaltungsbereich innerhalb von SNMP) möglich. Durch diese Maskerade täuscht ein nicht autorisierter Benutzer eine autorisierte Identität vor und kann alle Informationen der Agents (im Netz zu verwaltende Objekte, bspw. Router) auslesen sowie sämtliche Managementoperationen durchführen. Der Agent hat keine Möglichkeit zwischen der richtigen und der falschen Identität zu unterscheiden.

# G 5.62 Missbrauch von Ressourcen über abgesetzte IT-Systeme

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen.

# G 5.63 Manipulationen über den ISDN-D-Kanal

Die Summe aller physikalischen Verbindungen der Kommunikationsteilnehmer zu einer ihnen zugeordneten digitalen Vermittlungsstelle bezeichnet man als Anschlussnetz. Innerhalb des Anschlussnetzes existieren zahlreiche Verteiler und Übergabepunkte, die teilweise frei zugänglich und nicht aufwendig gesichert sind (z. B. Kabelverzweiger). Die Kommunikation auf dem Anschlussnetz kann im einfachsten Fall durch das mechanische Beschädigen einer Anschlussleitung unterbrochen werden.

Weiterhin ist es mit Hilfe eines ISDN-Protokollanalysators möglich, Kommunikationsinhalte aufzuzeichnen und auszuwerten. Mittels Einschleifen eines Protokollanalysators ist ebenfalls das Manipulieren von Steuerungsinformationen im D-Kanal des ISDN möglich. Die Kommunikationskomponenten des angegriffenen Kommunikationsteilnehmers (also ISDN-Karten, ISDN-Router, TK-Anlagen etc.) können so zu Reaktionen veranlasst werden, die ihren ordnungsgemäßen Betrieb beeinträchtigen oder zur Kompromittierung gespeicherter Daten führen.

# G 5.64 Manipulation an Daten oder Software bei Datenbanksystemen

Durch ein gezieltes Manipulieren von Daten werden diese vorsätzlich verfälscht oder unbrauchbar gemacht. Die entsprechenden Folgen sind in G 4.28 *Verlust von Daten einer Datenbank* und G 4.30 *Verlust der Datenbankintegrität/-konsistenz* beschrieben.

Werden die Dateien einer Datenbank oder der Datenbank-Standardsoftware gezielt gelöscht oder verändert, so führt dies zur vorsätzlichen Zerstörung des gesamten Datenbanksystems (siehe G 4.26 *Ausfall einer Datenbank*).

Es ist prinzipiell nicht verhinderbar, dass Benutzer mit den entsprechenden Zugangs- und Zugriffsberechtigungen gezielt Datenmanipulationen durchführen oder eine Datenbank zerstören können. Ist es außerdem möglich, die Zugangs- und Zugriffsberechtigungen zu umgehen (z. B. durch eine fehlerhafte Administration des DBMS), so können sich auch unberechtigte Benutzer Zugang zur Datenbank verschaffen und dort Manipulationen vornehmen.

# G 5.65 Verhinderung der Dienste eines Datenbanksystems

Um die IT-Benutzer daran zu hindern, Funktionen und Dienste eines Datenbanksystems zu verwenden, die ihnen normalerweise zur Verfügung stehen, können gezielte Angriffsmethoden eingesetzt werden. Neben den in G 5.28 *Verhinderung von Diensten* (Denial of Service) aufgeführten Beispielen kann diese Gefährdungslage im Bereich Datenbanken unter folgenden Bedingungen entstehen:

**Zu viele Abfragen**

Das Problem einer hohen Anzahl paralleler Abfragen tritt häufig bei Internet-Datenbanken auf, die über Schnittstellen (Interfaces), z. B. Common Gateway Interface (CGI) oder Active Server Pages (ASP), Ausgaben für Web-Browser produzieren.

**Zu komplexe Abfragen**

Wenn in großen Datenbanken nach Begriffen gesucht wird, die in keiner Tabelle enthalten sind, dauern Abfragen am längsten, da zumindest alle Einträge der Index-Tabelle durchsucht werden müssen. Werden in einer Abfrage mehrere solcher Begriffe mit ODER verknüpft, verlängert sich die Antwortzeit der Abfrage entsprechend.

**Fehlerhafte Statements**

Der Parser stellt im Datenbankmanagementsystem (DBMS) die Implementierung der vom DBMS zur Verfügung gestellten Abfragesprache (z. B. SQL) dar. Der Parser überprüft jede an die Datenbank gerichtete Abfrage auf Korrektheit gegenüber der gegebenen Abfragesprache und führt die Abfrage nach erfolgreicher Prüfung aus. Sollte die Abfragesprache nicht eindeutig und abgeschlossen definiert oder die Implementierung der Abfragesprache im Parser fehlerhaft sein, können manipulierte Statements zur Verhinderung von Diensten der Datenbank ausgenutzt werden, wenn die Statements durch den Parser akzeptiert werden. Der Parser überprüft diese Statements und führt sie nach erfolgreicher Prüfung aus, mit nicht vorhersagbaren Ergebnissen, bis hin zum Absturz.

**Zu lange Ausgabe-Ergebnisse**

Abfragen, die uneingeschränkt oder auf Kriterien eingeschränkt sind, die sehr oft zu finden sind, erzeugen unter Umständen sehr lange Ausgabe-Ergebnisse, die das DBMS überlasten können.

**Buffer Overflow**

Der Ausfall eines Datenbanksystems kann möglicherweise auch durch einen Speicherüberlauf (Buffer Overflow) herbeigeführt werden. Hierbei kann ein Angreifer beispielsweise versuchen, eine komplexe Abfrage zu konstruieren, die das DBMS stark belastet. Zusätzlich wird die Komplexität der Abfrage erhöht, indem überlange Parameterwerte hinzugefügt werden, um den Parser zu überlasten. Die Folgen sind nicht vorhersehbar und reichen bis zum Absturz des DBMS oder unkontrollierten Veränderungen an den Daten.

# G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz

Grundsätzlich kann der unberechtigte Anschluss eines IT-Systems in ein bestehendes Netz (durch ein Aufschalten auf die zugehörige Verkabelung oder durch die Nutzung von Schnittstellen in Verteiler- oder Büroräumen) nicht verhindert werden. Es gibt keinen Verkabelungstyp, der ein solches Ankoppeln verhindern würde, lediglich der erforderliche Aufwand zum Auftrennen der Verkabelung und zum Lesen bzw. Einspielen von Daten unterscheidet die verschiedenen Typen.

Die unberechtigte Integration eines Rechners in ein Netz ist nur sehr schwer zu entdecken und bleibt meistens unbemerkt. Ein solcher Zugriff betrifft den gesamten Netzverkehr in dem zugehörigen Segment und kann z. B.

- die Manipulation an Daten oder Software,
- das Abhören von Leitungen,
- die Manipulation an Leitungen,
- das Wiedereinspielen von Nachrichten,
- die Maskerade als anderer Kommunikationsteilnehmer,
- eine Analyse des Nachrichtenflusses,
- die Verhinderung von Diensten,
- die unberechtigte Ausführung von Netzmanagement-Funktionen oder
- den unberechtigten Zugang zu den aktiven Netzkomponenten

begünstigen.

# G 5.67 Unberechtigte Ausführung von Netzmanagement-Funktionen

Durch die unberechtigte Ausführung von Netzmanagement-Funktionen können aktive Netzkomponenten teilweise oder vollständig kontrolliert werden. Die Kontrollmöglichkeiten werden u. a. durch das verwendete Netzmanagement-Protokoll, wie z. B. SNMP bestimmt. Daraus kann ein Verlust der Netzintegrität, der Verfügbarkeit einzelner oder aller Netzbestandteile sowie der Vertraulichkeit bzw. Integrität von Daten resultieren.

Unter Verwendung eines Netzmanagement-Protokolls, wie z. B. SNMP, können dedizierte Ports aktiver Netzkomponenten aktiviert oder insbesondere auch deaktiviert werden. Weiterhin können z. B. die VLAN-Konfiguration, Routing-Tabellen, die Router-Konfiguration sowie die Konfiguration von Filtern manipuliert werden (siehe G 3.28 *Ungeeignete Konfiguration der aktiven Netzkomponenten*). Daneben kann die Möglichkeit einer Verteilung von Firmware-Updates über das Netz genutzt werden, um unberechtigt Software auf aktiven Netzkomponenten zu installieren, mit deren Unterstützung wiederum vielfältige Angriffe auf Komponenten innerhalb des Netzes durchgeführt oder unterstützt werden können.

# G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten

Aktive Netzkomponenten haben üblicherweise eine serielle Schnittstelle (RS-232), an die von außen ein Terminal oder ein tragbarer PC angeschlossen werden kann. Dadurch ist es möglich, aktive Netzkomponenten auch lokal zu administrieren.

Bei unzureichend gesicherten Schnittstellen ist es denkbar, dass Angreifer einen unberechtigten Zugang zur Netzkomponente erlangen. Sie können somit nach Überwindung der lokalen Sicherheitsmechanismen (z. B. des Passwortes) ggf. alle Administrationstätigkeiten ausüben.

Dabei können durch das Auslesen der Konfiguration aktiver Netzkomponenten ggf. schutzbedürftige Informationen über die Topologie, die Sicherheitsmechanismen und die Nutzung eines Netzes in Erfahrung gebracht werden. Ein Auslesen der Konfigurationsdaten ist z. B. durch den Anschluss eines Terminals oder tragbaren PCs an die serielle Schnittstelle der aktiven Netzkomponente, durch den Zugriff auf die aktive Netzkomponente über das lokale Netz oder durch das Mitlesen der Daten auf einem Bildschirm oder Display möglich, falls die aktive Netzkomponente gerade administriert bzw. konfiguriert wird.

# G 5.69 Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Der häusliche Arbeitsplatz ist in der Regel nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder einer Behörde. Dort ist, bedingt durch aufwendigere Vorkehrungen wie beispielsweise der Verwendung von Sicherheitstüren, einem Einbruchschutz oder dem Pförtnerdienst, die Gefahr, dass jemand unbefugt in das Gebäude eindringt, weitaus geringer als bei einem Privathaus.

Ziel von Einbrüchen und Diebstählen in Privathäuser ist meist die Bereicherung. Daher werden vorrangig Gegenstände wie Schmuck oder IT-Geräte gestohlen, die schnell und einfach verkauft werden können. Dabei kann auch dienstliche IT-Ausstattung gestohlen werden. Die auf den entwendeten dienstlichen IT-Systemen vorhandenen Informationen besitzen aber im Allgemeinen einen höheren Wert als die IT-Systeme selber. Einbrecher könnten versuchen, durch Erpressung oder Weitergabe der Daten an Konkurrenzunternehmen einen höheren Gewinn als durch den Verkauf der Hardware zu erzielen.

# G 5.70 Manipulation durch Familienangehörige und Besucher

Am häuslichen Arbeitsplatz ist mit Angehörigen und Besuchern der Familie zu rechnen, so dass die Gefahr besteht, dass bei unzureichender Sicherung die dienstliche IT durch diese manipuliert werden kann. So sollte auch betrachtet werden, dass durch Familienangehörige private Software (z. B. Computerspiele) aufgespielt werden könnte, dass durch Kinder die IT zerstört werden kann oder dass dienstliche Datenträger zweckentfremdet weitergegeben werden können. Diese teils fahrlässigen oder auch absichtlichen Manipulationen können sowohl die Vertraulichkeit und Integrität der dienstlichen Daten betreffen als auch die Verfügbarkeit von Daten und IT beeinträchtigen.

# G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

Vertraulichkeit ist die Anforderung, dass eine Information nur den zur Kenntnisnahme berechtigten Personen zugänglich gemacht werden darf. Neben der Integrität und der Verfügbarkeit gehört die Vertraulichkeit zu den Grundwerten der Informationssicherheit.

Für Informationen, die einen Schutzbedarf bezüglich ihrer Vertraulichkeit besitzen (wie Passwörter, personenbezogene Daten, firmen- oder amtsvertrauliche Informationen, Entwicklungsdaten), besteht die inhärente Gefahr, dass die Vertraulichkeit durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen beeinträchtigt wird.

Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (USB-Sticks, CDs oder DVDs),
- in gedruckter Form auf Papier (Ausdrucke, Akten),
- unter Ausnutzung von Schwachstellen oder bewusst eingebauten Hintertüren in Anwendungssoftware oder Betriebssystemen,
- durch den Missbrauch von Fernwartungsmechanismen und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie die vertraulichen Informationen gewonnen werden, kann sehr unterschiedlich sein, zum Beispiel:

- Auslesen von Dateien,
- Kopieren von Dateien,
- Wiedereinspielen von Datensicherungsbeständen,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen,
- Infektion mit Schadprogrammen,
- Mitlesen am Bildschirm,
- Ausspähen von Daten durch Wartungs- oder Fremdpersonal,
- Weitergabe von Daten durch einen IT-Dienstleister.

Werden Informationen unberechtigt gelesen oder preisgegeben, kann dies schwerwiegende Folgen für eine Institution haben. Unter anderem kann der Verlust der Vertraulichkeit zu folgenden negativen Auswirkungen für eine Institution führen:

- Verstoß gegen Gesetze, zum Beispiel Datenschutz, Bankgeheimnis
- Wettbewerbsnachteile durch Preisgabe von Geschäftsgeheimnissen wie Kundenlisten, Preisstrategien oder Konstruktionspläne
- Negative Innenwirkung, zum Beispiel Demoralisierung der Mitarbeiter
- Negative Außenwirkung, zum Beispiel Beeinträchtigung der Beziehungen zu Geschäftspartnern, verlorenes Vertrauen von Kunden
- Finanzielle Auswirkungen, zum Beispiel Schadensersatzansprüche, Bußgelder, Prozesskosten
- Beeinträchtigung des informationellen Selbstbestimmungsrechtes

Zu beachten ist außerdem, dass ein Verlust der Vertraulichkeit nicht immer sofort bemerkt wird. Oft stellt sich erst später heraus, dass Unbefugte sich Zugang zu vertraulichen Informationen verschafft haben und dadurch Schäden entstanden sind.

# G 5.72 Missbräuchliche Groupware-Nutzung

Der Missbrauch von Groupware-Systemen kann an verschiedenen Punkten aufsetzen, bei den Benutzern, im internen Netz, bei einem der übertragenden Groupware- oder Mailserver oder beim Empfänger von Nachrichten.

Wenn der Zugang zu den Groupware-Anwendungen bei den Benutzern oder zum Groupware-System einer Institution nicht gut genug geschützt ist, kann ein Unbefugter sich unberechtigt Zugang für manipulative Zwecke verschaffen. Dabei können neben den Übertragungskosten auch Schäden dadurch entstehen, dass ein Unbefugter sich als Berechtigter ausgibt.

Ebenso muss verhindert werden, dass Informationen in geschlossenen Groupware-Systemen von Unbefugten gelesen werden können. Vertrauliche Informationen können so bekannt werden, ihren Wert verlieren oder zum Schaden des Empfängers genutzt werden.

**Beispiele:**

- Ein Abteilungsleiter verließ für kurze Zeit sein Büro mit ungesichertem IT-System, auf dem das Groupware-Programm bereits gestartet war und für das er sich bereits authentisiert hatte. Ein zufällig vorbeigekommener Kollege hielt es für einen gelungenen Scherz, unter dessen E-Mail-Kennung anderen Kollegen "Kündigungen" oder Arbeitsaufträge zu schicken.
- Ein Mitarbeiter verbreitete unter seiner dienstlichen E-Mail-Adresse private Ansichten, die dem Ansehen seines Arbeitgebers schaden können.
- Um häufig wiederkehrende E-Mail-Adressen nicht ständig neu eingeben zu müssen, kann über die Vergabe von Alias-Namen eine "sprechende" Schreibweise für E-Mailadressen gewählt werden oder es kann über die Erstellung von Verteilerlisten ein größerer Empfängerkreis komfortabel angewählt werden. Werden solche Alias-Namen oder Verteilerlisten unbefugt geändert, kann auf diese Weise die Weiterleitung einer E-Mail an einen gewünschten Empfänger unterbunden oder die Weiterleitung zu einem unerwünschten Empfänger erfolgen. Besonders gefährdet sind hier Alias-Dateien oder Adressbücher, die zentral geführt werden.

# G 5.73 Vortäuschen eines falschen Absenders

Es ist relativ einfach, beim Versand von E-Mail einen falschen Absender anzugeben, da bei der Weiterleitung von SMTP-basierender E-Mail meist nicht überprüft wird, wo die Nachricht herkommt, nur wo sie hingehen soll. Darüber hinaus erlauben es viele E-Mail-Clients, beliebige Absenderangaben einzutragen. Dadurch können Schäden entstehen, wenn der Empfänger die darin enthaltenen Informationen als authentisch und verbindlich ansieht.

**Beispiele:**

- Die meisten der zahllosen Spam-E-Mails, die täglich die Postfächer der Benutzer verstopfen, tragen einen gefälschten Absender.
- Einige der verschiedenen E-Mail-Würmer, die seit mehreren Jahren im Internet ihr Unwesen treiben, benutzen als Absenderadresse eine Adresse aus dem E-Mail-Adressbuch des Benutzers, dessen E-Mail-Programm sie gerade befallen haben. So erhalten die nächsten Opfer die E-Mail, die den Wurm enthält, mit einer bekannten Absenderadresse und sind so eher gefährdet, die E-Mail oder gar das infizierte Attachment zu öffnen.
- Mit vielen verbreiteten E-Mail-Programmen ist es ohne Probleme möglich, eine E-Mail mit gefälschten Absenderangaben ohne Passwortüberprüfung auf den E-Mail-Server weiterzuleiten. Die so versandte E-Mail wird zwar eventuell bei nicht erfolgter Benutzer-Authentisierung im Feld "X-Sender" mit "Unverified" gekennzeichnet. Dies wird aber erfahrungsgemäß von kaum einem Empfänger bemerkt, ohnehin werden diesese Felder von den meisten E-Mail-Programmen in der Standardkonfiguration nicht angezeigt.

# G 5.74 Manipulation von Alias-Dateien oder Verteilerlisten

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.75 Überlastung durch eingehende E-Mails

Eine E-Mail-Adresse kann absichtlich blockiert werden, indem andauernd umfangreiche E-Mails (möglicherweise mit sinnlosem Inhalt) zugesandt werden. Dies kann beispielsweise passieren, weil ein Benutzer die Netiquette nicht beachtet hat und sich dadurch unbeliebt gemacht hat oder weil die Institution angegriffen werden soll. Als Netiquette (die Netz-Etiquette) werden die Höflichkeitsregeln bezeichnet, die sich mit der Zeit bei der Nutzung des Internet, insbesondere in den Newsgruppen, eingebürgert haben und deren Einhaltung gewährleisten soll, dass jeder das Internet effizient und zu aller Zufriedenheit benutzen kann.

Durch vorsätzlich erzeugtes hohes Verkehrsaufkommen kann das lokale Mailsystem überlastet werden, so dass es funktionsuntüchtig wird. Dies kann sogar solche Ausmaße annehmen, dass der Provider den Benutzer bzw. dessen ganze Institution vom Netz nimmt.

Ein Mailsystem kann auch überlastet werden, wenn die Mitarbeiter an E-Mail-Kettenbrief-Aktionen teilnehmen. So hat schon Mitte der achtziger Jahre eine Kettenmail-Aktion zu Weihnachten weltweit viele IT-Systeme lahm gelegt. Hierbei erhielten Benutzer eine E-Mail mit Weihnachtsgrüßen und einer ansprechenden Graphik und wurden aufgefordert, diese E-Mail zu kopieren und zehn andere Benutzer weiterleiten.

**Mailbomben**

Als Mailbomben werden E-Mails bezeichnet, die absichtlich eingebaute Schadfunktionen enthalten. Diese sind üblicherweise in den Anlagen der E-Mail enthalten. Eine solche Anlage erzeugt z. B. beim Aktivieren zum Lesen oder nach dem Auspacken Unmengen von Unterverzeichnissen oder beansprucht sehr viel Festplattenplatz. Vielfach wird auch die gezielte Überlastung von E-Mail-Adressen durch eingehende E-Mails mit meist sinnlosem Inhalt als Mailbombing bezeichnet.

# G 5.76 Mailbomben

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.77 Mitlesen von E-Mails

E-Mail wird im Normalfall im Klartext übertragen. Auf allen IT-Systemen, über die die Daten übertragen werden, können diese mitgelesen oder sogar unbemerkt verändert werden, wenn sie nicht kryptographisch gesichert sind. Bei der Übertragung von E-Mails über das Internet können sehr viele IT-Systeme beteiligt sein, ohne dass der genaue Übertragungsweg vorher bekannt ist. Der Übertragungsweg hängt von der Auslastung und Verfügbarkeit der Gateways und Teilen des Netzes ab. Eine E-Mail von einem Stadtteil in den anderen kann sogar über das Ausland weitergeleitet werden.

Der Zugriff auf eingehende E-Mails kann auch über die beim Mailserver des Empfängers geführte Mailbox erfolgen. Sie enthält alle empfangenen E-Mails, je nach Konfiguration nicht nur die ungelesenen, sondern ein Archiv aller in den letzten Monaten eingegangenen Nachrichten. Hierauf hat mindestens der Systemadministrator des Mailservers Zugriff. In manchen Fällen werden auch Kopien ausgehender E-Mails auf dem Mailserver gespeichert. Häufig jedoch legt das Benutzer-Mailprogramm diese auf dem Rechner des Absenders ab.

**Beispiele:**

- Mehrere Microsoft-interne E-Mails wurden im Antitrust-Verfahren von der Gegenseite benutzt, um deren Position zu untermauern. Diese E-Mails enthielten teilweise diffamierende Aussagen über Microsofts Konkurrenten.
- Ein Anbieter stellt Dienstleistungen über das Internet zur Verfügung. Für die Nutzung ist eine Anmeldung am Server des Dienstleisters erforderlich. Die dafür notwendigen Authentisierungsinformationen werden per E-Mail an die Kunden versandt. Durch Mitlesen dieser E-Mails ist ein Angreifer in der Lage, sich unberechtigt am Server des Dienstleisters anzumelden und auf Kosten der registrierten Kunden Dienste in Anspruch zu nehmen.

# G 5.78 DNS-Spoofing

Um im Internet mit einem anderen Rechner kommunizieren zu können, wird dessen IP-Adresse benötigt. Da solche Nummern nicht sehr einprägsam sind, ordnet das Domain Name System (DNS) einer solchen IP-Adresse einen Name zu.

Von DNS-Spoofing ist die Rede, wenn es einem Angreifer gelingt, die Zuordnung zwischen einem Rechnernamen und der zugehörigen IP-Adresse zu fälschen, also wenn ein Name in eine falsche IP-Adresse bzw. die IP-Adresse in einen falschen Namen umgewandelt wird. Beim klassischen DNS-Spoofing wird nicht der Client-PC durch Schadsoftware manipuliert, sondern es werden Schwachstellen in der DNS-Kommunikation ausgenutzt. Hierdurch sind unter anderem die folgenden Angriffe möglich:

- r-Dienste (rsh, rlogin, rsh): Diese Dienste erlauben eine Authentisierung anhand des Namens des Clients. Der Server kennt die IP-Adresse des Clients und fragt über DNS nach dessen Namen. Durch DNS-Manipulationen kann sich ein Angreifer unbefugt beim r-Dienst anmelden und Zugriff auf schützenswerte Informationen erlangen.
- Web-Spoofing: Ein Angreifer könnte die Adresse *www.bsi.bund.de* einem falschen Rechner zuweisen. Bei der Eingabe von *http://www.bsi.bund.de* würde dieser falsche Rechner angesprochen werden.

Wie leicht es ist, DNS-Spoofing durchzuführen, hängt davon ab, wie das Netz des Angegriffenen konfiguriert ist. Da kein Rechner alle DNS-Informationen der Welt besitzen kann, ist er immer auf Informationen anderer DNS-Server angewiesen. Um die Häufigkeit von DNS-Abfragen zu verringern, speichern die meisten Resolving DNS-Server Informationen, die sie von anderen DNS-Servern erhalten haben, für eine gewisse Zeit zwischen.

Eine weitere Möglichkeit, um Schaden per DNS-Spoofing anzurichten, ist ein Einbruch in einen DNS-Server. Dieser Fall soll hier aber nicht weiter betrachtet werden. Vielmehr geht es darum, prinzipielle Gefahren beim Einsatz von DNS aufzuzeigen.

**Beispiele:**

- Ein Benutzer auf dem Rechner *pc.kunde.de* will zuerst auf *www.firma-x.de* und dann auf den Konkurrenten *www.firma-y.de* zugreifen. Um auf *www.firma-x.de* zugreifen zu können, muss er die zugehörige IP-Adresse bei seinem Resolving DNS-Server *ns.kunde.de* nachfragen. Dieser kennt die Adresse noch nicht und fragt beim Advertising DNS-Server *ns.firma-x.de* nach. Dieser antwortet mit der IP-Adresse, die von *ns.kunde.de* an den Benutzer weitergeleitet und gespeichert wird. Befindet sich in dem Antwortpaket von *ns.firma-x.de* neben der IP-Adresse von *www.firma-x.de* auch eine falsche IP-Adresse für den Rechnernamen *www.firma-y.de*, so wird diese gespeichert. Versucht der Benutzer nun, auf *www.firma-y.de* zuzugreifen, fragt der eigene Resolving DNS-Server nicht mehr beim DNS-Server *ns.firma-y.de* nach, vielmehr gibt er die Informationen weiter, die ihm von *ns.firma-x.de* untergeschoben wurden. In aktuellen Versionen von DNS-Server-Produkten ist der Angriff in dieser Form nicht mehr möglich. Es existieren jedoch modifizierte, beziehungsweise verbesserte Varianten des Angriffs, die auch bei aktuellen Versionen erfolgreich sind.
- Firma X weiß, dass ein Benutzer mit dem Rechner *pc.kunde.de* auf den Konkurrenzrechner *www.firma-y.de* zugreifen will. Firma X verhindert dies, indem sie den DNS-Server *ns.kunde.de* nach der Adresse *www.firma-x.de* fragt. Dieser muss beim DNS-Server *ns.firma-x.de* nachfragen und be-

kommt wie im ersten Beispiel auch die falschen Angaben über *www.firma-y.de* zurück.

Diese beiden Beispiele beruhen darauf, dass ein DNS-Server zusätzliche Daten akzeptiert, die er gar nicht angefordert hat. In neuen Versionen von DNS-Software (z. B. *BIND*) ist dieser Fehler beseitigt, so dass diese Art von Angriffen verhindert wird. Es ist allerdings unter Verwendung von IP-Spoofing noch immer möglich, falsche DNS-Einträge zu erzeugen. Dieser Angriff ist aber technisch anspruchsvoller, vergleiche dazu auch G 5.48 *IP-Spoofing*.

Beide Angriffsformen haben eines gemeinsam: Ziel ist es, dass der angegriffene Rechner falsche Zuordnungen von IP-Adressen und Namen zwischenspeichert, man spricht hierbei von Cache-Poisoning. Da DNS-Server Domain-Informationen, wie im zweiten Beispiel beschrieben, zwischenspeichern, können sich diese gefälschten Daten weit verbreiten. Werden entsprechende Anfragen an den manipulierten DNS-Server gestellt, liefert dieser als Antwort die gefälschten Daten. Der Empfänger der Antwort speichert die gefälschten Daten ebenfalls zwischen und sein Cache ist somit ebenfalls "vergiftet". Die gespeicherten Daten haben eine definierbare Haltbarkeit (Time To-Live, TTL). Wird der Resolving DNS-Server nach einer manipulierten Adresse gefragt, so wird er erst dann wieder einen anderen DNS-Server anfragen, wenn die Haltbarkeit abgelaufen ist. So ist es möglich, dass sich manipulierte DNS-Informationen lange halten können, obwohl sie auf dem ursprünglich angegriffenen DNS-Serer bereits wieder korrigiert sind.

Cache-Poisoning ist bezüglich DNS eine der gefährlichsten Angriffsformen. Gelingt es einem Angreifer beispielsweise die Namensauflösung für eine Domain zu übernehmen, indem er die Einträge so manipuliert, dass seine DNS-Server befragt werden, sind alle Subdomains automatisch mitbetroffen.

# G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows-Systemen

Bei jeder Standardinstallation eines Windows-NT-basierten Systems wird ein lokales Administratorkonto angelegt. Dies betrifft sowohl die Client- als auch die Server-Versionen. Im Gegensatz zu selbst angelegten Konten kann dieses lokale vordefinierte Administratorkonto unter Windows NT und Windows 2000 weder gelöscht noch gesperrt werden. Damit soll verhindert werden, dass der Administrator vorsätzlich oder versehentlich ausgesperrt und somit die Verwaltung unmöglich wird. Problematisch in diesem Zusammenhang ist, dass das vordefinierte Administratorkonto selbst dann nicht gesperrt wird, wenn die in der Kontorichtlinie für eine Sperre eingetragene Anzahl ungültiger Kennworteingaben überschritten wird. Ohne entsprechende Gegenmaßnahmen ermöglicht dies das planmäßige Ausprobieren von Passwörtern mit Hilfe von speziellen Programmen. Erst ab Windows XP beziehungsweise Windows Server 2003 ist es möglich, das lokale vordefinierte Administratorkonto zu deaktivieren. Ab Windows Vista ist dieses Konto bei einer Standardinstallation bereits deaktiviert. Das Konto kann aber weiterhin nicht gelöscht werden.

Es gibt weitere Möglichkeiten, um in den Besitz eines zu einem Administratorkonto gehörenden Passwortes zu kommen, um damit Administratorrechte zu erlangen. Wird ein Windows NT-basiertes System fernadministriert, so besteht die Gefahr, dass beim Authentisierungsvorgang das Anmeldepasswort, je nach verwendetem Authentisierungsverfahren, im Klartext übertragen wird und damit von einem Angreifer aufgezeichnet werden kann. Windows Vista und Server 2008 stellen zwar bereits bei einer Standardinstallation IPSec-Unterstützung zur Verfügung, die Verschlüsselung muss jedoch konfiguriert und aktiviert werden. Selbst wenn durch Eingriffe in das System sichergestellt ist, dass die Anmeldepasswörter nur verschlüsselt übertragen werden, ist es möglich, dass ein Angreifer das verschlüsselte Passwort aufzeichnet und mit Hilfe entsprechender Software entschlüsselt. Dies gilt insbesondere für Windows NT, wenn das ältere NTLM-Verfahren eingesetzt wird. Ab Windows 2000 wird in einer Domänenumgebung standardmäßig das Kerberos-Verfahren eingesetzt, das robuster gegen solche Angriffe ist.

Weiterhin wird bei Windows XP und Windows Server 2003 jedes Passwort in der Registrierung und in einer Datei, die sich im Verzeichnis *%SystemRoot%\System32\Repair* bzw. *%Systemroot%/Repair* auf den Notfalldisketten und gegebenenfalls auf Bandsicherungen befindet, verschlüsselt gespeichert. Gelangt ein Angreifer in den Besitz der Datei, kann er mit Hilfe entsprechender Software versuchen, das benötigte Passwort zu entschlüsseln. Windows Versionen ab Vista und Server 2008 haben kein *Repair*-Verzeichnis mehr.

Mit einer speziellen Schadsoftware ist es möglich, dass ein Angreifer auf dem Windows NT-Rechner, an dem er lokal angemeldet ist, ein beliebiges Benutzerkonto der Gruppe *Administratoren* hinzufügt und dem Kontoinhaber damit Administratorrechte verschafft.

Andere Beispiele für Attacken zum unberechtigten Erlangen von administrativen Berechtigungen sind:

- Die Erweiterung der Berechtigungen (Privilege Escalation) ist auch durch die Ausnutzung von Schwachstellen in Programmen oder Diensten möglich, die mit administrativen oder Systemberechtigungen ausgeführt werden.

- Technische Attacken können zusammen mit Social Engineering-Methoden eingesetzt werden. Beispielsweise kann das lokale System mit normalen Benutzerrechten manipuliert und ein Keylogger installiert werden. Bringt ein Angreifer dann einen Administrator dazu, sich anzumelden, zeichnet der Keylogger seinen Benutzernamen und sein Passwort auf.
- Kennwörter könnten unter Verwendung eines anderen Boot-Mediums (z. B. Diskette/CD-ROM/USB-Speicher) überschrieben werden.

# G 5.80 Hoax

Ein Hoax (englisch für Streich, Trick, falscher Alarm) ist eine Nachricht, die eine Warnung vor neuen spektakulären Computer-Viren oder anderen IT-Problemen enthält und Panik verbreitet, aber nicht auf realen technischen Fakten basiert. Meist werden solche Nachrichten über E-Mails verbreitet. Beispielsweise wird dabei vor Computer-Viren gewarnt, die Hardware-Schäden verursachen können oder durch das bloße Öffnen einer E-Mail (nicht eines Attachments) zu Infektionen und Schäden führen können und die durch keine Antiviren-Software erkannt werden. Neben dieser Warnung wird darum gebeten, die Warnmeldung an Freunde und Bekannte weiterzuleiten. Noch wirksamer wird ein solcher Hoax, wenn als Absender eine gefälschte Adresse angegeben wird, wie zum Beispiel die eines namhaften Herstellers.

Ein solcher Hoax ist nicht zu verwechseln mit einem Computer-Virus, der tatsächlich Manipulationen am IT-System vornehmen kann. Vielmehr handelt es sich um eine irreführende Nachricht, die ohne Schaden gelöscht werden kann und sollte. Die einzigen Schäden, die ein Hoax herbeiführt, sind die Verunsicherung und Irritation der Empfänger und ggf. die Kosten an Zeit und Geld für den Weiterversand des Hoax.

Im Bereich des Mobilfunks gab es eine ganze Reihe solcher Hoax-Nachrichten, bei denen davor gewarnt wurde, dass an Mobiltelefonen die Eingabe bestimmter Tastenkombinationen oder die Wahl bestimmter Rufnummern dazu führen könnten, Gespräche abzuhören oder auf Kosten anderer zu telefonieren. Durch die Nennung bestimmter Mobiltelefon-Marken und einiger technischer Ausdrücke wird der Anschein von Seriosität erweckt. Solche Gerüchte halten sich hartnäckig und verunsichern die Benutzer.

**Beispiel:**

- Im Frühjahr 2000 kursierte folgende Falschmeldung per E-Mail (und teilweise sogar per Brief):
  "Wenn Sie eine Nachricht auf Ihr Handy erhalten, dass Sie unter der Nummer 0141-455xxx zurückrufen sollen, antworten Sie auf keinen Fall darauf. Ihre Rechnung steigt sonst ins Unermessliche.
  Diese Information wurde von der "Zentralstelle zur Unterdrückung von betrügerischen Machenschaften" (Office Central de Repression du Banditisme) herausgegeben."

# G 5.81 Unautorisierte Benutzung eines Kryptomoduls

Gelingt es einem Dritten, ein Kryptomodul unautorisiert zu benutzen, so können Schäden verschiedenster Art die Folge sein. Beispiele für solche Schäden sind:

- Bei der unautorisierten Nutzung gelingt es dem Angreifer, geheime Schlüssel auszulesen, die Schlüssel zu verändern oder auch kritische Sicherheitsparameter zu manipulieren. Die Folge wäre, dass die kryptographischen Verfahren keine ausreichende Sicherheit mehr bieten.
- Bei der unautorisierten Nutzung manipuliert der Angreifer das Kryptomodul so, dass es zwar auf den ersten Blick korrekt arbeitet, sich jedoch tatsächlich in einem unsicheren Zustand befindet.
- Der Angreifer nutzt das Kryptomodul in Form einer Maskerade. Signiert er oder verschlüsselt er Daten bei der unautorisierten Benutzung des Kryptomoduls, so wird dies vom Empfänger der Daten so interpretiert, als hätte der autorisierte Benutzer dies vorgenommen.

**Beispiel:**

- Eine unautorisierte Benutzung eines Kryptomoduls wird dann möglich, wenn der reguläre Benutzer kurzfristig seinen Arbeitsplatz verlässt und das funktionsfähige Kryptomodul einsetzbar ist, ohne dass es vor unbefugtem Zugriff geschützt ist, also beispielsweise wenn eine Signatur- oder Verschlüsselungschipkarte im Rechner stecken bleibt. Damit kann jeder, der zufällig vorbeikommt, E-Mail im Namen des regulären Benutzers signieren oder auf dem IT-System gespeicherte Dateien so verschlüsseln, dass der Benutzer sie nicht mehr verwenden kann.

# G 5.82 Manipulation eines Kryptomoduls

Ein Angreifer kann versuchen, ein Kryptomodul zu manipulieren, um geheime Schlüssel auszulesen oder die Schlüssel zu verändern oder auch um kritische Sicherheitsparameter zu verändern. Ein Kryptomodul kann auf verschiedene Art und Weise manipuliert sein, es kann z. B.

- ein Super-Passwort, mit dem alle anderen Passwörter umgangen werden können,
- nicht dokumentierte Testmodi, über die jederzeit Zugriff auf sensitive Bereiche genommen werden kann,
- Trojanische Pferde, d. h. Software, die neben ihrer eigentlichen Aufgabe andere, nicht direkt erkennbare Aktionen wie das Aufzeichnen von Passwörtern, durchführt,
- manipulierte Zugriffsrechte auf bestimmte Kommandos

enthalten. Andere Beispiele für solche Angriffe sind

- die Modifikation von kryptographischen Schlüsseln,
- die Beeinträchtigung der internen Schlüsselgenerierung, z. B. durch Manipulation des Zufallszahlengenerators,
- die Modifizierung der Abläufe innerhalb des Kryptomoduls,
- Modifikationen am Sourcecode oder am ausführbaren Code des Kryptomoduls,
- Über- oder Unterschreitung des zulässigen Arbeitsbereichs bzgl. Spannungsversorgung, Temperatur, EMV-Grenzwerte etc. des Kryptomoduls.

Bei Manipulationen am Kryptomodul wird der Angreifer meist versuchen, diesen Angriff zu vertuschen, so dass das Kryptomodul für Benutzer zwar auf den ersten Blick vermeintlich korrekt arbeitet, sich jedoch in einem unsicheren Zustand befindet. Es gibt allerdings auch zerstörerische Angriffe, bei denen auch die Zerstörung des Kryptomoduls bewusst in Kauf genommen wird, beispielweise wenn ein Angreifer Informationen über die Funktionsweise des Kryptomoduls erhalten will oder wenn die kryptographischen Schlüssel ausgelesen werden sollen.

Ein Angreifer kann versuchen, seine Angriffe am Aufstellungsort des Kryptomoduls durchzuführen oder es entwenden. Bei einem schlecht geschützten Aufstellungsort lassen sich die Manipulationen unter Umständen sehr schnell durchführen und bleiben dadurch evtl. lange unbemerkt. Durch den Diebstahl von Kryptomodulen kann ein Angreifer wichtige Informationen darüber bekommen, wie eine Komponente am einfachsten manipulierbar ist. Er kann die entwendeten Komponenten benutzen, um daraus sensitive Informationen wie Schlüssel, Software oder Kenntnis über Hardwaresicherheitsmechanismen zu gewinnen. Er kann aber auch die entwendete Komponente dazu benutzen, um ein authentisches Kryptomodul vorzutäuschen.

# G 5.83 Kompromittierung kryptographischer Schlüssel

Beim Einsatz kryptographischer Verfahren hängt der Sicherheitszugewinn entscheidend davon ab, wie vertraulich die verwendeten geheimen kryptographischen Schlüssel bleiben. Mit Kenntnis sowohl des verwendeten Schlüssels als auch des eingesetzten Kryptoverfahrens ist es meist einfach, die Verschlüsselung umzukehren und den Klartext zu gewinnen. Daher wird ein potentieller Angreifer versuchen, die verwendeten Schlüssel zu ermitteln. Angriffspunkte dazu sind:

- Bei der Schlüsselerzeugung werden ungeeignete Verfahren eingesetzt, beispielsweise zur Bestimmung von Zufallszahlen oder zur Ableitung der Schlüssel.
- Bei der Schlüsselerzeugung werden Schlüssel ausgelesen, bevor sie auf sicheren Speichermedien gespeichert werden.
- Im laufenden Betrieb werden Schlüssel aus Kryptomodulen durch technische Angriffe ausgelesen.
- Als Backup hinterlegte Schlüssel werden entwendet.
- Bei der Eingabe von kryptographischen Schlüsseln werden die Schlüssel ausgespäht.
- Die eingesetzten Kryptoverfahren werden gebrochen. So ist es heute beispielsweise bei symmetrischen Verschlüsselungsverfahren wie dem DES möglich, den verwendeten Schlüssel mittels massiv paralleler Rechner durch Ausprobieren zu ermitteln (Brute-Force-Attacke).
- Verwendete kryptographische Schlüssel werden durch Innentäter verraten.

# G 5.84 Gefälschte Zertifikate

Zertifikate dienen dazu, einen öffentlichen kryptographischen Schlüssel an eine Person zu binden. Diese Bindung des Schlüssels an den Namen der Person wird wiederum kryptographisch mittels einer digitalen Signatur einer vertrauenswürdigen dritten Stelle abgesichert. Diese Zertifikate werden von Dritten dann verwendet, um digitale Signaturen der im Zertifikat ausgewiesenen Person zu prüfen bzw. um dieser Person Daten mit dem im Zertifikat aufgezeichneten Schlüssel verschlüsselt zuzusenden.

Ist ein solches Zertifikat gefälscht, werden digitale Signaturen fälschlicherweise als korrekt geprüft und der Person im Zertifikat zugeordnet oder es werden Daten mit einem ggf. unsicheren Schlüssel verschlüsselt und versandt. Beide Angriffsmöglichkeiten können einen Täter bewegen, gefälschte Zertifikate in Umlauf zu bringen.

Gefälschte Zertifikate können auf verschiedene Weise erzeugt werden:

- Ein Innentäter der vertrauenswürdigen Stelle erstellt mit dem eigenen Signaturschlüssel ein Zertifikat mit gefälschten Angaben. Dieses Zertifikat ist authentisch und wird bei einer Prüfung als korrekt verifiziert.
- Ein Täter gibt sich als eine andere Person aus und beantragt ein Zertifikat, welches auf diese andere Person ausgestellt wird, obwohl der Täter im Besitz des geheimen Schlüssels ist, der mit dem öffentlichen Schlüssel im Zertifikat korrespondiert.
- Ein Täter erzeugt ein Zertifikat und signiert es mit einem eigenen Schlüssel. Die Fälschung fällt nur auf, wenn das Zertifikat geprüft wird und dabei festgestellt werden kann, dass das Zertifikat von einer nichtvertrauenswürdigen Stelle ausgestellt wurde.

Wenn ein Täter erst einmal ein Zertifikat mit falschen Angaben auf irgendeinem Weg erhalten hat, kann er sich gegenüber Kommunikationspartnern jederzeit als eine andere Person ausgegeben, und zwar sowohl beim Versand als auch beim Empfang von Nachrichten.

# G 5.85 Integritätsverlust schützenswerter Informationen

Integrität ist die Anforderung, dass eine Information unverfälscht sein muss. Das heißt, dass keine unbefugten Veränderungen an der Information vorgenommen werden dürfen. Integrität bedeutet dabei auch, dass ein Datenbestand insgesamt konsistent ist, d. h. dass Beziehungen der Daten untereinander korrekt aufgelöst werden können und dass die Aktualität aller Daten den Erwartungen der Benutzer entspricht.

Neben der Vertraulichkeit und der Verfügbarkeit gehört die Integrität zu den Grundwerten der Informationssicherheit.

Wenn Daten nicht mehr integer sind, kann es zu einer Vielzahl von Problemen kommen:

- Daten können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden.
- Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an den falschen Empfänger ausgelöst werden, die Absenderangaben von E-Mails könnten manipuliert werden oder vieles mehr.
- Auf der Grundlage von falschen, unvollständigen oder veralteten Daten können falsche Geschäftsentscheidungen getroffen werden mit weitreichenden Konsequenzen.
- Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren - und hier reicht die Änderung eines Bits - können sie u. U. nicht mehr entschlüsselt bzw. entpackt werden.
- Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.
- Durch die Manipulation hinterlegter kryptographischer Zertifikate können z. B. Authentisierungs- oder Signaturverfahren ausgehebelt werden und auf diese Weise Schadsoftware in geschützten Umgebungen zur Ausführung gebracht oder verschlüsselte Tunnel unterbrochen werden (Man-in-the-Middle-Angriff).
- Auswertungen von Datenbeständen schlagen fehl, weil Referenzen nicht mehr stimmen oder sich Widersprüche im Datenbestand ergeben.
- Personenbezogene Daten können an falsche Empfänger übermittelt werden (Datenschutzverstöße). Bei falschen personenbezogenen Daten besteht für die Betroffenen ein gesetzlicher Anspruch auf Berichtigung.
- Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

Zu Integritätsverlusten kann es auf verschiedene Weise kommen:

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- Bei der Datenübertragung kann es zu Übertragungsfehlern kommen.
- Durch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.
- Durch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die sogar häufig lange Zeit nicht bemerkt werden.

- Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.
- Durch bewusste Sabotage können z. B. Steuerdaten für Industrieanlagen so verändert werden, dass große Folgeschäden durch die Zerstörung von Maschinen oder Gütern daraus resultieren. Die Schäden können dabei mit erheblicher zeitlicher Verzögerung einsetzen (z. B. durch bewusst erhöhten Verschleiß) und lassen sich dann nur sehr schwer mit der Manipulation als Fehlerursache in Verbindung bringen.
- Protokolldaten oder Zeitstempel können bewusst verfälscht werden, um Angriffe und Manipulationen zu verschleiern.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

# G 5.86 Manipulation von Managementparametern

Auch Managementsysteme können durch bewusst herbeigeführte Fehlkonfigurationen zu einem Angriff auf ein lokales Rechnersystem benutzt werden. Die Fehlkonfigurationen können dabei auf verschiedene Arten herbeigeführt werden. Dabei sind Manipulationen sowohl an der Managementplattform als auch an den verwalteten Geräten möglich. Insbesondere Netzmanagementsysteme, die SNMP benutzen, sind für Angriffe anfällig, bei denen bewusst Managementparameter fehlkonfiguriert werden (z. B. durch einen eigenen SNMP-Client). Je nach einstellbaren Parametern reichen die Attacken von einfachen "Denial-of-service-Attacken" (z. B. durch Verstellen von IP-Adressen) bis hin zur Datenveränderung (z. B. nach Verstellen von Zugriffsrechten).

Werden Netzkomponenten durch ein Managementsystem verwaltet, so sollten alle durch das Managementsystem verwalteten Konfigurationsparameter auch nur durch das Managementsystem verändert werden. Je nach Managementsystem ist es jedoch immer noch möglich, die Konfigurationsparameter der Komponente auch lokal zu verändern. Wird ein PC z. B. über SNMP durch ein Netzmanagementsystem verwaltet, so kann ein lokaler Benutzer mit einem lokalen SNMP-Client-Programm (mit Kenntnis des SNMP-Passwortes) oder aber über ein lokales Bedienelement (z. B. bei einem Drucker) die Einstellungen verändern. Dies führt u. U. zumindest zu Inkonsistenzen im Netzmanagementsystem, kann jedoch auch bewusst zur Herbeiführung von Sicherheitslöchern benutzt werden. Beispielsweise könnte das Abfragen freigegebener Verzeichnisse über SNMP über Netz für einen Windows Rechner nachträglich ermöglicht werden.

# G 5.87 Web-Spoofing

Bei Web-Spoofing fälscht ein Angreifer eine existierende Webseite, d. h. er gestaltet eine seiner eigenen Webseiten so, dass diese wie die Webseite einer bekannten Institution aussieht. Die bereits vorhandene Webseite, die nachgebildet wurde, wird dabei nicht verändert, sondern ist weiterhin in der ursprünglichen Form erreichbar. Mithilfe verschiedener Tricks versucht der Angreifer dann, Benutzer auf die von ihm ins Netz gestellte Webseite zu locken.

Dazu wählt er beispielsweise deren Web-Adresse so, dass viele Benutzer alleine durch die Adresswahl davon ausgehen, mit einer bestimmten Institution verbunden zu sein. So kann er zum Beispiel eine Seite registrieren, bei der der Hostname mit dem der Original-Webseite identisch ist, aber die Top-Level-Domain ausgetauscht wurde. Er kann aber auch eine Adresse verwenden, die häufige Tipp- oder Schreibfehler ("Typosquatting") enthält, und so Benutzer auf die gefälschte Seite locken.

Eine weitere Möglichkeit besteht darin, manipulierte Links zu verbreiten. Es können unterschiedliche Zeichensätze und gleich aussehende Buchstaben benutzt werden, um täuschend echt aussehende Links zu erzeugen. Beispielsweise lassen sich dafür Zahlen, die auf den ersten Blick wie Buchstaben aussehen oder Buchstaben, die sich ähneln, verwenden. Neben dem kaum zu erkennenden Unterschied zwischen "I" (großes "i") und "l" (kleines "L") können auch ähnlich aussehende Buchstaben verwendet werden. Ein Beispiel hierfür ist die lateinische und die kyrillische Schreibweise des Buchstabens "a", der am Monitor gleich aussieht, aber unterschiedlich kodiert wird.

Benutzern können auch Adressen angezeigt werden, die aber nicht mit denen identisch sind, zu denen der Link führt. Beispielsweise ist es möglich, durch die Nutzung eines HTML-Links die URL der vertrauenswürdigen Seite anzuzeigen, obwohl der Link zu einer gefälschten Seite führt. Ebenso können Benutzername und Passwort in der URL dem Seitennamen vorangestellt werden. Benutzer, die diese Schreibweise nicht kennen, nehmen an, dass sie zu der Webseite, die als Benutzername/Passwort angegeben ist, geleitet werden, obwohl sich der tatsächlich verwendete Hostname wesentlich weiter hinten in der URL befindet.

**Beispiele:**

- Die XY Bank verwendet die URL www.xy-bank.de für ihren Internetauftritt. Ein Angreifer richtet unter den URLs www.xybank.de oder www.xy-bank.com eine Webseite ein, die auf den ersten Blick derjenigen der XY Bank ähneln. Zusätzlich sorgt er dafür, dass diese Adressen von XY-Kunden über Suchmaschinen gefunden werden.
- Benutzer, die diese Seiten aufrufen, werden annehmen, dass sie mit dem Webserver ihrer Bank kommunizieren. Daher sind sie bereit, ihre Kontonummer und PIN oder andere Zugangsdaten einzugeben.
- Die Seite whitehouse.com durchlebte eine wechselhafte Geschichte. Hier befand sich allerdings nie, wie von vielen Benutzern zunächst vermutet, der Webauftritt des amerikanischen Weißen Hauses, sondern wechselnde kommerzielle oder pornografische Inhalte.
- Die beiden URLs www.BSI.bund.de und www.BSl.bund.de sehen zumindest auf den ersten Blick identisch aus. Erst beim genauen Hinsehen ist zu erkennen, dass nur der erste zum Webauftritt des Bundesamtes für Sicherheit in der Informationstechnik führt. Beim zweiten Link wurde das große "I" durch ein kleines "L" ersetzt.
- In einer serviceorientierten Architektur (SOA) fälscht ein Angreifer die Identität eines Service-Providers, z. B. durch eine manipulierte URL mit ei-

ner Domain, die dem Namen eines bekannten Unternehmens ähnelt. Benutzer gehen davon aus, dass es sich um einen vertrauenswürdigen Service-Provider handelt und übermitteln Daten an den angebotenen Dienst. So erhält ein Angreifer vertrauliche Informationen des Service-Consumers, mit denen er nun den "echten" Dienst benutzen kann.

# G 5.88 Missbrauch aktiver Inhalte

Aktive Inhalte sind Programmteile oder Skripte, die im Browser ausgeführt werden. Weit verbreitete Arten von aktiven Inhalten sind JavaScript, Java-Applets, ActiveX-Elemente, Flash etc. Sie dienen häufig dazu, Webseiten interaktiver zu gestalten, besondere grafische Effekte zu erzielen oder Multimedia-Inhalte einzubetten.

Andererseits können aktive Inhalte jedoch auch gezielt zu dem Zweck erstellt worden sein, vertrauliche Daten auszuspionieren, Manipulationen vorzunehmen oder den Computer mit Schadprogrammen zu infizieren. Auch Angriffe auf die Verfügbarkeit des jeweiligen Clients sind möglich. Die gängigen Browser enthalten Sicherheitsmechanismen, die die Zugriffsmöglichkeiten von aktiven Inhalten einschränken. Es werden jedoch immer wieder Schwachstellen und Möglichkeiten bekannt, diese Sicherheitsmechanismen zu unterlaufen.

Die folgenden Aspekte tragen dazu bei, dass das Ausführen aktiver Inhalte zu Sicherheitsproblemen führen kann:

- Aktive Inhalte können aus dem Netz geladen und ausgeführt werden, ohne dass die Benutzer aktiv daran beteiligt sind. Häufig ist die Ausführung für die Benutzer auch nicht erkennbar.
- Aktive Inhalte können über Standardnetzprotokolle, beispielsweise SMTP, mit Computern im Internet kommunizieren. Auf diese Weise können zum Beispiel vertrauliche Informationen an Unbefugte weitergeleitet werden.
- Für die verschiedenen Arten von aktiven Inhalten bestehen unterschiedliche Möglichkeiten, auf die Ressourcen des Betriebssystems und der Hardware zuzugreifen.

Anders als bei Java und JavaScript ist die Funktionsvielfalt von ActiveX-Controls kaum eingeschränkt. Die Controls können direkt auf dem Rechner ablaufen und Zugriff auf die Hardware und das Betriebssystem haben. Aufgrund dieser vielfältigen Zugriffsmöglichkeiten ist mit der Ausführung von ActiveX-Komponenten ein hohes Risiko verbunden.

Bei entsprechender Voreinstellung seines Browsers kann ein Benutzer dafür sorgen, dass nur digital signierte ActiveX-Controls ausgeführt werden. Eine solche gültige Signatur beweist allerdings nur, dass der Hersteller des ActiveX-Controls bei einer Zertifizierungsstelle bekannt ist und dass das von diesem Hersteller bereitgestellte Control unverändert geladen wurde. Hierdurch wird nichts über die Funktionsweise oder Unbedenklichkeit eines solchen Controls ausgesagt und auch keine Gewähr dafür übernommen.

# G 5.89 Hijacking von Netz-Verbindungen

Weitaus kritischer als das Abhören einer Verbindung ist das Übernehmen einer Verbindung. Hierbei werden Pakete in das Netz eingeschleust, die den Client entweder blockieren oder umleiten. Der Serverprozess kann daraufhin nicht erkennen, dass ein anderes Programm an die Stelle des Original-Clients getreten ist. Bei dieser Übernahme einer bestehenden Verbindung kann der Angreifer nach erfolgreicher Authentisierung einer berechtigten Person beliebige Aktionen in deren Namen ausüben.

# G 5.90 Manipulation von Adressbüchern und Verteillisten

Auf Faxservern besteht in der Regel die Möglichkeit, Adressbücher und Verteillisten zu führen. In Adressbüchern werden u. a. die Empfänger-Faxnummern gespeichert. Auch ist es möglich, mehrere Faxempfänger in einer Gruppe z. B. für den Versand von Serien-Faxsendungen zusammenzufassen. Der Gebrauch von solchen Adressbüchern ist für den Benutzer sehr komfortabel, da eine einmal gespeicherte Empfängernummer nicht noch einmal manuell eingegeben werden muss. Vielfach wird von den Benutzern eines Faxservers vor dem Faxversand nicht mehr die Richtigkeit einer im Adressbuch eingetragenen Empfängernummer überprüft. Gleiches gilt auch für die Zuordnung einzelner Empfänger zu Gruppen. Häufig wird vor dem Versand von Serien-Faxsendungen nicht mehr überprüft, ob sich der gewünschte Kreis von Empfängern mit den Mitgliedern einer Gruppe deckt.

Mittels Verteillisten können eingehende Faxsendungen (mehreren) Empfängern zugeordnet werden.

Sofern ein Unbefugter Adressbücher und Verteillisten verändern kann, besteht die Gefahr, dass Faxsendungen an unerwünschte Empfänger übermittelt werden. Es ist damit auch möglich, dass der Versand eines Faxes an den gewünschten Empfänger unterbunden wird. Besonders gefährdet sind hier naturgemäß die zentral geführten Adressbücher und Verteillisten.

# G 5.91 Abschalten von Sicherheitsmechanismen für den RAS-Zugang

Diese Gefährdung ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in G 3.42 *Unsichere Konfiguration der VPN-Clients für den Fernzugriff* integriert.

# G 5.92 Nutzung des VPN-Clients als VPN-Server

Die auf VPN-Clients eingerichtete Software zur Einwahl in ein Remote-Access-VPN erlaubt es häufig, dass auch der Client als VPN-Server fungieren und eingehende Verbindungen entgegennehmen kann. Dadurch besteht grundsätzlich die Gefahr, dass Unbefugte versuchen, sich mit dem VPN-Client zu verbinden und über diesen auf das LAN zuzugreifen.

Gelingt es einem Angreifer, den VPN-Authentisierungsmechanismus zu überwinden, kann er auch auf die Daten des VPN-Clients zugreifen. Beispielsweise könnte ein Angreifer sich unbefugt an dem Client anmelden, indem er Passwörter erfolgreich rät oder ausprobiert oder indem er nicht passwortgeschützte Benutzerkonten oder Gast-Kennungen mit Standardpasswörtern auf dem Client nutzt. Je nach Art der Anbindung des VPN-Clients an das Firmen- bzw. Behörden-LAN kann der Angreifer dadurch außerdem auf interne Ressourcen zugreifen.

# G 5.93 Erlauben von Fremdnutzung von VPN-Komponenten

Wird Unbefugten erlaubt, die Komponenten eines Virtuellen Privaten Netzes (VPN) zu nutzen, also das vorhandene Berechtigungskonzept umgangen, ist die Sicherheit des VPNs nicht mehr gewährleistet (siehe auch G 3.30 *Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners*). Besonders für Remote-Access-VPNs bestehen folgende Gefahren:

- VPN-Zugänge können unautorisiert verwendet werden, wenn die Sicherheitsrichtlinien nicht eingehalten werden. Beispielsweise geschieht es immer wieder, dass Administratoren aus falsch verstandener Freundlichkeit die VPN-Einwahl für nicht berechtigte Personen erlauben (beispielsweise zur Internet-Nutzung).
- VPN-Benutzer geben Authentisierungsdaten oder -token an unberechtigte Dritte weiter, um diesen unter ihrer Kennung den entfernten Zugang zum LAN zu gewähren. Mögliche Motive dafür sind z. B. die Übergabe an einen Kollegen, der gemäß VPN-Sicherheitskonzept nicht zur VPN-Nutzung berechtigt ist oder vergessen hat, die VPN-Nutzung rechtzeitig vor Antritt einer Dienstreise zu beantragen. Das VPN-Benutzerkonto wird im Folgenden von mehreren Benutzern verwendet, so dass im Schadensfall keine eindeutige Identifizierung des Verursachers mehr möglich ist.
- Für den Bereich der Telearbeit ergibt sich häufig die Problematik, dass der VPN-Client durch Familienmitglieder oder Freunde von Familienmitgliedern benutzt wird. Organisationsfremde Personen, die mit dem VPN-Client arbeiten, werden die für den VPN-Client geltenden Sicherheitsvorschriften in der Regel nicht beachten. Hierdurch kann die Sicherheit des LANs der Institution beeinträchtigt werden.

An entfernten Standorten kann nie ausgeschlossen werden, dass die dortigen IT-Systeme fremdgenutzt werden. Da hierauf auch Externe physikalischen Zugriff nehmen können, könnten sie außerdem manipuliert worden sein. Die Sicherheitsmechanismen könnten dadurch unterlaufen werden.

# G 5.94 Missbrauch von SIM-Karten

Jeden Tag werden Mobiltelefone verloren oder gestohlen. Neben dem unmittelbaren Verlust kann dabei weiterer finanzieller Schaden entstehen. Gelangt ein Unbefugter mit dem Gerät auch in den Besitz einer SIM-Karte, kann er auf Kosten des rechtmäßigen Karteninhabers telefonieren, sofern:

- ihm die SIM PIN bekannt ist,
- keine SIM PIN gesetzt wurde,
- das Telefon eingeschaltet ist (Standby ohne Display-Password)
- oder die SIM PIN erraten kann.

Mit dem Aufkommen von Datendiensten über Mobilfunk ist zudem das rechtliche Risiko durch Kartenmissbrauch deutlich erhöht worden. Nutzt der Unbefugte die SIM-Karte, beispielsweise um urheberrechtlich geschütztes Material herunterzuladen, Spam-E-Mails zu verschicken oder für Denial-of-Service-Attacken, kann zunächst der Inhaber der SIM-Karte dafür belangt werden.

Daten wie Telefonbuch oder Kurznachrichten, die im Mobiltelefon oder auf der SIM-Karte gespeichert sind, können durchaus einen vertraulichen Charakter haben. Ein Verlust des Mobiltelefons oder der Karte bedeutet dann unter Umständen die Offenlegung dieser gespeicherten Informationen.

Die kryptografischen Sicherheitsmechanismen der SIM-Karten einiger Netzbetreiber waren gegen 1998 schwach ausgelegt. Dadurch war es möglich, SIM-Karten dieser Netzbetreiber zu kopieren. Dazu musste dem Angreifer allerdings die Original-Karte zur Verfügung stehen. Außerdem muss die PIN bekannt sein oder die PIN-Abfrage abgeschaltet sein, damit die IMSI ausgelesen werden kann.

Benutzer können einen solchen Angriff durch Setzen einer schlecht erratbaren SIM PIN nahezu verhindern.

# G 5.95 Abhören von Raumgesprächen über Mobiltelefone

Mobiltelefone können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Im einfachsten Fall wird z. B. bei einer Besprechung ein Mobiltelefon, mit dem eine Verbindung zu einem interessierten Mithörer aufgebaut wurde, unauffällig in einem Raum platziert. Die meisten Mobiltelefone sind mit einer Freisprechfunktion ausgestattet und können problemlos Gespräche im gesamten Raum erfassen. Ferner können die Mobiltelefone so eingestellt werden, dass sie ohne Nutzerinteraktion Anrufe automatisch annehmen, und so in der Nähe stattfindende Gespräche abhören können. Auch wenn die Akkukapazität begrenzt ist, reichen die mehrtägige Bereitschaftszeit und die mehrstündige Gesprächszeit für einen wirkungsvollen Abhörversuch aus.

Mobiltelefone können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Im einfachsten Fall wird z. B. bei einer Besprechung ein Mobiltelefon, mit dem eine Verbindung zu einem interessierten Mithörer aufgebaut wurde, unauffällig in einem Raum platziert. Die meisten Mobiltelefone sind mit einer Freisprechfunktion ausgestattet und können problemlos Gespräche im gesamten Raum erfassen. Ferner können die Mobiltelefone so eingestellt werden, dass sie ohne Nutzerinteraktion Anrufe automatisch annehmen, und so in der Nähe stattfindende Gespräche abhören können. Auch wenn die Akkukapazität begrenzt ist, reichen die mehrtägige Bereitschaftszeit und die mehrstündige Gesprächszeit für einen wirkungsvollen Abhörversuch aus.

Raumgespräche können auch oft dadurch einfach abgehört werden, in dem ein Mobiltelefon mit aktivierter Diktiergerätefunktion geschickt platziert wird.

Für diesen Zweck können aber auch Mobiltelefone benutzt werden, denen nicht anzusehen ist, dass sie eingeschaltet sind. Das Mobiltelefon dient dabei als Abhöranlage, die über das Telefonnetz von jedem Ort der Welt aktiviert werden kann, ohne dass dies am Mobiltelefon erkennbar wäre. Es waren auch Geräte bekannt, bei denen diese Funktion mittels zusätzlicher Schaltungseinbauten realisiert ist. Diese Manipulation war durch eine Sichtprüfung nach Zerlegen des Gerätes oder durch spezielle Untersuchungsmethoden relativ leicht nachzuweisen. Der Betrieb solcher Geräte ist in Deutschland illegal. Neben diesen technischen Vorkehrungen zum Abhören von Raumgesprächen über Mobiltelefone kann der gleiche Effekt durch geeignete Applikationen (Apps) von Smartphones erzielt werden (siehe G 5.96 *Manipulation von Mobiltelefonen*).

# G 5.96 Manipulation von Mobiltelefonen

Der in G 5.95 *Abhören von Raumgesprächen über Mobiltelefone* erwähnte Einbau zusätzlicher elektronischer Schaltungen ist eine typische Hardware-Manipulation. Damit diese Manipulation durchgeführt werden kann, muss sich das zu manipulierende Gerät für eine gewisse Zeit im Besitz des Angreifers befinden.

Täter können Mobiltelefone oder Smartphones aber auch dadurch für Abhörangriffe nutzbar machen, dass sie die geräteinterne Steuersoftware (Firmware) oder eine Applikation manipulieren. Derartige Manipulationen sind meistens weitaus schwerer zu entdecken als Hardware-Manipulationen.

Eine versteckte, nicht dokumentierte Abhörfunktion könnte schon bei der Entwicklung des Gerätes (bewusst oder unbewusst) in die Steuersoftware einprogrammiert sein

Denkbar ist jedoch auch eine nachträgliche Veränderung der Steuersoftware durch einen Dritten, z. B. wenn das Gerät bei einer Reparatur oder aus sonstigen Gründen (Verlust, Entwendung) für den Benutzer (kurzzeitig) nicht kontrollierbar ist. Die Manipulation erfordert aber eingehende Spezialkenntnis, die neben den Firmware-Entwicklern nur wenigen Angreifern zugänglich ist. Für Außenstehende ist diese Manipulation praktisch nicht nachweisbar.

Durch die Erweiterung der Menüfunktionen der Mobiltelefone mittels "SIM-Toolkit" und einer neuen Generation von SIM-Karten, die diese Funktionalität unterstützen, werden Mobiltelefone noch flexibler. Ein so ausgestattetes Mobiltelefon lässt sich per Mobilfunk vom Service-Provider mit neuen Funktionen programmieren. So kann der Kartenanbieter zum Beispiel die Menüstruktur individuell an die Bedürfnisse eines Kunden anpassen.

Dies birgt nun erst recht die Gefahr der Firmware-Manipulation, da Funktionen bereits serienmäßig in der Firmware enthalten sein können, die auch für den Umbau als Lauschsender notwendig sind. Die Wahrscheinlichkeit steigt, dass Funktionen von "außen" aufgerufen werden können, die das Mobiltelefon zu einem Lauschsender umfunktionieren. Denkbar ist auch, dass diese Funktionen ein- und ausschaltbar sind.

Bei Smartphones manipulieren Angreifer eher die Applikationen als die Firmware, da dies deutlich einfacher ist. Denn viele Applikationen haben großzügig eingeräumte Rechte über die Schnittstellen des Smartphones. Sie sind beispielsweise ständig mit dem Internet verbunden und dürfen Umgebungsgeräusche aufnehmen. Ein Angreifer kann unbemerkt über das Internet diese Funktion starten und so nahezu risikolos einen Abhörangriff erfolgreich ausführen. Zudem kann die Abhörfunktion ereignisbasiert eingeschaltet werden, z. B. zu einer gewissen Uhrzeit, wenn sich das Mobiltelefon an einem bestimmten Ort befindet oder wenn ein Telefonat geführt wird. Auch reguläre Applikationen können durch Schwachstellen für Angreifer aus dem Internet gegebenenfalls durch Schwachstellen so manipuliert werden, dass mit ihnen Raumgespräche abgehört und vertrauliche Daten abgeschöpft werden können.

# G 5.97 Unberechtigte Datenweitergabe über Mobiltelefone

Mobiltelefone ermöglichen den Datentransport von einem IT-System, z. B. einem PC oder Notebook, zum anderen, ohne dass eine drahtgebundene Verbindung hergestellt werden muss.

Informationen können dort, wo ein offener Zugang zu IT-Systemen möglich ist, unauffällig abgefragt und übermittelt werden. Mithilfe eines Mobiltelefons mit angeschlossenem oder eingebautem Modem können gespeicherte Informationen drahtlos an nahezu jeden beliebigen Ort der Welt übertragen werden. Heutige Smartphones sind nahezu ständig mit dem Internet verbunden. Sie nutzen WLAN und schnelle Datendienste wie HSDPA und LTE und können daher wesentlich einfacher große Datenmengen unberechtigt weitergeben.

Diese Art der unbefugten Datenweitergabe kann sowohl mit einem eigens dafür mitgebrachten oder sogar mit einem internen Mobiltelefon durchgeführt werden. Auf diese Weise lassen sich große Datenbestände unbemerkt nach außen schaffen. Durch neue Technologien wird die Übertragung von großen Datenmengen über Mobiltelefone zunehmend attraktiver. Bei GSM beträgt die maximale Datenübertragungsrate derzeit 14,4 Kbit/s. Neuere Protokolle erreichen wesentlich höhere Bandbreiten. So ist mit GPRS eine Übertragung von 53,6 Kbit/s, mit UMTS eine Übertragung von 384 Kbit/s und mit LTE oder LTE-Advances eine Übertragung von 300 Mbit/s bzw. 900 Mbit/s möglich.

Für eine unberechtigte Datenweitergabe kann ein eigens dafür mitgebrachtes oder sogar ein internes Mobiltelefon eingesetzt werden. Eine nachträgliche Überprüfung ist nicht immer möglich, da die Verbindungsdaten beim Netzbetreiber schon gelöscht sein können.

**Beispiele:**

- Ein Mitarbeiter eines Unternehmens wird aus einer Besprechung mit einem Externen gerufen, um ein wichtiges Telefonat entgegenzunehmen. Der Externe nutzt die kurze Zeitspanne ohne Beaufsichtigung, um den im Besprechungsraum aufgestellten PC mit seinem GSM-Modem zu verbinden. Anschließend initiiert er eine Datenübertragung zu einem Anschluss seiner Wahl.
- Viele Smartphones können als WLAN-Hotspots (sogenanntes "Tethering") eingesetzt werden. Ein Angreifer könnte in einem Raum (beispielsweise eine Hotelhalle), in dem es regulär einen WLAN-Zugang gibt, mit einem solchen Smartphone das Funksignal des eigentlichen WLANs ersetzen. So kann er alle Datenverbindungen der Teilnehmer in diesem Raum, die nun über dieses Smartphone mit dem Internet verbunden sind, mitschneiden und abhören.

# G 5.98 Abhören von Mobiltelefonaten

Die einfachste Art, ein über ein Mobiltelefon geführtes Gespräch mitzuhören, ist in unmittelbarer Nähe zuzuhören. Sehr häufig kann man erleben, wie in der Öffentlichkeit laut telefoniert wird und dabei sehr viele Interna preisgegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*).

Generell sind mit unterschiedlich hohem Aufwand aber auch verschiedene technische Abhörmethoden denkbar.

Wenn sich z. B. ein Angreifer Zugang zu den technischen Einrichtungen des Netzbetreibers (Leitungen, Vermittlungseinrichtungen, Basisstationen) verschaffen kann, ist er in der Lage, alle Telefongespräche abzuhören, die über diese Einrichtungen geführt werden. Dies gilt sowohl für Verbindungen im Mobilfunknetz als auch im Festnetz. Ein gezieltes Abhören von Gesprächen, die einer bestimmten Rufnummer zugeordnet sind, ist aber angesichts der riesigen Datenflut extrem aufwendig.

Werden die Verbindungen über leitungsgebundene Wege von der Basisstation zu der Mobilfunkvermittlung geführt, ist ein physischer Angriff auf die Leitungswege erforderlich. Ist eine Basisstation über eine unverschlüsselte Richtfunkverbindung an die Mobilfunkvermittlung angebunden, was bei einigen Netzbetreibern der Fall sein kann, besteht die Möglichkeit, diese Funksignale mit Antennen und Spezialempfängern unbemerkt aufzufangen und abzuhören. Die Gefährdung kann sich gegebenenfalls dadurch erhöhen, dass auf diesen Richtfunkstrecken alle Telefonate der angebundenen Basisstation übertragen werden.

Auch im Festnetz werden Telefongespräche gebündelt über Richtfunkstrecken übertragen. Da diese Übertragung in der Regel unverschlüsselt erfolgt, sind die übertragenen Gespräche mit einigem technischen Aufwand auch dort abhörbar.

Die Funkübertragung zwischen dem Mobiltelefon und der Basisstation wird in Deutschland in allen GSM-Mobilfunknetzen verschlüsselt. Diese Verschlüsselung gilt jedoch als gebrochen: Mit im Internet erhältlichen Anleitungen und mit Geräten aus dem Elektronikfachmarkt kann relativ leicht die Verbindung zwischen Mobiltelefon und Basisstation abgehört werden. Es gibt spezielle Angriffsgeräte (IMSI-Catcher), die die Schwäche der einseitigen Authentisierung im GSM-Netz (nur Mobiltelefon gegenüber Basisstation) ausnutzen, indem sie den Mobiltelefonen eine Basisstation vortäuschen, die Verschlüsselung abschalten und Klarbetrieb vorgeben. Abhängig von gesetzlichen Regelungen kann in einigen Ländern die Übertragungsverschlüsselung auch ganz abgeschaltet sein. Auch andere Sicherheitsparameter wie die Häufigkeit des Schlüsselwechsels können schwächer sein.

Andere denkbare Möglichkeiten, um diese Verschlüsselung abzuschalten, sind technische Manipulationen am Mobiltelefon oder an technischen Einrichtungen des Netzbetreibers.

Die Verschlüsselung im UMTS-Netz ist im Vergleich zum GSM-Netz deutlich sicherer. Es sind bei guter Implementierung der Verschlüsselung keine erfolgreichen Angriffe auf die Verbindung zwischen Mobiltelefon und Basisstation bekannt. Zudem ist die Authentisierung im UMTS-Netz zwischen Mobiltelefon und Basisstation zertifikatsgestützt. Ohne Besitz dieser Zertifikate sind IMSI-Catcher in UMTS-Netzen daher nicht einsetzbar. Jedoch lassen sich Mo-

biltelefone mit einigem Aufwand so manipulieren, dass sie vom UMTS-Netz auf das GSM-Netz umschalten, wodurch dann wieder alle bekannten Angriffe auf das GSM-Netz möglich sind.

# G 5.99 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen

Bei der Mobil-Kommunikation lässt sich auf der Funkstrecke nicht physikalisch verhindern, dass mit entsprechend technischem Aufwand die übertragenen Signale unbefugt mitgehört und aufgezeichnet werden. Darum hätte ein Angreifer nicht das bei leitungsgebundener Kommunikation bekannte Zugriffsproblem.

Ein zweites, generell bei den meisten Funkdiensten auftretendes Problem resultiert daraus, dass die mobilen Kommunikationspartner aus technischen Gründen geortet werden müssen, um erreichbar zu sein.

Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls - im Zuge des Verbindungsaufbaus - Informationen über ihren Standort ab. Diese Standort-Informationen könnten durch den Netzbetreiber oder Dienstbetreiber zur Bildung von Bewegungsprofilen verwendet werden.

Die meisten Mobiltelefone und Smartphones haben das sogenannte "Radio Resource Location Services Protocol" (RRLP) umgesetzt, welches der Ortung eines Mobilfunkteilnehmers bei Notrufen dient und das sogar den gegebenenfalls eingebauten GPS-Empfänger zur genaueren Ortung nutzen kann.

In der Regel kann RRLP nicht abgeschaltet werden. Diese Informationen liegen beim Netzbetreiber vor.

# G 5.100 Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes/Domino

Für Lotus Notes/Domino-Datenbanken können aktive Komponenten definiert werden, die beim Eintreten gewisser Ereignisse, wie der Eingabe von Daten in definierte Felder, ausgeführt werden. Die aktiven Komponenten bestehen dabei z. B. aus Lotus Script- oder auch Java-Programmen und werden *Agenten* genannt. Durch die Ausführung eines Agenten können wiederum andere Agenten gestartet werden (z. B. wenn ein Agent Daten in eine andere Datenbank kopiert und diese Aktion das Ausführen von Agenten der Zieldatenbank auslöst). Generell kann zwischen serverseitiger und clientseitiger Ausführung von Agenten unterschieden werden, es sind jedoch immer beide Varianten möglich.

Darüber hinaus können sowohl in Lotus Notes Clients wie auch in zum Zugriff auf Lotus Domino genutzten Browsern oder fremden Clients aktive Inhalte zur Ausführung kommen.

Damit ist die Möglichkeit eines Angriffs auf die Lotus Notes/Domino-Plattform durch das Einschleusen schädlicher aktiver Inhalte (*malicious active content*) gegeben. Vielfach materialisiert sich diese Gefährdung nur bei fehlerhafter Konfiguration des Lotus Domino Servers oder des genutzten Clients. Diese Situationen werden durch die Gefährdungen G 3.46 *Fehlerhafte Konfiguration eines Lotus Domino Servers* und G 3.113 *Fehlerhafte Konfiguration eines Lotus Notes Clients oder eines Fremdclients mit Zugriff auf Lotus Domino* beschrieben.

Es ist jedoch möglich, dass auch bei richtiger Konfiguration aufgrund von Schwächen der genutzten Skriptsprachen oder der Software (siehe G 4.22 *Software-Schwachstellen oder -Fehler*) ein Missbrauch aktiver Inhalte erfolgt. Gleichfalls ist möglich, dass eine kaskadierende Ausführung von Agenten durch nicht ausreichend modellierte Abhängigkeiten aktiver Inhalte zu Problemen führt, ohne dass direkt eine fehlerhafte Konfiguration ursächlich ist.

Einen Sonderfall stellt die Gefährdung G 5.111 *Missbrauch aktiver Inhalte in E-Mails* dar, die die spezielle Situation beschreibt, in der schädliche aktive Inhalte über E-Mail eingebracht werden.

# G 5.101 Hacking Lotus Notes/Domino

Die in den Datenbanken eines Lotus Domino Servers gespeicherten Daten können auch für den öffentlichen Zugriff aus dem Internet bereitgestellt werden. Dies stellt besondere Anforderungen an die Sicherheit des dazu benutzten Lotus Domino Servers. Sicherheitslücken können in diesem Fall dazu führen, dass ein Angreifer nicht nur unerlaubt auf den Lotus Domino Server selbst zugreifen kann, sondern unter Umständen auch in der Lage ist, in das dahinter liegende interne Netz einzudringen.

Nachfolgend sind einige Problemfelder und potentielle Sicherheitslücken aufgeführt, die insbesondere beim öffentlichen Zugriff auf einen Lotus Domino-Server aus dem Internet beachtet werden müssen:

- Ein Lotus Domino Server ist ein komplexes System. Ein Serververbund erhöht die Komplexität weiter. Durch die Komplexität (auch der sicherheitsrelevanten Einstellungen) kann es zu Fehlkonfigurationen und somit auch zu Sicherheitslücken kommen.
- Durch den großen Funktionsumfang eines Lotus Domino Servers und die mögliche Einbindung in entsprechende Hintergrundsysteme können Sicherheitslücken unter Umständen von einem Lotus Domino Server auf die Hintergrundsysteme durchschlagen. Dabei genügt es in der Regel, eine einzelne Schwachstelle in einem einzelnen Funktionspaket auszunutzen.
- Ist der Web-Zugriff auf einen Lotus Domino Server aktiviert, betrifft dies immer *alle* Datenbanken auf dem jeweiligen Server. Dies kann leicht für vorsätzliche Angriffe, insbesondere gegen Standard-Datenbanken, ausgenutzt werden, wenn nicht für jede Datenbank sichere Zugriffsrechte vergeben sind.
- Ein bekanntes Verfahren zum Hacking eines Lotus Domino Servers ist der Zugriff per HTTP auf *names.nsf* unter Verwendung eines legitimen Benutzer-Accounts und das Auslesen der Personendokumente inklusive Passwort-Hashes, aus denen mittels entsprechender Crack-Programme die Passwörter ermittelt werden.

# G 5.102 Sabotage

Sabotage bezeichnet die mutwillige Manipulation oder Beschädigung von Sachen mit dem Ziel, dem Opfer Schaden zuzufügen. Besonders attraktive Ziele können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

Die komplexe Infrastruktur eines Rechenzentrums kann durch gezielte Beeinflussung wichtiger Komponenten, gegebenenfalls durch Täter von außen, vor allem aber durch Innentäter, punktuell manipuliert werden, um Betriebsstörungen hervorzurufen. Besonders bedroht sind hierbei nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur sowie zentrale Versorgungspunkte, die organisatorisch oder technisch gegebenenfalls auch nicht überwacht werden und für Externe leicht und unbeobachtet zugänglich sind.

**Beispiele:**

- In einem großen Rechenzentrum führte die Manipulation an der USV zu einem vorübergehenden Totalausfall. Der Täter, er wurde ermittelt, hatte wiederholt die USV von Hand auf Bypass geschaltet und dann die Hauptstromversorgung des Gebäudes manipuliert. Der Totalausfall - insgesamt fanden in drei Jahren vier Ausfälle statt - führte partiell sogar zweimal zu Hardware-Schäden. Die Betriebsunterbrechungen dauerten zwischen 40 und 130 Minuten.
- Innerhalb eines Rechenzentrums sind auch sanitäre Einrichtungen untergebracht. Durch Verstopfen der Abflüsse und gleichzeitiges Öffnen der Wasserzufuhr entstehen durch Wassereinbruch in zentralen Technikkomponenten Schäden, die zu Betriebsunterbrechungen des Produktivsystems führen.
- Für elektronische Archive stellt Sabotage ein besonderes Risiko dar, da hier meist auf kleinem Raum viele schützenswerte Dokumente verwahrt werden. Dadurch kann unter Umständen durch gezielte, wenig aufwendige Manipulationen ein großer Schaden verursacht werden.

# G 5.103 Missbrauch von Webmail

Wenn Benutzerangaben nicht ausreichend geprüft werden, kann sich ein Angreifer eine E-Mail-Adresse auf den Namen einer anderen Person besorgen und damit z. B. durch Spammails oder Beschimpfungen unter diesem Namen deren Ruf unterminieren. Wenn die E-Mail-Adressen bei einem Anbieter frei gewählt werden können, kann sich ein Angreifer eine Adresse aussuchen, mit der andere Benutzer bestimmte Assoziationen verbinden und diese damit zu unvorsichtigem Verhalten animieren.

Bei vielen Webmail-Anbietern ist der Benutzername für den Zugriff auf die Postfächer identisch mit der E-Mail-Adresse bzw. lässt sich daraus einfach ableiten. Wenn dann das Passwort nicht gut genug gewählt worden ist oder beliebig viele Fehleingaben möglich sind, kann ein Angreifer durch simples Ausprobieren das Passwort herausbekommen und hat dann freien Zugriff auf das Benutzerkonto.

Durch falsch verstandene Benutzerfreundlichkeit wird es potentiellen Angreifern auch teilweise sehr einfach gemacht, sich ein Passwort und damit vollen Zugriff für ein fremdes Postfach geben zu lassen. Ein typisches Beispiel ist ein Mailprovider, der auf der Einstiegsseite schon einen Link "Passwort vergessen?" anbietet, durch den man dann zu einer Seite weitergeleitet wird, auf der nach einem vorher vereinbarten, nicht schwer zu erratenen Angabe des Postfach-Inhabers gefragt wird. Beliebt ist hier das Geburtsdatum, bei dessen Erraten auch noch durch Angaben wie "Der Monat ist nicht korrekt" weitergeholfen wird.

**Beispiele:**

- In dem Beispiel in G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon und Kamera* wird geschildert, wie eine deutsche Politikerin in einer gefälschten Virenwarnung per E-Mail aufgefordert wurde, ein als Anlage mitgeschicktes Schutzprogramm zu öffnen, welches aber ein Trojanisches Pferd enthielt. Diese E-Mail hatte den Absender *support@xyz.de* und kam aus der Domain ihres E-Mail-Providers XYZ. Eine E-Mail von einem Absender, den sie als unbekannt eingestuft hätte, hätte sie wahrscheinlich nicht geöffnet.
- Im Webmail-Angebot Hotmail sind bereits mehrmals Sicherheitslücken bekannt geworden. Zu Problemen führt insbesondere in E-Mails eingebettetes Javascript, das dann beim Lesen der E-Mail im Browser des Empfängers ausgeführt wird. Dadurch kann der Benutzer beispielsweise durch einen Angreifer dazu aufgefordert werden, sein Passwort erneut einzugeben und dieses anschließend an den Angreifer übermittelt wird. Da Javascript auf mehrere unterschiedliche Arten in HTML-formatierte E-Mails eingebettet werden kann, gab es in der Vergangenheit Lücken beim Herausfiltern dieser aktiven Inhalte.

Bei aktuellen Virenwarnungen kann es einige Stunden dauern, bis die Hersteller der Virenschutzprogramme die ersten wirksamen Updates bereit stellen können und diese erfolgreich auch auf allen IT-Systemen installiert sind. E-Mails, die in dieser Zeit auf dem E-Mail-Server eintreffen, können dort solange in Quarantäne genommen werden. Wenn nicht gleichzeitig auch verhindert wird, dass E-Mails über Webmail-Accounts abgerufen werden, können hierüber PCs und Server im LAN infiziert werden.

**Beispiel:**

- Ende September 2001 verursachte der Virus *Nimda* etliches an Ärger und Aufregung. Nimda ist ein Wurm mit mehreren Schadfunktionen. Er ver-

breitet sich mittels Anhang von E-Mails, über eine bekannte Schwachstelle des Internet Information Server (IIS) von Microsoft sowie über freigegebene Laufwerke. Es dauerte teilweise bis zu 24 Stunden, ehe nach Bekanntwerden des ersten Auftretens wirksame Signaturen für Virenschutzprogramme zur Verfügung standen. In einigen großen Unternehmen infizierten Benutzer ihre PCs über Webmail mit Nimda. Über diese wurden dann IIS-Webserver innerhalb des Firmennetzes infiziert, was wiederum zu erheblichen Beeinträchtigungen im LAN führte.

# G 5.104 Ausspähen von Informationen

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen. Da sensitive Daten oft nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischen Weg ausgespäht werden.

**Beispiele:**

- Die meisten IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Benutzer-ID- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist es einem Angreifer möglich, dieses auszulesen.
- Um mit einer ec- oder Kreditkarte Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass ein Angreifer einem Kunden bei der Eingabe der PIN ohne Mühe über die Schulter schauen kann. Wenn er ihm hinterher die Karte stiehlt, kann er damit das Konto plündern. Der Kunde hat anschließend außerdem das Problem, dass er nachweisen muss, nicht fahrlässig mit seiner PIN umgegangen zu sein, sie also beispielsweise nicht auf der Karte notiert hat.
- Um Zugriffsrechte auf einem Benutzer-PC zu erhalten oder diesen anderweitig zu manipulieren, kann ein Angreifer dem Benutzer ein Trojanisches Pferd schicken, das er als vorgeblich nützliches Programm einer E-Mail beigefügt hat. Erfahrungsgemäß öffnen Benutzer trotz aller Aufklärung sogar dann E-Mail-Anhänge, wenn diese nicht erwartet wurden oder merkwürdige Namen tragen. Neben unmittelbaren Schäden können über Trojanische Pferde Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausspäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.
- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können Kollegen, aber auch Besucher unter Umständen Gespräche mitgehören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

# G 5.105 Verhinderung der Dienste von Archivsystemen

Die Dienste eines elektronischen Archivs bestehen aus den folgenden Grundfunktionen:

- Erfassen und Indizieren der zu archivierenden Dokumente,
- Verwalten und Speichern der Dokumente,
- Suchen und Finden archivierter Dokumente,
- Visualisieren und Reproduzieren der Dokumente sowie
- Pflegen und Administrieren des Archivsystems.

Wenn die Dienste eines Archivsystems gestört werden, können Schäden entstehen, wie die folgenden Beispiele erläutern sollen:

- Wird die Indizierung von archivierten Daten verhindert oder gestört, z. B. durch die Angabe falscher Kontextdaten, so hat das unter Umständen zur Folge, dass Daten später gar nicht oder nur unter erheblichem Aufwand wiedergefunden werden können.
- Wird die Archivierung neuer Daten verhindert oder blockiert, indem z. B. durch einen Denial-of-Service-Angriff die Netzverbindung des Archivsystems blockiert wird, so kann das zur Folge haben, dass je nach Datenaufkommen ein erheblicher Rückstau entsteht, der nicht durch Backup gesichert ist. Bei einem Systemausfall wäre dann mit dem Verlust derjenigen Dokumente zu rechnen, die noch zur Archivierung anstehen. Wenn ein Archivsystem ausgewählt wird, das keine für den Benutzer sichtbare Archivbestätigung erzeugt, so besteht das Risiko, dass eventuelle Dokumentverluste zunächst unerkannt bleiben. Wenn andererseits ein System mit Archivbestätigung eingesetzt wird, so kann ein Ausbleiben der Bestätigung nachfolgende Geschäfts- oder Verwaltungsvorgänge ebenfalls verzögern.
- Wird die Reproduktion archivierter Daten unterbunden, gestört oder verzögert, so kann das zur Folge haben, dass erforderliche Dokumente nicht termingerecht beigebracht werden können, wodurch sich wirtschaftliche Schäden oder rechtliche Nachteile ergeben können.
- Wenn die Administration des Archivsystems behindert oder verzögert wird, z. B. durch Überlastung des Personals mit Anfragen, so kann es vorkommen, dass Personen, denen der Zugriff gesperrt werden soll, weiterhin Zugriff auf das Archiv haben und dort unberechtigt Dokumente einstellen oder abrufen.
- Durch Behinderung der Administration können auch dann Schäden hervorgerufen werden, wenn dadurch die Wartung des Archivsystems beeinträchtigt oder verzögert wird. Möglicherweise können dadurch sicherheitsrelevante Software-Updates nicht zeitgerecht eingespielt oder nicht ausreichend getestet werden.

# G 5.106 Unberechtigtes Überschreiben oder Löschen von Archivmedien

Auf Archivmedien sollen wichtige Daten langfristig und unverändert gespeichert werden. Daher dürfen diese nicht unberechtigt überschrieben, gelöscht oder anderweitig verändert werden. Unberechtigtes Löschen ist dann möglich, wenn Benutzerrechte falsch vergeben worden sind, d. h. wenn

- Benutzer das Recht zum "Löschen" haben, sie aber aufgrund der ihnen zu Verfügung stehenden Informationen keine sinnvolle Entscheidung treffen können, ob Datensätze gelöscht werden dürfen oder nicht, oder
- durch fehlerhafte Administration Benutzer fälschlicherweise die Berechtigung zum "Löschen" haben.

Hierbei sind wiederbeschreibbare Medien und WORM-Medien zu unterscheiden:

- Bei wiederbeschreibbaren Medien ist ein physikalisches Löschen oder Überschreiben von Datensätzen grundsätzlich möglich.
- Bei WORM-Medien ist ein physikalisches Löschen oder Überschreiben grundsätzlich nicht möglich. Allerdings bieten Archivierungssysteme in der Regel die Möglichkeit, Datensätze logisch als gelöscht zu markieren. Diese Datensätze werden beim Umkopieren auf einen neuen Datenträger dann nicht mehr mitkopiert. Sie werden also erst im Moment des Kopierens auf den neuen Datenträger aus den Datenbeständen entfernt.

In beiden Fällen kann es also bei falschem Umgang mit den Medien zu einem Integritätsverlust der gespeicherten Informationen und Daten kommen (siehe hierzu auch G 5.85 *Integritätsverlust schützenswerter Informationen*).

# G 5.107 Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

Outsourcing-Dienstleister haben in der Regel mehrere Kunden. Es ist daher immer möglich, dass sich darunter auch Wettbewerber befinden. Dies ergibt sich vor allem bei großen Outsourcing-Dienstleistern und solchen, die spezielle Anforderungsbereiche wie Sicherheitsdienstleistungen abdecken. Wenn ein Outsourcing-Partner parallel die Aufträge zweier Konkurrenzorganisationen bearbeitet, kann es zu Interessenskonflikten kommen, sofern keine strikte Trennung der Auftragsbearbeitung vorgenommen wird (Mandantenfähigkeit des Outsourcing-Dienstleisters).

In derartigen Situationen könnten möglicherweise Arbeitsergebnisse und Erkenntnisse aus der Projektbearbeitung durch Mitarbeiter oder Unterauftragnehmer des Dienstleisters absichtlich dem Mitbewerber direkt verfügbar gemacht werden. Ein so entstandener Schaden ist in aller Regel nicht mehr zu beheben, auch wenn einzelne Personen oder der Outsourcing-Dienstleister als ganzes später juristisch zur Verantwortung gezogen werden kann.

Werden im Rahmen des Outsourcing-Vorhabens personenbezogene Daten beim Dienstleister verarbeitet oder gespeichert, so müssen auch zusätzliche Datenschutzgesichtspunkte beachtet werden. Werden etwa Kundeninformationen eines Auftraggebers kompromittiert und veröffentlicht, so besteht die Gefahr, dass das Vertrauensverhältnis zwischen dem Auftraggeber und seinen Kunden nachhaltig gestört wird.

# G 5.108 Ausnutzen von systemspezifischen Schwachstellen des IIS

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.109 Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.110 Web-Bugs

Als Web-Bugs werden in E-Mail oder WWW-Seiten eingebettete Bilder bezeichnet, die beim Öffnen von einem fremden Server nachgeladen werden. Diese Bilder können sehr klein sein, beispielsweise ein mal ein Pixel große Minigrafiken. Die Bilder sind so eingebettet, dass sie im allgemeinen nicht sichtbar sind, aber beim Laden vom Ursprungsserver die Ausführung eines Skripts oder Programms veranlassen.

Werden Web-Bugs in HTML-formatierte E-Mails eingebettet, kann dadurch der Absender z. B. erkennen, welche E-Mail wann gelesen wurde. Beispielsweise im Zusammenhang mit unverlangt versendeten Massen-E-Mails kann dies unerwünscht sein.

Bei der Nutzung des World Wide Web müssen Benutzer grundsätzlich damit rechnen, dass außer zu dem Server, dessen WWW-Angebot sie gerade nutzen, auch zu anderen Servern Verbindungen aufgebaut werden. Dies ist zum Beispiel der Fall, wenn von einer WWW-Seite aus Bilder referenziert werden, die auf einem anderen Server liegen. Obwohl dies im Prinzip ein normaler Vorgang ist, können unter Umständen über diesen Mechanismus ungewollt Informationen an Dritte übertragen werden, wie das unten beschriebene Beispiel zeigt. Insbesondere können hierdurch vertrauliche Daten des Benutzers oder des Server-Betreibers kompromittiert werden.

**Beispiel:**

- Eine Universität verwendet ein frei im Internet erhältliches Software-Paket, um dynamische Inhalte auf dem WWW-Server anzubieten (CGI-Skripte). Abhängig von den Eingaben des Benutzers generiert die Software auf dem WWW-Server passende Antwort-Seiten und schickt sie an den Benutzer. Neben den eigentlichen Inhalten enthalten die generierten HTML-Seiten aber auch Verweise auf Bilder, die sich nicht auf dem Server der Universität, sondern des Programmierers der CGI-Skripte befinden. Als Folge werden diese Bilder jedes Mal vom Server des Programmierers abgerufen, wenn ein Benutzer auf das Internet-Angebot der Universität zugreift. Auf diese Weise erhält der Programmierer ausführliche Informationen über die Nutzung des von ihm entwickelten Software-Pakets, aber leider auch über die Nutzung des Internet-Angebots der Universität.

# G 5.111 Missbrauch aktiver Inhalte in E-Mails

Immer mehr E-Mails sind heutzutage auch HTML-formatiert. Einerseits ist dies oft lästig, weil nicht alle E-Mail-Clients dieses Format anzeigen können. Andererseits kann dies auch dazu führen, dass bereits bei der Anzeige solcher E-Mails auf dem Client ungewollte Aktionen ausgelöst werden, da HTML-Mail z. B. eingebetteten JavaScript- oder VisualBasic-Skript-Code enthalten kann.

Durch Kombination verschiedener Sicherheitslücken in E-Mail-Clients und Browsern ist es in der Vergangenheit immer wieder zu Sicherheitsproblemen mit HTML-formatierten E-Mails gekommen (siehe auch G 5.110 *Web-Bugs*). Ein Beispiel hierfür findet sich unter anderem im CERT-Advisory CA-2001-06 (unter *http://www.cert.org/advisories/CA-2001-06.html*).

# G 5.112 Manipulation von ARP-Tabellen

Im Gegensatz zu einem Hub kann bei einem Switch grundsätzlich die Kommunikation zwischen zwei Stationen von keiner der anderen Stationen abgehört werden. Zu diesem Zweck pflegt der Switch eine Tabelle, die die MAC-Adressen der beteiligten Stationen den verschiedenen Ports zuordnet. Datenpakete beziehungsweise Ethernet-Frames, die an eine bestimmte MAC-Adresse adressiert sind, werden nur an den Port weitergeleitet, an dem der betreffende Rechner angeschlossen ist.

Doch nicht nur der Switch pflegt eine Tabelle mit MAC-Adressen, sondern auch die beteiligten Rechner. Mit ARP-Anfragen können diese ARP-Tabellen am beteiligten Rechner gefüllt werden. Ziel des ARP-Spoofings ist es, die ARP-Tabellen zu manipulieren (ARP-Cache-Poisoning). Dazu schickt ein Angreifer eine ARP-Antwort an das Opfer, in der er seine eigene MAC-Adresse als die des Routers ausgibt, der für das betreffende Subnetz als Standard-Gateway fungiert. Sendet das Opfer anschließend ein Paket zum eingetragenen Standard-Gateway, landet dieses Paket in Wirklichkeit beim Angreifer. Auf die selbe Weise wird der ARP-Cache des Routers so manipuliert, dass Ethernet-Frames, die eigentlich an das Opfer adressiert wurden, in Wirklichkeit beim Angreifer landen. Auf einschlägigen Internet-Seiten sind eine Reihe von Tools verfügbar, die diese Angriffsmethode ermöglichen.

MAC-Flooding ist eine Angriffsmethode, die die Funktionsweise eines Switches beeinflusst. Switches erlernen angeschlossene MAC-Adressen dynamisch. Die MAC-Adressen werden in der Switching-Tabelle gespeichert. Der Switch weiß dadurch, an welchen Ports die entsprechenden MAC-Adressen angeschlossen sind.

Wenn nun eine angeschlossene Station mit Hilfe eines geeigneten Tools eine Vielzahl von Paketen mit unterschiedlichen Quell-MAC-Adressen sendet, speichert der Switch diese MAC-Adressen in seiner Switching-Tabelle. Sobald der Speicherplatz für die Switching-Tabelle gefüllt ist, sendet ein Switch sämtliche Pakete an alle Switch-Ports. Durch dieses "Fluten" der Switching-Tabelle mit sinnlosen MAC-Adressen kann ein Switch nicht mehr feststellen, an welche Ports tatsächliche Ziel-MAC-Adressen angeschlossen sind. Diese Angriffsmethode wird verwendet, um das Mitlesen von Paketen in geswitchten Netzen zu ermöglichen. Es sind frei verfügbare Tools auf einschlägigen Seiten im Internet verfügbar, die auf einem Switch über 155.000 MAC-Adress-Einträge innerhalb einer Minute erzeugen können.

# G 5.113 MAC-Spoofing

Die MAC-Adresse ("media access control") eines Geräts ist eine vom Hersteller vorgegebene Adresse, mit der Geräte auf der OSI-Schicht 2 adressiert werden.

Verschiedene Sicherungsmechanismen auf der Netzebene (beispielsweise Port-Security bei Switches) beruhen darauf, dass eine Verbindung nur von einem Gerät mit einer bestimmten MAC-Adresse aufgebaut werden darf.

Mit Hilfe entsprechender Programme kann ein Angreifer die MAC-Adresse seines Gerätes ändern und Ethernet-Frames mit einer fremden Kennung in das Netzsegment schicken. Auf diese Weise können Sicherungsmechanismen umgangen werden, die allein auf der Verwendung einer MAC-Adresse beruhen. Der Angreifer muss sich dabei allerdings im selben Netzsegment befinden oder sogar Zugang zu demselben Switchport haben wie das Gerät, als das er sich mittels MAC-Spoofing ausgibt.

Eine Gefährdung durch MAC-Spoofing besteht auch bei drahtlosen Netzen (WLAN), bei denen am Access-Point eine entsprechende Zugangskontrolle konfiguriert wurde.

# G 5.114 Missbrauch von Spanning Tree

Das Spanning Tree Protokoll ist in IEEE 802.1d spezifiziert. Spanning Tree wird verwendet, um Schleifenbildungen innerhalb eines Netzes mit mehreren Switches zu vermeiden. Bei diesem Verfahren werden redundante Netzstrukturen ermittelt und in eine zyklenfreie Struktur abgebildet. Diese Maßnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzstruktur auf eine Baumstruktur.

In der folgenden Abbildung ist zu erkennen, dass ein Port des unteren Switches mithilfe von Spanning Tree geblockt wurde. Durch Aussenden von Bridge Protocol Data Units (BPDUs), wird eine Root-Bridge, basierend auf der eingestellten Priorität und MAC-Adresse des Switches, ermittelt. In der Abbildung stellt der Switch rechts oben die Root Bridge dar.

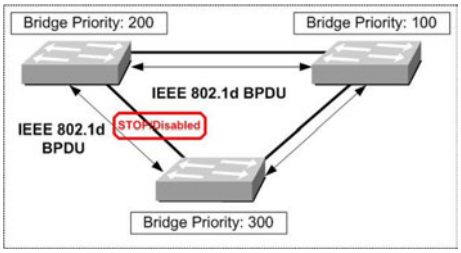



Abbildung: Spanning Tree

Spanning Tree bietet keine Authentisierung beim Austausch von BPDUs. Dies kann in geswitchten Netzen durch Angreifer ausgenutzt werden. Wenn ein Angreifer von einer am Switch angeschlossenen Station in der Lage ist, BPDUs auszusenden, wird mit Hilfe des Spanning Tree-Algorithmus die Topologie neu berechnet. Die Konvergenz zur Berechnung der Topologie-Änderung kann beim Spanning-Tree 30 Sekunden betragen. Dadurch kann bei der Aussendung von BPDUs die Verfügbarkeit des Netzes empfindlich gestört werden.

# G 5.115 Überwindung der Grenzen zwischen VLANs

Virtual LANs (VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden. Ein VLAN bildet gleichzeitig eine separate Broadcast-Domäne. Das bedeutet, dass Broadcasts nur innerhalb des VLANs verteilt werden. Ein VLAN kann sich hierbei über ein ganzes geswitchtes Netz hinziehen und braucht nicht nur auf einen einzelnen Switch beschränkt zu bleiben.

VLANs über mehrere Switches auszudehnen, wird durch unterschiedliche sogenannte Trunking-Protokolle realisiert. Hierbei wird pro Switch ein physischer Port für die Inter-Switch-Kommunikation reserviert, die logische Verbindung zwischen den Switches wird als Trunk bezeichnet. Ein Ethernet-Rahmen wird beim Informationsaustausch zwischen den Switches in das Trunking-Protokoll gekapselt. Dadurch ist der Ziel-Switch in der Lage, die Information dem entsprechenden VLAN zuzuordnen. Als Standards werden IEEE 802.1q und die proprietären Protokolle ISL (Inter Switch Link) und VTP (VLAN Trunking Protocol) des Herstellers Cisco verwendet.

Wenn sich ein Angreifer, der an einem Switch angeschlossen ist beispielsweise durch die Verwendung der Trunking-Protokolle ISL (Inter Switch Link) oder IEEE 802.1q als Switch ausgibt, ist es möglich, dadurch auf alle konfigurierten VLANs Zugriff zu erhalten und so Daten mitzulesen, die zu einem VLAN gehören, auf das der Angreifer normalerweise keinen Zugriff hat.

Mit Hilfe des proprietären Protokolls VTP werden Informationen über konfigurierte VLANs zwischen Cisco-Switches ausgetauscht. Dabei ist es möglich, die VLAN-Konfiguration eines zentralen VTP-Servers innerhalb einer VTP-Domäne auf alle beteiligten Switches zu verteilen. Dies vereinfacht zwar die Verwaltung von VLANs mit mehreren Switches, stellt gleichzeitig aber ein zusätzliches Sicherheitsrisiko dar: VTP unterstützt zwar die Authentisierung innerhalb einer VTP-Domäne, falls jedoch kein Passwort für die Authentisierung von Switches innerhalb einer Domäne gesetzt ist, kann ein Angreifer (beispielsweise auf einem eigenen Switch, der als VTP-Server konfiguriert ist) die gesamte VLAN-Architektur auf Switches der VTP-Domäne überschreiben.

# G 5.116 Manipulation der z/OS-Systemsteuerung

z/OS-Systeme lassen sich über vielfältige Schnittstellen beeinflussen, zum Beispiel über die *Hardware Management Console*, die *MVS-Master-Konsole*, den *Enhanced MVS Console Service*, Automationsverfahren, entfernte MVS-Konsole und Fernwartungszugänge. Einige Sicherheitsprobleme, die mit der Verwendung dieser Schnittstellen verbunden sein können, werden nachfolgend aufgezeigt.

**HMC (Hardware Management Console)**

Der unbefugte Zugriff auf die HMC kann zu erheblichen Sicherheitsproblemen führen. Denn von der HMC aus kann das Systemverhalten während des Betriebs beeinflusst werden. Es können einzelne LPARs (*Logical Partitions*) bis hin zu einem ganzen Rechner-Verbund neu initialisiert werden. Darüber hinaus lassen sich über die HMC auch neue *Input/Output Control Datasets* einspielen, die beim nächsten *Initial Program Load* (IPL) aktiv werden. Dadurch besteht zum Beispiel die Gefahr, dass einer LPAR eigentlich nicht zugehörige Platten zugewiesen werden.

**MVS-Master-Konsole**

z/OS-Betriebssysteme werden unter anderem über MVS-Konsolen gesteuert. Die Standard-Konsolen sind mit dem System fest verbunden und benötigen weder Kennung noch Passwort. Das bedeutet, dass Personen, die physischen Zugriff auf eine hoch autorisierte MVS-Konsole haben (z. B. auf die Master-Konsole), jedes beliebige MVS-Kommando eingeben können. In der Folge können unbefugt *Batch-Jobs* oder *Started Tasks* gestoppt oder gestartet werden. Ferner lassen sich Platten an jedem System *Online* setzen, falls sie dort generiert sind. Unter Umständen lassen sich auch über MVS-Kommandos Kanalpfade nachgenerieren, und danach Platten anhängen, die gar nicht zu dieser LPAR gehören.

**Enhanced MVS Console Service**

Über die normalen MVS-Konsolen hinaus stellt das z/OS-Betriebssystem den EMCS (*Enhanced MVS Console Service*) zur Verfügung. Dieser wird von verschiedenen Anwendungen, wie zum Beispiel TSO, CICS oder NetView, auch als Funktion angeboten. Über EMCS können dynamisch Konsolen im Rahmen eines Script-Ablaufs angelegt werden, die nahezu alle Kommandos unterstützen, die auch bei den normalen Konsolen benutzt werden können. Wird EMCS nicht oder unzureichend über RACF-Profile geschützt, kann u. U. von jedem Terminal aus das z/OS-Betriebssystem manipuliert werden.

**Gefahren bei Automation**

Automationsverfahren können so programmiert sein, dass sie durch Nachrichten ausgelöst werden. Wenn die Automationsverfahren nicht speziell geschützt werden, besteht die Gefahr, dass durch das Erzeugen einer gefälschten Nachricht Automationsfunktionen unbefugt gestartet werden.

**Entfernte MVS-Konsole**

z/OS-Systeme können an unterschiedlichen Standorten von einer zentralen Konsole aus gesteuert werden. Hierfür wird häufig ein Software-Tool eingesetzt, das es z. B. erlaubt, die LPARs der z/OS-Systeme auch über große Entfernungen zu steuern. Das Software-Tool emuliert eine MVS-Konsole auf

einem gewöhnlichen PC. Wenn der physische oder der logische Zugang zu solchen Steuerkonsolen unzureichend geschützt ist, besteht die Gefahr, dass von dort aus unbefugt Manipulationen an entfernten z/OS-Systemen vorgenommen werden.

**Fernwartungszugänge**

Eine weitere Gefährdung des z/OS-Systems kann durch unsachgemäße Konfiguration der RSF-Konsole (*Remote Support Facility*) bestehen. Ein externer Angreifer kann unter Umständen Fehler in der Konfiguration ausnutzen und sich in diese Konsole einwählen (siehe auch G 5.10 *Missbrauch von FernwartungszugängenMissbrauch von Fernwartungszugängen*).

**Beispiel:**

- RACF wurde in einem Rechenzentrum so eingerichtet, dass RACF-Kommandos auch von einer *MVS-Master-Konsole* aus eingegeben werden konnten. Ein nicht autorisierter Mitarbeiter hatte Zutritt zu dem Raum, in dem diese Konsolen standen. Als Folge konnte er das *Special*-Privileg seiner eigenen User-ID zuweisen. Dies blieb über einen längeren Zeitraum unbemerkt.

# G 5.117 Verschleiern von Manipulationen unter z/OS

Durch Änderungen an Protokolldateien oder Abschalten von Protokollierungs-Funktionen ist es möglich, Manipulationen am z/OS-System zu verschleiern.

Die meisten Komponenten des z/OS-Systems erzeugen Protokollierungsinformationen über Systemaktivitäten und -ereignisse. Diese werden regelmäßig entladen und in entsprechenden Protokolldateien (z. B. *System-Log*, *SMF-Datensätze*) gespeichert, die später ausgewertet werden können.

Protokolldateien sind veränderbar oder manipulierbar, wenn ein entsprechendes Zugriffsrecht auf die Datei besteht. Dieses kann beispielsweise durch Nachlässigkeiten bei der Systemadministration unabsichtlich vergeben worden sein, oder ein Angreifer hat sich - etwa durch entsprechende Manipulationen - dieses Zugriffsrecht verschafft.

Eine weitere Angriffsmöglichkeit auf die Systemprotokollierung besteht darin, die Erzeugung von Protokolldaten durch entsprechende Manipulation der generierenden Komponente zu verhindern. Welche *SMF-Datensätze* geschrieben werden, ist bei z/OS beispielsweise in einem *Konfigurations-Member* eingetragen. Durch Änderungen an diesem *Member* oder durch das Setzen von *Exits* lässt sich erreichen, dass bestimmte *SMF-Sätze* nicht mehr geschrieben werden. Die üblichen Sicherheitsmonitore sind nicht in der Lage, unterdrückte Verstöße zu erkennen und zu melden, wenn keine *SMF-Sätze* oder keine Systemnachrichten geschrieben werden.

**Beispiel:**

- In einem Rechenzentrum gelang es einem Anwender, das Schreiben von SMF-Datensätzen abzustellen. Daraufhin nahm er bestimmte Manipulationen vor und schaltete die SMF-Funktion anschließend wieder ein. Die in diesem Zeitraum am z/OS-System vorgenommenen Änderungen ließen sich später nicht mehr nachvollziehen, denn es fehlten die Protokolldaten. Es konnte lediglich im System-Log nachgewiesen werden, dass die Kommandos von einer MVS-Konsole aus eingegeben wurden, die mehreren Personen zur Verfügung stand.

# G 5.118 Unbefugtes Erlangen höherer Rechte im RACF

Gelingt es einem Anwender, seine Berechtigungen im z/OS-Sicherheitssystem RACF zu erhöhen, kann er unter Umständen unbefugt auf Dateien zuzugreifen und das System manipulieren.

**Trace im Netz**

Mit einem sogenannten *Trace* (Abhören des Netzverkehrs) der TCP/IP- oder TPX-Protokolle kann ein Angreifer je nach Absicherung des Netzes die Kennung und das Passwort eines Anwenders mit *Special*-Rechten ausspähen. Unter Ausnutzung dieser Kenntnisse können die eigenen Berechtigungen erhöht werden, bis zur Vergabe der *Special*-Rechte an die eigene Kennung.

**APF, SVC**

Zwei weitere Möglichkeiten, sich als Benutzer im z/OS-System höhere Berechtigungen zu verschaffen, sind das APF (*Authorized Programming Facility*) und die SVCs (*SuperVisor Calls*).

Gelingt es dem Anwender, Programme in APF-autorisierte Dateien einzustellen, oder gelingt es ihm, SVCs zu installieren, so kann er sich über diese mit *Special-* oder *Operations*-Rechten ausstatten (Manipulation des eigenen ACEE-Kontrollblocks). Diese stehen zwar nur temporär für die jeweilige Sitzung zur Verfügung, das Programm kann aber jedes Mal neu aufgerufen werden.

**Akkumulierte Rechte**

Eine weitere Gefahr besteht durch sogenannte *akkumulierte Rechte* aufgrund eines unzureichenden Berechtigungsmanagements. Typisch ist dabei das folgende Szenario:

Ein Anwender wechselt in ein neues Tätigkeitsfeld. Der Anwender erhält die Rechte, die seine neue Aufgabe fordern, ohne dass die alten Rechte gelöscht werden. Auf diese Weise akkumuliert der Anwender über einen langen Zeitraum Rechte, die erheblich über die eigentlich benötigten Berechtigungen hinaus gehen.

**Beispiel:**

- Fachwissen ist im z/OS-Umfeld wenig verbreitet. Als Folge hielten sich fachkundige z/OS-Berater über lange Zeit in einer Firma auf und akkumulierten Rechte. Ein Administrator hat dies nur zufällig bemerkt, als das Berechtigungskonzept der Firma vollständig überarbeitet wurde.

# G 5.119 Benutzung fremder Kennungen unter z/OS-Systemen

Die *Surrogat*-Berechtigung des z/OS-Sicherheitssystems RACF ermöglicht es einem Benutzer A, einen Batch-Job unter der Kennung eines anderen Benutzers B laufen zu lassen, ohne dass Benutzer A das Passwort von Benutzer B kennt. Alle Sicherheitsprüfungen erfolgen für die Kennung von Anwender B und die Protokoll- und SMF-Daten notieren Anwender B als Ausführenden der Befehle.

Es besteht die Gefahr, dass die Berechtigung *Surrogat* missbräuchlich verwendet wird, wenn nicht die notwendigen Sicherheitsvorkehrungen bei der Vergabe und bei der Überwachung eingehalten werden:

- Benutzer können u. U. unbefugt Aktionen ausführen, zu denen sie mit ihrer eigenen Kennung nicht berechtigt sind.
- Benutzer können u. U. vortäuschen, dass ein anderer Benutzer für eigene (unerlaubte) Aktionen verantwortlich sei.

# G 5.120 Manipulation der Linux/zSeries Systemsteuerung

Es sind drei unterschiedliche Betriebsarten von Linux unter zSeries möglich:

- Linux Native auf zSeries Hardware
- Linux in einer zSeries LPAR
- Linux unter dem Träger-System z/VM

Weitere Informationen zu den Betriebsarten von Linux unter zSeries finden sich in der Maßnahme M 3.41 *Einführung in Linux und z/VM für zSeries-Systeme*.

In allen drei Betriebsarten von Linux unter zSeries bestehen die in Baustein B 3.102 *Server unter Unix* beschriebenen Gefährdungen.

**Mainframe-spezifische Gefährdungen beim Einsatz von Linux**

Über die in Baustein B 3.102 *Server unter Unix* beschriebenen Gefährdungen hinaus können beim Einsatz von Linux auf zSeries-Mainframes unter anderem die folgenden Sicherheitsprobleme bestehen:

**Linux in einer zSeries LPAR**

Mainframe-spezifische Gefährdungen ergeben sich aus den möglichen Einwirkungen auf die zSeries Hardware:

- Durch den Zugang zu *HCD*-Funktionen (*Hardware Configuration Definition*) können Mitarbeiter Hardware-Ressourcen, wie z. B. Festplatten, unbefugt zur Linux-Partition zuordnen. Damit hat das Linux-Betriebssystem Zugriff auf die Hardware-Ressourcen.
- Der Zugang zur *HMC* (*Hardware Management Console*) erlaubt Manipulationen wie Starten, Stoppen und Zuordnung von Ressourcen zu einer LPAR. Analog ist dies in G 5.116 *Manipulation der z/OS-Systemsteuerung* für das z/OS-Betriebssystem beschrieben. Ähnlich sicherheitskritisch ist der Zugriff auf *SEs* (*Service Elements*). Das Service Element ist eine Komponente der zSeries-Hardware, die die gleichen Funktionalitäten wie eine HMC bietet.

**Linux unter dem Träger-System z/VM**

In diesem Szenario wird Linux auf einer emulierten Hardware einer virtuellen Maschine betrieben. Die emulierte Hardware der virtuellen Maschine wird von z/VM auf der realen zSeries-Hardware realisiert. Der physische Zugriff auf die realen Ressourcen erfolgt nur über z/VM.

Die Mainframe-spezifischen Gefährdungen ergeben sich einerseits aus den möglichen Einwirkungen auf die emulierte Hardware, andererseits aus den möglichen Einwirkungen auf z/VM.

- Der Zugang zu *HCD*-Funktionen und zur *HMC* kann - wie in der Betriebsart *Linux in einer zSeries LPAR* - missbraucht werden.
- Mitarbeiter, die kritische z/VM-Kommandos absetzen dürfen, können u. U. die Betriebsstabilität des z/VM und damit die darauf laufenden Linux-Betriebssysteme erheblich gefährden.
- Mitarbeiter, die unbefugt Zugriff auf das *DIRMAINT* Utility erhalten, können darüber z. B. neue virtuelle Systeme generieren oder Minidisks eines Linux einem anderen zuordnen. Wird z/VM RACF nicht benutzt, können über *DIRMAINT* auch Benutzerkennungen administriert werden.

- Ist im z/VM-Betriebssystem die Sicherheitskomponente z/VM RACF (Resource Access Control Facility) eingesetzt, so bestehen unter z/VM vergleichbare Gefährdungen, wie in G 3.72 *Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF* für das z/OS-Betriebssystem beschrieben. Mitarbeiter, die hohe RACF/VM-Autorisierungen besitzen (z. B. *SPECIAL*), können über RACF/VM andere z/VM-Kennungen und -Berechtigungen manipulieren.
- Falls die Authentisierung unter Linux über eine LDAP-Anbindung mit PAM-Modul (*Pluggable Authentication Module*) durch ein z/OS-RACF erfolgt, können Linux-Kennungen und -Berechtigungen auch von Mitarbeitern mit hoher z/OS-RACF-Autorisierung beeinflusst werden.

**Beispiel:**

- Ein Mitarbeiter hatte aus historischen Gründen noch die Berechtigung, unter z/VM die Funktion DIRMAINT zu verwenden. Dies nutzte er aus, um für sich ein privates Linux zu generieren und zu benutzen. Dies führte zum Verbrauch von Ressourcen, die dadurch den ordnungsgemäßen Prozessen auf der zSeries-Maschine nicht mehr zur Verfügung standen.

# G 5.121 Angriffe über TCP/IP auf z/OS-Systeme

Um ein z/OS-System über die Netzanbindung anzugreifen, sind häufig keine Spezialkenntnisse der SNA-Netzarchitektur oder von MVS erforderlich. Durch die TCP/IP-Anbindung an öffentliche Netze und die *Unix System Services* sind viele z/OS-Systeme über Standardprotokolle und Dienste, wie z. B. HTTP oder FTP, für externe Angreifer erreichbar.

Externe Angreifer können unter Umständen über die TCP/IP-Anbindung an öffentliche Netze Denial-of-Service-Angriffe gegen die angebotenen Dienste durchführen oder übertragene Daten unbefugt lesen oder manipulieren.

Interne Angreifer können über die TCP/IP-Anbindung an interne Netze versuchen, ihre Berechtigungen zu erhöhen, indem sie etwa Kennung und Passwort eines Anwenders mit *Special*-Rechten ausspähen.

# G 5.122 Missbrauch von RACF-Attributen unter z/OS

Im z/OS-Sicherheitssystem RACF sind die Attribute *SPECIAL*, *OPERATIONS* und *AUDITOR* mit besonders hohen Berechtigungen ausgestattet.

**Attribut *SPECIAL***

Die Kennung mit dem Attribut *SPECIAL* ist für die Administration des Sicherheitssystems RACF erforderlich. Der Besitzer dieses Attributs verfügt über die Möglichkeit, im RACF Einstellungen zu ändern. Er gibt beispielsweise den Benutzern den Zugriff auf Systemressourcen und Dateien frei. Der Inhaber der Berechtigung kann sich selbst auf sämtliche Ressourcen und Dateien des Systems Rechte vergeben. Er kann auch die im Weiteren aufgeführten Attribute an alle Benutzerkennungen vergeben.

Eine mögliche Schwachstelle besteht beim Einsatz von Systemmonitoren, die über hoch autorisierte Programmteile ihre eigene Kennung mit dem Attribut *SPECIAL* versehen können. Anwender mit Zugang zu den Systemmonitoren können dies - bei entsprechenden RACF-Rechten - ausnutzen, um ihre eigene Kennung mit höheren Zugriffsrechten zu versehen.

**Attribut *OPERATIONS***

Die Kennung mit dem Attribut *OPERATIONS* wird hauptsächlich für das *Space-Management* im z/OS-System angefordert. Es beinhaltet die Rechte zum Kopieren, Lesen, Löschen oder Neuanlagen von Dateien, ohne dass ein explizites Recht für die Datei und die Benutzerkennung vergeben wurde. Dies ermöglicht es prinzipiell einem Anwender, das Attribut *OPERATIONS* für unbefugte Datenzugriffe zu missbrauchen.

**Attribut *AUDITOR***

Auditoren sollen sicherheitsrelevante Ereignisse erkennen, nachvollziehen und überprüfen können. Änderungen an RACF-Definitionen sind mit dieser Berechtigung nur für audit-relevante Definitionen möglich (im Gegensatz zu *SPECIAL*), d. h. höhere Autorisierungen lassen sich damit nicht erreichen. Allerdings birgt das Attribut *AUDITOR* die Gefahr, dass umfassende Informationen, z. B. sämtliche RACF-Einstellungen, über das System ausgespäht werden können.

**Beispiele:**

- Ein Systemprogrammierer verfügte nicht über das Attribut *SPECIAL*. Er schrieb ein spezielles Programm und stellte es in eine APF-autorisierte Datei. Den Zugriff auf die APF-Dateien benötigte er für seine reguläre Arbeit. Über das selbst geschriebene Programm gelang es dem Systemprogrammierer, sich das Attribut *SPECIAL* zuzuweisen und unbefugt Änderungen an RACF-Einstellungen durchzuführen.
- Als in einem Unternehmen bekannt wurde, dass ein Konkurrent Kunden abwarb, wurden umgehend Nachforschungen angestellt. Wie sich herausstellte, verfügte die Benutzerkennung eines Anwenders über das Attribut *OPERATIONS*. Mit Hilfe dieses Attributs gelang es ihm, die Kundenadressen regelmäßig unerlaubt zu kopieren und weiterzugeben.

# G 5.123 Abhören von Raumgesprächen über mobile Endgeräte

Nahezu alle mobilen Endgeräte wie Laptops, Smartphones, Tablets, PDAs und Mobiltelefone werden mit integriertem Mikrofon und/oder eingebauter Kamera ausgeliefert. So können die Geräte dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören (siehe G 4.95 *Ausfall von Komponenten einer Speicherlösung*). Hierzu genügt ein unauffällig im Raum platziertes Smartphone, zum Beispiel in einer Besprechung.

Beispiel:

- In einer Besprechung haben fast alle Beteiligten ihre Laptops dabei und benutzen diese auch fortwährend. Einer der Teilnehmer hat unauffällig sein Rechnermikrofon aktiviert. Wie bei den meisten mobilen Endgeräten ist auch hier für die anderen Teilnehmer nicht erkennbar, dass das Mikrofon eingeschaltet ist. Er fertigt darüber einen kompletten Mitschnitt der Besprechung an und schneidet daraus kleinere Beiträge heraus. Da diese aus dem Sinnzusammenhang herausgerissen wurden, kann er damit erfolgreich ein anderes Besprechungsergebnis vorspiegeln.

# G 5.124 Missbrauch der Informationen von mobilen Endgeräten

Mobile Endgeräte gehen leicht verloren und sind einfach zu stehlen (siehe G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*). Je kleiner und begehrter solche Geräte sind, desto höher ist dieses Risiko. Neben dem unmittelbaren Verlust kann dabei durch den Verlust bzw. die Offenlegung wichtiger Daten weiterer Schaden entstehen. Dieser mittelbare Schaden wiegt in vielen Fällen deutlich schwerer als der rein materielle Verlust des Gerätes.

**Beispiele:**

- Daten wie E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente, die im Smartphone, Tablet oder PDA gespeichert sind, können durchaus einen vertraulichen Charakter haben. Ein Verlust des Geräts bedeutet dann unter Umständen die Offenlegung dieser gespeicherten Informationen.
- Viele mobile Endgeräte haben Sicherheitsmechanismen, die sie vor einem unbefugten Zugriff schützen sollen. Diese Sicherheitsmechanismen sind aber meistens zu schwach ausgelegt, sodass Angreifer sie überwinden können. Selbst wo wirksame Sicherungen vorhanden sind, werden sie häufig aus Bequemlichkeit nicht benutzt, sodass die vertraulichen Daten im Verlustfall überhaupt nicht geschützt sind.
- Oft sind auf mobilen Endgeräten Zugangsdaten für andere IT-Systeme oder für das LAN der Behörde bzw. des Unternehmens gespeichert. Wenn ein Unbefugter in den Besitz eines Laptops oder PDAs mit (statischen) Zugangskennungen gelangt, ist damit ein missbräuchlicher Zugriff auf interne Daten möglich.
- Mit Smartphones und Mobiltelefonen kann ein Dieb auf Kosten des rechtmäßigen Besitzers telefonieren, sofern ihm die PIN bekannt ist oder er sie leicht erraten kann oder wenn die Sicherheitsmechanismen des Gerätes leicht überwunden werden können.
- Mit Smartphones, Tablets oder PDAs mit einer SIM-Karte für den Zugang zum Internet über das Mobilfunknetz kann ein Dieb zum Schaden des rechtmäßigen Besitzers Daten aus dem Internet beziehen. Da innerhalb Deutschlands in der Regel Pauschaltarife angeboten werden, beläuft sich der Schaden lediglich auf die Gebühr, die Karte zu sperren und eine neue Karte in Betrieb zu nehmen. Wenn der Dieb jedoch über die Datenverbindung Spam verschickt oder urheberrechtlich geschütztes Material heruntergeladen hat, sieht sich der Eigentümer des Geräts unter Umständen hohen Schadenersatzforderungen gegenüber. Ihm droht dann zumindest ein hoher Aufwand für rechtliche Auseinandersetzungen.
- Viele Smartphones, Tablets, PDAs und Laptops haben Schnittstellen für den Einsatz austauschbarer Datenspeicher wie z. B. Speicherkarten oder USB-Sticks. Bei einem solchen unbeaufsichtigten mobilen Endgerät mit der entsprechenden Hard- und Software besteht die Möglichkeit, dass über diese Speichermedien große Datenmengen schnell herunterkopiert werden können. Dabei werden nicht einmal Spuren hinterlassen.

# G 5.125 Datendiebstahl mithilfe mobiler Endgeräte

Mobile Endgeräte wie Notebooks, Smartphones, Tablets oder PDAs sind größtenteils darauf ausgelegt, einen einfachen Datenaustausch mit anderen IT-Systemen zu ermöglichen. Dies kann über ein Verbindungskabel oder auch drahtlos, z. B. über WLAN, Bluetooth oder eine Mobilfunkverbindung, erfolgen.

Wo ein offener Zugang zu IT-Systemen möglich ist, können Angreifer mithilfe mobiler Endgeräte Informationen unauffällig abfragen, verändern oder mitnehmen. Eine nachträgliche Überprüfung oder gar ein Nachweis sind nicht immer möglich, da häufig die Zugriffe nicht entsprechend protokolliert werden.

Falls das mobile Endgerät über eine drahtlose Kommunikationsschnittstelle verfügt (z. B. WLAN, SIM-Karte oder Bluetooth), können die gespeicherten Informationen auch unmittelbar an jeden Ort der Welt übermittelt werden (siehe G 5.97 *Unberechtigte Datenweitergabe über Mobiltelefone*).

Beispiel:

- Ein Mitarbeiter eines Unternehmens wird aus einer Besprechung mit einem Externen gerufen, um ein wichtiges Telefonat entgegenzunehmen. Der Externe nutzt die kurze Zeitspanne ohne Beaufsichtigung, um den im Besprechungsraum aufgestellten PC mit seinem mobilen Endgerät zu verbinden. Anschließend transferiert er alle zugreifbaren Daten auf sein mobiles Endgerät.
- Ein größeres Unternehmen betreibt ein eigenes drahtloses Netz (WLAN), das jedoch nicht ausreichend abgesichert ist. Ein Angreifer nutzt das aus und verbindet sein Tablet mit dem WLAN. Er kann nun problemlos alle übermittelten Daten "mitschneiden" und hat im schlechtesten Fall Zugriff auf die Dateien im Unternehmensnetz.

# G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Viele mobile Endgeräte sind inzwischen mit eingebauten Kameras ausgerüstet, zum Beispiel Laptops, Smartphones oder Mobiltelefone. In der Regel ist mit diesen Kameras auch die Aufzeichnung von Filmen möglich. Solche mobilen Endgeräte können leicht dazu benutzt werden, in geschäftskritischen Bereichen (beispielsweise in einer Entwicklungsabteilung) unauffällig Foto- oder Filmaufnahmen anzufertigen. Die Bildqualität reicht meist an die Qualität gewöhnlicher Kleinbildkameras heran.

Wie beim "allgemeinen Datenklau" (siehe G 5.125 *Datendiebstahl mithilfe mobiler Endgeräte*) können die gemachten Bilder unmittelbar nach draußen übertragen und anschließend wieder vom Gerät gelöscht werden. In diesem Fall ist selbst dann, wenn jemand Verdacht schöpft, ein Nachweis ggf. nur mit forensischen Methoden möglich. Sind auf einem Smartphone Applikationen von sozialen Netzen oder Videoportalen wie YouTube installiert, können die gerade erstellten Bilder und Videos im auch Internet veröffentlicht werden. Abgesehen von der Urheberrechtsproblematik können so schützenswerte Daten schnell an Unberechtigte weitergegeben werden. Personen und Institutionen können durch kompromittierende Bilder einen Imageverlust erleiden.

**Beispiele:**

- In vielen Schwimmbädern und Sportstudios dürfen mittlerweile keine Foto-Handys mehr mitgenommen werden, da es verschiedene Beschwerden über heimlich aufgenommene Fotos aus Umkleidekabinen gab. Unter anderem wurde dies öffentlich, da einige Hobby-Paparazzi ihre Fotos stolz auf Webseiten präsentiert haben.
- Viele Laptop-Modelle haben neben einem integrierten Mikrofon auch eine kleine integrierte Kamera, die je nach Auslegung für Standbilder, Videoaufnahmen oder als Webcam benutzt werden kann. Mit solchen Kameras ist es problemlos möglich, sogar aus den hintersten Reihen in einem Hörsaal nicht nur die Folien lesbar und den Redner hörbar aufzuzeichnen. Sogar Zwischenfragen können damit erstaunlich gut mitgeschnitten werden. Da die Geräte nicht als Kamera wahrgenommen werden, ist es hier schon zu unangenehmen Überraschungen gekommen, als nachträglich ungenehmigte Mitschnitte veröffentlicht wurden.

# G 5.127 Spyware

Diese Gefährdung ist 2011 mit der 12. Ergänzungslieferung entfallen.

# G 5.128 Unberechtigter Zugriff auf Daten durch Einbringen von Code in ein SAP System

Kann ein Angreifer ABAP-Code in ein SAP System einbringen, so sind unberechtigte Zugriffe auf Daten möglich, da die Sicherheit eines SAP Systems durch den ABAP-Code implementiert werden muss.

**Beispiele:**

- Ein Entwickler bringt im Rahmen eins Software-Updates eigenen, zusätzlichen Code in ein SAP ein, welcher ihm entfernten Zugriff auf alle Programme des SAP Systems gewährt.
- Einem externen Angreifer gelingt es, durch eine Schwäche in einer unternehmenseigenen Applikation eigene Transportdateien im SAP Transportverzeichnis abzulegen. Diese werden ohne Prüfung eingespielt und installiert und können so ihre Schadwirkung entfalten.

# G 5.129 Manipulation von Daten über das Speichersystem

Über eine mangelhaft konfigurierte SAN-Installation kann eine ungewollte Verbindung zwischen Netzen entstehen. Eine gravierende Gefährdung für interne Daten einer Institution kann z. B. entstehen, wenn ein Server mit SAN-Anschluss aus dem Internet erreichbar ist und so von außen kompromittiert wird.

Die Anbindung eines an das Speichersystem angeschlossenen Servers, der nicht genügend vom Internet abgeschottet ist, kann bei einer Kompromittierung des Servers auch zur Kompromittierung des Speichersystems führen. So können gegebenenfalls Daten im SAN, die anderen Maschinen zugeordnet sind, gelesen oder verändert werden.

Da so alle Sicherheits- und Überwachungsmaßnahmen wie Firewalls oder IDS (Intrusion Detection Systeme) in den IT-Netzen der Institution übergangen werden, ist das Schadenspotential sehr groß.

# G 5.130 Manipulation der Konfiguration einer Speicherlösung

Zentrale Speicherlösungen konzentrieren eine Vielzahl wichtiger Daten einer Institution. Für sie ergeben sich daher in der Regel besondere Sicherheitsanforderungen, denen im Rahmen einer sorgfältigen Konfiguration Rechnung zu tragen ist.

Wenn es einem Angreifer gelingt, an Passwörter zu gelangen, die den Zugriff auf Konfigurationsprogramme (Element Manager) der Speicherlösung erlauben, kann er eine Vielzahl von Sicherheits- und Kontrollmaßnahmen umgehen.

Fehlt in einem solchen Fall ein Rechte- und Rollenkonzept oder ist dies nur unzureichend umgesetzt, bieten sich dem Angreifer Möglichkeiten, die Konfiguration der Speicherlösung zu verändern. Nachfolgend ist beschrieben, wie sich die Manipulation an bestimmten Konfigurationsparametern auswirkt.

- Die Konfigurationsveränderungen betreffen die Einstellungen des Zonings. In der Folge ist es möglich, zusätzliche Komponenten im FC-Netz anzumelden, die ursprünglich nicht über die benötigten Zugriffsrechte verfügten.
- Manipuliert ein Angreifer die Konfiguration des Zonings, ist es ihm möglich, die Zugriffswege zwischen Servern und Speicherressourcen zu verändern. Damit kann er unberechtigt auf Informationen zugreifen bzw. die Zugriffsrechte für andere Benutzer einschränken.
- Manipuliert ein Angreifer die LUN-Konfiguration, ist es ihm möglich, auf Speicherressourcen zuzugreifen, die für ihn im Vorfeld nicht verfügbar waren.
- WWN-Spoofing (siehe hierzu G 5.186 *Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing*)

In der Folge unberechtigter Manipulationen und Konfigurationsänderungen kann nicht mehr gewährleistet werden, dass die Sicherheitsanforderungen an die Speicherlösung eingehalten werden. Unberechtigte Zugriffe auf Speicherressourcen oder die Manipulation von Daten sind möglich.

# G 5.131 SQL-Injection

Greift eine Anwendung auf die Daten einer SQL-Datenbank zu, so werden Befehle in Form von SQL-Anweisungen an die Datenbank übermittelt. Ist die Anwendung anfällig für SQL-Injection, kann ein Angreifer durch Manipulation der Eingabedaten geänderte oder zusätzliche SQL-Anweisungen injizieren, die von der Anwendung an die Datenbank weitergeleitet und dort bearbeitet werden. Auf diese Weise können wie bei einem direkten Datenbankzugriff beliebige SQL-Anweisungen ausgeführt werden und so Sicherheitsmechanismen der Anwendung beim Datenzugriff umgangen werden.

Eine SQL-Injection kann daher z. B. die folgenden Auswirkungen haben:

- unberechtigter Zugriff auf Daten,
- Erzeugen, Auslesen, Verändern oder Löschen von Daten,
- Ausführen von Betriebssystembefehlen,
- Kontrolle über die Datenbank,
- Zugriff auf weitere Server (z. B. HTTP-Get-Request oder DNS-Abfrage).

Das Einschleusen der SQL-Anweisung wird dabei durch eine unzureichende Validierung von Eingabedaten innerhalb der Anwendung ermöglicht, die in dieser Form direkt in eine dynamische Datenbankabfrage eingebaut werden (siehe auch G 4.84 *Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services*).

Die SQL-Injection ist ein spezieller Injection-Angriff (siehe G 5.174 *Injection-Angriffe*), der sich ausschließlich gegen SQL-Datenbanken richtet. So ist das grundsätzliche Vorgehen zum Einschleusen von Befehlen auch bei anderen Interpretern möglich (z. B. LDAP-Injection, XML-Injection).

# G 5.132 Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003

Die Remotedesktop-Freigabe auf Basis des *Remote Desktop Protocol* (RDP) ist ein effektives und verbreitetes Mittel zur Fernwartung eines Windows-Servers und zur Nutzung von Programmen auf entfernten Computern (Remotedesktop). Der Verbindungsaufbau von einem Client zum RDP-Server findet ohne vorherige Authentisierung des Benutzers statt. Der komplette Anmeldebildschirm des Remotedesktops wird unmittelbar auf den Bildschirm des lokalen Clients gespiegelt. Es besteht die Gefahr, dass auch ein Angreifer durch die Windows-RDP-Anmeldung Remote-Zugriff auf das System erlangen kann.

Informationen zur Betriebssystemversion und zur Domänenmitgliedschaft des Windows-Servers liegen für jeden Remotedesktop-Benutzer ohne Eingabe von Benutzernamen und Kennwort offen. Weitere Informationen könnten über Hintergrundbilder preisgegeben werden. Häufig blenden Administratoren Verwaltungsinformationen als Hintergrundbild ein oder der Serverhersteller hat bei vorinstallierten Betriebssystemen ein herstellerspezifisches Hintergrundbild vorgegeben. Darüber können verwertbare Informationen erlangt werden, um das System zu analysieren und entsprechende Sicherheitslücken auszunutzen.

Im Falle einer Unterbrechung der Netzverbindung während einer RDP-Sitzung stellt Windows Server 2003 die Sitzung automatisch ohne erneute Anmeldung wieder her, sobald der Client die Netzverbindung zum Server wieder aufgenommen hat. Zeiträume bis in den Minutenbereich können überbrückt werden. Die erhöhte Fehlertoleranz wird mit der Gefährdung der Integrität einer RDP-Sitzung erkauft. Ein Angreifer kann durch Social Engineerung oder durch Abfangen der Verbindung Remote-Zugriff auf das System bekommen. Eine Verbindung mit RDP Version 5.2 von Windows Server 2003 kann durch Dritte leicht abgefangen und unbemerkt umgeleitet werden. Seit Windows Server 2003 mit Service Pack 1 gibt es zwar eine Absicherung mittels SSL, aber viele Clients können dann keine Verbindung mehr herstellen, zum Beispiel Remotedesktop-Clients früherer Windows-Versionen und RDesktop für Unix/Linux. Daher kann die Absicherung mit SSL meist nicht flächendeckend eingesetzt werden und es besteht weiterhin die Gefahr, dass die Verbindung abgefangen und unerlaubter Zugriff auf das System ausgeübt wird.

Aufgrund der beschriebenen Gefahren ist von einer erhöhten Gefährdung des Servers auszugehen, sobald RDP verwendet wird.

- Ein amerikanischer Hersteller lieferte Server mit vorinstallierten OEM-Versionen von Windows Server 2003 an seine Kunden aus. Beim Anmelden am Betriebssystem via Konsole oder Remotedesktop erschien ein Hintergrundbild mit Logo des Herstellers und einem Foto der Server-Hardware. Dadurch konnten Schwachstellen über das System ermittelt und für Angriffe genutzt werden.
- Während einer Netzunterbrechung verlässt der Administrator kurz den Verwaltungs-PC, auf dem eine RDP-Sitzung läuft. Ist er nicht rechtzeitig wieder vor Ort und ist kein Bildschirmschoner mit Kennwortschutz aktiv, könnte ein Dritter die RDP-Sitzung weiterverwenden, sobald die Netzunterbrechung beseitigt worden ist. Er hätte die vollen Berechtigungen des Administrators und könnte versehentlich oder vorsätzlich großen Schaden verursachen.

# G 5.133 Unautorisierte Benutzung web-basierter Administrationswerkzeuge

Die Administration mit Webbrowser-basierten Werkzeugen hat stark an Bedeutung gewonnen. Einer der entscheidenden Vorteile für das technisch verantwortliche Personal ist die Unabhängigkeit von

- der Betriebssystem-Plattform des zu betreuenden IT-Systems
- dem Standort des zu betreuenden IT-Systems.

Allen Werkzeugen gemein ist, dass sie kritische Anmeldedaten verwenden. Sie sind auf gängige für das Internet standardisierte Authentisierungsmethoden angewiesen, um technischem Personal autorisierten Zugriff auf die kritischen lokalen Systeme zu gewähren. Viele Administrationswerkzeuge besitzen zusätzlich eigene Authentisierungsmechanismen oder bedienen sich lokaler, teils nicht standardisierter Authentisierungs- und Sicherheitsmechanismen. Es besteht die Gefahr der Kompromittierung durch nicht autorisierte Benutzer.

Eine hohe Gefährdung entsteht, wenn die Sicherheitsrichtlinie für die Authentisierung im Netz bzw. deren Umsetzung im betrachteten Informationsverbund durch ungeeignete Authentisierungsverfahren für Web-basierte Administrationswerkzeuge unterlaufen wird. Die häufigsten Ursachen dafür sind:

- die Wahl einer falschen oder veralteten Authentisierungsmethode, weil das jeweilige Werkzeug keine stärkere Authentisierung unterstützt oder weil andere beteiligte IT-Systeme (z. B. Sicherheitsgateways) das favorisierte Protokoll nicht unterstützen
- die ungeeignete Umsetzung bzw. Übernahme der Web-basierten Authentisierung in das lokale Authentisierungssystem.

Eine Gefährdung kann z. B. entstehen, wenn zum Zwecke der Nutzung Webbasierter Administrationshilfen die Windowskomponente Internetinformationsdienst aktiviert wird, ohne diese entsprechend den Empfehlungen zu konfigurieren. Eine Gefahr könnte dann darin bestehen, dass in der Standardkonfiguration nur schwächere Authentisierungsverfahren aktiviert sind. Es ist darauf hinzuweisen, dass eine mangelhafte Konfiguration ein großes Risiko für alle auf dem Markt befindlichen Lösungen zur Web-basierten Administration darstellt.

# G 5.134 Fehlende Identifizierung zwischen Gesprächsteilnehmern

Sowohl bei der leitungsvermittelnde Telefonie als auch bei VoIP kann der Anrufer oft über seine Telefonnummer identifiziert werden. Der Angerufene kann dabei in seinem Telefondisplay den Anrufer erkennen, ohne dass er das Telefongespräch annehmen muss. Integrated Services Digital Network (ISDN) bietet die Möglichkeit, über CLIP (Calling Line Identification Presentation) und COLP (Connected Line Identification Presentation) der Gegenstelle die Telefonnummer zu signalisieren. Bei VoIP können diese Informationen über die Caller ID ermittelt werden. Verallgemeinert wird dies als Rufnummernanzeige bezeichnet.

Sehr oft wird die Telefonnummerübermittlung auch zur Authentisierung verwendet. Ein häufig realisiertes Beispiel für diesen Mechanismus ist, dass die Benutzer ihren Anrufbeantworter abhören können, ohne ihre PIN oder sein Passwort eingeben zu müssen.

Ein Angreifer könnte durch Änderungen an der vermittelnden Telefonanlage einem Telefon jede beliebige Telefonnummer zuweisen, die dann an den Empfänger übertragen wird. Dadurch kann er versuchen, seinem Gesprächspartner eine falsche Identität vorzuspiegeln (siehe G 5.42 *Social Engineering*).

Viele Telefone beinhalten eine Inkognito-Funktion. Der Anrufer kann diese Funktion aktivieren, wenn er verhindern möchte, dass die eigene Telefonnummer auf dem Display des Angerufenen angezeigt wird. Die Telefonnummer des Anrufers muss dennoch für den Verbindungsaufbau übertragen werden. Die Telefonübermittlungsstelle, an die das Telefon des Angerufenen angeschlossen ist, entscheidet nach dieser Angabe, ob die Telefonnummer an den Angerufenen übertragen wird. Durch eine entsprechende Programmierung der Telefonübermittlungsstelle kann die Inkognito-Funktion ignoriert werden, ohne dass die Benutzer dies wissen.

In homogenen VoIP-Netzen, in denen nur über das Datennetz telefoniert wird, treten diese Probleme in dieser Form nicht auf, da keine Inkognito-Funktionalität vorgesehen ist. In der Praxis sind homogene VoIP-Netze jedoch nur sehr selten zu finden. In der Regel sind die lokalen Netze mit einem entsprechenden Gateway verbunden, der die Kommunikation mit Anwendern anderer Telefonsysteme ermöglicht. Zwischen dem Gateway und dem Empfänger des Telefongesprächs können daher die oben genannten Probleme auch auftreten.

Innerhalb des Netzes, in dem über VoIP telefoniert wird, werden die Teilnehmer anhand ihrer IP-Adressen (bzw. MAC-Adressen) zugeordnet. Eine portbasierte Zuordnung, wie an einer leitungsvermittelnden Telefonanlage, ist bei VoIP nicht vorgesehen.

Ähnlich wie bei einer E-Mail wird dem Empfänger eines VoIP-Anrufs über die Signalisierungsinformationen unabhängig von der Absender-IP-Adresse die Caller-ID des Senders übermittelt. Die Caller-ID lässt sich ähnlich leicht wie die Absenderadresse einer E-Mail fälschen. Eine solche Fälschung kann wiederum dazu führen, dass der Empfänger falsche Rückschlüsse auf die Identität des Senders zieht. Ein Angreifer könnte sich so für einen anderen Benutzer ausgeben und ein Gespräch zu einem weiteren Benutzer aufbauen.

Der Empfänger könnte auf Grundlage der gefälschten IP-Adresse falsche Rückschlüsse auf die Identität des Senders ziehen.

**Beispiel:**

- Durch eine Manipulation an der Telefonanlage wird von dem Telefon eines Angreifers die Telefonnummer des Geschäftsführers eines größeren Unternehmens signalisiert. Der Angreifer nutzt diese Manipulation, um einen Mitarbeiter, der den Geschäftsführer nicht persönlich kennt, nach bestimmten internen Informationen fragen. Da er den Anrufer wegen der übertragenen Telefonnummer für den Geschäftsführer hält, gibt er alle Informationen heraus.

# G 5.135 SPIT und Vishing

Der Einsatz von VoIP bietet viele Möglichkeiten, unter Vorspiegelung falscher Tatsachen an Informationen zu gelangen oder unaufgeklärte Benutzer auszunutzen. Über VoIP können Anbieter beispielsweise kostengünstig unerwünschte Werbung für ihre Produkte oder Dienstleistungen platzieren. SPIT (*Spam over IP-Telephone*), ebenso wie SPAM, der in ähnlicher Form schon bei E-Mail sehr verbreitet ist, kosten die Empfänger Zeit und Geld. Je nach Häufigkeit sind SPIT-Anrufe nicht nur eine Belästigung, sondern sie stören unter Umständen die Arbeitsabläufe in einer Institution erheblich.

Der Versand von SPIT ist für einen Anbieter vergleichsweise günstig. Kann eine paketorientierte Verbindung zu einem Benutzer über das Internet hergestellt werden, so fallen für den Anbieter keine weiteren Telefonkosten an. Durch eine entsprechend dimensionierte Internetanbindung kann er zahlreiche Werbeangebote zur gleichen Zeit versenden.

SPIT kann beispielsweise eine Sprachwerbeansage sein. Dabei wird nach Annahme des Anrufs eine Aufnahme abgespielt. Auf diese Art und Weise können Produkte oder Dienstleitungen angepriesen werden. Es kann aber auch SPIT mit betrügerischer Absicht versendet werden. Ein Beispiel hierfür ist Vishing.

Bei Vishing (Voice Phishing) handelt es sich um eine Angriffsform, um an persönliche Informationen eines oder mehrerer Opfer zu gelangen. Hierbei ruft ein VoIP-basierter Dialer eine große Anzahl von gesammelten VoIP-Adressen an. Bei Rufannahme wird eine Sprachmitteilung abgespielt, die dem Opfer vortäuschen soll, dass der Anruf von einer vertrauenswürdigen Institution, wie dem Kreditinstitut, bei dem er Kunde ist, stammt. Während des Telefonats werden die Opfer aufgefordert, Informationen wie Kontonummern, PINs und TANs preiszugeben.

**Vishing**

Der Begriff "Vishing" steht für "Voice Phishing" oder "Phishing via VoIP" und bezeichnet den organisierten Datenklau via Telefon, indem Benutzer ähnlich wie beim Phishing (siehe G 5.157 *Phishing und Pharming*) durch gut ausgedachte Geschichten animiert werden, vertrauliche oder finanzrelevante Informationen weiterzugeben. Hierbei kann sowohl die Angriffsvorbereitung als auch der Informationsabgriff telefonisch erfolgen.

- Bei einer Form von Vishing rufen VoIP-basierte Dialer eine große Anzahl von gesammelten VoIP-Adressen an. Bei Rufannahme wird eine Sprachmitteilung abgespielt, die dem Opfer vortäuschen soll, dass der Anruf von einer vertrauenswürdigen Institution, wie dem Kreditinstitut, bei dem er Kunde ist, stammt. Während des Telefonats werden die Opfer aufgefordert, Informationen wie Kontonummern, PINs und TANs preiszugeben.
- Bei einer anderen Angriffsvariante verschicken Betrüger E-Mails, die mit gut erfundenen Texten dazu auffordern, unter einer angegebenen Telefonnummer eine Voice-Box anzurufen. Durch diese Voice-Box werden dann gezielt PIN-Daten und andere vertrauliche Informationen abgefragt. Diese Angriffsform kann gefährlich sein, weil es den Ratschlag vieler Finanzinstitute ausnutzt, nicht auf vorgebliche E-Mails zu reagieren, sondern telefonischen Kontakt zu suchen.

Ziel von Vishing ist es, möglichst viele Opfer irrezuführen und zur Herausgabe ihrer Zugangsdaten, Passwörter, Kreditkartendaten etc. zu bewegen. Dadurch können Betrüger genügend Informationen sammeln, um beispielsweise

im Namen des Kunden Geld von Konten abzubuchen: Namen, Kreditkarten- und Kontonummer, PIN- und TAN-Nummern.

**Beispiele:**

- Ein Kunde erhält eine elektronische Nachricht von seinem Kreditinstitut. Die Absenderadresse ist gefälscht, was dem Opfer nicht auffällt. In der Nachricht wird er dazu animiert, seinen Online-Banking-Zugang zu prüfen, indem er seinen Berater über eine Mailbox informiert. Beim Anruf wird eine Sprachmitteilung abgespielt, die dem Opfer vortäuschen soll, dass der Anruf von einer vertrauenswürdigen Institution, wie dem Kreditinstitut, bei dem er Kunde ist, stammt. Während des Telefonats werden die Opfer aufgefordert, Informationen wie Kontonummern, PINs und TANs preiszugeben.
- In einer E-Mail wird glaubhaft dargestellt, dass die Kredit- oder EC-Karte missbraucht worden sei. Außerdem werden die Angeschriebenen aufgefordert, die Angelegenheit "sicher" telefonisch zu klären. Unter der genannten Telefonnummer werden die Kunden aufgefordert, ihre persönlichen Zugangsdaten per Tasteneingabe preisgeben, um das Problem zu beheben.

# G 5.136 Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinem Benutzer persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiele solche in Druckerräumen, sind nur einem beschränkten Personenkreis zugänglich. Aber häufig sind auch Telefone in Parkhäusern, vor Zugangskontrollsystemen oder in für Besucher zugänglichen Bereichen zu finden.

Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, so besteht die Gefahr, dass solche internen Telefonnummern ungewollt nach außen gelangen.

Beim Einsatz von VoIP-Telefonen in frei zugänglichen Bereichen müssen weitere Aspekte beachtet werden. VoIP-Telefone haben einen hohen Software-Anteil und werden häufig in Datennetzen betrieben, die auch für andere IT-Anwendungen genutzt werden. Ein Angreifer könnte deshalb versuchen, durch den direkten Zugriff auf das Gerät Schwachstellen in der VoIP-Software auszunutzen oder selbst schädliche Software zu installieren. Besonders bei Softphones besteht auch die Gefahr, dass ein Angreifer versucht, beispielsweise mit Hilfe einer bootbaren CD-ROM Administratoren-Rechte auf dem Endgerät oder auf anderen IT-Systemen im gleichen Netz zu erlangen.

VoIP-Telefone müssen an ein Datennetz angeschlossen sein. Ein Angreifer könnte an diesen Netzanschluss einen tragbaren Computer anschließen und so unter Umständen auf das von außen durch eine Firewall geschützte Netz zugreifen. Diesen Zugang kann er möglicherweise für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit ausnutzen. Auch ein Innentäter könnte versuchen, diese Anschlüsse zu missbrauchen, ohne dass die Angriffe von seinem Arbeitsplatzrechner ausgehen und dies protokolliert wird.

# G 5.137 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

Bei der drahtlosen Kommunikation können die übertragenen Signale auf der Funkstrecke nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden. Deshalb könnte ein Angreifer seinen Angriff ohne das bei leitungsgebundener Kommunikation bekannte Zugriffsproblem durchführen. In Funknetzen mit mehreren Basisstationen zur Versorgung großflächiger Areale, wie z. B. zellulare Mobilfunknetze, ist es zudem üblich, dass der ungefähre Aufenthaltsort der mobilen Endgeräte ermittelt wird, um deren schnelle Erreichbarkeit zu gewährleisten. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls - im Zuge des Verbindungsaufbaus - Informationen über ihren Standort ab. Diese Standort-Informationen könnten durch den Netzbetreiber oder Dienstbetreiber - aber auch von Dritten - zur Bildung von Bewegungsprofilen verwendet werden.

**Beispiele:**

- Bei WLANs auf Basis von IEEE 802.11 wird die Hardware-Adresse einer WLAN-Karte, die sogenannte MAC-Adresse, bei jeder Datenübertragung mit versendet. Dadurch ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar.
  Auf diese Weise könnten Bewegungsprofile über mobile Nutzer erstellt werden, z. B. wenn diese sich in öffentliche Hotspots einbuchen. Da dies MAC-Adresse unverschlüsselt übertragen wird, ist das Erstellen von Bewegungsprofilen keinesfalls nur den Betreibern der Hotspots möglich. Prinzipiell kann jeder, der an geeigneten öffentlichen Plätzen eine Funk-LAN-Komponente installiert, die MAC-Adressen anderer Nutzer mitlesen.
- Der Funkverkehr von Bluetooth-Verbindungen kann mit Hilfe von Bluetooth-Protokollanalysatoren passiv mitempfangen und aufgezeichnet werden. Die Synchronisation auf die Frequency-Hopping-Sequenz gelingt bei Kenntnis der Geräteadressen auch dann, wenn sich die Geräte im "Non-discoverable"-Modus befinden. Alle Schichten des Bluetooth-Protokoll-Stacks können offline betrachtet bzw. analysiert werden. Das Extrahieren und Mitlesen der übertragenen Nutzdaten (Payload) ist bei fehlender Verschlüsselung möglich. Durch den Einsatz einer Antenne mit starker Richtcharakteristik und geeigneter Elektronik zur Verstärkung eines empfangenen Bluetooth-Signals kann ein solcher "Lauschangriff" auch noch in einer größeren Entfernung als der üblichen Funktionalitätsreichweite durchgeführt werden. Eine Sendeleistungsregelung ist optional und wird nicht von jedem Bluetooth-Gerät unterstützt.
  Die Verwendung des Frequenzsprungverfahren alleine stellt leider auch kein ernsthaftes Hindernis für einen ausreichend informierten Angreifer dar, auch wenn häufig zu lesen ist, dies würde eine unberechtigte Teilnahme bzw. den Empfang und das Abhören von Bluetooth-Verbindungen wesentlich erschweren. Der Grund für die Verwendung eines Frequenzsprungverfahrens liegt darin, Übertragungsfehler aufgrund von Störungen durch den Betrieb anderer Geräte (z. B. WLANs), die dasselbe Frequenzband nutzen, klein zu halten und somit eine gute Verfügbarkeit sicherstellen zu können.
- Die eindeutigen Bluetooth-Geräteadressen können zum Verfolgen einzelner Geräte missbraucht werden. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen. Die Geräteadresse wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Masters ist zum Teil (24 der 48 Bit) in jedem Datenpaket enthalten.

# G 5.138 Angriffe auf WLAN-Komponenten

Sicherheitsmängel bei der drahtlosen Kommunikation, bei einzelnen WLAN-Clients, Access Points oder dem Distribution System können dazu führen, dass Angriffe erfolgreich sind. Dabei können interne Daten mitgelesen oder verändert werden. Es können aber auch WLAN-Komponenten so manipuliert werden, dass sie wiederum als Einstiegspunkt für Angriffe auf andere Netze und Netzkomponenten genutzt werden können.

**Beabsichtigte Störung des Funknetzes**

Durch das Betreiben von Störquellen, so genannten Jammern, kann ein WLAN absichtlich gestört werden. Dies kann zum kompletten Ausfall eines WLAN führen und stellt damit einen Denial-of-Service-Angriff auf physikalischer Ebene dar. Die Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Geländes, auf dem das WLAN genutzt wird, befinden.

**Vortäuschen einer gültigen Authentisierung**

Ein Angreifer könnte bestimmte Steuer- und Managementsignale aufzeichnen, analysieren und diese dann erneut senden. Dadurch kann dem WLAN eine gültige Authentisierung einer WLAN-Komponenten vorgetäuscht und ein unberechtigter Zugriff auf das WLAN erschlichen werden.

**Vortäuschung eines gültigen Access Points**

Durch das Einschleusen fremder Access Points in ein WLAN können Man-in-the-Middle-Attacken durchgeführt werden ("Cloning" oder "Evil Twin"). Hierzu kann ein weiterer Access Point in der Nähe eines Clients installiert werden. Wenn dieser dem WLAN-Client eine stärkere Sendeleistung anbietet als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls keine beidseitige Authentisierung erzwungen wird. Zusätzlich könnte auch der offizielle Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzer nehmen dann an einem Netz teil, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es einem Angreifer möglich, die Kommunikation abzuhören.

Auch durch Poisoning- oder Spoofing-Methoden kann ein Angreifer eine falsche Identität vortäuschen bzw. den Netzverkehr zu Systemen des Angreifers umlenken. So kann er die Kommunikation belauschen und kontrollieren.

**Kompromittierung des Distribution System**

Neben dem Anschluss eines fremden Access Points ist eine Kompromittierung des Distribution System ebenfalls möglich, indem ein fremder Hub oder Switch zwischen Access Point und Distribution System zwischengeschaltet wird, sofern dieser Bereich zugänglich ist.

Mit einem angeschlossenen Protokoll-Analysator kann dann der gesamte Verkehr zwischen Access Point und Distribution System aufgezeichnet werden. Zusätzlich kann über entsprechende andere Werkzeuge ein aktiver Angriff auf die Infrastruktur oder einen am Access Point assoziierten Client durchgeführt werden. Das "Brechen" der WLAN-Verschlüsselung ist dabei noch nicht einmal erforderlich, da im LAN-Bereich des Distribution Systems die Datenübertragung vollständig unverschlüsselt erfolgt, sofern nicht Verschlüsselungsmechanismen auf Protokollebene, beispielsweise mittels VPN-Techniken, oder auf Applikationsebene eingesetzt werden.

**Angriffe auf WLAN-Clients**

Durch die Teilnahme eines Clients an einem WLAN entstehen auf den Clients zusätzliche Bedrohungen für die lokalen Daten. Angriffe könnten einerseits auf WLAN-Mechanismen, aber auch auf Schwachstellen des verwendeten Betriebssystems erfolgen. Ein hierdurch manipulierter Client kann zu einer Kompromittierung des gesamten WLANs und schlimmstenfalls der gesamten IT-Infrastruktur der Institution führen.

Erfolgt die Datenübertragung im WLAN unverschlüsselt, kann ein Angreifer im Falle von leicht verwertbaren Daten, beispielsweise VoIP-Gesprächsdaten, auch auf einfachste Weise die Kommunikation belauschen.

Der fehlerhaft geplante Einsatz eines WLAN-Clients beispielsweise in einem nicht vertrauenswürdigen Funknetz (Hotspot oder Ad-hoc-Netz) bringt weitere Gefahren mit sich. Einige sind im Folgenden beispielhaft aufgelistet:

- Mit Hilfe von Spoofing könnte ein Angreifer kompromittierende Werkzeuge auf dem Client eines WLAN-Benutzers installieren.
- Ein Angreifer könnte die Netzdienste und -funktionalitäten des Clients auf Schwachstellen prüfen und diese unter Umständen ausnutzen. Dadurch könnte beispielsweise ein Zugriff auf den Rechner möglich sein, weil Kennwörter ungeeignet gewählt waren oder die Personal Firewall unzureichend konfiguriert.

**Angriffe auf Access Points**

Angriffe können aber auch über die Clients auf andere WLAN-Komponenten und damit gekoppelte Netze erfolgen. Wenn Sicherheitsmechanismen bei mobilen Komponenten und Übertragungsstandards fehlen oder schlecht konfiguriert sind, kann dies von Angreifern ausgenutzt werden, um unbefugten Zugriff auf interne Netze von Behörden oder Unternehmen zu nehmen. Jede zusätzliche Komponente, die in ein Netz eingebunden wird, schafft zusätzliche, teilweis schwer kontrollierbare Netzzugänge. Jeder Netzanschluss kann potentiell zum Abhören des Netzes missbraucht werden.

# G 5.139 Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Shared Medium handelt, können die über ein WLAN übertragenen Daten problemlos aufgezeichnet werden. Aus den aufgezeichneten Daten können unter anderem nachfolgende Informationen gewonnen werden:

- WLAN-Parameter wie SSID, genutzter Funkkanal und eingesetztes Verschlüsselungsverfahren
- MAC-Adressen der Kommunikationspartner im WLAN

Weiterhin können die Broad- und Multicasts aller Stationen in der Broadcast-Domäne, also mitunter auch von Stationen im kabelbasierten LAN, auf dem WLAN beobachtet werden, sofern diese Pakete nicht am Access Point gefiltert werden. Ein Angreifer kann damit trotz funktionierender Verschlüsselung zumindest die MAC-Adressen, und damit die Hersteller, aller Stationen in der Broadcast-Domäne, sowie verwendete Multicast-Adressen ermitteln und damit Informationen über den Einsatz von Layer-2-Protokollen erhalten. Bei mangelhafter Verschlüsselung sind beispielsweise NETBIOS Browser-Nachrichten und damit Informationen über Server-Dienste im LAN direkt zugreifbar.

Bei nicht genutzter oder zu schwacher Verschlüsselung kann weiterhin auf folgende Informationen zugegriffen werden:

- IP-Adressen und genutzte Ports der Kommunikationspartner des WLANs
- Eventuell übertragene Nutzdaten, sofern diese nicht über VPN, SSL oder sonstige Verschlüsselungsmechanismen auf Applikationsebene geschützt sind.

# G 5.140 Auswertung von Restinformationen in Druckern, Kopierern und Multifunktionsgeräten

Viele digitale Kopierer, Drucker und Multifunktionsgeräte sind mit einem umfangreichen internen Speicher ausgestattet. Soll ein Dokument öfters ausgegeben werden, reicht es aus, nur einmal das Quelldokument einzulesen oder an das Gerät zu übertragen. Das Dokument wird digitalisiert (wenn es nicht schon digital vorliegt), im Speicher des Gerätes abgelegt und kann von dort direkt vervielfältigt werden.

Zu unterscheiden sind hierbei zwei Arten von Speichern: flüchtige und nichtflüchtige Speicher. Bei flüchtigen Speichern werden die Daten gelöscht, sobald keine Versorgungsspannung mehr anliegt. Im Gegensatz dazu werden die abgelegten Informationen bei nichtflüchtigen Speichern dauerhaft gespeichert, sie können also auch noch nach einem Ausschalten ausgelesen werden. Beispiele für nichtflüchtige Speicher sind Festplatten und Flashspeicher.

Je nach Arbeitsweise und Konfiguration des Gerätes können die Speicherinhalte bei verschiedenen Ereignissen gelöscht werden. Dies kann zum einen bereits beim Einlesen des nächsten Dokuments möglich sein, zum anderen aber auch erst, wenn Speicherplatz benötigt wird.

Wenn Informationen im Speicher abgelegt wurden, können unter Umständen auch unberechtigte Personen hierauf zugreifen. Im einfachsten Fall ist es dabei lediglich möglich, das zuletzt gespeicherte Dokument auszudrucken. Problematischer ist es, wenn Angreifer den gesamten Speicher auslesen können, um dessen Inhalt zu analysieren.

Auch wenn die gespeicherten Informationen direkt nach der Verwendung gelöscht werden, können die gelöschten Daten unter Umständen rekonstruiert werden. Nicht jedes Gerät überschreibt die gelöschten Daten nach dem Löschen. Ein solches Überschreiben würde die Wiederherstellung gelöschter Daten erheblich erschweren.

Häufig werden digitale Kopierer oder Drucker nur gemietet. Nach einem vorher festgelegten Zeitraum wird das Gerät dann zurückgegeben und eventuell gegen ein aktuelleres ausgetauscht. Alle folgenden Besitzer des Geräts könnten so Zugriff auf noch vorhandene Informationen im Speicher erhalten.

# G 5.141 Datendiebstahl über mobile Datenträger

Viele IT-Systeme haben Schnittstellen für den Einsatz austauschbarer Datenspeicher, wie z. B. Zusatzspeicherkarten oder USB-Speichermedien. Bei einem unbeaufsichtigten IT-System mit der entsprechenden Hard- und Software besteht die Gefahr, dass über diese Datenspeicher große Mengen an Daten unbefugt kopiert werden können. Dieser Vorgang ist in der Regel nach kurzer Zeit abgeschlossen und noch nicht einmal direkt erkennbar.

Natürlich können diese Schnittstellen auch in umgekehrter Weise benutzt werden, um hierüber Schadprogramme auf einem IT-System oder in ein Netz einzuschleusen.

Mobile Datenträger können auch in Geräten mit weiteren Aufzeichnungsfunktionen integriert sein, z. B. in Mobiltelefonen, MP3-Playern oder Digitalkameras. Auch hierüber können unter Umständen sensible Informationen unbefugt aufgenommen werden (siehe G 5.126 *Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten*).

# G 5.142 Verbreitung von Schadprogrammen über mobile Datenträger

Mobile Datenträger werden oft für den Austausch von Daten zwischen dem heimischen PC und dem Arbeitsplatz genutzt. Private Rechner werden jedoch nicht immer in dem Maße geschützt, das dem Sicherheitsniveau der Behörde oder des Unternehmens entspricht. Beispielweise werden private Rechner häufig von Personen, die weniger für Informationssicherheit sensibilisiert sind, zum Zugriff auf das Internet genutzt. Typisches Beispiel ist die Nutzung von Web-Seiten mit aktiven Inhalten durch Kinder oder Jugendliche, um an Online-Spielen oder Chats teilzunehmen.

Durch die oft weniger restriktive Konfiguration und die oft weniger kontrollierte Nutzung des heimischen PCs können sich Schadprogramme dort leichter einnisten und sich gegebenenfalls über mobile Datenträger auf den Arbeitsplatz übertragen.

Gefahr durch Schadprogramme geht jedoch nicht nur von privaten IT-Systemen aus. Auf Messen, Kongressen und ähnlichen Veranstaltungen werden zum Beispiel häufig mobile Datenträger genutzt, um Dokumente, Vortragsfolien und andere Informationen auszutauschen. Auch hier besteht die Gefahr, dass sich Schadprogramme auf diesem Weg verbreiten.

**Beispiele:**

- MP3-Player werden wegen ihrer hohen Speicherkapazität auch gerne als mobile Datenspeicher eingesetzt, und zwar nicht nur für Musikdateien. Dies kann bei der Nutzung im betrieblichen Umfeld dazu führen, dass durch die Vermischung privater und dienstlicher Dateien versehentlich dienstliche Informationen an Freunde und Bekannte weitergegeben werden. Dabei können aber auch umgekehrt Schadprogramme in eine Institution eingeschleppt werden.
- Auf einem Kongress möchte ein Besucher die Folien des eben gehaltenen Vortrags haben und fragt den Dozenten, ob er ihm die Folien zur Verfügung stellen kann. Der Dozent gibt dem Besucher seinen USB-Stick, auf dem sich die Vortragsfolien befinden. Als der Besucher den USB-Stick in seinen Laptop gesteckt hat, um sich die Folien zu kopieren, installiert sich unbemerkt ein auf dem USB-Stick befindliches Schadprogramm.

# G 5.143 Man-in-the-Middle-Angriff

Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer "in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf die Antworten des Empfängers kann der Angreifer wiederum ebenfalls zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind.

Der für den Angreifer schwierigste Teil eines Man-in-the-Middle-Angriffs ist häufig, den Verbindungsaufbau auf sich umzuleiten. Durch entsprechende Verfahren, wie Spoofing oder DNS-Manipulationen, kann dieser Angriff eingeleitet werden.

Sogar eine verschlüsselte Verbindung schützt nicht immer vor Man-in-the-Middle-Angriffen. Wird die Identität der Kommunikationspartner gefälscht oder nicht geprüft, könnte jeweils eine verschlüsselte Verbindung vom Sender zum Angreifer und vom Angreifer zum Empfänger aufgebaut werden. Da der Angreifer jeweils der Endpunkt der einzelnen Verbindungen ist, kann er in diesem Fall die Informationen entschlüsseln, einsehen und verändern, bevor er sie wieder verschlüsselt und weitersendet.

Eine spezielle Form eines Man-in-the-Middle-Angriffs ist das sogenannte Malicious Morphing. Der Angreifer modifiziert dabei den Inhalt oder die Struktur einer Nachricht und kann so beim Service-Provider sowohl die Integrität von Daten als auch die Funktionsweise von Systemkomponenten gefährden, zum Beispiel durch einen Denial-of-Service-Angriff.

**Beispiele:**

- Einem Angreifer gelingt es durch DNS-Spoofing, einige Nameserver so zu manipulieren, dass bei DNS-Abfragen statt der IP-Adresse einer bestimmten Bank die IP-Adresse seines Rechners zurückgegeben wird. Ein Benutzer möchte daraufhin eine Verbindung zum Webserver der Bank aufbauen, um Homebanking zu nutzen. Um für den Verbindungsaufbau die IP-Adresse des Webservers zu ermitteln, sendet der Rechner des Benutzers eine Anfrage mit dem Rechnernamen der Bank an den DNS-Server, der aber mit der gefälschten IP-Adresse des Angreifers antwortet. Daraufhin baut der Benutzer aufgrund der gefälschten IP-Adresse eine HTTPS-Verbindung zum Rechner des Angreifers auf. Der Browser zeigt zwar Warnhinweise an, dass das SSL-Zertifikat ungültig ist, der Benutzer ignoriert diese Hinweise jedoch, da er sie nicht versteht. Als Folge wird der Benutzer auf den Webserver des Angreifers umgeleitet. Der Angreifer baut daraufhin eine verschlüsselte https-Verbindung zur Bank auf. Alle Transaktionen, die der Benutzer in der anschließenden Web-Session durchführt, kann der Angreifer einsehen und manipulieren.
- Um Man-in-the-Middle-Attacken in einem WLAN durchzuführen, könnten zusätzliche Access Points in das WLAN eingeschleust werden ("Cloning" oder "Evil Twin"). Wenn ein solcher Access Point einem in der Nähe befindlichen WLAN-Client eine stärkere Sendeleistung anbietet als der echte

Access Point, wird der Client diesen als Basisstation benutzen, falls keine beidseitige Authentisierung erzwungen wird.

# G 5.144 Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff

Wenn es einem Angreifer gelungen ist, eine notwendige Authentisierung gegenüber dem Verzeichnisdienst erfolgreich zu umgehen, kann er danach im Allgemeinen auf eine Vielzahl von Daten zugreifen, für die er keine Berechtigung besitzt. Somit kann der gesamte Verzeichnisdienst durch das Umgehen der Authentisierungsmethoden kompromittiert werden.

Eine weitere Gefahr besteht darin, dass durch Erweiterung von Berechtigungen, Unbefugten Zugriffe auf Netzressourcen oder Dienste ermöglicht wird. Dies kann bis zu einer vollständigen Durchdringung aller Verteidigungsmaßnahmen des Verzeichnisdienstes durch einen Angreifer führen. Dadurch könnte das betroffene System beeinträchtigt oder gar zerstört werden. Beispiel-Szenarien hierzu wären das missbräuchliches Aneignen unbeschränkter Rechte oder Spoofing einer Identität mit mehr Rechten als der eigenen, um höhere Berechtigungen zu erhalten.

Für den Fall, dass es einem Dritten gelingt, einen Verzeichnisdienst unautorisiert zu benutzen, können Schäden verschiedenster Art die Folge sein. Beispiele für solche Schäden sind:

- Bei der unautorisierten Nutzung eines Verzeichnisdienstes könnte es dem Angreifer gelingen, geheime Schlüssel auszulesen, die Schlüssel zu verändern, die Schlüssel einer Zertifizierungsstelle im Verzeichnisdienst zu nutzen oder auch kritische Sicherheitsparameter zu manipulieren. Die Folge wäre, dass die kryptographischen Verfahren die erwartete Sicherheit nicht mehr bieten, also die Vertraulichkeit oder Integrität der damit geschützten Daten nicht mehr gewährleistet ist.
- Wenn der Verzeichnisdienst für Anmelde-Prozeduren vorgesehen ist und eine Autorisierung aufgrund einer festgestellten Identität allgemein im Netz gültig ist, können durch unberechtigte Authentisierungen weitere Ressourcen, insbesondere anderen Systemen im Netz, gefährdet werden. Somit können weitere Systeme kompromittiert werden, wenn auch der Verzeichnisdienst kompromittiert wurde. Ein Verzeichnisdienst kann dazu dienen, dass eine einmalige Authentisierung zur Erlangung von Rechten auf anderen Systemen führt, die ohne Verzeichnisdienst erst nach einer weiteren Authentisierung auf diesen Systemen erreicht würden. Dadurch könnten auch diese Systeme kompromittiert werden, wenn der Verzeichnisdienst kompromittiert wird.

Die Sicherheit eines Verzeichnisdienstes kann ebenfalls gefährdet werden, wenn anonyme Benutzer zugelassen werden. Dadurch, dass deren Identität nicht überprüft wird, können anonyme Benutzer zunächst beliebige Abfragen an den Verzeichnisdienst richten, durch die sie zumindest Teilinformationen über dessen Struktur und Inhalt erlangen. Wenn ein sogenanntes "Anonymes Binden" (bei LDAP) an den Verzeichnisdienst (außer zur Authentisierung selbst) nicht möglich ist, werden Anfragen grundsätzlich mit einer Fehlermeldung beantwortet, andernfalls bekommen Angreifer zumindest Teilinformationen über den Verzeichnisdienst. Diese Informationen können als Vorbereitung auf weitere Angriffe dienen.

Dies ist besonders dann der Fall, wenn Informationen über Ressourcen im Netz und über das Netz selbst preisgegeben werden.

Wenn anonyme Zugriffe zugelassen werden, sind außerdem DoS-Attacken auf den Verzeichnisdienst leichter durchführbar, da Angreifer mehr schlecht kontrollierbare Zugriffsmöglichkeiten haben.

# G 5.145 Manipulation von Daten und Werkzeugen beim Patch- und Änderungsmanagement

Das Patch- und Änderungsmanagement agiert in der Regel von zentraler Stelle aus. Aufgrund seiner exponierten Stellung ist es besonders gefährdet für Angriffe. Wenn es Angreifern gelingen sollte, die beteiligten Server zu übernehmen, könnten sie über diesen zentralen Punkt manipulierte Softwareversionen gleichzeitig auf eine Vielzahl von IT-Systemen verteilen.

Oft entstehen weitere Angriffspunkte dadurch, dass diese Systeme von externen Partnern betrieben werden (Outsourcing). Es könnten auch Wartungszugänge eingerichtet sein, die es Angreifern ermöglichen können, Zugriff auf den zentralen Server zur Verteilung von Patches und Änderungen zu erhalten.

**Beispiel:**

- Lädt ein Werkzeug zum Patch- und Änderungsmanagement Daten aus einer Internetquelle herunter, ohne dass die Authentizität der Webseite geprüft und die Verbindung abgesichert wird, so besteht die Gefahr, dass ein Angreifer über diesen Datenstrom manipulierte Pakete einschleusen könnte. Dadurch könnte er Zugriff auf das zentrale System des Änderungsmanagements und die gepatchten Systeme erhalten.
- Angreifern gelang es in einem Unternehmen, den zentralen Updateserver einer Linux-Distribution zu übernehmen. Danach ersetzten sie wichtige Programmpakete durch trojanisierte Versionen. Jeder Benutzer des Updateservers installierte sich somit Schadsoftware und damit einen Zugang für die Angreifer auf seinem Rechner.

# G 5.146 Vertraulichkeitsverlust durch Auslagerungsdateien

Damit Anwendungen vom Prozessor eines IT-Systems ausgeführt werden können, müssen sie vollständig oder teilweise in den Arbeitsspeicher kopiert werden. Moderne Betriebssysteme sind Multitasking-fähig, so dass mehrere Anwendungen gleichzeitig ausgeführt werden können. Dabei reicht besonders bei umfangreichen Anwendungen der vorhandene Arbeitsspeicher oft nicht aus. Daher wird bei vielen Betriebssystemen der zur Zeit nicht verwendete Teil des Arbeitsspeichers auf die Festplatte ausgelagert.

Diese Auslagerungen werden als Auslagerungsdateien oder Auslagerungspartition ("Swap") bezeichnet, wobei der Begriff "Auslagerungsdatei" hauptsächlich durch das Betriebssystem Microsoft Windows geprägt ist. Das Betriebssystem verwaltet die Auslagerungsdatei selbständig und passt sie dynamisch der Größe des benötigten Speichers an. Benötigt die Ausführung eines Prozesses mehr Speicherplatz, wird die Auslagerungsdatei größer. Sobald weniger Speicherplatz gebraucht wird, weil beispielsweise Anwendungen beendet werden, verkleinert sich die Auslagerungsdatei wieder. Wird die Größe der Auslagerungsdatei im Voraus festgelegt, kann die Arbeit mit Windows, vor allem bei geringem Hauptspeicher, beschleunigt werden.

Meldet sich ein Benutzer vom System ab bzw. wird das System ausgeschaltet, werden die Auslagerungsdateien nicht automatisch gelöscht. Daher finden sich in der Auslagerungsdatei Teile der Informationen wieder, die die Benutzer während ihrer Arbeit mit dem IT-System verwendet haben. Dazu können auch sensible Daten wie Passwörter oder kryptographische Schlüssel gehören. Der Schutz der Daten ist somit nicht gewährleistet, da diese z. B. unter Umgehung sämtlicher Zugriffskontrollen ausgelesen werden können, wenn die Festplatte ausgebaut und in einem anderen Computer eingebaut wird.

**Beispiel:**

Einige Benutzer eines Unternehmens haben sich darüber beschwert, wie lange es dauert, ihre Clients herunterzufahren. Daher setzt der zuständige Administrator den entsprechenden DWORD-Wert auf 0, so dass die Auslagerungsdateien beim Herunterfahren der Clients nicht mehr automatisch gelöscht werden.

Als ein Laptop mit wichtigen Unternehmensdaten auf einer Dienstreise verschwindet, werden kurz darauf interne Informationen auf einer fremden Webseite veröffentlicht. Dies legt den Verdacht nahe, dass es einem Unbefugten gelang, kritische Daten auszulesen und das System zu starten.

# G 5.147 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes

Für den Betrieb einer virtuellen Infrastruktur sind vielfältige Netzverbindungen notwendig. Diese Verbindungen werden genutzt, um auf Speichernetze zugreifen zu können. Weiterhin werden Verbindungen zwischen den einzelnen Virtualisierungsservern benötigt, um die Steuerung und Überwachung der Virtualisierungsserver und der virtuellen IT-Systeme zu ermöglichen. Für Hochverfügbarkeitsfunktionen oder die so genannte *Live Migration* (Verschieben von virtuellen IT-Systemen zwischen Virtualisierungsservern im laufenden Betrieb) werden ebenfalls Netzverbindungen benötigt. Diese Netzverbindungen werden im Folgenden als "Virtualisierungsnetz" bezeichnet.

Innerhalb einer virtuellen Infrastruktur können zwischen Virtualisierungsservern einzelne virtuelle IT-Systeme übertragen werden (*Live Migration*). Dies geschieht z. B. zur Lastverteilung, zu Wartungszwecken oder zur Ausfallkompensation. Dabei müssen der Prozessorzustand und der Hauptspeicherinhalt sowie die Konfigurationsdaten des virtuellen IT-Systems von dem einen Virtualisierungsserver auf den anderen übertragen werden. Diese Übertragung erfolgt durch das so genannte Virtualisierungsnetz. Die von den Herstellern der Virtualisierungslösungen verwendeten Übertragungsprotokolle sehen häufig keine Verschlüsselungsmechanismen für diesen Datenstrom vor. Hierdurch ist es möglich, dass Personen, die unautorisiert Zugang zum Virtualisierungsnetz erlangen, vertrauliche Inhalte der transferierten Gastsysteme wie z. B. den Hauptspeicherinhalt mitlesen. Beispielsweise können im Hauptspeicher enthaltene vertrauliche Daten, die sonst nur verschlüsselt durch das Netz übertragen werden, mit gelesen und eventuell sogar verändert werden. Nutzen die Virtualisierungsservern ein zentrales Speichernetz, betrifft die mögliche Kompromittierung auch die Inhalte des angeschlossenen Speichernetzes (siehe hierzu auch G 5.129 *Manipulation von Daten über das Speichersystem* sowie G 5.7 *Abhören von Leitungen* und G 5.8 *Manipulation von Leitungen*).

Ein manipulierter Virtualisierungsserver kann das Virtualisierungsnetz darüber hinaus stören, in dem der Angreifer auf die im Netz übertragenen Informationen zugreift und Netzpakete unterdrückt oder verändert. Es kann beispielsweise sein, dass Veränderungen an Hauptspeicherinhalten eines virtuellen IT-Systems bei deren Übertragung während einer *Live Migration* durch den Virtualisierungsserver nicht geprüft werden. So könnten dann Hauptspeicherinhalte eines Gastsystems durch einen Angreifer verändert werden.

Wird die Kommunikation im Virtualisierungsnetz gestört, können Migrationen im laufenden Betrieb fehlschlagen. Hierdurch kann es zu Ressourcenengpässen in der virtuellen Infrastruktur kommen, wenn diese Migrationen ausgelöst wurden, um diese Engpässe zu verhindern.

**Beispiel:**

Ein mittelständisches Unternehmen setzt einen Datenbankserver zur Verarbeitung der Personaldaten seiner Mitarbeiter ein. Um diese Personaldaten zu schützen, werden die Datenbankinhalte nur verschlüsselt auf die Festplatten des Datenbankservers geschrieben. Die Client-Anwendung, mit der die Benutzer der Personalabteilung arbeiten, kommuniziert ebenfalls verschlüsselt mit dem Datenbankserver. Das Datenbanksystem selbst hält allerdings während der Verarbeitung die Daten teilweise unverschlüsselt in seinem Hauptspeicher.

Dieses Datenbanksystem ist im Zuge des Virtualisierungsprojektes im Unternehmen virtualisiert worden. Der Administrator der Virtualisierungsserver möchte nun an Gehaltsdaten der Personaldatenbank gelangen, um bei Gehaltsverhandlungen seine Position zu verbessern, da er das Gefühl hat, im Vergleich zu seinen Kollegen unterbezahlt zu sein. Er hat das Datenbanksystem aufgebaut und weiß daher, wie dieses System arbeitet. Er besitzt jedoch keine Möglichkeit, über Funktionen des Servers oder der Datenbanksoftware unbemerkt an die Daten des Systems heranzukommen. Daher installiert er im Virtualisierungsnetz ein Netzüberwachungswerkzeug, mit dem er den Netzverkehr in diesem Netz mitlesen kann.

Er weist nun die Virtualisierungsserver an, den Datenbankserver im laufenden Betrieb (*Live Migration*) zwischen zwei Servern zu verschieben. Er liest die Übertragung des Hauptspeichers im Netz mit und zeichnet sie auf. Nach mehreren mitgeschnittenen Migrationen kann er eine vollständige Kopie der Gehaltstabelle aus den aufgezeichneten Inhalten des Hauptspeichers des Datenbankservers rekonstruieren.

Dieser Angriff auf die Vertraulichkeit der Daten der Personalverwaltung bleibt unbemerkt, da die Live Migration völlig transparent für das Datenbanksystem und die Client-Anwendung verläuft.

# G 5.148 Missbrauch von Virtualisierungsfunktionen

Die meisten Virtualisierungsprodukte enthalten Werkzeuge, um virtuelle Maschinen oder bestimmte Zustände der virtuellen Maschinen einfrieren zu können. Diese Funktionen basieren in der Regel darauf, dass die Festplattencontainer der virtuellen IT-Systeme kopiert oder die Zustände des Arbeitsspeichers und des Prozessors des virtuellen IT-Systems auf einen Massenspeicher des Virtualisierungsserver abgespeichert werden.

Jeder Virtualisierungsserver hat Zugriff auf alle Speicherressourcen der von ihm verwalteten virtuellen Maschinen. Es besteht daher die Gefahr, dass vom Virtualisierungsserver auf solche Ressourcen unautorisiert zugegriffen wird, um Daten unerlaubt zu kopieren oder zu verändern. Daher kann ein Angreifer leicht eine Kopie einer virtuellen Maschine herstellen, um diese unerlaubt aus dem Rechenzentrum zu entfernen und beispielsweise auf einem eigenen Virtualisierungsserver zu betreiben. Die erstellte Kopie kann er dazu nutzen, um die virtuelle Maschine zu untersuchen.

Des Weiteren kann ein unveränderter Klon einer virtuellen Maschine zu einem IP-Adressen- oder sonstigen Ressourcenkonflikt im Rechenzentrumsbetrieb führen, wenn ein solcher Klon vor dem Start nicht angepasst wird.

Bei einigen Virtualisierungsprodukten können Snapshots einer virtuellen Maschine auch im laufenden Betrieb erzeugt werden. In diesem Fall wird der Prozessorzustand und der Inhalt des Hauptspeichers auf eine Festplatte des Virtualisierungsservers geschrieben. Des Weiteren wird der Festplattencontainer der virtuellen Maschine ebenfalls eingefroren und Änderungen werden in eine Differenzdatei geschrieben. Diese Daten können kopiert werden, um mittels eines anderen Virtualisierungsservers einen laufenden Klon der virtuellen Maschine zu erzeugen. Die gespeicherten Inhalte des Prozessorzustands und des Hauptspeichers der virtuellen Maschine können zudem von einem Angreifer verwendet werden, um Speicherbereiche der virtuellen Maschine zu analysieren. Hier können beispielsweise Schlüssel von Verschlüsselungswerkzeugen, die unverschlüsselt im Hauptspeicher der virtuellen Maschine gespeichert sind, extrahiert werden.

Weiterhin ist es möglich, durch die Verwendung von Snapshots virtuelle Maschinen auf einen alten Stand zurück zu setzen. Hierdurch können Maßnahmen unterlaufen werden, die beispielsweise unternommen wurden, um Sicherheitslücken zu schließen.

Durch das Zurücksetzen einer virtuellen Maschine auf einen Snapshot können auch Angriffe verschleiert werden, die ansonsten in den Protokolldateien der virtuellen Maschinen aufgezeichnet würden. Mit dem Zustand der virtuellen Maschine wird ebenfalls ihre Protokolldatei zurückgesetzt.

Werden ältere Snapshots aktiviert, können auch Daten wiederhergestellt werden, die gelöscht sein sollten. Wird das virtuelle IT-System auf den Snapshot zurückgesetzt, sind die vermeintlich gelöschten Daten wieder vorhanden. Auch die Verwendung von Werkzeugen, die den Inhalt einer Datei mehrfach überschreiben, um eine Wiederherstellung unmöglich zu machen, ist wirkungslos, wenn ein Snapshot erzeugt wurde, bevor das Werkzeug innerhalb des virtuellen IT-Systems verwendet wird. Ist für eine virtuelle Maschine ein Snapshot erzeugt worden, wirken sich die Überschreibvorgänge nur auf die Differenzdatei aus, die die Änderungen enthält, die seit Erzeugung des Snapshots erfolgt sind. Wird der Snapshot gelöscht und die Änderungen in der Diffe-

renzdatei werden auf den Festplattencontainer angewandt, werden die scheinbar mehrfachen Überschreibvorgänge nur einmal in den Festplattencontainer geschrieben.

**Beispiel:**

Im Rechenzentrum eines Unternehmens, das in der Grundlagenforschung tätig ist, werden in einem virtuellen IT-System Daten mit einer hohen Schutzbedarfskategorie bezüglich Vertraulichkeit verarbeitet. Daher wird in der virtuellen Maschine ein Festplattenverschlüsselungsprogramm installiert. Dieses erfordert die Angabe eines Kennworts während des Startvorgangs. Das Kennwort ist nur wenigen, besonders vertrauenswürdigen Mitarbeitern des Unternehmens bekannt.

Das Festplattenverschlüsselungsprogramm arbeitet für das Betriebssystem der virtuellen Maschine transparent. Das heißt, es muss während des Betriebs der virtuellen Maschine kein weiteres Kennwort eingegeben werden.

Während des Betriebs der virtuellen Maschine sind die Daten durch die Einschränkung von Berechtigungen geschützt. Zudem werden Benutzerkonten automatisch gesperrt, wenn mehrfach versucht wird, mittels dieser Konten unberechtigt Zugang zu den Daten zu erlangen.

Durch den Einsatz des Festplattenverschlüsselungsprogramms sind die Daten der virtuellen Maschine im Speichernetz geschützt. Der Rechenzentrumsbetreiber geht daher davon aus, dass das Kopieren des Festplattencontainers der virtuellen Maschine keine für einen Angreifer verwertbaren Daten ergibt. Zudem glaubt er durch die Berechtigungsvergabe und die automatische Kontensperre ein ausreichendes Sicherheitsniveau erreicht zu haben.

Ein Mitarbeiter dieses Rechenzentrums befindet sich in finanziellen Schwierigkeiten. Ein Mitbewerber des Rechenzentrumsbetreibers bietet nun diesem Mitarbeiter eine hohe Summe an Geld, wenn dieser ihm Zugriff auf die Daten, die in der virtuellen Maschine verarbeitet werden, verschafft.

Der Mitarbeiter erzeugt infolgedessen auf dem Virtualisierungsserver einen Snapshot der virtuellen Maschine im laufenden Betrieb. In dem Snapshot sind die Arbeitsspeicherinhalte sowie der Prozessorzustand des virtuellen IT-Systems enthalten. Er kopiert die Konfigurationsdatei, den Festplattencontainer, den Inhalt des Arbeitsspeichers und den CPU-Zustand der virtuellen Maschine auf einen transportablen Massenspeicher und verlässt mit diesem die Institution.

Die Kopie der virtuellen Maschine kann jetzt auf dem Virtualisierungsserver des Mitbewerbers ausgeführt werden. Da der Virtualisierungsserver die Laufzeitumgebung der virtuellen Maschine aus den gespeicherten Daten wiederherstellt, erfolgt keine Passwortabfrage durch das Festplattenverschlüsselungsprogramm. Das Betriebssystem in der virtuellen Maschine "bemerkt" nichts von dieser Betriebsunterbrechung.

Der Angreifer versucht durch Brute Force-Attacken die Kennwörter der berechtigten Benutzer zu ermitteln. Um den Vorgang zu beschleunigen, erzeugt er mehrere Kopien der virtuellen Maschine. Wird ein Konto aufgrund der Fehlversuche gesperrt, setzt er die virtuelle Maschine wieder auf den Zustand vor der Kontensperre zurück und fährt mit der Brute Force-Attacke fort.

# G 5.149 Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen

Bei vielen Virtualisierungsprodukten werden in den virtuellen IT-Systemen sogenannte Gastwerkzeuge installiert. Mit diesen Gastwerkzeugen können zum Einen die für Betriebssystemvirtualisierung notwendigen Gerätetreiber für virtuelle oder emulierte Geräte wie Netzwerkkarten, Festplatten oder Grafikkarten bereitgestellt werden. Zum Anderen werden mit diesen Werkzeugen innerhalb der virtuellen IT-Systeme Programme zur Kommunikation mit dem Hypervisor oder dem Hostbetriebssystem, zur Steigerung der Leistung des virtuellen IT-Systems und zur Vereinfachung der Bereitstellung neuer virtueller IT-Systeme installiert. Mit Hilfe der Gastwerkzeuge können des Weiteren die virtuellen IT-Systeme überwacht werden. Der Hypervisor oder das Hostbetriebssystem überwacht hierüber beispielsweise die Verfügbarkeit und die Leistung des Gastes.

Die Gastwerkzeuge werden wegen ihrer systemnahen Funktion häufig mit sehr hohen Berechtigungen ausgeführt. Häufig laufen sie im Kontext und damit mit den Rechten des Betriebssystemkerns der virtuellen Maschine.

Funktionen wie die Überbuchung von Hauptspeicher oder Massenspeicherplatz für virtuelle IT-Systeme werden zwischen dem Hypervisor und dem virtuellen IT-System durch die Gastwerkzeuge koordiniert. Diese Funktionen stellen einen wesentlichen Mehrwert der Virtualisierungstechnik im Rechenzentrumsbetrieb dar.

Bei einigen für die Software-Entwicklung spezialisierten Virtualisierungsprodukten ist weiterhin eine Möglichkeit für den komfortablen Aufbau komplexer Testszenarien vorgesehen. Dies wird häufig ebenfalls über die Gastwerkzeuge realisiert oder unterstützt. Hierzu haben die Gastwerkzeuge Schnittstellen, um Skriptdateien auf virtuelle IT-Systeme zu übertragen. Diese Skripte können dann ebenfalls über die Gastwerkzeuge im virtuellen IT-System ausgeführt werden. Es können alle in dem virtuellen IT-System verfügbaren Skriptsprachen genutzt werden. Der Start der Skripte kann entweder beim Systemstart, der Anmeldung eines Benutzers oder auch zu jeder anderen beliebigen Zeit angestoßen werden. Die Schnittstellen benötigen in der Regel keine Netzverbindung zwischen den Gastsystemen, sondern werden über den Hypervisor oder das Hostbetriebssystem bereitgestellt.

Diese Schnittstellen für Skripte können durch einen Angreifer ausgenutzt werden, um eine unerwünschte und nicht mit klassischen Mitteln kontrollierbare Kommunikation über mehrere virtuelle IT-Systeme hinweg aufzubauen. Hierbei überträgt der Angreifer die Daten über die Schnittstelle zum Transport von Skriptdateien.

Weiterhin ist es einem Angreifer bei den beschriebenen für die Software-Entwicklung konzipierten Virtualisierungsprodukten möglich, mittels der Gastwerkzeuge von einem virtuellen IT-System aus eigene Skriptdateien auf ein anderes virtuelles IT-System zu übertragen. Diese können mit den Rechten, mit denen die Gastwerkzeuge laufen, ausgeführt werden. Auf Grund der weit reichenden Berechtigung der Gastwerkzeuge ist dies besonders kritisch, da damit beliebige Aktionen in dem betroffenen Gastsystem ausführbar sind. Es können beispielsweise Schadprogramme gestartet, Benutzer angelegt, Grup-

penmitgliedschaften verändert oder die Konfiguration des Betriebssystems des virtuellen IT-Systems manipuliert werden.

**Denial of Service durch Überbuchung von Ressourcen**

Einige Virtualisierungsprodukte ermöglichen die Überbuchung verschiedener Ressourcen wie Festplattenplatz oder RAM. Konkurrieren beispielsweise zwei virtuelle IT-Systeme um Arbeitsspeicher, kann das Hostbetriebssystem oder der Hypervisor die Gastwerkzeuge anweisen, virtuelles RAM in dem einen virtuellen IT-System zu reservieren. Die physikalische Repräsentation dieses Speichers wird nun durch das virtuelle IT-System nicht genutzt. Der Hypervisor kann diesen physikalischen Speicher dem anderen virtuellen IT-System als virtuelles RAM zur Verfügung stellen. Andersherum kann ein virtuelles IT-System über die Gastwerkzeuge auch Hauptspeicher anfordern.

Hat ein Angreifer ein virtuelles IT-System unter seiner Kontrolle, könnte er über ein Schadprogramm so viel Hauptspeichern anfordern, dass dieser für andere virtuelle IT-Systeme knapp wird. Hierdurch wird die Leistungsfähigkeit der anderen virtuellen IT-Systeme bis hin zu einer Denial of Service-Attacke beeinflusst. Der gleiche Effekt tritt auf, wenn ein Angreifer von außen auf einen Dienst eines virtuellen IT-Systems in der Weise zugreift, dass dieser sehr viel Speicher belegt.

Wird eine Funktion zur Überbuchung von Festplattenplatz genutzt, existiert meist ebenfalls eine Möglichkeit, diesen Speicher wieder frei zu geben. Dies geschieht dadurch, dass unbenutzter Speicherplatz zusammengefasst und als frei markiert wird.

Löst ein Angreifer einen solchen Prozess in einem virtuellen IT-System aus, werden die Speichersysteme stark belastet. Auch hierdurch kann die Leistungsfähigkeit anderer IT-Systeme verringert werden.

**Beispiele:**

- Ein Systemhaus bearbeitet Softwareentwicklungsaufträge für verschiedene Kunden. Hierzu wird durch das Systemhaus eine auf Entwicklungsaufgaben spezialisierte Virtualisierungsumgebung betrieben, da für die Entwicklung von Client-Server-Anwendungen umfangreiche Testszenarien aufgebaut werden müssen. Die Testsysteme für diese Szenarien werden über mehrere Vorlagen für verschiedene virtuelle Server und Clients bereitgestellt, die bei Bedarf kopiert und an das jeweilige Testszenario angepasst werden.
  Aufgrund der schlechten Auftragslage des Systemhauses müssen einige Entwickler entlassen werden. Einer der entlassenen Entwickler will sich für seine Entlassung rächen und entwickelt ein Skript, dass ein virtuelles Testsystem immer wieder auf den Ursprungszustand der Vorlage zurücksetzt, sobald sich ein Benutzer zum zweiten Mal an dem virtuellen System anmeldet. Dabei sieht es so aus, als hätte der Benutzer, der sich angemeldet hat, den Rücksetzvorgang ausgelöst. Tatsächlich wird dieses Skript jedes mal durch die Virtualisierungssoftware in das Testsystem eingebracht, sobald es zum zweiten Mal gestartet wird. Zusätzlich überträgt sich das Skript selbständig über eine Virtualisierungsfunktion auf jedes in der virtuellen Infrastruktur laufende virtuelle Testsystem.
  Die Verantwortlichen des Systemhauses vermuten einen Wurmbefall ihrer Systeme und beauftragen ein IT-Beratungsunternehmen mit der Durchführung einer Netzanalyse, um die Ursache des Problems zu ermitteln. Das Beratungsunternehmen kann aber keine Auffälligkeiten im Netz des Systemhauses feststellen. Nur durch einen Zufall bemerkt einer der Ent-

wickler den von seinem ehemaligen Kollegen durchgeführten Angriff auf die Testumgebung.
Durch die Fehlersuche und die Störung des Testbetriebs wurden erhebliche personelle Ressourcen gebunden und Termine nicht eingehalten. Dadurch entstand dem schon finanziell geschwächten Systemhaus weiterer Schaden.

- Ein Dienstleister betreibt eine Webserverfarm für mehrere Kunden. Um Hardwarekosten zu sparen, hat er die Webserver virtualisiert. Dabei stellt er den Kunden für deren virtuelle Systeme in Summe sehr viel mehr Hauptspeicher zur Verfügung als in der virtuellen Infrastruktur tatsächlich vorhanden ist. Da die Webserver der Kunden in der Regel nur schwach ausgelastet sind, kommt es zu keinen spürbaren Performanceeinschränkungen in den virtuellen Systemen.
  Einer der Webserver der Kunden wird nun Opfer eines Denial of Service-Angriffs. Dabei verbraucht dieses virtuelle IT-System sehr viel Hauptspeicher. Dieser Speicher steht allerdings in dem physischen Virtualisierungsserver, auf dem der virtuelle Webserver läuft, nicht als frei zur Verfügung, sondern wird von anderen virtuellen Webservern genutzt. Um dem angegriffenen System diesen Speicher zur Verfügung stellen zu können, muss dieser von anderen virtuellen IT-Systemen freigegeben werden. Der Hypervisor des Virtualisierungsservers verknappt somit den Hauptspeicher für alle anderen unter seiner Kontrolle laufenden, virtuellen Webserver. In der Folge steigen die Antwortzeiten der virtuellen Webserver stark an. Teilweise kommt es hier zu Verbindungsabbrüchen, so dass auch die virtuellen Webserver, die nicht direkt Ziel des DoS-Angriffs waren, nicht mehr verfügbar sind.

# G 5.150 Kompromittierung des Hypervisor virtueller IT-Systeme

Der Hypervisor ist die zentrale Komponente eines Virtualisierungsservers, er steuert alle auf diesem Virtualisierungsserver ausgeführten virtuellen Maschinen. Er teilt ihnen Prozessor- und Hauptspeicherressourcen zu und verteilt die zur Verfügung stehende Rechenzeit auf die virtuellen Maschinen. Des Weiteren verwaltet er den Zugriff der virtuellen IT-Systemen auf das Netz und die Speicher-Ressourcen. Ein erfolgreicher Angriff auf diese Komponente bedeutet den Verlust der Kontrolle über alle virtuellen IT-Systeme, die im Kontext dieses Hypervisors ausgeführt werden. Ein Angriff auf den Hypervisor kann im Wesentlichen folgendermaßen ausgeführt werden:

- Manipulation der CPU-Register, die bei Prozessoren mit integrierter Virtualisierungsunterstützung die Virtualisierungsfunktionen steuern. Mittels solcher Angriffe kann beispielsweise festgestellt werden, ob sich der Angreifer in einer virtuellen Umgebung befindet. Bei einigen Virtualisierungsprodukten kann über bestimmte Prozessorbefehle der Hypervisor selbst virtualisiert werden und so unter die Kontrolle eines Schadprogramms gebracht werden. Dies ist sogar aus einem virtuellen IT-System heraus möglich.
- Ausnutzung eines Fehlers in der Implementierung der Ressourcen, die den virtuellen IT-Systemen durch den Hypervisor zur Verfügung gestellt werden. Dies kann beispielsweise emulierte Netzwerkkarten, Massenspeichergeräte oder Grafikkarten betreffen. Bei einigen Virtualisierungsprodukten werden auch Kernkomponenten wie Prozessor und Hauptspeicher emuliert. Die Geräteemulationen werden durch die virtuellen IT-Systeme verwendet, um die entsprechenden Funktionen des Hypervisors bzw. des Hostbetriebssystems zu nutzen.
- Als zentrale Komponente übernimmt der Hypervisor eine Reihe von sicherheitskritischen Funktionen einer Virtualisierungslösung. Gelingt es einem Angreifer, den Hypervisor zu kompromittieren, ist dadurch der sichere Betrieb der jeweiligen virtuellen IT-Systeme und der jeweiligen Virtualisierungsserver in hohem Maße gefährdet. Angreifer können versuchen, auf diesem Wege virtuelle IT-Systeme zu manipulieren oder zu stören. Unter Umständen können dadurch auch vertrauliche Informationen an Unbefugte gelangen. Schwachstellen im eingesetzten Hypervisor-Produkt können deshalb erhebliche Risiken für die Informationsverarbeitung mit sich bringen.
- Einige Virtualisierungssysteme beinhalten zudem Funktionen zur Kommunikation zwischen dem Hypervisor und den virtuellen IT-Systemen. Diese werden in der Regel durch Gastwerkzeuge realisiert, die im virtuellen IT-System installiert werden. Um die Kommunikation zwischen den Gastwerkzeugen und dem Hypervisor zu ermöglichen, besitzt jedes virtuelle IT-System einen Kommunikationskanal für die Gastwerkzeuge zum Hypervisor. Hierzu existiert zum Beispiel in virtuellen IT-Systemen auf der Basis der Produkte des Herstellers VMware ein spezieller DMA-Kanal, der einen solchen Kanal öffnet, wenn die bestimmte Prozessorregister mit bestimmten Werten geladen werden. Dieser Weg kann nicht ausschließlich durch die Gastwerkzeuge sondern auch durch Schadprogramme genutzt werden. Kann ein Angreifer diesen Kommunikationskanal besetzen, hat er die Möglichkeit, Sicherheitslücken oder Designschwächen des Hypervisors auszunutzen, um die Kontrolle über den Hypervisor zu erhalten oder eigenen Code im Kontext des Hypervisors auszuführen. Hierüber kann der Angreifer andere virtuelle IT-Systeme unter seine Kontrolle bekommen. Da der Hypervisor alle Funktionen eines virtuellen IT-Systems über-

wacht und steuert, können über den Hypervisor Prozessorfunktionen oder Hauptspeicherinhalte des virtuellen IT-Systems direkt manipuliert werden, um Schadprogramme in das virtuelle IT-System einzubringen. Dies erfordert nicht notwendigerweise eine ausnutzbare Sicherheitslücke in dem über den Hypervisor angegriffenen virtuellen IT-System.

**Beispiel:**

Ein Rechenzentrumsdienstleister betreibt IT-Systeme für mehrere Kunden, die in einem Konkurrenzverhältnis zu einander stehen. Um die Kosten für den Systembetrieb für seine Kunden zu senken und weiterhin konkurrenzfähig zu sein, führt er eine Virtualisierungslösung in seinen Rechenzentrumsbetrieb ein. Er informiert seine Kunden darüber, dass ihre Systeme nun als virtuelle IT-Systeme betrieben werden. Da das Netz des Rechenzentrumsdienstleisters so aufgebaut ist, dass zwischen den IT-Systemen unterschiedlicher Kunden keine Kommunikationsbeziehungen über das Netz aufgebaut werden können, garantiert der Dienstleister weiterhin, dass die Vertraulichkeit der Daten der Kunden gewährleistet ist. Er überprüft dies durch regelmäßige Audits und räumt seinen Kunden ebenfalls Auditmöglichkeiten ein.

Ein Datenbankadministrator einer der Kunden hat die Möglichkeit, sich auf den IT-Systemen, die vom Rechenzentrumsdienstleister betrieben werden, interaktiv anzumelden. Er besitzt auf dem Datenbanksystem Administratorrechte. In der Hoffnung, Informationen über einen Mitbewerber seines Arbeitgebers zu gewinnen, startet er nun ein Schadprogramm, dass es ihm durch einen Fehler in der Grafikkartenemulation der Hypervisors ermöglicht, eigenen Code im Kontext des Hypervisors auszuführen. Dieser Code ermöglicht ihm die Überwachung aller Hypervisor-Funktionen. Dadurch kann er ein Datenbanksystem eines anderen Kunden des Rechenzentrumsdienstleisters als eines identifizieren, dass einem direkten Mitbewerber gehört. Über die Massenspeicherschnittstelle des Hypervisors gelingt es ihm, aus der Datenbank dieser virtuellen Maschine Daten auszulesen und Inhalte zu verändern. Hierdurch wird die Produktion des Konkurrenten empfindlich gestört und es entsteht dem Unternehmen des Administrators ein Wettbewerbsvorteil.

# G 5.151 DNS-Flooding - Denial-of-Service

Ein Denial-of-Service-Angriff (DoS-Angriff) hat das Ziel, legitime Benutzer von IT-Systemen an der Nutzung dieser Systeme zu hindern. Es werden dabei begrenzte Ressourcen wie CPU-Rechenzeit, Arbeitsspeicher, Plattenplatz, Netzbandbreite oder Ähnliches absichtlich überlastet.

Bei einem DoS-Angriff auf einen DNS-Server werden so viele Anfragen an diesen gesendet, dass die Netzverbindung zum DNS-Server bzw. der DNS-Server selbst überlastet wird. In der Regel werden die Anfragen über ein Bot-Netz versendet, um das notwendige Datenverkehrsaufkommen zu erreichen. Weil bei dieser Angriffsform ein DNS-Server regelrecht mit Anfragen "überflutet" wird, ist sie auch als "DNS-Flooding" bekannt. Ein auf diese Weise überlasteter DNS-Server kann keine legitimen Anfragen mehr beantworten. In der Regel werden alle für die Domain zuständigen DNS-Server attackiert, somit können Namen dieser Domain nicht mehr aufgelöst werden.

**Beispiel:**

- Zwei Firmen haben sehr ähnliche Produkte entwickelt und stehen daher in direktem Konkurrenzkampf. Der Vertrieb des Produktes erfolgt über den jeweils firmeneigenen Webshop. Eine Firma liegt, gemessen am stückmäßigen Umsatz, weiter abgeschlagen hinter der anderen Firma zurück. Um diesen Nachteil aufzuholen, beschließt die umsatzschwächere Firma, einen DoS-Angriff gegen die DNS-Server der Konkurrenten durchführen zu lassen. Dadurch kann der Domainname des Webshops der angegriffenen Firma nicht mehr aufgelöst werden. Interessierte Kunden werden bei einem Verbindungsversuch scheitern, da die DNS-Server aufgrund der Überlastung keine Anfragen mehr verarbeiten können. Der Geschäftsentgang und der Imageschaden stellen für das Opfer einen großen Schaden dar.

# G 5.152 DNS-Hijacking

DNS-Hijacking ist eine Angriffsmethode, die verwendet wird, um die Kommunikation zwischen Advertising DNS-Servern und Resolvern über das IT-System eines Angreifers zu leiten. Es handelt sich hierbei also um eine Man-in-the-Middle-Attacke. Die Kommunikation wird nicht direkt zwischen den beiden Kommunikationspartnern geführt, sondern über einen Dritten geleitet.

Der Angreifer hat die Möglichkeit die Kommunikation abzuhören und aufzuzeichnen. Die weitaus größere Gefahr besteht jedoch darin, dass ein erfolgreicher Angreifer jeglichen Verkehr der beiden Kommunikationspartner beliebig verändern kann. Ein Angreifer kann somit:

- Pakete verwerfen,
- Pakete modifizieren und weiterleiten oder,
- eigene Antwortpakete senden.

Wird nach einem erfolgreichen DNS-Hijacking Angriff vom Resolver eines Client-IT-Systems eine Anfrage an einen DNS-Server gesendet, unabhängig ob es sich dabei um einen Advertising oder einen Resolving DNS-Server handelt, kann der Angreifer beispielsweise die Zuordnung von Namen und IP-Adresse nach seinen Wünschen abändern.

DNS-Hijacking kann auch mit anderen Angriffen kombiniert werden, besonders Phishing bietet sich in diesem Fall an. Bei Phishing (abgeleitet aus "Passwort" und "Fishing") werden Benutzern Passwörter oder ähnliche Informationen entlockt (siehe beispielsweise auch G 5.42 *Social Engineering* und G 5.78 *DNS-Spoofing*), um diese Daten weiter zu verkaufen oder für den eigenen Vorteil zu benutzen.

**Beispiel:**

- Eine Firma betreibt einen Webshop und ein Kunde möchte dort einkaufen. Einem Angreifer gelingt es, sämtlichen DNS-Verkehr des Kunden und der Firma über ihn zu leiten. Der Kunde gibt in seinem Browser den Domainnamen des Webshops ein. Im Normalfall wird im Hintergrund der Name automatisch in die zugehörige IP-Adresse aufgelöst. Da nun aber der Angreifer zwischengeschaltet ist, verwirft er die DNS-Anfrage und sendet sein eigenes Antwortpaket. Dabei vertauscht er die Zuordnung von IP-Adresse und Namen so, dass der Kunde nicht auf den Webshop der Firma, sondern auf den Webshop des Angreifers gelangt. Der Webshop des Angreifers ist ein optischer Nachbau des Webshops der gewünschten Firma, somit fällt dem Kunden kein Unterschied auf. Er gibt seine Logindaten und nach dem Einkauf seine Kreditkartennummer ein, welche er somit dem Angreifer verraten hat. Als Folge kann der Angreifer die Daten benutzen, um Einkäufe auf Kosten des Kunden zu tätigen, oder die erhaltenen Daten weiterverkaufen.

# G 5.153 DNS-Amplification Angriff

Ein DNS-Amplification Angriff ist ein Denial-of-Service-Angriff (DoS-Angriff). Bei einem DoS-Angriff wird versucht, einen oder mehrere Dienste durch Überlastung in einen arbeitsunfähigen Zustand zu versetzen. Im Gegensatz zu DNS-Flooding (G 5.151 *DNS-Flooding - Denial-of-Service*) ist hier nicht der DNS-Server, an den die Anfragen gestellt werden, das Ziel, sondern der Empfänger der Antworten.

Es wird ausgenutzt, dass bestimmte Anfragen eine verhältnismäßig große Antwortdatenmenge erzeugen. Es ist dabei möglich, einen Verstärkungsfaktor von 50 und mehr zu erreichen. Das bedeutet, dass die Antwort, gemessen in Bytes, 50-mal größer ist als die Anfrage. Durch die Anzahl und Größe der Antworten wird die Netzbandbreite bzw. der Rechner selbst über die Leistungskapazität hinaus überlastet. Somit kann jede beliebige technische IT-Komponente das Angriffsziel sein.

**Beispiel:**

- Eine Firma (das Angriffsziel) betreibt ein zentrales Sicherheitsgateway. Dieses Sicherheitsgateway stellt den einzigen Verbindungspunkt zwischen internem Netz und dem Internet dar. Der Angreifer missbraucht nun die DNS-Server einiger Firmen, um einen DNS-Amplification Angriff gegen das Sicherheitsgateway des Angriffsziels durchzuführen. Dazu verwendet der Angreifer ein Bot-Netz, um kontinuierlich eine große Menge an Anfragen zu erzeugen. Zusätzlich verwendet er IP-Spoofing (G 5.48 *IP-Spoofing*) um die IP-Adresse des Sicherheitsgateways als Absenderadresse einzutragen, dadurch werden alle Antworten an dieses gesendet. Durch die große Menge an Daten wird das Sicherheitsgateway überlastet, somit ist die angegriffene Firma vom Internet abgeschnitten. Ein möglicher Nebeneffekt ist, dass die befragten DNS-Server überlastet werden.

# G 5.154 DNS Information Leakage

Die Hauptfunktionalität von DNS ist es, Namen und IP-Adressen aufzulösen. Um diese Anforderungen erfüllen zu können, wird unter anderem die Zuordnung von Namen und IP-Adressen sämtlicher Rechner und Netzkomponenten von DNS-Servern gespeichert. Ein Teil dieser Informationen muss veröffentlicht werden:

- DNS-Server
- Webserver
- Mailserver
- Fileserver
- VPN-Verbindungspunkte

Wären diese Domain-Informationen nicht öffentlich zugänglich, könnte keine Verbindung unter Verwendung von Domainnamen über das Internet zu diesen Servern aufgebaut werden. Domain-Informationen über interne Rechner und Netzkomponenten hingegen sind in der Regel nicht für die Öffentlichkeit bestimmt und sollten daher institutionsintern bleiben. Da Domain-Informationen meist etwas über die Funktion bzw. den Standort der betreffenden IT-Komponente aussagen, spricht man von DNS Information Leakage, wenn diese Informationen veröffentlicht werden.

Die Veröffentlichung selbst stellt für den Informationsverbund keinen direkten Schaden dar. Die gewonnenen Domain-Informationen können jedoch zur Vorbereitung eines Angriffs auf den Informationsverbund genutzt werden. Ein Angreifer kann sich einen Überblick über das Netz, die sicherheitsrelevanten Komponenten und die lohnenden Ziele verschaffen. Je mehr Informationen ein Angreifer über das Angriffsziel sammeln kann, desto höher ist die Wahrscheinlichkeit, dass er eine Schwachstelle findet.

Es gibt mehrere Ansätze für Information Leakage:

- Ist die Sichtbarkeit der Domain-Informationen nicht eingeschränkt, können sämtliche Domain-Informationen legitim abgefragt werden.
- Werden Zonentransfers (G 3.104 *Fehlerhafte Konfiguration eines DNS-Servers* ) uneingeschränkt zugelassen, können die gesamten Domain-Informationen mithilfe einer einzigen Abfrage abgefragt werden.

# G 5.155 Ausnutzen dynamischer DNS-Updates

Dynamische Updates werden dazu verwendet, um automatisiert Daten des Domain-Namensraums zu modifizieren, hinzuzufügen oder zu löschen. Vor allem im Zusammenhang mit DHCP spielen dynamische Updates eine wichtige Rolle. Wird vom DHCP-Server eine IP-Adresse an einen Host vergeben, müssen diese Informationen auch in den Domain-Namensraum eingepflegt werden. Dies geschieht in der Regel über dynamische Updates.

Es besteht jedoch die Gefahr des Missbrauchs von dynamischen Updates. Domain-Informationen werden automatisiert geändert, die Sicherheit beruht somit auf der Vertrauenswürdigkeit jener Rechner die dynamische Updates vornehmen dürfen und auf den Regeln, die definieren was modifiziert werden darf. Werden dynamische Updates von jeglicher Quelle akzeptiert, kann jeder Host Domain-Informationen nach seinem Willen ändern. Ein Angreifer kann somit sämtliche Dienste, die DNS benötigen, manipulieren. Des Weiteren ist eine Kombination mit Angriffen wie Phishing, Infizierung mit Schadsoftware, etc. sehr wahrscheinlich.

**Beispiel:**

- Ein Angreifer hat erfahren, dass die DNS-Server einer Firma durch einen Konfigurationsfehler bedingungslos dynamische Updates akzeptieren. Der Angreifer nutzt dies aus und manipuliert die Domain-Informationen so, dass sämtlicher E-Mail-Verkehr der Firma über seinen Mailserver geleitet wird. Der Angreifer erhält somit geschäftswichtige Informationen, die er an die Konkurrenten der angegriffenen Firma verkauft. Des Weiteren manipuliert er die Domain-Informationen so, dass jegliche Verbindung zum Intranet- und Webserver der Firma auf den Webserver des Angreifers umgeleitet wird. Dort wird versucht die Rechner mit Malware zu infizieren und ins Bot-Netz des Angreifers zu integrieren. Danach erfolgt eine Weiterleitung an den ursprünglich gewünschten Intranet- bzw. Webserver, um unentdeckt zu bleiben. Somit wurden nicht nur firmeninterne, sondern auch Rechner, die von außerhalb auf den Webserver zugreifen wollen, kompromittiert.

# G 5.156 Bot-Netze

Bei einem Bot handelt es sich um ein Programm, das von einem Angreifer auf dem Rechner eines Anwenders ohne dessen Wissen installiert wird, z. B. über entsprechende Schadsoftware, und das aus der Ferne Anweisungen des Angreifers ausführen kann. Werden viele Bots zusammengeschlossen, entsteht ein Bot-Netz.

Bot-Netze werden für viele illegale Aktivitäten eingesetzt. Der massenhafte Versand von Spam-Mails oder E-Mails mit bösartigen Anhängen und Links (z. B. für Phishing) aber auch die Aufzeichnung von Tastaturanschlägen (Keylogging) und damit einhergehend die Entwendung bzw. der Diebstahl persönlicher Informationen wie (Passwörter, PIN, etc.) oder vertraulicher Geschäftsinformationen (Wirtschaftsspionage) sind Einsatzgebiete von Bot-Netzen. Darüber hinaus können mit Bots infizierte Rechner missbraucht werden, um dort illegale Software abzulegen oder diese sogar über die infizierten Rechner anzubieten, z. B. per File-Sharing. Eine besonders für Netze und Dienste sehr ernst zu nehmende Angriffsform sind so genannte DDoS-Angriffe (DDoS, Distributed Denial of Service). DDoS-Angriffe werden aus politischen, ideologischen, vorwiegend aber aus finanziellen Gründen heraus unternommen.

Vereinfacht dargestellt ist der typische Aufbau eines Bot-Netzes wie folgt:

- Der Bot-Master (auch Bot Herder) entwickelt einen Bot-Client. Über das Internet infiziert er unter Ausnutzung einer bestehenden Sicherheitslücke den PC eines Endanwenders.
- Der Bot-Client verbindet sich zum Command and Control Server (C&C Server).
- Der Bot-Master aktualisiert den Bot-Client mit neuen Angriffen und Instruktionen.
- Der Bot scannt einen zufälligen IP-Adressbereich nach Schwachstellen und infiziert andere Rechner.
- Infizierte Computer verbinden sich ihrerseits zum Command and Control Server und nehmen Befehle entgegen.

**Infektions- und Ausbreitungs-Mechanismus**

In der Vergangenheit erfolgte die Infektion eines PCs mit Bots meist unter Ausnutzung bekannter Sicherheitslücken in Systemdiensten und Applikationen. So enthielten die Würmer *SDBot* und *Agobot* Scanroutinen, um Sicherheitslücken in ungeschützten Systemen aufzuspüren. *SDBot* verbreitet sich unter anderem unter Ausnutzung der folgenden Sicherheitslücken: NetBIOS (Port 139), NTPass (Port 445), DCOM (Ports 135 und 1025) und WebDav (Port 80). Agobot verfügt über ein Exploit-Framework zur Ausnutzung von Schwachstellen entfernter Dienste (z. B. Ports 135 und 445). Darüber hinaus sucht *Agobot* nach Hintertüren, die von anderen Schadprogrammen hinterlassen wurden, z. B. von *Bagle* auf Port 2745.

Eine aus Sicht der Angreifer weitere effektive Infektionsmethode ist der Einsatz von Social Engineering, um Benutzer zu einer spontanen unbedachten Handlung, wie Klicken auf manipulierte Links in E-Mails bzw. Instant Messaging-Nachrichten oder die Ausführung von E-Mail-Anhängen, zu verleiten. Viele Schädlinge werden auch über File-Sharing (Peer-to-Peer-Netze) verteilt. In jüngster Zeit ist zunehmend auch zu beobachten, dass legitime und stark frequentierte Webseiten manipuliert und als Verteilungspunkt für Schadprogramme missbraucht werden, indem Skriptcode in die Webseite eingefügt wird, um Schadprogramme auf dem Rechner der Benutzer automatisch zu installieren (Drive-by-Download oder Drive-by-Infection).

Ein weiterer wichtiger Aspekt bei der Betrachtung von Bot-Netzen ist ihre Kommunikations- und Steuerungsstruktur. In den meisten Fällen erfolgt die Steuerung über einen oder mehrere Command and Control Server. Zentral gesteuerte Bot-Netze lassen sich einfach entwickeln und administrieren. Allerdings führt eine Sperrung der wenigen Command and Control Server dazu, dass das Bot-Netz nicht mehr genutzt werden kann. Zum Schutz der Bot-Netze vor Entdeckung und Deaktivierung werden daher zunehmend andere Kommunikationsmodelle wie z. B. Peer-to-Peer-Protokolle (wegen ihrer dezentralen Architektur) und HTTP sowie Verschleierungstechniken wie Kompression, Verschlüsselung und Fast-Fluxing, eingesetzt.

**Beispiele:**

- Das Bot-Netz *Zeus* bestand aus mehr als 100.000 gekaperten Rechnern, vornehmlich in Spanien und Polen, und wurde mit Hilfe des kostengünstigen Bot-Netz-Toolkits Zeus zusammengestellt. Das Bot-Netz *Zeus* sammelte vor allem Finanzdaten, wie Konten- oder Kreditkartendaten, und andere vertrauliche Informationen. Es wurde zentral von einem Server kontrolliert. Von diesem Server ging im April 2009 dann ein "Kill Operating System"-Befehl aus, der dafür sorgte, dass bei allen an das Bot-Netz angeschlossenen Rechnern wichtige Einträge in der Registrierungsdatei von Windows gelöscht und der virtuelle Speicher von Windows mit Nullen überschrieben wurde. Das Betriebssystem konnte in der Folge nicht mehr gestartet werden, so dass die Rechner vollständig neu installiert werden mussten.
- *Torpig* ist ein Trojanisches Pferd, das Windows-Betriebssysteme befällt und die entsprechenden Rechner zu einem Bot-Netz zusammenschließt. Im Jahr 2006 wurde *Torpig* als ausführbare Datei via E-Mail versendet, inzwischen wird es auch als Skriptcode auf Webseiten verteilt. Die einzelnen befallenen Rechner generierten aus Zufallselementen und Suchergebnissen von Twitter-Beiträgen eigene Domainnamen, von denen sie dann Schadcode und Updates nachluden. Die Aufgabe des Bot-Netzes war es, Daten für Bankkonten, Kreditkartendaten und FTPAccounts auszuspionieren. Die gesammelten Informationen wurden an einen zentralen Server übermittelt.
  Wissenschaftlern gelang es Anfang 2009, den Datenverkehr des Bot-Netzes für rund 10 Tage mitzuschneiden und zu untersuchen. So soll *Torpig* die Daten von mehr als 300.000 verschiedenen Konten, darunter Bankkontodaten und Kreditkartendaten der unterschiedlichsten Kreditinstitute, ausgespäht haben.

# G 5.157 Phishing und Pharming

**Phishing**

Phishing ist ein Kunstwort aus "Passwort" und "Fishing" und bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden. Hierzu werden häufig Methoden des Social Engineering, teilweise in Verbindung mit Identitätsdiebstahl, verwendet. Beispielsweise können die Angreifer geschickt formulierte E-Mails an die Benutzer senden.

Wenn das Opfer meint, den Absender zu kennen und diesen als vertrauenswürdig einstuft, wird es meist auch die E-Mail als vertrauenswürdig einstufen und darin beschriebene Schritte durchführen, z. B. einen beigefügten Link oder Anhang öffnen.

Andere Formen des Phishing verwenden spezialisierte Schadprogramme, die direkt an die Benutzer gesendet werden oder über Umwege auf den Computern der Opfer platziert werden.

**Beispiel:**

- Viele Online-Banking-Benutzer erhielten E-Mails, die scheinbar von der Service-Abteilung ihrer Bank kamen. Darin wurden sie informiert, dass sie sich aufgrund von Service-Änderungen auf der angegebenen Webseite mit ihrem Standard-Banking-Passwort anmelden und die neuen Dienstleistungen mit einer TAN freischalten sollten. Die Webseite sah zwar authentisch aus, hatte aber mit der genannten Bank nichts zu tun, sondern war von Angreifern präpariert und ins Internet gestellt worden. Der Zweck der Webseite war ausschließlich, Zugangsdaten zu fremden Konten für die Angreifer zu sammeln.
  Ähnliche Angriffe gab es auch auf Nutzer beliebter E-Commerce- und Auktionswebseiten.

**Pharming**

Beim Pharming werden Manipulationen an der Namensauflösung von Internet-Domainnamen vorgenommen, um Client-Zugriffe auf gefälschte Server umzuleiten. Ein Angreifer kann damit beispielsweise erreichen, dass im Browser des Opfers eine gefälschte Webseite statt der eigentlich gewünschten Seite angezeigt wird. Pharming hat sich aus Phishing weiterentwickelt. Der Begriff "Pharming" leitet sich aus "Phishing" und "Farming" ab.

Auf technischer Ebene gibt es mehrere Möglichkeiten, wie der Angreifer die Manipulation der Namensauflösung erreichen kann, zum Beispiel:

- Angreifer können DNS-Informationen auf DNS-Servern verfälschen, indem sie Schwachstellen oder Fehlkonfigurationen ausnutzen.
- Angreifer können falsche DNS-Informationen in DNS-Zwischenspeicher einfügen (DNS Cache Poisoning).
- Mit Hilfe von Schadprogrammen kann die "hosts"-Datei auf dem Client modifiziert werden.
- Es können unerlaubt Konfigurationsänderungen an Routern vorgenommen werden, beispielsweise wenn die Geräte schwache Passwörter aufweisen.

Durch Pharming könnte ein Angreifer dem Rechnernamen eines Internet-Banking-Servers die IP-Adresse eines falschen Servers zuordnen und dadurch die Benutzeranfragen umleiten. Häufig sind bei solchen Angriffen die Webseiten

auf dem falschen Server optisch nicht von den Original-Webseiten zu unterscheiden, so dass der Benutzer keinen Verdacht schöpft.

# G 5.158 Missbrauch sozialer Netzwerke

Soziale Netzwerke sind als Plattformen sehr erfolgreich und gewinnen immer mehr Mitglieder. Allerdings gibt es hier neben diversen Vorteilen auch Sicherheitsrisiken, die Benutzer nicht aus den Augen verlieren sollten:

- Die in sozialen Netzwerken oder virtuellen Welten von einem Benutzer verwendete Identität (z. B. Benutzerbeschreibung oder Avatar) steht meistens in einem engen Zusammenhang mit dessen realer Identität. Eine virtuelle Identität kann unter Umständen durch andere missbraucht werden, beispielsweise indem in dieser Rolle sozusagen unter falscher Flagge Aktionen durchgeführt werden, ohne dass der Inhaber dies weiß.
- Benutzer sozialer Netzwerke geben eine Vielzahl von Informationen über sich bekannt, um in diesen Netzwerken wahrgenommen zu werden und mitwirken zu können. Je nach Intention des sozialen Netzwerks können dies Name und Foto des Benutzers, eine oder mehrere E-Mail-Adressen, Wohnort, Arbeitgeber, persönliche und berufliche Hintergründe sein. Diese Informationen sind für große Benutzergruppen zugänglich und der Benutzer hat keinen Einfluss mehr über deren Verbreitung.
- Informationen über Benutzer können als Grundlage für Social Engineering Angriffe benutzt werden. Ziel solcher Angreifer ist es, möglichst viele Hintergrundinformationen zu erlangen, um sich das Vertrauen des Opfers zu erschleichen und es zu weiteren Handlungen zu überreden, beispielsweise bestimmte Dateien zu öffnen.
- Vertrauliche Informationen könnten offengelegt werden, beispielsweise weil die Grundidee eines "sozialen Netzwerkes" enge Beziehungen und ein Vertrauensverhältnis zwischen den Teilnehmern widerspiegelt, das nicht immer gegeben ist.
- Die über soziale Netzwerke zugänglichen Daten können zum geschickten Passwortraten benutzt werden. Typischerweise werden bereits bei der Anmeldung an solche Dienste Daten wie Geburtstag, Geburtsort, frühere Schulen, Universitäten und andere Wirkungsstätten angegeben, um interessante Kontakte herstellen zu können. Bei vielen Internet-Anbietern und Anwendungen ist es aber mittlerweile üblich, bei der Vergabe von Passwörtern auch direkt persönliche Informationen zu erfassen, die abgefragt werden, wenn jemand sein Passwort vergessen hat. So reicht es beim Telefon-Banking zur Authentisierung häufig aus, das korrekte Geburtsdatum zu kennen, welches über soziale Netzwerke einfach erfahren werden kann.

**Beispiel**

"Böser Zwilling": Ein soziales Netzwerk wurde von einem Daten-Phisher genutzt, in dem er ein gefälschtes Profil eines Prominenten erstellte. Aufgrund des öffentlich verfügbaren Bildmaterials und der raschen Erstellung einer authentisch wirkenden Webseite war es Besuchern des Online-Profils nicht ohne weiteres möglich, die Identität als Fälschung zu erkennen. Der Angreifer platzierte auf der Profilseite einen Link zu einem angeblichen Video. Tatsächlich führte dieser Link zu einer gefälschten Anmelde-Seite auf einem externen Webserver. Die ausgespähten Anmelde-Daten der Opfer legte der Angreifer in einer sogenannten Dropzone ab.
Das Ausspähen von Zugangsdaten eines sozialen Netzwerkes bedeutet für die Opfer in der Regel keinen unmittelbaren finanziellen Verlust. Geraten die Anmelde-Daten in die falschen Hände, kann jedoch ein Imageverlust die Folge eines durch die Phisher manipulierten Online-Profils sein. Der Angreifer hat im vorliegenden Fall keine Schwachstelle in der Webanwendung ausgenutzt. Diese Form der Phishing-Variante ist auf jeder Online-Plattform möglich, die keine Verifikation der Benutzeridentitäten vornimmt. Größeren Schaden

als Profil-Manipulationen kann jedoch der Versand von Nachrichten innerhalb der Online-Plattform verursachen, in denen auf mit Schadsoftware präparierte Webseiten verlinkt wird. Aufgrund der Vertrauensbasis zwischen den Nutzern dürfte die Erfolgsquote für den Angreifer hoch ausfallen. Analog zu Phishing E-Mails gilt für soziale Netzwerke, zugesandten Links mit gesundem Misstrauen zu begegnen.

# G 5.159 Erstellung von Bewegungsprofilen unter Bluetooth

Wenn bei Geräten die Bluetooth-Schnittstelle eingeschaltet ist, ist es möglich, die Position dieser Geräte zu orten. Hierzu sind in der Regel mehrere Bluetooth-Empfänger erforderlich, deren Empfang idealerweise durch zusätzliche Antennen oder Verstärker verbessert wurden. In Laborumgebungen sind bereits Reichweiten von bis zu 2 Kilometern erreicht worden, in denen Bluetooth-Geräte noch geortet werden konnten. Je nach Art der Ausstattung der Angreifer spielt es darüber hinaus keine Rolle, ob das Bluetooth-Gerät als sichtbar oder unsichtbar konfiguriert wurde.

Hierüber ist es prinzipiell auch möglich, ein Bewegungsprofil einer Person zu erstellen, wenn die Positionen des Bluetooth-Gerätes längere Zeit aufgezeichnet werden, da die Bluetooth-Geräte-ID stets einem Gerät und somit meist auch einer Person zugeordnet werden kann.

# G 5.160 Missbrauch der Bluetooth-Profile

Bluetooth stellt einzelne Profile zur Verfügung, über die standardisiert Daten ausgetauscht, Nachrichten übertragen oder Konfigurationen vorgenommen werden können. Diese Profile können unter Umständen ausgenutzt werden, um auf Bluetooth-Endgeräte zuzugreifen und diese zu manipulieren oder abzuhören bzw. Daten zu entwenden. Einige Gefährdungen, die auf einen Missbrauch dieser Profile zurückzuführen sind, sind im Folgenden beispielhaft beschrieben.

Damit auf ein anderes Bluetooth-Endgerät zugegriffen werden kann, ist normalerweise ein Pairing zwischen den Endgeräten notwendig. Teil des Pairings ist stets auch eine Authentisierung. Allerdings sieht es die Bluetooth-Spezifikation vor, dass bereits vor dem Pairing ohne eine entsprechende Authentisierung ein Zugriff auf das Service Discovery Protocol (SDP) möglich ist. Mit diesem Protokoll tauschen die Bluetooth-Endgeräte die jeweils verfügbaren Profile aus. In der Vergangenheit wurden Bluetooth-Implementierungen bekannt, bei denen Profile vorgesehen waren, die nicht über das SDP angezeigt wurden. Die Hersteller hatten offensichtlich eine Art Hintertür geöffnet. Auf Basis dieser Schwachstelle ließen sich unter anderem einzelne Profile ausnutzen, so dass ohne ein vorheriges Pairing, also ohne Authentisierung, Daten zwischen Bluetooth-Endgeräten ausgetauscht werden konnten.

- Ein Angreifer konnte beispielsweise das OBEX Push Profile nutzen, das für den einfachen Datenaustausch vorgesehen ist, um Kalendereinträge oder Telefonbücher auszulesen. Unterstützt das Endgerät auch einen OBEX-basierenden FTP-Server, so erhält der Angreifer gleichzeitig auch schreibenden Zugriff auf das Endgerät.
- Durch die fehlende Authentisierung kann auch das HID Profil ausgenutzt werden, das für die Eingabe von Eingabegeräten, sprich Maus oder Tastaturen, gedacht ist. Wird auch hier auf die Authentisierung verzichtet und existiert bereits ein erfolgreiches Pairing, beispielsweise zwischen einer Tastatur und einem Rechner, dann kann mit diesen Informationen ein weiteres Eingabegerät simuliert werden und beispielsweise über eine Keylogger-Software Tastatureingaben mitgeschnitten werden.

Problematischer ist der Missbrauch des SIM Access Profils. Mit diesem Profil besteht die Möglichkeit, direkt über Bluetooth auf die SIM-Karten von Mobiltelefonen zuzugreifen. Dieses Profil wird typischerweise bei einem eingebauten Autotelefon angewendet, das mittels Bluetooth auf ein anderes Telefon zugreifen möchte. Durch diesen direkten Zugriff auf die SIM-Karte könnten Manipulationen an der Mobilfunkverbindung vorgenommen werden, ohne dass der Nutzer das mitbekommt. So kann über das SIM Access Profil beispielsweise das SIM Application Toolkit, das in vielen SIM-Karten implementiert ist, dazu verwendet werden, um den für die Verschlüsselung der Mobilfunkverbindung verwendeten Sitzungsschlüssel per SMS zu versenden. Mit diesem Sitzungsschlüssel kann eine aufgezeichnete Kommunikation über die Funkschnittstelle eines Mobiltelefons entschlüsselt und somit ausgespäht werden. Somit entstehen durch die Kombination der beiden Techniken Bluetooth und Mobilfunk Angriffsszenarien, die mit jeder Technik für sich genommen nicht möglich wären.

# G 5.161 Gefälschte Antworten auf XDMCP-Broadcasts bei Terminalservern

Das häufig unter Unix-Systemen anzutreffende X-Window-System ist eine Applikation, um Fenster auf den Bildschirm ausgeben und um Tastatur- und Bildschirmeingaben einlesen zu können. Erst in Verbindung mit einer graphischen Benutzeroberfläche, wie KDE oder Gnome, können Benutzer intuitiv Unix-Systeme ohne eine Befehlseingabe über die Kommandozeile bedienen.

Das X-Window System besteht aus einem X-Server und einem X-Client. Der X-Server empfängt Signale von den Eingabegeräten, wie Maus und Tastatur und gibt Informationen an die Ausgabegeräte, wie Bildschirme, aus. Der X-Client ist die eigentliche Applikation, das die Ein- und Ausgaben des X-Servers verarbeitet und an die jeweiligen Anwendungen weitergibt. Der X-Client kommuniziert mit dem X-Server, verarbeitet die Signale und führt so die Befehle aus. Der X-Client und der X-Server können sich auf einem IT-System befinden, beide Komponenten können aber auch über eine Netzverbindung miteinander kommunizieren. Hierfür wird der X-Server auf den Arbeitsplatz-PCs, an die Ein- und Ausgabegeräte angeschlossen sind, und der X-Client auf einem zentralen Terminalserver installiert. Ein IT-System, auf dem ausschließlich ein X-Server, aber keine X-Client oder weitere Applikationen installiert sind, wird als X-Terminal bezeichnet.

### X Display Manager

Damit sich die Benutzer authentisieren, kann ein X Display Manager (XDM) verwendet werden, der wie der X-Client auf dem Terminalserver installiert ist. Der XDM beinhaltet einen graphischen Anmeldebildschirm, über dem in der Regel der Benutzernamens und das Passwort eingegeben werden kann. Um sich gegenüber dem X-Client authentisieren zu können, baut das X-Terminal eine Datenverbindung über das Netz zum XDM auf.

### X Display Manager Control Protocol (XDMCP)

Die X-Terminals und die XDM kommunizieren in der Regel über XDMCP (*X Display Manager Control Protocol*). Für den Verbindungsaufbau müssen die X-Terminals wissen, unter welchem Hostnamen oder IP-Adresse die XDMs zu erreichen sind. Hierfür können folgende Modi verwendet werden:

- Direct
  Im Modus *Direct* wird dem X-Terminal der Hostname oder die IP-Adresse des XDM in dessen Konfiguration vorgegeben. Nach dem Startvorgang des Terminals oder der Terminalemulation verbindet sich der Client mit dem XDM und stellt ein Anmeldefenster dar.
- Indirect
  Bei Verwendung des Modus *Indirect* erfolgt ebenfalls eine Verbindung zu einem dedizierten Host. Dieser stellt im ersten Schritt eine Liste möglicher XDM bereit, die nachfolgend durch den Anwender über ein Menü des sogenannten *Chooser* ausgewählt werden können.
- Broadcast
  Wird durch das Terminal eine Rundruf Meldung (*Broadcast*) an das Netz ausgesendet, signalisieren entsprechend konfigurierte XDM ihre Bereitschaft. Infolge dessen verbinden sich Terminals mit dem ersten antwortenden Host oder bieten dem Anwender die Wahl des Servers über den *Chooser*.

Durch den Modus "Broadcast" können sich die Benutzer auf verschiedene XDM anmelden, ohne dass sie auf den X-Terminals eingetragen werden müssen. Kommen neue XDM hinzu oder werden vorhandene entfernt, müssen die X-Terminals im Gegensatz zum Modus "Direct" nicht umkonfiguriert werden. Sollen mehrere *Chooser* eingesetzt werden oder ändert sich die IP-Adresse des XDM des *Choosers*, muss beim Modus "Broadcast" die Konfiguration des X-Terminals ebenfalls nicht geändert werden.

Wird "Broadcast" verwendet, könnte ein Angreifer einen eigenen XDM installieren, der die Anfragen der X-Terminals beantwortet. Gibt der Benutzer sein Benutzernamen und sein Passwort im Anmeldebildschirm des XDM ein, kann der Angreifer auf diese Weise die Login-Informationen erlangen und für spätere Angriffe nutzen.

Je nach Kenntnisstand des Angreifers kann er dem Benutzer eine Umgebung auf einem Terminalserver, der wie der XDM unter der Kontrolle des Angreifers steht, zu Verfügung stellen. Bemerkt der Benutzer nicht, dass er den Terminalserver des Angreifers nutzt und innerhalb seiner Sitzung auf Programme, Ressourcen und Backends zugreift, können unter Umständen weitere vertrauliche Informationen ausgespäht werden.

# G 5.162 Umleiten von X-Window-Sitzungen

Durch die Trennung des X-Server vom X-Client beim X-Window System können diese Komponenten auf verschiedenen IT-Systemen betrieben werden. So können Applikationen und grafische Benutzeroberflächen auf unterschiedlichen IT-Systemen ausgeführt und angezeigt werden. Die Terminalserver, auf denen die Applikationen ausgeführt werden, sind hierbei durch eine Datenverbindung mit dem X-Terminal, auf dem die Ein- und Ausgabegeräte angeschlossen sind, verbunden. Die Bildschirminhalte werden im Terminalserver generiert, aber die Ausgabe wird auf das X-Terminal umgeleitet.

In der Regel können nicht nur die Ein- und Ausgaben, einzelne Instanzen der Applikationen oder Benutzeroberflächen vom Terminalserver auf das X-Terminal umgeleitet werden, sondern mehrere Instanzen. Der Benutzer kann beispielsweise mehrere verschiedene grafische Benutzeroberflächen gleichzeitig auf einem Terminalserver öffnen, zwischen denen er wechseln kann.

Aber nicht nur verschiedene Instanzen auf einem Terminalserver können an einem X-Terminal umgeleitet werden, sondern auch eine Instanz auf dem Terminalserver kann auf verschiedene X-Terminals umgeleitet werden. Gelingt es einem Angreifer, dass die Bildschirmausgabe nicht nur auf dem X-Terminal des Benutzers, sondern auch auf seinem umgeleitet wird, kann er die Ein- und Ausgabe des Benutzers abfangen und mitlesen.

Zusätzlich kann er die grafische Benutzeroberfläche oder die Anwendungen eines vom Angreifer kontrollierten Terminalservers auf das X-Terminal des Anwenders umleiten. Gelingt es dem Angreifer, die Arbeitsumgebung zu fälschen und bemerkt dies der Anwender nicht, übergibt er eventuell sensible Informationen dem Angreifer. Ein Beispiel hierfür ist die Eingabe eines Passwortes, das auf dem Bildschirm nicht angezeigt wird, aber dennoch vom Angreifer mitgelesen werden kann.

Kombinationen der oben genannten Angriffe sind ebenfalls möglich.

**Beispiel:**

Bestandteil vieler Systeme, auf denen X-Window installiert wird, ist "xnest". Diese Applikation erlaubt es, innerhalb einer Terminalsitzung eine oder mehrere weitere Sitzungen zu starten und in beliebiger Größe auf dem Bildschirm anzuzeigen. Siekann zum Testen von neuer Konfiguration oder für die Fernwartung genutzt werden.

Einem Angreifer gelingt es nun, diese Software auf dem Client des Anwenders zu starten, z. B. weil der Benutzer sich nicht bei Verlassen seines Arbeitsplatzes abgemeldet hat oder aufgrund einer Schwachstelle in der Implementierung des X-Server-Dienstes. Innerhalb von xnest, das mit voller Bildschirmauflösung gestartet wird, startet der Eindringling den üblichen Anmeldedialog des Terminals, leitet jedoch dessen Ausgabe über das Netz an einen zweiten Rechner und kommt so in den Besitz der Authentisierungsinformationen des Benutzers.

# G 5.163 Angriffe auf Exchange-Systeme

Die in den Datenbanken eines Microsoft-Exchange-Servers gespeicherten Informationen können auch für den mobilen Zugriff aus dem Internet bereitgestellt werden. Die lokalen Postfachspeicher eines Exchange-Servers befinden sich üblicherweise im internen LAN des Betreibers und müssen durch angemessene Sicherheitsmaßnahmen geschützt werden, so dass ein Angreifer nicht unerlaubt auf den Microsoft-Exchange-Server selbst zugreifen kann und auch nicht in der Lage ist, in das interne Netz einzudringen.

Nachfolgend sind einige Problemfelder und potentielle Sicherheitslücken aufgeführt, die insbesondere beim öffentlichen Zugriff auf ein Microsoft-Exchange-System aus dem Internet beachtet werden müssen:

- Über das Kommunikations-Protokoll Remote Procedure Call (RPC) von Microsoft Exchange sind viele Schwachstellen bekannt. Auch bei bereits optimierter Konfiguration muss mit einem Restrisiko gerechnet werden.
- Ein Microsoft-Exchange-System ist sehr komplex. Ein Verbund aus Exchange-Servern und Outlook-Clients erhöht die Komplexität weiter. Durch die Komplexität (auch der sicherheitsrelevanten Einstellungen) kann es zu Fehlkonfigurationen und somit auch zu Sicherheitslücken kommen.
- Durch den großen Funktionsumfang eines Microsoft-Exchange-Systems und die mögliche Einbindung in entsprechende Hintergrundsysteme, wie beispielsweise Unified-Messaging-, Content-Management- und Enterprise-Ressource-Planning-Systeme können sich Sicherheitslücken unter Umständen von einem Server auf die Hintergrundsysteme auswirken. Dabei genügt es in der Regel, eine einzelne Schwachstelle in einem einzelnen Funktionspaket auszunutzen.
  Beispiele:
- Bei Outlook-Web-Access kann ein Angreifer über das Netz einen Denial-of-Service-Angriff durchführen, indem eine manipulierte URL an den Server gesendet wird, wodurch die betroffenen Komponenten mit einem Speicherüberlauf abstürzen.
- Durch ein manipuliertes Kommando unter SMTP könnte ein Angreifer einen Exchange-Server zum Absturz bringen. Der Exchange-Server wird durch ein manipuliertes Kommando unter SMTP zum Absturz gebracht oder ein Angreifer kann zusätzlich beliebigen Code ausführen.

# G 5.164 Missbrauch von Programmierschnittstellen unter Outlook

Viele Softwarehersteller sehen aus Gründen der Interoperabilität in ihren Tools und Anwendungen Programmierschnittstellen vor, z. B. als Application Programming Interface (API). Diese erlauben es, bestimmte Funktionen auch aus anderen Programmen heraus zu nutzen oder den Funktionsumfang der Anwendung zu erweitern. Neben dem positiven Nutzen der Programmierschnittstellen können diese auch dazu verwendet werden, Schadsoftware zu entwickeln und deren Schadwirkung über APIs auszulösen.

Für Microsoft Outlook werden Programmierschnittstellen angeboten, mit denen Benutzer eigene Anwendungen oder Funktionserweiterungen (Makros) schreiben können, die über den Client Nachrichten, Termine, und Aufgaben verschicken und empfangen können. Dadurch kann Microsoft Outlook zur Verbreitung von Schadsoftware missbraucht werden.

**Beispiel:**

- Ein Innentäter mit Programmiererfahrung erstellt ein Tool, das regelmäßig die freigegebenen Verzeichnisse des Firmennetzes mit bestimmten Suchmustern wie beispielsweise "Patentanmeldung" durchläuft und gefundene Dateien automatisch über Microsoft Outlook an einen Mitbewerber verschickt.
- Durch ein bösartiges Makro werden E-Mails unbemerkt aus dem Posteingang eines Benutzers gelöscht. Der Benutzer kann auf eine Anfrage nicht zeitnah reagieren, worüber sich Kunden beschweren.

# G 5.165 Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services

Wenn ein Benutzer eine Webanwendung bedient oder wenn ein Programm auf einen Web-Service zugreift, werden Daten übertragen und üblicherweise sowohl client- als auch serverseitig gespeichert (zum Beispiel in Protokolldateien, Browser- und Proxy-Cache). Wenn diese Daten bei der Übertragung und Speicherung nicht angemessen geschützt sind, können sie unbefugt durch Dritte eingesehen oder manipuliert werden.

Aufgrund der unterschiedlichen Übertragungswege und Speicherorte der Daten ergeben sich besondere Gefährdungen, die anhand nachfolgender Beispiele erläutert werden:

- Zugangs- und Formulardaten, die ein Benutzer im Web-Browser eingibt, werden im Browser-Cache zwischengespeichert. Kann ein Angreifer auf den Rechner zugreifen, dann kann er den Browser-Cache und somit die schützenswerten Daten auslesen, da der Browser-Cache üblicherweise nicht gesondert geschützt ist (zum Beispiel durch Verschlüsselung).
- Werden GET-Parameter in der URL übertragen, können diese auf dem Weg von der Webanwendung zum Client von den dazwischenliegenden IT-Systemen (zum Beispiel Proxy-Server) in deren Protokolldateien gespeichert werden. Proxy-Server protokollieren üblicherweise die aufrufende URL inklusive übertragener GET-Parameter. Personen mit Zugriff auf die Protokolle können daher die Daten in den GET-Parametern lesen. Werden von der Webanwendung schützenswerte Daten in GET-Parametern übermittelt, kann demzufolge der Schutz der Daten nicht gewährleistet werden. Darüber hinaus können vertrauliche Daten in GET-Parametern beim Versenden eines Links oder durch Einsicht der Browser-Historie offengelegt werden.
- Müssen Sitzungsdaten einer Webanwendung auf dem Client hinterlegt werden, geschieht dies häufig über eine Speicherung in Cookies. Hierbei kann es sich um schützenswerte Daten wie die Session-ID handeln. Erlangt ein Angreifer Zugriff auf den Client (zum Beispiel durch das clientseitige Ausführen von Schadcode), so ist es möglich, den Inhalt von Cookies unbefugt auszulesen oder zu verwenden und unbemerkt an den Angreifer zu versenden (siehe auch G 5.170 *Cross-Site Scripting (XSS)*).
- Wird die Verbindung zwischen dem Web-Service-Client und dem Web-Service nicht ausreichend durch Verschlüsselung oder elektronische Signaturen abgesichert, besteht die Möglichkeit, dass Angreifer vertrauliche Daten während der Übertragung einsehen oder manipulieren können.

# G 5.166 Missbrauch einer Webanwendung durch automatisierte Nutzung

Bei der automatisierten Bedienung von Webanwendungen werden Funktionen der Anwendung computergesteuert genutzt, z. B. durch Skripte, die Eingaben durch Tastatur und Maus emulieren. Dadurch können Vorgänge in kurzer Zeit durchgeführt werden und Angreifer können somit auf Wiederholung basierende Angriffe gegen die Webanwendung effizient durchführen. Mithilfe eines wiederholt durchgeführten Login-Prozesses können z. B. gültige Kombinationen aus Benutzernamen und Passwort systematisch ermittelt (Brute-Force) oder Listen mit gültigen Benutzernamen erzeugt werden (Enumeration).

Darüber hinaus kann das wiederholte Aufrufen von ressourcenintensiven Funktionen (z. B. komplexe Datenbankabfragen) für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden. Während Denial-of-Service-Angriffe auf Netzwerkebene häufig viele Verbindungsversuche erfordern, können Angriffe auf Webanwendungsebene oft effizienter durchgeführt werden.

**Beispiele:**

- Kann bei einer Online-Umfrage das Formular automatisiert ausgefüllt und abgeschickt werden, so kann ein Angreifer das Umfrageergebnis durch eine automatisierte Stimmabgabe per Skript leicht verfälschen.
- Die Informationen über registrierte Benutzer (z. B. Profilnamen und E-Mail-Adressen) können über eine URL der Webanwendung (z. B. http://host.tld/app/userDetails.php?UserID=###) abgerufen werden. Wird diese Funktion automatisiert aufgerufen (z. B. durch einfache Inkrementierung der numerischen UserID), kann so mit wenig Aufwand eine große Anzahl von Benutzerinformationen gesammelt werden (Enumeration). Die gesammelten Informationen können beispielsweise für den Versand von SPAM verwendet werden.
- Werden Benutzerkonten nach fünf fehlgeschlagenen Anmeldeversuchen für 10 Minuten gesperrt, um Brute-Force-Angriffe zu erschweren, und sind einem Angreifer die Benutzernamen der Webanwendung bekannt, so können automatisiert fehlgeschlagene Anmeldeversuche auf diese Benutzerkonten provoziert werden. In der Folge sind diese Benutzerkonten dauerhaft gesperrt und die Webanwendung kann von den Benutzern nicht mehr genutzt werden.

# G 5.167 Fehler in der Logik von Webanwendungen und Web-Services

Damit Geschäftsprozesse von einer Webanwendung abgebildet werden können, werden in der Regel einzelne Funktionen zu einer komplexen Anwendungslogik zusammengefasst. Dabei ist es für einen Prozess entscheidend, in welcher Reihenfolge die einzelnen Funktionen oder Prozessschritte aufgerufen werden. In einer Service-orientierten Architektur beschreibt der Begriff "Orchestrierung" die Zusammenstellung einzelner Web-Services. In der Orchestrierung werden die logische Abfolge der Web-Services sowie die Bedingungen zum Aufruf und sämtliche Abhängigkeiten der einzelnen Services untereinander definiert.

Werden solche logischen Abläufe bei sicherheitsrelevanten Funktionen verwendet, wie zum Beispiel bei der Authentisierung von Benutzern, kann dieser Ablauf unvorhergesehen manipuliert (zum Beispiel durch Übergehen von Einzelschritten) und somit gesteuert werden. Einem Angreifer ist es so unter Umständen möglich, den Sicherheitsmechanismus zu umgehen.

Darüber hinaus können schadhafte Aktionen auch ausgelöst werden, wenn Funktionen der Webanwendung oder des Web-Service für nicht vorgesehene Zwecke verwendet werden können. Beispielsweise kann ein Kontaktformular einer Webanwendung zum Versand von SPAM missbraucht werden, wenn die vorgegebene Kontaktadresse des Formulars geändert werden kann.

Weitere Beispiele:

- Eine Webanwendung hat ein Eingabefeld, das auf eine Länge von 20 Zeichen begrenzt werden soll. Die Eingabedaten dieses Feldes werden von der Webanwendung zusätzlich gefiltert. Dabei ist die Filterung der Eingabedaten rechenintensiver als die Prüfung der Länge der Zeichenkette. Findet die aufwendigere Filterung vor der Längenprüfung statt, kann ein Angreifer das Feld mit einer sehr langen Zeichenkette füllen, die von der ressourcenintensiven Filterkomponente verarbeitet wird. Damit kann aufgrund der Prüfreihenfolge ein hoher Ressourcenverbrauch provoziert werden, der für Denial-of-Service-Angriffe ausgenutzt werden kann.
- In einem Online-Shop wird ein Preisnachlass gewährt, wenn ein bestimmtes Produkt (Produkt X) bestellt wird. Ein Käufer möchte allerdings nicht Produkt X kaufen, sondern Produkt Y. Indem der Käufer sowohl Produkt X als auch Produkt Y zu seinem Warenkorb hinzufügt, wird der Preisnachlass gewährt. Der Zahlungsvorgang wird allerdings durch den Benutzer abgebrochen und Produkt X aus dem Warenkorb entfernt. Somit besteht kein Anspruch mehr auf einen Preisnachlass. Trotzdem wird dieser auf das Produkt Y nach einem erneuten Wechsel in den Zahlungsprozess gewährt. Aufgrund einer fehlenden Abschlussprüfung der Kriterien für den Preisnachlass kann demzufolge ein Betrüger den Kaufpreis für Produkt Y unbefugt ändern.
- Ein Angreifer verändert bei einem Web-Service Routing-Regeln und Funktionen zum Informationsaustausch, so dass eine Durchführung der abgebildeten Geschäftsprozesse verhindert wird oder vertrauliche Nachrichten an nicht-vertrauenswürdige Systeme weitergeleitet werden. Die durch die Orchestrierung abgebildete Logik in den Geschäftsprozessen kann nicht mehr sichergestellt werden und erweist sich als fehlerhaft. Informationen können falsch oder unvollständig beim Web-Service-Client ankommen.

# G 5.168 Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services

Auf Webanwendungen wird gewöhnlich mit generischen Clients (zum Beispiel Web-Browsern) zugegriffen. Diese können üblicherweise durch den Benutzer konfiguriert und angepasst werden. Sie unterliegen damit nicht der Kontrolle der Webanwendung, sondern sind von einem Angreifer, der sich Zugriff verschafft hat, beliebig manipulierbar. So können clientseitige Sicherheitsfunktionen außer Kraft gesetzt werden. Sind keine zusätzlichen, serverseitigen Schutzmaßnahmen vorgesehen, kann ein Angreifer somit unbefugt auf Ressourcen der Webanwendung zugreifen.

Auch Web-Services werden zum Teil durch Anwendungen genutzt, die sich nicht in einem vom Betreiber kontrollierbaren Sicherheitskontext befinden, zum Beispiel als Anwendungen auf mobilen Endgeräten ("Apps"). Werden Web-Services für solche Nutzungsszenarien realisiert, darf auch hier nicht von der Umsetzung von Sicherheitsfunktionen durch den aufrufenden Client ausgegangen werden, da für den Web-Service nicht erkennbar ist, ob der aufrufende Client manipuliert oder gegen einen anderen Client ohne entsprechende Sicherheitsfunktionen ausgetauscht wurde.

In der Praxis tritt diese Gefährdung besonders häufig in Verbindung mit Berechtigungsprüfungen auf, die clientseitig durchgeführt, aber nach dem Aufruf des Web-Service nicht vom Server verifiziert werden. So schützt beispielsweise das Ausblenden einer Schaltfläche im Client nicht davor, die für diese Schaltfläche hinterlegte Funktion auf Serverseite aufzurufen, indem zum Beispiel der Client manipuliert wird, URLs direkt aufgerufen werden oder Replay- oder Man-in-the-Middle-Attacken bei der Kommunikation durchgeführt werden.

Beispiele:

- Die Eingabevalidierung ist ausschließlich clientseitig in der Programmiersprache JavaScript umgesetzt. Ist die JavaScript-Unterstützung auf dem Client deaktiviert, wird daher die Validierungsfunktion nicht ausgeführt und somit umgangen. Somit können beliebige Eingaben (wie Schadcode) an die Webanwendung gesendet und ungeprüft verarbeitet werden. Ein Angreifer kann dies ausnutzen, um beispielsweise unbefugt Befehle an Hintergrundsysteme der Webanwendung zu übermitteln (zum Beispiel in Form von Datenbankabfragen um eine SQL-Injection auszuführen).
- Die Webanwendung prüft ausschließlich einen clientseitig gesetzten Parameter zur Authentisierung (zum Beispiel admin=true). Ist einem Angreifer dieser Parameter bekannt, so kann er den Parameter manuell setzen und verwenden, um sich ohne Kenntnis der Zugangsdaten an der Webanwendung anzumelden.
- Eine Anwendung zeigt den Menüpunkt "Benutzerverwaltung" nur an, wenn der eingeloggte Anwender Administrationsrechte hat. Durch einen direkten Aufruf des entsprechenden Web-Services ist aber auch eine Bearbeitung der Benutzerverwaltung ohne Administrationsrechte möglich, weil der Programmierer des Web-Service sich darauf verlassen hat, dass eine Berechtigungsprüfung im Client bereits durchgeführt wurde.

# G 5.169 Unzureichendes Session-Management von Webanwendungen und Web-Services

Da das von Webanwendungen und Web-Services verwendete Protokoll HTTP zustandslos ist, wird ein zusätzlicher Mechanismus benötigt, um den Benutzer über die Dauer einer Sitzung zu identifizieren. Webanwendungen verwenden hierbei typischerweise Session-IDs in Form eines Cookies. Bei Web-Services kann alternativ der Standard WS-SecureConversation verwendet werden. Hier werden Sessions als sogenannter *Security Context* repräsentiert, welcher wiederum über eine Session-ID innerhalb eines *Security Context Token* referenziert werden kann. Dieser Standard umfasst zusätzlich Mechanismen zur Transportsicherung, welche bei Webanwendungen sonst typischerweise über SSL/TSL realisiert wird.

Kann eine dritte Person aufgrund eines unzureichenden Session-Managements die Session-ID ermitteln, so kann sie die Webanwendung oder den Web-Service im Kontext dieser Sitzung verwenden. Dies hat zum Beispiel zur Folge, dass ein Angreifer mit der Webanwendung als legitimer authentisierter Benutzer interagieren kann, ohne die eigentlichen Zugangsdaten (Benutzername, Passwort) zu kennen.

Die Funktionalität der Webanwendung, beziehungsweise des Web-Service kann somit von Dritten mit den Rechten des legitimen Benutzers genutzt werden, um unbefugt auf schützenswerte Daten zuzugreifen oder Befehle auszuführen.

Die folgenden Beispiele beschreiben Szenarien, die zu einer kompromittierten Sitzung führen können.

- Bei einem Session-Fixation-Angriff lässt sich ein Angreifer zunächst eine Session-ID von der Webanwendung zuweisen und übermittelt diese dem Opfer (zum Beispiel über einen Link in einer E-Mail). Folgt das Opfer diesem Link und authentisiert sich anschließend gegenüber der Webanwendung mit der vom Angreifer übermittelten Session-ID, so kann der Angreifer die Anwendung anschließend mit der ihm bekannten Session-ID verwenden. Auf diese Weise ist es ihm möglich, im Sicherheitskontext des angegriffenen Benutzers auf die Webanwendung zuzugreifen und so Funktionen zu nutzen, die einem unauthentisierten Benutzer nicht zur Verfügung stehen.
- Im Falle eines Session-Hijacking-Angriffs (Sitzungsübernahme) ist das Opfer bereits an der Webanwendung beziehungsweise dem Web-Service mit einer gültigen Session-ID angemeldet. Wird die Session-ID nicht zufällig gewählt (zum Beispiel einfaches Inkrementieren eines Zählers bei der Vergabe von Session-IDs) kann ein Angreifer gültige Session-IDs durch gezieltes Ausprobieren erraten und die entsprechenden Sitzungen der angemeldeten Benutzer übernehmen.
- Werden Sitzungen von inaktiven Benutzern einer Webanwendung oder eines Web-Service nicht automatisch nach einem bestimmten Zeitintervall ungültig (Session Timeout), bleiben die Sitzungen von nicht ordnungsgemäß von der Anwendung abgemeldeten Benutzern (zum Beispiel durch Browser-Schließung) weiterhin gültig. Erlangt ein Angreifer Kenntnis von einer solchen gültigen, aber nicht mehr genutzten Session-ID oder Zugriff-

stoken, so kann er die Webanwendung im Sicherheitskontext des nicht abgemeldeten Benutzers weiter verwenden.

# G 5.170 Cross-Site Scripting (XSS)

Cross-Site Scripting-Angriffe (XSS-Angriffe) richten sich gegen die Benutzer einer Webanwendung und deren Clients. Hierbei versucht ein Angreifer indirekt Schadcode (in der Regel Browser-seitig ausführbare Skripte, wie z. B. JavaScript) an den Client des Benutzers der Webanwendung zu senden.

Werden die Ein- und Ausgaben von einer Webanwendung nicht ausreichend validiert, so kann ein Angreifer schadhaften Code in die Webanwendung einschleusen (z. B. innerhalb eines Kommentars zu einem Artikel) und so verteilen. Wird eine infizierte Webseite von einem Benutzer aufgerufen, führt der Client (z. B. Browser) den eingefügten Schadcode aus. Aus Sicht des Benutzers stammt der schadhafte Code von der Webanwendung und wird somit als vertrauenswürdig eingestuft. Daher wird der Schadcode im Sicherheitskontext der Webanwendung interpretiert und es ist dem Angreifer möglich, Befehle im Kontext einer möglicherweise bestehenden Sitzung des betroffenen Benutzers auszuführen.

Es werden drei Klassen von XSS-Angriffen unterschieden:

- persistent (beständig)
- reflektiert (nicht-persistent)
- DOM-basiert (lokal)

Die folgenden Beispiele verdeutlichen die Unterschiede der Angriffsklassen:

- Einem Angreifer gelingt es einen Eintrag in einem Gästebuch zu hinterlassen, der JavaScript-Code enthält. Ruft ein Benutzer den entsprechenden Gästebucheintrag auf, wird das Skript übermittelt und vom Browser ausgeführt. Das Skript wird im Sicherheitskontext der Webanwendung ausgeführt und hat somit Zugriff auf die clientseitig im Cookie gespeicherte SessionID des Benutzers, wenn dieses Session-Cookie (fehlerhaft) ohne HttpOnly-Flag gesetzt wurde. Diese Information wird von dem Skript an den Angreifer weitergeleitet, der die SessionID nutzen und damit die Sitzung eines authentisierten Benutzers übernehmen kann. Da der JavaScript-Code vom Browser lediglich interpretiert und nicht angezeigt wird, kann dieser Vorgang von dem Benutzer nur schwer erkannt werden. Hierbei handelt es sich um einen persistenten XSS-Angriff, da der Schadcode in dem Gästebuch-Eintrag und somit in der Webanwendung dauerhaft gespeichert wird.
- Ein Angreifer präpariert den GET-Parameter einer URL so, dass dieser JavaScript-Code enthält. Da die Webanwendung den verwendeten Parameter ungeprüft für die Aufbereitung der Webseite verwendet, wird der eingeschleuste JavaScript-Code an den Client übermittelt und vom Browser im Sicherheitskontext der Webanwendung ausgeführt. Gelingt es dem Angreifer, einen derart präparierten Link so zu verteilen (z. B. per E-Mail) und klickt ein angemeldeter Benutzer diesen Link an, so wird das schadhafte Skript im Browser des Benutzers ausgeführt. Ein solcher XSS-Angriff wird als reflektiert oder nicht-persistent bezeichnet, da der Schadcode nicht dauerhaft gespeichert wird, sondern nach der Eingabe direkt von der Webanwendung zurückgesendet wird.
- JavaScript-Code in einer Webseite verarbeitet Parameter aus der URL (z. B. http://host.tld/param="Inhalt") und bindet sie zur Anzeige in die Webseite ein. Über die Manipulation der Parameter können somit beliebige Inhalte in die Webseite eingefügt werden. Wird die Seite mit schadhaftem JavaScript-Code im Parameter aufgerufen, so wird dieser Code in die Webseite eingebunden und vom Browser ausgeführt. Im Gegensatz zu vorherigen Angriffstypen wird der Schadcode nicht von der Webanwendung

in die Webseite eingefügt, sondern erst lokal vom Browser durch die clientseitige JavaScript-Verarbeitung der URL-Parameter. Hierbei kann der Schadcode die Document Object Model (DOM)-Umgebung manipulieren und darüber die Webseitenstruktur und Inhalte verändern.

# G 5.171 Cross-Site Request Forgery (CSRF, XSRF, Session Riding)

Können schreibende Aktionen einer Webanwendung ohne weitere Überprüfung der Authentizität des HTTP-Requests (z. B. durch Tokens in versteckten Formularfeldern) genutzt werden, kann ein Angreifer dem Benutzer einen präparierten Link zur Ausführung eines Befehls übermitteln.

Der Link kann beispielsweise mithilfe von Social Engineering-Methoden (z. B. als Link in einer E-Mail) einem Benutzer mit der Aufforderung zur Ausführung übermittelt werden. Ist der Benutzer an einer Webanwendung mit einer bestehenden Sitzung angemeldet und folgt diesem präparierten Link, wird der übertragene Befehl von der Webanwendung ausgeführt. Die Webanwendung interpretiert hierbei den HTTP-Request als eine vom Benutzer bewusst durchgeführte Aktion. Dabei können sich hinter einem solchen Link privilegierte Befehle wie das Ändern der Zugangsdaten oder das Anlegen eines neuen Benutzers verbergen. Dem Benutzer bleibt unter Umständen der Vorgang verborgen und es wird lediglich eine Mitteilung zur erfolgreich durchgeführten Aktion angezeigt.

Im Gegensatz zu XSS (siehe G 5.170 *Cross-Site Scripting (XSS)*) ist das Angriffsziel nicht das Ausführen von Skriptcode, sondern von unbefugten, schreibenden Aktionen im Kontext des angemeldeten Benutzers.

Mit einer Kombination von CSRF und XSS ist es möglich, den Client über die Ausführung von Skripten unbemerkt zu steuern, sodass eine Interaktion durch den Anwender nicht mehr notwendig ist. Anweisungen im Skript können z. B. eine Weiterleitung auf einen präparierten Link automatisieren.

**Beispiel:**

- Während ein Anwender an der Administrationsoberfläche eines Routers angemeldet ist, surft er mit demselben Browser gleichzeitig im Internet. Durch einen präparierten Link auf einer Webseite wird eine Anfrage zur Änderung des Zugangspasswortes an den Router gesendet. Hierbei sendet der Browser automatisch das Session Cookie mit, worüber die Webanwendung die Authentizität der Anfrage verifiziert und die Änderung durchführt. Da der Benutzer mit einer gültigen Sitzung an der Administrationsoberfläche angemeldet ist, wird der Befehl ausgeführt und das Zugangspasswort auf ein ihm unbekanntes Passwort abgeändert.

# G 5.172 Umgehung der Autorisierung bei Webanwendungen und Web-Services

Wenn ein Benutzer oder ein Web-Service-Client sich ordnungsgemäß an einer Webanwendung oder einem Web-Service angemeldet hat, so hat er (in Abhängigkeit von der ihm zugewiesenen Rolle) nicht zwangsläufig Zugriff auf alle Funktionen, welche die Webanwendung oder der Web-Service bereitstellen. Daher muss die Webanwendung oder der Web-Service nach erfolgreicher Authentisierung des Benutzers oder des Clients für einzelne Funktionen verifizieren, ob dieser für die Ausführung berechtigt ist (Autorisierung).

Bei Angriffen gegen die Autorisierungskomponente wird versucht, auf Funktionen oder Daten zuzugreifen, die eigentlich nur einer eingeschränkten Benutzergruppe zur Verfügung stehen. Ist die Autorisierung der Zugriffe fehlerhaft umgesetzt, kann ein Angreifer seine Berechtigungen erweitern und Zugriff auf geschützte Bereiche und Daten erhalten. Dies geschieht üblicherweise durch gezielte manipulierte Eingaben eines Angreifers.

Denkbare Angriffsziele sind zum Beispiel Konfigurationsdateien mit fest codierten Zugangsdaten für Hintergrundsysteme, geschützte Bereiche oder Funktionen der Webanwendung.

Im Folgenden werden mögliche Schwachstellen bei der Autorisierung von Zugriffen auf Web-Ressourcen aufgeführt.

**Beispiele:**

- Bei der Eingabe von Pfadangaben können über einen relativen Bezug (durch sogenanntes Path Traversal) nicht für den Zugriff über die Webanwendung vorgesehene Ressourcen abgerufen werden (zum Beispiel *../../../config.xml*). Hierdurch können unbefugt schützenswerte Dateien wie Konfigurationsdateien aus dem Dateisystem heruntergeladen oder auch überschrieben werden. Über relative Pfadangaben lassen sich nicht nur Dateien der Webanwendung erreichen, sondern es können unter Umständen ebenso Ressourcen des darunter liegenden IT-Systems abgerufen werden.
- Webanwendungen verwenden häufig Objekt-Referenzen zur Adressierung einer Ressource in Hintergrundsystemen (zum Beispiel http://host.tld/get.php?id=2). So können Ressourcen wie Inhalte zur Darstellung einer Webseite einem Datenbankeintrag zugeordnet werden. Werden Objekt-Referenzen von der Autorisierungskomponente nicht berücksichtigt, kann über eine Manipulation der Referenz *id* in der URL gegebenenfalls auf vertrauenswürdige Ressourcen zugegriffen werden.
- Eine manchmal genutzte Möglichkeit Informationen einer Webanwendung zu schützen besteht darin, die URL, die diese Informationen verlinkt, nur autorisierten Benutzern anzuzeigen. Unautorisierten Benutzern ist die URL nicht bekannt. Ein Angreifer kann durch systematisches Ausprobieren versuchen, die URL zu erraten und so Zugriff auf geschützte Informationen beziehungsweise Funktionen der Webanwendung zu erhalten. Dieser Angriff wird "Forced Browsing" genannt.
- Ist die Autorisierungskomponente eines Web-Service fehlerhaft konfiguriert, sodass sie zum Beispiel auch anonyme Zugriffe oder Zugriffe auf falsche Dienste erlaubt, so kann ein Unberechtigter diese Dienste aufrufen und sich so Zugang zu Daten und Funktionen verschaffen.

# G 5.173 Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services

Werden die Ein- und Ausgabedaten einer Webanwendung oder eines Web-Service nicht ausreichend validiert, so kann ein Angreifer Inhalte, wie zum Beispiel Schadcode zur Manipulation von Server, Clients oder nachgelagerten Systemen, einbinden. Die eingebundenen Daten werden dem Benutzer im Sicherheitskontext der Webanwendung oder des Web-Service zurückgegeben. Demzufolge ist es dem Benutzer der Webanwendung beziehungsweise dem Consumer des Web-Service nicht oder nur eingeschränkt möglich, die manipulierten Anteile der Ausgabe zu erkennen. Der Angreifer kann so die Vertrauensstellung des authentisierten Benutzers gegenüber der Webanwendung oder dem Web-Service ausnutzen.

Bei Web-Services kann Schadcode auf den Web-Service selbst oder aber auf einen Consumer des Web-Service (Endanwendung oder nachgelagerter Web-Service) abzielen. Bei Webanwendungen können sowohl die Clients als auch die Server der Webanwendung durch eingebundenen Schadcode angegriffen werden. So können von einem Angreifer eingebettete Daten beispielsweise Schadcode zur Ausführung auf den Clients (zum Beispiel zum Auslesen von vertraulichen Daten) oder gefälschte Anmelde-Formulare zum Diebstahl von Zugangsdaten beinhalten. Wird der eingebundene Programmcode von der Webanwendung oder dem Web-Service ausgeführt, so kann darüber hinaus das Betriebssystem des Servers kompromittiert werden.

Beispiele:

- Über Parameter in der URL können in dynamischen Webseiten fremde Inhalte eingebunden werden, die sich nicht von den Inhalten der Webanwendung unterscheiden lassen (zum Beispiel http://host.tld/index.php?frame=http://angreifer.tld&title=modifizierter Titel). Hierbei wird der übermittelte Parameter *title* in der zurückgelieferten Webseite der Webanwendung als Titel im HTML-Dokument eingebettet. Ebenso wird der Parameter *frame* als Quelle für einen Frame auf der Webseite verwendet. Hiermit lassen sich über die Parameterwerte beliebige Inhalte und Programmcode (zum Beispiel JavaScript) in die Webseite einfügen. Derselbe Angriff ist auf Web-Services übertragbar, welche über eine REST-Schnittstelle angesprochen werden, ihre Parameter also als Teil der URL übergeben bekommen.
- Eine Weiterleitungsfunktion akzeptiert beliebige Werte als Zieladresse. In der Folge kann über einen manipulierten Parameter eine Weiterleitung auf nicht vertrauenswürdige Webseiten durch einen Angreifer veranlasst werden (zum Beispiel http://host.tld/redirect.php?target=http://angreifer.tld). Der Benutzer erwartet aufgrund der Ursprungs-Domäne der Webanwendung die Weiterleitung auf eine vertrauenswürdige Adresse. Dies kann von einem Angreifer ausgenutzt werden, um über die Weiterleitung auf eine gefälschte Anmeldeseite zur Eingabe der Zugangsdaten einen Phishing-Angriff zu realisieren.
- In Webanwendungen können fremde Inhalte von Partnern (zum Beispiel Werbeanzeigen in einem iFrame) eingebunden werden. Die Kontrolle über diese Inhalte liegt üblicherweise beim Partner und nicht beim Betreiber der Webanwendung. Werden Schadsoftware oder unerwünschte Inhalte über den Partner eingebunden, so kann dies den Ruf des Webanwendungs-Be-

treibers schädigen, da die Inhalte dem Benutzer im Kontext der Webanwendung dargestellt werden. Darüber hinaus können die Clients der Besucher von der Schadsoftware infiziert und somit kompromittiert werden.

- Über eine Upload-Funktion der Webanwendung lassen sich beliebige Dateien in der Verzeichnisstruktur auf dem Server speichern. Dadurch können gegebenenfalls schadhafte Skripte zur Ausführung auf der Webanwendung gespeichert oder bestehende Dateien (zum Beispiel Konfigurationsdateien) überschrieben werden. Der Upload von großen Mengen an Daten kann auch zu einer Verhinderung des Dienstes führen.
- In die XML-formatierten Parameter für einen Web-Service werden externe Referenzen eingebettet, zum Beispiel <!DOCTYPE sample PUBLIC "foo" "">. Falls die serverseitige Anwendung bei der Interpretation der Ergebnisse der externen Referenz folgt, kann der Angreifer damit ausgehende IP-Verbindungen vom Server aus initiieren und so entweder den Betrieb stören (Denial-of-Service) oder Informationen über interne Netzstrukturen gewinnen.

# G 5.174 Injection-Angriffe

Bei einem Injection-Angriff versucht ein Angreifer, Befehle in eine Webanwendung oder einen Web-Service zu injizieren und auszuführen. Der Angriff richtet sich dabei in der Regel gegen serverseitig verwendete Interpreter oder einen Parser.

Werden beispielsweise eingehende Daten unzureichend validiert, so können Eingaben (zum Beispiel Formulardaten, Cookies, SOAP-Nachrichten oder HTTP-Header) so gewählt werden, dass sie von der Webanwendung und den verwendeten Interpretern beziehungsweise Parsern (zum Beispiel SQL-Datenbank, XML-Prozessoren, LDAP-Verzeichnisdienst) als Befehl interpretiert werden. Auf diese Weise können unbefugt Befehle zum Auslesen oder Manipulieren von Daten übermittelt werden.

Können mittels Injection beliebige System-Kommandos ausgeführt werden, so kann ein Angreifer die Webanwendung oder den Web-Service als Ersatz für eine System-Shell nutzen. Die abgesetzten System-Kommandos werden dabei üblicherweise im Sicherheitskontext und somit mit den Privilegien der Webanwendung/des Web-Service oder des verwendeten Interpreters beziehungsweise Parsers ausgeführt.

Injection-Angriffe werden anhand der angegriffenen Interpreter/Parser in Angriffstypen klassifiziert. Die folgenden Beispiele verdeutlichen diese Klassifizierung:

- SQL-Injection (siehe auch G 5.131 *SQL-Injection*)
- LDAP-Injection
- Mail-Command-Injection
- OS-Command-Injection
- SSI-Injection
- XPath-Injection
- Code-Injection

# G 5.175 Clickjacking

Bei einem Clickjacking-Angriff werden Teile einer Webseite bei der Darstellung überdeckt, sodass für den Benutzer nicht sichtbare, transparente Ebenen die angezeigten Inhalte der Webseite überlagern.

In diesen transparenten Ebenen können beliebige Inhalte oder Bedienelemente eingebunden werden, ohne dass sie für den Benutzer sichtbar sind. Klickt der Benutzer auf die vermeintlichen Inhalte der Webseite, so wird der Klick nicht an die sichtbare Ebene, sondern an die überlagerten Ebenen gesendet und somit entführt (engl. *Hijacking*). Die Angriffsbezeichnung Clickjacking ergibt sich aus der Wortkombination *Click* für Mausklick und *Jacking* von Hijacking.

Neben Mausklicks können darüber hinaus auch Tastatureingaben mittels transparent eingeblendeter Textfelder auf fremde Server umgeleitet werden (z. B. Platzierung über Passwortfelder).

**Beispiele:**

- Ein Angreifer nimmt an einem Programm für Werbeanzeigen teil, bei dem die Höhe der Provision anhand der Klicks durch die Besucher ermittelt wird (Klickvergütung oder Pay-per-Click). Dabei überlagert er einen Teil einer Webanwendung mit einem unsichtbaren Link zur Werbeanzeige, sodass der Benutzer unbemerkt auf die Werbeanzeige klickt. Dadurch erhöht sich die Anzahl der Klicks und damit die auszuzahlende Provision.
- Ein Angreifer platziert auf einer Webseite einen unsichtbaren "Gefällt mir"-Button für seine eigene Facebook-Seite, der immer dem Mauszeiger folgt. Für den Benutzer ist das nicht erkennbar. Klickt er irgendwo übermittelt auf der Seite, wird die "Gefällt- mir"-Funktion von Facebook ausgeführt er übermittelt seine Facebook-Daten an den Angreifer, der diese dann weiter ausnutzen kann.

# G 5.176 Kompromittierung der Protokolldatenübertragung bei zentraler Protokollierung

Bei einer zentralen Speicherung der Protokolldaten werden die aufgezeichneten Informationen an einen Protokollierungsserver übermittelt, der sie verarbeitet und auswertet. Die übertragenen Protokollierungsereignisse können personenbezogene Informationen wie Benutzernamen enthalten, die sich einer konkreten Person zuordnen lassen. Werden die Protokolldaten über ungesicherte und nicht verschlüsselte Übertragungswege übermittelt, können sie abgehört und manipuliert werden.

**Ausnutzen von In-Band-Verbindungen**

Wenn IT-Systeme in einem unsicheren Netz betrieben werden, sind sie mit großer Wahrscheinlichkeit Angriffen aus diesem Netz ausgesetzt. Ein Beispiel ist ein Paketfilter in einem Sicherheitsgateway, der zwischen das öffentliche Netz und das Application-Level-Gateway geschaltet wird. Sollen Protokollinformationen des Paketfilters an einen zentralen Protokollierungsserver gesendet werden, ist eine Datenverbindung über das Application-Level-Gateway und über eventuell weitere Systeme zum zentralen Protokollierungsserver notwendig (In-Band). Die Möglichkeit dieser Verbindung könnte auch von einem Angreifer ausgenutzt werden, da von Außen initiierte Verbindungen in das interne Netz eine Schwachstelle darstellen. Bei einer Out-of-Band-Verbindung treten diese Probleme nicht auf, weil die Protokolldaten innerhalb eines eigenen, abgeschlossenen Netzes transportiert werden. Allerdings ist der dafür notwendige Aufwand deutlich höher. Es muss eine eigene Netzinfrastruktur aufgebaut sowie ein weiteres Netz administriert werden. Zudem können die möglichen Schäden gravierend sein, falls es einem Angreifer gelingen würde, das Out-of-Band-Netz zu kompromittieren.

**Kompromittierung des zentralen Protokollierungsservers**

Wird ein zentraler Protokollierungsserver, der nicht in einem eigenen Administrationsnetz platziert wurde, kompromittiert, erleichtert er aufgrund seiner zentralen Platzierung Angriffe auf weitere Komponenten. Weil er sowohl von IT-Systemen vor als auch hinter dem Sicherheitsgateway erreichbar sein muss, bietet er einem Angreifer die Möglichkeit, das Sicherheitsgateway eines Informationsverbundes zu umgehen. Dadurch könnten beispielsweise der Datenverkehr zwischen dem E-Mail-Server und dem Protokollierungsserver mit einem Netzanalyse-Tool aufgezeichnet und eventuelle personenbezogene Daten ausgelesen werden. Des Weiteren hat ein Angreifer dadurch die Möglichkeit, Protokolldaten einzusehen und diese zu manipulieren.

**Manipulierte Protokolldaten**

Manipuliert ein Angreifer Protokolldaten, sind deren Integrität und Vollständigkeit infrage gestellt und ihre Beweiskraft und Verlässlichkeit nicht mehr gewährleistet. Auch bei einem IT-Frühwarnsystem können manipulierte Protokollmeldungen zu großen Problemen führen, wenn kein vollständiges Lagebild erzeugt werden kann und dadurch beispielsweise Angriffe auf IT-Systeme oder Anwendungen unentdeckt bleiben. Ein Grund für unvollständige Protokolldaten kann der Einsatz von Netz-Protokollen wie dem User Datagram Protocol (UDP) sein, die keine Mechanismen vorsehen, um zu überprüfen, ob alle Pakete komplett übertragen wurden.

**Bandbreitenengpässe**

Durch die große Menge an Protokolldaten, die über das Netz zusätzlich zu den Nutzdaten übertragen werden, kann es bei Bandbreitenengpässen dazu kommen, dass die Übertragung der Protokollmeldungen die der Nutzdaten beeinträchtigt. Des Weiteren kann es passieren, dass durch die Bandbreitenengpässe die Protokollinformationen zeitverzögert weitergeleitet werden oder ganz verloren gehen. Dies führt bei einem IT-Frühwarnsystem unter Umständen zu erheblichen Problemen, weil nur durch die Summe der einzelnen Teilinformationen der verschiedenen IT-Systeme ein Gesamtbild des Informationsverbundes dargestellt werden kann.

**Beispiel:**

- Bei der Planung, einen zentralen Protokollserver einzusetzen, wurde beschlossen, dass die Protokolldaten über eine Netzschnittstelle (In-Band) übertragen werden sollen. Durch das Tunneling der Protokollmeldungen über SSL werden die Meldungen im Netz verschlüsselt übertragen. Allerdings entsteht durch das Tunneling eine Sicherheitslücke im Sicherheitsgateway, die ein Angreifer ausnutzen kann, um in das interne Netz einzudringen.
- Die Protokolldatenübertragung von den verschiedenen IT-Systemen zum zentralen Protokollierungsserver erfolgt über das syslog-Protokoll, das die Nachrichten verbindungslos per UDP-Protokoll verschickt. Durch einen vorübergehenden Bandbreitenengpass gehen einige Protokollnachrichten verloren. Da keine zusätzlichen Mechanismen eingesetzt werden, um zu gewährleisten, dass alle Datenpakte am Ziel ankommen, wird ein kurzzeitiger Webserver-Ausfall nicht bemerkt.
- Seit Jahren werden im Informationsverbund eines mittelständischen Unternehmens sowohl die Nutz- als auch die Protokolldaten über ein und dieselbe Netzschnittstelle (In-Band) übertragen. Aufgrund gestiegener Auslastungen und fehlender Zwischenspeicher (Caching) wurden in den letzten Monaten immer wieder relevante Protokolldaten zugunsten höher priorisierter Nutzdaten verworfen. Dies führt dazu, dass der Ausfall eines Datei-Servers zu spät erkannt wurde und der Betrieb für einen ganzen Tag eingestellt werden musste.

# G 5.177 Missbrauch von Kurz-URLs oder QR-Codes

Webseiten werden üblicherweise über eine URL (Uniform Resource Locator) angesteuert, die daher auch Web-Adresse genannt wird. Die Komplexität vieler Webseiten führt häufig zu relativ langen Web-Adressen, die schwer zu merken sind und vor allem bei mobilen Endgeräten wie Smartphones nicht in einer Zeile dargestellt werden können. Daher haben sich verschiedene Methoden entwickelt, um den Benutzern die Nutzung von Webadressen zu erleichtern. Prominente Vertreter sind Kurz-URLs und QR-Codes.

**Kurz-URLs**

Kurz-URLs bezeichnen einen weitverbreiteten Dienst im Internet, bei dem lange URLs durch kürzere URLs ersetzt werden. Kurz-URLs erleichtern es, Referenzen und Verweisen in Zeitschriftenartikeln zu folgen. Viele Artikel in papiergebundenen Zeitschriften verweisen auf Quellen aus dem Internet bzw. enthalten Hinweise zu Internetseiten. Anders als bei Online-Artikeln müssen diese per Hand abgetippt werden. Kurz-URLs verringern den Aufwand dafür erheblich. Kurz-URLs haben also einige Vorteile, aber auch einige Risiken:

- Verfügbarkeit: Kurz-URLs werden, ohne dass die Benutzer eingreifen müssen, über die Datenbank eines Dienstleisters in die dort hinterlegte ursprüngliche Web-Adresse aufgelöst. Diese Datenbank mit den Zuordnungen zwischen den kurzen und langen URLs muss verfügbar sein. Große Datenbanken haben Milliarden an Einträgen. Fällt die Datenbank zeitweise oder dauerhaft aus, sind Milliarden von Kurz-URLs unbrauchbar. Ferner kann es sein, dass der bisherige Anbieter eines Dienstes die Nutzungsbedingungen ändert, so dass die darüber generierten Kurz-URLs nicht mehr ohne weiteres genutzt werden können.
- Datenschutz: Durch die Benutzung von Kurz-URLs kann der Anbieter des Dienstes nachvollziehen, welche IP-Adresse wann auf welche Seite zugegriffen hat.
- Integrität: Aus einer Kurz-URL ist nicht ersichtlich, wohin sie verweist. Daher sind Kurz-URLs für alle Formen von Angriffen attraktiv, bei denen Benutzer auf manipulierte Webseiten gelockt werden sollen. So ist beispielsweise bei einer gefälschten E-Mail-Adresse eines eventuell bekannten Absenders, die eine Kurz-URL enthält, die Chance größer, dass der Link wirklich angeklickt wird. Ferner kann die Datenbank des Anbieters der Kurz-URL manipuliert worden sein, so dass die Kurz-URLs gar nicht mehr auf ihr eigentliches Ziel verweisen.

**QR-Codes**

QR-Codes (Quick Response) sind, ähnlich wie Barcodes, Darstellungen von Daten in maschinenlesbarer Form, in diesem Fall handelt es sich typischerweise um Quadrate, in denen mit Mustern aus kleineren Quadraten Informationen standardisiert gespeichert sind. QR-Codes finden sich oft auf Produkten oder Verbraucherinformationen und dienen dazu, Anwender auf zusätzliche Informationsquellen zu verweisen, die für diese nützlich oder interessant sein könnten. Die Anwender müssen den jeweiligen QR-Code zunächst abfotografieren oder einscannen, z. B. mit ihrem Smartphone. Auf dem Endgerät muss außerdem eine Applikation installiert sein, um die in den QR-Codes enthaltenen Informationen wie beispielsweise URLs, Adressen, Telefonnummern oder WLAN-Zugangsinformationen aufzulösen. Ein häufiges Anwendungsszenario sind QR-Codes auf Prospekten, in denen eine URL codiert ist, aber auch in industriellen Umgebungen und in der Logistik werden sie oft eingesetzt.

QR-Codes sind mit einer hohen Fehlertoleranz maschinenlesbar, lassen sich aber von Menschen nicht ohne weiteres dekodieren. Daher können Benutzer vor dem Einlesen eines QR-Codes nicht erkennen, welche Informationen in diesem kodiert wurden. Die Gefährdungen sind ähnlich wie bei Kurz-URLs. Beispielsweise könnten QR-Codes auf Webseiten mit Schadsoftware oder auf kostenpflichtige Service-Rufnummern verweisen. Außerdem könnten QR-Codes auch Informationen enthalten, über die Schwachstellen im Betriebssystem des auslesenden Endgerätes ausgenutzt werden. Beispielweise könnte ein QR-Code Programmaufrufe beinhalten, die zu einen Buffer Overflow oder zu einem Injection-Angriff führen.

**Beispiel:**

- Ein Angreifer erstellte einen QR-Code, der auf über eine URL auf eine Webseite verwies, die mit Schadsoftware für ein weitverbreitetes Smartphone-Betriebssystem verseucht war. Diesen druckte er im passenden Format aus und überklebte damit zahlreiche QR-Codes auf Litfaßsäulen und anderen Werbeträgern auf einer gut besuchten Technik-Messe. Zahlreiche Anwender lasen den QR-Code ein, wodurch deren Smartphones mit der Schadsoftware infiziert und kostenpflichtige SMS an einen ausländischen Dienst auf Kosten der Anwender verschickt wurden.

# G 5.178 Missbrauch von Administratorrechten im Cloud-Management

Das Cloud-Management, das über den Cloud-Verwaltungsserver gesteuert wird, muss Funktionen und Mittel für die Verwaltung der Cloud-Ressourcen bereitstellen. Dies umfasst die Ansteuerung von physischen und virtuellen Cloud-Ressourcen, um Konfigurationen manuell oder automatisiert vorzunehmen. Der Verwaltungsserver steuert die Provisionierung und De-Provisionierung von Cloud-Diensten, registriert die Cloud-Dienste für Cloud-Mandanten und dient als zentrales Verzeichnis der Cloud-Dienste.

Die Einflussmöglichkeiten des Cloud-Verwaltungsservers auf die Cloud-Dienste sind weitreichend und können zum Missbrauch der Funktionen des Cloud-Managements führen.

Eine missbräuchliche Administration liegt vor, wenn vorsätzlich Administrator-Privilegien ausgenutzt (ob rechtmäßig oder unrechtmäßig erworben) werden, um der Cloud-Infrastruktur oder deren Benutzern zu schaden.

**Beispiele:**

- Die Funktionen des Cloud-Verwaltungsservers ermöglichen die Zuordnung von Speicherbereichen oder virtuellen Maschinen. Hiervon können unautorisiert Kopien erstellt und aus den gesicherten Cloud-Umgebungen unerlaubt entfernt werden.
- Die Cloud-Verwaltungssoftware kann über die Virtualisierungsfunktionen Prozessor-Zwischenstände und Inhalte des Arbeitsspeichers auf das Speichersystem oder in das Speichernetz des Verwaltungsservers schreiben.
- Die virtuellen Maschinen für Cloud-Dienste können unautorisiert unterbrochen werden.
- Die Funktion zum Einfrieren (Erstellen sogenannter *Snapshots*) von virtuellen Maschinen und Cloud-Diensten kann dazu zweckentfremdet werden, um Sicherheitsmaßnahmen zu umgehen.

# G 5.179 Angriffe auf Protokolle

Innerhalb einer Service-orientierten Architektur (SOA) können unterschiedliche Protokolle zum Nachrichten- und Daten-Austausch eingesetzt werden. Nicht alle Protokolle bringen dabei ausreichende Sicherheitsmechanismen mit, um die Vertraulichkeit und Integrität der übertragenen Informationen und die Authentizität der Kommunikationspartner sicherzustellen.

So können zum Beispiel beim Einsatz von HTTP ohne zusätzliche Sicherheitsschicht (wie SSL/TLS) die übertragenen Informationen im Netz mitgelesen und gegebenenfalls sogar verändert werden. Die Sicherheit eines Web-Service ist damit abhängig von der Sicherheit der eingesetzten oder unterstützten Kommunikationsprotokolle.

Auch beim Einsatz proprietärer oder selbst entwickelter Protokolle für die Kommunikation ist besondere Vorsicht geboten. Die Gefahr von Implementierungsfehlern, die sich von einem Angreifer ausnutzen lassen, ist hier gegenüber etablierten, veröffentlichten Protokollen hoch.

Werden kryptographisch abgesicherte Protokolle eingesetzt, so ist die Schutzwirkung abhängig von den eingesetzten Kryptoverfahren, Schlüssellängen und der Implementierung der Protokolle. So kann auch der Einsatz von SSL/TLS nur einen geringen Schutz bieten, wenn veraltete Versionen des Standards genutzt werden oder schwache Kryptoverfahren zum Einsatz kommen.

Ein häufig für die Kommunikation von Web-Services eingesetztes Protokoll ist SOAP, das auf der Übertragung von XML-Nachrichten, im Regelfall per HTTP, basiert. Fehlende Sicherheitsmechanismen von HTTP beziehungsweise dem genutzten Übertragungsprotokoll müssen dabei durch entsprechende Strukturen in XML, insbesondere XML-Signaturen, XML-Verschlüsselung und Authentisierungstoken ersetzt werden. Andernfalls drohen Angriffe wie das Abhören oder Verfälschen von Nachrichteninhalten, die Manipulation von Parametern beim Diensteaufruf per SOAP oder Injection-Angriffe.

# G 5.180 Angriffe auf Registries und Repositories

In einer serviceorientierten Architektur (SOA) werden Metainformationen zentral in Diensteverzeichnissen ("Registries") und Metadaten-Speichern ("Repositories") hinterlegt. Die dort hinterlegten Informationen umfassen Dienstbeschreibungen, Schnittstellen und Aufrufparameter, aber auch Service oder Security Policies.

Die Repositories sind dabei als Datenbanken oder Verzeichnisdienste mit einer definierten Schnittstelle zum Abruf der Informationen (in der Regel per HTTP) realisiert. Bei unsauberer Implementierung oder unsicherer Konfiguration können die Repositories von einem Angreifer manipuliert werden (zum Beispiel durch Injection-Angriffe). Damit kann der Angreifer nicht nur Informationen über die angebotenen Dienste und die eingesetzten Sicherheitsmechanismen erlangen (siehe auch G 5.184 *Informationsgewinnung über Web-Services*), sondern auch die bereitgestellten Service-Beschreibungen und Policies verändern oder durch eigene ersetzen. Dadurch kann er unter Umständen Dienst-Aufrufe oder XML-Nachrichten umleiten oder vorgesehene Sicherheitsfunktionen außer Kraft setzen.

Durch die Verfälschung oder Löschung von Metainformationen kann ein Angreifer auch die Funktionsfähigkeit oder Nutzbarkeit der angebotenen Web-Services beeinträchtigen (Denial-of-Service). Ebenso ist es denkbar, durch einen Denial-of-Service-Angriff auf die Registry beziehungsweise das Repository selbst die Funktionsfähigkeit der SOA sehr effektiv an einem zentralen Punkt zu attackieren.

# G 5.181 Angriffe auf das Identitäts- und Zugriffsmanagement bei Web-Services

Um angebotene Web-Services vor einem missbräuchlichen Zugriff zu schützen, müssen entsprechende Zugriffsschutzmechanismen umgesetzt sein, die die Identität eines aufrufenden Benutzers oder Dienstes prüfen und den Zugriff wirksam verwehren, wenn dem Benutzer oder Dienst die Berechtigung zum Aufruf des Dienstes fehlt. Dabei kann die Berechtigung auch abhängig sein von den übergebenen Parametern: So ist es zum Beispiel denkbar, dass ein Kunde nur Daten zu den eigenen Aufträgen abfragen darf, oder ein Berechtigungsverwalter nur Mitarbeiter seiner eigenen Institution mit Berechtigungen ausstatten kann.

Der erste mögliche Ansatzpunkt für einen Angreifer ist das verwendete Zugriffsschutzsystem selbst. Findet der Angreifer Fehler in der Berechtigungsprüfung, so kann er diese ausnutzen, um sich unbefugten Zugriff zu verschaffen. Dies ist insbesondere der Fall, wenn Berechtigungsprüfungen nicht umgesetzt werden, weil die Entwickler implizite Annahmen darüber machen, wer die Services in welchem Kontext aufruft. Dass eine Funktion innerhalb einer Anwendung erst nach erfolgreicher Anmeldung zur Verfügung steht, heißt aber nicht, dass der dahinterstehende Web-Service von einem Angreifer nicht auch außerhalb des Anwendungskontextes aufgerufen werden kann.

Wird innerhalb einer serviceorientierten Architektur (SOA) die Zugriffskontrolle manipuliert, können Angreifer unberechtigte Informationen über Dienste der SOA-Infrastruktur erhalten.

Nutzt das Zugriffsschutzsystem für die Berechtigungsprüfung Informationen aus einer externen Quelle, zum Beispiel einem Verzeichnisdienst, so kann ein Angreifer auch versuchen, die Berechtigungsinformationen in der externen Quelle zu manipulieren oder dem Zugriffsschutzsystem falsche oder manipulierte Berechtigungsdaten unterzuschieben, zum Beispiel durch einen Man-in-the-Middle-Angriff (siehe G 5.143 *Man-in-the-Middle-Angriff*).

Ein zweiter Angriffspunkt ist die Identität des aufrufenden Benutzers oder Dienstes. Gelingt es dem Angreifer, einen Dienstaufruf mit der Identität eines berechtigten Benutzers oder Dienstes zu initiieren, so kann er effektiv dessen Berechtigungen für die Durchführung seines Angriffs missbrauchen.

Ein solcher Identitätsdiebstahl kann beispielsweise durch eine schwache Implementierung des Sitzungsmanagements möglich werden: "Session Hijacking" oder "Session Fixation" (siehe G 5.169 *Unzureichendes Session-Management von Webanwendungen und Web-Services*). Ziel eines Session-Hijacking-Angriffs ist es, Nutzerprivilegien für ein System, einen Dienst oder eine Anwendung zu erhalten. Manche Web-Services verwenden für ihre Sessions eine eindeutige Identifikationsnummer. Gelingt es einem Angreifer, Nachrichten mit einer solchen Session-ID abzufangen, kann er an der entsprechenden Transaktion teilnehmen.

Andere Angriffsarten umfassen das Mitschneiden von Nachrichten und das Wiedereinspielen der aufgezeichneten Nachrichten (mit gültigen Authentisierungsinformationen des originalen Absenders) in einem anderen Kontext ("Replay-Attacken"). Bei einer Replay-Attacke werden Nachrichten, die von einem Web-Service akzeptiert wurden, nochmals verwendet. Ein Angreifer fängt dazu in der Regel valide Nachrichten von Benutzern ab und sendet sie erneut an

den Web-Service. Replay-Angriffe werden meist als Basis für weitere Angriffe wie zum Beispiel Denial-of-Service- oder Man-in-the-Middle-Attacken benutzt. Häufig dienen sie Angreifern dazu, Authentisierungsmechanismen zu umgehen. Sofern hiergegen keine Schutzmaßnahmen vorgesehen sind, kann der Angreifer dabei gegebenenfalls sogar verschlüsselte Nachrichten abfangen und verwenden, ohne dass er die eingesetzte Verschlüsselung brechen muss.

Schließlich können auch externe, vom Web-Service genutzte Identitätsmanagement-Dienste angegriffen werden mit dem Ziel, sich gegenüber dem Web-Service wirksam als ein berechtigter Service-Consumer auszuweisen. Bei fehlenden Mechanismen zur Diensteauthentisierung kann der Angreifer dabei auch entweder gegenüber dem Web-Service oder dem Service-Consumer einen eigenen Identitäts-Dienst einsetzen und so entweder dem Dienst eine falsche Identität vorgaukeln oder den legitimen Benutzer zur Preisgabe von Authentisierungsdaten bewegen.

# G 5.182 Manipulation von Routen (Routing Detours)

SOAP-Nachrichten können unter Verwendung des Standards WS-Routing oder WS-Addressing Informationen über die Route enthalten, die die Nachricht durchlaufen soll. Dadurch können zum Beispiel Kommunikationsflüsse abgebildet werden, ebenso aber auch Geschäftsprozesse, indem zum Beispiel eine Bestellnachricht nacheinander an verschiedene Dienste (Verfügbarkeitsprüfung, Bezahlung, Bestellung) weitergereicht wird. Bei Verwendung von WS-Routing enthält die Nachricht dabei bereits die gesamte Abfolge von Zieladressen, bei WS-Addressing nur den jeweils nächsten Empfänger.

Gelingt es einem Angreifer, mit einem Man-in-the-Middle-Angriff (siehe auch G 5.143 *Man-in-the-Middle-Angriff*) die SOAP-Nachrichten beim Versand oder auf dem Übertragungsweg zu manipulieren, so können dabei neben einer Veränderung der Nachrichteninhalte auch die eingebetteten Routing-Informationen verändert werden. Dadurch erhält der Angreifer Kontrolle über die weitere Verarbeitung der Nachricht. Mögliche Angriffe auf diesem Weg sind:

- Der Angreifer kann die Route der SOAP-Nachricht um zusätzliche Systeme erweitern, die unter seiner eigenen Kontrolle sind. Beim Einsatz von WS-Routing ist es dabei gegebenenfalls sogar möglich, die Nachricht nach der Verarbeitung durch einen der vorgesehenen Services zurück an den Angreifer zu spielen. So könnte er zum Beispiel eine Preisangabe verringern, die Nachricht an den Bezahldienst leiten und von dort wieder an ein eigenes System, das die Manipulation rückgängig macht, bevor die Nachricht weiter an die nachgelagerten Services übergeben wird.
- Der Angreifer kann die Übermittlung der SOAP-Nachricht an vorgesehene Services unterbinden. So kann zum Beispiel der Bezahlvorgang oder ein zwischengeschobener Prüfschritt ausgelassen werden, indem die Nachricht direkt an den nächsten vorgesehenen Service übermittelt wird.
- Der Angreifer kann die Reihenfolge oder Abfolge der Services ändern, an die die Nachricht übermittelt wird. Je nach der Logik der Anwendungsarchitektur kann das Effekte haben, die vom Angreifer zu seinen Gunsten ausgenutzt werden.
- Der Angreifer kann ungültige Adressen in die Route einbringen und damit Nachrichten unterdrücken oder Fehlerzustände hervorrufen (Denial of Service).

# G 5.183 Angriffe auf XML

Web-Services verwenden häufig XML als Grundlage für ihr Nachrichtenformat. Das hat zur Folge, dass alle eingehenden Nachrichten zunächst an einen XML-Parser übergeben werden, der die XML-Strukturen auswertet und die enthaltenen Daten zur Verarbeitung durch den Web-Service extrahiert.

Der XML-Parser wird dabei sinnvollerweise nicht für jeden Web-Service neu entwickelt, sondern als fertige Drittkomponente eingebunden. Solche XML-Parser bieten dabei einen Funktionsumfang, der häufig über die vom Web-Service tatsächlich benötigten Parserfunktionen hinausgeht. Damit erhöht sich jedoch auch die Angriffsfläche des Web-Service. Immer wieder finden sich in den eingesetzten XML-Parsern auch Schwachstellen, die ein Angreifer durch die entsprechende Gestaltung von XML-Eingaben ausnutzen kann. Gerade Schwachstellen durch ungenutzte Parserfunktionen werden dabei oft übersehen oder in ihrer Bedeutung unterschätzt.

Da XML-Dokumente sehr komplex sein können, kann auch der Ressourcenverbrauch für das XML-Parsen entsprechend ansteigen. Dies können Angreifer ausnutzen, indem sie XML-Strukturen so gestalten (Verschachtelung, Rekursion, externe Verweise), dass sie den Ressourcenverbrauch des Parsers gezielt erhöhen und das verarbeitende System damit an seine Lastgrenzen bringen.

Es sind verschiedene Angriffsarten bekannt, die auf der Gestaltung spezieller XML-Nachrichten zur Erreichung des Angriffsziels basieren:

**Coercive Parsing**

Beim Coercive Parsing überlastet der Angreifer den eingesetzten XML-Parser, indem er ihm als Eingabe eine sehr große oder unbegrenzte Anzahl von Startelementen (Opening Tags) für XML-Elemente schickt. Hat der Parser kein Abbruchkriterium für die Verarbeitung, so belegt er für jedes neu geöffnete Element neuen Speicher auf einer neuen Verschachtelungsebene, bis die vorhandenen Ressourcen erschöpft sind.

**XML Entity Expansion (XML Bomb)**

Bei dieser Attacke werden durch starke Verschachtelung oder Rekursion von Entity-Definitionen mit sehr kurzen XML-Dokumenten sehr umfangreiche Datenstrukturen beschrieben. XML-Parser, die diese Art von Attacke nicht erkennen und über ein sinnvolles Abbruchkriterium verhindern, konstruieren bei der Auswertung des XML-Dokuments die beschriebene Datenstruktur im Speicher. Der Angreifer kann dadurch mit sehr geringem Aufwand die vorhandenen Systemressourcen vollständig blockieren. Varianten dieses Angriffs nutzen externe Verweise und belegen so zusätzliche Ressourcen für deren Auflösung.

**XML Document Size**

Der Angreifer sendet ein überlanges Dokument an den Web-Service, um den XML-Parser zur Ausschöpfung der vorhandenen Systemressourcen zu bringen.

**Oversized XML**

Bei dieser Angriffsvariante nutzt der Angreifer den Umstand, dass der Standard keine Längenbeschränkungen für XML-Bestandteile wie Elementnamen,

Attributnamen oder Namensräume vorsieht, und versucht, durch Überlängen in diesen Bestandteilen den XML-Parser zum Absturz zu bringen.

**XML Document Width/XML Document Depth**

Auch dieser Angriff zielt auf die Belegung von Systemressourcen durch den Parser, hier allerdings durch eine übergroße Anzahl von Attributen (Width) oder Verschachtelungsstufen (Depth) und dadurch die Belegung übergroßer Speichermengen.

**XML Wellformedness**

Auch über bewusst in die XML-Struktur eingebrachte Fehler lassen sich XML-Parser angreifen. Dies können zum Beispiel überlappende oder nicht geschlossene XML-Elemente sein. Je nach Implementierung können dadurch Fehlerzustände im Parser hervorgerufen werden, die gegebenenfalls nicht geeignet behandelt werden.

**XML Schema Poisoning**

XML-Schemata werden verwendet, um die Konformität von XML-Daten zu den erwarteten Strukturen zu überprüfen. Gelingt es dem Angreifer, extern referenzierte Schemata zu manipulieren oder durch eigene zu ersetzen, so kann er damit unter Umständen Prüfungen der übergebenen Daten durch den Web-Service aushebeln und so schadhafte Bestandteile einbetten.

**XML External Entities/XML External References**

XMLDokumente können Verweise auf externe Dokumente oder Entitäten enthalten, die bei der Verarbeitung des XML-Dokuments durch den Parser automatisch aufgelöst werden, indem der Parser die externe Ressource nachlädt und auswertet. Dadurch kann der Angreifer erreichen, dass das Parsersystem Verbindungen zu den angegebenen URLs initiiert. Neben Denial-Of-Service-Angriffen durch das Nachladen von übergroßen oder nicht erreichbaren Dokumenten kann der Angreifer das auch ausnutzen, um zum Beispiel Sicherheitsgateways auszuhebeln, in dem das Parsersystem Verbindungen aus seiner eigenen Netzumgebung heraus initiiert. So können zum Beispiel andere Web-Services in einer DMZ, die von außen nicht direkt aufrufbar sind, auf diesem Wege angesprochen werden.

Gelingt es dem Angreifer, die Inhalte extern abgelegter Ressourcen zu ändern, kann er damit mittelbar auch den Web-Service angreifen, wenn dieser im Rahmen eines legitimen Aufrufs durch einen anderen Nutzer die manipulierten Ressourcen inklusive der schadhaften Inhalte des Angreifers nachlädt.

**XML Signature Wrapping**

XML-Signaturen sichern die Integrität und/oder Authentizität von XML-Dokumenten, indem sie kryptographische Prüfsummen über Elemente bilden, die durch eine entsprechende Referenz in der Signatur bezeichnet sind. Die Signatur sichert dabei nur das referenzierte Element, unabhängig von seiner Einbindung in den XML-Kontext. Ein Angreifer kann daher durch eine Veränderung der XML-Dokumentstruktur dafür sorgen, dass das durch die Signatur gesicherte Element zwar in sich unverändert erhalten bleibt, aber vom Parser nicht oder nicht in der beabsichtigten Form ausgewertet wird, weil zum Beispiel weitere, gleichartige Elemente mit manipuliertem Inhalt auf höherer Ebene in die XML-Struktur eingebracht werden. Die Signaturprüfung führt dann

weiter zu einem positiven Ergebnis, obwohl der Web-Service manipulierte Inhalte verarbeitet.

Die hier aufgeführten Angriffsarten sind nur Beispiele, zahlreiche weitere Angriffe sind bekannt oder werden neu entwickelt, basieren aber auf denselben oder sehr ähnlichen Angriffsprinzipien.

# G 5.184 Informationsgewinnung über Web-Services

Damit in einer Service-orientierten Architektur (SOA) Web-Services zur Erfüllung übergreifender Aufgaben dynamisch kombiniert werden können (Orchestrierung), stellen die einzelnen Web-Services Informationen über sich und ihre Schnittstellen in standardisierter Form als WSDL-Dokumente bereit (Web Service Description Language). Die Consumer können dadurch in standardisierter, maschinenlesbarer Form alle nötigen Informationen zum Aufruf des Dienstes abrufen. Die WSDL-Dokumente werden in einer SOA über ein zentrales Verzeichnis (engl. *Repository*) bereitgestellt.

Die aus diesen Schnittstellenbeschreibungen ersichtlichen Informationen können jedoch auch für Angreifer wertvolle Hinweise enthalten und damit Angriffe auf die Dienste vorbereiten oder erleichtern. Da WSDL-Dateien oft automatisiert aus den verwendeten Entwicklerframeworks generiert werden, enthalten sie häufig mehr Angaben, als für den Einsatz tatsächlich benötigt werden.

Angreifer, die sich gegen Web-Services richten, beginnen häufig mit einer Erkundungsphase, in der der Angreifer versucht, WSDL-Dateien zu den angebotenen Services abzurufen und auszuwerten, zum Beispiel mit Hilfe einer Suchmaschine (*WSDL Google Hacking*).

Zu den Informationen, die für einen Angreifer von Interesse sein können, gehören:

- Namen von aufrufbaren Methoden und zugehörige Parameter. Gerade bei automatisch generierten WSDL-Dokumenten sind hier oft auch Methoden enthalten, die für einen Aufruf von außen gar nicht vorgesehen sind. Angreifer können durch den direkten Aufruf solcher Methoden versuchen, Sicherheitsfunktionen wie Berechtigungsprüfungen zu umgehen.
- Informationen über verwendete Namensschemata. So können Angreifer aus den Namen von veröffentlichten Methoden versuchen, die Namen weiterer, nicht veröffentlichter Methoden zu erraten und diese direkt aufzurufen. Das Ausprobieren nicht veröffentlichter, aber aus veröffentlichten Namen abgeleiteter Methoden wird auch *WSDL Scanning* oder *WSDL Enumeration* genannt.

Mit den Informationen über die erreichbaren (veröffentlichten oder abgeleiteten) Methoden und Aufrufparameter kann der Angreifer versuchen, nicht für ihn bestimmte Funktionen direkt aufzurufen. Weiter kann er aber auch, durch die Veränderung von Aufrufparametern, Fehlerzustände provozieren, um zum Beispiel aus den Fehlermeldungen weitere Rückschlüsse auf die technische Realisierung zu ziehen (zum Beispiel zu Datenbanktabellen und Feldnamen, verwendeten Bibliotheken und Frameworks). Aus den Fehlermeldungen lässt sich unter Umständen auch schließen, wie der Service die übermittelten Parameter prüft. Auf Grundlage der Erkenntnisse können dann weitere Angriffe (zum Beispiel Injection-Angriffe) gestartet werden.

Eine weitere Angriffsvariante besteht darin, die URL zum Aufruf eines Web-Service zu manipulieren, um dadurch andere, nicht zum Aufruf von außen bestimmte Services zu finden und auszunutzen (zum Beispiel durch Wechsel des Server-Verzeichnisses mit *Directory Traversal*). Solche Angriffe drohen insbesondere bei REST-Schnittstellen durch die semantische Bedeutung der URL für den Diensteaufruf.

# G 5.185 Erlangung physischen Zugangs auf SAN-Switches

Existieren in einer Institution unzureichende Zugangskontrollen zu den Komponenten einer Speicherlösung oder fehlen diese gänzlich, ist es einem Angreifer möglich, sich physischen Zugang zu vorhandenen Switches zu verschaffen bzw. zusätzliche FC-SAN-Switches an das Netz anzuschließen.

Hinter einem solchen Angriff verbergen sich möglicherweise folgende Absichten, die eine Gefährdung für die Institution darstellen:

- Ziel eines Zugangs könnte es sein, dem Angreifer zu gestatten, auf die verteilte Zoning-Datenbank zuzugreifen, um diese so zu verändern, dass er auf die Speichersysteme zugreifen kann.
- Zusätzliche FC-SAN-Switches werden in den Datenstrom eingeschliffen, um Daten mitzuschneiden, beispielsweise indem das FC-Routing verändert wird.
- Die Name Server Database wird dahingehend verändert, dass sich ein Angreifer als Zielsystem darstellt und damit die Daten der Initiatoren abfangen kann.
- WWN-Spoofing als Basis für die Durchführung weiterer Angriffe (siehe z. B. G 5.186 *Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing*)

Der physische Zugang zu Komponenten der Speicherlösung kann darüber hinaus auch mit der Absicht erfolgen, einen Denial-of-Service-Angriff (DoS) durchzuführen. Dem Angreifer stehen hierzu unterschiedliche Varianten der Manipulation zur Verfügung:

- Ausschalten einzelner Komponenten
- Umstecken oder Entfernen gesteckter Kabel
- Verletzen der Biegeradien von Kabeln, um den Datentransfer zu stören oder die Datenübertragung komplett zu verhindern
- Senden von Reconfigure-Fabric-Nachrichten (RCF), um den normalen Datenverkehr zu stören

# G 5.186 Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing

Mittels Programmen, die durch den Hersteller des Host Bus Adapters (HBA) zur Verfügung gestellt werden, kann der World Wide Name (WWN) eines HBAs geändert werden. Der Angreifer kann somit auf Daten zugreifen, für deren Einsicht er keine Berechtigung besitzt. Die Kenntnis der WWN der zu spoofenden HBA erleichtert einen solchen Angriff, jedoch besteht für Angreifer auch die Möglichkeit, diese auf andere Weise zu ermitteln. Einen einfach zu ermittelnden Teil der WWN stellt der Object Identifier (OID) des jeweiligen Herstellers dar. Sofern die HBAs aus einer Produktionscharge stammen, liegen die WWNs mit großer Wahrscheinlichkeit dicht zusammen. Mittels Brute-Force-Attake kann daher die WWN komplettiert werden.

Die Manipulation von WWNs, auch als WWN-Spoofing bezeichnet, birgt für eine Institution erhebliches Gefahrenpotenzial. Insbesondere im Zusammenhang mit mandantenfähigen Speicherlösungen können unberechtigte Zugriffe auf Informationen anderer Mandanten die Folge solcher Angriffe sein.

Mögliche Ausprägungen von Angriffen durch WWN-Spoofing sind:

- Ein fehlendes oder unzureichendes Rechte- und Rollenkonzept ermöglicht den administrativen Zugriff auf Werkzeuge zur Manipulation der WWN auf dem HBA.
- Bei Einsatz von WWN-Zoning ermöglicht WWN-Spoofing unberechtigten Zugriff auf Netzressourcen.
- Bei Einsatz von Port-Zoning ermöglicht ein physischer Zugang zum Switch den Anschluss von Komponenten an entsprechende Ports. Durch diesen Angriff können alle Informationen in der betroffenen WWN durch den Angreifer manipuliert werden.
- Die Manipulation des LUN-Maskings mittels WWN-Spoofing führt dazu, dass Systeme auf Speicherressourcen zugreifen können, für die sie ursprünglich nicht berechtigt waren.

# G 5.187 Überwindung der logischen Netzseparierung

Erfolgt die Trennung von Netzstrukturen unterschiedlicher Mandanten nicht durch den Aufbau physisch getrennter Netze, sondern kommen hierfür virtuelle Storage Area Networks (VSANs) oder Local Area Networks (VLANs) zum Einsatz, kann dies unter Umständen zu einer Gefährdung für die Informationssicherheit der Institution führen.

Gelingt es einem Angreifer, beispielsweise durch Ausnutzen von Schwachstellen, in das Netz eines anderen Mandanten einzudringen, kann er auf diesem Weg sowohl administrativen Zugriff auf das SAN oder LAN dieses Mandanten erlangen als auch auf die übertragenen Nutzdaten. Fehlende oder unzureichende Rechte-, Rollen- sowie Zonenkonzepte erhöhen dabei das Schadenspotenzial solcher Angriffe.

Grundsätzlich ist die Überwindung der Separierung über mehrere Wege möglich (siehe hierzu auch G 5.115 *Überwindung der Grenzen zwischen VLANs*):

- Der Angreifer erlangt physischen Zugriff auf einen Switch und kann diesen manipulieren.
- Der Angreifer nutzt eine vorhandene Fehlkonfiguration aus. Hierbei kann zum einen die Mandantenfähigkeit falsch konfiguriert worden sein, sodass der Angreifer Zugriff auf andere Mandanten erhält. Zum anderen kann die eigentliche Zuordnung eines Anwenders zu einem virtuellen SAN oder LAN falsch vorgenommen worden sein. Der Angreifer erhält daraufhin Zugriff auf Daten innerhalb eines virtuellen Netzes, für die er ursprünglich keine Berechtigung besitzt.
- Der Angreifer nutzt eine ungepatchte Software-Schwachstelle aus.

N-Port ID Virtualization (NPIV) wird in virtuellen Storage Area Networks (VSAN) eingesetzt, bei denen der physische SAN-Server über eine unzureichende Anzahl an Fibre-Channel-Ports verfügt. NPIV erlaubt einem physischen Host Bus Adapter Port, mit mehreren World Wide Port Name (WWPN) verknüpft zu werden. Der Einsatz von NPIV in Fibre-Channel-Netzen kann dazu führen, dass ein Server sich durch Nutzung des gleichen WWPN unberechtigt Zugriff auf Daten eines anderen Servers verschaffen kann.

# G 5.188 Unberechtigter Zugriff auf Daten innerhalb einer Cloud-Storage-Lösung

Innerhalb einer Cloud-Storage-Lösung besteht die Gefahr unberechtigter Zugriffe auf Daten anderer Mandanten durch ein fehlendes oder unzureichendes Rechte- und Rollenkonzept sowie Zonenkonzept.

Wird bei Auswahl und Konfiguration der Komponenten einer Cloud-Storage-Lösung nicht ausreichend auf die Möglichkeiten der Mandantenfähigkeit des Speichersystems und der Netzkomponenten des Storage Area Networks (SAN) und Local Area Networks (LAN) geachtet, ermöglicht dies ebenfalls den unberechtigten Zugriff bzw. die Manipulation von Daten.

# G 5.189 Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden

Storagebasierte Replikationsmethoden haben ursprünglich den Zweck, gespeicherte oder archivierte Daten in Echtzeit über ein Speichernetz zu duplizieren und damit zusätzliche Redundanzen zu erzeugen. Hierdurch wird dem Verlust von Daten vorgebeugt.

Die automatisierte Replikation unverschlüsselter Daten birgt allerdings sowohl im eigenen Campus-Netz als auch bei der Nutzung öffentlicher Netzanbieter Risiken. Sowohl bei der IP-Replikation als auch bei der FC-Replikation könnten Angreifer möglicherweise Schwachstellen der storagebasierten Replikation ausnutzen, um unberechtigt auf die Daten zuzugreifen.

Zu unterscheiden sind grundsätzlich folgende Angriffsszenarien:

- Der unberechtigte Zugriff erfolgt auf legitimen Replikationsverkehr, beispielsweise mittels Einsatz von FC-Analysern (FC-Replikation) oder Sniffern (IP-Replikation). Siehe dazu auch G 5.7 *Abhören von Leitungen*.
- Ein Angreifer initiiert eine nicht autorisierte Replikation mit einem durch ihn kontrollierten System als Ziel.
- Ein Angreifer verschafft sich Zugriff auf eine vorhandene Replikation, wenn diese nicht oder nur unzureichend geschützt ist.

# G 5.190 Missbrauch von Services

Cloud Services, die von einer Institution beauftragt werden, können unter Umständen von Angreifern missbräuchlich verwendet werden. Ein solcher Missbrauch wird dabei zunächst in der Regel auf den ursprünglichen Auftraggeber zurückgeführt. Dies kann zu finanziellen Schäden und zu Reputationsverlusten für den Cloud-Anwender führen.

Werden Services durch Dritte missbräuchlich verwendet, erfolgt dies meist mit dem Ziel, eine oder mehrere der folgenden illegalen Aktivitäten durchzuführen:

- Versand von Spam-Nachrichten
- Betreiben von Bot-Netzen
- Verschleierung der Herkunft bei weiteren illegalen Aktivitäten
- Hosting von Schadsoftware
- Kostenlose Nutzung des Services für eigene Zwecke

Grundsätzlich kann der Missbrauch von Cloud Services durch Dritte über mehrere Wege erfolgen. Ein Angreifer kann sich beispielsweise über die eingesetzten Schnittstellen Zugriff auf den Service verschaffen (siehe hierzu G 5.89 *Hijacking von Netz-Verbindungen*). Schwachstellen in Web-Schnittstellen beziehungsweise Protokollen, die von den angebundenen Clients genutzt werden, stellen ebenfalls ein Risiko dar. Weiterhin ist das Ausnutzen von Schwachstellen in der technischen Realisierung des Cloud Services denkbar. Wird beispielsweise keine oder lediglich eine unzureichende Validierung von Benutzern (zum Beispiel mittels Verifizierung der angegebenen E-Mail-Adresse) vorgenommen, ermöglicht dies die Kompromittierung des Cloud Services durch Hacker beziehungsweise Spammer oder das Hosting von Schadsoftware.

# G 5.191 Manipulation der Abrechnungsinformationen

Bei der Nutzung von Cloud Services erfolgt in der Regel eine verbrauchsorientierte Abrechnung der in Anspruch genommenen Leistungen durch den Cloud-Diensteanbieter.

Die beauftragende Institution sollte nach der Erstellung dieser Abrechnungsinformationen eine Prüfung hinsichtlich deren Nachvollziehbarkeit und Korrektheit durchführen.

In der Praxis ist der Nachweis der tatsächlich in Anspruch genommenen Leistungen durch den Anwender jedoch nur schwer zu erbringen. Auswirkungen auf die Leistungserbringung, die sich durch Service-Ausfälle oder durch die Nichteinhaltung vereinbarter Service Level Agreements ergeben, sind für den Anwender unter Umständen nicht transparent.

Der Cloud-Diensteanbieter könnte diese Gegebenheiten zu seinen Gunsten ausnutzen und die Abrechnungsinformationen der beauftragenden Institution manipulieren. In der Folge ist die Integrität der Abrechnung nicht mehr gegeben. Dem Anwender werden Services in Rechnung gestellt, die tatsächlich nicht erbracht wurden.

# G 5.192 Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender

Derzeit kann mit relativ geringem Aufwand einem Angerufenen eine falsche Telefonnummer des Anrufers (Caller-ID-Spoofing) bzw. des SMS-Absenders (SMS-ID-Spoofing) vorgetäuscht werden. Angreifer können so einem Mitarbeiter auf Dienstreise einen Anruf aus der eigenen Institution oder eines Kunden vortäuschen, um an vertrauliche Informationen zu gelangen. Auch einer Kurzmitteilung eines bekannten Absenders wird eher vertraut und ein eventueller Anhang mit Schadsoftware leichtfertiger geöffnet.

**Beispiele:**

- Für das iPhone gibt es seit einiger Zeit eine SpoofApp, mit der Anrufer die Rufnummer, die den Angerufenen angezeigt wird, frei wählen können. So erhält der Mitarbeiter auf Dienstreise beispielsweise einen Anruf vom vermeintlichen Prokuristen seiner Firma, der schnell die Höhe eines gerade abgegebenen Angebots wissen möchte. Er gibt die Zahlen heraus und der Angreifer verkauft die Informationen an einen Konkurrenten, der den Preis unterbietet.
- Beim SMS-Spoofing ist es möglich, statt der Rufnummer einen Namen beim Empfänger anzeigen zu lassen. So kann ein Angreifer beispielsweise verhindern, dass der Chef eines großen Unternehmens zu einer wichtigen Besprechung reist. Dafür muss er nur eine SMS von der Fluggesellschaft des Chefs vortäuschen, dass der Flug gestrichen sei.

# G 5.193 Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs

Smartphones, Tablets und PDAs besitzen meistens nur ein aktives Benutzerkonto mit eingeschränkten Rechten. Das Administrator-Konto ist in der Regel abgeschaltet. Das heißt, Benutzer können zwar neue Anwendungen installieren oder deinstallieren, jedoch keine tiefen Veränderungen am Betriebssystem selbst vornehmen. Solche administrativen Rechte sind nur durch Manipulationen am Betriebssystem zugänglich ("rooten" oder "jailbreaking").

Anders als bei PCs ist es daher nicht möglich, Programme zur Abwehr von Schadprogrammen mit so hohen Rechten auszustatten, dass sie von diesen nicht manipuliert werden können. So gibt es Schadsoftware, die Schwachstellen im Betriebssystem ausnutzt, um sich administrative Rechte auf dem Endgerät zu verschaffen. Damit verfügt sie dann über höhere Rechte als jedes Schutzprogramm. Solche Schadprogramme sind sehr schwer zu entdecken und können mit normalen Mitteln nicht mehr vom Endgerät entfernt werden.

Eine weitere Hürde für Schutzprogramme ist, dass der Zugriff von einer Anwendung auf eine andere Anwendung in der Regel eingeschränkt und auf manchen Plattformen sogar komplett ausgeschlossen ist. Das erschwert die Arbeit von Schutzprogrammen oder macht sie sogar unmöglich.

Zudem arbeiten Schutzprogramme meistens nur mit Virensignaturen, um Schadsoftware zu erkennen. Weitere Methoden, wie heuristische Analysen der Daten oder eine Verhaltensanalyse, sind in der Regel aufgrund der begrenzten Akku-Kapazität nicht verfügbar. Verfahren, die dieses Problem durch eine externe Datenverkehrsanalyse lösen wollen, werfen jedoch datenschutzrechtliche Fragen und zusätzliche Sicherheitsrisiken auf, da hier der gesamte Datenstrom auf das Gerät mit heuristischer Suche analysiert wird. Dafür müssen verschlüsselte Verbindungen entweder aufgebrochen werden oder können nicht analysiert werden.

# G 5.194 Einschleusen von GSM-Codes in Endgeräte mit Telefonfunktion

GSM-Codes (oder auch USSD- oder MMI-Codes) bestehen aus Zahlenkombinationen, die mit Stern, Raute oder beidem beginnen bzw. enden. Sie veranlassen das Endgerät dazu, bestimmte Funktionen auszuführen. Ein bekannter GSM-Code ist **#06#*, der bei allen Endgeräten mit Telefonfunktion dazu führt, dass die international eindeutige Geräteidentifikationsnummer (IMEI-Nummer) im Display angezeigt wird. Im Weiterem können mit GSM-Codes auch die PIN und die PUK geändert werden.

Neben den GSM-Codes gibt es noch herstellerspezifische Codes, die beispielsweise das Gerät in den Werkszustand versetzen oder Servicemenus aufrufen. Eine weitere Klasse von Codes ist abhängig vom Netzbetreiber- bzw. Mobilfunkanbieter z. B. um das Guthabenkonto abzufragen.

Eine Gefährdung für die Informationssicherheit entsteht dadurch, dass diese GSM-Codes nicht nur durch direkte Eingabe am Gerät, sondern auch über andere Schnittstellen an die Endgeräte übergeben werden können. So können entsprechend konfigurierte Internetseiten GSM-Codes über den Browser an das Endgerät übermitteln. Auch QR-Codes (siehe G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*) können GSM-Codes enthalten und nach dem Einscannen an das Endgerät weitergeben. Zudem ist es möglich, über die "Near-Field-Communication"-Schnittstelle (NFC-Schnittstelle) solche Codes einzuschleusen. Dadurch ist es Angreifern möglich, zum Beispiel Schadsoftware zur Datenspionage auf dem Gerät zu installieren oder die SIM-Karte zu sperren.

**Beispiele:**

- Auf einer von Angreifern präparierten Internetseite ist der GSM-Code für dreimaliges Ändern der PIN und anschließendes zehnmaliges Ändern der PUK enthalten. Ein Mitarbeiter besucht mit seinem Smartphone die Internetseite und der GSM-Code wird an sein Gerät übermittelt. Danach ist die SIM-Karte so gesperrt, dass es für den Benutzer nicht mehr möglich ist, diese ohne Hilfe der IT-Abteilung zu entsperren.
- Angreifer haben den QR-Code auf einem Werbeplakat mit einem anderen QR-Code überklebt. Dieser enthält nun, statt eines Links zu einer Internetseite mit weiteren Informationen, den GSM-Code für einen Firmware-Reset. . Ein solcher Vorfall gefährdet nicht nur die Informationssicherheit, sondern schädigt auch die öffentliche Reputation der jeweiligen Institution, von der das Poster stammt.

# G 5.195 Ausnutzen von Schwachstellen in Backend-Anwendungen

Allgemein kann ein XML-Transportcontainer verwendet werden, um entfernte Prozeduraufrufe an Backend-Anwendungen zu übermitteln, so dass deren Funktionen nutzbar sind. Indem die Systeme für die entfernte Nutzung geöffnet werden, können jedoch erhebliche Sicherheitsrisiken entstehen, die es im schlimmsten Fall ermöglichen, das gesamte IT-System zu übernehmen. Insbesondere Legacy-Systeme enthalten oftmals schwerwiegende Sicherheitslücken, die Angreifer leicht ausnutzen können. Beispielsweise sind diese Systeme anfällig für Buffer-Overflow-Attacken.

# G 5.196 Unterbinden einer Informations- und Dienstesynchronisation in einer verteilten SOA-Umgebung

In einer verteilten SOA-Umgebung, zum Beispiel in einem mobilen Umfeld, sind die einzelnen Service-Provider mehrfach redundant ausgelegt, um deren Verfügbarkeit zu erhöhen. Für die Konsistenz von Diensten und Informationen ist es erforderlich, dass die Service-Provider sich untereinander periodisch oder eventbezogen synchronisieren.

Ein Angreifer, der Kenntnisse über die Informationsstruktur besitzt, kann durch einen gezielten Angriff auf kritische Kommunikationsverbindungen be- oder verhindern, dass sich die Service-Provider zeitgerecht synchronisieren.

# G 5.197 Missbrauch von SAML-Token in SOA-Umgebungen

Beim Zugriff eines Clients aus einer Informationsdomäne A auf einen Service-Provider in einer Informationsdomäne B muss zum einen geprüft werden, ob der jeweilige Client berechtigt ist, auf diese entfernte Ressource zuzugreifen. Zum anderen muss der angesprochene Provider unabhängig davon prüfen, ob dieser Fernzugang akzeptiert werden kann.

Ist die Berechtigung einmal festgestellt, wird in der Kommunikation ein Security-Assertion-Markup-Language-(SAML)-Token verwendet, das den Zugang ermöglicht. Ein SAML-Token kann hierbei sowohl vom Security-Token-Service (STS) der Domäne A als auch der Domäne B ausgestellt werden.

Zwei Modelle der SAML-Token-Vergabe stehen sich hier gegenüber:

- **Föderiertes Modell:** Der Client der Domäne A beantragt bei seinem lokalen STS-Provider ein SAML-Token zum definierten Service-Provider der Domäne B. Der STS-Provider der Domäne A hat das erforderliche Wissen über den Provider der Domäne B und kann daher ein SAML-Token für beide ausstellen.
- **Enterprise-Modell:** Hier hat nur der STS-Provider der Domäne B auch das notwendige Wissen über den nachgefragten Service-Provider der Domäne B. In diesem Fall kontaktiert der STS-Provider der Domäne A den STS-Provider der Domäne B und handelt mit diesem das SAML-Token aus, das dann der jeweilige STS-Provider an seinen Client (oder Provider) übermittelt.

Im ersten Fall vertrauen alle Instanzen dem STS-Provider der aufrufenden Domäne, im zweiten Fall vertrauen die Instanzen einer Domäne nur jeweils ihrem lokalen STS-Provider. Zwischen den STS-Providern wird dann parallel verhandelt.

Die Gefahr besteht generell darin, dass ein Vertrauensverhältnis über Domänengrenzen hinweg aufgebaut wird bzw. bestehen muss. Eingriffsmöglichkeiten im Aufbau dieses Vertrauensverhältnisses führen dazu, dass SAML-Token womöglich unberechtigt ausgestellt werden, ohne dass die beteiligten Kommunikationsinstanzen hierüber Kenntnis erhalten.

# G 5.198 Missbrauch der WS-Notification-Broker in einer SOA

Ein *NotificationBroker* erhält eine *Subscription* für einen *NotificationConsumer*, wobei diese durch einen Stellvertreter initiiert wurde. Damit besteht die Gefahr eines Denial-of-Service-(DoS)-Angriffs auf eine bekannte Adresse, indem der Broker viele Nachrichten (*Notifications*) an die vorgegebene Adresse verschickt.

Jeder kann eine Operation auf einem Interface auslösen, sofern mit einer gültigen Richtlinie gearbeitet wird (siehe G 5.183 *Angriffe auf XML*). In einer Subscription wird die Zieladresse für den Consumer spezifiziert. Sofern der Subscriber auch der Empfänger einer Nachricht ist, wird eine Peer-to-Peer-Beziehung etabliert.

Für den Zugriff auf Informationen unterstützen die WS-Notification-Standards das Publish/Subscribe-Verfahren.

Wird ein *NotificationBroker* benutzt, kann der Fall auftreten, dass neben Brokern in der eigenen Informationsdomäne auch solche aus anderen Domänen verwendet werden.

Informationen, die ein Service-Provider an Broker in einer anderen Domäne weitergibt, unterliegen jedoch nicht mehr der administrativen Kontrolle der eigenen Domäne. Ohne Schutz der zu verteilenden Information besteht so die Gefahr, dass nicht-autorisierte *NotificationConsumer* unter einer fremden Richtlinie Zugang zu diesen Informationen erhalten.

*NotificationConsumer* können sich für spezifische Themen (*Topics*) anmelden. Verteilt der *NotificationBroker* Nachrichten (*Notifications*) mit diesen *Topics* an die Empfängergruppe, kann er die relevanten *NotificationConsumer* über ihre IP-Adresse zu einer Gruppe zusammenfassen und die zugehörigen Notifications an diese Gruppe übersenden (One-Way-Notification).

Werden verschiedene Consumer auf eine gemeinsame Gruppenadresse abgebildet, birgt dies Risiken, da es sich bei der Multicast-Adressierung im Internet um eine anonyme Gruppe handelt, deren Kontroll- und Replikationsmechanismen weder unter der Administration des Brokers noch der Consumer stehen.

Die Anmeldung an eine Gruppe und das Versenden von Notifications an eine Gruppe können durch eine Richtlinie unterstützt werden. Muss die Richtlinie bei einer Gruppenkommunikation durchgesetzt werden, erhöht sich jedoch das Risiko einer Peer-to-Peer-Kommunikation: Durch Zugang zu einem Multicast-Provider kann ein Angreifer sich in den Informationsfluss einhängen, ohne die erforderliche Authentisierung am Broker durchlaufen zu haben, zum Beispiel an einem "Sparse Mode Rendezvous Point (RP)" im Netz.

Meldet sich ein *NotificationConsumer* für ein bestimmtes *Topic* an, wird er mit der entsprechenden Information vom *NotificationBroker* per One-Way-Notification informiert, gemäß den lokal gültigen Richtlinien (Policies) für den Broker.

Beim Broker kann jedoch eine *Subscription* verloren gehen, z. B. wenn diese automatisch, technisch oder bewusst manuell gelöscht wird. Für den Consumer ist nicht erkennbar, ob er keine Publikation erhält, weil keine Nachrichten im Broker vorliegen oder weil keine Subscription mehr definiert ist. Es gibt der-

zeit kein Protokollmittel, mit dem der Status einer einmal eingerichteten Subscription überprüft werden kann.

Für den Schutz des Inhalts einer WS-Notification und die korrekte Klassifizierung ist der Verursacher (Erzeuger) verantwortlich. Da der mögliche Empfängerkreis dieser WS-Notification im Voraus nicht bekannt ist, kann kein Nutzerzertifikat der Empfänger verwendet werden.

Als Ersatz kann ein Attributzertifikat genutzt werden. Allerdings stellt sich hierbei das Problem, wie der private Schlüsselanteil an die berechtigten Empfänger verteilt werden kann. Diese Gefährdung wird noch komplexer, wenn die betreffende WS-Notification über mehr als eine Informationsdomäne verteilt wird. Insbesondere besteht die Gefährdung auch darin, dass der Besitz eines solchen privaten Schlüsselanteils noch nichts über die Berechtigung zu dessen Verwendung aussagt.

# G 5.199 Ungenügende Absicherung der SOAP-Kommunikation

Web-Services sind grundsätzlich zustandslos. Das "Web Services Resource Framework" (WSRF) beschreibt, wie zustandsbehaftete Ressourcen abgefragt, geändert und repräsentiert werden können. Die Ressourcen-Informationen werden selbst in einem Token abgebildet und damit transparent vom Provider an den Client geschickt.

Soll der Ressourcenzustand erfasst werden, findet dies jedoch zumeist außerhalb der gesicherten Umgebung statt, sodass hier die Information einen Übergang unterschiedlicher Klassifikationshöhe passieren muss. Dabei können Angreifer einen Parameterwert beim Übergang in eine höhere Klassifikationsstufe manipulieren, ohne dass dies erkannt wird.

Als eine Variante für die SOAP-Kommunikation lässt das World Wide Web Consortium (W3C) den verbindungslosen Betrieb zu. Statt SOAP mit HTTP/ TCP zu verwenden, kann nunmehr direkt SOAP mit UDP genutzt werden. Dieser Betriebsfall ist zustandslos, es wird nicht auf der Transportebene quittiert. Wird ein Sequenzzähler eingeführt, zum Beispiel bei SOAP/UDP mit WS-Policy, ändert sich an diesem zustandslosen Betrieb nichts. Hier wird lediglich die richtige Paketreihenfolge korrekt wiederhergestellt, aber keine Verbindungssteuerung durchgeführt. Dadurch besteht die Gefahr, dass Nachrichten an unberechtigte Empfänger weitergeleitet werden. Ohne Sequenzzähler besteht zusätzlich die Gefahr von Replay-Attacken.

Für die Verbindungssteuerung ist somit die Anwendung verantwortlich, die SOAP-Kommunikation nutzt. Solange die Verbindung nicht aktiv beendet wird, belegt sie hierfür Rechnerressourcen auf der Sende- und Empfangsseite.

# G 5.200 Manipulation von Richtlinien in einer SOA

WS-Policy ermöglicht es einem Service-Provider, die Richtlinien (Policies) bezüglich Sicherheit, Qualität und Version seines Services in Form von maschinenlesbaren XML-Daten für den Service-Consumer bereitzustellen. Auch ein Service-Consumer spezifiziert seine Anforderungen in Form von XML-Daten. Treffen die beiden Forderungen aufeinander, so kann nur zur Laufzeit eine effektive Richtlinie zwischen beiden Seiten ausgehandelt werden. Dafür werden sogenannte WS-Policy-Assertions benutzt, also eine Menge an Standardrichtlinien, die innerhalb einer Richtlinie anwendbar sind.

Wird in einer Informationsdomäne das Element einer WS-Policy genutzt, muss dies von allen Instanzen, wie z. B. Provider, Broker und Consumer berücksichtigt werden.

Es besteht die Gefahr, dass ein Angreifer die Richtlinien manipuliert und in Form eines Links, eines angehängten Inhalts oder einer ID mitschickt. Dadurch kann es zu einem ungewollten Zugriff auf Informationen oder Dienste kommen. Diese Fälle treten auf:

- wenn Informationen an unberechtigte Empfänger weitergeleitet werden, auch in fremden Informationsdomänen, und
- wenn Informationen an berechtigte Empfänger nicht weitergeleitet werden.

Weiterhin können Gefährdungen dadurch entstehen, dass Richtlinien nicht oder nur ungenügend harmonisiert sind. Findet ein Informationszugang mittels Subscription über einen NotificationBroker statt, treffen gegebenenfalls drei Richtlinien (Policies) aufeinander:

- Provider-Policy,
- Consumer-Policy,
- separate Broker-Policy.

In diesem Fall muss der Broker alle drei Richtlinien miteinander harmonisieren. Broker können jedoch in verschiedenen Informationsdomänen angesiedelt sein, die jeweils ihre eigenen Richtlinien verwenden. Sind diese nicht miteinander harmonisiert, besteht die Gefahr des unberechtigten Informationszugangs über die Domänen-Grenzen hinweg.

# G 5.201 Einspielen (Flashen) von manipulierten Software-Updates/-Upgrades bei eingebetteten Systemen

In der Vergangenheit war bei eingebetteten Systemen die Firmware in ROM (Read Only Memory) Bausteinen geschrieben und konnte nur durch deren Austausch geändert werden. Eine Vielzahl moderner eingebetteter Systeme hat seine Software in Flash-Speicher bzw. EEPROMs und bietet die Möglichkeit, die Firmware nach Anschluss an ein Programmiergerät, über eine Datenschnittstelle oder Remote über eine Netzverbindung zu aktualisieren.

Ein Angreifer kann versuchen, über diese Wege manipulierte Software-Updates oder -Upgrades einzuspielen. Für einen Angriff mittels eines für das eingebettete System vorgesehenen Programmiergerätes, z. B. einem Notebook mit entsprechender Software, kommen überwiegend Innentäter in Frage, da diese physisch auf das Gerät zugreifen können. Ein Angriff über ein Datennetz könnte grundsätzlich von beliebigen Personen erfolgen und würde durch fehlende oder schwache Authentisierung und Software-Integritätschecks vereinfacht werden. Hierzu muss es dem Angreifer zusätzlich gelingen, in das Datennetz zu gelangen, um darüber auf das eingebettete System zuzugreifen.

Gelingt das Einspielen manipulierter Software, kann die Funktionalität des Systems im Sinne eines Angreifers modifiziert werden. So können die ursprünglichen Aufgaben des Systems unterbrochen oder manipuliert werden.

# G 5.202 Seitenkanalangriffe auf eingebettete Systeme

Ein Angreifer könnte mittels eines Seitenkanalangriffs Kenntnis von Kryptovariablen erhalten und somit Verschlüsselungen oder Signaturen brechen. Er nutzt dazu beobachtbare Eigenschaften der physikalischen Implementierung eines Kryptosystems aus. Typische Angriffe sind:

- Simple Power Analysis und Differential Power Analysis (DPA): Aus dem Energieverbrauch eines Mikroprozessors während kryptologischer Berechnungen werden Rückschlüsse auf ausgeführte Operationen und auf Schlüssel gezogen.
- Rechenzeitangriffe: Der Schlüssel wird sukzessive durch Analyse der Laufzeitunterschiede bei verschiedenen Eingaben an kryptografische Verfahren hergeleitet.
- Mikroarchitekturelle Angriffe: Es wird der Umstand ausgenutzt, dass beim Ausführen kryptologischer Software Daten und Routinen schlüsselabhängig in den Cache bzw. Instruktionscache geladen werden.
- (Semi-)Invasive Angriffe: Bei der Ausführung von kryptologischen Algorithmen werden kurzzeitige Fehlfunktionen erzeugt. Das Verhalten des Systems bei unterschiedlichen Störungen wird verglichen und daraus auf den verwendeten Schlüssel geschlossen.

**Beispiele:**

- 2012 wurde ein Forschungspapier veröffentlicht, in dem beschrieben wird, wie mittels DPA und der Pipeline Emission Analysis (PEA) in einem Field-Programmable Gate Array Chip (FPGA-Chip) eine Hintertür entdeckt und ein geheimer Schlüssel extrahiert werden konnte. PEA ist eine Weiterentwicklung herkömmlicher Seitenkanalangriffe mit verbesserter Wellenformanalyse mit dem Ziel nutzbare Ergebnisse in kürzerer Zeit und auch bei verrauschten Signalen zu erhalten.
- 2011 konnten Wissenschaftler den geheimen Schlüssel eines TLS/SSL-Servers ermitteln, der den Digital Signature Algorithm (DSA) mit Elliptischer-Kurven-Kryptographie verwendet. Der Angriff beruhte auf der Tatsache, dass die benötigte Zeit für eine Multiplikation Rückschlüsse auf deren Operanden zulässt.
- 2008 konnten Forscher den geheimen Schlüssel einer in vielen Kraftfahrzeugen eingesetzten elektronischen Wegfahrsperre und Türöffnung rekonstruieren. Dazu führten sie sowohl beim Sender als auch beim Empfänger eine DPA und eine differentielle elektromagnetische Analyse (DEMA) während der Übertragung durch.

# G 5.203 Physikalischer Eingriff in ein eingebettetes System

Wenn Angreifer in den Besitz eines eingebetteten Systems gelangen, können sie mittels physikalischer Verfahren Daten lesen und manipulieren. Dieser Angriff erfordert das Chipgehäuse zu öffnen, um an das Substrat zu gelangen. Er kann nur durch Experten mit entsprechender Laborausstattung durchgeführt werden. Eine typische Vorgehensweise, mittels derer in der Vergangenheit bereits diverse Sicherheits-Chips geknackt worden sind, setzt an der Chipvorderseite an. Die Kontakte und Schaltkreise werden dazu schichtweise freigelegt. Danach dann wird der Schaltkreis mit Laserstrahlen oder feinen Drähten analysiert und manipuliert. Diese Vorgehensweise ist bei Sicherheitschips so nicht mehr möglich, da Hersteller inzwischen Metallisierungsebenen, sogenannte Meshes oder Shields einfügen um sicherzustellen, dass niemand von der Vorderseite auf den Schaltkreis zugreift.

Bei Chips, die noch unzureichend geschützt sind, kann ein Reverse-Engineering beginnend mit dem physischen Zugang erfolgen. Im ersten Schritt wird dazu der Halbleiter aus dem Gehäuse freigelegt, beispielsweise chemisch mittels Salpeter- oder Schwefelsäure (HNO3 oder H2SO4). Eine anschließende Reinigung kann mittels Aceton und Ultraschall erfolgen. Professionelle Angreifer könnten auch über eine Maschine verfügen, die den Halbleiter mittels eines HNO3-Dampfstrahls herauslöst. Dadurch würden die Abdeckschichten und gleichzeitig die Lösungsreste besser entfernt werden. Als nächstes werden die verschiedenen Ebenen des Chips freigelegt. Dazu können mechanische Verfahren wie Abschleifen und Polieren und chemische Verfahren wie Flourwasserstoffgas bzw. Flusssäure kombiniert werden. Die Chipebenen können dann Schicht für Schicht mit einem Mikroskop aufgenommen und begutachtet werden. Es gibt zahlreiche weitere Einstiegspunkte zum Reverse Engineering und viele Forschungsarbeiten sind noch im Gange. Ein Beispiel dafür ist der Einsatz eines Infrarotlasers, bei dem die Wellenlänge so gewählt wird, dass das Silizium dafür durchscheinend wird. Dadurch ist es möglich den individuellen Zustand eines Transistors festzustellen. Bei einem anderen Verfahren wird ein dünner Film aus Palladium oder Gold aufgebracht. Dieser Film bildet mit dem Siliziummaterial, aufgrund des Schottkyeffekts, je nach Dotierung des Untergrunds, eine Diode. Diese Dioden können mit einem weiterentwickelten Elektronenmikroskop erkannt und mit spezieller Software ausgewertet werden.

Von der Rückseite her einzudringen galt lange als nicht praktikabel. 2013 haben Forscher allerdings gezeigt, dass auch dies möglich ist indem die relativ dicke Schicht Silizium über den Transistoren kontrolliert abgetragen wird. Mit einer Ionenfeinstrahl-Anlage wird weiter ausgedünnt, soweit dass auf den Strukturen die einzelnen Transistoren erkennbar sind. Es können auch neue Verbindungen geschaffen oder vorhandene getrennt werden. Beispielsweise könnte ein im Chip vorhandener Einbruchssensor abgetrennt werden. Mit weiteren Messgeräten ist es möglich, Informationen die auf dem Schaltkreis übertragen werden mitzulesen, also grundsätzlich auch einen geheimen Schlüssel. Grundsätzlich ist auch das Einschleusen von Signalen möglich sowie ein Zugriff auf nicht sicher gelöschte Daten.

Ein weiteres Beispiel für einen Angriff, der einen Sicherheitsmechanismus aushebelt, richtet sich gegen das Sicherheitsbit, welches in einigen Mikrocontrollern verwendet wird. Wenn dieses gesetzt ist, verhindert es den externen elektrischen Zugriff zum Programmspeicher und soll erst durch die vollständige Löschung des Programmspeichers zurückgesetzt werden können. Bei Mikrocontrollern mit EPROM und genügend großem Abstand der Sicherheitsbit-

zelle vom Rest des Speichers kann es aber mittels UV-Licht zurückgesetzt werden, das auf die Sicherheitsbitzelle gerichtet wird.

Angreifer können versuchen mittels Extremwerten bei Eingabedaten abnorme Effekte zu produzieren. Durch Extremwerte an den Ober- und Untergrenzen des Wertebereichs von Variablen kann ein nicht sorgfältig programmiertes eingebettetes System zum Absturz gebracht oder es können Fehlfunktionen hervorgerufen werden. Werte in der Nähe von Null können zu einer Division durch Null und somit einem Fehlverhalten oder gar zum Absturz des Systems führen. Die Ursachen können z. B. in Rundungsfehlern, besonderen Prozessoreigenschaften oder der verwendeten Arithmetik liegen.

# G 5.204 Eindringen und Manipulation über die Kommunikationsschnittstelle von eingebetteten Systemen

Eingebettete Systeme sind oft hinsichtlich Codegröße, Zeitverhalten, Energieverbrauch, Kosten sowie Größe und Gewicht eingeschränkt. Sie sind daher oft nicht mit ausreichenden Sicherheitsfunktionen, wie z. B. starker Kryptographie, ausgestattet. Allerdings sind moderne eingebettete Systeme zunehmend mittels weit verbreiteten Technologien und Protokollen vernetzt und somit potenziell angreifbar.

Angreifer können versuchen, Daten oder Software auf einem eingebetteten System zu manipulieren, indem sie die standardmäßig vorgesehenen Kommunikationsschnittstellen und -protokolle für ihre Zwecke missbrauchen. Sind z. B. die IP-Kommunikation oder Ethernet-, WLAN-, Bluetooth- und Mobil- bzw. Digitalfunk-Schnittstellen nicht ausreichend gesichert, kann ein Angreifer Verbindungen übernehmen, Nachrichten fälschen oder in ein System eindringen und Folgeangriffe durchführen.

Moderne eingebettete Systeme werden oft über das Web fernadministriert. Dazu ist auf dem System ein minimalisierter eingebetteter Webserver vorhanden. Angreifer können Verwundbarkeiten eines solchen Webservers auszunutzen.

Weiterhin kann ein Angreifer auch versuchen, mittels anderer verfügbarer Kommunikationsschnittstellen, z. B. USB-Ports, in das System einzudringen.

# G 5.205 Einsatz gefälschter Komponenten

Im Produktionsprozess oder im Servicefall beim Austausch von Komponenten können gefälschte Komponenten eingebaut werden. Dies kann auch ohne Absicht geschehen, da für viele Bauteile Fälschungen im Umlauf sind. Das Ziel für die Massenanfertigung gefälschter Bauteile ist finanzieller Art und wird durch deren Verkauf erreicht. Die gefälschten Bauteile sind erheblich kostengünstiger in der Herstellung und das Ziel der Fälscher ist es, die Bauteile möglichst identisch zum Original herzustellen, daher sind oft keine dedizierten Schadfunktionen vorhanden.

Dennoch haben die Fälschungen oft nicht die exakte Funktionalität des Originals und sind vor allem wegen billigerer Produktionsmethoden weniger zuverlässig. Wenn derartige Fälschungen verbaut werden, kann das betroffene System ausfallen oder fehlerhaft funktionieren, was durch die Transformationswirkung des übergeordneten Systems Menschen, Umwelt und Anlagen enorm schädigen kann.

Angreifer können auch gezielt ein Gerät oder Bauteil entwickeln, das genauso aussieht wie das Original und dessen Funktion manipuliert ist, um einen bestimmten Zweck zu erreichen. Durch eine derartige Komponente könnten beispielsweise Hintertüren eingebaut, einzelne Funktion manipuliert oder die Verfügbarkeit angegriffen werden.

**Beispiel:**

Nach Forschungsberichten, unter anderem von der Ruhr Universität Bochum aus 2013, ist es auch möglich, kryptographische Verfahren durch manipulierte Hardware zu schwächen. Es könnten Störstellen im Halbleiter eingearbeitet werden, indem das Grundmaterial gezielt verunreinigt wird. Durch diese sogenannte Dotierung würde die elektrische Leitfähigkeit verändert. Dadurch könnte sich die Leistung eines Zufallsgenerators erheblich mindern. Dies würde dazu führen, dass der Zufallszahlengenerator schwache kryptographische Schlüssel erzeugt.

# G 5.206 Reverse Engineering

Beim Reverse Engineering (Re-Engineering) wird versucht, aus einem fertigen System durch Analyse der Strukturen, Zustände und Verhaltensweisen die Konstruktionselemente zu extrahieren. Dieses können Hardware- und Software-Elemente sein.

Der erste Schritt bei einem systematischen Hardware Reverse Engineering besteht darin, sich grundlegende Informationen zum Zielsystem, dessen Komponenten und internen Boards zu beschaffen. Daraufhin werden Funktionen, Zeitverhalten und Signalpfade analysiert. Anschließend wird mittels physikalischer Bearbeitung, wie beispielsweise in G 5.203 *Physikalischer Eingriff in ein eingebettetes System* beschrieben, der Aufbau des Bauteils analysiert. Mittels Rasterelektronenmikroskop, Transmissionselektronenmikroskop oder Rastersondenmikroskop und spezieller Chemikalien können Materialübergänge, Strukturgrößen, Schichtenanzahl und p/n-dotierte Zonen sichtbar gemacht werden. So kann nach und nach jede Schicht eines Chips erfasst werden und die Transistoren, Spulen, Widerstände, Kondensatoren und Leitungen können mittels spezieller Software strukturiert und dokumentiert und der Schaltplan verifiziert werden.

Zum Software Reverse Engineering muss ein Angreifer zunächst Zugriff auf den Maschinencode haben. Mit Hilfe eines Disassemblers kann er Maschinencode in Assemblercode rücküberführen und mit einem Decompiler diesen in einen verständlicheren Pseudocode transferieren.

# M 1 Maßnahmenkatalog Infrastruktur

| | |
|---|---|
| M 1.31 | Fernanzeige von Störungen |
| M 1.32 | Geeignete Aufstellung von Druckern und Kopierern |
| M 1.33 | Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz |
| M 1.34 | Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz |
| M 1.35 | Sammelaufbewahrung tragbarer IT-Systeme |
| M 1.36 | Sichere Aufbewahrung der Datenträger vor und nach Versand |
| M 1.37 | Geeignete Aufstellung eines Faxgerätes |
| M 1.38 | Geeignete Aufstellung eines Modems |
| M 1.39 | Verhinderung von Ausgleichsströmen auf Schirmungen |
| M 1.40 | Geeignete Aufstellung von Schutzschränken |
| M 1.41 | Schutz gegen elektromagnetische Einstrahlung |
| M 1.42 | Gesicherte Aufstellung von Novell Netware Servern **- entfallen** |
| M 1.43 | Gesicherte Aufstellung aktiver Netzkomponenten |
| M 1.44 | Geeignete Einrichtung eines häuslichen Arbeitsplatzes |
| M 1.45 | Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger |
| M 1.46 | Einsatz von Diebstahl-Sicherungen |
| M 1.47 | Eigener Brandabschnitt |
| M 1.48 | Brandmeldeanlage im Rechenzentrum |
| M 1.49 | Technische und organisatorische Vorgaben für das Rechenzentrum |
| M 1.50 | Rauchschutz |
| M 1.51 | Brandlastreduzierung |
| M 1.52 | Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur |
| M 1.53 | Videoüberwachung |
| M 1.54 | Brandfrühesterkennung / Löschtechnik |
| M 1.55 | Perimeterschutz |
| M 1.56 | Netzersatzanlage |
| M 1.57 | Aktuelle Infrastruktur- und Baupläne |
| M 1.58 | Technische und organisatorische Vorgaben für Serverräume |
| M 1.59 | Geeignete Aufstellung von Speicher- und Archivsystemen |

# M 1.1 Einhaltung einschlägiger Normen und Vorschriften

**Verantwortlich für Initiierung:** Planer, Leiter Beschaffung
**Verantwortlich für Umsetzung:** Bauleiter, Errichterfirma

Für nahezu alle Bereiche der Technik gibt es Richtlinien, Normen bzw. Vorschriften. Diese können von Standardisierungsorganisationen, Branchenvereinigungen, Anwendergruppen oder staatlichen Institutionen herausgegeben worden sein, z. B. DIN (Deutsches Institut für Normung), ISO (International Standards Organization), VDE (Verband der Elektrotechnik, Elektronik und Informationstechnik), VDMA (Verband Deutscher Maschinen- und Anlagenbau), VdS (Verband der Sachversicherer).

Diese Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für die Benutzer und Sicherheit für den Betrieb gewährleisten.

Bei der Planung und Errichtung von Gebäuden, bei deren Betrieb und Umbau sowie beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

Die Beachtung von Normen ist für sich keine Sicherheitsmaßnahme. Sie bedeutet, dass Mindestanforderungen erfüllt werden und der aktuelle Stand der Technik und des Wissens beachtet wird.

Prüffragen:

- Werden alle relevanten Normen und Vorschriften bei Planung, Errichtung und Umbau von Gebäuden sowie dem Einbau von technischen Einrichtungen berücksichtigt?

# M 1.2 Regelungen für Zutritt zu Verteilern

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Die Verteiler (z. B. für Energieversorgung, Datennetze, Telefonie) sind nach Möglichkeit in Räumen für technische Infrastruktur (siehe Baustein B 2.6 *Raum für technische Infrastruktur*) unterzubringen. Die dort geforderten Maßnahmen sind zu berücksichtigen.

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) in einem Gebäude muss **möglich** und **geordnet** sein.

Mit **möglich** ist gemeint,

- dass Verteiler nicht bei Malerarbeiten mit Farbe oder Tapeten so verklebt werden, dass sie nur noch mit Werkzeug zu öffnen oder unauffindbar sind,
- dass Verteiler nicht mit Möbeln, Geräten, Paletten etc. zugestellt werden,
- dass für verschlossene Verteiler die Schlüssel verfügbar sind und die Schlösser funktionieren.

Mit **geordnet** ist gemeint, dass festgelegt ist, wer welchen Verteiler öffnen darf. Verteiler sollten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch unterschiedliche Schließungen und eine entsprechende Schlüsselverwaltung geregelt werden (siehe dazu M 2.14 *Schlüsselverwaltung* und M 1.80 *Zutrittskontrollsystem und Berechtigungsmanagement*).

Sind in Verteilern des Stromversorgungsnetzes Schmelzsicherungen eingebaut, sollten entsprechende Ersatzsicherungen (im Verteiler) bereit liegen. Eine Dokumentation der Verteiler ist entsprechend M 2.19 *Neutrale Dokumentation in den Verteilern* auszuführen.

Alle im Verteiler eingebauten Einrichtungen sind exakt und verständlich zu beschriften.

Prüffragen:

- Ist der Zutritt zu den Verteilern aller Versorgungseinrichtungen in einem Gebäude im Bedarfsfall schnell möglich?
- Ist der Zutritt zu Verteilern auf einen engen Kreis von Berechtigten beschränkt?

# M 1.3 Angepasste Aufteilung der Stromkreise

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

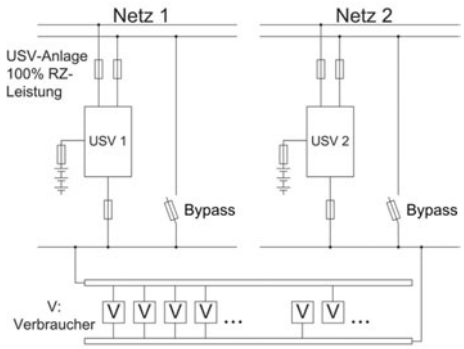
Die Raumbelegung und die Anschlusswerte, für die eine Elektroinstallation ausgelegt wurde, stimmen erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerlässlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimageräte, Beleuchtung, etc.) die Elektroinstallation zu prüfen und gegebenenfalls anzupassen. Das kann in einfachen Fällen durch Umrangierung von Leitungen geschehen. Teilweise kann es aber auch erforderlich werden, zusätzliche bzw. vollkommen neue Einspeisungen, Leitungen, Verteiler etc. zu installieren.

Sowohl mit Blick auf die Sicherheit als auch mit in Betracht der immer schnelleren Datenverbindungen auf Kupferleitungen ist es sehr empfehlenswert, das Stromverteilnetz im gesamten Gebäude komplett als TN-S-Netz auszulegen. Das ist auch Vorgabe der DIN VDE0100-444. Dabei wird der PE- und der N-Leiter ab der Potentialausgleichsschiene (PAS) getrennt geführt. Einzelmaßnahmen an IT-Geräten sind dann in der Regel nicht mehr erforderlich. Zu beachten ist jedoch der Hinweis in M 1.28 *Lokale unterbrechungsfreie Stromversorgung* hinsichtlich der Bildung eines neuen TN-S-Netzes für die angeschlossenen Geräte.

Um die Wirksamkeit des TN-S-Netz-Aufbaus dauerhaft zu gewährleisten, muss sicher gestellt werden, dass die Verbindung zwischen PE- und N-Leiter an der PAS (Nullung) die einzige im gesamten Netz ist. Es kann aber in der Praxis nicht ausgeschlossen werden, dass beim Anschluss neuer Geräte oder bei Schaltarbeiten im Netz versehentlich eine weitere Verbindung zwischen PE- und N-Leiter geschaffen wird. Daher sollten Änderungen im Datennetz mit der Haustechnik abgestimmt werden. Zudem sollte ein TN-S-Netz in regelmäßigen Abständen auf korrekte Nullung hin geprüft werden. Das kann bei den ohnehin durchzuführenden Prüfungen des Stromversorgungsnetzes und bei Verdachtsmomenten (beispielsweise länger andauernde unspezifische Störungen im Datennetz) erfolgen. Idealerweise wird ein TN-S-Netz mit einer permanenten Differenzstromüberwachung ausgestattet.

Sobald hohe oder sehr hohe Anforderungen an die Verfügbarkeit der IT gestellt werden, ist eine Versorgungen der IT über zwei voneinander unabhängige elektrische Versorgungsstränge und der Einsatz von IT-Geräten mit zwei Netzteilen üblich und angemessen.

Die wichtigen Verbraucher (Speicherkomponenten, zentrale Netzknoten, wichtige Server) werden an die unabhängigen Versorgungen "Netz 1" und "Netz 2" angeschlossen (siehe Abbildung). Andere IT-Komponenten, an die wenige hohe Anforderungen gestellt werden, werden gleichmäßig auf die Versorgungsstränge verteilt.




Sichere Energieversorgung über zwei Stränge

Hierbei ist besonders bei den nur einfach angeschlossenen Geräten darauf zu achten, dass Geräte, die sich gegenseitig Redundanz geben, nicht an der gleichen Versorgung angeschlossen werden. Zudem müssen die Geräte entsprechend ihrer Leistungsaufnahme gleichmäßig auf beide Stränge verteilt werden.

Prüffragen:

- Wird regelmäßig überprüft, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen genügen?
- Bei Hochverfügbarkeit: Wird die IT über zwei voneinander unabhängige Versorgungsstränge gespeist?

# M 1.4 Blitzschutzeinrichtungen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Dachstuhlbrand u.ä.) lassen sich durch die Installation einer geeigneten Blitzschutzanlage verhindern. Über diesen "Äußeren Blitzschutz" hinaus ist fast zwingend der "Innere Blitzschutz", der Überspannungsschutz, erforderlich. Denn der äußere Blitzschutz schützt die elektrischen Betriebsmittel im Gebäude **nicht**. Dies ist nur durch einen Überspannungsschutz möglich (siehe dazu M 1.25 *Überspannungsschutz*).

**Beispiel:**

- Durch Blitzschlag entstand in der süddeutschen Niederlassung eines Dienstleistungsunternehmens ein Schaden an IT-Geräten (PCs, Server, Laserdrucker) in Höhe von ca. 10.000 Euro. Aufgrund dieses Ereignisses wurde das Gebäude mit einem äußeren Blitzschutz **ohne** inneren Blitzschutz (Überspannungsschutz) ausgestattet. Ein erneuter Blitzschlag führte nun trotz äußeren Blitzschutzes zu Schäden in annähernd gleicher Höhe.

Die seit Oktober 2006 gültige Norm DIN EN 62305 "Blitzschutz" (entspricht den Normen VDE 0185-305 und IEC 62305) ordnet den gesamten Blitz- und Überspannungsschutz neu. Mit einer Übergangszeit von 2 Jahren haben seit dem 01. Oktober 2008 alle vorher den Blitz- und Überspannungsschutz regelnden Normen ihre Gültigkeit verloren.

Jede Institution sollte auf Basis der neuen Norm DIN EN 62305 ein Blitzschutzkonzept erstellen. In Teil 2 "Risiko-Management" beschreibt diese Norm erstmals allgemeinverbindlich den Weg zu einem risikoorientierten Blitz- und Überspannungsschutz. Im Teil 3 wird darin der "Schutz von baulichen Anlagen und Personen", also der äußere Blitzschutz behandelt.

Der äußere Blitzschutz, die Fangeinrichtung (vulgo Blitzableiter), wird hinsichtlich ihrer Wirksamkeit in vier Schutzklassen (auch Lightning-Protection-Level, kurz LPL genannt) unterteilt. Die Schutzklasse IV (LPL IV) hat den geringsten Schutzwert, während eine Fangeinrichtung der Schutzklasse I den besten Schutz bietet. Leicht erkennbarer Unterschied zwischen den 4 Schutzklassen ist die Maschenweite der Fangeinrichtungen. Diese reicht von 20 x 20 m für die Schutzklasse IV in 5 m-Schritten hinunter bis 5 x 5 m für die Schutzklasse I. Für Gebäude mit umfangreicher IT-Ausstattung sollte die Fangeinrichtung mindestens der Schutzklasse II, besser Schutzklasse I entsprechen.

Der durch die Fangeinrichtung zur Erdung abfließende eingeprägte Blitzstrom bewirkt eine entlang der Fangeinrichtung vom Einschlagspunkt des Blitzes zum Erdungspunkt hin abnehmende Spannung. Am höchsten Punkt der Fangeinrichtung kann diese Spannung einige 100.000 Volt betragen. Es ist daher zu beachten, dass gerade in oberen Geschossen eines Gebäudes galvanisch leitende Installationen (Daten, Strom, Wasser etc.) einen ausreichenden Abstand von den Fangeinrichtungen haben müssen. Auch dieser Aspekt ist unter der Bezeichnung Trennungsabstand in der neuen Norm berücksichtigt. Mit Überlegungen zum Schutz gegen kompromittierende Einkopplung hat das nichts zu tun, auch wenn der Aspekt des Trennungsabstandes bisher häufig fälschlich mit dem Schutz gegen Einkopplung von den zu nahe am Blitzableiter liegenden Datenleitungen auf den Blitzableiter gleichgesetzt wurde.

Da der Spannungsabfall entlang der Fangeinrichtung am Erdungspunkt wegen des verbleibenden Erdübergangswiderstandes nie bis auf 0 V sinkt und der Fußpunkt der Fangeinrichtung mit dem Hauptpotentialausgleich des Gebäudes verbunden sein muss, wird das gesamte PE-System des Gebäudes und damit auch der N-Leiter auf diese Restspannung angehoben. Hier sind Spannungen im Bereich von immerhin noch weit über 10.000 Volt zu erwarten. Es werden also Spannungen zwischen N-/PE-Leitern und den Leitern L1/L2/L3 erreicht, die das betriebsübliche Maß von 230/400 V deutlich überschreiten. Damit diese Spannungen den innerhalb des Gebäudes betriebenen elektrotechnischen Einrichtungen nicht schaden, muss als unverzichtbare Folge aus dem Aufbau des äußeren Blitzschutzes der innere Blitzschutz, also der Überspannungsschutz aufgebaut werden (siehe M 1.25 *Überspannungsschutz*).

Die installierte Fangeinrichtung muss regelmäßig geprüft werden. Fangeinrichtungen der Schutzklassen I und II sind jährlich einer Sichtprüfung und alle 2 Jahre einer umfassenden Prüfung zu unterziehen. Für die Schutzklassen III und IV sind hier 2 bzw. 4 Jahre vorgesehen. Bei kritischen Systemen also solchen zum Schutz hoch- oder höchst verfügbarer Einrichtungen ist eine umfassende Prüfung sogar jährlich durchzuführen. Erkannte Mängel sind umgehend zu beheben. Selbstverständlich sind die Durchführung der Prüfung, die dabei getroffenen Feststellungen sowie durchgeführte Mängelbehebungen schriftlich zu dokumentieren.

Prüffragen:

- Ist eine Blitzschutzanlage nach geltender Norm installiert?
- Ist ein Blitzschutzkonzept vorhanden?
- Entsprechen die Fangeinrichtungen bei Gebäuden mit umfangreicher IT-Ausstattung mindestens der Schutzklasse II?
- Wird die Blitzschutzanlage regelmäßig geprüft und gewartet?

# M 1.5 Galvanische Trennung von Außenleitungen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Einige Störungen, die sich nachteilig auf die ordnungsgemäße Funktion der IT und damit negativ auf deren Verfügbarkeit und Integrität auswirken, erfolgen über elektrisch leitende Medien. Besonders relevant sind hier Einkopplungen von Störsignalen unterschiedlichster Herkunft sowie Überspannungen durch Blitz oder Schalthandlungen. Recht wirkungsvoll können diese Störungen dadurch unterbunden werden, wenn Außenleitungen galvanisch getrennt werden und somit der elektrische Ausbreitungsweg der Störung unterbrochen wird, allerdings ist dies nicht immer möglich.

In der normalen Stromversorgung und bei kupferbasierten Datenübertragungen wäre der Einsatz von Trenntransformatoren zwar tatsächlich eine galvanische Trennung. Störende Spannungsspitzen und andere Störsignale würden aber auch eins zu eins übertragen. Einzig die Bandpass-Wirkung eines Transformators würde die Störung ggf. etwas reduzieren.

Aufgrund der Tatsache, dass Trenntransformatoren nur begrenzt wirken und da diese in Datenleitungen in der Regel nicht einsetzbar sind, ist die oben erwähnte galvanische Trennung für die Praxis nicht relevant. Stattdessen lassen sich Risiken, die durch Spannungsspitzen und Überspannungen auf der Energieversorgung und kupferbasierten Datenleitungen entstehen, ausreichend reduzieren, wenn die Maßnahmen des Überspannungsschutzes umgesetzt werden. Nähere Informationen hierzu finden sich in M 1.25 *Überspannungsschutz*.

Bei Datenleitungen bietet sich die Verwendung von Lichtwellenleitern (LWL) anstelle von Kupferleitungen, mindesten aber die "Unterbrechung" der Kupferleitung durch einen Optokoppler als galvanische Trennung, an.

Sonstige Medienleitungen (Kühlmittel und Kondenswasser einer Kälteversorgung, normale Wasser oder Gasleitungen etc.) müssen natürlich auch betrachtet werden. Ist das geführte Medium selbst elektrisch leitend, also Wasser (auch Hauptbestandteil von Kühlflüssigkeiten), dann ist es kaum zielführend die ansonsten in Kupfer oder Stahl ausgeführte Verrohrung durch Kunststoff zu unterbrechen. Auch hierbei greifen dann nur die einschlägigen Maßnahmen des Überspannungsschutzes.

Einzig bei Gas-Leitungen kann ein nicht-leitendes Rohrstück eine echte galvanische Trennung bewirken. Da aber Gasleitungen grundsätzlich in IT-Bereichen ohnehin nicht verlegt werden sollen, reduziert sich auch die Möglichkeit der Maßnahmen auf den Überspannungsschutz.

# M 1.6 Einhaltung von Brandschutzvorschriften

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter, Haustechnik

Die bestehenden Brandschutzvorschriften (z. B. nach der Norm DIN 4102 Brandverhalten von Baustoffen und Bauteilen) und die Auflagen der Bauaufsicht für Gebäude sind unbedingt einzuhalten. Die örtliche Feuerwehr sollte bei der Brandschutzplanung hinzugezogen werden.

Für Räume, in denen wichtige IT-Geräte und Datenträger (Server, Datensicherungen, etc.) untergebracht sind, sollten zudem die Regelungen der Norm EN 1047 Teil 2 beachtet werden. Ziel ist hier, durch besondere Maßnahmen wie dem Einbau von Türen mit Brand- und Rauchschutzqualität, der sorgfältigen Ausführung von Schottungen und eventuell sogar der Ertüchtigung von Wänden, die Wirkung eines Brandes auf die Inhalte solcher Räume möglichst gering zu halten.

Bei Besprechungs-, Schulungs- und Veranstaltungsräumen sind unter Umständen die entsprechenden Regelungen für den Brandschutz in Versammlungsstätten zu beachten. Da es hier je nach Nutzungsart unterschiedliche Zusatzforderungen wie beispielsweise hinsichtlich der Öffnungsart und -breite von Türen im Verlauf von Flucht- und Rettungswegen und Beschilderungen gibt, sollte auch hier bei der Planung die örtliche Feuerwehr befragt werden.

Es sollte eine Person benannt werden, die für die Einhaltung von Brandschutzvorschriften verantwortlich ist. Dies kann ein Brandschutzbeauftragter oder eine mit dem Aufgabengebiet betraute Person sein, die auch entsprechend geschult ist.

Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel in den Publikationen der VdS Schadenverhütung GmbH zu finden sind.

Besonders wichtig ist es, die Fluchtwege gut auszuschildern. Dafür sind die vorgeschriebenen Kennzeichen zu verwenden und die Vorschriften zu deren Anbringung einzuhalten. Die Fluchtwege müssen immer offen gehalten werden, das heißt insbesondere, dass sie nicht versperrt werden dürfen, z. B. durch im Flur abgestelltes Inventar oder indem die Fluchttüren abgeschlossen werden.

Damit die Feuerwehr im Brandfall schnell mit der Brandbekämpfung beginnen kann, ist es wichtig, dass die Brandmeldezentrale, das Brandmeldetableau und die Einspeisepunkte für Löschwasser durch Beschilderung schnell gefunden werden können.

Zur Verwirklichung eines effizienten Brandschutzes ist die Zusammenarbeit aller zuständigen Verfahrensbeteiligten notwendig. Hierunter fallen die Funktionen

- des Brandschutzbeauftragten (Arbeitgeber ist für die Einhaltung der Brandschutzvorschriften verantwortlich),
- der Fachkraft für Arbeitssicherheit (in Deutschland erforderlich nach §§ 5, 6 Arbeitssicherheitsgesetz, diese ist zuständig für die Ausgestaltung des betrieblichen Brandschutzes) und

- des Sicherheitsbeauftragten (in Deutschland erforderlich nach § 22 SGB VII, dieser hat ausführende Tätigkeiten, z. B. zur Verhütung von Arbeitsunfällen und Berufskrankheiten, und arbeitet der Fachkraft für Arbeitssicherheit zu).

Prüffragen:

- Werden die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht eingehalten?
- Besteht ein Gedankenaustausch mit der örtlichen Feuerwehr zur Einhaltung von Brandschutzvorschriften?
- Gibt es einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute Person, die auch entsprechend geschult ist?
- Sind die Fluchtwege vorschriftsmäßig ausgeschildert und offen gehalten?

# M 1.7 Handfeuerlöscher

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter, Haustechnik

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Zudem ist auf dem Instandhaltungsnachweis jedes Löschers regelmäßig zu prüfen, dass die Löscher auch regelmäßig inspiziert und gewartet werden, damit sie im Ernstfall funktionieren.

Wasserlöscher mit Eignung für Brandklasse A bis 1000 V sind durchaus für elektrisch betriebene Geräte geeignet.

Für elektronisch gesteuerte Geräte, z. B. Rechner, sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird durch Verdrängung des Sauerstoffs erreicht, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten.

Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind. Es wird daher dringend empfohlen, im direkten Umfeld von Serverräumen, Datenträgerarchiven, Räumen für technische Infrastruktur und Rechenzentren keine Pulverlöscher, sondern ausschließlich geeignete Gaslöscher bereit zu halten. Nur so kann verhindert werden, dass in der Ausregung eines Brandes fälschlicher Weise ein Pulverlöscher verwendet wird.

Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind. Die Beschäftigten sollten sich den Standort des nächsten Feuerlöschers einprägen. Die Standorte von Löschern und Hydranten sind durch vorgeschriebene Schilder kenntlich zu machen. Tragbare Feuerlöscher sind zugelassen bis zu einem Gesamtgewicht von 20 kg. Mit den überwiegend eingesetzten Geräten von 6 und 12 kg lassen sich größere Brandherde löschen als von Laien üblicherweise angenommen wird, dies ist allerdings nur bei konsequenter Vorgehensweise gegeben. Bis zur vollständigen Entladung des Löschmittels vergehen nur wenige Sekunden. Daher sind bei entsprechenden Brandschutzübungen die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen und die Bedienung der Löscher auch zu üben.

Prüffragen:

- Sind geeignete Handfeuerlöscher im Brandfall leicht erreichbar?
- Werden die Handfeuerlöscher regelmäßig inspiziert und gewartet?
- Sind die Mitarbeiter in die Benutzung der Handfeuerlöscher eingewiesen worden?

# M 1.8 Raumbelegung unter Berücksichtigung von Brandlasten

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter, Haustechnik

Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge und Gardinen. Nähere Erläuterungen zur Brennbarkeit oder Nichtbrennbarkeit von Baustoffen (Baustoffklasse A bzw. B) sind in der DIN 4102-Teil 1 und Teil 4 zu finden.

Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. Zum Beispiel sollte das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager untergebracht sein.

Auch im laufenden Betrieb muss auf die Vermeidung unnötiger Brandlasten geachtet werden. Die regelmäßige Entsorgung von Müll, vor allem von Altpapier und von Verpackungsabfällen ist aktiver Brandschutz.

Prüffragen:

- Werden unnötige Brandlasten vermieden?

# M 1.9 Brandabschottung von Trassen

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter, Haustechnik

Elektroleitungen und IT-Verkabelung werden typischerweise in Installationstrassen konzentriert. Es ist oft festzustellen, dass Trassen entlang von Flucht- und Rettungswegen, durch Tiefgaragen, Lager, Werkstätten oder als Transittrassen durch fremde Nutzungsbereiche führen.

Bei Gebäuden mit mehreren Brandabschnitten unterliegt die Ausführung von Elektroleitungen und der IT-Verkabelung brandschutztechnischen Auflagen. Dies betrifft insbesondere Leitungen, die Brandabschnitte, Wände oder Decken durchqueren oder die in Verkehrswegen verlegt wurden. Speziell wenn die Trassen für Brandmelde-, Alarmierungs-, Löschtechnik oder Sicherheitsbeleuchtung genutzt werden, sind zusätzliche Forderungen nach Funktionserhalt von Elektroleitungen im Brandfall einzuhalten. Daher sollte bei der Planung der Trassen in jedem Fall der Brandschutzbeauftragte hinzugezogen werden. Trassen müssen sowohl Brandschutz als auch Schutz gegen Sabotage bieten. Beides lässt sich durch eine fachgerechte Schottung der Trassen erreichen.

Wenn Elektrokabel in erheblicher Packungsdichte im brandschutztechnisch abgetrennten Kabelkanal geführt sind, können größere Temperaturerhöhungen entstehen. Dies kann ein Ansteigen des elektrischen Leitungswiderstandes mit zusätzlicher Erwärmung nach sich ziehen. Abhilfe lässt sich entweder durch eine Leitungsreduktion oder durch eine ausreichende Be- und Entlüftung erreichen. Daher sind die Vorgaben in DIN VDE 0100-520 *"Errichten von Niederspannungsanlagen - Teil 5: Auswahl und Errichtung elektrischer Betriebsmittel - Kapitel 52: Kabel- und Leitungsanlagen"* als deutsche Fassung der IEC 60364-5-52 in Abhängigkeit der Verlegeart zu beachten. Dies liegt im Verantwortungsbereich des Elektrofachplaners.

Die marktüblichen Be- und Entlüftungsmethoden bzw. -techniken z. B. durch Lüftungsbausteine haben den Nachteil, dass sie keinen ausreichenden Schutz vor Sabotagehandlungen bieten. Das bedeutet, dass Leitungen mit hohem oder sehr hohem Schutzbedarf, die durch ungeschützte Bereiche führen, wie z. B. eine Tiefgarage, in dieser Ausführung kaum gegen deliktische Handlungen geschützt sind. Hier sind individuelle Planungsmaßnahmen gefordert. Das kann die ausreichende Dimensionierung des Kanals sein, die eine Belüftung des Kanals im gefährdeten Bereich unnötig macht, oder ein spezielles Belüftungskonzept, das auf die spezifischen Sicherungsanforderungen ausgerichtet ist.

Durchbrüche sind nach Verlegung der Leitungen entsprechend der Feuerwiderstandsklasse der Wand bzw. Decke zu schotten. Um die Nachinstallation zu erleichtern, können geeignete Materialien wie Weichschotts oder Brandschutzkissen bei Maßnahmen mit temporärem Charakter verwendet werden. Entsprechende Normen und Richtlinien, wie die DIN 4102 *"Brandverhalten von Baustoffen und Bauteilen"*, sind zu beachten. Kabeltrassen dehnen sich bei Erwärmung z. B. durch Brandeinwirkung aus und können ein Weich- oder Kissenschott zerstören, wenn sie durch Wände geführt werden.

Daher sollten Trassen nicht durch das Schott hindurch geführt werden, sondern beidseitig mindestens 10 cm vor der Wand enden. Diese Praxis erleich-

tert auch das Ausfächern der Kabel und Leitungen, die nicht als Bündel, sondern einzeln durch das Schott geführt werden müssen.

Häufig werden in einer Trasse unterschiedliche Kabel, z. B. für Telefon, LAN und Haustechnik, geführt. Falls Änderungen der Verkabelung anstehen, sollte bereits in der Planungsphase geklärt werden, ob in absehbarer Zeit auch andere Kabelsysteme ausgewechselt werden sollen. Eine entsprechende Zusammenlegung von Projekten minimiert Ausfallzeiten und erspart zusätzliche Kosten für eine mehrmalige Brandschottung.

Ist die geplante Trassenführung gemäß den brandschutztechnischen Auflagen nicht möglich, so ist eine alternative Trassenführung zu prüfen. Darüber hinaus sollten nach Abschluß der Installationsarbeiten die Brandabschottung in regelmäßigen Abständen, beispielsweise jährlich, kontrolliert werden.

Prüffragen:

- Werden die brandschutztechnischen Auflagen und Vorschriften bei der Ausführung der Elektro- und IT-Verkabelung eingehalten?
- Sind alle Durchbrüche nach Verlegung der Leitungen entsprechend der Feuerwiderstandsklasse geschottet?

# M 1.10 Sichere Türen und Fenster

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Wenn Türen und Fenster einen Übergang zwischen Sicherheitszonen bilden, müssen sie angemessenen Schutz bieten. Eine Außentür muss z. B. vor Einbrüchen schützen, ebenso müssen die erreichbaren Fenster gesichert werden. Im Innenbereich müssen Türen, die die Grenze eines Brandabschnitts bilden, selbst Brandschutzqualität haben, zudem können sie oder auch andere Innentüren eine zweite Linie des Einbruchschutzes bilden.

Sicherheitstüren und -fenster sind in Normen klassifiziert. Aus dem Schutzziel des zu sichernden Bereichs und dem Schutzbedarf der Institution lässt sich eine Auswahl der angemessenen Ausführung von Türen und Fenstern treffen:

- In der Norm DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung" sind die Bauelemente in Widerstandsklassen (RC, engl. Resistance Class) eingeordnet worden. Türen gemäß der Klassifizierungen RC1 bis RC4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Serverräumen, Räumen mit technische Infrastruktur sowie bei Keller- und Lieferanteneingängen). Die Widerstandsklassen RC5 und RC6 sind in der Regel nur bei sehr speziellen Erfordernissen angemessen und spielen daher bei IT-Grundschutzbetrachtungen keine Rolle.
- Selbstschließende feuerhemmende und gegebenenfalls rauchdichte Türen (z. B. Feuerschutztüren T30 bzw. T30-RS, nach DIN 18082 "Feuerschutzabschlüsse") verzögern die Ausbreitung eines Brandes und in der RS-Ausführung auch von Rauch.
- Sie schützen in der Ausführung als selbstschließende Rauchschutztür (DIN 18095-1 "Türen; Rauchschutztüren; Begriffe und Anforderungen") die Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten hindurch kommt. Für die geringen Flughöhen von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden.

Es können auch mehrere Schutzeigenschaften in einer Tür kombiniert werden, es gibt beispielsweise rauchdichte Brandschutztüren, die zudem Schutz gegen Einbruch bieten.

Die Sicherungsmaßnahmen aller raumumschließenden Bauelemente müssen gleichwertig sein:

- Bei Verwendung einbruchhemmender Türen ist im Fassadenbereich die Verwendung einbruchhemmender Fenster oder Fassadenelemente (siehe DIN EN1627-1630:2011 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung") zu erwägen.
- Weiterhin ist es z. B. nicht zweckmäßig, eine einbruchhemmende Tür der höchsten Widerstandsklasse in eine Gipskartonwand einzubauen.
- Beim Einbau einer feuerhemmenden oder rauchdichten Tür ist darauf zu achten, dass auch die umgebende Wand gleichwertig feuerhemmend und rauchdicht ist und nicht durch offene Oberlichter oder ungeschottete Kabeldurchführungen ein Bypass besteht.

Anforderungen zur Ausführung von Sicherheitstüren finden sich in den Maßnahmen M 1.47 *Eigener Brandabschnitt* und M 1.19 *Einbruchsschutz*.

Der Einsatz von Sicherheitstüren ist hinsichtlich der Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus (siehe M 1.6 *Einhaltung von Brandschutzvorschriften*) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches den Einbau von Sicherheitstüren und die Gefahrenmeldung und Alarmierung zur Prüfung und Intervention berücksichtigt. Denn hat ein potentieller Angreifer ein ganzes Wochenende Zeit für einen Einbruchsversuch, wird ihn auch eine hochwertige einbruchhemmende Tür nicht von seinem Ziel abhalten, Daten oder Einrichtung zu entwenden oder zu zerstören.

Für die Ausstattung von Rechenzentren sollte für die Türen inklusive deren Einbausituation die Widerstandsklasse RC3 gemäß DIN EN 1627-1630:2011 als Mindestwert angesetzt werden. Lediglich wenn für die Sicherheit ganz besonders günstige Bedingung vorliegen, insbesondere falls die Interventionszeit hilfeleistender Kräfte kurz ist (maximal 2 Minuten), kann in Ausnahmefällen eine RC2-Tür ausreichen. Liegt die Interventionszeit hilfeleistender Kräfte hingegen bei 5 Minuten und höher, ist sogar eine RC3-Tür als unzureichend anzusehen und es empfiehlt sich der Einbau von RC4-Türen. Sinngemäß gelten die gleiche Überlegungen natürlich auch für alle anderen, die RZ-Hülle bildenden Bauelemente.

**Hinweis:** Ziel eines Einbruches könnte es auch sein, Daten oder IT-Systeme zu manipulieren. Daher sollten zentrale IT-Systeme nach Einbrüchen auf ihre Integrität überprüft werden (siehe dazu auch M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

Außerdem ist regelmäßig zu prüfen, dass die Sicherheitstüren und -fenster funktionstüchtig sind. Sie müssen in einem ordentlichen mechanischen Zustand sein, sicher öffnen und schließen und überwachende Installationen wie Schließkontakte müssen funktionieren.

Prüffragen:

- Sind alle raumumschließenden Sicherungsmaßnahmen durch Fenster, Türen und Wände bzgl. Einbruch, Brand und Rauch gleichwertig und angemessen?
- Wird regelmäßig überprüft, dass die Sicherheitstüren und -fenster funktionstüchtig sind?
- Sind bei einem Rechenzentrum die Widerstandswerte von Türen, Fenstern und anderen raumbildenden Bauelementen einerseits und die Interventionszeit hilfeleistender Kräfte andererseits aufeinander abgestimmt?

# M 1.11 Lagepläne der Versorgungsleitungen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Es sind genaue Lagepläne aller Versorgungsleitungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) im Gebäude und auf dem dazugehörenden Grundstück zu führen und **alle** die Leitungen betreffenden Sachverhalte aufzunehmen:

- genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- genaue technische Daten (Typ und Abmessung),
- eventuell vorhandene Kennzeichnung,
- Nutzung der Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- Gefahrenpunkte und
- vorhandene und zu prüfende Sicherheitsmaßnahmen.

Es muss möglich sein, sich anhand der Pläne einfach und schnell ein genaues Bild der Situation zu machen. Nur so kann das Risiko, dass Leitungen bei Arbeiten versehentlich beschädigt werden, auf ein Mindestmaß reduziert werden. Eine Schadstelle ist dadurch schneller zu lokalisieren, die Störung schneller zu beheben.

Es ist sicherzustellen, dass alle Arbeiten an Leitungen rechtzeitig und vollständig dokumentiert werden. Daher ist klar zu regeln, wer für die Pflege und Aktualisierung der Lagepläne aller Versorgungsleitungen zuständig ist. Die Pläne sind gesichert aufzubewahren, da sie schützenswerte Informationen beinhalten. Sie sind so zu lagern, dass ausschließlich berechtigte Personen darauf zugreifen können, sie aber im Bedarfsfall schnell verfügbar sind.

Prüffragen:

- Existieren aktuelle Lagepläne aller Versorgungsleitungen?
- Ist klar geregelt, wer dafür verantwortlich ist, die Lagepläne aller Versorgungsleitungen zu führen?
- Können auf sicherheitskritische Lagepläne ausschließlich berechtigte Personen zugreifen?

# M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

In jedem Gebäude gibt es Bereiche mit unterschiedlichen Nutzungsszenarien und unterschiedlichem Schutzbedarf. Schützenswerte Gebäudeteile sind z. B. Serverraum, Rechenzentrum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalt- und Rangierräume, Ersatzteillager.

Solche Bereiche sollten keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z. B. RECHENZENTRUM oder ARCHIV geben einem potentiellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender vorbereiten zu können.

Ist es unvermeidbar, geschäftsrelevante Informationen oder IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde leicht von außen einsehbar sind (siehe auch M 1.13 *Anordnung schützenswerter Gebäudeteile*), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z. B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

Prüffragen:

- Sind Lagehinweise auf schutzwürdige Bereiche vermieden worden?
- Ist sichergestellt, dass schutzwürdige Gebäudebereiche von außen nicht leicht einsehbar sind?

# M 1.13 Anordnung schützenswerter Gebäudeteile

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Planer
**Verantwortlich für Umsetzung:** Bauleiter, Leiter Haustechnik

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein:

- Kellerräume sind eventuell durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.
- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Gut einsehbare Räume im Erdgeschoss oder in Bereichen mit Publikumsverkehr sind gefährdet, da dadurch Spontandiebstähle oder unerwünschte Einsichtnahmen in geschäftsrelevante Informationen ermöglicht werden können.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.
- Tiefgaragen können eine ganze Reihe von Risiken mit sich bringen: schlecht einsehbare Hintereingänge, offen zugängliche Versorgungsleitungen oder IT-Verkabelungen, sie bieten aber auch häufig Unbefugten die Möglichkeit, aus Autos heraus auf ungenügend gesicherte WLANs zuzugreifen. Aus Sicht des Brandschutzes sind auch Bereiche in Tiefgaragen problematisch, die als Lagerraum missbraucht werden.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.

Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen. Bei bereits genutzten Gebäuden wird eine entsprechende Nutzungsanordnung oft mit internen Umzügen verbunden sein. Ersatzweise sollten die sich aus ohnehin erforderlichen Änderungen der Raumbelegung ergebenden Gelegenheiten konsequent genutzt werden.

Wenn schützenswerte Räume nicht anders als in exponierter Lage angeordnet werden können, so sollte das explizit im Sicherheitskonzept dokumentiert werden. Außerdem sind zusätzliche kompensierende Maßnahmen zu ergreifen, die der besonderen Gefährdung entgegenwirken.

So kann z. B. bei elektrischen Betriebsräumen oder IT-Räumen im Keller eine bestehende Gefährdung durch Wasser durch umfassende Wasserdetektion, Schwellenbildung und Vorbereitung von Entwässerungsmaßnahmen beherrscht werden.

Prüffragen:

- Sind schützenswerte Räume in exponierter Lage dokumentiert?
- Sind ausreichende Maßnahmen ergriffen, um schützenswerte Räume in exponierter Lage zu sichern?

# M 1.14 Selbsttätige Entwässerung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Planer
**Verantwortlich für Umsetzung:** Bauleiter, Leiter Haustechnik

Alle Bereiche innerhalb von Gebäuden, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit einer selbsttätigen Entwässerung und mit Wassermeldern ausgestattet sein. Zu diesen Bereichen gehören u. a.:

- Keller,
- Lufträume unter Doppelböden,
- Lichtschächte,
- Heizungsanlage.

Erfolgt die Entwässerung passiv, also durch Bodengullys direkt in das Abwassersystem des Gebäudes, sind Rückstauklappen unerlässlich. Ohne solche Klappen wird diese Entwässerung zur Wassereintrittsöffnung, wenn das Abwassersystem überlastet wird. Nach extremen Niederschlägen dringt in der Mehrzahl aller Fälle Wasser über diesen Weg in Keller ein. Die Rückstauklappen müssen regelmäßig auf ihre Funktionstüchtigkeit hin untersucht werden.

Ist eine passive Entwässerung nicht möglich, weil das Niveau des Abwassersystems zu hoch ist, können Pumpen eingesetzt werden, die über Schwimmerschalter oder Wassersensoren automatisch eingeschaltet werden. Beim Einsatz dieser Technik sind insbesondere folgende Punkte zu beachten:

- Die Pumpenleistung muss ausreichend bemessen sein.
- Die Druckleitung der Pumpe ist mit einem Rückstauventil auszustatten.
- Es sind Vorkehrungen zu treffen, damit die Pumpe nicht durch mitgeschwämmte Gegenstände blockiert werden kann (Ansaugfilter etc.).
- Das Anlaufen der Pumpe sollte automatisch (z. B. beim Hausmeister oder der Haustechnik) angezeigt werden.
- Die Funktion von Pumpe und Schalter ist regelmäßig zu testen.
- Die Druckleitung der Pumpe darf nicht an eine in unmittelbarer Nähe vorbeigeführte Abwasserleitung angeschlossen werden. Bei einem Leck dieser Leitung würde die Pumpe das Wasser nur "im Kreis pumpen".

Um zu verhindern, dass Wasser z. B. bei Starkregen von Außen in das Gebäude dringt, ist auch der Zustand der Grundstücksentwässerung zu prüfen und diese gegebenenfalls instand zu setzen. Falls die Lage oder das Profil des Grundstücks besondere Gefährdungen des Gebäudes durch Oberflächenwasser mit sich bringen, kann der Einbau besonderer Wasserschutztüren erwogen werden.

Prüffragen:

- Sind alle wassergefährdeten Bereiche mit einer selbsttätigen Entwässerung wasserbedrohten Räume mit einer selbsttätigen Entwässerung ausgestattet?
- Wird die Funktionstüchtigkeit aktiver und passiver Entwässerungseinrichtungen regelmäßig geprüft?

# M 1.15 Geschlossene Fenster und Türen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik, Mitarbeiter

Fenster und nach außen gehende Türen (Balkone, Terrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Außentüren sind abzuschließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution genutzt werden.

Mitarbeiter sollten darauf hingewiesen werden, dass Fenster und Türen beim Verlassen von Räumen zu schließen sind. Wenn während normaler Arbeitszeiten sichergestellt ist, dass die Räume nur kurzzeitig leer stehen, kann von einer zwingenden Regelung für Büroräume sowie für Besprechungs-, Veranstaltungs- und Schulungsräumen abgesehen werden.

Keine Ausnahme darf bei Brand- und Rauchschutztüren zugelassen werden. Solche Türen bieten nur im verschlossenen Zustand Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden.

Es ist sinnvoll, wenn Pförtner oder Mitarbeiter der Haustechnik regelmäßig überprüfen, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden.

In Besprechungs-, Veranstaltungs- und Schulungsräumen gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

Prüffragen:

- Gibt es eine Anweisung, die das Verschließen der Fenster und Außentüren fordert?
- Wird regelmäßig überprüft, ob die Fenster und Türen nach Verlassen der Räume verschlossen sind?
- Wird darauf geachtet, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden?

# M 1.16 Geeignete Standortauswahl

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Bei der Auswahl und Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten, auch Umfeldgegebenheiten, die Einfluss auf die Informationssicherheit haben, zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen.
- Gebäude, die direkt an Hauptverkehrstrassen (Eisenbahn, Autobahn, Bundesstraße, Flughafen) liegen, können durch Unfälle beschädigt werden.
- Die Nähe zu optimalen Verkehrs- und somit Fluchtwegen kann die Durchführung eines Anschlages erleichtern.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z. B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.

Es kann auch möglich sein, Gefährdungen aus der Nachbarschaft z. B. durch passende Anordnung schützenswerter Gebäudeteile zu kompensieren. Dies sollte bei der Auswahl und Planung berücksichtigt werden.

Die standortbedingten Gefährdungen und die erforderlichen schadensvorbeugenden oder -reduzierenden Maßnahmen sollten im Sicherheitskonzept dokumentiert werden. Außerdem sollten sie ins Notfallkonzept einfließen.

Prüffragen:

- Gibt es eine Übersicht über standortbedingte Gefährdungen?
- Wird diesen Gefährdungen mit zusätzlichen kompensierenden Maßnahmen begegnet?

# M 1.17 Pförtnerdienst

**Verantwortlich für Initiierung:** Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Innerer Dienst

Die Einrichtung eines Pförtnerdienstes hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Voraussetzung ist allerdings, dass bei der Durchführung des Pförtnerdienstes einige Grundprinzipien beachtet werden.

- Der Pförtner beobachtet bzw. kontrolliert alle Personenbewegungen an der Pforte und an allen anderen Eingängen.
- Unterstützt durch Videoüberwachung können entfernte Türen und Tore vom Pförtner überwacht und auch gesteuert werden (siehe M 1.53 *Videoüberwachung*).
- Dem Pförtner müssen die Mitarbeiter bekannt sein. Es ist zu empfehlen, dass sich auch bekannte Personen beim Pförtner legitimieren, also z. B. einen Hausausweis vorzeigen. Scheidet ein Mitarbeiter aus der Institution aus oder ändert seine Position innerhalb der Institution, ist auch der Pförtner zu unterrichten, ab wann diesem Mitarbeiter der Einlass zu verwehren ist oder ob sich Zutrittsberechtigungen ändern.
- Unbekannte Personen ("selbst der neue Chef") haben sich beim Pförtner auszuweisen.
- In einem Besucherbuch kann der Zutritt von Fremdpersonen zum Gebäude dokumentiert werden. Die Ausgabe von Besucherausweisen oder Besucherbegleitscheinen ist zu erwägen.
- Besucher werden zu den Besuchten begleitet oder an der Pforte abgeholt. Falls Besucher unbegleitet das Gebäude betreten dürfen, muss vorher verifiziert werden, dass dies ohne Sicherheitsbedenken möglich ist. Die jeweiligen Rahmenbedingungen sind vorab zu dokumentieren. Beispielsweise könnte eine Liste mit vertrauenswürdigen Dauerbesuchern geführt werden, die nach Erhalt eines Besucherausweises das Gebäude ohne Begleitung betreten dürfen.
- Wenn die Pforte rund um die Uhr besetzt ist, können dort immer oder nur außerhalb der normalen Dienstzeiten Meldungen der alarmierenden und überwachenden Technik auflaufen. Anhand von Alarmlisten zu den Meldungen leitet die Pforte die Meldungen an zuständige Mitarbeiter in Bereitschaft oder zuständige externe Stellen weiter.

Die Arbeitsbedingungen des Pförtners sind für die Aufgabenwahrnehmung geeignet auszugestalten. Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben dem Pförtner im Zusammenspiel mit weiteren Schutzmaßnahmen zukommt (z. B. Gebäudesicherung nach Dienst- oder Geschäftsschluss, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).

Bei der Definition der Aufgaben muss beachtet werden, dass die zugewiesenen Aufgaben keine Sicherheitslücken aufreißen. Wenn eine Pforte mit nur einem Pförtner besetzt ist und dieser keine Möglichkeit hat, die Pforte vorübergehend zu verschließen, so darf er nicht die Anweisung haben oder erhalten, Besucher selbst zu bestimmten Besuchten zu begleiten.

Prüffragen:

- Sind die Aufgaben des Pförtnerdienstes klar dokumentiert?
- Müssen sich Mitarbeiter und Besucher beim Pförtner legitimieren?
- Werden Besucher zu den Besuchten begleitet bzw. an der Pforte abgeholt?

- Werden die Pförtner rechtzeitig darüber informiert, wenn sich Zutrittsberechtigungen ändern?

# M 1.18 Gefahrenmeldeanlage

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, IT-Sicherheitsbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen und die Anforderungen der DIN EN 50518 "Notruf- und Serviceleitstellen" zu beachten.

Es sollte ein Konzept für die Gefahrenerkennung, Weiterleitung und Alarmierung für die verschiedenen Gebäudebereiche erstellt werden. Dieses muss an Veränderungen bei der Nutzung angepasst werden. Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das dem Gebäude und dem Risiko entsprechend geplant und installiert werden muss. Planung, Installation und Wartung einer Gefahrenmeldeanlage sollte daher durch Experten durchgeführt werden. Falls diese nicht im eigenen Haus vorhanden sind, sollte auf externe Unterstützung zurückgegriffen werden. So gibt es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme, die entsprechend der Sicherheitsanforderungen und der Umgebung ausgewählt werden müssen. Zur Einbruchserkennung können z. B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras u. a. eingesetzt werden.

Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert sein müssen und möglichst wenig Änderungen an der Trassenbelegung vorgenommen werden sollten.

Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (siehe DIN VDE 0833 Teil 1-3 "Gefahrenmeldeanlagen für Brand, Einbruch und Überfall") vorzusehen.

Ist keine GMA vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (eventuell Telefonleitung) an anderer Stelle.

Für den Betrieb eines Rechenzentrums muss eine GMA zur Brand- und Einbruchdetektion installiert sein. Weitere Detektionsbereiche können nach Lage des Standorts und dessen Infrastruktur sinnvoll sein.

Es gibt Räume wie Serverraum, Datenträgerarchiv, die einen erhöhten Schutzbedarf haben. Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.

Vor der Planung einer GMA muss ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Bei der Planung von Gefahrenmeldeanlagen für private bzw. gewerbliche Objekte sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.

Prüffragen:

- Gibt es eine den Räumlichkeiten und den Risiken angemessene Gefahrenmeldeanlage?
- Wird die Gefahrenmeldeanlage regelmäßig gewartet bzw. geprüft?
- Sind die Empfänger von Gefahrenmeldung in der Lage, auf Alarmmeldungen angemessen zu reagieren?

# M 1.19 Einbruchsschutz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Erfahrungsgemäß wählen Einbrecher ihre Ziele danach aus, wie hoch das Risiko und Aufwand im Verhältnis zum erwarteten Gewinn sind. Daher sollten alle Maßnahmen zum Einbruchsschutz darauf zielen, die Erfolgsaussichten von Tätern zu minimieren. Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden. Dazu gehören:

- einbruchhemmende Türen und Fenster, beispielsweise mit der Widerstandsklasse RC2 (nach DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung") oder höherwertig, wenn die Gefährdungslage es erforderlich macht,
- Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenster,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluss von nicht benutzten Nebeneingängen,
- einbruchgesicherte Notausgänge,
- Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Empfehlungen hierzu geben die örtlichen Beratungsstellen der Kriminalpolizei.

Alle Maßnahmen zum Einbruchsschutz sollten sinnvoller Weise eine durchgehend gleichwertige Hülle um den Bereich bilden, der gegen unbefugten Zutritt geschützt werden soll. Türen sind in ausreichend feste Wände einzubauen. Lüftungsöffnungen sind in geeigneter Form zu vergittern. (maximale Gitterweite 10x20 cm). Auch in Doppelbodenbereichen und über abgehängten Decken sind Maßnahmen zum Zutrittsschutz umzusetzen. Die Gleichwertigkeit und Durchgängigkeit des Einbruchsschutzes sollte durch eine fachkundige Person während der Planung, bei der Umsetzung und später im Betrieb regelmäßig begutachtet werden.

Bei der Planung materieller Sicherungsmaßnahmen ist darauf zu achten, dass Bestimmungen des Brand- und Personenschutzes, z. B. die Nutzbarkeit von Fluchtwegen, nicht verletzt werden. Dies gilt insbesondere für Änderungen an Brandschutzelementen, die einer Typenfreigabe unterliegen.

Den Mitarbeitern ist bekanntzugeben, welche Regelungen und Maßnahmen zum Einbruchsschutz beachtet werden müssen, also beispielsweise dass Türen, Fenster oder Rollladensicherungen abends abgeschlossen werden müssen.

Auch innerhalb eines Gebäudes kann der Einbau von einbruchhemmenden Elementen sinnvoll sein. Die Absicherung ist zu erwägen bei besonderen zutrittskontrollierten Bereichen wie den Räumen der Geschäftsleitung, Serverräumen oder den Kerneinheiten eines Rechenzentrums.

Prüffragen:

- Wurden ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen zum Einbruchsschutz umgesetzt?

- Werden Gleichwertigkeit und Durchgängigkeit des Einbruchsschutzes bei der Planung, der Umsetzung und im Betrieb regelmäßig durch eine fachkundige Person begutachtet?
- Sind die Regelungen zum Einbruchsschutz den Mitarbeitern bekannt?

# M 1.20 Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Planer, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik, Leiter IT

Bei der Auswahl von Kabeln sind neben den übertragungstechnischen Notwendigkeiten auch die Umgebungsbedingungen bei der Verlegung sowie im Betrieb zu berücksichtigen. Um diesen unterschiedlichen Anforderungen gerecht zu werden, bieten die Kabelhersteller unterschiedliche Arten von Kabeln am Markt an oder entwickeln entsprechende Lösungen.

In Bezug auf den Kabelmantel für Verlegung im Innen- oder Außenbereich müssen folgende Kriterien berücksichtigt werden:

- Temperatur,
- umgebendes Medium (Wasser, Abwasser, Säure, Gas, Licht),
- Nagetierschutz, Hieb- und Spatenstichfestigkeit, Steinschlagfestigkeit, Wasserdruckfestigkeit,
- Funktionserhalt in feuergefährdeten Bereichen,
- spezielle Zugkräfte durch z. B. Freileitungsverwendung.

Außerdem sind die vorgesehenen Trassensysteme zu beachten, wie Kabelpritschen, Kabelleiter, Kabelkanäle, Kabelzugrohre, Kabelformsteine, Steigebereiche und Freileitungsbau.

Der weitere Kabelaufbau muss folgende Faktoren berücksichtigen:

- Zugkräfte durch maschinelle Verlegung, z. B. Kabelzugwinde, Einblassystem oder Handverlegung,
- Biegeradius und Querdruckstabilität, entsprechend Verlegeart und Ruhezustand im Betrieb,
- Feucht- oder Nassbereiche durch Längswasserschutz,
- spezielle Zugkräfte im verlegten Zustand, die durch große Spann- oder Abfangweiten bei Freileitungen oder extremen Steigungen entstehen,
- starke elektrische und induktive Störfelder durch Kabelschirmung.

Die richtige und den Vorschriften gemäße Auswahl von Elektrokabeln und die Beachtung der einschlägigen Normen (DIN VDE 0100 *"Bestimmungen für das Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V"*, DIN 4102 *"Brandverhalten von Baustoffen und Bauteilen"*) und Vorschriften sowie der anerkannten Regeln der Technik stellt die grundlegende Notfallvorsorge der elektrotechnischen Installation dar.

Individuelle Anforderungen für die Auswahl von Kabeln dürfen gerade bei Betriebsumgebungen, in denen Umwelteinflüsse oder besondere bauliche Gegebenheiten zu beachten sind, nicht ausschließlich durch die IT selbst definiert werden. Insbesondere Mitarbeiter der Haustechnik, die mit Betriebsabläufen und sonstigen besonderen Bedingungen vertraut sind, müssen zur geplanten Kabelführung, bei der Feststellung der relevanten Einflüsse und damit der besonderen Anforderung an die Ausführung von Kabeln beteiligt werden.

Prüffragen:

- Wurden bei der Auswahl von Kabeln sowohl die übertragungstechnischen Anforderungen, als auch die Umgebungsbedingungen bei der Verlegung sowie im Betrieb berücksichtigt?
- Wurden im Hinblick auf den Kabelmantel die notwendigen Kriterien (z. B.: Temperaturbereich, Funktionserhalt, Wasserdruckfestigkeit, etc.) beachtet?
- Werden die anzuwendenden Normen und Vorschriften (z. B. zum Brandschutz, Betriebssicherheit) bei Auswahl der Elektrokabel beachtet?

# M 1.21 Ausreichende Trassendimensionierung

**Verantwortlich für Initiierung:** Haustechnik, Planer, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Kabeltrassen (z. B. Fußbodenkanäle, Fensterbank-Kanäle, Pritschen, Rohrtrassen im Außenbereich) sind ausreichend zu dimensionieren. Es muss einerseits genügend Platz vorhanden sein, um eventuell notwendige Erweiterungen des Netzes vornehmen zu können. Andererseits sind zur Verhinderung des Übersprechens (gegenseitige Beeinflussung von Kabeln) eventuell Mindestabstände zwischen den Kabeln einzuhalten. Insbesondere ist bei der Nutzung von gemeinsamen Trassen für Energie- und IT-Verkabelung sicherzustellen, dass die Trassen durch einen Mittelsteg getrennt sind. Schon durch eine einfache getrennte Führung von Stromkabeln und IT-Kabeln lassen sich Störungen der IT meist vermeiden.

Ist es nicht möglich, Trassen mit ausreichenden Reserven zu errichten, sollte zumindest darauf geachtet werden, dass im Bereich der Trassenführung genügend Platz ist, um Erweiterungen unterzubringen. Werden Wand- und Deckendurchbrüche in hinreichender Größe ausgelegt, kann auf spätere lärm-, schmutz- und kostenintensive Arbeiten verzichtet werden. Bei Verwendung von nachinstallationsfähigen Brandschotten können Durchbrüche so gerüstet werden, dass der Schutz vor Feuer und Verrauchung stets gewährleistet ist, zugleich die Nachführung von Kabeln aber jederzeit problemlos möglich bleibt.

Zu beachten ist, dass Durchbrüche durch Wände mit einer Feuerwiderstandsklasse nur zu 60 % belegt werden dürfen, um eine wirksame Schottung dieser Öffnungen erreichen zu können. Gegebenenfalls sollten für spätere Erweiterungen bei der Errichtung Durchbrüche vorgesehen und diese vorerst mittels Weichschott oder Brandschutzkissen verschlossen werden.

Wichtig ist, dass die Trassendimensionierung immer im Zusammenhang mit der Auswahl der Kabeltypen geplant werden muss (siehe M 1.20 *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht* und M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*). Beispielsweise kann durch Verwendung einiger vieladriger Kabel gegenüber vielen kleinen Kabeln Platz eingespart werden. Durch den Einsatz von geschirmten Kabeln oder Lichtwellenleitern kann Übersprechen verhindert werden. So kann auch auf Trassenwegen mit wenig Platz ein störungsfreier Betrieb gewährleistet werden.

Prüffragen:

- Sind die Kabeltrassen im Hinblick auf mögliche Erweiterungen oder einzuhaltende Mindestabstände ausreichend dimensioniert?
- Sind IT- und Elektroverkabelung mindestens durch einen Mittelsteg getrennt, besser jedoch auf jeweils eigenen Trassen geführt?
- Wird bei Wanddurchbrüchen mit einer bestimmten geforderten Feuerwiderstandsklasse die maximale Belegung mit Kabeln eingehalten?

# M 1.22 Materielle Sicherung von Leitungen und Verteilern

**Verantwortlich für Initiierung:** Planer, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes kann es sinnvoll sein, Leitungen und Verteiler zusätzlich gegen unbefugte Zugriffe zu sichern. Dies kann auf verschiedene Weise erreicht werden:

- Verlegung der Leitungen oder Kabelkanäle unter Putz,
- Verlegung der Leitungen in Stahlpanzerrohr,
- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluss von Verteilern und
- elektrische Überwachung von Verteilern und Kanälen.

In jedem Fall ist die Zahl der Stellen, an denen das verlegte Kabel zugänglich ist, auf ein Mindestmaß zu reduzieren und die Länge der vor unberechtigten Zugriff zu schützenden Verbindungen möglichst klein zu halten.

Besonders die Absicherung zentraler Trassen und Kabel der elektrischen Versorgung und der IT-Verkabelung muss im gesamten Kabelweg an die Gefährdungslage angepasst werden. In Bereichen wie Tiefgaragen und auch in Fluren, die als Transportwege genutzt werden, muss ein angemessener Schutz gegen zufällige mechanische Beschädigung und gegebenenfalls auch gegen Sabotagehandlungen durch eine stabile Ummantelung der Trasse oder des Kabels getroffen werden.

Wenn Verteiler verschlossen werden, sind Regelungen nötig, die Zutrittsrechte zum Verteiler, Verteilung der Schlüssel und Zugriffsmodalitäten festlegen. Darin ist unter anderem vorzugeben, was vor Änderungen an Kabeln oder Verteilern und nach der Ausführung solcher Arbeiten zu tun ist. Es muss sichergestellt sein, dass Änderungen abgestimmt und genehmigt werden und dass die Dokumentation nachgeführt wird.

Prüffragen:

- Ist die Anzahl der Stellen, an denen verlegte Kabel frei zugänglich sind, auf ein Mindestmaß reduziert?
- Sind in öffentlich zugänglichen Bereichen Kabel und Trassen gegen mechanische Beschädigungen und Sabotageversuche geschützt?
- Existieren Regelungen für den Zutritt und den Zugang zu verschlossenen Verteilern?
- Existieren Regelungen zur Ausführung von Arbeiten und Änderungen an der IT- und Elektro-Verkabelung (z. B..: Genehmigung, Abnahme, Fortführung der Dokumentation)?

# M 1.23 Abgeschlossene Türen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik, Mitarbeiter

Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen. Das Abschließen einzelner Büros ist insbesondere dann wichtig, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.

Auf das Verschließen der Türen kann verzichtet werden, wenn diese flurseitig über einen Blindknauf verfügen. Voraussetzung hierfür ist allerdings, dass die befugten Mitarbeiter ihren Schlüssel stets mit sich führen.

In manchen Fällen, z. B. in Großraumbüros, können Büros nicht abgeschlossen werden. Dann sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen ("Clear-Desk-Politik") und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank und PC(Schloss für Diskettenlaufwerk, Tastaturschloss), Telefon.

Auf das Verschließen der Türen kann verzichtet werden, wenn keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen und keine unbefugten Zugriffe auf die IT-Systeme im Raum (und die damit vernetzten IT-Systeme) möglich sind.

Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn Zugriffe nur nach erfolgreicher Authentisierung möglich sind, also z. B. ein passwortunterstützter Bildschirmschoner aktiviert ist. Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn das Booten des Rechners die Eingabe eines Passwortes verlangt. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren.

Es ist sinnvoll, wenn Pförtner oder Mitarbeiter der Haustechnik sporadisch überprüfen, ob die Türen nach Verlassen der Räume verschlossen wurden.

Prüffragen:

- Wird sporadisch überprüft, ob Büros beim Verlassen verschlossen werden?
- Werden Mitarbeiter angewiesen, bei Abwesenheit ihr Büro zu verschließen oder ihre Arbeitsunterlagen wegzuschließen?

# M 1.24 Vermeidung von wasserführenden Leitungen

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen wie z. B. Server befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes oder Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden schnell entdeckt werden kann. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen. Durch Sichtprüfungen müssen die vorhandenen Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft werden.

Es ist zu erwägen, wasserführende Leitung durch Wassermelder zu überwachen. Dafür können besondere Meldekabel unterhalb von Leitungen verlegt werden. Werden diese an eine Wassermeldeanlage angeschlossen, ist darüber eine schnelle und recht genaue Lokalisierung des Wasseraustritts möglich. Eine solche Anlage muss auf eine ständig besetzte Stelle aufgeschaltet werden, um in Verbindung mit entsprechenden Reaktionsplänen und einer aktuellen Dokumentation ein schnelles Eingreifen möglich zu machen. Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.

Als zusätzliche oder alternative Maßnahme empfiehlt sich eine selbsttätige Entwässerung (siehe M 1.14 *Selbsttätige Entwässerung*).

Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass in Gebäudeteilen mit IT-Systemen mit hohen Verfügbarkeitsanforderungen wasserführende Leitungen problematisch sind und was zu beachten ist. Es sollten Reaktionspläne vorhanden sein, in denen beschrieben ist, welche Maßnahmen bei Wasserleckagen zu ergreifen sind.

Prüffragen:

- Sind wasserführende Leitungen in IT-Räumen weitgehend vermieden worden?
- Sind Vorkehrungen getroffen worden, um im Notfall einen Wasseraustritt bei wasserführenden Leitungen frühzeitig erkennen zu können?
- Werden vorhandene Wasserleitungen an kritischen Stellen durch Sichtkontrollen regelmäßig auf ihre Dichtigkeit hin überprüft?
- Kann in Gebäudeteilen mit Hochverfügbarkeitsanforderungen ein Wasseraustritt bei wasserführenden Leitungen frühzeitig genau lokalisiert werden?

- Existieren für Gebäudeteile mit Hochverfügbarkeitsanforderungen Reaktionspläne, die zielgerichtete Handlungen bei Meldungen von Wasserleckagen vorgeben?

# M 1.25 Überspannungsschutz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

In jedem elektrisch leitenden Netz, gleichgültig ob es der Energieversorgung oder der Datenübertragung dient, kann es zu jeder Zeit zu Überspannungen kommen. Überwiegend werden solche Überspannungen durch andere Stromverbraucher im gleichen Versorgungsnetz verursacht. Überspannungen durch Blitz sind dagegen zwar sehr viel seltener, haben aber ein ungleich höheres Schadenspotential.

Nicht nur über die im Haus verlegten Leitungen, sondern auch über alle elektrisch leitenden Außenanbindungen wie Telefon-, Wasser- oder Gasleitungen können Überspannungen in ein Gebäude und die dort betriebene IT gelangen. Darüber hinaus können Überspannungen auch auf interne Leitungen eingekoppelt werden.

Die erforderlichen Maßnahmen zum Schutz von IT-Geräten sind unabhängig von der Ursache der Überspannung im wesentlichen die gleichen. Die seit Oktober 2006 gültige Norm DIN EN 62305 "Blitzschutz" (entspricht der Norm VDE 0185-305 und IEC 62305) ordnet den gesamten Blitz- und Überspannungsschutz neu. Mit einer Übergangszeit von 2 Jahren haben seit dem 01. Oktober 2008 alle vorher den Blitz- und Überspannungsschutz regelnden Normen ihre Gültigkeit verloren.

Auf Basis der neuen Norm DIN EN 62305 ist ein Überspannungsschutzkonzept zu erstellen.

Die DIN EN 62305 beschreibt in ihrem Teil 2 "Risiko-Management" erstmals allgemeinverbindlich den Weg zu einem risikoorientierten Blitz- und Überspannungsschutz. Im Teil 3 wird der "Schutz von baulichen Anlagen und Personen" behandelt, in Teil 4 "Elektrische und elektronische Systeme in baulichen Anlagen".

Im Überspannungsschutzkonzept sind natürlich auch Netzersatzanlagen (NEA) und unterbrechungsfreier Stromversorgungen (USVen) zu berücksichtigen. Obwohl USVen einen gewissen Schutz der angeschlossenen Geräte bewirken, sind sie keinesfalls als Überspannungsschutzeinrichtung zu betrachten, sondern einzig und allein als zu schützendes elektronisches Gerät.

An die Stelle der bisherigen drei Stufen Grob-, Mittel- und Feinschutz ist das Konzept der energetischen Koordination getreten. Nach der Norm ist eine energetische Koordination zwar nur dann zwingend erforderlich, wenn es einen äußeren Blitzschutz gibt. Im Sinne der Informationssicherheit sollte die energetische Koordination auch in Fällen ohne äußeren Blitzschutz berücksichtigt werden. Vereinfacht dargestellt bedeutet das folgendes:

- Hinter jedem Schutzelement (SPD - Surge Protecting Device) darf maximal so viel durch Überspannung verursachte Energie wirken, wie alle dahinter befindlichen elektrischen Einrichtungen (inklusive der folgenden SPDs) verkraften. Ein reines Leitungsnetz ist natürlich wesentlich robuster und verträgt deutlich mehr Energie als z. B. die Schnittstelle einer Netzwerkkarte in einem PC.
- Alle eingesetzten SPDs müssen sich miteinander vertragen. Der Ausgang eines vorderen SPDs und der Eingang des folgenden müssen aufeinander

angepasst sein. Der Nachweis der energetischen Koordination kann auf dreierlei Weise erbracht werden:

1. Einzelfallprüfung durch einen Fachprüfer,
2. Computersimulation mittels geeigneter Näherungsverfahren,
3. Einbau von SPDs aus einer Produktfamilie, für die der Hersteller den Nachweis erbringt.

Durch den Aufbau des Blitz- und Überspannungsschutzes werden wie Zwiebelschalen ineinander liegende Blitzschutzzonen (LPZ, Lightning Protection Zone) gebildet. Mit steigendem Schutz werden sie von außen nach innen mit LPZ 0, LPZ 1, LPZ 2 etc. bezeichnet. Dabei kann eine Zone nur dann gebildet werden, wenn es die nächst äußere gibt: So ist es nicht möglich, eine LPZ 2 zu realisieren, ohne auch die LPZ 1 zu haben.

Für einfache elektrische und elektromechanische Geräte ist die LPZ 1 meist ausreichend. Zum Schutz elektronischer Geräte (IT-Hardware, USV etc.) ist mindestens die LPZ 2 zu realisieren. Bei besonders empfindlichen Geräten, z. B. in der Medizin- oder Messtechnik kann durchaus die LPZ 3 erforderlich werden.

Hinweis:

Die LPZ (Blitzschutzzonen) sind nicht zu verwechseln mit den Schutzklassen des äußeren Blitzschutzsystems, das mit LPS (Lightning Protection System) bezeichnet wird.

Ob ein LPS erforderlich ist und mit welcher Schutzklasse, muss anhand der Risikobewertung (gemäß Teil 2 der DIN EN 62305) entscheiden werden. Der früher ausreichende Blick in eine Gebäudeliste genügt nicht mehr!

In vielen Fällen ist der gebäudeweite Aufbau einer LPZ 2 oder LPZ 3 gar nicht erforderlich. Während der Übergang von der LPZ 0 (das ist alles außerhalb eines Gebäudes, wo der Blitz also tatsächlich direkt einschlagen kann) zur LPZ 1 tatsächlich möglichst nah an der Gebäudehülle zu erfolgen hat, kann der Aufbau höherer LPZ an beliebiger Stelle und in beliebigem Umfang erfolgen. Wichtig ist dabei aber darauf zu achten, dass keine Leitung, die nur den Schutz der LPZ 1 genießt (z. B. Heizungsrohre) durch höherwertige LPZ hindurch läuft.

Die früher notwendigen Mindestleitungslängen zwischen den SPDs, also den Schutzelementen, und der unterschiedlichen LPZ sind heute nicht mehr zwingend. Es gibt SPDs, die in einem Bauteil den Übergang von der LPZ 0 direkt in die LPZ 2 realisieren.

Die Schutzwirkung eines SPDs reicht nach beiden Seiten (auf die kommende und die gehende Leitung) nur über eine bestimmte Kabelstrecke, die im einzelnen vom Hersteller zu benennen ist. Wird die Kabellänge abgehend überschritten, sind wiederholt SPDs einzubauen, um den Schutz aufrecht zu erhalten.

Nach DIN EN 62305 müssen Blitzschutzsysteme (LPS) abhängig von der Schutzklasse in Abständen von 1 bis 4 Jahren überprüft werden. Für die Überspannungsschutzeinrichtungen sieht die Norm keine ausdrücklichen Prüfintervalle vor. Im Sinne der Informationssicherheit sollten aber alle SPDs periodisch (mindestens einmal pro Jahr) und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt werden. Um diese Prüfung überhaupt durchführen zu können, sollten, sofern verfügbar, ausschließlich solche SPDs eingebaut

werden, die eine integrierte Defektanzeige oder (noch besser) eine Lebensdaueranzeige besitzen.

Neben dem Überspannungsschutz auf allen elektrisch leitenden Systemen müssen in Serverräumen und den Kerneinheiten eines Rechenzentrums Maßnahmen gegen elektrostatische Aufladung getroffen werden. Der Durchgangswiderstand der Bodenbeläge in solchen Räumen muss zwischen 10 und 100 Megaohm liegen. Die Einstufung nach DIN-Vorschrift 4102-1 "Brandverhalten von Baustoffen und Bauteilen" muss mindestens "B1 schwer entflammbar" erreichen. Dies gilt auch für einen Doppelboden oder Installationsboden.

Unabhängig von Umfang und Ausbau des Überspannungsschutzes ist zu beachten, dass ein umfassender Potentialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich ist! Die Mehrzahl der Schäden an IT-Geräten durch Überspannungen ist auf nicht konsequent umgesetzten Potentialausgleich zurückzuführen.

Prüffragen:

- Ist die energetische Koordination der Überspannungsschutzeinrichtungen nachgewiesen?
- Werden Blitz- und Überspannungsschutzeinrichtungen periodisch und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt?
- Ist ein durchgängiger Potentialausgleich realisiert?
- Wird bei Nachinstallationen darauf geachtet, dass der Potentialausgleich mitgeführt wird?

# M 1.26 Not-Aus-Schalter

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Bei Räumen, wie beispielsweise Server- oder Technikräumen, in denen elektrische Geräte in der Weise betrieben werden, dass z. B. durch deren Abwärme, durch hohe Gerätedichte oder durch Vorhandensein zusätzlicher Brandlasten ein erhöhtes Brandrisiko besteht, ist die Installation eines Not-Aus-Schalters zu erwägen. Da zur Betätigung des Not-Aus-Schalters Personal erforderlich ist, kommt er jedoch nur in solchen Bereichen in Frage, in denen ständig oder meistens Personen anwesend sind. In nicht oder nur sporadisch besetzten Bereichen ist eine Notabschaltung durch eine Brandfrühesterkennung wesentlich effektiver.

Mit Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen oder beginnenden Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.

Zu beachten ist, dass unterbrechungsfreie Stromversorgungen (USV) nach Ausschalten der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, dass auch die USV abgeschaltet und nicht nur von der externen Stromversorgung getrennt wird.

Der Not-Aus-Schalter sollte innerhalb des Raumes neben der Eingangstür (eventuell mit Lagehinweis außen an der Tür) oder außerhalb des Raumes neben der Tür angebracht werden. Dabei ist allerdings zu bedenken, dass dieser Not-Aus-Schalter auch ohne Gefahr versehentlich oder absichtlich betätigt werden kann. Daher ist der Not-Aus-Schalter mit einer Abdeckung gegen versehentliche Betätigung zu schützen.

Falls ein Not-Aus-Schalter von der Feuerwehr gefordert wird, kann dieser als Feuerwehr-Schlüsselschalter realisiert werden. Damit kann weitestgehend ausgeschlossen werden, dass er versehentlich oder unbefugt vorsätzlich betätigt wird.

**Negativbeispiel:**

Ein Serverraum einer mittleren Behörde wurde mit circa 10 Servern, 5 Laserdruckern und weiteren Geräten bestückt. Der Raum war nach den Gesichtspunkten des Einbruchschutzes mit entsprechenden Wänden, Fenstern und Türen ausgestattet. Ein Not-Aus-Schalter war nicht vorhanden. Es gab nur zwei Punkte, um diesen Raum gezielt stromlos schalten zu können: die Gebäudehauptverteilung im Keller oder die Verteilung des Raumes. Diese befand sich jedoch an der Wand, die der Eingangstür gegenüberlag, im Brandfalle nahezu unerreichbar.

Prüffragen:

- Ist für alle Technik- und IT-Räume überprüft worden, ob die Installation eines Not-Aus-Schalters sinnvoll ist?
- Ist bei der Installation eines Not-Aus-Schalters berücksichtigt, dass bei seiner Betätigung nicht nur die externe Energieversorgung, sondern auch die USV ausgeschaltet wird?

- Sind alle Not-Aus-Schalter gegen unbeabsichtigte Betätigung geschützt?

# M 1.27 Klimatisierung der Technik / in Technikräumen

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Um IT-Geräte dauerhaft zuverlässig zu betreiben, muss sichergestellt werden, dass die Umgebungsbedingungen innerhalb der von den Herstellern genannten Grenzen gehalten werden. Der in diesem Zusammenhang stets genutzte Begriff Klimatisierung umfasst die folgenden vier Bereiche der Luftkonditionierung:

- Lufttemperatur
- Luftfeuchtigkeit
- Frischluftanteil
- Schwebstoffbelastung

Die größte Bedeutung kommt der Einhaltung der Temperaturgrenzwerte zu. Nahezu die gesamte, der IT zugeführten elektrische Energie muss in Form von Wärmeenergie wieder aus dem Bereich abgeführt werden. Reicht der normale Luft- und Wärmeaustausch eines Raumes nicht aus, wird der Einbau einer zusätzlichen Kühlung erforderlich.

Neben der Temperatur muss oft auch die Luftfeuchtigkeit innerhalb bestimmter Grenzen gehalten werden, um elektrostatische Aufladungen (bei zu geringer Luftfeuchtigkeit) oder Oxidation und Schimmelbildung (bei zu hoher Luftfeuchtigkeit) zu vermeiden.

Der Schwebstoffgehalt der Luft wird meist schon durch die normalen Filter in Klimaanlagen hinreichend niedrig gehalten. Nur bei besonders stark belasteter Umgebungsluft oder spezieller Hardware ist hier eine weitergehende Filterung erforderlich. Um den erforderlichen Luftdurchsatz zu gewährleisten, müssen die Filter der Klimaanlage regelmäßig kontrolliert und rechtzeitig gewechselt werden.

Die vierte Komponente einer Klimatisierung, die Frischluftbeimischung, ist für den eigentlichen IT-Betrieb belanglos. In dem Umfang jedoch, in dem die klimatisierten Flächen als Arbeitsplatz ausgewiesen sind, muss entsprechend der einschlägigen Arbeitsstättenverordnungen eine Frischluftbeimischung erfolgen.

Um ihrem Hauptzweck dienen zu können, muss eine Klimatisierung ausreichen dimensioniert sein. Werden gewisse Ungleichmäßigkeiten im Energieverbrauch aller IT-Systeme berücksichtigt, kann in erster Näherung davon ausgegangen werden, dass jedes Kilo-Voltampere (kVA) elektrischer Energie mit 0,8 kW bis 1 kW Wärmelast zu Buche schlägt.

Die Kühlleistung sollte auf Basis einer exakten Wärmelastberechnung und mit großzügiger Leistungsreserve dimensioniert werden und einfach erweiterbar sein. Die tatsächliche Wärmelast in den gekühlten Bereichen muss in regelmäßigen Abständen (circa alle 12 bis 24 Monate) sowie bei größeren Umbauten der IT-Hardware durch Berechnung oder Messung überprüft werden. Durch Messungen zu verschiedenen Tageszeiten ist zu bestimmen, ob eine Luftbe- oder -entfeuchtung erforderlich ist.

Bei der Berechnung sollte angesichts steigender sommerlicher Höchsttemperaturen von bis zu 40°C Außentemperatur ausgegangen werden, was zu einem höheren Kühlaufwand führen kann. Andererseits lassen moderne IT-

Geräte auch Lufttemperaturen von 30°C und mehr zu, so dass eventuell der Kühlaufwand reduziert werden kann.

Die Spanne der sinnvoll einsetzbaren Technik reicht, abhängig von der abzuführenden Wärmemenge, von einfachen Splittgeräten (Kühleinheit im IT-Raum, Rückkühler draußen im Freien) bis zu hochkomplexen Klimaanlagen. Bei jeder Lösung ist zu prüfen, wie sich diese bei einer kurzfristigen Unterbrechung der Energieversorgung verhält. Während einfache Splittgeräte kurz abschalten, bei Wiederkehr der Stromversorgung aber problemlos weiterkühlen, sieht das bei großen Klimaanlagen meist ganz anders aus.

Klimaanlagen sind, wegen ihres enormen Eigenbedarfs an Strom, so gut wie niemals über USV versorgt. Daher gehen sie schon bei kleineren Unterbrechungen der Stromversorgung in Störung und schalten ab. Selbst wenn sie über NEA versorgt werden, und diese sehr rasch anläuft, steht die Kühlleistung keineswegs sofort wieder zur Verfügung. Aus kühltechnischen Gründen (unter anderem zum Schutz gegen Vereisung) wird eine Klimaanlage in mehreren Schritten angefahren. Bis zur Wiederherstellung der vollen Kühlleistung können so durchaus bis zu 10 oder gar 15 Minuten vergehen.

Während dieser Zeit wird die IT typischerweise über USV oder NEA weiter mit Energie versorgt und produziert damit Abwärme. Wenn diese Wärme aber nicht oder nur unzureichend abgeführt wird, kann es durch die Unterbrechung der Kühlung zu massiven Überhitzungsschäden bis hin zu Totalausfällen kommen.

Bei einem Ausfall der Klimatisierung kann je nach den Verhältnissen die Raumtemperatur ohne Kühlung schon nach 3 Minuten deutlich über 60°C liegen! Diese kurze Zeitspanne reicht meist noch nicht einmal aus, um die IT-Systeme geordnet herunter zu fahren. Es sind also in jedem Fall Überlegungen dahingehend anzustellen, wie lange eine Unterbrechung der Kühlung andauern kann, welche Folgen sie bewirken kann und welche Maßnahmen dagegen zu ergreifen sind.

Das übliche Mittel ist hier die Bildung eines Kältespeichers. Das kann sowohl ein eigens dafür installierter Eisspeicher sein, es kann aber auch ein eventuell vorhandener Löschwassertank genutzt werden. Mit der im Normalbetrieb überschüssigen Kühlleistung wird dieser Speicher heruntergekühlt und diese Kälte dann bei Bedarf genutzt. Damit ist es bei entsprechend konzipierter Klimaanlage möglich, nahezu unmittelbar nach Wiederkehr der Stromversorgung (gleichgültig ob vom EVU oder von der NEA) Kühlleistung zur Verfügung zu stellen.

In modernen Rechenzentren ist eine ständig steigende Energiedichte zu verzeichnen. Waren noch in den 1980er Jahren 500 W / m² (niedrig verdichtete Energie) üblich, sind heute 5 bis 10 kW / m² und mehr (hochverdichtete Energie) durchaus nichts Ungewöhnliches.

Bei hochverdichteter Energie reicht die herkömmliche freie Luftkühlung aus dem Doppelboden durch die Racks in den Raum nicht mehr aus. Hierfür sind inzwischen den Erfordernissen angepasste rackbezogen arbeitende Hochleistungskühlsysteme am Markt erhältlich.

Ein Klimagerät ist mindestens an Kältemittel- und Kondenswasserleitungen angeschlossen und, sofern die Luft befeuchtet wird, auch an eine Wasserleitung angeschlossen. Die Maßnahme M 1.24 *Vermeidung von wasserführenden Leitungen* ist also in jedem Fall zu beachten. So kann sichergestellt wer-

den, dass eine Leckage in Wärmetauschern über den Fortfall der Kühlung hinaus zu Schäden durch Feuchtigkeit führt.

Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen. Eine zusätzliche Überwachungseinrichtung für die Klimatisierung ist zu empfehlen.

Mitunter läuft das Regelungsverhalten einer Klimaanlage vornehmlich bei Temperatur und Luftfeuchte in Grenzbereiche, die man noch nicht als Fehler ansehen muss, die aber schon zu unerklärlichen Störungen der IT führen können. Solche Verschiebungen im Regelungsverhalten gehen oft mit Änderungen der IT-Auslastung, der Außentemperatur oder anderen zeitlich variablen Parametern einher. Um in solchen Fällen Klarheit über die Zusammenhänge und damit über möglich Ursachen erlangen zu können, ist es empfehlenswert, die beiden Parameter Temperatur und Feuchte im Verdachtsfall zumindest über eine Woche hinweg in 15-Minutenschritten aufzuzeichnen. Ist es nicht möglich, dies vollelektronisch durchzuführen, sollte mindestens ein konventioneller Thermo-Hygrograph mit 7-Tage-Trommel für den jederzeitigen Einsatz bereitgehalten werden.

Die Rückkühlwerke einer Klimaanlage sind bei Aufstellung im Freien gegen direkten Blitzeinschlag zu schützen. Bestehen hohe oder sehr hohe Anforderungen an die Verfügbarkeit, sollten die Rückkühlwerke nicht für jedermann zugänglich sein und gegebenenfalls gegen Sabotage materiell geschützt werden.

Die Klimatechnik ist bei der Notfallplanung (siehe Baustein B 1.3 *Notfallmanagement*) zu berücksichtigen.

Prüffragen:

- Werden regelmäßig Wärmelastberechnungen durchgeführt?
- Ist sichergestellt, dass die für die IT zulässigen Höchst- und Tiefstwerte für Temperatur und Luftfeuchtigkeit eingehalten werden, z. B. durch eine geeignete Kühlung?
- Ist die Kühlung in dem gleichen Maß verfügbar, wie es für die gekühlte IT gefordert wird?
- Werden eingesetzte Klimageräte regelmäßig gewartet?
- Können die Werte von Lufttemperatur und -feuchte bei Bedarf für eine Woche in maximal 15-Minuten-Schritten aufgezeichnet und dokumentiert werden?

# M 1.28 Lokale unterbrechungsfreie Stromversorgung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

Eine lokale unterbrechungsfreien Stromversorgung (USV) hat die Aufgabe, ein einzelnes IT-System oder sehr wenige IT-Geräte gegen die Folgen kurzfristiger Unterbrechungen der Stromversorgung zu schützen. Diese Zielsetzung ist meist in kleineren IT-Strukturen gegeben, die zudem nicht über eine Netzersatzanlage verfügen.

Für größere IT-Strukturen oder gar die Versorgung ganzer Gebäude werden vornehmlich zentrale USV-Systeme eingesetzt (siehe M 1.70 *Zentrale unterbrechungsfreie Stromversorgung*).

Gleichgültig, ob eine lokale USV als Beistellgerät oder als 19-Zoll-Einschub eingesetzt wird, ist ihre Leistung und ihre Stützzeit durch die Geräteeigenschaften festgeschrieben und können in der Regel nicht verändert werden.

Bei den heute verfügbaren lokalen USV-Geräten und den üblicherweise durch sie bereitzustellenden geringen Leistungen (im Bereich bis circa 1 kVA) können diese Stromausfälle bis zu 120 Minuten problemlos überbrücken (Stützzeit). Welche Stützzeit tatsächlich im konkreten Szenario erforderlich ist, hängt davon ab, wie lange einerseits das Herunterfahren der angeschlossenen Geräte (Shutdown) dauert und wie lange andererseits darauf gewartet werden soll, dass die Stromversorgung wieder anspringt (Wartezeit). Da ein großer Teil aller Stromausfälle nur wenige Minuten dauert, dürfte eine Wartezeit von 15 Minuten meistens ausreichen, um eine Versorgungsunterbrechung zu überbrücken. Dauert die Versorgungsunterbrechung länger als die Wartezeit, und muss das versorgte IT-System heruntergefahren werden, um Datenverluste zu vermeiden, sollte die gesamte Stützzeit nach der Formel

*Stützzeit = Wartezeit plus zweifache Shutdown-Zeit*

dimensioniert werden. Durch den zweifachen Ansatz der Shutdown-Zeit ist eine Sicherheitsreserve gegeben, falls das Herunterfahren länger dauert als angenommen. Bei jedem Austausch oder Ergänzung von IT-Geräten, die durch eine USV versorgt werden, muss erneut geprüft werden, ob die vorhandene Stützzeit ausreicht.

Drei USV-Arten sind zu unterscheiden:

- *VFD-USV*
  Bei der VFD-USV (VFD steht für Voltage and Frequency Dependent) werden die angeschlossenen Verbraucher im Normalbetrieb direkt aus dem Stromversorgungsnetz gespeist. Kleinere Störungen im Versorgungsnetz können also direkt bis zu den angeschlossenen Verbrauchern gelangen. Erst wenn dieses ausfällt, schaltet sich die VFD-USV selbsttätig zu und übernimmt die Versorgung. Dazu benötigt sie bis zu 10 ms (Umschaltlücke), was für manche IT-Geräte schon zu viel sein kann. Die VFD-USV wurde früher auch Offline-USV genannt.
- *VI-USV (Voltage Independent)*
  Hierbei wird die Versorgungsspannung bei kleineren Schwankungen nachgeregelt (VI steht für Voltage Independent), ohne dass die USV als solche die Versorgung der angeschlossenen Verbraucher komplett über-

nimmt. Die Frequenz am Ausgang einer VI-USV ist aber wie bei einer VFD-USV direkt vom Versorgungsnetz abhängig. Auch bei der VI-USV kann es bei der Umschaltung auf Batteriebetrieb zu einer Umschaltlücke kommen.

- *VFI-USV (Voltage and Frequency Independent)*
  Bei der VFI-USV (Voltage and Frequency Independent) gibt es im Normalfall keine direkte Verbindung zwischen USV-Eingang und -Ausgang. Die elektrische Energie wird eingangsseitig gleichgerichtet und in den Zwischenkreis gespeist. Von dort werden die Batterien im optimalen Ladezustand gehalten und der Wechselrichter versorgt. Dieser erzeugt die für die angeschlossenen Verbraucher erforderliche Wechselspannung.
  Da die Ausgangsenergie unabhängig vom Eingang permanent über den Wechselrichter erzeugt wird, gibt es hier keine Umschaltlücke. Die VFI-USV wurde früher als Online-USV bezeichnet.

Da die VFI-USV als einzige der drei Systeme wirklich unterbrechungsfrei arbeitet, sollt diesem immer der Vorzug geben werden. Unter Berücksichtigung weiterer, hier nicht behandelter Qualitätsmerkmale stellt eine USV, die nach DIN IEC 62040-3 gemäß VFI-SS-111 klassifiziert ist, das Optimum für die IT-Versorgung dar.

Eine USV gleich welcher Bauart stellt keinen Überspannungsschutz im eigentlichen Sinn dar. Im Gegenteil, eine USV muss wie alle anderen elektrischen Verbraucher durch geeignete Schutzmaßnahmen gegen Überspannungen geschützt werden (siehe hierzu M 1.25 *Überspannungsschutz*).

Um mögliche Probleme mit Schutzleiterströmen zu vermeiden, sollten IT-Geräte, die über eine lokale USV versorgt werden, nicht über geschirmte Leitungen (z. B. Druckerkabel) mit anderen IT-Geräten verbunden werden, die über einen anderen Weg versorgt werden.

Da die Batterien einer lokalen USV in den seltensten Fällen in ihrem optimalen Temperaturbereich (typischerweise um 20°C) betrieben werden, ist die Batterie-Lebensdauer bei lokalen USV-Geräten recht gering, im günstigsten Fall bis zu 5 Jahre, meist weniger. Während dieser Betriebszeit verlieren die Batterien permanent an Leistung, so dass eine lokale USV nach vielleicht zwei oder drei Jahren allenfalls noch die Hälfte der Stützzeit im Neuzustand bereitstellen kann. Um sicher zu stellen, dass die USV die erforderliche Stützzeit bereitstellt, sollte etwa einmal pro Jahr die tatsächliche Stützzeit ermittelt werden. Manche USV-Systeme verfügen dazu über eingebaute Prüfmechanismen. Ist das nicht der Fall, kann der Wert durch einen Lasttest ermittelt werden.

Wie bei allen anderen elektrischen Geräten ist auch bei USV-Systemen darauf zu achten, dass sie in den vom Hersteller genannten Temperaturbereichen betrieben werden. Dies ist bei der Dimensionierung der Kühlung zu berücksichtigen.

Um die Schutzwirkung einer USV aufrechtzuerhalten, muss sie regelmäßig gewartet werden. Dafür sind die vom Hersteller vorgesehenen Wartungsintervalle der USV einzuhalten.

Sofern eine lokale USV gemeinsam mit der darüber versorgten IT in einem Brandüberwachungsbereich steht und die Brandüberwachung eine Spannungsfreischaltung im Überwachungsbereich initiiert, muss unbedingt dafür gesorgt werden, dass auch die lokale USV komplett funktionslos geschaltet wird. Da bedeutet, dass nicht nur die Versorgung der USV (Eingang der USV) abgeschaltet wird. Auch der Wechselrichter (Ausgang der USV) muss abgeschaltet werden und die Batterien sind elektrisch von der USV zu trennen.

Prüffragen:

- Ist die USV hinsichtlich Leistung und Stützzeit ausreichend dimensioniert?
- Wird erneut geprüft, ob die Stützzeit ausreichend ist, wenn Änderungen an den Verbrauchern durchgeführt wurden?
- Existiert eine Regelung zum Abschalten und ordnungsgemäßen Herunterfahren von IT-Systemen bei Stromausfall, um Datenverluste zu vermeiden?
- Existiert für die USV-Geräte und die IT-Geräte ein Überspannungsschutz?
- Werden Verbindungen zwischen USV-geschützten IT-Geräten und anderweitig versorgten IT-Geräten über geschirmte Leitungen vermieden?
- Wurden bei der Dimensionierung der Kühlung bzw. der Raumtemperatur die vom Hersteller angegebenen Temperaturbereiche der USV-Geräte geprüft?
- Wird die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV regelmäßig getestet?
- Werden die Wartungsintervalle der USV eingehalten?
- Wird bei einer BMA-gesteuerten Spannungsfreischaltung der IT auch die lokale USV komplett funktionslos geschaltet?

# M 1.29 Geeignete Aufstellung eines IT-Systems

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Haustechnik

Bei der Aufstellung eines IT-Systems sollten verschiedene Voraussetzungen beachtet werden, die die Sicherheit, aber auch Lebensdauer und Zuverlässigkeit der Technik verbessern und die Ergonomie berücksichtigen (siehe auch M 3.9 *Ergonomischer Arbeitsplatz*). Einige seien hier genannt:

- Ein IT-System sollte möglichst so aufgestellt sein, dass nur die befugten Benutzer die Bildschirminhalte einsehen können. Bei einem Standort in der Nähe eines Fensters oder einer Tür können die Bildschirmaktivitäten eventuell von außerhalb beobachtet werden.
- Um zu verhindern, dass IT-Systeme manipuliert werden können, sollten sie so aufgestellt werden, dass nur Berechtigte Zutritt haben. IT-Systeme in Bereichen, in denen sich häufig Externe aufhalten, müssen mit zusätzlichen Maßnahmen gegen Diebstahl und Manipulationen geschützt werden.
- Ein IT-System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden, um eine Überhitzung zu vermeiden.
- Ein IT-System sollte nicht der direkten Sonneneinstrahlung ausgesetzt sein.
- Staub und Verschmutzungen sollten vermieden werden, da die mechanischen Bauteile (Laufwerke für Wechselmedien, mechanische Maus, Festplatten) beeinträchtigt werden können.
- Der Aufstellungsort sollte so gewählt sein, dass Schäden durch Außeneinwirkungen wie Überschwemmungen, Rohrbrüche, erhöhte Luftfeuchtigkeit, elektrische Interferenzen, elektromagnetische Einstrahlungen möglichst vermieden werden.

Alle Mitarbeiter sollten darüber informiert sein, welche Einwirkungen schädlich für IT-Systeme sind, damit sie mithelfen können, diese zu vermeiden. Dazu gehören z. B. Verschmutzungen durch Essen oder Getränke, Zigarettenrauch oder -asche, aber auch der falsche Einsatz von Reinigungsmitteln.

Je nach Umgebung kann es auch sinnvoll sein, zusätzliche Hilfsmittel zum Schutz der IT einzusetzen, wie z. B. Abdeckungen für Tastaturen oder Bildschirmfolien, die den seitlichen Einblick verhindern.

Prüffragen:

- Werden IT-Systeme so aufgestellt, dass nur befugte Benutzer die Bildschirminhalte einsehen können?
- Werden IT-Systeme so aufgestellt, dass Sie vor Manipulationen oder Diebstahl geschützt werden?
- Werden IT-Systeme so aufgestellt, dass Sie vor schädlichen Umwelteinflüssen geschützt werden?
- Sind die Benutzer über einen geeigneten Umgang mit IT-Systemen informiert?

# M 1.30 Absicherung der Datenträger mit TK-Gebührendaten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Auf den TK-Anlagen fallen während des Betriebes Gebührendaten an. Diese enthalten Informationen über:

- Zeit und Datum eines Gespräches,
- Quell- und Zielrufnummer sowie die
- Gesprächsdauer.

Gebührendaten sind personenbezogene Daten im Sinne der einschlägigen Bundes- und Landesdatenschutzgesetze. Hieraus folgt, dass auch nach den im folgenden vorgeschlagenen Maßnahmen des IT-Grundschutzes in jedem Fall eine gesonderte Betrachtung im Hinblick auf die Anforderungen der Datenschutzgesetze (z. B. aus der Anlage zum § 9 Bundesdatenschutzgesetz) durchzuführen ist.

Diese Daten können sowohl auf der Festplatte der TK-Anlage selbst als auch auf einem externen Gebührenrechner gespeichert werden. In vielen Fällen wird es eine Kombination beider Varianten geben. Die Rechner sind - wenn möglich - so zu schützen, dass nur Berechtigte auf die Gebührendaten zugreifen können. Dazu ist es erforderlich, den Gebührenrechner in einem besonders geschützten Raum (siehe Baustein B 2.4 *Serverraum*) aufzustellen. Für Einrichtungen, auf denen Gebührendaten gespeichert sind, müssen ferner die Maßnahmen M 1.23 *Abgeschlossene Türen*, M 2.5 *Aufgabenverteilung und Funktionstrennung*, M 2.6 *Vergabe von Zutrittsberechtigungen*, M 2.7 *Vergabe von Zugangsberechtigungen*, M 2.8 *Vergabe von Zugriffsrechten*, M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und M 2.17 *Zutrittsregelung und -kontrolle* realisiert werden.

Es ist zu dokumentieren, welche Personen in welchen Rollen Zugriff auf die Gebührendaten haben.

Prüffragen:

- Können nur Berechtigte auf Gebührendaten zugreifen und sind die Berechtigungen dokumentiert?
- Existiert eine Regelung zur Dokumentation, welche Personen in welchen Rollen Zugriff auf die Gebührendaten haben?

# M 1.31 Fernanzeige von Störungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

IT-Geräte und Supportgeräte, die keine oder nur seltene Bedienung durch eine Person erfordern, werden oft in ge- und verschlossenen Räumen untergebracht (z. B. Serverraum). Das führt dazu, dass Störungen, die sich in ihrem Frühstadium auf die IT noch nicht auswirken und einfach zu beheben sind, erst zu spät, meist durch ihre Auswirkungen auf die IT, entdeckt werden. Feuer, Funktionsstörungen einer USV oder der Ausfall eines Klimagerätes seien als Beispiele für solche "schleichenden" Gefährdungen angeführt.

Durch eine Fernanzeige ist es möglich, solche Störungen früher zu erkennen. Viele Geräte, auf die man sich verlassen muss, ohne sie ständig prüfen oder beobachten zu können, haben heute einen Anschluss für Störungsfernanzeigen. Die technischen Möglichkeiten reichen dabei von einfachen Kontakten, über die eine Warnlampe eingeschaltet werden kann, bis zu Rechnerschnittstellen mit dazugehörigem Softwarepaket für die gängigen Betriebssysteme. Über die Schnittstellen ist es oft sogar möglich, jederzeit den aktuellen Betriebszustand der angeschlossenen Geräte festzustellen und so Ausfällen rechtzeitig begegnen zu können.

Prüffragen:

- Existiert eine Fernanzeige von Störungen für schutzbedürftige IT-Geräte und Supportsysteme ohne unmittelbare Überwachung durch Personen?

# M 1.32 Geeignete Aufstellung von Druckern und Kopierern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um zu verhindern, dass Drucker manipuliert werden oder die Druckausgaben von Unbefugten kopiert oder mitgelesen werden können, sollten Drucker so aufgestellt werden, dass nur Berechtigte Zutritt haben. Zumindest sollten Drucker nicht in Bereichen aufgestellt werden, in denen sich häufig Externe aufhalten, insbesondere also nicht in der Nähe von Besprechungs-, Veranstaltungs- oder Schulungsräumen. Hiervon ausgenommen sind lediglich solche Drucker, die speziell für diese Bereiche vorgesehen sind, beispielsweise in Schulungsräumen.

Häufig stehen in Druckerräumen auch Kopierer. Aus Sicherheitssicht ist zu hinterfragen, ob hierdurch die Gefahr steigt, dass auf die Schnelle Kopien von herumliegenden Ausdrucken angefertigt werden. Andererseits zeigt die Erfahrung, dass selbst wenn Ausdrucke einfach mitgenommen werden, schimpfen erfahrungsgemäß die meisten Benutzer auf die Technik und denken nicht daran, dass der Ausdruck auch in böser Absicht von jemand anderem entfernt worden sein kann.

Um solche Probleme zu vermeiden, ist es sinnvoll, Drucker und Kopierer so aufzustellen, dass sie vom eigenen Personal gut eingesehen werden können. Also beispielsweise sollten Drucker und Kopierer nicht in eine düstere Ecke gestellt werden, sondern durch eine Glastür vom Sekretariat einsehbar sein.

Besser ist es, Drucker und Kopierer in einem geschlossenen Raum aufzustellen, zu dem nur Berechtigte Zutritt haben. Dies ist bei höherem Schutzbedarf zu empfehlen.

Noch besser ist es bei großen Druckern, wenn die Ausdrucke in nur für den jeweiligen Empfänger zugängliche Fächer durch eine vertrauenswürdige Person verteilt werden. Druckerausgaben müssen daher mit dem Namen des Empfängers gekennzeichnet sein. Dieses kann automatisch durch die Druckprogramme erfolgen. Bei sehr hohem Schutzbedarf sollte geprüft werden, ob diese Lösung geeignet ist.

Benutzer stellen häufig erst am Drucker fest, dass sie das falsche Dokument ausgedruckt haben oder dass noch eine Kleinigkeit geändert werden muss. Solche Ausdrucke werden dann häufig direkt beim Drucker in einen offenen Papierkorb geworfen. Da damit auch vertrauliche Dokumente in falsche Hände geraten können, empfiehlt es sich, einen Vernichter direkt neben Netz-Druckern aufzustellen. Ersatzweise müssen die Benutzer darauf hingewiesen werden, dass solche Dokumente nicht liegengelassen werden dürfen und anderweitig zu vernichten sind.

Prüffragen:

- Werden die Drucker, Kopierer und Multifunktionsgeräte so aufgestellt, dass nur befugte Benutzer hierzu Zutritt haben?
- Sind die Benutzer hinsichtlich eines Vertraulichkeitsverlustes durch ungeeigneten Umgang mit Ausdrucken sensibilisiert?

# M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Benutzer mobiler IT-Systeme wie Laptops, Mobiltelefone, Smartphones, Tablets oder PDAs müssen darauf achten, dass sie die Geräte auch außerhalb des Unternehmens sicher aufbewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

- Mobile Endgeräte sollten möglichst nicht unbeaufsichtigt bleiben.
- Wird ein Laptop, Smartphone, Tablet oder PDA in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein mobiles IT-System kann einen hohen Wert darstellen, der potenzielle Diebe anlockt, zumal tragbare IT-Systeme leicht veräußert werden können.
- Wird das mobile IT-System in fremden Büroräumen benutzt, so ist auch bei kurzzeitigem Verlassen des Raumes dieser zu verschließen oder das Gerät mitzunehmen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das mobile IT-System ausgeschaltet oder ein Zugriffsschutz aktiviert werden, um eine unerlaubte Nutzung zu verhindern.
- In Hotelräumen sollte das mobile IT-System nicht unbeaufsichtigt herumliegen. Wird das Gerät in einen Schrank eingeschlossen, hält das zumindest Gelegenheitsdiebe ab.
- Einige neuere Geräte können zusätzlich durch ein Schloss gesichert werden. Ein Dieb braucht dann Werkzeug, um es zu stehlen.
- Ein mobiles IT-System sollte nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku und das Display können anderenfalls beschädigt werden. Auch sollten weder IT-Geräte noch Akkus in geparkten Autos zurückgelassen werden, wenn die Außentemperatur extrem hoch oder niedrig ist.
- Ebenso sollten mobile Endgeräte vor Umwelteinflüssen geschützt werden, die diese schädigen können, also beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser.
- Mobile Endgeräte sind nicht unzerstörbar, daher sollten sie auch bei kürzeren Transportwegen möglichst stoßgeschützt befördert werden. Bei Laptops sollte beispielsweise das Gerät zusammengeklappt werden, da sowohl die Scharniere als auch der Bildschirm bei einem Sturz leicht beschädigt werden können. Grundsätzlich ist es immer empfehlenswert, für den Transport ein schützendes Behältnis zu verwenden. Beispielsweise haben viele Taschen und Rucksäcke für mobile Endgeräte eigene Fächer mit Polsterungen. Nach Möglichkeit sollten solche Taschen und Rucksäcke bereitgestellt und genutzt werden.

Es ist empfehlenswert, für die Benutzer mobiler IT-Systeme ein Merkblatt zu erstellen, das die wichtigsten Hinweise und Vorsichtsmaßnahmen zur geeigneten Aufbewahrung und zum sicheren Transport der Geräte enthält.

Prüffragen:

- Werden die Benutzer von tragbaren IT-Systemen auf die geeignete Aufbewahrung hingewiesen?

# M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Tragbare IT-Systeme wie Laptops, PDAs oder Mobiltelefone sind durch ihre Bauform immer beliebte Ziele für Diebstähle. Daher müssen sie auch dann sicher aufzubewahrt werden, wenn sie sich im vermeintlichen sicheren Büro befinden. Aus diesem Grund sind natürlich die in Baustein B 2.3 *Büroraum / Lokaler Arbeitsplatz* beschriebenen Maßnahmen zu beachten. Da ein tragbares IT-Systeme jedoch besonders leicht zu transportieren und zu verbergen ist, sollte das Gerät außerhalb der Nutzungszeiten weggeschlossen werden, also beispielsweise in einem Schrank oder Schreibtisch verschlossen werden oder angekettet werden.

Prüffragen:

- Werden tragbare IT-Systeme außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt?

# M 1.35 Sammelaufbewahrung tragbarer IT-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sind in einer Behörde bzw. einem Unternehmen eine Vielzahl von tragbaren IT-Systemen im (mobilen) Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Laptops in einer Sammelaufbewahrung (Pool) zu halten. Der dafür genutzte Raum sollte den Anforderungen, die in Baustein B 2.6 *Raum für technische Infrastruktur* beschriebenen werden, entsprechen.

Darüber hinaus ist die Stromversorgung der Laptops sicherzustellen, damit die Batterien dieser Geräte den sofortigen Einsatz erlauben. Zusätzlich müssen die Rücknahme und die Ausgabe von tragbaren IT-Systemen dokumentiert werden.

Prüffragen:

- Werden nicht im Einsatz befindliche tragbare IT-System vor einem unbefugtem Zugriff geschützt?

# M 1.36 Sichere Aufbewahrung der Datenträger vor und nach Versand

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer, Poststelle

Vor dem Versand eines Datenträgers ist zu gewährleisten, dass für den Zeitraum zwischen dem Speichern der Daten auf dem Datenträger und dem Transport ein ausreichender Zugriffsschutz besteht. Beschriebene Datenträger sollten so aufbewahrt werden, dass nur berechtigte Benutzer darauf zugreifen können, egal ob es sich um analoge oder digitale Datenträger handelt. Sind die zu übermittelnden Daten vertraulich, so müssen die Datenträger, auf denen sie sich befinden, bis zum Transport in entsprechenden Behältnissen (Schrank, Tresor) verschlossen aufbewahrt werden. Die für den Transport oder für die Zustellung Verantwortlichen (z. B. Poststelle) sind auf sachgerechte und sichere Aufbewahrung und Handhabung der Datenträger hinzuweisen.

Prüffragen:

- Werden beschriebene Datenträger so aufbewahrt, dass ein Zugriff nur für berechtigte Benutzer besteht?
- Sind alle beteiligten Mitarbeiter auf eine sachgerechte und sichere Aufbewahrung und Handhabung der Datenträger hingewiesen?

# M 1.37 Geeignete Aufstellung eines Faxgerätes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Benutzer, Fax-Verantwortlicher, Haustechnik

Ein Faxgerät sollte in einem Bereich installiert werden, der nicht öffentlich zugänglich ist. Eine Kontrolle des Zutritts zu diesem Bereich oder der Nutzung des Faxgerätes ist sinnvoll.

Sinnvollerweise kann dies durch die Aufstellung in einem ständig besetzten Raum (z. B. Geschäftszimmer, Sekretariat, Poststelle) erreicht werden. Außerhalb der Dienstzeiten oder bei Abwesenheit der berechtigten Benutzer sollte das Gerät eingeschlossen werden (Raum oder Schrank). Wichtig ist in diesem Zusammenhang, dass verhindert werden muss, dass eingegangene Faxsendungen von Unberechtigten eingesehen oder entnommen werden können (siehe M 2.48 *Festlegung berechtigter Faxbediener*).

Prüffragen:

- Sind alle Faxgeräte in einem nicht öffentlich zugänglichen Bereich installiert?
- Wird das Faxgerät außerhalb der Dienstzeiten oder bei Abwesenheit gegen unberechtigte Nutzung und Einsichtnahme eingegangener Faxsendungen geschützt?

# M 1.38 Geeignete Aufstellung eines Modems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Um den Missbrauch von Modems zu verhindern, muss sichergestellt werden, dass nur Berechtigte physikalischen Zugriff darauf haben. Missbrauch bedeutet hier zum einem die Durchführung unbefugter Datenübertragungen, durch die Kosten verursacht, Viren eingeschleppt oder Interna nach außen transferiert werden können, und zum anderen das unbefugte Ändern oder Auslesen der Modem-Konfiguration, wodurch Sicherheitslücken entstehen können.

Um den physikalischen Zugriff auf ein externes Modem oder ein PCMCIA-Modem abzusichern, ist z. B. bei einem ständig benutzten Modem das Abschließen des Raumes oder bei einem nur zeitweise benutzten Modem das sichere Aufbewahren des inaktiven Modems in einem Schrank zu gewährleisten. Die Maßnahmen des Bausteins B 2.3 *Büroraum / Lokaler Arbeitsplatz*, sind zu beachten.

Ein internes Modem besitzt aufgrund des Einbaus in ein IT-System einen höheren inhärenten physikalischen Zugriffsschutz. Hier würde es reichen, die Maßnahmen der Bausteine B 2.3 *Büroraum / Lokaler Arbeitsplatz* oder B 2.4 *Serverraum* zu beachten.

Wenn über ein Modem oder einen Modem-Pool Zugänge zum internen Netz geschaffen werden, ist das Baustein B 3.301 *Sicherheitsgateway (Firewall)* zu beachten. Über Modems darf kein Zugang zum internen Netz unter Umgehung einer bestehenden Firewall geschaffen werden.

Wenn mit einem Modem-Pool weitere externe Zugänge zu einem durch eine Firewall geschützten Netz geschaffen werden sollen, muss dieser auf der unsicheren Seite der Firewall aufgestellt werden (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway*). Der Modem-Pool sollte zusammen mit dem zugehörigen Server in einem gesicherten Serverraum aufgestellt sein. Die Maßnahmen des Bausteins B 2.4 *Serverraum* sind zu beachten.

Prüffragen:

- Werden externe Modems gegen physischen Zugriff gesichert?
- Ist sichergestellt, dass über Modems keine Zugänge zum internen Netz unter Umgehung einer bestehenden Firewall möglich sind?
- Zugang zu einem geschützten Netz über einen Modem-Pool: Befindet sich der Modem-Pool auf der unsicheren Seite der Firewall?

# M 1.39 Verhinderung von Ausgleichsströmen auf Schirmungen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

In den Normen für die IT-Infrastruktur (DIN EN 50173, DIN EN 50174-2 "Installation von Kommunikationsverkabelung") sind sowohl geschirmte als auch ungeschirmte Datenverkabelungen sowie die Anforderungen an die Erdung und Schirmung dieser Anlagen beschrieben. Bei der Verwendung von geschirmten Datenleitungen wird in den Normen zwischen technisch genutzten Räumen (z. B. Serverräumen und Rechenzentren) und Räumen mit einer allgemeinen IT-Nutzung unterschieden. Für die technisch genutzten Räume ist das beidseitige Auflegen der Schirmung und eine enge Vermaschung der Systeme und Komponenten vorgegeben. Für die allgemeine Nutzung der IT-Infrastruktur, wie die Etagenverkabelung in Gebäuden, wird in den Normen das einseitige Auflegen der Schirmung vorgegeben. Das beidseitige Auflegen ist optional.

Ist der Netzbetrieb durch Ausgleichsströme bei Verwendung geschirmter Leitungen gestört, sollte zunächst die Ursache analysiert werden. Durch die immer höher frequent werdenden Übertragungsverfahren der IT werden die Anlagen empfindlicher gegen hochfrequente Störungen. Zudem werden sie unter Umständen auch selbst zu hochfrequenten Störern für umgebende Anlagen und Systeme. Wenn Betriebsstörungen festgestellt werden, muss abhängig von den Bedingungen vor Ort der richtige Lösungsweg erarbeitet werden. Da hierfür viel Fachwissen erforderlich ist, ist es im Allgemeinen empfehlenswert, eine Fachfirma zur Begutachtung, Analyse und Erarbeitung einer Lösung zu beauftragen.

Um beispielsweise Ausgleichsströme auf den Schirmungen von Datenleitungen in Gebäuden zu verhindern, gibt es verschiedene Möglichkeiten:

Ausgleichsströme können im TN-C-System vermieden werden, indem nur solche IT-Geräte über geschirmte Datenleitungen miteinander verbunden werden, die an einer gemeinsamen Elektro-Verteilung angeschlossen sind. Bei jeder Erweiterung des Datennetzes ist diese Bedingung zu prüfen und sicherzustellen.

Als Maßnahme gegen Ausgleichsströme im TN-C- bzw. TN-CS-System wird häufig das ausschließlich einseitige Auflegen der Schirmung von Datenleitungen vorgeschlagen. Hinsichtlich der Ausgleichsströme ist dieses Vorgehen auch tatsächlich wirksam. Aus anderen Gründen sollte dieses Mittel aber als absolute Ausnahme äußerst restriktiv angewandt werden:

- Geschirmte Leitungen, deren Schirmung nur einseitig aufgelegt ist, werden deutlich stärker durch Störstrahlungen von außen beeinflusst. Gleichzeitig strahlen sie selbst stärker ab als ungeschirmte symmetrische Leitungen. Es muss also bei einseitiger Schirmauflegung mit mehr Störungen der Datenübertragung (z. B. der Verfügbarkeit bzw. Integrität) gerechnet werden, als bei allen anderen Kabeln.
  Die stärkere Aussendung auswertbarer Abstrahlung derartiger Leitungen kommt als Risiko bei der Betrachtung der Vertraulichkeit von Informationen hinzu.
- Selbst wenn alle technischen Nachteile der einseitigen Schirmauflegung hingenommen werden, bleibt das Problem der durchgängigen Umsetzung.

Es bedarf konsequenter Kontrolle bei allen Arbeiten am Datennetz, um sicher zu stellen, dass einseitig aufgelegte Schirmungen nicht doch irgendwann beidseitig aufgelegt werden. Solche Fehlauflegungen sind nachträglich nur mit sehr großem Aufwand zu finden.

Die aus Sicherheitssicht optimale Möglichkeit besteht darin, das Stromverteilnetz im gesamten Gebäude komplett als TN-S-System auszulegen. Dabei wird der PE- und der N-Leiter ab der Potentialausgleichsschiene (PAS) getrennt geführt. Einzelmaßnahmen an IT-Geräten sind dann in der Regel nicht mehr erforderlich. Zu beachten ist jedoch der Hinweis in M 1.28 *Lokale unterbrechungsfreie Stromversorgung* hinsichtlich der Bildung eines neuen TN-S-System für die angeschlossenen Geräte.

Um die Wirksamkeit des TN-S-Systems dauerhaft zu gewährleisten, muss sicher gestellt werden, dass die Verbindung zwischen PE- und N-Leiter an der PAS (Nullung) die einzige im gesamten Netz ist. Es kann aber in der Praxis nicht ausgeschlossen werden, dass beim Anschluss neuer Geräte oder bei Schaltarbeiten im Netz versehentlich eine weitere Verbindung zwischen PE- und N-Leiter geschaffen wird. Daher sollten Änderungen im Datennetz mit der Haustechnik abgestimmt werden. Zudem sollte ein TN-S-System in regelmäßigen Abständen auf korrekte Nullung hin geprüft werden. Das kann bei den ohnehin durchzuführenden Prüfungen des Stromversorgungsnetzes und bei Verdachtsmomenten (beispielsweise länger andauernde unspezifische Störungen im Datennetz) erfolgen. Als Mindestmaßnahme ist ein TN-S-System in der Niederspannungshauptverteilung (NSHV) mit einer permanenten Differenzstromüberwachung über die drei Phasen und den N-Leiter sowie einer weiteren permanenten Stromüberwachung über den Zentralen Erdungspunkt (ZEP) auszustatten. Alle weiteren der Qualitätssicherung des TN-S-System dienenden technischen Maßnahmen sind in M 1.74 *EMV-taugliche Stromversorgung* erläutert.

Die nachfolgenden Zeichnungen erläutern die Entstehung von Ausgleichsströmen auf Schirmungen und die möglichen Gegenmaßnahmen:

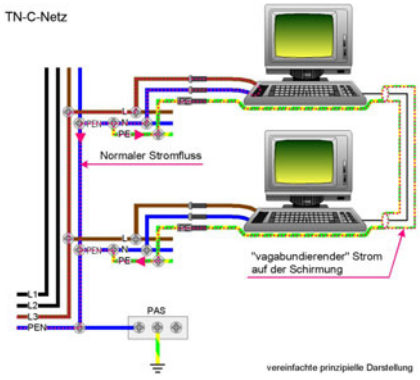



Abbildung 1: Entstehung von Ausgleichsströ-

men auf Schirmungen und die möglichen Gegenmaßnahmen bei einem TN-C-System

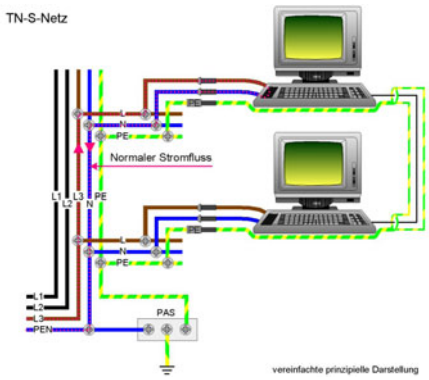



Abbildung 2: Entstehung von Ausgleichsströmen auf Schirmungen und die möglichen Gegenmaßnahmen bei einem TN-S-System

Prüffragen:

- Ist die Netzform zur Stromversorgung der IT-Komponenten so gewählt, dass Störungen durch Ausgleichsströme auf den Schirmungen von Datenleitungen verhindert werden?
- Einsatz der Netzform TN-C oder TN-CS: Werden Vorkehrungen für den Schutz der IT-Komponenten gegen Einstrahlung von außen, Abstrahlung durch die Leitung sowie zur Erkennung von Ausgleichsströmen getroffen?
- Ist durch geeignete Fachkunde und Kontrolle sichergestellt, dass die gewählte Netzform auch bei Änderungen am Stromversorgungsnetz erhalten bleibt?

# M 1.40 Geeignete Aufstellung von Schutzschränken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Innerer Dienst

Aufgrund des in der Regel hohen Gewichts von Schutzschränken muss vor der Aufstellung die Tragfähigkeit des Fußbodens am Aufstellungsort geprüft werden.

Schutzschränke, die aufgrund ihrer geringen Größe relativ einfach weggetragen werden könnten, sollten in der Wand oder im Boden verankert werden.

Eventuell vorhandene Herstellerhinweise zur geeigneten Aufstellung (z. B. freie Lüftungsöffnungen, Kabelführungen) sind zu berücksichtigen.

Prüffragen:

- Ist die Tragfähigkeit des Fußbodens vor der Aufstellung der Schutzschränke überprüft worden?
- Bei transportablen Schutzschränken: Sind die Schutzschränke am Aufstellungsort fest verankert?
- Sind Schutzschränke so aufgestellt, dass Lüftungsöffnungen frei bleiben und Kabelführungen ohne übergroße Spannungen oder Biegungen möglich sind?

# M 1.41 Schutz gegen elektromagnetische Einstrahlung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Beschaffer, Haustechnik

Werden in einem Schutzschrank informationstechnische Geräte untergebracht, so kann durch benachbarte Einrichtungen elektromagnetische Strahlung erzeugt werden, die die Funktion der Geräte beeinträchtigt (insbesondere in industriellen Produktionsbereichen). Durch Nachrüstung von Filtern und Türdichtungen kann die Einstrahlung innerhalb des Schutzschrankes reduziert werden. Gleichzeitig verhindern diese Maßnahmen auch eine Verbreitung von kompromittierender Abstrahlung der im Schrank befindlichen Geräte.

Prüffragen:

- Existieren ausreichende Schutzmaßnahmen gegen Störungen durch elektromagnetische Einstrahlung aus der Umgebung?

# M 1.42 Gesicherte Aufstellung von Novell Netware Servern

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 1.43 Gesicherte Aufstellung aktiver Netzkomponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Planer, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter Haustechnik

Um den manipulationssicheren Betrieb eines Netzes sicherzustellen, ist es erforderlich, aktive Netzkomponenten (wie Router, Switches, ISDN-Router) in einer gesicherten Umgebung zu betreiben. Dies kann entweder ein Serverraum sein (siehe Baustein B 2.4 *Serverraum*) oder, wenn kein separater Serverraum zur Verfügung steht, ein Serverschrank (siehe Baustein B 2.7 *Schutzschränke*). Unbefugte Personen dürfen zum Aufstellungsort der Geräte keinen unbeaufsichtigten Zugang erhalten.

Dabei sollte beachtet werden, dass Hersteller von Schutzschränken oft Standardschlösser einsetzen, so dass mit einem beliebigen Schlüssel des Schrankherstellers alle Schränke geöffnet werden können. Daher muss gegebenenfalls das serienmäßige Schloss eines Schutzschranks gegen ein individuelles Schloss ausgetauscht werden.

Außerdem sollten die Geräte so aufgestellt werden, dass sie vor elektromagnetischen oder magnetischen Feldern geschützt sind. Zusätzlich sollten sie mit Kontrollmechanismen ausgestattet sein, die eine Überschreitung der zulässigen Toleranzen bei Feuchtigkeit und Temperatur signalisieren.

Der Schutz von Routern und Switches vor unbefugtem Zugriff ist auch deswegen sehr wichtig, weil für viele Geräte Passwort-Recovery-Prozeduren für das Rücksetzen von Passwörtern bekannt sind, die zumeist den physikalischen Zugang zu den Geräten (Konsolenanschluss) voraussetzen. Oft verfügen die Geräte auch über PCMCIA-Slots: Entsprechende PCMCIA-Karten können für die allgemeine Speicherung von Daten verwendet werden und bieten eine komfortable Möglichkeit, Konfigurationsdaten auszutauschen, Updates vorzunehmen oder Image-Dateien einzuspielen.

Das serielle Konsolen-Interface (RS-232-Port) ermöglicht den Anschluss eines PC oder Terminals, um Administrations- oder Konfigurationsarbeiten durchzuführen. Das Passwort für den Zugriff auf die Konsole muss schriftlich an einem sicheren Ort hinterlegt sein (siehe auch M 2.22 *Hinterlegen des Passwortes*).

Zusätzlich muss den Gefahren durch Diebstahl, Vandalismus und unbefugtem Ausschalten des Geräts vorgebeugt werden.

Prüffragen:

- Werden Netzkomponenten wie Router und Switches in einer gesicherten Umgebung betrieben?
- Sind die Passwörter für den Zugriff auf die Konsolen der Netzkomponenten schriftlich an einem sicheren Ort hinterlegt?
- Sind Maßnahmen getroffen, um Gefahren durch Beeinträchtigungen der Einsatzumgebung (z. B. Feuchtigkeit, Temperatur), Diebstahl, Vandalismus und unbefugtem Ausschalten der Netzkomponenten vorzubeugen?

# M 1.44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

**Verantwortlich für Initiierung:** Personalrat/Betriebsrat, Vorgesetzte, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik, Mitarbeiter

Für den häuslichen Arbeitsplatz ist die Nutzung eines eigenen Arbeitszimmers wünschenswert. Zumindest sollte der häusliche Arbeitsplatz von der übrigen Wohnung durch eine abschließbare Tür abtrennbar sein, damit sich dort befindliche Unterlagen und IT-Systeme außerhalb der Bereiche befinden, in denen sich weitere Bewohner oder Besucher aufhalten. Bei spontanen Besuchen kann so der Arbeitsplatz kurzfristig verlassen und vor unbefugtem Zugriff geschützt werden.

Die Einrichtung sollte unter Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz ausgewählt werden.

Dies bedeutet unter anderem:

- ausreichend Platz für Möbel und Bildschirmarbeitsplatz,
- regelbare Raumtemperatur und ausreichende Lüftungsmöglichkeiten,
- Abschirmung gegenüber Lärmquellen,
- Tageslicht sowie ausreichend künstliche Beleuchtung,
- Sichtschutz des Monitors, falls er durch ein Fenster beobachtet werden könnte,
- Vermeidung von störenden Blendungen, Reflexen oder Spiegelungen am Arbeitsplatz und
- Anschlüsse für Telefon und Strom.

Die dienstlich genutzte IT sollte vom Arbeitgeber bereitgestellt werden, um Sicherheitsrichtlinien durchsetzen zu können. Nur dann kann z. B. per Dienstanweisung ausgeschlossen werden, dass die IT für private Zwecke benutzt wird.

Am häuslichen Arbeitsplatz müssen dieselben Vorschriften und Richtlinien bezüglich der Gestaltung des Arbeitsplatzes (z. B. Einrichtung eines Bildschirmarbeitsplatzes) und der Arbeitsumgebung beachtet werden wie in der Institution. Ein häuslicher Arbeitsplatz muss also für die jeweiligen Aufgaben ausreichend ausgestattet sein, d. h. es muss nicht nur geeignetes Mobiliar, sondern es sollten auch angemessene Schutzvorkehrungen wie beispielsweise abschließbare Schränke vorhanden sein.

Mitarbeiter mit einem häuslichen Arbeitsplatz sollten regelmäßig befragt werden, ob der Arbeitsplatz ihren gesundheitlichen und betrieblichen Ansprüchen genügt. Stichprobenhafte Besuche zur Überprüfung seitens der Institution können nach Absprache mit den Mitarbeitern durchgeführt werden.

Prüffragen:

- Kann der häusliche Arbeitsplatz von den übrigen Wohnbereichen getrennt werden?
- Sind an den häuslichen Arbeitsplätzen angemessene Arbeitsmittel und Möbel vorhanden?
- Können Unterlagen und IT-Systeme am häuslichen Arbeitsplatz vor unbefugtem Zugriff geschützt werden?

# M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Mitarbeiter

Dienstliche Unterlagen und Datenträger dürfen nur autorisierten Personen zugänglich sein. Dies ist auch außerhalb der offiziellen Bürogebäude, also z. B. an einem häuslichen oder einem mobilen Arbeitsplatz, zu beachten. Außerhalb der Nutzungszeit müssen sie so aufbewahrt werden, dass kein Unbefugter darauf zugreifen kann.

Alle Mitarbeiter sollten die Möglichkeit haben, an ihrem Büro-Arbeitsplatz wichtige und vor allem hochschutzbedürftige Datenträger und Dokumente wegzuschließen. Dazu können beispielsweise verschließbare Schreibtische, Rollcontainer oder Schränke genutzt werden. Die Mitarbeiter müssen darauf hingewiesen werden, dass schutzbedürftige Unterlagen und Datenträger verschlossen aufzubewahren sind.

Die Schlösser dieser Behältnisse müssen mindestens Angriffen mit einfach herzustellenden oder einfach zu erwerbenden Nachschließmitteln (Büroklammer, Dietrich, etc.) standhalten. Es sollten Möbelschlösser mit mindestens 4 Zuhaltungen und mindestens 1000 Schließvarianten eingesetzt werden. Zudem ist darauf zu achten, dass der Verschluss nicht durch einfaches Entfernen z. B. einer Rückwand leicht umgangen werden kann. Insgesamt sollte die Schutzwirkung des Behältnisses den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger entsprechen.

Auch an häuslichen Arbeitsplätzen müssen aus diesem Grund ausreichende verschließbare Behältnisse (Schreibtisch, Rollcontainer, Schrank oder Ähnliches) mit angemessener Schutzwirkung vorhanden sein.

Bei Arbeitsplätzen unterwegs sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert werden, also beispielsweise mit Diebstahlsicherungen versehen werden, in Schränke geschlossen werden oder andere, einfache Maßnahmen ergriffen werden. Außerdem ist es empfehlenswert, dienstliche Unterlagen und mobile IT-Systeme in einem verschließbaren Aktenkoffer zu transportieren.

Prüffragen:

- Werden dienstliche Unterlagen und Datenträger angemessen gesichert?
- Stehen an allen Büro-Arbeitsplätzen verschließbare Behältnisse in ausreichender Menge zur Verfügung, um Unterlagen und Datenträger sicher aufbewahren zu können?
- Sind die Mitarbeiter darauf hingewiesen worden, dass Unterlagen und Datenträger, die Informationen mit erhöhtem Schutzbedarf enthalten, verschlossen aufzubewahren sind?

# M 1.46 Einsatz von Diebstahl-Sicherungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen - z. B. geeignete Zutrittskontrolle zu den Arbeitsplätzen - nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahl-Sicherungen machen außerdem dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

### Verhindern einer "Cold Boot Attacke"

In Bereichen, die nicht ausreichend gegen unbefugten Zutritt geschützt sind, könnte beispielsweise durch eine "Cold Boot Attacke" der Arbeitsspeicher ausgelesen werden. Gleiches gilt für Systeme, die durch "Suspend to RAM" in einen Energiesparmodus versetzt wurden.

Bei einer Cold Boot Attacke werden die Speicherbausteine stark gekühlt, bevor das System ausgeschaltet wird. Der Speicherinhalt bleibt dadurch mehrere Minuten erhalten und kann währenddessen mit geeignetem Gerät ausgelesen werden.

Cold Boot Attacken können nur verhindert werden, wenn Angreifer keine Möglichkeit haben, ungestört auf den Arbeitsspeicher eines aktiven IT-Systems zuzugreifen. Ein Zugriffsschutz, wie ein physisch verriegeltes Computer-Gehäuse, erschwert es, ein IT-System unbefugt zu öffnen, um den Arbeitsspeicher zu kühlen und auszubauen, kann es aber nicht dauerhaft unterbinden. Daher sollte ein unbenutztes IT-System stets ausgeschaltet werden, wenn es in keinem zutrittsgeschützten Bereich steht.

### Arten von Diebstahl-Sicherungen

Mit Diebstahl-Sicherungen sollten je nach zu schützendem Objekt nicht nur das IT-System selber, sondern auch Monitor, Tastatur und anderes Zubehör ausgestattet werden.

Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einem Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. durch das Verbinden des IT-Systems mit einem Schreibtisch. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die das Öffnen des Gehäuses verhindern sollen, um dem Diebstahl von Teilen oder der Manipulation von sicherheitsrelevanten Einstellungen wie dem Entfernen von Sicherheitskarten vorzubeugen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt auf alle Gerätesicherungen einer Institution, Abteilung, etc. Dies hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber auch den Nachteil, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Dies hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Dies hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Notebooks - aber auch viele andere Geräte - haben einen kleinen Schlitz, welcher mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist. Diese kleine Öffnung (ca. 3 x 7 mm) befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, welche diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann nur eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt, das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen werden.

Für Geräte, die diese Öffnung nicht haben - oder diese nicht stark genug ist - gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungs-Alarm am Gerät selber auslösen, der potentielle Diebe dazu bringen soll, dass Gerät liegen zu lassen.

Bei Neuanschaffung von IT-Geräten sollte darauf geachtet werden, dass diese Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können, und dass die Gehäuse abschließbar sind.

Prüffragen:

- Gibt es Regelungen zur Beschaffung und zum Einsatz von Diebstahlsicherungen?

# M 1.47 Eigener Brandabschnitt

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Die Festlegung von Brandabschnitten ist für den Brandschutz eines Rechenzentrums von größter Wichtigkeit. Die Wirkung zuverlässiger Brand- und Rauchabschnitte hat sich bei vielen Großbränden eindrucksvoll bestätigt.

Die an Brandwände bzw. an die Größe der Brandabschnitte von Rechenzentren gestellten Anforderungen sollten über die in einschlägigen Normen, wie z. B. den Landesbauordnungen bzw. der DIN 4102 "Brandverhalten von Baustoffen und Bauteilen", gestellten Forderungen hinaus gehen.

Schutzziel für die Brandwand bzw. den Brandabschnitt sollte nicht nur der Personen- und Gebäudeschutz, sondern auch der Schutz des Inventars und dessen Verfügbarkeit sein. Somit ist nicht nur die Brandausbreitung durch Flammenwirkung und heiße Rauchgase, sondern auch Wärmestrahlung und Ausbreitung von kaltem Rauch zu verhindern.

Die nach DIN 4102 noch zulässige Wärmestrahlung kann für die Gebäudeeinrichtung, insbesondere im wärmeempfindlichen IT-Bereich, bereits vernichtende Wirkung haben. Aus diesen Gründen sollten mehrere Brand- und Rauchabschnitte im Bauvorhaben realisiert werden, die so groß wie nötig und so klein wie möglich sind.

Für ein Rechenzentrum ist zu prüfen, inwieweit weitere interne Brandabschnitte geschaffen werden sollten. Sollte ein eigener Brandabschnitt für die Kerneinheiten (IT-Räume, Datenträgerarchiv) erforderlich sein, so müssen Wände, Türen und auch notwendige Wand- und Deckendurchbrüche den F90-Anforderungen genügen.

Neben der baurechtlich erforderlichen Berücksichtigung der Norm DIN 4102 sollte für Rechenzentren, Serverräume und Datenträgerarchive die Einhaltung von Grenzwerten der maximalen relativen Luftfeuchte (aus der Norm EN 1047-2, Abschnitt 4.1, Tabelle 1) beachtet werden.

Wenn der Brandabschnitt des Rechenzentrums z. B. Büroeinheiten beherbergt, die in direktem betrieblichen Zusammenhang mit dem Rechenzentrum stehen, so sind innerhalb des Brandabschnitts F30-Wände und T30-Türen zwischen diesen Büros und dem Rechenzentrum-Kernbereich hinreichend. Die Büros sind dann in die Brandmeldeanlage mit einzubeziehen. Büroeinheiten ohne betrieblichen Bezug zum Rechenzentrum sind in anderen Brandabschnitten anzuordnen.

Es ist in der Planung und auch im Betrieb sicherzustellen, dass in solchen Räumen, die im Brandabschnitt des Rechenzentrums liegen, keine besonderen Brandlasten vorhanden sind.

Prüffragen:

- Sind die Räumlichkeiten in sinnvolle Brandabschnitte unterteilt?
- Erfüllen die Brandwände und die Brandabschnitte die Schutzziele sowohl für Personen- und Gebäudeschutz, als auch für den Schutz des Inventars?

# M 1.48 Brandmeldeanlage im Rechenzentrum

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

In einem Rechenzentrum ist, neben der Aufstellung einer speziell auf den IT-Bereich zugeschnittenen Brandschutzordnung sowie von Alarm- und Einsatzplänen, die Installation einer Brandmeldeanlage von größter Wichtigkeit.

Da mehr als 90 % aller Brandschäden in Rechenzentren durch Feuer im Umfeld verursacht werden, empfiehlt es sich, diese Bereiche in die Überwachung durch die Brandmeldeanlage zu integrieren. Zum Einsatz sollten Puls- bzw. Trendmelder (z. B. mit optischem Streulichtprinzip) kommen.

Für die Überwachung der IT-Bereiche ist mindestens dann, wenn ein sehr hoher Schutzbedarf in Bezug auf Verfügbarkeit festgestellt wird, zusätzlich zu den Meldern an Decke und gegebenenfalls im Doppelboden eine Anlage zur Brandfrühesterkennung (siehe M 1.54 *Brandfrühesterkennung / Löschtechnik* empfehlenswert.

Die Identifikation des auslösenden Melders muss möglich sein. Zur Lokalisierung des Brandherdes und der Brandausbreitung ist diese Identifikation der Brandmelder ein besonders wichtiges Hilfsmittel.

Eine empfehlenswerte Mindestkonfiguration einer Brandmeldeanlage in der Infrastruktur besteht aus

- Rauchmeldern an der Decke und im Doppelboden aller Räume der Elektroversorgung (Verteilungen, USV)
- Thermomaximal- oder Thermodifferenzmeldern in den Räumen der Netzersatzanlage
- Rauchmeldern an der Decke und im Doppelboden aller Räume der Klimatechnik
- Kanalmeldern in den Klimakanälen für Zuluft und Abluft
- Meldern in der Frischluftansaugung, mit automatischer Sperrung der Frischluft, wenn Störgrößen erkannt werden.

Alle Meldungen der Brandmeldeanlage und auch Störmeldungen sollten auf einer ständig besetzte Stelle, z. B. der Pförtnerloge, auflaufen.

Nach Möglichkeit sollte eine direkte Aufschaltung zur Berufsfeuerwehr erfolgen. Durch die Aufschaltebedingungen der Berufsfeuerwehr werden die weiteren Rahmenbedingungen zum Betrieb der BMA vorgegeben.

**Beispiel:**

Während einer Besprechung der Leitungsebene eines Rechenzentrums bemerkte ein Teilnehmer, der sich kurz in einem Nebenzimmer aufhielt, zufällig das Entstehen eines Großbrandes in einen nahegelegenen Chemiebetrieb. Sein Hinweis auf den Brand ermöglichte dem Leiter des Rechenzentrums, die Abschaltung der Frischluftzufuhr zu veranlassen. Nur wenige Minuten später wäre der rußige Brandrauch von der Ansaugung, die über keine Detektion verfügte, in die Rechnerräume befördert worden.

Die Funktionsfähigkeit aller Komponenten einer Brandmeldeanlage muss regelmäßig überprüft werden. Auch wenn die Instandhaltung der Brandmeldeanlage über eine Wartungsfirma erfolgt, sollten zwei Mitarbeiter mit den ele-

mentaren Grundfunktionen (zumindest mit allen Betriebszuständen und Statusmeldungen) der Anlage vertraut sein und als Ansprechpartner für die Wartungsfirma dienen.

Es sollten sporadisch einige der Melderlinien manuell auf ihre Funktionsfähigkeit getestet werden.

Prüffragen:

- Wird die Funktionsfähigkeit der Brandmeldeanlage regelmäßig überprüft?
- Gibt es eine speziell auf den IT-Bereich zugeschnittene Brandschutzordnung?

# M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Ein Rechenzentrum sollte in Gänze als geschlossener Sicherheitsbereich konzipiert sein. Bei der Planung eines Rechenzentrums oder der Auswahl geeigneter Räumlichkeiten sollten potentielle Gefährdungen durch Umgebungseinflüsse möglichst minimiert werden. So ist Gefahrenpotentialen wie Zutritt Unbefugter, Wassereinbrüchen bei Flachdächern oder in Kellerräumen genauso zu begegnen wie EMV-Störquellen, wie z. B. Mobilfunk-Sendeeinrichtungen oder Drehstromaggregaten.

Um eine Mischung zwischen der Grobtechnik (Energieversorgung, Klimatechnik) und der Feintechnik (Rechner) im Rechenzentrum zu vermeiden, sollten getrennte Raumeinheiten geplant werden. Die technische Infrastruktur des Rechenzentrums ist in separaten Räumen zu installieren.

Es ist zu beachten, dass der Schutzbedarf der aktiven Netzkomponenten, die an der Außenkommunikation beteiligt sind (wie Router und Switches), dem Schutzbedarf der Kernbereiche des Rechenzentrums entspricht. Die Sicherheitsmaßnahmen müssen also gleichwertig sein, die kommunikations- und nachrichtentechnischen Komponenten müssen genauso hoch abgesichert wie die internen Komponenten. Dies betrifft sowohl den materiellen Schutz, als auch Detektion, Meldung und Alarmierung.

Empfehlenswert ist es daher, die Gewerke für

- Nachrichtentechnik,
- Klimatisierung und Lüftung,
- Energieversorgung,
- Lager usw.

jeweils in einem eigenen Raum (optional auch eigenen Brandabschnitt) unterzubringen.

Bei der Planung sollte darauf geachtet werden, dass die Trassen der Versorgungsleitungen des Gebäudes, z. B. für Wasser oder Gas (siehe M 1.24 *Vermeidung von wasserführenden Leitungen*), nicht in unmittelbarer Nähe oder sogar durch sensible Bereiche des Rechenzentrums verlaufen.

Bei der Planung von Umbau- oder Neubaumaßnahmen für ein Rechenzentrum sollten die im Folgenden beschriebenen Parameter berücksichtigt werden.

In der Praxis hat sich für einen Rechnersaal ein Seitenverhältnis von 1:1 bis maximal 2:3 als günstig erwiesen. Diese Aufteilung erleichtert die strukturierte Anordnung von IT-Komponenten und deren Verkabelung im Rechenzentrum.

Sofern die baulichen Gegebenheiten es zulassen, ist die Installation eines Doppelbodens empfehlenswert. Seine Höhe ist abhängig von der technischen Ausstattung und Nutzung des Rechenzentrums. Wenn der Doppelboden zur Klimatisierung genutzt wird, sollte er mindestens 50 cm lichte Höhe haben. Bei hohen Wärmelasten von mehr als 1000 Watt pro Quadratmeter ist eine lichte Höhe von 90-100 cm empfehlenswert.

Bei der Bemaßung von IT-Räumen sind mindestens folgende Rahmenmaße empfehlenswert:

| **Objekt** | **Höhe** |
|---|---|
| Lichte Raumhöhe ab Doppelboden | 3,00 m |
| Stützenabstände | 6,00 m |
| Rohbaumaß Türenbreite | 1,10 m |
| Rohbaumaß Türenhöhe | 2,10 m |

Decken und Doppelböden sollten auf eine Traglast von mindestens 10 kN/m2 ausgelegt sein.

Der Doppelboden muss eine hohe Passgenauigkeit und ab einer Höhe von 20 cm eine Brandschutzqualität von F30 in geschlossenem Zustand aufweisen. Generell sollten die einschlägigen Sicherheitsrichtlinien beachtet werden, wie z. B. DIN EN 12825 Doppelböden.

**Hinweis:** Die Doppelböden und abgehängten Decken müssen mit dem IT-Raum abschließen. Es dürfen durch solche Konstruktionen keine ungesicherten Zugänge geschaffen werden.

Flure sollten mindestens eine Breite von 1,80 m aufweisen und mit rutschfesten, glatten Bodenbelägen, die höheren Transportlasten widerstehen, ausgelegt sein.

Aufzüge als vertikale Transportwege innerhalb des Rechenzentrums sollten eine Tragkraft von mindestens 1500 kg haben. Die lichten Kabineninnenmaße sollten mindestens 2,80 m in der Tiefe, 1,50 m in der Breite und 2,20 m in der Höhe betragen.

Der gesamte Sicherheitsbereich Rechenzentrum sollte möglichst nur eine oder zwei Zugangstüren und keine Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen (siehe auch M 1.10 *Sichere Türen und Fenster*). Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden (siehe auch M 1.73 *Schutz eines Rechenzentrums gegen unbefugten Zutritt*).

Ein angemessener baulicher und technischer Einbruchsschutz ist für ein Rechenzentrum unabdingbar. Weitere Empfehlungen hierzu sind in Maßnahme M 1.19 *Einbruchsschutz* aufgeführt.

Ein Rechenzentrum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und wichtiger noch für nur zeitweilig Beschäftigte, z. B. zu Wartungsarbeiten im Rechenzentrum tätige, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.

Es sollte verboten werden, in ein Rechenzentrum tragbare IT-Systeme, Mobiltelefone oder Kameras mitzubringen, wenn diese nicht unter der Kontrolle der jeweiligen Institution stehen. Generell sollte der Betrieb von Mobiltelefonen in Rechenzentren untersagt werden, da diese den Betrieb der IT-Systeme erheblich stören können. Ausnahmen hiervon müssen abgestimmt sein (siehe M 2.188 *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung*).

Für die in Rechenzentren betriebenen IT-Komponenten wird in vielen Fällen ein hohes Maß an Verfügbarkeit gefordert. Diesen Anforderungen kann durch redundante Auslegung der infrastrukturellen und technischen Einrichtungen Rechnung getragen werden (siehe Maßnahme M 1.52 *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur*).

Prüffragen:

- Gibt es technische und organisatorische Vorgaben für das Rechenzentrum?
- Ist das Rechenzentrum als geschlossener Sicherheitsbereich konzipiert worden?
- Ist der Zutritt zu Technikräumen und Räumen mit IT-Komponenten jeweils angemessen geregelt?
- Wurde bei der Planung auf eine ausreichende Trennung der Grob- und Feintechnik geachtet?

# M 1.50 Rauchschutz

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Rauch stellt bei Bränden die größte Personengefährdung dar. Mehr als 90 % der Brandtoten sind durch Raucheinwirkungen (Vergiftungen) zu beklagen. Aber auch die IT-Hardware kann durch Rauch erheblich in Mitleidenschaft gezogen werden. Daher ist auf einen umfassenden Rauchschutz Wert zu legen.

Die folgenden Empfehlungen sollten zum Rauchschutz berücksichtigt werden:

- Brandschutztüren sollten Rauchschutzqualität aufweisen.
- Rauchschutztüren in Fluren sollten durch Rauchschalter gesteuert werden. Solche Türen können immer offen stehen, da sie bei Rauchdetektion selbsttätig schließen.
- Die Lüftungsanlage bzw. die Klimaanlage sollte eine Entrauchung von IT-Räumen gestatten.
  In Klimakanälen (Zu- und Abluft) sollten Kanalmelder installiert sein.

In der Frischluftansaugung sollten Melder installiert sein, die diese automatisch sperren, wenn Störgrößen (Rauch) erkannt werden.

Nach Installations- und Umbauarbeiten ist sicherzustellen, dass Rauch-Schottungsmaßnahmen wirksam geblieben sind oder wieder hergestellt wurden.

Die Mitarbeiter müssen unterrichtet werden, welche Warnsignale die Rauchschutz-Komponenten haben und wie sie darauf zu reagieren haben.

Die Funktionsfähigkeit aller Rauchschutz-Komponenten muss regelmäßig überprüft werden. Dazu gehört es auch, zu überprüfen, ob Durchbrüche zur Durchführung von Verkabelungen im Doppelboden und in abgehängten Decken wirksam geschottet wurden.

Prüffragen:

- Wird die Funktionsfähigkeit der Rauchschutz-Komponenten regelmäßig überprüft?
- Wird der bauliche Rauchschutz nach Installations- und Umbauarbeiten direkt mit überprüft?

# M 1.51 Brandlastreduzierung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Leiter IT, Planer

Hohe Brandlasten entstehen z. B. durch die Konzentration von IT-Systemen, falsche Auswahl von Baumaterialien, leicht brennbare Büroausstattung und große Papiermengen. In vielen Fällen können solche Brandlasten auf einfache Weise vermieden werden.

Bei Rechenzentren - ebenso wie bei anderen Gebäuden - sollte bereits in der Planungsphase die Reduzierung unnötiger Brandlasten berücksichtigt werden. Nicht brennbare Materialien sind für den Ausbau zu bevorzugen (Baustoffklasse A).

Um den sicheren Betrieb unter Gesichtspunkten des Brandschutzes zu gewährleisten und Grenzwerte nicht zu überschreiten, sollte schon in der Planungsphase von Gebäuden eine überschlägige Berechnung der späteren Brandlasten erfolgen. Dabei sind die Brandklassen der Einrichtungen bzw. der Baustoffklassen der Materialien zu berücksichtigen. Dadurch werden später Schwierigkeiten bei der brandschutztechnischen Abnahme durch Bauaufsichtsbehörden und Feuerwehr vermieden.

Auch im laufenden Betrieb muss dafür gesorgt werden, dass Brandlasten reduziert werden. Unnötige Brandlasten sind zeitnah zu beseitigen. Beispielsweise ist im laufenden Rechenzentrums-Betrieb dafür Sorge zu tragen, dass Brandlasten im Doppelboden in Form von nicht mehr benötigten Kabeln entfernt werden. Aus Büroräumen sollten nicht mehr benötigte Akten entfernt und in speziell dafür vorgesehenen Archiven gelagert werden.

Eine der häufigsten Beispiele für unnötige Brandlasten in Räumen, die für die IT genutzt werden, ist Verpackungsmaterial, beispielsweise Pappe oder Styropor. Aus den IT-Räumen ist Verpackungsmaterial umgehend zu entfernen und in dafür vorgesehene Lagerräume zu transportieren, wenn es noch benötigt wird.

Die regelmäßige Entsorgung von Müll, vor allem von Altpapier und von Verpackungsabfällen, ist aktiver Brandschutz.

Prüffragen:

- Wird regelmäßig überprüft, ob sich Brandlasten in den genutzten Räumlichkeiten anhäufen?
- Werden unnötige Brandlasten zeitnah beseitigt?

# M 1.52 Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Das bewährteste Mittel zur Sicherstellung der Verfügbarkeit technischer Einrichtungen ist die Redundanz. Redundanz bedeutet, von etwas mehr zu haben, als für die eigentliche Aufgabenstellung erforderlich ist (aus dem Lateinischen: "*redundare*", im Überfluss vorhanden sein"). Im Bereich der IT bedeutet Redundanz damit auch das Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems. Damit wird sofort das Hauptproblem von Redundanz sichtbar: Um Redundanz zu haben, müssen Überkapazitäten geschaffen werden.

Die Modularität beschreibt, ob eine erforderliche technische Leistung durch eine große oder mehrere kleinere Einheiten zur Verfügung gestellt wird. Durch geschickte Nutzung der Modularität kann die erforderliche Überkapazität bei der Redundanz deutlich reduziert werden.

Keine noch so weitsichtige Planung kann so gut sein, dass es nicht nach einiger Zeit erforderlich ist, vorhandene technische Systeme einem geändertem, meist gestiegenem Leistungsbedarf anzupassen. Je einfacher ein System durch simples Hinzufügen zusätzlich Einheiten erweiterbar ist, desto besser ist es skalierbar. Auch bei der Skalierbarkeit kann sich die Modularität günstig auswirken.

Die einfachste Redundanz ist die (N+1)-Redundanz. Bei ihr wird der erforderlichen Zahl von Einheiten (N, typisch ist N=1) eine weitere hinzugestellt. Fällt dabei die ursprünglich erforderliche Einheit aus, übernimmt die zusätzliche deren Funktion. Diese Redundanz bietet ausreichenden Schutz gegen eine Betriebsstörung der technischen Einrichtung selbst. Die (N+1)-Redundanz wird daher auch "Betriebsredundanz" genannt.

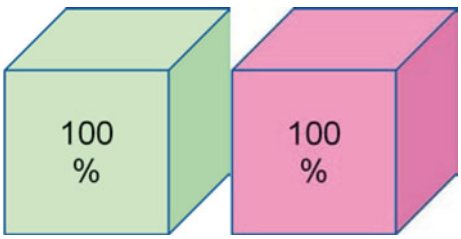


Abbildung 1: (N+1)-Redundanz mit (N=1)

Befindet sich jedoch eine der beiden Einheiten in Wartung und ist damit nicht betriebsbereit, ist keine Redundanz mehr vorhanden. Zudem ist schon für diese einfache Betriebsredundanz bei diesem Modell eine Überkapazität von 100 % erforderlich.

Soll die Redundanz auch während einer Wartung gewährleistet sein, ist eine (N+2)-Redundanz aufzubauen. Dabei werden dem Wirksystem (N=1) zwei zusätzliche Systeme zur Seite gestellt.

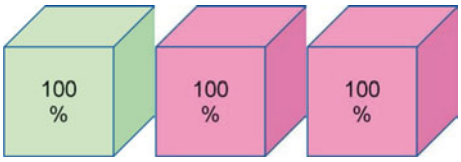



Abbildung 2: (N+2)-Redundanz mit (N=1)

Zwar ist nun selbst bei wartungsbedingtem Ausfall eines der drei Systeme immer noch eine Redundanz gegeben. Dafür ist aber eine Überkapazität von 200 % erforderlich. Solche Lösungen stoßen daher rasch an räumliche und finanzielle Grenzen.

Hier schafft die Modularität sehr gut Abhilfe. Wird z. B. statt des Wertes 1 der Wert 2 für N gewählt, stellt sich der Aufbau einer (N+2)-Redundanz schon deutlich günstiger dar.

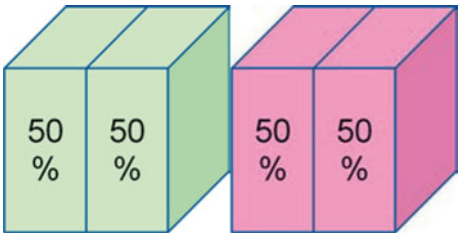



Abbildung 3: (N+2)-Redundanz mit (N=2)

Bei gleicher Redundanzwirkung (Betriebs- und Wartungsredundanz) reduziert sich die Überkapazität von 200 % auf 100 %. Wird die Modularität z. B. auf (N=4) erweitert, sieht das Bild noch günstiger aus:


Abbildung 4: (N+2)-Redundanz mit (N=4)

Zur Deckung der Grundlast stehen 4 Einheiten für jeweils 25 % der erforderlichen Leistung zur Verfügung. Weitere zwei 25 %-Einheiten bilden die Betriebs- und Wartungsredundanz. Die Überkapazität beträgt nur mehr 50 %.

Je höher der Wert für N getrieben wird, desto geringer wird die Überkapazität. Dass dieser Weg nicht endlos beschritten werden kann, ist klar. Zwar sinken durch die Modularität die Kosten für die Überkapazität. Gleichzeitig steigen aber die Kosten für die Unterbringung der Einheiten. Es ist erforderlich, alle Einheiten (im letzten Beispiel sind das schon 6) so unterzubringen und zu versorgen, dass durch ein externes Ereignis keinesfalls alle Einheiten zugleich betroffen sind.

Die Modularität enthält zugleich automatisch den Vorteil der Skalierbarkeit. Sobald der Leistungsbedarf steigt, kann den 4 Einheiten zu 25 % eine weitere kleine hinzugefügt werden. Bei der (N=1) Variante wäre eine Verdopplung des Erstsystems erforderlich, um das Redundanz-Prinzip aufrecht zu erhalten.

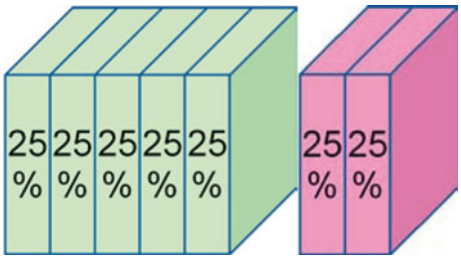



Abbildung 5: Einfache Skalierbarkeit

Die Modularität hat als weiteren Vorteil, dass die Restkapazität beim Ausfall von mehr als 2 Einheiten größer ist.

Bei einer (N+2)-Redundanz ist gewährleistet, dass beim Ausfall von zwei Einheiten die Restkapazität mit 100 % ausreicht, um den Betrieb normal fortzuführen. Fällt bei (N+2) mit (N=1) tatsächlich eine dritte Einheit aus, ist die Restkapazität gleich Null. Wird N hingegen mit 4 festgelegt und fallen von den nun bei (N+2)-Redundanz vorhandenen 6 Einheiten tatsächlich 3 aus, steht immerhin noch eine Restkapazität von 75 % zur Verfügung. Bei entsprechendem Lastmanagement kann damit noch ein recht störungsfreier Betrieb aufrecht erhalten werden.

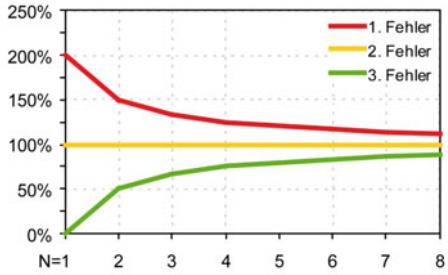



Abbildung 6: Darstellung der Restkapazität bei (N+2)-Redundanz mit steigendem Wert für N

Da häufig die vorhandenen Ressourcen begrenzt sind, ist es nicht immer möglich, zur Erlangung einer Betriebs- und Wartungsredundanz tatsächlich 2 zusätzliche Einheiten zu installieren. Da Wartungsfälle in der Regel mit ausreichendem Vorlauf planbar sind, kann die zweite Einheit im Bedarfsfall auch als mobile Einheit temporär angeschlossen werden.

Eine solche mobile Einheit kann in der Institution selber vorrätig gehalten oder über einen externen Dienstleister angemietet werden. Hierzu sind entsprechende SLAs mit dem Dienstleister zu vereinbaren und es müssen die erforderlichen Anschlusspunkte vorbereitet sein.

**Beispiele:**

- Beim Einsatz von Klimaanlagen sollte ausreichend Redundanz vorgehalten werden. Werden von einer Komponente 6 Stück benötigt, so sollten 7 beschafft werden. Damit können Lastspitzen, z. B. in heißen Sommern abgefangen werden und auch bei Ausfall eines Gerätes oder bei Wartungsarbeiten bleibt die Verfügbarkeit der Klimatisierung insgesamt erhalten.
- Auch für Kommunikationsverbindungen sollte geprüft werden, in welchen Bereichen Redundanzen vorgehalten werden müssen (siehe auch M 6.18 *Redundante Leitungsführung*). Dies gilt um so mehr, wenn sich zentrale Netzknoten oder zentrale aktive Komponenten in unkontrollierten Bereichen befinden.

- In einem Rechenzentrum ist die Stromversorgung redundant auszulegen. Empfehlungen hierzu finden sich in M 1.56 *Netzersatzanlage*. Falls sich die sekundäre Stromversorgung nicht in einem angrenzenden Brandabschnitt befindet, sollte über eine redundante Verkabelung der Stromversorgung nachgedacht werden.

Prüffragen:

- Ist durch Lastermittlung sichergestellt, dass auch bei ungünstigen Bedingungen der IT-Betrieb nach Wegfall redundanter Systeme unbeeinträchtigt bleibt?

# M 1.53 Videoüberwachung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Die Maßnahmen zur Außenhautsicherung (siehe M 1.55 Perimeterschutz) und Zutrittskontrolle können durch den Einsatz von Videotechnik ergänzt werden. Videoüberwachungsanlagen, ob eigenständig oder ergänzend zu anderen Sicherheitstechniken, werden zur Erreichung folgender Schutzziele eingesetzt:

- Abschreckung
- Fassadenüberwachung
- Identifizierung
- Überwachung
- Alarmierung
- Erkennung und Lokalisierung von Gefahren
- Schadenverhütung
- Dokumentation und Auswertung von Regelabweichungen

Bei der Planung einer Videoüberwachung ist auf eine konsistente Einbettung in das gesamte Sicherheitskonzept. zu achten. Dies gilt umso mehr, wenn die Überwachungsterminals weit vom zu schützenden Bereich entfernt sind. Eine Videoüberwachung ohne Auswertungs- und Alarmierungsmechanismen macht außer zur Abschreckung keinen Sinn. Die benötigten zentralen Technikkomponenten sind in geeigneter Umgebung aufzustellen und zu schützen. Sie sollten, falls vorhanden, an eine zuverlässige Stromversorgung mit USV-Pufferung und Netzersatzanlage angeschlossen werden. Die Funktionsfähigkeit der Videoüberwachungsanlage sollte regelmäßig überprüft werden.

Videoüberwachung kann eine sehr wirksame Unterstützung eines Pförtnerdienstes (siehe M 1.17 *Pförtnerdienst*) sein. Eine Vielzahl von Abläufen lässt sich durch Einsatz geeigneter Kameratechnik von der Pforte aus überwachen und auch steuern:

- Kameras (meist Schwenk-/Neige-Zoomkameras) können zur Verifikation von Alarmzuständen anderer Systeme (z. B. Einbruchmeldeanlage) genutzt werden. So lässt sich eine Alarmmeldung beurteilen, ohne den Pförtnerplatz verlassen zu müssen.
- Kameras können zur Überprüfung einer vorgegeben Identität (Gesichtserkennung, Kennzeichenerkennung) dienen. Auf diese Weise können abgesetzte Zugänge oder Einfahrten von der zentralen Pforte aus überwacht und Türen oder Toren von dort aus für Berechtigte geöffnet werden.
- Kameras können zur Überprüfung der Personenvereinzelung in Großraumschleusen bei Zutritt zu kritischen Bereichen wie Rechenzentren dienen.
- Kameras können zur Erkennung von Bewegung oder Änderung einer Situation genutzt werden. Das Kamerabild wird durch eine Detektionssensorik nur aufgeschaltet, wenn die Lage im überwachten Bereich Aufmerksamkeit des Benutzers der Videoanlage erfordert.

Bei der Planung bzw. Installation einer Videoüberwachung sollte der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat hinzugezogen werden.

Prüffragen:

- Ist die Videoüberwachung konsistent in das Sicherheitskonzept eingebettet?
- Wird die Funktionsfähigkeit der Videoüberwachungsanlage regelmäßig überprüft?

# M 1.54 Brandfrühesterkennung / Löschtechnik

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Um Brände in IT-Anlagen bereits in einem sehr frühen Stadium erkennen zu können, ist der Einsatz einer Anlage zur Brandfrühesterkennung zu erwägen. Typischerweise detektieren solche Anlagen in Form eines Rauchansaug- und Analysesystems im Umluftstrom der Klimatisierung bereits wenige und feinste Rauchpartikel.

Auch für die Überwachung von einzelnen IT-Systemen kann eine objektbezogene Überwachung durch sogenannte Multidetektoren vorgenommen werden. In Ergänzung der konventionellen Brandmeldetechnik (geometrische Raumüberwachung) stellt die Objektüberwachung (also die Überwachung innerhalb einzelner IT-Komponenten) eine zusätzliche Melderebene dar. Diese Multidetektoren können sowohl für eine objektbezogene Löschung als auch für die Abschaltung der Stützenergie des betroffenen Gerätes herangezogen werden.

Bei entstehenden Bränden kann bereits das Wegschalten der elektrischen Energie ausreichend sein, um den Brand zu verzögern oder zu beenden.

Wenn eine zusätzliche Löschung als notwendig anzusehen ist, bietet es sich aus Kosten- und Personenschutz-Gründen an, nur einzelne Objekte (z. B. 19 Zoll Schränke) mit Löschgasen individuell abzusichern. Die Objektschutzanlagen sollten sich an einschlägigen Standards wie der VdS-Richtlinie 2304 bezüglich Planung, Brandmeldung, Löschung orientieren sowie an den Einbauhinweisen der Hersteller und deren Vorgaben für den Betrieb und die Instandhaltung.

Für die Raumüberwachung im IT-Bereich eignet sich die Installation von optischen Rauchmeldern. Auch der Doppelboden sollte durch ebensolche Rauchmelder überwacht werden.

Bestehen besondere Anforderungen an die Verfügbarkeit eines Rechenzentrums bzw. Serverraums oder beinhalten diese besonders hochwertige oder schwer nachzubeschaffende IT-Komponenten, ist der Einsatz einer automatischen Löschanlage mit Inertgasen (Kohlendioxid, Inergen, Argon, Stickstoff, FM 200, etc.) zu erwägen.

Der Erstickungseffekt für Flammen gilt ebenso für Menschen, wenn sauerstoff-verdrängende Löschgase eingesetzt werden. So besteht bei einer Kohlendioxid-Konzentration von mehr als 8 Volumenprozent akute Lebensgefahr. Daher fordern in der Bundesrepublik Deutschland die berufsgenossenschaftlichen Richtlinien (BGR 134 Einsatz von Feuerlöschanlagen mit sauerstoffverdrängenden Gasen) den Einsatz von Alarmierungs- und Verzögerungseinrichtungen, "für Löschanlagen, bei denen die kritischen Konzentrationen, von denen an eine Gefährdung von Personen besteht, über- bzw. unterschritten werden, z. B. bei Konzentrationen von mehr als 5 Volumenprozent CO2 oder weniger als 10 Volumenprozent Sauerstoff", um rechtzeitig Personen aus dem Löschbereich evakuieren zu können.

Die Planung einer Löschgasanlage sollte grundsätzlich nur durch einen Fachplaner erfolgen.

Prüffragen:

- Wird sichergestellt, dass Brände so früh wie möglich erkannt werden?

# M 1.55 Perimeterschutz

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Falls das Gebäude oder Rechenzentrum innerhalb eines Grundstücks liegt, auf dem zusätzliche Sicherheitseinrichtungen installiert werden können, sollten Maßnahmen ergriffen werden, um von außen wirkende Gefährdungen vom Gebäude oder Rechenzentrum abzuhalten.

Insbesondere kann hier die erste Stufe einer Zutritts- und vor allem Zufahrtsregelung geschaffen werden.

Je nach Schutzbedarf und topologischen Gegebenheiten kann ein Perimeterschutz aus folgenden Komponenten bestehen:

- Äußere Umschließung oder Umfriedung, z. B. Zaunanlage, Mauerwerk und Zaunüberwachung.
  Dies bietet
- Schutz gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Schutz gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze sowie
- Schutz gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze.
- Freiland-Sicherungsmaßnahmen, z. B. Geländegestaltung, Zufahrtssperren, Beleuchtung des Geländes und des Gebäudes, Bewachungsunternehmen, Videoüberwachung und Detektionssensorik (siehe auch M 1.53 *Videoüberwachung*).auf dem Gelände
  Dies bietet Schutz gegen unbemerkten Zutritt eines Eindringlings für die Fläche zwischen Umfriedung und Gebäude.
- Äußere Personen- und Fahrzeugidentifikation, z. B. Videogegensprechanlage, Personen- bzw. Fahrzeugschleuse, Tür- bzw. Toröffnung und Zutrittskontrolleinheiten.
  Dies bietet Schutz gegen erkennbar (visuell, akustisch oder sensorisch) unberechtigte Zutrittsversuche als erste Stufe des Zutrittskontrollkonzeptes. Diese Aufgabe kann durch einen Pförtnerdienst unterstützt werden (siehe auch M 1.17 *Pförtnerdienst*).

Bevor Maßnahmen aus dem Bereich Perimeterschutz realisiert werden, muss in jedem Fall ein stimmiges Sicherheitskonzept für das Gebäude und sein Umfeld (siehe M 1.79 *Bildung von Sicherheitszonen*) erarbeitet werden, das die oben genannten Aspekte und den Gebäudeschutz umfasst. Anderenfalls besteht die Gefahr, dass vergleichsweise teure Sicherheitsmaßnahmen umgesetzt werden, beispielsweise aufwändige Zaunanlagen und ausgefeilte Gelände-Videoüberwachung, die in keinem Verhältnis zur Gebäudesicherung stehen und daher nicht angemessen sind.

Das Schutzkonzept sollte darauf ausgerichtet sein, mit den zur Verfügung stehenden Ressourcen möglichst wirksame Sicherheitsmaßnahmen aufzubauen. Dies betrifft besonders den Bereich Perimeterschutz. Die hier ergriffenen Maßnahmen sollten die Gesamtsicherheit erhöhen und nicht nur das Image einer "Hochsicherheitskulisse" vermitteln, da sich qualifizierte Angreifer allein durch den Anblick von hohen Zäunen und Videoüberwachung kaum von ihrem Vorsatz abbringen lassen.

**Beispiel:**

Wenn ein Angreifer zwei Minuten benötigt, um den Weg über den Zaun bis zum Gebäude zu nehmen und anschließend nur eine halbe Minute für das Eindringen ins Gebäude, stimmt die Relation nicht. Dies gilt um so mehr, wenn das Eintreffen von Einsatzkräften der örtlichen Polizei nach Alarmierung durch ein privates Bewachungsunternehmen beispielsweise acht Minuten dauert. In dieser Zeit könnte ein Einbrecher schon wieder nach vollbrachter Tat das Gelände verlassen haben. Er wäre zwar bemerkt und auf Videomaterial aufgenommen worden, bei geeigneter Maskierung jedoch kaum zu identifizieren.

Prüffragen:

- Gibt es ein Konzept, das sowohl den Perimeterschutz als auch den Gebäudeschutz umfasst?

# M 1.56 Netzersatzanlage

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Fachabteilung, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Die primäre Energieversorgung aus dem Netz eines Energieversorgungs-Unternehmens (EVU) muss bei erhöhten Anforderungen an die Verfügbarkeit um Maßnahmen zur Notfall-Versorgung des Rechenzentrums selbst ergänzt werden.

Die sekundäre Energieversorgung eines Rechenzentrums besteht üblicherweise aus einer zentralen USV für das Rechenzentrum und einer Netzersatzanlage (NEA). Falls die örtlichen Gegebenheiten und das Anforderungsprofil an die Verfügbarkeit des Rechenzentrums es zulassen, kann statt einer NEA auch eine zweite Einspeisung aus dem Netz eines zweiten Energieversorgungs-Unternehmens diese Auffang-Funktion erfüllen.

Während eine USV (siehe M 1.70 *Zentrale unterbrechungsfreie Stromversorgung*) Schwankungen oder kurzfristige Unterbrechungen der Stromversorgung überbrückt, fängt eine Netzersatzanlage längerfristige Stromausfälle auf.

Bei der Dimensionierung der Netzersatzanlage sollte darauf geachtet werden, dass deren Nennleistung über der Volllast-Betriebsleistung des Rechenzentrums liegt. Damit kann sichergestellt werden, dass die Netzersatzanlage auch bei gleichzeitigem Anlauf mehrerer Verbraucher die benötigte Leistung zur Verfügung stellen kann.

Der Betriebsmittelvorrat einer NEA muss regelmäßig kontrolliert werden, er sollte für mindestens 48 Stunden ausreichen. Bei hohen oder sehr hohen Anforderungen an die Verfügbarkeit kann dieser Wert auch leicht auf bis zu 120 Stunden steigen. Bei der Festlegung der Vorratsmenge ist zu berücksichtigen, ob es technisch und logistisch möglich ist, innerhalb der Laufzeit eine Nachbefüllung der Betriebsmittel durchzuführen. Bei der Frage der technischen Möglichkeit ist insbesondere bei dieselbetriebenen Geräten zu untersuchen, ob beim Nachtanken aufgewirbelter Bodensatz im Tank nicht zu Betriebsstörungen (z. B. verstopfte Filter) führt. Bei der logistischen Möglichkeit ist z. B. zu prüfen, ob die vorgesehene Nachbefüllung nicht eventuell selbst durch einen Stromausfall beeinträchtigt werden kann.

Je nach der Anforderung an die Verfügbarkeit der über die NEA versorgten IT kann eine einfache NEA ausreichen oder diese muss redundant aufgebaut werden. Ist ein redundanter Aufbau erforderlich, bietet eine (N+1)-Redundanz ausreichenden Schutz gegen eine Betriebsstörung der NEA selbst. Soll die Redundanz auch während der Wartung einer NEA gewährleistet sein, ist eine (N+2)-Redundanz aufzubauen.

Weitere Ausführungen zum Thema Redundanz und den damit eng verbundenen Aspekten Modularität und Skalierbarkeit sind in M 1.52 *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur* zu finden.

Es ist nicht immer möglich, zur Erlangung einer Betriebs- und Wartungsredundanz tatsächlich 2 zusätzliche Einheiten zu installieren. Da Wartungsfälle in der Regel mit ausreichendem Vorlauf planbar sind, kann die zweite Einheit im Bedarfsfall auch als mobile NEA temporär angeschlossen werden. Eine mobile NEA kann in der Institution selber vorrätig gehalten oder über einen ex-

ternen Dienstleister angemietet werden. Hierzu sind natürlich entsprechende SLAs mit dem Dienstleister zu vereinbaren.

Bei einem länger andauernden Ausfall der primären Energieversorgung ist eine NEA für die Aufrechterhaltung des IT-Betriebs unverzichtbar. Ihr Schutzbedarf entspricht also dem der IT, die sie versorgt. Dabei ist besonders auf den Schutz vor Brand und Wasser sowie Zugriff Unbefugter zu achten.

Ein sinnvoller Schutz gegen Brand macht es nahezu unverzichtbar, die einzelnen Einheiten der NEA in getrennten Brandabschnitten unterzubringen. Nur so kann verhindert werden, dass bei Brand einer Einheit nach kurzer Zeit auch alle anderen durch Brand ausfallen.

Um die Schutzwirkung der Netzersatzanlage aufrechtzuerhalten, sind zwei Dinge unerlässlich:

- regelmäßige Wartung
- Testläufe unter Echtbedingungen.

Um die Schutzwirkung einer NEA aufrechtzuerhalten, muss sie regelmäßig gewartet werden. Dafür sind die vom Hersteller vorgesehenen Wartungsintervalle der NEA einzuhalten. Bei diesen Wartungen sollten auch Belastungs- und Funktionstests durchgeführt werden.

Testläufen unter Echtbedingungen kommt besondere Bedeutung zu. Nur so kann verlässlich festgestellt werden, ob alle der Not-Energieversorgung dienenden Komponenten störungsfrei zusammenwirken. Die vielfach praktizierte Übung, die EVU-Versorgung erst nach erfolgreichem Start der NEA abzuschalten, bringt keine Erkenntnis darüber, ob im Ernstfall automatisch alles klappt. Einzig das harte Abschalten der EVU-Versorgung im laufenden Betrieb bringt die nötige Sicherheit zu erkennen, ob die Notstromversorgung auch funktioniert. Ebenso kann auch der Weg zurück in den Normalbetrieb nur verlässlich geprüft werden, indem die EVU-Versorgung wieder zugeschaltet wird und alle Komponenten selbsttätig wieder in Bereitschaft gehen. Testläufe sollten mindestens einmal in zwei Jahren durchgeführt werden.

Prüffragen:

- Wird der Betriebsmittelvorrat der NEA regelmäßig kontrolliert?
- Werden die Wartungsintervalle der NEA eingehalten?
- Werden bei den Wartungen Belastungs- und Funktionstests durchgeführt?
- Wird mindestens einmal in 2 Jahren ein Testlauf der NEA unter Echtbedingung durchgeführt?

# M 1.57 Aktuelle Infrastruktur- und Baupläne

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Baupläne, Fluchtwegpläne, Feuerwehrlaufkarten etc. (siehe auch M 1.11 *Lagepläne der Versorgungsleitungen* und M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*) sollten umgehend nach jeder Umbaumaßnahme, Erweiterung der Infrastruktur und Sicherheitstechnik auf den aktuellen Stand gebracht werden.

Dies ist erforderlich, um

- das definierte Sicherheitsniveau halten,
- Notfallsituationen optimal begegnen,
- Revisionen erleichtern und
- Maßnahmen vollständig und angemessen planen und durchführen zu können.

Es ist nicht ausreichend, die Pläne beispielsweise nur bei der zuständigen Bauverwaltung zu lagern. Im Schadens- oder Notfall, z. B. bei Kabelschäden oder Wasserrohrbrüchen kann wichtige Zeit für die Fehlerlokalisierung und -beseitigung verloren gehen. Derjenige, der die Pläne verwaltet, z. B. im Hausdienst, sollte auch in der Lage sein, sie zu lesen. Gegebenenfalls ist Personal entsprechend zu schulen und einzuweisen.

Prüffragen:

- Sind die Infrastruktur- und Baupläne auf dem aktuellen Stand?

# M 1.58 Technische und organisatorische Vorgaben für Serverräume

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Informationssicherheitsmanagement

Ein Serverraum sollte als geschlossener Sicherheitsbereich konzipiert sein. Dieser sollte möglichst gut zu sichernde Zugangstüren und Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen (siehe auch M 1.10 *Sichere Türen und Fenster*). Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei der Planung eines Serverraumes bzw. der Auswahl geeigneter Räumlichkeiten sollten potentielle Gefährdungen durch Umgebungseinflüsse möglichst minimiert werden. So ist Gefahrenpotentialen wie Wassereinbrüchen bei Flachdächern oder in Kellerräumen genauso zu begegnen wie EMV-Störquellen, z. B. Mobilfunk-Sendeeinrichtungen oder Drehstromaggregaten.

Bei der Planung sollte auch darauf geachtet werden, dass die Trassen der Versorgungsleitungen des Gebäudes, z. B. für Wasser oder Gas (siehe M 1.24 *Vermeidung von wasserführenden Leitungen*), nicht in unmittelbarer Nähe oder gar durch sensible Bereiche des Serverraums verlaufen.

Für die in Serverräumen betriebenen IT-Komponenten wird in vielen Fällen ein hohes Maß an Verfügbarkeit gefordert. Diesen Anforderungen kann durch redundante Auslegung der infrastrukturellen und technischen Einrichtungen Rechnung getragen werden (siehe Maßnahme M 1.52 *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur*).

Ein Serverraum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und wichtiger noch für nur zeitweilig Beschäftigte, z. B. zu Wartungsarbeiten tätige, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.

IT-Systeme, die von Externen betreut werden, sollten in separaten Räumen aufgestellt werden. Es ist außerdem zu überlegen, IT-Systeme mit unterschiedlichem Schutzbedarf oder aus verschiedenen Bereichen in getrennten Serverräumen aufzustellen, um den Kreis der Zutrittsberechtigten klein zu halten.

In einem Serverraum sollten sich auf keinen Fall Geräte oder Ausrüstung befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, also z. B. Fax-Geräte oder Fotokopierer. Brennbare Materialen wie Druckerpapier sollten ebenfalls nicht in einem Serverraum gelagert werden.

Es sollte verboten werden, in einen Serverraum tragbare IT-Systeme, Mobiltelefone oder Kameras mitzubringen, wenn diese nicht unter der Kontrolle der jeweiligen Institution stehen. Generell sollte der Betrieb von Mobiltelefonen in Rechenzentren untersagt werden, da diese den Betrieb der IT-Systeme erheblich stören können. Ausnahmen hiervon müssen abgestimmt sein (siehe M 2.188 *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung*).

Prüffragen:

- Bildet der Serverraum einen eigenen Sicherheitsbereich?
- Werden die Zutritte zu einem Serverraum kontrolliert?
- Sind bei der Auswahl der Räumlichkeiten für einen Serverraum Gefährdungen durch Umgebungseinflüsse weitgehend vermieden worden?
- Weisen die Türen, Fenster und Wände der Serverräume einen ausreichenden Einbruch-, Rauch- und Feuerschutz auf?
- Ist bei der Planung berücksichtigt worden, dass die Trassen der Versorgungsleitungen nicht in unmittelbarer Nähe oder gar durch sensible Bereiche eines Serverraumes verlaufen?
- Sind die infrastrukturellen und technischen Einrichtungen zur Sicherstellung der Hochverfügbarkeit im Wartungs- oder Fehlerfall ausreichend redundant ausgelegt?
- Existieren organisatorische Vorgaben für Serverräume?

# M 1.59 Geeignete Aufstellung von Speicher- und Archivsystemen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Da in Speicher- und Archivsystemen wichtige Behörden- bzw. Unternehmensdaten konzentriert aufbewahrt werden, müssen deren IT-Komponenten in gesicherten Räumen aufgestellt werden, zu denen nur Berechtigte Zutritt haben. Dies betrifft neben den eingesetzten Servern und Netzkomponenten insbesondere die Speichereinheiten (Plattenarrays, Bandlaufwerke, Disc-Jukeboxen).

Für die geeignete Aufstellung dieser IT-Komponenten sind alle relevanten Maßnahmen, die in den IT-Grundschutz-Katalogen zur Infrastruktur-Sicherheit beschrieben sind, zu realisieren. Je nach Art und Größe des Speicher- oder Archivsystems sind die Bausteine B 2.1 *Allgemeines Gebäude*, B 2.9 *Rechenzentrum*, B 2.4 *Serverraum* bzw. B 2.7 *Schutzschränke* heranzuziehen. Hierbei sollte besonders auf eine ausreichende Zuverlässigkeit der infrastrukturellen Komponenten (Stromzufuhr, etc.) geachtet werden. Beim Einsatz von Speichersystemen sind zudem angemessene Redundanzen in der technischen Infrastruktur zu schaffen (siehe M 1.52 *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur*), um die Verfügbarkeit dieser zentralen Ressourcen so gut wie möglich zu unterstützen.

Für die langfristige Aufbewahrung der verwendeten Archiv-Speichermedien sind die in M 1.60 *Geeignete Lagerung von Archivmedien* genannten Lagerbedingungen einzuhalten. Vor allem die zweckmäßige Klimatisierung von Speichermedien, aber auch der Archivsysteme selbst, ist hier zu beachten.

Häufig werden elektronische Archive so realisiert, dass Archivmedien im dauerhaften Zugriff durch die Speichereinheit gehalten werden. Hierzu kommen vielfach dedizierte Speichereinheiten zum Einsatz, die selbsttätig Wechselmedien verwalten und einlegen können, beispielsweise Roboter für Bandlaufwerke oder Jukeboxen für Disc-Medien. Wenn ein Speicher- oder Archivsystem solche Komponenten beinhaltet, werden in der Regel die Archivmedien während ihrer gesamten Lebensdauer nicht mehr aus der Speichereinheit ausgelagert. Das bedeutet, dass die an Archivmedien zu stellenden Lagerbedingungen (bezüglich Klimatisierung, Zugriffsschutz, etc.) bereits in der Speicherkomponente erfüllt und überwacht werden müssen.

Bei Auswahl des Speicher- oder Archivsystems ist daher als Kriterium zu berücksichtigen, dass die erforderlichen Lagerbedingungen für Archivmedien in Speicherkomponenten eingehalten werden können bzw. welcher Zusatzaufwand hierfür entsteht.

Prüffragen:

- Erfolgt die Aufstellung der IT-Komponenten in gesicherten Räumen?
- Ist der Zutritt zu den Räumlichkeiten der IT-Komponenten nur berechtigten Personen vorbehalten?
- Ist die Zuverlässigkeit der infrastrukturellen Komponenten sichergestellt?
- Bei Hochverfügbarkeit: Sind Redundanzen hinsichtlich der technischen Infrastruktur gegeben?
- Werden bei langfristiger Aufbewahrung die Lagerbedingungen der Archiv-Speichermedien eingehalten?

# M 1.60 Geeignete Lagerung von Archivmedien

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für den Langzeiteinsatz von Archivmedien sind besonders der Zugriffsschutz sowie klimatische Lagerbedingungen zu beachten und deren Einhaltung zu überwachen.

Sofern Archivmedien im Online-Zugriff, also im Archivsystem bzw. in Speicherlaufwerken gehalten werden, ist keine räumliche Trennung zwischen Archivsystem und Archivmedium realisierbar. Für die geeignete Lagerung von Archivmedien sind damit die in M 1.59 *Geeignete Aufstellung von Speicher- und Archivsystemen* genannten Empfehlungen umzusetzen.

Wenn Archivmedien außerhalb des Archivsystems "offline" gelagert werden, so sind die im Baustein B 2.5 *Datenträgerarchiv* beschriebenen Maßnahmen unter besonderer Berücksichtigung der Anforderungen an die Klimatisierung anzuwenden.

**Klimatisierung**

Die klimatischen Anforderungen an die Haltbarkeit von Archivmedien hängen von den eingesetzten Archivmedien ab. Hersteller geben hierzu vereinzelt unverbindliche Hinweise zu den Lagerbedingungen (z. B. hinsichtlich der Temperatur und Luftfeuchte) und zur Haltbarkeit der Medien an.

Für den langfristigen Einsatz elektronischer Archivsysteme müssen die konkreten Lagerbedingungen jedoch von den Herstellern der eingesetzten Archivmedien verbindlich erfragt werden. Da hiervon die Haltbarkeit der Archivmedien abhängt, sollten folgende Punkte vor der Auswahl der verwendeten Archivmedien geklärt werden (siehe auch M 4.169 *Verwendung geeigneter Archivmedien*):

- Die klimatischen und physikalischen Lagerbedingungen für die betrachteten Archivmedien sollten seitens des Herstellers ausreichend detailliert beschrieben sein (inklusive der Auswirkungen auf die maximale Lebensdauer). Diese Angabe sollte verbindlich sein, möglichst mit einer Garantieerklärung des Herstellers bei Einhaltung der Lagerbedingungen.
- Die technische Realisierung einer geeigneten Lagerung kann unter Umständen sehr komplex sein. Je nach den vorhandenen technischen und infrastrukturellen Vorgaben können bestimmte Archivmedien auch gänzlich ungeeignet sein. Daher müssen im Vorfeld die Möglichkeit und der Aufwand für die technische Realisierung einer geeigneten Lagerung geprüft werden.

Die Lagerbedingungen sollten im Betriebshandbuch des Archivsystems dokumentiert werden. Zusätzlich muss sichergestellt werden, dass die Lagerbedingungen kontinuierlich eingehalten und überwacht werden (siehe auch M 1.27 *Klimatisierung der Technik / in Technikräumen*).

**Physikalische Schutzmaßnahmen**

Über die klimatischen Bedingungen hinaus müssen die verwendeten Archivmedien vor unautorisiertem Zugriff und mechanischer Beschädigung oder

Veränderung geschützt werden. Hierzu wird insbesondere auf die im Baustein B 2.5 *Datenträgerarchiv* genannten Maßnahmen verwiesen.

Neben einer Kontrolle des Zutritts zum Datenträgerraum, Brandschutz und Schutz vor Wassereinwirkung sind je nach Art der verwendeten Archivmedien weitere Maßnahmen zu realisieren, z. B. zum Schutz vor Einwirkung von Magnetfeldern auf Magnetbänder.

Hierfür sind verbindliche Empfehlungen von Herstellern zu mechanischen Lagerbedingungen einzuholen und zu beachten.

Bei Nichteinhaltung der Lagerbedingungen muss eine Alarmierung und Reaktion erfolgen. Hierzu sind organisationsspezifisch Eskalationsprozeduren und -wege zu definieren.

Prüffragen:

- Werden die klimatischen Lagerbedingungen der Archivmedien beachtet und deren Einhaltung überwacht?
- Werden die Archivmedien vor unautorisierten Zugriff, mechanischer Beschädigung oder Veränderung geschützt?
- Sind Eskalationsprozeduren für bei Nichteinhaltung der Lagerbedingungen der Archivmedien definiert?

# M 1.61 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes

**Verantwortlich für Initiierung:** Benutzer, IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Benutzer

Dank immer kleinerer und leistungsfähigerer IT-Systeme ist es heutzutage möglich, nahezu überall zu arbeiten. Dadurch kann jede beliebige Umgebung zu einem mobilen Arbeitsplatz werden, also beispielsweise ein Hotelzimmer, der Sitzplatz in Eisenbahn oder Flugzeug oder eine Räumlichkeit beim Kunden. Solche mobilen Arbeitsplätze können vom IT-Benutzer leider nur sehr beschränkt eingerichtet werden und müssen im Allgemeinen so genutzt werden, wie sie vorgefunden wurden. Daher ist immer zuerst von jedem mobilen IT-Benutzer zu entscheiden, ob die jeweilige Umgebung geeignet ist, um als mobiler Arbeitsplatz genutzt zu werden. Gründe, die dagegen sprechen könnten, sind beispielsweise die folgenden:

- Die zu bearbeitenden Informationen sind zu sensibel, um außerhalb der geschützten Büroumgebung bearbeitet zu werden (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen* und M 2.218 *Regelung der Mitnahme von Datenträgern und IT-Komponenten*).
- Die Umgebung erlaubt es nicht, ohne Einsichtnahme Dritter zu arbeiten, z. B. bei engen Sitzplätzen in der Bahn oder dem Flugzeug.
- Es ist keine Stromversorgung oder keine Netzanbindung vorhanden.
- Die Nutzung von mobilen IT-Geräten ist verboten, z. B. im Flugzeug oder in fremden Büros.

Einige für mobiles Arbeiten wünschenswerte Aspekte sind außerdem die folgenden:

- Es sollte ein stabiler Platz zum Abstellen der mobilen IT-Systeme vorhanden sein. Viele mobile IT-Systeme werden durch Stürze zerstört.
- Die Umgebung sollte nicht zu laut sein.
- Die Umgebung sollte ausreichend beleuchtet sein, Monitorlicht alleine reicht auf Dauer nicht. Störende Blendungen, Reflexen oder Spiegelungen sollten vermieden werden.
- Der Monitor sollte so aufgestellt werden können, dass die Eingaben nicht beobachtet werden können. Für Laptops gibt es auch spezielle Monitor-Folien, die eine Einsichtnahme von der Seite verhindern.
- Die Umgebung sollte außerdem so sein, dass die mobilen IT-Systeme nicht beeinträchtigt werden, also nicht zu feucht, zu kalt oder zu warm sein. Während der Benutzung liegt dies natürlich auch im eigenen Interesse des Benutzers, die IT-Geräte sollten aber auch entsprechend aufbewahrt werden.
- Mobile IT-Geräte sollten gegen Diebstahl geschützt werden (siehe auch M 1.46 *Einsatz von Diebstahl-Sicherungen*). Die Umgebung sollte hierfür die notwendigen Bedingungen bieten. Um beispielsweise einen Laptop mit einem Kabelschloss gegen einfache Wegnahme zu sichern, muss es die Möglichkeit geben, das Kabelschloss an einen festen Gegenstand anzuschließen. Wenn möglich, sollten Fenster und Türen des mobilen Arbeitsplatzes beim Verlassen geschlossen werden. Dies ist z. B. bei Hotelzimmern oder Besprechungsräumen möglich, im Zug unter Umständen schwierig.

In fremden Umgebungen wie z. B. Hotels ist auch immer empfehlenswert, sich über das richtige Verhalten bei Bränden oder anderen Notfällen zu informieren, z. B. über Warntöne und Fluchtwege.

Prüffragen:

- Sind die IT-Benutzer angewiesen, vor jedem mobilen Einsatz zu entscheiden, ob die jeweilige Umgebung als mobiler Arbeitsplatz geeignet ist?

# M 1.62 Brandschutz von Patchfeldern

**Verantwortlich für Initiierung:** Brandschutzbeauftragter
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter, Haustechnik, Planer

Sowohl die internen Leitungen des Hausnetzes als auch die externen des öffentlichen Netzes laufen auf Leitungsverteilern oder Patchfeldern auf, von denen aus sie über Anschlussleitungen mit Servern, Routern, etc. verbunden sind.

Häufig sind in kleineren Standorten Verteiler und aktive Komponenten (Server, Router, etc.) in einem Raum stationiert. Um zu verhindern, dass die Leitungsverteiler und Patchfelder durch einen Brand der aktiven IT beschädigt werden, sind sie mit einem geeigneten Brandschutz gegenüber der aktiven IT abzuschotten.

Sind Möglichkeiten und Einrichtungen vorhanden, um einen Brand frühzeitig zu erkennen und zu löschen (Objekt- oder Raumlöschung), kann eine E-30-Schottung (nach DIN 4102 Brandverhalten von Baustoffen und Bauteilen) ausreichend sein. Sind solche Einrichtungen nicht vorhanden und sieht das Brandschutzkonzept ausschließlich die Löschung durch hilfeleistende Kräfte (eigenes Personal, Feuerwehr) vor, ist eine E-90-Schottung dringend zu empfehlen.

Sind die Leitungsverteiler und Patchfelder einerseits in einem Raum für technische Infrastruktur (siehe B 2.6 *Raum für technische Infrastruktur*) und die Server, Router, etc. andererseits in einem Serverraum (siehe B 2.4 *Serverraum*) sauber voneinander getrennt untergebracht, kann die entsprechende Abschottung durch geeignete Maßnahmen im Baukörper realisiert werden.

Wenn keine getrennten Räume genutzt werden können und die Leitungsverteiler und Patchfelder im Serverraum angeordnet werden müssen, besteht die Möglichkeit, diese in geeigneten Wand- oder Standverteilern mit dem erforderlichen Funktionserhalt (E-30 oder E-90) anzuordnen. Dabei ist aber besonders darauf zu achten, dass auch alle von außen kommenden Zuleitungen aus dem Haus- und dem öffentlichen Netz innerhalb des Raums in gleicher Weise (z. B. durch geeignete Kabelkanäle) gegen Brand geschützt werden.

Bei beiden Lösungen ist darauf zu achten, dass die Durchführung der Anschlussleitungen von den Leitungsverteilern und Patchfeldern zu den IT-Geräten durch die Brandschutzkonstruktion zu jeder Zeit mit geeigneten Brandschutzmitteln verschlossen ist. Wegen der Notwendigkeit, einfach und rasch an diesen Durchführungen arbeiten zu können, ohne den Brandschutz jedes Mal aufwändig wiederherstellen zu müssen, empfehlen sich hierfür (bei häufigen Arbeiten) Brandschutzkissen oder (bei selteneren Arbeiten) Pressschotts. Verwendete Brandschutzkissen müssen gegen Herausfallen gesichert werden.

Prüffragen:

- Ist bei den Leitungsverteilern und Patchfeldern sowie bei den Zuführungsleitungen ein ausreichender Brandschutz vorhanden?
- Stimmt der gewählte und realisierte Funktionserhalt (E-30 oder E-90) mit den vorhandenen Möglichkeiten der Brandmeldung und -löschung überein?

- Werden die Durchführungen nach Arbeiten im Bereich der Rangierung wieder ordnungsgemäß verschlossen?
- Werden gegebenenfalls verwendete Brandschutzkissen gegen Herausfallen gesichert?

# M 1.63 Geeignete Aufstellung von Access Points

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Innerer Dienst

### Sichere Montage von Access Points

Um Manipulationen an den Access Points vorzubeugen, sollten diese in Metallgehäusen untergebracht oder mit Metallbügeln gesichert werden, die eine Wandmontage ermöglichen. Möglich ist die Unterbringung in Doppelböden, Zwischendecken oder abgehängten Decken und die Nutzung von externen Antennen. Je nach Antennenform kann so selbst durch einen Fachmann nicht mehr erkannt werden, ob es sich um einen Brandmelder oder um die Antenne eines Access Points handelt.

Räumlichkeiten bzw. Örtlichkeiten, in denen sich nicht vertrauenswürdige Personen für eine längere Zeit unbeobachtet aufhalten können, scheiden bei Anbringung der Access Points im Sichtbereich und ohne tarnende Form prinzipiell als Montage-Ort aus (Außengelände, Treppenhäuser). In diesen Bereichen können jedoch Access Points ohne Routing-Funktionalitäten aufgestellt werden. Dadurch können Informationen zum detaillierten Aufbau des Netzes nicht von unbefugten Personen ausgelesen werden. Somit wird die Angriffsfläche auf das WLAN und ein eventuell damit verbundenes LAN verringert.

Als Mindestschutz sollte eine feste Verschraubung des Access Points an einer ohne Hilfsmittel nicht zugängliche Stelle bzw. an eine nicht einsehbare Stelle erfolgen.

### Positionierung der Access Points

Durch die Aufstellung und Ausrichtung von Access Points wird die Übertragungsqualität und der Durchsatz eines WLANs essentiell beeinflusst. Generell gilt, dass die Ausbreitung der Funkwellen in Bereichen, die nicht durch das WLAN versorgt werden sollen, möglichst stark zu reduzieren ist. Auf diese Weise wird nicht nur die Angriffsfläche verringert, sondern auch der eigentlich gewünschte Abdeckungsbereich besser versorgt. Hierzu können Richtantennen verwendet werden, welche die Abstrahlung von elektromagnetischen Wellen in gewisse Raumrichtungen bündeln und so einen richtungsabhängigen Verstärkungseffekt (als Antennengewinn bezeichnet) erzielen. Dieser Verstärkungseffekt muss mit der Sendeleistung am Access Point abgestimmt werden. Manche Access Points unterstützen eine flexible Einstellung der Sendeleistung. Auf diese Weise kann der Abdeckungsbereich mit der notwendigen Leistung ausgeleuchtet werden, und der Zugriff auf das WLAN von außen wird gleichzeitig erschwert, da hier nun vergleichsweise schlechte Empfangsbedingungen herrschen. Voraussetzung ist eine geeignete Positionierung der Access Points bzw. der Antennen. Diese kann auf Basis einer entsprechenden Ausleuchtungsmessung geschehen.

Bei der Versorgung von Außenbereichen sind Außeninstallationen (Antennen und gegebenenfalls Access Points) vor Witterungseinflüssen, elektrischen Entladungen und unberechtigtem Zugriff geeignet zu schützen. Die Anbringung von Access Points außerhalb von Gebäuden ist nach Möglichkeit zu vermeiden.

Die Anbringung von Antennen auf Gebäudedächern muss so erfolgen, dass die Antenne gegen Blitzschlag gesichert ist. Die Höhe der Antenne muss ge-

nügend unter der des Blitzableiters liegen, und der Abstand zum Blitzableiter muss genügend groß sein. Dies gilt auch für den einzuhaltenden Abstand zu Hochspannungsleitungen. Antennen im Außenbereich, die möglicherweise von der Gefahr elektrischer Entladungen betroffen sind (dies gilt stets für Antennen, die auf Dächern montiert werden), sollten über einen speziellen Überspannungsschutz angeschlossen werden, der Strom- und Spannungsstöße schnell erkennt und ableitet. Dieser Überspannungsschutz wird zwischen Antenne und Access Point (typischerweise innerhalb des Gebäudes oder an einem vergleichbar geschützten Platz) montiert und muss über eine ausreichende Erdung verfügen. Access Points sollten generell nicht in Bereichen installiert werden, die von elektrischen Entladungen betroffen sein können.

Werden im Ausnahmefall Access Points außerhalb eines geeignet klimatisierten Gebäudes installiert, ist sicher zu stellen, dass der Access Point ausreichend gegen eindringende Feuchtigkeit, Frost und Hitze geschützt ist. Außenantennen sind geeignet gegen Schnee-Ablagerung zu schützen. Sie sind entweder windgeschützt anzubringen, oder die Anbringung muss auch bei hohen Windstärken so fest sein, dass sich die Antennenausrichtung nicht verstellt.

Prüffragen:

- Sind die Access Points gegen unerlaubte physikalische Zugriffe geschützt?
- Wurde eine Ausleuchtungsmessung durchgeführt, um den Sendebereich der Access Points zu bestimmen?
- Sind die Empfangsbereiche für den WLAN-Zugriff auf die relevanten Bereiche beschränkt?
- WLAN-Antennen sind auf den Gebäudedächern angebracht: Sind die Antennen gegen Blitzschlag gesichert?
- WLAN-Antennen sind im Außenbereich angebracht: Sind Maßnahmen gegen elektrische Entladungen getroffen?

# M 1.64 Vermeidung elektrischer Zündquellen

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik, Mitarbeiter

Der überwiegende Teil baulicher Brandschutzmaßnahmen zielt darauf ab, sich entwickelnde Brände einzugrenzen, sowie die Flucht von Personen und den Einsatz von Rettungskräften zu ermöglichen. Auf die Entstehung von Bränden haben diese Maßnahmen meist nur geringen Einfluss.

Hier muss der Mensch in seinem täglichen Arbeitsumfeld besondere Aufmerksamkeit und Vorsorge walten lassen. Neben den allseits bekannten und offensichtlichen Brandquellen wie Aschenbechern, der "Kippe im Papierkorb" oder weihnachtlichem Kerzenschmuck muss auch den weniger offensichtlichen elektrischen Zündquellen Beachtung geschenkt werden.

**Elektrogeräte**

Beim Kauf neuer privater Haushaltsgeräte werden die noch funktionierenden Altgeräte als "Spende" im Betrieb weiter genutzt. Dabei wird übersehen, dass gerade alte Elektrogeräte mit ihren altersbedingt viel wahrscheinlicheren Defekten eine besonders hohe Brandgefährdung darstellen.

Die Nutzung privater Elektrogeräte innerhalb eines Unternehmens oder einer Behörde ist daher klar zu regeln. Sie sollte nur als Ausnahme gestattet sein, wenn derartige Geräte vorher durch eine Elektrofachkraft geprüft und für sicher befunden wurden. Genehmigte Geräte sollten speziell gekennzeichnet werden, so dass ungenehmigte Geräte einfach erkannt und aus dem Verkehr gezogen werden können.

Besonders Kühlschränke, die im Dauerbetrieb laufen, und Kaffeemaschinen, die oft stundenlang eingeschaltet bleiben, sollten nur in Räumen betrieben werden, die ausdrücklich und baulich dafür vorgesehen sind (Teeküchen etc.).

**Steckdosenleisten**

Egal wie viele Steckdosen vom Architekten vorgesehen wurden, es sind immer zu wenig oder sie sind am falschen Platz. Um dann fehlende Steckdosen bereitzustellen, werden oft Steckdosenleisten verwendet. Sind diese von unzureichender Qualität oder werden sie unsachgemäß eingesetzt (siehe auch G 4.62 *Verwendung unzureichender Steckdosenleisten*), stellen solche Steckdosenleisten eine gefährliche Zündquelle dar.

Die Verwendung von Steckdosenleisten sollte so weit wie möglich vermieden werden. Fehlende Steckdosen sollten durch eine Elektrofachkraft in vorhandenen Kanalsystemen nachgerüstet oder fachgerecht auf Putz montiert werden.

Ist dies nicht möglich und somit die Verwendung von Steckdosenleisten unvermeidbar, ist zu beachten:

- Es dürfen ausschließlich hochwertige Steckdosenleiste verwendet werden, die von einer Elektrofachkraft geprüft und für sicher befunden wurden.
- Es sollten einzelne ausreichend große Steckdosenleiste benutzt werden statt mehrerer kleiner.
- Steckdosenleisten dürfen keinesfalls hintereinander gesteckt werden.

- Steckdosenleisten dürfen auf keinen Fall überlastet werden. In der Regel liegt die Grenze bei 3500 Watt. Hier ist unbedingt das Typenschild zu beachten.
- Steckdosenleisten dürfen sich weder im Fußbereich am Arbeitsplatz noch in Verkehrsflächen befinden.

**Elektroverteilung**

Die gesamte Elektroverteilung, hauptsächlich Schutzschalter sowie Verschraubungen und Klemmstellen, unterliegt wie alle technischen Geräte einer Alterung. Sie ist daher in regelmäßigen Abständen gemäß DIN VDE 0105-100:2005-06 "Betrieb von elektrischen Anlagen" zu überprüfen.

Im Schadensfall muss ein Gewerbetreibender den Nachweis über den einwandfreien Zustand der Elektroanlage gegenüber den Gewerbeaufsichtsämtern, den Berufsgenossenschaften und den Versicherungen führen.

In Deutschland schreibt die Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit (BGV, A3 - Elektrische Anlagen und Betriebsmittel) folgende regelmäßige Prüfungen vor:

- elektrische Anlagen und ortsfeste Geräte: mindestens alle 4 Jahre,
- ortsveränderliche Geräte: je nach Gerätetyp mindestens alle 6 Monate bis zu mindestens alle 2 Jahre.

Zu den ortsveränderlichen Geräten gehören unter anderem Steckdosenleisten, aber auch viele IT-Geräte wie beispielsweise Arbeitsplatzrechner.

**Lüfter**

Durch Staub blockierte Lüfter können zur Überhitzung der zu kühlenden IT-Geräte führen, aber auch selbst zu einem Brandherd werden (siehe auch G 4.63 *Verstaubte Lüfter*).

Lüfter sind folglich in regelmäßigen Abständen auf freien Rundlauf und auf Staubablagerung hin zu untersuchen und zu reinigen. Dies sollte mindestens einmal im Jahr und bei erkennbarem Bedarf auch öfter erfolgen (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*).

**Protokollierung**

Alle Prüfungen und deren Ergebnisse sind in geeigneter Form zu dokumentieren.

Prüffragen:

- Gibt es Regelungen für die Nutzung privater Haushaltsgeräte im Betrieb?
- Ist der Einsatz von Steckdosenleisten weitgehend vermieden worden?
- Wurde bei dem Einsatz von Steckdosenleisten auf hohe Qualität und eine Abnahme durch eine Elektrofachkraft geachtet?
- Wird die Elektroverteilung (speziell Verschraubungen, Klemmstellen und Schutzschalter) regelmäßig überprüft?
- Werden die Lüfter der zu kühlenden IT-Geräte regelmäßig auf Staubablagerungen untersucht und entsprechend gereinigt?
- Werden die Prüfungen elektrischer Geräte und der Elektroverteilung mit ihren Ergebnissen dokumentiert?

# M 1.65 Erneuerung der IT-Verkabelung

**Verantwortlich für Initiierung:** Planer, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Die schnelle Weiterentwicklung der Informationstechnik und insbesondere die Anforderungen, die durch neue IT-Anwendungen gestellt werden, führen in Gebäuden, die eine ältere IT-Verkabelung aufweisen, oft zu Überlegungen, den Bestand der IT-Verkabelung zu modernisieren oder gänzlich zu erneuern.

Der Aufwand, die vorhandene IT-Verkabelung durch eine komplett neue Sekundär- und Tertiärverkabelung zu ersetzen, darf nicht unterschätzt werden. Die Erfahrung zeigt, dass bereits nach einer ersten Betrachtung des finanziellen und organisatorischen Aufwands eines umfassenden Modernisierungsprojekts meist beschlossen wird, dass eine existierende IT-Verkabelung so lange wie möglich genutzt werden sollte.

Eine umfassende Erneuerung der IT-Verkabelung sollte nur in Angriff genommen werden, wenn als gesichert anzunehmen ist, dass die geschäftlichen Abläufe der Institution mit der vorhandenen IT-Verkabelung nicht mehr ausreichend unterstützt werden. Deutliche Anzeichen, dass sich die vorhandene IT-Verkabelung nicht mehr nutzen lässt, sind beispielsweise folgende:

- Nachverkabelungen, die zum Anschluss weiterer Benutzer benötigt werden, führen zu ständigen Störungen des Netzbetriebes.
- Das vorhandene Netz leidet unter häufigen Netzausfällen, z. B. durch Kurzschlüsse in einem Token Ring oder Loop-Bildungen durch Wackelkontakte auf IBM IVS Typ-1 Ethernet-Kabeln.
- Die vorhandene Verkabelung kann den Kapazitätsanforderungen nicht mehr standhalten, weil z. B. ganze Etagen über IBM IVS Typ-1 Verkabelung, also mit einer maximalen Übetragungsrate von 10 Mbit/sec, angebunden sind.

Wenn die IT-Verkabelung erneuert werden soll, sind alle Planungsschritte wie bei einer Ersterrichtung durchzuführen (siehe M 2.395 *Anforderungsanalyse für die IT-Verkabelung*). Auch hier stehen die Anforderungsanalyse und die Abschätzung der Bedarfsentwicklung am Anfang.

Zu beachten ist, dass beim Austausch alter Typ-1 Verkabelungen besonders im Tertiärbereich zu prüfen ist, ob die Kabelwege auch mit neuer Verkabelung unverändert möglich bleiben. Da Typ-1 Kabel eine maximale Kabellänge von 150 Metern erlauben, kann es nötig sein, zusätzliche Etagenverteiler an geeigneter Stelle zu installieren, um die Begrenzung von Kabeln der Kategorie 5 oder höher auf eine Verbindungslänge von maximal 100 Metern zu beachten. Dabei berechnet sich die Verbindungslänge aus der Länge des Tertiärkabels plus der Länge der Patchkabel.

Wenn ein leerstehendes Gebäude modernisiert wird, kann für die Migration eine reine Technikplanung vorgenommen werden. Bei Gebäuden, die beispielsweise als Büro- und nicht nur als Lagergebäude genutzt werden, ist für die Migration der vorhandenen IT-Verkabelung auf eine aktuelle Verkabelungstechnik auch eine Modernisierungsplanung vorzunehmen.

Sie muss vorgeben, wie eine neue IT-Verkabelung im laufenden Geschäftsbetrieb so vorgenommen werden kann, dass der Geschäftsbetrieb möglichst wenig gestört wird.

Prüffragen:

- Bei Verwendung vorhandener Kabelwege: Sind die Verbindungslängen auch für die neue Verkabelung erlaubt?

# M 1.66 Beachtung von Normen bei der IT-Verkabelung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Unter dem Begriff "Anwendungsneutrale Kommunikationskabelanlagen" wurde 1995 erstmalig eine Norm veröffentlicht, welche Topologie und Klassifizierung von Übertragungsstrecken mit definierten Eigenschaften sowie eine einheitliche Schnittstelle zum Anschluss der Endgeräte beschreibt. Diese Vorgaben gelten nicht nur für den Einsatz in Bürogebäuden, sondern lassen sich auch auf andere Anwendungsgebiete übertragen.

Unter der Verantwortung des Europäischen Komitees für Elektrotechnische Normung (CENELEC) werden die Normen überwacht, mit den Internationalen Gremien (ISO/IEC) abgestimmt und bei Bedarf weiterentwickelt und verfeinert.

Die Normen unterstützen die Anwender in den Phasen der Gebäudeplanung, des Verkabelungsentwurfs, der Planung, der Realisierung und des Betriebs von Kommunikationskabelanlagen.

Neben der *EN 50173-1 - Anwendungsneutrale Kommunikationskabelanlagen, Allgemeine Anforderungen* sowie der zum Zeitpunkt der Erarbeitung dieses Dokuments als Entwurf vorliegenden Teile 2 *Bürogebäude*, 3 *Industriell genutzte Gebäude*, 4 *Wohneinheiten* und 5 *Rechenzentren* gibt es weitere Normen, die in der Planung und Ausführung der IT-Verkabelung Anwendung finden.

Übertragen auf das Phasenmodell der IT-Grundschutz-Kataloge lassen sich Normen wie folgt zuordnen:

**Gebäudeplanung**
- EN 50310 - Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
  5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Gebäude
  6.3: AC-Verteilung und Anschluss des Schutzleiters (TN-S)

**Verkabelungsentwurf**
- EN 50173-1 - Anwendungsneutrale Kommunikationskabelanlagen, Allgemeine Anforderungen und Bürobereiche
  4: Topologie
  5: Leistungsvermögen der Übertragungsstrecken
  7: Anforderungen an Kabel
  8: Anforderungen an Verbindungstechnik
  9: Anforderungen an Schnüre
  A.1: Grenzwerte für Strecken

**Planung**
- EN 50174-1 - Installation von Kommunikationsverkabelung, Spezifikation und Qualitätssicherung
  4: Betrachtungen zu Festlegungen
  5: Qualitätssicherung
  7: Verwaltung der Verkabelung
- EN 50174-2 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken in Gebäuden
  4: Sicherheitsanforderungen

5: Allgemeine Festlegungen für die Verlegung von metallener Verkabelung und Lichtwellenleiterverkabelung
6: Zusätzliche Festlegungen für die Verlegung metallener Verkabelung
7: Zusätzliche Festlegungen für die Verlegung von Lichtwellenleiterverkabelung
- EN 50174-3 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken im Freien
- EN 50310 - Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Gebäude
6.3: AC-Verteilung und Anschluss des Schutzleiters (TN-S)

**Realisierung**
- EN 50174-1 - Installation von Kommunikationsverkabelung, Spezifikation und Qualitätssicherung
6: Dokumentation
7: Verwaltung der Verkabelung
- EN 50174-2 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken in Gebäuden
4: Sicherheitsanforderungen
5: Allgemeine Festlegungen für die Verlegung von metallener Verkabelung und Lichtwellenleiterverkabelung
6: Zusätzliche Festlegungen für die Verlegung metallener Verkabelung
7: Zusätzliche Festlegungen für die Verlegung von Lichtwellenleiterverkabelung
- EN 50174-3 - Installation von Kommunikationsverkabelung, Installationsplanung und -praktiken im Freien
- EN 50310 - Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Gebäude
6.3: AC-Verteilung und Anschluss des Schutzleiters (TN-S)
- EN 50346 - Installation von Verkabelung, Prüfen installierter Verkabelung
4: Allgemeine Anforderungen
5: Prüfparameter für symmetrische Verkabelung
6: Prüfparameter für Lichtwellenleiterverkabelung

**Betrieb**
- EN 50174-1 - Installation von Kommunikationsverkabelung, Spezifikation und Qualitätssicherung
5: Qualitätssicherung
7: Verwaltung der Verkabelung
8: Instandsetzung und Instandhaltung

Prüffragen:

- Wurden im Rahmen der Planung des Gebäudes und der IT-Verkabelung die einschlägigen Normen wie EN 50310, EN 50173 und EN 50174 berücksichtigt?

# M 1.67 Dimensionierung und Nutzung von Schranksystemen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Zur Verbesserung der Betriebssicherheit von Servern, aktiven und passiven Netzkomponenten sollten diese Geräte in Schranksystemen eingebaut oder aufgestellt werden. Schranksysteme werden je nach Einsatzart häufig als 19-Zoll-Rack, Serverschrank oder auch Netzschrank bezeichnet.

Systemschänke sind nach DIN IEC 60297 und DIN 41494 *"Bauweisen für elektronische Einrichtungen"* genormt. Dadurch ist der Einbau beliebiger Geräte möglich, solange diese auch den genannten Normen entsprechen. Komponenten, die den oben genannten Normen entsprechen, sind häufig an dem Stichwort "19-Zoll-Einbau" erkennbar.

Schranksysteme gibt es in verschiedenen Innen- und Außenmaßen. Die größte Verbreitung haben Schränke mit einem Netto-Raumangebot von 42 Höheneinheiten (HE). Abhängig davon, ob die Schranksysteme in abgeschlossenen Verteilerräumen aufgestellt sind oder in allgemein zugänglichen Bereichen, müssen diese mit angepassten Türen, Seitenwänden und Schließungen ausgestattet werden, die dem jeweiligen Schutzbedarf entsprechen. Sockel unter den Schränken erleichtern die Einführung der erforderlichen Verkabelung. Ein weiterer Vorteil eines Sockels ist der zusätzliche Abstand zwischen dem Raumboden und den IT-Systemen. In diesem Fall führt ein möglicher Wassereintritt durch die erhöhte Positionierung der Geräte nicht automatisch zu Schäden an den IT-Systemen. Bei entsprechend abgesicherten Verteilerräumen kann auf Türen und Seitenwände nach Überprüfung der Umgebungsbedingungen verzichtet werden.

Der schrankinterne Aufbau sollte unbedingt wartungstechnischen Gesichtspunkten Rechnung tragen. Beispielsweise sollte ein schnellstmöglicher Austausch von Baugruppen in einem gepatchten Switchingsystem ohne nachteilige Beeinflussung benachbarter Systeme möglich sein. Dies setzt den vorausschauenden Einbau aller Komponenten und ein entsprechendes Management von Patchkabeln voraus. Von Vorteil ist es daher, wenn die elektrotechnische Verkabelung und die IT-Verkabelung stabil und geschützt geführt werden können. Viele Hersteller von Schranksystemen bieten Einbauteile an, mit denen die schrankinterne Kabelführung an spezifische Anforderungen und Wünsche des Anwenders angepasst werden kann. Überlängen von Patchkabeln sind zu vermeiden.

Bei der Planung der Schrankbelegung ist zu beachten, dass die Kapazität des Schrankes meistens durch die Wärmeabgabe der eingebauten Geräte und nicht durch die möglichen Einbaumaße beschränkt ist. Es kann zu Problemen der Wärmeabfuhr kommen, wenn die thermische Last der eingebauten Geräte zu groß ist.

Ähnliche Probleme können in Netzschränken entstehen, die sehr viele passive Komponenten (Patchfelder) enthalten und eine zu dichte Belegung mit Kabeln aufweisen.

In diesem Fall kann die Luftdurchströmung des Schrankes derart gestört werden, dass Bauteile oder aktive Komponenten Fehlfunktionen erleiden. Auch

dieser Aspekt muss bei der Planung der Schrankbelegung berücksichtigt werden.

Bei nebeneinander aufgestellten Schränken muss zusätzlich auf die Luftführung der aktiven Komponenten in benachbarten Schränken geachtet werden. Es ist unbedingt zu vermeiden, dass die von Komponenten ausströmende Warmluft die Kaltluftzufuhr einer benachbarten Komponente beeinträchtigt. Mit der Schottung der Einzelschränke in der Schrankreihe kann dieser Problematik begegnet werden.

Damit die aktiven Komponenten innerhalb der vorgeschriebenen Temperaturbereiche betrieben werden können, sind die Schränke entsprechend auszustatten. Im einfachsten Fall reicht eine passive Kühlung des Schrankes bei ausreichend kühler Umgebungsluft im Raum aus. Diese kann bei geschlossenen Schränken durch Lüftersysteme im Schrank unterstützt werden. Sind die Wärmelasten zu groß, können aktive Kühlsysteme unterschiedlicher Bauart verwendet werden. Zu unterscheiden sind dabei Möglichkeiten der Raumkühlung einerseits und andererseits Kühlsysteme, welche an oder auf den Schränken angebracht werden können.

Um IT-Komponenten betreiben zu können, die eine sehr hohe Wärmeabgabe bei geringem Platzbedarf aufweisen, kann der Einsatz spezieller Schranksysteme mit eigenständigen Klimasystemen erwogen werden. Solche Schränke, die intern meist eine Flüssigkeitskühlung aufweisen, sollten nur nach einer sorgfältigen Bedarfs- und Risikoanalyse verwendet werden.

Jegliche Art der Klimatisierung erfordert eine genaue Planung unter Berücksichtigung aller beeinflussenden Parameter einschließlich einer entsprechenden Wirtschaftlichkeitsbetrachtung. Beim Einsatz von Schränken mit eigener Klimatisierung ist zudem darauf zu achten, dass Klimageräte an Seitenwänden oder Türen den Öffnungswinkel von Schranktüren verringern können und unter Umständen in Fluchtwege hineinragen. Das Raumlayout sollte möglichst so geplant werden, dass Klimatechnik an Schränken im Bedarfsfall nachgerüstet werden kann.

Es ist empfehlenswert, in der Institution einheitliche Vorgaben für die Ausstattung und Nutzung von Schranksystemen zu machen. Auch die Verkabelung der Schränke untereinander ist sorgfältig zu planen (siehe auch M 1.69 *Verkabelung in Serverräumen*).

Prüffragen:

- Besitzen die Schranksysteme dem Schutzbedarf der darin eingebauten IT-Systeme entsprechende Sicherheitseigenschaften?
- Sind die eingesetzten Schranksysteme für die Wartbarkeit und Kühlung der darin eingebauten IT-Komponenten geeignet?
- Existieren einheitliche Vorgaben für die Auswahl und Ausstattung der eingesetzten Schranksysteme?

# M 1.68 Fachgerechte Installation

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Die Installationsarbeiten der IT-Verkabelung erfordern besondere Fachkunde und Sorgfalt. Sofern Hersteller von Kabeln und passiven Komponenten Gewährleistungen anbieten, die über gesetzliche Mindestgrenzen hinaus gehen, erfolgt dies oft nur unter der Voraussetzung, dass ein Unternehmen mit bestätigter Qualifikation die Installation vornimmt.

Die entscheidenden Kriterien für eine fachgerechte Ausführung der IT-Verkabelung sollten vom Auftraggeber in allen Phasen überprüft werden.

Zunächst ist bei Anlieferung des Materials zu prüfen, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Zueinander passende Kategorien von Kabeln und Anschlusskomponenten (z. B. Schirmung) sind dabei der erste Prüfschritt.

Wenn die gelieferten Kabel und zugehöriges Material nicht unmittelbar eingebaut werden, so ist eine angemessene Lagerung sicherzustellen. Der Lagerort muss trocken und vor starken klimatischen Einflüssen geschützt sein.

Es wird empfohlen, das eingelagerte Material in der Originalverpackung zu belassen, bis es installiert wird.

Bei der Verlegung von IT-Kabeln sollte besondere Sorgfalt darauf gelegt werden, dass die Montage keine Beschädigungen hervorruft und dass die Kabelwege so gewählt sind, dass Beschädigungen der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen sind.

Zudem ist generell darauf zu achten, dass IT-Kabel getrennt von der elektrotechnischen Verkabelung geführt werden. Schon Trennstege auf gemeinsam genutzten Trassen helfen meist, Beeinflussungen des IT-Kabels durch Stromkabel zu verhindern.

Bei der Verlegung müssen schützende Maßnahmen und Belastungsgrenzen beachtet werden:

- Vor der Verlegung müssen Mauerdurchbrüche und vergleichbare Durchgänge entgratet und gerundet werden, um beim Einziehen und Befestigen eine mechanische Beschädigung der Kabelummantelung zu vermeiden.
- Der Mindest-Biegeradius für Verlegung und Betrieb darf nicht unterschritten werden. Falls dieser nicht auf dem Kabel vermerkt ist, gilt nach EN 50173, dass der geringst zulässige Biegeradius nicht kleiner als der 8-fache Außendurchmesser des Kabels sein darf. Entsprechend ist sicherzustellen, dass Biegungen in Kabelkanälen und Kabeltrassen den zulässigen Biegeradien entsprechen.
- Gegebenenfalls gibt der Hersteller in Datenblätter zu den Kabeln typspezifisch zwei Biegeradien an: der angegebene Biegeradius mit dem größeren Wert gilt als maximale Biegebelastung für das Einziehen der Kabel. Der kleinere Wert gilt für das fertig verlegte Kabel.
- Ebenfalls ist dem Datenblatt die maximale Zugbelastung des Kabeltyps zu entnehmen.
- Beim Kabeleinzug dürfen nur geeignete Schmiermittel als Einzugshilfe verwendet werden. Generell sind öl- und fettfreie Schmiermittel (z. B. Talkum) einzusetzen.

- Bei der Befestigung der Kabel auf Kabeltrassen mit Kabelbindern oder Kabelschellen dürfen die Kabel keinesfalls gequetscht werden.

Kabel sollten unter Putz, in Kabelkanälen oder auf Kabeltrassen verlegt werden. Die offene Verlegung von Kabeln ist durchaus zulässig, es ist aber sicherzustellen, dass keine Beschädigung des Kabels etwa durch Überfahren von Kabeln mit Büromöbeln oder Transportgeräten auftreten kann.

Prüffragen:

- Ist die IT-Verkabelung unter Einhaltung der gültigen Normen sowie der Herstellervorgaben fachgerecht installiert?

# M 1.69 Verkabelung in Serverräumen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, Planer

Auch und gerade in Serverräumen und Rechenzentren müssen die Grundsätze der strukturierten Verkabelung nach EN 50173-1 *"Informationstechnik - Anwendungsneutrale Kommunikationskabelanlagen - Teil 1: Allgemeine Anforderungen"* beachtet werden. Eine speziell für Rechenzentren erarbeitete Erweiterung EN 50173-5 ist als Norm-Entwurf erschienen. Die Umsetzung der Anforderungen der Norm wird damit für den Anwender erleichtert.

Die Anforderungen aus dem vorhandenen oder geplanten Netzkonzept der Institution bilden die Grundlage für die Strukturierung der IT-Verkabelung in Serverräumen und Rechenzentren. Die Struktur legt fest, wie die Server vernetzt werden und wie sie an das LAN, an externe Netze und an Provider angebunden werden. In der Institution eingesetzte oder geplante betriebsunterstützende Systeme, wie z. B. Terminalserver, KVM-Switches und SAN/NAS (Storage Area Network, Network Attached Storage), sind vorausschauend zu berücksichtigen. Die Grundlagen für die Struktur der so genannten Access- und Konzentrationsbereiche der IT-Verkabelung in Analogie zu den Gebäudestrukturen mit Etagenverteilern und Gebäudeverteilern sind damit festgelegt.

In größeren Installationen werden häufig Gruppen von Schränken, in denen Server aufgestellt sind, einem "Netzschrank" zugeordnet. Zwischen Netzschränken und den zugeordneten Serverschränken wird eine feste Verkabelung oder eine spezielle Systemverkabelung für Serverräume verlegt. Die Netzschränke wiederum sind untereinander nach Anforderung der Institution verbunden.

Um die Fläche des Serverraums bzw. Rechenzentrums bestmöglich zu nutzen, ist es erforderlich, ein auf die Anforderungen abgestimmtes Raumlayout zu entwickeln. In diesem Raumlayout sind die benötigten Flächen für die Schränke mit den Systemen, die die Institution betreibt (neben Servern auch Speichersysteme und aktive und passive Netzkomponenten), mit Reserven für die Zukunft zu gliedern. Es müssen dabei Sicherheitsaspekte wie die Anordnung der Fluchtwege, Betriebsaspekte wie die Anordnung der Transportwege und auch klimatechnische Gesichtspunkte berücksichtigt werden. Auf dieser Grundlage kann die Planung der elektrotechnischen Versorgung und der Trassenführung erfolgen.

Die Verwendung eines hochbelastbaren Doppelbodens ist für Serverräume und Rechenzentren zu empfehlen (siehe M 1.49 *Technische und organisatorische Vorgaben für das Rechenzentrum*). Wird der Doppelboden in die Luftführung der Schrankklimatisierung mit einbezogen, so sind die Trassensysteme zu berücksichtigen. Durch viele querende Trassen zwischen Frischluftzuführung in den Doppelböden und weiter entfernt davon stehenden Schränken, die eine hohe Wärmelast aufweisen, können "Wärmenester" entstehen. Obwohl die Klimaleistung für den Raum ausreichend bemessen ist, erhalten einige Schränke und die darin stationierten IT-Komponenten zu wenig gekühlte Luft. Das birgt die Gefahr von Ausfällen von Servern oder aktiven Netzkomponenten durch Überhitzung.

Zudem ist unbedingt auf eine nicht staubende Versiegelung des Estrichs bzw. Rohfussbodens zu achten.

Es ist zu empfehlen, so umfassend wie möglich fest zu verkabeln. Dies fördert eine fachgerechte Belegung der Trassensysteme im Doppelboden oder unter der Decke. Server sollten möglichst nicht mit Patchkabeln ohne zusätzliche Trassensysteme an zentral im Raum stationierte Server-Switches angeschlossen werden, auch wenn diese Verkabelungsart in der Praxis häufig angewandt wird. Eine solche "fliegende Verkabelung" ist besonders bei Nachverkabelungen gefährdet.

Auf die Anforderungen der Institution abgestimmte Schranksysteme, in denen Systeme zur Kabelführung und Überlängenablage vormontiert sind, erlauben eine übersichtliche und wartungsfreundliche Kabelführung im Schrank.

Auch wenn nur wenige Schränke vernetzt werden, ist es zweckmäßig, in den Schranksystemen Patchfelder für den Anschluss der Server und eine feste Verbindung dieser Patchfelder an den Netzknoten im Serverraum zu installieren. Wenn eine Neukonzeption ansteht, ist es zum Beispiel zu erwägen, pro Schrank ein Patchfeld für Kupferkabel der Kategorie 6 oder 7 (CAT-6 oder CAT-7, tauglich für 10 Gigabit-Anschluss) und gegebenenfalls zusätzlich ein LWL-Patchfeld vorzurüsten. Letzteres kann beispielsweise zum Anschluss der Server an Speichernetze dienen. Selbstverständlich ist die Vorrüstung von Schränken auf die Planungen der Institution abzustimmen.

Wenn keine baulichen Gründe dagegen sprechen, ist in vielen Fällen eine Kabelführung über Trassen, die unter der Decke des Serverraums verlaufen, der Kabelführung durch den Doppelboden vorzuziehen. Insbesondere wenn der Doppelboden der Klimatisierung dient, kann eine Doppelboden-Verkabelung die Führung der benötigten Kühlluft beeinträchtigen. Außerdem birgt die Verlegung der Kabel im Doppelboden erfahrungsgemäß die erhöhte Gefahr, dass nicht mehr benötigte Kabel nicht entfernt werden. Bei einer Verlegung der Kabel in gut zugänglichen Deckentrassen ist das Entfernen alter Kabel in der Regel deutlich einfacher.

Prüffragen:

- Werden die Grundsätze der strukturierten Verkabelung nach geltenden Normen in Serverräumen und Rechenzentren eingehalten?
- Basiert die IT-Verkabelung auf dem Netzkonzept der Institution und berücksichtigt dabei sicherheitstechnische und betrieblichen Anforderungen?

# M 1.70 Zentrale unterbrechungsfreie Stromversorgung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

Mit einer unterbrechungsfreien Stromversorgung (USV) kann ein kurzzeitiger Stromausfall überbrückt werden oder die Stromversorgung solange aufrechterhalten werden, dass ein geordnetes Herunterfahren angeschlossener Rechner möglich ist. Dies ist insbesondere dann sinnvoll,

- wenn im Rechner umfangreiche Daten zwischengespeichert werden (z. B. Cache-Speicher im Netz-Server), bevor sie auf nichtflüchtige Speicher ausgelagert werden,
- beim Stromausfall ein großes Datenvolumen verloren gehen würde und nachträglich nochmals erfasst werden müsste,
- wenn die Stabilität der Stromversorgung nicht ausreichend gewährleistet ist.

Drei USV-Arten sind zu unterscheiden:

- VFD-USV (Voltage and Frequency Dependent)
  Hierbei werden die angeschlossenen Verbraucher im Normalbetrieb direkt aus dem Stromversorgungsnetz gespeist. Erst wenn dieses ausfällt, schaltet sich die USV selbsttätig zu und übernimmt die Versorgung. Dazu benötigt eine VFD-USV bis zu 10 ms (Umschaltlücke), was für manche IT-Geräte schon zu viel sein kann. Da die VFD-USV im Normalbetrieb nicht an der Stromversorgung der angeschlossenen Verbraucher beteiligt ist, wurde sie früher auch Offline-USV genannt.
  VFD steht für Voltage and Frequency Dependent, also dafür, dass im Normalbetrieb der Ausgang der USV sowohl hinsichtlich der Spannung als auch der Frequenz direkt vom Eingang abhängig ist. Das bedeutet, dass kleinere Störungen im Versorgungsnetz direkt bis zu den von einer VFD-USV gespeisten Verbrauchern gelangen können.
- VI-USV (Voltage Independent)
  Bei einer VI-USV wird die Versorgungsspannung bei kleineren Schwankungen nachgeregelt (VI steht für Voltage Independent), ohne dass die USV als solche die Versorgung der angeschlossenen Verbraucher komplett übernimmt. Die Frequenz am Ausgang einer VI-USV ist aber wie bei einer VFD-USV direkt vom Versorgungsnetz abhängig. Auch bei der VI-USV kann es bei der Umschaltung auf Batteriebetrieb zu einer Umschaltlücke kommen.
- VFI-USV
  Bei der VFI-USV (Voltage and Frequency Independent) gibt es im Normalfall keine direkte Verbindung mehr zwischen USV-Eingang und -Ausgang. Die gesamte elektrische Energie wird eingangsseitig gleichgerichtet und in den Zwischenkreis gespeist. Von dort werden die Batterien im optimalen Ladezustand gehalten und der Wechselrichter versorgt.
  Erst dieser erzeugt die für die angeschlossenen Verbraucher erforderliche Wechselspannung.
  Die VFI-USV ist also ständig zwischen Netz und Verbraucher geschaltet. Dadurch entsteht keine Umschaltlücke, weshalb nur die VFI-USV wirklich unterbrechungsfrei ist. Da die gesamte Stromversorgung hier immer über die USV läuft, wurde sie früher auch als Online-USV bezeichnet.

Werden diese drei USV-Typen im Vergleich betrachtet, steht außer Frage, dass die VFI-USV die mit dem besten Ausgangsverhalten ist und mindestens

für die Versorgung empfindlicher IT-System zu bevorzugen ist. Unter Berücksichtigung weiterer, hier nicht behandelter Qualitätsmerkmale stellt eine USV, die nach DIN IEC 62040-3 gemäß VFI-SS-111 klassifiziert ist, das Optimum für die IT-Versorgung dar.

Entgegen einer immer wieder geäußerten Annahme stellt eine USV gleich welcher Bauart keinen Überspannungsschutz im eigentlichen Sinn dar. Eine USV ist zwar in der Lage, im Rahmen ihrer normalen Funktion zu hohe Spannungen von den angeschlossenen Verbrauchern fernzuhalten. Gegen Überspannungen, wie sie durch die technischen Einrichtungen des Überspannungsschutzes abgefangen werden, hilft aber eine USV keinesfalls. Im Gegenteil, eine USV muss wie alle anderen elektrischen Verbraucher durch geeignete Schutzmaßnahmen gegen Überspannungen geschützt werden (siehe M 1.25 *Überspannungsschutz*).

Bei der Dimensionierung einer USV sind zwei Aspekte von Bedeutung: die Stützzeit und die Ausgangsleistung.

Für die Festlegung der Stützzeit ist der Zweck des USV-Einsatzes, die Art der versorgten IT und die Existenz weiterer energiesichernder Maßnahmen zu berücksichtigen.

Ist die USV-versorgte IT in der Lage, nach einem schlagartigen Abschalten der Stromversorgung und deren Wiederkehr problemlos wieder an- und weiterlaufen, reicht es aus, die USV für kurzfristige Stromausfälle auszulegen. Da die meisten Stromausfälle binnen weniger Minuten behoben sind, erscheint hierfür eine Überbrückungszeit von 10 bis 15 Minuten angemessen.

Macht die IT hingegen ein geordnetes Herunterfahren erforderlich, dürfte eine so kurze Stützzeit nicht ausreichen. Hier ist es sinnvoll, nach Beginn des Stromausfalls erst eine Weile zu warten und nicht sofort die Systeme herunter zu fahren. Diese Wartezeit ist mit circa 10 Minuten anzusetzen. Die für das Herunterfahren (Shutdown) erforderliche Zeit ist sehr unterschiedlich und muss für die angeschlossenen IT-Systeme individuell ermittelt werden. Als Faustformel für die Stützzeit ergibt sich für solche Fälle:

*Stützzeit = Wartezeit plus zweifache Shutdown-Zeit*

Typische Werte für die Stützzeit liegen bei 30 bis 60 Minuten. Der doppelte Ansatz der Shutdown-Zeit bewirkt ein Sicherheitspolster.

Für spezielle Anwendungsfälle (z. B. TK-Anlagen) kann die erforderliche Stützzeit auch mehrere Stunden betragen. Bei jedem Austausch oder Ergänzung von Geräten, die durch eine USV versorgt werden, muss erneut geprüft werden, ob die vorhandene Stützzeit ausreicht.

Änderungen der erforderlichen Stützzeit lassen sich relativ einfach durch eine Anpassung der Batteriekapazität vornehmen. Bei der Ausgangsleistung sieht das anders aus. Die maximale Ausgangsleistung wird durch die in den Gleich- und Wechselrichtern eingebauten elektronischen Bauteile bestimmt. Hier ist eine einfache Nachrüstung und damit Erhöhung der Ausgangsleistung meist nicht oder nur durch umfangreiche Umbauten möglich. Bei der Festlegung der Ausgangsleistung sollte man also ausreichende Reserven einplanen.

Empfindlichster Teil einer USV ist die Batterie. Nur wenn diese bei der vom Hersteller genannten optimalen Temperatur (typischerweise um 20°C) untergebracht wird, kann sie ihre maximale Leistung und Lebensdauer erreichen. Pro 10 Kelvin, um die diese Solltemperatur überschritten wird, vermindern sich

Leistung und Lebensdauer um circa 50 %. Damit wird deutlich, dass besonders bei großen USV-Systemen die kälteliebende Batterie und die wärmeerzeugende Leistungselektronik keinesfalls in einen gemeinsamen Raum gehören. Um sicher zu stellen, dass die USV die erforderliche Stützzeit bereitstellt, sollte etwa einmal pro Jahr die tatsächliche Stützzeit ermittelt werden. Manche USV-Systeme verfügen dazu über eingebaute Prüfmechanismen. Ist das nicht der Fall, kann der Wert durch einen Lasttest ermittelt werden.

Da die USV die letzte Bastion gegen den Stromausfall vor der IT-Hardware ist, kommt ihr große Bedeutung für die Sicherstellung der Verfügbarkeit zu. Sie hat also denselben Schutzbedarf wie die durch die USV versorgte IT. Wenn die USV-versorgten IT-Systeme redundant ausgelegt sind, sollten auch USV-Systeme redundant vorhanden sein. Ergänzend sei hier auf M 1.52 *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur* hingewiesen.

Außerdem ist bei einer USV besonders auf den Schutz vor dem Zugriff Unbefugter, Brand und Wasser zu achten. Ein sinnvoller Schutz gegen Brand macht es nahezu unverzichtbar, einander Redundanz bietenden USV-Einheiten in getrennten Brandabschnitten unterzubringen. Nur so kann verhindert werden, dass bei Brand einer Einheit nach kurzer Zeit auch alle anderen durch Brand ausfallen.

Wie bei allen anderen elektrischen Geräten ist auch bei USV-Systemen darauf zu achten, dass sie in den vom Hersteller genannten Temperaturbereichen betrieben werden. Dies ist bei der Dimensionierung der Kühlung zu berücksichtigen.

Um die Schutzwirkung einer USV aufrechtzuerhalten, muss sie regelmäßig gewartet werden. Dafür sind die vom Hersteller vorgesehenen Wartungsintervalle der USV einzuhalten.

Prüffragen:

- Wird sichergestellt, dass die Batterie im erforderlichen Temperaturbereich gehalten wird?
- Werden die Wartungsintervalle der USV eingehalten?
- Wird die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV regelmäßig getestet?
- Wird erneut geprüft, ob die Stützzeit ausreichend ist, wenn Änderungen bei den Verbraucher durchgeführt wurden?

# M 1.71 Funktionstests der technischen Infrastruktur

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Im Bereich der technischen Infrastruktur werden leider echte Funktionstests immer noch äußerst selten durchgeführt. So wird z. B. die ordnungsgemäße Funktion der Notenergieversorgung oder das korrekte Zusammenspiel von Klimatisierung und Brandschutz zu selten getestet. In vielen Fällen wird zwar ein hoher Aufwand für die Ausfallvorsorge betrieben, trotzdem werden die umgesetzten Maßnahmen häufig nicht getestet, da Folgeschäden durch die Tests befürchtet werden. Die stattdessen durchgeführten Tests sind aber nicht geeignet, die gesamte Reaktionskette, wie sie im Echtfall ablaufen muss, wirklich zu prüfen. Grundsätzlich gilt jedoch, dass es besser ist, Tests durchzuführen und eventuelle Folgeschäden im Testbetrieb zu behandeln (und daraus zu lernen), als unerwartet von diesen Folgeschäden im Echtbetrieb getroffen zu werden, wenn Notfallmaßnahmen aktiviert werden. Eine Inspektion der technischen Infrastruktur beschränkt sich in aller Regel jeweils auf die einzelne betrachtete technische Einrichtung, z. B. die Energieversorgung. Allenfalls werden noch die Schnittstellen zu funktional benachbarten Einrichtungen behandelt. Eine umfassende Betrachtung ganzer Funktionsketten erfolgt hingegen meist nicht. Eine typische Funktionskette ist die Aufeinanderfolge der Reaktionen "Stromnetz fällt aus, NEA läuft automatisch an". Diese Funktionskette kann nicht hinreichend getestet werden, indem ein Handstart der NEA durchgeführt und anschließend die Energieversorgung weggeschaltet wird, da damit nicht kontrolliert wurde, wie bei einem spontanen Ausfall der Primärenergie die Funktionskette reagiert.

Generell kann durch eine klassische Inspektion die ordnungsgemäße Funktion komplexer Reaktionsketten nicht mit ausreichender Sicherheit festgestellt werden. So kommt es immer wieder dazu, dass trotz optimaler Inspektion und Wartung aller einzelnen Einheiten, das Gesamtsystem im Fall eines Ausfalls nicht wie geplant funktioniert.

Beispiel: In einem konkreten Fall war die NEA sowie die Netzausfallerkennung einschließlich des angesetzten Signals als funktionsfähig inspiziert worden. Bei einem Stromausfall hat dann auch die Netzausfallerkennung richtig reagiert und ein Signal an die Netzersatzanlage (NEA) abgesetzt. Diese hat aber aus unbekannten Gründen das Signal nicht richtig interpretiert und ist daher nicht gestartet, obwohl die NEA bei der Inspektion mit dem vom NEA-Hersteller vorgesehenen Signal angesteuert wurde und bei diesem Einzeltest ordnungsgemäß reagiert hat.

Es ist daher unerlässlich, Reaktionsketten einem echten Funktionstest (Echttest) zu unterziehen. Das heißt, dass die zu testenden Einrichtungen als komplettes System gezielt mit dem Problem konfrontiert werden, zu dessen Bewältigung sie vorgesehen sind. Da es Zweck eines solchen Echttests ist, nur im Gesamtsystem erkennbare Fehler festzustellen, muss damit gerechnet werden, dass eben solche Fehler auftreten, und die Reaktion nicht in der geplanten Weise erfolgt.

Daher sollten Echttests nicht in Hauptbetriebszeiten durchgeführt und Vorbereitungen getroffen werden, um die Folgen eventuell auftretender Fehler beherrschen zu können. Letzteres sollte ohnehin Teil der Notfallvorsorge sein.

Echttests der technischen Infrastruktur eines Rechenzentrums sollten alle ein bis zwei Jahre sowie nach Systemumbauten und umfangreichen Reparaturen durchgeführt werden.

Prüffragen:

- Werden für alle wesentlichen Reaktionsketten echte Funktionstest durchgeführt?
- Werden die Funktionstests in regelmäßigen Abständen durchgeführt?

# M 1.72 Baumaßnahmen während des laufenden Betriebs

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Aus wirtschaftlichen Gründen ist es oftmals ratsam, statt einen Serverraum oder ein Rechenzentrum neu zu bauen, die bestehenden Fläche der vorhandenen IT-Räume durch die Integration benachbarter Flächen zu erweitern. Solche Flächenerweiterungen haben oftmals erhebliche Eingriffe in die bestehende Bauwerksstruktur zur Folge, weil Wände verändert, entfernt oder auch neu gebaut werden müssen. Weiterhin sind die Erweiterungsflächen mit der entsprechenden Infrastruktur (Doppelboden, Elektroversorgung, Klimatisierung, Sicherheitstechnik, etc.) auszustatten, so dass auch hier Arbeiten massiven Ausmaßes anfallen.

Um die Geschäftstätigkeit der Institution nicht einzuschränken, ist es häufig notwendig, die bestehende IT-Infrastruktur während der Bauarbeiten weiter zu betreiben. Gleichzeitig sollen die Baumaßnahmen durch den laufenden IT-Betrieb möglichst nicht eingeschränkt oder Auflagen unterworfen werden, damit sich die Kosten nicht über das erforderliche Maß hinaus erhöhen.

Zunächst ist planerisch und durch vorbereitende Änderungen der Infrastruktur sicher zu stellen, dass die unterstützende Technik wie beispielsweise Stromversorgung, Klimatechnik, überwachende und alarmierende Technik, durch die Baumaßnahmen nicht beeinträchtigt wird und weiter funktionsfähig bleibt. Anschließend ist der betroffene Bereich, in dem die IT betrieben wird, vor Verunreinigung, aber auch vor unbefugtem Zutritt zu bewahren. Gleichzeitig sollte die Baustelle nicht unnötig behindert werden. Bewährte Maßnahmen zum Schutz vor Verunreinigungen sind:

- Erstellen einer Folien-Staubschutzwand
- Erstellen einer Staubschutzwand aus Gipskarton-Bauplatten (GKB)
- Abkleben oder Ausspritzen von Fugen und Bauwerksspalten
- Einsatz von Luftreinigern
- Erzeugung von Unterdruck im Baustellenbereich
- Anwendung von speziellen Arbeitsverfahren

Eine Folien-Staubschutzwand kommt lediglich für kurze Baumaßnahmen mit minimaler Staubentwicklung in Betracht. Dabei wird schwere Baufolie auf einem Holzständerwerk angebracht. Die entstehenden Fugen zu angrenzenden Bauteilen sowie Durchdringungen der Folie (z. B. für erforderliche Leitungen) werden mittels Klebeband verschlossen.

Bei dieser Ausführung besteht jedoch die Gefahr, dass durch eine Beschädigung der Folie die Staubschutzwirkung wegfällt. Ebenso wird so keine sichere Durchgangssperre geschaffen, so dass zusätzliche Maßnahmen nötig werden, damit keine Unbefugten in die Betriebsbereiche gelangen können.

Einfache Folien-Staubschutzwände (ohne die Errichtung eines festen Ständerwerks) werden oft temporär erstellt, um eine GKB-Staubschutzwand errichten zu können, bei der durch die notwendigen Bohrungen mit einer geringen Staubentwicklung zu rechnen ist.

In den meisten Fällen ist der Aufbau einer GKB-Staubschutzwand dringend zu empfehlen. Dabei wird der ein ausreichender Staubschutz schon durch eine einseitige doppelte Beplankung des Ständerwerks erreicht. Diese doppelte

Beplankung verhindert, dass der zu schützende Bereich durch Feinstaub kontaminiert wird, der sonst problemlos durch die Plattenstöße gelangen kann.

An das bestehende Bauwerk angearbeitete Flächen sowie unvermeidbare Arbeitsfugen sollten durch eine elastische Dichtungsmasse abgedichtet werden, um auch hier den Durchtritt von Staub zu verhindern. Wandöffnungen und Kabeldurchführungen sind zu vermeiden. Ist das nicht möglich, sind diese durch geeignete Schottungen so zu verschließen, dass auch hier eine größtmögliche "Staubdichte" gewährleistet wird.

Die Integration von Türen in Staubschutzwände ist grundsätzlich möglich, bedeutet aber eine erhebliche Schwachstelle beim Staubschutz. Die Türöffnung sollte unbedingt als Schleuse ausgeführt werden, damit Zugluft und ein damit verbundener Staubtransport in die IT-Räume vermieden wird. Die Ausbildung einer solchen Schleuse mit doppelt hintereinander gehängter Baufolie ist als Staubschutz keinesfalls ausreichend.

Es sind möglichst zugdichte Baustellentüren einzubauen. Sehr große Spaltmaße in der eingesetzten Baustellentür können beispielsweise behelfsweise mit Gummilippen abgedichtet werden.

Ein weiterer Vorteil dieser massiven Staubschutzwand ist die physische Trennung des Baustellenbereiches von den Rechenzentrumsflächen, da nach der Erstellung der GKB-Wand keiner der Bauarbeiter direkten Zugang zu den RZ-Flächen hat.

Bei der Durchführung der Bauarbeiten hat es sich bewährt, im Baustellenbereich mit einem ständigen Unterdruck zu arbeiten. Bei diesem Verfahren saugt ein Ventilator die Luft im Baustellenbereich an und führt sie über ein geschlossenes System nach außen. Hierdurch wird gewährleistet, dass ein Großteil des entstehenden Staubes direkt abgeführt wird und der verbleibende Staub nicht in den benachbarten Bereich gelangen kann. Durch eventuell vorhandene Undichtigkeiten wird allenfalls die staubarme Luft des RZ-Bereichs in den Baustellenbereich gesogen. Ein Nachteil dieser Maßnahme ist, dass eine Ausblasöffnung für das Abführen der Abluft in der Fassade benötigt wird.

Bei Arbeiten mit starker Staubentwicklung kann es auch empfehlenswert sein, auf der Bauseite Luftreiniger einzusetzen. Dabei ist die Luftreinigung durch Luftfilterung (sogenannte Entstauber) zu bevorzugen. Bei einer Luftreinigung auf Wasserbasis wird die Luft bis zur Sättigungsgrenze befeuchtet, so dass bei höheren Raumtemperaturen ein "subtropisches" Klima die Arbeiten erschwert.

Als weitere Maßnahmen zum Staubschutz können besondere Arbeitsverfahren geforderte werden:

- der Einsatz von speziellen Nass-Bohr- oder -Schneidverfahren
- die Absaugung von Stäuben direkt am Entstehungsort mittels fest installierter oder mobiler Absauganlage (Ausblasen der Luft direkt nach außen oder Filterung der Luft)
- das Aufsaugen des Staubs einer Bohrung mittels Staubsauger
- die Aufnahme und Transport von Abbruchmaterial mit Staubsaugern oder entsprechenden Kehrzeugmaschinen
- Ausschluss der Reinigung mit Besen oder mittels Druckluft

Die Einhaltung von geltenden Vorschriften wie beispielsweise die Berufsgenossenschaftliche Regel für Sicherheit und Gesundheit bei der Arbeit BGR 217 "Umgang mit mineralischem Staub" oder die Technische Regel für Gefahrstoffe TRGS 500 "Schutzmaßnahmen Mindeststandards" sollte regelmä-

ßig vom Auftraggeber oder dem von ihm eingesetzten Sicherheits- und Gesundheitsschutzkoordinator kontrolliert werden.

Zum Abschluss der Bauarbeiten ist eine Baufeinreinigung durchzuführen. Falls die nicht durch eigene Arbeitskräfte durchgeführt wird, ist sie explizit in die Ausschreibung aufzunehmen, da sie über die in der VOB (Vergabe- und Vertragsordnung für Bauleistungen) definierte Baureinigung durch Auftragnehmer hinausgeht.

**Beispiel:**
Nach Umbau eines größeren Serverraums wurde vom Auftragnehmer eine scheinbar gründliche Endreinigung vorgenommen. Eine Inspektion der gereinigten Räume zeigte jedoch, dass die Doppelbodenplatten nicht gereinigt worden waren. Auf der gesamten Stützen- und Strebenkonstruktion des Doppelbodenunterbaus befanden sich noch beträchtliche Mengen an Sägestaub. Dieser wäre ohne diese Kontrolle und Nachreinigung bei Betriebsaufnahme durch die Umluftgeräte aufgewirbelt worden und hätte bereits montierte IT-Komponenten wie Patchfelder, Switches und Server massiv verschmutzt.

Neben dem Staubschutz ist bei Umbaumaßnahmen sicherzustellen, dass die weiterbetriebene IT ausreichend gekühlt wird. Bei Luftkühlung ist die zusätzliche Staubbelastung durch die Umbaumaßnahmen zu berücksichtigen.

Es ist ratsam, entsprechende Hinweise für alle geforderten Maßnahmen in die Leistungsverzeichnisse aufzunehmen, um Missverständnisse und teure Nachträge der Auftragnehmer zu vermeiden.

Durch die Bautätigkeiten entstehen aber nicht nur Staub und Unruhe, sondern es könnte auch die vorhandene Technik durch Unachtsamkeit oder fehlerhafte Planung beschädigt werden (z. B. Anbohren von Leitungen). Außerdem arbeitet dabei auch typischerweise wechselndes Fremdpersonal an vielen Stellen gleichzeitig. Hier muss dafür gesorgt werden, dass dieses entweder adäquat beaufsichtigt werden kann oder die IT-Bereiche von den Bereichen mit Bautätigkeiten so abgetrennt werden, dass dort kein unbefugter Zutritt möglich ist.

Prüffragen:

- Sind Auflagen zur Durchführung von Staubschutzmaßnahmen detailliert in den Text zur Ausschreibung von Umbaumaßnahmen in IT-Räumen eingeflossen?
- Ist die Beaufsichtigung von Fremdpersonal in IT-Bereichen während der Bauarbeiten sichergestellt, solange in diesen Bereichen die IT weiter betrieben wird?
- Wird die ordnungsgemäße Funktion aller Staubschutzmaßnahmen sowie die Einhaltung von Regelungen zum Staubschutz während der gesamten Bauzeit in ausreichend engen Zeitanständen durch Personen kontrolliert, die selbst nicht an den Baumaßnahmen beteiligt sind?

# M 1.73 Schutz eines Rechenzentrums gegen unbefugten Zutritt

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik

Ein Rechenzentrum stellt eine wichtige zentrale Einheit und damit eine Funktionseinheit mit besonderen Anforderungen an den Schutz gegen unbefugten Zutritt dar.

Die Maßnahmen M 2.6 *Vergabe von Zutrittsberechtigungen* und M 2.17 *Zutrittsregelung und -kontrolle* sind die unabdingbare Basis für den Schutz eines RZ gegen unbefugten Zutritt. Regelungen allein reichen hier aber nicht aus. Die Einhaltung der Regelungen muss durch weitere Maßnahmen unterstützt werden.

Die Zutrittskontrolle in Gebäudebereichen mit niedrigerem Schutzbedarf beschränkt sich meist auf die Abprüfung eines der beiden Kriterien Besitz (z. B. Karte) oder Wissen (z. B. PIN). Für den Schutz gegen unbefugten Zutritt bei einem Rechenzentrum sind dem deutlich höheren Schutzbedarf folgend zwingend starke Zutrittskontrollmechanismen erforderlich.

Im ersten Schritt kommt hier die kombinierte Abfrage von mindestens zwei der drei Kriterien Besitz, Wissen und biometrische Merkmale in Betracht. Aus heutiger Sicht sind biometrische Verfahren in unbeobachteten Bereichen als alleinige Zutrittskontrolle für Sicherheitsbereiche nicht zu empfehlen. Durch die kombinierte Abfrage zweier Kriterien wird mit ausreichender Sicherheit gewährleistet, dass die verwendeten Kriterien auch tatsächlich zu der jeweiligen Person gehören.

Alle Besucher müssen eindeutig Personen zugeordnet werden, die für sie während ihres Aufenthaltes verantwortlich sind und sie durchgehend beaufsichtigen. Die im normalen Umfeld hinnehmbare Tatsache, dass eine berechtigte Person weitere Personen, z. B. Besucher, einfach so mit in den zutrittsgeschützten Bereich nimmt, ist für ein Rechenzentrum nicht akzeptabel. Hier ist es erforderlich, jeden Zutritt einer Person eindeutig zu erfassen. Für den Besucherzutritt bedeutet das, dass jeder Besucher beispielsweise einen auf ihn persönlich ausgestellten Besitz erhält, etwa einen Besucherausweis. Das Fehlen des zweiten Kriteriums wird dadurch ausgeglichen, dass jeder Besucherausweis im System mit der für diesen Besuch verantwortlichen Person verknüpft wird.

In einem Rechenzentrum ist jeder Zutritt zu protokollieren, sowohl von autorisierten Personen als auch von solchen mit temporärer Zutrittsberechtigung. Beispielsweise könnte in einem Besucherbuch der Zutritt von Fremdpersonen zum Rechenzentrum dokumentiert werden. Die Nutzung eines Besucherbuchs kann den Zutritt Unberechtigter nicht regeln, sondern nur dokumentieren. Ein Buch, das innerhalb des RZ ausliegt und in das sich der Besucher ohne direkte Kontrolle der Richtigkeit der Angaben durch einen Befugten einträgt, besitzt im Sinne einer starken Zutrittskontrolle keinerlei Wert.

Um zu verhindern, dass eine berechtigte Person weitere Personen mit in den kontrollierten Bereich nimmt, ist der Aufbau einer Vereinzelungsschleuse sinnvoll. Sofern dies nicht möglich ist, sind entsprechende organisatorische und technisch unterstützte Regelungen umzusetzen. Als technische Unterstützung kann die Anti-Passback-Funktion genutzt werden. Dabei muss sich

jede Person, die mittels der geeigneten Kriterien Zutritt zu einem Bereich erlangt hat, beim Verlassen des Bereichs auch wieder abmelden. Eine Person, die das unterlässt, wird beim nächsten Zutrittsversuch abgewiesen, da sie im Zutrittskontrollsystem als anwesend gebucht ist und daher nicht noch einmal eintreten kann. Umgekehrt wird eine Person, die mitgegangen ist, ohne sich selber zu legitimieren, beim Ausgang als nicht im Bereich anwesend erkannt. Konsequenzen könnten beispielsweise sein, dass sich die Ausgangstür nicht wieder öffnen lässt oder eine entsprechende Ermahnung, die Zutrittsregeln einzuhalten, ertönt.

Neben der erzieherischen Wirkung einer Anti-Passback-Funktion gegen das "Mitgehen" kann darüber neben dem "Hinein" auch das "Heraus" sicher nachvollzogen werden. Das ist bei der Behandlung von Sicherheitsvorfällen ein nicht unwesentlicher Wissensvorteil.

Die Anti-Passback-Ausgangsbuchung kann sich auf die Abfrage eines einzelnen Kriteriums beschränken. Das könnte z. B. der Besucherausweis sein.

Prüffragen:

- Werden beim Zutritt zu einem Rechenzentrum zwingend mindestens zwei Authentikationsmerkmale abgefragt?
- Ist sichergestellt, dass jeder Besucher bei der Zutrittskontrolle individuell erfasst wird?
- Werden Besucher eindeutig einer verantwortlichen Person zugeordnet, die sie durchgehend beaufsichtigt?
- Wird ein Anti-Passback realisiert?
- Gibt es Mechanismen oder Regelungen, die verhindern, dass unautorisierte Personen in ein Rechenzentrum mitgenommen werden können?

# M 1.74 EMV-taugliche Stromversorgung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Absolut unverzichtbare Grundlage für die störungsfreie Funktion moderner IT-Systeme sowie der für deren Betrieb erforderlichen Supportsysteme (von der USV über die NEA bis hin zur Klimatechnik) ist eine EMV-taugliche Stromversorgung. Zwar ist diese Thema so komplex, dass es sich einer umfassenden Beschreibung in einer IT-Grundschutz-Maßnahme entzieht, es sollen hier aber die wesentlichen Grundlagen dargestellt werden, ohne deren Umsetzung alle weiterführenden Maßnahmen erfolglos bleiben.

TN-S-System und Zentraler Erdungspunkt

Seit Oktober 2010 enthält die Norm DIN VDE 0100-444 "Errichten von Niederspannungsanlagen, Teil 4-444: Schutzmaßnahmen -Schutz bei Störspannungen und elektromagnetischen Störgrößen" im Teil 444.4.3.1 zu TN-C-Systemen folgende Feststellung:

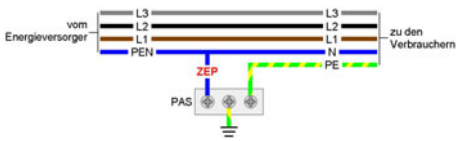
"TN-C-Systeme dürfen in neu errichteten Gebäuden, die eine wesentliche Anzahl von informationstechnischen Betriebsmitteln enthalten oder wahrscheinlich enthalten werden, nicht verwendet werden. Es wird empfohlen, in bestehenden Gebäuden TN-C-Systeme nicht beizubehalten, wenn diese Gebäude eine wesentliche Anzahl von informationstechnischen Betriebsmitteln enthalten oder wahrscheinlich enthalten werden."

Und zu TN-S-Systemen heißt es dort im Teil 444.4.3.2:

"Anlagen in neu errichteten Gebäuden müssen von der Einspeisung an als TN-S-System errichtet werden. In bestehenden Gebäuden, die bedeutende informationstechnische Betriebsmittel enthalten oder wahrscheinlich enthalten werden und die aus einem öffentlichen Niederspannungsnetz versorgt werden, sollte ab dem Anfang der Installationsanlage ein TN-S-System errichtet werden."

Damit trägt die VDE der Tatsache Rechnung, dass für den ordnungsgemäßen Betrieb von IT-Systeme als Mindestvoraussetzung das Stromversorgungsnetz als TN-S-System aufgebaut sein muss. Die Richtlinie VDI 3551 "Elektromagnetische Verträglichkeit (EMV) in der Technischen Gebäudeausrüstung" von 01-2011 unterstützt zudem verbindlich die Forderungen nach einem TN-S-System mit automatischer Überwachung.

Der wesentliche Unterschied zwischen den beiden Formen TN-C und TN-S ist der, dass es im TN-S-System nur einen einzigen Punkt gibt, an dem der N-Leiter und der PE-Leiter miteinander verbunden sind. Dieser Punkt ist der Zentrale Erdungspunkt (ZEP).




Da bei einem TN-S-System ab dem ZEP die gesamte weitere Installation 5-drähtig ausgeführt ist (die drei Phasen sowie N und PE getrennt), wird es auch "5-Leiter-Netz" genannt.

Der ZEP liegt so nah wie möglich bei der Einspeisung. Er ist nicht nur das funktionale Herzstück eines TN-S-Systems. Er stellt auch einen ersten, sehr einfach nutzbaren Messpunkt für die Güte des TN-S-Systems dar, also für die EMV-Tauglichkeit der Stromversorgung. Da vom ZEP aus gesehen das gesamte PE-System der Stromversorgung eine Sackgasse ist, es also keine weitere Verbindung mit einem anderen Leitersystem, speziell mit dem N-Leiter gibt, kann der reinen Physik nach auch kein Strom über den ZEP fließen.

Hinweis: In der Schweiz gehen einige verantwortungsbewusste Energieversorger inzwischen sogar schon dazu über, den ZEP in ihrem Zuständigkeitsbereich, also schon direkt an dem Verteiler zu realisieren, aus dem heraus eine Endverbraucher versorgt wird. Damit entfällt der ZEP beim Endverbraucher.

Leider verfügen moderne elektronische Geräte, also nahezu alle IT-Geräte über Netzteile, die einen mehr oder weniger hohen Strom auf dem PE-System bewirken, den sogenannten Ableitstrom. Dieser darf entsprechend der aktuellen Normenentwürfe ca. 0,2 Promille des Arbeitsstroms nicht überschreiten. Pro 1 A Arbeitsstrom sind also maximal 0,2 mA Ableitstrom zulässig. Dieser Strom fließt zwangsläufig auch über den ZEP und kann dort gemessen werden. Da der Ableitstrom in einem begrenzten Verhältnis zum Arbeitsstrom steht, kann aus dem Vergleich zwischen den tatsächlichen Werten von Arbeits- und Ableitstrom ermittelt werden, ob das TN-S-System ordnungsgemäß betrieben wird.

Ist der Strom über den ZEP zu hoch, kann das mehrere Ursachen haben. Die beiden wesentlichen Ursachen sind zum einen Defekte in Geräten oder zum anderen, dass es neben dem ZEP irgendwo im Netz mindestens eine weitere, also unzulässige Verbindung zwischen dem PE-System und dem N-Leiter gibt. Im ersten Fall ist das defekte Gerät auszutauschen. Im zweiten Fall muss diese zusätzliche PE-N-Verbindung (auch Nullung genannt) beseitigt werden.

Messpunkt, Messbarkeit

Allein die Messung des Stroms über den ZEP ist aber bei weitem noch nicht alles, was für den ordnungsgemäßen Betrieb eines TN-S-Systems getan werden kann und muss. Das Netz, und hier in vorderster Linie die Verteilungen, müssen mechanisch, also mit ausreichend Platz, so aufgebaut werden, dass zumindest in den Zuleitungen der Verteilungen folgende Messungen mit einer Strommesszange durchgeführt werden können:

- Strom über den ZEP (Dieser sollte durch entsprechende Beschriftung seines Installationsortes leicht auffindbar sein.)
- Strom jedes einzelnen Leiters (L1, L2, L3, N, PE)
- Strom aller drei Phasen gemeinsam (L1 & L2 & L3)
- Strom über die drei Phasen und den N-Leiter (L1 & L2 & L3 & N)

Mit diesen Messwerten können Fachleute weitere wichtige Erkenntnisse über den Betriebszustand des TN-S-Systems gewinnen.

Solche Messungen mit einer Strommesszange liefern aber immer nur Momentaufnahmen, die zwar wertvoll sein können, aber eine abschließende Aussage über die EMV-Tauglichkeit der Stromversorgung nicht zulassen. Hierfür sind weitere Maßnahmen erforderlich.

Netzanalyse

Eine wirklich belastbare Aussage über das Geschehen in der Stromversorgung ist nur durch eine permanente Netzüberwachung und -analyse möglich.

Dabei müssen folgende Werte an wichtigen Knoten der Stromversorgung in Echtzeit gemessen und für eine spätere Auswertung aufgezeichnet werden:

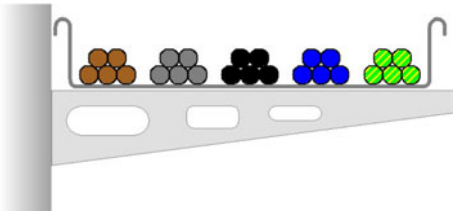
- Ströme, Spannungen und Frequenzen auf allen 5 Leitern
- Wirk-, Blind- und Scheinleistung
- Frequenzpegel bis in den Bereich von 100 kHz

Nur mit derartigen Echtzeitaufnahmen lassen sich Zeitverläufe erkennen und damit Aussagen darüber machen, welche Ursachen einzelnen Störungen zugrunde liegen. Es reicht keinesfalls aus, lediglich die Pegel der Harmonischen bis 1 kHz als Summengraph über ein bestimmtes Zeitfenster zu ermitteln.

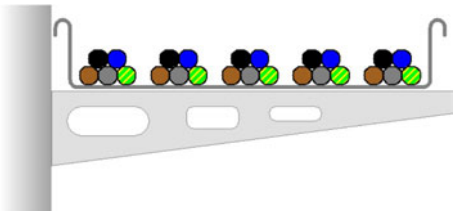
Trennungsabstände auf Trassen und in Verteilungen

Eine der wichtigen Ursachen für Störungen, die über die Stromversorgung auf IT-Systeme wirken, sind magnetische Felder. Magnetische Felder sind nur mit extremem Aufwand und damit in der Praxis nicht abschirmbar. Das einzige, was hier zweckmäßig wäre, ist Abstand. Der ist aber in den Verteilungen und auf Kabelbahnen in der Regel nicht gegeben. Daher muss besonderes Augenmerk darauf gelegt werden, solche Felder gar nicht erst entstehen zu lassen. Auch hierzu werden wegen der Komplexität des Themas nur ein paar wesentliche Hinweise gegeben.

Der Abstand zwischen den drei Phasen und dem zugehörigen N-Leiter soll immer so gering wie möglich gehalten werden. Auf Kabelbahnen ist das relevant, wenn z. B. aus verlegetechnischen Gründen die fünf Leiter (L1, L2, L3, N, PE) als Einzelleiter verlegt werden.



Bei dieser Art der Verlegung entstehen durch die relativ großen Abstände zwischen den drei Phasen (L1, L2, L3) und dem N-Leiter große magnetische Felder, die sowohl auf den PE-Leiter als auch auf das Kabeltragsystem einkoppeln und dort unerwünschte Ströme induzieren.



Werden die Einzeladern hingegen als 5-Leiter-Bündel verlegt, also jedes Bündel mit L1, L2, L3, N und PE, fallen die magnetischen Felder wesentlich kleiner aus und damit auch die induzierten Ströme und deren negative Folgen.

In Verteilungen ist darauf zu achten, dass der N-Leiter nicht auf getrennten Wegen durch die Verteilung geführt wird, sondern auch hier immer möglichst nah bei den drei Phasen verlegt wird. Eine solche enge Verlegung ist das einfachste und zugleich wirksamste Mittel, der Entstehung elektromagnetischer Felder entgegenzuwirken.

Der PE-Leiter darf und sollte hingegen in Verteilungen räumlich deutlich getrennt von dem L1-L2-L3-N-Quartett verlegt werden. Durch diesen Abstand wird die magnetische Überkopplung von Strömen auf den PE-Leiter stark reduziert.

Ergänzend sei an dieser Stelle darauf hingewiesen, dass die in der Blitzschutznorm DIN EN 62305:2006-10 "Blitzschutz" genannten Leiterabstände beim Einbau von Überspannungsableitern einzuhalten sind.

Des Weiteren ist der Trennungsabstand nach DIN EN 50174-2 "Installation von Kommunikationsverkabelung - Teil 2: Installationsplanung und Installationspraktiken in Gebäuden" und nach der Norm VDE 0100-444:2010 "Errichten von Niederspannungsanlagen - Teil 4-444: Schutzmaßnahmen - Schutz bei Störspannungen und elektromagnetischen Störgrößen" zu beachten. Die darin erhobenen Forderungen können im Bestand jedoch selten eingehalten werden. Hier sind aber zumindest die normativ vorgegebenen Abstände soweit wie irgend möglich zu realisieren.

Prüffragen:

- Ist das Stromverteilungsnetz als TN-S-System aufgebaut?
- Ist der ZEP in den Plänen und an seinem Standort deutlich erkennbar beschriftet?
- Ist der ZEP für eine Messung mit einem Zangenamperemeter zugänglich?
- Ist die Güte des TN-S-Systems lediglich durch die Ablesung von Momentanwerten beurteilbar oder gibt es eine in Echtzeit aufzeichnende Netzanalyse?
- Wird bei Aufbau und Betrieb des Stromverteilnetzes die empfohlenen Trennungsabstände soweit wie möglich eingehalten?

# M 1.75 Branderkennung in Gebäuden

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Planer

Maßnahmen zum baulichen und technischen Brandschutz, Branderkennung und rechtzeitige Alarmierung im Brandfall sind elementare Maßnahmen, um Gesundheit und Leben aller Menschen, die sich in einem Gebäude aufhalten, zu schützen.

Welche Maßnahmen des baulichen und technischen Brandschutzes für ein Gebäude gefordert sind, geben in Deutschland die jeweils gültigen Bauordnungen vor. Um die verschiedenen Landesbauordnungen zu vereinheitlichen, wurde die Musterbauordnung (MBO) als Orientierungsrahmen erstellt. Zudem ist ein nach Größe und Nutzung des Gebäudes angemessenes Brandschutzkonzept aufzustellen.

Es gilt immer, dass es in Gebäuden, je nach Art der Nutzung und der Bauweise, aus verschiedenen Gründen zu Bränden kommen kann. Um Personen zu schützen und um einen Brand rechtzeitig eindämmen zu können, muss seine Entstehung schnellstmöglich detektiert und der Brand bekämpft werden.

Für eine frühzeitige Erkennung von Bränden sollten Rauchmelder eingesetzt werden. Üblich sind punktförmige Melder gemäß DIN-EN 54-7 "Brandmeldeanlagen, Teil 7: Rauchmelder - Punktförmige Melder nach dem Streulicht-, Durchlicht- oder Ionisationsprinzip". Es empfiehlt sich, alle Arten von Gebäuden mit einer ausreichenden Anzahl von Rauchmeldern auszustatten.

Lokale Melder können über eine Brandmeldezentrale (BMZ) gesteuert und ausgewertet werden. Melder aller Art und Brandmeldezentrale bilden gemeinsam die Brandmeldeanlage (BMA).

Empfehlenswert ist eine Mindestausstattung bestehend aus

- Rauchmeldern an der Decke aller Flure sowie
- Rauchmeldern an der Decke aller Technikräume und Räumen der Elektroversorgung (Verteilungen, USV).
- Bei größeren Gebäuden ist es empfehlenswert, eine BMZ einzusetzen, auf die alle Melder aufgeschaltet sind.
- Falls eine Raumlufttechnische Anlage vorhanden ist, müssen auch deren Lüftungskanäle überwacht werden. Die RLT-Anlage muss zentral durch die BMZ abgeschaltet werden können, um zu verhindern, dass Brandrauch im Gebäude verteilt wird.

Es ist auf den korrekten Einbau der Rauchmelder entsprechend der Herstellervorgaben zu achten. Planung, Errichtung und Betrieb einer BMA sind nach Vorgaben der DIN 14675 "Brandmeldeanlagen - Aufbau und Betrieb" zu konzipieren und zwischen Auftraggeber, Bauaufsicht, Feuerwehr und gegebenenfalls Versicherer abzustimmen.

Falls eine Brandmeldezentrale vorhanden ist, sollten alle deren Meldungen inklusive der Störmeldungen auf einer ständig besetzten Stelle, z. B. der Pförtnerloge, auflaufen.

Die Funktionsfähigkeit aller Rauchmelder bzw. aller Komponenten einer Brandmeldeanlage muss regelmäßig überprüft werden. Es sollten sporadisch einige der Melderlinien manuell auf ihre Funktionsfähigkeit getestet werden.

Bei Rauchdetektion muss eine Alarmierung im Gebäude ausgelöst werden, bei der sichergestellt ist, dass alle im Gebäude anwesenden Personen diese wahrnehmen können.

Um ein gefahrloses Verlassen des Gebäudes sicherzustellen, muss immer gewährleistet sein, dass die vorgesehenen Flucht- und Rettungswege benutzbar sind. Sie dürfen nicht durch Möbel oder gar elektrische Geräte wie Kopierer oder Drucker, die eine erhebliche Brandlast darstellen, in ihrer vorgeschriebenen Breite eingeschränkt werden. Die minimale Breite von Fluchtwegen ist in Deutschland in der Technischen Richtlinie für Arbeitsstätten ASR A2.3 "Fluchtwege und Notausgänge, Flucht und Rettungsplan" vorgeschrieben. Es muss regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind.

Prüffragen:

- Gibt es ausreichend Rauchmelder im Gebäude?
- Wird regelmäßig kontrolliert, dass die Fluchtwege ohne Hindernisse sind?

# M 1.76 Geeignete Auswahl und Nutzung eines lokalen Arbeitsplatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Mitarbeiter, Vorgesetzte
**Verantwortlich für Umsetzung:** Mitarbeiter, Vorgesetzte

Lage und Ausstattung eines Arbeitsplatzes müssen in Einklang mit der Tätigkeit stehen, die an diesem Arbeitsplatz verrichtet werden soll. Bei der generellen Verteilung von Arbeitsplätzen in einem Gebäude müssen grundsätzliche Bedingungen und Abläufe und der Schutzbedarf der Tätigkeit in Einklang gebracht werden.

Arbeitsplätze mit Publikumsverkehr müssen so platziert sein, dass sie von den Kunden und Besuchern erreicht werden können, ohne dass diese sicherheitsrelevante Bereiche durchschreiten müssen. Auf der anderen Seite müssen Arbeitsabläufe, in denen die Vertraulichkeit der bearbeiteten Dokumente eine besondere Rolle spielt, vorzugsweise dort stattfinden, wo Besucher, aber auch Mitarbeiter anderer Abteilungen keinen freien Zugang haben.

Die technische Ausstattung, die Möblierung, die Platzverhältnisse und die allgemeinen Arbeitsbedingungen müssen der hauptsächlichen Tätigkeit angemessen sein. Neben der Grund-Arbeitsfläche muss genügend Platz für weitere typische Tätigkeiten vorhanden sein.

- Die Arbeitsfläche muss genügend Platz für PC, Telefon, Akten und sonstige Arbeitsmittel bieten.
- Es müssen ausreichend Stauflächen, wie beispielsweise abschließbare Schränke, vorhanden sein, um Material vor unbefugtem Zugriff schützen zu können.
- Es müssen genügend Anschlüsse für Strom, IT-Netze und Telefon für den Mitarbeiter selbst und eventuell auch weitere Mitarbeiter oder Besucher vorhanden sein.
- Die Arbeitsumgebung muss durch regelbare Raumtemperatur, ausreichende Lüftungsmöglichkeiten, eine ausreichende Beleuchtung und Abschottung vor Lärmquellen produktives Arbeiten ermöglichen.
- Dort wo oft Aufgaben von Gruppen erledigt werden, muss ausreichend Platz für Besprechungen sein. Zudem müssen Organisations- und Arbeitsmittel der Gruppenarbeit wie Tafeln, Kartentische oder Projektionsflächen und Projektoren verfügbar sein und es muss genügend Platz für deren Nutzung geben.

Es empfiehlt sich, die Arbeitsräume von Gruppen von Mitarbeitern, deren Aufgaben hohen oder sehr hohen Schutzbedarf haben, in Abschnitten des Gebäudes so zusammenzufassen, dass auch Sanitärbereiche und Gemeinschaftsräume wie Besprechungsräume und Teeküchen, sowie Plätze für Drucker und Kopierer in einem solchen zusammenhängenden separaten Abschnitt des Gebäudes vorhanden sind. Dieser Abschnitt des Gebäudes kann dann leicht zu einem autonomen Zutrittskontrollbereich gemacht werden.

Viele Arbeitsplätze können von den Mitarbeitern nur sehr beschränkt eingerichtet werden und müssen im Allgemeinen so genutzt werden, wie sie vorgefunden wurden. Daher ist immer zuerst von den Vorgesetzten zu entscheiden, ob das Sicherheitsniveau der jeweiligen Umgebung geeignet ist, um die Aufgaben dort wahrnehmen zu können.

Prüffragen:

- Ist die Ausstattung der lokalen Arbeitsplätze angemessen für die Aufgaben der dort tätigen Mitarbeiter?
- Entspricht das Sicherheitsniveau der lokalen Arbeitsplätze dem Schutzbedarf der dort bearbeiteten Informationen?

# M 1.77 Klimatisierung für Menschen

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

In größeren Gebäuden muss die Luftversorgung durch raumlufttechnische (RLT-) Anlagen geleistet werden. RLT-Anlagen sorgen für den Transport (Lüftung) und die Konditionierung (Klimatisierung) der Luft. RLT-Anlagen sollen ein für Menschen günstiges Raumklima schaffen. Zudem müssen sie eine hygienisch einwandfreie Qualität der Innenraumluft sicherstellen. Das heißt, dass die durch eine RLT-Anlage aufbereitete Luft keine Gefährdung der Gesundheit oder Störungen der Befindlichkeit mit sich bringt, Geruchsbelästigungen unterbleiben und die thermische Behaglichkeit erhalten bleibt.

Eine gute Luftqualität kann nicht ausschließlich durch die RLT-Anlage erzeugt werden. Auch bei der Auswahl der Bauwerkstoffen, Bodenbelägen und Möbeln muss auf den Einsatz von Materialien geachtet werden, die die Raumluft nicht zusätzlich und unnötig mit Schadstoffen belasten.

Die Planung von Lüftungs- und Klimaanlagen nach Stand der Technik für Nichtwohngebäude ist in der DIN EN 13779 "Lüftung von Nichtwohngebäuden - Allgemeine Grundlagen und Anforderungen für Lüftungs- und Klimaanlagen und Raumkühlsysteme" beschrieben. Zusammen mit der Arbeitsstättenverordnung legt sie fest, in welchen Räumen des Gebäudes welche Anforderungen an die Luftqualität zu erfüllen sind. Die DIN EN 13779 enthält detaillierte Festlegungen für

- die operative Temperatur
- das Zugluftrisiko
- die relative Raumluftfeuchte
- die bewerteten Schalldruckpegel
- und weitere für Menschen relevante Faktoren.

Während für Büros und sonstige ständig besetzte Räume hohe Anforderungen an die Luftqualität bestehen, ist der Anspruch in nicht ständig besetzten Räumen geringer. Umso wichtiger ist, dass, wie auch in der Norm gefordert, die Vorgaben für die Klimaplanung vom Bauherrn bzw. dem zukünftigen Nutzer vorgegeben werden.

Während Kälte fast nie ein Problem bei Erzeugung eines behaglichen Raumklimas darstellt, kann sommerliche Hitze ein größeres Problem sein. Die Arbeitsstättenverordnung fordert für Arbeitsräume gesundheitlich zuträgliche Raumtemperaturen und den Schutz gegen übermäßige Sonneneinstrahlung. Um an warmen Sommertagen ein erträgliches Raumklima zu erhalten, muss die RLT-Anlage durch eine wirkungsvolle Beschattung der Fenster unterstützt werden.

RLT-Anlagen müssen regelmäßig gewartet werden. Bei RLT-Anlagen dienen Wartungsarbeiten nicht nur dazu, den zuverlässigen Betrieb zu sichern, sondern auch dazu, Hygiene und damit die Gesundheit aller Nutzer des Gebäudes zu garantieren. Die Einhaltung von Wartungsintervallen und die sorgfältige Durchführung von Reinigungsarbeiten und Filterwechseln muss kontrolliert und dokumentiert werden.

RLT-Anlagen dürfen nicht für jedermann zugänglich sein und müssen gegebenenfalls gegen Sabotage materiell geschützt werden.

Die RLT-Anlagen müssen auch bei der Notfallplanung (siehe Baustein B 1.3 *Notfallmanagement*), insbesondere bei Abschalt- und Wiederanlaufplanungen, berücksichtigt werden.

Prüffragen:

- Sind die RLT-Anlagen auf die tatsächliche Nutzung des Gebäudes ausgelegt?
- Werden die RLT-Anlagen regelmäßig gewartet?

# M 1.78 Sicherheitskonzept für die Gebäudenutzung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Planer

Um ein praxistaugliches und wirtschaftliches Sicherheitskonzept für die Nutzung eines Gebäudes zu erarbeiten, sind der Schutzbedarf der dort betriebenen Geschäftsprozesse und die grundsätzlichen Schutzziele, die sich häufig aus der Geschäftstätigkeit ergeben, zu ermitteln. Solche Schutzziele können zum Beispiel der Schutz der Wirtschaftsgüter, besonderer Schutz einiger oder aller Mitarbeiter gegen Angriffe oder der Zutritts- oder Inhaltsschutz für besondere Bereiche oder einzelne Räume des Gebäudes sein.

Bei einem Gebäude müssen viele verschiedene Sicherheitsaspekte beachtet werden, von Brandschutz über Elektrik bis hin zur Zutrittskontrolle. Je nach Größe der Institution und der Gebäude kann es hierfür unterschiedliche Zuständige geben. Daher müssen die verschiedenen Rollen und Aufgaben abgestimmt werden. Die zuständigen Personen sollten sich untereinander abstimmen, um aufbauend auf den Schutzzielen angemessene Sicherheitsmaßnahmen für die verschiedenen Bereiche auszuwählen.

Es ist bewährte Praxis, zur Planung von Gebäuden zunächst Zonen zu betrachten (siehe M 1.79 *Bildung von Sicherheitszonen*). Viele Schutzziele lassen sich dadurch erreichen, dass es weder nötig noch möglich ist, von einer Zone mit geringem Sicherheitsniveau direkt in eine mit höherem Sicherheitsniveau zu gelangen. Dabei sollte zunächst die räumliche Aufteilung mit der vorgesehenen Nutzung des Gebäudes abgestimmt werden (siehe M 1.13 *Anordnung schützenswerter Gebäudeteile*). Zwischen verschiedenen Sicherheitszonen sollten klar erkennbare und möglichst einfach abzusichernde Übergänge geschaffen werden. Zulässige Übergänge zwischen den Zonen werden dann angepasst an den Schutzbedarf ausgeführt. Unzulässige Übergänge werden entweder unterbunden oder besonders abgesichert. So müssen Fluchttüren aus Sicherheitszonen mit höherem Sicherheitsniveau in den Außenbereich so gesichert werden, dass der unberechtigte Zutritt von außen nach innen verhindert wird. Fenster und Zugänge müssen entsprechend ihres Schutzbedarfs abgesichert sein (siehe M 1.10 *Sichere Türen und Fenster*).

In jeder Sicherheitszone sollten nur Geschäftsprozesse betrieben werden, deren Schutzbedarf dem der Sicherheitszone entspricht. Es sollten auch nur die Personen Zutritt haben, deren Aufgaben dies erfordern. Die Zugänge zu den Sicherheitszonen müssen entsprechend ihres Schutzbedarfs kontrolliert werden, so dass keine Unbefugten diese Bereiche betreten können.

Ergänzt werden muss diese Betrachtung fast immer um weitere Maßnahmen gegen unerlaubtes Eindringen oder Einschleichen. Einen Überblick dazu bildet die Maßnahme M 1.19 *Einbruchsschutz*.

Wenn das Gebäude öffentliche oder halböffentliche Bereiche aufweist oder wenn z. B. durch Fensterfronten im Straßenbereich Einblick in das Gebäude möglich ist, ist die M 1.12 *Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile* zu prüfen.

Überall wo der Schutz der Inhalte des Gebäudes, seien es Waren, sei es die technische Infrastruktur, in besonderer Weise gefordert ist, muss das Sicher-

heitskonzept den Schutz vor Wasser betrachten. Hinweise dazu gibt die Maßnahme M 1.14 *Selbsttätige Entwässerung*.

Alle auf die Schutzziele abgestimmten vorbeugenden oder schadensmindernden Maßnahmen müssen schließlich noch um detektierende Maßnahmen (siehe M 1.18 *Gefahrenmeldeanlage*) ergänzt werden. Das Gebäude-Schutzkonzept ist erst dann vollständig, wenn durch Planung und Ausführung den relevanten Gefährdungen entgegengewirkt wird und durch überwachende Maßnahmen sichergestellt wird, dass schadenbringende Ereignisse oder zufällige oder vorsätzliche Versuche, Schutz- und Sicherungsmaßnahmen zu überwinden möglichst frühzeitig bemerkt werden. Nur dann ist es möglich, Gegenmaßnahmen einzuleiten.

Das Sicherheitskonzept für das Gebäude muss mit dem Gesamt-Sicherheitskonzept der Institution abgestimmt sein. Es sollte regelmäßig aktualisiert werden, vor allem wenn sich Änderungen in der Gebäudenutzung ergeben, also beispielsweise nach organisatorischen Änderungen in der Institution.

Prüffragen:

- Gibt es ein Sicherheitskonzept für das Gebäude?
- Werden alle Zugänge kontrolliert, damit keine Unbefugten geschützte Bereiche betreten können?

# M 1.79 Bildung von Sicherheitszonen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Planer, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Innerer Dienst

Der Schutzbedarf von Räumen in einem Gebäude hängt von ihrer Nutzung ab. Die erforderlichen Sicherheitsmaßnahmen müssen diesem Schutzbedarf angepasst sein. Entsprechend muss die bauliche Ausführung von Wänden, Fenstern und Türen sein und die ergänzende Ausstattung mit Sicherheits- und Überwachungstechnik. Bei der Planung eines neuen Gebäudes oder der Bewertung eines Bestandsgebäudes sollten deshalb Räume ähnlichen Schutzbedarfs in Zonen zusammengefasst werden. Damit lassen sich vergleichbare Risiken einheitlich behandeln und die Kosten der Umsetzung von Maßnahmen werden reduziert.

Um z. B. nicht jeden einzelnen Raum im Gebäude permanent abschließen oder überwachen zu müssen, sollten Zonen mit Besucherverkehr von schutzbedürftigen Bereichen getrennt werden. Öffentliche Räume wie eine Kantine, die externes Publikum anzieht, oder halb-öffentliche Räume wie Besprechungs-, Schulungs- oder Veranstaltungsräume sollten in der Nähe des Gebäudeeingangs angeordnet sein. Der Zugang zu Gebäudeteilen mit internen Bereichen wie den Büros kann dann z. B. von einem Pförtner einfach überwacht werden. Besonders sensitive Bereiche wie eine Entwicklungsabteilung, Räume der Gebäudetechnik oder IT-Räume sollten mit einer zusätzlichen Zugangskontrolle abgesichert werden.

Zur physischen Sicherung eines Gebäudes und gegebenenfalls des umgebenden Grundstücks hat es sich bewährt, ein Sicherungskonzept mit tiefengestaffelten Sicherheitsmaßnahmen (Zwiebelschalenprinzip) zu planen und umzusetzen. Bewährt ist eine Aufteilung in vier Sicherheitszonen, Außenbereich, kontrollierter Innenbereich, interner Bereich und Hochsicherheitsbereich:

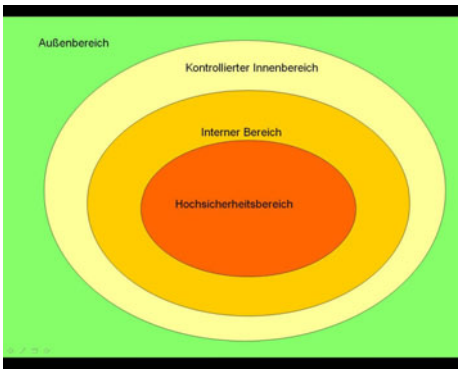



Abbildung: Sicherheitszonenmodell

Die Sicherheitszone 0, also der Außenbereich, wird von der Grundstücksgrenze umfasst. Wenn die Situation es zulässt, sollte diese juristische Grenze deutlich durch eine Einfriedung angezeigt werden. Hier kann bereits die erste Zutritts- und Zufahrtskontrolle vorgenommen werden. Öffentliche Gebäudebereiche sind dieser Zone zuzurechnen.

Die Sicherheitszone 1 ist der kontrollierte Innenbereich. Durch eine angemessene Zutrittskontrolle, z. B. einen Pförtner oder ein Zutrittskontrollsystem, erhalten nur Berechtigte (Mitarbeiter, geladene Besucher) Zutritt zu dieser Zo-

ne. Bei hohem Schutzbedarf sollte in dieser Zone bereits die Verpflichtung bestehen, stets sichtbar Ausweise zu tragen. Die Außenhaut der Zone 1 (Gebäudeaußenhaut) sollte durch bauliche und technische Maßnahmen gegen Sabotage und Einbruch geschützt werden.

Die Zone 2 als interner Bereich ist nur für einen eingeschränkten Kreis von Berechtigten zu betreten. Hier gibt es definierte Zutrittsberechtigungen. Räume oder Gebäudeabschnitte der Zone 2 sollten jeweils nur einen Zugang aufweisen. Weitere Zuwegungen dienen ausschließlich als Flucht- und Rettungswege und sind im Betrieb immer geschlossen zu halten. Sie sind permanent zu überwachen und durch elektromechanische Sicherungseinrichtungen (Fluchtwegsicherungssysteme) gegen missbräuchliche Nutzung zu sichern.

Die Zone 3 bildet den Hochsicherheitsbereich (z. B. Vorstandsbereiche, kritische IT-Räume). Der Kreis der Zutrittsberechtigten ist sehr eingeschränkt. Die Sicherheitsmaßnahmen sollten entsprechend hoch sein. Beispiel: Der Zutritt ist nur über eine Sicherheitsschleuse mit Zwei-Faktor-Authentisierung und Vereinzelung, der Austritt mit Ein-Faktor-Authentisierung und Vereinzelung möglich. Es erfolgt eine Bilanzierung des Zutritts, sobald keine Personen mehr als anwesend gemeldet sind, erfolgt die automatische Scharfschaltung der Einbruchmeldeanlage.

Poststellen, Anlieferungs- und Ladezonen sollten sich in Sicherheitszone 1 befinden. Sie sollten so gestaltet sein, dass Lieferungen angenommen werden können, ohne dass die Lieferanten weitere Bereiche des Gebäudes betreten müssen. Die Türen in diesen Bereichen sollten nicht über längere Zeit offenstehen. Bei höherem Schutzbedarf sollte sich entweder nur die Außentür oder die Tür zu den inneren Bereichen öffnen lassen. Eingehende Lieferungen sollten in der Lieferzone daraufhin untersucht werden, ob damit Risiken verbunden sein könnten (siehe M 2.90 *Überprüfung der Lieferung*). Die Art und Tiefe der Überprüfungen ist abhängig vom jeweiligen Gefährdungspotential (z. B. Briefbomben). Ein- und ausgehende Lieferungen sollten möglichst getrennt voneinander aufbewahrt werden.

Prüffragen:

- Wurde ein Sicherheitszonenkonzept für Gebäude und Grundstück entwickelt und dokumentiert?

# M 1.80 Zutrittskontrollsystem und Berechtigungsmanagement

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Leiter Organisation

Der Schutz vor unbefugtem Zutritt zu einem Gebäude, schutzbedürftigen Gebäudeteilen oder Räumen soll oftmals mehrere Schutzziele unterstützen. Nicht nur der Schutz des Eigentums, sowohl der Institution als auch des Eigentums der Mitarbeiter, soll sichergestellt sein, sondern auch der Arbeitsschutz, der Schutz von Know-How und eventuell auch der Personenschutz. Hinzu kommt, dass der Nachweis über eine angemessene Vergabe von Zutrittsberechtigungen und über die Kontrolle der Nutzung dieser Berechtigungen auch gefordert ist, wenn die Erfüllung von vertraglichen oder gesetzlichen Vorgaben dargelegt werden muss ("Compliance"). Die Anforderungen der Institution an ein Zutrittskontrollsystem sollten genügend detailliert dokumentiert werden.

Mechanische Schließanlagen mit ihren Schlüsseln und Gruppenschlüsseln werden problematisch, wenn auf Verlust von Schlüsseln schnell reagiert werden muss oder wenn Nutzungsänderungen im Gebäude eine schnelle Umrüstung erfordern. Deshalb werden vielerorts IT-gestützte Zutrittskontrollsysteme (ZKS) eingesetzt, wie sie in der Norm DIN EN50133-1 / VDE 0830-8-1 "Alarmanlagen - Zutrittskontrollanlagen für Sicherungsanwendungen" definiert sind.

Ein solches System besteht aus verschiedenen Grundelementen, die in Schichten zusammenwirken. Ein Zutrittskontrollserver verwaltet den zentralen Datenbestand, also Daten von Personen, denen Berechtigungen zugeteilt werden, und die Regeln (Wer, Wann, Wohin), die für die Organisation der Berechtigungen gelten und angewandt werden. Angeschlossen an den Zutrittskontrollserver sind Steuereinheiten. An diese Einheiten werden per IT-Netz vom Server Berechtigungsprofile für die angeschlossenen Türen, Tore und Schranken übertragen. Alle Entscheidungen zur Steuerung der angeschlossenen Türen etc. werden in dieser dezentralen Einheit getroffen. Somit ist die Türsteuerung auch ohne Verbindung zum zentralen Server handlungsfähig. In die Steuereinheiten sind Datenspeicher integriert, welche alle Bewegungsdaten aufzeichnen.

An die Steuereinheiten sind Sensoren (Leseeinheiten), Aktoren (z. B. Stellglieder, Türöffner, Schleusen) und Detektoren angeschlossen.

Zur Identifikation (und teilweise auch Authentikation) der Benutzer dienen Ausweiskarten oder "Token", welche von den Leseeinheiten ausgelesen werden. Diese werden allgemein als Identifikationsmerkmalträger bezeichnet. Die Ausweise sollten einheitlich und mit gut lesbaren Zuordnungsmerkmalen (z. B. Name und Abteilung) versehen sein. Dies erleichtert es, direkt erkennen zu können, ob sich Unbefugte in geschützten Bereichen aufhalten.

Ein berechtigter Zutritt findet dadurch statt, dass der Träger eines Ausweises den Ausweis an einen Leser führt. Der Leser meldet die Ausweis-ID an seine Steuereinheit weiter. Wenn diese den Ausweis als für diese Tür berechtigt identifiziert, wird ein Aktor ausgelöst, der die Tür öffnet.

In Bereichen mit höherem Schutzbedarf sollte eine Zwei-Faktor-Authentikation vorgenommen werden. Die Prüfung des Besitzes (z. B. der berechtigten

Chipkarte) wird dann ergänzt um die Prüfung von Wissen (z. B. Eingabe einer PIN) oder die Prüfung eines biometrischen Merkmals des Ausweisträgers.

Ergänzend kann ein Zutrittskontrollsystem genutzt werden, um die Vergabe von Berechtigungen, die Vergabe von Identifikationsmerkmalträgern und auch die Zuteilung von konventionellen Schlüsseln zu organisieren. Auch Sonderberechtigungen wie Parkausweise für Mitarbeiter und kurzzeitig gültige Besucherausweise sollten auf diesem einen System verwaltet werden. Ebenso wird die Protokollierung der Nutzung des gesamten Zutrittskontrollsystems auf dem Server konzentriert.

Der Leistungsumfang eines Zutrittskontrollsystems, mit dem auch mechanische Schlüssel verwaltet werden, sollte alle in M 2.14 *Schlüsselverwaltung* beschriebenen Abläufe unterstützen.

Ein Zutrittskontrollsystem gestattet, jederzeit leicht zu überprüfen, wer die Zutrittsberechtigung zu sicherheitskritischen Bereichen eines Gebäudes hat und mit welchen Ausweisen zu welchem Zeitpunkt Türen benutzt wurden. Auch ist es einfach, Berechtigungen von Personen bei Wechsel des Aufgabenbereiches oder Ausscheiden aus der Institution zu entziehen oder zu ändern. Es ist nicht nötig, ein Objekt zurückzufordern, also z. B. einen Schlüssel einzuziehen, es reicht aus, dem Ausweis die damit verbundenen Rechte zu entziehen.

Es muss immer darauf geachtet werden, dass die Entscheidung über die Vergabe von Zutrittsberechtigungen beim Verantwortlichen für den jeweiligen Gebäudebereich liegt. Der Administrator des Zutrittskontrollsystems ist in Folge verantwortlich für die korrekte Umsetzung der Anweisungen, nicht etwa für die Vergabe von Zutrittsrechten selbst.

Wegen der umfangreichen Möglichkeiten der Protokollierung und Auswertung (beispielsweise von Bewegungsdaten von Mitarbeitern) sollte die Einführung eines solchen Systems rechtzeitig mit dem Datenschutzbeauftragten und der Mitarbeitervertretung abgestimmt werden.

Die Planung eines Zutrittskontrollsystems muss auf die individuellen Anforderungen einer Institution eingehen. Die Schnittstellen eines solchen Systems zum Beispiel zu Türen und zur Videoüberwachung sind spezifisch zum verfolgten Schutzziel zu definieren und umzusetzen und Sonderprobleme wie die Steuerung und Überwachung von Fluchttüren sind zu lösen. Zudem besteht die Gefahr durch die Abhängigkeit von einem Lieferanten auf Einschränkungen in Bezug auf mögliche Änderungen oder Erweiterungen des Systems zu stoßen. Bei Neubeschaffung oder großen Änderungen eines Zutrittskontrollsystems sollte deshalb ein Fachplaner zugezogen werden.

Prüffragen:

- Wurden die Anforderungen der Institution an die Zutrittskontrolle dokumentiert?
- Ist der Prozess der organisatorischen Zuteilung und der anschließenden Ausgabe von Identifikationsmerkmalträger ausreichend dokumentiert?

# M 1.81 Materielle Sicherung von eingebetteten Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Planer, Administrator, Entwickler

Eingebettete Systeme dürfen nicht aufgrund von Staub oder Verschmutzungen ausfallen oder versagen. Eingebettete Systeme sind entsprechend ihrer vorgesehenen Einsatzart und des vorgesehenen Einsatzorts vor Staub und Verschmutzungen zu schützen. Das eingebettete System kann in ein umschließendes, robustes Gehäuse eingebaut werden oder an einer geschützten Stelle im Inneren des umgebenden Systems oder der tragenden Infrastruktur verbaut werden.

Falls Systeme wegen einer notwendigen Luftzufuhr nicht ausreichend ummantelt werden können, sind Luftfilter vorzusehen. Diese müssen hinsichtlich Dimensionierung und Filterleistung für die vorgesehenen Einsatzarten geeignet sein.

Die Vorkehrungen zum Schutz gegen Staub und Verschmutzung sind bereits in der Planung zu berücksichtigen.

Prüffragen:

- Wurden für das eingebettete System die Anforderungen an den Schutz vor Staub und Verschmutzung bereits in der Planung analysiert?
- Sind die Vorkehrungen zum Schutz vor Staub und Verschmutzung mit den Anforderungen des übergeordneten Systems verträglich?
- Verfügt das eingebettete System über einen ausreichenden Schutz vor Staub und Verschmutzung?

# M 2 Maßnahmenkatalog Organisation

M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung

M 2.33 Aufteilung der Administrationstätigkeiten unter Unix

M 2.34 Dokumentation der Veränderungen an einem bestehenden System

M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems

M 2.36 Geregelte Übergabe und Rücknahme eines tragbaren PC

M 2.37 Der aufgeräumte Arbeitsplatz

M 2.38 Aufteilung der Administrationstätigkeiten

M 2.39 Reaktion auf Verletzungen der Sicherheitsvorgaben

M 2.40 Rechtzeitige Beteiligung des Personal-/Betriebsrates

M 2.41 Verpflichtung der Mitarbeiter zur Datensicherung

M 2.42 Festlegung der möglichen Kommunikationspartner

M 2.43 Ausreichende Kennzeichnung der Datenträger beim Versand

M 2.44 Sichere Verpackung der Datenträger

M 2.45 Regelung des Datenträgeraustausches

M 2.46 Geeignetes Schlüsselmanagement

M 2.47 Ernennung eines Fax-Verantwortlichen

M 2.48 Festlegung berechtigter Faxbediener

M 2.49 Beschaffung geeigneter Faxgeräte

M 2.50 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen

M 2.51 Fertigung von Kopien eingehender Faxsendungen

M 2.52 Versorgung und Kontrolle der Verbrauchsgüter

M 2.53 Abschalten des Faxgerätes außerhalb der Bürozeiten

M 2.54 Beschaffung geeigneter Anrufbeantworter **- entfallen**

M 2.55 Einsatz eines Sicherungscodes **- entfallen**

M 2.56 Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter **- entfallen**

M 2.57 Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche **- entfallen**

M 2.58 Begrenzung der Sprechdauer **- entfallen**

M 2.59 Auswahl eines geeigneten Modems in der Beschaffung

M 2.60 Sichere Administration eines Modems

M 2.61 Regelung des Modem-Einsatzes

M 2.62 Software-Abnahme- und Freigabe-Verfahren

M 2.63 Einrichten der Zugriffsrechte

M 2.64 Kontrolle der Protokolldateien

M 2.65 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System

M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung

M 2.67 Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste **- entfallen**

M 2.68 Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten **- entfallen**

M 2.69 Einrichtung von Standardarbeitsplätzen

M 2.70 Entwicklung eines Konzepts für Sicherheitsgateways

M 2.71 Festlegung einer Policy für ein Sicherheitsgateway

M 2.72 Anforderungen an eine Firewall **- entfallen**

M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways

M 2.74 Geeignete Auswahl eines Paketfilters

M 2.75 Geeignete Auswahl eines Application-Level-Gateways

M 2.76 Auswahl und Einrichtung geeigneter Filterregeln

M 2.77 Integration von Servern in das Sicherheitsgateway

M 2.78 Sicherer Betrieb eines Sicherheitsgateways

M 2.79 Festlegung der Verantwortlichkeiten im Bereich Standardsoftware

M 2.80 Erstellung eines Anforderungskatalogs für Standardsoftware

M 2.81 Vorauswahl eines geeigneten Standardsoftwareproduktes

M 2.82 Entwicklung eines Testplans für Standardsoftware

M 2.83 Testen von Standardsoftware

M 2.84 Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware

M 2.85 Freigabe von Standardsoftware

M 2.86 Sicherstellen der Integrität von Standardsoftware

M 2.87 Installation und Konfiguration von Standardsoftware

M 2.88 Lizenzverwaltung und Versionskontrolle von Standardsoftware

M 2.89 Deinstallation von Standardsoftware

M 2.90 Überprüfung der Lieferung

M 2.91 Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz **- entfallen**

M 2.92 Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz **- entfallen**

M 2.93 Planung des Windows NT Netzes **- entfallen**

M 2.94 Freigabe von Verzeichnissen unter Windows NT **- entfallen**

M 2.95 Beschaffung geeigneter Schutzschränke

M 2.96 Verschluss von Schutzschränken

M 2.97 Korrekter Umgang mit Codeschlössern

M 2.98 Sichere Installation von Novell Netware Servern **- entfallen**

M 2.99 Sichere Einrichtung von Novell Netware Servern **- entfallen**

M 2.100 Sicherer Betrieb von Novell Netware Servern **- entfallen**

M 2.101 Revision von Novell Netware Servern **- entfallen**

M 2.102 Verzicht auf die Aktivierung der Remote Console **- entfallen**

M 2.103 Einrichten von Benutzerprofilen unter Windows 95 **- entfallen**

M 2.104 Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95 **- entfallen**

M 2.105 Beschaffung von TK-Anlagen

M 2.106 Auswahl geeigneter ISDN-Karten in der Beschaffung

M 2.107 Dokumentation der ISDN-Karten-Konfiguration

M 2.108 Fernwartung der ISDN-Netzkoppelelemente

M 2.109 Rechtevergabe für den Fernzugriff

M 2.110 Datenschutzaspekte bei der Protokollierung

M 2.111 Bereithalten von Handbüchern

M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

M 2.113 Regelungen für Telearbeit

M 2.114 Informationsfluss zwischen Telearbeiter und Institution

M 2.115 Betreuungs- und Wartungskonzept für Telearbeitsplätze

M 2.116 Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit

M 2.117 Erstellung eines Sicherheitskonzeptes für Telearbeit

M 2.118 Konzeption der sicheren E-Mail-Nutzung **- entfallen**

M 2.119 Regelung für den Einsatz von E-Mail **- entfallen**

M 2.120 Einrichtung einer Poststelle **- entfallen**

M 2.121 Regelmäßiges Löschen von E-Mails **- entfallen**

M 2.122 Einheitliche E-Mail-Adressen

M 2.123 Auswahl eines Groupware- oder Mailproviders

M 2.124 Geeignete Auswahl einer Datenbank-Software

M 2.125 Installation und Konfiguration einer Datenbank

M 2.126 Erstellung eines Datenbanksicherheitskonzeptes

M 2.127 Inferenzprävention

M 2.128 Zugangskontrolle einer Datenbank

M 2.129 Zugriffskontrolle einer Datenbank

M 2.130 Gewährleistung der Datenbankintegrität

M 2.131 Aufteilung von Administrationstätigkeiten bei Datenbanksystemen

M 2.132 Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen

M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems

M 2.134 Richtlinien für Datenbank-Anfragen

M 2.135 Gesicherte Datenübernahme in eine Datenbank

M 2.136 Einhaltung von Regelungen zu Arbeitsplatz und Arbeitsumgebung **- entfallen**

M 2.137 Beschaffung eines geeigneten Datensicherungssystems

M 2.138 Strukturierte Datenhaltung

M 2.139 Ist-Aufnahme der aktuellen Netzsituation

M 2.140 Analyse der aktuellen Netzsituation

M 2.141 Entwicklung eines Netzkonzeptes

M 2.142 Entwicklung eines Netz-Realisierungsplans **- entfallen**

M 2.143 Entwicklung eines Netzmanagement-Konzeptes

M 2.144 Verwendung von SNMP als Netzmanagement-Protokoll

M 2.145 Anforderungen an ein Netzmanagement-Tool

M 2.146 Sicherer Betrieb eines Netzmanagement-Systems

M 2.147 Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze **- entfallen**

M 2.148 Sichere Einrichtung von Novell Netware 4.x Netzen **- entfallen**

M 2.149 Sicherer Betrieb von Novell Netware 4.x Netzen **- entfallen**

M 2.150 Revision von Novell Netware 4.x Netzen **- entfallen**

M 2.151 Entwurf eines NDS-Konzeptes **- entfallen**

M 2.152 Entwurf eines Zeitsynchronisations-Konzeptes **- entfallen**

M 2.153 Dokumentation von Novell Netware 4.x Netzen **- entfallen**

M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme

M 2.155 Identifikation potentiell von Computer-Viren betroffener IT-Systeme **- entfallen**

M 2.156 Auswahl einer geeigneten Computer-Virenschutz-Strategie **- entfallen**

M 2.157 Auswahl eines geeigneten Viren-Schutzprogramms

M 2.158 Meldung von Schadprogramm-Infektionen

M 2.159 Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen

M 2.160 Regelungen zum Schutz vor Schadprogrammen

M 2.161 Entwicklung eines Kryptokonzepts

M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte

M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte

M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens

M 2.165 Auswahl eines geeigneten kryptographischen Produktes

M 2.166 Regelung des Einsatzes von Kryptomodulen

M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten

M 2.168 IT-System-Analyse vor Einführung eines Systemmanagement-Systems

M 2.169 Entwickeln einer Systemmanagementstrategie

M 2.170 Anforderungen an ein Systemmanagement-System

M 2.171 Geeignete Auswahl eines Systemmanagement-Produktes

M 2.172 Entwicklung eines Konzeptes für Webangebote

M 2.173 Festlegung einer Webserver-Sicherheitsstrategie

M 2.174 Sicherer Betrieb eines Webservers

M 2.175 Aufbau eines Webservers

M 2.176 Geeignete Auswahl eines Internet Service Providers

M 2.177 Sicherheit bei Umzügen

M 2.178 Erstellung einer Sicherheitsleitlinie für die Faxnutzung

M 2.179 Regelungen für den Faxserver-Einsatz

M 2.180 Einrichten einer Fax-Poststelle

M 2.181 Auswahl eines geeigneten Faxservers

M 2.182 Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen **- entfallen**

M 2.183 Durchführung einer RAS-Anforderungsanalyse **- entfallen**

M 2.184 Entwicklung eines RAS-Konzeptes **- entfallen**

M 2.185 Auswahl einer geeigneten RAS-Systemarchitektur **- entfallen**

M 2.186 Geeignete Auswahl eines RAS-Produktes **- entfallen**

M 2.187 Festlegen einer RAS-Sicherheitsrichtlinie **- entfallen**

M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

M 2.189 Sperrung des Mobiltelefons bei Verlust

M 2.190 Einrichtung eines Mobiltelefon-Pools

M 2.191 Etablierung des IT-Sicherheitsprozesses **- entfallen**

M 2.192 Erstellung einer Leitlinie zur Informationssicherheit

M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit

M 2.194 Erstellung einer Übersicht über vorhandene IT-Systeme **- entfallen**

M 2.195 Erstellung eines Sicherheitskonzepts

M 2.196 Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan **- entfallen**

M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess

M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit

M 2.199 Aufrechterhaltung der Informationssicherheit

M 2.200 Management-Berichte zur Informationssicherheit

M 2.201 Dokumentation des Sicherheitsprozesses

M 2.202 Erstellung eines Handbuchs zur IT-Sicherheit **- entfallen**

M 2.203 Aufbau einer Informationsbörse zur IT-Sicherheit **- entfallen**

M 2.204 Verhinderung ungesicherter Netzzugänge

M 2.205 Übertragung und Abruf personenbezogener Daten

M 2.206 Planung des Einsatzes von Lotus Notes/Domino

M 2.207 Sicherheitskonzeption für Lotus Notes/Domino

M 2.208 Planung der Domänen und der Zertifikatshierarchie von Lotus Notes **- entfallen**

M 2.209 Planung des Einsatzes von Lotus Notes im Intranet **- entfallen**

M 2.210 Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff **- entfallen**

M 2.211 Planung des Einsatzes von Lotus Notes in einer DMZ **- entfallen**

M 2.212 Organisatorische Vorgaben für die Gebäudereinigung

M 2.213 Inspektion und Wartung der technischen Infrastruktur

M 2.214 Konzeption des IT-Betriebs

M 2.215 Fehlerbehandlung

M 2.216 Genehmigungsverfahren für IT-Komponenten

M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen

M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten

M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung

M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle

M 2.221 Änderungsmanagement

M 2.222 Regelmäßige Kontrollen der technischen IT-Sicherheitsmaßnahmen **- entfallen**

M 2.223 Sicherheitsvorgaben für die Nutzung von Standardsoftware

M 2.224 Vorbeugung gegen Schadprogramme

M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten

M 2.226 Regelungen für den Einsatz von Fremdpersonal

M 2.227 Planung des Windows 2000 Einsatzes **- entfallen**

M 2.228 Festlegen einer Windows 2000 Sicherheitsrichtlinie **- entfallen**

M 2.229 Planung des Active Directory

M 2.230 Planung der Active Directory-Administration

M 2.231 Planung der Gruppenrichtlinien unter Windows

M 2.232 Planung der Windows-CA-Struktur ab Windows 2000

M 2.233 Planung der Migration von Windows NT auf Windows 2000 **- entfallen**

M 2.234 Konzeption von Internet-PCs

M 2.235 Richtlinien für die Nutzung von Internet-PCs

M 2.236 Planung des Einsatzes von Novell eDirectory

M 2.237 Planung der Partitionierung und Replikation im Novell eDirectory

M 2.238 Festlegung einer Sicherheitsrichtlinie für Novell eDirectory

M 2.239 Planung des Einsatzes von Novell eDirectory im Intranet

M 2.240 Planung des Einsatzes von Novell eDirectory im Extranet

M 2.241 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

M 2.242 Zielsetzung der elektronischen Archivierung

M 2.243 Entwicklung des Archivierungskonzepts

M 2.244 Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung

M 2.245 Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung

M 2.246 Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung

M 2.247 Planung des Einsatzes von Exchange und Outlook

M 2.248 Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000 **- entfallen**

M 2.249 Planung der Migration von Exchange-Systemen

M 2.250 Festlegung einer Outsourcing-Strategie

M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters

M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister

M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben

M 2.255 Sichere Migration bei Outsourcing-Vorhaben

M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb

M 2.257 Überwachung der Speicherressourcen von Archivmedien

M 2.258 Konsistente Indizierung von Dokumenten bei der Archivierung

M 2.259 Einführung eines übergeordneten Dokumentenmanagements

M 2.260 Regelmäßige Revision des Archivierungsprozesses

M 2.261 Regelmäßige Marktbeobachtung von Archivsystemen

M 2.262 Regelung der Nutzung von Archivsystemen

M 2.263 Regelmäßige Aufbereitung von archivierten Datenbeständen

M 2.264 Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung

M 2.265 Geeigneter Einsatz digitaler Signaturen bei der Archivierung

M 2.266 Regelmäßige Erneuerung technischer Archivsystem-Komponenten

M 2.267 Planen des IIS-Einsatzes **- entfallen**

M 2.268 Festlegung einer IIS-Sicherheitsrichtlinie **- entfallen**

M 2.269 Planung des Einsatzes eines Apache Webservers **- entfallen**

M 2.270 Planung des SSL-Einsatzes beim Apache Webserver **- entfallen**

M 2.271 Festlegung einer Sicherheitsstrategie für den WWW-Zugang **- entfallen**

M 2.272 Einrichtung eines Internet-Redaktionsteams

M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

M 2.274 Vertretungsregelungen bei E-Mail-Nutzung

M 2.275 Einrichtung funktionsbezogener E-Mailadressen **- entfallen**

M 2.276 Funktionsweise eines Routers

M 2.277 Funktionsweise eines Switches

M 2.278 Typische Einsatzszenarien von Routern und Switches

M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches

M 2.280 Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches

M 2.281 Dokumentation der Systemkonfiguration von Routern und Switches

M 2.282 Regelmäßige Kontrolle von Routern und Switches

M 2.283 Software-Pflege auf Routern und Switches

M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse

M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien

M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit

M 2.340 Beachtung rechtlicher Rahmenbedingungen

M 2.341 Planung des SAP Einsatzes

M 2.342 Planung von SAP Berechtigungen

M 2.343 Absicherung eines SAP Systems im Portal-Szenario

M 2.344 Sicherer Betrieb von SAP Systemen im Internet

M 2.345 Outsourcing eines SAP Systems

M 2.346 Nutzung der SAP Dokumentation

M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme

M 2.348 Sicherheit beim Customizing von SAP Systemen

M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme

M 2.350 Aussonderung von SAP Systemen

M 2.351 Planung von Speicherlösungen

M 2.352 Erstellung einer Sicherheitsrichtlinie für NAS-Systeme **- entfallen**

M 2.353 Erstellung einer Sicherheitsrichtlinie für SAN-Systeme **- entfallen**

M 2.354 Einsatz einer hochverfügbaren SAN-Lösung

M 2.355 Auswahl von Lieferanten für eine Speicherlösung

M 2.356 Vertragsgestaltung mit Dienstleistern für Speicherlösungen

M 2.357 Aufbau eines Administrationsnetzes für Speichersysteme

M 2.358 Dokumentation der Systemeinstellungen von Speichersystemen

M 2.359 Überwachung und Verwaltung von Speicherlösungen

M 2.360 Sicherheits-Audits und Berichtswesen bei Speichersystemen

M 2.361 Außerbetriebnahme von Speicherlösungen

M 2.362 Auswahl einer geeigneten Speicherlösung

M 2.363 Schutz gegen SQL-Injection

M 2.364 Planung der Administration ab Windows 2003

M 2.365 Planung der Systemüberwachung unter Windows Server 2003

M 2.366 Nutzung von Sicherheitsvorlagen unter Windows Server 2003

M 2.501 Datenschutzmanagement

M 2.502 Regelung der Verantwortlichkeiten im Bereich Datenschutz

M 2.503 Aspekte eines Datenschutzkonzeptes

M 2.504 Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten

M 2.505 Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

M 2.506 Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten

M 2.507 Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten

M 2.508 Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten

M 2.509 Datenschutzrechtliche Freigabe

M 2.510 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten

M 2.511 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

M 2.512 Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten

M 2.513 Dokumentation der datenschutzrechtlichen Zulässigkeit

M 2.514 Aufrechterhaltung des Datenschutzes im laufenden Betrieb

M 2.515 Datenschutzgerechte Löschung/Vernichtung

M 2.516 Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender

M 2.517 Vertragsgestaltung mit Dritt-Dienstleistern

M 2.518 Einsatz einer hochverfügbaren Firewall-Lösung

M 2.519 Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing

M 2.520 Sicheres und vollständiges Löschen von Cloud-Anwenderdaten

M 2.521 Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten

M 2.522 Berichtswesen und Kommunikation zu den Cloud-Anwendern

M 2.523 Sichere Automatisierung der Cloud-Regelprozesse

M 2.575 Regelmäßige Sicherheitsaudits für die Software-Entwicklungsumgebung

M 2.576 Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen

M 2.577 Auswahl geeigneter Kryptoverfahren für Netze

M 2.578 Installation, Konfiguration und Betreuung eines lokalen Netzes durch Dritte

M 2.579 Regelmäßige Audits des lokalen Netzes

M 2.580 Außerbetriebnahme von Netzkomponenten

M 2.581 Aufbau eines Administrationsnetzes für das Netzmanagement

M 2.582 Möglichkeiten zur Einrichtung eines Managementnetzes

M 2.583 Geeignete Auswahl eines Netzmanagement-Systems

M 2.584 Geregelte Außerbetriebnahme eines Netz- und Systemmanagement-Tools

M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements

M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen

M 2.587 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement

# M 2.1 Festlegung von Verantwortlichkeiten und Regelungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Organisation

Für alle wesentlichen Aufgaben und Geschäftsprozesse in einer Institution sollten die Verantwortlichkeiten nachvollziehbar geregelt sein. Die Aufgaben sollten dabei so zugeschnitten sein, dass es keine Überschneidungen zwischen ähnlichen Aufgaben gibt, aber auch keine Zuständigkeitslücken. Dies sollte für alle Bereiche eine Selbstverständlichkeit sein, für alle sicherheitsrelevanten Aufgaben ist es aber unabdingbar.

Die sicherheitsrelevanten Aufgaben aller internen und externen Mitarbeiter und Dienstleister müssen nachvollziehbar festgelegt sein. Sie müssen mit den Sicherheitszielen der Institution abgestimmt sein. Zu den Bereichen, die geregelt werden sollten, gehören beispielsweise:

- explizite Zuweisung der Verantwortlichkeiten und Befugnisse an Rollen bzw. Organisationseinheiten bei allen sicherheitsrelevanten Aufgaben (Dabei ist sicherzustellen, dass alle Rollen konkreten Personen zugeordnet sind),
- geeigneter Umgang mit geschäftskritischen Informationen, so dass deren Vertraulichkeit, Integrität und Verfügbarkeit angemessen geschützt sind,
- Vertraulichkeitsvereinbarungen,
- Einbeziehung des Sicherheitsbeauftragten bei Aufträgen und Projekten, die geschäftskritische Informationen betreffen,
- Unterrichtungen über den geeigneten Umgang mit geschäftskritischen Informationen, beispielsweise im Kontakt mit Kunden oder auf Reisen,
- Festlegung von Verhaltensregeln und Informationspflichten bei sicherheitsrelevanten Aktionen und bei Sicherheitsvorfällen,
- Klassifikation von Informationen entsprechend ihres Schutzbedarfs.

Die Regelungen für Informationssicherheit sollten mit denen für Datenschutz und Geheimschutz in geeigneter Weise zusammengeführt werden, damit sie von den Mitarbeitern leichter adaptiert und besser wahrgenommen werden können. Wichtig ist auch, dass alle Regelungen zusammengenommen widerspruchsfrei sind.

Übergreifende Regelungen zur Informationssicherheit müssen als ein Aspekt der Informationsverarbeitung verbindlich festgelegt werden.

Es empfiehlt sich, Regelungen unter anderem über die Themen

- Datensicherung,
- Datenarchivierung,
- Datenträgertransport,
- Datenübertragung,
- Datenträgervernichtung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Zutritts-, Zugangs- und Zugriffsberechtigungen,
- Wartungs- und Reparaturarbeiten,
- Datenschutz,
- Schutz gegen Schadsoftware,
- Revision,
- Notfallvorsorge und

- Vorgehensweise bei der Verletzung von Sicherheitsrichtlinien

zu treffen. Hinweise dazu finden sich in den Maßnahmenbeschreibungen der jeweils relevanten IT-Grundschutz-Bausteine.

Die in Kraft gesetzten Regelungen sind den betroffenen Mitarbeitern in geeigneter Weise bekannt zu geben (siehe M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*). Es empfiehlt sich, die Bekanntgabe zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.

Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu vermeiden und gegebenenfalls aufzulösen. Alle Regelungen sollten deshalb auch ein Erstellungsdatum oder eine Versionsnummer enthalten.

Prüffragen:

- Sind die Verantwortlichkeiten und Befugnisse bei allen sicherheitsrelevanten Aufgaben klar geregelt?
- Werden die Regelungen regelmäßig überarbeitet und auf einem aktuellen Stand gehalten?
- Wurden die Regelungen allen Mitarbeitern bekannt gegeben?

# M 2.2 Betriebsmittelverwaltung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Organisation

Als Betriebsmittel (oder Sachmittel) werden alle Arbeitsmittel bezeichnet, die zur Erfüllung einer Aufgabe oder eines Geschäftsprozesses erforderlich sind. Dazu gehören beispielsweise alle erforderlichen Werkzeuge, Einrichtungen und Möbel. Betriebsmittel für den IT-Einsatz sind Mittel wie Hardware-Komponenten (Rechner, Tastatur, Drucker usw.), Software (Systemsoftware, Individualprogramme, Standardprogramme und Ähnliches), Verbrauchsmaterial (Papier, Toner, Druckerpatronen), Datenträger (Magnetbänder, Festplatten, Wechselplatten, CD-ROMs und Ähnliches). Die Betriebsmittelverwaltung umfasst die Abwicklung der Aufgaben:

- Beschaffung der Betriebsmittel,
- Prüfung vor Einsatz,
- Kennzeichnung und
- Bestandsführung.

Die **Beschaffung** von Betriebsmitteln ist beim Einsatz von Informationstechnik von besonderer Bedeutung. Mit einem geregelten Beschaffungsverfahren lassen sich insbesondere die Ziele unterstützen, die mit dem Einsatz von Informationstechnik angestrebt werden: Leistungssteigerung, Wirtschaftlichkeit, Verbesserung der Kommunikationsmöglichkeiten.

Neben reinen Wirtschaftlichkeitsaspekten kann durch ein geregeltes Beschaffungsverfahren - das von zentraler Stelle aus vorgenommen werden kann - auch die Neu- und Weiterentwicklung im Bereich der Informationstechnik stärker berücksichtigt werden.

Eine zentrale Beschaffung sichert darüber hinaus die Einführung und Einhaltung eines "Hausstandards", der die Schulung der Mitarbeiter und Wartungsaktivitäten vereinfacht.

Mit einem geregelten **Prüfverfahren vor Einsatz** der Betriebsmittel lassen sich unterschiedliche Gefährdungen abwenden. Beispiele sind:

- Die Vollständigkeit von Lieferungen (z. B. Handbücher oder Anschlusskabel) sollte überprüft werden, um die Verfügbarkeit aller Lieferteile zu gewährleisten.
- Neue PC-Software sowie neue vorformatierte Datenträger sollte mit einem Computer-Viren-Suchprogramm getestet werden.
- Es sollten Testläufe neuer Software auf speziellen Test-Systemen durchgeführt werden, damit diese reibungslos in den Betrieb übernommen werden können.
- Die Kompatibilität neuer Hardware- und Softwarekomponenten mit den vorhandenen sollte vor der Beschaffung überprüft werden, damit es nicht zu Fehlkäufen kommt.

Erst mit Hilfe einer **Bestandsführung** der eingesetzten Betriebsmittel ist es möglich, den Verbrauch zu ermitteln und rechtzeitig erforderliche Nachbestellungen zu veranlassen. Darüber hinaus ermöglicht die Bestandsführung Vollständigkeitskontrollen, Überprüfung des Einsatzes von nicht genehmigter Software oder die Feststellung der Entwendung von Betriebsmitteln. Hierzu bedarf es einer eindeutigen **Kennzeichnung** der wesentlichen Betriebsmittel mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierte fortlaufende Inventarnummern). Zusätzlich sollten die Seriennummern vorhandener Geräte

wie Bildschirm, Drucker, Festplatten etc. dokumentiert werden, damit sie nach einem Diebstahl identifiziert werden können.

Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Ein solches Bestandsverzeichnis muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib der Betriebsmittel,
- Lagervorhaltung,
- Aushändigungsvorschriften und
- Wartungsverträge, Wartungsintervalle.

Um den Missbrauch von Daten zu verhindern, muss die Löschung oder Vernichtung von Betriebsmitteln geregelt sein. Insbesondere ist der Umgang mit Altpapier zu regeln. Es muss geeignete Entsorgungsmöglichkeit für Verbrauchsgüter mit höherem Schutzbedarf geben, z. B. so genannte Schredder oder Aktenvernichter für Papier. Alles nähere ist im Baustein B 1.15 *Löschen und Vernichten von Daten* beschrieben.

Prüffragen:

- Kann der Bestand und der Verbleib von Betriebsmitteln über Bestandsverzeichnisse nachvollzogen werden?
- Wird nicht mehr benötigtes Verbrauchsmaterial ordnungsgemäß entsorgt?

# M 2.3 Datenträgerverwaltung

**Verantwortlich für Initiierung:** Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Archivverwalter, Fachverantwortliche

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten. Bei analogen Datenträgern haben die meisten Institutionen eine eingespielte und erprobte Verfahrensweise für deren Verwaltungen, nämlich die klassische Aktenführung. Daher werden in dieser Maßnahme die digitalen Datenträger in den Vordergrund gestellt, die einzelnen Empfehlungen gelten aber sinngemäß für alle Arten von Datenträgern.

**Bestandsverzeichnisse** ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben beispielsweise Auskunft über Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.

Die äußerliche **Kennzeichnung** von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Magnetbandes mit dem Stichwort "Telefongebühren"), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der **Aufbewahrung** von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Der **Versand oder Transport** von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine "Restdaten" enthalten. Dies kann durch physikalisches Löschen erreicht werden. Stehen hierzu keine Werkzeuge zur Verfügung, so sollte der Datenträger zumindest formatiert werden. Dabei sollte sichergestellt werden, dass mit dem zugrunde liegenden Betriebssystem eine Umkehr des Befehls nicht möglich ist.

Weiterhin ist zu beachten, dass vor Abgabe wichtiger Datenträger eine Sicherungskopie erstellt wird. Weitere Ausführungen zum Versand und Transport von Datenträgern enthält der Baustein B 5.2 *Datenträgeraustausch*.

Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel digitale Daten übermittelt, sollte generell ein Computer-Viren-Check des Datenträgers bzw. der Datensätze erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer digitaler Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von digitalen Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern muss die Löschung der gespeicherten Daten vorgenommen werden (siehe hierzu B 1.15 *Löschen und Vernichten von Daten*).

Prüffragen:

- Gibt es aktuelle Bestandsverzeichnisse über alle eingesetzten Datenträger?
- Werden die Datenträger gemäß der Herstellerangaben sachgerecht behandelt?
- Ist für alle Arten von Datenträgern der ordnungsgemäße Umgang inklusive Aufbewahrung, Weitergabe, Transport und Löschung geregelt?

# M 2.4 Regelungen für Wartungs- und Reparaturarbeiten

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Leiter IT

Um die IT vor Störungen zu bewahren, müssen regelmäßig Wartungsarbeiten durchgeführt werden. Die **rechtzeitige Einleitung** von Wartungsarbeiten und die Überprüfung ihrer Durchführung sollte von einer zentralen Stelle aus wahrgenommen werden (z. B. Beschaffungsstelle). Dabei sollten die Wartungsarbeiten von vertrauenswürdigen Personen oder Firmen ausgeführt werden, falls sie nicht von eigenem Personal durchgeführt werden können. Die Hinweise des Herstellers müssen dabei unbedingt beachtet werden. Bei regelmäßigen Wartungsarbeiten durch Externe kann der Abschluss eines Wartungsvertrages vorteilhaft sein.

Für jedes IT-System sollte dokumentiert werden, wann es gewartet wurde und welche Fehler dabei behoben wurden(z. B. Gerätepass oder Geräte- bzw. Konfigurationsmanagementsystem). Es empfiehlt sich außerdem, ein Informationssystem für Wartungs- und Reparaturarbeiten einzurichten. Mit einem solchen System können anstehende Arbeiten geplant und durchgeführte Arbeiten dokumentiert sowie der erfolgreiche Verlauf kontrolliert werden.

Außerdem sollte darin dokumentiert sein, wer für die Wartung oder Reparatur von Geräten verantwortlich ist.

**Regelmäßige Reinigung von IT-Geräten**

Alle Arten von IT-Geräten sollten regelmäßig gereinigt werden. Die hierfür empfehlenswerten Intervalle hängen von der Art des Gerätes bzw. der Einsatzumgebung ab. Mindestens einmal pro Jahr sollte aber eine Reinigung erfolgen, nicht nur weil es unangenehm ist, mit verschmutzten Geräten zu arbeiten, sondern auch weil Verschmutzungen deren Funktionsfähigkeit beeinträchtigen können.

**Beispiele:** Tastaturen sollten spätestens dann gesäubert werden, wenn sie klebrig werden oder einzelne Tasten klemmen. Ein Arbeitsplatz-PC sollte gelegentlich (z. B. einmal jährlich) auch innen von Staub befreit werden, sofern die Herstellerangaben nicht eine andere Vorgehensweise vorschlagen. Bei Druckern kann bei nachlässiger Reinigung die Druckqualität leiden oder Komponenten in der Funktion eingeschränkt oder sogar beschädigt werden. Typische Problempunkte sind Druckerwalzen, Druckköpfe und Tonerstaub-Ansammlungen.

Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen. Durch Verunreinigungen auf Platinen (besonders wirkungsvoll sind Kombinationen aus Staub und Teer- und Nikotinablagerungen) können Kriechströme verursacht werden.

Ablagerungen sollten daher regelmäßig vorsichtig entfernt werden. Insbesondere sollte für eine wirkungsvolle Lüftung aller IT-Systeme gesorgt werden. Alle Belüfter und Lüftungskomponenten müssen von störenden Verunreinigungen frei gehalten werden.

Bei der Reinigung von IT-Geräten sind unbedingt die Vorgaben des Herstellers zu beachten, sowohl bei der Vorgehensweise und Werkzeug-Auswahl als auch bei den Mindest-Wartungsintervallen.

**Wartungs- und Reparaturarbeiten im Hause**

Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren **Beaufsichtigung** zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde.

Als **Maßnahmen vor und nach Wartungs- und Reparaturarbeiten** sind einzuplanen:

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen und vertrauenswürdige Firmen auszuwählen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind, je nach "Eindringtiefe" des Wartungspersonals, Passwortänderungen erforderlich. Im PC-Bereich sollte ein Computer-Viren-Check durchgeführt werden.
- Nach den Wartungsarbeiten sollten die Geräte mit einem aktuellen Computer-Viren-Schutzprogramm auf Schadsoftware überprüft werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie eventuell Name des Wartungstechnikers).
- Beauftragte Firmen sollten schriftlich zusichern, dass sie einschlägige Sicherheitsvorschriften und Richtlinien (z. B. Brandschutz, VdS 2008 Schweiß-, Löt- und Trennschleifarbeiten) beachten. Dies gilt für alle Tätigkeiten, bei denen eine direkte oder indirekte Gefahr für Gebäude oder Menschen entstehen können. Letztlich kommt es darauf an, dass das vor Ort eingesetzte Personal mit diesen Regeln vertraut ist.
- Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren.

**Externe Wartungs- und Reparaturarbeiten**

Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen Informationssicherheitsmaßnahmen zu verpflichten. Entsprechend M 3.55 *Vertraulichkeitsvereinbarungen* sind mit diesen vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Bei der Durchführung externer Wartungsarbeiten muss protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, was der Wartungs- bzw. Reparaturauftrag umfasst, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde. Um dies nachhalten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.

Beim Versand oder Transport der zu reparierenden Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Reparaturauftrag, Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.

Bei IT-Systemen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung, alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie "REPARATUR" gesetzt werden, damit die Wartungstechniker auf die Geräte zugreifen können.

Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. **Alle** Passwörter sind zu ändern. PC-Datenträger sind nach der Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Computer-Viren zu überprüfen. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

**Fernwartung**

Regelungen für die Fernwartung können der Maßnahme M 5.33 *Absicherung von Fernwartung* entnommen werden.

Prüffragen:

- Wissen die Mitarbeiter, dass Wartungspersonal bei Arbeiten im Haus beaufsichtigt werden muss?
- Werden Nachweise über durchgeführte Wartungsarbeiten geführt?
- Liegt ein Fristenplan für Wartungsarbeiten vor?

# M 2.5 Aufgabenverteilung und Funktionstrennung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation

Die von der Behörde bzw. dem Unternehmen im Zusammenhang mit dem IT-Einsatz wahrzunehmenden Funktionen sind festzulegen. Zu unterscheiden sind hier zwei Ebenen:

- Die erste Ebene besteht aus den Funktionen, die den IT-Einsatz ermöglichen oder unterstützen wie Arbeitsvorbereitung, Datennachbereitung, Operating, Programmierung, Netzadministration, Rechteverwaltung, Revision.
- Die zweite Ebene besteht aus den Funktionen, die die zur Aufgabenerfüllung bereitstehenden IT-Verfahren anwenden. Beispiele solcher Funktionen sind: Fachverantwortlicher, IT-Anwendungsbetreuer, Datenerfasser, Sachbearbeiter, Zahlungsanordnungsbefugter.

Im nächsten Schritt ist die **Funktionstrennung** festzulegen und zu begründen, d. h. welche Funktionen nicht miteinander vereinbar sind, also auch nicht von **einer** Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. **Beispiele** dafür sind:

- Rechteverwaltung und Revision,
- Netzadministration und Revision,
- Programmierung und Test bei eigenerstellter Software,
- Datenerfassung und Zahlungsanordnungsbefugnis,
- Revision und Zahlungsanordnungsbefugnis.

Insbesondere wird deutlich, dass meistens operative Funktionen nicht mit kontrollierenden Funktionen vereinbar sind.

Nach der Festlegung der einzuhaltenden Funktionstrennung kann die Zuordnung der Funktionen zu Personen erfolgen. Vertreterregelungen sind ebenfalls zu berücksichtigen und zu dokumentieren (siehe auch M 3.3 *Vertretungsregelungen*).

Die hier getroffenen Festlegungen sind zu dokumentieren und bei Veränderungen im IT-Einsatz zu aktualisieren. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.

Prüffragen:

- Sind alle relevanten Funktionen innerhalb der Institution definiert, die Informationen zu ihrer Aufgabenerfüllung verwenden oder dabei unterstützend tätig sind?
- Sind Funktionstrennungen für unvereinbare Funktionen vollständig festgelegt und dokumentiert?
- Wird die Funktionstrennung personell aufrechterhalten?

# M 2.6 Vergabe von Zutrittsberechtigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Leiter Organisation

Vor der Vergabe von Zutrittsberechtigungen für Personen sind die schutzbedürftigen Räume eines Gebäudes zu bestimmen, z. B. Büro, Datenträgerarchiv, Serverraum, Operating-Raum, Maschinensaal, Belegarchiv, Rechenzentrum. Der Schutzbedarf eines Raumes leitet sich ab aus dem Schutzbedarf der im jeweiligen Raum verarbeiteten Informationen, der dort vorhandenen IT-Systeme und der Datenträger, die in diesem Raum gelagert und benutzt werden.

Anschließend ist festzulegen, welche Person zur Ausübung der wahrgenommenen Funktion welches Zutrittsrecht benötigt. Dabei ist die vorher erarbeitete Funktionstrennung (M 2.5 *Aufgabenverteilung und Funktionstrennung*) zu beachten. Unnötige Zutrittsrechte sind zu vermeiden.

Um die Zahl zutrittsberechtigter Personen zu einem Raum möglichst gering zu halten, sollte der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert z. B. eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern den unerlaubten Zugriff eines Wartungstechnikers auf die Datenträger.

Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Bei der Rücknahme einer Zutrittsberechtigung muss die Rücknahme der Zutrittsmittel gewährleistet sein. Zusätzlich ist zu dokumentieren, welche Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen aufgetreten sind. Gründe für Konflikte können vorliegen, weil Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder aufgrund räumlicher Notwendigkeiten.

Zur Überwachung der Zutrittsberechtigung können Personen (Pförtner, Schließdienst) oder technische Einrichtungen (Ausweisleser, biometrische Verfahren wie Irisscanner oder Fingerabdruck, Sicherheitstürschloss bzw. Schließanlage) eingesetzt werden (siehe M 2.14 *Schlüsselverwaltung*). Der Zutritt zu schutzbedürftigen Räumen von nicht autorisiertem Personal (z. B. Besuchern, Reinigungs- und Wartungspersonal) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.

Regelungen über die Vergabe und Rücknahme von Zutrittsberechtigungen für Fremdpersonal und Besucher müssen ebenfalls getroffen werden.

Prüffragen:

- Wurde festgelegt, welche Zutrittsrechte an welche Personen im Rahmen ihrer Funktionen vergeben wurden?
- Ist die Dokumentation der Zutrittsberechtigungen aktuell und vollständig in Bezug auf schutzbedürftige Räume?

# M 2.7 Vergabe von Zugangsberechtigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, Leiter IT

Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Zugangsberechtigungen sollten möglichst restriktiv vergeben werden. Diese sind für jede nutzungsberechtigte Person aufgrund ihrer Funktion, unter Beachtung der Funktionstrennung (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*), im einzelnen festzulegen. Entsprechend der Funktion ist der Zugang zum Rechner zu definieren, z. B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT-Anwendung (Anwender). Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Der Zugang zu IT-Systemen oder IT-Anwendungen sollte erst nach einer Identifikation (z. B. durch Name, Benutzer-Kennung oder Chipkarte) und Authentisierung (z. B. durch ein Passwort oder über ein Authentisierungstoken) des Nutzungsberechtigten möglich sein und protokolliert werden.

Die Ausgabe bzw. der Entzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentisierungsmitteln (z. B. Umgang mit Chipkarten, Passworthandhabung, siehe M 2.11 *Regelung des Passwortgebrauchs*) müssen ebenfalls getroffen werden. Alle Zugangsberechtigten müssen auf den korrekten Umgang mit den Zugangsmitteln hingewiesen werden.

Zugangsberechtigungen sollten bei längeren Abwesenheiten von berechtigten Personen vorübergehend gesperrt werden, um Missbrauch zu verhindern, z. B. bei Krankheit oder Urlaub. Dies sollte zumindest bei Personen mit weitreichenden Berechtigungen wie Administratoren erfolgen.

Es ist notwendig, die vorgenannten Festlegungen auf ihre korrekte Einhaltung sporadisch zu kontrollieren.

Prüffragen:

- Liegt eine aktuelle Dokumentation über Vergabe sowie Entzug von Zugangsberechtigungen und Zugangsmitteln vor?
- Orientiert sich die Vergabe von Zugangsberechtigungen an den Funktionen der Zugangsberechtigten?
- Werden die Zugangsberechtigten auf den korrekten Umgang mit Zugangsmitteln hingewiesen?
- Werden Zugangsberechtigungen bei längeren Abwesenheiten von berechtigten Personen vorübergehend gesperrt?

# M 2.8 Vergabe von Zugriffsrechten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z. B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, die die Person wahrnimmt, z. B. Anwenderbetreuung, Arbeitsvorbereitung, Systemprogrammierung, Anwendungsentwicklung, Systemadministration, Revision, Datenerfassung, Sachbearbeitung. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Eine Vielzahl von IT-Systemen lassen es zu, dass verschiedene Rechte als Gruppenrechte bzw. als Rechteprofil definiert werden (z. B. Gruppe Datenerfassung). Diese Definition entspricht der technischen Umsetzung der Rechte, die einer Funktion zugeordnet werden. Für die Administration der Rechte eines IT-Systems ist es vorteilhaft, solche Gruppen oder Profile zu erstellen, da damit die Rechtezuteilung und deren Aktualisierung erheblich vereinfacht werden kann.

Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Aus der Dokumentation muss hervorgehen:

- welche Funktion unter Beachtung der Funktionstrennung (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) mit welchen Zugriffsrechten ausgestattet wird,
- welche Gruppen bzw. Profile eingerichtet werden,
- welche Person welche Funktion wahrnimmt,
- welche Zugriffsrechte eine Person im Rahmen welcher Rolle erhält (hierbei sollten auch die Zugriffsrechte von Vertretern erfasst werden) und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Diese Konflikte können z. B. daraus resultieren, dass eine Person unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom IT-System die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.
- welche Personen in einem Notfall welche Zugriffsrechte erhalten, z. B. da sie zum Krisenstab gehören.

Die Vorgehensweise bei der Funktionstrennung und der Rechtevergabe wird am nachfolgenden Beispiel erläutert.

Die betrachtete Anwendung ist ein Reisekosten-Abrechnungssystem. Die relevanten Räume sind in nachfolgender Graphik erläutert. Das IT-System besteht aus einem LAN, an dem neben einem Server und der Bedienkonsole drei PCs als Arbeitsplatzrechner angeschlossen sind.

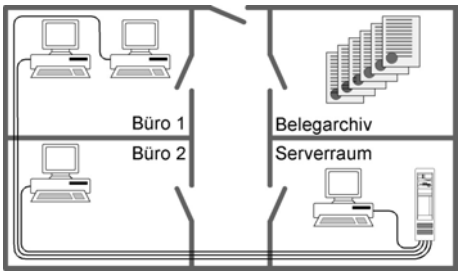



Abbildung: Aufgabenverteilung und Funktionstrennung

**Schritt 1: Aufgabenverteilung und Funktionstrennung**

Folgende Funktionen sind für das betrachtete Reisekosten-Abrechnungssystem notwendig:

1. LAN-Administration
2. Revision
3. Datenerfassung
4. Sachbearbeitung mit Feststellung der rechnerischen Richtigkeit
5. Sachbearbeitung mit Feststellung der sachlichen Richtigkeit
6. Sachbearbeitung mit Anordnungsbefugnis

Folgende Funktionen sind aufgrund der Sachzwänge nicht miteinander vereinbar:

- Funktion 1 und Funktion 2 (die Administration darf sich nicht selbst kontrollieren)
- Funktion 2 und Funktion 6 (der Anordnungsbefugte darf sich nicht selbst kontrollieren)
- die Kombination der Funktionen 4 oder 5 mit 6 (das Vier-Augen-Prinzip wäre verletzt für Zahlungsanweisungen)

Diese Funktionen werden durch folgende Personen wahrgenommen:

| | | **Hr. Mayer** | **Fr. Schmidt** | **Hr. Müller** | **Fr. Fleiß** |
|---|---|---|---|---|---|
| 1. | LAN-Administration | X | | | |
| 2. | Revision | | X | | |
| 3. | Datenerfassung | | | X | |
| 4. | Sachbearbeitung rechn. | | | X | |
| 5. | Sachbearbeitung sachl. | | | X | |
| 6. | Anordnungsbefugnis | | | | X |

**Schritt 2: Vergabe von Zutrittsrechten**

Nachfolgend wird der Schutzbedarf der einzelnen Räume begründet und in der Tabelle die Vergabe der Zutrittsrechte dokumentiert:

- Serverraum:
  Der unbefugte Zutritt zum Server muss verhindert werden, weil die Verfügbarkeit, Integrität und Vertraulichkeit der gesamten Anwendung von dieser zentralen Komponente abhängig ist.
- Belegarchiv:
  Für die Rechnungslegung müssen die Reisekostenabrechnungen längerfristig aufbewahrt werden. Es ist sicherzustellen, dass die Belege vollständig und unverändert aufbewahrt werden.
- Büro 1:
  In diesem Büro werden die notwendigen Daten erfasst sowie die rechnerische und sachliche Richtigkeit festgestellt. Für die Gewährleistung der Korrektheit dieser Vorgänge muss verhindert werden, dass Unbefugte Zutritt zu den Arbeitsplatzrechnern erhalten.
- Büro 2:
  Hier wird die Auszahlung der Reisekosten am APC angeordnet. Dieser Vorgang darf nur von einer befugten Person vorgenommen werden. Unbefugten ist der Zutritt zu verwehren.

| | | **Serverraum** | **Belegarchiv** | **Büro 1** | **Büro 2** |
|---|---|---|---|---|---|
| 1. | LAN-Administration | X | | | |
| 2. | Revision | X | X | X | X |
| 3. | Datenerfassung | | | X | |
| 4. | Sachbearbeitung rechn. | | X | X | |
| 5. | Sachbearbeitung sachl. | | X | X | |
| 6. | Anordnungsbefugnis | | X | X | X |

**Schritt 3: Vergabe von Zugangsberechtigungen**

Aufgrund der Funktionen ergeben sich folgende Zugangsberechtigungen:

| | | **Betriebssystem Server** | **Anwendung Protokollauswertung** | **Anwendung Datenerfassung** | **Anwendung Belegbearbeitung** |
|---|---|---|---|---|---|
| 1. | LAN-Administration | X | | | |
| 2. | Revision | X | X | | X |

| | | Betriebssystem Server | Anwendung Protokollauswertung | Anwendung Datenerfassung | Anwendung Belegbearbeitung |
|---|---|---|---|---|---|
| 3. | Datenerfassung | | | X | |
| 4. | Sachbearbeitung rechn. | | | | X |
| 5. | Sachbearbeitung sachl. | | | | X |
| 6. | Anordnungsbefugnis | | | | X |

**Schritt 4: Vergabe von Zugriffsrechten**

Im folgenden werden die Zugriffsrechte, die eine Funktion zur Ausübung benötigt, dargestellt. Es bezeichnen:

A = Recht zur Ausführung der Anwendung/Software

L = Leserecht auf Daten

S = Schreibrecht, d.h. Erzeugen von Daten

M = Recht zum Modifizieren von Daten

Ö = Recht zum Löschen von Daten

U = Recht zum Unterschreiben von Zahlungsanweisungen

| | | Betriebssystem Server | Protokollauswertung | Anwendung Datenerfassung | Anwendung Belegbearbeitung |
|---|---|---|---|---|---|
| 1. | LAN-Administration | A,L,S,M,Ö | | | |
| 2. | Revision | A,L | A,L,Ö | | A,L |
| 3. | Datenerfassung | | | A,S | |
| 4. | Sachbearbeitung rechn. | | | | A,L,M |
| 5. | Sachbearbeitung sachl. | | | | A,L,M |
| 6. | Anordnungsbefugnis | | | | A,L,U |

Eine solche Dokumentation erleichtert die Rechteverteilung. Angenommen, dass Frau Schmidt den Arbeitgeber wechseln würde und ihre Stelle neu besetzt werden müsste, so lässt sich anhand der obigen Tabellen einfach feststellen, welche der ehemaligen Rechte Frau Schmidts zu löschen und für die neue Kraft einzurichten sind. Wenn die neue Kraft zusätzlich vertretungsweise die Funktion Sachbearbeitung mit Anordnungsbefugnis übernehmen soll, so wird anhand der durchzuführenden Rechteverteilung der Konflikt offenbar, dass die neue Kraft im Vertretungsfall Manipulationen unbemerkt durchführen könnte.

Prüffragen:

- Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?
- Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?
- Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?
- Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?

# M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Es ist durchaus üblich, dass Mitarbeiter eigene Hard- und Software wie beispielsweise private Mobiltelefone, PDAs oder Kameras auch dienstlich oder zumindest in den Diensträumen verwenden. Da die Nutzung von zusätzlicher Hardware über Standardschnittstellen wie USB und weitgehende Plug-and-Play-Funktionalität immer einfacher wird, muss deren Einsatz geregelt werden. Die Informationssicherheit kann dabei beispielsweise durch externe USB-Speichermedien (z. B. Festplatten, Memory-Sticks) oder private PDAs beeinträchtigt werden.

Es muss daher geregelt sein, wie Hard- und Software abgenommen, freigegeben, installiert bzw. benutzt werden darf. Maßnahmen, die zu diesem Zweck umgesetzt werden sollten, sind z. B.: M 2.216 *Genehmigungsverfahren für IT-Komponenten*, M 2.62 *Software-Abnahme- und Freigabe-Verfahren* bzw. Baustein B 1.10 *Standardsoftware* und M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*.

Das Einspielen bzw. Benutzen nicht freigegebener Hard- und Software muss verboten und außerdem durch technische Möglichkeiten soweit möglich verhindert werden. Bei den meisten Betriebssystemen kann dies durch Einschränkung der Benutzerumgebung erreicht werden. Damit soll verhindert werden, dass Programme mit unerwünschten Auswirkungen eingebracht werden. Zusätzlich soll verhindert werden, dass das System über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird. Es kann sinnvoll sein (z. B. um Makro-Viren vorzubeugen), dieses Nutzungsverbot auch auf das Einspielen privater Daten auszudehnen.

Bei Software ist zu dokumentieren, welche Versionen ausführbarer Dateien freigegeben wurden (inklusive Erstellungsdatum und Dateigröße). Die freigegebenen Programme sind regelmäßig auf Veränderungen zu überprüfen.

Nutzungsverbote nicht freigegebener Hard- und Software sollten schriftlich fixiert werden, alle Mitarbeiter sind darüber zu unterrichten. Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.

Prüffragen:

- Existiert eine Regelung zur Abnahme, Freigabe, Installation und Nutzung von Hard- und Software?
- Wurden alle Mitarbeiter über das Verbot für die Nutzung nicht freigegebener Hard- und Software informiert?
- Wird das Nutzungsverbot allen Mitarbeitern zur Kenntnis gebracht?
- Bei Ausnahmeregelungen: Wird ein Erlaubnisvorbehalt vorgesehen?
- Wird die Nutzung nicht freigegebener Hard- und Software technisch soweit möglich unterbunden?
- Werden freigegebene Programme regelmäßig auf Veränderungen überprüft?

# M 2.10 Überprüfung des Hard- und Software-Bestandes

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Vorgesetzte, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um Verstöße gegen das Verbot der Nutzung nicht freigegebener Hard- und Software feststellen zu können, ist eine regelmäßige Überprüfung des Hard- und Software-Bestandes notwendig. Ist die Zahl der IT-Systeme sehr groß, kann eine stichprobenartige Überprüfung durchgeführt werden. Die Ergebnisse der Überprüfung sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.

Wird bei der Überprüfung nicht genehmigte Hardware gefunden, muss dafür gesorgt werden, dass die IT-Komponenten nicht weiter vorschriftswidrig betrieben werden. Es muss zudem ermittelt werden, wer für den Betrieb verantwortlich ist, um geeignete Konsequenzen ergreifen zu können. Bei konkreten Verdachtsfällen ist bei der Kontrolle der Hardware auf Manipulationen und Zusatzgeräte, die z. B. zur Aufzeichnung von Tastaturanschlägen verwendet werden, zu achten.

Sollte bei der Überprüfung nicht freigegebene Software gefunden werden, so ist die Entfernung zu veranlassen. Um diese Überprüfung durchführen zu können, muss der überprüfenden Instanz die entsprechende Befugnis durch die Unternehmens- bzw. Behördenleitung verliehen werden. Zusätzlich muss der prüfenden Instanz bekannt sein, welche Software auf welchem IT-System freigegeben ist (Software-Bestandsverzeichnis).

Um bei der Vielzahl der üblicherweise eingesetzten Software effizient ein Software-Bestandsverzeichnis führen zu können, sollte hierfür ein entsprechendes Tool eingesetzt werden. Für die typische Client-Server-Umgebung sollte es netzfähig sein.

Vor der Festlegung einer Regelung zur Überprüfung des Hard- und Software-Bestandes sollte der Betriebs- bzw. Personalrat hinzugezogen werden.

Für solche IT-Systeme, die für den Wirkbetrieb des IT-Verbunds nicht erforderlich sind wie z. B. Testsysteme, kann anstelle einer regelmäßigen Überprüfung eine anlassbezogene Überprüfung durchgeführt werden. Beispielsweise kann die Prüfung auf solchen IT-Systemen immer dann vorgenommen werden, wenn Änderungen an der Konfiguration vorgenommen werden oder wenn das IT-System nach längerer Pause wieder in Betrieb gesetzt wird. Voraussetzung ist jedoch, dass für alle IT-Systeme die Maßnahme M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software* in Kraft ist.

Prüffragen:

- Findet eine regelmäßige, dokumentierte Überprüfung des Hard- und Software-Bestandes statt?
- Existiert ein Software-Bestandsverzeichnis?
- Bei Auffinden nicht genehmigter Hard- und Software: Wird der vorschriftswidrige Weiterbetrieb von Hard- und Software unverzüglich unterbunden?

- Bei Auffinden nicht genehmigter Hard- und Software: Wird der Verantwortliche für den Betrieb der nicht genehmigten Hard- und Software ermittelt?
- Bei Auffinden nicht genehmigter Hardware: Wird bei konkreten Verdachtsfällen eine weitergehende Kontrolle des IT-Systems auf weitere Manipulationen und Zusatzgeräte durchgeführt?
- Bei Untersuchung auf nicht genehmigte Software: Wird der untersuchenden Instanz eine entsprechende Befugnis durch die Leitung der Organisation verliehen?

# M 2.11 Regelung des Passwortgebrauchs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, IT-Sicherheitsbeauftragter

Werden in einem IT-System oder einer Anwendung Passwörter zur Authentisierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass die Passwörter korrekt gebraucht werden. Dafür ist es empfehlenswert, eine Regelung zum Passwortgebrauch einzuführen und die Benutzer von IT-Systemen diesbezüglich zu unterweisen.

Vorgaben für die Passwortgestaltung müssen immer einen praktikablen Kompromiss zwischen folgenden Sicherheitszielen darstellen:

- Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist.
- Die Anzahl der möglichen Passwörter im vorgegebenen Schema muss so groß sein, dass es nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann.
- Das Passwort darf nicht zu kompliziert sein, damit der Besitzer mit vertretbarem Aufwand in der Lage ist, es auswendig zu lernen.

Folgende Regeln zu Passwortgestaltung und -gebrauch sollten deshalb beachtet werden:

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Zeichenarten verwendet werden.
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.
- Wenn für das Passwort nur Ziffern zur Verfügung stehen, sollte es mindestens 6 Zeichen lang sein **und** das Authentisierungssystem sollte den Zugang nach wenigen Fehlversuchen sperren (für eine bestimmte Zeitspanne oder dauerhaft).
- Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner wirklich überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Passwörter müssen geheim gehalten werden und sollten nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte allenfalls für die Hinterlegung schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muss. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren (siehe M 2.22 *Hinterlegen des Passwortes*).
- Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.

- Da Menschen sich lange und komplizierte Passwörter in der Regel nicht merken können und zudem für jede Anwendung ein anderes Passwort zu verwenden ist, kann in der Praxis die Nutzung eines Passwort-Speicher-Tools geprüft werden. Überlegungen hierzu enthält M 4.306 *Umgang mit Passwort-Speicher-Tools*.

Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern (z. B. "BBBBBBBB", "123456", Namen, Geburtsdaten) sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Die Benutzer sollten bei der Änderung von Passwörtern durch eine Entropie-Messung (Anzeige der Passwort-Güte) unterstützt werden.
- Für die Erstanmeldung neuer Benutzer sollten Initial-Passwörter vergeben werden, die nach einmaligem Gebrauch gewechselt werden müssen.
- In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern (siehe M 5.34 *Einsatz von Einmalpasswörtern*).
- Erfolglose Anmeldeversuche sollten mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt werden. Insbesondere darf bei erfolglosen Anmeldeversuchen nicht erkennbar sein, ob der eingegebene Benutzername oder das eingegebene Passwort (oder beides) falsch sind. Nach fünf aufeinanderfolgenden fehlerhaften Passworteingaben für dieselbe Kennung sollte das Authentisierungssystem den Zugang hierfür sperren (für eine bestimmte Zeitspanne oder dauerhaft). Die Sperrung einer Kennung darf bei nachfolgenden erfolglosen Anmeldeversuchen ebenfalls nicht erkennbar sein, sondern sollte dem jeweiligen Benutzer auf einem separaten Weg mitgeteilt werden.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter selbst im Intranet nicht unverschlüsselt übertragen werden. Erfolgt die Authentisierung über ein ungesichertes Netz hinweg, so dürfen Passwörter keinesfalls unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Die Passwörter müssen im System zugriffssicher gespeichert werden, z. B. mittels Einweg-Verschlüsselung (Hashfunktionen).
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passworthistorie).

Prüffragen:

- Gibt es eine verbindliche Regelung für den Passwortgebrauch?
- Sind die Benutzer angewiesen, Passwörter mit ausreichender Komplexität zu verwenden, die dem Schutzbedarf angemessen sind?
- Sind die Benutzer angewiesen, ihr Passwort geheim zu halten?
- Wird getestet, wie viele Stellen des Passwortes tatsächlich vom IT-System überprüft werden?
- Werden Passwörter in regelmäßigen Abständen gewechselt?
- Werden Passwörter sofort gewechselt, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht?
- Bei erfolglosen Anmeldeversuchen: Wird nicht bekannt gegeben, ob Benutzername und/oder Passwort falsch waren?

# M 2.12 Betreuung und Beratung von IT-Benutzern

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Der Einsatz von IT-Systemen erfordert eine umfassende Schulung der IT-Benutzer. Neben der Schulung, die die IT-Benutzer in die Lage versetzt, die eingesetzte Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-Benutzer für die im laufenden Betrieb auftretenden Probleme. Diese Probleme können aus Hardware-Defekten oder fehlerhafter Software-Installation resultieren, aber auch aus Bedienungsfehlern. Alle Benutzer sollten die Stelle bzw. Personen kennen, an die sie sich bei IT-Problemfällen wenden können. Der IT-Support sollte auch Hinweise auf potenzielle Sicherheitsprobleme aufnehmen und an die Zuständigen, z. B. das Sicherheitsmanagement-Team, weiterleiten.

In größeren Institutionen kann es daher sinnvoll sein, eine zentrale Stelle mit der Betreuung der IT-Benutzer zu beauftragen und diese allen Mitarbeitern bekannt zu geben. Diese Notwendigkeit kann sich insbesondere bei einer hohen Zahl dezentraler Systeme wie PCs als praktikabel erweisen. Dabei ist sicherzustellen, dass der IT-Support während der Arbeitszeiten der Benutzer zur Verfügung steht, damit IT-Probleme zeitnah gelöst werden können. Da bei gleitender Arbeitszeit Benutzer zu unregelmäßigen Zeiten an ihrem Arbeitsplatz sein können, sollten Service-Zeiten festgelegt werden, die den Anforderungen der jeweiligen Institution gerecht werden und die sich an den Zeiten orientieren sollten, zu denen der Großteil der Mitarbeiter arbeiten.

Für die Betreuung von IT-Benutzern sollte eine telefonische Hotline eingerichtet werden, da viele Probleme telefonisch schneller als auf schriftlichem Weg gelöst werden können. Eine Unterstützung nur per E-Mail ist nicht ausreichend, da beim Ausfall eines IT-Systems, des Netzes oder der beteiligten Server das Problem unter Umständen auf diese Weise nicht geschildert werden kann.

Prüffragen:

- Wird sichergestellt, dass der IT-Support den Benutzern während der Arbeitszeiten zur Verfügung steht?
- Bei Gleitzeit innerhalb der Organisation: Gibt es für die Organisation geeignete Support-Zeiten auch bei Gleitzeit?
- Kennen die Benutzer ihre Ansprechpartner für IT-Problemfälle?
- Ist eine Erreichbarkeit der Betreuung auch ohne Funktion des IT-Systems gewährleistet?

# M 2.13 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Mitarbeiter

Betriebsmittel oder Sachmittel (z. B. Druckerpapier, Disketten, Streamertapes, Magnetbänder, Festplatten, CD-ROM, DVDs, USB-Sticks, Flash-Speicher oder -karten, aber auch spezielle Tonerkassetten, Kohlepapier oder Carbonbänder) werden irgendwann nicht mehr benötigt oder müssen aufgrund von Defekten ausgesondert werden. Wenn sie schützenswerte Daten enthalten, müssen sie so entsorgt werden, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern sollten die Daten physikalisch gelöscht werden. Nicht funktionierende oder nur einmal beschreibbare Datenträger wie Akten oder CD-ROMs und auch DVDs müssen mechanisch zerstört werden (siehe B 1.15 *Löschen und Vernichten von Daten*).

Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Sicherheitsrichtlinie geregelt werden. In der Institution müssen die dafür benötigten Entsorgungseinrichtungen wie Aktenvernichter vorhanden sein.

Wird schutzbedürftiges Material vor der Entsorgung gesammelt, so ist die Sammlung unter Verschluss zu halten und vor unberechtigtem Zugriff zu schützen.

Soweit im Unternehmen bzw. in der Behörde keine umweltgerechte und sichere Entsorgung durchgeführt werden kann, sind damit beauftragte Unternehmen auf die Einhaltung erforderlicher Sicherheitsmaßnahmen zu verpflichten. Ein Mustervertrag findet sich unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten. Es sollte regelmäßig geprüft werden, ob der Entsorgungsvorgang verlässlich ist.

Prüffragen:

- Ist sichergestellt, dass alle schutzbedürftigen Materialien ordnungsgemäß entsorgt werden?
- Ist die Entsorgung von schutzbedürftigen Materialien geregelt?
- Sind zur Entsorgung von schutzbedürftigem Material geeignete Entsorgungseinrichtungen wie z. B. Aktenvernichter vorhanden?
- Spätere Entsorgung: Wird zur Entsorgung gesammeltes schutzbedürftiges Material vor unberechtigtem Zugriff geschützt?
- Werden die beauftragten Unternehmen für die Entsorgung von schützenswerten Betriebsmitteln regelmäßig daraufhin überprüft, ob der Entsorgungsvorgang verlässlich ist?

# M 2.14 Schlüsselverwaltung

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter Organisation
**Verantwortlich für Umsetzung:** Leiter Haustechnik

Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten. Zu beachten bleibt:

- Ist eine Schließanlage vorhanden, sind für schutzbedürftige Bereiche eigene Schließgruppen zu bilden. Je nach Anforderungen sind einzelne Räume aus der Schließgruppe herauszunehmen und mit Einzelschließung zu versehen.
- Nicht ausgegebene Schlüssel und die Reserveschlüssel sind gegen unbefugten Zugriff geschützt aufzubewahren.
- Die Ausgabe der Schlüssel erfolgt nur in begründeten und nachvollziehbaren Fällen an hierfür autorisierte Personen gegen Quittung und ist zu dokumentieren. Auch im Vertretungsfall darf ein Schlüssel nicht einfach weitergegeben werden, sondern hat über die Schlüsselausgabe zu erfolgen. Nur über diesen Umweg kann eine lückenlose Dokumentation als Nachweis über den Verbleib des Schlüssels erfolgen.
- Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist (Meldung, Ersatz, Kostenerstattung, unter Umständen Regressfrage wegen mangelnder Sorgfaltspflicht prüfen), Austausch des Schlosses, Austausch von Schließgruppen etc.).
- Bei Zuständigkeitsänderungen von Mitarbeitern sind deren Schließberechtigungen zu prüfen und nicht mehr benötigte Schlüssel einzuziehen.
- Beim Ausscheiden von Mitarbeitern sind alle Schlüssel einzuziehen (Aufnahme der Schlüsselverwaltung in den Laufzettel der noch vor dem Ausscheiden zu erledigenden Stationen).
- Schlösser und Schlüssel zu besonders schutzbedürftigen Bereichen (zu denen nur sehr wenige Schlüssel ausgegeben werden sollten) können bei Bedarf auch ohne vorherige Ankündigung im Verdachtsfall getauscht werden, um so illegal nachgefertigten Schlüsseln die Funktion zu nehmen.

Prüffragen:

- Werden nicht ausgegebene Schlüssel sicher aufbewahrt?
- Ist jede Schlüsselausgabe dokumentiert?

# M 2.15 Brandschutzbegehungen

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter

Bei der Errichtung und der Nutzung von Gebäuden sind alle geltenden Brandschutzvorschriften zu beachten. Diese werden durch DIN- und VDE-Normen festgeschrieben und durch Auflagen der Bauaufsicht ergänzt (siehe auch M 1.6 *Einhaltung von Brandschutzvorschriften*).

Die Erfahrungen zeigen, dass nach Nutzungsbeginn im täglichen Betrieb diese Regelungen immer nachlässiger gehandhabt werden - bis hin zur völligen Ignoranz. Einige **Beispiele:**

- Fluchtwege werden blockiert, z. B. durch Möbel und Papiervorräte.
- Brandabschnittstüren bzw. Rauchschutztüren werden durch Keile offen gehalten.
- Zulässige Brandlasten werden durch anwachsende Kabelmengen oder geänderte Nutzungen überschritten.
- Brandabschottungen werden bei Arbeiten geöffnet und/oder beschädigt und nicht ordnungsgemäß wiederhergerichtet.
- Rauchmelder in der Nähe von "Raucherecken" werden bewusst außer Funktion gesetzt.

Brandschutzbegehungen sollten ein- bis zweimal im Jahr angekündigt oder unangekündigt erfolgen.

Da die Handlungsweise der Mitarbeiter in der Regel nicht vom böswilligen Vorsatz, sondern von der betrieblichen Notwendigkeit oder Bequemlichkeit bestimmt wird, kann es nicht Sinn einer Brandschutzbegehung sein, Täter zu finden und zu bestrafen. Vielmehr sollten die vorgefundenen Mängel dazu Anlass geben, die Zustände und auch deren Ursachen unverzüglich zu beheben.

Prüffragen:

- Werden regelmäßig Brandschutzbegehungen durchgeführt?
- Werden bei Brandschutzbegehungen festgestellte Mängel unverzüglich behoben?

# M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen

**Verantwortlich für Initiierung:** Leiter Organisation
**Verantwortlich für Umsetzung:** Mitarbeiter

Personen, die nicht der Institution angehören, wie Besucher, Handwerker, Wartungs- und Reinigungspersonal sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch M 2.6 *Vergabe von Zutrittsberechtigungen*). Alle Mitarbeiter sollten darauf hingewiesen werden, dass sie Betriebsfremde, die sie unbeaufsichtigt innerhalb der Behörde oder des Unternehmens antreffen, von diesem Moment an unter ihre Obhut nehmen müssen. Dies dient nicht nur der Sicherheit aller, sondern ist auch ein positiver Serviceaspekt für Betriebsfremde.

Wird es erforderlich, einen Externen allein im Büro zurückzulassen, sollte ein Kollegen ins Zimmer oder der Besucher zu einem Kollegen gebeten werden.

Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Zugriffssperre aktiviert), siehe auch M 2.37 *Der aufgeräumte Arbeitsplatz*.

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und Besucher sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugriffsschutz gesichert ist.

Die Notwendigkeit dieser Maßnahme ist den Mitarbeitern zu erläutern und in einer Sicherheitsrichtlinie festzuhalten. Eine Dokumentation über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

Prüffragen:

- Werden die Mitarbeiter dazu angehalten, betriebsfremde Personen nicht unbeaufsichtigt zu lassen?

# M 2.17 Zutrittsregelung und -kontrolle

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter Organisation
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Mitarbeiter, Planer

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*). Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu aufwendigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloss eine Zutrittsregelung darstellt. Für eine Zutrittsregelung und -kontrolle ist es erforderlich, dass

- der von der Regelung betroffene Bereich eindeutig bestimmt wird,
- die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert wird; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können,
- der Zutritt anderer Personen (Besucher) erst nach vorheriger Prüfung der Notwendigkeit erfolgt,
- erteilte Zutrittsberechtigungen dokumentiert werden.

Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung bzw. Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen sollte nach dem Grundsatz erfolgen, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik. Beispiele hierfür sind:

- Information und Sensibilisierung der Berechtigten,
- Bekanntgabe von Berechtigungsänderungen,
- sichtbares Tragen von Hausausweisen, ergänzt durch Vergabe von Besucherausweisen,
- Begleitung von Besuchern,
- Verhaltensregelungen bei erkannter Berechtigungsüberschreitung und
- Einschränkung des ungehinderten Zutritts für nicht Zutrittsberechtigte (z. B. Tür mit Blindknauf, Schloss für Berechtigte mit Schlüssel, Klingel für Besucher).

Bei der Zutrittskontrolle werden verschiedene bauliche, organisatorische und personelle Maßnahmen benötigt. Deren Zusammenwirken sollte in einem Zutrittskontrollkonzept geregelt sein, das die generellen Richtlinien für den Perimeter-, Gebäude- und Geräteschutz festlegt. Dazu gehören:

- Festlegung der Sicherheitszonen
  Zu schützende Bereiche können etwa Grundstücke, Gebäude, Serverräume, Räume mit Peripheriegeräten, Archive, Kommunikationseinrichtungen und die Haustechnik sein. Da diese Bereiche häufig sehr unterschiedliche Sicherheitsanforderungen aufweisen, kann es sinnvoll sein, diese in verschiedene Sicherheitszonen aufzuteilen (siehe M 1.79 *Bildung von Sicherheitszonen*).
- Vergabe von Zutrittsberechtigungen (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*)
- Bestimmung eines Verantwortlichen für Zutrittskontrolle
  Dieser vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den in der Sicherheitspolitik festgelegten Grundsätzen.
- Definition von Zeitabhängigkeiten
  Es ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit, Zutritt einmal täglich oder befristeter Zutritt bis zu einem fixierten Datum.
- Festlegung der Beweissicherung

Hier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden. Dabei bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre des Einzelnen.

- Behandlung von Ausnahmesituationen
  Auch in Ausnahmesituationen sollten keine Unbefugten das Gebäude oder die Liegenschaften betreten können. Oberste Priorität ist allerdings sicherzustellen, dass im Brandfall alle Personen schnellstmöglich die gefährdeten Zonen verlassen können.

Ergänzend kann der Einbau von Ausweislesern verschiedenster Qualitäten, von Schleusen und Vereinzelungseinrichtungen sinnvoll sein. Zur Schlüsselverwaltung siehe M 2.14 *Schlüsselverwaltung*.

Um ein umfassenderes Konzept umzusetzen, Flexibilität im Einsatz zu erhalten und um Transparenz und Nachprüfbarkeit sicherzustellen, ist der Einsatz eines IT-gestützten Systems zum Berechtigungsmanagement zu empfehlen (siehe M 1.80 *Zutrittskontrollsystem und Berechtigungsmanagement*).

Die Terminals zur Zutrittskontrolle müssen gegen Manipulationen geschützt werden. Dafür müssen diese so angebracht werden, dass Vertraulichkeit bei der Eingabe von Daten gewährleistet ist. Außerdem sollten alle zur Dateneingabe erforderlichen Einheiten in einem Gerät kombiniert sein, also beispielsweise eine Tastatur zur PIN-Eingabe.

Befinden sich nicht alle Einheiten in einem Gerät, muss die Datenübertragung zwischen diesen verschlüsselt erfolgen. Werden also z. B. berührungslose Ausweisleser eingesetzt, so muss die Datenübertragung zwischen Karte und Leser verschlüsselt erfolgen.

Im Betrieb muss die Wirksamkeit aller technischen und organisatorischen Maßnahmen stetig kontrolliert werden. Es empfiehlt sich, vor allem an bekannten problematischen Stelle regelmäßig zu überprüfen, ob keine Möglichkeiten entstanden sind, um die Zutrittskontrolle zu umgehen, z. B. in Liefer- oder Raucherzonen.

Prüffragen:

- Wird der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen geregelt und kontrolliert?
- Existiert ein Konzept für die Zutrittskontrolle?
- Werden die Zutrittskontroll-Maßnahmen regelmäßig auf ihre Wirksamkeit überprüft?

# M 2.18 Kontrollgänge

**Verantwortlich für Initiierung:** Haustechnik, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Haustechnik, IT-Sicherheitsbeauftragter

Eine Maßnahme kann nur so gut wirken, wie sie auch tatsächlich umgesetzt wird. Kontrollgänge bieten das einfachste Mittel, die Umsetzung von Maßnahmen und die Einhaltung von Auflagen und Anweisungen zu überprüfen.

Die Kontrollgänge sollen nicht dem Finden von Tätern dienen, um diese zu bestrafen. Sinn der Kontrollen soll es in erster Linie sein, erkannte Nachlässigkeiten möglichst sofort zu beheben (Fenster zu schließen, Unterlagen in Aufbewahrung zu nehmen etc.). In zweiter Linie können Ursachen für diese Nachlässigkeiten erkannt und eventuell in der Zukunft vermieden werden.

Die Kontrollgänge sollten durchaus auch während der Dienstzeit erfolgen und zur Information der Mitarbeiter über das Wie und Warum von Regelungen genutzt werden. So werden sie von allen Beteiligten eher als Hilfe denn als Gängelung angesehen.

Prüffragen:

- Werden Kontrollgänge durchgeführt, um die Umsetzung von Maßnahmen zu überprüfen?

# M 2.19 Neutrale Dokumentation in den Verteilern

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Planer

In jedem Verteiler sollte sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation ist möglichst neutral zu halten. Nur bestehende und genutzte Verbindungen sind darin aufzuführen. Es sollten, soweit nicht ausdrücklich vorgeschrieben (z. B. für Brandmeldeleitungen), keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Leitungs-, Verteiler-, und Raumnummern reichen in vielen Fällen aus. Alle weitergehenden Informationen sind in einer Revisions-Dokumentation aufzuführen.

Prüffragen:

- Befindet sich in jedem Verteiler eine Dokumentation über den aktuellen Stand der Rangierungen und Leitungsbelegungen?
- Wird darauf geachtet, die Dokumentation in den Verteilern möglichst neutral zu halten und weitergehende Informationen (Nutzungsart der Leitungen) in Revisionsdokumenten zu beschreiben?

# M 2.20 Kontrolle bestehender Verbindungen

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Planer

Alle Verteiler und Zugdosen der Verkabelung sind regelmäßig einer (zumindest stichprobenartigen) Sichtprüfung zu unterziehen. Dabei ist auf folgende Punkte zu achten:

- Spuren von gewaltsamen Öffnungsversuchen an verschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltungen und Rangierungen mit der Dokumentation,
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen und
- unzulässige Einbauten oder Veränderungen.

Neben der reinen Sichtkontrolle kann zusätzlich eine funktionale Kontrolle durchgeführt werden. Dabei werden bestehende Verbindungen auf ihre Notwendigkeit und die Einhaltung technischer Werte hin geprüft. Bei Verbindungen, die nicht in zutrittsgeschützten Bereichen sind, ist in zwei Fällen diese Prüfung anzuraten:

- Bei Verbindungen, die sehr selten genutzt und bei denen Manipulationen nicht sofort erkannt werden.
- Bei Verbindungen, auf denen häufig und regelmäßig besonders schützenswerte Informationen übertragen werden.

Alle Unregelmäßigkeiten, die bei Sichtkontrollen oder funktionalen Kontrollen festgestellt werden, müssen unverzüglich dokumentiert und den zuständigen Organisationseinheiten gemeldet werden, damit zeitnah die notwendigen weiteren Schritte eingeleitet werden können. Wichtig ist außerdem, dass die festgestellten Unregelmäßigkeiten nicht nur beseitigt, sondern dass auch deren Ursachen ermittelt werden.

Prüffragen:

- Werden Verteiler und Zugdosen der Verkabelung regelmäßig kontrolliert?
- Werden bei der Kontrolle der Verkabelung festgestellte Unregelmäßigkeiten dokumentiert, behoben und ihre Ursache ermittelt?

# M 2.21 Rauchverbot

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Mitarbeiter

In den meisten Räumlichkeiten von Unternehmen und Behörden ist Rauchen generell verboten, meistens sogar aufgrund gesetzlicher Vorgaben. So verpflichtet in Deutschland die Arbeitsstättenverordnung die meisten Institutionen, den Nichtraucherschutz am Arbeitsplatz zu gewährleisten. Auch in Gebäuden, in denen kein umfassendes Rauchverbot herrscht, muss sichergestellt werden, dass in Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen zu hohen Schäden führen können, ein Rauchverbot erlassen wurde. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

Dabei muss sichergestellt werden, dass nicht als Folge eines Rauchverbots im Gebäude der Zutrittsschutz geschwächt wird. Es ist häufig zu beobachten, dass Außentüren in schwer einsehbaren Bereichen ständig offen stehen, weil der Nahbereich der Tür die Raucherzone bildet und die Tür aus Bequemlichkeit während der Arbeitszeiten nie geschlossen wird.

Prüffragen:

- Wird das Rauchverbot in schutzbedürftigen Räumen eingehalten?
- Bleibt der Zutrittsschutz bei Einrichtung oder Duldung von Raucherzonen erhalten?

# M 2.22 Hinterlegen des Passwortes

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Ist der Zugriff auf ein IT-System durch ein Passwort geschützt, so müssen Vorkehrungen getroffen werden, die bei Abwesenheit eines Mitarbeiters, z. B. im Urlaubs- oder Krankheitsfall, seinem Vertreter den Zugriff auf das IT-System ermöglichen.

Hierfür gibt es verschiedene Möglichkeiten, die von den benutzten IT-Systemen bzw. IT-Anwendungen und von den Sicherheitsrichtlinien der jeweiligen Organisation abhängen. So kann z. B. das Passwort an einer geeigneten Stelle hinterlegt werden. Bei typischen Mehrbenutzersystemen kann auch der Administrator die benötigten Benutzerrechte freigeben oder das Passwort auf einen neuen Wert setzen. Bei vielen IT-Systemen bzw. IT-Anwendungen können aber Gruppen eingerichtet werden, so dass die eingetragenen Vertreter im Abwesenheitsfall Zugriff auf das System haben.

Alle genannten Lösungen haben verschiedene Vor-, aber auch Nachteile, so dass genau abgewogen werden muss, welche Lösung die in der jeweiligen Situation am geeignetsten ist.

Die folgenden Beispiele sollen dies aufzeigen:

Die Buchhalterin Frau Müller arbeitet an einem Windows-PC, der als Client in einem LAN angeschlossen ist. Um für den Vertretungsfall alle potentiellen Problembereiche abzudecken, wurden ihre Tätigkeitsbereiche mit ihr durchgegangen und Lösungen entwickelt.

- Sie ist für die Bearbeitung aller Vorgänge mit den Partnerfirmen A-K zuständig. Die zu bearbeitenden Daten befinden sich in einer Datenbank auf dem Server PF1. Im Vertretungsfall können ihre Kollegen Schmidt und Eifrig unter ihren eigenen Benutzer-Kennungen diese Daten bearbeiten, da sie die entsprechenden Berechtigungen in der Datenbank haben.
- Einige von ihr erstellte Dokumente befinden sich auf ihrem PC. Es wurde eine Vereinbarung getroffen, dass sie alle für den Betrieb wichtigen Dateien in Projektverzeichnisse auf den Server einstellt. Falls im Vertretungsfall ein Zugriff notwendig wird, kann der Administrator diesen ermöglichen. Dies muss schriftlich dokumentiert werden. Frau Müller erhält darüber anschließend eine E-Mail.
- Frau Müller benutzt für die Kundenverwaltung der betreuten Firmen eine alte, aber stabile IT-Anwendung. Da diese es technisch nicht zulässt, dass Vertretungsregelungen auf dem Weg von Zugriffsberechtigungen eingeführt werden, erhält der Vertreter Herr Schmidt das Passwort für ihren Zugang. Dadurch kann er bei ihrer Abwesenheit anfallende Änderungen einpflegen.
- Einige finanzrelevante Vorgänge müssen mit einer digitalen Signatur autorisiert werden. Allen Mitarbeitern sind dafür persönliche kryptographische Schlüssel auf Chipkarten ausgehändigt worden, die nicht weitergegeben werden dürfen. Im Vertretungsfall unterzeichnet ihr Vertreter mit seiner digitalen Signatur.

Eine Hinterlegung von Passwörtern ist immer mit einem großen organisatorischen Aufwand verbunden: Bei der Passwort-Hinterlegung sind die benötigten aktuellen Passwörter durch jeden Mitarbeiter an einer geeigneten Stelle (z. B. im Sekretariat in einem Safe in einem geschlossenen Umschlag) zu hinterlegen. Bei jeder Änderung eines der Passwörter ist dieses zu aktualisie-

ren. Es darf kein Passwort dabei vergessen werden. (Manchmal werden für den Zugriff auf eine Anwendung auf einem Rechner bis zu fünf verschiedene Passwörter benötigt.) Es darf nicht möglich sein, dass Unbefugte auf die hinterlegten Passwörter Zugriff nehmen. Wird es notwendig, eines der hinterlegten Passwörter zu nutzen, so sollte dies nach dem Vier-Augen-Prinzip, d. h. von zwei Personen gleichzeitig, geschehen. Jeder Zugriff darauf muss dokumentiert werden.

Passwörter sollten möglichst nur dann hinterlegt werden, wenn es keine andere (technische) Lösung gibt. Dabei ist immer zu beachten, dass die Hinterlegung von Passwörtern einen falschen Signalcharakter für den sicheren Umgang mit Passwörtern vermittelt. Passwörter dürfen nicht unter Tastaturen oder ähnlichen Orten "hinterlegt" und auch nicht unter Kollegen weitergegeben werden, nur weil es einfacher ist, als den Administrator um die Vergabe einer notwendigen Zugriffsberechtigung zu bitten.

Passwörter sollten aber immer dann sicher hinterlegt werden, wenn diese die einzige Möglichkeit sind, auf das IT-System oder die IT-Anwendung Zugriff zu nehmen. Dies ist z. B. meistens bei Administrator-Zugängen oder Einzelplatz-Systemen der Fall.

Es sollte daher eine Regelung geben, in der beschrieben ist, welche Art von Passwörtern hinterlegt werden sollten und welche Rahmenbedingungen dafür geschaffen werden müssen.

Bei einem Telearbeiter ist sicherzustellen, dass dessen Passwörter für die IT-Systeme am häuslichen Arbeitsplatz auch in der Institution hinterlegt werden, damit im Notfall sein Vertreter auf die im Telearbeitsrechner gespeicherten Daten zugreifen kann.

Bei allen von Administratoren betreuten Systemen, insbesondere bei vernetzten Systemen, ist durch regelmäßige Überprüfung sicherzustellen, dass das aktuelle Systemadministrator-Passwort hinterlegt ist.

Prüffragen:

- Ist sichergestellt, dass benannte Vertreter auf die benötigten Anwendungen und IT-Systeme zugreifen können?
- Ist geregelt, welche Passwörter hinterlegt werden müssen und welche Sicherheitsvorkehrungen dabei einzuhalten sind?
- Werden Passwörter nur dann hinterlegt, wenn es keine andere zweckmäßige Vorgehensweise gibt, die notwendigen Zugriffsmöglichkeiten zu schaffen?
- Wenn Passwörter hinterlegt werden: Werden die Passwörter an einem sicheren Ort hinterlegt?
- Wenn Passwörter hinterlegt werden: Werden die hinterlegten Passwörter auf dem aktuellen Stand gehalten?
- Wenn Passwörter hinterlegt werden: Wird der Zugriff auf hinterlegte Passwörter dokumentiert?

# M 2.23 Herausgabe einer PC-Richtlinie

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Leiter IT

Um einen sicheren und ordnungsgemäßen Einsatz von Informationstechnik in größeren Unternehmen bzw. Behörden zu fördern, sollte eine Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie ist allen Benutzern zur Kenntnis zu geben, beispielsweise in elektronischer Form auf einem Intranet-Server. Jeder neue Benutzer muss die Kenntnisnahme der Richtlinie bestätigen, bevor er die Informationstechnik nutzen darf. Nach größeren Änderungen an der Richtlinie oder nach spätestens 2 Jahren ist eine erneute Bestätigung erforderlich.

Im Folgenden soll grob umrissen werden, welche Inhalte für eine solche Richtlinie sinnvoll sind:

### Zielsetzung und Begriffsdefinitionen

Der erste Teil der Richtlinie dient dazu, die Anwender für Informationssicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert, wie z. B. PC, Server, Netz, Anwender, Benutzer, schutzbedürftige Objekte.

### Geltungsbereich

In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die Richtlinie gilt.

### Rechtsvorschriften und interne Regelungen

Hier wird im Überblick dargestellt, welche wesentlichen Rechtsvorschriften, z. B. das Bundesdatenschutzgesetz und das Urheberrechtsgesetz, einzuhalten sind. Anhand von Beispielen sollte deutlich gemacht werden, welche Auswirkungen dies auf die Nutzung der Informationstechnik im jeweiligen Umfeld hat. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.

### Verantwortungsverteilung

In diesem Teil wird definiert, welcher Funktionsträger im Zusammenhang mit dem IT-Einsatz welche Verantwortung tragen muss. Dabei sind insbesondere die Rollen Benutzer, Vorgesetzte, Administrator, Revisor, Datenschutzbeauftragter und Sicherheitsmanagement-Team zu unterscheiden.

### Ansprechpartner

Die Richtlinie sollte Ansprechpartner und Kontaktinformationen (Telefon, E-Mail etc.) für die Benutzer zu Fragen der Informationssicherheit enthalten oder aufzeigen, wo diese Informationen gefunden werden können. Dabei sollte beachtet werden, dass es häufig zu Verwirrung führt, wenn den Benutzern zu viele unterschiedliche Ansprechpartner genannt werden. Besser ist es meist, nur wenige unterschiedliche Ansprechpartner zu benennen, die dann bei Bedarf die Benutzer an die richtige Stelle verweisen (Help-Desk-Konzept).

**Umzusetzende und einzuhaltende Sicherheitsmaßnahmen**

Im letzten Teil der Richtlinie für die IT-Nutzung ist festzulegen, welche Sicherheitsmaßnahmen vom Benutzer einzuhalten bzw. umzusetzen sind. Dies kann je nach Schutzbedarf auch über die IT-Grundschutz-Maßnahmen hinausgehen. Typische Beispiele für Sicherheitsmaßnahmen am Arbeitsplatz sind das sichere An- und Abmelden am PC, der ordnungsgemäße Umgang mit Passwörtern und Verhaltensregeln bei der Nutzung des Internets.

Sind Telearbeiter im Unternehmen bzw. in der Behörde beschäftigt, sollte die Richtlinie um die Telearbeitsplatz-spezifischen Regelungen ergänzt werden.

Prüffragen:

- Wird die PC-Richtlinie regelmäßig, spätestens nach 2 Jahren, aktualisiert?
- Ist sichergestellt, dass die PC-Richtlinie allen relevanten Parteien zur Verfügung steht?
- Ist die Kenntnisnahme der PC-Richtlinie durch den Benutzer vor erstmaliger Nutzung eines organisationseigenen IT-Systems verpflichtend?
- Bei Nutzung von Telearbeit: Enthält die PC-Richtlinie gesonderte Telearbeitsplatz-spezifischen Regelungen?

# M 2.24 Einführung eines IT-Passes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Der erste Schritt bei der Erstellung eines Sicherheitskonzeptes besteht darin, sich einen Überblick über die vorhandenen Systeme, Anwendungen und Daten zu verschaffen. Für eine kleine Institution ist es im Allgemeinen effektiv, anhand der vorhandenen IT-Systeme vorzugehen. Daher sollte eine entsprechende Übersicht vorhanden sein. Ein Möglichkeit ist es, für jedes IT-System einen IT-Pass auszufüllen, der die wichtigsten Informationen über das IT-System zusammenfasst.

Der IT-Pass soll den IT-Verantwortlichen einen Überblick über die vorhandenen IT-Systeme in der Institution verschaffen und ein schnelles effektives Reagieren bei Problemen ermöglichen. Der IT-Pass ist immer dann sinnvoll einzusetzen, wenn es sich um eine sehr kleine Institution mit wenigen IT-Systemen handelt, bei der sich umfangreiche Strukturanalysen nicht lohnen. Hierzu sollten zunächst für jedes IT-System folgende Informationen erfasst werden:

- Bezeichnung des IT-Systems (Inventarisierungsnummer)
- Ansprechpartner für Problemfälle, z. B. Service- und Hotline-Nummern für den Ausfall und die Wartung des Systems
- Informationen zum Betriebssystem
- Informationen zum Virenscanner
- Standort des Systems (Raum)
- Übersicht über die wichtigsten Informationen und Anwendungen, die auf dem System gespeichert sind bzw. laufen
- Schutzbedarf abhängig von Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit
- Informationen zur Systeminstallation und zur Systemkonfiguration
- zur Verfügung stehendes Zubehör
- durchgeführte Wartungen und Reparaturen
- Art der durchgeführten Datensicherungen

Hinweis: Die direkt an Endgeräte angeschlossenen Drucker werden nicht als eigenständige Komponenten, sondern als Teil des jeweiligen Endgeräts erfasst. In den IT-Pässen können sie unter Peripherie oder Hardware aufgeführt werden.

Gleichartige IT-Systeme wie Anwender-PCs können auch in Gruppen zusammengefasst werden. Für Mobiltelefone, PDAs oder ähnliche Geräte sollten ebenfalls zusammenfassend IT-Pässe erstellt werden, wobei die Felder des Passes entsprechend anzupassen sind.

Auch für Telefonanlagen und Anschlüsse an Datennetze sollten die wichtigsten Informationen in Form eines IT-Passes dokumentiert werden.

Um den Schutzbedarf eines IT-Systems zu dokumentieren, sollte der IT-Pass für jede wichtige Anwendung festhalten, ob dort z. B. personenbezogene Daten verarbeitet werden, und den Schutzbedarf abhängig von den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit festlegen.

Zusätzlich können die durchgeführten Sicherheitsmaßnahmen am IT-System dokumentiert werden, so dass z. B. im Schadensfall schnell reagiert werden kann.

Die IT-Pässe sollten entweder vom Sicherheitsmanagement oder vom Administrator geführt werden. Sie können auch durch Mitarbeiter ausgefüllt werden, müssen aber dann danach inhaltlich und auf Vollständigkeit geprüft werden. Die IT-Pässe sollten zentral gespeichert werden, aber möglichst auch lokal verfügbar sein. Da sich bei gleichartigen IT-Systemen wie PCs viele Antworten wiederholen, ist es hilfreich, die IT-Pässe elektronisch zu führen. Die IT-Pässe sollten zentral gespeichert werden, aber möglichst auch lokal verfügbar sein.

Bei Änderungen an einem IT-System sind die Einträge im IT-Pass sofort anzupassen, so dass die Dokumentation immer auf dem aktuellen Stand ist.

IT-Pässe erleichtern die Durchführung von Kontrolltätigkeiten entschieden, da die Dokumentation aller durchgeführten relevanten Änderungen und Sicherheitsmaßnahmen aus den IT-Pässen hervorgehen. Außerdem unterstützt das Führen solcher IT-Pässe die regelmäßige Pflege der IT und Sicherheitsmaßnahmen, beispielsweise in Bezug auf Datensicherungen. Dies dient somit auch der Notfallvorsorge.

Ein Muster eines solchen IT-Passes findet sich unter den Hilfsmitteln zum IT-Grundschutz auf dem BSI-Webserver im "IT-Grundschutzprofil für eine kleine Institution".

Prüffragen:

- Gibt es einen Überblick über die vorhandenen Systeme, Anwendungen und Daten in der Institution, z. B. in Form von IT-Pässen?

# M 2.25 Dokumentation der Systemkonfiguration

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Planung, Steuerung, Kontrolle und Notfallvorsorge des IT-Einsatzes basieren auf einer aktuellen Dokumentation des vorhandenen IT-Systems. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf des IT-Systems.

Bei einem Netzbetrieb ist die physikalische Netzstruktur (siehe M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*) und die logische Netzkonfiguration zu dokumentieren. Dazu gehören auch die Zugriffsrechte der einzelnen Benutzer (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*) und der Stand der Datensicherung. Weiterhin sind die eingesetzten Applikationen und deren Konfiguration sowie die Dateistrukturen auf allen IT-Systemen zu dokumentieren.

Dabei ist auf Aktualität und Verständlichkeit der Dokumentation zu achten, damit auch ein Vertreter die Administration jederzeit weiterführen kann. Die System-Dokumentation ist so aufzubewahren, dass sie im Bedarfsfall jederzeit verfügbar ist. Wenn sie in elektronischer Form geführt wird, sollte sie entweder regelmäßig ausgedruckt oder auf einem transportablen Datenträger gespeichert werden. Der Zugriff auf die Dokumentation ist auf die zuständigen Administratoren zu beschränken.

In der System-Dokumentation sollten alle Schritte dokumentiert sein, die beim Herauf- bzw. Herunterfahren von IT-Systemen zu beachten sind. Dies ist insbesondere bei vernetzten IT-Systemen wichtig. Hier muss z. B. häufig eine bestimmte Reihenfolge beim Mounten von Laufwerken oder Starten von Netzdiensten eingehalten werden.

Prüffragen:

- Ist die aktuelle Konfiguration der Anwendungen, Systeme und Netze dokumentiert?
- Umfasst die Systemdokumentation auch den aktuellen Stand der Datensicherung?
- Ist die Systemdokumentation so abgefasst, dass sie auch für Vertreter verständlich ist?

# M 2.26 Ernennung eines Administrators und eines Vertreters

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Personal

Um einen geordneten Betrieb von IT-Systemen zu ermöglichen, sind für alle IT-Systeme und Netze Administratoren zu bestimmen. Ihnen obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich sind sie für die Sicherheitsbelange aller von ihnen betreuten IT-Systeme zuständig.

Bei größeren Behörden bzw. Unternehmen mit einer Vielzahl verschiedener IT-Systeme und Teilnetzen muss außerdem sichergestellt sein, dass die Aufgaben zwischen den verschiedenen Administratoren so verteilt sind, dass es zu keinen Zuständigkeitsproblemen kommt, also weder zu Überschneidungen noch zu Lücken in der Aufgabenverteilung. Darüber hinaus sollte die Kommunikation zwischen den verschiedenen Administratoren möglichst reibungslos ablaufen. Hierzu können z. B. regelmäßige Administratoren-Treffen durchgeführt werden, bei denen typische Probleme und Lösungsmöglichkeiten bei der täglichen Arbeit thematisiert werden.

Beim Einsatz von Protokollierung sollte auf die Rollentrennung von Administration und Revision geachtet werden. Hier ist zu überprüfen, inwieweit die IT-Systeme dies unterstützen.

Um bei Verhinderung eines Administrators die Funktionen weiter aufrechtzuerhalten, ist ein Vertreter zu benennen. Hierbei ist darauf zu achten, dass dieser eine eigene Administratorkennung erhält (siehe auch M 2.38 *Aufteilung der Administrationstätigkeiten*). Auf keinen Fall darf aus Bequemlichkeit im Vertretungsfall einfach das Passwort weitergegeben werden.

Für die Übernahme von Administrationsaufgaben muss gewährleistet sein, dass jedem Administrator und ebenso den Vertretern für eine sorgfältige Aufgabenerfüllung auch die hierfür erforderliche Zeit zur Verfügung steht. Hierbei muss auch berücksichtigt werden, dass Aus- und Fortbildungsmaßnahmen erforderlich sind.

Die spezifischen Administrationstätigkeiten beim Einsatz von z/OS-Systemen werden in M 2.295 *Systemverwaltung von z/OS-Systemen* erläutert.

Prüffragen:

- Wurden für alle IT-Systeme und Netze entsprechende Administratoren sowie deren Stellvertreter bestimmt?
- Wurde die Aufgabenteilung zwischen den einzelnen Administratoren so vorgenommen, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen?
- Haben die Administratoren und deren Vertreter ausreichend Zeit zur sorgfältigen Erfüllung ihrer Aufgaben?
- Bei Einsatz von Protokollierung: Wird die Rollentrennung von Administration und Revision - soweit technisch möglich - berücksichtigt?
- Haben alle Administratoren und deren Vertreter ausreichend Möglichkeiten zur Fortbildung?

- Hat jeder Administrator und jeder Vertreter eines Administrators eine eigene, eindeutige Administratorkennung?

# M 2.27 Wartung einer TK-Anlage

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In einer TK-Anlage gibt es eine Wartungseinheit, mit der die TK-Anlage konfiguriert und administriert werden kann. Bei älteren Anlagen kann das eine spezielle Hardware sein, bei neueren Anlagen ist es meist eine Steuerungssoftware. Von außen kann auf diese Einheit je nach TK-Anlage mit unterschiedlichen Mitteln zugegriffen werden, beispielsweise:

- über ein Systemtelefon, also ein Endgerät mit erweiterter Funktionalität gegenüber normalen Endgeräten,
- über einen lokal an die Telefonanlage angeschlossenen Computer (z. B. über RS232, USB, Ethernet),
- über einen PC im LAN, der spezielle Administrationssoftware installiert hat, falls die TK-Anlage auch an das LAN angeschlossen ist,
- über einen Browser eines PCs im LAN, falls die TK-Anlage auch an das LAN angeschlossen ist.

Bei einem IP-Anlagenanschluss, bei dem die TK-Anlage physisch bei einem externen Anbieter steht, wird die TK-Anlage in der Regel über einen Browser administriert.

Die Wartungseinheit sollte so konfiguriert werden, dass nur dedizierte Wartungsrechner zugreifen dürfen. Beispielsweise indem nur IT-Systeme mit fest zugeordneten IP-Adressen mit der Wartungseinheit kommunizieren können. Verbindungsversuche von anderen IT-Systemen sollten abgewiesen werden. Der Zutritt zu den Wartungsrechnern sollte ebenfalls beschränkt werden. Hierfür könnten sie beispielsweise in einem separaten Sicherheitsbereich aufgestellt werden, den unbefugte Personen nicht betreten können.

Generell sollte der Zugriff auf die Wartungseinheit nur nach einer erfolgreichen Authentisierung möglich sein. Wenn möglich, sollte die Datenverbindung zwischen den Geräten, die zur Wartung genutzt werden und der Wartungseinheit verschlüsselt sein, außer es handelt sich um eine ausschließlich für diesen Zweck genutzte Verbindung (wie ein serielles Kabel). Die Geräte, über die die TK-Anlage gewartet und konfiguriert wird, müssen mit Passwörtern oder PINs abgesichert werden. Hierfür ist auch die Maßnahme M 2.11 *Regelung des Passwortgebrauchs* zu beachten. Nicht nur interne, sondern auch externe Wartungsmitarbeiter müssen sich authentisieren.

Die Wartung einer TK-Anlage sollte von Mitarbeitern mit entsprechendem Wissen, beispielsweise geschulten Administratoren, durchgeführt werden. Fehlen den vorhandenen Mitarbeitern die notwendigen Kenntnisse, um die TK-Anlage optimal zu warten und zu administrieren, und können diese nicht zeitnah geschult werden, sollte überlegt werden, externe Experten zu beauftragen.

Unabhängig davon, von wem die TK-Anlage gewartet wird, muss auch die Maßnahme M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten* beachtet werden.

**Fernwartung**

Unter Umständen kann es erforderlich sein, dass TK-Anlagen von Dritten, wie beispielsweise externen Experten, konfiguriert und gewartet werden. Erfolgt die Administration über ein Datennetz, wird hierfür eine Kommunikationsver-

bindung zur TK-Anlage benötigt. Ist die TK-Anlage an das LAN des Standorts ("Hausnetz") angeschlossen, könnte ein Angreifer sowohl auf die TK-Anlage als auch auf das LAN zugreifen. Daher müssen die Zugänge abgesichert werden. Das kann wie folgt geschehen:

Sollen externe Experten für die Wartungs- und Reparaturarbeiten beauftragt werden, müssen entsprechende Regelungen getroffen werden. Hierzu gehört beispielsweise, wie externe Personen während ihrer Tätigkeit beaufsichtigt werden und wie mit Geräten umzugehen ist, die für eine Reparatur außer Haus gegeben werden. Weitere Informationen hierzu sind in M 1.1 *Einhaltung einschlägiger Normen und Vorschriften* zu finden. Generell können durch eine Fernwartung zahlreiche Sicherheitsprobleme auftreten. Um diese zu verringern, muss der Fernwartungszugriff geschützt werden. Mögliche Sicherheitsfunktionen hierfür sind in M 5.33 *Absicherung von Fernwartung* zu finden. Die Datenverbindung bei IP-basierten Zugängen über öffentliche Netz sollte z. B. mit Secure Shell (SSH) oder über ein Virtuelles Privates Netz (VPN) abgesichert und verschlüsselt werden.

Prüffragen:

- Sind die Wartungszugänge der TK-Anlage durch technische und organisatorische Maßnahmen vor unbefugter Benutzung geschützt?
- Können nur die Wartungsrechner mit der Wartungseinheit der TK-Anlage kommunizieren?
- Werden die Geräte zur Wartung und Konfiguration von TK-Anlagen mit Passwörtern bzw. PINs abgesichert?
- Ist die Datenverbindung bei IP-basierten Zugängen zur TK-Anlage verschlüsselt?

# M 2.28 Bereitstellung externer TK-Beratungskapazität

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, TK-Anlagen-Verantwortlicher

Um in schwierigen Fällen schnell auf fachkundige Hilfe zurückgreifen zu können, sollte schon beim Kauf bzw. der Miete einer TK-Anlage an die Bereitstellung entsprechender Beratungsdienstleistung gedacht werden. Wichtig hierbei ist, dass in einer Notfallsituation die Unterstützung schnell erfolgen kann, da der Ausfall einer TK-Anlage die Handlungsfähigkeit einer gesamten Institution erheblich beeinträchtigen und ggf. nur für kurze Zeit toleriert werden kann.

Prüffragen:

- Entsprechen die vereinbarten SLAs den Anforderungen der Organisation?
- Kann in Notfallsituationen auf externe Beratungskapazität für die TK-Anlage zurückgegriffen werden?

# M 2.29 Bedienungsanleitung der TK-Anlage für die Benutzer

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Dem Benutzer der TK-Anlage sind die notwendigen Unterlagen zur Bedienung seiner Endgeräte (z. B. Bedienungsanleitung für das Telefon) zur Verfügung zu stellen. Neben der normalen Bedienung seines Telefons sollte der Benutzer vor allem in der Lage sein, etwaige Warnanzeigen (LEDs oder Piktogramme im Display) und -töne zu interpretieren (siehe M 3.12 *Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne*).

Prüffragen:

- Haben die Benutzer alle notwendigen Unterlagen und Informationen zur Bedienung und Nutzung der Endgeräte?
- Existiert eine Regelung zur Sensibilisierung der Benutzer?

# M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Regelungen für die Einrichtung von Benutzern / Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs.

Es sollte ein Formblatt existieren, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen:

- Name, Vorname,
- Vorschlag für die Benutzer- bzw. Gruppenkennung, wenn diese nicht durch Konventionen vorgegeben sind,
- Organisationseinheit,
- Erreichbarkeit (z. B. Telefon, Raum),
- ggf. Projekt,
- ggf. Angaben über die geplante Tätigkeit im System und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit,
- ggf. Restriktionen auf Zeiten, Endgeräte, Plattenvolumen, Zugriffsberechtigungen (für bestimmte Verzeichnisse, Remote-Zugriffe, etc.), eingeschränkte Benutzerumgebung,
- ggf. Zustimmung von Vorgesetzten.

Falls Zugriffsberechtigungen vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden. Dieses kann auch in elektronischer Form erfolgen durch ein spezielles Login, dessen Name und Passwort den einzurichtenden Benutzern bekanntgegeben wird. Dort wird ein entsprechendes Programm durchlaufen, das mit einem Logout endet. Die erfassten Daten können zur Vorlage beim Vorgesetzten ausgedruckt werden. Ein Passwort, das einem neuen Benutzer für die erstmalige Systemnutzung mitgeteilt wird, muss danach gewechselt werden. Dies sollte vom System initiiert werden.

Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die systemspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten. Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppennamen festzulegen (z. B. Benutzer-ID = Kürzel Organisationseinheit || lfd. Nummer).

Die Zugriffsberechtigung für Dateien ist auf Benutzer bzw. Gruppen mit berechtigtem Interesse zu beschränken. Wenn mehrere Personen auf eine Datei zugreifen müssen, soll für diese eine Gruppe eingerichtet werden. In der Regel muss jedem Benutzer eine eigene Benutzer-Kennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten. Für jeden Benutzer muss ein eindeutiges Heimatverzeichnis angelegt werden.

Für die Einrichtungsarbeiten im System sollte eine administrative Rolle geschaffen werden: Die Einrichtung sollte mit Hilfe eines speziellen Logins, unter dem ein entsprechendes Programm oder Shellskript gestartet wird, erfolgen. Die zuständigen Administratoren können Benutzer bzw. Benutzergrup-

pen somit nur auf definierte Weise einrichten, und es ist nicht erforderlich, ihnen Rechte für andere Administrationsaufgaben zu geben.

Diese Maßnahme wird unter Unix ergänzt durch folgende Maßnahmen:

- M 4.13 *Sorgfältige Vergabe von IDs*
- M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*
- M 4.20 *Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen*

Diese Maßnahme wird unter z/OS ergänzt durch folgende Maßnahmen:

- M 2.289 *Einsatz restriktiver z/OS-Kennungen*
- M 2.297 *Deinstallation von z/OS-Systemen*
- M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*

Bei anderen Betriebssystemen sind die dort beschriebenen Hinweise in ähnlicher Weise umzusetzen (siehe dazu auch die betriebssystemspezifischen Bausteine).

Prüffragen:

- Bei zusätzlichen Zugriffsberechtigungen, die über das Standardprofil hinausgehen: Werden diese nur nach zusätzlicher Begründung vergeben?
- Gibt es eine geregelte Vorgehensweise zur Einrichtung von Benutzern und Benutzergruppen?
- Existiert eine separate administrative Rolle für das Einrichten von Rechten bzw. Rechteprofilen?

# M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es muss eine Dokumentation der am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile erfolgen. Dabei gibt es verschiedene Dokumentationsmöglichkeiten wie beispielsweise über

- vorgegebene Administrationsdateien des Systems,
- individuelle Dateien, die vom zuständigen Administrator verwaltet werden,
- in Papierform.

Es sollte eine geeignete Form ausgewählt werden, möglichst einheitlich für die gesamte Institution.

Dokumentiert werden sollten insbesondere folgende Angaben zur Rechtevergabe an Benutzer und Benutzergruppen:

Zugelassene Benutzer:

- zugeordnetes Rechteprofil (gegebenenfalls Abweichungen vom verwendeten Standard-Rechteprofil)
- Begründung für die Wahl des Rechteprofils (und gegebenenfalls der Abweichungen)
- Zuordung des Benutzers zu einer Organisationeinheit, Raum- und Telefonnummer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Zugelassene Gruppen:

- zugehörige Benutzer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Die Dokumentation der zugelassenen Benutzer und Rechteprofile sollte regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht. Die vollständige Dokumentation ist Voraussetzung für Kontrollen der vergebenen Benutzerrechte.

Die Dokumentation muss so gespeichert beziehungsweise aufbewahrt werden, dass sie vor unbefugtem Zugriff geschützt ist und so, dass auch bei einem größeren Sicherheitsvorfall oder IT-Ausfall darauf zugegriffen werden kann. Falls die Dokumentation in elektronischer Form erfolgt, muss sie in das Datensicherungsverfahren einbezogen werden.

Prüffragen:

- Sind die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert?
- Wird die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile regelmäßig auf Aktualität überprüft?
- Ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt?

- Wird die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile - sofern sie elektronisch erfolgt - in das Datensicherungsverfahren einbezogen?

# M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Falls Benutzer nur bestimmte Aufgaben wahrnehmen müssen, ist es oftmals nicht erforderlich, ihnen alle mit einem eigenen Login verbundenen Rechte oder sogar Systemadministrator-Rechte zu geben. Beispiele sind bestimmte Tätigkeiten der routinemäßigen Systemverwaltung wie die Erstellung von Backups oder das Einrichten eines neuen Benutzers, die mit einem Programm menügesteuert durchgeführt werden, oder Tätigkeiten, für die ein Benutzer nur ein einzelnes Anwendungsprogramm benötigt. Insbesondere bei Aushilfskräften und externen Dienstleistern sollte darauf geachtet werden, dass diese nur die Dienste verwenden und nur auf die Daten zugreifen dürfen, die sie tatsächlich benötigen. Wenn ihre Tätigkeit beendet ist, sollten deren Accounts deaktiviert und alle Zugangsberechtigungen entfernt werden (siehe auch M 4.17 *Sperren und Löschen nicht benötigter Accounts und Terminals*).

Für diese Benutzer sollte eine eingeschränkte Benutzerumgebung geschaffen werden. Sie kann zum Beispiel unter Unix durch eine Restricted Shell (*rsh*) und eine Beschränkung der Zugriffspfade mit dem Unix-Kommando *chroot* realisiert werden. Für einen Benutzer, der nur ein Anwendungsprogramm benötigt, kann dieses als Login-Shell eingetragen werden, so dass es nach dem Einloggen direkt gestartet und der Benutzer nach Beendigung des Programms automatisch ausgeloggt wird.

Der verfügbare Funktionsumfang des IT-Systems kann für einzelne Benutzer oder Benutzergruppen eingeschränkt werden. Die Nutzung von Editorprogrammen oder Compilern sollte verhindert werden, wenn sie nicht für die Aufgabenerfüllung des Benutzers erforderlich sind. Dies kann bei Stand-alone-Systemen durch die Entfernung solcher Programme und bei vernetzten Systemen durch die Rechtevergabe geregelt werden.

**Microsoft Windows**

Nachfolgend werden Sicherheitsmerkmale von Microsoft-Windows-Versionen vorgestellt, mit denen sich eine eingeschränkte Benutzerumgebung durch technische Maßnahmen durchsetzen lässt.

Microsoft Windows ab einschließlich der Version NT bietet die Möglichkeit, Startskripte zu verwenden, um die Zugriffe eines Benutzers auf einzelne Anwendungen zu beschränken. Es muss darauf geachtet werden, dass ein Benutzer die Ausführung der Skripte nicht unterbrechen oder verändern kann. Beispielsweise können die Skripte für einen sich anmeldenden Benutzer unsichtbar ausgeführt werden. Auch die gestartete Anwendung darf dem Benutzer keine Möglichkeit bieten, andere Programme zu starten.

Ab Windows 7 und Windows Server 2008 R2 kann der Zugang zu Anwendungen mit AppLocker blockiert und durch einen Administrator bei Bedarf freigeschaltet werden (siehe M 4.419 *Anwendungssteuerung ab Windows 7 mit AppLocker*).

Ab Windows Vista erleichtert die Benutzerkontensteuerung (User Account Control, UAC, siehe auch M 4.340 *Einsatz der Windows-Benutzerkonten-*

*steuerung UAC ab Windows Vista*) das flexible Arbeiten mit eingeschränkten Benutzerrechten für Administratoren und normale Benutzer. Durch die UAC laufen alle Benutzervorgänge systemintern grundsätzlich mit Standardbenutzer-Berechtigungen, auch wenn der Benutzer mit einem Administratorkonto angemeldet ist. Für administrative Vorgänge wie Druckerinstallation oder Netzkonfiguration und für Programme, die nur mit Administratorrechte laufen können, zum Beispiel ältere Fachapplikationen, zeigt Windows ein Bestätigungsfenster an, das zusätzlich gegen Trojaner und Schadprogramme schützen soll. Erst nach Bestätigung durch den Benutzer werden die Administratorberechtigungen aktiviert. Sie sind auf den bestimmten Vorgang oder die Applikation beschränkt. Alle anderen und folgenden Vorgänge laufen parallel mit eingeschränkten Benutzerrechten weiter. Standardbenutzer erhalten statt der Bestätigungsmeldung ein geschütztes Anmeldefenster, in dem sie oder ein Mitarbeiter des IT-Support sich mit einem Administratorkonto anmelden können. Die laufenden Benutzervorgänge werden auch hier nicht unterbrochen. Dies stellt eine benutzerfreundliche Alternative zu den Befehlen *runas* und *Ausführen als ...* dar.

Über *Jugendschutz* kann ein Administrator für einen Benutzer Einschränkungen bei der Nutzung eines Systems ab Windows Vista und Windows Server 2008 festlegen. Jugendschutz unterstützt die Gestaltung der Nutzungseinschränkung anhand folgender Kriterien:

- Zeiten, an denen der Benutzer sich anmelden kann,
- Programme, die der Benutzer starten kann und
- Web-Seiten (URLs), die der Benutzer aufrufen kann.

Jugendschutz ist allerdings für den nicht professionellen Einsatz konzipiert. Die durch den Jugendschutz ermöglichten Einschränkungen sollten im professionellen Umfeld durch alternative Maßnahmen durchgesetzt werden.

**KDE und GNOME unter Linux**

In den Linux-Benutzeroberflächen KDE und GNOME ist eine mit der Windows Benutzerkontensteuerung vergleichbare Abfrage von erhöhten Rechten innerhalb eingeschränkter Benutzerumgebungen enthalten. Diese sollte analog genutzt werden.

Prüffragen:

- Sind Benutzerumgebung und Startprozedur für den jeweiligen Benutzer an seine Aufgaben angepasst?
- Wird die Nutzung von Editor-Programmen oder Compilern verhindert, wenn diese nicht für die Aufgabenerfüllung des Benutzers erforderlich sind?
- Wurde darauf geachtet, dass die Benutzer Startskripte beim Start von Windows nicht verändern oder abbrechen können?
- Existiert eine Regelung für die Benutzerumgebung temporärer Benutzerkonten?
- Sind vorhandene Sicherheitsmaßnahmen und -merkmale des eingesetzten IT-/ Betriebssystems wie die Benutzerkontensteuerung (UAC) aktiv, um die Einschränkung der Benutzerumgebung durchzusetzen?

# M 2.33 Aufteilung der Administrationstätigkeiten unter Unix

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In den meisten Unix-Systemen gibt es nur eine Administrationsrolle (den *Super-User* namens *root* mit der Benutzer-ID (UID) 0). Personen mit Zugang zu dieser Rolle haben die volle Kontrolle über das System. Insbesondere können sie unabhängig von Zugriffsrechten jede Datei lesen, verändern und löschen.

Das Super-User-Passwort darf nur den Administratoren bekannt sein. Die Weitergabe des Passworts ist auf die in Regelungen festgelegte Fälle zu beschränken und zu dokumentieren. Der Super-User-Login *root* kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z. B. durch organisatorische Maßnahmen wie ein geteiltes Passwort. Dabei muss das Passwort eine erhöhte Mindestlänge (12 oder mehr Zeichen) haben. Hierbei muss darauf geachtet werden, dass das Passwort in voller Mindestlänge vom System überprüft wird.

Bei etlichen Unix-Systemen ist eine Aufgabenteilung durch die Ausnutzung vorhandener Administratorrollen möglich. Diese Rollen sollen dann durch verschiedene Personen wahrgenommen werden.

Eine Reihe von Administrationstätigkeiten können auch ohne Zugang zum Login *root* ausgeführt werden. Wenn es Administratoren mit solchen Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere, wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko durch eine entsprechende Aufgabenteilung vermindert werden. Es gibt dazu zwei Möglichkeiten:

- Schaffung administrativer Logins: Sie haben zwar die UID 0, jedoch wird beim Login nur ein Programm gestartet, mit dem die administrative Aufgabe ausgeführt werden kann und das mit einem Logout endet. Beispiele: Einrichten neuer Benutzer, Mounten eines Laufwerks. Zu UNIX V.4 können z. B. die administrativen Login-Namen *setup*, *sysadm*, *powerdown*, *checkfsys*, *mountfsys* und *umountfsys* mit den gleichnamigen Programmen eingerichtet werden.
- Benutzung von Logins ohne UID 0: Diese Login-Namen (*sys*, *bin*, *adm*, *uucp*, *nuucp*, *daemon* und *lp*) sind Eigentümer von Dateien und Programmen, die für die Funktionalität des Systems entscheidend sind und die daher besonderem Schutz unterliegen. Sie sind in den meisten Unix-Systemen zur Verwaltung der entsprechenden Dienste vorgegeben.

Um festzustellen, welche Logins Administratorrechte haben, sollten regelmäßig Hilfsprogramme (z. B. *cops, tiger*) eingesetzt werden, die nach Logins mit der UID 0 in der Passwort-Datei suchen.

Prüffragen:

- Existiert eine Regelung zum Umgang mit Super-User-Passwörtern unter Unix (Rolle "root" bzw. Benutzer mit UID 0)?
- Wird das Passwort in voller Mindestlänge vom IT-System überprüft?
- Existiert eine Regelung zur Rollentrennung und Aufteilung der Administrationstätigkeiten an Unix-Systemen?

- Wird bei Unix-Systemen regelmäßig überprüft, welche Logins Administratorrechte haben?

# M 2.34 Dokumentation der Veränderungen an einem bestehenden System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um einen reibungslosen Betriebsablauf zu gewährleisten, muss der Administrator einen Überblick über das System haben bzw. sich verschaffen können. Dieses muss auch für seinen Vertreter möglich sein, falls der Administrator unvorhergesehen ausfällt. Der Überblick ist auch Voraussetzung, um Prüfungen des Systems (z. B. auf problematische Einstellungen, Konsistenz bei Änderungen) durchführen zu können.

Daher sollten die Veränderungen, die Administratoren am System vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.

Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten des IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden.

Unter Unix müssen ausführbare Dateien, auf die auch andere Benutzer als der Eigentümer Zugriff haben oder deren Eigentümer *root* ist, vom Systemadministrator freigegeben und dokumentiert werden (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*). Insbesondere müssen Listen mit den freigegebenen Versionen dieser Dateien geführt werden, die außerdem mindestens das Erstellungsdatum, die Größe jeder Datei und Angaben über evtl. gesetzte s-Bits enthalten. Sie sind Voraussetzung für den regelmäßigen Sicherheitscheck und für Überprüfungen nach einem Verlust der Integrität.

Prüffragen:

- Werden Systemänderungen ausreichend und für eine fachkundige Person nachvollziehbar dokumentiert?

# M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Gegen bekannt gewordene und durch Veröffentlichungen zugänglich gemachte Sicherheitslücken müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen werden. Sicherheitsrelevante Updates oder Patches für die eingesetzte Hard- und Software müssen gegebenenfalls installiert werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Sind keine entsprechenden Updates oder Patches verfügbar, so muss eventuell zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden.

Es ist daher sehr wichtig, dass sich die Systemadministratoren regelmäßig über neu bekannt gewordene Schwachstellen informieren. Informationsquellen zu diesem Thema sind beispielsweise:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) (siehe *http://www.bsi.bund.de/*)
- Hersteller bzw. Distributoren von Programmen und Betriebssystemen. Diese informieren oft registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung.
- Computer Emergency Response Teams (CERTs).
  Dies sind Computer-Notfallteams, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in bezug auf sicherheitsrelevante Vorfälle in Computersystemen dienen. CERTs informieren in sogenannten *Advisories* über aktuelle Schwachstellen in Hard- und Softwareprodukten und geben Empfehlungen zu deren Behebung. Verschiedene Organisationen oder Verbände unterhalten eigene CERTs.
  Das ursprüngliche CERT der Carnegie Mellon Universität diente als Vorbild für viele weitere derartige Teams und ist heute eine Art "Dach-CERT": Computer Emergency Response Team / Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890,
  Telefon: +1-412-268-7090 (24-Stunden-Hotline), E-Mail: *cert@cert.org*, WWW: *http://www.cert.org*
  Die CERT-Mitteilungen werden in Newsgruppen (*comp.security.announce* und *info.nsfnet.cert*) und über Mailinglisten (Aufnahme durch E-Mail an: *cert-advisory-request@cert.org*) veröffentlicht.
  In Deutschland existieren unter anderem folgende CERTs:
- CERT-Bund, Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn, Telefon: 0228 99-9582-222, Fax: 022899-9582-5427, E-Mail: *certbund@bsi.bund.de*, WWW: *https://www.bsi.bund.de/certbund/*
- DFN-CERT, Zentrum für sichere Netzdienste GmbH, DFN-CERT, DFN-CERT Services GmbH, Sachsenstraße 5, D-20097 Hamburg, Telefon: 040-808077-555, Fax: -556, E-Mail: info@dfn-cert.de, WWW: http://www.dfn-cert.de.
- An verschiedenen Hochschulen existieren CERTs, die auch Informationen öffentlich zur Verfügung stellen. Ein Beispiel ist das RUS-CERT der Universität Stuttgart (siehe *http://cert.uni-stuttgart.de*).
- Hersteller- und systemspezifische sowie sicherheitsspezifische Newsgruppen oder Mailinglisten. In solchen Foren werden Hinweise auf existie-

rende oder vermutete Sicherheitslücken oder Fehler in diversen Betriebssystemen und sonstigen Softwareprodukten diskutiert. Besonders aktuell sind meist die englischsprachigen Mailinglisten wie *Bugtraq*, von denen es an vielen Stellen öffentlich zugängliche Archive gibt, beispielsweise unter *http://www.securityfocus.com*.
- Manche IT-Fachzeitschriften veröffentlichen ebenfalls regelmäßig Beiträge mit einer Übersicht über neue Sicherheitslücken in verschiedenen Produkten.

Idealerweise sollten sich die Administratoren und der IT-Sicherheitsbeauftragte bei mindestens zwei verschiedenen Stellen über Sicherheitslücken informieren. Dabei ist es empfehlenswert, neben den Informationen des Herstellers auch eine "unabhängige" Informationsquelle zu benutzen.

Die Administratoren sollten jedoch in jedem Fall auch produktspezifische Informationsquellen des Herstellers nutzen, um beispielsweise darüber Bescheid zu wissen, ob für ein bestimmtes Produkt beim Bekanntwerden von Sicherheitslücken überhaupt Patches oder Updates bereitgestellt werden. Bei Produkten, für die der Hersteller keine Sicherheitspatches mehr zur Verfügung stellt, muss rechtzeitig geprüft werden, ob ein Einsatz unter diesen Umständen noch zu verantworten ist und durch welche zusätzlichen Maßnahmen ein Schutz der betroffenen Systeme trotzdem gewährleistet werden kann.

Prüffragen:

- Informieren sich die Administratoren regelmäßig bei verschiedenen Quellen über neu bekannt gewordene Schwachstellen?
- Werden sicherheitsrelevante Updates zeitnah eingespielt?
- Bei fehlenden Updates für bekannte Schwachstellen: Werden andere technische oder organisatorische Maßnahmen ergriffen?

# M 2.36 Geregelte Übergabe und Rücknahme eines tragbaren PC

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Laptops und andere tragbare IT-Systeme werden je nach Einsatzzweck nur von einem einzelnen Mitarbeiter eingesetzt, z. B. als Arbeitsplatzrechner, der auch mobil genutzt wird. Sie können aber auch abwechselnd von verschiedenen Mitarbeitern genutzt werden, z. B. für Präsentationen. Je nach Einsatzart ergeben sich verschiedene Sicherheitsanforderungen. Daher sollte Einsatzzweck und -art im Vorfeld sorgfältig geplant werden.

Bei der Nutzung als Arbeitsplatzrechner werden diese typischerweise abwechselnd mobil und stationär genutzt. Dabei kann auf verschiedene Netze zugegriffen werden. Dafür müssen die Laptops so abgesichert sein, dass auf der einen Seite durch den mobilen Einsatz weder wichtige Daten der Laptops kompromittiert, manipuliert oder verloren gehen können. Auf der anderen Seite dürfen über die Laptops keine Gefährdungen in die internen Netze eingeschleppt werden.

Wenn Laptops abwechselnd von verschiedenen Personen genutzt werden, ist eine geregelte Übergabe extrem wichtig. Damit dies gut funktioniert, sollte ein Laptop-Pool eingerichtet werden (siehe M 1.35 *Sammelaufbewahrung tragbarer IT-Systeme*).

Bei der Übergabe und Rücknahme eines tragbaren IT-Systems sind folgende Punkte zu beachten:

**Übergabe:**
- Der neue Benutzer wird aufgefordert, direkt bei der Übergabe das alte Passwort des Laptops bzw. das Standardpasswort zu ändern.
- Dem neuen Benutzer sollte ein Merkblatt für den sicheren Umgang mit dem tragbaren IT-system übergeben werden.
- Damit jederzeit nachvollziehbar ist, wo sich die Geräte befinden, sollte jeder Benutzer mit Namen, Organisationseinheit, Telefonnummer, Einsatzzweck in ein Übergabe-/Rücknahmejournal eingetragen werden.

**Rücknahme bzw. Weitergabe:**
- Der Benutzer gibt sein zuletzt benutztes Passwort bekannt bzw. stellt ein Standardpasswort wie "LAPTOP" ein.
- Der Laptop muss mittels eines aktuellen Viren-Suchprogramms auf einen Computer-Viren-Befall überprüft werden.
- Der Benutzer muss sicherstellen, dass vor Übergabe des Gerätes sämtliche Daten, die der Benutzer noch benötigt, auf ihm zugängliche Datenträger (z. B. seinen PC) übertragen werden. Darüber hinaus hat der Benutzer dafür Sorge zu tragen, dass sämtliche von ihm erzeugten Dateien und Daten (nach Möglichkeit physikalisch) gelöscht werden. Hierfür müssen geeignete Tools vorhanden sein.
- Die Rückgabe des Laptops und das Untersuchungsergebnis der Virensuche werden dokumentiert. Die Vollständigkeit des Gerätes, des Zubehörs und der Dokumentation ist sicherzustellen.
- Um sicherzustellen, dass die definierte sichere Grundkonfiguration vorhanden ist und sich keine sensiblen Dateien mehr auf dem Laptop befinden, sollte der Laptop mit einer Referenzinstallation neu installiert werden

(siehe hierzu M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops*).
- Zurückgegebene Datenträger werden neu formatiert.

Die vorgesehenen Einsatzarten der Laptops sind zu dokumentieren.

Prüffragen:

- Sind alle sicherheitsrelevanten Aspekte bei der Übergabe und Rücknahme von tragbaren PC geregelt, wenn Laptops abwechselnd von verschiedenen Personen genutzt werden?
- Wird mit dem tragbaren IT-Systemen ein Merkblatt für den sicheren Umgang ausgegeben?

# M 2.37 Der aufgeräumte Arbeitsplatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Organisation
**Verantwortlich für Umsetzung:** Mitarbeiter

Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz "aufgeräumt" zu hinterlassen. IT-Benutzer müssen dafür sorgen, dass Unbefugte keinen Zugang zu IT-Anwendungen oder Zugriff auf Daten erhalten. Alle Mitarbeiter müssen mit der gleichen Sorgfalt ihre Arbeitsplätze überprüfen und sicherstellen, dass keine sensiblen Informationen frei zugänglich sind und die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten nicht negativ beeinflusst werden kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger (wie Disketten, USB-Sticks oder Festplatten) oder Unterlagen (z. B. Ausdrucke) zugreifen können.

Für eine kurze Abwesenheit während der Arbeitszeit ist es ausreichend, den Raum, sofern möglich, zu verschließen und/oder den Bildschirm so zu sperren, dass Zugriffe nur nach erfolgreicher Authentisierung möglich sind. Bei geplanter Abwesenheit eines Mitarbeiters (z. B. längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und verschließbare Staumöglichkeiten, wie z. B. stabile Schränke.

Auch Passwörter dürfen auf keinen Fall sichtbar (als Klebezettel am Monitor, an einem leicht zu erratenden Ort wie z. B. unter der Schreibtischauflage oder in der unverschlossenen Schreibtischschublade) aufbewahrt werden (siehe M 2.2 *Betriebsmittelverwaltung*). Ebenfalls sollten eindeutige Hinweise (z. B. Namen von Familienangehörigen oder sogenannte Trivialpasswörter wie aufeinanderfolgende Buchstaben und Zahlen) für das schnelle Erraten ausgeschlossen werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Vorgesetzte und Mitarbeiter des Sicherheitsmanagements sollten sporadisch Arbeitsplätze überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind und die Mitarbeiter auf korrektes Aufräumen hinweisen.

Prüffragen:

- Wurden alle Mitarbeiter darauf hingewiesen, dass an unbeaufsichtigten Arbeitsplätzen keine sensiblen Informationen frei zugreifbar sein dürfen?
- Werden Arbeitsplätze stichprobenartig kontrolliert, ob schutzbedürftige Informationen offen zugreifbar sind?

# M 2.38 Aufteilung der Administrationstätigkeiten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Viele Netzbetriebssysteme bieten die Möglichkeit, die Administratorrolle aufzuteilen und Administrationstätigkeiten an verschiedene Benutzer zu verteilen.

So können zum Beispiel unter Novell Netware 3.11 die folgenden Administratorrollen eingerichtet werden: Workgroup Manager, User Account Manager, File Server Console Operator, Print Server Operator, Print Queue Operator.

Unter Windows NT können durch die gezielte Vergabe von Benutzerrechten an einzelne Benutzer oder besser an Gruppen definierte Administratorrollen geschaffen werden. Neben der Gruppe der Administratoren sind hier die Gruppen Hauptbenutzer (d. h. Administratoren mit eingeschränkten Rechten), Sicherungs-Operatoren, Druck-Operatoren, Server-Operatoren sowie Reproduktions-Operatoren zu nennen. Darüber hinaus können weitere Rollen durch explizite Zuweisung von Benutzerrechten definiert werden (siehe auch M 4.418 *Planung des Einsatzes von Windows Server 2008*).

Wenn es Administratorrollen für Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere, wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko der übergroßen Machtbefugnis der Administratorrollen durch eine entsprechende Aufgabenteilung vermindert werden, so dass Administratoren nicht unkontrolliert unautorisierte oder unbeabsichtigte Veränderungen am System vornehmen können.

Trotz des Aufteilens von Administrationstätigkeiten legt das System meist noch automatisch einen Account für einen Administrator an, der keinen Beschränkungen unterliegt, den Supervisor. Das Supervisor-Passwort sollte, wenn überhaupt, nur einem kleinen Personenkreis bekannt sein. Es darf keinem der Subadministratoren bekannt sein, damit diese nicht auf diese Weise ihre Rechte erweitern können. Das Passwort ist gesichert zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*). Das Supervisor-Login kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z. B. durch organisatorische Maßnahmen wie ein geteiltes Passwort. Dabei muss das Passwort eine erhöhte Mindestlänge (12 oder mehr Zeichen) haben. Hierbei muss darauf geachtet werden, dass das Passwort in voller Mindestlänge vom System überprüft wird.

Prüffragen:

- Existieren unterschiedliche Administratorrollen für Teilaufgaben?
- Bei vorhandenem Supervisor-Account: Ist das Supervisor-Passwort nur einem minimalen Personenkreis bekannt?
- Bei vorhandenem Supervisor-Account: Ist das Supervisor-Passwort gesichert hinterlegt?

# M 2.39 Reaktion auf Verletzungen der Sicherheitsvorgaben

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Es ist festzulegen, welche Reaktion auf Verletzungen der Sicherheitsvorgaben erfolgen soll, um eine klare und sofortige Reaktion gewährleisten zu können.

Untersuchungen sollten durchgeführt werden, um festzustellen, wie und wo die Verletzung entstanden ist. Anschließend müssen die angemessenen schadensbehebenden oder -mindernden Maßnahmen durchgeführt werden. Soweit erforderlich, müssen zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen sowohl von der Art der Verletzung als auch vom Verursacher ab.

Es muss geregelt sein, wer für Kontakte mit anderen Organisationen verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*) oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es muss dafür Sorge getragen werden, dass eventuell. mitbetroffene Stellen schnellstens informiert werden (siehe Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*).

Prüffragen:

- Ist die Vorgehensweise bei Verdacht auf Verletzung der Sicherheitsvorgaben klar definiert?

# M 2.40 Rechtzeitige Beteiligung des Personal-/Betriebsrates

**Verantwortlich für Initiierung:** Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Personalabteilung

Bei allen Maßnahmen, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Mitarbeitern ermöglichen, zum Beispiel Protokollierung, bedarf es der Mitbestimmung der Personalvertretung. Maßnahmen, die geeignet sind, eine Verhaltens- oder Leistungsüberwachung eines Mitarbeiters zu ermöglichen, bedürfen der Mitbestimmung der Personalvertretung. Grundlage dessen sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. In anderen Ländern ist die Einbeziehung der Personalvertretung nicht immer erforderlich. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrates empfiehlt sich aber grundsätzlich, da dies Zeitverzögerungen bei der Umsetzung von Maßnahmen im Bereich der Informationssicherheit verhindern kann.

Bei bereits bestehendem Verdacht, dass ein Sicherheitsvorfall (siehe Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*) durch einen internen Mitarbeiter ausgelöst wurde und entsprechende Nachforschungen durchgeführt werden sollen, die auf Sanktionen hinauslaufen, sind die Beteiligungsrechte des Personal- beziehungsweise Betriebsrates unbedingt zu beachten. Unterbleibt eine ordnungsgemäße Beteiligung der Mitarbeitervertretung, kann das eventuell erforderliche weitere Verfahren (gegebenenfalls vor dem Arbeitsgericht) je nach Schwere des Vorfalls für eine Abmahnung oder Kündigung aufgrund von Formfehlern gravierend beeinflusst werden.

Große Outsourcing-Dienstleister berichten aus der Praxis, dass eine frühzeitige Einbindung der Personalvertretung des Auftraggebers, möglichst schon in der Angebotsphase, sehr zum Gelingen des Projektes beitragen kann. Wechselbereitschaft der Mitarbeiter, Motivation, Arbeitszufriedenheit und zügige Projektabwicklung können durch Kooperation aller Beteiligten positiv beeinflusst werden. Gleiches gilt für die geplante Nutzung von Cloud-Diensten. Als Besonderheit ist hierbei anzusehen, dass die oben genannten Vorgaben auch dann zu beachten sind, wenn sich eine Institution für eine Private Cloud entscheidet.

Prüffragen:

- Wird die Personalvertretung (Arbeitnehmer-, Mitarbeitervertretung) bei sie betreffenden Verfahren und Projekten rechtzeitig informiert?

# M 2.41 Verpflichtung der Mitarbeiter zur Datensicherung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Da die Datensicherung eine wichtige Sicherheitsmaßnahmen ist, sollten die betroffenen Mitarbeiter auf die Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes darüber informiert werden, welches ihre Aufgaben bei der Erstellung von Datensicherungen sind. Auf deren sorgfältige Durchführung sollten sie verpflichtet werden. Dies ist vor allem dort wichtig, wo zentral durchgeführte Datensicherungen nicht greifen, also z. B. bei nicht-vernetzten oder mobilen Endgeräten. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollte erfolgen.

Prüffragen:

- Wurden die Mitarbeiter darüber informiert, welches ihre Aufgaben bei der Erstellung von Datensicherungen sind?

# M 2.42 Festlegung der möglichen Kommunikationspartner

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Sollen Informationen an einen Kommunikationspartner außerhalb der eigenen Institution übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzt. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so sollte für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat beziehungsweise erhalten wird. Um die oben genannten Kriterien zu erfüllen, muss festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen. Hierfür ist es erforderlich, dass alle Informationen entsprechend ihrer strategischen Bedeutung für die Institution klassifiziert sind (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Die Empfänger sind darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck benutzt werden dürfen, zu dem sie weitergegeben wurden. Auch aus Datenschutzgründen (siehe zum Beispiel BDSG, Weitergabekontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenübertragung oder Datenträgeraustausch zu erhalten.

**Beispiel:**

Eine Institution schließt mit einem Cloud-Diensteanbieter einen Vertrag zur Nutzung eines definierten Cloud Services. Der gewählte Cloud-Diensteanbieter nutzt zur Leistungserbringung seinerseits Services eines Subauftragnehmers und gibt die Daten der Institution zur Verarbeitung an diesen weiter. Alle Kommunikationswege sowie die Art und der Umfang der weitergegebenen Daten sind in diesem Fall durch den Cloud-Diensteanbieter transparent darzulegen.

Prüffragen:

- Ist festgelegt, welche Kommunikationspartner welche Informationen erhalten dürfen?

# M 2.43 Ausreichende Kennzeichnung der Datenträger beim Versand

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Benutzer

Neben den in Maßnahme M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen ist bei einer ausreichenden Kennzeichnung von auszutauschenden Datenträgern darauf zu achten, dass Absender und (alle) Empfänger unmittelbar zu identifizieren sind. Die Kennzeichnung der Datenträger bzw. deren Verpackung muss den Inhalt der Datenträger eindeutig für den Empfänger erkennbar machen. Es ist jedoch bei schützenswerten Informationen wichtig, dass diese Kennzeichnung für Unbefugte keinen Rückschluss auf die Art und Inhalte der gespeicherten Informationen zulässt.

Für Verschlusssachen sind in jedem Fall die jeweils gültigen Geheimschutzvorschriften einzuhalten.

Darüber hinaus sollten die Datenträger mit den **verwendeten Formaten** beziehungsweise den für das Auslesen **notwendigen Parametern** gekennzeichnet werden. So ist bei der Übermittlung von DVDs unter anderem zu vermerken, ob es sich um Video-, Audio- oder Daten-DVDs handelt.

Datum des Versandes, eventuelle Versionsnummern oder Ordnungsmerkmale können ebenfalls nützliche Kennzeichnungen für Datenträger sein.

Prüffragen:

- Ist festgelegt, welche Kommunikationspartner welche Informationen erhalten dürfen?
- Ist für alle Beteiligten an der Kommunikation ersichtlich, wer welche Informationen erhalten darf?
- Macht die Kennzeichnung der Datenträger deren Inhalt für den Empfänger eindeutig erkennbar?
- Lässt die Kennzeichnung der Datenträger mit schützenswerten Informationen keinen Rückschluss auf Art und Inhalte der Informationen zu?

# M 2.44 Sichere Verpackung der Datenträger

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer, Poststelle

Neben den in Maßnahme M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen sollte die Versandverpackung von Datenträgern dergestalt sein, dass Manipulationen an den Datenträgern durch Veränderungen an der Verpackung erkennbar sind.

Mögliche Maßnahmen sind die Verwendung von

- Umschlägen mit Siegel,
- verplombten Behältnissen,
- Umschlägen, die mit Klebefilm überklebt und anschließend mit nicht-wasserlöslicher Tinte mehrmals unregelmäßig überzeichnet werden,
- Sicherheitsetiketten, mit denen die Briefhüllen versiegelt werden.

Für den Geheimschutzbereich gibt es spezielle, hierfür eignungsgeprüfte Sicherheitsbriefhüllen, Siegelbänder und Sicherheitsetiketten.

Falls digitale Datenträger über einen Schreibschutz verfügen (z. B. Schieber bei Disketten, Schreibring bei Bändern), so sollte dieser genutzt werden. Je nach Schutzbedarf der auf den Datenträgern gespeicherten Daten sollte geprüft werden, welche der folgenden Sicherheitsmechanismen zweckmäßig sind:

- Die Dateien sollten möglichst schreibgeschützt auf den Datenträgern gespeichert werden. Hierfür kann beispielsweise der in vielen Office-Programmen vorhandene Zugriffsschutz genutzt werden (siehe auch M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*).
- Sollen Manipulationen an den Informationen auf dem Datenträger selbst erkannt werden können, sind Verschlüsselungs- oder Checksummen-Verfahren einzusetzen (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).
- Um unbefugtes Auslesen zu verhindern, sollte der komplette Datenträger oder die einzelnen Dateien verschlüsselt werden.

Prüffragen:

- Werden sichere Versandverpackungen für Datenträger verwendet, die Manipulationen durch Veränderungen an der Verpackung erkennen lassen?

# M 2.45 Regelung des Datenträgeraustausches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Benutzer, Poststelle

Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch eine Reihe von Empfehlungen zu beachten.

Es muss eine geeignete Versandart festgelegt werden. Dabei sind insbesondere die Art der Datenträger und der Schutzbedarf der Informationen zu berücksichtigen.

Die Adressierung muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollte neben dem Namen des Empfängers auch die Organisationseinheit und die genaue Bezeichnung der Behörde bzw. des Unternehmens angegeben sein. Innerhalb einer Institution sollten Verzeichnisse der gebräuchlichsten Adressen gepflegt werden, damit möglichst aktuelle und korrekte Adressen der Empfänger verwendet werden.

Auch die Adresse des Absenders muss eindeutig und vollständig angegeben werden. Hierfür sollte innerhalb der Institution eine Vorgabe erstellt werden, die den Umfang und den Aufbau der Absender-Angabe einheitlich regelt.

Digitalen Datenträgern sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der folgende Informationen umfasst:

- Absender,
- Empfänger,
- Art und Menge der Datenträger,
- Seriennummer (soweit vorhanden),
- Identifikationsmerkmal für den Inhalt des Datenträgers,
- Datum des Versandes, gegebenenfalls Datum bis wann der Datenträger spätestens den Empfänger erreicht haben muss,
- Hinweis, dass Datenträger auf Viren überprüft sind,
- Parameter, die zum Lesen der Informationen benötigt werden, z. B. Bandgeschwindigkeit.

Jedoch sollte nicht vermerkt werden,

- welches Passwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel für eine Verschlüsselung der Informationen verwendet wurde,
- welchen Inhalt der Datenträger hat.

Der Versand des Datenträgers kann (optional) dokumentiert werden. Bei personenbezogenen oder anderen sensiblen Daten muss der Versand dokumentiert werden.

Der korrekte Empfang sollte überprüft werden. Bei Sendungen mit hochvertraulichen oder termingebundenen Inhalten sollten die Empfänger über die Absendung und den gewählten Transportweg informiert werden. Bei hohem Schutzbedarf empfiehlt es sich, den Empfänger um eine Empfangsbestätigung zu bitten.

Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen. Ergeben sich Hinweise auf Manipulationen oder einen Verlust, ist sofort das Sicherheitsmanagement zu unterrichten.

Prüffragen:

- Wird bei der Wahl der Versandart die Art der Datenträger und der Schutzbedarf der Informationen berücksichtigt?
- Ist sichergestellt, dass der Versand personenbezogener oder anderer sensiblen Daten dokumentiert wird?
- Sind die Verantwortlichkeiten für den Versand und den Empfang von Datenträgern geregelt?

# M 2.46 Geeignetes Schlüsselmanagement

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Die Verwendung kryptographischer Sicherheitsmechanismen (z. B. Verschlüsselung, digitale Signatur) setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus. Schlüssel, die Unbefugten zur Kenntnis gelangt sind, bei der Verteilung verfälscht worden sind oder gar aus unkontrollierter Quelle stammen (dies gilt auch für die Schlüsselvereinbarung zwischen Kommunikationspartnern), können den kryptographischen Sicherheitsmechanismus genauso kompromittieren wie qualitativ schlechte Schlüssel, die auf ungeeignete Weise erzeugt worden sind. Qualitativ gute Schlüssel werden in der Regel unter Verwendung geeigneter Schlüsselgeneratoren erzeugt (siehe unten). Für das Schlüsselmanagement sind folgende Punkte zu beachten:

**Schlüsselerzeugung**

Die Schlüsselerzeugung sollte in sicherer Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptographische Schlüssel können zum einen direkt am Einsatzort (und dann meistens durch den Benutzer initiiert) oder zum anderen zentral erzeugt werden. Bei der Erzeugung vor Ort müssen meistens Abstriche an die Sicherheit der Umgebung gemacht werden, bei einer zentralen Schlüsselgenerierung muss sichergestellt sein, dass sie ihre Besitzer authentisch und kompromittierungsfrei erreichen.

Geeignete Schlüsselgeneratoren müssen kontrollierte, statistisch gleichverteilte Zufallsfolgen unter Ausnutzung des gesamten möglichen Schlüsselraums produzieren. Dazu erzeugt z. B. eine Rauschquelle zufällige Bitfolgen, die mit Hilfe einer Logik nachbereitet werden. Anschließend wird unter Verwendung verschiedener Testverfahren die Güte der so gewonnenen Schlüssel überprüft.

Einige Kryptomodule, insbesondere solche, die keinen integrierten Zufallszahlengenerator besitzen, greifen auf Benutzereingaben zur Schlüsselerzeugung zurück. Beispielsweise werden hier Passwörter abgefragt, aus denen dann ein Schlüssel abgeleitet wird, oder der Benutzer wird gebeten, beliebigen Text einzutippen, um zufällige Startwerte für die Schlüsselgenerierung zu erhalten. Solche Passwörter sollten dabei gut gewählt sein und möglichst lang sein. Wenn möglichst "zufällige" Benutzereingaben angefordert werden, sollten diese auch zufällig, also schlecht vorhersagbar, sein.

**Schlüsseltrennung**

Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen. Insbesondere sollten für die Verschlüsselung immer andere Schlüssel als für die Signaturbildung benutzt werden. Dies ist sinnvoll,

- damit bei der Offenlegung eines Schlüssels nicht alle Verfahren betroffen sind,
- da es manchmal erforderlich sein kann, Verschlüsselungsschlüssel weiterzugeben (Vertretungsfall),
- da es unterschiedliche Zyklen für den Schlüsselwechsel geben kann.

**Schlüsselverteilung / Schlüsselaustausch**

Kryptographische Kommunikationsbeziehungen können nur dann funktionieren, wenn die Kommunikationspartner über aufeinander abgestimmte kryptographische Schlüssel verfügen. Dazu müssen alle Kommunikationspartner mit den dazu erforderlichen Schlüsseln versorgt werden. Zur Schlüsselverteilung und zum Schlüsselaustausch können unterschiedliche Verfahren verwendet werden. Die Unterschiede ergeben sich aus der Anwendung verschiedener kryptographischer Verfahren und Mechanismen bzw. aus ihrer Kombination (siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Unter Schlüsselverteilung wird hier die initiale Versorgung der Kommunikationspartner mit Grundschlüsseln verstanden. Die Schlüssel werden dazu von einer meist zentralen Schlüsselerzeugungsstelle (z. B. einem Trust Center) an die einzelnen Kommunikationspartner übermittelt.

Die Verteilung der Schlüssel sollte auf geeigneten Datenträgern (z. B. Chipkarten) oder über Kommunikationsverbindungen (z. B. LAN, WAN) vertraulich (z. B. mit KEK - Key Encryption Key - verschlüsselt), integer (z. B. MAC-gesichert) und authentisch (z. B. digital signiert gemäß Signatur-Gesetz) erfolgen. Die unbefugte Kenntnisnahme bzw. Verfälschung der Schlüssel muss verhindert oder wenigstens erkannt werden können.

Mit Schlüsselaustausch wird die Schlüsseleinigungsprozedur zwischen zwei Kommunikationspartnern auf einen Sitzungsschlüssel (Session Key) bezeichnet. Der Session Key ist ein Schlüssel, der nur eine begrenzte Zeit, etwa für die Dauer einer Kommunikationsverbindung, verwendet wird. Diese Zeit muss festgelegt werden, da Sitzungen sehr lange dauern können. Die Festlegung erfolgt z. B. durch einen relativen Zeitablauf oder durch einen Paketzähler. Für jede neue Verbindung wird ein neuer Session Key zwischen den Kommunikationspartnern ausgehandelt.

Moderne Systeme bedienen sich heute asymmetrischer kryptographischer Verfahren zur Schlüsselverteilung und zum Schlüsselaustausch. Zum Nachweis der Authentizität der öffentlichen Schlüssel kann eine vertrauenswürdige Zertifizierungsstelle eingerichtet werden. Die Kommunikationsteilnehmer müssen sich gegenüber der Zertifizierungsstelle ausweisen und dort ihren öffentlichen Schlüssel mittels einer digitalen Signatur der Zertifizierungsstelle beglaubigen lassen. Das so erzeugte digitale Zertifikat sollte mindestens den öffentlichen Schlüssel und ein Identifikationsmerkmal des Kommunikationsteilnehmers, die Gültigkeitsdauer des Zertifikats und die digitale Signatur der Zertifizierungsstelle enthalten. Mit Kenntnis des öffentlichen Signaturschlüssels der Zertifizierungsstelle ist jeder Kommunikationsteilnehmer in der Lage, die Authentizität des öffentlichen Schlüssels des Kommunikationspartners zu verifizieren.

**Schlüsselinstallation und -speicherung**

Im Zuge der Schlüsselinstallation ist die authentische Herkunft sowie die Integrität der Schlüsseldaten zu überprüfen. Generell sollten Schlüssel nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Bei Software-Verschlüsselungsprodukten muss berücksichtigt werden, dass Schlüssel zumindest zeitweise während des Ver-/Entschlüsselungsprozesses in Klarform im PC-System vorliegen müssen. Bieten die IT-Systeme, auf denen das kryptographische Produkt eingesetzt ist, keinen ausreichenden Zugriffsschutz für die Schlüssel, sollten diese nicht auf diesem IT-System gespeichert werden. Es bietet sich dann eine bedarfsorientierte manuelle Eingabe an. Eine andere Möglichkeit wäre die Auslagerung der Schlüssel auf einen

externen Datenträger, der dann aber sicher verwahrt werden muss, wie unter Schlüsselarchivierung beschrieben. Aus Sicherheitsaspekten ist deshalb der Einsatz von Hardware-Verschlüsselungskomponenten vorzuziehen, bei denen die Schlüssel vom Datenträger (z. B. Chipkarte) verschlüsselt auf direktem Weg in die Verschlüsselungskomponente geladen werden und diese nie in Klarform verlassen.

Auf jeden Fall muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens voreingestellte Schlüssel geändert werden.

**Schlüsselarchivierung**

Für Archivierungszwecke sollte das kryptographische Schlüsselmaterial auch außerhalb des Kryptomoduls in überschlüsselter Form speicherbar und gegebenenfalls wieder einlesbar sein. Dazu können mehrere Schlüssel zu einem Satz zusammengefasst werden, der dann ebenfalls mit Hilfe eines KEK (Key-Encryption-Key: Überschlüsselungsschlüssel) kryptiert wird. Der KEK muss entsprechend sicher (z. B. auf Chipkarte im Safe) aufbewahrt werden. Wird der KEK in zwei Teilschlüssel geteilt, so lässt sich das "Vier-Augen-Prinzip" umsetzen: zwei verschiedene Personen haben Zugriff auf je einen Datenträger (z. B. Chipkarte, Diskette), auf der sich nur jeweils einer der beiden Teilschlüssel befindet. Um den KEK zu generieren, müssen sich beide Datenträger gleichzeitig oder nacheinander in der Leseeinheit des Kryptomoduls befinden.

**Zugriffs- und Vertreterregelung**

In der Sicherheitsrichtlinie sollten Fragen bzgl. der Zugriffs- und Vertretungsrechte geregelt sein. Entsprechende Mechanismen müssen vom Schlüsselmanagement und von den einzusetzenden Kryptomodulen und -geräten unterstützt werden (z. B. Schlüsselhinterlegung für den Fall, dass ein Mitarbeiter das Unternehmen verlässt oder wegen Krankheit längere Zeit ausfällt, siehe auch Schlüsselarchivierung).

**Schlüsselwechsel**

Im Kryptokonzept muss basierend auf der Sicherheitsrichtlinie festgelegt werden, wann und wie oft Schlüssel gewechselt werden müssen. Je größer die Menge verschlüsselter Daten ist, die einem Angreifer für eine Analyse zur Verfügung steht, um so größer ist bei manchen Verfahren die Chance, dass das Analyseverfahren erfolgreich ist. Ein regelmäßiger Schlüsselwechsel minimiert die Angriffsmöglichkeiten auf verschlüsselte Daten. Die Wechselfrequenz ist von verschiedenen Faktoren abhängig. Dabei spielt die Art des verschlüsselten Mediums (z. B. Langzeitdatenträger, Datenübertragungsmedium) ebenso eine Rolle wie der kryptographische Algorithmus, die Detektion von Angriffen (z. B. Diebstahl oder Verlust eines Schlüssels) und die Schutzwürdigkeit der Daten. Weitere Faktoren bei der Festlegung der Wechselfrequenz sind die Häufigkeit des Schlüsseleinsatzes, das relevante Bedrohungspotential und die Sicherheit der lokalen Aufbewahrung der Schlüssel.

Je nach verwendetem Verfahren sind für jede einzelne Kommunikationsverbindung neue Schlüssel auszuhandeln, also Sitzungsschlüssel (Session Keys) zu verwenden. Dies sollte natürlich für die Benutzer unbemerkt durch die Verfahren gesteuert werden. Schlüsselwechsel bedeutet hierbei den Austausch der Masterkeys, die die Grundlage bilden, auf der die Sitzungsschlüssel gebildet werden, und sollte natürlich auch regelmäßig durchgeführt werden.

Besteht der Verdacht, dass ein verwendeter Schlüssel offen gelegt wurde, so ist dieser Schlüssel nicht mehr zu verwenden und alle Beteiligten sind zu informieren. Bereits mit diesem Schlüssel verschlüsselte Informationen sind zu entschlüsseln und mit einem anderen Schlüssel zu verschlüsseln.

**Schlüsselvernichtung**

Nicht mehr benötigte Schlüssel (z. B. Schlüssel, deren Gültigkeitsdauer abgelaufen sind) sind auf sichere Art zu löschen bzw. zu vernichten (z. B. durch mehrfaches Löschen/Überschreiben und/oder mechanische Zerstörung des Datenträgers). Auf Produkte mit unkontrollierbarer Schlüsselablage sollte generell verzichtet werden.

Prüffragen:

- Werden kryptographische Schlüssel in sicherer Umgebung unter Einsatz eines geeigneten Schlüsselgenerators erzeugt?
- Werden für Verschlüsselung und Signaturbildung unterschiedliche kryptographische Schlüssel benutzt?
- Wird bei der Schlüsselinstallation die authentische Herkunft und die Integrität der Schlüsseldaten überprüft?
- Werden im Zuge der Installation eines Kryptoproduktes alle voreingestellten kryptographischen Schlüssel geändert?
- Wurde ein geeignetes Schlüsselmanagement etabliert?
- Sind die Zugriffs- und Vertretungsrechte bei den genutzten Kryptoprodukten geregelt?
- Werden die verwendeten kryptographischen Schlüssel hinreichend häufig gewechselt?
- Gibt es eine festgelegte Vorgehensweise für den Fall, dass ein Schlüssel offen gelegt wurde?
- Gibt es eine festgelegte Vorgehensweise für das sichere Löschen und Vernichten von Schlüsseln?

# M 2.47 Ernennung eines Fax-Verantwortlichen

**Verantwortlich für Initiierung:** Vorgesetzte, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Innerer Dienst

Für jedes Faxgerät ist ein Verantwortlicher zu benennen, der folgende Aufgaben übernehmen muss:

- Verteilung der eingehenden Faxsendungen an die Empfänger,
- Koordination der Versorgung des Faxgerätes mit notwendigen Verbrauchsgütern,
- geeignete Entsorgung von Fax-Verbrauchsgütern,
- Löschen von Restinformationen im Faxgerät vor Wartungs- und Reparaturarbeiten,
- Beaufsichtigung von Wartungs- und Reparaturarbeiten (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*),
- gelegentliche Kontrolle programmierter Zieladressen und Protokolle, insbesondere nach Wartungs- und Reparaturarbeiten,
- Ansprechpartner bei Problemen bei der Faxnutzung.

Prüffragen:

- Ist für jedes Faxgerät ein Verantwortlicher benannt?
- Werden Restinformationen in Faxgeräten gelöscht, bevor sie Dritten zugänglich gemacht werden?

# M 2.48 Festlegung berechtigter Faxbediener

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Innerer Dienst

Die Berechtigung zur Bedienung des Faxgerätes ist auf einen ausgewählten Kreis zuverlässiger Mitarbeiter zu beschränken. Diese Mitarbeiter sind in die korrekte Handhabung des Gerätes einzuweisen und mit den erforderlichen Sicherheitsmaßnahmen vertraut zu machen. Jeder berechtigte Benutzer sollte darüber unterrichtet werden, wer das Gerät bedienen darf und wer der Fax-Verantwortliche ist. Darüber hinaus sollte am Faxgerät eine verständliche Bedienungsanleitung ausliegen.

Durch die Einschränkung des Faxbedienerkreises auf die für den operativen Einsatz notwendige Mindestzahl wird erreicht, dass die Anzahl der Personen, die eingehende Faxsendungen mitlesen können, begrenzt ist.

Prüffragen:

- Ist die Berechtigung zur Bedienung des Faxgerätes auf einen ausgewählten Kreis zuverlässiger Mitarbeiter beschränkt?
- Sind die berechtigten Mitarbeiter zur Bedienung des Faxgerätes in die korrekte Handhabung des Faxgerätes eingewiesen und mit den erforderlichen Sicherheitsmaßnahmen vertraut?
- Liegt am Faxgerät eine verständliche Bedienungsanleitung aus?

# M 2.49 Beschaffung geeigneter Faxgeräte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Beschaffungsstelle

Bei Neuanschaffungen von Faxgeräten sollte darauf geachtet werden, dass übliche Standardsicherheitsfunktionen implementiert sind wie:

- Austausch einer Teilnehmerkennung,
- Sendebericht,
- Journalführung.

Unter Beachtung des Preis-/Leistungsverhältnisses sind darüber hinaus folgende zusätzliche Sicherheitsfunktionen zu begrüßen:

- passwortgeschützter Zugang,
- passwortgeschützter Pufferspeicher,
- Einrichten einer geschlossenen Benutzergruppe,
- Ausschließen bestimmter Faxanschlüsse von Versendung oder Empfang.

Prüffragen:

- Wird bei Neubeschaffung von Faxgeräten auf implementierte Standardsicherheitsfunktionen geachtet?
- Wird bei der Beschaffung von Faxgeräten auf angemessene zusätzliche Sicherheitsfunktionen unter Berücksichtigung des Schutzbedarfs geachtet?

# M 2.50 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Fax-Verantwortlicher

Alle Fax-Verbrauchsgüter, aus denen Informationen über Faxtexte gewonnen werden könnten, wie z. B. Zwischenträgerfolien oder fehlerhafte Ausdrucke, sollten vor der Entsorgung vernichtet oder durch eine zuverlässige Fachfirma entsorgt werden.

Das gleiche gilt beim Austausch informationstragender Ersatzteile, wie z. B. photo-elektrische Trommeln.

Wartungsfirmen, die Faxgeräte periodisch warten oder reparieren, sind auf eine entsprechende Handhabung zu verpflichten und ggf. zu kontrollieren.

Prüffragen:

- Werden Fax-Verbrauchsgüter und -Ersatzteile, aus denen Informationen über Faxtexte gewonnen werden können, sicher entsorgt?

# M 2.51 Fertigung von Kopien eingehender Faxsendungen

**Verantwortlich für Initiierung:** Fax-Verantwortlicher
**Verantwortlich für Umsetzung:** Benutzer

Ein Fax auf Thermopapier kann nach einiger Zeit stark verblassen oder schwarz werden. Daher sollten von Faxen auf Thermopapier, deren Informationsgehalt länger benötigt wird, Kopien auf Normalpapier erstellt werden.

Prüffragen:

- Faxgeräte mit Thermopapier: Wird eine Kopie auf Normalpapier erstellt, wenn der der Informationsgehalt des Fax länger benötigt wird?

# M 2.52 Versorgung und Kontrolle der Verbrauchsgüter

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Innerer Dienst

Viele im Büroalltag eingesetzte Geräte wie Fax, Drucker, etc. sind auf bestimmte Verbrauchsgüter (z. B. Papier, Toner, Datensicherungsbänder) angewiesen, um funktionieren zu können. Daher muss die Versorgung mit diesen Verbrauchsgütern vor Ort sichergestellt sein. Es sollten klare und eindeutige Regelungen existieren, welche Verbrauchsgüter von wem nachgefüllt bzw. bestellt werden.

Bestimmte Ressourcen dürfen nicht von jedem Mitarbeiter nachgefüllt oder beschafft werden, sondern nur von autorisierten Personen, beispielsweise sehr teure Produkte oder technisch komplexe Komponenten.

Alle Benutzer sollten informiert sein, wer zu benachrichtigen ist, wenn Verbrauchsgüter nachbeschafft oder aufgefüllt werden müssen. Für jede Sorte von Verbrauchsmaterial sollte jemand benannt werden, der für Versorgung und Kontrolle verantwortlich ist. Dieser Verantwortliche sorgt dafür, dass

- regelmäßig geprüft wird, ob ausreichende Vorräte vorhanden sind und vor Ort nachgefüllt werden muss,
- die Beschaffungsstelle rechtzeitig benachrichtigt wird, wenn Verbrauchsmaterial nachbestellt werden muss,
- verbrauchte oder leere Verbrauchsmaterialien geeignet entsorgt werden, und
- die Verbrauchsmaterialien am Gerät ausgetauscht werden, falls dies nicht durch die Benutzer erfolgen soll.

Die Versorgung mit Verbrauchsgütern ist von der Beschaffungsstelle ausreichend sicherzustellen.

Prüffragen:

- Ist geregelt, wer welche Verbrauchsgüter nachfüllt bzw. bestellt?
- Sind die Benutzer darüber informiert, wer zu benachrichtigen ist, wenn Verbrauchsgüter nachbeschafft oder aufgefüllt werden müssen?

# M 2.53 Abschalten des Faxgerätes außerhalb der Bürozeiten

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fax-Verantwortlicher

Um die Brandgefahr, die von Faxgeräten immer ausgehen kann, zu reduzieren, sollten Geräte, die außerhalb der Arbeitszeit nicht benötigt werden (Abteilungs-Faxgerät, persönliches Gerät) zum Dienstschluss abgeschaltet werden. Damit kann auch erreicht werden, dass eingehende Faxsendungen nicht unkontrolliert längere Zeit im Faxgerät verbleiben. Realisierbar ist die Abschaltung auf einfache Weise durch Zeitschaltuhren, die die Stromversorgung des Gerätes auf die üblichen Bürozeiten einschränken.

Für später eingehende Sendungen kann ein anderer (möglichst ständig kontrollierter) Fax-Anschluss benannt werden oder bei modernen TK-Anlagen eine Anrufumleitung eingerichtet werden.

Gleichzeitig kann mit dem Abschalten des Faxgerätes die Überlastung des Gerätes aufgrund eines technischen Versagens oder aufgrund beabsichtigter Massenfaxsendungen außerhalb der Bürozeit verhindert werden.

Das Abschalten sollte unterbleiben, wenn für die Verfügbarkeit des Gerätes besondere Anforderungen bestehen, die bei den Ausweichlösungen nicht umgesetzt werden können.

Prüffragen:

- Werden Faxgeräte außerhalb der Bürozeit abgeschaltet, wenn sie ansonsten nicht benötigt werden?

# M 2.54 Beschaffung geeigneter Anrufbeantworter

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.55 Einsatz eines Sicherungscodes

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.56 Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.57 Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.58 Begrenzung der Sprechdauer

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.59 Auswahl eines geeigneten Modems in der Beschaffung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Beschaffungsstelle

Bei der Beschaffung eines Modems sind folgende Punkte zu beachten:

**Modem-Zulassung**

Ein Modem, dass in Deutschland an das öffentliche Telekommunikationsnetz angeschlossen werden soll, muss eine BZT-Zulassung (früher ZZF-Zulassung, davor FTZ-Zulassung, im allgemeinen Sprachgebrauch auch Post-Zulassung genannt) haben. Hinweis: Entgegen der Angaben in vielen Modem-Handbüchern muss die Inbetriebnahme eines zugelassenen Modems nicht mehr der Telekom gemeldet werden.

**Bauweise**

Ein internes Modem bietet den Vorteil, dass die Modem-Konfiguration nur über den Rechner, in dem es eingebaut ist, geändert werden kann. Verfügt der Rechner über Zugangs- oder Zugriffsschutzmechanismen, können sie zum Schutz der Modem-Konfigurationsdaten eingesetzt werden. Gleichzeitig kann damit die Nutzung des Modems auf autorisierte Personen beschränkt werden. Manipulationen am Modem sind durch den Einbau im Rechner erschwert. Bei vernetzten Systemen, die nicht über derartige Schutzmechanismen verfügen (einige Peer-to-Peer-Netze), besteht der Nachteil eines internen Modems darin, dass das Modem unkontrolliert von allen Arbeitsplätzen genutzt werden kann.
Ein externes Modem kann nach Nutzung verschlossen aufbewahrt werden. Es bietet außerdem den Vorteil, dass es üblicherweise über diverse Anzeigen sowie den Modem-Lautsprecher über den aktuellen Status informieren kann. Über den Modem-Lautsprecher kann auch gehört werden, ob von extern eine Verbindung aufgebaut wird oder ob eine Applikation unaufgefordert versucht, Informationen über die Installation und die System-Konfiguration an den Hersteller zu übertragen. Ein weiterer Vorteil eines externen Modems ist, dass es unabhängig vom IT-System nur für die jeweilige Datenübertragung eingeschaltet werden kann und somit z. B. sichergestellt werden kann, dass die letzte Verbindung getrennt worden ist und dass keine Verbindung von außerhalb aufgebaut werden kann. Nachteilig ist, dass ein externes Modem zur Manipulation der Konfigurationsdaten oder zum Auslesen gespeicherter Passwörter einfach an ein nicht geschütztes IT-System angeschlossen werden kann.
PCMCIA-Modems bieten aufgrund der Baugröße den Vorteil, dass sie nach Nutzung einfach verwahrt werden können. Eine sichere Aufbewahrung verhindert, dass sie zur Manipulation an ungeschützte Rechner angeschlossen werden.

**Übertragungsgeschwindigkeit**

Je höher die Übertragungsgeschwindigkeit eines Modems ist, desto geringer sind die Kosten für die Übertragung großer Datenmengen aufgrund der Zeiteinsparung.
Zunächst ist zu klären, welche Übertragungsgeschwindigkeiten für den gewünschten Einsatzzweck notwendig ist. Ausreichend sind z. B. bei ASCII-Terminalemulation 2400 bit/sec, bei Faxübertragung 9600 bit/sec, bei Datex-J (T-Online) zurzeit 14400 bit/sec. Für Datenübertragung großen Ausmaßes

sind die aktuell größtmöglichen Übertragungsgeschwindigkeiten einzusetzen. Übertragungsgeschwindigkeiten von mehr als 2400 bit/sec erschweren darüber hinaus das Abhören erheblich.
Anschließend muss bei Geschwindigkeiten über 9600 bit/sec überprüft werden, ob die Schnittstelle des IT-Systems, an dem das Modem betrieben werden soll, höhere Geschwindigkeiten zulässt.

Bei der Auswahl des Modems sollte beachtet werden, dass die Leistungsmerkmale, die für die tatsächlich erreichte Übertragungsgeschwindigkeit ausschlaggebend sind, genormt sind. Dies sind zum einen Normen für die Übertragungsgeschwindigkeit wie V.32bis für 14400 bit/sec und zum anderen Protokolle zur Übertragungsoptimierung durch Datenkompression und Fehlerkorrektur wie MNP 5 oder V.24bis.

**Befehlssatz**

Die meisten Modems arbeiten heute nach dem herstellerabhängigen Hayes-Standard (auch AT-Standard genannt). Aufgrund der weiten Verbreitung dieses Standards kann bei Einsatz eines Modems, das diesen Standard beherrscht, davon ausgegangen werden, dass die Kommunikation mit anderen Modems meist problemlos möglich ist. Bei der Anschaffung von Modems der neuesten Generation sollte bedacht werden, dass die versprochenen hohen Übertragungsraten oftmals nur erreicht werden können, wenn Geräten desselben Herstellers auf beiden Seiten eingesetzt werden.

**Handbuch**

Ein gut lesbares und ausführliches Handbuch ist zur schnellen Installation und bestmöglichen Konfiguration eines Modems wichtig.

**Sicherheitsmechanismen**

Es gibt vielfältige Sicherheitsmechanismen, die in Modems integriert sein können wie Passwortmechanismus oder Callback-Funktion. Einige Modems bieten sogar die Möglichkeit, die übertragenen Daten zu verschlüsseln.

Die Anschaffung eines Modems mit Verschlüsselungsoption ist vorteilhaft, wenn regelmäßig Übertragungen großer Datenmengen innerhalb einer Organisation mit verstreuten Liegenschaften durchgeführt werden sollen. Diese Online-Verschlüsselung bedingt einen geringeren organisatorischen Aufwand als das Verschlüsseln der Daten mittels Zusatzprodukten. Generelle Aussagen zur Sicherheit der eingesetzten Algorithmen können nicht gemacht werden. Für den IT-Grundschutz bietet der DES-Algorithmus bei entsprechendem Schlüsselmanagement ausreichende Sicherheit.

Die vielfach angebotene Callback-Funktion bietet unter Sicherheitsgesichtspunkten den Vorteil, dass auf einfache Weise unautorisierte Anrufer abgewiesen werden können (siehe auch M 5.30 *Aktivierung einer vorhandenen Callback-Option*).

Prüffragen:

- Ist sichergestellt, dass Kommunikationskomponenten wie Modems nicht unter Umgehung der offiziellen Genehmigungswege beschafft werden?

# M 2.60 Sichere Administration eines Modems

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Der sichere Einsatz eines Modems bedingt einige administrative Maßnahmen:

- Die Telefonnummer eines Modem-Zugangs darf nur den Kommunikationspartnern bekanntgegeben werden, um den Zugang vor Einwählversuchen zu schützen. Sie darf nicht im Telefonverzeichnis der Institution erscheinen. Es sollten regelmäßig Dial-up-Tests durchgeführt werden, um zu überprüfen, ob es Telefonnummern gibt, unter denen von extern IT-Systeme oder Faxgeräte angewählt werden können, die aber nicht dafür freigegeben worden sind.
- Nur berechtigte Benutzer dürfen Zugriff auf Modems bzw. die Kommunikationssoftware zur Datenübertragung erhalten. Ist ein Modem in einen Netzserver integriert, können Benutzer von ihren Arbeitsplatzrechnern auf das Modem zugreifen. Dann darf ein Zugriff auf die Kommunikationssoftware nur den Benutzern möglich sein, die für die Datenübertragung berechtigt sind (siehe auch M 2.42 *Festlegung der möglichen Kommunikationspartner*).
- Außerdem müssen regelmäßig die Einstellungen des Modems und der Kommunikationssoftware überprüft werden, insbesondere ob die sicherheitsrelevanten Einstellungen noch aktiviert und wirksam sind. Die per Modem durchgeführten Datenübertragungen sollten protokolliert werden.
- Es muss sichergestellt sein, dass das Modem die Telefonverbindung unterbricht, sobald der Benutzer sich vom System abmeldet. Bei einem Stand-alone-System kann dies dadurch realisiert sein, dass das Modem nur solange mit dem Telefonnetz verbunden ist, wie es für die Datenübertragung eingesetzt wird, und es anschließend ausgeschaltet bzw. von der Leitung getrennt wird. Bei einem im Netzserver integrierten Modem muss dies über die Konfiguration sichergestellt werden. Ein externes Modem kann einfach ausgeschaltet werden. Außerdem müssen alle Benutzer darauf hingewiesen werden, dass nach der Datenübertragung auch das Kommunikationsprogramm zu beenden ist.
- Es muss außerdem darauf geachtet werden, dass nach einem Zusammenbruch der Modem-Verbindung externe Benutzer automatisch vom IT-System ausgeloggt werden. Andernfalls kann der nächste Anrufer unter dieser Benutzer-Kennung weiterarbeiten, ohne sich einzuloggen.

Es muss regelmäßig überprüft werden, ob die gewählten Einstellungen noch aktiviert und wirksam sind, um eine unbefugte Nutzung des Modems wirksam zu verhindern.

Prüffragen:

- Haben nur berechtigte Benutzer Zugriff auf Modems bzw. die Kommunikationssoftware zur Datenübertragung per Modem?
- Wird regelmäßig überprüft, ob die gewählten Einstellungen noch aktiviert und wirksam sind?
- Werden die durchgeführten Datenübertragungen von Modems protokolliert?
- Ist sichergestellt, dass Modems die Telefonverbindung unterbrechen, sobald der jeweilige Benutzer sich vom System abmeldet?
- Werden Benutzer abgemeldet, wenn die Modemverbindung getrennt wird?

# M 2.61 Regelung des Modem-Einsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Es ist festzulegen:

- wer der Verantwortliche für den sicheren Betrieb des Modems ist (beispielsweise im Stand-alone Einsatz der IT-Benutzer, in vernetzten Systemen der Administrator),
- wer das Modem benutzen darf,
- in welchen Fällen vertrauliche Informationen bei der Übertragung verschlüsselt werden sollten,
- in welchen Fällen durchgeführte Datenübertragungen zu protokollieren sind (z. B. bei Übermittlung personenbezogener Daten). Bietet die Kommunikationssoftware Protokollierungsfunktion an, sollte diesen im sinnvollen Rahmen genutzt werden.

Alle Login-Vorgänge, ob erfolgreich oder erfolglos, müssen protokolliert werden. Korrekt eingegebene Passwörter sollten nicht mitprotokolliert werden, es ist aber zu überlegen, die bei erfolglosen Login-Versuchen eingegebenen Passwörter mitzuprotokollieren, um Passwort-Attacken zu entdecken.

Indizien für Passwort-Attacken können z. B. sein: häufige erfolglose Login-Versuche für einen Benutzer, erfolglose Login-Versuche immer vom selben Anschluss, Versuche sich auf verschiedene Benutzernamen anzumelden während einer Verbindung oder von einem Anschluss.

Nach dem Verbindungsaufbau muss dem Anrufenden ein Anmelde-Prompt angezeigt werden. Dabei sollte darauf geachtet werden, dass vor der erfolgreichen Anmeldung möglichst wenig Informationen über das angewählte IT-System weitergegeben werden. Es sollte weder die Art der eingesetzten Hardware noch des Betriebssystems gegeben werden. Der Anmelde-Prompt sollte den Namen des IT-Systems und/oder der Organisation enthalten, einen Hinweis, dass alle Verbindungen protokolliert werden und eine Eingabeaufforderung für Benutzername und Passwort. Bei erfolglosen Anmeldeversuchen darf keine Ursache angezeigt werden (falscher Benutzername, falsches Passwort).

**Trennung Dial-In / Dial-Out**

Für ein- bzw. abgehende Verbindungen sollten getrennte Leitungen und Modems benutzt werden. Ein Anrufer sollte keine Möglichkeit haben, sich über das angewählte IT-System wieder nach außen verbinden zu lassen. (Wenn dies für Außendienstmitarbeiter unbedingt notwendig ist, muss dem eine starke Authentisierung vorangehen, z. B. über Chipkarten.) Ansonsten besteht die Gefahr, dass Hacker den Zugang missbrauchen, zum einen um teure Fernverbindungen aufzubauen und zum anderen um ihre Spuren zu verwischen.

Beim Callback sollte für den Rückruf ein anderes Modem oder eine andere Leitung benutzt werden, als das anrufende Modem benutzt hat (siehe auch M 5.44 *Einseitiger Verbindungsaufbau*).

Prüffragen:

- Sind die Rahmenbedingungen für die Nutzung von Modems geregelt?
- Sind den Mitarbeitern die Regelungen für die Nutzung von Modems bekannt?

# M 2.62 Software-Abnahme- und Freigabe-Verfahren

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Der Einsatz von IT zur Aufgabenbewältigung setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei arbeitet, da die Kontrolle der Einzelergebnisse in den meisten Fällen nicht mehr zu leisten ist. Im Zuge eines Software-Abnahme-Verfahrens wird deshalb überprüft, ob die betrachtete Software fehlerfrei arbeitet, das heißt, ob die Software die erforderliche Funktionalität zuverlässig bereitstellt und ob sie darüber hinaus keine unerwünschten Nebeneffekte hat. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Stelle wird die Erlaubnis erteilt, die Software zu nutzen. Gleichzeitig übernimmt diese Stelle damit auch die Verantwortung für das IT-Verfahren, dass durch die Software realisiert wird.

Bei der Software-Abnahme unterscheidet man sinnvollerweise zwischen Software, die selbst oder im Auftrag entwickelt wurde, und Standardsoftware, die nur für den speziellen Einsatzzweck angepasst wird.

**Abnahme von selbst- oder im Auftrag entwickelter Software**

Bevor der Auftrag zur Software-Entwicklung intern oder extern vergeben wird, muss die Anforderungsdefinition für die Software erstellt sein, aus der dann das Grob- und Feinkonzept für die Realisierung entwickelt wird. Anhand dieser Dokumente erstellt die fachlich zuständige Stelle, nicht die für die Software-Entwicklung zuständige Stelle, im allgemeinen einen Abnahmeplan.

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet und der Abgleich zwischen berechnetem und erwartetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.

Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- die Testfälle werden von der fachlich zuständigen Stelle entwickelt,
- für Testfälle werden keine Daten des Wirkbetriebs benutzt,
- Testdaten, insbesondere wenn sie durch Kopieren der Wirkdaten erstellt werden, dürfen keine vertraulichen Informationen beinhalten; personenbezogene Daten sind zu anonymisieren oder zu simulieren,
- die Durchführung der Tests darf keine Auswirkungen auf den Wirkbetrieb haben; nach Möglichkeit sollte ein logisch oder physikalisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn:

- schwerwiegende Fehler in der Software festgestellt werden,
- Testfälle auftreten, in denen die erwarteten Ergebnisse nicht mit den berechneten übereinstimmen und
- Benutzerhandbücher oder Bedienungsanleitungen nicht vorhanden oder von nicht ausreichender Qualität sind und
- die Software, unter anderem der Quellcode und die Abläufe, nicht oder nicht ausreichend dokumentiert ist.

Die Ergebnisse der Abnahme sind schriftlich festzuhalten. Die Dokumentation des Abnahmeergebnisses sollte umfassen:

- Bezeichnung und Versionsnummer der Software und gegebenenfalls des IT-Verfahrens,
- Beschreibung der Testumgebung,
- Testfälle und Testergebnisse und
- Abnahmeerklärung.

**Abnahme von Standardsoftware**

Wird Standardsoftware beschafft, so sollte auch diese einer Abnahme und einer Freigabe unterzogen werden. In der Abnahme sollte überprüft werden, ob

- die Software frei von Computer-Viren ist,
- die Software kompatibel zu den anderen eingesetzten Produkten ist,
- die Software in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind,
- die Software komplett einschließlich der erforderlichen Handbücher ausgeliefert wurde und
- die geforderte Funktionalität erfüllt wird.

**Freigabe-Verfahren**

Ist die Abnahme der Software erfolgt, muss die Software für die Nutzung freigegeben werden. Dazu ist zunächst festzulegen, wer berechtigt ist, Software freizugeben. Die Freigabe der Software ist schriftlich festzulegen und geeignet zu hinterlegen.

Die Freigabeerklärung sollte umfassen:

- Bezeichnung und Versionsnummer der Software und gegebenenfalls des IT-Verfahrens,
- Bestätigung, dass die Abnahme ordnungsgemäß vorgenommen wurde,
- Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis,...),
- Freigabedatum, ab wann die Software eingesetzt werden darf und
- die eigentliche Freigabeerklärung.

Falls IT-technisch möglich, muss verhindert werden, dass Software nach der Freigabe unbemerkt verändert oder manipuliert werden kann, beispielsweise durch geeignete Verfahren zum Integritätsschutz. Andernfalls müssen geeignete organisatorische Regelungen festgelegt werden, um Änderungen an der Software zu verhindern bzw. zeitnah festzustellen.

Auch nach intensiven Abnahmetests kann es vorkommen, dass im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall ist festzulegen, wie in einem solchen Fehlerfall verfahren werden soll (Ansprechpartner, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle).

Für weiterführende Erklärungen siehe Baustein B 1.10 *Standardsoftware*.

Prüffragen:

- Gibt es für sämtliche eingesetzte Software eine Abnahmebestätigung und eine Freigabeerklärung?
- Existiert ein Verfahren, welches die Fehlerbehebung während des laufenden Einsatzes definiert?

# M 2.63 Einrichten der Zugriffsrechte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Verantwortliche der einzelnen Anwendungen

Arbeiten mit einem IT-System mehrere Benutzer, so muss durch eine ordnungsgemäße Administration der Zugriffsrechte sichergestellt werden, dass die Benutzer das IT-System nur gemäß ihren Aufgaben nutzen können.

Vorausgesetzt sei, dass von den Fachverantwortlichen die Zugangs- und Zugriffsberechtigungen für die einzelnen Funktionen festgelegt wurden (siehe M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*). Anschließend werden die Benutzer des IT-Systems den einzelnen Funktionen zugeordnet. Die Ergebnisse sind schriftlich zu dokumentieren.

Der Administrator muss dann das IT-System so konfigurieren, dass diese Benutzer Zugang zum IT-System erhalten und mit den ihnen zugewiesenen Zugriffsrechten nur ihre Aufgaben wahrnehmen können. Bietet das IT-System keine Möglichkeit, Zugriffsrechte zuzuweisen (z. B. beim DOS-PC mit mehreren Benutzern), so ist ein Zusatzprodukt zu diesem Zweck einzusetzen (siehe z. B. M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*).

Lässt das IT-System es zu, so sind die sinnvoll einsetzbaren Protokollfunktionen zur Beweissicherung durch den Administrator zu aktivieren. Dazu gehören erfolgreiche und erfolglose An- und Abmeldevorgänge, Fehlermeldungen des Systems, unerlaubte Zugriffsversuche.

Für den Vertretungsfall muss der Administrator vorab kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist. Erst dann darf er die erforderlichen Zugriffsrechte im akuten Vertretungsfall einrichten.

Prüffragen:

- Stellt die Konfiguration des IT-Systems sicher, dass Benutzer nur die Ihnen zugewiesenen Aufgaben erledigen können?
- Falls das IT-System keine Möglichkeit bietet, Zugriffsrechte zuzuweisen: Kommt ein zusätzliches Sicherheitsprodukt zum Einsatz, das sicherstellt, dass Zugriffe nur gemäß der vorher definierten Vorgaben erfolgen können?
- Wurden Protokollfunktionen, z. B. für erfolglose Anmeldevorgänge, unerlaubte Zugriffsversuche sowie Systemfehler aktiviert?
- Bei Vertretungslösungen: Wird die Autorisierung des Vertreters vor Erteilung von Zugriffsrechten durch den Administrator geprüft?

# M 2.64 Kontrolle der Protokolldateien

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Revisor, Verantwortliche der einzelnen Anwendungen

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Ist es personell oder technisch nicht möglich, die Rolle eines unabhängigen Revisors für Protokolldateien zu implementieren, kann ihre Auswertung auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich ist. Das Ergebnis der Auswertung sollte daher dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Die regelmäßige Kontrolle dient darüber hinaus auch dem Zweck, durch die anschließende Löschung der Protokolldaten ein übermäßiges Anwachsen der Protokolldateien zu verhindern. Je nach Art der Protokolldaten kann es sinnvoll sein, diese auf externen Datenträgern zu archivieren.

Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (siehe § 14 Abs. 4 BDSG und M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Organisation abgestimmt werden.

Aus verschiedenen gesetzlichen Regelungen können sich einerseits Mindestaufbewahrungsfristen, aber andererseits auch Höchstaufbewahrungsfristen an Protokolldaten ergeben. So kann durch datenschutzrechtliche Regelungen eine Löschung erforderlich sein (siehe dazu auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Für bestimmte Protokolldaten gelten aber unter Umständen gesetzliche Mindestaufbewahrungsfristen, z. B. wenn sie Aufschluss über betriebswirtschaftliche Vorgänge geben. Diese Fristen müssen auf jeden Fall eingehalten werden. Vor der Löschung von Protokolldaten ist daher sorgfältig zu prüfen, ob entsprechende Rechtsvorschriften zu beachten sind und ggf. welche Aufbewahrungsfristen sich daraus ergeben. Hierbei sollte die Rechtsabteilung beteiligt werden.

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passwörter zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?

- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzerwechsel stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?
- Gibt es auffallend lange Verbindungszeiten in öffentliche Netze hinein (siehe G 4.25 *Nicht getrennte Verbindungen*)?
- Wurde in einzelnen Netzsegmenten oder im gesamten Netz eine auffällig hohe Netzlast oder eine Unterbrechung des Netzbetriebes festgestellt (Hinweis auf Versuche, die Dienste des Netzes zu verhindern bzw. zu beeinträchtigen oder auf eine ungeeignete Konzeption bzw. Konfiguration des Netzes)?

Bei der Auswertung der Protokolldateien sollte besonderes Augenmerk auf alle Zugriffe gelegt werden, die unter Administratorkennungen durchgeführt wurden.

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfacher fehlerhafter Anmeldeversuch) hervorheben.

Das oben Gesagte gilt analog auch für die Erhebung von Auditdaten, da es sich dabei im Prinzip nur um die Protokollierung sicherheitskritischer Ereignisse handelt.

Prüffragen:

- Gibt es einen Verantwortlichen für die Auswertung von Protokolldaten?
- Werden die Ergebnisse der Auswertung dem IT-Sicherheitsbeauftragten oder einem anderen hierfür bestimmten Mitarbeiter vorgelegt?
- Existiert ein Konzept, das den Umfang und die Auswertung der Protokollierung festlegt?
- Werden die gesetzlichen Vorgaben in Bezug auf die Protokolldaten eingehalten?

# M 2.65 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Revisor

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die Benutzer von IT-Systemen sich regelmäßig nach Aufgabenerfüllung abmelden oder ob mehrere Benutzer unter einer Kennung arbeiten.

Sollte festgestellt werden, dass tatsächlich mehrere Benutzer unter einer Kennung arbeiten, sind sie auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hinzuweisen. Gleichzeitig sollte der Sinn dieser Maßnahme erläutert werden, die im Interesse desr einzelnen Benutzer liegt.

Stellt sich heraus, dass die An- und Abmeldevorgänge zu zeitintensiv sind und trotz Aufforderung nicht akzeptiert werden, sollten alternative Maßnahmen diskutiert werden wie zum Beispiel:

- Das IT-System kann für bestimmte Zeitintervalle einem Benutzer zugeordnet werden, so dass in dieser Zeit andere Benutzer das IT-System nicht nutzen dürfen. Dies setzt voraus, dass der Arbeitsprozess dementsprechend zeitlich variabel ist.
- Es können zusätzliche IT-Systeme angeschafft werden, mit denen die quasiparallele Arbeit an einem IT-System vermieden werden kann. Wenn diese Geräte weggeschlossen werden, wenn sie benutzt werden, kann auch auf eine An- und Abmeldung für die Nutzungsintervalle verzichtet werden.
- Statt zeitaufwendigen mehrstufigen Authentisierungsverfahren könnten automatisierte Authentisierungsverfahren wie beispielsweise über RFID-basierte Token oder biometrische Verfahren eingesetzt werden.
- Wenn sich die Datenbestände der einzelnen Benutzer separieren lassen (beispielsweise Benutzer A bearbeitet die Daten A-L, Benutzer B die Daten M-Z), so sollten dafür unterschiedliche Zugriffsrechte eingeräumt werden.

Prüffragen:

- Wird regelmäßig überprüft, ob alle Benutzer ausschließlich unter ihrer eigenen Kennung arbeiten?
- Sofern Akzeptanzproblemen bezüglich des ordnungsgemäßen Benutzerwechsels bestehen: Werden alternative Maßnahmen untersucht?

# M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Beschaffungsstelle

Bei der Beschaffung von IT-Produkten, IT-Systemen und Sicherheitsdienstleistungen muss frühzeitig festgelegt werden, ob die bloße Zusicherung des Herstellers, Vertreibers oder Anbieters über implementierte Sicherheitsfunktionen und angebotene Dienstleistungen als ausreichend vertrauenswürdig anerkannt werden kann. Insbesondere bei einem hohen oder sehr hohen Schutzbedarf kann die Vertrauenswürdigkeit der Produkte und Dienstleistungen in Hinblick auf Informationssicherheit nur dadurch gewährleistet werden, dass unabhängige Prüfstellen die Produkte bzw. die Dienstleistungen und das Managementsystem des Dienstleisters untersuchen und bewerten (evaluieren). Darauf aufbauend kann dann ein Zertifikat erteilt werden.

**Zertifizierung von Produkten**

Allgemein anerkannte Grundlage der Evaluierung und Zertifizierung von Produkten bilden seit 1991 die europaweit harmonisierten "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" und seit 1998 die weltweit angestimmten "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik", kurz Common Criteria (CC). In Deutschland führt das BSI solche Zertifizierungen durch. Bei positivem Evaluationsergebnis und bei Einhaltung der Rahmenbedingungen von ITSEC bzw. der Common Criteria wird für das untersuchte Produkt oder System vom BSI als Zertifizierungsstelle ein Sicherheitszertifikat erteilt.

Aus dem dazugehörenden Zertifizierungsreport geht hervor, welche Funktionalität mit welcher Prüftiefe untersucht wurde und welche Bewertung vorgenommen wurde. Dabei reichen die Prüftiefe von Evaluationsstufe E 1 (geringste Prüftiefe) bis Evaluationsstufe E 6 (höchste Prüftiefe) bei den ITSEC bzw. von Vertrauenswürdigkeitsstufe EAL 1 (geringste Prüftiefe) bis Vertrauenswürdigkeitsstufe EAL 7 (höchste Prüftiefe) bei den CC. Dabei entspricht die Evaluationsstufe E 1 der ITSEC in etwa der Vertrauenswürdigkeitsstufe EAL 2 der CC usw. Zusätzlich wird die geprüfte Mechanismenstärke der Implementation der Sicherheitsfunktionen angegeben, die ein Maß für den Aufwand darstellt, der zum Überwinden der Sicherheitsfunktionen erforderlich ist. ITSEC und CC unterscheiden hier die Mechanismenstärken niedrig, mittel und hoch. Darüber hinaus werden Hinweise gegeben, welche Randbedingungen beim Einsatz des Produktes beachtet werden müssen.

Stehen bei der IT-Beschaffung mehrere Produkte mit angemessenem Preis-/Leistungsverhältnis zur Auswahl, so kann ein eventuell vorhandenes Sicherheitszertifikat als Auswahlkriterium positiv berücksichtigt werden. Hierbei sollten Sicherheitszertifikate insbesondere dann berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht (siehe M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*). Je höher dann die im Zertifikat angegebene Prüfungstiefe ist, desto mehr Vertrauen in Wirksamkeit und Korrektheit der Sicherheitsfunktionen kann dem Produkt entgegengebracht werden.

**Zertifizierung von Managementsystemen**

Vor dem Einkauf externer Dienstleistungen sollte geprüft werden, ob der Dienstleister über ein zertifiziertes Sicherheitsmanagementsystem verfügt. Im Rahmen der Zusammenarbeit mit externen Dienstleistern werden meistens viele interne und schützenswerte Informationen an diese weitergegeben. Die Informationen müssen von den Dienstleistern entsprechend ihres Schutzbedarfs geschützt werden. Es wird daher empfohlen, auf Dienstleister zurückzugreifen, die ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO 27001 auf der Basis von IT-Grundschutz vorweisen können. Bei Dienstleistungen, die hochverfügbar sein müssen, kann es sinnvoll sein, auf Dienstleister zurückzugreifen, welche ein zertifiziertes Notfallmanagement nach ISO 22301 nachweisen können.

**Zertifizierung von Personen**

Sollen IT-Dienstleistungen oder Sicherheitsdienstleistungen wie beispielsweise Beratungen zur Verbesserung eines Sicherheitsmanagementsystems beauftragt werden, sollte überlegt werden, hierfür auf entsprechend zertifizierte Personen zurückzugreifen.

Es gibt eine Vielzahl von Zertifikaten, mit denen Personen ihre Qualifikation in bestimmten Bereichen nachweisen können. Dabei gibt es diverse Personenzertifizierungen, die sich speziell an den Bereich Informationssicherheit bzw. Datenschutz richten. Hierzu gehören beispielsweise

- CISSP (Certified Information Systems Security Professional) und weitere Personenzertifikate von (ISC)², einer unabhängigen Vereinigung von Sicherheitsexperten weltweit
- TISP (TeleTrusT Information Security Professional), ein auf den deutschsprachigen Markt fokussiertes Expertenzertifikat von TeleTrusT, einem deutschen Sicherheitsverband
- CISA (Certified Information Systems Auditor) und CISM (Certified Information Security Manager) sind Zertifikate von ISACA, eines Berufsverbandes der IT-Revisoren und Sicherheitsmanager
- IT Security Coordinator nach ISO 17024
- Für die deutschen Behörden zertifiziert die Bundesakademie für öffentliche Verwaltung (BAköV) in Zusammenarbeit mit dem BSI "IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung".

Diese Zertifikate genießen insgesamt eine relativ hohe Anerkennung, da für deren Erwerb klar definierte, praxisnahe und nachvollziehbare Kompetenzen und Qualifikationen nachzuweisen sind. Im Vorfeld der Zertifizierung muss das hierfür notwendige Wissen durch Ausbildung und Berufserfahrung erworben werden, für die Aufrechterhaltung des Zertifikates muss außerdem nachgewiesen werden, dass sich die Inhaber regelmäßig in ihrem Fachgebiet weiterbilden.

**Zertifizierung von Dienstleistern**

Für bestimmte Formen von Dienstleistungen gibt es ebenfalls Zertifikate, mit denen Dienstleister die Qualität und Vergleichbarkeit ihrer Arbeitsergebnisse nachweisen können. Das BSI stellt beispielsweise Zertifikate für IS-Revisionen, IS-Beratungen und Penetrationstest aus. Sollten solche Dienstleistungen eingekauft werden, wird empfohlen, auf entsprechend zertifizierte Dienstleister zurückzugreifen.

**Übersichten**

Die Zertifizierungsstellen geben regelmäßig Übersichten heraus, welche Produkte und Dienstleister ein Zertifikat erhalten haben. Eine Zusammenstellung der vom BSI zertifizierten IT-Produkte, IT-Systeme, Informationssicherheitsmanagementsysteme, IS-Revisoren, IS-Berater und Penetrationstester findet sich auf der BSI-Webseite. Weiterhin veröffentlicht das BSI neu erteilte Zertifikate in der Zeitschrift KES, Zeitschrift für Informationssicherheit. Diese Informationen lassen sich ebenfalls von den Internetseiten des BSI abrufen.

Prüffragen:

- Wird beim Einsatz von Produkten mit hohem oder sehr hohem Schutzbedarf eine Zertifizierung nach Common Criteria in Betracht gezogen?

# M 2.67 Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.68 Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.69 Einrichtung von Standardarbeitsplätzen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Ein Standardarbeitsplatz ist gekennzeichnet durch einheitliche Hardware und Software sowie deren Konfiguration. Die Planung und Einrichtung erfolgt üblicherweise unter den Aspekten der Aufgabenstellung, Zuverlässigkeit, Ergonomie, Geschwindigkeit und Wartbarkeit. Sie wird durch fachkundiges Personal durchgeführt. Die Einrichtung von Standardarbeitsplätzen ist in mehrfacher Hinsicht vorteilhaft:

**Informationssicherheit:**
- Standardarbeitsplätze sind leichter in Sicherheitskonzepte einzubinden.
- Der Aufwand für die Dokumentation des IT-Bestandes wird reduziert.

**IT-Management:**
- Die Beschaffung größerer Stückzahlen gleicher Komponenten ermöglicht Preisvorteile.
- Der Einsatz nicht zulässiger Software ist einfacher festzustellen.
- Durch gleiche IT-Ausstattung entfallen "Neidfaktoren" zwischen den einzelnen Benutzern.

**IT-Nutzer:**
- Bei Gerätewechsel ist keine erneute Einweisung in die IT-Konfiguration erforderlich, Ausfallzeiten werden somit minimiert.
- Bei Fragen zu Hard- und Software können sich Anwender gegenseitig helfen.

**Systemadministration bei Installation und Wartung:**
- Eine gewissenhaft geplante und getestete Installation kann fehlerfrei und mit geringem Arbeitsaufwand installiert werden.
- Die einheitliche Arbeitsumgebung erleichtert den Benutzerservice (Wartung, Support und Pflege).

**Schulung:**
- Die Teilnehmer werden in dem Umfeld geschult, das sie am Arbeitsplatz vorfinden.

Prüffragen:

- Sind für die Organisation Standardarbeitsplätze definiert?
- Werden Abweichungen vom Standardarbeitsplatz nur in begründeten Ausnahmefällen zugelassen?

# M 2.70 Entwicklung eines Konzepts für Sicherheitsgateways

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Kopplung von lokalen Netzen mit globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot. Die lokale Vernetzung von Rechnersystemen sorgt dafür, dass von jedem Arbeitsplatzrechner aus auf die vielfältigen Informationen zugegriffen werden kann.

Diese Netzkopplung lässt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Datenfluss von außen in das zu schützende Netz stattfinden kann, sondern auch ein Datenabfluss in die andere Richtung. Darüber hinaus gefährdet die Möglichkeit, von einem entfernten Rechner aus (z. B. aus dem Internet) Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Integrität und die Verfügbarkeit der lokalen Rechner und dadurch indirekt auch die Vertraulichkeit der lokalen Daten.

Ein zu schützendes Teilnetz sollte daher nur dann an ein nicht-vertrauenswürdiges Netz angeschlossen werden, wenn dies unbedingt erforderlich ist. Dies gilt insbesondere für Anschlüsse an das Internet, das aufgrund der hohen Nutzerzahl das wohl am wenigsten vertrauenswürdige existierende Netz darstellt. Dabei ist auch zu prüfen, inwieweit das zu schützende Netz in Teilnetze segmentiert werden muss, weil bestimmte Rechner oder Bereiche des zu schützenden Netzes überhaupt nicht oder nur bedingt ans Internet angeschlossen werden sollten, und ob für die Kopplung mit dem Internet nicht ein Stand-alone-System ausreicht (siehe M 5.46 *Einsatz von Stand-alone-Systemen zur Nutzung des Internets* und Baustein B 3.208 *Internet-PC*).

Um die Sicherheit des zu schützenden Netzes zu gewährleisten, muss ein geeignetes Sicherheitsgateway eingesetzt werden. Damit ein Sicherheitsgateway effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein:

Das Sicherheitsgateway muss

- auf einer umfassenden Sicherheitsrichtlinie aufsetzen,
- im Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Der Anschluss an ein nicht-vertrauenswürdiges Netz darf erst dann erfolgen, wenn überprüft worden ist, dass mit dem gewählten Sicherheitsgateway-Konzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Es gibt verschiedene Arten, Sicherheitsgateways zu realisieren. Um festzustellen, welches Konzept für den Einsatzzweck am besten geeignet ist, muss zunächst geklärt werden, welche Sicherheitsziele durch das Sicherheitsgateway erfüllt werden sollen.

Beispiele für Sicherheitsziele sind:

- Schutz des vertrauenswürdigen (internen) Netzes gegen unbefugten Zugriff aus dem nicht-vertrauenswürdigen Netz,
- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität,

- Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit (Insbesondere gilt dies auch für Informationsserver, die Informationen aus dem internen Bereich für die Allgemeinheit zu Verfügung stellen.),
- Verfügbarkeit der Informationen des externen Netzes im zu schützenden internen Netz, (die Verfügbarkeit dieser Informationen muss aber gegenüber dem Schutz der lokalen Rechner und Informationen zurückstehen!),
- Schutz vor Angriffen, die auf IP-Spoofing beruhen, die Source-Routing Option, das Protokoll ICMP oder Routing-Protokolle missbrauchen,
- Schutz vor Angriffen durch neue sicherheitsrelevante Softwareschwachstellen. (Da die Anzahl der potentiellen Angreifer und deren Kenntnisstand bei einer Anbindung an das Internet als sehr hoch angesehen werden muss, ist dieses Sicherheitsziel von besonderer Bedeutung.)
- Schutz vor ungewünschtem Datenabfluss.

Auf den Sicherheitszielen aufbauend muss eine Sicherheitsrichtlinie erarbeitet werden, in der Aufgaben und Anforderungen an das Sicherheitsgateway festgelegt werden. Diese Sicherheitsrichtlinie muss in die Sicherheitsstrategie der jeweiligen Organisation eingebettet sein und daher mit dem Sicherheitsmanagement abgestimmt werden.

Die Entscheidungen, die bei der Erarbeitung der Sicherheitsrichtlinie für das Sicherheitsgateway getroffen wurden, sollten - ebenso wie die Gründe für diese Entscheidungen - nachvollziehbar dokumentiert werden.

Die Umsetzung der Sicherheitsrichtlinie für das Sicherheitsgateway erfolgt dann durch die Realisierung des Sicherheitsgateways, durch geeignete Auswahl von Hardware-Komponenten, Paketfilter und Application-Level-Gateway und die sorgfältige Festlegung und Einrichtung von Filterregeln.

Die Begriffe Paketfilter und Application-Level-Gateway sind für die weiteren Abschnitte wichtig und werden daher kurz erläutert, um Missverständnisse zu vermeiden:

- *Paketfilter* sind IT-Systeme mit spezieller Software, die die Informationen anhand der Header-Daten der unteren Schichten (Transportschicht oder Verbindungsschicht) des OSI-Modells filtern und anhand spezieller Regeln Pakete weiterleiten oder verwerfen (siehe M 2.74 *Geeignete Auswahl eines Paketfilters*). Paketfilter treffen ihre Entscheidungen beispielsweise anhand von Quell- und Ziel-Adressen oder -Ports eines Paketes, ohne den Inhalt zu berücksichtigen.
- Ein *Application-Level-Gateway* ist ein IT-System, das die Informationen der Anwendungsschicht (das heisst, den tatsächlichen Inhalt (die Nutzdaten) eines Paketes oder mehrerer zusammengehöriger Pakete) filtert und anhand spezieller Regeln Verbindungen oder auch bestimmte Kommandos verbieten oder erlauben kann (siehe M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*). Während Paketfilter auf Schicht 3 und 4 des OSI-Modells arbeiten, arbeiten Gateways auf Schicht 7. Ein Application-Level-Gateway ist im Allgemeinen auf einem IT-System implementiert, das ausschließlich für diese Aufgabe eingesetzt wird und dessen Befehlsumfang auf das Notwendigste reduziert ist.

Damit ein Sicherheitsgateway einen wirkungsvollen Schutz eines Netzes gegen Angriffe von außen darstellt, müssen einige grundlegende Voraussetzungen erfüllt sein:

- Die gesamte Kommunikation zwischen den beteiligten Netzen muss über das Sicherheitsgateway geführt werden. Dafür muss sichergestellt sein, dass das Sicherheitsgateway die einzige Schnittstelle zwischen den beiden Netzen darstellt. Es müssen Regelungen getroffen werden, dass kei-

ne weiteren externen Verbindungen unter Umgehung des Sicherheitsgateways geschaffen werden dürfen.
- Ein Sicherheitsgateway darf ausschließlich als schützender Übergang zum internen Netz eingesetzt werden. Daher dürfen auf einem Sicherheitsgateway selbst nur die dafür erforderlichen Dienste verfügbar sein und keine weiteren Dienste, wie z. B. ein Webserver, angeboten werden. Wie Informationsserver und andere Komponenten, die auf eigenen Systemen laufen, geeignet in ein Sicherheitsgateway integriert werden können, wird in einer Reihe eigener Maßnahmen für verschiedene Systeme beschrieben, siehe beispielsweise M 4.223 *Integration von Proxy-Servern in das Sicherheitsgateway* oder M 5.115 *Integration eines Webservers in ein Sicherheitsgateway*.
- Die Administration der Komponenten des Sicherheitsgateways darf nur über einen gesicherten Zugang möglich sein, also z. B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz (Administrationsnetz). Eine Konsole sollte in einem Serverraum aufgestellt sein (siehe B 2.4 *Serverraum*).
- Ein Sicherheitsgateway baut auf einer Sicherheitsrichtlinie auf, die für das zu schützende Netz definiert wurde, und gestattet nur die dort festgelegten Verbindungen. Diese Verbindungen müssen gegebenenfalls sehr detailliert (bis hin zu einer individuellen Angabe von IP-Adresse, Dienst, Zeit, Richtung und Benutzer getrennt) festgelegt werden können.
- Für die Konzeption und den Betrieb eines Sicherheitsgateways muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Sicherheitsgateways darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt oft viel Zeit in Anspruch. Der Administrator muss fundierte Kenntnisse der eingesetzten IT-Komponenten besitzen und entsprechend geschult werden.
- Die Benutzer des lokalen Netzes sollten durch den Einsatz eines Sicherheitsgateways möglichst wenig Einschränkungen hinnehmen müssen.

Ein Sicherheitsgateway kann das interne Netz vor vielen Gefahren beim Anschluss an das Internet schützen, aber nicht vor allen. Beim Aufbau eines Sicherheitsgateways und der Erarbeitung einer Sicherheitsrichtlinie sollte man sich daher die Grenzen eines Sicherheitsgateways verdeutlichen:

- Es werden Protokolle überprüft, nicht die übertragenen Informationen. Eine Protokollprüfung bestätigt beispielsweise, dass eine E-Mail mit ordnungsgemäßen Befehlen zugestellt wurde, kann aber keine Aussagen zum eigentlichen Inhalt der E-Mail machen.
- Die Filterung von aktiven Inhalten ist unter Umständen nur teilweise erfolgreich, da eventuell nicht alle verschiedenen Möglichkeiten zur Einbettung von aktiven Inhalten erkannt werden.
- Sobald ein Benutzer eine Kommunikation über ein Sicherheitsgateway herstellen darf, kann er über das verwendete Kommunikationsprotokoll beliebige andere Protokolle tunneln. Damit könnte ein Innentäter einem Externen den Zugriff auf interne Rechner ermöglichen oder selbst unerlaubte Protokolle nutzen. Die unberechtigte Nutzung von Tunnel-Verfahren ist meist nur schwer feststellbar.
- Eine Einschränkung der Internet-Zugriffe auf festgelegte Webserver ist praktisch unmöglich, da viele Webserver auch über Proxies nutzbar sind. Daher kann eine Sperrung bestimmter IP-Adressen leicht umgangen werden.
- Software zum Filtern anhand von Web-Adressen ("URLs") ist häufig noch unausgereift. Beispielweise ist es möglich, dass nicht alle Arten der Adressierung erfasst werden. Das folgende Beispiel mit dem BSI-Webserver soll aufzeigen, welche Möglichkeiten zur Adressierung vorhanden sind. Die Li-

ste ist bei weitem nicht vollständig, da einzelne Buchstaben auch durch Escape-Sequenzen dargestellt werden können.

*www.bsi.bund.de*
*www.bsi.de*
*194.95.176.226*
*3261051106*

- Zudem können URL-Filter durch Nutzung von "Anonymizern" umgangen werden.
- Die Filterung von Spam-Mails ist noch nicht ausgereift. Kein SMTP-Proxy kann zweifelsfrei feststellen, ob eine E-Mail vom Empfänger erwünscht ist oder nicht. Spam-Mails dürften frühestens dann verschwinden, wenn die Absender von E-Mails zweifelsfrei nachweisbar sind. Dies ist aber mit dem herkömmlichen Protokoll SMTP alleine nicht realisierbar.
- Sicherheitsgateways schützen nicht vor allen Denial-of-Service-Angriffen. Wenn ein Angreifer z. B. die Anbindung zum Provider lahmlegt, hilft auch das beste Sicherheitsgateway nicht. Außerdem gibt es immer wieder Fehler in der Implementierung von Protokollen auf Endgeräten, die von Sicherheitsproxies nicht abfangen werden können.
- Ein Sicherheitsgateway kann zwar einen Netzübergang sichern, er hat aber keinen Einfluss auf die Sicherheit der Kommunikation innerhalb der Netze!
- Auch die speziell unter Sicherheitsaspekten entwickelten Komponenten von Sicherheitsgateways können trotz großer Sorgfalt Programmierfehler enthalten.
- Sicherheitsgateways können nur begrenzt gegen eine absichtliche oder versehentliche Fehlkonfiguration der zu schützenden Clients und Server schützen.
- Eingebaute Hintertüren in der verwendeten Software können eventuell auch durch ein Sicherheitsgateway hindurch ausgenutzt werden. Im Extremfall kann die Software des Sicherheitsgateways selbst Hintertüren enthalten.
- Die korrekte Konfiguration der Komponenten des Sicherheitsgateways ist oft sehr anspruchsvoll. Fehler in der Konfiguration können zu Sicherheitslücken oder Ausfällen führen.
- Ist die Dokumentation der technischen Ausstattung des Sicherheitsgateways durch den Hersteller mangelhaft, so begünstigt dies Fehler bei Konfiguration und Administration.
- Wenn die Komponenten des Sicherheitsgateways falsch dimensioniert sind, kann die Verfügbarkeit beeinträchtigt werden. Wird beispielsweise der Rechner, auf dem ein HTTP-Sicherheitsproxy läuft, zu schwach dimensioniert (zu wenig Arbeitsspeicher, zu langsamer Prozessor), so kann dies die Geschwindigkeit des Internetzugriffes stark beeinträchtigen.
- Es kann nicht verhindert werden, dass Angreifer die Komponenten des Sicherheitsgateways mit Hilfe von Schwachstellenscannern analysieren.
- Ein Sicherheitsgateway kann nicht gegen die bewusste oder unbewusste Missachtung von Sicherheitsrichtlinien und -konzepten durch die Anwender schützen.
- Ein Sicherheitsgateway schützt nicht vor dem Missbrauch freigegebener Kommunikation durch Innentäter ("Insider-Angriffe").
- Ein Sicherheitsgateway schützt nicht vor Social Engineering.
- Werden mobile Endgeräte (Laptop, PDA etc.), die von Mitarbeitern auch extern benutzt werden, an das interne Netz angeschlossen, so kann auf diese Weise Schadsoftware (Viren, Würmer, Trojanische Pferde) in das vertrauenswürdige Netz eingeschleppt werden.

- Ein Sicherheitsgateway schützt auch nicht davor, dass Schadprogramme auf Austauschmedien, z. B. CD-ROM, Diskette, USB-Stick in das vertrauenswürdige Netz eingeschleppt werden.

Prüffragen:

- Besteht ein Konzept für das Sicherheitsgateway, das den Einsatzzweck und die Sicherheitsziele erfasst?
- Wird die Verwendung des Sicherheitsgateways für die gesamte Netzwerkkommunikation vorgeschrieben?
- Sind für die Administration der Komponenten des Sicherheitsgateways ausschließlich gesicherte Zugangsmöglichkeiten vorgesehen?

# M 2.71 Festlegung einer Policy für ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Policy des Sicherheitsgateways bestimmt das Verhalten des Sicherheitsgateways. Sie definiert, welche Informationen, Dienste und Protokolle das Sicherheitsgateway wie behandelt und wer sie nutzen darf. Die Policy ist nicht zu verwechseln mit der Sicherheitsrichtlinie für das Sicherheitsgateway, in der Vorgaben für den sicheren Betrieb des Sicherheitsgateway selbst gemacht werden.

**Kommunikationsanforderungen**

Für die Erstellung einer Policy muss als erstes festgelegt werden, welche Arten der Kommunikation mit dem äußeren Netz zugelassen werden. Bei der Festlegung der Kommunikationsanforderungenmüssen speziell die folgenden Fragen beantwortet werden:

- Welche Informationen dürfen durch das Sicherheitsgateway nach außen hindurch- bzw. nach innen hereingelassen werden?
- Welche Informationen soll das Sicherheitsgateway verdecken (z. B. die interne Netzstruktur oder die Benutzernamen)?
- Welche Authentisierungsverfahren sollen innerhalb des zu schützenden Netzes bzw. für das Sicherheitsgateway benutzt werden (z. B. Einmalpasswörter oder Chipkarten)?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider oder auch über einen Modem-Pool)?
- Welcher Datendurchsatz ist zu erwarten?

**Auswahl der Dienste**

Aus den Kommunikationsanforderungen wird dann abgeleitet, welche Dienste im zu sichernden Netz erlaubt werden.

Es muss unterschieden werden zwischen denjenigen Diensten, die für die Benutzer im zu schützenden Netz und denjenigen, die für externe Benutzer zugelassen werden.

Wenn zum Beispiel E-Mail empfangen werden soll (was im allgemeinen die Minimalanforderung ist) muss das Protokoll SMTP vom Sicherheitsgateway durchgelassen werden können.

In der Policy muss explizit festgelegt werden, welche Dienste für welche Benutzer und/oder Rechner zugelassen werden sollen und für welche Dienste Vertraulichkeit und/oder Integrität gewährleistet werden müssen. Es sollten nur die Dienste zugelassen werden, die unbedingt notwendig sind. Alle anderen Dienste müssen verboten werden. Dies muss auch die Voreinstellung sein: Alle Dienste, für die noch keine expliziten Regeln festgelegt wurden, dürfen nicht zugelassen werden.

Für jeden erlaubten Dienst muss festgelegt werden, welche Funktionen des verwendeten Protokolls genutzt werden dürfen und welche unterbunden werden sollen (z. B. der "PORT"-Befehl von FTP zur Verhinderung von aktivem FTP) und welche der übertragenen Nutzdaten gefiltert werden sollen (z. B. zur Kontrolle auf Computer-Viren).

Es muss festgelegt werden, zu welchen Wochentagen und Tageszeiten die bereitgestellten Dienste genutzt werden können.

Für kurzzeitige Änderungen (z. B. für Tests) oder neue Dienste sollten Ausnahmeregelungen vorgesehen werden.

Es sind Forderungen an die Filter zu stellen, und zwar einmal an die Paketfilter, die die Header-Informationen der Dienste der Schichten 3 und 4 des OSI-Schichtenmodells (IP, ICMP, ARP, TCP und UDP) verwenden, sowie an die Sicherheitsproxies, die die Informationen der Dienste der Anwendungsschicht (z. B. Telnet, FTP, SMTP, DNS, NNTP, HTTP) verwenden. Einen Überblick, was für einen sicheren Einsatz der einzelnen Protokolle und Dienste zu beachten ist, gibt M 5.39 *Sicherer Einsatz der Protokolle und Dienste*. Darauf aufbauend müssen Filterregeln formuliert werden (siehe M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln*).

**Organisatorische Regelungen**

Neben der sorgfältigen Aufstellung und Umsetzung der Filterregeln sind darüber hinaus folgende organisatorische Regelungen erforderlich:

- Es müssen Verantwortliche sowohl für den Entwurf als auch für die Umsetzung und das Testen der Filterregeln benannt werden. Es muss geklärt werden, wer befugt ist, die Filterregeln z. B. für Tests neuer Dienste zu verändern.
- Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.
- Die Benutzer müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdaten-Filterung umfassend informiert werden.
- Es ist empfehlenswert, den Benutzern eine Dokumentation zur Verfügung zu stellen, aus der hervorgeht, welche Dienste in welchem Umfang genutzt werden können und ob dabei besondere Dinge zu beachten sind.
- Angriffe auf das Sicherheitsgateway sollten nicht nur erfolgreich verhindert, sondern auch schnell erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Das Sicherheitsgateway sollte aber auch in der Lage sein, aufgrund von vordefinierten Ereignissen, wie z. B. häufigen fehlerhaften Passworteingaben auf einem Application-Level-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen.
- Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z. B. der Angreifer verfolgt werden soll oder ob die Netzverbindungen nach außen getrennt werden sollen. Da hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt und die entsprechende Maßnahmen einleiten. Die Aufgaben und Kompetenzen für die betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.

Folgende Fragen müssen bei der Festlegung der Policy geklärt werden:

- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn das Sicherheitsgateway überwunden wird? Da es keine absolute Sicherheit geben kann, muss entschieden werden, ob der maximal auftretende Schaden tragbar ist oder ob zusätzliche Maßnahmen ergriffen werden müssen.
- Welche Restrisiken existieren bei einem ordnungsgemäßen Betrieb des Sicherheitsgateways? Dies sind z. B. Schwachstellen in den benutzten Geräten und Betriebssystemen.

- Wie schnell wird ein Angriff auf das Sicherheitsgateway bemerkt?
- Welche Protokoll-Informationen sind auch nach einem erfolgreichen Angriff noch verfügbar?
- Sind die Benutzer bereit, die Einschränkungen durch das Sicherheitsgateway zu akzeptieren?

In der Policy müssen die getroffenen Entscheidungen dokumentiert werden. Darüber hinaus ist es wichtig, dass auch die für die Entscheidungen relevanten Informationen und Entscheidungsgründe so dokumentiert sind, dass sie zu einem späteren Zeitpunkt (etwa bei der Revision der Policy) nachvollzogen werden können. Diese Hintergrundinformationen brauchen nicht direkt in der Policy selbst enthalten zu sein, sondern es ist eher empfehlenswert, sie in einem eigenen Dokument festzuhalten.

Prüffragen:

- Existiert eine Policy für das Sicherheitsgateway, die das Verhalten in Bezug auf Informationen, Dienste und Protokolle definiert und nachvollziehbar dokumentiert?
- Ist festgelegt, dass auf dem Sicherheitsgateway ausschließlich zwingend erforderliche Dienste und Programme verfügbar sein dürfen?
- Sind Verantwortliche benannt, die für den Entwurf sowie für die Umsetzung und das Testen der Filterregeln zuständig sind?
- Sind Gegen-Maßnahmen bei erkannten Angriffen gegenüber dem Sicherheitsgateway definiert?
- Verfügt das Sicherheitsgateway über Alarmierungsmöglichkeiten für vordefinierte Ereignisse?
- Sind die bestehenden Restrisiken bei einem ordnungsgemäßen Betrieb des Sicherheitsgateways bekannt?

# M 2.72 Anforderungen an eine Firewall

Die Maßnahme ist mit Version November 2004 entfallen.

# M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Nachdem eine Sicherheitsrichtlinie für das Sicherheitsgateway festgelegt worden ist, muss entschieden werden, mit welchen Komponenten das Sicherheitsgateway realisiert werden soll. Dafür ist eine geeignete Anordnung auszuwählen.

### Grundlegende Strukturen von Sicherheitsgateways

Im Wesentlichen bieten sich zwei sinnvolle Grundstrukturen an, die als Anhaltspunkt zum Aufbau eines Sicherheitsgateways dienen können. Die grundlegenden Strukturen werden im Folgenden erläutert.

#### 1. Paketfilter - Application-Level-Gateway - Paketfilter (P-A-P)

Bei dieser Grundstruktur werden ein Paketfilter, ein Application-Level-Gateway (ALG) und ein weiterer Paketfilter "hintereinander geschaltet", so dass jeglicher Datenverkehr alle drei Komponenten überqueren muss. In der folgenden Abbildung sind beispielhaft einige Möglichkeiten zur Einrichtung von "Demilitarisierten Zonen" (DMZ) eingezeichnet, in denen weitere Komponenten des Sicherheitsgateways in einer geschützten Umgebung betrieben werden können.

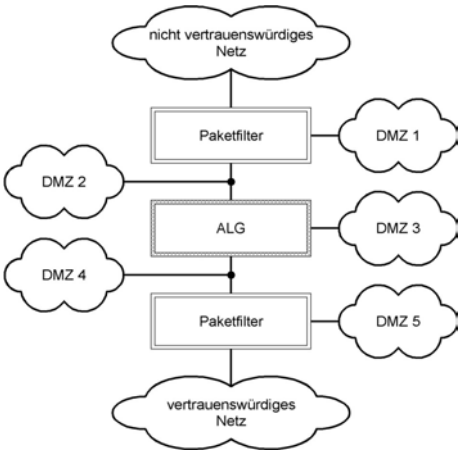



Abbildung 1: Mehrstufiger Aufbau bestehend aus Paketfilter - ALG - Paketfilter

Der Einsatzbereich für diesen Typ von Sicherheitsgateways ist vor allem die Trennung zweier Netze, falls sich das Maß der Vertrauenswürdigkeit dieser Netze erheblich unterscheidet (z. B. Trennung des Internets von einem Intranet), oder Trennung zweier Teilnetze des internen Netzes mit deutlich unterschiedlichen Sicherheitsanforderungen.

Bei den beiden Paketfiltern braucht es sich nicht notwendigerweise um dedizierte IT-Systeme (Rechner oder Appliances) zu handeln. Falls die eingesetzten Router eine integrierte Paketfilter-Funktionalität besitzen, so können die Router die Funktion des Paketfilters im Sicherheitsgateway mit übernehmen.

Die Möglichkeiten der Paketfilter-Funktionalität in Routern sind jedoch oft eingeschränkt, so dass in bestimmten Einsatzszenarien ein dedizierter Paketfilter erforderlich sein kann.

**2. Nur Paketfilter**

Die einfachste Grundstruktur eines Sicherheitsgateways besteht ausschließlich aus einem Paketfilter.

Das Grundproblem bei der Filterung der Kommunikation alleine mit einem Paketfilter liegt darin, dass die Entscheidung darüber, ob ein Zugriff erlaubt oder abgewiesen werden soll, anhand der leicht zu fälschenden Daten aus den Headern der verschiedenen IP-basierten Protokolle gefällt wird.

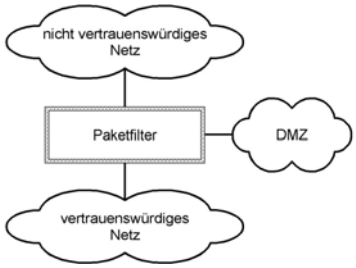



Abbildung 2: Einstufiger Aufbau bestehend aus einem Paketfilter.

Einsatzbereiche sind deshalb vor allem:

- Trennung zweier Netze, falls sich das Maß der Vertrauenswürdigkeit dieser Netze nur wenig voneinander unterscheidet (z. B. Trennung des Internets von einem Intranet mit nur geringem Schutzbedarf).
- Trennung zweier organisationsinterner Netze.
- Privater Bereich (Schutz des "heimischen" Rechners beim Zugriff auf das Internet).

Die Verwendung eines zusätzlichen IP-Proxys kann verhindern, dass Informationen des IP-Headers, wie beispielsweise die IP-ID oder die TTL ("Time-To-Live"), das vertrauenswürdige Netz verlassen. Mittels der IP-ID kann trotz NAT-Funktion die Anzahl der Rechner in einem vertrauenswürdigen Netz bestimmt werden und die TTL lässt Rückschlüsse auf verwendete Betriebssysteme zu. Über Paketfilterregeln oder entsprechendes Routing muss sichergestellt werden, dass der IP-Proxy nicht umgangen werden kann.

**Vor- und Nachteile der Grundstrukturen**

Prinzipiell ist der oben dargestellte P-A-P-Aufbau zur Erzielung eines hohen Sicherheitsniveaus in allen Anwendungszusammenhängen zu empfehlen. Wird auf Komponenten dieses Aufbaus verzichtet, so ist dies stets mit Sicherheitseinbußen verbunden.

In der folgenden Tabelle werden Vor- und Nachteile bzw. Einsatzumgebungen sowohl für den P-A-P-Aufbau, als auch für einen einzelnen Paketfilter beschrieben.

| **Paketfilter - ALG - Paketfilter (P-A-P)** | **Paketfilter** |
|---|---|
| - Kann als Grundlage Sicherstellung eines hohen Sicherheitsniveau dienen. | - Kein hohes Sicherheitsniveau, höchstens für normalen Schutzbedarf ausreichend. |

| Paketfilter - ALG - Paketfilter (P-A-P) | Paketfilter |
|---|---|
| - Hohe Komplexität aufgrund der Verwendung mehrerer Module.<br>- Nicht in jedem Anwendungszusammenhang einsetzbar. Beispielsweise kann IPSEC-Verkehr nicht über einen TCP/IP-Proxy geleitet werden.<br>- Einfache Erweiterungsmöglichkeiten, z. B. kann ein Virenscanner oder ein Spam-Filter ohne großen Aufwand an das ALG angeschlossen werden.<br>- Die Ausnutzung von Sicherheitslücken in Client-Software kann teilweise verhindert werden.<br>- Umfangreiche Protokollierungsmöglichkeiten. | - Gegenüber einem P-A-P-Aufbau relativ einfache Administration.<br>- Geringe Investitionskosten (kostenlose Software unter verschiedenen Betriebssystemen vorhanden).<br>- Keine wesentliche Einschränkung des maximalen Datendurchsatzes am Netzübergang.<br>- Einfache, grundlegende Absicherung.<br>- Integration auf einem zu schützenden Rechner theoretisch möglich (z. B. kann ein Web-Server gleichzeitig als Paketfilter genutzt werden).<br>- Bereitstellung neuer Dienste gegenüber P-A-P-Aufbau stark vereinfacht. |

Tabelle 1: Vor- und Nachteile des P-A-P Aufbaus und von Paketfiltern

Auf dem Application-Level-Gateway laufen so genannte Proxy-Prozesse (oft auch Proxy-Server genannt), die den Verbindungsaufbau zum Zielrechner durchführen, nachdem eine Authentisierung des Benutzers stattgefunden hat, und die Daten gemäß den Informationen der Anwendungsschicht filtern. Verbindungen, für die keine Proxy-Prozesse existieren, sind nicht möglich.

Rechner, auf denen einzelne Komponenten des Sicherheitsgateways realisiert werden, müssen so eingerichtet werden, dass nur die unbedingt notwendigen Programme auf ihnen laufen (Minimalsystem). Die eingesetzten Programme müssen richtig konfiguriert sind und alle bekannten Schwachstellen müssen beseitigt werden.

Werden zur Erzielung eines hohen Sicherheitsniveaus mehrere Systeme hintereinander geschaltet, so ist es dringend zu empfehlen, diese Systeme auf verschiedenen Systemen zu realisieren (z. B. mit unterschiedlichen Betriebssystemen). Dadurch wird verhindert, dass ein Angreifer das Sicherheitsgateway besonders leicht überwinden kann, indem er auf allen beteiligten Systemen die gleiche Sicherheitslücke ausnutzt.

**Hinweise zur Auswahl einer Grundstruktur**

Die Frage, welcher Typ eines Sicherheitsgateways eingesetzt werden soll, ist einerseits davon abhängig, wie groß der Unterschied der Vertrauenswürdigkeit der zu trennenden Netze ist (d. h. "wie wenig vertrauenswürdig" das nicht-vertrauenswürdige Netz ist), und andererseits davon, wie hoch der Schutzbedarf des Netzes ist, das durch das Sicherheitsgateway geschützt werden soll.

Das Internet ist in diesem Zusammenhang das am wenigsten vertrauenswürdige Netz. Soll das eigene Netz mit dem Internet verbunden werden, so sollte grundsätzlich der mehrstufige P-A-P-Aufbau gewählt werden. Nur in Ausnahmefällen kann davon abgewichen werden, beispielsweise bei sehr kleinen Netzen, bei denen ein mehrstufiges Sicherheitsgateway einen unverhältnismäßig hohen Aufwand bedeuten würde, oder wenn das eigene Netz nur einen

geringen Schutzbedarf hat. Auch in solchen Fällen muss jedoch mindestens ein Paketfilter eingesetzt werden, der besonders sorgfältig zu konfigurieren ist.

Falls das weniger vertrauenswürdige Netz "nur in geringem Maße nicht-vertrauenswürdig" ist, brauchen die Netze nicht durch ein mehrstufiges Sicherheitsgateway getrennt zu werden. In diesem Fall ist ein sorgfältig konfigurierter Paketfilter meist ausreichend.

Nur in geringem Maße nicht-vertrauenswürdige Netze können beispielsweise folgende Netztypen darstellen:

- andere (organisations-) interne Netze
- Netze ohne Verbindung zum Internet
- Netze mit Verbindung zum Internet, die ihrerseits durch besondere Sicherheitsmaßnahmen (z. B. durch ein eigenes Sicherheitsgateway) vom Internet abgeschottet sind

Folgende Tabelle fasst die Empfehlungen zusammen:

| **Einsatzgebiet** | **Empfohlener Aufbau** |
|---|---|
| Trennung zweier Teilnetze des internen Netzes mit gleichem Schutzbedarf | Paketfilter. Bei normalem Schutzbedarf genügt ein Router mit integrierter Paketfilter-Funktion. |
| Trennung zweier Teilnetze des internen Netzes mit unterschiedlichem Schutzbedarf (insbesondere: Teilnetz mit hohem Schutzbedarf und Teilnetz mit normalem Schutzbedarf) | Mindestens Paketfilter.<br>Falls vom weniger vertrauenswürdigen Netz aus auf einen Dienst im Netz mit hohem Schutzbedarf zugegriffen werden soll, dann ist es empfehlenswert, diesen Zugriff über ein ALG abzusichern. |
| Trennung eines Teilnetzes mit besonderen Sicherheitsanforderungen von einem anderen internen Netz | Mehrstufiger Aufbau aus Paketfilter - ALG - Paketfilter.<br>Zusätzlich ist in diesem Fall eine ergänzende Sicherheitsbetrachtung notwendig.<br>Der mehrstufige Aufbau kann hier nur als Grundlage für sehr hohe Sicherheit dienen. In der Regel werden zusätzliche Maßnahmen notwendig sein, für die aber keine allgemeinen Empfehlungen möglich sind. |
| Trennung des eigenen Netzes vom Internet | Grundsätzlich mehrstufiger Aufbau aus Paketfilter - ALG - Paketfilter.<br>In Ausnahmefällen (sehr kleines Netz, kein hoher Schutzbedarf) kann ein Paketfilter (beispielsweise in Verbindung mit einem NAT-Router) ausreichend sein.<br>Zumindest für Dienste wie E-Mail und HTTP wird der Einsatz eines entsprechenden Proxyservers dringend empfohlen.<br>Bei normalem Schutzbedarf kann gegebenenfalls auf den inneren Paketfilter verzichtet werden. |

| Einsatzgebiet | Empfohlener Aufbau |
|---|---|
| | Falls kein P-A-P-Aufbau gewählt wird, wird eine zusätzliche Risikobetrachtung dringend empfohlen. |

Tabelle 2: Empfehlungen für Grundstrukturen

**Andere Strukturen**

Neben den bisher beschriebenen Strukturen sind weitere Strukturen möglich, die meist aus einem Verzicht auf Komponenten des P-A-P-Aufbaus resultieren. Dies ist jedoch immer mit Einbußen bei der Sicherheit verbunden.

Gelegentlich wird beispielsweise auf den "inneren" Paketfilter verzichtet, der das ALG vom vertrauenswürdigen (bzw. internen) Netz trennt. Da einerseits die meisten Router bereits eine integrierte Paketfilter-Funktionalität bieten und angesichts der vergleichsweise geringen Kosten für einen entsprechend ausgestatteten Rechner gibt es jedoch kaum schlüssige Gründe, auf einen der Paketfilter zu verzichten.

**Appliances**

Verschiedene Hersteller bieten Sicherheitsgateways als Appliances an. Dabei handelt es sich um vorkonfigurierte Geräte, die zwar teilweise aus normalen Rechner-Komponenten aufgebaut sind und unter einem darauf angepassten herkömmlichen Betriebssystem laufen, aber nur für einen genau vorgegebenen Einsatzzweck (hier: Paketfilter bzw. ALG) hergestellt und konfiguriert wurden. Die Bandbreite der angebotenen Geräte reicht von reinen Paketfiltern bis zu mehrstufigen Lösungen, die in einem Gerät mehrere Komponenten eines Sicherheitsgateway integrieren.

Gegenüber einem Aufbau des Sicherheitsgateways aus "normalen" Rechnern, die (in Eigenregie oder durch einen Dienstleister) entsprechend konfiguriert werden, bieten Appliances oft den Vorteil einer einfacheren Konfiguration. Dem steht jedoch meist der Nachteil gegenüber, dass die Konfiguration weniger flexibel ist und weniger Möglichkeiten zur Anpassung an individuelle Bedürfnisse bietet.

Appliances, die mehrere Funktionen (z. B. Paketfilter und ALG) unter einer Betriebssysteminstallation betreiben, haben gegenüber einer Realisierung des Sicherheitsgateways durch drei getrennte Systeme den weiteren Nachteil, dass ein Angreifer nur die Sicherheitsmechanismen eines einzigen Betriebssystems überwinden muss, um das Sicherheitsgateway komplett zu kompromittieren. Dieser Aspekt muss bei der Planung des Sicherheitsgateways mit berücksichtigt werden. Soll trotzdem ein entsprechendes Gerät eingesetzt werden, so können gegebenenfalls zusätzliche Sicherheitsmaßnahmen erforderlich werden, um das angestrebte Sicherheitsniveau zu erreichen.

**Dokumentation**

Die Entscheidung für eine bestimmte Struktur sollte zusammen mit den Gründen, die für die Entscheidung ausschlaggebend waren, nachvollziehbar dokumentiert werden.

Prüffragen:

- Sind geeignete Strukturen für das Sicherheitsgateway auf der Grundlage der Sicherheitsrichtlinie auswählt?

# M 2.74 Geeignete Auswahl eines Paketfilters

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Funktionen eines Sicherheitsgateways auf Transport- und Netzwerkebene werden von den so genannten Paketfiltern übernommen. Aufgabe eines Paketfilters ist es, Datenpakete anhand der Informationen in den Header-Daten der UDP/IP- bzw. TCP/IP-Schicht (z. B. IP-Adresse und Portnummer) zu verarbeiten. Diese Entscheidung trifft der Paketfilter anhand den vom Administrator vorgegebenen Filterregeln. Vielfach bieten die Paketfilter auch eine Möglichkeit zur "Network Address Translation" (NAT), bei der die Absender-Adressen von IP-Paketen durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes verdeckt.

Die Filterregeln werden für jedes eintreffende Datenpaket sequentiell abgearbeitet. Sobald eine Regel auf ein Paket zutrifft, bricht in der Regel die Überprüfung ab und die betreffende Regel wird auf dieses Paket angewendet.

Paketfilter lassen sich anhand der Filtermöglichkeiten weiter unterteilen.

### Statische Paketfilter

Paketfilter, die eine Entscheidung anhand der Header-Daten der UDP/IP- und TCP/IP-Schichten (z. B. anhand der IP-Quelladresse, der IP-Zieladresse und der TCP-Flags) treffen, werden statische Paketfilter genannt.

### Dynamische Paketfilter/Stateful Inspection

Dynamische Paketfilter (oder auch Paketfilter mit "Stateful Inspection" genannt) erweitern die Funktionalität der statischen Paketfilter um die Möglichkeit zur Betrachtung des Kommunikationkontextes. Dynamische Paketfilter können auch bei verbindungslosen Protokollen (wie z. B. UDP) eine Entscheidung treffen, ob ein eintreffendes Paket die Antwort auf eine Anfrage ist oder ob dieses Paket zu einer Kommunikationsinitiierung gehört. Zudem ist es möglich, Dienste sicher bereitzustellen, die nicht mit festen Portnummern verbunden sind, da auch hier Pakete unabhängig von Portnummern immer dann weitergeleitet werden, wenn es vorher eine passende Anfrage aus dem vertrauenswürdigen Netz gab.

Ein dynamischer Paketfilter speichert für eine bestimmte Zeitspanne die Quell-IP-Adresse und die Quell-Portnummer ausgehender Pakete. Eintreffende IP-Pakete werden nur dann weitergeleitet, wenn deren Ziel-IP-Adresse und Ziel-Portnummern noch im Speicher vorhanden sind, das heißt, wenn vorher eine Anfrage vom vertrauenswürdigen Netz aus gestartet wurde und die festgelegte Wartezeit noch nicht überschritten wurde.

Paketfilter mit Stateful Inspection stellen zudem meist die Möglichkeit zur Betrachtung der übertragenen Daten auf der Anwendungsebene bereit.

**Realisierungsformen von Paketfiltern**

1. Einrichtung eines Rechners als Paketfilter unter Nutzung eines Betriebssystems, das die notwendigen Funktionalitäten bereitstellt

| Vorteile | Nachteile |
|---|---|
| - Je nach verwendetem Betriebssystem relativ geringe Investitionskosten. | - Evtl. lange Ausfallzeiten bei Defekten, da u. U. das Betriebssystem aufgrund ausgetauschter Hardware neu installiert oder konfiguriert werden muss.<br>- Relativ hoher Aufwand zur Konfiguration als Minimalsystem (im Vergleich zu einem Router mit Paketfilterfunktion).<br>- Know-How-Aufbau notwendig zur Konfiguration als Minimalsystem.<br>- Die Hardware von PC-Systemen ist oft anfälliger als die Hardware von Appliances, da letztere z. B. meist keine Festplatten oder Lüfter enthalten.<br>- Die Administrationskosten sind in der Regel höher als bei Appliances, da Konfigurationsoberflächen meist nicht zur Verfügung stehen.<br>- Die Komplexität ist oft höher als bei Appliances. |

Tabelle 1: Einrichten eines Rechners als Paketfilter

2. Einrichtung von Filterregeln auf einem Router

| Vorteile | Nachteile |
|---|---|
| - Keine Investitionskosten, falls ein Router schon vorhanden ist.<br>- Im Vergleich zu rechnerbasierten Paketfiltern besteht eine geringe Ausfallwahrscheinlichkeit, da Router in der Regel eine bessere Verfügbarkeit aufweisen. | - Die Erweiterungsmöglichkeiten von Routern sind oft eingeschränkt.<br>- Die Konfiguration ist evtl. schwieriger als bei Appliances oder rechnerbasierten Paketfiltern.<br>- Keine Kontrolle über die Sicherheitsfunktionen des Routers durch organisationsinternes Personal, falls dieser bei einem Dienstleister aufgestellt ist und von diesem administriert wird. |

Tabelle 2: Vor- und Nachteile der Einrichtung von Filterregeln auf einem Router

3. Verwendung einer Appliance

| Vorteile | Nachteile |
|---|---|
| - Geringer Zeitaufwand nötig bis zur Inbetriebnahme. | - Geringe Erweiterungsmöglichkeiten der proprietären Hard- und Software. |

| Vorteile | Nachteile |
|---|---|
| - Vereinfachte Konfiguration der bereitgestellten Funktionen (ggf. über Web-Oberfläche)<br>- Einfache Konfiguration, da Appliances oft Administrationsoberflächen anbieten.<br>- Appliances unterstützen oft automatische Updates.<br>- Im Vergleich zu rechnerbasierten Paketfiltern eher geringere Ausfallwahrscheinlichkeit, da Appliances oft weniger "bewegliche Teile" enthalten (z. B. Festplatte oder Lüfter) als normale Rechner. | - Lange Ausfallzeiten, falls das Gerät im Fehlerfalle oft zum Hersteller gesandt werden muss, falls keine entsprechenden Wartungsverträge geschlossen wurden. Gegebenenfalls muss deshalb ein Ersatzgerät beschafft werden, das als "Cold Standby" vorgehalten wird.<br>- Wenig Informationen zur sicheren Konfiguration und zum sicheren Betrieb zu speziellen Produkten erhältlich (über die Informationen des Herstellers hinaus). Dies ist besonders dann problematisch, wenn der Hersteller den Support einstellt.<br>- Bestimmte Appliances besitzen u. U. eine geringe Verbreitung. In diesem Fall existieren evtl. wenig Berater bzw. Dienstleister zur Administration. |

Tabelle 3: Verwendung einer Appliance

**Anforderungen an Paketfilter**

Bei allen drei Realisierungsformen lässt sich gegebenenfalls die Paketfilterkonfiguration aus den Einstellungen eines eventuell vorhandenen ALGs automatisch ableiten. Dies besitzt zum einen den Vorteil des geringen Konfigurationsaufwandes, zum anderen den Nachteil der geringeren Sicherheit, da eine Fehlkonfiguration des ALGs automatisch eine Fehlkonfiguration des Paketfilters bewirkt.

Vor der Beschaffung sollte überprüft werden, welche der folgenden Anforderungen das ALG erfüllt. Je nach Anwendungszusammenhang kann dabei auf einige Anforderungen verzichtet werden, d. h. es muss eine Bewertung der aufgelisteten Anforderungen im Anwendungszusammenhang erfolgen.

Folgende Möglichkeiten sollten vom Paketfilter unterstützt werden:

- Weiterleiten oder Verwerfen von Paketen anhand
  - der Quell-IP- und Ziel-IP-Adresse einzelner Rechner oder Netze
  - des Quell- und Zielports
  - des ICMP-Typs
  - aller TCP-Flags (URG, ACK, PSH, RST, SYN, FIN). Mit Hilfe des ACK-Bits kann beispielsweise zwischen Paketen zum Verbindungsaufbau und Paketen im Rahmen einer etablierten Verbindung unterschieden werden. Durch Kontrolle der anderen Bits können IP-Pakete mit unsinnigen Kombinationen von TCP-Flags abgelehnt werden
  - der IP-Optionen.
- Unterstützung der Aktionen
  - Weiterleiten des Pakets ("allow")
  - Verwerfen des Pakets ("deny & drop")
  - Verwerfen des Pakets und Meldung an den Absender ("deny & reject")

- Erstellung von Filterregeln getrennt für jede Schnittstelle des Paketfilters
- Getrennte Filterung kommender und gehender Pakete
- Unveränderbare Festlegung der Reihenfolge zur Abarbeitung der Filterregeln
- Protokollierung von IP-Adresse, Dienst, Zeit und Datum für jedes Paket, aber auch eingeschränkt auf bestimmte Pakete
- Im Falle, dass ein Router als Paketfilter eingesetzt wird, muss das dynamische Routing so konfigurierbar sein, dass Routing-Pakete (z. B. RIP), die das zu schützende Netz betreffen, nur an dem Interface zugelassen werden, das auch mit dem zu schützenden Netz verbunden ist.
- Schutz vor IP-Spoofing
- Falls nur ein Paketfilter ohne ALG als Sicherheitsgateway eingesetzt wird, müssen zusätzlich folgende Funktionen unterstützt werden:
    - Port-Forwarding (auch oft "Destination NAT" genannt)
    - Network Address Translation (NAT). Auch Unterstützung für:
        - Ersetzen der IP-ID
        - Ersetzen der TTL
    - Stateful Inspection

Die Anforderungen an den Paketfilter und die Gründe, die für die getroffene Auswahl ausschlaggebend waren, sollten nachvollziehbar dokumentiert werden.

Prüffragen:

- Wurden die Anforderungen an den Paketfilter und die Gründe, die für die getroffene Auswahl ausschlaggebend waren, nachvollziehbar dokumentiert?

# M 2.75 Geeignete Auswahl eines Application-Level-Gateways

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den Schichten 1-3 wahr. ALGs werden oft auch Sicherheitsproxies genannt, im Folgenden wird aber abkürzend der Begriff "Proxy" verwendet. Proxies unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikation zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy.

Einige Vor- und Nachteile von Sicherheitsproxies werden in der folgenden Tabelle zusammengestellt:

**Vorteile von Proxies**
- Oft geringere Anzahl von Programmierfehlern als in den vom Proxy geschützten Client- bzw. Serverdienstprogrammen.
- Filterung einzelner Protokollbefehle (z. B. bei HTTP der Befehl POST) in Abhängigkeit von der Parametrisierung der Befehle, der Zeit und des Benutzer möglich.
- Entfernung unerwünschter Inhalte in den übertragenen Daten.
- Abwehr von Angriffen, die auf fehlerhaften Header-Daten beruhen.
- Ersetzung der Absender-Adresse eines weitergeleiteten IP-Pakets durch die IP-Adresse der Netzschnittstelle, über die das Paket den Proxy verlässt. Dadurch werden IP-Adressen des vertrauenswürdigen Netzes verheimlicht. Im DNS braucht zudem nur eine IP-Adresse eingetragen werden.
- Erzwingen einer starken Authentisierung möglich.
- Umfangreiche Protokollierungsmöglichkeiten. Für jede Verbindung auf der Anwendungsebene kann protokolliert werden:
  - Benutzeridentifikation
  - IP-Adresse des Quell- und Zielrechners
  - Portnummern
  - Zeit und Datum

In Abhängigkeit vom Dienst können weitergehende Informationen protokolliert werden (z. B. URL bei HTTP).

**Nachteile von Proxies**
- Verringerung des maximalen Datendurchsatzes.
- Längere Antwortzeiten (Latenzzeiten) beim Abruf von Informationen.

Eventuell Einschränkung der Funktionalität der Clientprogramme (z. B. durch Filterung aktiver Inhalte).

Proxies können in zwei verschiedenen Betriebsarten arbeiten, dem sogenannten transparenten und dem nicht-transparentem Modus. Ein transparenter Proxy braucht den Clients nicht mitgeteilt zu werden. Er liest alle im Netz befindlichen IP-Pakete mit und entscheidet anhand von IP-Adresse und Port-

nummer, welche davon in ein anderes Netz weitergeleitet werden sollen. Bei Verwendung eines nicht-transparenten Proxies hingegen muss dessen IP-Adresse und Portnummer in der Client-Software (z. B. dem Webbrowser) eingetragen werden, um eine Verbindung über den Proxy hinweg zu ermöglichen.

Vor der Beschaffung sollte überprüft werden, welche der folgenden Anforderungen das ALG erfüllt. Je nach Anwendungszusammenhang kann dabei auf einige Anforderungen verzichtet werden.

Die aufgelisteten Anforderungen müssen im Anwendungszusammenhang bewertet werden. Wenn ein bestimmtes Protokoll nicht genutzt wird, braucht das ALG keine Unterstützung für das Protokoll zu bieten. Unterstützt das ALG Protokolle, die nicht genutzt werden, so sollte die Möglichkeit bestehen, das betreffende Protokoll zu deaktivieren.

Wurde für einige der im folgenden aufgeführten Protokolle in der Policy des Sicherheitsgateways festgelegt, dass sie nicht erlaubt sein sollen, so brauchen sie natürlich auch nicht unterstützt zu werden.

Die Kriterien der Bewertung und die getroffenen Entscheidungen müssen nachvollziehbar dokumentiert werden.

**Allgemein**

- Unterstützung der wichtigsten verwendeten Protokolle (beispielsweise Telnet, FTP, SMTP, NNTP, HTTP und HTTPS) auf Anwendungsschicht. Für die Nutzung anderer Dienste sollten generische Proxies für TCP- und UDP vorhanden sein.
- Die Proxies des Application-Level-Gateways sollten transparent betrieben werden können.
- Es sollte ein eigener MTA auf dem ALG integriert werden können, um gegebenenfalls mehrere MTAs in verschiedenen vertrauenswürdigen Netzen bedienen zu können.
- Es sollte eine Schnittstelle zum Anbinden von externen Analyseprogrammen zum Auffinden von Schadsoftware (z. B. Virensuchprogramme) vorhanden sein.
- Die Kommunikation mit einem Directory-Dienst für die Authentisierung der Anwender sollte unterstützt werden.
- Für jedes unterstützte Protokoll muss eine Filterung nach den in M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln* spezifizierten Kriterien möglich sein. Insbesondere müssen die Filterregeln benutzerabhängig formulierbar sein, und es muss möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen.
- Eine Filterung in Abhängigkeit von Inhalten sollte unterstützt werden, damit eine zentrale Virenprüfung und das Blockieren aktiver Inhalte möglich ist (siehe G 5.23 *Schadprogramme* bzw. G 5.88 *Missbrauch aktiver Inhalte*).
- Bei dem Einsatz eines Application-Level-Gateways sollte keine Änderung der Software im zu schützenden Netz oder im externen Netz nötig sein.
- Für jede aufgebaute und abgewiesene Verbindung auf der Anwendungsschicht muss eine Protokollierung von IP-Adresse des Quell- und Zielrechners, Portnummern, Zeit, Datum und der zutreffenden Regel durchgeführt werden, wobei auch Einschränkungen auf bestimmte Verbindungen möglich sein müssen.
- Die übertragene Datenmenge sollte protokolliert werden können.
- Die Uhrzeit des Verbindungsaufbaus und des Verbindungsabbaus sollten protokolliert werden können.

Im Folgenden werden spezifischere Anforderungen für einige häufig genutzte Protokolle zusammengestellt:

**HTTP:**
- Filtern anhand der Request-Methode, z. B. GET, HEAD, PUT oder CONNECT
- Sperren von Web-Seiten bzw. Web-Sites anhand der URL
- Filtern anhand des MIME-Types
- Entfernen von aktiven Inhalten und Cookies aus Web-Seiten
- Filtern anhand von HTTP-Header-Daten
- Filtern der folgenden Header-Felder sollte möglich sein:
  - Referrer
  - Via
  - From
  - Server
- Filtern von "Web-Bugs"
- Erzwingen einer starken Authentisierung am Proxy
- Accounting zur Feststellung der von einen Nutzer abgerufenen Datenmenge
- Unterstützung zur Signaturprüfung von signierten aktiven Inhalten
- Protokollierung der abgerufenen Web-Seite
- Protokollierung der Nutzung von gesperrten Request-Methoden

**HTTPS:**
- Temporäre Entschlüsselung des Datenverkehrs, um das Entfernen aktiver Inhalte aus Web-Seiten, die mittels HTTPS abgerufen werden, zu ermöglichen. Temporäre Entschlüsselung bedeutet, dass übermittelte Daten erst entschlüsselt, nach der Filterung auf aktive Inhalte aber wieder verschlüsselt werden.
- Protokollierung der abgerufenen Web-Seite
- Benachrichtigung des Administrators bei automatischem Update abgelaufener oder ungültiger Zertifikate

**SMTP:**
- Entfernen von aktiven Inhalten aus HTML-E-Mails
- Filtern anhand des MIME-Types
- Filtern anhand der Absender- und Empfängeradresse
- Filtern anhand der IP-Adresse des MTAs
- Kontrolle auf Mail-Relaying anhand des Domain-Namens
- Überprüfung auf Zustellbarkeit der E-Mail anhand des Domain-Namens
- Entfernung bedenklicher E-Mailanhänge anhand der Dateiendung. Zu blockierende Anhänge sollen frei vorgegeben werden können.
- Erkennung von Spam-Mails mit Hilfe einer Kombination verschiedener Filter-Verfahren.
- Erkannte Spam-Mails sollten wie folgt behandelt werden können:
  - Löschen
  - Isolierung ("Quarantäne")
  - Markieren
- Erkannte E-Mails mit nicht spezifikationskonformen Headern ("Bad-Mails"), sollten wie folgt behandelt werden können:
  - Löschen
  - Isolierung ("Quarantäne")
  - Markieren
- Bereitstellung einer Schnittstelle, die die Anbindung eines Spam-Filters ermöglicht.

- Blockieren von (ausgehenden) E-Mails aufgrund der Erkennung von Schlüsselwörtern
- Protokollierung der E-Mail-Adressen des Absenders und des Adressaten
- Protokollierung des Erfolgs bzw. des Fehlschlagens der E-Mail- Weiterleitung
- Möglichkeit zur Einrichtung eines
    - Mail-Relay (Weiterleitung von einem MTA im vertrauenswürdigen Netz zu einem MTA im nicht-vertrauenswürdigen Netz)
    - Mail-Server (Möglichkeit zum Abruf mit POP3 oder IMAP und zur Weiterleitung mit SMTP)

**FTP (passiv und aktiv):**
- Filterung anhand von FTP-Befehlen (z. B. GET, PUT, PASV, PORT)
- Nutzerbasierte Freigabe bzw. Sperrung von FTP-Befehlen
- Restriktionen anhand des Dateinamens (z. B. Sperrung von *.exe)
- Erzwingen einer starken Authentisierung am Proxy
- Protokollierung der Nutzung von gesperrten Request-Methoden
- Protokollierung des Benutzernamens im Falle einer Authentisierung und des Dateinamens

**NNTP:**
- Filtern anhand der Request-Methode, z. B. ARTICLE, BODY, HEAD und STAT
- Protokollierung der Nutzung von gesperrten Request-Methoden
- Entfernen von aktiven Inhalten und Cookies aus Web-Seiten
- Erzwingen einer starken Authentisierung am Proxy
- Gezielte Sperrung einzelner Foren

**Telnet:**
- Erzwingen einer starken Authentisierung am Proxy
- Protokollierung des Benutzernamens im Falle einer Authentisierung

**POP:**
- Filtern anhand der Request-Methode, z. B. STAT, LIST, RETR oder DELE
- Entfernen von aktiven Inhalten und Cookies aus HTML-E-Mails
- Protokollierung der Nutzung von gesperrten Request-Methoden

**UDP- und TCP-Relays:**
- Erzwingen einer starken Authentisierung am Proxy
- Protokollierung des Benutzernamens im Falle einer Authentisierung

**IP-Relay:**
- Der Aufbau von VPNs über das Application-Level-Gateway sollte mittels IP-Relays unterstützt werden.

**DNS:**
- Bereitstellung einer integrierten Lösung bestehend aus öffentlichem und privatem DNS-Server
- Sichere Abschottung des DNS-Proxies vom Rest des Betriebssystems des ALGs

Klartextprotokolle wie Telnet und FTP sollten nach Möglichkeit nicht mehr in öffentlichen Netzen benutzt werden und durch sicherere Alternativen (SSH / SCP) ersetzt werden. Auch im internen Netz sollten sie nur dann noch verwendet werden, wenn aus zwingenden Gründen ein Umstieg auf SSH oder ein anderes sicheres Protokoll nicht möglich ist.

Auch POP sollte nach Möglichkeit allenfalls noch intern verwendet werden. Sollen von einem externen Mailserver (etwa bei einem Provider) E-Mails abge-

rufen werden, so sollte der Variante "POP über SSL" der Vorzug gegeben werden. In diesem Fall ist allerdings ein SSL-Proxy (analog zum HTTPS-Proxy) nötig, der die verschlüsselte Verbindung am Sicherheitsgateway unterbricht und es so ermöglicht, E-Mails zentral auf Viren und andere schädliche Inhalte zu prüfen.

Prüffragen:

- Wurde die Auswahl und Bewertung der Anforderungen an das ALG dokumentiert?
- Erfüllen die eingesetzten Proxies die aufgeführten Anforderungen?

# M 2.76 Auswahl und Einrichtung geeigneter Filterregeln

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Aufstellen und die notwendige Aktualisierung der Filterregeln für ein Sicherheitsgateway ist keine einfache Aufgabe. Die Administratoren müssen dafür fundierte Kenntnisse der eingesetzten Protokolle besitzen und entsprechend geschult werden.

Beim **Aufstellen der Filterregeln** sollten folgende Punkte beachtet werden:

- Anlass und Initiator der Regeleinrichtung müssen geeignet dokumentiert werden. Dies ist wichtig, damit später nachvollzogen werden kann, warum die jeweilige Filterregel implementiert wurde. Ohne diese Information ist es häufig schwierig, zeitnah Ansprechpartner der freigeschalteten Anwendungen zu identifizieren und zu entscheiden, ob die Regel gelöscht oder geändert werden kann.
- Grundsätzlich sollte die "Whitelist"-Strategie verwendet werden, das heißt die Regeln sollten so formuliert werden, dass alle Zugänge, die nicht explizit erlaubt werden, verboten sind.
- Falls es Bedarf für eine benutzerspezifische Authentisierung gibt, muss geklärt werden, welche Benutzer aus dem internen Netz welche Dienste verwenden dürfen und welche Authentisierungsverfahren eingesetzt werden sollen.
- Alle Rechner im internen Netz müssen berücksichtigt werden.
- Es muss festgelegt werden, welche Dienste zu welchen Zeiten zur Verfügung stehen sollen.

Die Filterregeln für Paketfilter sollten in einer Tabelle zusammengefasst werden, deren eine Achse die Ziel-IP-Adressen und deren andere Achse die Quell-IP-Adressen enthält. Die Einträge enthalten dann die erlaubten Portnummern, dabei ist die obere der Quell-, die untere der Zielport. Paketfilter können die Überprüfung der Pakete unter anderem unmittelbar nach dem Empfang oder unmittelbar vor der Weiterleitung durchführen. Normalerweise sollte die erste Variante gewählt werden. Außerdem müssen die Paketfilter so konfiguriert werden, dass als Absenderadresse nur die Nummern der an dem Interface angeschlossenen Rechner zugelassen werden ("Ingress-Filterung"). Adressen, die mit den anderen Interfaces verknüpft sind, dürfen nicht durchgelassen werden. Dies verringert die Gefahr von IP-Spoofing-Angriffen.

**Beispiel:**

Die folgende Tabelle enthält Filterregeln für das interne Interface eines Paketfilters zwischen einem internen Netz und dem Zwischennetz, das sich zwischen dem internen und dem externen Paketfilter befindet.

Die Einträge enthalten die erlaubten Verbindungen, dabei bezeichnet der obere Eintrag den Quellport und der untere Eintrag den Zielport.

| Quellsystem | Zielsystem | Quellport | Zielport |
|---|---|---|---|
| Interner Mailserver | Externer Mailserver im Zwischennetz | TCP > 1023 | TCP: 25 |

| Quellsystem | Zielsystem | Quellport | Zielport |
|---|---|---|---|
| Interner DNS-Server | Externer DNS-Server im Zwischennetz | UDP: 53 | UDP: 53 |
| IT-System mit der IP-Adresse 192.168.0.5 | Appl.-Level-Gateway im Zwischennetz | TCP > 1023 | TCP: 20,21 |
| IT-System mit der IP-Adresse 192.168.0.7 | Appl.-Level-Gateway im Zwischennetz | TCP > 1023 | TCP: 23 |
| IT-System mit dem IP-Adressbereich 192.168.0.* | Appl.-Level-Gateway im Zwischennetz | TCP > 1023 | TCP: 22,80 |
| IT-System mit dem IP-Adressebereich 192.168.1.* | Appl.-Level-Gateway im Zwischennetz | TCP > 1023 | TCP: 80 |

Tabelle 1: Filterregeln für das interne Interface eines Paketfilters

Der Verbindungsaufbau zwischen den nicht aufgeführten Systemen, wie beispielsweise zwischen internem Mailserver und externem DNS-Server, muss unterdrückt werden. Alle nicht aufgelisteten Portnummern sind zu blocken. Sofern weitere Dienste oder Kommunikationsbeziehungen benötigt werden, muss die Tabelle 1 entsprechend ergänzt werden.

Dies bedeutet beispielsweise, dass der interne Mailserver mit TCP von einem Port mit einer Portnummer > 1023 auf Port 25 (SMTP) des externen Mailservers im Zwischennetz zugreifen darf. Ports mit einer Portnummer > 1023 werden auch als unprivilegierte Ports bezeichnet, im Gegensatz zu Ports mit niedrigeren Portnummern, die als privilegierte oder "well-known Ports" bezeichnet werden, da die Dienste hinter diesen Portnummern von der "Internet Assigned Numbers Authority" (IANA) zugewiesen sind.

Diese Tabelle muss dann in entsprechende Filterregeln umgesetzt werden. Dies ist häufig nicht einfach und muss deshalb sehr genau kontrolliert werden.

Ggf. können die Filterregeln mit Hilfe von Tools umgesetzt werden, die über Bedienoberflächen die Modellierung des Netzes und der zugehörigen Filterregeln erleichtern. Durch regelmäßige Tests muss überprüft werden, dass die Filterregeln den aktuellen Anforderungen entsprechen und dass alle Filterregeln korrekt umgesetzt worden sind. Insbesondere muss sichergestellt werden, dass nur die Dienste zugelassen werden, die in der Sicherheitsrichtlinie vorgesehen sind.

Für die Regeln eines Application-Level-Gateways sind analoge Tabellen zu erstellen und in die entsprechenden Filterregeln umzusetzen.

**Beispiel:**

| Org.einheit | Dienst | Befehle | Authentisierung |
|---|---|---|---|
| F23 | FTP | ..., RETR, STOR | Einmalpasswort |
| R01 | FTP | ..., RETR | Chipkarte |

Tabelle 2: Tabelle für die Regeln eines Application-Level-Gateways

Die Benutzer der Organisationseinheit F23 dürfen (unter anderem) die Befehle RETR und STOR des Dienstes FTP benutzen, d. h. sie dürfen über FTP Dateien laden und senden, während die Benutzer der Organisationseinheit R01 nur Dateien laden dürfen.

Prüffragen:

- Wird für die Filterregeln des Sicherheitsgateways das Whitelist-Verfahren angewendet, um alle Verbindungen, die nicht explizit erlaubt werden, zu verbieten?
- Werden in den Filterregeln alle Rechner im inneren Netz berücksichtigt?
- Sind die eingerichteten Filterregeln des Sicherheitsgateways, z. B. durch Beschreibung der jeweiligen Funktion, dokumentiert?
- Werden am Sicherheitsgateway ausschließlich Dienste zugelassen, die den Anforderungen der Sicherheitsrichtlinie entsprechen?

# M 2.77 Integration von Servern in das Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Neben Installation und Betrieb des Sicherheitsgateways müssen oft auch Server sicher angeordnet werden. Dazu gehören z. B. Informationsserver für die Bereitstellung von Informationen an interne oder externe Benutzer, Mailserver und DNS-Server.

Für die Anordnung von Servern ist zu unterscheiden, ob diese im zu schützenden Netz, im Netz zwischen den beiden Paketfiltern (im Folgenden nur noch "Zwischennetz" genannt) oder auf der externen Seite des Sicherheitsgateways angesiedelt werden sollen.

### Externe Zugänge

Externe Zugänge zum vertrauenswürdigen Netz, beispielsweise mit SSH über einen Modem-Pool, sollten wie Zugänge aus dem nicht-vertrauenswürdigen Netz behandelt werden. Dies lässt sich erreichen, indem z. B. ein Terminalserver mit angeschlossenen Modems auf die externe Seite des Sicherheitsgateways gestellt wird, so dass ein Zugang von dort nur über SSH zum internen Rechner durchgeführt werden kann.

Es müssen klare Regelungen darüber getroffen werden, dass keine externen Zugänge unter Umgehung des Sicherheitsgateways geschaffen werden dürfen. Diese Regelungen müssen allen Mitarbeitern bekanntgemacht werden. Es muss sichergestellt werden, dass sowohl das Sicherheitsmanagement als auch der Administrator des Sicherheitsgateways rechtzeitig über entsprechende Pläne unterrichtet wird, um eine Einbettung in das Sicherheitskonzept und die Sicherheitsrichtlinie des Sicherheitsgateways zu gewährleisten.

Weitere Informationen zur Behandlung externer Zugänge finden sich auch im Baustein B 4.4 *VPN*.

### Anordnung von Informationsservern

Server, die der Bereitstellung von Informationen für externe Benutzer dienen, sollten generell "möglichst nahe" am nicht-vertrauenswürdigen Netz platziert werden (z. B. hinter dem externen Paketfilter) und wie andere im nicht-vertrauenswürdigen Netz vorhandene Server betrachtet werden. Die Platzierung "möglichst weit außen" erschwert bei einer Kompromittierung des Informationsservers den Zugriff auf das vertrauenswürdige Netz, da der Angreifer noch mehrere Komponenten des Sicherheitsgateways überwinden muss. Ihre Verwaltung sollte entweder nur lokal oder über speziell abgesicherte und gegebenenfalls sogar zeitlich begrenzte Zugänge vom vertrauenswürdigen Netz aus erfolgen.

Da Informationsserver, die Informationen für externe Benutzer anbieten, wie Rechner des nicht vertrauenswürdigen Netzes behandelt werden sollten, sollte durch Filterregeln und gegebenenfalls durch eine entsprechende Konfiguration des Servers sichergestellt werden, dass von einem solchen Server aus keine Verbindungen ins vertrauenswürdige Netz hinein möglich sind, sondern nur vom vertrauenswürdigen Netz aus zum Server.

Beispielsweise sollten für einen Webserver, dessen Administration vom vertrauenswürdigen Netz aus über eine SSH-Verbindung erfolgt, keine SSH-Verbindungen erlaubt werden, die vom Server ausgehen, sondern nur Verbindungen, die vom vertrauenswürdigen Netz zum Server gehen.

Gibt es Daten, die nur für die Benutzer des vertrauenswürdigen Netzes erreichbar sein sollen (etwa einen Intranet-Webserver), so sollten diese möglichst nicht auf einem Server gespeichert werden, der auch Dienste für externe Benutzer anbietet. In diesem Fall wird empfohlen, weitere Informationsserver im Zwischennetz einzusetzen, die von außen nicht erreichbar sind und gegen Angriffe von innen durch den Paketfilter geschützt werden.

Falls die Daten, die nur für interne Benutzer erreichbar sein sollen einen hohen Schutzbedarf bezüglich der Vertraulichkeit haben, so darf der entsprechende Informationsserver nicht im gleichen Zwischennetz angesiedelt werden, wie Informationsserver für externe Benutzer. In diesem Fall muss eine eigene DMZ für die betreffenden Server eingerichtet werden.

Für folgende Informationsserver werden in eigenen Maßnahmen Hinweise zur Integration in ein Sicherheitsgateway gegeben:

- Webserver (siehe M 5.115 *Integration eines Webservers in ein Sicherheitsgateway*)
- E-Mailserver (siehe M 5.116 *Integration eines E-Mailservers in ein Sicherheitsgateway*)
- Datenbankserver (siehe M 5.117 *Integration eines Datenbank-Servers in ein Sicherheitsgateway*)
- DNS-Server (siehe M 5.118 *Integration eines DNS-Servers in ein Sicherheitsgateway* )
- Webanwendung mit Web-, Applikations- und Datenbankserver (siehe M 5.119 *Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway*)

Prüffragen:

- Sind Maßnahmen umgesetzt, sodass keine weiteren externen Verbindungen unter Umgehung des Sicherheitsgateways geschaffen werden?
- Erfolgt der administrative Zugriff auf Informationsserver für externe Benutzer ausschließlich über vertrauenswürdige Pfade?
- Wird eine direkte Verbindung der von extern erreichbaren Informationsserver gegenüber dem vertrauenswürdigem Netz verhindert?
- Besteht eine netzwerktechnische Trennung der Informationsserver für den internen und externen Bereich?
- Sind Informationsserver mit sensiblen Daten für den internen Bereich in einer eigenen DMZ angesiedelt?

# M 2.78 Sicherer Betrieb eines Sicherheitsgateways

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Für einen sicheren Betrieb eines Sicherheitsgateways sind die umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre korrekte Einhaltung zu überprüfen. Insbesondere müssen die für den Betrieb des Sicherheitsgateways getroffenen organisatorischen Regelungen regelmäßig/sporadisch auf ihre Einhaltung überprüft werden. Es sollte in regelmäßig kontrolliert werden, ob neue Zugänge unter Umgehung des Sicherheitsgateways geschaffen wurden.

Durch regelmäßige Tests muss außerdem überprüft werden, dass alle Filterregeln korrekt umgesetzt worden sind. Dabei ist zu testen, dass nur die Dienste zugelassen werden, die in der Policy des Sicherheitsgateways erlaubt sind.

Falls nachträgliche Änderungen der Policy erforderlich sind, müssen diese streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden.

Die bei der Beschaffung an Paketfilter bzw. an Application-Level-Gateways gestellten Forderungen sind umzusetzen. Sie sind regelmäßig zu aktualisieren und auf Vollständigkeit zu prüfen.

Die Default-Einstellung der Filterregeln und die Anordnung der Komponenten muss sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muss auch bei einem völligen Ausfall der Komponenten des Sicherheitsgateways gelten.

Es muss die Regel **"Alles was nicht ausdrücklich erlaubt ist, ist verboten"** realisiert sein. So darf z. B. ein Benutzer, der keinen Eintrag in einer Access-Liste hat, keine Möglichkeit haben, Dienste des Internets zu benutzen.

Darüber hinaus sind die folgenden Punkte zu beachten:

- Alle Geräte (Rechner, Router oder Appliances), die Bestandteil eines Sicherheitsgateways sind, müssen besonders sorgfältig und sicher konfiguriert werden.
- Auf den eingesetzten Komponenten dürfen nur Programme vorhanden sein, die für die Funktionsfähigkeit des Sicherheitsgateways nötig sind. Der Einsatz dieser Programme muss ausführlich dokumentiert und begründet werden. Beispielsweise sollten Dienste deaktiviert und Treiber entfernt werden, die nicht benötigt werden. Treiber sollten nach Möglichkeit auch aus dem Betriebssystem-Kern entfernt werden. Das Verbleiben von Software muss dokumentiert und begründet werden.
- Um ein Mitlesen oder Verändern der Authentisierungsinformationen zu verhindern, dürfen Administratoren und Revisoren nur über einen vertrauenswürdigen Pfad auf das Sicherheitsgateway zugreifen, beispielsweise direkt über die Konsole, über eine verschlüsselte Verbindung oder über ein separates Administrationsnetz (Out-of-Band Management).
- Es muss dafür gesorgt werden, dass die Betriebssysteme und Programme auf den Komponenten des Sicherheitsgateways jederzeit auf einem sicheren Patch-Stand sind. Die Systemadministratoren müssen sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren und sicherheitskritische Patches besonders sorgfältig zeitnah installieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des*

*Systems*, M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*, sowie M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*). Im Fehlerfall muss das Sicherheitsgateway abgeschaltet werden.
- Das Sicherheitsgateway muss auf sein Verhalten bei einem Systemabsturz getestet werden. Insbesondere sollte kein automatischer Neustart möglich sein und es muss möglich sein, die Access-Listen auf einem schreibgeschützten Medium zu speichern.
  Die Access-Listen sind die wesentlichen Daten für den Betrieb des Sicherheitsgateways sind. Daher muss durch einen entsprechenden Schutz sichergestellt werden, dass auch dann keine alten oder fehlerhaften Access-Listen benutzt werden, falls es einem Angreifer gelingt, einen Neustart des Sicherheitsgateways oder einzelner Komponenten zu verursachen.
- Bei einem Ausfall des Sicherheitsgateways muss sichergestellt sein, dass in dieser Zeit keine Netzverbindungen aus dem zu schützenden Netz heraus oder zu diesem aufgebaut werden können (siehe auch M 2.302 *Sicherheitsgateways und Hochverfügbarkeit* und M 6.94 *Notfallvorsorge bei Sicherheitsgateways*).
- Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren Betrieb des Sicherheitsgateways relevante Dateien wie Access-Listen, Passwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

Prüffragen:

- Werden die auf den Sicherheitsgateways umgesetzten Maßnahmen regelmäßig auf ihre Korrektheit überprüft?
- Werden Änderungen am Filterregelwerk im Vorfeld auf mögliche sicherheitsrelevante Auswirkungen hin überprüft?
- Sind die auf dem Sicherheitsgateway eingesetzten Programme und Dienste auf das erforderliche Maß reduziert?
- Erfolgt der administrative Zugriff auf die Komponenten des Sicherheitsgateways ausschließlich über vertrauenswürdige Pfade?
- Werden die an den Sicherheitsgateways vorgenommenen Einstellung regelmäßig gesichert?

# M 2.79 Festlegung der Verantwortlichkeiten im Bereich Standardsoftware

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Organisation

Vor der Einführung von Standardsoftware müssen eine Reihe von Verantwortlichkeiten geregelt werden. Beispielhaft seien die Verantwortlichkeiten genannt für die Erstellung eines Anforderungskataloges, die Vorauswahl von Produkten, das Testen und Freigeben und die Installation.

Nachfolgend wird zum Vergleich aufgezeigt, wie diese Verantwortlichkeiten sinnvoll verteilt werden können. Da jedoch die Bezeichnungen in den meisten Organisationen voneinander abweichen, werden vorab einige Instanzen anhand ihrer Aufgaben definiert, denen anschließend die einzelnen Verantwortlichkeiten zugeordnet werden können:

- Die **Fachabteilung** ist der Anwender der Standardsoftware. Sie äußert ihren Bedarf an neuer Software und gibt damit den Anstoß zu deren Beschaffung. Sie wird bei Vorauswahl und Test beteiligt, um die Anforderungen der Anwender einzubringen.
- Die **Behörden-/Unternehmensleitung** ist verantwortlich für die Freigabe von Standardsoftware. Diese Verantwortung wird meist an den **Leiter der Fachabteilung** delegiert, womit nach Freigabe die Verantwortung für den korrekten Einsatz der Standardsoftware auf die Fachabteilung übergeht.
- Der **IT-Bereich** hat die Aufgabe, IT-Lösungen für die Erfüllung der Aufgaben der Fachabteilung bereitzustellen und den sicheren und zuverlässigen Betrieb der IT zu gewährleisten.
- Die **Beschaffungsstelle** muss die Interoperabilität und Kompatibilität der zu beschaffenden Standardsoftware sowie die Einhaltung von Hausstandards und gesetzlichen Vorschriften sicherstellen. Oft gibt es in den einzelnen Fachabteilungen IT-Koordinatoren, die Teile der Aufgaben der Beschaffungsstelle für die Fachabteilung beratend wahrnehmen und evtl. auch die Haushaltsmittel der Fachabteilung koordinieren.
- Der **Haushalt** ist verantwortlich für das Rechnungswesen, die IT-Budgetverwaltung und für die Bereitstellung der benötigten Haushaltsmittel.
- Der **IT-Sicherheitsbeauftragte** muss überprüfen, ob mit den eingesetzten oder zu beschaffenden Produkte ein angemessenes Sicherheitsniveau gewährleistet werden kann. Im Rahmen des Sicherheitsmanagements (siehe Baustein B 1.0 *Sicherheitsmanagement*) muss er die IT-Sicherheit im laufenden Betrieb sicherstellen.
- Der **Datenschutzbeauftragte** muss die Einhaltung der datenschutzrechtlichen Bestimmungen und eines ausreichenden Schutzes personenbezogener Daten gewährleisten.
- Der **Personal- bzw. Betriebsrat** muss in vielen Fällen bei der Auswahl neuer Standardsoftware beteiligt werden, insbesondere wenn damit größere Änderungen im Arbeitsablauf verbunden sind oder wenn die zu beschaffende Software zur Leistungskontrolle geeignet ist (siehe M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*).

Im Gesamtprozess "Standardsoftware" muss für jeden einzelnen Schritt festgelegt werden, welche der zuvor beschriebenen Instanzen für die Durchführung verantwortlich sind und welche Instanzen dabei beteiligt werden müssen. Eine mögliche sinnvolle Verantwortungsverteilung ist zur Orientierung in nachfolgender Tabelle zusammengefasst:

| | verantwortlich | zu beteiligen |
|---|---|---|
| Erstellung des Anforderungskatalogs | Fachabteilung, IT-Bereich | Beschaffungsstelle, Haushälter, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat |
| Vorauswahl eines geeigneten Produktes | Beschaffungsstelle | IT-Bereich, Fachabteilung |
| Testen | Fachabteilung und IT-Bereich | IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat |
| Freigabe | Behörden-/Unternehmensleitung<br>evtl. delegiert an Leiter Fachabteilung | - |
| Beschaffung | Beschaffungsstelle | Haushalt |
| Sicherstellen der Integrität der Software | IT-Bereich | - |
| Installation und Konfiguration | IT-Bereich | - |
| Versionskontrolle und Lizenzverwaltung | IT-Bereich | - |
| Deinstallation | IT-Bereich | - |
| Kontrolle des IT-Betriebs | IT-Sicherheitsbeauftragter | - |

Die getroffenen Zuordnungen sind verbindlich festzuschreiben und deren Einhaltung ist periodischen Kontrollen zu unterziehen.

Prüffragen:

- Sind die Verantwortlichkeiten für die Einführung von Standardsoftware festgelegt (z. B. für Auswahl, Testen, Freigabe und Installation)?

# M 2.80 Erstellung eines Anforderungskatalogs für Standardsoftware

**Verantwortlich für Initiierung:** Leiter Fachabteilung
**Verantwortlich für Umsetzung:** Fachabteilung, Leiter IT

Zur Lösung einer Aufgabe, die mit IT bearbeitet wird, bietet der Markt meist eine Vielzahl gleichartiger Standardsoftwareprodukte an. In ihrer Grundfunktionalität vergleichbar, unterscheiden sie sich jedoch in Kriterien wie Anschaffungs- und Betriebskosten, Zusatzfunktionalitäten, Kompatibilität, Administration, Ergonomie und Informationssicherheit .

### Anforderungskatalog

Für die Auswahl eines geeigneten Produktes muss daher zunächst ein Anforderungskatalog erstellt werden. Der Anforderungskatalog sollte unter anderem zu den folgenden Punkten Aussagen enthalten:

- **Funktionale Anforderungen**, die das Produkt zur Unterstützung der Aufgabenerfüllung der Fachabteilung erfüllen muss. Die für die Fachaufgabe relevanten Einzelfunktionalitäten sollten hervorgehoben werden.
  Verkürzte Beispiele:
  - Textverarbeitung mit den Zusatzfunktionen Einbinden von Grafiken, Makro-Programmierung, Rechtschreibprüfung und Silbentrennung. Makro-Programmierung muss abschaltbar sein, Rechtschreibprüfung muss in Englisch, Französisch und Deutsch verfügbar sein. Die spezifizierten Textformate müssen im- und exportiert werden können.
  - Datenbank (Front-End und Back-End) für Multi-User-Betrieb mit Unterstützung der Standardabfragesprache SQL und grafischer Bedienoberfläche
  - Terminplaner zur Koordinierung und Kontrolle von Terminen der Abteilungsangehörigen mit integrierter Terminabstimmung, automatischem Versand von Einladungen und Aufgaben- und Prioritäten-Listen, Schnittstelle zum hausinternen Mailprogramm
- **IT-Einsatzumgebung**, diese wird einerseits beschrieben durch die Rahmenbedingungen, die durch die vorhandene oder geplante IT-Einsatzumgebung vorgegeben werden, und andererseits durch die Leistungsanforderungen, die durch das Produkt an die Einsatzumgebung vorgegeben werden.
  Verkürztes Beispiel:
  - Erforderliche IT-Einsatzumgebung und Leistungsanforderungen: Betriebssystem, Prozessor, Hauptspeicher, Festplattenkapazität, Schnittstellen für externe Datenträger und für Vernetzung
- **Kompatibilitätsanforderungen** zu anderen Programmen oder IT-Systemen, also Migrationsunterstützung und Aufwärts- und Abwärtskompatibilität.
  Verkürzte Beispiele:
  - Datenbestände aus der vorhandenen Datenbank XYZ müssen übernommen werden können.
  - Die Funktionen A, B, C müssen bei Versionswechseln erhalten bleiben.
  - Der Datenaustausch mit dem Unix-System XYZ muss möglich sein.

- **Performanceanforderungen** beschreiben die erforderlichen Leistungen hinsichtlich Durchsatz und Laufzeitverhalten. Für die geforderten Funktionen sollten möglichst genaue Angaben über die maximal zulässige Bearbeitungszeit getroffen werden.
  Verkürzte Beispiele:
  - Die maximale Antwortzeit bei Ausführung von Funktion X darf 2 Sekunden nicht überschreiten.
  - Andere gleichzeitig verarbeitete Prozesse dürfen durch das Produkt maximal um 30% verlangsamt werden.
- **Interoperabilitätsanforderungen**, d. h. die Zusammenarbeit mit anderen Produkten über Plattformgrenzen hinweg muss möglich sein.
  Verkürzte Beispiele:
  - Versionen des Textverarbeitungsprogramms sollen für Windows-, Unix- und MacOS-Plattformen verfügbar sein (in den zu benennenden Versionen). Dokumente sollen auf einem Betriebssystem erstellt und auf einem anderen weiterverarbeitet werden können.
  - Das Textverarbeitungsprogramm muss mit dem eingesetzten Mailprogramm zusammenarbeiten können.
- **Zuverlässigkeitsanforderungen** betreffen die Stabilität des Produktes, also Fehlererkennung und Toleranz sowie Ausfall- und Betriebssicherheit.
  Verkürzte Beispiele:
  - Fehleingaben des Benutzers müssen erkannt werden und dürfen nicht zum Programmabbruch oder Systemabsturz führen.
  - Die Datenbank muss über Mechanismen verfügen, die es erlauben, bei einem Systemabbruch mit Zerstörung der Datenbank alle Transaktionen zu rekonstruieren (Roll-Forward).
- **Konformität zu Standards**, dies können internationale Normen, De-facto-Standards oder auch Hausstandards sein.
  Verkürztes Beispiel:
  - Das Produkt muss der EU-Bildschirmrichtlinie 90/270/EWG entsprechen.
- **Einhaltung von internen Regelungen und gesetzlichen Vorschriften** (z. B. ausreichender Datenschutz bei der Verarbeitung personenbezogener Daten)
  Verkürzte Beispiele:
  - Das Produkt muss den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme genügen.
  - Da personenbezogene Daten verarbeitet werden, müssen die Bestimmungen des Bundesdatenschutzgesetzes mit den implementierten Funktionen erfüllt werden können.
- **Anforderungen an die Benutzerfreundlichkeit**, die durch die leichte Bedienbarkeit, Verständlichkeit und Erlernbarkeit gekennzeichnet ist, also insbesondere durch die Güte der Benutzeroberfläche sowie die Qualität der Benutzerdokumentation und der Hilfefunktionen.
  Verkürzte Beispiele:
  - Eine Online-Hilfefunktion muss implementiert sein.
  - Die Benutzeroberfläche muss so gestaltet sein, dass ungelernte Kräfte innerhalb von zwei Stunden in die Benutzung eingewiesen werden können.
  - Die Benutzerdokumentation und die Benutzeroberfläche sollten in der Landessprache vorliegen.

- **Anforderungen an die Wartbarkeit** ergeben sich für den Anwender hauptsächlich aus der Fehlerbehandlung des Produktes.
  Verkürzte Beispiele:

  - Der Administrationsaufwand darf nicht zu hoch sein.
  - Der Anbieter muss eine Hotline für Fragen anbieten.
  - Das Produkt muss einfach zu installieren und zu konfigurieren sein.
  - Das Produkt muss einfach zu deinstallieren sein.
- die **Obergrenze der Kosten**, die durch die Beschaffung dieses Produktes verursacht würden, werden vorgegeben. Dabei müssen nicht nur die unmittelbaren Beschaffungskosten für das Produkt selber einbezogen werden, sondern auch Folgekosten, wie z. B. eine Aufrüstung der Hardware, Personalkosten oder notwendige Schulungen.
  Verkürzte Beispiele:

  - Das Produkt darf maximal 15.000,- Euro kosten.
  - Die Schulungskosten dürfen 2.000,- Euro nicht überschreiten
- Aus den **Anforderungen an die Dokumentation** muss hervorgehen, welche Dokumente in welcher Güte (Vollständigkeit, Verständlichkeit) erforderlich sind.
  Verkürzte Beispiele:

  - Die Benutzerdokumentation muss leicht nachvollziehbar und zum Selbststudium geeignet sein. Die gesamte Funktionalität des Produktes ist zu beschreiben.
  - Die Systemverwalterdokumentation muss Handlungsanweisungen für mögliche Fehler enthalten.
- Bezüglich der **Softwarequalität** können Anforderungen gestellt werden, die von Herstellererklärungen zum eingesetzten Qualitätssicherungsverfahren, über ISO 9000 ff. Zertifikate bis hin zu unabhängigen Softwareprüfungen nach ISO/IEC 25051 reichen.
  Verkürzte Beispiele:

  - Der Software-Herstellungsprozess des Herstellers muss nach ISO 9000 zertifiziert sein.
  - Die Funktionalität des Produktes muss unabhängig gemäß ISO/IEC 25051 überprüft worden sein.
- Sollen durch das Produkt Sicherheitsfunktionen erfüllt werden, sind sie in Form von **Sicherheitsanforderungen** zu formulieren (siehe M 4.42 *Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung*). Dies wird nachfolgend noch ausführlich erläutert.

**Sicherheitsanforderungen**

Abhängig davon, ob das Produkt Sicherheitseigenschaften bereitstellen muss, können im Anforderungskatalog Sicherheitsfunktionen aufgeführt werden. Typische Sicherheitsfunktionen, die hier in Frage kommen, seien kurz erläutert. Weitere Ausführungen findet man in den Common Criteria (den "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik").

- **Identifizierung und Authentisierung**
  In vielen Produkten wird es Anforderungen geben, diejenigen Benutzer zu bestimmen und zu überwachen, die Zugriff auf Betriebsmittel haben, die vom Produkt kontrolliert werden. Dazu muss nicht nur die behauptete Identität des Benutzers festgestellt, sondern auch die Tatsache nachgeprüft werden, dass der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Dies geschieht, indem der Benutzer dem Produkt Informationen liefert, die fest mit dem betreffenden Benutzer verknüpft sind.

- **Zugriffskontrolle**
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass Benutzer und Prozesse, die für diese Benutzer tätig sind, daran gehindert werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung oder Änderung (einschließlich Löschung) von Informationen geben.
- **Beweissicherung**
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass über Handlungen, die von Benutzern bzw. von Prozessen im Namen solcher Benutzer ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später dem betreffenden Benutzer zugeordnet werden können und der Benutzer für seine Handlungen verantwortlich gemacht werden kann.
- **Protokollauswertung**
  Bei vielen Produkten wird sicherzustellen sein, dass sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit durch Nachprüfungen später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.
- **Unverfälschbarkeit**
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und dass Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden.
  Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, Benutzern und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.
- **Zuverlässigkeit**
  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, also nicht früher oder später, und es wird sicherzustellen sein, dass zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen Produkten erforderlich sein sicherzustellen, dass ein Zugriff in dem erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.
- **Übertragungssicherung**
  Dieser Begriff umfasst alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind:

  - Authentisierung
  - Zugriffskontrolle
  - Datenvertraulichkeit
  - Datenintegrität
  - Sende- und Empfangsnachweis

  Einige dieser Funktionen werden mittels kryptographischer Verfahren realisiert.

Darüber hinaus können weitere Sicherheitsanforderungen an Standardsoftware konkretisiert werden.

- **Datensicherung**

An die Verfügbarkeit der mit dem Produkt verarbeiteten Daten werden hohe Anforderungen gestellt. Unter diesen Punkt fallen im Produkt integrierte Funktionen, die Datenverlusten vorbeugen sollen wie die automatische Speicherung von Zwischenergebnissen oder die automatische Erstellung von Sicherungskopien vor der Durchführung größerer Änderungen.

- **Verschlüsselung**
  Verschlüsselung dient der Wahrung der Vertraulichkeit von Daten. Bei vielen Produkten wird es erforderlich sein, Nutzdaten vor einer Übertragung oder nach der Bearbeitung zu verschlüsseln und sie nach Empfang oder vor der Weiterverarbeitung zu entschlüsseln. Hierzu ist ein anerkanntes Verschlüsselungsverfahren zu verwenden. Es ist sicherzustellen, dass die zur Entschlüsselung benötigten Parameter (z. B. Schlüssel) in der Weise geschützt sind, dass kein Unbefugter Zugang zu diesen Daten besitzt.
- **Funktionen zur Wahrung der Datenintegrität**
  Für Daten, deren Integritätsverlust zu Schäden führen kann, können Funktionen eingesetzt werden, die Fehler erkennen lassen oder sogar mittels Redundanz korrigieren können. Meist werden Verfahren zur Integritätsprüfung eingesetzt, die absichtliche Manipulationen am Produkt bzw. den damit erstellten Daten sowie ein unbefugtes Wiedereinspielen von Daten zuverlässig aufdecken können. Sie basieren auf kryptographischen Verfahren (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).
- **Datenschutzrechtliche Anforderungen**
  Wenn mit dem Produkt personenbezogene Daten verarbeitet werden sollen, sind über die genannten Sicherheitsfunktionen hinaus zusätzliche spezielle technische Anforderungen zu stellen, um den Datenschutzbestimmungen genügen zu können.

**Stärke der Mechanismen / Angriffsresistenz**

Sicherheitsfunktionen werden durch Mechanismen umgesetzt. Je nach Einsatzzweck müssen diese Mechanismen eine unterschiedliche Stärke besitzen, mit der sie Angriffe abwehren können. Die erforderliche Stärke der Mechanismen ist im Anforderungskatalog anzugeben. Bei Anwendung der Common Criteria (CC) wird die Angriffsresistenz eines IT-Produktes, das in einer bestimmten Einsatzumgebung betrieben wird, an den in den Sicherheitsvorgaben oder gegebenenfalls in einem Schutzprofil definierten Bedrohungen der zu schützenden Datenobjekte und der für die Evaluierung angesetzten Prüftiefe bewertet. Die geforderte Prüftiefe beinhaltet die Festlegung der Angriffsresistenz und richtet sich nach dem Schutzbedarf und dem Einsatzzweck des Produktes. Die Prüftiefe wird anhand eines Kataloges (siehe CC, Teil 3) meist mittels vordefinierter Evaluierungsstufen (EAL 1 bis 7) festgelegt.

Für die Bewertung der Angriffsresistenz werden die für das Einsatzszenario relevanten Angriffe nach dem Stand der Technik bis zu einer bestimmten Stärke unter Berücksichtigung der erforderlichen Angriffszeit, technischen Expertise des Angreifers, Kenntnissen über das Produkt, Gelegenheit zum Angriff und benötigten Hilfsmittel analysiert. Die Bestätigung der Angriffsresistenz im Rahmen der Zertifizierung erfolgt dabei dann in den Abstufungen niedrig (basic), erweitert (enhanced basic), mittel (moderate) und hoch (high).

Basic bedeutet Schutz gegen öffentlich bekannte Angriffe und gegen Angreifer mit sehr begrenzten Fähigkeiten und Möglichkeiten. Hoch bedeutet, dass ein erfolgreicher Angriff sehr gute Fachkenntnisse, Produktkenntnisse, Gelegenheiten und Betriebsmittel erfordert, und damit insgesamt als extrem aufwändig gilt.

**Beispiele für Anforderungen zu Sicherheitseigenschaften**

Nachfolgend werden für einige wichtige Sicherheitsfunktionen Beispiele genannt, aus denen typische Anforderungen an Sicherheitseigenschaften deutlich werden.

Soll das Produkt über einen **Identifizierungs- und Authentisierungsmechanismus** verfügen, können beispielsweise folgende Anforderungen gestellt werden:

- Der Zugang darf ausschließlich über eine definierte Schnittstelle erfolgen. Dabei kann z. B. ein Anmeldemechanismus zum Einsatz kommen, der eine eindeutige Benutzer-Kennung und ein Passwort verlangt. Wird beim Zugang zum IT-System bereits die Identität des Benutzers sichergestellt, ist eine anonyme Passworteingabe ausreichend. Andere Möglichkeiten sind Verfahren, die auf dem Besitz bestimmter "Token" beruhen, wie z. B. einer Chipkarte.
- Das Zugangsverfahren selbst muss die sicherheitskritischen Parameter, wie Passwort, Benutzer-Kennung, usw., sicher verwalten. So dürfen aktuelle Passwörter nie unverschlüsselt auf den entsprechenden IT-Systemen gespeichert werden.
- Das Zugangsverfahren muss definiert auf Fehleingaben reagieren. Erfolgt zum Beispiel dreimal hintereinander eine fehlerhafte Authentisierung, ist der Zugang zum Produkt zu verwehren oder alternativ sind die zeitlichen Abstände, nach denen ein weiterer Zugangsversuch erlaubt wird, sukzessiv zu vergrößern.
- Das Zugangsverfahren muss das Setzen bestimmter Minimalvorgaben für die sicherheitskritischen Parameter zulassen. So sollte die Mindestlänge eines Passwortes acht Zeichen, die Mindestlänge einer PIN vier Ziffern betragen. Auch die Komplexität für Passwörter sollte vorgegeben werden.

Soll das Produkt über eine **Zugriffskontrolle** verfügen, können beispielsweise folgende Anforderungen gestellt werden:

- Das Produkt muss verschiedene Benutzer unterscheiden können.
- Das Produkt muss je nach Vorgabe Ressourcen einzelnen autorisierten Benutzer zuteilen können und Unberechtigten den Zugriff gänzlich verwehren
- Mittels einer differenzierten Rechtestruktur (lesen, schreiben, ausführen, ändern, ...) sollte der Zugriff geregelt werden können. Die für die Rechteverwaltung relevanten Daten sind manipulationssicher vom Produkt zu verwalten.

Soll das Produkt über eine **Protokollierung** verfügen, können folgende Anforderungen sinnvoll sein:

- Der Mindestumfang, den das Produkt protokollieren können muss, sollte parametrisierbar sein. Beispielsweise sollten folgende Aktionen protokollierbar sein:
  - bei Authentisierung: Benutzer-Kennung, Datum und Uhrzeit, Erfolg, ...,
  - bei der Zugriffskontrolle: Benutzer-Kennung, Datum und Uhrzeit, Erfolg, Art des Zugriffs, was wurde wie geändert, gelesen, geschrieben, ...
  - Durchführung von Administratortätigkeiten,
  - Auftreten von funktionalen Fehlern.
- Die Protokollierung darf von Unberechtigten nicht deaktivierbar sein. Die Protokolle selbst dürfen für Unberechtigte weder lesbar noch modifizierbar sein.

- Die Protokollierung muss übersichtlich, vollständig und korrekt sein.

Soll das Produkt über eine **Protokollauswertung** verfügen, können folgende Anforderungen sinnvoll sein:

- Eine Auswertefunktion muss nach den bei der Protokollierung geforderten Datenarten unterscheiden können (z. B. "Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum").
- Die Auswertefunktion muss auswertbare ("lesbare") Berichte erzeugen, so dass keine sicherheitskritischen Aktivitäten übersehen werden.

Soll das Produkt über Funktionen zur **Unverfälschbarkeit** verfügen, könnte beispielsweise folgende Anforderung gestellt werden:

- Ein Datenbank-Managementsystem muss über Möglichkeiten zur Beschreibung von Regeln bestimmter Beziehungen zwischen den gespeicherten Daten verfügen (z. B. referentielle Integrität). Außerdem müssen geeignete Mechanismen existieren, die verhindern, dass es durch Änderungen der Daten zu Verstößen gegen diese Regeln kommt.

Soll das Produkt über Funktionen zur **Datensicherung** verfügen, können beispielsweise folgende Anforderungen gestellt werden:

- Es muss konfigurierbar sein, welche Daten wann gesichert werden.
- Es muss eine Option zum Einspielen beliebiger Datensicherungen existieren.
- Die Funktion muss das Sichern von mehreren Generationen ermöglichen.
- Datensicherungen von Zwischenergebnissen aus der laufenden Anwendung sollen möglich sein.

Soll das Produkt über eine **Verschlüsselungskomponente** verfügen, sind folgende Anforderungen sinnvoll:

- Der implementierte Verschlüsselungsalgorithmus sollte dem Schutzbedarf entsprechen und eine ausreichende Mechanismenstärke besitzen (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*).
- Das Schlüsselmanagement muss mit der Funktionalität des Produktes harmonieren. Dabei sind insbesondere grundsätzliche Unterschiede der Algorithmen zu berücksichtigen:
  - symmetrische Verfahren benutzen einen geheim zu haltenden Schlüssel für die Ver- und Entschlüsselung,
  - asymmetrische Verfahren benutzen einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten (geheim zu haltenden) für die Entschlüsselung.
- Das Produkt muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar, auf den entsprechenden IT-Systemen abgelegt werden.

Soll das Produkt über Mechanismen zur **Integritätsprüfung** verfügen, sind folgende Anforderungen sinnvoll:

- Das Produkt führt bei jedem Programmaufruf einen Integritätscheck durch.
- Bei der Datenübertragung müssen Mechanismen eingesetzt werden, mit denen absichtliche Manipulationen an den Adressfeldern und den Nutzdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, unerkannte Manipulationen an den obengenannten Daten vorzunehmen.

Werden personenbezogene Daten mit dem Produkt verarbeitet, können beispielsweise folgende **datenschutzrechtlichen Anforderungen** gestellt werden:

- Das Produkt darf keine freie Abfrage für Datenauswertungen zulassen. Die Auswertungen von Datensätzen müssen auf bestimmte Kriterien einschränkbar sein.
- Es muss parametrisierbar sein, dass für bestimmte Dateien Änderungen, Löschungen oder Ausdrucke von personenbezogenen Daten nur nach dem Vier-Augen-Prinzip möglich sind.
- Die Protokollierung muss parametrisierbar sein, so dass aufgezeichnet werden kann, wer wann an welchen personenbezogenen Daten welche Änderungen vorgenommen hat.
- Die Übermittlung personenbezogener Daten muss durch geeignete Stichprobenverfahren festgestellt und überprüft werden können (BDSG, § 10). Die Art der Stichprobe muss sich individuell einstellen lassen.
- Das Produkt muss das Löschen von personenbezogenen Daten ermöglichen. Ersatzweise muss das Sperren personenbezogener Daten möglich sein, um ihre weitere Verarbeitung oder Nutzung einzuschränken bzw. zu verhindern.

**Bewertungsskala**

Um einen Vergleich verschiedener Produkte im Sinne einer Nutzwertanalyse durchführen zu können, müssen Kriterien vorhanden sein, wie die Erfüllung der einzelnen Anforderungen gewertet wird. Dazu ist es erforderlich, vorab die Bedeutung der einzelnen Anforderungen für die angestrebte IT-gestützte Aufgabenerfüllung quantitativ oder qualitativ zu bewerten.

Diese Bewertung kann beispielsweise in drei Stufen vorgenommen werden. In der ersten Stufe wird festgelegt, welche im Anforderungskatalog geforderten Eigenschaften **notwendig** und welche **wünschenswert** sind. Wenn eine notwendige Eigenschaft nicht erfüllt ist, wird das Produkt abgelehnt (so genanntes K.O.-Kriterium). Das Fehlen einer wünschenswerten Eigenschaft wird zwar negativ gewertet, dennoch wird aber das Produkt aufgrund dessen nicht zwingend abgelehnt.

Als zweite Stufe wird die **Bedeutung** der geforderten wünschenswerten Eigenschaft für die Aufgabenerfüllung angegeben. Dies kann z. B. quantitativ mit Werten zwischen 1 für niedrig und 5 für hoch erfolgen. Notwendige Eigenschaften müssen nicht quantitativ bewertet werden. Ist dies aber aus rechnerischen Gründen erforderlich, müssen sie auf jeden Fall höher bewertet werden als jede wünschenswerte Eigenschaft (um die Bedeutung einer notwendigen Eigenschaft hervorzuheben, kann sie z. B. mit 10 bewertet werden).

In der dritten Stufe wird ein **Vertrauensanspruch** für die Korrektheit der geforderten Eigenschaften für die Aufgabenerfüllung angegeben (z. B. mit Werten zwischen 1 für niedrig und 5 für hoch). Anhand des Vertrauensanspruchs wird später entschieden, wie eingehend die Eigenschaft getestet wird. Der Vertrauensanspruch der Sicherheitsmechanismen muss entsprechend ihrer Mechanismenstärke bewertet werden, beispielsweise kombiniert man

- Mechanismenstärke niedrig mit Vertrauensanspruch 1
- Mechanismenstärke mittel mit Vertrauensanspruch 3
- Mechanismenstärke hoch mit Vertrauensanspruch 5

Diese Orientierungswerte müssen im Einzelfall verifiziert werden.

**Beispiele:**

Auszugsweise sollen für einige typische Standardsoftwareprodukte Sicherheitsanforderungen erläutert werden:

**Textverarbeitungsprogramm:**

Notwendige Sicherheitseigenschaften:

- Automatische Datensicherung von Zwischenergebnissen im laufenden Betrieb

Wünschenswerte Sicherheitseigenschaften:

- Passwortschutz einzelner Dateien
- Verschlüsselung einzelner Dateien
- Makro-Programmierung muss abschaltbar sein

**Dateikompressionsprogramm:**

Notwendige Sicherheitseigenschaften:

- Im Sinne der Datensicherung dürfen nach Kompression zu löschende Dateien erst dann vom Kompressionsprogramm gelöscht werden, wenn die Kompression fehlerfrei abgeschlossen wurde.
- Vor der Dekomprimierung einer Datei muss deren Integrität überprüft werden, damit z. B. Bitfehler in der komprimierten Datei erkannt werden.

Wünschenswerte Sicherheitseigenschaften:

- Passwortschutz komprimierter Dateien

**Terminplaner:**

Notwendige Sicherheitseigenschaften:

- Eine sichere Identifikation und Authentisierung der einzelnen Benutzer muss erzwungen werden, z. B. über Passwörter.
- Eine Zugriffskontrolle für die Terminpläne der einzelnen Mitarbeiter ist erforderlich.
- Zugriffsrechte müssen für Einzelne, Gruppen und Vorgesetzte getrennt vergeben werden können.
- Eine Unterscheidung zwischen Lese- und Schreibrecht muss möglich sein.

Wünschenswerte Sicherheitseigenschaften:

- Eine automatisierte Datensicherung in verschlüsselter Form ist vorzusehen.

**Reisekostenabrechnungssystem:**

Notwendige Sicherheitseigenschaften:

- Eine sichere Identifikation und Authentisierung der einzelnen Benutzer muss erzwungen werden, z. B. über Passwörter.
- Eine Zugriffskontrolle muss vorhanden und auch für einzelne Datensätze einsetzbar sein.
- Zugriffsrechte müssen für Benutzer, Administrator, Revisor und Datenschutzbeauftragten getrennt vergeben werden können. Eine Rollentrennung zwischen Administrator und Revisor muss durchführbar sein.
- Datensicherungen müssen so durchgeführt werden können, dass sie verschlüsselt abgelegt werden und nur von Berechtigten wiedereingespielt werden können.
- Detaillierte Protokollierungsfunktionen müssen verfügbar sein.

Wünschenswerte Sicherheitseigenschaften:

- Ein optionaler Integritätscheck für zahlungsrelevante Daten sollte angeboten werden.

**Beispiel für eine Bewertungsskala:**

Eine Fachabteilung will für Datensicherungszwecke ein Komprimierungsprogramm beschaffen. Nach der Erstellung eines Anforderungskataloges könnten die dort spezifizierten Eigenschaften wie folgt bewertet werden:

| Eigenschaft | notwendig | wünschenswert | Bedeutung | Vertrauensanspruch |
|---|---|---|---|---|
| korrekte Kompression und Dekompression | X | | 10 | 5 |
| Erkennen von Bitfehlern in einer komprimierten Datei | X | | 10 | 2 |
| Löschung von Dateien nur nach erfolgreicher Kompression | X | | 10 | 3 |
| Windows-PC, x86, 256 MB | X | | 10 | 5 |
| Linux-tauglich | | X | 2 | 1 |
| Durchsatz bei 1 GHz über 10 MB/s | | X | 4 | 3 |
| Kompressionsrate über 40% bei Textdateien des Programms XYZ | | X | 4 | 3 |
| Online-Hilfefunktion | | X | 3 | 1 |
| Maximale Kosten 50.- Euro pro Lizenz | X | | 10 | 5 |
| Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch) | | X | 2 | 5 |

Prüffragen:

- Wird für die Auswahl von einzusetzenden Software-Produkten ein Anforderungskatalog erstellt, der Sicherheitsanforderungen umfasst?

- Wurde eine Bewertungsskala zu den einzelnen Anforderungen an Software-Produkte erstellt, um die Produkte vergleichen zu können?

# M 2.81 Vorauswahl eines geeigneten Standardsoftwareproduktes

**Verantwortlich für Initiierung:** Beschaffungsstelle
**Verantwortlich für Umsetzung:** Beschaffungsstelle, Fachabteilung, Leiter IT

Die Vorauswahl eines Standardsoftwareproduktes orientiert sich an dem durch die Fachabteilung und den IT-Bereich aufgestellten Anforderungskatalog. Zunächst sollte die für die Vorauswahl zuständige Stelle eine Marktanalyse durchführen, bei der anhand des Anforderungskatalogs eine tabellarische Marktübersicht erarbeitet werden sollte. In dieser Tabelle sollten für die in Frage kommenden Produkte Aussagen zu den im Anforderungskatalog festgehaltenen Punkten gemacht werden.

Die Marktübersicht sollte vom IT-Bereich erarbeitet werden, sie kann anhand von Produktbeschreibungen, Herstelleraussagen, Fachzeitschriften oder Händlerauskünften erstellt werden. Alternativ ist eine Ausschreibung möglich und teilweise vorgegeben. Der Anforderungskatalog ist Grundlage einer Ausschreibung, so dass anhand der eingehenden Angebote eine vergleichbare Marktübersicht erstellt werden kann.

Anschließend müssen die in der Marktübersicht erfassten Produkte bzgl. der Vorgaben des Anforderungskatalogs bewertet werden. Hierzu kann die in M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* erarbeitete Bewertungsskala eingesetzt werden. Anhand der vorliegenden Informationen wird festgestellt, welche der geforderten Eigenschaften des Produktes vorhanden sind. Fehlen dem Produkt notwendige Eigenschaften, wird es verworfen. Über die Bewertung der Bedeutung der einzelnen Eigenschaften jedes Produktes kann eine Summe ermittelt werden. Anhand dieser Summen kann nun eine Hitliste für die Produkte aus der Vorauswahl erstellt werden.

**Beispiel:**

Die im Anforderungskatalog geforderten und bewerteten Eigenschaften für ein Komprimierungsprogramm werden nun wie folgt gewichtet:

| **Eigenschaft** | **Notwendig/ Wünschenswert** | **Bedeutung** | **Produkt 1** | **Produkt 2** | **Produkt 3** | **Produkt 4** |
|---|---|---|---|---|---|---|
| korrekte Kompression und Dekompression | N | 10 | j | j | j | j |
| Erkennen von Bitfehlern in einer komprimierten Datei | N | 10 | j | j | K.O. | j |

| Eigenschaft | Notwendig/ Wünschenswert | Bedeutung | Produkt 1 | Produkt 2 | Produkt 3 | Produkt 4 |
|---|---|---|---|---|---|---|
| Löschung von Dateien nur nach erfolgreicher Kompression | N | 10 | j | j | j | j |
| DOS-PC, 80486, 8 MB | N | 10 | j | j | j | j |
| Windows-tauglich | W | 2 | n | j | j | j |
| Durchsatz bei 50 MHz über 1 MB/s | W | 4 | j | j | j | n |
| Kompressionsrate über 40% bei Textdateien des Programms XYZ | W | 4 | j | j | n | n |
| Online-Hilfefunktion | W | 3 | n | n | n | j |
| Maximale Kosten 50.- Euro pro Lizenz | N | 10 | j | j | j | j |
| Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch) | W | 2 | j | j | n | j |
| Bewertung | | 65 (=Max.) | 60 | 62 | K.O. | 57 |

Als Ergebnis ergibt sich, dass Produkt 3 herausfällt, da eine notwendige Eigenschaft nicht gegeben ist. Ansonsten wird die Hitliste angeführt von Produkt 2, gefolgt von Produkt 1 und 4.

Die erstellte Hitliste zusammen mit der Marktübersicht sollte dann der Beschaffungsstelle vorgelegt werden, damit dieser überprüfen kann, inwieweit die dort aufgeführten Produkte den internen Regelungen und gesetzlichen Vorgaben entsprechen. Dabei muss die Beschaffungsstelle auch darauf achten, dass die anderen Stellen, deren Vorgaben eingehalten werden müssen, wie der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte oder der Personal- bzw. Betriebsrat, rechtzeitig beteiligt werden.

Es muss entschieden werden, wie viele und welche Kandidaten der Hitliste getestet werden sollen. Sinnvollerweise sollten die ersten zwei oder drei Spitzenkandidaten ausgewählt werden und daraufhin getestet werden, ob sie die wichtigsten Kriterien des Anforderungskatalogs auch tatsächlich erfüllen. Dies ist insbesondere für die notwendigen Anforderungen wichtig. Hierfür sollten Testlizenzen beschafft werden und, wie in M 2.82 *Entwicklung eines Testplans für Standardsoftware* und M 2.83 *Testen von Standardsoftware* beschrieben, Tests durchgeführt werden.

Neben den Kriterien des Anforderungskatalogs können für die Entscheidung noch die folgenden Punkte berücksichtigt werden:

- **Referenzen**
  Kann der Hersteller oder Vertreiber für sein Produkt Referenzinstallationen angeben, so können die dort gemachten Erfahrungen hinterfragt und in die Produktbeurteilung einbezogen werden.
  Liegen externe Testergebnisse oder Qualitätsaussagen für das zu testende Softwareprodukt vor (z. B. Testergebnisse in Fachzeitschriften, Konformitätstests nach proprietären Standards, Prüfungen und Zertifikate nach einschlägigen Standards und Normen wie ISO 12119), so sollten auch diese Ergebnisse bei der Vorauswahl berücksichtigt werden.
- **Verbreitungsgrad des Produktes**
  Bei einem hohen Verbreitungsgrad hat der einzelne Anwender wenig oder keinen Einfluss auf den Hersteller des Produkts, wenn es um die Behebung von Fehlern oder die Implementation bestimmter Funktionalitäten geht. Er kann aber davon ausgehen, dass das Produkt weiterentwickelt wird. Oft gibt es externe Tests, die durch den Hersteller beauftragt oder von Fachzeitschriften durchgeführt wurden. Bei Produkten mit hohem Verbreitungsgrad ist im allgemeinen mehr über Schwachstellen bekannt, so dass der Anwender davon ausgehen kann, dass die wesentlichen Schwachstellen bereits bekannt sind, bzw. dass das Wissen über Schwachstellen schnell verbreitet wird und er nach dem Bekanntwerden Abhilfe schaffen kann.
  Bei einem niedrigen Verbreitungsgrad kann ein Anwender mehr Einfluss auf den Hersteller nehmen. Externe Tests liegen im allgemeinen nicht vor, da sie für Produkte kleiner Hersteller zu aufwendig und zu teuer sind. Produkte mit niedrigem Verbreitungsgrad enthalten meist nicht mehr oder weniger Schwachstellen als solche mit hohem Verbreitungsgrad. Nachteil ist hier, dass diese evtl. nicht so schnell bekannt werden und damit behoben werden können. Wenn es sich aber um Sicherheitslücken handelt, sind diese aber wahrscheinlich auch potentiellen Angreifer nicht bekannt bzw. keine lohnenden Angriffsziele.
- **Wirtschaftlichkeit / Kosten für Kauf, Betrieb, Wartung, Schulung**
  Vor der Entscheidung für ein Produkt sollte immer die Frage stehen, ob die Kosten für das Produkt in einem angemessenen Verhältnis zu dem damit

erzielbaren Nutzen stehen. In die unmittelbaren Anschaffungskosten sind darüber hinaus alle Folgekosten für Betrieb, Wartung und Schulung einzubeziehen. Dazu muss z. B. geklärt werden, ob die vorhandene Hardware-Plattform aufgerüstet werden muss oder ob für Installation und Betrieb Schulungen erforderlich sind.

Ist dann die Kaufentscheidung für ein Produkt gefallen, sollte der Kauf natürlich beim günstigsten Anbieter getätigt werden. Dieser hat sich evtl. schon bei der Marktsichtung herauskristallisiert.

Prüffragen:

- Wird zur Vorauswahl von Standardsoftware auf Basis des Anforderungskataloges eine Marktübersicht erstellt?
- Wird der Aufwand zur Schulung der Benutzer im Umgang mit neuen Standardsoftwareprodukten in die Auswahl einbezogen?

# M 2.82 Entwicklung eines Testplans für Standardsoftware

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter Fachabteilung, Leiter IT

Die im nachfolgenden beschriebene Vorgehensweise beim Testen orientiert sich an den Standardwerken DIN ISO/IEC 12119 "Software-Erzeugnisse, Qualitätsanforderungen und Prüfbestimmungen", Vorgehensmodell für die Planung und Durchführung von IT-Vorhaben (V-Modell) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), die als weiterführende Literatur empfohlen werden.

Vor der Entscheidung für ein geeignetes Standardsoftwareprodukt müssen die nach der Vorauswahl (siehe M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes*) in die engere Wahl gezogenen Produkte als Testlizenz beschafft und ausreichend getestet werden. War es aufgrund zeitlicher Beschränkungen, institutionsinterner Beschaffungsempfehlungen (Einhaltung von Hausstandards) oder anderen Gründen nicht möglich, dass Produkt vor der Beschaffung zu testen, müssen auf jeden Fall Tests vor der endgültigen Inbetriebnahme durchgeführt werden. Die Ergebnisse dieser Tests liefern dann die Grundlage für die Installationsvorschriften und anderer Freigabe-Bedingungen.

Obwohl bereits bei der Vorauswahl eine Überprüfung der notwendigen Anforderungen an das Produkt aufgrund der Herstelleraussagen stattgefunden hat, kann man nicht davon ausgehen, dass diese Anforderungen auch im gewünschten Maße erfüllt werden. Vielmehr muss nun durch systematisches Testen die Eignung und Zuverlässigkeit des Produktes auf Grundlage des Anforderungskataloges überprüft werden, um das geeignetste Produkt auszuwählen.

Dabei bietet es sich an, das Testen in vier Bereiche einzuteilen:

- Eingangsprüfungen (Prüfung auf Computer-Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, ....),
- funktionale Tests (Überprüfung der funktionalen Anforderungen),
- Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation), und
- sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen).

Das prinzipielle Vorgehen beim Testen von Standardsoftware zeigt die folgende Abbildung.

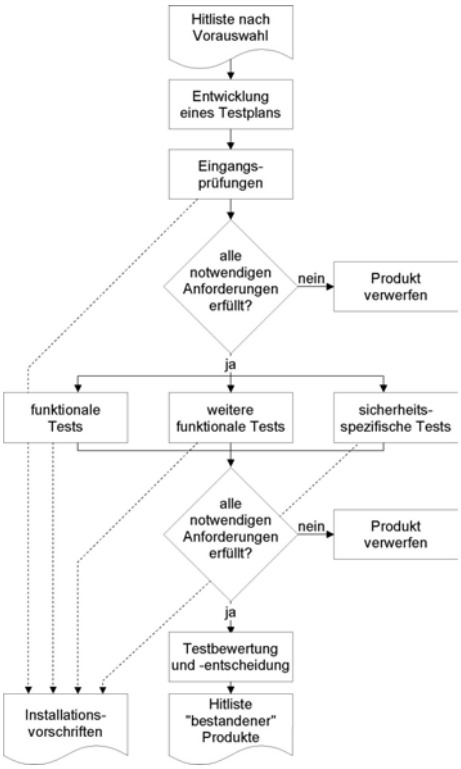



Abbildung 1: Prinzipielles Vorgehen beim Testen von Standardsoftware

Anhand der bei der Vorauswahl erstellten Hitliste sind diejenigen Produkte auszuwählen, die getestet werden sollen. Anschließend wird ein **Testplan** entwickelt.

Dieser umfasst folgende Inhalte:

- Festlegung der Testinhalte anhand des Anforderungskataloges,
- Überprüfung von Referenzen,
- Festlegung des Gesamtprüfaufwandes,
- Zeitplanung einschließlich Prüfaufwand je Testinhalt,
- Festlegung der Testverantwortlichen,
- Testumgebung,
- Inhalt der Testdokumentation,
- Festlegung von Entscheidungskriterien.

Die einzelnen genannten Punkte werden nachfolgend erläutert.

### Festlegung der Testinhalte anhand des Anforderungskataloges

Aus dem Anforderungskatalog werden diejenigen Anforderungen ausgewählt, die überprüft werden sollen. Dies sollten insbesondere diejenigen Eigenschaften sein, die eine große Bedeutung oder einen hohen Vertrauensanspruch besitzen.

### Überprüfung von Referenzen

Bei der Vorauswahl (siehe M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes*) wurden bereits erste Referenzen über die zu testenden Produkte eingeholt. Diese können ersatzweise herangezogen werden, wenn man der jeweiligen externen Testgruppe ausreichendes Vertrauen entgegenbringt.

Wurde für das Produkt ein Zertifikat nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) oder den Common Criteria (CC) vergeben, ist anhand des Zertifizierungsreportes zu prüfen, inwieweit die dort dokumentierten Testergebnisse berücksichtigt werden können.

Gegebenenfalls können dann eigene Test unterbleiben oder in geringerem Umfang stattfinden. Die frei werdenden Kapazitäten können auf andere Testinhalte verteilt werden.

**Festlegung des Gesamtprüfaufwandes**

Um den Aufwand für die Tests nicht ausufern zu lassen, sollte vorab der Gesamtprüfaufwand festgelegt werden, z. B. in Personentagen oder durch Fristsetzung.

**Zeitplanung einschließlich Prüfaufwand je Testinhalt**

Beim Testen mehrerer Produkte empfiehlt es sich, diese vergleichend zu testen. Das heißt, alle Produkte werden von einer Testgruppe bzgl. einer Anforderung des Anforderungskataloges getestet. Der Prüfaufwand ist damit für jede Anforderung des Anforderungskataloges festzulegen und wird damit automatisch gleichmäßig auf alle zu testenden Produkte verteilt. Der Prüfaufwand ergibt sich dabei aus Prüftiefe und Komplexität der Eigenschaft. Die Prüftiefe der jeweiligen Eigenschaften sollte sich zum einen an ihrem Vertrauensanspruch, das heißt an dem Vertrauen orientieren, das der Korrektheit dieser Eigenschaft entgegengebracht werden muss.

Zum anderen muss aber auch die Fehleranfälligkeit und Nutzungshäufigkeit der jeweiligen Eigenschaft berücksichtigt werden. Ausführlichere Informationen sind der Norm ISO 12119 zu entnehmen.

**Hinweise:**
- Für sicherheitsspezifische Anforderungen kann die Prüftiefe entsprechend der geforderten Mechanismenstärke zusätzlich relativiert werden.
- Der Prüfaufwand für die Eingangsprüfungen sollte gemessen an den anderen Tests gering sein.

Abschließend ist der Gesamtprüfaufwand entsprechend dem relativen Prüfaufwand der jeweiligen Eigenschaft auf die einzelnen Testabschnitte zu verteilen.

**Festlegung der Testverantwortlichen**

Für jeden Testinhalt ist nun festzulegen, welche Aufgaben durchzuführen sind und wer dafür verantwortlich ist. Insbesondere ist zu beachten, dass bei einigen Testinhalten der Personal- bzw. Betriebsrat, der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte zu beteiligen ist.

**Testumgebung**

Testen ist immer destruktiv, da vorsätzlich nach Fehlern gesucht wird. Aus diesem Grund muss das Testen immer in einer isolierten Testumgebung erfolgen.

Die Testumgebung sollte nach Möglichkeit ein genaues funktionales Abbild der Produktionsumgebung sein. In der Regel ist es jedoch nicht wirtschaftlich, die Produktionsumgebung in vollem Umfang nachzubilden.

Damit für die ausgewählten Produkte gleiche Randbedingungen gegeben sind, sollte eine Referenztestumgebung definiert werden. Für einzelne Tests kann diese weiter angepasst oder eingeschränkt werden.

Die für die einzelnen Prüfungen benötigten Ressourcen (Betriebsmittel, IT-Infrastruktur) sind zu spezifizieren. Es sollte im Detail beschrieben werden, wann und in welchem Umfang sie verfügbar sein müssen.

Wichtig ist, dass alle Betriebssysteme in allen im Produktionsbetrieb eingesetzten Versionen (Releases) in der Testumgebung zur Verfügung stehen. Die Intention ist dabei die Ermittlung von systembedingten Schwachstellen von Komponenten der Produktionsumgebung im Zusammenspiel mit dem zu installierenden Standardsoftwareprodukt. In Ausnahmefällen, wenn sich Aspekte verallgemeinern lassen, kann auf einzelne Komponenten verzichtet werden.

Folgende weitere Aspekte sind unbedingt zu beachten und helfen, eine sichere und geeignete Testumgebung aufzubauen:

- Die Freiheit von Schadprogrammen der Testumgebung ist durch ein aktuelles Viren-Suchprogramm sicherzustellen.
- Die Testumgebung muss frei sein von Seiteneffekten auf den Echtbetrieb. Um Wechselwirkungen von vornherein zu vermeiden, empfiehlt es sich, dedizierte IT-Systeme zu installieren.
- Die Zugriffsrechte müssen in der Testumgebung derart konfiguriert werden, wie sie dem Produktionsbetrieb entsprechen.
- Der Zutritt und Zugang zur Testumgebung muss geregelt sein.
- Es muss sichergestellt werden, dass das Produkt genau in der Testumgebung ermittelten Konfiguration in den Produktionsbetrieb übernommen wird. Daher ist in der Testumgebung ein geeignetes Verfahren zum Integritätsschutz einzusetzen (digitale Signaturen, Checksummen).
- Die Kosten für den Aufbau der Testumgebung müssen angemessen sein.

Nach Beendigung aller geplanten Tests ist zu entscheiden, ob die Testumgebung abgebaut werden soll. Ggf. sind weitere Tests auch nach der Beschaffung eines Produktes notwendig, so dass es eventuell wirtschaftlich ist, die Testumgebung vorzuhalten. Vor dem Abbau der Testumgebung sind die Testdaten zu löschen, falls sie nicht mehr benötigt werden (z. B. für eine spätere Installation). Druckerzeugnisse sind ordnungsgemäß zu entsorgen, Programme sind zu deinstallieren. Die Testlizenzen der nicht ausgewählten Produkte sind zurückzugeben.

**Inhalt der Testdokumentation**

Im Testplan ist vorzugeben, wie ausführlich die Testdokumentation zu erstellen ist. Hierbei sind die Aspekte der Nachvollziehbarkeit, Reproduzierbarkeit und Vollständigkeit zu berücksichtigen.

Die Testdokumentation muss Testpläne, -ziele, -verfahren und -ergebnisse enthalten und die Übereinstimmung zwischen den Tests und den spezifizierten Anforderungen beschreiben. Sämtliche Testaktivitäten sowie die getroffene Testbewertung (inklusive Entscheidungsargumentation) sind schriftlich festzuhalten. Dazu gehören im einzelnen

- Produktbezeichnung und Beschreibung,
- Testbeginn, -ende und -aufwand,
- Testverantwortliche,
- Konfiguration der Testumgebung,
- Beschreibung der Testfälle,
- Entscheidungskriterien, Testergebnisse und Argumentationsketten, und

- nicht erfüllte Anforderungen des Anforderungskataloges.

Der Testgruppe sollte eine Möglichkeit zur übersichtlichen Dokumentation und Protokollierung der Testaktivitäten und -ergebnisse zur Verfügung gestellt werden (z. B. Protokollierungstool, Formblätter o. Ä.).

Wird beim Testen ein automatisiertes Werkzeug verwendet, muss die Testdokumentation ausreichende Informationen über dieses Werkzeug und die Art seines Einsatzes enthalten, damit die Entscheidung nachvollzogen werden kann.

**Festlegung von Entscheidungskriterien**

Bei der Bewertung der jeweiligen Testinhalte kann beispielsweise folgende dreistufige Skala verwendet werden:

| **Note** | | **Entscheidungskriterien** |
|---|---|---|
| 0 | - | Anforderungen sind nicht erfüllt. |
| | oder | |
| | - | Es wurden nicht tolerierbare Fehler festgestellt, die sich nicht beheben lassen. |
| 1 | - | Anforderungen sind erfüllt, aber es bestehen Vorbehalte (z. B. Funktion ist nur eingeschränkt geeignet). |
| | oder | |
| | - | Es sind geringfügige Fehler festgestellt worden. Diese spielen nur eine untergeordnete Rolle, da sie tolerierbare Auswirkungen auf den Produktionsbetrieb haben oder da sie nur mit vernachlässigbarer Wahrscheinlichkeit vorkommen können. |
| 2 | - | Anforderungen sind in vollem Umfang erfüllt. |
| | oder | |
| | - | Fehler, die ggf. aufgetaucht sind, sind entweder zu beheben oder haben für den Betrieb keinerlei Bedeutung. |

Tabelle: Bewertungsskala

Sind Fehler aufgetaucht, die nicht reproduziert werden können, hat der Prüfer zu entscheiden, welcher Kategorie (Note) der Fehler zuzuordnen ist.

Sind Fehler aufgetreten, die während des Tests behoben werden können, ist nach deren Behebung erneut im erforderlichen Umfang zu testen.

**Beispiel:**

Das Beispiel des Kompressionsprogramms aus M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes* wird hier fortgesetzt, um eine Möglichkeit zu beschreiben, den Prüfaufwand für jede Anforderung des Anforderungskataloges festzulegen. Hier wird der Prüfaufwand aus Prüftiefe und Komplexität abgeleitet. Der Vertrauensanspruch kennzeichnet den Bedarf an Vertrauen in die Eigenschaft.

Die Nutzungshäufigkeit, Fehleranfälligkeit und Komplexität einer Eigenschaft werden wie folgt bewertet:

- 1 bedeutet "niedrig",
- 2 bedeutet "mittel",
- 3 bedeutet "hoch".

Ein besonderer Fall ist gegeben, wenn eine unveränderbare Eigenschaft des Produktes betrachtet werden soll, die unabhängig von der Fehleranfälligkeit oder Nutzungshäufigkeit ist. Für diesen Fall wird der Wert 0 vergeben. Für das Beispiel des Kompressionsprogramms ergibt sich folgende Abbildung:

| | Vertrauensanspruch | Fehleranfälligkeit | Nutzungshäufigkeit | Prüftiefe | Komplexität | Prüfaufwand | in % |
|---|---|---|---|---|---|---|---|
| korrekte Kompression und Dekompression | 5 | 2 | 3 | 10 | 2 | 20 | 23 |
| Erkennen von Bitfehlern in einer komprimierten Datei | 2 | 2 | 1 | 5 | 2 | 10 | 11 |
| Löschen von Dateien nur nach erfolgreicher Kompression | 3 | 2 | 1 | 6 | 1 | 6 | 7 |
| DOS-PC, 80486, 8 MB | 5 | 0 | 0 | 5 | 1 | 5 | 6 |
| Windows-tauglich | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| Durchsatz bei 50 MHz über 1 MB/s | 3 | 1 | 2 | 6 | 1 | 6 | 7 |
| Kompressionsrate über 40% für Textdateien des Programms XYZ | 3 | 2 | 2 | 7 | 1 | 7 | 8 |
| Online-Hilfefunktion | 1 | 1 | 2 | 4 | 1 | 4 | 5 |
| Maximal Kosten 50,00 EUR pro Lizenz | 5 | 0 | 0 | 5 | 1 | 5 | 5 |
| Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch) | 5 | 1 | 2 | 8 | 3 | 24 | 27 |

Abbildung 2: Beispiel für Kompressionsprogramm

In diesem Beispiel wurde der Prüfaufwand folgendermaßen definiert:

*Prüfaufwand = Komplexität * Prüftiefe*

dabei ist

*Prüftiefe = Vertrauensanspruch + Fehleranfälligkeit + Nutzungshäufigkeit*

(Die Prozentzahlen für den Prüfaufwand in der letzten Spalte der Tabelle ergeben sich aus den für den Prüfaufwand errechneten Werten bei Division durch die Summe dieser Werte.)

Ein Beispiel für eine andere Methode, den Prüfaufwand zu berechnen und die Prüfergebnisse zu bewerten, findet sich in der Norm ISO 12119. Hier wird folgende Gewichtung der einzelnen Anforderungen vorgenommen: *Bewertung jedes Prüfinhaltes =(Komplexität+Fehleranfälligkeit) * (Benutzungshäufigkeit + Wichtigkeit)*.

Letztendlich muss der Testverantwortliche eine dem Produkt und der Institution adäquate Bewertungsmethode individuell festlegen.

Nach Erstellung des Testplans wird für jeden im Testplan spezifizierten Testinhalt ein Tester oder eine Testgruppe mit der Durchführung des ihr zugeteilten Tests beauftragt. Der Testplan ist der Testgruppe zu übergeben und die für die Einzeltests vorgegebenen Zeiten sind mitzuteilen.

Prüffragen:

- Ist ein Testplan für das Testen von Standardsoftware auf Basis des Anforderungskataloges erstellt?
- Ist die Testumgebung logisch oder physisch von der Produktivumgebung getrennt?
- Existiert eine nachvollziehbare, reproduzierbare und vollständige Testdokumentation?
- Enthält die Testdokumentation Testpläne, -ziele, -verfahren und -ergebnisse und zeigt die Übereinstimmung zwischen den Tests und den spezifizierten Anforderungen?

# M 2.83 Testen von Standardsoftware

**Verantwortlich für Initiierung:** Leiter Fachabteilung, Leiter IT
**Verantwortlich für Umsetzung:** Tester

Das Testen von Standardsoftware lässt sich in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilen. In diesen Abschnitten sind folgende Aufgaben wahrzunehmen:

**Testvorbereitung**
- Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)
- Generierung von Testdaten und Testfällen
- Aufbau der benötigten Testumgebung

**Testdurchführung**
- Eingangsprüfungen
- Funktionale Tests
- Tests weiterer funktionaler Eigenschaften
- Sicherheitsspezifische Tests
- Pilotanwendung

**Testauswertung**

Die einzelnen Aufgaben werden nachfolgend beschrieben.

**Testvorbereitung**

**Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)**

Methoden zur Durchführung von Tests sind z. B. statistische Analyse, Simulation, Korrektheitsbeweis, symbolische Programmausführung, Review, Inspektion, Versagensanalyse. Hierbei muss beachtet werden, dass einige dieser Testmethoden nur bei Vorliegen des Quellcodes durchführbar sind. In der Vorbereitungsphase muss die geeignete Testmethode ausgewählt und festgelegt werden.

Es muss geklärt werden, welche Verfahren und Werkzeuge zum Testen von Programmen und zum Prüfen von Dokumenten eingesetzt werden. Typische Verfahren zum Testen von Programmen sind z. B. Black-Box-Tests, White-Box-Tests oder Penetrationstests. Dokumente können z. B. durch informelle Prüfungen, Reviews oder anhand von Checklisten kontrolliert werden.

Ein Black-Box-Test ist ein Funktionalitätstest ohne Kenntnis der internen Programmabläufe, bei dem z. B. das Programm mit allen Datenarten für alle Testfälle mit Fehlerbehandlung und Plausibilitätskontrollen durchlaufen wird.

Bei einem White-Box-Test handelt es sich um einen Funktionalitätstests unter Offenlegung der internen Programmabläufe, z. B. durch Quellcode-Überprüfung oder Tracing. White-Box-Tests gehen in der Regel über den IT-Grundschutz hinaus und können für Standardsoftware in der Regel nicht durchgeführt werden, da der Quellcode vom Hersteller nicht offengelegt wird.

Bei Funktionalitätstests soll der Nachweis erbracht werden soll, dass der Testinhalt der Spezifikation entspricht. Durch Penetrationstests soll festgestellt werden, ob bekannte oder vermutete Schwachstellen im praktischen Betrieb ausgenutzt werden können, beispielsweise durch Manipulationsversuche an

den Sicherheitsmechanismen oder durch Umgehung von Sicherheitsmechanismen durch Manipulationen auf Betriebssystemebene.

Weiterhin ist die Art und Weise der Ergebnissicherung und -auswertung festzuschreiben, insbesondere im Hinblick auf die Wiederholbarkeit von Prüfungen. Es muss geklärt werden, welche Daten während und nach der Prüfung festzuhalten sind.

**Generierung von Testdaten und Testfällen**

Die Vorbereitung von Tests umfasst auch die Generierung von Testdaten. Methode und Vorgehensweise sind zuvor festzulegen und zu beschrieben.

Für jeden einzelnen Testinhalt muss eine dem Testaufwand angemessene Anzahl von Testfällen generiert werden. Jede der folgenden Kategorien ist dabei zu berücksichtigen:

**Standardfälle** sind Fälle, mit denen die korrekte Verarbeitung der definierten Funktionalitäten überprüft werden soll. Die eingehenden Daten nennt man **Normalwerte** oder **Grenzwerte**. Normalwerte sind Daten innerhalb, Grenzwerte sind Eckdaten des jeweils gültigen Eingabebereichs.

**Fehlerfälle** sind Fälle, in denen versucht wird, mögliche Fehlermeldungen des Programms zu provozieren. Diejenigen Eingabewerte, auf die das Programm mit vorgegebenen Fehlermeldungen reagieren soll, nennt man **Falschwerte**.

**Ausnahmefälle** sind Fälle, bei denen das Programm ausnahmsweise anders reagieren muss als bei Standardfällen. Es muss daher überprüft werden, ob das Programm diese Fälle als solche erkennt und korrekt bearbeitet.

**Beispiele:**
- Wenn die Eingabeparameter zwischen 1 und 365 liegen dürfen, sind Testläufe mit Falschwerten (z. B. 0 oder 1000), den Grenzwerten 1 und 365, sowie mit Normalwerten zwischen 1 und 365 durchführen.
- Ein Programm zur Terminplanung soll Feiertage berücksichtigen. Ein Sonderfall ist dann gegeben, wenn ein bestimmter Tag Feiertag in allen Bundesländern ist, außer in einem. Für dieses Bundesland und für diesen Tag muss das Programm dann differenziert reagieren.

Ist die Generierung von Testdaten zu aufwendig oder schwierig, können auch anonymisierte Echtdaten für den Test eingesetzt werden. Aus Gründen des

Vertraulichkeitsschutzes müssen Echtdaten unbedingt zuverlässig anonymisiert werden. Zu beachten bleibt, dass die anonymisierten Echtdaten u. U. nicht alle Grenzwerte und Ausnahmefälle abdecken, so dass diese gesondert erzeugt werden müssen.

Über die Testdaten hinaus sollten auch alle Arten möglicher Benutzerfehler betrachtet werden. Problematisch sind insbesondere alle Benutzerreaktionen, die im Programmablauf nicht vorgesehen und dementsprechend nicht korrekt abgewiesen werden.

**Aufbau der benötigten Testumgebung**

Die im Testplan beschriebene Testumgebung muss aufgebaut und die zu testenden Produkte dort installiert werden. Die eingesetzten Komponenten sind zu identifizieren und deren Konfiguration ist zu beschreiben. Treten bei der Installation des Produktes Abweichungen von der beschriebenen Konfiguration auf, so ist dies zu dokumentieren.

**Testdurchführung**

Die Durchführung der Tests muss anhand des Testplans erfolgen. Jede Aktion sowie die Testergebnisse müssen ausreichend dokumentiert und bewertet werden. Insbesondere wenn Fehler auftreten, sind diese derart zu dokumentieren, dass sie reproduziert werden können. Die für den späteren Produktionsbetrieb geeigneten Betriebsparameter müssen ermittelt und für die spätere Erstellung einer Installationsanweisung festgehalten werden.

Werden zusätzliche Funktionen beim Produkt erkannt, die nicht im Anforderungskatalog aufgeführt, aber trotzdem von Nutzen sein können, so ist hierfür mindestens ein Kurztest durchzuführen. Zeigt sich, dass diese Funktion von besonderer Bedeutung für den späteren Betrieb sind, sind diese ausführlich zu testen. Für den zusätzlich anfallenden Prüfaufwand ist ggf. eine Fristverlängerungen bei den Verantwortlichen zu beantragen. Die Testergebnisse sind in die Gesamtbewertung mit einzubeziehen.

Zeigt sich bei Bearbeitung einzelner Testinhalte, dass eine oder mehrere Anforderungen des Anforderungskataloges nicht konkret genug waren, sind diese gegebenenfalls zu konkretisieren.

**Beispiel:** Im Anforderungskatalog wird zum Vertraulichkeitsschutz der zu bearbeitenden Daten Verschlüsselung gefordert. Während des Testens hat sich gezeigt, dass eine Offline-Verschlüsselung für den Einsatzzweck ungeeignet. Daher ist der Anforderungskatalog hinsichtlich einer Online-Verschlüsselung zu ergänzen. (Eine Offline-Verschlüsselung muss vom Anwender angestoßen und die zu verschlüsselnden Elemente jeweils spezifiziert werden; eine Online-Verschlüsselung erfolgt transparent für den Anwender mit voreingestellten Parametern.)

**Eingangsprüfungen**

Vor allen anderen Tests sind zunächst die folgenden grundlegenden Aspekte zu testen, da ein Misserfolg bei diesen Eingangsprüfungen zu direkten Aktionen oder dem Testabbruch führt:

- Die Computer-Virenfreiheit des Produktes ist durch ein aktuelles Virensuchprogramm zu überprüfen.
- In einem Installationstest muss festgestellt werden, ob das Produkt für den späteren Einsatzzweck einfach, vollständig und nachvollziehbar zu installieren ist. Ebenfalls muss überprüft werden, wie das Produkt vollständig deinstalliert wird.
- Die Lauffähigkeit des Produktes ist in der geplanten Einsatzumgebung zu überprüfen; dies beinhaltet insbesondere eine Überprüfung der Bildschirmaufbereitung, der Druckerausgabe, der Mausunterstützung, der Netzfähigkeit, etc.
- Die Vollständigkeit des Produktes (Programme und Handbücher) ist zu überprüfen, z. B. durch einen Vergleich mit dem Bestandsverzeichnis, der Produktbeschreibung oder ähnlichem.
- Es sollten Kurztests von Funktionen des Programms durchgeführt werden, die nicht explizit in den Anforderungen erwähnt wurden, im Hinblick auf Funktion, Plausibilität, Fehlerfreiheit, etc.

**Funktionale Tests**

Die funktionalen Anforderungen, die im Anforderungskatalog an das Produkt gestellt wurden, sind auf folgende Aspekte zu untersuchen:

- *Existenz der Funktion* durch Aufruf im Programm und Auswertung der Programmdokumentationen.

- Fehlerfreiheit bzw. Korrektheit der Funktion
  Um die Fehlerfreiheit bzw. Korrektheit der Funktion sicherzustellen, sind je nach Prüftiefe bei der Untersuchung unterschiedliche Testverfahren wie Black-Box-Tests, White-Box-Tests oder simulierter Produktionsbetrieb anzuwenden.
  Die in der Vorbereitungsphase erstellten Testdaten und Testfälle werden im Funktionalitätstest eingesetzt. Bei den Funktionalitätstests ist es notwendig, die Testergebnisse mit den vorgegebenen Anforderungen zu vergleichen. Außerdem ist zu überprüfen, wie das Programm bei fehlerhaften Eingabeparametern oder fehlerhafter Bedienung reagiert. Die Funktion ist auch mit den Grenzwerten der Intervalle von Eingabeparametern sowie mit Ausnahmefällen zu testen. Diese müssen entsprechend erkannt und korrekt behandelt werden.
- Eignung der Funktion
  Die Eignung einer Funktion zeichnet sich dadurch aus, dass die Funktion

  - tatsächlich die Aufgabe im geforderten Umfang und effizient erfüllt und
  - sich leicht in die üblichen Arbeitsabläufe integrieren lässt.

  Ist die Eignung der Funktion nicht offensichtlich, bietet es sich an, dies in einem simulierten Produktionsbetrieb, aber immer noch in der Testumgebung zu testen.
- Widerspruchsfreiheit
  Die Widerspruchsfreiheit der einzelnen Funktionen ist zu überprüfen und zwar jeweils zwischen Anforderungskatalog, Dokumentation und Programm. Eventuelle Widersprüche sind zu dokumentieren. Abweichungen zwischen Dokumentation und Programm sind so festzuhalten, dass sie bei einem späteren Einsatz des Produktes in den Ergänzungen zur Dokumentation aufgenommen werden können.

**Tests weiterer funktionaler Eigenschaften**

Die im Anforderungskatalog neben den funktionalen und den sicherheitsspezifischen Anforderungen spezifizierten weiteren funktionalen Eigenschaften sind ebenfalls zu überprüfen:

- Performance
  Das Laufzeitverhalten sollte für alle geplanten Konfigurationen des Produktes ermittelt werden. Um die Performance ausreichend zu testen, sind in der Regel Tests, in denen der Produktionsbetrieb simuliert wird oder auch Pilotanwendung bei ausgewählten Anwendern sinnvoll. Es muss festgestellt werden, ob die gestellten Performanceanforderungen erfüllt sind.
- Zuverlässigkeit
  Das Verhalten bei zufälligen oder mutwillig herbeigeführten Systemabstürzen ("Crash-Test") ist zu analysieren und es ist festzustellen, welche Schäden dabei entstehen. Es ist festzuhalten, ob nach Systemabstürzen ein ordnungsgemäßer und korrekter Wiederanlauf des Produktes möglich ist. Es ist ebenfalls zu überprüfen, ob ein direkter Zugriff auf Datenbestände unabhängig von der regulären Programmfunktion erfolgen kann. In vielen Fällen kann ein solcher Zugriff zu Datenverlusten führen und sollte dann vom Produkt verhindert werden. Ebenfalls sollte festgehalten werden, ob das Programm Möglichkeiten unterstützt, "kritische Aktionen" (z. B. Löschen, Formatieren) rückgängig zu machen.
- Benutzerfreundlichkeit

Ob das Produkt benutzerfreundlich ist, ist in besonderem Maße vom subjektiven Empfinden der Testperson abhängig. Jedoch können bei der Beurteilung folgende Aspekte Anhaltspunkte liefern:

- Technik der Menüoberflächen (Pull-Down-Menüs, Scrolling, Drag & Drop, etc.),
- Design der Menüoberflächen (z. B. Einheitlichkeit, Verständlichkeit, Menüführung),
- Tastaturbelegung,
- Fehlermeldungen,
- problemloses Ansprechen von Schnittstellen (Batchbetrieb, Kommunikation, etc.),
- Lesbarkeit der Benutzerdokumentation,
- Hilfefunktionen.

Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des Produktes beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.

- Wartbarkeit
  Der personelle und finanzielle Aufwand für die Wartung und Pflege des Produktes sollte während des Testens ermittelt werden. Dieser kann z. B. anhand von Referenzen wie anderen Referenzinstallationen oder Tests in Fachzeitschriften oder anhand des während des Testens ermittelten Installationsaufwandes geschätzt werden. Hierfür muss dokumentiert werden, wie viele manuelle Eingriffe während der Installation notwendig waren, um die angestrebte Konfiguration zu erreichen. Sind bereits Erfahrungen mit Vorgängerversionen des getesteten Produktes gesammelt worden, sollte hinterfragt werden, wie aufwendig deren Wartung war.
  Es sollte nachgefragt werden, inwieweit Support durch den Hersteller oder Vertreiber angeboten wird und zu welchen Konditionen. Wird vom Hersteller oder Vertreiber eine Hotline angeboten, sollte auch deren Erreichbarkeit und Güte betrachtet werden.
- Dokumentation
  Die vorliegende Dokumentation muss daraufhin überprüft werden, ob sie vollständig, korrekt und widerspruchsfrei ist. Darüber hinaus sollte sie verständlich, eindeutig, fehlerfrei und übersichtlich sein.
  Es muss weiterhin kontrolliert werden, ob sie für eine sichere Verwendung und Konfiguration ausreicht. Alle sicherheitsspezifischen Funktionen müssen beschrieben sein.

Darüber hinaus sind als weitere Punkte des Anforderungskatalogs zu testen:

- Kompatibilitätsanforderungen
- Interoperabilität
- Konformität zu Standards
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften
- Softwarequalität

**Sicherheitsspezifische Tests**

Wurden sicherheitsspezifische Anforderungen an das Produkt gestellt, so sind zusätzlich zu den vorgenannten Untersuchungen auch folgende Aspekte zu untersuchen:

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und
- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweise beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung und zur Einführung in die Thematik.

Zu Beginn muss durch funktionale Tests zunächst nachgewiesen werden, dass das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt.

Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen. Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen sind **Penetrationstests** durchzuführen. Penetrationstests sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potentielle Schwachstellen ergeben können.

Durch Penetrationstests kann das Testobjekt oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden.

Penetrationstests können durch Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Passwörtern.

Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch ein potentieller Angreifer zur Ausnutzung von Schwachstellen benutzen würde, wie z. B.

- Ändern der vordefinierten Befehlsabfolge,
- Ausführen einer zusätzlichen Funktion,
- Direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten,
- Ausführen von Daten, deren Ausführung nicht vorgesehen ist,
- Verwenden einer Funktion in einem unerwarteten Kontext oder für einen unerwarteten Zweck,
- Aktivieren der Fehlerüberbrückung,
- Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung,
- Unterbrechen der Abfolge durch Interrupts, oder
- Erzeugen einer unerwarteten Eingabe für eine Funktion.

Die Mechanismenstärken werden anhand der Begriffe Fachkenntnisse, Gelegenheiten und Betriebsmittel definiert, in der ITSEM werden diese näher erläutert. Beispielsweise können zur Bestimmung der Mechanismenstärke folgende Regeln angewandt werden:

- Kann der Mechanismus innerhalb von Minuten von einem Laien allein überwunden werden, dann kann er **nicht einmal als niedrig** eingestuft werden.
- Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, dann ist der Mechanismus als **niedrig** einzustufen.
- Wenn für einen erfolgreichen Angriff ein Experte benötigt wird, der mit der vorhandenen Ausstattung Tage braucht, dann ist der Mechanismus als **mittel** einzustufen.

- Kann der Mechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit einem Systemverwalter treffen muss, dann ist er als **hoch** einzustufen.

Es muss sichergestellt werden, dass die durchgeführten Tests alle sicherheitsspezifischen Funktionen umfassen. Wichtig ist zu beachten, dass durch Testen immer nur Fehler oder Abweichungen von den Spezifikationen festgestellt werden können, niemals jedoch die Abwesenheit von Fehlern.

An einigen **Beispielen** sollen typische Untersuchungsaspekte aufgezeigt werden:

**Passwortschutz:**
- Gibt es vom Hersteller voreingestellte Passwörter? Typische Beispiele für solche Passwörter sind der Produktname, der Herstellername, "SUPERVISOR", "ADMINISTRATOR", "USER", "GUEST".
- Welche Datei ändert sich, wenn ein Passwort geändert wurde? Kann diese Datei durch eine alte Version aus einer Datensicherung ersetzt werden, um alte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert oder sind sie im Klartext auslesbar? Ist es möglich, in dieser Datei Änderungen vorzunehmen, um neue Passwörter zu aktivieren?
- Wird der Zugang tatsächlich nach mehreren fehlerhaften Passworteingaben gesperrt?
- Werden in Zeitschriften oder Mailboxen Programme angeboten, die die Passwörter des untersuchten Produkts ermitteln können? Für einige Standardapplikationen sind solche Programme erhältlich.
- Wenn Dateien mit Passwörtern geschützt werden, kann durch einen Vergleich einer Datei vor und nach der Passwortänderung die Stelle ermittelt werden, an der das Passwort gespeichert wird. Ist es möglich, an dieser Stelle Änderungen oder alte Werte einzugeben, um bekannte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert? Wie ist die Stelle belegt, wenn der Passwortschutz deaktiviert ist?
- Kann die Passwort-Prüfroutine unterbrochen werden? Gibt es Tastenkombinationen, mit denen die Passworteingabe umgangen werden kann?

**Zugriffsrechte:**
- In welchen Dateien werden Zugriffsrechte gespeichert und wie werden sie geschützt?
- Können Zugriffsrechte von Unberechtigten geändert werden?
- Können Dateien mit alten Zugriffsrechten zurückgespielt werden und welche Rechte benötigt man dazu?
- Können die Rechte des Administrators so eingeschränkt werden, dass er keinen Zugriff auf die Nutz- oder Protokolldaten erhält?

**Datensicherung:**
- Können erstellte Datensicherungen problemlos rekonstruiert werden?
- Können Datensicherungen durch ein Passwort geschützt werden? Wenn ja, können die oben dargestellten Untersuchungsansätze für Passwörter eingesetzt werden.

**Verschlüsselung:**
- Bietet das Produkt an, Dateien oder Datensicherungen zu verschlüsseln?
- Werden mehrere verschiedene Verschlüsselungsalgorithmen angeboten? Hierbei ist im allgemeinen folgende Faustregel zu beachten: "Je schneller ein in Software realisierter Verschlüsselungsalgorithmus ist, um so unsicherer ist er."

- Wo werden die zur Ver- oder Entschlüsselung genutzten Schlüssel gespeichert?
  Bei einer lokalen Speicherung ist zu untersuchen, ob diese Schlüssel passwortgeschützt oder mit einem weiteren Schlüssel überschlüsselt geschützt werden. Bei einem **Passwortschutz** sind die obigen Punkte zu berücksichtigen. Bei einer Überschlüsselung ist zu betrachten, wie der zugehörige Schlüssel geschützt wird.
  Dazu können folgende Punkte betrachtet werden: Welche Datei ändert sich, wenn ein Schlüssel geändert wurde? Durch den Vergleich dieser Datei vor und nach der Schlüsseländerung kann die Stelle ermittelt werden, an der dieser Schlüssel gespeichert wird. Ist es möglich, an dieser Stelle Änderungen vorzunehmen, um neue Schlüssel zu aktivieren, die dann vom Anwender genutzt werden, ohne dass dieser die Kompromittierung bemerkt?
- Gibt es vom Hersteller voreingestellte Schlüssel, die vor der erstmaligen Benutzung des Programms geändert werden müssen?
- Was passiert, wenn bei der Entschlüsselung ein falscher Schlüssel eingegeben wird?
- Wird nach der Verschlüsselung einer Datei die unverschlüsselte Variante gelöscht? Wenn ja, wird sie zuverlässig überschrieben? Wird vor der Löschung überprüft, ob die Verschlüsselung erfolgreich war?

**Protokollierung:**
- Wird der Zugriff auf Protokolldaten für Unbefugte verwehrt?
- Werden die zu protokollierenden Aktivitäten lückenlos aufgezeichnet?
- Hat der Administrator die Möglichkeit aufgrund seiner privilegierten Rechte, sich unberechtigt und unbemerkt Zugriff auf Protokolldaten zu verschaffen oder kann er die Protokollierung unbemerkt deaktivieren?
- Wie reagiert das Programm, wenn der Protokollierungsspeicher überläuft?

Darüber hinaus muss festgestellt werden, ob durch das neue Produkt Sicherheitseigenschaften an anderer Stelle unterlaufen werden. **Beispiel:** das zu testende Produkt bietet eine Schnittstelle zur Betriebssystemumgebung, das IT-System war aber vorher so konfiguriert, dass keine solchen Schnittstellen existierten.

**Pilotanwendung:**

Nach Abschluss aller anderen Tests kann noch eine Pilotanwendung, also ein Einsatz unter Echtbedingungen, für notwendig gehalten werden.

Erfolgt der Test in der Produktionsumgebung mit Echtdaten, muss vorab durch eine ausreichende Anzahl von Tests die korrekte und fehlerfreie Funktionsweise des Programms bestätigt worden sein, um die Verfügbarkeit und Integrität der Produktionsumgebung nicht zu gefährden. Dabei kann das Produkt beispielsweise bei ausgewählten Benutzern installiert werden, die es dann für einen gewissen Zeitraum im echten Produktionsbetrieb einsetzen.

**Testauswertung:**

Anhand der festgelegten Entscheidungskriterien sind die Testergebnisse zu bewerten, alle Ergebnisse zusammenzuführen und mit der Testdokumentation der Beschaffungsstelle bzw. Testverantwortlichen vorzulegen.

Anhand der Testergebnisse sollte ein abschließendes Urteil für ein zu beschaffendes Produkt gefällt werden. Hat kein Produkt den Test bestanden, muss überlegt werden, ob eine neue Marktsichtung vorgenommen werden soll, ob

die gestellten Anforderungen zu hoch waren und geändert werden müssen oder ob von einer Beschaffung zu diesem Zeitpunkt abgesehen werden muss.

**Beispiel:**

Am Beispiel eines Kompressionsprogramms wird nun eine Möglichkeit beschrieben, Testergebnisse auszuwerten. Getestet wurden vier Produkte, die nach der dreistufigen Skala aus M 2.82 *Entwicklung eines Testplans für Standardsoftware* bewertet wurden.

| **Eigenschaft** | **Notwendig/ wünschenswert** | **Bedeutung** | **Produkt 1** | **Produkt 2** | **Produkt 3** | **Produkt 4** |
|---|---|---|---|---|---|---|
| korrekte Kompression und Dekompression | N | 10 | 2 | 2 | j | 0 |
| Erkennen von Bitfehlern in einer komprimierten Datei | N | 10 | 2 | 2 | n | 2 |
| Löschung von Dateien nur nach erfolgreicher Kompression | N | 10 | 2 | 2 | j | 2 |
| DOS-PC, 80486, 8 MB | N | 10 | 2 | 2 | j | 2 |
| Windows-tauglich | W | 2 | 0 | 2 | j | 2 |
| Durchsatz bei 50 MHz über 1 MB/s | W | 4 | 2 | 2 | j | 2 |
| Kompressionsrate über 40% | W | 4 | 2 | 1 | n | 0 |
| Online-Hilfefunktion | W | 3 | 0 | 0 | n | 2 |
| Passwortschutz für | W | 2 | 2 | 1 | n | 2 |

| Eigenschaft | Notwendig/ wünschenswert | Bedeutung | Produkt 1 | Produkt 2 | Produkt 3 | Produkt 4 |
|---|---|---|---|---|---|---|
| komprimierte Dateien | | | | | | |
| Bewertung | | | 100 | 98 | K.O. | K.O. |
| Preisermittlung (maximale Kosten 50.- EUR pro Lizenz) | | | 49,- EUR | 25,- EUR | | 39,- EUR |

Tabelle: Testplan für Standardsoftware

Produkt 3 war bereits in der Vorauswahl gescheitert und wurde daher nicht getestet.

Produkt 4 scheiterte in dem Testabschnitt "korrekte Kompression und Dekompression", weil die Erfüllung der Eigenschaft mit 0 bewertet wurde, es sich dabei aber um eine notwendige Eigenschaft handelt.

Bei der Berechnung der Bewertungspunktzahlen für die Produkte 1 und 2 wurden die Noten als Multiplikatoren für die jeweilige Bedeutungskennzahl benutzt und schließlich die Summe gebildet:

Produkt 1: 10*2+10*2+10*2+10*2+2*0+4*2+4*2+2*2 = 120
Produkt 2: 10*2+10*2+10*2+10*2+2*2+4*2+4*1+2*1 = 118

Nach der Testauswertung ist somit Produkt 1 auf dem ersten Platz, wird aber knapp gefolgt von Produkt 2. Die Entscheidung für ein Produkt hat jetzt die Beschaffungsstelle anhand der Testergebnisse und des daraus resultierenden Preis-/Leistungsverhältnisses zu treffen.

Prüffragen:

- Werden in der Testvorbereitung die Testmethoden für die Einzeltests mit Testarten, -verfahren und -werkzeugen festgelegt?
- Sind im Testumfang Standard-, Fehler- und Ausnahmefälle berücksichtigt?
- Bei Einsatz von Echtdaten zu Testzwecken: Werden die Echtdaten für Tests anonymisiert?
- Ist die Installation und Konfiguration der Testumgebung dokumentiert?
- Erfolgt die Durchführung der Tests anhand von Testplänen?
- Werden funktionale Tests durchgeführt, die auch fehlerhafte Eingabeparameter überprüfen?
- Werden sicherheitsspezifische Tests durchgeführt, die auch Penetrationstests umfassen?
- Existiert eine Dokumentation der Tests, die alle Testergebnisse anhand der Entscheidungskriterien bewertet?

# M 2.84 Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Beschaffungsstelle, Leiter Fachabteilung, Leiter IT

Nach Abschluss aller Tests müssen die Testergebnisse der Beschaffungsstelle vorgelegt werden. Die Entscheidung für ein Produkt hat jetzt die Beschaffungsstelle unter Beteiligung der Leiter der Fachabteilung und des IT-Bereichs aufgrund der Testergebnisse und des daraus resultierenden Preis-/Leistungsverhältnisses zu treffen. Hierbei ist insbesondere der Erfüllungsgrad der einzelnen Produkte gegenüber dem Anforderungskatalog in Relation zum Kaufpreis zu stellen. Auch sollten zusätzliche Funktionen der Produkte, die nicht im Anforderungskatalog aufgeführt wurden, aber dennoch für den Einsatz sinnvoll sind, bei der Entscheidung berücksichtigt werden.

**Erstellen einer Installationsanweisung**

Nach der Entscheidung für ein Produkt muss anschließend für das ausgewählte Produkt eine Installationsanweisung erstellt werden. Während des Testens wurde diejenige Konfiguration des Produktes ermittelt, die einen sicheren und effizienten Produktionsbetrieb erlaubt. Damit soll Benutzerfreundlichkeit, Ordnungsmäßigkeit und Sicherheit am Arbeitsplatz sichergestellt werden.

Um die geeignete Konfiguration des Produktes im Wirkbetrieb sicherzustellen, müssen bestimmte Parameter vorgegeben werden. Teilweise muss dies durch organisatorische Regelungen begleitet werden.

Für einige Eigenschaften eines Produktes wird im folgenden beispielhaft aufgezeigt, was im Rahmen einer Installationsanweisung vorgegeben werden kann.

**Beispiel:**

Benutzerfreundlichkeit:

- Mit dem Produkt sind die Treiber X, Y und Z (Bildschirm, Drucker, Maus, Netz) zu installieren, um eine für den Benutzer akzeptable Arbeitsumgebung zu schaffen (Bildschirm flimmerfrei, vernünftige Druckaufbereitung, etc.).
- Diejenigen Einstellungen, bei denen einzelne Funktionen die größte Verarbeitungsgeschwindigkeit haben, sind vorzugeben, wenn nicht andere Kriterien wie Sicherheit dagegen sprechen (die Größe der Auslagerungsdateien ist auf mindestens 10 MB festzusetzen, die Option Verifikation ist für die Datensicherung zu aktivieren, obwohl die Verifikation zusätzlichen Zeitaufwand erfordert).

Sicherheit:

- Die Parameter für Sicherheitsfunktionen sind voreinzustellen (z. B. die Mindestlänge von Passwörtern muss festgelegt werden (siehe dazu auch M 2.11 *Regelung des Passwortgebrauchs*), Datensicherungen sind täglich zu erstellen, die Protokollierung ist im vollen Umfang zu aktivieren, Zugriffsrechte auf personenbezogene Protokolldateien sind nur dem Datenschutzbeauftragten einzurichten, ...).

- Werden mehrere sicherheitsrelevante Verfahren unterstützt (z. B. Verschlüsselungsalgorithmus, Hashfunktionen), sind diejenigen auszuwählen, mit denen ein angemessenes Schutzniveau erreicht wird (zur Auswahl siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*).

Funktion:

- Nur die Funktionen X, Y, und Z sind zu aktivieren, unerwünschte oder nicht benötigte Funktionen sind abzuschalten.
- Die Funktion der automatischen Datensicherung ist mit dem Parameter "alle 10 Minuten" zu aktivieren.

Organisation:

- Die Installation ist vom Administrator durchzuführen.
- Regelungen für den Betrieb müssen erlassen werden (z. B. Datensicherungen sind eigenverantwortlich vom Anwender durchzuführen, Passwörter müssen nach 30 Tagen gewechselt werden).

Randbedingungen:

- Die Konfiguration der Plattform, auf der das Standardsoftwareprodukt zum Einsatz kommen soll, muss insbesondere dann beschrieben und vorgegeben werden, wenn systembedingte Schwachstellen der Plattform damit beseitigt werden.

Prüffragen:

- Wird für die ausgewählten Produkte eine Installationsanweisung erstellt, welche auch die Einstellung von Sicherheitsparametern berücksichtigt?

# M 2.85 Freigabe von Standardsoftware

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter Fachabteilung, Leiter IT

Vor der Übernahme der Standardsoftware in den Wirkbetrieb steht die formelle Freigabe. Verantwortlich für die Freigabe eines Produktes ist die Behörden- bzw. Unternehmensleitung, sie kann dies aber an die Leitung der Fachabteilung oder die Leitung des IT-Bereichs delegieren. Die Fachabteilung kann die durch Behörden- bzw. Unternehmensleitung vorgegebene Freigaberegelung durch eigene Restriktionen weiter einschränken. Der Einsatz nicht freigegebener Software ist zu untersagen (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Der Freigabe geht immer der erfolgreiche Abschluss aller notwendigen Tests voraus (siehe M 2.83 *Testen von Standardsoftware*). Eine Freigabe darf nicht erfolgen, wenn während der Tests nicht tolerierbare Fehler, z. B. erhebliche Sicherheitsmängel, festgestellt wurden.

Für die Freigabe sind Installations- bzw. Konfigurationsvorschriften zu erarbeiten, deren Detaillierungsgrad davon abhängig ist, ob die Installation durch die Systemadministration oder den Benutzer vorgenommen werden soll. Die Installations- bzw. Konfigurationsvorschriften sind Ergebnisse der im Rahmen der Beschaffung durchgeführten Tests (siehe M 2.83 *Testen von Standardsoftware*). Wenn unterschiedliche Konfigurationen zulässig sind, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Insbesondere muss festgelegt werden, ob für alle oder nur einige Benutzer Einschränkungen der Produktfunktionalität oder der Zugriffsrechte vorzunehmen sind. Für die Festlegung dieser Randbedingungen sind der Personal- bzw. Betriebsrat, der Datenschutzbeauftragter sowie der IT-Sicherheitsbeauftragte rechtzeitig zu beteiligen.

Die Freigabe sollte in Form einer schriftlichen **Freigabeerklärung** erfolgen. In der Freigabeerklärung sollten Aussagen gemacht werden zu den folgenden Punkten:

- Programmname und Versionsnummer,
- Bezeichnung des IT-Verfahrens, in dem das Produkt eingesetzt werden soll,
- Bestätigung, dass die eingesetzten IT-Komponenten den fachlichen Anforderungen entsprechen,
- Datum der Freigabe, Unterschrift des Freigabe-Verantwortlichen,
- Unbedenklichkeitserklärung seitens IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- bzw. Betriebsrat,
- vorgesehener Zeitpunkt des Einsatzes im Wirkbetrieb,
- für welche Benutzer das Produkt freigegeben wird,
- Installationsanweisung, insbesondere an welchen Arbeitsplätzen es mit welcher Konfiguration installiert wird,
- wer berechtigt ist, es zu installieren,
- wer Zugriff auf die Installationsdatenträger hat und
- welche Schulungen vor Nutzung des Produktes vorzunehmen sind.

Die Freigabeerklärung muss allen Beteiligten zur Kenntnis gegeben werden, insbesondere sollten bei der Freigabeinstanz, dem IT-Bereich, der Fachabteilung und ggf. beim IT-Anwender Kopien vorhanden sein.

Darüber hinaus ist organisatorisch zu regeln, dass die Freigabe und ggf. die notwendigen Tests wiederholt werden, wenn sich durch Versionswechsel oder

Patches grundlegende Eigenschaften, insbesondere im Bereich der Sicherheitsfunktionen, geändert haben. Änderungen der genannten Art sind dem für die Freigabe des Produktes Verantwortlichen mitzuteilen.

Weiterhin kann festgelegt werden, welche Standardsoftware-Produkte, abhängig vom Einsatzort und -zweck, generell freigegeben werden. Voraussetzung ist, dass sie zumindest auf Computer-Viren geprüft, dass die Lizenzfragen geklärt und dass sie registriert sind. Beispiele hierfür wären:

- Demo-Versionen zu Testzwecken, die auf speziellen Rechnern zur Verfügung gestellt werden,
- Public-Domain-Software, die auf speziellen Servern installiert werden,
- Spielprogramme auf speziellen Rechnern, die in Pausenräumen aufgestellt werden.

Prüffragen:

- Ist sichergestellt, dass Software erst nach formeller Freigabe in den Wirkbetrieb übernommen wird?
- Ist festgelegt, dass die Freigabe von Software erst nach erfolgreichem Abschluss aller notwendigen Tests erfolgt?
- Existiert eine schriftliche Freigabeerklärung und wurden alle Beteiligten in Kenntnis darüber gesetzt?
- Wird der Freigabeprozess bei Versionswechseln und Patches von Software wiederholt?

# M 2.86 Sicherstellen der Integrität von Standardsoftware

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter IT

Es ist sicherzustellen, dass die freigegebene Standardsoftware nur unverändert installiert werden kann. Damit soll verhindert werden, dass zwischenzeitlich gewollte oder ungewollte Veränderungen vorgenommen werden können, z. B. durch Computer-Viren, Bitfehler aufgrund technischer Fehler oder Manipulationen in Konfigurationsdateien.

Die Installation darf daher ausschließlich von Originaldatenträgern bzw. von nummerierten Kopien der Originaldatenträger erfolgen. Eine Alternative zur lokalen Installation von Datenträgern ist die Installation über ein lokales Netz von einer dafür freigegebenen Version. Dabei sollte sichergestellt sein, dass nur berechtigte Personen darauf Zugriff haben.

Von den Originaldatenträgern sollten, falls der Datenumfang (z. B. CD-ROM) es zulässt, Sicherungskopien angefertigt werden. Originaldatenträger und alle Kopien müssen vor unberechtigtem Zugriff geschützt aufbewahrt werden (siehe M 6.21 *Sicherungskopie der eingesetzten Software*). Die angefertigten Kopien sollten nummeriert und in Bestandsverzeichnisse aufgenommen werden. Kopien, die nicht mehr benötigt werden, sind zu löschen. Vor der Installation muss eine Computer-Virenprüfung durchgeführt werden.

Optional kann über die Originaldatenträger oder über eine während des Tests installierte Referenzversion eine Checksumme (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*) gebildet werden, anhand derer vor der Installation die Integrität der dafür eingesetzten Datenträger bzw. der in lokalen Netzen hinterlegten Versionen oder anhand derer die korrekte Installation überprüft werden kann. Darüber hinaus können installierten Programme zusätzlich zum Schutz vor unberechtigten Veränderungen der freigegebenen Konfiguration mit Checksummen versehen werden. Auf diese Weise können auch Infektionen mit bisher unbekannten Computer-Viren erkannt werden. Damit kann auch festgestellt werden, ob eine Vireninfektion vor oder nach der Installation stattgefunden hat.

Prüffragen:

- Ist sichergestellt, dass freigegebene Standardsoftware nur unverändert installiert werden kann?
- Ist sichergestellt, dass die Installation ausschließlich von Originaldatenträgern oder von nummerierten Kopien derer erfolgt und nur Berechtigte Zugriff auf die Installationsroutinen haben?
- Werden von Originaldatenträgern Sicherungskopien angefertigt?
- Wird vor der Installation eine Computer-Virenprüfung durchgeführt?
- Werden über die Originaldatenträger mit hohem Schutzbedarf hinsichtlich der Integrität Checksummen gebildet?

# M 2.87 Installation und Konfiguration von Standardsoftware

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die freigegebene Software wird entsprechend der Installationsanweisung auf den dafür vorgesehenen IT-Systemen installiert. Die Installationsanweisung beinhaltet neben den zu installierenden Programmen auch Konfigurationsparameter und die Einrichtung der Hardware- und Softwareumgebung.

Abweichungen von der Installationsanweisung bedürfen der Zustimmung der Freigabeinstanz.

Wenn die Benutzer die Software selbst installieren sollen, muss ihnen eine Installationsanweisung zur Verfügung gestellt werden, die eine selbständige Installation ermöglicht. Mindestens die Pilot-Installation durch einen ausgewählten typischen Benutzer sollte durch die IT-Abteilung begleitet werden, um die Verständlichkeit der Installationsanweisung zu überprüfen.

Da Standardsoftware für eine Vielzahl von Einsatzfelder entwickelt wird, enthält sie meist mehr Funktionen, als für die Erfüllung der Fachaufgabe benötigt werden. Damit es zu weniger Problemen und Fehlern bei der Arbeit mit der Software kommt, sollten nur die tatsächlich benötigten Funktionalitäten installiert werden. Funktionalitäten, die zu Sicherheitsproblemen führen können, dürfen nicht freigegeben werden.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann bei nachfolgenden Problemen während der Installation zur Wiederherstellung eines konsolidierten Aufsetzpunktes verwendet werden. Nach der erfolgreichen Installation sollte erneut eine vollständige Datensicherung durchgeführt werden, damit bei späteren Problemen wieder auf den Zustand nach der erfolgreichen Installation des Produktes aufgesetzt werden kann.

Die erfolgreiche Installation wird schriftlich an die für die Aufnahme des Wirkbetriebes zuständige Stelle gemeldet.

Optional kann die Installation durch den Einsatz eines sog. "Delta-Tools" begleitet werden, das alle Veränderungen in einer IT-Umgebung zwischen zwei bestimmbaren Zeitpunkten dokumentiert. Diese Dokumentation von Veränderungen ist insbesondere bei der Deinstallation der Software hilfreich.

Beim Einsatz eines neuen Produktes müssen evtl. Datenbestände übernommen werden, die mit einem Vorgängerprodukt erzeugt wurden. Hat sich bei den Tests gezeigt, dass es dabei zu Schwierigkeiten kommen kann, sind Hilfestellungen für die Benutzer zu erarbeiten oder die Übernahme von alten Datenbeständen ist zentral durch geschultes Personal durchzuführen.

Prüffragen:

- Erfolgt die Installation freigegebener Software entsprechend der Installationsanweisung?
- Bedürfen Abweichungen von der Installationsanweisung einer Zustimmung durch die Freigabeinstanz?
- Wird mindestens die Pilot-Installation durch die IT-Abteilung begleitet?

- Werden bei der Installation von Software nur die tatsächlich benötigten Funktionalitäten installiert?
- Werden vor und nach der Installation von Software Datensicherungen auf allen betroffenen IT-Systemen durchgeführt?

# M 2.88 Lizenzverwaltung und Versionskontrolle von Standardsoftware

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Organisation

Ohne eine geeignete Versionskontrolle und Lizenzkontrolle kommt es erfahrungsgemäß schnell zur Verwendung verschiedenster Software-Versionen auf einem IT-System oder innerhalb einer Organisationseinheit, von denen eventuell einige ohne Lizenz benutzt werden.

Auf allen IT-Systemen einer Institution darf ausschließlich lizenzierte Software eingesetzt werden. Diese Regelung muss allen Mitarbeitern bekanntgemacht werden, die Administratoren der verschiedenen IT-Systeme müssen sicherstellen, dass nur lizenzierte Software eingesetzt wird. Dafür müssen sie mit geeigneten Werkzeugen zur Lizenzkontrolle ausgestattet werden.

Häufig werden in einer Institution verschiedene Versionen einer Anwendung eingesetzt. Im Rahmen der Lizenzkontrolle sollte es auch möglich sein, einen Überblick über alle eingesetzten Software-Versionen zu erhalten. Damit kann gewährleistet werden, dass alte Versionen durch neuere ersetzt werden, sobald dies notwendig ist, und dass bei der Rückgabe von Lizenzen alle Versionen gelöscht werden.

Darüber hinaus sind die verschiedenen Konfigurationen der installierten Software zu dokumentieren. Damit muss es möglich sein, sich einen Überblick zu verschaffen, an welchem IT-System welche sicherheitsrelevanten Einstellungen eines Produktes durch die Freigabe vorgegeben und welche tatsächlich installiert wurden. Damit kann z. B. schnell geklärt werden, an welchen Rechnern beim Produkt XYZ die Makro-Programmierung installiert worden ist und an welchen nicht.

Damit Lizenzen bei Hardware-Defekten nicht ungültig werden, sollten möglichst Hardware-unabhängige Lizenzen eingesetzt werden. So kann ein IT-System mit weniger Aufwand ersetzt werden, wenn die Hardware ausfällt.

Wenn es notwendig ist, ein Produkt online über einen Lizenzierungsserver des Herstellers zu aktivieren, kann die Lizenz nachträglich verfallen und das Produkt deaktiviert werden. Wenn möglich, sollten Produkte gewählt werden, die nicht online aktiviert werden müssen.

Wenn es möglich und wirtschaftlich sinnvoll ist, sollten unbefristete Lizenzen bevorzugt werden. Damit kann eine Funktionseinschränkung verhindert werden, wenn die Lizenz abgelaufen ist oder die Systemzeit stark abweicht.

Prüffragen:

- Existiert eine Regelung zur ausschließlichen Nutzung von lizenzierter Software und ist diese allen Mitarbeitern bekannt gemacht?
- Sind die Administratoren mit Werkzeugen zur Lizenzkontrolle ausgestattet?
- Existiert eine Übersicht aller eingesetzten Software-Versionen?
- Sind die verschiedenen Konfigurationen installierter Software dokumentiert?

# M 2.89 Deinstallation von Standardsoftware

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind, und alle Einträge in Systemdateien, die bezüglich des Produktes vorgenommen wurden, gelöscht werden. Bei vielen Softwareprodukten werden während der Installation in diversen Verzeichnissen auf dem IT-System Dateien angelegt oder bestehende Dateien verändert. Häufig wird der Benutzer nicht einmal über alle bei der Installation durchgeführten Veränderungen am IT-System informiert.

Um eine vollständige Deinstallation durchführen zu können, ist es daher hilfreich, die bei der Installation durchgeführten Systemänderungen nachzuhalten, entweder manuell oder mit Hilfe von speziellen Tools. Wird dies nicht vorgenommen, kommt es erfahrungsgemäß dazu, dass eine Deinstallation nur rudimentär stattfindet oder dass sie unterlassen wird aus Furcht, wichtige Dateien bei der Deinstallation zu löschen.

Prüffragen:

- Existiert eine Übersicht aller eingesetzten Software-Versionen?
- Ist sichergestellt, dass bei der Deinstallation von Software alle angelegten Dateien und Einträge in Systemdateien entfernt bzw. gelöscht werden?
- Werden während der Installation von Software durchgeführte Systemänderungen aufgezeichnet?

# M 2.90 Überprüfung der Lieferung

**Verantwortlich für Initiierung:** Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Beschaffungsstelle

Nach Eingang einer Lieferung ist anhand der vorhandenen Unterlagen zu überprüfen,

- ob die Lieferung bestellt wurde,
- für wen sie bestimmt ist,
- ob Transportschäden zu erkennen sind,
- ob sie vollständig ist, d. h. ob einerseits alle bestellten Komponenten und andererseits alle gemäß Produktbeschreibung zum Lieferumfang des Produktes gehörenden Komponenten vorhanden sind.

Die Ergebnisse dieser Prüfungen sind in einem Wareneingangsverzeichnis zu dokumentieren, zusammen mit:

- Produktname und Version,
- Produktart, z. B. Textverarbeitung,
- Lieferumfang, also Beschreibung der einzelnen Komponenten inklusive Anzahl und Lieferform (Buch, Diskette, CD-ROM, ...),
- Lieferdatum,
- Lieferart,
- wer es in Empfang genommen hat,
- Aufbewahrungsort und
- an wen es weitergegeben wurde.

Für die Durchführung der funktionalen Tests, sowie die anschließende formelle Freigabe, die Installation und Konfiguration müssen die gelieferten Produkte an die IT-Abteilung weitergegeben werden.

Werden die Produkte nur vorübergehend eingesetzt oder zur Verfügung gestellt, z. B. im Rahmen von Tests, müssen zumindest die Seriennummer und andere produktspezifische Identifizierungsmerkmale in entsprechende Bestandsverzeichnissen vermerkt werden. Wenn die gelieferten Produkte für den dauerhaften Verbleib vorgesehen sind, sind sie mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierte fortlaufende Inventarnummern) zu kennzeichnen. Anschließend müssen sie in ein Bestandsverzeichnis aufgenommen werden. Dieses muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib,
- Freigabedatum,
- Installationsdatum und Konfigurationsbesonderheiten und
- Wartungsverträge, Wartungsintervalle.

Prüffragen:

- Erfolgt nach Eingang einer Lieferung eine Überprüfung auf Vollständigkeit und Korrektheit?
- Werden die Ergebnisse der Überprüfung in einem Wareneingangsverzeichnis dokumentiert?
- Werden gelieferte Produkte mit eindeutigen Identifizierungsmerkmalen gekennzeichnet und in ein Bestandsverzeichnis aufgenommen?

# M 2.91 Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.92 Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.93 Planung des Windows NT Netzes

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.94 Freigabe von Verzeichnissen unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.95 Beschaffung geeigneter Schutzschränke

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Beschaffungsstelle

Schutzschränke können ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten Zugriff schützen. Als erstes ist daher zu klären, was die Schutzziele sind, die mit einem Schutzschrank erreicht werden sollen. Als nächstes ist zu analysieren, welche Inhalte geschützt werden sollen, da z. B. sich die Temperatur- und Feuchtigkeits-Empfindlichkeit von Dokumenten, Datenträgern und Wertgegenständen stark unterscheiden kann. Je nach angestrebter Schutzwirkung sind bei der Auswahl geeigneter Schutzschränke folgende Hinweise zu beachten:

- **Schutz gegen Feuereinwirkung:**
  Bei Datensicherungsschränken nach EN 1047-1 unterscheidet man bezüglich Schutz gegen Feuereinwirkung die Güteklassen S60 und S120. In diesen Güteklassen werden die Schutzschränke darauf geprüft, ob in ihnen bis zu einer Beflammungszeit von 60 bzw. 120 Minuten während eines normierten Testes für die geschützten Datenträger verträgliche Temperaturen erhalten bleiben. Durch Zusätze in der Klassifizierung werden die zu schützenden Datenträger bezeichnet. Die Kürzel bedeuten im einzelnen:

  - P = Papierdokumente
  - D = Datenträger mit Belastungsgrenzwert bis 70° C (z. B. Magnetbänder, Filme)
  - DIS = Datenträger mit Belastungsgrenzwert bis 50° C (z. B. Disketten, Magnetbandkassetten einschließlich aller anderen Datenträger)

  Die Unterschiede zwischen den Klassen liegen in der Isolationsleistung, die bei DIS-Schränken am höchsten ist.
  Für den normalen Schutzbedarf sollten bei Schutz gegen Feuer Datensicherungsschränke der Güteklasse S60 ausreichend sein. Für die Verwendung als Serverschränke werden Datensicherungsschränke nach EN 1047-1 oder Datensicherungscontainer nach EN 1047-2 mit einer Klimaanlage angeboten.
  Bei Schutzschränken, die zum Schutz vor Feuer und Rauch dienen, sollte eine Vorrichtung zum automatischen Schließen der Türen im Brandfall vorgesehen werden. Die Schließung sollte lokal durch Rauchgasmelder und/oder extern durch ein Signal einer Brandmeldeanlage (soweit vorhanden) ausgelöst werden können.
- **Schutz gegen unbefugten Zugriff:**
  Der Schutzwert gegen unbefugten Zugriff wird neben der mechanischen Festigkeit des Schutzschrankes entscheidend durch die Güte des Schlosses beeinflusst.
  Für den normalen Schutzbedarf sollten Wertschutzschränke nach EN 1143-1 "Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl, Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume" oder Sicherheitsschränke nach EN 14450 "Wertbehältnisse - Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl - Sicherheitsschränke" eingesetzt werden. Sicherheitsschränke liegen im Widerstandswert unterhalb von Wertschutzschränken.
  Sind Zugriffsschutz und Brandschutz in Kombination erforderlich, so können Datensicherungsschränke verwendet werden, die sowohl die Anfor-

derungen der EN 1143-1 als auch der EN 1047-1 erfüllen (sogenannte Duplexschränke).

Bei der Auswahl von Schutzschränken ist auch die zulässige Deckenbelastung, also die Tragfähigkeit des Fußbodens, am Aufstellungsort zu berücksichtigen. Außerdem sollte im Vorfeld geprüft werden, wie der Schutzschrank an den Aufstellungsort transportiert werden kann. Dazu gehört die Tragfähigkeit der Aufzüge, die Breite der Treppen, Flure und Türen zu kontrollieren.

Nach diesen Auswahlkriterien für den Schutzwert des Schutzschrankes ist als nächstes die Ausstattung des Schrankes bedarfsgerecht festzulegen. Dazu sollte vor der Beschaffung eines Schutzschrankes festgelegt werden, welche Geräte bzw. welche Arten von Datenträgern in ihm aufbewahrt werden sollen. Die Innenausstattung des Schutzschrankes ist dieser Festlegung angemessen auszuwählen. Nachrüstungen sind in der Regel schwierig, da der Schutzwert des Schrankes und seine spezifische Zulassung beeinträchtigt werden können. Es sollte auch Raum für zukünftige Erweiterungen mit eingeplant werden.

In Serverschränken sollte außer für den Server und eine Tastatur auch Platz für einen Bildschirm und weitere Peripheriegeräte wie z. B. Bandlaufwerke vorgesehen werden, damit Administrationsarbeiten vor Ort durchgeführt werden können. Dazu ist zu beachten, dass die Ausstattung ergonomisch gewählt ist, damit Administrationsarbeiten am Server ungehindert durchgeführt werden können. So ist zum Beispiel ein ausziehbarer Boden für die Tastatur wünschenswert, der in einer Höhe angebracht wird, dass der Administrator seine Arbeiten sitzend durchführen kann. Je nach Nutzung des Schrankes können auch eine Klimatisierung und/oder eine USV-Versorgung erforderlich sein. Die entsprechenden Geräte sollten dann im Schrank mit untergebracht werden. Andernfalls muss zumindest eine Lüftung vorhanden sein. Die Ausstattung des Schrankes mit einem lokal arbeitenden Brandfrüherkennungssystem, das im Brandfall die Stromzufuhr der Geräte unterbricht (auf der Eingangs- **und** der Ausgangsseite der USV, sofern diese vorhanden ist), ist empfehlenswert.

**Nicht** im gleichen Schrank untergebracht werden sollten Backup-Datenträger und Protokolldrucker. Backup-Datenträger würden im Falle einer Beschädigung des Servers vermutlich ebenfalls beschädigt. Die Protokollierung der Aktionen am Server dient auch zur Kontrolle des Administrators. Es ist also nicht sinnvoll, ihm, gegebenenfalls sogar als Einzigem, Zugriff auf die Protokollausdrucke zu gewähren.

Prüffragen:

- Wird bei der Beschaffung von Schutzschränken ein ausreichender Feuerschutz nach EN 1047 berücksichtig?
- Bieten die Serverschränke ausreichend Platz für alle zusätzlichen Peripheriegeräte?
- Verfügt der Serverschrank über eine ausreichende Klimatisierung?
- Verfügt der Serverschrank über eine ausreichende USV-Versorgung?
- Wird darauf geachtet, Backup-Datenträger oder Protokolldrucker nicht im selben Schrank wie den Server aufzubewahren?

# M 2.96 Verschluss von Schutzschränken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Generell sind Schutzschränke bei Nichtbenutzung zu verschließen. Werden Arbeiten, die ein Öffnen des Schutzschrankes erfordern, unterbrochen, so ist auch bei kurzfristigem Verlassen des Raumes der Schutzschrank zu verschließen. Bei Verwendung von mechanischen Codeschlössern (Zahlungskombinationsschlösser) sind diese nach dem Schließen der Tür jedes Mal zu verwerfen, also abzuschließen. Einige Hersteller empfehlen beispielsweise hierzu an einem Zahlenkombinationsschloss vier Umdrehungen durchzuführen. Dadurch ist sichergestellt, dass das Schloss tatsächlich wieder verschlossen ist und außerdem keine Rückschlüsse auf die Kombination möglich sind.

Prüffragen:

- Wird darauf geachtet, dass Schutzschränke bei Nichtbenutzung verschlossen werden?

# M 2.97 Korrekter Umgang mit Codeschlössern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Werden Schutzschränke mit mechanischen oder elektronischen Codeschlössern verwendet, so muss der Code für diese Schlösser geändert werden:

- nach der Beschaffung,
- bei Wechsel des Benutzers,
- nach Öffnung in Abwesenheit des Benutzers,
- wenn der Verdacht besteht, dass der Code einem Unbefugten bekannt wurde und
- mindestens einmal alle zwölf Monate.

Der Code darf nicht aus leicht zu ermittelnden Zahlen (z. B. persönliche Daten, arithmetische Reihen) bestehen.

Die jeweils gültigen Codes von Codeschlössern sind aufzuzeichnen und gesichert zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes* in analoger Anwendung). Zu beachten ist, dass eine Hinterlegung im zugehörigen Schutzschrank sinnlos ist.

Wenn der Schutzschrank neben einem Codeschloss ein weiteres Schloss besitzt, so ist abzuwägen, ob Code und Schlüssel gemeinsam hinterlegt werden, was im Notfall einen schnelleren Zugriff erlauben würde, oder getrennt hinterlegt werden, so dass es für einen Angreifer schwieriger ist, sich Zugriff zu verschaffen.

Prüffragen:

- Gibt es Regelungen zur Änderung der Codes von Codeschlössern an Schutzschränken?
- Werden bei der Auswahl der Codes keine leicht zu ermittelnden Zeichenfolgen verwendet?
- Werden die gültigen Codes gesichert hinterlegt?
- Schutzschrank mit Code und Schlüssel: Ist deren getrennte bzw. gemeinsame Aufbewahrung geregelt?

# M 2.98 Sichere Installation von Novell Netware Servern

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 2.99 Sichere Einrichtung von Novell Netware Servern

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 2.100 Sicherer Betrieb von Novell Netware Servern

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 2.101 Revision von Novell Netware Servern

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 2.102 Verzicht auf die Aktivierung der Remote Console

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.103 Einrichten von Benutzerprofilen unter Windows 95

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 2.104 Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 2.105 Beschaffung von TK-Anlagen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Haustechnik, Beschaffungsstelle

Bei der Beschaffung der TK-Anlagen oder anderer Komponenten, wie der Erweiterung einer klassischen TK-Anlage um VoIP, sollten die Ergebnisse der Anforderungsanalyse und der Planung mit einbezogen werden. Die Vielfalt der Funktionen und Einsatzmöglichkeiten machen die Auswahl und Beschaffung relativ kompliziert und zeitaufwändig.

Darüber hinaus müssen vorhandene Kommunikationssysteme und -komponenten des Unternehmens und bei der Beschaffung berücksichtigt werden. Wird eine TK-Anlage nicht vollkommen neu beschafft, muss darauf geachtet werden, dass Altbestand und Neubeschaffungen kompatibel zueinander sind. Bei der Beschaffung neuer TK-Anlagen ist darauf zu achten, dass diese so ausgewählt werden, dass im späteren Betrieb mit geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann. Hierfür müssen in erster Linie auf

- das Vorhandensein geeigneter Funktionalitäten für die Anlagenadministration,
- ausreichende Protokollmechanismen und Auswertemöglichkeiten sowie auf
- die Revisionsfähigkeit der TK-Anlage

geachtet werden.

Bei der Beschaffung einer klassischen TK-Anlage ist überdies zu beachten, ob sie neben digitalen auch analoge Teilnehmeranschlüsse anbieten muss. Analoge Anschlüsse können notwendig sein, weil analoge Endgeräte wie Faxgeräte, Anrufbeantworter, schnurlose Telefone, Modems für Datenanwendungen, wie Signalisierungen oder Notruf angeschlossen werden sollen. Dazu kommen die, entsprechend der gewünschten Leistungsmerkmale ausgewählten, analogen oder digitalen Geräte.

Bei Hybridanlagen werden klassische TK-Anlagen um IP-Funktionen erweitert und ermöglicht, IP-Endgeräte an die TK-Anlage anzuschließen. Beschafft werden müssen neben der TK-Anlage herkömmliche oder IP-fähige Endgeräte. Wird ein PC als Endgerät eingesetzt, dann muss er die Netzschnittstellen, Telefonie-Software, Soundkarte, Mikrofon und evtl. ein Headsetaufweisen.

Bei einer VoIP-basierten Lösung müssen folgende Elemente betrachtet werden: VoIP-TK-Anlage, VoIP-Telefone, Softphones, VoIP-Serversoftware und weitere Netzwerkelemente. Dazu kommt optional noch die Integration von Funklösungen und Mehrwertdiensten wie beispielsweise Unified Communications, zu denen CTI (Computer Telephone Integration), Unified Messaging und Voice-Mail gehören sowie ein Vermittlungsplatz oder Billing-System.

Zur Unterstützung bei der Beschaffung von TK-Anlagen kann Teil 2 (Beschaffungsleitfaden) der vom BSI erarbeiteten Technischen Leitlinie "Sichere TK-Anlagen" verwendet werden. Der Beschaffungsleitfaden nennt zunächst Auswahlkriterien für die Komponenten einer TK-Lösung, die aus den, in Teil 1 der Technischen Leitlinie spezifizierten Maßnahmen, abgeleitet werden. Die Anforderungen werden in einer Bewertungstabelle je nach betrachteten Szenarien unterschiedlich stark gewichtet. Die Struktur orientiert sich an der Methodik der "Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (UfAB IV)". Für die Produktauswahl und die Abnahme werden Prüfkriterien

entwickelt, die neben Prüfungen der Konfiguration auch Tests auf Ebene der Protokollschnittstellen unter Einsatz von Protokollanalysatoren und Simulationswerkzeugen beschreiben.

# M 2.106 Auswahl geeigneter ISDN-Karten in der Beschaffung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle

Bei der Beschaffung von ISDN-Karten besteht die Möglichkeit, diese von vornherein so auszuwählen, dass im späteren Betrieb Sicherheitsfunktionalitäten nicht teuer hinzugekauft werden müssen. Erforderliche Sicherheitsfunktionalitäten sollten bereits auf der Karte vorhanden sein oder durch mitgelieferte Kommunikationssoftware und Treiberprogramme realisiert werden können.

Mögliche Kriterien für die Auswahl geeigneter ISDN-Karten sind:

- Fähigkeit zur Durchführung einer Authentisierung über PAP und CHAP (Password Authentikation Protocol und Challenge Handshake Authentication Protocol, RFC 1994),
- Vorhandensein eines Verschlüsselungsverfahrens (symmetrisch/asymmetrisch) in Hard- oder Software,
- Möglichkeit der Auswertung von CLIP-Rufnummern (Calling Line Identification Presentation) zur Authentisierung,
- Möglichkeit des Führens einer Rufnummerntabelle für das Durchführen eines Callbacks,
- Möglichkeit der Protokollierung nicht erfolgreicher Verbindungsaufbauten (Ablehnung aufgrund falscher Rufnummern- oder PAP/CHAP-Authentisierung).

Außerdem sind die ISDN-Karten auf Funktionalitäten hin zu untersuchen, die für einen sicheren Betrieb nicht vorhanden sein dürfen, oder falls sie dennoch vorhanden sind, zumindest durch Konfiguration eine Deaktivierung herbeigeführt werden kann. Hierzu zählt z. B. die "Remote-Control"-Funktionalität, die einen direkten Kommunikationsaufbau zum IT-System aus dem öffentlichen Netz zulässt.

Die für die Institution und das Einsatzumfeld relevanten sicherheitsrelevanten Anforderungen an ISDN-Karten müssen daher ermittelt und der Beschaffungsstelle mitgeteilt worden sein.

Beachtet werden sollte, dass sowohl im Bereich der IT-Systeme, die mit ISDN-Karten ausgestattet werden sollen, als auch im Bereich der Netzkoppelelemente (z. B. ISDN-Router) ISDN-Karten mit möglichst gleichen Sicherheitsfunktionalitäten eingesetzt werden. Ist dies nicht gewährleistet, entfalten Sicherheitsfunktionalitäten, die auf beiden Seiten erforderlich sind, nicht die gewünschte Wirkung.

Prüffragen:

- Sind der Beschaffungsstelle die sicherheitsrelevanten Anforderungen an ISDN-Karten bekannt?

# M 2.107 Dokumentation der ISDN-Karten-Konfiguration

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Je nach Einsatzgebiet ergeben sich für eine ISDN-Karte nahezu beliebig komplexe Konfigurationseinstellungen. Für das Sicherstellen eines geordneten Wiederanlaufs (z. B. nach Austausch einer ISDN-Karte oder deren Kommunikationssoftware) wird empfohlen, mindestens die folgenden Einstellungen zu dokumentieren:

- Typenbezeichnung der eingesetzten Karte und Seriennummer,
- Rufnummer(n) für den Kommunikationsaufbau und eine evtl. durchzuführende Authentisierung,
- Verwendetes D-Kanal-Protokoll (1TR6, EDSS-1 etc.),
- Verwendetes B-Kanal-Protokoll (X.25, PPP, TCP/IP, Bittransparent etc.),
- Stand der verwendeten CAPI-Version,
- Stand der verwendeten Treiber-Software,
- Art der Datenkompression, wenn verwendet,
- Art der Authentisierung (z. B. PAP/CHAP), wenn verwendet.

Beim Einsatz von Authentisierungsverfahren, die auf dem Besitz eines gemeinsamen Geheimnisses (z. B. Passwort) beruhen, kann auch dieses Geheimnis dokumentiert werden. Beachtet werden muss dann allerdings, dass die erstellte Dokumentation nur einem eingeschränkten Personenkreis zugänglich gemacht werden darf, um das Bekanntwerden des Geheimnisses zu verhindern.

Prüffragen:

- Sind die für die ISDN-Karten vorgenommenen Konfigurationseinstellungen nachvollziehbar dokumentiert?

# M 2.108 Fernwartung der ISDN-Netzkoppelelemente

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Verzicht auf Fernwartung ist eine wirkungsvolle Maßnahme, um Externe an Manipulationen an ISDN-Routern und IT-Systemen mit ISDN-Karten zu hindern.

Auf eine Fernwartung sollte daher möglichst verzichtet werden. Wenn es trotzdem Gründe gibt, die gegen den Verzicht auf Fernwartung sprechen, müssen diese nachvollziehbar dokumentiert werden.

Bei IT-Systemen mit ISDN-Karte sollte überprüft werden, ob die verwendete Kommunikationssoftware "Remote-Control"-Funktionalitäten bietet. Hierdurch kann das betreffende IT-System über das öffentliche ISDN angerufen werden, die ISDN-Karte nimmt den Anruf entgegen und der Anrufende bedient das IT-System so, als ob es "vor Ort" wäre. Diese Funktionalität ist zu deaktivieren.

Bei ISDN-Routern sollte die Fernwartung über reservierte Bandbreiten (oder reservierte ISDN-Rufnummern) deaktiviert werden, da hier in der Regel eine nur über ein Passwort geschützte Verbindung zur Management Information Base des Routers hergestellt wird, in der nahezu alle Konfigurationseinstellungen vorgenommen werden können.

**Rechtevergabe für den Fernzugriff**

Der externe Zugriff auf ein Behörden- oder Unternehmensnetz muss hinsichtlich der eingeräumten Rechte auf das erforderliche Maß eingeschränkt werden. Über die in M 2.8 *Vergabe von Zugriffsrechten* beschriebenen Anforderungen ist weiterhin zu berücksichtigen, dass die Rechtevergabe für den Fernzugriff noch restriktiver zu handhaben ist. Beispielsweise müssen für einen Telearbeitsplatz nicht zwingend Zugriffsrechte auf Verzeichnisse mit Software bestehen.

Die für den Fernzugriff eingeräumten Rechte sollten regelmäßig hinsichtlich ihrer Erforderlichkeit und Aktualität überprüft werden.

Prüffragen:

- Ist der externe Zugriff auf das interne Netz auf das erforderliche Maß eingeschränkt?
- Werden die für den Fernzugriff eingeräumten Rechte bzw. aktivierten Funktionen regelmäßig hinsichtlich ihrer Erforderlichkeit und Aktualität überprüft?

# M 2.109 Rechtevergabe für den Fernzugriff

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der externe Zugriff auf ein Behörden- oder Unternehmensnetz muss hinsichtlich der eingeräumten Rechte auf das erforderliche Maß eingeschränkt werden. Über die in M 2.8 *Vergabe von Zugriffsrechten* beschriebenen Anforderungen ist weiterhin zu berücksichtigen, dass die Rechtevergabe für den Fernzugriff noch restriktiver zu handhaben ist.

Beispielsweise müssen für einen Telearbeitsplatz nicht zwingend Zugriffsrechte auf Verzeichnisse mit Software bestehen.

Die für den Fernzugriff eingeräumten Rechte sollten regelmäßig hinsichtlich ihrer Erforderlichkeit und Aktualität überprüft werden.

Prüffragen:

- Ist der externe Zugriff auf das interne Netz auf das erforderliche Maß eingeschränkt?

# M 2.110 Datenschutzaspekte bei der Protokollierung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

Art und Umfang von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab.

Die Protokollierung der Administrationsaktivitäten entspricht einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend im allgemeinen Datenschutzrecht, während die verfahrensorientierte Protokollierung oft durch bereichsspezifische Regelungen definiert wird. Beispiele für verfahrensorientierte Protokollierung sind u. a. Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze.

### Mindestanforderungen an die Protokollierung

Bei der Administration von IT-Systemen sind die folgenden Aktivitäten vollständig zu protokollieren:

- **Systemgenerierung und Modifikation von Systemparametern**
  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.
- **Einrichten von Benutzern**
  Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.
- **Erstellung von Rechteprofilen**
  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat (siehe auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).
- **Einspielen und Änderung von Anwendungssoftware**
  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.
- **Änderungen an der Dateiorganisation**
  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (siehe z. B. Datenbankmanagement).
- **Durchführung von Datensicherungsmaßnahmen**
  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

- **Sonstiger Aufruf von Administrations-Tools**
  Die Benutzung aller Administrations-Tools ist zu protokollieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.
- **Versuche unbefugten Einloggens und Überschreitung von Befugnissen**
  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormalitäten" beim Einloggen und der Benutzung von Hard- und Software-Komponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

Bei der Verarbeitung von personenbezogenen Daten sind folgende Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. Daten vollständig bzw. selektiv zu protokollieren:

- **Eingabe von Daten**
  Die so genannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, sollte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden.
- **Datenübermittlungen**
  Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.
- **Benutzung von automatisierten Abrufverfahren**
  In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.
- **Löschung von Daten**
  Die Durchführung der Löschung ist zu protokollieren.
- **Aufruf von Programmen**
  Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

**Zweckbindung bei der Nutzung von Protokolldaten**

Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung. Sie dürfen nur zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden und die Kontrollen durch interne oder externe Datenschutzbeauftragte. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z. B. zur Strafverfolgung, zu.

**Aufbewahrungsdauer**

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Protokolldaten sind unverzüglich zu

löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht.

Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten.

**Technische und organisatorische Rahmenbedingungen**

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Es sollte ein Konzept erstellt werden, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert (siehe auch B 5.22 *Protokollierung*).
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle müssen so gestaltet sein, dass eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten sollten vorab abgestimmt und festgelegt sein.
- Kontrollen sollten so zeitnah durchgeführt werden, dass bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen müssen rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen sollten nach dem Vier-Augen-Prinzip erfolgen.
- Die Mitarbeiter sollten darüber informiert sein, dass Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen sollten automatisierte Verfahren (z. B. watch dogs) verwendet werden.
- Personal- bzw. Betriebsräte sollten bei der Erarbeitung des Protokollierungskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

Prüffragen:

- Wurde ein Konzept erstellt, das den Zweck der Protokollierung, deren Kontrollen sowie Schutzmechanismen für die Rechte der betroffenen Personen beschreibt?
- Wird die Zweckbindung der Protokolldaten beachtet, insbesondere bei den Zugriffsregelungen?
- Lässt die Form der Protokollierung effektive Auswertungsmöglichkeiten zu?

- Wurden die Auswertungsmöglichkeiten mit dem Datenschutzbeauftragten und der Personalvertretung abgestimmt?

# M 2.111 Bereithalten von Handbüchern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Bei der Beschaffung von Informationstechnik, egal ob es sich um Hardware oder Software handelt, müssen die zugehörigen Handbücher und technischen Referenzen in ausreichender Anzahl mitbeschafft werden.

Im Lieferumfang von IT-Produkten ist zunehmend keine weiterführende Dokumentation mehr enthalten, sondern es werden neben Online-Hilfen nur noch Installationshilfen und einführende Texte mitgeliefert. Dieser eingeschränkte Umfang an Dokumentationshilfen ist insbesondere bei auftretenden Fehlern unzureichend. Es ist daher darauf zu achten, dass die erforderlichen Handbücher, technische Referenzen und Fehlerkataloge zusätzlich beschafft werden. Hierbei muss nicht ausschließlich auf die vom Hersteller angebotene Literatur zurückgegriffen werden.

Alle Handbücher zu einem IT-Produkt müssen jederzeit in der Anwendungsumgebung verfügbar sein. Beispielweise müssen die Handbücher zu einem Server-Betriebssystem bei diesem Server aufbewahrt werden, und nicht in einer evtl. geschlossenen Bibliothek. Bei der Notfallplanung ist der Zugriff auf diese Literatur einzuplanen (siehe M 6.3 *Erstellung eines Notfall-Handbuches*).

Prüffragen:

- Steht für alle IT-Komponenten die erforderliche Dokumentation zur Verfügung?

# M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Mitarbeiter

Damit dienstliche Aufgaben an einem häuslichen Arbeitsplatz erledigt werden können, müssen dort alle nötigen Informationen vorhanden sein. Akten, Datenträger und andere Unterlagen müssen dabei sicher transportiert werden. Dafür ist die Art und Weise des Austauschs von Datenträgern zwischen häuslichem Arbeitsplatz und Institution zu regeln. Folgende Punkte sollten daher mindestens betrachtet bzw. geregelt werden:

- Welche Akten, Datenträger und Unterlagen dürfen über welchen Transportweg (Postweg, Kurier, Paketdienst, ...) ausgetauscht werden (siehe M 5.23 *Auswahl einer geeigneten Versandart für Datenträger*)?
- Welche Schutzmaßnahmen sind beim Transport zu beachten? Dazu gehört auch die Auswahl einer geeigneten Verpackung (siehe auch M 2.44 *Sichere Verpackung der Datenträger*). Informationen auf digitalen Datenträgern sollten vor dem Transport verschlüsselt werden, um unbefugtes Auslesen zu verhindern.
- Welche Akten und Datenträger dürfen nur persönlich transportiert werden?

Da es sich bei Schriftstücken, Dokumenten und Akten oftmals um Unikate handelt, muss bei der Auswahl eines geeigneten Aktenaustauschverfahrens der Schaden im Falle eines Verlustes beachtet werden. Sofern möglich und zulässig sollten vor dem Datenträgeraustausch Kopien angefertigt werden.

Alle betroffenen Mitarbeiter müssen darüber informiert sein, wie Akten und Datenträger zu transportieren und dabei angemessen zu schützen sind.

Prüffragen:

- Ist geregelt, wie Akten, Datenträger und andere Unterlagen beim Transport zwischen häuslichem Arbeitsplatz und Institution geschützt werden müssen?
- Sind Akten, Datenträger und andere Unterlagen ausreichend vor Transportverlusten geschützt?
- Sind betroffene Mitarbeiter darüber informiert, wie Akten und Datenträger zu transportieren sind?

# M 2.113 Regelungen für Telearbeit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Für die Ausgestaltung der Rahmenbedingungen für Telearbeit sind verschiedene arbeitsrechtliche und arbeitsschutzrechtliche Aspekte zu beachten. So sollten strittige Punkte entweder durch Betriebsvereinbarungen oder zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen Telearbeiter und Arbeitgeber geklärt werden. In diesen Vereinbarungen sollten beispielsweise die Punkte "Freiwilligkeit der Teilnahme an der Telearbeit", "Mehrarbeit und Zuschläge", "Aufwendungen für Fahrten zwischen Betrieb und häuslicher Wohnung", "Aufwendungen z. B. für Strom und Heizung", "Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit)" und "Beendigung der Telearbeit" geklärt bzw. geregelt werden.

Die für die Telearbeit im Umgang mit Informationen und der Informations- und Kommunikationstechnik notwendigerweise umzusetzenden Sicherheitsmaßnahmen sind zusätzlich in einer Sicherheitsrichtlinie zur Telearbeit zu dokumentieren.

Folgende Aspekte sollten beispielsweise in den Regelungen für Telearbeit beachtet werden:

- **Arbeitszeitregelung:** Die Verteilung der Arbeitszeiten auf Tätigkeiten in der Institution und am häuslichen Arbeitsplatz muss geregelt sein. Auch müssen feste Zeiten der Erreichbarkeit am häuslichen Arbeitsplatz festgelegt werden.
- **Reaktionszeiten:** Es sollte geregelt werden, in welchen Abständen die Telearbeiter aktuelle Informationen abrufen (z. B. wie häufig E-Mails gelesen werden) und in welchem Zeitraum sie darauf zu reagieren haben.
- **Umgang mit vertraulichen Informationen:** Bei der Telearbeit werden Informationen sowohl analog, also z. B. auf Papier, als auch digital bearbeitet. Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden. Daher ist der komplette Lebensweg geschäftskritischer Informationen angemessen abzusichern.
- **Arbeitsmittel:** Es sollte festgeschrieben werden, welche Arbeitsmittel die Telearbeiter einsetzen können und welche nicht genutzt werden dürfen (z. B. nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten wird untersagt. Weiterhin könnte die Nutzung von Datenträgern, wie beispielsweise CDs, DVDs oder USB-Sticks untersagt werden, wenn der Telearbeitsplatz dies nicht erfordert.
- **Datensicherung:** Die Telearbeiter sind zu verpflichten, regelmäßig Datensicherungen der lokal gespeicherten Daten durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherungen in der Institution zur Unterstützung der Verfügbarkeit hinterlegt wird.
- **Synchronisation von Datenbeständen:** Datenbestände, die sowohl in der Institution als auch an Telearbeitsplätzen bearbeitet werden sollen, müssen geeignet synchronisiert werden. Das Vorgehen bei der Synchronisation muss genau geplant werden, damit es nicht zu Konflikten und damit zu einem Datenverlust kommt, wenn zwei Benutzer den gleichen Da-

tensatz in gespiegelten Datenbeständen geändert bzw. gelöscht haben. Es empfiehlt sich, hierfür geeignete Software einzusetzen.
- **Datenschutz:** Die Telearbeiter sind auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen.
- **Datenkommunikation:** Es muss festgelegt werden, welche Daten auf welchem Weg übertragen bzw. welche Daten nicht oder nur verschlüsselt elektronisch übermittelt werden dürfen. Ebenso ist festzulegen, welche Dokumente zwischen Institution und häuslichem Arbeitsplatz transportiert werden dürfen und wie diese dabei geschützt werden.
- **Transport von Dokumenten und Datenträgern:** Die Art und Absicherung des Transportes von Dokumenten und Datenträgern zwischen häuslichem Arbeitsplatz und Institution ist zu regeln. Vertrauliche Daten auf digitalen Datenträgern sollten nur verschlüsselt transportiert werden.
- **Meldeweg:** Die Telearbeiter sind zu verpflichten, sicherheitsrelevante Vorkommnisse unverzüglich an eine im Vorfeld zu bestimmende Stelle in der Institution zu melden.
- **Zutrittsrecht zum häuslichen Arbeitsplatz:** Für die Durchführung von Kontrollen und für die Verfügbarkeit von Akten und Daten im Vertretungsfall kann ein Zutrittsrecht zum häuslichen Arbeitsplatz (gegebenenfalls mit vorheriger Anmeldung) vereinbart werden.
- **Vertretungsregelung**: Für jeden Telearbeiter sollte ein Vertreter bestimmt werden, der über die laufenden Aktivitäten informiert sein muss, damit er auch kurzfristig die Vertretung übernehmen kann. Dazu müssen die Arbeitsergebnisse durch die Telearbeiter immer sorgfältig dokumentiert werden. Gegebenenfalls sind sporadische oder regelmäßige Treffen zwischen dem Telearbeiter und seinem Vertreter sinnvoll. Ergänzend muss geregelt werden, wie der Vertreter im unerwarteten Vertretungsfall Zugriff auf die Daten auf den Telearbeitsrechner oder am Telearbeitsplatz vorhandene Unterlagen nehmen kann. Dieser Vertretungsfall sollte probeweise durchgespielt und vom Telearbeiter und seiner Vertretung ausgewertet werden.

Die Regelungen sind jedem Telearbeiter auszuhändigen. Entsprechende Merkblätter sind regelmäßig zu aktualisieren.

Prüffragen:

- Sind alle relevanten Aspekte zur Telearbeit geregelt worden?
- Sind alle für die Telearbeit relevanten Sicherheitsmaßnahmen in einer Sicherheitsrichtlinie zur Telearbeit dokumentiert?
- Sind alle Telearbeiter auf die Einhaltung der Sicherheitsrichtlinie zur Telearbeit verpflichtet worden?
- Wurden den Telearbeitern die Regelungen und die Sicherheitsrichtlinie zur Telearbeit oder ein Merkblatt ausgehändigt, in dem die von ihnen zu beachtenden Sicherheitsmaßnahmen erläutert werden?
- Sind Vertreter für alle Telearbeiter benannt worden?
- Sind Vertretungsfälle für Telearbeiter erprobt worden?

# M 2.114 Informationsfluss zwischen Telearbeiter und Institution

**Verantwortlich für Initiierung:** Telearbeiter, Vorgesetzte
**Verantwortlich für Umsetzung:** Telearbeiter, Vorgesetzte

Damit Telearbeiter nicht vom betrieblichen Geschehen ausgeschlossen werden, muss ein regelmäßiger Informationsaustausch zwischen den Telearbeitern und den Arbeitskollegen institutionalisiert werden. Hierfür sind sowohl die Vorgesetzten, als auch die Telearbeiter selber verantwortlich. Die jeweiligen Vorgesetzten müssen sicherstellen, dass die Telearbeiter alle notwendigen Informationen für ihre Arbeitsbereiche erhalten. Die Telearbeiter müssen jedoch auch selbstständig nach Informationen und Neuigkeiten fragen. Der regelmäßige Informationsaustausch ist wichtig, damit die Telearbeiter über Planungen und Zielsetzungen in ihrem Arbeitsbereich informiert sind. Frustrationen können so vermieden und ein positives Telearbeitsklima geschaffen und erhalten werden.

Die Telearbeiter sollten an den Umlaufverfahren für Hausmitteilungen, einschlägige Informationen und Zeitschriften beteiligt werden. Dies stellt ein Problem dar, wenn Telearbeiter ausschließlich zu Hause arbeiten. Eine Lösungsmöglichkeit ist das Einscannen wichtiger Schriftstücke, um sie den Telearbeitern per E-Mail zuzustellen. Die Telearbeiter müssen auf jeden Fall zeitnah über Änderungen von Sicherheitsmaßnahmen und anderen sicherheitsrelevanten Aspekten unterrichtet werden.

Die Arbeitskollegen in der Institution müssen über die Anwesenheits- und Erreichbarkeitszeiten der Telearbeiter in Kenntnis gesetzt werden. Die entsprechenden E-Mail-Adressen und Telefonnummern sollten allen Kollegen bekannt sein. Außerdem sollte zur besseren Erreichbarkeit die Möglichkeit der Anrufweiterleitung vom Telefonanschluss des Mitarbeiters in der Institution zum Telefon am häuslichen Arbeitsplatz genutzt werden.

Folgende Punkte müssen darüber hinaus bei der Telearbeit geklärt werden:

- Wer ist Ansprechpartner bei technischen und/oder organisatorischen Problemen bei der Telearbeit?
- Wem müssen Sicherheitsvorkommnisse mitgeteilt werden?
- Wie erfolgt die Aufgabenzuteilung?
- Wie erfolgt die Übergabe der Arbeitsergebnisse?

Treten technisch-organisatorische Probleme auf, müssen diese vom Telearbeiter unverzüglich der Institution gemeldet werden.

Prüffragen:

- Sind alle Telearbeiter in die innerbetrieblichen Informationsflüsse eingebunden?
- Werden die Telearbeiter zeitnah über Änderungen von Sicherheitsmaßnahmen und andere sicherheitsrelevante Aspekte informiert?
- Ist allen Kollegen bekannt, wann und wo die Telearbeiter erreicht werden können?

# M 2.115 Betreuungs- und Wartungskonzept für Telearbeitsplätze

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT, Telearbeiter

Für die Telearbeitsplätze muss ein spezielles Betreuungs- und Wartungskonzept erstellt werden, das folgende Punkte vorsieht:

- **Benennen von Ansprechpartnern für den Benutzerservice:** An diese Stelle können sich Telearbeiter bei Software- und Hardware-Problemen wenden. Der Benutzerservice versucht (auch telefonisch) kurzfristig Hilfestellung zu leisten bzw. leitet Wartungs- und Reparaturarbeiten ein. Dazu sollte dem Benutzerservice die Konfiguration der Telearbeitsrechner bekannt sein.
- **Wartungstermine:** Die Termine für Wartungsarbeiten an den Telearbeitsgeräten sollten frühzeitig bekanntgegeben werden, damit die Telearbeiter zu diesen Zeiten den Wartungstechnikern Zutritt zum häuslichen Arbeitsplatz oder den Zugriff auf Telearbeitsrechner gewähren oder zu wartende IT-Geräte in die Institution bringen können.
- **Einführung von Standard-Telearbeitsrechnern:** Die IT-Ausstattung aller Telearbeiter einer Institution sollte standardisiert sein, damit der Benutzerservice schnell bei Problemen helfen kann. Auch wird dadurch der konzeptionelle und administrative Aufwand für den Aufbau eines sicheren Telearbeitsrechners erleichtert.
- **Fernwartung:** Falls der Telearbeitsrechner über Fernwartung administriert und gewartet werden kann, sind die notwendigen Sicherheitsmaßnahmen zu klären. Außerdem ist mit den betroffenen Telearbeitern der Zeitpunkt für einen Online-Zugriff zur Wartung zu vereinbaren. Um den Missbrauch des Fernwartungszugangs zu verhindern (siehe M 5.33 *Absicherung von Fernwartung*) müssen angemessene Sicherungsverfahren festgelegt werden.
- **Transport der IT:** Es sollte aus Gründen der Haftung festgelegt werden, wer autorisiert ist, IT-Geräte und andere Ausstattung für die Telearbeitsplätze zwischen der Institution und den häuslichen Arbeitsplätzen der Telearbeiter zu transportieren. Dabei muss auch der Schutz der Geräte beachtet werden. Ein Laptop kann beispielsweise vom Telearbeiter persönlich transportiert werden, sollte aber mit einer Diebstahlsicherung versehen und die Informationen verschlüsselt sein.

Weitere Regelungen können der Maßnahme M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten* entnommen werden.

Prüffragen:

- Gibt es ein Betreuungs- und Wartungskonzept für Telearbeitsplätze?
- Sind für die Telearbeiter Ansprechpartner für Hard- und Softwareprobleme benannt worden?
- Ist der sichere Transport von IT-Geräten zwischen Institution und häuslichem Arbeitsplatz geregelt?

# M 2.116 Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Telearbeiter

Bei der Telearbeit werden typischerweise verschiedene Möglichkeiten zur Kommunikation wie beispielsweise Telefon-, Fax- und Internet-Anbindung, aber auch Postaustausch sowie Akten- und Datenträgertransport benötigt. Daher muss ein Telearbeitsrechner über diverse elektronische Kommunikationsmöglichkeiten verfügen.

Es muss geregelt werden, auf welche Weise die vorhandenen Kommunikationsmöglichkeiten genutzt werden dürfen. Auch der Postaustausch sowie der Akten- und Datenträger-Transport zwischen Institution und Telearbeitsplatz muss dabei betrachtet werden. Grundsätzlich sollte die private Nutzung der Kommunikationsmöglichkeiten klar geregelt werden. Die Regelungen über die Nutzung der Kommunikationsmöglichkeiten bei Telearbeit sind schriftlich zu fixieren, z. B. in der Sicherheitsrichtlinie zur Telearbeit (siehe M 2.113 *Regelungen für Telearbeit*). Diese Regelungen sind den Telearbeitern auszuhändigen.

Zu klären sind zumindest folgende Punkte:

- **Datenflusskontrolle**
  Der Austausch von Informationen zwischen dem Telearbeitsplatz und der Institution muss so geregelt sein, dass die Sicherheit der Informationen gewährleistet ist.
  - Welche Dienste dürfen zum Informationsaustausch und zur Datenübertragung genutzt werden?
  - Welche Informationen dürfen dabei an wen weitergegeben werden?
  - Welche Dienste dürfen explizit nicht genutzt werden?
  - Welcher Schriftverkehr darf über E-Mail abgewickelt werden? Ist eine Unterschriftenregelung für die Kommunikation vorgesehen?
  - Welche Authentisierungsverfahren werden für den Schriftverkehr und für den Datenaustausch genutzt?
  - Werden digitale Signaturen eingesetzt?
- **Zugriffsberechtigungen**
  Erfordert die Telearbeit den Zugriff auf die IT der Institution (zum Beispiel auf einen Server), muss zuvor festgelegt werden, welche Objekte wie Daten oder IT ein Telearbeiter tatsächlich für die Erfüllung seiner Aufgaben benötigt. Für die Erteilung der Zugangs- und Zugriffsrechte siehe M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*.
  - Sind die notwendigen Rechte wie Lese- und Schreibrechte auf diese Objekte zugewiesen worden? Auf Objekte, die ein Telearbeiter für seine Aufgabenwahrnehmung nicht braucht, sollte er auch nicht zugreifen können.
- **Sicherheitsmaßnahmen beim Informationsaustausch**

Der Informationsaustausch bei der Telearbeit muss angemessen abgesichert werden. Vertrauliche Informationen müssen sicher transportiert werden.

- Für welche Datenträger soll welche Versandart eingesetzt werden (z. B. Kurierdienst)? Welche Art der Transportsicherung ist angemessen (z. B. Umschläge mit Sicherheitsetiketten)?
- Für welche Daten sollen welche Verschlüsselungsverfahren eingesetzt werden? Daten sollten bei der Datenübertragung und auf Datenträgern möglichst immer verschlüsselt werden, damit Transportverluste höchstens deren Verfügbarkeit und nicht deren Vertraulichkeit gefährden kann.
- Werden von zu übertragenden Daten, die nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden sind, Sicherungskopien dieser Zusammenstellung vorgehalten? Bei Verlust oder Beschädigung des Datenträgers kann auf diese Weise der Versand mit geringfügigem Aufwand erneut erfolgen.
- Für welche Daten ist eine Löschung nach erfolgreicher Übertragung notwendig? Dies kann beispielsweise für personenbezogene Daten gelten.
- Von welchen Daten soll trotz der erfolgreichen Übertragung eine Kopie der Daten auf dem Telearbeitsrechner verbleiben?
- Vor Versand und nach Erhalt von Daten sollte ein Computer-Viren-Check der Daten durchgeführt werden.
- Für welche Datenübertragungen sollte eine Protokollierung erfolgen? Falls eine automatische Protokollierung von Datenübertragungen nicht möglich sein sollte, ist festzulegen, ob und in welchem Umfang eine handschriftliche Protokollierung vorzusehen ist.

- **Internet-Nutzung**
  Es ist zu regeln, ob über den Telearbeitsrechner Internet-Dienste genutzt werden dürfen. Dabei ist auch zu klären, ob eine private Nutzung erlaubt wird.

  - Wird die Nutzung von Internet-Diensten generell verboten?
  - Welche Internet-Dienste dürfen genutzt werden?
  - Dürfen Daten aus dem Internet geladen werden? Bei Daten von fremden Servern besteht die Gefahr, dass sie Schadsoftware enthalten.
  - Welche Rahmenbedingungen und technischen Sicherheitsmaßnahmen müssen bei der Internet-Nutzung beachtet werden? Welche Sicherheitsmechanismen sollen beispielsweise im Browser aktiviert werden?
  - Dürfen sich Telearbeiter am Informationsaustausch über Internet-Plattformen, Newsgruppen, Blogs oder ähnlichem beteiligen? Ist hierfür ein Pseudonym erforderlich?

- **Informationsgewinnung**
  Vom Telearbeitsplatz aus können verschiedene Dienstleistungen zur Informationsgewinnung in Anspruch genommen werden, z. B. Datenbankabfragen, Suchmaschinen, Dokumentationssysteme oder Recherchedienstleister. Da deren Nutzung teilweise kostenpflichtig ist, ist das Budget, welches die Institution hierfür zur Verfügung stellt, zu berücksichtigen.

  - Welche Dienstleistungen zur Informationsgewinnung dürfen vom Telearbeitsplatz aus in Anspruch genommen werden?
  - Abfragen sollten möglichst über eine verschlüsselte Verbindung erfolgen, damit aus der Art der Abfragen keine Rückschlüsse auf Interna wie beispielsweise Unternehmensstrategien gezogen werden können.

- Reicht die Bandbreite der Kommunikationsanbindung am Telearbeitsrechner für Online-Recherchen und Datenbankabfragen?

Prüffragen:

- Ist klar geregelt, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen benutzt werden dürfen?
- Ist gewährleistet, dass der Informationsaustausch bei der Telearbeit angemessen abgesichert ist?
- Sind dienstliche und private Nutzung von Internet-Diensten bei der Telearbeit geregelt?

# M 2.117 Erstellung eines Sicherheitskonzeptes für Telearbeit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Organisation, Vorgesetzte

Damit Telearbeit in einem sicheren Rahmen erfolgen kann, müssen verschiedene Rahmenbedingungen geklärt werden. Es sollte ein Sicherheitskonzept für Telearbeit erstellt werden, in dem die Sicherheitsziele, der Schutzbedarf der bei der Telearbeit zu bearbeitenden Informationen sowie die Risiken und Sicherheitsmaßnahmen aufgezeigt werden.

Bei Telearbeit werden Informationen außerhalb der geschützten Betriebsumgebung verarbeitet. Eine Schutzbedarfsfeststellung der betroffenen Informationen, Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume (vor allem der Telearbeitsplätze) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit ist daher im Vorfeld durchzuführen. Aus dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz leiten sich die Sicherheitsziele und damit die sicherheitstechnischen Anforderungen an die Telearbeiter, die Telearbeitsrechner und die Telearbeitsplätze ab.

Neben einem Überblick über die Gefährdungslage und den organisatorischen, infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Dokumenten und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und zum Löschen bzw. Vernichten von Datenträgern
- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Institution und Telearbeitsplatz, um vertrauliche Daten zu schützen
- Authentisierungsmechanismen
- Regelungen für weitere Netzanbindungen
- Regelungen für den Datenaustausch
- Datensicherung

Zur Ausgestaltung der Telearbeit sind zusätzlich diverse Gesetze und Vorschriften zu beachten (siehe M 2.113 *Regelungen für Telearbeit*).

Die Anforderungen, Ziele und die zu ergreifenden Maßnahmen zur Sicherheit bei Telearbeit sind zu dokumentieren. Das Sicherheitskonzept zur Telearbeit ist mit dem übergreifenden Sicherheitskonzept der Institution abzustimmen und zu harmonisieren. Außerdem muss es regelmäßig aktualisiert werden und an Änderungen in der Organisation oder der Technik angepasst werden.

Die von den Telearbeitern umzusetzenden Sicherheitsmaßnahmen sind in einer Sicherheitsrichtlinie zur Telearbeit zielgruppengerecht zusammenzufassen.

Prüffragen:

- Liegt ein Sicherheitskonzept zur Telearbeit vor?
- Ist das Sicherheitskonzept zur Telearbeit aktuell?

- Sind im Sicherheitskonzept zur Telearbeit alle Sicherheitsanforderungen und -maßnahmen ausreichend detailliert beschrieben?

# M 2.118 Konzeption der sicheren E-Mail-Nutzung

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.119 Regelung für den Einsatz von E-Mail

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.120 Einrichtung einer Poststelle

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.121 Regelmäßiges Löschen von E-Mails

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.122 Einheitliche E-Mail-Adressen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

E-Mail-Adressen sollten aufgrund von klaren Namenskonventionen vergeben werden. Wichtig ist, dass keine Nicht-ASCII-Zeichen wie Umlaute innerhalb von E-Mail-Adressen verwendet werden.

Um Angriffe zu erschweren, Spam und Werbe-E-Mail zu vermeiden bzw. um möglichst wenig Information nach außen weiterzugeben, kann es sinnvoll sein, statt benutzer- und organisationsbezogenen E-Mail-Adressen wie *nachname@organisation.de* schwer erratbare E-Mail-Adressen zu verwenden. Dies macht aber auch die Adressweitergabe unbequemer und kann die Kommunikation mit Externen erschweren.

Wenn E-Mail-Adressen geändert werden oder wegfallen, ist darauf zu achten, dass zumindest für eine Übergangszeit E-Mails, die noch an diese Adressen gerichtet ist, an die jetzt aktuellen Adressen weitergeleitet wird.

**Einrichtung funktionsbezogener E-Mail-Adressen**

In vielen Institutionen werden Geschäftsprozesse inzwischen ganz oder teilweise per E-Mail abgewickelt. Dabei ist es wichtig, dass Nachrichten rechtzeitig den richtigen Empfänger erreichen. Durch Urlaub, Dienstreisen, Krankheit oder personelle Veränderungen können zu unterschiedlichen Zeitpunkten aber ganz verschiedene Personen für die Bearbeitung einer E-Mail zuständig sein.

Daher sollten für bestimmte Funktionen organisations- bzw. funktionsbezogene E-Mail-Adressen eingerichtet werden, um unabhängig von Personen die Zustellung zur richtigen Organisationseinheit zu garantieren. Dies ist insbesondere bei zentralen Anlaufstellen wichtig. Dieser Ansatz hat unter anderem folgende Vorteile:

- E-Mails an funktionsbezogene Adressen können gegebenenfalls direkt an Stellvertreter verteilt werden. Dadurch kann auch bei Abwesenheit des Hauptansprechpartners eine zügige Bearbeitung erreicht werden. Werden E-Mails an funktionsbezogene Adressen nicht direkt an den jeweiligen Ansprechpartner weitergeleitet, sondern in eigenen Postfächern abgelegt, so hat dies einen zusätzlichen Vorteil im Bezug auf Datenschutz. In diesem Fall braucht nämlich im Fall einer ungeplanten Abwesenheit (beispielsweise Unfall, Krankheit) des eigentlichen Empfängers nicht dessen persönliches Postfach "geöffnet" zu werden.
- Bei einem Wechsel der Zuständigkeit müssen nicht alle Kommunikationspartner informiert werden. In diesem Fall müssen lediglich alle E-Mails, die an die funktionsbezogene E-Mail-Adresse gerichtet sind, an die neuen Ansprechpartner weitergeleitet werden.
- Funktionsbezogene E-Mail-Adressen können aussagekräftig benannt werden,z. B. *beratung@..., webmaster@..., vertrieb@...*, und lassen sich dadurch oft leichter merken als personenbezogene Adressen.
- Durch die Adressierung an die funktionsbezogene E-Mail-Adresse können die Empfänger auch unabhängig vom Betreff (*Subject*) erkennen, um welches Thema es in der E-Mail wahrscheinlich geht.

Für verschiedene Funktionen, die direkt mit dem Betrieb einer Internet-Domain zusammen hängen, wird darüber hinaus die Existenz gewisser funktionsbezogener E-Mail-Adressen (beispielsweise *postmaster*) in den relevanten De-

Facto-Standards (IETF RFCs, hier insbesondere die RFC 822 und RFC 2142) explizit gefordert (siehe auch M 2.456 *Sichere Administration von Groupware-Systemen*).

Es sollte dokumentiert sein, welche organisations- und funktionsbezogenen Adressen existieren und zu welchem Zweck sie dienen.

Prüffragen:

- Gibt es eine eindeutige Namenskonvention für E-Mail-Adressen?

# M 2.123 Auswahl eines Groupware- oder Mailproviders

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Vor der Auswahl eines Groupware- oder Mailproviders sollten sich die Verantwortlichen über die beim Provider geltenden Regelungen informieren, beispielsweise ob und wie lange Vorgänge und Kommunikationsdaten archiviert werden, ob es Obergrenzen für den Umfang von E-Mails beim Empfang oder Versand gibt, ob E-Mails gefiltert werden, und wenn ja, nach welchen Regeln.

Institutionen nehmen Dienstleistungen von Groupware- oder Mailprovidern in Anspruch, wenn sie auf den Aufbau und Wartung eigener Systeme verzichten wollen oder eigene Systeme flexibler gestalten wollen. Daneben gibt es neben der Komplett-Auslagerung von Groupware-Diensten auch die Möglichkeit, einzelne Dienstleistungen von Groupware-Providern zu nutzen, die im Internet angeboten werden, um die Arbeit in Teams oder unterwegs zu erleichtern, wie Web-Mail-Dienste und Gruppen-Terminkalender. Viele Mitarbeiter benutzen solche Dienste auch privat. Daher muss hier allen Mitarbeitern klar sein, dass sie dienstlich nur von ihrer Institution freigegebene externe Groupware-Dienste benutzen dürfen. Generell muss für alle Mitarbeiter verständlich geregelt sein, was sie bei der Nutzung von externen Groupware-Diensten beachten müssen.

Die Institution sollte vorab klären, welche Sicherheitsmechanismen beim Groupware- oder Mailprovider umgesetzt werden und ob damit die internen Sicherheitsanforderungen erfüllt werden. Die Sicherheitsverantwortlichen sollten sich überzeugen, dass beim Groupware- oder Mailprovider deren Server sicher betrieben werden, also die in M 5.56 *Sicherer Betrieb eines Mailservers* beschriebenen Anforderungen erfüllt sind.

Beim Provider sind Daten über die Benutzer für Abrechnungszwecke gespeichert (Name, Adresse, Benutzer-Kennung, Bankverbindung) ebenso wie Verbindungsdaten und für eine je nach Provider kürzere oder längere Zeitspanne auch die übertragenen Inhalte.

Die Anwender sollten sich bei ihrem Groupware- oder Mailprovider erkundigen, welche Daten wie lange über sie gespeichert werden. Bei der Auswahl von Providern sollte berücksichtigt werden, dass deutsche Betreiber den einschlägigen datenschutzrechtlichen Regelungen für die Verarbeitung dieser Daten unterliegen.

Bei E-Mail können die Benutzer durch den Einsatz von Verschlüsselung verhindern, dass der Provider die Inhalte der übertragenen Informationen mitlesen kann. Bei anderen Groupware-Diensten wie Adressbüchern oder Kalendern ist dies meist nicht möglich, daher sollten sich Anwender vor der Nutzung solcher Dienste informieren, wie hierbei die Daten vor unberechtigten Zugriffen abgeschirmt werden.

Große Provider mit großem eigenem Netz haben den Vorteil, dass E-Mails oder andere Informationen, die nur innerhalb dieses Netzes ausgetauscht werden, sicherer vor Manipulationen ist als bei Weiterleitung über das Internet.

Bei Providern, die ihren Hauptsitz im Ausland haben, werden häufig auch alle E-Mails und andere Informationen über dieses Land geroutet. Dieser Punkt sollte berücksichtigt werden, wenn man sich Gedanken darüber macht, über

wie viele Gateways die Informationen weiterverteilt werden, also wer sie beispielsweise mitlesen kann.

Prüffragen:

- Ist sichergestellt, dass alle erforderlichen Sicherheitsmechanismen beim Groupware- oder Mailprovider umgesetzt werden?
- Ist allen Mitarbeitern bekannt, was bei der Nutzung von externen Groupware-Diensten, z. B. Web-Mail-Diensten, zu beachten ist?

# M 2.124 Geeignete Auswahl einer Datenbank-Software

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bei der Beschaffung neuer Datenbank-Software besteht die Möglichkeit, diese von vornherein so auszuwählen, dass im späteren Betrieb mit nur geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann.

Zu Beginn muss der Einsatzbereich und Verwendungszweck des Datenbanksystems geklärt werden, um die Anforderungen bezüglich der Verfügbarkeit, der Integrität und der Vertraulichkeit formulieren zu können. Weiterhin sind die Anforderungen hinsichtlich der zu verarbeitenden Datenmengen, der Verarbeitungsgeschwindigkeit und des Durchsatzes zu quantifizieren. Daraus leiten sich die zu erfüllenden Eigenschaften für die zu beschaffende Datenbank-Software ab, wie z. B. Verfügbarkeit für bestimmte Hardware-Plattformen bzw. Betriebssysteme oder Umfang von notwendigen Sicherheitsmechanismen. In diesem Planungsstadium kann bereits erkannt werden, ob und in welchem Maße für den späteren Betrieb des Datenbanksystems Hardware nach- bzw. umgerüstet werden muss. Anhand der Verfügbarkeitsanforderungen sind auch die benötigten Überwachungsmöglichkeiten zu definieren, d. h. es muss festgelegt werden, welche Datenbankzustände in welcher Form erkennbar sein sollen (z. B. durch eine Protokollierung in einer Datei), sowie die Art der Benachrichtigung verantwortlicher Personen bzw. Personengruppen über kritische Zustände der Datenbank (z. B. durch eine Meldung an der Konsole).

Für die Beschaffung einer Datenbank-Software sollten insbesondere die folgenden Punkte berücksichtigt werden:

- Die Datenbank-Software muss über eigene geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen (siehe M 2.128 *Zugangskontrolle einer Datenbank*).
- Die Datenbank-Software muss über geeignete Mechanismen zur Ressourcenbeschränkung verfügen (siehe M 4.73 *Festlegung von Obergrenzen für selektierbare Datensätze*).
- Falls in der Datenbank vertrauliche Daten verwaltet werden sollen, so muss einem unberechtigten Zugriff vorgebeugt werden können. Die zu beschaffende Datenbank-Software muss in diesem Fall entsprechende Zugriffskontrollmechanismen zur Verfügung stellen (siehe M 2.129 *Zugriffskontrolle einer Datenbank*).
  Es sollte auch die Zusammenfassung mehrerer Benutzer mit gleichen Zugriffsrechten zu Gruppen möglich sein. Eine Unterscheidung zwischen der Gruppe der Administratoren und der Gruppe der Benutzer ist dabei obligatorisch. Weiterhin sollte eine Trennung von verschiedenen Administrator-Rollen unterstützt werden (siehe M 2.131 *Aufteilung von Administrationstätigkeiten bei Datenbanksystemen*).
- Es gibt Datenbanken mit unterschiedlich starken Zugriffsschutzmechanismen. Ähnliche Sicherheitsmechanismen können dabei auch in unterschied-
  licher Granularität angeboten werden. Im Vorfeld ist zu klären, welcher Zugriffsschutz erforderlich ist und welche Datenbank-Software den definierten Sicherheitsanforderungen entspricht. Maßgeblich hierfür sind die

Möglichkeiten, Zugriffsrechte auf Datenbankobjekte und die Daten selbst einzuschränken.
**Beispiele:**

  - Den Anwendern kann das Recht entzogen werden, Datenbankobjekte (z. B. Tabellen) anzulegen oder zu modifizieren.
  - Die Anwender können zwar eine lesende Zugriffsberechtigung auf eine Tabelle erhalten, gleichzeitig können aber modifizierende Zugriffsrechte ausgeschlossen werden.
  - Für bestimmte Tabellen oder bestimmte Felder einer Tabelle kann der Zugriff je nach Anwender verboten werden.
  - Anwender erhalten keinerlei Zugriffsberechtigungen auf Datensätze mit bestimmten Merkmalen (z. B. ein Sachbearbeiter aus Bonn hat keinen Zugriff auf die Daten eines Sachbearbeiters aus Köln).
- Einige Hersteller bieten sowohl die Möglichkeit der Definition von Gruppen als auch die von Rollen an. Dadurch kann eine differenziertere Zugriffskontrolle auf die Datenbankobjekte realisiert werden. Im Vorfeld sind die diesbezüglichen Anforderungen zu klären und mit den zur Auswahl stehenden Datenbank-Softwareprodukten abzugleichen.
- Die Datenbank-Software muss ebenfalls hinsichtlich ihrer Überwachungs- und Kontrollmechanismen überprüft werden. Die diesbezüglichen Anforderungen müssen definiert und mit den Leistungsprofilen der Produkte abgeglichen werden (Beispiele siehe M 2.133 *Kontrolle der Protokolldateien eines Datenbanksystems* bzw. M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*).
- Es muss geprüft werden, ob die Datenbank-Software eine Rollentrennung zwischen Administrator und Revisor unterstützt. Es muss möglich sein, die Rolle eines Revisors einzurichten, der als einziger in der Lage ist, die Protokolldateien auszuwerten und zu löschen. Dies verhindert potentielle Manipulationen durch den Datenbank-Administrator.
- Zum Schutz der Datenbankintegrität muss die Datenbank-Software über ein vollständiges Transaktionssystem verfügen, welches dem ACID-Prinzip genügt. Diese Anforderung wird heutzutage von allen wesentlichen relationalen Datenbankmanagementsystemen erfüllt.
- Es müssen Mechanismen zur Datensicherung der Datenbank vorhanden sein (siehe M 6.49 *Datensicherung einer Datenbank*).
  Im Vorfeld muss in diesem Zusammenhang geklärt werden, welche Möglichkeiten hinsichtlich der Datensicherung die Datenbank-Software zur Verfügung stellen muss. So wird beispielsweise eine partielle Datenbanksicherung nicht für alle am Markt erhältlichen Produkte angeboten. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann.

Anhand dieser Kriterien müssen die zur Auswahl stehenden Datenbanksysteme geprüft und bewertet werden. Es ist dann diejenige Software auszuwählen, die die spezifischen Anforderungen am besten erfüllt. Weitergehende Anforderungen müssen entweder durch Zusatzprodukte oder durch Eigenentwicklung abgedeckt werden. Es sollte jedoch schon vor der Beschaffung abgeklärt werden, zu welcher Datenbank-Software welche Zusatzprodukte verfügbar sind, um nicht auf teure Eigenentwicklungen zurückgreifen zu müssen.

Von den meisten Datenbankmanagementsystemen sind in der Regel mehrere unterschiedliche Versionen auf dem Markt erhältlich. Dabei unterscheiden sich auch die einzelnen Versionen desselben Datenbankmanagementsystems in ihrer Funktionalität, unter anderem auch in sicherheitsrelevanten Bereichen. Der starke Wettbewerb führt dazu, dass einige Hersteller auch noch nicht voll-

ausgereifte Software ausliefern, bei der dann mit Fehlern und eingeschränkter Funktionalität gerechnet werden muss.

In einer Testphase sollte deshalb überprüft werden, ob die ausgewählte Datenbank-Software die erforderlichen Funktionen in der vorgegebenen Einsatzumgebung auch erfüllt. Dies gilt insbesondere für die Anforderungen an die Performance und die benötigten Mechanismen zur Notfallvorsorge.

Vor der Beschaffung sollten auch Erfahrungen aus vergleichbaren Installationen herangezogen werden.

Prüffragen:

- Wurden die Anforderungen an die Datenbank-Software festgelegt und dokumentiert?
- Erfolgte anhand der festgelegten Anforderungen die Auswahl zwischen verschiedenen Datenbank-Software-Produkten?

# M 2.125 Installation und Konfiguration einer Datenbank

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Grundsätzlich muss zwischen der Erstinstallation einer Datenbank-Software und der Installation auf bestehenden Datenbanksystemen unterschieden werden.

Da bei der erstmaligen Installation einer Datenbank-Software noch keine Benutzer auf die Datenbank zugreifen wollen und auch noch keine Altdaten vorhanden sind (es sei denn in anderen Datenbanksystemen), gestaltet sich dies relativ unproblematisch und stört den normalen IT-Betrieb kaum.

Für Installationen auf bestehenden Systemen sollten dagegen die Arbeiten, wenn möglich, außerhalb der regulären Arbeitszeiten erfolgen, um Behinderungen des normalen IT-Betriebs weitestgehend zu minimieren. In jedem Fall sollten die Benutzer über bevorstehende Arbeiten informiert werden, um sie auf eventuell mögliche Störungen oder längere Antwortzeiten hinzuweisen.

Die Installation und Konfiguration einer Datenbank gliedert sich in die folgenden Aktivitäten:

### 1. Installation der Datenbank-Software

Vor der Installation der Datenbank-Software ist zu überprüfen, ob das IT-System entsprechend der Planung vorbereitet wurde, z. B. genügend Speicherplatz zur Verfügung steht und die notwendigen Betriebssystemeinstellungen vorgenommen wurden.

Bei der Installation der Datenbank-Software sind die Installationsanweisungen des Herstellers zu befolgen. Wenn möglich, sollten die vom Hersteller vorgeschlagenen Default-Einstellungen übernommen werden. Dies gilt vor allem für technische Parameter, die z. B. die Größe verschiedener interner Tabellen des DBMS steuern. Für Parameter, die sich auf sicherheitsrelevante Eigenschaften beziehen, muss unter Umständen von den vorgegebenen Werten abgewichen werden.

Die Installation der Datenbank-Software ist geeignet zu dokumentieren. Dies gilt insbesondere für Abweichungen von den vom Hersteller vorgeschlagenen Default-Einstellungen, die ausführlich zu begründen sind.

Sollen vom Hersteller angebotene optionale Funktionalitäten genutzt werden, so ist während der Installation darauf zu achten, dass sie auch entsprechend eingerichtet werden.

Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt.

### 2. Erstellen der Datenbank

Bereits bei der Erstellung der Datenbank sind Parameter anzugeben, die später während des Betriebs des Datenbanksystems nicht mehr geändert werden können.

Die Bedeutung dieser Parameter und die geeignete Auswahl ihrer Werte werden in den Installationsunterlagen und Handbüchern des Herstellers ausführlich erläutert und sind dort entsprechend nachzulesen.

Dem Installationshandbuch bzw. Administrationshandbuch sind außerdem Hinweise über eventuell erforderliche Nacharbeiten nach der Erstellung der Datenbank zu entnehmen.

Auch dieser Vorgang ist im Rahmen einer Dokumentation festzuhalten.

Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt, wobei ihm die anwendungsspezifischen Administratoren beratend zur Seite stehen müssen (z. B. um die Größe der Datenbank festlegen zu können).

**3. Konfiguration der Datenbank**

Im dritten Schritt ist das Benutzer- und Gruppenkonzept sowie das ggf. zum Einsatz kommende Rollenkonzept umzusetzen. Dazu erstellt der fachlich übergreifende Administrator die einzelnen Berechtigungsprofile und legt alle Gruppen sowie die administrativen Benutzer-Kennungen (für die anwendungsspezifischen Administratoren) an. Dabei sind die in M 2.132 *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen* festgelegten Regelungen anzuwenden und zu überprüfen. Hängen die entsprechenden Zugriffsberechtigungen von einzelnen Datenbankobjekten ab, können diese natürlich erst dann definiert werden, wenn die Datenbankobjekte auch existieren (siehe Schritt 4).

Falls die Datenbank-Software eine Verteilung der Daten auf mehrere Dateien oder Festplatten unterstützt, sind zusätzliche Parametereinstellungen vorzunehmen, die das Anlegen dieser Dateien respektive der zugehörigen Speicherbereiche festlegen.

Alle vorgenommenen Einstellungen sind detailliert zu dokumentieren (siehe M 2.25 *Dokumentation der Systemkonfiguration*).

Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt.

**4. Erstellen und Konfigurieren von Datenbankobjekten**

Gemäß des Datenbanksicherheitskonzeptes (siehe M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*) werden im letzten Schritt die Datenbankobjekte der einzelnen Anwendungen angelegt. Dieser Vorgang sollte, wenn möglich, durch den Einsatz von Skripten automatisiert und protokolliert werden. Nach Anlage der Datenbankobjekte sind die notwendigen Zugriffsberechtigungen für Rollen, Gruppen und Benutzer zu ergänzen. Ebenso können jetzt die konkreten Benutzer anhand der existierenden Berechtigungsprofile erstellt werden.

Alle Tätigkeiten in diesem Schritt werden von den anwendungsspezifischen Administratoren durchgeführt.

Prüffragen:

- Werden die Installation der Datenbank-Software und die Erstellung der Datenbank geeignet dokumentiert?

- Werden die Unterlagen des Herstellers zur Installation der Datenbank-Software und Erstellung der Datenbank berücksichtigt?
- Werden alle vorgenommenen Einstellungen bei der Datenbank-Konfiguration detailliert dokumentiert?
- Wird das Berechtigungskonzept bei der Datenbank-Konfiguration berücksichtigt?
- Wird die Erstellung und Konfiguration der Datenbankobjekte einschließlich der Zugriffsberechtigungen protokolliert bzw. dokumentiert?

# M 2.126 Erstellung eines Datenbanksicherheitskonzeptes

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Datenhaltung in Datenbanken über einen längeren Zeitraum hinweg ist meist ein zentraler und kritischer Aspekt des Informationsmanagements einer Behörde bzw. eines Unternehmens. Zur Organisation eines reibungslosen Datenbankbetriebs muss deshalb frühzeitig ein Datenbanksicherheitskonzept erstellt werden, in dem Sicherheitsaspekte bei der Planung, Installation, Konfiguration, Betrieb, Migration und Deinstallation beschrieben sind.

Werden Datenbanken nicht ausreichend geschützt, kann es zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität der gespeicherten Daten kommen. Um diesem vorzubeugen, ist es unumgänglich, ein schlüssiges Datenbanksicherheitskonzept zu erstellen.

Im Konzept müssen insbesondere Aussagen darüber gemacht werden,

- wie die Abgrenzung der Zugriffsrechte zwischen Datenbankadministration und Anwendungsadminstration erfolgt,
- wie die Speicherung der Daten und gegebenenfalls Spiegelung der Datenbank erfolgt,
- wie die Datensicherung erfolgt,
- welche Mechanismen zur Überwachung und Kontrolle der Datenbankaktivitäten eingesetzt werden und
- wie die Datenbankkapazität überwacht werden soll.

Die Sicherheit einer Datenbank wird auf Software-Ebene durch das zugehörige Datenbankmanagementsystem (DBMS) gewährleistet. Damit ein DBMS effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein.

Das DBMS muss,

- auf einer umfassenden Sicherheitspolitik aufsetzen,
- im Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Direkte Zugriffe auf die Datenbank (z. B. über SQL-Interpreter wie SQL*Plus) dürfen nur für administrative Benutzer zugelassen werden, um Manipulationen an den Daten bzw. Datenbankobjekten (z. B. Tabellen und Indizes) zu verhindern (siehe M 2.134 *Richtlinien für Datenbank-Anfragen*). Datenbankobjekte dürfen ausschließlich über spezielle Benutzerkennungen kontrolliert modifiziert werden.

Dementsprechend muss das DBMS über ein geeignetes Zugriffs- und Zugangskonzept verfügen (siehe M 2.129 *Zugriffskontrolle einer Datenbank* und M 2.128 *Zugangskontrolle einer Datenbank*). Benutzer-Kennungen, die nur über eine Anwendung Datenmodifikationen durchführen können, dürfen keinen direkten Zugang zur Datenbank erhalten, während Kennungen zur Verwaltung der Datenbankobjekte der kontrollierte direkte Zugriff erlaubt sein muss.

Die physische Speicherung bzw. Spiegelung der Datenbankdateien (z. B. der DBMS-Software, der Datenbank an sich oder der Protokolldateien) sowie de-

ren Verteilung ist festzulegen, um z. B. die Verfügbarkeit und Ausfallsicherheit zu erhöhen. Aus Verfügbarkeitsgründen sollten gespiegelte Kontrolldateien auf verschiedenen Festplatten abgelegt sein. Der Ausfall einer Platte bedeutet dann nicht gleichzeitig den Verlust aller Kontrolldateien. Falls die Datenbankobjekte einer Anwendung in eigenen Datendateien abgelegt werden, so sollte man bei der Verteilung der Datendateien darauf achten, dass bei einem Ausfall einer Festplatte nicht alle Anwendungen betroffen sind.

**Beispiel:**

Eine Datenbank verwaltet die Daten zweier Anwendungen, mit jeweils einer Datendatei für die Tabellen und Indizes. Die Datendateien können beliebig auf vier Festplatten verteilt werden.

Eine ungünstige Verteilung der Datendateien sieht folgendermaßen aus:

| **Festplatte** | **Art der Ablage der Datendateien** |
|---|---|
| Festplatte 1 | Ablage der Datendateien für die Indizes beider Anwendungen |
| Festplatte 2 | Ablage der Datendateien für die Tabellen der ersten Anwendung |
| Festplatte 3 | Ablage der Datendateien für die Tabellen der zweiten Anwendung |
| Festplatte 4 | - |

Bei Ausfall der ersten Festplatte wären somit beide Anwendungen betroffen und könnten nicht mehr genutzt werden.

Eine günstigere Verteilung der Datendateien erhält man dagegen so:

| **Festplatte** | **Art der Ablage der Datendateien** |
|---|---|
| Festplatte 1 | Ablage der Datendateien für die Indizes der ersten Anwendung |
| Festplatte 2 | Ablage der Datendateien für die Tabellen der ersten Anwendung |
| Festplatte 3 | Ablage der Datendateien für die Indizes der zweiten Anwendung |
| Festplatte 4 | Ablage der Datendateien für die Tabellen der zweiten Anwendung |

Bei Ausfall einer beliebigen Festplatte wäre immer nur eine Anwendung betroffen.

Sind Festplatte 1 und 2 auf Festplatte 3 und 4 zusätzlich gespiegelt und umgekehrt Festplatte 3 und 4 auf Festplatte 1 und 2, könnten bis zu zwei beliebige Platten ausfallen, ohne dass die Datenbank für eine der beiden Anwendungen vollständig ausfiele.

Weiterhin müssen folgende wichtige Aspekte in einem Datenbanksicherheitskonzept geregelt werden:

- Es muss eine regelmäßige Prüfung des tatsächlich anfallenden Datenvolumens bzw. des Zuwachses des Datenvolumens im späteren laufenden Betrieb durchgeführt werden, um den benötigten Speicherplatz auch für zukünftige Bedürfnisse geeignet dimensionieren zu können.

- Geeignete Mechanismen zur Datensicherung müssen angewendet werden (siehe M 6.49 *Datensicherung einer Datenbank*).
- Der Einsatz von Überwachungs- und Kontrollmechanismen ist festzulegen, d. h. ob und in welchem Umfang Datenbankaktivitäten protokolliert werden sollen. Hier stellt sich unter anderem die Frage, ob beispielsweise nur der Zeitpunkt einer Datenmodifikation festgehalten wird, oder ob auch die Modifikation selbst protokolliert werden soll (siehe M 2.133 *Kontrolle der Protokolldateien eines Datenbanksystems*).

Für die Konzeption und den Betrieb eines Datenbanksystems muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Datenbanksystems darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Ein Datenbank-Administrator muss fundierte Kenntnisse über die eingesetzte DBMS-Software besitzen und auch entsprechend geschult werden.

Prüffragen:

- Gibt es ein Datenbanksicherheitskonzept, in dem Sicherheitsaspekte bei Planung, Installation, Konfiguration, Betrieb, Migration und Deinstallation beschrieben sind?

# M 2.127 Inferenzprävention

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zum Schutz personenbezogener und anderer vertraulicher Daten eines Datenbanksystems ist grundsätzlich jedem Benutzer nur der Zugriff auf diejenigen Daten zu gestatten, die für seine Tätigkeiten notwendig sind. Alle anderen Informationen, die sich zusätzlich in der Datenbank befinden, sind vor ihm zu verbergen.

Zu diesem Zweck müssen die Zugriffsberechtigungen auf Tabellen bis hin zu deren Feldern definiert werden können. Dies kann mittels Verwendung von Views und Grants durchgeführt werden (siehe M 2.129 *Zugriffskontrolle einer Datenbank*). Damit ist es einem Benutzer nur möglich, die für ihn bestimmten Daten einzusehen und zu verarbeiten. Stellt er Datenbankabfragen, die auf andere Informationen zugreifen wollen, werden diese vom DBMS zurückgewiesen.

Im Zusammenhang mit statistischen Datenbanken, die Daten über Personengruppen, Bevölkerungsschichten oder ähnliches enthalten, treten dagegen andere Schutzanforderungen auf. In einer statistischen Datenbank unterliegen die einzelnen, personenbezogenen Einträge dem Datenschutz, statistische Informationen sind jedoch allen Benutzern zugänglich.

Hier gilt es zu verhindern, dass aus Kenntnissen über die Daten einer Gruppe auf die Daten eines individuellen Mitglieds dieser Gruppe geschlossen werden kann. Es muss außerdem verhindert werden, dass durch das Wissen der in der Datenbank gespeicherten Informationen bzw. der Ablagestrukturen der Daten in der Datenbank die Anonymität dieser Daten durch entsprechend formulierte Datenbankabfragen umgangen werden kann (z. B. wenn die Ergebnismenge einer Datenbankabfrage nur einen Datensatz beinhaltet). Diese Problematik wird Inferenzproblem, der Schutz vor solchen Techniken Inferenzprävention genannt.

Auch wenn die Daten einer statistischen Datenbank anonymisiert sind, kann durch Inferenztechniken der Personenbezug zu bestimmten Datensätzen wiederhergestellt werden. Eine Zurückweisung bestimmter Anfragen (z. B. Anfragen mit nur einem oder wenigen Ergebnistupeln) reicht im allgemeinen nicht aus, da auch die Verweigerung einer Antwort durch das DBMS Informationen beinhalten kann.

Durch das Erstellen verschiedener Statistiken kann die Anonymität der Daten ebenfalls verloren gehen. Ein solcher indirekter Angriff zielt darauf ab, aus mehreren Statistiken Rückschlüsse auf die persönlichen Daten eines einzelnen Individuums ziehen zu können. Eine Schutzmaßnahme ist in diesem Fall, die Freigabe von so genannten sensitiven Statistiken nicht zu erlauben, was als unterdrückte Inferenzprävention bezeichnet wird. Eine weitere Möglichkeit ist die Verzerrung solcher Statistiken durch kontrolliertes Runden (gleiche Statistiken sind gleich zu runden) oder die Beschränkung auf statistisch relevante Teilmengen mit der Auflage, dass gleiche Anfragen immer Bezug auf die gleichen Teilmengen nehmen. Dieses Verfahren wird als verzerrende Inferenzprävention bezeichnet.

Werden weitergehende Anforderungen an die Vertraulichkeit der Daten gestellt, ist deren Verschlüsselung erforderlich (vergleiche M 4.72 *Datenbank-Verschlüsselung*).

Prüffragen:

- Wurden die Vertraulichkeits- und Datenschutzanforderungen an die Daten des Datenbanksystems erfasst und dokumentiert?
- Sind die Zugriffsberechtigungen der Benutzer (z. B.über Views und Grants) derart eingeschränkt, dass jeder Benutzer nur Zugriff auf die Daten hat, die er für seine Tätigkeiten benötigt?
- Finden Techniken der Interferenzprävention im Falle von statistischen Datenbanken Anwendung?

# M 2.128 Zugangskontrolle einer Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Datenbank-Software muss über geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen, um eine wirkungsvolle Zugangskontrolle zu gewährleisten. Die Vergabe von Zugangsberechtigungen hat nach festgelegten Regeln zu erfolgen (siehe M 2.132 *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen*).

Generell sollte für normale Benutzer der Zugang zu einer Produktionsdatenbank über einen interaktiven SQL-Interpreter unterbunden werden. Auf solche Datenbanken sollte ausschließlich ein indirekter Zugang über die entsprechenden Anwendungen möglich sein. Die einzige Ausnahme bilden hier Datenbankkennungen zu Administrationszwecken.

Remote-Zugänge zu Datenbanken sollten äußerst restriktiv gehandhabt werden. Ist diese Art des Zugangs nicht zwingend erforderlich, so sind diese zu unterbinden. Ansonsten sollte nur denjenigen Benutzern ein Remote-Zugang ermöglicht werden, die diesen auch tatsächlich benötigen. Andere Benutzer dürfen nicht in der Lage sein, sich selbst einen Remote-Zugang zu verschaffen. Keinesfalls darf ein Remote-Zugang ohne Angabe einer gültigen Benutzer-Kennung und Eingabe eines Passwortes möglich sein.

Bei erhöhten Sicherheitsanforderungen sollte geprüft werden, ob eine starke Authentisierung, die über Benutzername und Passwort hinausgeht, erforderlich ist. Hier kommt beispielsweise der Einsatz von Chipkarten oder sogenannten Tokens in Frage.

Prüffragen:

- Sofern Remote-Zugänge zur Datenbank erforderlich sind, werden diese besonders restriktiv gehandhabt oder sind sie andernfalls deaktiviert?
- Entsprechen die verwendeten Mechanismen zur Identifikation und Authentisierung der Benutzer den Sicherheitsanforderungen an die Datenbank?
- Ist außer zu Administrationszwecken ausschließlich ein indirekter Zugang über die entsprechenden Anwendungen auf die Datenbank möglich?

# M 2.129 Zugriffskontrolle einer Datenbank

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um einen wirkungsvollen Schutz der Vertraulichkeit und Integrität der Daten einer Datenbank zu erreichen, müssen eine Reihe von Maßnahmen umgesetzt werden. Neben einer Zugangskontrolle der Datenbank, die in M 2.128 *Zugangskontrolle einer Datenbank* beschrieben wird, sind dies im wesentlichen die folgenden Möglichkeiten der Zugriffskontrolle:

**Schutz der Datenbankobjekte**

Es sollte eine logische Zuordnung der Datenbankobjekte, also der Tabellen, Indizes, Datenbankprozeduren, etc., zu den Anwendungen erfolgen, die diese Objekte benutzen. Die daraus entstehenden Gruppen von Datenbankobjekten je Anwendung werden eigens hierfür einzurichtenden Kennungen zugeordnet. Damit können die Zugriffsberechtigungen der Datenbankobjekte so eingestellt werden, dass nur über diese speziellen Kennungen eine Modifikation der Objekte stattfinden kann. Greifen mehrere Anwendungen auf dieselben Datenbankobjekte zu, sollten diese als eigene Gruppe isoliert werden.

Werden beispielsweise die Daten zweier Anwendungen A und B in der Datenbank verwaltet, so sind zwei Datenbankkennungen AnwA und AnwB anzulegen. Alle Datenbankobjekte, die eindeutig der Anwendung A zugeordnet werden können, werden mit der Datenbankkennung AnwA angelegt und verwaltet. Analog wird mit den Datenbankobjekten von Anwendung B verfahren.

Ein Beispiel für ein zentrales Datenbankobjekt, das von beiden Anwendungen benutzt wird, sei eine Tabelle, die alle ansteuerbaren Drucker beinhaltet. Datenbankobjekte dieser Kategorie sollten nicht einer Kennung der Anwendungen (AnwA oder AnwB) zugeordnet werden, statt dessen sollten solche Datenbankobjekte unter einer eigenen Kennung (z. B. Druck) zusammengefasst und mit dieser zentralen Kennung verwaltet werden.

Diese speziellen Kennungen sind nicht personenbezogen. Statt dessen erhalten eigens hierfür autorisierte Personen (z. B. der Datenbankadministrator oder der Administrator der zugehörigen Anwendung) das Passwort der benötigten Kennung, falls Modifikationen an den Datenbankobjekten vorgenommen werden müssen (siehe zu diesem Themenbereich auch M 4.68 *Sicherstellung einer konsistenten Datenbankverwaltung*).

**Schutz der Daten**

Durch eine Definition von *Views* und *Prozeduren* können spezielle Benutzer-Sichten auf die Daten erzeugt werden, so dass die Daten der Datenbank nach bestimmten Kriterien sichtbar gemacht bzw. unsichtbar gehalten werden. Über einen *View* oder eine *Prozedur* wird explizit festgelegt, welche Felder aus einer oder mehreren Tabellen einem Benutzer in welcher Reihenfolge angezeigt werden. Durch spezielle Bedingungen können hierbei die Daten gefiltert und durch spezifische Beschränkungen in ihrem Umfang begrenzt werden. Durch die restriktive Vergabe von Zugriffsrechten (den im folgenden beschriebenen *Grants*) auf solche *Views* und *Prozeduren* können vertrauliche Daten vor unberechtigtem Zugriff geschützt werden.

Durch Trennung von Daten und Funktionalitäten, hier die Trennung der *Views* und *Prozeduren* von den echten Daten durch Speicherung in einer eigenständigen Datenbank kann die Sicherheit zusätzlich erhöht werden. Der Benutzer oder die Anwendung greift ausschließlich auf die *Views* und *Prozeduren* in der ausgelagerten Datenbank zu. Erst diese *Views* und *Prozeduren* greifen auf die in der Datenbank abgelegten Daten zu. In der ausgelagerten Datenbank werden die Zugriffsrechte der Benutzer und Anwendungen zusammengefasst.

Hierbei können Zugriffsrechte (*Grants*) auf Tabellen, *Views*, etc. oder sogar auf einzelne Felder einer Tabelle vergeben werden. Diese Rechte sind immer an bestimmte Benutzer, Rollen oder Benutzergruppen gebunden. Vorzuziehen ist hierbei die klare Trennung zwischen Zugangsrechten von Benutzern (meist über Kennung und Passwort) einerseits und Zugriffsrechten von Benutzergruppen und Rollen auf DB-Objekte andererseits. Die Koppelung von Benutzern zu DB-Objekten geschieht dann über die Zuordnung einzelner Benutzer zu den mit den notwendigen Zugriffsrechten ausgestatteten Benutzergruppen oder Rollen. Es können Zugriffsberechtigungen lesender (*read*), ändernder (*update*), löschender (*delete*), neu einfügender (*insert*) oder neu erstellender (*create*) Art unterschieden werden, bei *Prozeduren* kommt die Ausführungsberechtigung (*execute*) hinzu. Die Schritte zur Vergabe von Zugriffsberechtigungen sollten im Datenbankkonzept präzise beschrieben sein. Grundsätzlich sollten nur die wirklich erforderlichen Zugriffsberechtigungen vergeben werden. Anderenfalls besteht die Gefahr, dass der Überblick über die aktuellen Zugriffsrechte verloren geht und zusätzliche Sicherheitslücken entstehen können. Insbesondere sollte die vom DBMS zur Verfügung gestellte Möglichkeit, Rechte an alle zu vergeben (GRANT ... TO PUBLIC), nicht genutzt werden.

Im allgemeinen ist es nur dem Besitzer eines Datenbankobjektes erlaubt, Zugriffsberechtigungen an andere Benutzer weiterzugeben. Einige Datenbanksysteme stellen jedoch die Möglichkeit zur Verfügung, dass der Besitzer eines Datenbankobjektes auch das Recht, Zugriffsrechte weiterzugeben, an andere Benutzer vergeben kann. Von dieser Möglichkeit sollte nur in begründeten Ausnahmefällen Gebrauch gemacht werden, da der Besitzer des Datenbankobjektes auf diese Weise die Kontrolle über den Zugriff auf die Daten bzw. die Datenbankobjekte verliert.

**Restriktiver Datenzugriff über Anwendungen**

Anwendungen sollten einen restriktiven Zugriff auf die Daten unterstützen, d. h. in Abhängigkeit der Benutzer-Kennung und der Gruppenzugehörigkeit sollten nur diejenigen Funktionalitäten und Daten zur Verfügung gestellt werden, die ein Benutzer für die Ausführung seiner Aufgaben benötigt. Eine Form der DB-seitigen Realisierung einer solchen Anwendung ist hier die Verwendung von sogenannten *Stored Procedures*.

Stored Procedures sind Abfolgen von SQL-Anweisungen, die in der Datenbank voroptimiert gespeichert werden. Beim Aufruf einer Stored Procedure müssen nur ihr Name und eventuelle Parameter angegeben werden, um die dahinterstehenden Anweisungen auszuführen. Dies hat zum einen den Vorteil, dass nicht die gesamten Anweisungen zum Datenbank-Server übertragen werden müssen, was bei komplexeren Operationen die Netzbelastung vermindert.

Zum anderen kann das Datenbanksystem die Anweisungen in einer optimierten, vor-compilierten Form ablegen, so dass sie bei Aufruf schneller ausgeführt werden. Die restriktivste Form der Rechtevergabe ist die Vergabe von

Zugriffsrechten auf Stored Procedures statt auf Tabellen oder Views. Wenn Zugriffsrechte nur auf Stored Procedures vergeben werden, können die Benutzer nur die von den Datenbankverantwortlichen ausgewählten Operationen ausführen.

**Beispiele:**

- In Microsoft Access können verschiedene Berechtigungen vergeben werden, die sich entweder auf die Datenbank selbst (Öffnen/Ausführen, Exklusiv, Verwalten) oder auf die Tabellen und Abfragen beziehen (Daten lesen, Daten aktualisieren, Daten löschen, Daten einfügen). Diese Berechtigungen können dann unterschiedlichen Benutzern oder Benutzergruppen zugeordnet werden. Standardmäßig sind bei Microsoft Access die Gruppen "Administratoren" und "Benutzer" eingerichtet, wobei die Gruppe "Benutzer" die Berechtigungen "Daten lesen" und "Daten aktualisieren" für Tabellen und Abfragen sowie die Berechtigung "Öffnen/Ausführen" für Datenbanken enthält. Für eine detailliertere Kontrolle der Zugriffsrechte können eigene Gruppen definiert werden, an die unterschiedliche Berechtigungen vergeben werden können.
- In einer Oracle-Datenbank kann mit den Kommandos CREATE ROLE und GRANT die Gruppe "Abteilung_1" erstellt und die Berechtigung erteilt werden, z. B. eine Verbindung zur Datenbank herzustellen (connect), eine Session zu eröffnen (create Session) und Auswahlabfragen auf bestimmte Tabellen durchzuführen (select).
  Indem existierende Datenbank-Benutzer der Gruppe "Abteilung_1" zugeordnet werden, erhalten diese Benutzer alle Berechtigungen der zugeordneten Benutzergruppe. In diesem Beispiel könnte ein ausschließlich der Gruppe "Abteilung_1" zugeordneter Benutzer nur auf die der Gruppe zugeordneten Tabellen und hier ausschließlich lesend (select) aber nicht modifizierend (insert, delete, update, etc.) zugreifen.
- Eine Stored Procedure unter Oracle mit PL/SQL-Anweisungen hat einen Eingabeparameter, der die Artikelnummer angibt. Die Stored Procedure durchsucht alle zur Berechnung der Ausgabeparameter benötigten Tabellen und gibt unter anderem den Artikelpreis zurück.
  Benutzer erhalten über die Zugriffsrechtevergabe ein Nutzungsrecht nur auf die Stored Procedure, jedoch keinerlei Rechte auf die entsprechenden Tabellen. Damit werden z. B. auch zeitaufwendige Suchoperationen durch eine Auswahlberechtigung direkt auf die zugehörigen Tabellen verhindert.

Prüffragen:

- Sind die Datenbankobjekte eindeutig einer Datenbankkennung zugeordnet und werden darüber die Zugriffsberechtigungen auf die Datenbankobjekte gruppiert?
- Werden Zugriffsrechte (Grants) vorzugsweise über Benutzergruppen und Rollen vergeben, denen dann einzelne Benutzer zugeordnet sind?
- Sind die Schritte zur Vergabe von Zugriffsberechtigungen im Datenbankkonzept präzise beschrieben, so dass nur die für die Aufgabenerfüllung erforderlichen Zugriffsberechtigungen vergeben werden?
- Unterstützen Anwendungen einen restriktiven Zugriff auf die Datenbank (z. B. über Stored Procedures) in Abhängigkeit der Benutzer-Kennung und der Gruppenzugehörigkeit?

# M 2.130 Gewährleistung der Datenbankintegrität

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Verantwortliche der einzelnen Anwendungen

Die Integritätssicherung und -überwachung einer Datenbank soll die Korrektheit der zugehörigen Daten bzw. einen korrekten Zustand der Datenbank gewährleisten. Die folgenden Techniken sind zur Vermeidung inkorrekter Daten bzw. Zustände innerhalb einer Datenbank zu beachten:

- **Zugriffskontrolle**
  Damit ist der Schutz der betreffenden Datenbank vor unautorisiertem Zugriff mittels der Vergabe von Zugriffsrechten gemeint, wie in M 2.129 *Zugriffskontrolle einer Datenbank* beschrieben. Damit wird dem manipulativen Ändern von Daten bzw. Datenbankobjekten (wie z. B. Tabellen) vorgebeugt.
  Verantwortlich für die Umsetzung der Zugriffskontrolle ist der Datenbankadministrator.
  Auf eine detaillierte Ausführung wird an dieser Stelle verzichtet und statt dessen auf die Maßnahme M 2.129 *Zugriffskontrolle einer Datenbank* verwiesen
- **Synchronisationskontrolle**
  Die Synchronisationskontrolle dient der Verhinderung von Inkonsistenzen, die durch einen parallelen Zugriff auf denselben Datenbestand entstehen können. Es gibt dazu verschiedene Techniken, wie z. B. das Sperren von Datenbankobjekten (*Locking*) oder die Vergabe von Zeitstempeln (*Time-stamps*).
  Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen, insofern ein zusätzlicher Mechanismus zur Verfügung gestellt werden muss, der über die Möglichkeiten des Datenbankmanagementsystems (DBMS) hinausgeht.
  Auf eine detaillierte Ausführung wird verzichtet, da im allgemeinen jedes DBMS eine Synchronisationskontrolle durchführt. Vom Einsatz eines DBMS, welches dies nicht leisten kann, wird dringend abgeraten.
- **Integritätskontrolle**
  Hierunter fällt die Vermeidung semantischer Fehler bzw. semantisch unsinniger Zustände der Datenbank durch Einhaltung und Überwachung der geforderten Integritätsbedingungen. Diese können sich auf einzelne Relationen beziehen oder mehrere Relationen miteinander in Beziehung setzen (referentielle Integrität). Beispiele sind die Angabe eines Primärschlüssels für eine Relation, die Definition von Wertebereichen zu den einzelnen Attributen oder die Formulierung spezieller Bedingungen mittels einer *assertion*-Klausel.
  Dies kann durch das DBMS automatisch mittels eines Monitors überprüft werden, der z. B. durch die Verwendung von *Triggern* oder *Stored Procedures* realisiert werden kann. Damit sind prinzipiell beliebige Transaktionen möglich, jedoch werden diejenigen vom DBMS zurückgewiesen, die die Datenbank-Konsistenz verletzen würden.
  Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen respektive der fachliche Administrator, falls es sich um eine Umsetzung der Integritätsbedingungen in Form von Relationen, Primärschlüsseln oder allgemeinen Datenbankobjekten handelt.
  Im Rahmen der **Konzeption** einer IT-Anwendung sind zu erstellen

- ein Datenmodell, welches neben den Datenbankobjekten auch deren Beziehungen untereinander abbildet, und
- ein Fachkonzept, welches unter anderem Bedingungen beschreibt, unter denen Daten manipuliert werden dürfen.

Im Rahmen der **Realisierung** einer IT-Anwendung sind die folgenden Punkte zu beachten:

- Die konkrete Umsetzung des in der konzeptionellen Phase definierten Datenmodells muss festgelegt werden. Hierzu gehören die Definition und Anlage von Tabellen, Indizes, Wertebereichen usw.
- Die Definition von *Triggern* oder *Stored Procedures* erfolgt im Rahmen der Realisierung des Fachkonzepts. Trigger und Stored Procedures können dabei sowohl innerhalb der Anwendung (in den Programmen), als auch der Datenbank (für Tabellen) Verwendung finden. Trigger, die auf Datenbankebene eingesetzt werden, wirken unabhängig von darüberliegenden Anwendungen und sind aus diesem Grund zentral zu verwalten.
  Beispiel: *Trigger "Update"* für eine Tabelle:
  Immer wenn ein Datensatz der Tabelle geändert wird, dann sind die für den Trigger definierten Anweisungen auszuführen. Eine dieser Anweisungen kann der Aufruf einer *Stored Procedure* sein.

Im Rahmen von Anwendungen kann eine Integritätssicherung durch einen geeigneten Einsatz von Commit bzw. Rollback für das Betätigen bzw. Widerrufen von Transaktionen realisiert werden.

Prüffragen:

- Werden Techniken der Synchronisationskontrolle zur Vermeidung von Inkonsistenzen eingesetzt?
- Werden Techniken der Integritätskontrolle zur Vermeidung semantischer Fehler bzw.. semantisch unsinniger Zustände der Datenbank eingesetzt?
- Wird die Integritätssicherung auch innerhalb von Anwendungen, die die Datenbank verwenden, berücksichtigt?

# M 2.131 Aufteilung von Administrationstätigkeiten bei Datenbanksystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Um einen geordneten Betrieb von Datenbanksystemen zu ermöglichen, sind Administratoren zu bestimmen. Diesen obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich sind sie für die Sicherheitsbelange der betreuten Datenbanksysteme zuständig.

Neben den in M 2.26 *Ernennung eines Administrators und eines Vertreters* und M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* genannten Maßnahmen sind speziell für Datenbanksysteme folgende Dinge zu beachten.

Es sollten grundsätzlich zwei verschiedene Administrator-Rollen unterschieden werden:

- die fachlich übergreifende Administration der Datenbank-Software und
- die Administration der anwendungsspezifischen Belange.

Diese beiden Aufgaben sollten von verschiedenen Personen durchgeführt werden, um eine Trennung der anwendungsspezifischen und fachlich übergreifenden Administration einer Datenbank zu erreichen.

Der grundsätzliche Betrieb des DBMS, die Durchführung der Datensicherungen oder die Archivierung von Datenbeständen sind beispielsweise Bestandteil der fachlich übergreifenden Datenbankadministration.

Bei der anwendungsspezifischen Administration werden dagegen die Erfordernisse der einzelnen Anwendungen an die Datenbank bearbeitet. Dies kann z. B. die Verwaltung der zugehörigen Datenbankobjekte, die Unterstützung der Benutzer bei Problemen bzw. Fragen oder die Verwaltung der entsprechenden Datenbankkennungen beinhalten. Letzteres ist allerdings nur dann möglich, wenn die Verwaltung der Datenbankkennungen je Anwendung über ein entsprechendes Berechtigungskonzept durch die Datenbank-Software unterstützt wird, also von den fachlich übergreifenden Berechtigungen getrennt werden kann.

Der fachlich übergreifende Administrator richtet die für die anwendungsspezifischen Belange zuständigen Administratorkennungen mit den zugehörigen Berechtigungen ein. Dazu gehört insbesondere das Recht, Datenbanken anzulegen. Die Rechtevergabe für die einzelnen Benutzer sollte dagegen für jede anwendungsspezifische Datenbank getrennt durchgeführt werden und zwar vom jeweils zuständigen anwendungsspezifischen Administrator.

Prüffragen:

- Gibt es verschiedene Administrator-Rollen für die fachlich übergreifende Administration der Datenbank-Software und für die Administration der anwendungsspezifischen Belange?
- Sind die beiden Datenbank-Administrator-Rollen für die fachlich übergreifende Administration der Datenbank-Software und für die

Administration der anwendungsspezifischen Belange verschiedenen Personen im Sinne einer Rollentrennung zugeordnet?

# M 2.132 Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Einrichtung von Benutzern/Benutzergruppen aus einer Datenbank bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten (siehe M 2.129 *Zugriffskontrolle einer Datenbank*) und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs. Grundsätzlich erhält dazu jeder Datenbankbenutzer eine interne Datenbankkennung, über die ihn das Datenbanksystem identifiziert. Damit können nur autorisierte Personen auf die Datenbank zugreifen.

Modifizierende Operationen (Update, Insert, Delete, etc.), die nicht vom DBMS sondern von Benutzern mit Administrationsrechten ausgeführt werden, stellen ein hohes Risiko dar, das zur Zerstörung der Datenbank führen kann. Auf die Vergabe von modifizierenden Rechten auf die System-Tabellen sollte deshalb grundsätzlich verzichtet werden. Selbst ein lesender Zugriff sollte beschränkt werden, da über die System-Tabellen alle Informationen der Datenbank ermittelt werden können.

In Anlehnung an M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen* sollte ein Formblatt erstellt werden, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen, die für eine organisierte Benutzerverwaltung erforderlich sind:

- Name, Vorname,
- Vorschlag für die Benutzer-Kennung (wenn nicht durch Konventionen vorgegeben),
- Organisationseinheit,
- Erreichbarkeit (z. B. E-Mail, Telefon, Raum),
- Zustimmung von Vorgesetzten,
- Projekt (optional),
- Anwendungen, die benutzt werden sollen und auf das Datenbanksystem zugreifen (optional),
- Angaben über die geplante Tätigkeit im Datenbanksystem und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit (optional) und
- Restriktionen auf Zeiten, Zugriffsberechtigungen (für bestimmte Tabellen, Views etc.), eingeschränkte Benutzerumgebung (optional).

Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem oder mehreren Profilen zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die datenbankspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu nutzen, die bereits bei der Auswahl der Datenbanksoftware zu berücksichtigen sind (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*). Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppenkennungen festzulegen (z. B. Benutzer-ID = Kürzel der Organisationseinheit plus laufende Nummer).

Dabei können Benutzer-, Rollen- und Gruppenprofile benutzt werden. Soweit möglich, sollten jedoch keine benutzerspezifischen Profile verwendet werden, da dies bei einer großen Anzahl von Benutzern zu einem hohen administrativen Aufwand führt. Bei der Definition von Gruppenprofilen muss man zwischen restriktiven und großzügigen Berechtigungsprofilen abwägen. Werden

die Gruppenprofile zu restriktiv gehandhabt, muss eine große Anzahl von Gruppen verwaltet werden, was zu einem hohen administrativen Aufwand führt. Werden die Gruppenprofile dagegen zu großzügig definiert, kann es zu Redundanzen zwischen verschiedenen Gruppen kommen oder zur Einräumung von unnötig umfangreichen Rechten, was wiederum zur Verletzung der Vertraulichkeit oder Integrität von Daten führen kann.

Jedem Benutzer muss eine eigene Datenbankkennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten.

Grundsätzlich muss zwischen der der Datenbankkennung und der Benutzerkennung des zugrunde liegenden Betriebssystems unterschieden werden. Einige Hersteller bieten in ihrer Datenbank-Software jedoch die Möglichkeit an, die Betriebssystemkennung in das Datenbanksystem zu übernehmen. Dies erspart den Anwendern eine Authentisierung für den Zugang zur Datenbank, falls diese sich bereits mit ihrer eigenen Betriebssystemkennung angemeldet haben.

So können beispielsweise unter Oracle so genannte OPS$-Kennungen verwendet werden. Eine solche Kennung setzt sich aus dem Präfix "OPS$" und der Betriebssystemkennung des Benutzers zusammen. Nur wenn sich ein Benutzer mit seiner Betriebssystemkennung am Datenbanksystem anmeldet, wird kein Passwort vom DBMS abgefragt. Meldet sich der Benutzer dagegen unter einer anderen Kennung an, so erfolgt eine Passwortabfrage.

Diese Möglichkeit beinhaltet allerdings die Gefahr, dass bei einer unerlaubten Authentisierung auf Betriebssystemebene (z. B. bei Überwindung des entsprechenden Passwortschutzes) der Zugriff auf die Datenbank nicht mehr verhindert werden kann. Vor der Verwendung von OPS$-Kennungen sollte deshalb geprüft werden, ob die Sicherheitsmechanismen des Betriebssystems auf den Clients für den vorliegenden Anwendungsfall ausreichend sind.

Bei der Forderung nach einer einfachen Handhabung für die Benutzer (Stichwort *Single-Sign-On* - SSO) sollte alternativ der Einsatz eines Zusatzproduktes zur zentralen Benutzerverwaltung für den gesamten IT-Betrieb erwogen werden. Aber auch hier müssen die konkreten Sicherheitsanforderungen mit dem entsprechenden Zusatzprodukt abgeglichen werden.

Prüffragen:

- Gibt es Regelungen für die Einrichtung von Datenbankbenutzern bzw. -benutzergruppen?
- Wird auf die Vergabe von modifizierenden Rechten auf die System-Tabellen verzichtet?
- Werden die Zugriffsrechte auf die Datenbank über Benutzergruppen, Profile oder Rollen vergeben?
- Erhält jeder Benutzer nur die zur Erfüllung seiner Aufgabe notwendigen Rechte?
- Erhält jeder Datenbank-Benutzer eine eigene interne Datenbankkennung, die von der Benutzerkennung des zugrunde liegenden Betriebssystems verschieden ist?

# M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die in einem Datenbanksystem mögliche Protokollierung bzw. Auditierung ist in einem sinnvollen Umfang zu aktivieren. Werden zuviele Ereignisse protokolliert, wird die Performance der Datenbank negativ beeinflusst und die Protokolldateien wachsen stark an. Es muss also immer zwischen dem Bedürfnis, möglichst viele Informationen zur Sicherheit der Datenbank zu sammeln, und der Möglichkeit, diese Informationen zu speichern und auszuwerten, abgewogen werden.

Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- Anmeldezeiten und -dauer der Benutzer,
- Anzahl der Verbindungen zur Datenbank,
- fehlgeschlagene bzw. abgewiesene Verbindungsversuche,
- Auftreten von Deadlocks innerhalb des Datenbanksystems,
- I/O-Statistik für jeden Benutzer,
- Zugriffe auf die Systemtabellen (siehe auch M 4.69 *Regelmäßiger Sicherheitscheck der Datenbank*),
- Erzeugung neuer Datenbankobjekte und
- Datenmodifikationen (eventuell mit Datum, Uhrzeit und Benutzer).

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme allerdings nur dann wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher sind die Protokolldateien in regelmäßigen Abständen durch einen Revisor auszuwerten. Ist es organisatorisch oder technisch nicht möglich, einen unabhängigen Revisor mit der Auswertung der Protokolldateien zu betrauen, ist eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich.

Weiterhin ist bei bei der Protokollierung sicherheitsrelevanter Ereignisse sowie bei der Prüfung (Monitoring) der Protokolldateien folgendes zu beachten:

Für die Überprüfung der Protokolldateien sind diese grundsätzlich in eine andere Umgebung zu kopieren. Geeignete Tools sollten dabei genutzt werden. Die Verantwortlichkeiten für die Protokollierung und die Verantwortlichkeiten für die zu protokollierenden Aktivitäten müssen getrennt werden. Bei der Protokollierung sicherheitsrelevanter Ereignisse sollten Änderungen nur im Vier-Augen-Prinzip möglich sein.

Die Protokollierung ist zu schützen vor:

- Deaktivierung,
- Änderungen der zu protokollierenden Ereignistypen,
- Änderung der Protokolldaten (Inhalt) und
- Datenverlust bei Protokoll-Medien, z. B. durch Überschreiben, falsches Beschreiben, falsche Lagerung.

Die Protokolldaten müssen auf dem Produktivsystem regelmäßig gelöscht werden, um ein übermäßiges Anwachsen der Protokolldateien zu verhindern. Sie dürfen allerdings nur dann gelöscht werden, wenn die Protokolldateien vorher ausgewertet und kontrolliert wurden. Unter Umständen müssen die Protokolldaten archiviert werden. Die Archivierung oder gegebenenfalls auch die

Löschung der Protokolldateien kann manuell oder automatisch geschehen, falls entsprechende Werkzeuge zur Verfügung stehen.

Bei Auffälligkeiten ist das Sicherheitsmanagement zu unterrichten.

Weiterhin ist der Zugriff auf die Protokolldateien strikt zu beschränken. Einerseits muss verhindert werden, dass Angreifer ihre Aktionen durch nachträgliche Änderung der Protokolldateien verbergen können, andererseits könnten über die gezielte Auswertung von Protokolldateien Leistungsprofile der Benutzer erstellt werden. Deshalb dürfen beispielsweise Änderungen überhaupt nicht vorgenommen werden können und lesender Zugriff darf nur den Revisoren gestattet werden.

Bei der Konzeption der Vorgehensweise für die Protokollierung und Auswertung der Protokolldaten müssen frühzeitig der Datenschutzbeauftragte und die Personalvertretung beteiligt werden.

Um die Auswertung der Protokolldaten zu vereinfachen, können vom Datenbank-Administrator zusätzliche Tools eingesetzt werden, die eine automatisierte Überwachung durchführen. Solche Produkte können beispielweise die Protokolldateien von Datenbanksystemen nach vorgegebenen Mustern auswerten und bei Bedarf einen Alarm erzeugen.

Weitere Maßnahmen, die in diesem Zusammenhang beachtet werden müssen, sind in M 2.64 *Kontrolle der Protokolldateien* zu finden.

Prüffragen:

- Wurden bei den Datenbanksystemen die Protokollierungs- bzw. Auditierungsmöglichkeiten in einem sinnvollen Umfang aktiviert?

# M 2.134 Richtlinien für Datenbank-Anfragen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler

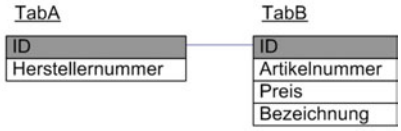
Die relationale Datenbanksprache SQL (Structured Query Language) ist eine international standardisierte Sprache für relationale Datenbanksysteme (DBS), die eine weite Verbreitung erfahren hat und in den meisten Datenbankmanagementsystemen (DBMS) implementiert ist. Der Sprachumfang wird in zyklisch überarbeiteten Normen (ANSI SQL-92, ANSI SQL-99, ANSI SQL-2003) festgelegt. Mittels SQL können sowohl Modifikationen der Daten (UPDATE, INSERT, DELETE), als auch der Datenbankobjekte (CREATE, ALTER, DROP) formuliert, sowie Informationen abgefragt werden (SELECT).

Es müssen Richtlinien für eine effiziente, wartbare und nachvollziehbare Programmierung von Datenbankabfragen erstellt und im Rahmen der Programmierung umgesetzt werden. Folgende Grundsätze sollten in dieser Richtlinie beschrieben sein:

- Anfragen an die Datenbank sollten möglichst nicht direkt auf Tabellen, sondern über *Views* und *Prozeduren* ausgeführt werden. Einerseits kann dadurch der Schutz der Daten besser gewährleistet werden (siehe M 2.129 *Zugriffskontrolle einer Datenbank*). Andererseits kann sichergestellt werden, dass den Benutzern die notwendigen Informationen in entsprechender Formatierung und Menge zur Verfügung gestellt werden. Zusätzlich können diese *Views* und *Prozeduren* in eine eigene DB ausgelagert werden und Benutzer sowie Anwendungen können nur auf diese ausgelagerte DB Zugriff erhalten. Die Daten in den Tabellen sind dann außer über die *Prozeduren* und *Views* der ausgelagerten DB nur einem speziellen Benutzerkreis zugänglich (Administratoren, etc.).
- SQL-Anfragen sollten exakt und explizit in Anlehnung an das DB-Modell formuliert werden. Dabei sollten alle erfragten Felder explizit angegeben und der "*"-Operator vermieden werden. Damit ist sichergestellt, dass die Daten in der erwarteten Reihenfolge zur Verfügung gestellt und nur diejenigen Daten selektiert werden, die tatsächlich benötigt werden.
  **Beispiel:**
  Ein DB-Modell enthält eine Tabelle mit den Feldern "Artikelnummer", "Artikelbezeichnung", "Verwendungszweck" und "Nettopreis". Im Zuge einer Erweiterung der Applikation wird hinter dem "Verwendungszweck" ein weiteres Feld mit dem Namen "Bestellnummer" eingefügt. Aus Gründen der optimalen Speicherausnutzung fügt das DBMS das neue Feld jedoch nicht dort, sondern an die zweite Stelle hinter "Artikelnummer" ein. Weil die Daten mit Hilfe einer SELECT-*-Anweisung abgefragt werden, liefert die Datenbank die Informationen in einer anderen Reihenfolge zurück, als die Applikation sie erwartet. Dies führt bei der Applikation zu Problemen, deren Ursache zunächst nicht erkennbar ist.
- Bei einschränkenden Datenbankanfragen (WHERE-Klausel) ist die Reihenfolge der angegebenen Selektionsbedingungen von großer Bedeutung für die Ausführungsgeschwindigkeit. Die WHERE-Klausel sollte so formuliert werden, dass zuerst die Bedingung angegeben wird, die in kürzester Zeit die kleinstmögliche Ergebnismenge selektiert. Dabei sollte zuerst auf indizierte Felder zugegriffen werden, dann erst auf nicht-indizierte Felder, wobei hier Prüfungen auf Ziffern schneller sind als Prüfungen auf Texte. Das gleiche gilt analog für Datenbankanfragen, die über mehrere Tabellen hinweg formuliert werden (so genannte Joins).

Viele DBMS optimieren bereits Datenbankanfragen selbständig. Oft werden zusätzlich sogar mehrere Optimierungsstrategien zur Auswahl angeboten, die über verschiedene Parameter ausgewählt werden können.
Einige DBMS bieten die Möglichkeit, die Abarbeitung von Datenbankanfragen zu untersuchen (z. B. in Oracle mit EXPLAIN oder für Ingres mittels SETOEP). Des weiteren besteht die Möglichkeit, über so genannte HINTS in der Datenbankanfrage deren Abarbeitung explizit zu definieren und somit den Optimizer im Prinzip auszuschalten. Von dieser Möglichkeit sollte allerdings vorsichtig Gebrauch gemacht werden.

- Welche Optimizer das DBMS unterstützt sowie deren Vor- und Nachteile sind in den Handbüchern des DBMS normalerweise dokumentiert. Der Einsatz alternativer Optimizer innerhalb eines DBMS sollte mit dem Administrator abgesprochen werden.
- Im Falle von Joins sollte zusätzlich beachtet werden, dass die Zuordnung von Feldern zu den Tabellen eindeutig erfolgt.
- **Beispiel:**




```
select
  TabA.ID,
  TabB.Bezeichnung,
  TabB.Preis
from
  TabA join TabB on
    TabA.ID = TabB.ID
```

Abbildung: Feldzuordnung bei Joins

Das Feld "ID" ist in beiden Tabellen vorhanden und **muss** deshalb bei der Datenbankanfrage explizit mit dem zugehörigen Tabellennamen angegeben werden. Andernfalls ist die Eindeutigkeit der Auswahl nicht mehr sichergestellt und die Datenbankanfrage wird mit einer entsprechenden Fehlermeldung abgebrochen.
Alle anderen Felder sind in diesem Fall eindeutig den jeweiligen Tabellen zuzuordnen. Eine explizite Angabe des zugehörigen Tabellennamens für jedes Feld wird von SQL nicht gefordert. Trotzdem sollte für die einzelnen Felder die eindeutige Zuordnung zur Tabelle erfolgen, wie im obigen Beispiel für die Felder "Preis" und "Bezeichnung" der Tabelle TabB. Das Hinzufügen eines Feldes "Bezeichnung" für TabA würde im obigen Beispiel zu keinen Problemen führen. Dies wäre jedoch nicht der Fall, wenn die SQL-Anweisung die Zuordnung der Felder zu den Tabellen nicht explizit beinhalten würde. Es wäre nicht mehr eindeutig, ob das Feld "Bezeichnung" von TabA oder TabB selektiert werden soll, da beide Tabellen nach der Änderung von TabA ein Feld mit diesem Namen haben. Die SQL-Anweisung würde mit einer Fehlermeldung abgebrochen.

- Alle Datenbanktransaktionen sollten explizit mit einem COMMIT bestätigt werden. Falls das DBMS ein automatisches COMMIT unterstützt, sollte dieses nicht aktiviert werden, da es sonst unter Umständen zu ungewollten Inkonsistenzen in der Datenbank kommen kann.
  **Beispiel:**
  Mehrere einzelne Modifikationen gehören logisch zusammen, werden aber nach der Ausführung jeder einzelnen Modifikation automatisch durch ein COMMIT bestätigt. Kommt es nun zu einem unkontrollierten Abbruch der Transaktion und infolgedessen zu einem Rollback, sind die zuerst ausgeführten Operationen bereits bestätigt und verbleiben in der Datenbank, während der Rest noch gar nicht durchgeführt werden konnte.

- Zur Vermeidung von Sperrkonflikten oder gar Deadlocks ist für jede fachliche Datenbank eine Sperrstrategie festzulegen (z. B. hierarchisches Sperren oder explizites Sperren aller Tabellen am Anfang der Transaktion).
- Anwendungsentwickler sollten nach jeder SQL-Anweisung den Fehlerstatus prüfen, so dass die Anwendung so früh wie möglich auf eingetretene Fehler reagieren kann.
- Berechtigungen auf systemspezifische Kommandos, mit denen beispielsweise die Protokollierung ausgeschaltet oder das Locking-Verfahren verändert werden kann, sollten Benutzern entzogen und auf Administratoren beschränkt werden.
- Bei der Entwicklung von Anwendungen sollten alle Datenbankzugriffe in einem Modul oder einem bestimmten Teil des Programmcodes zusammengefasst werden, da sonst zur Überprüfung der obigen Grundsätze der gesamte Programmcode des Anwendungssystems herangezogen werden müsste. Hierdurch wird die Wartung und Pflege des Anwendungssystems, z. B. bei Änderungen des Datenmodells, erleichtert.

Prüffragen:

- Gibt es Richtlinien für die Programmierung von Datenbankabfragen?
- Sind Anfragen an die Datenbank gemäß Richtlinien über Views und Prozeduren statt direkt auf Tabellen auszuführen?
- Fordern die Richtlinien für Datenbank-Anfragen, sofern Views und Prozeduren in eine eigene Datenbank ausgelagert werden, einen eingeschränkten Benutzerkreis für den Zugriff auf die Daten in deren Tabellen?
- Umfassen die Richtlinien für Datenbank-Anfragen, dass SQL-Anfragen exakt und explizit in Anlehnung an das Datenbank-Modell unter Vermeidung des "*"-Operators zu formulieren sind?
- Enthalten die Richtlinien für Datenbank-Anfragen, sofern deren Ausführungsgeschwindigkeit von Bedeutung ist, Anforderungen zur geeigneten Optimierung von Datenbankanfragen?
- Fordern die Richtlinien für Datenbank-Anfragen im Falle von Joins bei der Datenbankanfrage immer eine eindeutige explizite Zuordnung von Feldern zu Tabellen?
- Umfassen die Richtlinien für Datenbank-Anfragen, dass alle Datenbanktransaktionen explizit mit einem COMMIT zu bestätigen sind?
- Ist in den Richtlinien für Datenbank-Anfragen eine Sperrstrategie zur Vermeidung von Sperrkonflikten festgelegt?
- Existiert die Richtlinie, Berechtigungen für systemspezifische Kommandos auf der Datenbank nur an Administratoren zu vergeben?

# M 2.135 Gesicherte Datenübernahme in eine Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In vielen Datenbanksystemen besteht aus Anwendungssicht die Notwendigkeit, Daten aus anderen Systemen zu übernehmen. Dabei lassen sich prinzipiell die beiden folgenden Kategorien unterscheiden:

**Erst- oder Altdatenübernahme**

Bei der Übernahme von Daten aus Altsystemen, wenn beispielsweise ein neues Datenbanksystem beschafft wurde und produktiv eingesetzt werden soll, ist insbesondere sicherzustellen, dass

- die Daten in einem Format vorliegen, das in die Zieldatenbank übernommen werden kann,
- die Daten vollständig sind, d. h. für alle Felder, die in der Zieldatenbank gefüllt werden sollen, müssen Daten zur Übernahme zur Verfügung gestellt werden, und
- die Konsistenz und Datenintegrität der Datenbank gewährleistet ist.

Im Vorfeld der Datenübernahme ist ein Konzept zu erstellen, wie die zu übernehmenden Daten aufbereitet werden müssen und wie die Übernahme konkret durchgeführt werden soll. Weiterhin ist eine Komplettsicherung der Altdaten vorzunehmen. Erfolgt die Datenübernahme in mehreren Schritten, sollte vor jedem einzelnen Schritt eine unabhängige Datensicherung durchgeführt werden.

**Regelmäßige Datenübernahme**

Befinden sich in der Zieldatenbank bei einer Datenübernahme bereits Daten, die nicht verändert werden dürfen, oder werden in regelmäßigen Zeitabständen Daten in eine Datenbank übernommen, so

- ist vor der Datenübernahme eine Komplettsicherung der Datenbank durchzuführen,
- sollte die Datenübernahme wenn möglich außerhalb der regulären Betriebszeiten stattfinden,
- sind Vorkehrungen zu treffen, um eine mehrfache Übernahme der gleichen Daten zu verhindern,
- ist vor der ersten Datenübernahme ein Konzept zu erstellen, wie die zu übernehmenden Daten aufbereitet werden müssen bzw. wie die Übernahme konkret durchzuführen ist. Insbesondere muss in diesem Konzept berücksichtigt werden, wie Konflikte zwischen den bereits existierenden Daten in der Zieldatenbank und den zu übernehmenden Daten vermieden werden, d. h. inwieweit die Integrität und Konsistenz der Zieldatenbank gewahrt bleibt.

Von einer Datenbankaktualisierung betroffene Benutzer müssen über die bevorstehende Datenübernahme rechtzeitig informiert werden, insbesondere dann, wenn mit Einschränkungen hinsichtlich der Verfügbarkeit oder des Antwortzeitverhaltens zu rechnen ist.

Vor der Durchführung einer Datenübernahme ist festzulegen, was beim Auftreten von Fehlern zu unternehmen ist. Dies beinhaltet z. B., ob beim Auftreten eines fehlerhaften Datensatzes mit dem nächsten Satz fortgefahren werden kann, oder ob die komplette Datenübernahme abgebrochen werden muss.

Weiterhin ist festzulegen, wie die Datenübernahme nach einem Abbruch wieder aufgesetzt wird.

Prüffragen:

- Gibt es ein Konzept zur Datenübernahme aus anderen Systemen in eine bestehende Datenbank?
- Erfolgt vor einer Datenübernahme eine Komplettsicherung der Datenbank?
- Werden die betroffenen Benutzer vor einer Datenübernahme rechtzeitig und umfassend informiert?
- Ist festgelegt, wie beim Auftreten von Fehlern während einer Datenübernahme zu verfahren ist?

# M 2.136 Einhaltung von Regelungen zu Arbeitsplatz und Arbeitsumgebung

Die Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen, die Inhalte wurden in M 1.44 *Geeignete Einrichtung eines häuslichen Arbeitsplatzes* integriert.

# M 2.137 Beschaffung eines geeigneten Datensicherungssystems

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Großteil der Fehler, die beim Erstellen oder Restaurieren einer Datensicherung auftreten, sind Fehlbedienungen. Daher sollte bei der Beschaffung eines Datensicherungssystem nicht allein auf seine Leistungsfähigkeit geachtet werden, sondern auch auf seine Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.

Bei der Auswahl von Sicherungssoftware sollte darauf geachtet werden, dass sie die folgenden Anforderungen erfüllt:

- Die Datensicherungssoftware sollte ein falsches Medium ebenso wie ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort, oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die zu sichernden Daten sollten auch auf Festplatten und Netzlaufwerken abgespeichert werden können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall,

dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch Passwort geschützt werden kann, sollte diese Option genutzt werden. Das Passwort ist dann gesichert zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*).

Bei den meisten Betriebssystemen werden Programme für Datensicherungen mitgeliefert. Nicht alle erfüllen allerdings die Ansprüche an Produkte für professionelle und komfortable Datensicherungen. Stehen aber keine solchen Produkte zur Verfügung, so sollten die systemzugehörigen Programme verwendet werden.

Prüffragen:

- Wurden Datensicherungssysteme beschafft, die die Anforderungen des Sicherheits- und des Backup-Konzepts erfüllen?

# M 2.138 Strukturierte Datenhaltung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Eine schlecht strukturierte Datenhaltung kann zu einer Vielzahl von Problemen führen. Alle IT-Benutzer sind daher darauf hinzuweisen, wie eine gut strukturierte und übersichtliche Datenhaltung aussehen sollte. Auf allen Servern sollten entsprechende Strukturen durch die Administratoren vorgegeben werden. Dies ist ohnehin Voraussetzung, um eine differenzierte Vergabe von Zugriffsrechten realisieren zu können.

Programm- und Arbeitsdateien sollten immer in getrennten Bereichen gespeichert werden. Dies sorgt für eine bessere Übersicht und erleichtert auch die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes. Bei den meisten Applikationsprogrammen ändern sich nach der Installation keine oder nur sehr wenige Konfigurationsdateien. Soweit möglich, sollten alle Dateien, die sich regelmäßig ändern, in gesonderten Verzeichnissen abgespeichert werden, damit nur diese in die regelmäßigen Datensicherungen mitaufgenommen werden müssen.

Bei einer sauberen Trennung von Programmen und Daten reicht es, die Daten in die regelmäßigen Datensicherungen aufzunehmen. Wichtig ist es, die Arbeitsdateien sorgfältig gesichert zu haben, diese können dann notfalls auch auf anderen Systemen weiterverarbeitet werden.

Bei vernetzten Systemen stellt sich außerdem die Frage, welche Programme bzw. Dateien auf den lokalen Festplatten oder auf einem Netzserver abgelegt werden sollten. Beides hat Vor- und Nachteile und muss sowohl von der organisatorischen Struktur als auch von der eingesetzten Hard- und Software abhängig gemacht werden. So sollten z. B. Dateien mit hohen Verfügbarkeitsansprüchen zusammen mit den zugehörigen Applikationsprogrammen besser auf den Arbeitsplatzrechnern gehalten werden als auf einem Netzserver. Dann muss allerdings auch die entsprechende Notfallvorsorge für diese Arbeitsplatzrechner betrieben werden.

Es sollten aufgaben- oder projektbezogene Verzeichnisse eingerichtet werden, um die Zuordnung von Dateien zu erleichtern. Es sollten möglichst wenig Daten in personenbezogenen Verzeichnissen abgelegt werden.

Um zu verhindern, dass für die weitere Arbeit grundlegenden Dateien wie Briefvorlagen, Formularen, Projektplänen oder Ähnlichem unterschiedliche Versionsstände existieren, sollten diese zentral verwaltet werden. Sie sollten beispielsweise auf einem Server so vorgehalten werden, dass jeder lesend darauf zugreifen kann, aber es sollte für jede solche Datei jeweils nur eine Person geben, die sie verändern darf.

Wie auf einem Server durch Verzeichnisvorgaben Daten strukturiert werden könnten, wird in dem folgenden Beispiel gezeigt:

```
\
\bin
\bin\program1
\bin\program2
\bin\program3
\user
\user\user1
```

\user\user2
\projekte
\projekte\p1
\projekte\p1\texte
\projekte\p1\bilder
\projekte\p2
\projekte\p2\projektplan
\projekte\p2\teilprojekt1
\projekte\p2\teilprojekt2
\projekte\p2\teilprojekt3
\projekte\p2\ergebnis
\vordrucke

Es sollte regelmäßig überprüft werden,

- ob Daten aus dem Produktionssystem entfernt werden können, weil sie archiviert oder gelöscht werden können,
- ob Zugriffsrechte entzogen werden können, weil Mitarbeiter die Projektgruppe verlassen haben,
- ob auf allen IT-Systemen die aktuellsten Versionen von Formularen, Vorlagen, etc. gespeichert sind.

Dies ist durch die Benutzer für deren IT-Systeme bzw. die von ihnen verwalteten Verzeichnisse und von den Administratoren der Server regelmäßig zu überprüfen. Diese Prüfungen sollten mindestens vierteljährlich durchgeführt werden, da sonst die Kenntnisse über Inhalt und Herkunft der Dateien wieder aus den Gedächtnissen der Mitarbeiter verschwunden sind.

Prüffragen:

- Werden auf allen Servern der Organisation Strukturen für eine strukturierte Datenhaltung geschaffen?
- Sind alle Benutzer darüber informiert, wie eine strukturierte Datenhaltung aussieht?
- Werden Programm- und Arbeitsdaten voneinander getrennt gespeichert?
- Ist geregelt, welche Daten lokal bzw. im Netz gespeichert werden sollen?
- Wird die Datenspeicherung in personenbezogenen Verzeichnissen vermieden?
- Werden Vorlagedateien zentral verwaltet?
- Wird mindestens vierteljährlich überprüft, ob die Vorgaben zur strukturierten Datenhaltung auf den Servern eingehalten werden?

# M 2.139 Ist-Aufnahme der aktuellen Netzsituation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um ein bestehendes Netz gezielt sicherheitstechnisch analysieren zu können, ist die Bestandsaufnahme der aktuellen Netzsituation erforderlich. Sie ist ebenso erforderlich, wenn ein bestehendes Netz erweitert wird. Bei der Planung von Netzen sind die im Folgenden beschriebenen Punkte bei der Konzeption zu berücksichtigen.

Hierzu ist eine Ist-Aufnahme mit einhergehender Dokumentation der folgenden Aspekte, die zum Teil aufeinander aufbauen, notwendig:

- physische Netztopologie,
- logische Netztopologie,
- verwendete Netzprotokolle,
- Kommunikationsübergänge im LAN und zum WAN sowie
- Netzperformance und Verkehrsfluss.

In den einzelnen Schritten ist im Wesentlichen Folgendes festzuhalten:

**Ist-Aufnahme der physischen Netztopologie**

Die physische Topologie beschreibt die Anordnung der Geräte und die Führung der Kabel, um die Geräte physisch miteinander zu verbinden. Um die physische Struktur des Netzes zu erfassen, ist es sinnvoll, sich an den räumlichen Verhältnissen zu orientieren, unter denen das Netz aufgebaut wird. Es ist ein Netzplan zu erstellen bzw. fortzuschreiben, der folgendes enthält:

- die aktuelle Kabelführung (siehe auch M 5.4 *Dokumentation und Kennzeichnung der Verkabelung* und M 2.396 *Vorgaben zur Dokumentation und Kennzeichnung der IT-Verkabelung* sowie M 1.69 *Verkabelung in Serverräumen*),
- die verwendeten Kabeltypen sowie die entsprechenden Kabellängen (siehe M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*) und die festgelegten Anforderungen an den Schutz von Kabeln (siehe M 1.22 *Materielle Sicherung von Leitungen und Verteilern*) sowie
- IT-Systeme, d. h. Client- und Server-Computer, aktive Netzkomponenten (wie Router, Switches, WLAN Access Points), Netzdrucker etc.

Für jedes IT-System sollte zumindest Folgendes vermerkt sein:

- eine eindeutige Bezeichnung (beispielsweise der vollständige Hostname oder eine Identifikationsnummer) sowie die verwendete IP-Adresse,
- Typ und Funktion (beispielsweise Datenbank-Server für Anwendung X),
- die zugrunde liegende Plattform (d. h. Hardware-Plattform und Betriebssystem oder Firmware),
- der Standort (beispielsweise Gebäude- und Raumnummer),
- zuständige Administratoren,
- die vorhandenen Kommunikationsschnittstellen (z. B. Internet-Anschluss, Bluetooth, WLAN-Adapter).

Zur Pflege dieses Plans ist es sinnvoll, ein entsprechendes Tool zur Unterstützung einzusetzen). Eine konsequente Aktualisierung dieser Pläne bei Umbauten oder Erweiterungen ist ebenso zu gewährleisten wie eine eindeutige und nachvollziehbare Dokumentation (vergleiche auch M 1.11 *Lagepläne der*

*Versorgungsleitungen* und M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*).

**Ist-Aufnahme der logischen Netztopologie**

Um die logische Topologie eines Netzes zu erstellen, ist die logische Struktur des Netzes zu betrachten. Dazu ist es notwendig, die Segmentierung der einzelnen OSI-Schichten und gegebenfalls die VLAN-Struktur zu erfassen.

Anhand der Darstellung der Netztopologie muss feststellbar sein, über welche aktiven Netzkomponenten eine Verbindung zwischen zwei beliebigen Endgeräten aufgebaut werden kann. Zusätzlich sind die Konfigurationen der aktiven Netzkomponenten zu dokumentieren, die zur Bildung der Segmente verwendet werden. Dies können bei logischer Segmentierung die Konfigurationsdateien sein, bei physischer Segmentierung die konkrete Konfiguration der Netzkomponenten.

Werden virtuelle IT-Systeme (virtuelle Switches, virtuelle Server etc.) und virtuelle Netzverbindungen, wie z. B. virtuelle LANs (VLANs) oder virtuelle Private Netze (VPNs), eingesetzt, dann sind diese ebenfalls in einem logischen Netzplan darzustellen. Hierbei sind virtuelle IT-Systeme gemäß ihrem Typ und Einsatzzweck genauso wie physische IT-Systeme zu behandeln. Darüber hinaus muss die Zuordnung von virtuellen IT-Systemen zu physischen Host-Systemen nachvollziehbar sein. Um die Übersichtlichkeit zu verbessern, ist es bei zunehmender Größe eines Netzes sinnvoll, den Netzplan in mehrere Teilnetzpläne aufzuteilen.

Ähnlich wie bei der physischen Topologie ist auch bei der logischen Topologie auf eine konsequente Aktualisierung des logischen Netzplans bei wesentlichen Konfigurationsänderungen, beispielsweise wenn neue VLANs eingefügt werden, zu achten.

**Ist-Aufnahme der verwendeten Netzprotokolle**

Die Netzprotokolle, die in den einzelnen Netzsegmenten verwendet werden, und die hierfür notwendigen Konfigurationen (z. B. die MAC-Adressen, die IP-Adressen und die Subnetzmasken) sind zu dokumentieren. Darüber hinaus sollte auch dokumentiert werden, welche Dienste zugelassen sind (z. B. HTTP, SMTP) und welche gesperrt werden. Auch sollten die zu Grunde liegenden Kriterien, die für die Filterung herangezogen werden, dokumentiert werden.

**Ist-Aufnahme von Kommunikationsübergängen im LAN und WAN**

Die Kommunikationsübergänge im LAN und WAN sind, soweit sie nicht in der bereits erstellten Dokumentation enthalten sind, zu beschreiben. Für jeden Kommunikationsübergang zwischen zwei Netzen ist zu beschreiben,

- welche Übertragungsstrecken (z. B. Funkstrecke für eine LAN/LAN-Kopplung) hierfür eingesetzt werden,
- welche Kommunikationspartner und -dienste in welche Richtung hierüber zugelassen sind, und
- wer für die technische Umsetzung zuständig ist.

Hierzu gehört auch die Dokumentation der verwendeten WAN-Protokolle (z. B. ISDN, ATM etc.). Bei Einsatz einer Firewall ist zusätzlich deren Konfiguration (z. B. Filterregeln) zu dokumentieren, siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*.

**Ist-Aufnahme der Netzperformance und des Verkehrsflusses**

Um frühzeitig mögliche Engpässe im Netz erkennen zu können, ist eine Messung der Netzperformance und eine Analyse des Verkehrsflusses in und zwischen den Segmenten oder Teilnetzen durchzuführen.

Bei jeder Änderung der Netzsituation sind die zuletzt durchgeführten Ist-Aufnahmen zu wiederholen. Die im Rahmen der Ist-Aufnahmen erstellte Dokumentation ist so aufzubewahren, dass sie einerseits vor unbefugtem Zugriff geschützt ist, aber andererseits für das Sicherheitsmanagement oder die Administratoren jederzeit verfügbar ist.

Prüffragen:

- Existiert eine aktuelle Ist-Aufnahme der logischen und physischen Netztopologie?
- Ist die Dokumentation der physischen und logischen Netztopologie auch für Dritte verständlich und nachvollziehbar?
- Umfasst die Dokumentation der Netzsegmentierung auch die zugelassenen Dienste und Netzprotokolle sowie die für die Filterung zu Grunde liegenden Kriterien?
- Umfasst die Dokumentation der Netzsituation alle Kommunikationsübergänge zwischen den Netzen und die hierfür eingesetzten Übertragungsstrecken?
- Ist anhand der Dokumentation der Kommunikationsübergänge der Kommunikationsfluss bzw. Datenfluss zwischen den Kommunikationspartnern ersichtlich?
- Ist die Dokumentation zur Netzsituation vor unbefugtem Zugriff geschützt, für die Zuständigen aber jederzeit verfügbar?

# M 2.140 Analyse der aktuellen Netzsituation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Diese Maßnahme baut auf den Ergebnissen der Ist-Aufnahme nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* auf und erfordert spezielle Kenntnisse im Bereich Netzdesign und Netzaufbau sowie der Analyse von netzspezifischen Schwachstellen. Darüber hinaus ist auch Erfahrung bei der Beurteilung der eingesetzten individuellen IT-Anwendungen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit notwendig. Da dies ein komplexes Gebiet ist, das neben tief gehenden Kenntnissen in allen genannten Bereichen auch viel Zeit erfordert, kann es zur Analyse der aktuellen Netzsituation hilfreich sein, externe Berater hinzuzuziehen. Im Bereich der deutschen Bundesverwaltung kann das Bundesamt für Sicherheit in der InformationstechnikBSI Hilfestellung leisten.

Eine Analyse der aktuellen Netzsituation besteht im Wesentlichen aus einer Strukturanalyse, einer Schutzbedarfsfeststellung und einer Schwachstellenanalyse.

Eine **Strukturanalyse** besteht aus einer Analyse der nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* angelegten Dokumentationen. Die Strukturanalyse muss von einem Analyseteam durchgeführt werden, das in der Lage ist, alle möglichen Kommunikationsbeziehungen nachzuvollziehen oder auch herleiten zu können. Als Ergebnis muss das Analyseteam die Funktionsweise des Netzes verstanden haben und über die prinzipiellen Kommunikationsmöglichkeiten informiert sein. Häufig lassen sich bei der Strukturanalyse bereits konzeptionelle Schwächen des Netzes identifizieren.

Eine erfolgreich durchgeführte Strukturanalyse ist unbedingte Voraussetzung für die sich anschließende detaillierte Schutzbedarfsfeststellung bzw. die Schwachstellenanalyse.

### Detaillierte Schutzbedarfsfeststellung

An die Strukturanalyse schließt sich eine Schutzbedarfsfeststellung an, die über die in der IT-Grundschutz-Vorgehensweise beschriebene hinausgeht. Hier werden zusätzlich die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität in einzelnen Netzbereichen bzw. Segmenten berücksichtigt. Hierzu ist es notwendig festzustellen, welche Anforderungen aufgrund der verschiedenen IT-Verfahren bestehen und wie diese auf die gegebene Netzsegmentierung Einfluss nehmen. Als Ergebnis muss erkenntlich sein, in welchen Netzsegmenten besondere Sicherheitsanforderungen bestehen.

### Analyse von Schwachstellen im Netz

Basierend auf den bisher vorliegenden Ergebnissen erfolgt eine Analyse der Schwachstellen des Netzes. Hierzu gehört insbesondere bei entsprechenden Verfügbarkeitsanforderungen die Identifizierung von nicht redundant ausgelegten Netzkomponenten (Single-Point-of-Failures). Weiterhin müssen die Bereiche benannt werden, in denen die Anforderungen an Verfügbarkeit, Vertraulichkeit oder Integrität nicht eingehalten werden können bzw. besonderer Aufmerksamkeit bedürfen. Zudem ist festzustellen, ob die gewählte Segmentierung hinsichtlich Durchsatz und Performance geeignet ist (anhand der Er-

gebnisse der Verkehrsflussanalyse aus M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*).

**Beispielhafte Schwachstelle**: Die Performance- und Verkehrsflussanalyse zeigt eine überlastete aktive Netzkomponente. Für den betreffenden Kommunikationsweg wurden im Rahmen der Schutzbedarfsfeststellung hohe Anforderungen an die Verfügbarkeit und damit auch an die Performance festgestellt. Diese Schwachstelle erfordert eine Anpassung der Segmentierung des Netzes oder den Austausch der Netzkomponente gegen ein leistungsfähigeres Modell (siehe M 5.61 *Geeignete physische Segmentierung*, M 5.62 *Geeignete logische Segmentierung*, sowie M 5.60 *Auswahl einer geeigneten Backbone-Technologie* und M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*).

Prüffragen:

- Ist dokumentiert, in welchen Netzsegmenten welche Sicherheitsanforderungen bestehen?
- Sind die Schwachstellen des Netzes hinsichtlich der Sicherheitsanforderungen analysiert, definiert und den einzelnen Netzbereichen zugeordnet?

# M 2.141 Entwicklung eines Netzkonzeptes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um den Anforderungen bezüglich Verfügbarkeit (auch Durchsatz und Performance), Vertraulichkeit und Integrität zu genügen, muss der Aufbau, die Änderung bzw. die Erweiterung eines Netzes sorgfältig geplant werden. Hierzu dient die Erstellung eines Netzkonzeptes.

Ein Netzkonzept besteht aus einem analytischen und einem konzeptionellen Teil:

**Analyse**

Zunächst ist zu unterscheiden, ob ein bestehendes Netz zu erweitern bzw. zu verändern ist oder ob das Netz vollständig neu aufgebaut werden soll.

Im ersten Fall sind vorab die Maßnahmen M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und M 2.140 *Analyse der aktuellen Netzsituation* zu bearbeiten. Im zweiten Fall entfallen diese Maßnahmen. Stattdessen sind die Anforderungen an die Netzkommunikation zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

Um die Kommunikationsanforderungen zu ermitteln, ist zunächst der zukünftig zu erwartende Daten- und Verkehrsfluss in und zwischen den Netzsegmenten festzustellen, da die zu erwartende Last die Segmentierung des zukünftigen Netzes beeinflussen muss. Darüber hinaus sind die notwendigen logischen bzw. physischen Kommunikationsbeziehungen (dienste-, anwender-, gruppenbezogen) zu eruieren und die Kommunikationsübergänge zur LAN/LAN-Kopplung oder über ein WAN zu ermitteln.

Soll ein bestehendes Netz verändert oder erweitert werden, ist in einem Soll/Ist-Vergleich das erarbeitete Netzkonzept mit der vorhandenen Situation nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* zu vergleichen. Ausgehend von Differenzen kann unter Berücksichtigung der oben genannten Maßnahmen ein Realisierungsplan für die so genannte Netzmigration erstellt werden. Dabei ist zu berücksichtigen, dass der Realisierungsaufwand um so größer ist, je mehr das Netzkonzept vom Ist-Zustand abweicht.

Die Schutzbedarfsanforderungen des Netzes werden aus denen der geplanten oder bereits bestehenden IT-Verfahren abgeleitet. Daraus werden physische und logische Segmentstrukturen gefolgert, so dass diesen Anforderungen (z. B. hinsichtlich Vertraulichkeit) durch eine Realisierung des Netzes Rechnung getragen werden kann. Zum Beispiel bestimmt der Schutzbedarf einer IT-Anwendung die zukünftige Segmentierung des Netzes.

Schließlich muss versucht werden, die abgeleiteten Kommunikationsbeziehungen mit den Schutzbedarfsanforderungen zu harmonisieren. Unter Umständen sind hierzu Kommunikationsbeziehungen einzuschränken, um dem festgestellten Schutzbedarf gerecht zu werden.

Abschließend sind die verfügbaren Ressourcen zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür not-

wendigen finanziellen Ressourcen. Die Ergebnisse sind entsprechend zu dokumentieren.

**Konzeption**

Nachdem das bestehende oder neu aufzubauende Netz analysiert worden ist, wird ein Netzkonzept analog M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* erstellt. Dazu sind prinzipiell folgende Schritte zu durchlaufen, wobei diese Schritte nicht in jedem Fall streng aufeinander folgend ausgeführt werden können. In einigen Teilen beeinflussen sich die Ergebnisse der Schritte gegenseitig, so dass eine regelmäßige Überprüfung und Konsolidierung der Teilergebnisse vorgenommen werden muss.

- Konzeption der physischen und logischen Netztopologie sowie der physischen und logischen Segmentierung
- Konzeption der verwendeten Nezprotokolle
- Konzeption von Kommunikationsübergängen im LAN und WAN

In den einzelnen Schritten sind im Wesentlichen die folgenden Tätigkeiten auszuführen:

**Schritt 1 - Konzeption der physischen und logischen Netztopologie**

Basierend auf der Analysesituation und den konkreten baulichen Gegebenheiten muss eine geeignete physische und logische Netztopologie ausgewählt werden (siehe hierzu M 5.60 *Auswahl einer geeigneten Backbone-Technologie*, M 5.1 *Entfernen oder Deaktivieren nicht benötigter Leitungen*, M 5.2 *Auswahl einer geeigneten Netz-Topologie* und M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*). Aber auch zukünftige Anforderungen wie Skalierbarkeit müssen hier Berücksichtigung finden. Die so erstellte Konzeption muss dokumentiert werden (Verkabelungspläne, physische und logische Netzpläne etc.).

Auf der Grundlage der Anforderungen an das Netz, die sich beispielsweise aus der Schutzbedarfsfeststellung ergeben sowie unter Berücksichtigung der Ergebnisse der Datenflussanalyse muss bei der Konzeption der physischen und logischen Netztopologie eine geeignete physische und logische Segmentierung durchgeführt werden (siehe M 5.61 *Geeignete physische Segmentierung*, M 5.62 *Geeignete logische Segmentierung* und M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*).

**Schritt 2 - Konzeption der Netzprotokolle**

In diesem Schritt geht es im Wesentlichen darum, ein für das Netz geeignetes Adressierungs- und Namenschema festzulegen und darauf aufbauend Teilnetze zu bilden. Insbesondere bei großen Netzen müssen in diesem Schritt auch geeignete Routing- und Switching-Protokolle ausgewählt werden.

**Schritt 3 - Konzeption der Kommunikationsübergänge im LAN und WAN**

Bezogen auf den ermittelten Datenfluss über Kommunikationsübergänge hinweg und die Anforderungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit können in diesem Schritt die Kommunikationsübergänge konzipiert werden. Hierzu gehört die Auswahl geeigneter Koppelelemente (siehe M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*), aber auch die sichere Konfiguration derselben (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)* und M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*).

**Weitere Schritte**

Nachdem das Netzkonzept erstellt worden ist, können nun die Maßnahmen zur Erstellung eines Netzmanagement-Konzeptes durchgeführt werden (siehe M 2.143 *Entwicklung eines Netzmanagement-Konzeptes*, M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll* und M 2.145 *Anforderungen an ein Netzmanagement-Tool*).

Außerdem sollte überlegt werden, einen Netzrealisierungsplan auszuarbeiten.

Für die Erstellung eines Netz-Realisierungsplans ist zu unterscheiden, ob es sich um einen vollständigen Neuaufbau des Netzes, um eine Veränderung der bestehenden Konzeption und/oder eine Erweiterung handelt.

Bei einer vollständigen Neuplanung sind anhand der entwickelten Netzkonzeption die notwendigen Schritte abzuleiten. Dabei erfolgt nach abgeschlossener Planung der Aufbau des Netzes über das Verlegen der notwendigen Kommunikationskabel, das Einrichten von Räumen für die technische Infrastruktur, das Installieren der versorgenden technischen Infrastruktur, die Integration der notwendigen Koppelelemente (Switches, Router etc.), das Einrichten der Netzmanagement-Stationen, den Einbau der entsprechenden Netzadapter in den Endgeräten, bis hin zur Konfiguration dieser Endgeräte.

Soll ein bestehendes Netz verändert oder erweitert werden, ist in einem Soll/Ist-Vergleich das erarbeitete Netzkonzept mit der vorhandenen Situation nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* zu vergleichen. Ausgehend von Differenzen kann unter Berücksichtigung der oben genannten Maßnahmen ein Realisierungsplan für die so genannte Netzmigration erstellt werden. Dabei ist zu berücksichtigen, dass der Realisierungsaufwand um so größer ist, je mehr das Netzkonzept vom Ist-Zustand abweicht.

Prüffragen:

- Existiert ein aktuelles Netzkonzept?
- Werden die Anforderungen bezüglich Verfügbarkeit, Vertraulichkeit und Integrität bei Erweiterung, Änderung oder Aufbau eines Netzes im Netzkonzept berücksichtigt?
- Entsprechen die physischen und logischen Segmentstrukturen des Netzes dem Schutzbedarf?

# M 2.142 Entwicklung eines Netz-Realisierungsplans

Die Maßnahme ist in der 15. Ergänzungslieferung 2015 entfallen. Die Inhalte wurden in M 2.141 integriert.

# M 2.143 Entwicklung eines Netzmanagement-Konzeptes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, IT-Sicherheitsbeauftragter

Die in einem lokalen Netz zusammengefassten vielfältigen IT-Systeme, wie z. B. Serversysteme, Endgeräte, Drucker, aktive Netzkomponenten usw., sollten auf Netzebene an einer geeigneten Stelle zentral administriert und überwacht werden. Eine zentrale Administration der Netzkomponenten ist dabei einer dezentralen vorzuziehen, da in diesem Fall Administrationsaufwände verringert und Anforderungen an die Sicherheit zentral definiert und kontrolliert werden können. In erster Linie wird ein zentrales Netzmanagement verwendet, um die Verfügbarkeit und Integrität des Netzes sowie die Integrität und Vertraulichkeit der übermittelten Daten zu gewährleisten. Diese Aufgabe hat eine hohe Komplexität und sollte durch den Einsatz eines Netzmanagement-Tools unterstützt werden.

Vor der Beschaffung und dem Betrieb eines solchen Netzmanagement-Systems ist im ersten Schritt ein Konzept zu erstellen, in dem alle Sicherheitsanforderungen an das Netzmanagement formuliert und angemessene Maßnahmen für den Fehler- oder Alarmfall vorgeschlagen werden. Dabei sind insbesondere die folgenden Bestandteile eines Netzmanagement-Konzeptes bei der Erstellung zu berücksichtigen und in einem Gesamtzusammenhang darzustellen.

- Performance-Messungen zur Netzanalyse (siehe M 2.140 *Analyse der aktuellen Netzsituation*),
- Auswahl eines Managementnetzes (siehe M 2.582 *Möglichkeiten zur Einrichtung eines Managementnetzes*),
- Reaktionen auf Fehlermeldungen der überwachten Netzkomponenten,
- Fernwartung / Remote-Control, insbesondere der aktiven Netzkomponenten,
- Generierung von Trouble-Tickets und Eskalation bei Netzproblemen (Hierüber kann eine Anbindung an Systemmanagement- und User-Help-Desksysteme bzw. an externe Nachrichtenübermittler erfolgen.),
- Protokollierung und Audit des Netzverkehrs (Online und/oder Offline),
- Einbindung eventuell vorhandener proprietärer Systeme bzw. von Systemen mit unterschiedlichen Managementprotokollen (z. B. im Telekommunikationsbereich),
- Konfigurationsmanagement aller im Einsatz befindlichen IT-Systeme (siehe unter anderen M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*),
- Verteilter Zugriff auf die Netzmanagement-Funktionalitäten (Für die Administration oder für das Audit kann ein Remote-Zugriff auf die Netzmanagement-Funktionalitäten notwendig sein. Hier ist insbesondere eine sorgfältige Definition und Vergabe der Zugriffsrechte notwendig.).

Die konkreten Anforderungen an ein Netzmanagement-Tool sind in M 2.145 *Anforderungen an ein Netzmanagement-Tool* beschrieben. Diese müssen eine Umsetzung des Netzmanagement-Konzeptes ermöglichen.

Prüffragen:

- Werden die Netzkomponenten zentral administriert?
- Sind Reaktionen auf Fehlermeldungen der überwachten Netzkomponenten vorgesehen?

- Ist die Generierung von Trouble-Tickets und die Eskalation bei Netzproblemen vorgesehen?
- Werden Protokollierungen und Audits des Netzverkehrs durchgeführt?
- Werden vorhandene proprietäre Systeme bzw. unterschiedliche Managementprotokolle angemessen in das Netzmanagement eingebettet?

# M 2.144 Verwendung von SNMP als Netzmanagement-Protokoll

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, IT-Sicherheitsbeauftragter

Das Simple Network Management Protocol (SNMP) gilt derzeit als Standardprotokoll für Netzmanagement.

Die wesentlichen Vor- und Nachteile von SNMP sind:

- SNMP zeichnet sich durch ein einfaches Design und damit auch durch eine einfache Implementation aus. Dies reduziert die Fehleranfälligkeit und verbessert die Stabilität des Protokolls.
- SNMP ist sehr weit verbreitet und gilt als ein De-Facto-Standard. Dadurch wird es durch fast jedes Produkt im Netz- und Systemtechnikumfeld unterstützt.
- Das Protokoll kann sehr einfach an zukünftige Bedürfnisse angepasst werden. Aus diesem Grund und der oben genannten weiten Verbreitung von SNMP kann es als sehr zukunftssicheres Protokoll (Investitionsschutz) bezeichnet werden.
- Es handelt sich um ein verbindungsloses, einfaches Protokoll auf Transportebene. Damit ist die Performance der Übertragung der SNMP-Pakete im Netz besser als beim verbindungsorientierten CMIP (Common Management Information Protocol).
- SNMPv3 bietet ausreichend gute Möglichkeiten zur Authentisierung und Verschlüsselung an, so dass diese in den Versionen SNMPv1 und SNMPv2 bestehenden Mängel beseitigt wurden.
- Der Einsatz von SNMPv1 oder SNMPv2 birgt Sicherheitsrisiken, die es unter Umständen einem Angreifer ermöglichen, weitgehende Informationen über die System- und Netzumgebung zu erhalten. Insbesondere existiert, abgesehen von den Community-Namen (die bei SNMP die Möglichkeit zur Bildung von Gruppen und bei SNMPv1 und SNMPv2 einen rudimentären Passwortschutz bieten), kein echter Passwortschutz beim Zugriff auf die Netzkomponenten.
- Aufgrund der Einfachheit des Protokolls und der verfügbaren Möglichkeiten weist SNMP Schwächen im Umgang mit sehr großen oder stark expandierenden Netzen auf.
- Die Performance der Version 1 ist bei aufwendigeren MIB-Abfragen ungenügend, da immer der gesamte MIB-Baum angegeben werden muss.

SNMP ist ein einfach zu implementierendes Protokoll, das dazu eingesetzt wird, Managementinformationen zwischen einzelnen Netzkomponenten (Agenten) und einer zentralen Managementstation (Manager) auszutauschen. Hierzu werden in einem lokalen Netz ein oder eventuell mehrere Manager und je ein Agent pro IT-System, das mit SNMP überwacht bzw. konfiguriert werden soll, installiert. Die Agenten sind auf den überwachten IT-Systemen (z. B. Router, Switches, Server etc.) installiert. Sie ermitteln Statusinformationen von den Komponenten, auf denen sie installiert sind und können die Konfiguration abfragen bzw. ändern. Sie sammeln über diese Systeme Informationen und legen sie in einer Managementdatenbank (Management Information Base, MIB) ab.

Die Managementinformationen bestehen im Wesentlichen aus Werten von Statusvariablen, die im Managementagenten vorgehalten werden und den jeweiligen Zustand des zugehörigen verwalteten Objektes beschreiben. Welche Statusvariablen (Name und Typ) in den einzelnen Agenten existieren, ist in

der MIB beschrieben. Dabei ist die Information hierarchisch organisiert, und jedem Wert ist eine eindeutige Identifikationsnummer zugeordnet, die auf den Variablen damit eine eindeutige Reihenfolge definiert.

Die Nachrichtentypen sind im Einzelnen:

- GetRequest: wird vom Manager an Agenten geschickt, um von ihnen den Wert einer oder mehrerer Statusvariablen abzufragen.
- GetNextRequest: wird vom Manager an Agenten geschickt, um von ihnen den Wert oder die nächsten Werte gemäß der Reihenfolge der Variablen in der MIB abzufragen.
- GetBulkRequest: ist eine Sonderform bei der der GetNextRequest Befehl mehrfach wiederholt wird. Die Anzahl der Wiederholungen lässt sich mit Hilfe des Max-Repetitions Wert festlegen.
- SetRequest: wird vom Manager an Agenten geschickt, um dort den Wert einer Variablen zu setzen.
- GetResponse: wird von Agenten zum Manager geschickt, um die angefragten Werte zu senden oder das Setzen eines Variablenwertes zu bestätigen.
- Trap: wird von Agenten verwendet, um den Manager über Ausnahmeereignisse zu informieren. Das Senden einer Trap-Nachricht erfolgt, im Gegensatz zur GetResponse-Nachricht, ohne vorherige Anfrage vom Manager.
- InformRequest: wird von Agenten oder einem anderen Manager verwendet, um über ein Ausnahmeereignis zu informieren. Im Gegensatz zur Trap muss der Empfang des InformRequest vom Manager bestätigt werden.
- Report: kann über das Setzen des reportableFlags angefordert werden und informiert über das Ergebnis einer zuvor gesendeten Anforderung.

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten "Community Strings". Als Standardeinstellung bei nahezu allen Herstellern ist der read-Community-String auf den Wert "public" eingestellt, während der write-Community-String auf den Wert "private" gesetzt ist. Die SNMP Community Strings werden im Klartext über das Netz übertragen. Allerdings gibt es auch in SNMPv2 bezüglich der unterstützten Sicherheit unterschiedliche Varianten. Wenn die unsicheren SNMP-Versionen genutzt werden und für die Administration kein eigenes Administrationsnetz eingerichtet wurde, kann ein Angreifer leicht die Kontrolle über Netzkomponenten erlangen, wenn diese Default-Einstellungen beibehalten werden. SNMPv1 und SNMPv2 sollten daher nicht mehr eingesetzt, stattdessen sollte SNMPv3 (oder höher) verwendet werden. Erst ab dieser Version sind stärkere Authentisierungs- und Verschlüsselungsoptionen vorhanden.

In der Praxis werden jedoch noch immer Systeme eingesetzt, die Version 3 nicht unterstützen und die daher auf ältere Protokollversionen angewiesen sind. In diesem Fall muss der Einsatz einer älteren Version begründet und dokumentiert werden, vor allem sollten die Risiken offengelegt und akzeptiert werden. Diese unsicheren Protokolle sollten allenfalls nur innerhalb eines separaten abgeschotteten Administrationsnetzes (siehe M 2.582 *Möglichkeiten zur Einrichtung eines Managementnetzes*) eingesetzt werden. Dies sollte aber höchstens eine Übergangslösung darstellen, langfristig sollten nur noch Geräte eingesetzt werden, die SNMP-Protokolle ab Version 3 unterstützen.

Darüber hinaus müssen die voreingestellten Community-Namen unbedingt gegen andere, schwer zu erratende Namen ausgetauscht werden und auch regelmäßig gewechselt werden (siehe M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*). Die individuellen Netzelemente sollten unterschiedliche Community-Namen besitzen. Die mit den Community-Namen verbunde-

nen Zugriffsberechtigungen müssen auf das absolut erforderliche Minimum gesetzt werden. Weiterhin sollte der Zugriff per SNMP auf Netzelemente mit Hilfe von Access Control Listen auf die Netzmanagement-Stationen beschränkt werden (siehe M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration*). Wenn ältere Versionen von SNMP nicht benötigt werden, sollten diese deaktiviert werden.

In der Version SNMPv3 wurde das Konzept der Community-Namen durch einen Benutzernamen ersetzt. Jeder Benutzer ist einer Gruppe zugeordnet, die für die einzelnen überwachten Objekte fein einstellbare Rechte besitzen. Über die Gruppenzugehörigkeit kann auch eingestellt werden, welche Benachrichtigungen (traps) ein Benutzer sehen darf.

SNMPv3 bietet verschiedene Verfahren an, um die Authentisierung der Benutzer zu gewährleisten: einfache Überprüfung des Benutzernamens, Authentisierung mittels MD5 bzw. SHA. Die übertragenen Informationen können außerdem verschlüsselt werden. Es sollten jeweils die stärksten Sicherheitsmerkmale eingesetzt werden.

Aus Sicherheitssicht sollte deshalb auf den Einsatz von SNMPv1 und SNMPv2 verzichtet und SNMPv3 verwendet werden. Der überwiegende Teil moderner IT-Systeme und aktiver Netzkomponenten beherrschen SNMPv3 ebenso wie die Netzmanagement-Software. Der höhere Aufwand, der bei der Konfiguration von SNMPv3 zu leisten ist, wird durch die erhöhte Sicherheit ausgeglichen.

Für den Fall, dass ein herstellerspezifisches Protokoll eingesetzt wird, existiert meist die Möglichkeit, sogenannte Proxies zum Einbinden von SNMP zu verwenden. Auch in diesem Fall muss detailliert geprüft werden, ob das proprietäre Netzmanagement-Protokoll für den Verwendungszweck geeignet ist und ob es dieSicherheitsanforderungen der Institution an das Netzmanagement erfüllt.

Prüffragen:

- Wird auf den Einsatz veralteter Netzmanagement-Protokolle wie SNMPv1 und SNMPv2 verzichtet?
- Bei zwingendem Einsatz veralteter Netzmanagement-Protokolle: Sind die damit einhergehenden Risiken dokumentiert?
- Werden die Community-Namen geändert, individuell auf Netzelemente vergeben und regelmäßig gewechselt?
- Sind die mit den Community-Namen verbundenen Zugriffsberechtigungen auf das absolut erforderliche Minimum gesetzt?
- Ist der Zugriff per SNMP auf Netzelemente durch Access Control Listen auf die Netzmanagement-Stationen beschränkt?

# M 2.145 Anforderungen an ein Netzmanagement-Tool

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um ein effektives Netzmanagement durchführen zu können, ist der Einsatz eines Netzmanagement-Tools hilfreich. Derzeit stellt der Markt eine Vielzahl von Produkten für das Netzmanagement zur Verfügung, die alle hinsichtlich der eigenen individuellen Anforderungen geprüft werden müssen, bevor eine Entscheidung zur Beschaffung eines konkreten Tools gefällt werden kann. Dabei gilt es vor allem, die Sicherheitsanforderungen nach M 2.143 *Entwicklung eines Netzmanagement-Konzeptes* zu erfüllen und die folgenden Punkte zu beachten:

- Ein Netzmanagement-Tool muss das ausgewählte Netzmanagement-Protokoll unterstützen und sollte sinnvollerweise auch für künftige Entwicklungen Lösungen anbieten (siehe M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll*).
- Das Produkt muss skalierbar sein, d. h. es muss an zukünftige Anforderungen angepasst werden können (z. B. Erweiterung eines bestehenden Netzes).
- Es muss alle im lokalen Netz vorhandenen Netzkomponenten unterstützen und sollte möglichst darüber hinaus die Produkte mehrerer Hersteller unterstützen, um bei zukünftigen Investitionen nicht an einen Hersteller gebunden zu sein.
- Es muss alle im lokalen Netz eingesetzten Netzprotokolle unterstützen.
- Es sollte modular aufgebaut sein, um auch später weitere Funktionen ohne großen Aufwand in das bestehende Netzmanagement-System integrieren zu können.
- Es sollte eine grafische Oberfläche (Graphical User Interface, GUI) besitzen, um die relevanten Informationen übersichtlich und verständlich darstellen zu können.
- Da das Netzmanagement-System die Konfiguration des Netzes verwaltet, muss es ausreichend geschützt sein. So ist der Zugriff restriktiv zu handhaben und die gleichen Mindestanforderungen wie für Administratorzugänge zu fordern. Eine Zwei-Faktor-Authentisierung wird empfohlen und sollte vom Netzmanagement-System unterstützt werden.
- Werden außerdem Produkte zum Systemmanagement eingesetzt, sollte im Sinne eines "Single Point of Administration" eine Integration mit dem Netzmanagement unter einer Oberfläche möglich sein.

Neben diesen allgemein zu prüfenden Anforderungen sind zusätzlich die funktionalen Anforderungen an ein Netzmanagement-System zu definieren. Die folgenden Kriterien stellen dazu eine Übersicht über die Möglichkeiten in aktuell verfügbaren Produkten dar, nicht alle Funktionen sind jedoch in allen Produkten realisiert. Vor einer Produktentscheidung muss deshalb festgelegt werden, welche Funktionen notwendig sind und welche nicht benötigt werden:

- physische und logische topologische Darstellung des Netzes (z. B. auch die Möglichkeit der Einbindung von Hintergrundgrafiken wie Baupläne usw.),
- wählbare Darstellungsform der Topologie, automatisches Erkennen und Abbilden der Netztopologie und Segmentierung (Auto-Discovery),
- Anzeige der Konfiguration der aktiven Netzkomponenten auf Portebene,
- Anzeige der Performance auf Portebene,
- graphische Visualisierung der aktiven Netzkomponenten,

- interaktives Tool für das Managementprotokoll (z. B. MIB-Browser),
- einfache Navigation im Netzmanagement-Tool, z. B. durch Zoomfunktionen oder durch Ausschnittsvergrößerungen,
- eventuell Integration eines VLAN-Managers und graphische Darstellung der VLANs,
- intuitive Bedienbarkeit der Tool-Oberfläche, insbesondere desjenigen Teils, in dem die physischen und logischen topologischen Abbildungen editiert werden (beispielsweise durch "Drag & Drop"),
- Darstellung der Fehler- und Alarmmeldungen durch frei definierbare Farben und nach selbst zu definierenden Kriterien,
- Möglichkeit eines verteilten Managements (Client/Server und Manager-of-Manager) und
- Möglichkeit der Integration und Definition weiterer MIBs (Private-MIBs).

Prüffragen:

- Sind die Anforderungen an das einzusetzende Netzmanagement-Tool festgestellt?

# M 2.146 Sicherer Betrieb eines Netzmanagement-Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für den sicheren Betrieb eines Netzmanagement-Tools oder eines komplexen Netzmanagementsystems, welches beispielsweise aus mehreren verschiedenen Netzmanagement-Tools zusammengesetzt sein kann, ist die sichere Konfiguration aller beteiligten Komponenten zu überprüfen und sicherzustellen. Hierzu gehören die Betriebssysteme, auf denen das oder die Netzmanagementsystem/e betrieben werden, die zumeist notwendigen externen Datenbanken für ein Netzmanagementsystem, das verwendete Protokoll (siehe M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll*) und die aktiven Netzkomponenten selbst. Vor dem Betrieb eines Netzmanagementsystems muss die Ermittlung der Anforderungen an den Betrieb und die Erstellung eines Netzmanagement-Konzeptes stehen (siehe M 2.143 *Entwicklung eines Netzmanagement-Konzeptes*).

Insbesondere sind folgende Punkte zu beachten:

- Um ein Mitlesen oder Verändern der Netzmanagement-Informationen zu verhindern, muss der Rechner, auf dem die Netzmanagement-Konsole betrieben wird, geeignet geschützt werden. Dazu zählen beispielsweise die Aufstellung in einem besonders geschützten Raum, der Einsatz von Bildschirmsperren, Passwortschutz für die Netzmanagement-Konsole und weitere Sicherheitsmechanismen des zugrunde liegenden Betriebssystems.
- Die Maßnahme M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll* ist vor dem Hintergrund des sicheren Betriebes zu berücksichtigen. Insbesondere ist durch eine geeignete Konfiguration der aktiven Netzkomponenten auf der Basis des verwendeten Protokolls ein Auslesen der MIBs und anderer Informationen durch unautorisierte Personen zu verhindern (siehe M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration* und M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*).
- Werden Netzmanagement-Funktionen dezentral nach dem Client/Server-Modell oder durch Benutzung der X-Window-Technologie durchgeführt, muss für diese ebenfalls der sichere Betrieb gewährleistet werden.
- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden, um unautorisierte Änderungen frühzeitig zu erkennen.
- Das Netzmanagement-System muss auf sein Verhalten bei einem Systemabsturz getestet werden. Insbesondere sollte ein automatischer Neustart möglich sein, um die Zeitspanne, in der das lokale Netz nicht überwacht wird, so gering wie möglich zu halten. Die Netzmanagement-Datenbank darf durch einen Systemabsturz nicht beschädigt werden und muss nach einem Neustart wieder verfügbar sein, da die darin enthaltenen Konfigurationsdaten wesentlich für den Betrieb des Netzmanagementsystems sind. Diese Daten müssen daher besonders gesichert werden, damit sie einerseits noch verfügbar sind und andererseits keine alten oder fehlerhaften Konfigurationsdaten bei einem Neustart benutzt werden, der ggf. durch einen Angreifer aus diesem Grunde provoziert wurde. Für den Schutz der eingesetzten Datenbank ist unter Umständen auch der Baustein B 5.7 *Datenbanken* zu beachten.
- Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren Betrieb des Netzmanagement-Sy-

stems relevante Dateien wie Konfigurationsdaten, Passwortdateien und auch die Metakonfigurationsdateien für die eigentlichen Netzkomponenten auf dem aktuellsten Stand sind.
Für den sicheren Betrieb eines Netzmanagement-Systems sind folgende Daten relevant:

  - Konfigurationsdaten des Netzmanagementsystems, die sich in entsprechend geschützten Verzeichnissen befinden müssen.
  - Konfigurationsdaten der Netzkomponenten (Metakonfigurationsdateien), die sich ebenfalls in entsprechend geschützten Verzeichnissen befinden müssen.
  - Passwortdateien für das Netzmanagementsystem. Hierbei ist beispielsweise auf die Güte des Passworts und die Möglichkeit einer verschlüsselten Speicherung des Passworts zu achten (siehe M 2.11 *Regelung des Passwortgebrauchs*).

- Eine Administration der aktiven Netzkomponenten über das Netz sollte dann eingeschränkt werden und eine Administration über die lokalen Schnittstellen erfolgen, wenn die Erfüllung der Anforderungen an Vertraulichkeit und Integrität der Netzmanagement-Informationen nicht gewährleistet werden kann. In diesem Fall ist auf ein zentrales Netzmanagement zu verzichten.

Prüffragen:

- Ist der Rechner, auf dem die Netzmanagement-Konsole betrieben wird, geeignet geschützt?
- Verhindert die Konfiguration der aktiven Netzkomponenten ein Auslesen der MIBs und anderer Informationen durch unautorisierte Personen?
- Ist bei der Nutzung von Funktionen nach dem Client/Server-Modell oder dem Einsatz der X-Window-Technologie der sichere Betrieb gewährleistet?
- Werden regelmäßig Integritätstests der eingesetzten Software durchgeführt?
- Ist gewährleistet, dass das Netzmanagement-System nach einem Systemabsturz automatisch neu startet und dabei korrekte Konfigurationsdaten benutzt werden?
- Wird beim Wiedereinspielen von gesicherten Datenbeständen darauf geachtet, dass relevante Dateien wie Konfigurationsdaten, Passwortdateien und Metakonfigurationsdateien für die Netzkomponenten auf dem aktuellen Stand sind?
- Sind die Konfigurationsdaten des Netzmanagementsystems und der Netzkomponenten vor unbefugtem Zugriff geschützt?
- Ist der Zugriff auf das Netzmanagementsystem angemessen abgesichert?
- Erfolgt die Adminstration der aktiven Netzkomponenten so, dass die Anforderungen an Vertraulichkeit und Integrität der Netzmanagement-Informationen gewährleistet werden?

# M 2.147 Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.148 Sichere Einrichtung von Novell Netware 4.x Netzen

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.149 Sicherer Betrieb von Novell Netware 4.x Netzen

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.150 Revision von Novell Netware 4.x Netzen

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.151 Entwurf eines NDS-Konzeptes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.152 Entwurf eines Zeitsynchronisations-Konzeptes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.153 Dokumentation von Novell Netware 4.x Netzen

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um für eine gesamte Organisation einen effektiven Schutz vor Schadprogrammen zu erreichen, sind abgestimmte und angemessene Sicherheitsmaßnahmen auszuwählen und umzusetzen.

Eine konzeptionelle Vorgehensweise ist Voraussetzung, um sämtliche betroffene IT-Systeme mit geeigneten Sicherheitsmaßnahmen zu versehen und durch ständige Aktualisierung den notwendigen Schutz aufrecht zu halten.

Nachfolgend werden die notwendigen Inhalte eines Sicherheitskonzeptes gegen Schadprogramme beschrieben.

### Abhängigkeit der Institution vom IT-Einsatz

Im Rahmen der Sicherheitsleitlinie und der Schutzbedarfsfeststellung wird bereits die Abhängigkeit der Institution vom IT-Einsatz beurteilt. Daraus lässt sich ableiten, welche Folgen sich ergeben, wenn keine oder nur unzureichende Sicherheitsmaßnahmen gegen Schadprogramme realisiert werden. Der personelle und finanzielle Aufwand, Schadprogramme zu beseitigen und deren Folgeschäden zu beheben, ist meist erheblich höher als der Aufwand zur Vermeidung einer Infektion durch den Einsatz geeigneter Sicherheitsmaßnahmen. Durch die gewählten Sicherheitsmaßnahmen sollte ein angemessener Schutz vor Schadprogrammen erreicht werden.

### Beschreibung des Gefährdungspotentials

Schadprogramme sind eine Gefahr für den ordnungsgemäßen Betrieb. Sie wirken auf unterschiedliche Weise auf IT-Systeme und können zu erheblichen Beeinträchtigungen von Funktionalitäten führen. Durch Schadprogramme können Daten manipuliert, ausspioniert oder entwendet werden.

### Identifikation bedrohter IT-Systeme

Betroffen sind grundsätzlich alle IT-Systeme, die über Kommunikationsverbindungen oder Datenträger mit Schadprogrammen in Berührung kommen können.

Durch Schadprogramme bedroht sind derzeit vorrangig alle IT-Systeme mit Windows-Betriebssystemen sowie solche mit Anwendungsprogrammen, deren Dateien zum Beispiel durch Makro-Viren infiziert werden können. Schadprogramme können grundsätzlich aber auch bei Verwendung anderer Betriebssysteme oder Anwendungsprogramme auftreten. Dies gilt zum Beispiel auch bei Unix/Linux-Systemen, Mac-OS-Systemen und Betriebssystemen von Mobiltelefonen. Betriebssysteme, die nicht zur Windows-Familie gehören, stellen aufgrund ihrer geringeren Verbreitung derzeit noch kein lohnendes Ziel für Entwickler von Schadprogrammen dar. Das Bedrohungspotential ist bei solchen Systemen somit niedriger.

Bedroht sind auch IT-Systeme, die nicht an das interne Netz angeschlossen sind. Insbesondere müssen Laptops, PDAs, Mobiltelefone und andere mobile Geräte berücksichtigt werden.

Auch Stand-Alone-Systeme, die über alternative Kanäle (beispielsweise Wählleitungen oder Datenträger) mit anderen IT-Systemen kommunizieren können, sind mit zu betrachten.

Aufgrund der vorstehenden Feststellungen können Sicherheitsmaßnahmen eingerichtet werden. Besonders gefährdete IT-Systeme sind vorrangig zu behandeln. Da die Bedrohung durch Schadprogramme mit dem Vernetzungsgrad der IT-Systeme steigt, sind IT-Systeme, die Schnittstellen zum Internet bilden, besonders bedroht und sollten zuerst betrachtet werden.

**Benennung von Ansprechpartnern**

Ein wichtiger Aspekt der Übersicht ist die Benennung von Ansprechpartnern für die jeweiligen IT-Systeme. Primäre Anlaufstellen für die Benutzer sollten dabei unabhängig vom konkreten Schutz vor Schadprogrammen sein, da ein Benutzer meist nicht zuverlässig feststellen kann, ob sein Computer von einem Schadprogramm befallen ist oder ob er ein anderes Problem hat. Es ist nicht notwendig, dass für das Thema Schadprogramme ein separates manuelles Meldewesen aufgebaut wird. Stattdessen sollten die vorhandenen Strukturen genutzt werden, die auch für andere Arten von Sicherheitsvorfällen erforderlich sind (siehe M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle* und M 2.12 *Betreuung und Beratung von IT-Benutzern*). Die Benutzer sollten hierbei möglichst eine einheitliche Meldestelle für alle Arten von Sicherheitsproblemen haben (User Help Desk, Support oder ähnliches).

**Flankierende Sicherheitsmaßnahmen**

Verschiedene Sicherheitsmaßnahmen erhöhen den Schutz vor Schadprogrammen. Neben den in B 1.6 *Schutz vor Schadprogrammen* beschriebenen spezifischen Aspekten des Schutzes vor Schadprogrammen tragen weitere technische und organisatorische Maßnahmen zur Senkung des Risikos bei. Diese flankierenden Maßnahmen (Sicherheitsgateway, Änderungsmanagement usw.) sind im Rahmen eines Sicherheitskonzeptes gegen Schadprogramme ebenfalls zu erfassen.

**Viren-Schutzprogramme auf bedrohten IT-Systemen**

Eine wichtige technische Maßnahme zum Schutz vor Schadprogrammen ist der Einsatz von Viren-Schutzprogrammen. Sie schützen allgemein vor Schadprogrammen und nicht nur vor Viren.

Viren-Schutzprogramme sind inzwischen meist Bestandteil größerer Software-Pakete, die auch Firewalls und Intrusion Detection Systeme umfassen können. Bei Erstellung eines Konzepts zum Schutz vor Schadprogrammen sollten daher auch die Maßnahmen M 5.71 *Intrusion Detection und Intrusion Response Systeme* sowie M 4.238 *Einsatz eines lokalen Paketfilters* berücksichtigt werden.

Der Einsatz eines Viren-Schutzprogramms wird grundsätzlich für alle von Schadprogrammen bedrohten IT-Systeme empfohlen, bestimmte IT-Systeme sind jedoch besonders anfällig für Schadprogramme. In folgender Reihenfolge kann vorgegangen werden, um Viren-Schutzprogramme flächendeckend zu installieren.

In einem ersten Schritt sollten die Viren-Schutzprogramme auf den IT-Systemen installiert werden, bei denen ein besonders hohes Risiko einer Infektion besteht oder bei denen durch eine Infektion ein besonders hoher Schaden auftreten kann. Hierzu zählen insbesondere kritische Server und IT-Systeme

mit Zugang zu externen Netzen. Auch IT-Systeme, die einen Datenkanal vom oder zum Internet zur Verfügung stellen, sollten zuerst mit geeigneten Schutzprogrammen ausgestattet werden. Zu beachten ist, dass verschlüsselte Dateien nicht geprüft werden können. Inhalte verschlüsselter Dateien können erst während oder nach dem Entschlüsseln auf Schadprogramme untersucht werden.

Im nächsten Schritt sollten die restlichen Server und alle Clients mit Viren-Schutzprogrammen ausgestattet werden. File-Server können eine Verteilstelle für infizierte Programme und Dateien sein. Datenbestände auf File-Servern sollten daher regelmäßig mit einem Viren-Schutzprogramm auf Schadprogramme untersucht werden. Durch diese Untersuchung können auch Dateien, auf die seit längerer Zeit kein Zugriff mehr erfolgt ist, auf Schadprogramme geprüft werden. Dafür ist ein Benutzerkonto zu verwenden, das auf alle Dateien des File-Servers lesenden Zugriff hat.

Die Server-Betriebssysteme sind in das Sicherheitskonzept gegen Schadprogramme ebenfalls mit einzubeziehen. Spezialisierte Programme zum Schutz der Kommunikationskanäle oder Datenbestände bei File-Servern bieten in der Regel keinen ausreichenden Schutz für das Server-Betriebssystem.

Neben den stationären Clients müssen auch mobile Endgeräte, beispielsweise Laptops und PDAs, sowie Stand-Alone-Systeme mit einem Schutz gegen Schadprogramme ausgestattet werden.

Unabhängig davon, welche technischen Sicherheitsmaßnahmen gegen Schadprogramme umgesetzt werden, verbleibt immer ein Restrisiko. Viren-Schutzprogramme erkennen meist nur diejenigen Schadprogramme zuverlässig, die zum Entwicklungszeitpunkt der Signatur-Updates bekannt waren. Das heißt, dass neue Schadprogramme gegebenenfalls nicht erkannt werden und Schäden anrichten können. Auch die vielfach integrierte heuristische Analyse oder die Verhaltenskontrolle von Programmen kann das Restrisiko nur senken, nicht jedoch vollständig eliminieren.

**Organisatorische Regelungen und personelle Maßnahmen**

Im Sicherheitskonzept sollten auch organisatorische bzw. personelle Regelungen festgelegt werden. Weitere Hinweise hierzu finden sich unter anderem in den folgenden Maßnahmen:

- M 2.160 *Regelungen zum Schutz vor Schadprogrammen*
- M 2.158 *Meldung von Schadprogramm-Infektionen*
- M 2.224 *Vorbeugung gegen Schadprogramme*
- M 6.23 *Verhaltensregeln bei Auftreten von Schadprogrammen*

**Aktualisierung des Sicherheitskonzeptes gegen Schadprogramme**

Das Sicherheitskonzept gegen Schadprogramme muss auf einem aktuellen Stand gehalten werden. Insbesondere bei Änderungen am Informationsverbund müssen die notwendigen Anpassungen im Sicherheitskonzept vorgenommen werden (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Prüffragen:

- Gibt es ein Sicherheitskonzept gegen Schadprogramme?
- Deckt das Sicherheitskonzept gegen Schadprogramme alle bedrohten IT-Systeme ab?

- Sind die zum Schutz gegen Schadprogramme erforderlichen technischen und organisatorischen Maßnahmen festgelegt?
- Wird das Sicherheitskonzept gegen Schadprogramme auf dem aktuellen Stand gehalten?

# M 2.155 Identifikation potentiell von Computer-Viren betroffener IT-Systeme

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.156 Auswahl einer geeigneten Computer-Virenschutz-Strategie

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 2.157 Auswahl eines geeigneten Viren-Schutzprogramms

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Bei der Auswahl eines Viren-Schutzprogramms sind verschiedene Anforderungen zu beachten. Im Folgenden wird der Begriff Viren-Schutzprogramm verwendet, gemeint ist jedoch ein Programm zum Auffinden jeglicher Schadprogramme.

### Technische Forderungen

Das auszuwählende Schutzprogramm sollte einen Basis-Schutz gegen Schadprogramme (Computer-Viren, Würmer, Backdoors, Trojanische Pferde, Spionageprogramme und andere) bieten. Die meisten gängigen Viren-Schutzprogramme erkennen mehr als 95% aller Viren, die im Umlauf sind. Hilfe bei der Auswahl des passenden Schutzprogramms können entsprechende Artikel in Fachzeitschriften bieten. Dort werden häufig auch andere Programmeigenschaften (zum Beispiel Geschwindigkeit und Bedienungskomfort) beschrieben.

Das Programm muss in der Lage sein, die in der Organisation im Einsatz befindlichen Dateisysteme sowie externe Datenträger und andere mobile Endgeräte zu durchsuchen, also eine möglichst umfassende Interoperabilität bieten.

Im Sicherheitskonzept gegen Schadprogramme ist festgelegt, welche IT-Systeme mit einem Viren-Schutzprogramm ausgestattet werden müssen. Das ausgewählte Produkt muss für diese IT-Systeme geeignet sein.

Zumindest für Clients sollte das Programm in einer deutschen Sprachversion verfügbar sein.

Je nach vorliegender Systemlandschaft können diese Ziele unter Umständen nicht durch die Auswahl eines einzelnen Viren-Schutzprogramms erreicht werden, sondern es müssen gegebenenfalls mehrere unterschiedliche Produkte beschafft und eingesetzt werden.

Mehrere Viren-Schutzprogramme unterschiedlicher Anbieter auf dem gleichen IT-System in Betrieb zu nehmen, ist nicht sinnvoll, da sich diese in der Regel behindern. Dies kann zu unerwünschten Nebeneffekten führen.

### Betriebsarten

Bei Viren-Schutzprogrammen für Clients ist es erforderlich, dass sowohl eine speicherresidente Betriebsart (on-access), als auch eine Betriebsart, bei der ein Suchlauf manuell gestartet wird (on-demand), vorhanden ist. Mittels manuellem Suchlauf können auch einzelne Datenträger und aktuell nicht verwendete Dateien auf Schadprogramme überprüft werden.

### Zu prüfende Dateiformate

Es müssen alle Dateitypen geprüft werden. Eine Beschränkung auf "ausführbare" Dateiformate ist nicht ausreichend.

**Integritätstest**

Viren-Schutzprogramme für Clients sollten einen Integritätsmechanismus enthalten, durch den kritische Prozesse kontrolliert und ihre Aktivitäten analysiert werden. Kritische Prozesse können z. B. Systemprozesse oder Programme, die Verbindungen ins Internet aufbauen, sein. Es sollte auch beobachtet werden, welche Sub-Prozesse von diesen Prozessen gestartet werden.

**Selbsttest**

Das Viren-Schutzprogramm muss in der Lage sein, sich selbst bei Installation, Start und im weiteren Betrieb auf Unversehrtheit zu überwachen. Das Programm muss seine eigene Integrität feststellen, bevor Suchfunktionen ausgeführt werden. Um die Tarn-Mechanismen von Schadprogrammen unwirksam machen zu können, muss das Viren-Suchprogramm außerdem auch den Systemspeicher auf bekannte, residente Schadprogramme kontrollieren, bevor es mit der Durchsuchung von Dateien beginnt.

**Signatur-Erkennung**

Viren-Schutzprogramme nutzen verschiedene Methoden, um Schadprogramme zu entdecken. Die bekannteste und wichtigste Methode ist die "Signatur-Erkennung", bei der Schadprogramme an typischen Code-Sequenzen ("Signaturen") erkannt werden. Die Hersteller beobachten die Szene und erstellen möglichst schnell, nachdem ein neues Schadprogramm aufgetaucht ist, eine Signatur aus typischen Codezeilen.

Ein Nachteil der Signatur-Erkennung ist, dass ein Schadprogramm innerhalb des Zeitraums bis zur Auslieferung einer passenden Signatur auf diesem Weg nicht entdeckt werden kann. Schadprogramme, die nicht bekannt werden, können somit niemals mittels Signatur-Erkennung aufgespürt werden.

Trotz dieser immanenten Schwäche sollte die Signatur-Erkennung von einem Viren-Schutzprogramm in jedem Fall beherrscht werden.

**Heuristische Suche**

Um den Zeitraum bis zur Auslieferung der entsprechenden Signaturen für ein neues Schadprogramm zu überbrücken, sollten Viren-Suchprogramme zusätzlich über Mechanismen zur Erkennung noch nicht bekannter Schadprogramme verfügen. Bei einigen Viren-Suchprogrammen kann man durch die Betriebsart "heuristisches Suchen" neue, bisher noch nicht bekannte Schadprogramme aufspüren. Bei diesem Verfahren werden in den zu prüfenden Dateien verdächtige Befehlsfolgen gesucht, z. B. die Umleitung von Interrupts, das direkte Schreiben auf Sektor 1 eines Datenträgers (Boot-Sektor) und ähnliches.

Mit Hilfe der heuristischen Suche können selbst maßgeschneiderte Schadprogramme mit einer gewissen Wahrscheinlichkeit entdeckt werden. Diese Betriebsart eines Viren-Suchprogramms erfordert jedoch mehr Fachwissen vom Anwender, denn zum einen müssen Meldungen richtig interpretiert werden, andererseits sind Fehlalarme möglich.

**Erkennung von Schadprogrammen auch in komprimierten Dateien**

Das Viren-Schutzprogramm sollte Schadprogramme auch in komprimierten Dateien finden, wobei alle gängigen Komprimierungsfunktionen und Archivfor-

mate unterstützt werden sollten. Schadprogramme in geschachtelten Archivdateien sollten ebenfalls gefunden werden.

**Entfernung von Schadprogrammen**

Wünschenswert ist eine Funktionalität, die es erlaubt, erkannte Schadprogramme zu entfernen, ohne weitere Schäden an den Programmen oder Daten zu verursachen. Ob dies möglich ist, hängt jedoch von der jeweiligen Art der Schadprogramme ab. Es kann beispielsweise passieren, dass bereits Nutzdaten vernichtet wurden oder das Schadprogramm in einem abgesicherten Bereich läuft, auf den das Viren-Schutzprogramm keinen Zugriff hat.

**Überwachung von Aktiven Inhalten**

Sofern Aktive Inhalte (z. B. VBScript, JavaScript, ActiveX Controls oder Java Applets) auf den genutzten Systemen ausgeführt werden können, sollte das Viren-Schutzprogramm diese Inhalte auf Schadprogramme prüfen können.

**Schnittstelle zum E-Mail-Client**

Das Client-seitige Viren-Schutzprogramm sollte eine Schnittstelle für die E-Mail-Client-Software bereitstellen, so dass der E-Mail-Client das Schutzprogramm integrieren und für eine Prüfung auf Schadprogramme aufrufen kann.

**Weiterführende Informationen**

Das Viren-Schutzprogramm sollte Administratoren und Sicherheitsfachkräften für jedes gefundene Schadprogramm einen Link zu Seiten mit weiterführenden Informationen anzeigen (z. B. auf den Web-Seiten des Herstellers). Idealerweise können diese Angaben über ein Management-System abgerufen werden. Dort sollten zumindest folgende Informationen über das jeweilige Schadprogramm zu finden sein: Name, Beschreibung der Wirkungsweise, Verbreitungswege, mögliche Sofortmaßnahmen bei Befall, Maßnahmen zur Entfernung.

**Aktualisierung des Viren-Schutzprogramms**

Der Hersteller des Viren-Schutzprogramms muss eine regelmäßige Aktualisierung der Schadprogramm-Signaturen sowie der Such-Engine über das Internet anbieten. Die zeitlichen Abstände zwischen den Aktualisierungen sollten konfigurierbar sein und möglichst kurz gehalten werden. Die Signaturen müssen mindestens täglich auf den neuesten Stand gebracht werden.

Bei Verwendung eines nicht hinreichend aktuellen Programms oder einer veralteten Signatur (älter als 1 Tag) muss vom Viren-Schutzprogramm eine Warnung ausgegeben werden.

Bei konkreter Gefahr muss es möglich sein, ein sofortiges Update zu initiieren, um die aktuellsten Signaturen und Patches zu erhalten.

Werden Signaturen über Verbindungen verteilt, deren Übertragungskapazität knapp ist, ist es wichtig, dass die Signaturen inkrementell aktualisiert werden können. Der Betrieb sollte durch das Verteilen der Signaturen nicht mehr als notwendig beeinträchtigt werden.

Das Produkt muss über Funktionen verfügen, um die Integrität und Authentizität von heruntergeladenen Updates und Schadprogramm-Signaturen für das Viren-Schutzprogramm zu überprüfen. Es muss durch Mechanismen, die dem

Stand der Technik entsprechen, verhindert werden, dass gefälschte oder manipulierte Daten in das Viren-Schutzprogramm eingespielt werden.

**Betrieb in Netzen**

Bei einem Einsatz in Rechnernetzen sollte das Viren-Schutzprogramm eine zentrale Administration und Aktualisierung des Programms inklusive der Schadprogramm-Signaturen ermöglichen.

Ist keine allgemeine Software-Verteilungslösung vorhanden, sollte ein Produkt mit automatisierter Aktualisierung des Grundprogramms (Engine) gewählt werden.

Das Viren-Schutzprogramm sollte über ein zentrales Management verfügen, über das der Status der vorhandenen IT-Systeme ermittelt werden kann. Defekte Installationen, veraltete Engines, veraltete Signaturen und von Schadprogrammen befallene IT-Systeme müssen auf diese Weise zentral erkannt werden können. Der Zugriff auf infizierte Dateien der IT-Systeme sollte von zentraler Stelle aus möglich sein.

Die Möglichkeit zur individuellen Konfiguration des Clients durch den Benutzer muss abschaltbar sein.

**Meldewesen**

Gefundene Schadprogramme müssen auf dem System mit einer Bezeichnung und vollständiger Pfadangabe angezeigt werden.

Insbesondere bei Betrieb im Netz ist es wünschenswert, dass eine automatische E-Mail-Benachrichtigung bei aufgefundenen Schadprogrammen konfigurierbar ist.

**Protokollierungsfunktion**

Das Viren-Schutzprogramm sollte über eine Protokollierungsfunktion verfügen, die zumindest folgende Daten festhält:

- Versionsstand des Viren-Schutzprogramms und der Schadprogramm-Signaturen
- Datum und Uhrzeit der Überprüfung
- Ergebnis und Umfang der Überprüfung
- Anzahl und Identifikation der Dateien und Objekte, die nicht geprüft werden konnten

**Formale Anforderungen**

Neben den technischen und funktionalen Anforderungen spielen auch formale Forderungen eine Rolle. Um Planungssicherheit zu erreichen, sollte die Laufzeit des Vertrags mit dem Hersteller der Software zur Lieferung von Updates und aktuellen Schadprogramm-Signaturen genau geprüft werden. Weiterhin ist Support wichtig. Bei einem Support-Vertrag muss geklärt werden, welche Ansprechpartner in welchen Zeiträumen wie erreichbar sind und welche Zusatzkosten gegebenenfalls entstehen.

Prüffragen:

- Erfüllen die eingesetzten Viren-Schutzprogramme die Anforderungen, die aus dem Sicherheitskonzept zum Schutz vor Schadprogrammen resultieren?

- Sind die eingesetzten Viren-Schutzprogramme für die vorliegende Systemlandschaft geeignet?
- Unterstützen die eingesetzten Viren-Schutzprogramme die verwendeten Dateisysteme, Datenformate, Archivformate und Übertragungsprotokolle?
- Können die eingesetzten Viren-Schutzprogramme auch Aktive Inhalte auf Schadprogramme überprüfen?
- Verfügt das Client-seitige Viren-Schutzprogramm sowohl über eine speicherresidente Betriebsart, als auch über eine Betriebsart, bei der ein Suchlauf manuell gestartet werden kann?
- Können die eingesetzten Viren-Schutzprogramme ihre eigene Unversehrtheit überwachen?
- Geben die eingesetzten Viren-Schutzprogramme eine Warnung bei fehlenden Updates oder Verwendung einer veralteten Signatur (älter als 1 Tag) aus?
- Erhält der Anwender durch die eingesetzten Viren-Schutzprogramme weiterführende Informationen zu gefundenen Schadprogrammen?

# M 2.158 Meldung von Schadprogramm-Infektionen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Leiter IT

**Information der zentralen Ansprechpartner**

Bei Auftreten eines Schadprogramms muss vorrangig verhindert werden, dass weitere IT-Systeme infiziert werden. Generell sollte das jeweilige Viren-Schutzprogramm eine automatische Meldung von Schadprogramm-Infektionen unterstützen. Die automatische Meldung muss an einer zentralen Stelle angenommen und bearbeitet werden. Dabei sollten die zuständigen Mitarbeiter je nach Sachlage über das weitere Vorgehen entscheiden.

Unabhängig von einer automatischen Meldung muss sich jedoch auch der Benutzer an die ihm benannten Ansprechpartner wenden, wenn das Viren-Schutzprogramm eine mögliche Infektion anzeigt oder wenn anderweitig der Verdacht auf eine Schadprogramm-Infektion besteht. Hierbei ist es sinnvoll, dem Benutzer eine einheitliche Meldestelle für alle Arten von Sicherheitsvorfällen zur Verfügung zu stellen (z. B. ein User Help Desk, Support oder ähnliches). Ein Benutzer kann im Zweifelsfall nicht zuverlässig entscheiden, ob es sich wirklich um eine Schadprogramm-Infektion handelt, oder zum Beispiel um einen Hardware- oder Software-Defekt.

Die Ansprechpartner an der zentralen Meldestelle müssen entsprechend geschult sein und anhand der vorliegenden Informationen entscheiden, welche weiteren Schritte gegebenenfalls unternommen werden müssen (siehe hierzu auch B 1.8 *Behandlung von Sicherheitsvorfällen*). Wichtig ist in dem Zusammenhang auch, dass allen Mitarbeitern die Ansprechpartner und Meldewege bekannt sind (siehe M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

**Information weiterer Stellen durch den zentralen Ansprechpartner**

Neben eigenen Mitarbeitern oder Organisationseinheiten müssen unter Umständen auch Externe benachrichtigt werden, die eventuell durch die Schadprogramm-Infektion mit betroffen sind. Hierzu gehören insbesondere diejenigen, die die Schadprogramme möglicherweise weitergegeben oder erhalten haben.

Im Hinblick auf Sensibilisierung ist es unter Umständen sinnvoll, zusätzlich auch die nicht unmittelbar betroffenen eigenen Mitarbeiter zu informieren. Dabei sollten folgende Angaben zum Schadprogramm-Vorfall übermittelt werden:

- um welche Art von Schadprogramm es sich handelt,
- über welchen Infektionsweg das Schadprogramm eingedrungen ist (z. B. per E-Mail),
- ob das Schadprogramm sich durch bestimmte Symptome (spielt Melodie, zeigt Meldung an, etc.) bemerkbar macht,
- welcher Schaden durch das Schadprogramm angerichtet werden kann,
- welcher Schaden durch das Schadprogramm angerichtet wurde,
- welcher Schaden durch das Schadprogramm nicht angerichtet werden kann,
- welches Verhalten momentan angebracht ist und
- wie bzw. durch wen das Schadprogramm zu beseitigen ist.

Es müssen klare Regelungen getroffen werden, welche internen und externen Stellen im Fall einer Schadprogramm-Infektion informiert werden. Weitere Hinweise hierzu finden sich in M 6.65 *Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen*.

Prüffragen:

- Gibt es eine zentrale Meldestelle für Schadprogramm-Vorfälle?
- Wird automatisch eine Meldung an die zentralen Ansprechpartner gesendet, wenn die eingesetzten Viren-Schutzprogramme eine mögliche Infektion entdecken?
- Ist sichergestellt, dass die zentralen Ansprechpartner und Meldewege für Schadprogramm-Vorfälle allen Benutzern bekannt sind?
- Gibt es Regelungen, wann und in welchem Umfang externe Stellen bei Schadprogramm-Vorfällen informiert werden müssen?

# M 2.159 Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Für die mit Viren-Schutzprogrammen ausgestatteten IT-Systeme muss eine regelmäßige Aktualisierung des Viren-Schutzprogramms selbst (Engine) sowie der Schadprogramm-Signaturen erfolgen, damit neu aufgetretene Schadprogramme möglichst schnell und zuverlässig erkannt werden können.

Die zeitlichen Abstände zwischen den Aktualisierungen sollten dabei möglichst kurz gehalten werden. Die Häufigkeit von qualitätsgesicherten Signatur-Updates muss dabei dem aktuellen Stand der Technik entsprechen. Mindestens sollten die Signaturen einmal pro Tag aktualisiert werden. Bei Auftreten einer konkreten Gefahr (beispielsweise einer entsprechenden Viren-Warnung des BSI) ist ein sofortiges Update zu initiieren, um die aktuellsten Signaturen und Patches zu erhalten.

Bei der Aktualisierung der Viren-Schutzprogramme und Signaturen ist besonders darauf zu achten, dass auch Rechner, die keiner einzelnen Person zugeordnet oder nicht vernetzt sind, ebenfalls mit Updates versorgt werden.

Viren-Schutzprogramme müssen getestet und freigegeben werden, bevor sie erstmalig im Wirkbetrieb eingesetzt werden (siehe auch M 2.83 *Testen von Standardsoftware*).

Eine Überprüfung und Erprobung von Signatur-Updates wird aufgrund der Häufigkeit solcher Updates im Regelfall nicht möglich sein. Allenfalls können die Signatur-Updates auf einem gesonderten, der Standard-Installation entsprechenden IT-System grob auf mögliche Unverträglichkeiten getestet werden. In Bezug auf die Signatur-Updates ist deshalb der Kunde weitgehend auf die Qualitätssicherung durch den Software-Hersteller angewiesen. Hilfreich sind bereits in Viren-Schutzprogramme eingebaute Funktionen, die eine Rückkehr zu einer älteren Patch-Version des Programms oder älteren Schadprogramm-Signaturen erlauben.

Auch Updates für das Viren-Schutzprogramm selbst (Engine) erscheinen meist so häufig, dass ein ausführlicher Test jedes einzelnen Updates nicht realistisch ist. Bei der Installation von Programm-Updates ist jedoch darauf zu achten, dass die bestehende Konfiguration des Viren-Schutzprogramms nicht zum Nachteil verändert wird. So könnte beispielsweise durch ein Update ein zuvor residentes Viren-Schutzprogramm in einen Offline-Modus geschaltet werden.

Die Aktualisierung der Viren-Schutzprogramme und der Schadprogramm-Signaturen muss in das bestehende Patch- und Änderungsmanagement der Institution integriert werden. Bei den Aktualisierungen der Viren-Schutzprogramme und der Schadprogramm-Signaturen handelt es sich in der Regel um Standard-Änderungen, die nicht den vollständigen Patch- und Änderungsprozess durchlaufen müssen (siehe M 3.66 *Grundbegriffe des Patch- und Änderungsmanagements*).

Prüffragen:

- Werden Updates für die Viren-Schutzprogramme zeitnah eingespielt?
- Wird mindestens einmal pro Tag geprüft, ob Updates für die Schadprogramm-Signaturen verfügbar sind, und werden diese Updates unverzüglich eingespielt?
- Ist sichergestellt, dass die Updates für Viren-Schutzprogramme und für Schadprogramm-Signaturen auf allen IT-Systemen eingespielt werden, auf denen das entsprechende Viren-Schutzprogramm installiert ist?
- Wird die Konfiguration des Viren-Schutzprogramms nach dem Einspielen von Engine-Updates auf Veränderungen überprüft?
- Ist die Aktualisierung der Viren-Schutzprogramme und der Schadprogramm-Signaturen in das bestehende Patch- und Änderungsmanagement integriert?

# M 2.160 Regelungen zum Schutz vor Schadprogrammen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um einen effektiven Schutz vor Schadprogrammen zu erreichen, müssen über den Einsatz von technischen Sicherheitsmaßnahmen hinaus auch organisatorische und personelle Regelungen getroffen werden. Die wichtigsten Aspekte, die dabei berücksichtigt werden sollten, sind im Folgenden zusammengefasst:

- Alle Benutzer und Administratoren müssen für die Problematik der Schadprogramme sensibilisiert und hinsichtlich der einzuhaltenden Sicherheitsmaßnahmen zielgruppengerecht geschult werden.
- Die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Schutz vor Schadprogrammen müssen eindeutig geregelt sein. Dies betrifft insbesondere die Administratoren, die Benutzer, das IS-Management-Team und die zentralen Ansprechpartner für das Thema Schadprogramme.
- Es müssen Regelungen zum Umgang mit Software und IT-Systemen aufgestellt werden.
- Es muss geregelt werden, wie Sicherheitsvorfälle und insbesondere auch Schadprogramm-Infektionen an die zuständigen Stellen gemeldet werden (siehe M 2.158 *Meldung von Schadprogramm-Infektionen*).
- Um Schadprogramme bei Datenträgeraustausch und Datenübertragung rasch erkennen zu können und das Risiko einer Weiterverbreitung zu minimieren, muss festgelegt werden, dass bei Datenträgeraustausch und Datenübertragung eine Überprüfung auf Schadprogramme durchzuführen ist.
- Es müssen Regelungen getroffen werden, wie im Fall einer Infektion durch Schadprogramme verfahren wird. Insbesondere muss festgelegt werden, welche Personen und Institutionen in einem solchen Fall informiert werden müssen (siehe M 6.23 *Verhaltensregeln bei Auftreten von Schadprogrammen*).
- Auf IT-Systemen, auf denen kein residentes Viren-Schutzprogramm installiert ist, muss ersatzweise regelmäßig ein Viren-Schutzprogramm gestartet werden (siehe M 4.3 *Einsatz von Viren-Schutzprogrammen*).

Alle Mitarbeiter müssen in die Regelungen, die jeweils für sie gelten, eingewiesen werden.

Die Einhaltung der Regelungen sollte regelmäßig und stichprobenartig überprüft werden, um Abweichungen erkennen und gegebenenfalls darauf reagieren zu können.

Prüffragen:

- Sind die notwendigen Regelungen zum Schutz vor Schadprogrammen getroffen?
- Sind die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Schutz vor Schadprogrammen eindeutig geregelt?
- Sind die jeweils betroffenen Personen mit den für sie geltenden Regelungen zum Schutz vor Schadprogrammen vertraut?
- Wird die Einhaltung der Regelungen zum Schutz vor Schadprogrammen regelmäßig und stichprobenartig überprüft?

# M 2.161 Entwicklung eines Kryptokonzepts

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Unternehmen und Behörden sind mittlerweile zunehmend von ihrer informationstechnischen Infrastruktur abhängig. Aus diesem Grund sind Sicherheitsdienste erforderlich und in ein Gesamtsystem zu integrieren, die über die bloße Verschlüsselung hinausgehen.

Aufgrund der Vielfalt kryptographischer Problemstellungen und unterschiedlicher Einflussfaktoren gibt es auch vielfältige Lösungsansätze und Realisierungsmöglichkeiten. Man kann nicht davon ausgehen, dass es *eine* Lösung gibt, die alle Sicherheitsprobleme in Rechnernetzen und/oder Kommunikationssystemen beseitigen kann. Vielmehr kommt es auf ein abgestimmtes Zusammenspiel passend ausgewählter Komponenten an, um den benötigten Grad an Sicherheit zu erreichen. Daher ist es erforderlich, ein Kryptokonzept zu entwickeln, das in das Sicherheitskonzept der Behörde bzw. des Unternehmens integriert wird.

Die Auswahl geeigneter kryptographischer Komponenten muss dabei auf diesem Konzept basieren. Dabei ist das Schlüsselmanagement ein kritisches Element im gesamten Kryptokonzept. Konzepte und Lösungsansätze können nur dann erfolgreich erarbeitet und gezielt umgesetzt werden, wenn deutlich wird, welche speziellen Sicherheitsfunktionalitäten bzw. Sicherheitsdienste benötigt werden. Darüber hinaus gibt es eine Reihe systemrelevanter Fragestellungen und Aspekte, die nicht speziell in den Bereich der Sicherheitstechnik fallen. Dies umfasst z. B. Performanceanforderungen, Systemanbindungs- oder Interoperabilitäts- und Standardkonformitätsanforderungen.

Abbildung: Sichtweisen und Aspekte

In vernetzten IT-Infrastrukturen ist es nicht mehr ausreichend, die Sicherheit einer einzelnen Domäne zu gewährleisten. Vielmehr muss die Sicherheit *aller* beteiligten Endeinrichtungen und Übertragungssysteme aufeinander abgestimmt werden. Diese Abstimmung gestaltet sich insbesondere in solchen Fällen als besonders schwierig, in denen es sich nicht nur um vernetzte Einrichtungen innerhalb *einer* organisatorischen Einheit (z. B. LAN-Umgebung), sondern um einen Verbund von IT-Installationen unterschiedlicher Zuständigkeits- und Anwendungsbereiche handelt.

Der Einsatz - aber auch die Funktionalität und technologische Ausgestaltung - eines IT-Sicherheitssystems wird von zahlreichen Einflussfaktoren bestimmt, wie z. B. Lokalisierung, Sicherheitsniveau, Häufigkeit und Umfang der Anwendung, die für das Sicherheitsmanagement wichtige Rahmen- und Entschei-

dungsbedingungen darstellen. Des weiteren sind die technischen Möglichkeiten für die Realisierung und Gestaltung eines Sicherheitssystems vielfältig, z. B. integriert in einer Applikation auf dem Arbeitsplatzrechner, in einer Firewall oder als Spezialkomponente für Netzkomponenten wie Switch oder Router. Ein erschwingliches Preisniveau für ein Kryptoprodukt ist nur durch eine querschnittliche Nutzbarkeit zu erzielen. Hier spielen z. B. eine standardisierte Systemanbindung, einheitliche Einsatzbedingungen etc. eine wichtige Rolle. Ein letzter Punkt betrifft das Zusammenwirken der Sicherheitsdienste auf unterschiedlichen Protokollschichten. Die Sicherheitsdienste der höheren Protokollschichten (nach OSI-Referenzmodell) schützen in aller Regel nur dann ausreichend, wenn die unteren Schichten ebenso einen Schutz bieten (siehe M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*).

Des Weiteren ist die Definition einer organisationseigenen Kryptopolitik wichtig. Dabei muss aus Sicht des Managements geklärt werden,

- welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau es zu erreichen gilt,
- welches Budget und wie viel Personal zur Verfügung stehen, um die geplanten Sicherheitsmechanismen einzurichten und - ganz wichtig - auch den Betrieb zu gewährleisten,
- welche Systemanbindung angestrebt wird bzw. welche Einsatzbedingungen für Sicherheitskomponenten vorherrschen,
- welcher Funktions- und Leistungsumfang anzupeilen ist und
- wer letztendlich die Verantwortung übernimmt.

Im Kryptokonzept ist außerdem der technische bzw. organisatorische Einsatz der kryptographischen Produkte zu beschreiben, also z. B.

- wer welche Zugriffsrechte erhält,
- welche Dienste remote angeboten werden,
- wie die Verwaltung von Passwörtern und Schlüsseln bezüglich Gültigkeitsdauer, Verwendung von Zeichen, Länge, Vergabe gehandhabt werden soll,
- ob, wann und wie die Daten verschlüsselt oder signiert werden müssen,
- wer mit wem kryptographisch gesichert bzw. ungesichert kommunizieren darf,
- wer bestimmte Rechte vergeben darf, usw.

In Abhängigkeit von den systemtechnischen Rahmenbedingungen bezüglich

- des zu betrachtenden Datenvolumens und der Zeitabhängigkeit,
- der Verfügbarkeitsanforderungen und Gefährdungslage,
- Art und Häufigkeit der zu schützenden Anwendungen etc.

können darauf basierend geeignete Realisierungsmöglichkeiten analysiert und für konkrete Einsatzbereiche wie z. B. einen PC-Arbeitsplatz, im LAN-Bereich oder in Verbindung mit einer TK-Anlage konzipiert und technisch ausgestaltet werden. Nur aufgrund einer solch ganzheitlichen Betrachtungsweise gelingt es, Entscheidungsgrundlagen und -bedingungen für kryptographische Produkte zusammenzutragen, deren Einsatz bzw. Verwendung sowohl sicherheitstechnisch angemessen als auch wirtschaftlich vertretbar ist. Es sollte jedoch darauf hingewiesen werden, dass die vorgenommene Einteilung keinesfalls zwingend oder von grundsätzlicher Bedeutung, sondern bestenfalls hilfreich ist. Wesentlich ist nur, dass der Fragenumfang die Vorstellung nach einer möglichst umfassenden Klärung der Ausgangslage konsequent widerspiegelt. Natürlich ergeben sich in der Praxis zwischen einigen Fragestellungen bzw. Antworten Wechselwirkungen und Abhängigkeiten, die im allgemeinen allerdings zur Vervollständigung des Gesamtbildes beitragen.

Die diversen Einflussgrößen für den Einsatz kryptographischer Verfahren sind zu bestimmen und nachvollziehbar zu dokumentieren (siehe M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*). Anschließend muss eine geeignete Verfahrensweise für ihren Einsatz entwickelt und dokumentiert werden. Zum Abschluss muss durch die Behörden- bzw. Unternehmensleitung die Durchführung angeordnet werden.

Die Ergebnisse sollten aktualisierbar und erweiterbar im Kryptokonzept niedergelegt werden. Ein möglicher Aufbau eines Kryptokonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

**Inhaltsverzeichnis Kryptokonzept**

- **Definitionen**
  - Kryptographische Verfahren
  - ...
- **Gefährdungslage zur Motivation**
  - Abhängigkeit der Institution vom Datenbestand
  - Typische Gefährdungen wie ...
  - Institutionsrelevante Schadensursachen
  - Schadensfälle im eigenen Haus
- **Festlegung einer organisationsinternen Sicherheitspolitik**
  - Festlegung von Verantwortlichkeiten
  - Zielsetzung, Sicherheitsniveau
- **Einflussfaktoren**
  - Identifikation der zu schützenden Daten
  - Vertraulichkeitsbedarf der Daten
  - Integritätsbedarf der Daten
  - Verfügbarkeitsanforderungen an die Daten
  - Anforderungen an die Performance
  - Schlüsselverteilung
  - Datenvolumen
  - Art der Daten (lokal / verteilt (LAN/WAN))
  - Art der Anwendungen, bei denen kryptographische Verfahren zum Einsatz kommen sollen
  - Häufigkeit des Einsatzes des kryptographischen Verfahrens
  - Anforderungen an die Widerstandsfähigkeit der Algorithmen bzw. Verfahren (Manipulationsresistenz)
  - Wiederherstellbarkeit der gesicherten Daten
  - Personalaufwand
  - Erforderliche Funktionalität
  - Kosten einschließlich Folgekosten (Wartung, Administration, Updates, ...)
  - Kenntnisse/datenverarbeitungsspezifische Qualifikationen der IT-Benutzer
- **Festlegung des Einsatzes**
  - Art der kryptographischen Verfahren
  - Einsatzbedingungen an die kryptographischen Produkte
  - Häufigkeit und Zeitpunkt des Einsatzes
  - Benennung der Verantwortlichen
  - Festlegung der organisatorischen Regelungen
  - Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
  - Dokumentation der Einsatzbedingungen / Konfiguration

  - Interoperabilität, Standardkonformität, Investitionsschutz
- **Schlüsselmanagement**

Einzelne Punkte dieses Konzepts werden in den Maßnahmen M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*, M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*, M 2.166 *Regelung des Einsatzes von Kryptomodulen* etc. näher ausgeführt.

Bei der Erstellung eines Kryptokonzepts handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Kryptokonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden.

Prüffragen:

- Existiert ein aktuelles Kryptokonzept? Ist das Kryptokonzept in das Sicherheitskonzept der Institution integriert?
- Ist das Kryptokonzept in das Sicherheitskonzept der Institution integriert?
- Wird im Kryptokonzept der technische und organisatorische Einsatz von kryptographischen Produkten beschrieben?
- Sind sämtliche relevanten IT-Komponenten und Kommunikationsverbindungen im Kryptokonzept aufgeführt?
- Wird das Kryptokonzept regelmäßig den aktuellen Gegebenheiten angepasst?

# M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Verantwortliche der einzelnen Anwendungen

Um bei der Verarbeitung und Übertragung sensitiver Informationen zu realistischen, verlässlichen und anwendungsgerechten Bedarfsanforderungen und Rahmenbedingungen für den Einsatz kryptographischer Verfahren und Produkte zu kommen, müssen zunächst die schützenswerten Daten identifiziert und bewertet werden.

**Identifikation der zu schützenden Daten**

Zunächst muss festgestellt werden, für welche Aufgaben kryptographische Verfahren eingesetzt werden sollen und welche Daten damit gesichert werden sollen. Der Einsatz kryptographischer Verfahren kann aus verschiedenen Gründen erforderlich sein (siehe auch M 3.23 *Einführung in kryptographische Grundbegriffe*):

- zum Schutz der Vertraulichkeit bzw. der Integrität von Daten,
- zur Authentisierung,
- für Sende- oder Empfangsnachweise.

Je nach Einsatzzweck können verschiedene kryptographische Methoden wie z. B. Verschlüsselung oder Hashverfahren sinnvoll sein. Die typischen Einsatzfelder für kryptographische Verfahren sind:

- lokale Verschlüsselung,
- Kommunikationssicherung, auf Anwendungsebene bzw. auf Übertragungsebene,
- Authentikation,
- Nichtabstreitbarkeit,
- Integrität.

Im Folgenden werden einige Beispiele aus den verschiedenen typischen Einsatzfeldern für kryptographische Verfahren gegeben:

- Auf einer PC-Festplatte befinden sich Daten, die vor unbefugtem Zugriff durch Verschlüsselung geschützt werden sollen.
- Es sollen Informationen über Telefon, Fax oder Datennetze weitergegeben werden, z. B. sollen sie per E-Mail oder per Datenträgeraustausch versandt werden.
- Die zu schützenden Informationen sind nicht unter alleiniger Kontrolle der verantwortlichen Organisationseinheit (LAN führt durch Gebäudeteile, die von Fremdfirmen benutzt werden; ein Server mit Personaldaten wird durch Mitarbeiter betreut, die nicht zum Personalreferat gehören).
- Remote-Zugriffe sollen durch eine starke Authentisierung abgesichert werden.
- Bei E-Mails soll zweifelsfrei feststellbar sein, wer die Absender waren und ob die Inhalte unverändert übertragen wurden.

Um festzustellen, welche kryptographischen Verfahren bzw. Produkte benötigt werden und welche Daten damit zu schützen sind, sollte zunächst die aktuelle IT-Struktur ermittelt werden. Ermittelt werden sollte,

- welche IT-Systeme es gibt, auf denen Daten verarbeitet bzw. gespeichert (PCs, Laptops, Server, ...) oder mit denen Daten übermittelt werden (Bridge, Router, Gateway, Firewall, ...) und
- welche Übertragungswege es gibt. Dazu sollte die logische und physikalische Vernetzungsstruktur erfasst werden (siehe auch M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*).

**Schutzbedarf der Daten (Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit)**

Es sollten alle Anwendungen bzw. Daten ermittelt werden, bei denen ein besonderer Anspruch an Vertraulichkeit, Integrität, Authentizität bzw. Nichtabstreitbarkeit besteht. Allerdings werden nicht nur für IT-Systeme, Anwendungen oder Informationen mit höherem Schutzbedarf kryptographische Produkte benötigt, sondern auch für solche mit mittlerem Schutzbedarf.

Beispiele für Daten mit besonderem Vertraulichkeitssanspruch sind

- personenbezogene Daten,
- Passwörter und kryptographische Schlüssel,
- vertrauliche Informationen, deren Veröffentlichung Regressforderungen nach sich ziehen könnte,
- Daten, aus denen ein Konkurrenzunternehmen finanzielle Gewinne ziehen könnte,
- Daten, ohne deren Vertraulichkeit die Aufgabenerfüllung gefährdet ist (z. B. Ermittlungsergebnisse, Standortregister über gefährdete Pflanzen),
- Daten, deren Veröffentlichung eine Rufschädigung verursachen könnte.

**Hinweis:** Durch die Kumulation von Daten erhöht sich der Schutzbedarf einer Datensammlung, so dass eine Verschlüsselung erforderlich sein kann, auch wenn deren einzelne Datensätze nicht so sensitiv sind.

Beispiele für Daten mit besonderem Integritätsanspruch sind

- finanzwirksame Daten, durch deren Manipulation finanzielle Schäden entstehen können,
- Informationen, deren verfälschte Veröffentlichung Regressforderungen nach sich ziehen könnte,
- Daten, deren Verfälschung zu falschen Geschäftsentscheidungen führen kann,
- Daten, deren Verfälschung zu einer verminderten Produktqualität führen kann.

Ein Beispiel für Anwendungen mit besonderem Anspruch an Authentizität sind Remote-Zugriffe. Ein Beispiel für Daten mit besonderem Anspruch an Nichtabstreitbarkeit sind Bestellungen oder Reservierungen, bei denen der Besteller identifizierbar sein sollte.

Als Ergebnis der Schutzbedarfsfeststellung sollte festgelegt werden, welche Anwendungen oder Daten kryptographisch gesichert werden sollen. Diese Festlegung kann später noch verfeinert werden und sollte regelmäßig überarbeitet werden.

Als Resultat ergibt sich somit ein Überblick über alle Speicherorte und Übertragungsstrecken, die kryptographisch gesichert werden müssen. Damit erhält man praktisch eine IT-Landschaftskarte mit markierten Kryptobereichen.

**Bedarfs- und Anforderungsabfrage**

Als Hilfsmittel für eine derartige Bedarfserhebung bietet sich ein Fragenkatalog mit den in der Abbildung dargestellten Gliederungspunkten an. Dabei können die technischen, organisatorischen und wirtschaftlichen Aspekte jeweils in 4 weitere Unterkategorien aufgeteilt werden.

| **Technische Aspekte** | **Organisatorische Aspekte** | **Wirtschaftliche Aspekte** |
|---|---|---|
| Benutzerdienste und Anwendungen | Einsatzbereich | Rationalisierungsaspekte / Kosteneinsparungen |
| Nutzungsprofil | Migrationskonzept | Stückzahlen |
| Netzinfrastruktur | Zeitvorstellungen | Beschaffungskosten |
| IT-Endgerät | Betriebliche Rahmenbedingungen | Administrations- und Wartungsaufwendungen |

Tabelle: Gliederungsgesichtspunkte zur Erstellung eines Fragenkataloges

Bei den technischen Aspekten ist es unter "Benutzerdienste und Anwendungen" beispielsweise wichtig zu erfahren, ob vornehmlich Echtzeit- oder Nicht-Echtzeit-Daten betrachtet werden. In der Kategorie Nutzungsprofil ist zu erfragen, für welche Anwendungen und Daten kryptographische Verfahren eingesetzt werden sollen, z. B. für die externe Kommunikation oder für die kurzzeitige oder längerfristige Bearbeitung von VS-Daten. Weiterhin sind die Netzinfrastruktur und das Endgerät betreffende Informationen zu ermitteln, wie z. B. Anschlusskonfiguration.

Als organisatorische Aspekte sind der Einsatzbereich, d. h. Teilnehmer- oder Netzbereich; die Frage nach einem existierenden Migrationskonzept sowie die Zeitvorstellungen und betrieblichen Rahmenbedingungen des Endbenutzers zu betrachten.

Aus wirtschaftlicher Sicht sind die wesentlichen Punkte:

- Rationalisierungsaspekte, z. B. durch Einsatz eines Produktes mit transparenter Verschlüsselung statt manueller Ansteuerung,
- eine Abschätzung im Hinblick auf Stückzahlen und Beschaffungskosten sowie
- die zu erwartenden Administrations- und Wartungskosten.

Auf Basis dieser Abfrage kann ein möglichst praxisnahes Einsatz- und Anforderungskonzept erstellt werden, was dann als Ausgangspunkt für konkrete Realisierungsentscheidungen bzw. die Auswahl geeigneter Kryptokomponenten/-produkte (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*) dient.

Die hier vorgestellte Vorgehensweise soll dem Sicherheitsverantwortlichen helfen, den Einsatz und den Umfang einzusetzender Sicherheitstechnik in unterschiedlichen Systemlokalitäten, Netzübergängen und Endeinrichtungen festzustellen, zu bewerten und zu koordinieren. Ferner soll im Verlauf der Planungsphase durch die Ermittlung des notwendigen Schutzes (Schutzbedarf) die Frage nach Angemessenheit der Informationssicherheit beantwortet werden. Die skizzierte Vorgehensweise stellt einen pragmatischen Ansatz dar und berücksichtigt Sicherheitsaspekte in offenen, verteilten IT-Infrastrukturen, so wie sie sich vielerorts darstellen.

Die so betrachteten Sicherheitsinvestitionen müssen für den betroffenen Einsatzbereich wirtschaftlich vertretbar sein. Die Funktions- und Betriebsweise von realisierten Sicherheitsstrategien müssen den Erwartungen der Endbenutzer hinsichtlich der Flexibilität, Transparenz und Performance Rechnung tragen. Die geplanten und integrierten Sicherheitsdienste dürfen den Endbenutzer nicht über das notwendige Maß hinaus einschränken.

Prüffragen:

- Ist geklärt, für welche Aufgaben kryptographische Verfahren eingesetzt werden sollen und welche Daten damit geschützt werden sollen?
- Wurden die Anwendungen, IT-Systeme und Kommunikationsverbindungen ermittelt, die aufgrund ihres Schutzbedarfs kryptographisch abgesichert werden sollen?

# M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Verantwortliche der einzelnen Anwendungen

Bevor eine Entscheidung getroffen werden kann, welche kryptographischen Verfahren und Produkte eingesetzt werden sollen, müssen eine Reihe von Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren.

Für sämtliche in M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*festgelegten Speicherorte und Übertragungsstrecken sind folgende Einflussfaktoren zu ermitteln:

**Sicherheitsaspekte**

- Welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau gilt es zu erreichen?
- Welche kryptographischen Funktionen sind dafür notwendig (Verschlüsselung, Integritätsschutz, Authentizität und/oder Nichtabstreitbarkeit)?
- Angreiferpotential: Mit welchen Angreifern wird gerechnet (zeitliche und finanzielle Ressourcen, technische Fähigkeiten)?

Die Antworten auf diese Fragen ergeben sich aus M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*.

**Technische Aspekte**

Der Betrieb von weitverzweigten IT-Infrastrukturen mit ihrer Vielzahl von Einzelkomponenten und Spezialeinrichtungen (Netzknoten, Server, Datenbanken, etc.) macht ein ebenfalls weitverzweigtes Sicherheitssystem mit mehreren Funktionseinheiten (Sicherheitsmanagement, Sicherheitsserver, Sicherheitsanwenderkomponente, etc.) erforderlich. In der Regel müssen dabei Systembetrachtungen angestellt werden, die nicht nur auf die eigentlichen Funktionalitäten abzielen, sondern auch bauliche und organisatorische Aspekte einbeziehen. Auch in Bezug auf die konkrete technische Platzierung von Sicherheitskomponenten sowie deren Integration in Nicht-Sicherheitskomponenten gilt es zu differenzieren, da dies einen unmittelbaren Einfluss auf die Implementierung der Sicherheitsfunktionen, auf die notwendige Unterstützung durch die Betriebssysteme, die Aufwände und den Kostenfaktor und nicht zuletzt auf die erreichbare Sicherheit hat. Ganz entscheidend für die Sicherheitsbewertung ist der Umstand, an welchen geographischen Lokalitäten und in welchen Ebenen des Protokollstacks die jeweiligen Sicherheitsdienste realisiert sind und wie diese in die Prozesse des zu schützenden IT-Systems eingebunden sind. Somit ergeben sich als Fragen:

- Umfeldschutz: Welchen Schutz bietet das Umfeld, beispielsweise durch infrastrukturelle Sicherheitsmaßnahmen wie Zutrittskontrolle, organisatorische, personelle und technische Maßnahmen?
- IT-Systemumfeld: Welche Technik wird eingesetzt, welche Betriebssysteme, etc.?
- Datenvolumen: Welches Datenvolumen ist zu schützen?
- Häufigkeit: Wie häufig besteht Verschlüsselungsbedarf?

- Performance: Wie schnell müssen kryptographische Funktionen arbeiten (Offline, Online-Rate)?

**Personelle und organisatorische Aspekte**
- Benutzerfreundlichkeit: Benötigen die Benutzer für die Bedienung kryptographische Grundkenntnisse? Behindert der Einsatz eines Kryptoprodukts die Arbeit?
- Zumutbarkeit: Wie viel Belastung durch zusätzliche Arbeit ist für Benutzer zumutbar (Arbeitszeit, Wartezeit)?
- Zuverlässigkeit: Wie zuverlässig werden die Benutzer mit der Kryptotechnik umgehen?
- Schulungsbedarf: Inwieweit müssen die Benutzer geschult werden?
- Personalbedarf: Ist zusätzliches Personal erforderlich, z. B. für Installation, Betrieb, Schlüsselmanagement?
- Verfügbarkeit: Kann durch den Einsatz eines Kryptoprodukts die Verfügbarkeit reduziert werden?

**Wirtschaftliche Aspekte**
- Finanzielle Randbedingungen: Wie viel darf der kryptographische Schutz kosten? Wie hoch sind die
  - einmaligen Investitionen,
  - laufenden Kosten, inklusive der Personalkosten,
  - Lizenzgebühren?
- Investitionsschutz: Sind die geplanten kryptographischen Verfahren bzw. Produkte konform zu bestehenden Standards? Sind sie interoperabel mit anderen Produkten?

**Key-Recovery**

Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind auch die damit geschützten Daten verloren, sofern die unverschlüsselten Daten nicht zusätzlich an anderer Stelle vorliegen. Viele Kryptoprodukte bieten daher Funktionen zur Datenwiedergewinnung für solche Fälle an. Bevor solche Funktionen eingesetzt werden, sollte man sich auch deren Risiken klar machen: Wenn dadurch vertrauliche Schlüssel wiederhergestellt werden können, muss sichergestellt sein, dass dies nur Berechtigte können. Wenn es möglich ist, ohne Wissen des Original-Schlüsselbenutzers auf dessen Daten zuzugreifen, hat dieser keine Möglichkeit, böswillige Manipulationen zu beweisen. Der Einsatz von Key-Recovery-Mechanismen führt auch häufig aufgrund des entgegengebrachten Misstrauens zu Vorbehalten innerhalb des eigenen Unternehmens bzw. Behörde, aber auch bei den Kommunikationspartnern. Bei der Datenübertragung sollte daher generell auf Key-Recovery verzichtet werden. Hierfür gibt es auch keine Notwendigkeit, da beim Schlüssel- oder Datenverlust diese einfach noch einmal ausgetauscht werden können. Bei der lokalen Speicherung von Daten sollte der Einsatz sorgfältig überlegt werden (siehe auch M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*). Unter den Hilfsmitteln zum IT-Grundschutz befindet sich ein Artikel zu Möglichkeiten und Risiken von Key-Recovery.

**Lebensdauer von kryptographischen Verfahren**

Kryptographische Verfahren und Produkte müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen. Die verwendeten Algorithmen können durch neue technische Entwicklungen, z. B. schnellere, billigere IT-Systeme, oder durch neue mathematische Erkenntnisse zu schwach werden. Die eingesetzten kryptographischen Produkte können Implementierungsfehler aufweisen. Bereits bei der Auswahl kryptographischer Verfahren sollte daher eine zeitliche Grenze für deren Einsatz festgelegt wer-

den. Zu diesem Zeitpunkt sollte noch einmal gründlich überdacht werden, ob die eingesetzten Kryptomodule noch den erwarteten Schutz bieten.

**Gesetzliche Rahmenbedingungen**

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Daher muss untersucht werden (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*),

- ob innerhalb der zum Einsatzgebiet gehörenden Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind (innerhalb Deutschland gibt es keinerlei Einschränkungen) und
- ob für infrage kommende Produkte Exportbeschränkungen beachtet werden müssen.

Es gibt allerdings nicht nur Maximalanforderungen, sondern auch Minimalanforderungen an die verwendeten kryptographischen Algorithmen oder Verfahren. So müssen z. B. bei der Übermittlung von personenbezogenen Daten Verschlüsselungsverfahren mit ausreichender Schlüssellänge eingesetzt werden.

**Technische Lösungsbeispiele:**

Im Folgenden finden sich einige Anwendungsbeispiele zu den verschiedenen Einsatzfeldern für kryptographische Verfahren.

**Beispiel 1: Festplattenverschlüsselung**

Die auf einem Speicherbaustein, z. B. einer Festplatte oder einem Flashspeicher eines stationären oder mobilen Clients (wie z. B. ein PDA, Smartphone, Tablet, Laptop oder PC) gespeicherten sensiblen Daten sollen so geschützt werden, dass

- der Computer nur von autorisierten Benutzern gebootet werden kann,
- nur autorisierte Benutzer Zugriff auf die gespeicherten Daten erhalten,
- die gespeicherten Daten bei abgeschaltetem Computer - auch im Falle des Diebstahls - hinreichend vor Kenntnisnahme durch Unberechtigte geschützt sind.

Dabei soll der Computer gegen die folgenden Bedrohungen geschützt werden:

- Unbefugte Kenntnisnahme der gespeicherten Daten
- Manipulation der gespeicherten Daten
- Manipulation des Kryptosystems

Im Vordergrund soll hier der Schutz der Vertraulichkeit stehen.

Bei Diebstahl bzw. Verlust des Computers oder des Speicherbausteins steht dem Angreifer sehr viel Zeit für die unbefugte Kenntnisnahme zur Verfügung. Eine Schutzmaßnahme muss auch bei solchen Langzeitangriffen die Vertraulichkeit der gespeicherten Daten gewährleisten.

Als Schutzmaßnahme soll daher ein Produkt mit Boot-Schutz und Festplattenverschlüsselung eingesetzt werden. Auf dem Markt sind verschiedene Lösungen verfügbar.

Grundsätzlich sollte im eingesetzten Produkt ein etablierter Kryptoalgorithmus (z. B. AES) mit einer hinreichenden Schlüssellänge (128 Bit oder mehr) in einem verlässlichen Betriebsmodus (z. B. CBC, OFB oder GCM, kein XOR) implementiert sein.

Zum Einsatz kann entweder eine Verschlüsselungs-Software (Lösung A), eine Hardware-Verschlüsselungskomponente (Lösung B) oder eine Kombination aus Hardware- und Software-Komponente (Lösung C) kommen. Lösung C wird typischerweise aus einer Verschlüsselungs-Software in Kombination mit einem Hardware-Token, z. B. einer Chipkarte oder einem USB-Stick, zur Zugangskontrolle bestehen. Welche Lösung gewählt werden sollte, hängt von verschiedenen Entscheidungskriterien ab:

- Sicherheit
  Je nachdem, auf welcher Betriebssystem-Plattform Verschlüsselung betrieben wird, stößt eine Software-Lösung (Lösungen A oder C) unweigerlich an Grenzen. Kann kein sicheres Betriebssystem mit strikter Task- und Speicherbereichs-Trennung vorausgesetzt werden (bisher ist das bei keinem Betriebssystem sicher nachgewiesen!), muss der während der Ver- bzw. Entschlüsselung verwendete Schlüssel zumindest kurzzeitig ungeschützt im Arbeitsspeicher des Computers gehalten werden. Die Vertraulichkeit des Schlüssels ist somit möglicherweise nicht mehr sichergestellt. Hardware-Verschlüsselungskomponenten (Lösung B) können eventuell mehr bieten. Der Schlüssel kann in die Hardware-Komponente geladen und dort - gegen Auslesen gesichert - gespeichert werden. Der Schlüssel wird die Hardware-Komponente nicht mehr verlassen und ist vor Ausspähversuchen geschützt. Er kann nur durch berechtigte Benutzer mittels Besitz und Wissen (z. B. Chipkarte und Passwort) aktiviert werden. Wichtig sind weitere Aspekte, wie die Art und Weise der Einbindung in das Computer-System. Die Verschlüsselungs-Hardware sollte idealerweise so eingebunden werden, dass sie die gesamte Festplatte zwangsweise verschlüsselt und durch Angriffe nicht unbemerkt abgeschaltet bzw. umgangen werden kann. Werden im Gegensatz dazu lediglich einzelne Dateien verschlüsselt, besteht die Gefahr, dass die Inhalte dieser Dateien unkontrollierbar zumindest teilweise zusätzlich im Klartext auf die Festplatte geschrieben werden (z. B. in den Auslagerungsdateien verschiedener Betriebssysteme oder in Backup-Dateien).
- Performance (Geschwindigkeit der ausführbaren Programme)
  Software-Verschlüsselung nutzt die Systemressourcen des Computers, belastet also die CPU und benötigt Arbeitsspeicher. Vor allem bei der Verschlüsselung der gesamten Festplatte kann die Performance des Computers sinken. Hardware-Komponenten mit eigenem Prozessor können die Verschlüsselung ohne Belastung der CPU und somit ohne nennenswerten Performanceverlust durchführen. Hier ist je nach Bauart die Durchsatzrate der verwendeten Verschlüsselungs-Hardware mitentscheidend.
- Organisatorischer und personeller Aufwand (Administration, Schlüsselmanagement, Schulung etc.)
  Der organisatorische bzw. personelle Aufwand ist von der Umsetzung der Sicherheitspolitik und dem "Komfort" der Verschlüsselungskomponenten abhängig. Generelle Entscheidungskriterien für oder gegen eine der drei Lösungen können nicht allgemeingültig formuliert werden.
- Wirtschaftlichkeit (Anschaffung, Schulungs-/Administrationskosten, ...)
  Eine allgemeine Aussage zur Wirtschaftlichkeit ist schwierig. Betrachtet man nur die Anschaffungskosten, so werden Software-Lösungen oft preiswerter sein als Hardware-Lösungen. Kalkuliert man dagegen auch die Schäden ein, die durch unzureichenden Schutz auf längere Sicht entstehen können, kann sich im Vergleich die Investition in sicherere und vielleicht teurere Lösungen lohnen. Wirtschaftliche Nachteile können u. U. durch Performanceverlust des Computer-Systems entstehen.
- Restrisiken (Betriebssystem, Kompromittierung des Festplattenschlüssels etc.)

Bei der Auswahl der geeigneten Verschlüsselungskomponente spielt die Restrisikobetrachtung eine wesentliche Rolle. Es stellen sich u. a. die Fragen:

- Welche Restrisiken können in Kauf genommen werden?
- Welche Restrisiken werden durch andere Maßnahmen (z. B. materielle oder organisatorische Maßnahmen) minimiert?

Es können sich durchaus mehrere tragbare Lösungsmöglichkeiten durch die Kombination verschiedener Maßnahmen ergeben.

**Beispiel 2: E-Mail-Verschlüsselung**

Werden sensible Informationen (z. B. Firmengeheimnisse) per E-Mail über ungesicherte Netze ausgetauscht, sind Mechanismen zum Schutz der Vertraulichkeit und für die Gewähr der Authentizität von Nachrichten erforderlich.

Grundsätzlich bieten sich zwei Möglichkeiten, die sensiblen Daten zu schützen.

1. Die zu schützenden Informationen werden in einer Datei gespeichert, die Datei wird dann mit einem Dateiverschlüsselungsprogramm verschlüsselt und die verschlüsselte Datei wird der E-Mail als Anhang beigefügt. Der eigentliche Text der E-Mail bleibt dabei ungesichert.
2. Die gesamte E-Mail (Text und ggf. Anhänge) wird mithilfe eines speziellen E-Mail-Verschlüsselungsprogramms verschlüsselt.

Möglichkeit 2 setzt voraus, dass beim Benutzer ein E-Mail-Programm (z. B. Outlook, Kontact oder Thunderbird) installiert ist, welches die Einbindung eines E-Mail-Verschlüsselungsprogramms als Plugin ermöglicht. Im Falle, dass der Benutzer einen webbasierten E-Mail-Client verwendet, kommt nur Möglichkeit 1 in Frage.

Voraussetzung ist hierbei natürlich, dass nicht nur der Sender der E-Mail, sondern auch der Empfänger über ein kompatibles Verschlüsselungsprogramm verfügt.

Beide genannten Möglichkeiten bieten Ende-zu-Ende-Sicherheit zwischen Sender und Empfänger. Der Sender entscheidet dabei in der Regel, welche Informationen er für sensibel und schützenswert hält. In vielen Fällen (je nach eingesetztem Verschlüsselungsprogramm) sind Sender und Empfänger auch für das Schlüsselmanagement verantwortlich. Die Entscheidung des Senders, welche Daten er verschlüsselt und das Schlüsselmanagement werden ihm abgenommen, wenn grundsätzlich alle E-Mails, die beispielsweise zwischen den Liegenschaften einer Institution versendet werden, automatisiert vom E-Mail-Server ver- bzw. entschlüsselt werden. Das Schlüsselmanagement beschränkt sich dann personell auf die IT-Administratoren der Institution, und die E-Mails sind lediglich zwischen Sender und E-Mail-Server bzw. E-Mail-Server und Empfänger ungeschützt, also auf Strecken, die im Allgemeinen innerhalb einer Liegenschaft und somit in einem gesicherten Bereich verlaufen.

Selbstverständlich sind beide Methoden (Ende-zu-Ende-Verschlüsselung und automatisierte Verschlüsselung zwischen den E-Mail-Servern) miteinander kombinierbar und erhöhen so die Sicherheit.

Werden die E-Mails mittels eines Datei- oder eines E-Mail-Verschlüsselungsprogramms gesichert, stellt sich die Wahl zwischen einem Programm, welches mit symmetrischen oder mit asymmetrischen Mechanismen arbeitet (siehe M 3.23 *Einführung in kryptographische Grundbegriffe*). In jedem Fall sollte ein Produkt eines namhaften Herstellers verwendet werden, welches mit

etablierten und (auch aus Interoperabilitätsgründen) standardisierten Verfahren arbeitet. Auch Open-Source-Produkte bieten häufig eine gute Alternative. Produkte, die vollmundig mit "beweisbarer hunderprozentiger Sicherheit" werben, sind meist mit Vorsicht zu genießen.

Beide Arten, symmetrisch und asymmetrisch, bieten Vor- und Nachteile.

**Verschlüsselungsprogramme mit symmetrischen Mechanismen**

Ein symmetrisches Verfahren bietet sich beispielsweise an, wenn sensible Daten innerhalb eines kleinen Arbeitskreises ausgetauscht werden sollen. Der notwendige Schlüssel kann etwa auf einer konstituierenden Sitzung des Arbeitskreises ad hoc erzeugt und an die Mitglieder verteilt werden - ein aufwändiges Schlüsselmanagement oder gar eine Public-Key-Infrastruktur (siehe unten) sind nicht notwendig. Keinesfalls darf ein symmetrischer Schlüssel per E-Mail versendet werden.

Wird der Schlüssel für ein symmetrisches Verfahren selbstständig, d. h. ohne Verwendung eines Zufallszahlengenerators erzeugt, ist zu beachten, dass für den Schlüssel ein wesentlich höheres Sicherheitsniveau als beispielsweise für ein Passwort beim Online-Banking notwendig ist, da es für den Schlüssel keinen Fehlbedienungszähler gibt und ein Angreifer, der in Besitz einer verschlüsselten Datei kommt, beliebig viele Versuche hat, den Schlüssel systematisch und automatisiert zu ermitteln.

Auch einige ZIP-Programme bieten ausreichend sichere Verschlüsselungsoptionen, allerdings gibt es auch ZIP-Programme mit schlecht implementierter oder unzureichender Verschlüsselung. Bevor ZIP-Programme zur Verschlüsselung von vertraulichen Informationen genutzt werden, sollte das Sicherheitsmanagement die Güte der verwendeten Kryptoverfahren überprüfen oder entsprechende Testberichte einholen.

**Verschlüsselungsprogramme mit asymmetrischen Mechanismen**

Der Vorteil von asymmetrischer gegenüber symmetrischer Verschlüsselung ist, dass der Schlüssel, der zum Verschlüsseln verwendet wird, nicht geheim gehalten zu werden braucht. Deshalb wird ein asymmetrisches Verfahren auch Public-Key-Verfahren und der Schlüssel zum Verschlüsseln auch "öffentlicher Schlüssel" genannt. Die öffentlichen Schlüssel können also ruhigen Gewissens per E-Mail versendet oder in einem Verzeichnis veröffentlicht werden. Auf diese Weise können also sogar persönlich nicht miteinander bekannte Personen vertraulich miteinander per E-Mail kommunizieren.

Allerdings muss sich der Versender einer E-Mail davon überzeugen, dass der Schlüssel, den er zum Verschlüsseln der E-Mail verwendet, tatsächlich der öffentliche Schlüssel des Empfängers ist, der öffentliche Schlüssel also authentisch ist.

Die Authentizität der öffentlichen Schlüssel kann beispielsweise durch eine Public-Key-Infrastruktur (PKI) gewährleistet werden. Bei einer PKI stellt eine vertrauenswürdige Stelle Zertifikate für die öffentlichen Schlüssel der Benutzer aus. Der Versender einer E-Mail würde dem öffentlichen Schlüssel des Empfängers nur dann trauen, wenn er ein gültiges Zertifikat besitzt. Das Ausstellen von Schlüsselzertifikaten durch die vertrauenswürdige Stelle ist unter Umständen mit zusätzlichen Kosten verbunden.

Steht keine PKI zur Verfügung oder gehören Sender und Empfänger unterschiedlichen PKIs an, muss sich der Sender auf andere Weise von der Echtheit des öffentlichen Schlüssels überzeugen. Eine Möglichkeit, dies zu tun, ist,

den Empfänger telefonisch zu kontaktieren und den sogenannten Fingerabdruck des Schlüssels (das ist ein kryptographischer Hashwert des Schlüssels) zu vergleichen. Der Fingerabdruck eines öffentlichen Schlüssels lässt sich mit den gängigen asymmetrischen Verschlüsselungsprogrammen am Bildschirm anzeigen. Hierzu ist es jedoch erforderlich, dass der Sender den Empfänger am Telefon (z. B. anhand der Stimme) eindeutig identifizieren kann.

Weit verbreitet sind folgende (nicht miteinander kompatible) Standards:

- OpenPGP ("Pretty Good Privacy") und
- S/MIME (Secure Multipurpose Internet Mail Extensions).

OpenPGP wird etwa vom kommerziellen Produkt PGP und vom Open-Source-Produkt GnuPG unterstützt.

**Authentizität der empfangenen E-Mail**

Symmetrische Mechanismen bieten in der Regel eine implizite Gewähr für die Authentizität der empfangenen Informationen, da eine sinnvoll zu entschlüsselnde E-Mail nur von demjenigen erzeugt werden konnte, der in Besitz des Schlüssels ist.

Bei Verwendung eines asymmetrischen Verfahrens hingegen liefert die Tatsache, dass eine E-Mail korrekt entschlüsselt werden konnte, keinen Hinweis auf die Authentizität des Absenders, denn der Schlüssel, den er zum Verschlüsseln verwendet hat, ist wie gesagt öffentlich. Somit kann jeder, der Zugang zum öffentlichen Schlüssel des Empfängers hat, der potenzielle Absender gewesen sein.

Aus diesem Grunde bieten asymmetrische Verfahren dem Sender zusätzlich die Möglichkeit, eine Datei bzw. eine E-Mail elektronisch zu signieren. Um die Signatur zu prüfen, benötigt der Empfänger einen öffentlichen Signaturschlüssel des Senders. (Der öffentliche Signaturschlüssel sollte sich nach Möglichkeit vom öffentlichen Verschlüsselungsschlüssel des Senders unterscheiden. Bei vielen Produkten sind jedoch Signatur- und Verschlüsselungsschlüssel identisch.) Um die Echtheit des Signaturschlüssels zu verifizieren, wird auch hier eine PKI benötigt, oder der Empfänger muss den Fingerabdruck des Signaturschlüssels mit dem Sender abgleichen.

Prüffragen:

- Wurden die Einflussfaktoren für den Einsatz kryptographischer Verfahren und Produkte ermittelt und dokumentiert?

# M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Auswahl eines kryptographischen Verfahrens zerfällt in die beiden Teilaufgaben

- Auswahl des kryptographischen Algorithmus und
- Auswahl einer technischen Realisierung.

Bevor Anwender sich auf bestimmte Verfahren festlegen, sollte sie genaue Vorstellungen davon haben, welche Anforderungen sie an Vertraulichkeit und Authentizität der bearbeiteten Daten in jedem "Punkt" seines informationsverarbeitenden Systems stellen.

**Auswahl von kryptographischen Algorithmen**

Bei der Auswahl von kryptographischen Algorithmen ist zunächst zu klären, welche Art kryptographischer Verfahren benötigt werden, also symmetrische, asymmetrische oder hybride Verfahren, und dann sind geeignete Algorithmen, also solche mit entsprechender Mechanismenstärke auszuwählen. Aktuelle Empfehlungen zur Auswahl kryptographischer Verfahren gibt das BSI in der technischen Richtlinie BSI TR 02102-1.

**Verschlüsselungsverfahren**

- symmetrische Verschlüsselung: Die Vor- bzw. Nachteile symmetrischer Verfahren sind in M 3.23 *Einführung in kryptographische Grundbegriffe* beschrieben. Geeignete Algorithmen sind z. B. AES-128, AES-192, AES-256
- asymmetrische Verschlüsselung: Die Vor- bzw. Nachteile asymmetrischer Verfahren sind ebenfalls in M 3.23 *Einführung in kryptographische Grundbegriffe* beschrieben. Geeignete Algorithmen sind z. B. RSA oder auf Elliptischen Kurven basierende Verschlüsselungsverfahren (zur Schlüssellänge siehe unten).

**Authentisierungsverfahren**

- Nachrichtenauthentisierung
  Zur Nachrichtenauthentisierung können verschiedene Verfahren eingesetzt werden, etwa ein Message Authentication Code (MAC) oder ein digitales Signaturverfahren. Der Einsatz eines MACs ist von Vorteil, wenn extrem hohe Durchsatzraten gefordert sind (oder nur eine geringe Rechenkapazität zur Verfügung steht) und das Risiko der Schlüsseloffenlegung auf beiden Seiten sehr gering ist. Der Einsatz eines digitalen Signaturverfahrens ist von Vorteil, wenn das Risiko der (Signatur-) Schlüsseloffenlegung auf einer Seite wesentlich höher ist als auf der anderen Seite; und in aller Regel geboten, wenn Verbindlichkeitsdienste verlangt werden. Es sei noch einmal bemerkt, dass für den Dienst Verbindlichkeit eine Infrastruktur vertrauenswürdiger Dritter vorhanden sein muss.
  Einer der bekanntesten MAC-Algorithmen ist die Verschlüsselung einer Nachricht mit DES oder einem anderen Block-Chiffrierverfahren im CBC- oder CFB-Mode.
  Dabei wird als MAC der letzte verschlüsselte Block an die Nachricht angehängt. Solche Varianten sind z. B. in den Normen, ISO 8731-1 oder ISO 9797 spezifiziert.
  Unter den Vorschlägen für Blockchiffren-basierte MAC-Konstruktionen, hat sich das von der amerikanischen NIST standardisierte Verfahren C-

MAC (ehedem OMAC1) als allgemein akzeptiertes MAC-Verfahren durchgesetzt. Daneben gibt es dedizierte MAC-Konstruktionen auf Basis von Hashfunktionen, hier ist an erster Stelle der weithin akzeptierte und verwendete HMAC aus dem RFC 2104 zu nennen.
Geeignete Algorithmen für Digitale Signaturen sind z. B. RSA, DSA (Digital Signature Algorithm) oder auf elliptischen Kurven basierende DSA-Varianten, z. B. ISO/IEC 15946-2, IEEE-Standard P1363, Abschnitt 5.3.4 ("DSA Version"). Genaueres kann dem von der Bundesnetzagentur jährlich herausgegebenen "Algorithmenkatalog" entnommen werden (siehe unten).
Von den hier genannten digitalen Signaturen sind die elektronischen Signaturen, wie sie in den EU-Richtlinien oder Rechtsvorschriften Deutschlands definiert sind, zu unterscheiden. Inwiefern die hier genannten digitalen Signaturen als elektronische Signaturen im Sinne dieser Rechtsnormen gewertet werden können, muss gesondert geprüft werden und ist nicht Gegenstand dieser Maßnahme.

- Authentisierung von Benutzern oder Komponenten
  Ein einfaches Verfahren zur Authentisierung ist eine Passwortabfrage. Werden die Passwörter dabei aber unverschlüsselt über ein Netz übertragen, können diese verhältnismäßig einfach mitgelesen werden. Daher sollten hier bessere Verfahren verwendet werden. Geeignete Verfahren sind beispielsweise

  - Einmalpasswörter (siehe auch M 5.34 *Einsatz von Einmalpasswörtern*), die software- oder hardwaregestützt erzeugt werden können. Hierbei sind die hardwarebasierten Authentisierungsmethoden vorzuziehen, da sie einen geringeren organisatorischen Aufwand und höhere Sicherheit bieten.
  - Die Authentisierung mittels PAP oder besser CHAP, die bei der Nutzung des Point-to-Point-Protocol eingesetzt werden (siehe auch M 5.50 *Authentisierung mittels PAP/CHAP*).
  - Die Authentisierung mittels CLIP/COLP, die bei der Kommunikation über ISDN eingesetzt wird (siehe auch M 5.48 *Authentisierung mittels CLIP/COLP*).
  - Ein weiteres bekanntes Verfahren ist das Authentikationsprotokoll Kerberos, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Es wird in Netzen zur gegenseitigen Authentisierung von Benutzer/Client und Servern eingesetzt. Die zentrale Autorität bei Kerberos ist der Ticket-Granting-Server, der Tickets ausstellt, mit denen sich Clients und Server gegenseitig authentisieren können. Mit Hilfe dieser Tickets können Benutzer sich nach einmaliger Authentikation Sitzungsschlüssel für die verschiedensten Dienste anfordern.

**Hashverfahren**

Bei der Kryptoanalyse von Hash-Funktionen hat es seit etwa 2005 große Fortschritte gegeben. SHA-1 ist daher als Legacy-Mechanismus zu betrachten und darf nicht mehr als kollisionsresistente Hashfunktion angesehen werden. Sein Einsatz im Kontext der HMAC-Konstruktion zur symmetrischen Nachrichtenauthentisierung ist aber unkritisch

Geeignete Algorithmen sind vor allem die neueren SHA-2 Versionen (SHA-256, SHA-384, SHA-512), und der neu entwickelte Standard SHA-3 bei einer Hashlänge ab 256 Bit. Diese Hashfunktionen sind für Anwendungen mit höheren Anforderungen an die Kollisionresistenz ausgelegt..

Der Hash-Algorithmus MD5 ist veraltet und weist massive Schwächen auf, die auch bereits anhand praktischer Beispiele demonstriert werden konnten. MD5

sollte deshalb nicht mehr verwendet werden. Auch RIPEMD-160 wird nicht mehr empfohlen.

**Auswahlkriterien**

**Mechanismenstärke / Schlüssellänge**

Ein wesentliches Kriterium für die Auswahl von kryptographischen Verfahren ist ihre Mechanismenstärke. Bei symmetrischen Verfahren sollte insbesondere die Schlüssellänge ausreichend groß sein. Je größer die verwendete Schlüssellänge bei einem kryptographischen Verfahren ist, desto länger dauert es, ihn z. B. durch eine Brute-Force-Attacke zu berechnen. Andererseits werden die Verfahren bei der Verwendung längerer Schlüssel langsamer, so dass immer zu überlegen ist, welche Schlüssellänge unter Nutzen-/Leistungsgesichtspunkten angemessen ist. Als Faustregel für gute Verfahren (AES, HMAC-SHA-2/3, Serpent,...) und normalen Schutzbedarf gilt derzeit, dass die eingesetzten Schlüssel mindestens 100 Bit lang sein sollten. Bei Verwendung von Blockchiffren sollten nicht ideal zufällig verteilte Daten in einem geeigneten authentisierten Verschlüsselungsmodus wie dem GCM-Modus oder durch Kombination eines Blockchiffriermodus wie CBC, CFB, oder Counter-Modus mit einem sicheren MAC-Verfahren wie CMAC oder HMAC im Encrypt-then-MAC-Modus verschlüsselt werden (nähere Informationen hierzu finden sich in Kapitel 2 der TR-02102-1).

Bei asymmetrischen Verfahren sollte die Mechanismenstärke so gewählt werden, dass die Lösung der zu Grunde liegenden mathematischen Probleme einen unvertretbar großen bzw. praktisch unmöglichen Rechenaufwand erfordert (die zu wählende Mechanismenstärke hängt daher vom gegenwärtigen Stand der Algorithmik und der Rechentechnik ab). Gegenwärtig kann davon ausgegangen werden, dass man mit etwa 2 hoch 100 Operationen derzeit noch "auf der sicheren Seite" ist. Von maßgeblichen Experten wird vorhergesagt, dass 1024 Bit RSA-Moduli mit einem Aufwand von circa 2 hoch 70 Operationen faktorisierbar sind, und der Aufwand der besten generischen Algorithmen für das diskrete Logarithmusproblem in einer Gruppe der Ordnung 160 Bit liegt in der Größenordnung 2 hoch 80. Da der Aufwand von 2 hoch 80 Operationen mit Fortschreiten der Rechentechnik allmählich in den Bereich des technisch Machbaren gerät, sollten Algorithmen mit 80 Bit Sicherheitsniveau bei Neuentwicklungen nicht mehr verwendet werden und auf längere Sicht ganz abgelöst werden. Minimal gefordert sind

- Modullängen von 1536 Bit bei RSA bzw.
- Untergruppenordnungen in der Größe von 200 Bit bei ElGamal-Verfahren auf einer geeigneten elliptischen Kurve

Für langfristige Sicherheitsanwendungen sollten 2048 Bit RSA-Moduli bzw. Untergruppenordnungen von mindestens 224 Bit eingesetzt werden. Beispiele für geeignete elliptische Kurven findet man im Internet unter www.ecc-brainpool.org.

Es sollten keine "unbekannten" Algorithmen verwendet werden, d. h. es sollten Algorithmen eingesetzt werden, die veröffentlicht sind, die von einem breiten Fachpublikum intensiv untersucht worden sind und von denen keine Sicherheitslücken bekannt sind. Häufig bieten Hersteller Sicherheitsprodukte an mit neuen Algorithmen, die "noch viel sicherer und noch viel schneller" sein sollen als andere Algorithmen. Aber vor der Verwendung von unbekannten Algorithmen aus Quellen, deren kryptographische Kompetenz nicht ausreichend nachgewiesen ist, kann nur gewarnt werden.

**Symmetrische oder hybride Verfahren?**

Aus Performancegründen werden für Verschlüsselungszwecke keine reinen Public-Key-Implementierungen eingesetzt. Alle gängigen Implementierungen von Public-Key-Kryptographie nutzen hybride Verfahren (siehe auch M 3.23 *Einführung in kryptographische Grundbegriffe*).

In Anwendungen mit großen oder offenen Nutzergruppen empfiehlt sich meist die Verwendung eines hybriden Verfahrens (wegen der Vorzüge für das Schlüsselmanagement). Bei kleinen, geschlossenen Nutzergruppen (insbesondere natürlich bei einem einzelnen Benutzer) kann man sich auf symmetrische Verfahren beschränken. Bei Einsatz hybrider Verfahren ist es sinnvoll, die Stärken des symmetrischen und des asymmetrischen Anteils aufeinander abzustimmen. Da mit dem asymmetrischen Verfahren vor einem Schlüsselwechsel in der Regel viele Schlüssel für das symmetrische Verfahren überschlüsselt werden, sollte der asymmetrische Algorithmus eher etwas stärker ausgelegt werden. Das bedeutet bei Verwendung eines symmetrischen Verfahrens mit 128 Bit Sicherheit (z.B. AES-GCM mit 128 Bit Schlüssellänge) die Verwendung von RSA-Moduln einer Länge von etwa 3000 Bit und von elliptischen Kurven mit Punktordnung ab 2 hoch 256.

Ein zusätzliches Sicherheitsziel, das bei bestimmten asymmetrischen Schlüsseleinigungsverfahren wie z. B. Diffie-Hellman Schlüsselaustausch (DH) oder dessen auf elliptischen Kurven realisierte Varianten (EC-DH) erreicht werden kann, ist Perfect Forward Secrecy (PFS). Das bedeutet, dass ein Angreifer nur dann unkomprimittierte vergangene Schlüsselaushandlungen brechen kann, wenn er das darunterliegende "harte" mathematische Problem lösen kann. Das spätere Aufdecken von Langzeitschlüsseln hat also keine negativen Folgen für die Sicherheit früherer Schlüsselaushandlungen. PFS ist anstrebenswert, setzt aber die Verfügbarkeit hochwertiger Zufallsquellen voraus.

Die verwendeten Cipher-Suiten sollten Perfect Forward Secrecy (PFS) unterstützen, insbesondere bei TLS (siehe Technische Richtlinie des BSI TR-02102-1 "Kryptographische Verfahren: Kryptographische Algorithmen und Schlüssellängen").

**Realisierbarkeit von technischen Anforderungen**

Die Chiffrieralgorithmen müssen so beschaffen sein, dass die technischen Anforderungen, insbesondere die geforderte Performance, durch eine geeignete Implementation erfüllt werden können. Hierunter fallen Anforderungen an die Fehlerfortpflanzung (z. B. falls über stark rauschende Kanäle gesendet wird), aber auch Anforderungen an Synchronisationsoverhead und Zeitverzögerung (z. B. falls "Echtzeit"-Verschlüsselung von großen Datenmengen erfordert wird).

**Beispiel: Sprachverschlüsselung bei ISDN**

Für die Planung eines Kommunikationsnetzes ist eine Reihe von Parametern zu berücksichtigen, die einen Einfluss auf die zu erwartende Sprachqualität haben und sich in Form von Rauschen, Knacken, Nebensprechen oder Pfeifen bemerkbar machen. Zu solchen Einflussfaktoren zählen beispielsweise die eingesetzten Verschlüsselungsverfahren. Um eine zufrieden stellende Sprachqualität erzielen zu können, müssen alle Einrichtungen längs eines Übertragungsweges betrachtet und bewertet werden.

Eine isolierte Betrachtungsweise einer Einzelkomponente ist zwar aufgrund der Verkopplung aller relevanten Einzeleffekte als nicht gerechtfertigt anzusehen, dennoch ist die Kenntnis der Einflussfaktoren jeder Einzelkomponente

(z. B. der Kryptokomponente) wichtig. Hieraus können sowohl die Rahmenbedingungen für die Realisierung als auch für die Auswahl abgeleitet werden.

Das Verhalten einer Verschlüsselungskomponente wird dabei hauptsächlich durch folgende Faktoren charakterisiert:

- die verstreichende Zeitdauer bei der Verschlüsselung eines Datenblocks (führt im Allgemeinen zu Verzögerungen),
- die für Synchronisationszwecke zusätzlich in den Datenstrom eingeführten Steuerinformationen (führen unter Umständen zu Schwankungen),
- der von der Kryptokomponente maximal zu leistende Datendurchsatz (führt, -wenn Zwischenspeicherung notwendig ist- ebenfalls zu Schwankungen),
- die durch die Verschlüsselung resultierende Fehlerfortpflanzung (führt im Allgemeinen zu einem Anstieg der Fehlerrate).

Gerade bei einer Sprachverschlüsselung (Echtzeitdienst) machen sich die vorgenannten Einflussfaktoren in einer Erhöhung der Ende-zu-Ende-Laufzeit, in Laufzeitschwankungen sowie in einer höheren Fehlerrate negativ bemerkbar, d. h. in einer Qualitätsminderung, die messtechnisch ermittelt und der Kryptokomponente zugeordnet werden kann.

**Andere Einflussfaktoren**

Manche kryptographische Algorithmen (z. B. IDEA) sind patentiert, für ihren Einsatz in kommerziellen Anwendungen (wozu auch der behördliche Bereich zählt) sind eventuell Lizenzgebühren zu entrichten.

**Veröffentlichungen der Bundesnetzagentur**

Die Bundesnetzagentur veröffentlicht regelmäßig im Bundesanzeiger eine Übersicht über die Algorithmen, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet angesehen werden können. Diese Veröffentlichungen können auch vom Webserver der Bundesnetzagentur (www.bundesnetzagentur.de) herunter geladen werden. Sie können zusätzliche Hinweise zur Auswahl liefern.

Prüffragen:

- Wird beim Einsatz kryptographischer Verfahren eine aktuell empfohlene Schlüssellänge eingesetzt?
- Wird sichergestellt, dass etablierte Algorithmen verwendet werden, die von der Fachwelt intensiv untersucht worden sind und von denen keine Sicherheitslücken bekannt sind?

# M 2.165 Auswahl eines geeigneten kryptographischen Produktes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Das Spektrum kryptographischer Anwendungen ist sehr breit, es reicht von einem einfachen Programm zur Dateiverschlüsselung auf einem Single-User PC über Firewall-Rechner mit Kryptofunktionen zur Absicherung eines lokalen Netzes bis hin zur "Echtzeit"-Hardwareverschlüsselung von Videokonferenzen. Es ist klar, dass bei dieser Breite Empfehlungen zur Auswahl von kryptographischen Produkten allgemein gültig gehalten sind.

Vor einer Auswahl sollte der Nutzer **sämtliche** Anforderungen an das Produkt festlegen. Das ausgewählte Produkt sollte die Benutzeranforderungen in einem möglichst hohen Grad abdecken.

### Funktionalität

Das ausgewählte Produkt muss die vom Anwender spezifizierte Funktionalität aufweisen, insbesondere muss es

- die geforderten kryptographischen Grunddienste leisten,
- evtl. besonderen Anforderungen durch die Einsatzumgebung genügen (z. B. Single-User/Multi-User-PC, LAN-Umgebung, WAN-Anbindung),
- die geforderten technischen Leistungsmerkmale aufweisen (z. B. Durchsatzraten),
- die geforderten Sicherheitsfunktionalitäten aufweisen, insbesondere müssen die eingesetzten kryptographischen Mechanismen die erforderliche Stärke aufweisen.

### Interoperabilität

Das ausgewählte Produkt wird in der Regel in eine bestehende IT-Umgebung eingefügt. Es muss dort möglichst interoperabel sein. Die Einhaltung interner Standards ist nötig, um die Interoperabilität mit dem bereits vorhandenen IT-System bzw. Systemkomponenten zu gewährleisten. Die Anwendung internationaler Standards für kryptographische Techniken sollte selbstverständlich sein, sie erleichtert auch eine Sicherheitsevaluierung der kryptographischen Komponente.

### Wirtschaftlichkeit

Das ausgewählte Produkt sollte möglichst wirtschaftlich sein. Dabei müssen Anschaffungskosten, Stückzahlen, Kosten für Wartung und Produktpflege, aber auch Einsparungen durch etwaige Rationalisierungseffekte berücksichtigt werden.

### Zertifizierte Produkte

In den letzten Jahrzehnten hat sich eine international anerkannte Methodologie zur Bewertung von Sicherheitsprodukten durchgesetzt: die europäischen ITSEC (Information Technology Security Evaluation Criteria) bzw. deren Weiterentwicklung CC (The Common Criteria for Information Technology Security Evaluation). Die ITSEC bzw. CC bieten einen Rahmen, innerhalb dessen die Sicherheitsfunktionalitäten eines IT-Produktes durch Anlegen von etablierten Kriterien in eine genau spezifizierte Hierarchie von Sicherheitsstufen eingeordnet werden können. Die Informationssicherheitsbehörden mehrerer Staa-

ten haben jeweils ein nationales Zertifizierungsschema nach diesen Kriterien aufgebaut.

Der Einsatz eines zertifizierten Produktes bietet die Gewähr, dass die Sicherheitsfunktionalität dieses Produktes unabhängig geprüft wurde und den im Evaluationslevel spezifizierten Standard nicht unterschreitet (siehe auch M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*).

**Grenzüberschreitender Einsatz**

Viele Unternehmen und Behörden haben zunehmend das Problem, das sie auch ihre internationale Kommunikation, z. B. mit ausländischen Tochterunternehmen, kryptographisch absichern wollen. Hierfür muss zunächst untersucht werden,

- ob innerhalb der jeweiligen Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind und
- ob für in Frage kommende Produkte Export- oder Importbeschränkungen beachtet werden müssen.

**Fehlbedienungs- und Fehlfunktionssicherheit**

Das Gefährliche an kryptographischen Produkten ist, dass sie den Anwender in einer - mitunter trügerischen - Sicherheit wiegen: Es ist ja "alles verschlüsselt"! Insofern kommt Maßnahmen gegen Kompromittierungen durch Bedienungsfehler oder technisches Versagen besondere Bedeutung zu, da deren Folgen eben nicht nur auf einen schlichten Defekt beschränkt werden können, sondern sogleich einen Sicherheitseinbruch nach sich ziehen.

Allerdings ist die Bandbreite bezüglich redundanter Systemauslegung und zusätzlicher Überwachungsfunktionen - und damit an Gerätekosten - groß, so dass hier die Maßnahmen im Einzelfall in Abhängigkeit von den Anforderungen festzulegen sind.

**Implementierung in Software, Firmware oder Hardware**

Kryptographische Algorithmen können sowohl in Software, in Firmware als auch in Hardware implementiert werden. Softwarerealisierungen werden in der Regel vom Betriebssystem des jeweiligen IT-Systems gesteuert. Unter Firmware versteht man Programme und Daten, die permanent so in Hardware gespeichert sind, dass die Speicherinhalte nicht dynamisch verändert werden können, und die während ihres Ablaufs nicht modifiziert werden können. Bei Hardware-Lösungen wird das kryptographische Verfahren direkt in Hardware realisiert, z. B. als separates Sicherheitsmodul oder als Einsteckkarte.

Dazu, welche Art der Implementierung gewählt werden sollte, kann keine generelle Empfehlung abgegeben werden, da die Entscheidung eine Abwägung von verschiedenen Faktoren erfordert:

- den Schutzbedarf der durch das kryptographische Verfahren zu schützenden Daten bzw. das angestrebte Sicherheitsniveau,
- den angestrebten Datendurchsatz,
- wirtschaftliche Überlegungen und Zwänge,
- die Einsatzumgebung sowie umgebende Sicherungsmaßnahmen,
- eine evtl. vorliegende nationale Einstufung der bearbeiteten Daten.

Softwarelösungen bieten den Vorteil, leicht anpassbar und kostengünstig zu sein. Hardware-Realisierungen bieten im allgemeinen sowohl höhere Manipulationsresistenz (und damit Sicherheit) als auch höheren Datendurchsatz als Softwarerealisierungen, sie sind aber normalerweise auch teurer.

Firmwarelösungen kann man als Kompromiss der beiden vorangegangenen Möglichkeiten verstehen. Die Vor- und Nachteile der jeweiligen Realisierung beziehen sich jedoch immer nur auf lokale Aspekte (dazu gehört vor allem das Schlüsselmanagement). Sind die Daten einmal verschlüsselt und befinden sie sich auf dem Kommunikationsweg, ist im Prinzip das Zustandekommen der Verschlüsselung nicht mehr relevant.

Ein Beispiel für (relativ) preiswerte, transportable und benutzerfreundliche Kryptomodule sind Chipkarten, die im Bereich der lokalen Verschlüsselung als sicheres Speichermedium für die kryptographischen Schlüssel oder im Bereich der Authentikation zur Passwort-Generierung und Verschlüsselung eingesetzt werden können.

Wenn alle Anforderungen an das kryptographische Produkt festgelegt worden sind, erhält man damit einen Anforderungskatalog, der dann auch direkt für eine Ausschreibung verwendet werden kann, sofern eine solche notwendig ist.

Prüffragen:

- Erfüllen die eingesetzten kryptographischen Produkte sämtliche festgelegten Anforderungen?

# M 2.166 Regelung des Einsatzes von Kryptomodulen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von Kryptomodulen gestellt werden. Diese müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden.

Dafür müssen einige organisatorische Regelungen getroffen werden:

- Es müssen Verantwortliche benannt werden, und zwar für die Erstellung des Kryptokonzepts, für die Auswahl sowie für den sicheren Betrieb der kryptographischen Produkte.
- Es sind geeignete personelle Maßnahmen festzulegen bzw. durchzuführen (Schulung, Benutzer-Support, Vertretungsregelungen, Verpflichtungen, Rollenzuteilungen).
- Die Benutzer sollten nicht nur im Umgang mit den von ihnen zu bedienenden Kryptomodulen geschult werden, sie sollten darüber hinaus für den Nutzen und die Notwendigkeit der kryptographischen Verfahren sensibilisiert werden und einen Überblick über kryptographische Grundbegriffe erhalten (siehe auch M 3.23 *Einführung in kryptographische Grundbegriffe*).
- Falls Probleme oder gar der Verdacht auf Sicherheitsvorfälle beim Einsatz von Kryptomodulen auftritt, muss klar definiert sein, was in solchen Fällen zu unternehmen ist. Alle Benutzer müssen über die entsprechenden Verhaltensregeln und Meldewege informiert sein.
- Im Rahmen des Kryptokonzepts ist festzulegen, wer wann welche Kryptoprodukte benutzen muss bzw. darf und welche Randbedingungen dabei zu beachten sind (z. B. Schlüsselhinterlegung).
- Der korrekte Einsatz der Kryptomodule sollte regelmäßig überprüft werden. Ebenso ist regelmäßig zu hinterfragen, ob die eingesetzten kryptographischen Verfahren noch dem Stand der Technik entsprechen (siehe dazu auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).
- Je nach den definierten Verfügbarkeitsanforderungen sollten Ersatz-Kryptomodule vorrätig gehalten werden, um einen reibungslosen Betrieb zu gewährleisten. Dies ist insbesondere dort wichtig, wo der Zugriff auf verschlüsselte Daten von der Funktionsfähigkeit eines einzelnen Kryptomoduls abhängt, z. B. bei der Datenarchivierung oder der ISDN-Verschlüsselung.

Es ist ein sicherer Betrieb der Kryptomodule zu gewährleisten, dazu gehören:

- Vor der Inbetriebnahme muss die optimale Konfiguration der Kryptomodule festgelegt werden, z. B. hinsichtlich Schlüssellänge, Betriebsmodi oder Kryptoalgorithmen.
- Die festgelegte Konfiguration muss dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.
- Für die Benutzer müssen die Kryptoprodukte durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann.
- Bei komplexeren Kryptoprodukten müssen geeignete Handbücher verfügbar sein.

- Die Kryptomodule müssen sicher installiert werden und anschließend getestet werden (z. B. ob sie korrekt verschlüsseln und ob sie von Benutzer bedient werden können).
- Die Anforderungen an die Einsatzumgebung müssen festgelegt sein, eventuell sind dafür ergänzende Maßnahmen im IT-Umfeld zu treffen. Die sicherheitstechnischen Anforderungen an die IT-Systeme, auf denen die kryptographischen Verfahren eingesetzt werden, sind den jeweiligen systemspezifischen Bausteinen zu entnehmen, z. B. für Clients (inklusive Laptops) und für Server aus Schicht 3.
- Es muss festgelegt werden, wer wie häufig die Kryptomodule zu warten hat.

Auch im Rahmen des Schlüsselmanagements (siehe M 2.46 *Geeignetes Schlüsselmanagement*) müssen diverse Vorgaben gemacht werden:

- Vorgaben zur Schlüsselerzeugung und -auswahl,
- Vorgaben zur gesicherten Speicherung kryptographischer Schlüssel,
- Festlegung der Schlüsselwechsel-Strategie und -Intervalle.

Prüffragen:

- Sind Verantwortliche für die Erstellung des Kryptokonzepts, für die Auswahl, sowie für den sicheren Betrieb der kryptographischen Produkte benannt?
- Sind Benutzer und Administratoren ausreichend im Umgang mit den von ihnen zu bedienenden Kryptomodulen geschult?
- Sind die Benutzer für den Nutzen und die Notwendigkeit kryptographischer Verfahren sensibilisiert und haben sie einen Überblick über kryptographische Grundbegriffe?
- Sind alle Benutzer über Verhaltensregeln und Meldewege bei Problemen oder bei Verdacht auf einen Sicherheitsvorfall beim Einsatz von Kryptomodulen informiert?
- Ist im Rahmen des Kryptokonzepts festgelegt worden, wer wann welche Kryptoprodukte benutzen muss bzw. bedienen darf?
- Wird regelmäßig der korrekte Einsatz der Kryptomodule und die Aktualität des eingesetzten Kryptoverfahrens überprüft?
- Werden bei hohen Verfügbarkeitsanforderungen Ersatzkryptomodule vorrätig gehalten?
- Wird vor der Inbetriebnahme die optimale Konfiguration der Kryptomodule festgelegt?
- Werden die Kryptomodule sicher installiert und diese getestet, ob sie korrekt funktionieren?
- Sind Anforderungen an die Einsatzumgebung der Kryptomodule festgelegt?
- Ist festgelegt, wie häufig die Kryptomodule zu warten sind?

# M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation

Um die Vertraulichkeit schutzbedürftiger Informationen sicherzustellen, müssen diese Informationen nach Gebrauch so vernichtet oder gelöscht werden, dass eine Rekonstruktion der Informationen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.

Zur sicheren Löschung oder Vernichtung müssen zum einen geeignete Verfahren und zum anderen geeignete Geräte, Anwendungen oder Dienstleistungen zur Verfügung stehen.

Es gibt verschiedene Methoden, um Informationen auf Datenträgern zu löschen oder zu vernichten. Eine kurze Darstellung findet sich in M 2.433 *Überblick über Methoden zur Löschung und Vernichtung von Daten*. Die wichtigsten Empfehlungen zum Löschen und Vernichten der derzeit gebräuchlichen Datenträger werden hier kurz dargelegt.

**Empfehlungen zum Löschen von Datenträgern**

Die einfachen Löschkommandos der jeweiligen Betriebssysteme und auch die Formatierung der entsprechenden Datenträger reichen nicht aus, um dort gespeicherte Daten sicher zu löschen. Für das sichere Löschen sollten daher physikalische Maßnahmen wie die mechanische, thermische oder magnetische Behandlung des entsprechenden Datenträgers oder das gezielte, ein- oder mehrmalige Überschreiben des Datenträgers ausgewählt werden. Zum Überschreiben wird die Verwendung von zufälligen Datenmustern empfohlen. Bei Datenträgern, die im gleichen gesicherten Bereich weiterverwendet werden sollen, kann der Aufwand zum Löschen niedriger angesetzt werden als bei Datenträgern, die den Anwendungsbereich verlassen und z. B. verkauft werden. Im Folgenden wird ein Überblick über Methoden zum Löschen gebräuchlicher Datenträger gegeben:

- Papierdokumente:
  Keine zuverlässige Methode vorhanden.
- Mikrofilm, Mikrofiche:
  Keine zuverlässige Methode vorhanden.
- Festplatten (mit magnetischen Datenträger), Magnetbandkassetten, Disketten:
  Überschreiben des gesamten Datenträgers mit einem Zufallszahlenmuster und Verifikation.
- Festplatten mit Halbleiterspeicher (SSD / Hybrid):
  Für höheren Schutzbedarf ist derzeit noch keine zuverlässige Methode vorhanden. Empfohlen wird, den Datenträger von Anfang der Nutzung an vollständig zu verschlüsseln. Vor der Entsorgung sollte er wie vorgenannt überschrieben werden.
- Optische Datenträger (CD, DVD):
  Wiederbeschreibbare Datenträger wie CD-RW oder DVD-RW können bei normalem Schutzbedarf durch Überschreiben mit beliebigen Daten gelöscht werden.

- Flüchtige Halbleiterspeicher (SRAM, DRAM)
  Zum Löschen sollte die Stromversorgung ausgeschaltet werden. Wenn vorhanden, muss vorher die Pufferbatterie entfernt werden.
  Bei sehr hohem Schutzbedarf muss vorher der Speicher mit beliebigen Daten einmal überschrieben werden.
- Nichtflüchtige Halbleiterspeicher (EPROM, EEPROM, Flash EPROM) USB-Stick, Flash-Card, Flash-Disk, PCMCIA-Karten:
  Bei hohem Schutzbedarf muss der gesamte Speicherbereich mit geeigneter Software dreimal überschrieben werden.
- Chipkarten:
  Keine zuverlässige Methode vorhanden.
- Multifunktionsgeräte (Kopierer, usw.) mit Festplatten:
  Überschreiben: Bei normalem Schutzbedarf sollten die Informationen nach dem Ausdruck über eine Löschfunktion aus dem Zwischenspeicher gelöscht werden. Bei hohem Schutzbedarf muss die Festplatte mit geeigneter Software nach jedem Ausdruck überschrieben werden.
  Bei Abgabe oder Aussonderung eines Gerätes muss M 2.400 beachtet werden.

Von der Nutzung der folgenden Methoden als Löschverfahren wird abgeraten, da diese nicht zuverlässig sind und Daten wieder rekonstruiert werden können:

- Löschkommandos
- Überschreiben einzelner Dateien
- High-Level-Formatierung
- Low-Level-Formatierung

**Empfehlungen zum Vernichten von Datenträgern:**

In der Norm DIN 66399:2012 "Vernichten von Datenträgern", Teil 1 wird dem Schutzbedarf eine Schutzklasse zugeordnet. Aus der Schutzklasse leiten sich dann die anzuwendenden Sicherheitsstufen für die verschiedenen Datenträger ab. Für normalen Schutzbedarf ist die Schutzklasse 2 angemessen. Geeignete Vernichtungsverfahren und Partikelgrößen für die jeweiligen Schutzklassen finden sich in DIN 66399 Teil 2.

Für die Vernichtung von Datenträgern kann auch auf zuverlässige Dienstleister zurückgegriffen werden (siehe M 2.436).

- Papierdokumente:
  Papierdokumente sollten mit Aktenvernichtern zerkleinert werden. Bei normalem Schutzbedarf sollten hierfür Aktenvernichter der Sicherheitsstufe P-3 nach DIN 66399 genutzt werden, bei höherem Schutzbedarf solche der Sicherheitsstufe P-4, P-5 oder P-6 (siehe auch M 2.435).
- Mikrofilm, Mikrofiche:
  Zum mechanischen Zerkleinern wird Stufe F-4 nach DIN 66399 empfohlen, jedoch sind nur noch vereinzelt geeignete Geräte vorhanden. Daher sollten diese Datenträger verbrannt werden. Die Temperatur muss dabei über 300° C liegen, die Verweildauer mindestens 60 Minuten betragen.
- Festplatten:
  Festplatten können mechanisch mit einem Schredder zerkleinert werden. Dabei ist bei hohem Schutzbedarf mindestens die Sicherheitsstufe H-5 nach DIN 66399 anzuwenden. Die Anwendung der Sicherheitsstufe DIN 66399 H-6 sollte bei Festplatten mit hoher Kapazität oder hohen Datendichten in Erwägung gezogen werden. Bei normalem Schutzbedarf sind Partikelgrößen entsprechend DIN 66399, Stufe H-4, bis 2000 Quadratmillimeter durchaus vertretbar. Für mechanisch kleine Laufwerke ist die Verwendung höherer Sicherheitsstufen notwendig. Festplatten können auch

thermisch vernichtet werden, dafür muss das Festplattenlaufwerk mindestens 15 Minuten lang auf über 1.000° C erhitzt werden.
- Magnetbänder, Magnetbandkassetten:
  Magnetbänder sollten mit Geräten zerkleinert werden, die die Anforderungen der DIN 66399, Stufe T-3 erfüllen. Bei höherem Schutzbedarf sollte die Partikelgröße höchstens 30 Quadratmillimeter betragen (Stufe T-5).
- Disketten, Optische Datenträger (CD, DVD):
  Diese Datenträger können mechanisch mit einem Vernichter zerkleinert werden. Bei optischen Datenträgern darf die Größe der Partikel 160 Quadratmillimeter, gemäß DIN 66399, Stufe O-3 nicht überschreiten, bei höherem Schutzbedarf muss sie unter 30 Quadratmillimeter, Stufe O-4, liegen. Sie können auch thermisch vernichtet werden, dafür müssen sie mindestens 60 Minuten lang auf über 300° C erhitzt oder bei höheren Temperaturen verbrannt werden.
- Halbleiterspeicher (SRAM, DRAM, EPROM, EEPROM, USB-Stick, Flash-Speicher, SSD-Festplatten, PCMCIA-Karten):
  Diese Datenträger können mit geeignetem Gerät mechanisch zerkleinert werden. Die Geräte sollen der Sicherheitsstufe E-4 nach DIN 66399 entsprechen. Sie können auch verbrannt werden. Dabei müssen sie mindestens 15 Minuten lang auf über 800 C erhitzt werden.
- Chipkarten:
  Chipkarten können verbrannt oder mechanisch mit einem Vernichtungsgerät zerkleinert werden. Bei normalem Schutzbedarf sollten hierfür Vernichter der Sicherheitsstufe E-4 nach DIN 66399 genutzt werden.

Welche Verfahren geeignet sind, um die in der Institution vorkommenden Daten oder Datenträger zu löschen oder zu vernichten, hängt von der Art der Datenspeicherung, der Datenträger und vom Grad der Schutzbedürftigkeit der Informationen ab. Auch ist zu berücksichtigen, für welche weitere Verwendung der Datenträger vorgesehen ist. Daher sollte eine Anforderungsanalyse vor der Auswahl durchgeführt werden, um geeignete Verfahren zu finden.

Hierbei sollten unter anderem folgende Fragen beantwortet werden:

- Welche Datentypen (auf welchen Betriebssystemen und in welchen Anwendungen) und welche Datenträgertypen (z. B. optisch oder magnetisch) mit welchen Datenvolumen (z. B. Megabyte, Gigabyte, Terabyte) sollen sicher gelöscht werden?
- Wie hoch ist der Schutzbedarf der auf den Datenträgern gespeicherten Daten?
- Wie groß ist Datenträger selbst? Wird das Ergebnis der Vernichtung dem Schutzbedarf gerecht?
- Wurden bzw. werden die Datenträger in einem geschützten Bereich verwendet?
- Sind bereits Werkzeuge zum Löschen und Vernichten von Informationen vorhanden? Sind diese geeignet für den identifizierten Schutzbedarf und die vorhandenen Datenträger-Arten?
- Welche Arten von Lösch- und Vernichtungsverfahren existieren für den identifizierten Schutzbedarf und die vorhandenen Datenträger-Arten? Wie hoch ist der Schulungsaufwand, um diese zuverlässig zu benutzen?
- Wie groß ist die voraussichtliche Menge von Datenträgern eines Typs, der gelöscht bzw. vernichtet werden soll?

Das Löschen von Daten oder Vernichten von Datenträgern sollte arbeitsplatz- und zeitnah durchgeführt werden, damit die Datenträger möglichst nicht zwischengelagert werden müssen. Damit wird in der Regel auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit erhöht.

Je nach Schutzbedarf der Informationen und den verwendeten Datenträger müssen andere Werkzeuge oder Geräte verwendet werden, um die Daten zuverlässig zu löschen oder zu vernichten. Einige Werkzeuge und Geräte sind teuer in der Anschaffung bzw. nicht einfach korrekt zu bedienen. Daher kann es sinnvoll sein, hierfür Dienstleistungsverträge mit Externen abzuschließen. Zu diesem Zweck müssen die ausgesonderten Datenträger innerhalb der Institution eingesammelt werden. Dazu sollten an geeigneten Stellen einbruchsichere Behälter aufgestellt und regelmäßig geleert werden.

Vernichtungsgeräte sind durch die normale Nutzung einem Verschleiß unterworfen. Durch unsachgemäße Nutzung oder Vernichtung von Datenträgern, für die das Gerät nicht vorgesehen war, können Schäden am Gerät entstehen. Eine regelmäßige Überprüfung der Partikelgröße muss daher durchgeführt werden, beispielsweise durch eine einfache Sichtprüfung gegen die Daten aus dem Gerätehandbuch.

Es muss nachvollziehbar dokumentiert werden, welche Verfahren zum Löschen und Vernichten für die verschiedenen Datenarten und den jeweiligen Schutzbedarf ausgewählt wurden und wie diese anzuwenden sind.

Die Mitarbeiter müssen in die ausgewählten Verfahren zum Löschen und Vernichten von Informationen eingewiesen werden, vor allem, wenn sie die entsprechenden Werkzeuge selber benutzen sollen.

Prüffragen:

- Wurden für die verschiedenen Datenarten und den jeweiligen Schutzbedarf angemessene Verfahren zum Löschen oder Vernichten festgelegt?
- Wurden die Mitarbeiter in die Verfahren zum Löschen und Vernichten von Informationen eingewiesen, vor allem in den Gebrauch der vorhandenen Werkzeuge und Geräte?
- Stehen für die verschiedenen Arten von Datenträgern geeignete Geräte und Werkzeuge zum zuverlässigen Löschen oder Vernichten der gespeicherten Informationen zur Verfügung?
- Wird das Ergebnis der Vernichtung regelmäßig kontrolliert?
- Wird das für einen Datenträger gewählte Vernichtungsverfahren dem Stand der Technik (z. B. Größe des Datenträgers) gerecht?

# M 2.168 IT-System-Analyse vor Einführung eines Systemmanagement-Systems

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Vor der Einführung eines Systemmanagementsystems müssen die IT-Systeme, die zukünftig verwaltet werden sollen, untersucht und analysiert werden. Die daraus resultierende Systemdokumentation kann dann als Planungs- und Entscheidungsgrundlage für die festzulegende Systemmanagementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) dienen. Wichtig ist, dass schon zum Zeitpunkt der Planung alle relevanten Informationen über die zu verwaltenden Systeme möglichst vollständig vorliegen, um Fehlentscheidungen aufgrund mangelnder Information auszuschließen. Aus den lokalen Gegebenheiten lassen sich außerdem konkrete Anforderungen formulieren, die von dem zu beschaffenden Managementsystem erfüllt werden müssen (K.O.-Kriterien).

Es sind folgende Maßnahmen (mit den dort beschriebenen Untermaßnahmen) durchzuführen, die idealerweise bei der Planung und im laufenden Betrieb des Systems gemäß IT-Grundschutz schon durchgeführt wurden bzw. werden:

- Ist-Aufnahme der aktuellen Netzsituation (siehe M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*)
- Dokumentation der Systemkonfiguration (siehe M 2.25 *Dokumentation der Systemkonfiguration*)
  Es sollten alle IT-Systeme erfasst und dokumentiert werden. Insbesondere in heterogenen Systemen müssen z. B. alle vorhandenen Betriebssysteme erfasst werden, um die entsprechenden Anforderungen an das Managementsystem formulieren zu können.
- Feststellung und Überprüfung des Softwarebestandes (siehe M 2.10 *Überprüfung des Hard- und Software-Bestandes*)
  Soll im Rahmen des Systemmanagements auch Software verwaltet werden (Applikationsmanagement), so sollte hier eine Bestandsaufnahme erfolgen. Alternativ kann als Anforderung an das Managementsystem das automatische Feststellen des Softwarebestandes ("Autodiscovery", "Software-Discovery") formuliert werden. Welche der beiden Varianten im Einzelfall notwendig ist, hängt von der Aufgabe ab, die im Bereich Softwaremanagement erbracht werden soll. Wird das Managementsystem z. B. dazu angeschafft, um einen existierenden Softwarebestand, dessen Zusammensetzung nicht in Gänze bekannt ist, automatisch zu verwalten (Softwareupdate, Einspielen neuer Software), so muss dass Managementsystem nach seiner Installation in der Lage sein, den Softwarebestand automatisch zu erfassen. Sollen im Rahmen des Applikationsmanagements einzelne Softwarepakete zusätzlich auf Anwendungsebene verwaltet werden, so muss geprüft werden, ob die Software dies aktiv unterstützt (z. B. durch ein entsprechendes Protokoll), was eine vorherige Bestandsaufnahme der vorhandenen Software nötig macht. Daraus ergeben sich dann Anforderungen an den Funktionsumfang des zu beschaffenden Managementsystems (z. B. Unterstützung des Applikationsverwaltungsprotokolls).
  Soll z. B. ein Webserver über ein HTTP-basiertes Managementinterface verwaltet werden, so muss das Managementsystem HTTP-basierte Managementfunktionen besitzen oder aber ein Erweiterungsinterface anbieten, das es erlaubt, Eigenentwicklungen zu integrieren.

Neben der Dokumentation des Ist-Zustandes sollte auch die zukünftige Planung für das IT-System berücksichtigt werden, da ein Managementsystem auch auf zukünftige Änderungen im IT-System ausgelegt sein sollte (z. B. Skalierbarkeit).

Prüffragen:

- Applikationsmanagement im Rahmen des Systemmanagements: Wird eine Bestandsaufnahme der Software durchgeführt oder das automatische Feststellen des Softwarebestandes vom Managementsystem gefordert?
- Wird die zukünftige Planung der IT-Systeme bei der Auslegung des Systemmanagementsystems berücksichtigt?

# M 2.169 Entwickeln einer Systemmanagementstrategie

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die in einem Netz angesiedelten Komponenten müssen von einem Administrator regelmäßig verwaltet werden. Die zu erledigenden Aufgaben reichen von der Einrichtung neuer Benutzer bis hin zur Installation neuer Software, deren verteilte Natur die Installation von Teilsoftware auf jedem einzelnen Rechner verlangt (Workflowsystem, Dokumentenverwaltungssystem, o. Ä.). In großen Organisationen bedeutet alleine die Einrichtung eines neuen Benutzers, der sich auf allen für ihn freigegebenen Rechnern anmelden können soll, einen hohen administrativen Aufwand, da beim Stand-alone-Betrieb jeder einzelne dieser Rechner dementsprechend konfiguriert werden muss. Moderne netzfähige Betriebssysteme (z. B. Unix, Windows NT, Novell) sind daher mit Mechanismen ausgestattet, die den administrativen Aufwand verringern sollen (z. B. zentrale Benutzerverwaltung). Soll allerdings die Verwaltung aller Hard- und Software-Komponenten eines lokalen Netzes auf allen Ebenen (technisch und organisatorisch) in einheitlicher Weise erfolgen, so müssen einerseits technische Hilfsmittel in Form von Managementsystemen eingesetzt werden, deren erfolgreicher Einsatz andererseits aber auch von einer zu erstellenden Managementstrategie abhängt. Die Vorgaben und Regeln der Managementstrategie werden dann durch die Systemadministration mit Hilfe der Managementsoftware umgesetzt. Eine Managementstrategie muss individuell auf die Bedürfnisse der jeweiligen Unternehmen bzw. Behörden angepasst sein. Hierzu müssen folgende Schritte durchgeführt werden:

**Festlegung der vom Managementsystem zu verwaltenden Objekte**

Nach der Durchführung der Bestandsaufnahme (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagement-Systems*) muss festgelegt werden, welche Bereiche des IT-Systems durch ein zu beschaffendes Managementsystem verwaltet werden sollen:

- Welche Rechner bzw. Hardware sollen in das Managementsystem einbezogen werden?
- Welche Software soll einbezogen werden?
- Welche Benutzer bzw. Benutzergruppen werden einbezogen?

**Festlegung der im Managementsystem anzuwendenden Sicherheitsrichtlinien**

Neben diesen Entscheidungen müssen aber auch schon existierende Vorschriften und Methoden einbezogen werden. So muss z. B. die festgelegte Sicherheitspolitik der Behörde bzw. des Unternehmens, die Datenschutzrichtlinien und die Richtlinien zur Einführung neuer Software in das Managementkonzept einfließen, da die geltenden Vorschriften auch beim Einsatz eines Managementsystems beachtet und umgesetzt werden müssen. Auch für den Gebrauch des Managementsystems selbst sind Regelungen zu treffen bzw. existierende Regelungen auf Validität zu prüfen und gegebenenfalls anzupassen, und dann auch anzuwenden. Dies gilt insbesondere in den Bereichen:

- Zugriffsrechte auf Managementinformationen
- Dokumentation des Managementsystems
- Erstellung oder Abgleich von Notfallplänen für den Ausfall des Managementsystems oder einzelner Komponenten

Im Vorfeld sollten auch bereits die Reaktionen auf Verletzung der Sicherheitspolitik im Bereich Systemmanagement festgelegt werden. Ähnlich wie in anderen IT-Bereichen, muss auch für den Bereich des Systemmanagements eine Sicherheitspolitik festgelegt bzw. die vorhandene Sicherheitspolitik des Unternehmens bzw. der Behörde auch auf den Bereich Systemmanagement angewandt werden. Da ein Managementsystem mit wichtigen Netz- und Systemkomponenten interagiert und deren Funktion verwaltet und überwacht, sind Verletzungen der Sicherheitspolitik in diesem Bereich als besonders schwer anzusehen. Insbesondere sind hier Regelungen und Vorgehensweisen zu definieren, die nach einer solchen Sicherheitsverletzung zum Einsatz kommen. Diese sind einerseits technischer Natur (z. B. Vergabe neuer Passwörter für alle Benutzer nach Kompromittierung der Managementkonsole), aber auch organisatorischer Natur.

Revision, Datenschutzbeauftragte und Sicherheitsmanagement sollten schon in der Planungsphase einbezogen werden. Nach Einführung des Managementsystems müssen die ihnen hier obliegenden Aufgaben in Bezug auf das Managementsystem klar sein. Beispiel: Der Datenschutzbeauftragte kann schon in der Planungsphase auf die Einhaltung der Datenschutzrichtlinien achten, z. B. welche Benutzerinformationen im Rahmen des Systemmanagements erfasst werden sollen bzw. dürfen. Nach Einführung des Systems muss er zudem in der Lage sein, die Einhaltung der Richtlinien zu überprüfen. Ähnliches gilt für die Zuständigkeitsbereiche des Revisors und des IT-Sicherheitsbeauftragten.

**Festlegung der Randbedingungen für die Produktauswahl des Managementsystems**

Die Einführung eines Systemmanagementsystems erfordert eine umfangreiche und sorgfältige Planung. Teile der Systemmanagementstrategie hängen zudem davon ab, ob sie mit einem konkreten Produkt realisiert werden können oder nicht. Dies führt dazu, dass die Erstellung der Managementstrategie und die (Vor-)Auswahl eines Produktes iteriert werden müssen.

Folgende Punkte sollten bei der Erstellung der Systemmanagementstrategie Berücksichtigung finden:

- Ist mehr als eine Managementdomäne nötig? Wenn ja: Wie sind diese zu bilden? Managementdomänen erlauben die Einteilung der Komponenten des zu verwaltenden Systems in Gruppen. Die einzelnen Gruppen können voneinander getrennt verwaltet werden. Die Aufteilung in verschiedene Managementdomänen ist für kleinere und mittlere zu verwaltende Systeme nicht zwingend, unterstützt jedoch ein strukturierteres Systemmanagement. Für große zu verwaltende Systeme ist die Aufteilung in verschiedene Managementdomänen in der Regel zwingend. Die Planung der Managementregionen hängt dabei von mehreren Faktoren ab:
  - Netztopologie
    Insbesondere für mittlere Systemgrößen bietet sich die Aufteilung des Systems in Managementdomänen entsprechend der konkreten Netztopologie an (gerade auch, wenn es z. B. keine unterschiedlichen Verantwortlichkeiten gibt).
  - Organisatorische Verantwortlichkeiten innerhalb des Unternehmens oder der Behörde
    So kann die Organisationsstruktur mit dem Managementsystem nachgebildet werden, so dass z. B. Domänen wie "Rechnungswesen", "Programmierung" oder auch "Bereich Produktion", "Bereich Softwareentwicklung" entstehen.

Auch sicherheitstechnische Gründe, die sich in der Managementpolitik niederschlagen, können zu mehreren Managementregionen führen. Dies ist insbesondere dann der Fall, wenn Managementaufgaben für bestimmte Organisationseinheiten delegiert werden sollen, ohne dass der lokale Administrator Zugriffsrechte auf die Managementfunktionen für die Komponenten außerhalb seines Zuständigkeitsbereiches haben soll.

- vorhandene Infrastruktur
  Hier ist z. B. die geographische Verteilung von Filialen oder die räumliche Verteilung von Arbeitsgruppen über die Stockwerke eines Gebäudes zu betrachten.
- Sicherheitsbetrachtungen
  - Mehrere Managementregionen können dann nötig werden, wenn das Managementprodukt zwar verschiedene Verschlüsselungsmechanismen pro Region unterstützt, von denen jedoch pro Region in der Regel nur eine zum Einsatz kommen kann. Sollen zwischen einzelnen Managementkomponenten tatsächlich verschiedene Mechanismen zum Einsatz kommen, so sind mehrere Managementregionen nötig. Beispiel: Ein System aus mehreren Datenbank-Servern mit sensitiven Daten und den zugehörigen Clients, die selbst keine Daten speichern, wird verwaltet. Die Managementkonsole soll mit den Servern nur stark verschlüsselt kommunizieren, da auch die Datenbanken über das Managementsystem verwaltet werden. Die Kommunikation mit den Clients soll hingegen aus Performancegründen nur schwach verschlüsselt geschehen. In diesem Fall müssen in der Regel zwei Managementregionen gebildet werden: eine Region, in der die Server enthalten sind, und eine zweite Region, die die Clients umfasst.
  - Mehrere Managementregionen erhöhen die Ausfallsicherheit, da z. B. beim Ausfall einer Managementregion die restlichen Regionen unabhängig davon weiterhin verwaltet werden können.
  - Einfluss hat auch die Anzahl der zu verwaltenden Rechner pro Managementregion. Die meisten Produkte geben Empfehlungen über die Anzahl der Rechner, die durch den Managementserver einer Region verwaltet werden können. Eine Zahl von 200 Rechnern pro Server ist aber keine Seltenheit.
- Welche Maschinen sollen als Managementserver dienen? In der Regel ist mit steigender Anzahl von Clients an einem Managementserver mit Performanceeinbußen zu rechnen. Dies muss bei der Planung berücksichtigt werden.
- Welche physikalische Anordnung müssen die Managementserver haben und wo werden sie aufgestellt? Die Lokation eines Servers hat z. B. Einfluss darauf, wie Rechner, die von diesem Server verwaltet werden sollen, über das Netz an diesen angebunden sind. Bei einigen Plattformen gibt es z. B. Mindestanforderungen an die Kommunikationsbandbreite zwischen Server und Client (so unterstützt z. B. TME 10 keine Anbindung von Clients über Leitungen mit weniger als 14.4 Kbps). Dies hat direkte Auswirkungen auf die mögliche Managementsystemkonfiguration und macht z. B. die Neuanschaffung von Rechnern oder den Ausbau von Netzverbindungen nötig.
- Sind so genannte Gateways oder Proxies nötig, die ein hierarchisch aufgebautes Management und/oder den Anschluss an Produkte von Drittanbietern ermöglichen?

- Einige Systeme unterscheiden zwischen so genannten "Managed Nodes" und "Endpoints". Bei beiden handelt es sich um Arbeitsplatzrechner, sie unterscheiden sich aber in der Art und Weise, wie diese in das Managementsystem eingebunden sind: So halten "Endpoints" z. B. im Unterschied zu "Managed Nodes" keine eigene lokale Datenbank mit Managementinformationen vor und können auch nicht zur Weiterleitung von Managementinformationen an weitere Rechner benutzt werden. Hier muss entschieden werden, welche Maschinen als "Managed Nodes" in das Managementsystem eingebunden sein sollen und welche lediglich als "Endpoints" verwaltet werden. In der Regel sollte das Gros der Arbeitsplatzrechner als "Endpoint" eingebunden werden.

Die so erstellte Managementstrategie induziert eine Reihe von Anforderungen an das zu beschaffende Managementprodukt. Durch die Gewichtung der Anforderungen ergibt sich eine konkrete Produktauswahl. Die Managementstrategie muss nun dahingehend überprüft werden, ob sie mit dem zur Verfügung stehenden Funktionsumfang vollständig umgesetzt werden kann. Eine Reformulierung der Strategie kann dadurch in einzelnen Bereichen notwendig sein. Beispiel: Die Produktauswahl ergibt, dass das System, das starke Verschlüsselung unterstützt, leider nicht die Delegation von Verwaltungsaufgaben an "Subadministratoren" erlaubt. Daraufhin muss die Managementstrategie angepasst werden (korrekte Gewichtung der Anforderungen vorausgesetzt).

Prüffragen:

- Sind alle der vom System-Managementsystem zu verwaltenden Objekte festgelegt?
- Ist eine anzuwendende Sicherheitsrichtlinie für das System-Managementsystem spezifiziert?
- Existiert eine Sicherheitsrichtlinie, die den Bereich Systemmanagement abdeckt?
- Existieren Regelungen und Vorgehensweisen im Fall einer Sicherheitsverletzung bei Netz- und Systemkomponenten?
- Wird überprüft, ob die Systemmanagementstrategie mit möglichen Systemmanagementprodukten vollständig umgesetzt werden kann?

# M 2.170 Anforderungen an ein Systemmanagement-System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Ein Systemmanagement-System dient zur Unterstützung der Administratoren eines lokalen Netzes . Ein Systemmanagement-System muss daher gewisse Voraussetzungen erfüllen, um die Administratoren geeignet unterstützen zu können. Die Anforderungen an ein solches System hängen jedoch wesentlich vom geplanten Einsatz (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) und von der gewählten Architektur des Systemmanagement-Systems ab (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*).

Ein Systemmanagement-System sollte folgende Funktionen bereitstellen:

- Benutzermanagement
  Hierzu gehören das Hinzufügen, Verändern und Löschen von Benutzer- und Gruppenkonten.
- Policymanagement
  Zugriffsrechte sollten sowohl für Zugriffe aus dem und in das lokale Netz als auch für Zugriffe auf das bzw. vom Internet verwaltet werden können.
- Softwaremanagement
  Das Hinzufügen, Löschen und Aktualisieren von Softwarekomponenten sollte mit dem Systemmanagement-System möglich sein.
  Daneben ist insbesondere für die Einführungsphase das automatische Feststellen der installierten Software unter Umständen wichtig. Eine Verwaltung von Softwarelizenzen ist wünschenswert.
- Feststellen, Verändern und Verwalten von Systemkonfigurationsdaten.
- Verwalten von Applikationsdaten
  Es muss möglich sein, Dateien eines Datenbanksystems oder Konfigurationsdateien einer Applikation zu verwalten, so dass z. B. das Verteilen einer neuen Version einer Datenbank oder die Verteilung neuer Konfigurationsdateien möglich ist.
- Überwachen von Systemkomponenten
  Dies kann auch für externe Komponenten sinnvoll sein, die nicht der eigenen Administration unterliegen, zum Beispiel für den Router des Internet Service Providers (ISP), über den der Internet-Anschluss realisiert ist.
- Applikationsmanagement
  Das Verwalten von Software auf Anwendungsebene sollte möglich sein, z. B. die Verwaltung von HTTP-Zugriffsrechten auf die Daten eines WWW-Servers ("Realms").

Idealerweise lässt ein solches System die Delegation von administrativen Aufgaben zu, so dass z. B. ein Systemverwalter einem Arbeitsgruppensystemadministrator das Recht zum Installieren von Software auf den Rechnern der Arbeitsgruppe einräumen kann. Dieser Mechanismus ist insbesondere in mittleren und großen Netzen notwendig.

Die Netz- und Systemadministration werden in der Regel durch die gleichen administrativen Einheiten in einem Unternehmen bzw. einer Behörde durchgeführt. Esempfiehlt sich daher zu prüfen, inwieweit ein vorhandenes Netzmanagementsystem in ein zu beschaffendes Systemmanagement-System integriert werden kann.

Neben diesen vorwiegend funktionalen Anforderungen ergeben sich auch technische Anforderungen im Rahmen der Kriterien, die für die Auswahl einer Systemmanagement-Software relevant sind (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*). Besonders sind hier folgende hervorzuheben:

- Das Managementsystem muss in der Lage sein, die Betriebssysteme aller für das Management genutzten und aller verwalteten Rechner zu unterstützen (betriebssystemspezifische Komponenten des Managementsystems, graphische Benutzungsoberfläche).
- Existiert bereits ein lokales Datenbanksystem, so sollte das Managementsystem die Möglichkeit besitzen, seine Managementinformationen im vorhandenen Datenbanksystem zu speichern.
- Das Managementsystem sollte erweiterbar sein. Dies betrifft einerseits die Komponenten des Managementsystems (z. B. Modulkonzept mit der Möglichkeit, Module jederzeit nachkaufen und integrieren zu können), aber auch die Funktion des Managementsystems (z. B. Programmier-API, um eigene Komponenten anschließen zu können).

Generell können die in M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes* vorgestellten Kriterien zur Kategorisierung von Anforderungen im Rahmen der vorliegenden Maßnahme herangezogen werden. Für ausgesuchte Kategorien ergeben sich die Anforderungen durch die Festlegung einer Vorgabe im Rahmen des jeweiligen "Wertebereiches".

Prüffragen:

- Sind die Anforderungen an das einzusetzende Systemmanagement-System festgestellt?
- Mittlere und große Netze: Ermöglicht das Systemmanagementsystem die Delegation von administrativen Aufgaben?

# M 2.171 Geeignete Auswahl eines Systemmanagement-Produktes

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Nach Aufnahme der aktuellen Systemsituation (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagement-Systems*) und Festlegung der Managementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) muss ein geeignetes Systemmanagement-System ausgewählt werden. Je nach Größe des zu verwaltenden Systems können hier unterschiedliche Realisierungen zweckmäßig sein:

- Für kleine Systeme kann das Systemmanagement von der Systemadministration "von Hand" erledigt werden.
- Für kleine und mittlere Systeme kann das Systemmanagement auch durch eine Sammlung von einzelnen Tools durchgeführt werden.
- Für große Systeme sollte ein Systemmanagement-System benutzt werden.

Moderne netzfähige Betriebssysteme sind in der Regel schon mit Funktionen ausgestattet, die eine zentrale Verwaltung z. B. von Benutzern und Benutzergruppen erlauben. Für den Unix-Bereich kann hier z. B. NIS oder NIS+ genannt werden, im Windows-Bereich erlaubt das Windows Domänen-Konzept eine zentrale Benutzerverwaltung über den Domain Controller. In der Regel existieren zudem auch Möglichkeiten, ein netzweites Policymanagement zu betreiben.

In kleineren und mittleren Netzen stellen daneben das Softwaremanagement, das Management der Rechnerkonfigurationen sowie das Überwachen von Systemkomponenten die drängendsten Problembereiche dar. Hier können dann zusätzliche Softwaretools eingesetzt werden, die die Aufgaben einzeln übernehmen können. Insbesondere in den Bereichen, die auch durch das Netzmanagement abgedeckt sind (Konfigurationsmanagement, Überwachung), kann der Einsatz eines Netzmanagement-Tools in Betracht gezogen werden.

Für den Windows-Bereich lassen sich z. B. Tools wie die "Microsoft Management Console", die eine einheitliche zentrale Sicht auf alle Administrationstools anbietet, sowie den "Microsoft System Center Configuration Manager (SCCM)" nennen. So bietet z. B. das Produkt SCCM dem Administrator folgende Möglichkeiten:

- Inventarisieren von Hard- und Software-Komponenten
- Installieren und Verteilen von Daten und Applikationen auf Netzrechnern
- Fernwartung
- Unterstützung bei der Fernadministration von Rechnern über das Netz

Für den Unix-Bereich kann z. B. zur Verwaltung und Verteilung von Software das Programm "rdist" eingesetzt werden, mit dem auf entfernten Rechnern Software installiert oder aktualisiert werden kann. Dabei ist es möglich, aus einem zentralen Softwarepool genau die Produkte auf den jeweiligen Rechnern zu installieren, die von den Mitarbeitern für die Erledigung ihrer Aufgaben benötigt werden. Weitere, auch kostenfrei, erhältliche Zusatzprogramme (meist aus dem universitären Umfeld) erlauben z. B. die Überwachung des Netzes über SNMP.

Die so zusammengestellten Lösungen bieten für kleinere und mittlere Netze eine kostengünstige Alternative. Allerdings setzen sie in der Regel einen ver-

sierten Administrator voraus, der auch unter Umständen durch Eigenprogrammierung Anpassungen an lokale Gegebenheiten vornimmt oder Zusatzfunktionalität integriert.

Für größere und große Netze sind solche Lösungen jedoch ungeeignet, da die Funktionalitäten in verschiedenen, nicht integrierten Tools angesiedelt ist. Für große Unternehmens- oder Behördennetze kommen nur Systemmanagement-Systeme in Frage. Vor der Einführung eines solchen Systems sollte beachtet werden, dass dies in der Regel einen beträchtlichen Eingriff in das laufende System darstellt und gut geplant werden muss. Die Wahl des richtigen Managementsystems ist deshalb wichtig. Folgende Kriterien sollten bei der Wahl des zu beschaffenden Systems beachtet werden:

- Welchen Funktionsumfang bietet das Produkt an?
- Kosten
  - für die Anschaffung der Software
  - für die Anschaffung zusätzlicher Hardware (Bei einigen Systemen müssen ein oder mehrere zentrale Managementserver angeschafft werden.)
  - für Installations- und Betriebsaufwand (unter Umständen müssen sogar Externe engagiert werden.)
  - für die Schulung der Mitarbeiter
  - andere (z. B. Migrationskosten bei einer existierenden Plattform, Anpassung/Neuentwicklung lokaler Software, bauliche Maßnahmen z. B. gesicherter Serverraum)
- Investitionssicherung
  - Inwieweit ist das Systemmanagement-Produkt skalierbar (z. B. Anzahl der Rechner erweiterbar)?
  - Kann die Plattform mit dem Unternehmen wachsen (z. B. Anzahl der möglichen Managementdomänen, Delegation von Aufgaben)?
  - Wie sind die Migrationspfade zur Plattform?
  - Wie sind die Migrationspfade von dieser Plattform zu einer anderen Plattform?
- Integrationsmöglichkeit mit anderen Produkten
  - Welche Server- bzw. Client-Systemplattformen werden unterstützt?
  - Kann ein bestehendes Netzmanagement-System integriert werden?
  - Kann ein bestehendes Datensicherungssystem integriert werden?
  - Welche Applikationen von Drittanbietern gibt es für dieses Produkt?
- Zuverlässigkeit und Ausfallsicherheit
  - Gibt es Aussagen oder sogar Garantien über maximale Ausfallzeiten?
  - Ist ein Hotswap für zentrale Komponenten möglich?
  - Existiert ein systemeigener Backup- und Recovery-Mechanismus? Bei einem Ausfall des Managementsystems müssen innerhalb des Managementsystems Mechanismen zum geregelten Wiederanlaufen existieren. Dies umfasst unter Umständen das Einspielen von Daten aus einer Datensicherung und die automatische Konsistenzprüfung - idealerweise mit Konfliktauflösung bei der Feststellung von Inkonsistenzen.
  - Werden regelmäßig Updates zur Verfügung gestellt? Sind sie einfach einspielbar?
- Sicherheit: Zugriffsbeschränkungen auf die Managementfunktionen
  - Kann der Zugriff auf Benutzer-ID-Ebene (Welcher Benutzer darf was?) eingeschränkt werden?

  - Kann der Zugriff auf Komponentenebene (Welcher Rechner darf was?) eingeschränkt werden?
  - Kann der Zugriff auf die ausführbaren Kommandos Benutzer- oder Systemabhängig eingeschränkt werden?
  - Kann eine Aufteilung der Administrationstätigkeiten vorgenommen werden? Kann also z. B. die Verwaltung von Komponenten auf bestimmte Bereiche eingeschränkt werden (z. B. nur die Abteilungsrechner)?
- Sicherheit: Administration von Rechnern über das Netz
  - Wie sind Fernzugriffe abgesichert?
  - Können Fernzugriffe verschlüsselt erfolgen?
  - Ist sichergestellt, dass eine (starke) Authentisierung vor einer Fernadministration erforderlich ist?
  - Ist es möglich, die Berechtigung für Fernadministration auf bestimmte Personen oder Rollen einzuschränken?
  - Wird der Benutzer automatisch über Fernzugriffe informiert?
- Sicherheit: Datensicherheit, Datenschutz
  - Werden die gesammelten Daten sicher abgelegt (Zugriffsbeschränkungen, Verschlüsselung)?
  - Findet die Datenübertragung zwischen den Managementkomponenten gesichert statt (Authentisierung, Verschlüsselung, Integritätssicherung)?
  - Kann die Art der gesammelten Informationen reguliert werden (Anonymisierung, Rückverfolgung, Beweisbarkeit)?
  - Ist die Integration von Virensuchprogrammen möglich?
  - Welche Protokollierungsmöglichkeiten werden angeboten?
  - Kann die lokale Softwareeinspielung überwacht oder verhindert werden?
- Benutzerfreundlichkeit
  - Gibt es ein graphisches Benutzungsinterface ?
  - Wie einfach ist die Navigation?
  - Wird die lokale Sprache oder auch mehrere Sprachen (bei globalem Einsatz) unterstützt?
  - Lassen sich Programme einfach ausführen (auch auf entfernten Rechnern)?
  - Wie einfach lässt sich das Interface vom Benutzer umgestalten?
  - Werden Ausnahmen und Alarmierungen geeignet angezeigt?
  - Ist das Monitoring, auch im Detailgrad, einstellbar?
  - Wird die Komplexität von Netzkomponenten geeignet "versteckt" (So dass der Benutzer nicht ein Experte für die jeweilige Komponente, die verwaltet werden soll, sein muss)?
  - Können alle Funktionen über das gleiche Benutzungsinterface erreicht werden?
  - Sind Onlinehilfen und Anleitungen vorhanden?
- Ergonomie beim Management komplexer Systeme
  - Werden verschiedene Netzprotokolle, Netzkomponenten und Betriebssysteme unterstützt?
  - Wie geht die Plattform mit geographisch verteilten Systemen um und wie ist deren Repräsentation?
  - Wie einfach ist es, neue Komponenten zu integrieren oder aus dem System zu entfernen (Autodiscovery, manuell)?

- Konformität zu Standards (je nach Umgebung kann die Konformität zu mindestens einem Standard erforderlich sein)
    - Plattformen
        - Distributed Management Environment (DME) von der Open Software Foundation (OSF)
        - Spezifikation der Desktop Management Task Force (DMTF)
    - Datenbank
        - Welche DBMSe (Data Base Management Systeme) werden unterstützt?
        - Wird SQL als Anfragesprache unterstützt, für den Fall, dass die Managementsoftware eine eigene Datenbank enthält?
    - CORBA (Common Object Request Broker Architecture) der Object Management Group (OMG)
    - Application Program Interface (API), für den Fall, dass eigene Erweiterungen des Managementsystems notwendig sind (z. B. APIs für SNMP, XMP, DMI).

Die hier angeführten Aspekte sind als Anhaltspunkte bei der Bewertung von Managementsystemen zu verstehen. Je nach lokalen Gegebenheiten sollten aufgrund der aktuellen Systemsituation (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagement-Systems*) und aufgrund der Managementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) Anforderungen an das Managementsystem formuliert werden, die als "K.O.-Kriterien" bei der Entscheidung herangezogen werden können. Die obigen Kriterien sollten immer eine Gewichtung erfahren, die die lokalen Präferenzen wiedergeben.

Die Anforderungen an das Managementsystem und die Leistungen des ausgewählten Managementsystems sind in der Regel nicht vollständig in Einklang zu bringen. Dies macht es notwendig, die erstellte Managementstrategie nach Auswahl des konkreten Produktes an dessen Funktionsumfang anzupassen.

Prüffragen:

- Erfolgt die Auswahl eines geeigneten Systemmanagement-Systems auf Grundlage der zuvor festgestellten Anforderungen?

# M 2.172 Entwicklung eines Konzeptes für Webangebote

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Bevor ein Webangebot eingerichtet wird, muss zunächst in einem Konzept dargestellt werden, welche Informationen und Dienste über Webserver angeboten werden sollen. Das Konzept sollte mindestens einen allgemeinen und einen organisatorischen Teil enthalten:

Im allgemeinen Teil sollte beschrieben werden,

- welche Ziele die Institution mit dem Webangebot verfolgt (handelt es sich um ein reines Informationsangebot, um ein E-Commerce- oder ein E-Government-Angebot?),
- welches die Zielgruppen des Webangebots sind und
- welche Informationen oder Dienstleistungen in dem Webangebot zur Verfügung gestellt werden sollen.

Im organisatorischen Teil sollte eine grobe Übersicht darüber gegeben werden, wer in der Institution verantwortlich ist für

- die Bereitstellung und Aktualisierung der Informationen und
- die Ausarbeitung und Pflege des optischen Erscheinungsbildes des Webangebots (*Webdesign*).

Im organisatorischen Teil des Web-Konzepts sollte auch festgelegt werden, wer für die technischen Aspekte des Betriebs des Webservers verantwortlich ist.

Das Konzept für das Webangebot sollte regelmäßig auf Aktualität überprüft werden. Bei Änderungen in den Zielen oder Strategien der Institution muss geprüft werden, welche Auswirkungen diese auf das Web-Konzept haben.

Bei der Entwicklung des Konzeptes sollten folgende Aspekte berücksichtigt werden:

Ein Webangebot kann als rein interner Informationsdienst eingesetzt werden, als Mittelpunkt eines Intranets, oder als öffentliches Angebot im Internet, das verschiedene Dienste anbietet. Je nach Art der geplanten Ausgestaltung unterscheiden sich auch die Sicherheitsanforderungen, die an den Webserver gestellt werden müssen. In einer kleinen Institution, in der ein Webserver als Intranet-Server ohne kritische Anwendungen betrieben wird, sehen die Anforderungen ganz anders aus als für einen Webserver, der ans Internet angeschlossen werden soll und vielleicht sogar Daten enthält, die nicht jeder abrufen können soll.

Wenn sowohl im Intranet als auch im Internet Web-Dienste angeboten werden sollen, empfiehlt es sich, hierfür zwei getrennte Systeme einzusetzen: einen Intranet-Webserver und einen Internet-Webserver. Wenn der Internet-Webserver auch mit dem internen Netz verbunden werden soll, muss der Übergang zum internen Netz durch eine Firewall geschützt werden, siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*.

Wenn vorgesehen ist, dass Teile der Inhalte des Webservers aus einer Datenbank kommen sollen, muss auch die Verbindung zur Datenbank in das Firewall-Konzept für den Webserver einbezogen werden. Was bei der Anordnung

von Informationsservern zu beachten ist, ist in M 2.77 *Integration von Servern in das Sicherheitsgateway* beschrieben. Bei der Erarbeitung des Konzepts für das Webangebot sollte zumindest grob festgelegt werden, wie die Anbindung ans Internet geregelt ist und welche Arten von Verbindungen zum internen Netz benötigt werden.

Der Anschluss ans Internet darf erst dann erfolgen, wenn überprüft worden ist, dass mit dem gewählten Web-Konzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Ein Webserver für die Präsenz einer Institution im Internet muss nicht zwangsläufig von dieser selbst betrieben werden. Wenn die Betriebskosten oder der Administrationsaufwand zu hoch oder die Restrisiken zu unkalkulierbar erscheinen, können auch die entsprechenden Angebote von Internet Service Providern oder anderen Dienstleistern in Anspruch genommen werden, einen Webserver durch diese betreiben zu lassen. In diesem Fall muss der Baustein B 1.11 *Outsourcing* berücksichtigt werden.

Prüffragen:

- Gibt es ein Konzept für die Web-Nutzung mit einem allgemeinen und einem organisatorischen Teil?
- Werden die Ziele der Organisation, die Zielgruppen und die Informationen oder Dienstleistungen des Webangebots definiert?
- Werden Verantwortliche für die Bereitstellung und Aktualisierung der Informationen, die Ausarbeitung und Pflege des Webdesigns und die technischen Aspekte des Webserverbetriebs festgelegt?
- Wird das Konzept für das Webangebot regelmäßig auf Aktualität überprüft und nötigenfalls angepasst?
- Entsprechen die Sicherheitsanforderungen dem Verwendungszweck des Webservers?
- Wenn der Internet-Webserver mit dem internen Netz verbunden ist: Wird der Übergang vom Webserver zum internen Netz durch eine Firewall geschützt?
- Bei Anbindung des Webservers an eine Datenbank: Wird die Verbindung des Webservers zur Datenbank auch beim Firewall-Konzept eingeplant?

# M 2.173 Festlegung einer Webserver-Sicherheitsstrategie

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Webserver sind für Angreifer sehr attraktive Ziele, da einem erfolgreichen Angriff oft sehr große Publizität zuteil wird. Daher muss der Absicherung eines Webservers ein hoher Stellenwert eingeräumt werden. Vor dem Einrichten eines Webservers sollte in einer Webserver-Sicherheitsstrategie beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind. Anhand der in der Webserver-Sicherheitsstrategie festgelegten Anforderungen kann dann regelmäßig überprüft werden, ob die getroffenen Maßnahmen ausreichend sind.

In der Sicherheitsstrategie für den Betrieb eines Webservers sollten die folgenden Fragen beantwortet werden:

- Sind Verantwortliche für den sicheren Betrieb des Webservers (Administratoren) und für die inhaltliche Betreuung (Redakteure) benannt worden?
- Wie werden die Verantwortlichen geschult, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen?
- Wer erhält Zugriff auf den Webserver mit welchen Rechten?
- Wer darf welche Informationen einstellen?
- Wer ist für die Aktualität und Korrektheit der Informationen verantwortlich? Falls in einem Bereich mehrere Organisationseinheiten oder Personen Informationen einstellen dürfen, so muss außerdem ein Gesamtverantwortlicher benannt sein, der bei Konflikten entscheidet.
- Welche anderen Systeme und welche Netzverbindungen sind für den sicheren Betrieb des Webservers wichtig? Können zeitweise Störungen oder Ausfälle dieser Systeme gegebenenfalls überbrückt werden?
- Welche Informationen dürfen nicht auf dem Webserver eingestellt werden (z. B. weil die Inhalte vertraulich sind, nicht zur Veröffentlichung geeignet sind oder nicht der Firmen- bzw. Behördenpolitik entsprechen)?
- Muss die Integrität und die Vertraulichkeit der Daten bei der Übertragung vom Webserver zum Client geschützt werden? Ist eine Authentisierung des Webservers gegenüber den Clients oder der Clients gegenüber dem Webserver erforderlich?
- Welche Zugriffsbeschränkungen auf den Webserver sollen realisiert werden (siehe auch M 2.175 *Aufbau eines Webservers*)?

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zu gewährleisten:

- Auf Webservern dürfen nur Dateien eingestellt werden, die für die Veröffentlichung freigegeben wurden. Es muss festgelegt werden, welche Arten von Informationen zur Veröffentlichung geeignet sind und wer diese freigibt.
- Vor dem Einstellen von Dateien auf einem Webserver sind diese explizit auf Schadsoftware und Restinformationen zu überprüfen. Außerdem sind sie (zumindest stichprobenartig) daraufhin zu überprüfen, ob die Inhalte zur Veröffentlichung freigegeben sind.
- Es wird empfohlen, notwendige Funktionen im eigenen Webangebot nicht mit Aktiven Inhalten umzusetzen, sondern dies möglichst Server-seitig zu realisieren.

Alle Regelungen zum Webserver-Einsatz sind schriftlich zu fixieren und sollten den Mitarbeitern jederzeit zur Verfügung stehen.

Die Redakteure müssen vor der Webserver-Nutzung geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden.

Insbesondere wenn der Webserver ein öffentliches Webangebot beherbergt, müssen in der Sicherheitsstrategie auch Reaktionen auf bestimmte webserver-spezifische Sicherheitsvorfälle festgelegt werden (siehe auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*).

- Es sollte festgelegt werden, wie verfahren wird, wenn nicht freigegebene Informationen auf dem Webserver veröffentlicht wurden. Eventuell reicht das bloße Löschen der entsprechenden Dokumente nicht aus, da diese schon von Besuchern gelesen wurden. Ein solcher Vorfall muss zumindest dokumentiert werden. In Abhängigkeit von der Brisanz der Informationen müssen eventuell die Pressestelle, das IS-Management, die Behörden- oder Unternehmensleitung oder externe Stellen informiert werden.
- Es sollte beschrieben werden, was beim Verdacht auf einen Hackerangriff auf den Webserver zu tun ist. Wichtig ist vor allem die Frage, wann der Server notfalls vom Netz genommen werden muss und wer die Entscheidung dazu trifft.
- Es sollte eine Reaktion auf ein *Defacement* des Webservers festgelegt werden, also für den Fall, dass nach einem erfolgreichen Einbruch auf dem Webserver Daten oder besonders die Homepage von den Angreifern verändert wurden. In einem solchen Fall müssen grundsätzlich auch die Behörden- oder Unternehmensleitung sowie die Pressestelle bzw. die für Öffentlichkeitsarbeit zuständige Organisationseinheit informiert werden.

Diese Punkte sollten selbst dann berücksichtigt werden, wenn der Schutzbedarf des Webangebots ansonsten nur als niedrig eingeschätzt wird. Insbesondere ein Hackerangriff oder ein Defacement können unabhängig vom konkreten Schutzbedarf bei allen öffentlichen Webangeboten passieren.

Teil einer Sicherheitsstrategie muss auch die regelmäßige Informationsbeschaffung über potentielle Sicherheitslücken sein, um rechtzeitig Vorsorge dagegen treffen zu können. Neben den in M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* angesprochenen Informationsquellen ist für Sicherheitshinweise zur Web-Nutzung besonderes die "World Wide Web Security FAQ" eine wertvolle Quelle. Die Master-Kopie dieses Dokumentes ist unter *http://www.w3.org/Security/Faq/* zu finden.

Prüffragen:

- Gibt es eine Web-Sicherheitsstrategie in der Sicherheitsmaßnahmen mit ihrem jeweils geforderten Umfang festgehalten sind?
- Gibt es Regelungen für die Reaktion auf bestimmte webserverspezifische Sicherheitsvorfälle?
- Werden für die rechtzeitige Vorsorge gegen Sicherheitslücken regelmäßig Informationen beschafft?

# M 2.174 Sicherer Betrieb eines Webservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Webserver sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Das Betriebssystem und die Software müssen so konfiguriert sein, dass der Rechner so gut wie möglich gegen Angriffe geschützt wird. Solange der Rechner nicht entsprechend konfiguriert ist, darf er nicht ans Netz genommen werden.

Bei der Konfiguration der Webserver-Anwendung sollten, unabhängig von der eingesetzten Webserveranwendung, einige grundlegende Aspekte berücksichtigt werden. Wie diese im einzelnen konfiguriert werden, hängt von der Webserver-Anwendung ab.

Meist existieren Optionen, mit denen festgelegt werden kann, ob bei einer HTTP-Anfrage nach einem Verzeichnis (also ohne Angabe eines konkreten Dateinamens), der Inhalt des betreffenden Verzeichnisses aufgelistet werden soll, oder ob stattdessen bestimmte Dateien (beispielsweise *index.html*) zurückgegeben werden sollen. Dies sollte folgendermaßen konfiguriert werden:

- Falls eine Index-Datei existiert, wird diese zurückgeliefert.
- Falls nicht, wird eine entsprechende Fehlermeldung zurückgegeben.

Falls festgelegt werden kann, dass Programme oder CGI-Skripte nur in bestimmten Verzeichnissen ausgeführt werden dürfen, so sollte diese Option auf jeden Fall sehr eng eingestellt werden. Keinesfalls sollte die Ausführung von Programmen für den gesamten WWW-Bereich freigegeben werden. Es ist empfehlenswert, wenn möglich für Programme und Skripte ein eigenes Verzeichnis anzulegen und die Ausführung nur in diesem Verzeichnis zu gestatten.

Oft kann festgelegt werden, ob Dateien oder Verzeichnisse, die mittels eines symbolischen Links (Unix) oder einer Verknüpfung (Windows) in den WWW-Dateibaum "eingeblendet" wurden, angezeigt werden sollen. Dies sollte möglichst unterbunden werden, da auf diese Weise leicht Dateien zugreifbar werden können, die eigentlich nicht veröffentlicht werden sollen.

Es ist zu empfehlen, eine Checkliste wie die folgende regelmäßig abzuarbeiten, um einen sicheren Betrieb zu gewährleisten.

**Checkliste:**

1. Sind nur die benötigten Komponenten installiert?

2. Ist die Webserver-Anwendung so restriktiv wie möglich konfiguriert? Beispielsweise sollten CGI-Programme entweder ganz gesperrt werden oder aber die CGI-Programme auf ein eigenes Verzeichnis beschränkt sein. Der Dateizugriff des Webserver-Prozesses sollte auf einen Teil des Verzeichnisbaums eingeschränkt sein. Für Administration und Betrieb des Servers sollten eigene unprivilegierte Benutzerkennungen verwendet werden.

3. Sind alle überflüssigen CGI-Programme, asp-Seiten, sonstige Demo-Anwendungen und Web-Seiten gelöscht?

4. Sind nur die unbedingt nötigen Ports zugänglich (siehe auch M 4.97 *Ein Dienst pro Server*)? Auf einem Webserver wird der HTTP-Dienst üblicherweise über Port 80 angesprochen. Falls die Administration des Servers oder die Pflege der Webserver-Dateien über das Netz erfolgt, können noch weitere Dienste erforderlich sein. In diesem Fall sollte aber der Zugriff auf diese Dienste so restriktiv wie möglich geregelt werden (siehe auch M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken*).

5. Ist eine angemessene regelmäßige Sicherung des Datenbestandes gewährleistet (siehe Baustein B 1.4 *Datensicherungskonzept*)?

6. Falls CGI-Programme genutzt werden, sind diese ausreichend sicher programmiert? Es dürfen keine Eingabewerte ungeprüft übernommen werden. Es muss sichergestellt sein, dass Buffer-Overflows und Race-Conditions ausgeschlossen sind. In allen Perl-Skripten sollte der Taint-Check aktiviert sein.

7. Gibt es eine funktionierende Routine für einen regelmäßigen Integritätscheck (z. B. Tripwire, siehe M 4.93 *Regelmäßige Integritätsprüfung*)?

8. Wird die Konfiguration regelmäßig überprüft? Werden Konfigurationsänderungen dokumentiert?

**Beispiel: Aufbau eines einfachen Webservers**

Als einfacher Webserver wird ein Server betrachtet, bei dem sich die Inhalte einzelner Seiten nur selten ändern, keine CGI-Programme verwendet werden und es keinen besonderen Zugriffsschutz gibt. Die einzelnen WWW-Dokumente werden über einen Datenträger auf den Webserver eingespielt. Bei einem solchen Server können alle Systemdateien und auch alle HTML-Seiten mit einem Schreibschutz versehen werden. Ein Angreifer kann bei einem solchen Aufbau zwar noch temporäre Dateien und Protokolleinträge abändern, das System selber aber nicht mehr. Ein solcher Zugriffsschutz sollte durch ein physikalisch schreibgeschütztes Medium realisiert werden, z. B. eine oder mehrere CD-ROMs oder eine schreibgeschützte Wechselplatte. Zumindest aber sollten regelmäßige Integritätsprüfungen durchgeführt werden (siehe M 4.93 *Regelmäßige Integritätsprüfung*).

In dem http-Daemon sollten die nicht benötigten Funktionalitäten abgeschaltet werden, wie z. B. die Möglichkeit zum Ausführen von CGI-Skripten. Auf jeden Fall sollten mitgelieferte CGI-Programme entfernt werden.

Bei einer häufig vorkommenden Variante eines einfachen Webservers können die Dokumente mit entsprechenden Berechtigungen auf dem Webserver interaktiv abgeändert werden. In diesem Fall ist der Schutz vor unbefugten Veränderungen und eine regelmäßige Integritätsprüfung in kurzen Intervallen besonders wichtig.

Prüffragen:

- Sind das Betriebssystem und die Software der Webserver so konfiguriert, dass der Rechner so gut wie möglich gegen Angriffe geschützt ist?
- Liegen Verzeichnisse, in denen abrufbare Dateien gespeichert sind auf einer separaten Partition einer Festplatte?
- Bei HTTP-Anfrage nach einem Verzeichnis: Wird eine Fehlermeldung ausgegeben falls keine Index-Datei existiert und sonst die Index-Datei?

- Falls die Festlegung der Ausführungsorte von Programmen oder CGI-Skripten möglich ist: Können die Programme oder cgi-Skripte nur in den für sie bestimmten Verzeichnissen ausgeführt werden?
- Ist die Einblendung von Links (Unix) oder Verknüpfungen (Windows) in den WWW-Dateibaum nicht möglich?

# M 2.175 Aufbau eines Webservers

**Verantwortlich für Initiierung:** Administrator, Behörden-/ Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter IT

Um einen Webserver aufbauen zu können, muss neben adäquater Hardware auch entsprechende Software beschafft werden. Dafür stehen eine Vielzahl von Produkten zur Verfügung. Bei der Auswahl ist neben der Stabilität insbesondere Wert auf die Sicherheitsmechanismen zu legen (zur Beschaffung und Installation siehe auch Baustein B 1.10 *Standardsoftware*).

**Organisationsstruktur anpassen**

Es muss überlegt werden, welche Informationen im Internet bzw. in einem Intranet zur Verfügung gestellt werden sollen. Weiterhin ist zu klären, wie und wo Dokumente erstellt werden, wer welche Dokumente erzeugt, welche Dokumente wo zum Einsatz kommen und wer diese Dokumente benötigt. Auf Basis dieser Erkenntnisse sollten dann Richtlinien für ein einheitliches Erscheinungsbild von Dokumenten, Dateinamen und Verzeichnisnamen aufgestellt und nach Möglichkeit standardisierte Entwicklungswerkzeuge bestimmt werden. Eventuell sollte ein eigenes Webserver-Redaktionsteam eingerichtet werden (siehe M 2.272 *Einrichtung eines Internet-Redaktionsteams*).

**Verantwortliche benennen**

Beim Betrieb eines Webservers, egal ob intern oder extern, sollte nicht jeder Benutzer beliebig Dateien einstellen können. Es sollte daher ein Verantwortlicher für das Einstellen von Informationen benannt werden, der neue Dateien auch auf die Einhaltung der Richtlinien überprüft. Je nach Größe der Organisation können auch weitere Teil-Verantwortliche für einzelne Organisationseinheiten oder Teilbereiche des Webservers benannt werden. Entsprechend der hier gewählten Organisationsstruktur ist auch die Rechtevergabe und die Verzeichnisstruktur auf dem Webserver festzulegen. Vor allem sollte jeder Teil-Verantwortliche nur Zugriff auf die von ihm betreuten Unterverzeichnisse haben.

Um sicherzustellen, dass die angelegten Dateien und Verzeichnisse immer den jeweiligen Richtlinien genügen, sollte deren Einhaltung automatisiert überprüft werden, z. B. über geeignete Skripten oder Makros. Ein entsprechend vorbereitetes Programm sollte für alle zur Verfügung gestellt werden und nach jeder Änderung aufgerufen werden. Dabei sollte insbesondere überprüft werden, ob die Zugriffsrechte aller

- Verzeichnisse,
- Dateien und
- CGI-Skripte (falls eingerichtet)

korrekt gesetzt wurden.

Ein Protokoll über die durchgeführten Änderungen sollte ebenfalls direkt erzeugt werden.

Ein allgemeines Problem bei der Einrichtung und beim Betrieb eines Webservers ist die notwendige Zusammenarbeit vieler verschiedener Personen mit unterschiedlichen Kompetenzen. So werden Aufgaben wie

- Erstellen neuer Inhalte,
- Administration des Webservers,

- Durchführung des Designs des Webauftritts,
- Entwurf einzelner Grafiken,
- Programmierung von Zusatzfunktionalität für den Webserver (z.B. eine Datenbankanbindung) und
- Programmieren von Zusatzfunktionalität, die auf dem Web-Client genutzt wird (Javascript, etc.)

in der Regel von unterschiedlichen Personen wahrgenommen. Aus technischen Gründen ist in der Regel eine vollständige Trennung der Zugriffsrechte nicht oder zumindest nicht vollständig möglich. Die oben geforderten Zugriffsbeschränkungen lassen sich auf einem Entwicklungssystem daher in der Regel nicht durchsetzen. In diesem Fall muss darauf geachtet werden, dass das Entwicklungssystem keine sensitiven Daten enthält. Die Zugriffsrechte auf einem produktiven Webserver lassen sich jedoch auch in einer solchen Umgebung restriktiv handhaben. Neben der Zuständigkeit müssen auch die für den Transfer notwendigen Tätigkeiten geplant werden. Dies umfasst neben der oben erwähnten Kontrolle der vergebenen Zugriffsrechte auch eine Überprüfung der zu veröffentlichenden Inhalte.

**Zugriffsbeschränkungen auf den Webserver**

Vor der Inbetriebnahme bzw. jeder Aktualisierung eines Webservers muss festgelegt werden, wer Informationen vom Webserver abfragen darf. Es ist zu klären, ob nur Personen innerhalb der eigenen Organisation, eventuell zusätzlich Telearbeiter, oder auch jeder Externe oder nur ein eingeschränkter Kreis auf bereitgestellte Informationen zugreifen dürfen. Diese Einschränkungen können auch abhängig von den jeweiligen Informationen variieren

Wenn der Zugriff auf den Webserver nur einem begrenzten Personenkreis möglich sein soll, sind entsprechende Maßnahmen zu implementieren, wie z. B. in M 4.94 *Schutz der Webserver-Dateien*.

Es muss außerdem geklärt werden, ob grundsätzlich nur Informationen abgerufen werden dürfen oder ob es auch für Benutzer möglich sein soll, selber neue Informationen einzustellen. Auch hier ist wieder festzulegen werden, welcher Personenkreis welche Rechte hat.

**Übersichtliche Strukturierung**

Da HTML-Dateien nicht hierarchisch angeordnet werden müssen, ist die Verzeichnisstruktur innerhalb eines Webservers für die Funktionsweise irrelevant. Um die Wartung zu erleichtern, sollte allerdings auf eine übersichtliche Struktur geachtet werden.

Es ist empfehlenswert, die Verzeichnisstruktur so zu wählen, dass der URL, unter dem eine Datei erreichbar ist, bereits gewisse Informationen über die Datei gibt. Dies führt zwar unter Umständen zu relativ langen Pfadnamen, aber es macht es Besuchern leichter, sich bestimmte Stellen zu merken und wieder zu finden. Da viele Internet-Suchmaschinen bei einer Suche den vollständigen WWW-Pfad eines Treffers ausgeben, verbessert diese Art der Strukturierung auch die Auffindbarkeit der Informationen.

Da unter Umständen in anderen Webservern Links auf ihre Dokumente angelegt werden, sind Änderungen an Dokument- und Verzeichnisnamen zu vermeiden. Die Verzeichnisstruktur muss deshalb erweiterungsfähig geplant werden.

**Dokumente bereitstellen**

Ein öffentliches Webangebot im Internet ist eine Form der Außendarstellung einer Organisation. Entsprechend sorgfältig sollte daher die Internet-Präsenz vorbereitet werden.

Es empfiehlt sich, mit einem Webangebot im Intranet erste Erfahrungen zu sammeln, bevor ein Webserver an das Internet angebunden wird. Hier sollte mit wenigen, einfachen Anwendungen begonnen werden.

Informationen in einem Webangebot werden normalerweise in HTML-Dateien bereitgestellt, die direkt im Webbrowser dargestellt werden können. Es können aber auch Dateien in beliebigen anderen Formaten zum Download bereitgestellt werden. In diesem Fall muss die Anwendung zum Anzeigen des Dokuments beim Benutzer vorhanden sein und die Dateien müssen im Allgemeinen zunächst auf dem IT-System des Benutzers gespeichert werden, bevor sie weiterverarbeitet werden können.

Sofern es nicht erforderlich ist, dass Benutzer in den bereitgestellten Dokumenten Änderungen vornehmen (beispielsweise Ausfüllen von Formularen), sollten Dokumente in Formaten bereitgestellt werden, bei denen Veränderungen nicht einfach möglich sind. Proprietäre Dokumentenformate sollten so weit wie möglich vermieden werden.

Alle für die Veröffentlichung im Internet vorgesehenen HTML-Dokumente und WWW-Dateien sollten vor der Veröffentlichung genauso qualitätsgesichert und inhaltlich genehmigt werden wie jede andere Veröffentlichung.

HTML-Dokumente werden meist mit speziellen HTML-Editoren erstellt. In anderen Formaten erstellte Dokumente können mit HTML-Konvertern in HTML umgewandelt werden.

Sollen viele, sich oft ändernde Dokumente zur Verfügung gestellt werden, empfiehlt es sich, den Webserver mit einer Dokumentendatenbank zu verbinden. Diese Lösung bietet dem Benutzer schnelle Such-, Ansichts- und Dokumentenverwaltungsmöglichkeit. Nützlich ist es auch, wenn mit Hilfe einer Datenbankanbindung der Zugriff auf bereits vorhandene Firmendaten ermöglicht wird. In diesem Fall muss jedoch der Datenbankserver bzw. die Dokumentendatenbank in das Webserver-Sicherheitskonzept mit einbezogen werden.

Vor dem Einstellen neuer Dateien auf einem Webserver sind diese auf eventuell noch enthaltene Restinformationen zu überprüfen (siehe M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).

**Konfigurationsmanagement**

Da sich die Inhalte von Web-Seiten erfahrungsgemäß häufig ändern, ist es wichtig, ein funktionierendes Konfigurationsmanagement aufgebaut zu haben. Die Aktualität von Links und Verweisen ist zu überprüfen, ebenso wie vor Veröffentlichung eine Virenkontrolle mit einem aktuellen Computer-Virensuchprogramm durchzuführen ist.

**Kontrolle und Freigabeverfahren**

Es ist ebenso wichtig, dass alle Veröffentlichungen ein festgelegtes und nachvollziehbares Kontrollverfahren durchlaufen. Dies sollte eine inhaltliche Qualitätskontrolle ebenso umfassen wie eine formale Freigabe. Hier muss auch überprüft werden, ob die Informationen überhaupt für eine Veröffentlichung

geeignet sind oder ob sie z. B. vertraulich sind, dem Datenschutz unterliegen, Copyright-geschützt sind oder ähnliches.

Bei größeren Webangeboten kann es sinnvoll sein, ein Web-Content-Management-System einzusetzen. Solche Systeme vereinfachen viele Arbeitsabläufe, die im Zusammenhang mit der Pflege eines Webangebots anfallen. Informationen, die zur Veröffentlichung über elektronische Medien freigegeben worden sind, sollten digital signiert werden, um allen Lesern die Möglichkeit zu geben, die Authentizität der Informationen zu überprüfen.

Veröffentlichungen, die nicht die Meinung der Institution widerspiegeln, müssen als solche gekennzeichnet sein.

**Beachtung rechtlicher Rahmenbedingungen**

Beim Betrieb eines Webservers müssen verschiedene rechtliche Rahmenbedingungen (in Deutschland sind dies unter anderem das Telemedienegesetz, der Mediendienste-Staatsvertrag, Vorschriften zum Datenschutz) berücksichtigt werden.

Beispielsweise wird für ein gewerbliches Web-Angebot das Vorhandensein eines Impressums gefordert, in dem der Name der verantwortlichen Person und eine Kontaktadresse genannt werden müssen. Je nach dem Inhalt des Web-Angebots oder der Branche des Anbieters sind unter Umständen weitere Angaben erforderlich. Bevor ein Web-Angebot freigeschaltet wird, sollte geklärt sein, welche Informationen dies sind und wo und in welcher Form diese veröffentlicht werden müssen.

Prüffragen:

- Wird festgelegt welche Informationen im Internet und welche dem Intranet zur Verfügung gestellt werden?
- Werden Richtlinien für ein einheitliches Erscheinungsbild von Dokumenten, Dateinamen und Verzeichnisnamen auf Grundlage des ermittelten Dokumenterstellungsprozesses und der Dokumentverwendung erstellt?
- Werden Verantwortliche für das Einstellen und die Richtlinienüberprüfung von Informationen und Dateien festgelegt und haben diese nur Zugriff auf die ihnen zugewiesenen Bereiche des Webservers?
- Werden durchgeführte Änderungen an den Inhalten des Webservers protokolliert?
- Entwicklungssystem: Enthält das Entwicklungssystem keine sensitiven Daten?
- Wird festgelegt wer welche Informationen vom Webserver abfragen, einstellen oder modifizieren darf?
- Falls ein begrenzter Personenkreis zugriffsberechtigt ist: Werden Maßnahmen zur Einschränkung des Zugriffs ergriffen?
- Wird die Verzeichnisstruktur erweiterungsfähig geplant und werden Änderungen an Dokumentnamen und Verzeichnisnamen nach Möglichkeit vermieden?
- Falls Benutzer bereitgestellte Dokumente nur lesen: Werden Dokumentenformate benutzt die nur schwer veränderbar sind?
- Werden proprietäre Dokumentenformate vermieden?
- Unterliegen die zu veröffentlichenden Informationen einer redaktionellen Freigabe?
- Bei Verbindung des Webservers mit einem Datenbankserver oder einer Dokumentendatenbank: Ist der Datenbankserver oder die Dokumentendatenbank in das WWW-Sicherheitskonzept mit einbezogen?

- Gibt es ein funktionierendes Konfigurationsmanagement?
- Ist sichergestellt, dass die Integrität der zu veröffentlichenden Dateien gewährleistet ist (keine unerwünschten Restinformationen, Virenfreiheit)?
- Gibt es für alle Veröffentlichungen ein nachvollziehbares Kontrollverfahren, das die inhaltliche Qualität, formale Richtlinien und die Veröffentlichbarkeit überprüft?
- Werden alle rechtlichen Rahmenbedingungen, wie z. B. das Teledienstegesetz berücksichtigt?

# M 2.176 Geeignete Auswahl eines Internet Service Providers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Anbieter von Internetdiensten (Internet Service Provider oder kurz ISP) bieten verschiedene Dienste, Inhalte oder technische Leistungen an, die die Internet-Nutzung oder den Betrieb eigener Internet-Angebote unterstützen. Institutionen sollten Anbieter sorgfältig auswählen. Bei einem Provider, über den eine Institution an das Internet angeschlossen ist, fallen nicht nur Informationen über ein- und ausgehende E-Mail an, sondern auch über alle Webseiten, die die Benutzer aufrufen. Außerdem laufen alle Daten, die zwischen den Rechnern der Benutzer und einem Server im Internet ausgetauscht werden, über die IT-Systeme des Providers.

Bei der Auswahl eines Internet Service Providers sollte hinterfragt werden,

- ob Ansprechpartner zu technischen Problemen rund um die Uhr zur Verfügung stehen und wie kompetent diese sind,
- wie er auf den Ausfall einer oder mehrerer seiner IT-Systeme vorbereitet ist (Notfallplanung, Datensicherungskonzept),
- welche Verfügbarkeit (maximale Ausfallzeit) er garantieren kann,
- ob er regelmäßig überprüft, ob die Verbindungen zum Kunden noch stabil sind und im negativen Fall entsprechende Schritte unternimmt,
- welche Daten über die Internet-Nutzung seiner Kunden bei ihm anfallen und wie er diese vor unbefugtem Zugriff schützt,
- was er zur Absicherung seiner IT-Systeme und der seiner Kunden unternimmt.

Bei der Auswahl eines Providers sollte sich die Institution vom Provider dokumentieren lassen, dass dessen IT-Systeme sicher betrieben werden, also z. B. die in M 2.174 *Sicherer Betrieb eines Webservers* beschriebenen Anforderungen erfüllt sind. Alle relevanten Maßnahmen zu vernetzten Systemen und zu Datenübertragungseinrichtungen sollten umgesetzt sein. Bei jedem Provider sollte ein Sicherheitskonzept und entsprechende Sicherheitsrichtlinien selbstverständlich sein. Die Sicherheitsrichtlinien sollten für Externe einsehbar sein. Die Mitarbeiter des Providers sollten für Sicherheitsaspekte sensibilisiert sein, auf die Einhaltung der Sicherheitsrichtlinie verpflichtet worden sein und regelmäßig geschult werden (nicht nur in Sicherheitsfragen).

Beim Provider sind Daten über die Benutzer für Abrechnungszwecke gespeichert (Name, Adresse, Benutzer-Kennung, Bankverbindung) ebenso wie Verbindungsdaten und für eine je nach Provider kürzere oder längere Zeitspanne auch die übertragenen Inhalte.

Die Anwender sollten sich bei ihrem Provider erkundigen, welche Daten wie lange über sie gespeichert werden. Bei der Auswahl von Providern sollte berücksichtigt werden, dass deutsche Betreiber den einschlägigen datenschutzrechtlichen Regelungen für die Verarbeitung dieser Daten unterliegen.

Die genauen Modalitäten der Zusammenarbeit mit dem Dienstleister müssen vertraglich geregelt und geeignete Service Level Agreements (SLAs) vereinbart werden, z. B. Ansprechpartner, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der Sicherheitsvorkehrungen, Umgang mit vertraulichen Informationen (siehe hierzu M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister*).

Prüffragen:

- Werden sicherheitsrelevante, datenschutzrechtliche und leistungsrelevante Eigenschaften der Service Provider in Erfahrung gebracht?

# M 2.177 Sicherheit bei Umzügen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik, Leiter IT, Leiter Organisation

Bei einem Umzug müssen neben Möbeln auch die verschiedensten Datenträger (z. B. Papier, Magnetbänder, CD-ROMs, DVDs, Wechselfestplatten) und IT-Systeme hin und her transportiert werden. Dabei verlassen Informationen, IT-Systeme und sonstiges Material den gesicherten Bereich der Büroumgebung und werden durch Personal transportiert, das normalerweise keine Zugriffsrechte hat. Bei einem Umzug, insbesondere wenn größere Teile der Organisation davon betroffen sind, ist ein gewisses Durcheinander nie auszuschließen und es kann auch nicht jede Umzugskiste permanent persönlich beaufsichtigt werden. Trotzdem ist dafür Sorge zu tragen, dass bei einem Umzug sensitive Daten weder verloren, beschädigt, noch Unbefugten zugänglich werden.

In die Umzugsplanung sollte möglichst frühzeitig das Informationssicherheitsmanagement und der Datenschutzbeauftragte einbezogen werden, um die aus Sicht der Informationssicherheit festzulegenden Rahmenbedingungen festzulegen:

- Bei der Planung eines Umzuges muss im Vorfeld detailliert festgelegt werden, wer mit welchem Transportgut wann wohin umzieht (Erstellung eines Umzugskonzepts). Dies sollte ohnehin eine Selbstverständlichkeit sein, damit die Arbeit nach dem Umzug möglichst reibungslos wieder aufgenommen werden kann.
- In Abhängigkeit vom Schutzbedarf der Daten muss festgelegt werden, welche Randbedingungen für den Transport einzuhalten sind. Beispielsweise sollten für sensiblere Daten verschließbare Transportbehälter (siehe M 2.44 *Sichere Verpackung der Datenträger* benutzt werden oder die Datenträger vor dem Transport verschlüsselt werden.
- Vor jedem Transport von IT-Systemen sollten Datensicherungen angefertigt werden. Hierbei ist neben den in M 6.35 *Festlegung der Verfahrensweise für die Datensicherung* beschriebenen Modalitäten insbesondere zu beachten, dass die Datensicherungen auf keinen Fall zusammen mit den gesicherten IT-Systemen transportiert werden dürfen. Hierdurch wird sichergestellt, dass nicht alle Speichermedien gleichzeitig beschädigt werden oder abhanden kommen.
- Es sollte ein Merkblatt (Umzugsmerkblatt) für alle betroffenen Mitarbeiter ausgearbeitet werden, in dem alle durchzuführenden Sicherheitsmaßnahmen genau beschrieben sind.

Bei einem Umzug ist nicht nur der Transport eine kritische Phase, sondern auch der Zeitraum kurz vor bzw. danach. In dieser Phase kommen erfahrungsgemäß viele Sachen abhanden, da zu diesem Zeitpunkt die Standardsicherheitsverfahren wie z. B. die Zutrittskontrolle noch nicht greifen. Auch während des Umzugs sollten daher gewisse organisatorische Mindestanforderungen erfüllt sein:

- Für alle zu transportierenden Materialen sollten Transportpapiere ausgestellt werden, aus denen hervorgeht,
  - ob eine bestimmte Transportart zu beachten ist (z. B. zerbrechlich, Computerspezialtransport, etc.),

  - ob eine bestimmte Verpackungsart zu wählen ist (z. B. bei Datenträgern mit vertraulichen Informationen),
  - wohin sie gebracht werden sollen (genaue Gebäude-, Etagen- und Raumbeschreibung),
  - wer berechtigte Empfänger der transportierten Gegenstände sind,
  - wer sie abgeholt bzw. angeliefert hat (inklusive Name, Datum und Uhrzeit).
- Das Transportgut muss so gekennzeichnet sein, dass es eindeutig identifiziert werden kann, so dass auch der Transportweg nachvollzogen werden kann. Die Kennzeichnung sollte jedoch keine Rückschlüsse auf die Sensitivität des Inhalts erlauben. Die Art der Kennzeichnung sollte so gewählt sein, dass sie nicht problemlos nachgemacht und werden kann. Hierfür könnten die Umzugsvorbereiter spezielle Etiketten zur Verfügung stellen. Hierbei ist darauf zu achten, dass sich die Etiketten von den Gegenständen auch rückstandsfrei wieder ablösen lassen, ohne das Umzugsgut zu beschädigen bzw. zu verunreinigen.
- Auch während eines Umzuges sollte kein ungeordnetes Kommen und Gehen herrschen. Die beauftragten Umzugsfirmen sollten die Personalien der vorgesehenen Mitarbeiter vorher bekannt geben. Bei plötzlichen Personalwechsel (Urlaub, Krankheit, etc.) sollten die Namen des Ersatzpersonals kurzfristig mitgeteilt werden. Mit einer Namensliste der am Umzug Beteiligten können dann die Pförtner oder andere interne Mitarbeiter je nach Liegenschaft und Gegebenheit sporadisch oder kontinuierlich kontrollieren. Die am Umzug beteiligten externen Kräfte sollten mit gut sichtbaren Ausweisen (ggf. mit Namen) versehen werden, damit klar erkennbar ist, wer zutrittsberechtigt ist.
- Das Transportgut, insbesondere die Datenträger sind vor und nach dem Umzug sicher aufzubewahren. Die Räume, in denen keine Umzugstätigkeiten stattfinden, in denen sich aber keine Mitarbeiter aufhalten, also z. B. die, die noch nicht ausgeräumt bzw. bereits eingeräumt wurden, sollten abgeschlossen werden.

Nach erfolgtem Umzug sollte möglichst rasch ein geordneter Betrieb aufgenommen werden. Als Erstes ist die infrastrukturelle und organisatorische Sicherheit in den neuen Büros wiederherzustellen, also z. B.

- sollte die Zutrittskontrolle wieder in vollem Umfang aufgenommen werden,
- sollten die Brandlasten aus den Fluren entfernt werden, d. h. die Umzugskartons in die neuen Arbeitsräume geschafft werden,
- ist das angelieferte Umzugsgut darauf zu überprüfen, ob es vollständig und voll funktionsfähig ist und nicht manipuliert wurde,
- sollte die Vollständigkeit des Umzugsgutes von jedem Mitarbeiter sofort überprüft werden und gegebenenfalls eine Verlust-Liste angefertigt werden. Hierzu könnte den Betroffenen ebenfalls ein bereits im Vorfeld vorbereitetes Formular ausgehändigt werden, in dem bereits das abtransportierte Umzugsgut aufgelistet werden kann. So kann auch der Vertreter bei Abwesenheit wegen Urlaub, Krankheit oder dringender Dienstgeschäfte der betroffenen Kollegen sofort das Fehlen von Teilen des Umzugsgutes feststellen und melden. Der zu vertretende Mitarbeiter sollte hiervon eine Kopie erhalten, um im nachhinein noch etwaige Unstimmigkeiten melden zu können.

Besondere Sorgfalt sollte auf die Umzugsplanung für alle Server und Netzkoppelelemente verwendet werden, da auch bei Ausfall nur einer Komponente unter Umständen das ganze Netz nicht betriebsfähig ist.

Vor einem Umzug sollten daher auf Seiten der zentralen IT-Administration verschiedene Vorkehrungen getroffen werden, um den reibungslosen Arbeitsablauf sicherzustellen:

- Vor Beginn der Umzugsphase sollte frühzeitig ein Plan für die erforderlichen Änderungen der Benutzeranbindung erstellt werden. Hierbei sollte besonders analysiert werden, ob neue Beschaffungen für den reibungslosen Wechsel der Rechneranbindung von Mitarbeitern erforderlich sind. Auch aus Sicherheitsgründen ist es wichtig zu wissen, welche Änderungen sich durch den Umzug im Kommunikationsverhalten der IT-Systeme ergeben. Je nach dem Schutzbedarf der Arbeit von Mitarbeitern kann es beispielsweise erforderlich werden, eine Netzverbindung zu verschlüsseln oder den Zugriff auf bestimmte Datenbestände zu unterbinden.
- Bevor ein Mitarbeiter umzieht, sollte sichergestellt sein, dass er in seinem neuen Büro über das lokale Netz erreichbar ist und seine Applikationen und Dienste betriebsbereit sind. Dies erfordert gegebenenfalls neben Änderungen am Endgerät (Routing, Softwarekonfiguration etc.) auch baldige Änderungen auf Serverseite im LAN oder gar auf Routern im WAN. Hier kann es erforderlich sein, neue Adressen oder Routen einzurichten und alte zu löschen. Möglicherweise müssen vorher neue Netzkomponenten beschafft und eingerichtet werden.
- Bei einem Umzug ist es oft auch erforderlich, für die betroffenen Mitarbeiter Benutzer-Accounts auf einem neuen Server einzurichten. Es ist darauf zu achten, dass die erforderlichen Rechte und Zugriffe auf Applikationen und Protokolle eingerichtet werden. Auch die Sicherheitseinstellungen der Benutzerumgebung müssen seinem Sicherheitsprofil entsprechend gewahrt bleiben. Alte Benutzereinträge und Endgerät-Zugangseinträge müssen auf dem alten System angepasst oder gelöscht werden. Der Zugriff auf benutzereigene Datenbereiche sollte ihm dennoch für eine Übergangszeit, jedoch mit verbindlichem Hinweis auf Löschung nach einer Karenzzeit, gewährt bleiben. Nach dieser Karenzzeit muss die Löschung durch den Administrator vollzogen werden.

Besondere Vorkehrungen sind beim Umzug der Komponenten des Rechenzentrums, wie Daten- oder Kommunikationsservern, zu treffen. Im Folgenden werden Maßnahmen beschrieben, die möglichst kurze Ausfallzeiten der Komponenten gewährleisten sollen.

- Wenn möglich, sollte ein neuer Server vorab installiert und in der neuen Räumlichkeit getestet werden. Ist dies nicht möglich, so sollte der alte Server so gut wie möglich vorkonfiguriert werden und erst zu einer Zeit, zu der wenig Zugriffe zu erwarten sind, nach ausreichender Vorankündigung umgestellt werden. Hierbei sollte die alte Konfiguration immer vorab gesichert sein.
- Der Server sollte vor dem Umzug komplett gesichert werden. Wenn nicht bereits vorhanden, ist auch ein bootfähiges Sicherungsmedium zu erzeugen. Sensible Serverteile wie Festplatten sollten für den Ausfall des Originals als Image redundant vorgehalten sein und getrennt vom Server transportiert werden. Es ist darauf zu achten, dass die Datensicherung und das Image ebenso wie der Server beim Transport gesichert ist (z. B. Verschlüsselung, verschlossene Box, Bewachung).
- Vor dem Umzug ist sicherzustellen, dass die Infrastruktur in den neuen Räumlichkeiten für den einwandfreien Serverbetrieb vorhanden und getestet sind. Hier ist neben dem Vorhandensein des Netzes (Strom, LAN, WAN) auch auf die richtige Reihenfolge des Umzuges der Komponenten zu achten. Es ist beispielsweise wenig sinnvoll, zuerst den Internet-Webserver umziehen zu lassen, wenn der Firewall mit seinem Kommunikationsrouter erst wesentlich später aufgebaut wird.

- Vor dem Umzug sollte überprüft werden, ob unter den zu transportierenden IT-Komponenten solche sind, die besondere Umgebungsbedingungen während des Umzuges benötigen. Beispielsweise gibt es Controller für größere (und teurere!) IT-Systeme, die nicht nur in klimatisierten Räumen betrieben, sondern auch klimatisiert transportiert werden müssen.

Weiterhin sollte sichergestellt sein, dass die neuen Telefonnummern bereits erreichbar sind, sobald die Mitarbeiter ihre neuen Büros bezogen haben. Bei einem Umzug innerhalb eines Ortes sollte versucht werden, die alten Telefonnummern zumindest übergangsweise zu behalten. Während des Umzugs sollte sowohl in der alten als auch in der neuen Liegenschaft die telefonische Erreichbarkeit gewährleistet sein, damit bei auftretenden Problemen Rückfragen jederzeit möglich sind.

Prüffragen:

- Sind rechtzeitig vor einem geplanten Umzug Sicherheitsrichtlinien erarbeitet bzw. aktualisiert worden?
- Sind alle Mitarbeiter über die vor, während und nach dem Umzug zu beachtenden Sicherheitsmaßnahmen informiert worden?
- Wurde nach dem Umzug überprüft, dass das zu transportierende Umzugsgut vollständig und unbeschädigt bzw. unverändert angekommen ist?

# M 2.178 Erstellung einer Sicherheitsleitlinie für die Faxnutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Vor der Installation, Konfiguration und Freigabe von Faxservern sollte zunächst eine Sicherheitsleitlinie für die Faxnutzung festgelegt werden. Folgende Punkte werden üblicherweise mit solch einer Sicherheitsleitlinie geregelt:

**1. Einsatzkonzept**

Bevor ein Faxserver für die Nutzung freigegeben wird, muss zunächst festgelegt werden, in welcher Einsatzart das System betrieben werden soll. So ist z. B. denkbar, dass ein Faxserver nur dazu dient, Faxe über das LAN entgegenzunehmen und dann nach außen zu versenden. Ein Faxserver kann aber auch von außen eingehende Faxsendungen entgegennehmen. In diesem Fall muss festgelegt werden, wie die Eingangs-Faxsendungen an die Empfänger weitergeleitet werden. Die erste Möglichkeit besteht dabei in der Weiterleitung durch den Faxserver selbst, ggf. mit Anbindung an bereits bestehende E-Mail oder Workflow-Systeme. Eine andere Möglichkeit ist die manuelle Weiterleitung der Eingangs-Faxsendungen durch die Poststelle. Hier besteht einmal die Möglichkeit der Weiterleitung per E-Mail. Denkbar ist aber auch, dass die Poststelle eingehende Faxe ausdruckt und diese Ausdrucke an den Empfänger weiterleitet (siehe M 2.181 *Auswahl eines geeigneten Faxservers*).

**2. Integration in den Geschäftsablauf**

Von der Betriebsart hängt auch ab, wie bei Benutzung eines Faxservers versandte oder empfangene Faxe in den Geschäftsablauf integriert werden. Sofern die Poststelle alle Faxeingänge ausdruckt und die Ausdrucke an den jeweiligen Empfänger weiterleitet, entspricht dies dem Ablauf, wie er auch bei herkömmlichen Faxgeräten üblich ist. Werden aber Faxe direkt aus einer Applikation vom Arbeitsplatzrechner des Benutzers versandt oder werden Faxeingänge direkt vom Faxserver an den Empfänger übermittelt, unterscheiden sich diese Verfahren erheblich von denen bei der Benutzung herkömmlicher Faxgeräte. Daher sollte in diesem Fall in der Richtlinie für die Faxnutzung festgelegt werden, von welchen Faxeingängen und Faxausgängen Ausdrucke für die Akten gefertigt werden müssen.

**3. Regelungen zum Faxserver-Einsatz**

Um den sicheren Betrieb und Einsatz eines Faxservers sicherstellen zu können, müssen eine Reihe von Regelungen getroffen werden (siehe M 2.179 *Regelungen für den Faxserver-Einsatz*).

**4. Inhaltliche Restriktionen**

Weiterhin sollte in der Fax-Sicherheitsleitlinie festgelegt werden, welche Informationen überhaupt per Fax weitergegeben werden dürfen. Es kann in der Fax-Sicherheitsleitlinie zudem festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen.

Damit wird erreicht, dass der Empfänger auch die notwendigen Berechtigungen zum Weiterverarbeiten der Information besitzt. Beispielsweise kann fest-

gelegt werden, dass Preislisten nur an Einkäufer oder Projektunterlagen nur an Projektbeteiligte per Fax versendet werden dürfen.

**5. Notfallvorsorge und Ausfallsicherheit**

Außerdem sollten in der Faxsicherheitsleitlinie Aussagen zur Notfallvorsorge und zur Ausfallsicherheit des Faxbetriebes enthalten sein. Abhängig von den Anforderungen an den Wert Verfügbarkeit ist ggf. der Einsatz redundanter Faxserver sinnvoll. In diesen Bereich fallen auch Überlegungen, ob für den Notfall noch herkömmliche Faxgeräte verfügbar gehalten werden (siehe auch M 6.69 *Notfallvorsorge und Ausfallsicherheit bei Faxservern*).

**6. Datensicherung**

Der Faxserver sollte in das Datensicherungskonzept der Organisation aufgenommen werden (siehe Baustein B 1.4 *Datensicherungskonzept*). Insbesondere ist dabei festzulegen, wer für die Durchführung der Datensicherungen zuständig ist und was zu sichern ist. Gegenstand der Datensicherung können dabei die Software, Konfigurationsdaten, gespeicherte bzw. archivierte Faxdaten oder auch Protokolldateien sein. Außerdem sind Festlegungen hinsichtlich des Sicherungsintervalls und der Anzahl der aufzubewahrenden Generationen notwendig. Es muss festgelegt werden, wer für die Überprüfung der bei der Datensicherung anfallenden Protokolle zuständig ist. Schließlich sollten sowohl die Durchführung der Datensicherung als auch die Auswertung der Protokolle dokumentiert werden.

**7. Schulung**

Die Faxsicherheitsleitlinie sollte zudem um ein organisationsweites Schulungskonzept ergänzt werden. Zunächst ist das Personal, dass das IT-System und die Faxserver-Applikation administriert, entsprechend zu schulen. Dann sollten die Benutzer für die Gefährdungen sensibilisiert werden, die durch einen Faxserver im Vergleich zu einem herkömmlichen Faxsystem entstehen.

Prüffragen:

- Ist die Faxnutzung in einer Sicherheitsleitlinie festgelegt?
- Ist festgelegt, in welcher Einsatzart der Faxserver betrieben werden soll?
- Faxserver für eingehende Faxsendungen: Ist festgelegt, wie die Faxsendungen an die Empfänger weitergeleitet werden?
- Ist in der Fax-Sicherheitsleitlinie beschrieben, wie mit Faxeingängen und Faxausgängen umzugehen ist?
- Ist in der Fax-Sicherheitsleitlinie festgelegt, welche Informationen an welche Kommunikationspartner weitergegeben werden dürfen?
- Beinhaltet die Fax-Sicherheitsleitlinie Informationen und Anweisungen zur Notfallvorsorge und Ausfallsicherheit des Faxbetriebes?

# M 2.179 Regelungen für den Faxserver-Einsatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um den reibungslosen Betrieb des oder der Faxserver zu gewährleisten, müssen folgende Punkte geregelt werden:

**1. Festlegung von Zuständigkeiten**

Ein Faxserver besteht aus einem IT-System, dem darauf installierten Betriebssystem sowie der Faxserver-Applikation. Dazu kommen dann noch die Faxclients der Benutzer. Dementsprechend muss auch die Betreuung geregelt werden. Je nach der vorhandenen Organisationsstruktur müssen Verantwortliche für diese Bereiche benannt werden. Im Extremfall kann dies heißen, dass jeder dieser Bereiche von anderen Administratoren betreut wird. Die Administration des Betriebssystems kann z. B. durch die Organisationseinheit erfolgen, die auch für die Administration der sonstigen IT-Systeme zuständig ist. Die Administration der Faxapplikation sollte hingegen durch die Fax-Poststelle erfolgen. Je nach Einsatzart ist diese Stelle auch dafür verantwortlich, dass eingehende Faxsendungen an den zuständigen Bearbeiter weitergeleitet werden. Diese Stelle sollte dann auch für die Vergabe von Berechtigungen auf dem Faxserver verantwortlich sein. Weitere Aufgaben sind z. B. die Rücksetzung von Passwörtern und die Einrichtung von neuen Benutzern. Von besonderer Bedeutung ist daher die Festlegung der Aufgaben und Zuständigkeiten der Fax-Poststelle (siehe M 2.180 *Einrichten einer Fax-Poststelle*).

**2. Festlegung des Benutzerkreises**

Außerdem sollte der Personenkreis festgelegt werden, der berechtigt ist, den Faxserver zu benutzen. Dabei sind u. a. folgende Berechtigungen für eingehende Faxsendungen denkbar:

- lesen,
- weiterleiten,
- löschen.

Für ausgehende Faxsendungen sind folgende Berechtigungen denkbar:

- senden,
- anhalten,
- löschen,
- Sendeoptionen verändern.

Diese Berechtigungen sollten, wie in der Administration allgemein üblich, möglichst nur an Benutzergruppen und nur im Ausnahmefall an einzelne Benutzer vergeben werden (siehe auch M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

**3. Festlegung von Nutzungsprofilen**

Es sollte auch geregelt werden, in welchem Umfang berechtigte Benutzer den Faxserver in Anspruch nehmen dürfen. Dies ist insbesondere wichtig, um Überlastungen durch Serienfaxe zu verhindern.

**4. Nutzungszeiten**

Außerdem sollte überlegt werden, ob die Nutzung von Faxservern nur zu bestimmten Zeiten zugelassen wird. So kann z. B. verhindert werden, dass außerhalb der Arbeitszeiten Faxe versendet werden können.

**5. Einrichtung von Gruppen**

Sofern Faxeingänge automatisch an die Empfänger durch den Faxserver weitergeleitet werden, sollten für bestimmte Funktionen und Aufgaben eigene Faxnummern eingerichtet werden. Allen Mitgliedern einer Gruppe kann dann der Zugriff auf die für die entsprechende Rufnummer eingehenden Faxsendungen gewährt werden. Dies erleichtert auch etwaige Vertretungsregelungen.

**Beispiel:** In einem Unternehmen wird ein Faxserver betrieben, der eingehende Faxsendungen automatisch an die Empfänger weiterleitet. Eine -Rufnummer wird die Bestellannahme vergeben. Der Faxserver leitet alle Faxsendungen mit Bestellungen, die über diese Rufnummer an das Unternehmen übermittelt werden, nicht an einen einzelnen Mitarbeiter, sondern an alle Mitglieder der Bestellannahme weiter. Dabei muss durch das Unternehmen festgelegt werden, in welcher Reihenfolge die Mitarbeiter Eingangsfaxsendungen bearbeiten, um Bestellungen nicht doppelt auszuführen.

**6. Vertretungsregelung**

Gerade beim Einsatz von Faxservern, die Faxeingänge an einzelne Benutzer zustellen, ist eine Vertretungsregelung im Falle der Abwesenheit unumgänglich und daher eine entsprechende Verpflichtung in die Sicherheitspolitik aufzunehmen. Ansonsten kann nicht ausgeschlossen werden, dass wichtige Faxeingänge über einen längeren Zeitraum nicht zur Kenntnis genommen werden. Insoweit unterscheidet sich das Verfahren beim Einsatz von Faxservern erheblich von dem beim Einsatz herkömmlicher Faxgeräte. Bei letzteren werden Eingänge durch die Vertreter eher wahrgenommen, da die Faxe in Papierform vorliegen.

**7. Protokollierung**

Es sollten Regelungen für den Umgang mit anfallenden Protokolldaten erarbeitet werden. So sollte festgelegt werden, wer welche Protokolldaten in welchen Abständen auswerten muss (siehe M 2.64 *Kontrolle der Protokolldateien*).

**8. Adressbücher**

Auch sollte festgelegt werden, welche Adressbücher zum Einsatz kommen und wer die Pflege übernimmt. Viele Faxserver-Applikationen bieten die Möglichkeit, sowohl individuelle als auch unternehmensweit gültige Adressbücher anzulegen.

Zudem ist es häufig auch möglich, die Adressbücher von Faxservern mit den Verteilerlisten/Adressbüchern bereits vorhandener E-Mail-Systeme zu synchronisieren. Während organisationsweit gültige Adressbücher zentral durch die Fax-Poststelle gepflegt werden sollten, muss dies bei den individuellen Adressbüchern durch die Benutzer selbst erfolgen. Die Benutzer sollten außerdem verpflichtet werden, bei wichtigen Faxsendungen (z. B. individuelle Angebote) die Empfängerrufnummer zu überprüfen.

**9. Nutzung des Faxservers**

Außerdem müssen auch Regelungen für die Nutzung des Faxservers durch die Mitarbeiter erarbeitet werden (siehe M 3.15 *Informationen für alle Mitarbeiter über die Faxnutzung*). Schließlich ist festzulegen, welche Rechte die Mitarbeiter auf dem Faxserver ausüben dürfen.

**10. Schutz der Faxclients**

Es muss durch geeignete organisatorische und technische Maßnahmen sichergestellt werden, dass keine Faxe unbefugt gelesen oder unbefugt bzw. unbeabsichtigt gesendet werden. Die Benutzer sind daher für die Benutzung der Fax-Programme zu schulen und hinsichtlich der auftretenden Risiken zu sensibilisieren.

Von besonderer Bedeutung ist die Authentisierung der Mitarbeiter am Faxserver. Diese kann explizit über einen Faxclient oder aber auch mit der Anmeldung an einem Verzeichnisdienst, einem Domänen-Controller (bei Verwendung von Microsoft Windows) oder an einem E-Mail-System erfolgen. Sofern die Authentisierung zwischen Mitarbeiter und Faxserver über einen Client erfolgt, sollte möglichst darauf verzichtet werden, das Anmelde-Passwort auf der Festplatte abzulegen, da dadurch dieser Sicherheitsmechanismus seinen Wert verliert. Jeder, der auf den entsprechenden Faxclient Zugriff hat, kann unter fremdem Namen Faxe versenden und unbefugt eingehende Faxsendungen lesen. Weiterhin sind die Mitarbeiter dazu anzuhalten, sich nach der Abholung eingegangener Faxsendungen und nach der Versendung von Ausgangsfaxen wieder am Faxserver abzumelden. Es ist darauf hinzuwirken, dass Mitarbeiter beim Verlassen des Arbeitsplatzes den Rechner schützen, z. B. durch die Benutzung eines Bildschirmschoners mit Passwort oder über Mechanismen des eingesetzten Betriebssystems (siehe M 4.1 *Passwortschutz für IT-Systeme* und M 4.2 *Bildschirmsperre*).

**11. Reparatur und Wartung**

Es sollten auch Regelungen zur Durchführung von Reparatur- und Wartungsarbeiten des Faxservers festgelegt werden. Für die Administratoren des Systems muss klar sein, wer im Wartungs- und Reparaturfall zu benachrichtigen ist. Auch sollte geregelt werden, wie mit defekten Datenträgern, insbesondere defekten Festplatten umgegangen werden muss.

Prüffragen:

- Wurde überprüft, ob eine Nutzung der Fax-Systeme nur zu bestimmten Zeiten zugelassen sein soll?
- Sind Vertretungsregelungen und die entsprechenden Verpflichtungen hinsichtlich der Faxeingänge in der Sicherheitsleitlinie berücksichtigt?
- Ist der Umgang mit den Protokolldaten des Faxservers geregelt?
- Ist der Einsatz und die Pflege von Adressbüchern für die Fax-Systeme festgelegt?
- Ist sichergestellt, dass keine Faxe unbefugt gelesen oder gesendet werden können?
- Erfolgt eine Authentisierung der Mitarbeiter am Fax-Server?
- Ist die Durchführung von Reparatur- und Wartungsarbeiten des Faxservers geregelt?

# M 2.180 Einrichten einer Fax-Poststelle

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um den reibungslosen Betrieb des oder der Faxserver zu gewährleisten, muss eine Fax-Poststelle eingerichtet und damit ein Fax-Verantwortlicher benannt werden. Die Fax-Poststelle hat dabei diverse organisatorische und technische Aufgaben wahrzunehmen, die auch von der Betriebsart des Faxservers abhängen.

Da die Mitarbeiter der Fax-Poststelle im Regelfall Zugriff auf alle eingehenden und ausgehenden Faxsendungen haben, muss an die Auswahl des Personals ebenso hohe Anforderungen gestellt werden, wie dies bei Administratoren notwendig ist.

Die Fax-Poststelle muss außerdem mit den Verantwortlichen für die sonstigen Kommunikationsdienste (insbesondere E-Mail und Telekommunikationsanlage) eng zusammenarbeiten.

Die Fax-Poststelle sollte für alle Benutzer jederzeit erreichbar sein. Im Rahmen von Vertretungsregelungen ist sicherzustellen, dass die Fax-Poststelle ständig besetzt ist.

Typische Aufgaben einer Faxserver-Poststelle sind:

- Administration der Faxserver-Applikation. Dazu gehört:
  - Einrichtung neuer Benutzer,
  - Vergabe von Berechtigungen an Benutzer und Benutzergruppen,
  - Rücksetzen von Passwörtern,
  - Überprüfung der Kommunikationsverbindungen,
  - Auswertung der anfallenden Protokolle,
  - Anlaufstelle der Benutzer bei Problemen,
  - Pflege der zentralen Adressbücher und Verteilerlisten,
  - Durchführung von Datensicherungen, sofern dies nicht Aufgabe der Administration des Betriebssystems ist,
- Faxzustellung und Archivierung,
- Fehlerbehebung bei der Faxzustellung,
- Koordination der Zusammenarbeit mit TK-Anlagen- und E-Mail-Verantwortlichen.

Schließlich sollte auch die Faxclient-Software auf den Arbeitsplatzrechnern betreut werden. Diese Aufgabe kann sowohl durch die Fax-Poststelle als auch durch die Organisationseinheit erfolgen, die die Arbeitsplatzrechner betreut.

Einer besonderen Betrachtung bedürfen noch die Aufgaben im Zusammenhang mit den Faxeingängen, da diese von der Betriebsart des Faxservers abhängig sind.

**Manuelle Weiterleitung von Faxeingängen**

Sofern eingegangene Faxsendungen nicht automatisch an den Empfänger zugestellt werden, müssen diese durch die Fax-Poststelle manuell weitergeleitet werden.

Dies kann z. B. in der Form erfolgen, dass durch die Fax-Poststelle von den Faxeingängen ein Ausdruck gefertigt wird, der dann an den Empfänger auf dem üblichen Weg weitergeleitet wird. Dieses Verfahren unterscheidet sich nicht

wesentlich von dem beim Einsatz eines herkömmlichen Faxgerätes. Denkbar ist allerdings, dass eingegangene Faxsendungen digital auf externen Datenträgern archiviert werden.

**Automatische Weiterleitung von Faxeingängen**

Bei der automatischen Weiterleitung von eingegangene Faxsendungen an den Empfänger (automatisches Fax-Routing) ist es ebenfalls möglich, dass durch die Fax-Poststelle Ausdrucke zum Zwecke der Archivierung gefertigt werden. Auch hier besteht die Möglichkeit, eingehende Faxsendungen digital auf externen Datenträgern zu archivieren.

Sofern Faxsendungen nicht zugestellt werden können, muss die Fax-Poststelle hiervon Kenntnis erlangen und versuchen, die Fehlerquelle zu beheben. Sofern die Zustellung endgültig scheitert, ist der Absender entsprechend zu informieren. Gründe dafür, dass Faxeingänge unzustellbar sind, können sein:

- Der Absender hat eine falsche Durchwahl benutzt.
- Der Empfänger ist nicht mehr Mitglied der Institution.
- Die automatische Weiterleitung von Faxeingängen erfolgt aufgrund der Absenderkennung (CSID) und der Absender ist in der Institution noch nicht bekannt oder es existiert keine entsprechende Zuordnungsregel.

In all diesen Fällen muss von der Fax-Poststelle die Weiterleitung von Faxeingängen manuell erfolgen. Sofern Faxeingänge endgültig nicht zugestellt werden können, muss der Absender benachrichtigt werden.

Prüffragen:

- Ist eine Fax-Poststelle eingerichtet und ein Fax-Verantwortlicher benannt?
- Ist sichergestellt, dass die Fax-Poststelle für Benutzer jederzeit erreichbar ist?
- Sind die Abläufe bei der Weiterleitung von Faxeingängen definiert?
- Existiert eine Regelung zur Behandlung von nicht zustellbaren Fax-Sendungen?

# M 2.181 Auswahl eines geeigneten Faxservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Ein Faxserver besteht im Regelfall aus folgenden Komponenten: Dem IT-System selbst, dem Betriebssystem, der Kommunikationskomponente (z. B. Faxmodem, aktive oder passive ISDN-Karte bzw. dedizierte Faxkarte) und der eigentlichen Faxserver-Applikation. Zusätzlich wird unter Umständen für die Arbeitsplatzrechner ein entsprechender Faxclient benötigt.

Bevor Faxserver beschafft werden, sind zunächst die wesentlichen Einflussfaktoren für deren Einsatz zu erheben. Dies sind:

- Das voraussichtlich abzuwickelnde Faxvolumen,
- die Anzahl der Mitarbeiter, die den Faxserver benutzen sollen,
- die Anforderungen an die Verfügbarkeit des Faxservers,
- die Anforderungen an die Einbindung in bereits bestehende E-Mail- und Workflow-Systeme,
- die Anforderungen an die Protokollierung auf dem Faxserver,
- Anforderungen an die Art der Weiterleitung eingehender Faxsendungen an den Empfänger.

**IT-System**

Die Wahl des IT-Systems wird in der Regel durch die Anforderungen der Software und des Betriebssystems an die Leistungsfähigkeit bestimmt. Das IT-System muss zudem kompatibel zum ausgewählten Betriebssystem sein. Je nach Anforderungen an die Verfügbarkeit des Faxservers kann über den Einsatz zusätzlicher Schutzmechanismen nachgedacht werden. Möglichkeiten, die Verfügbarkeit sicherzustellen bzw. zu erhöhen, sind:

- RAID
- Replikation
- Lastverteilung

**Betriebssystem**

Faxserver-Applikationen gibt es für alle gängigen Netzbetriebssysteme wie Unix, Microsoft Windows und Novell Netware. Bei der Wahl des Betriebssystems sollte die Integrationsmöglichkeit in das bestehende Netz und die Anforderungen durch die Faxserver-Applikation den Ausschlag geben. Sofern bisher in einer Organisation ausschließlich ein Netzbetriebssystem zum Einsatz kommt, also z. B. nur Server unter dem Betriebssystem Unix im Einsatz sind, so sollte auch möglichst dieses Netzbetriebssystem ausgewählt und eine geeignete Faxserver-Applikation beschafft werden. Hiervon wird man abweichen müssen, wenn eine bestimmte Applikationssoftware als Einzige ein dringend benötigtes Leistungsmerkmal anbietet, aber nur auf einer anderen als der bisher eingesetzten Betriebssystemplattform einsetzbar ist. Ein neues Netzbetriebssystem bedeutet einen erheblichen Mehraufwand bei der Administration. Sofern im Netz bereits verschiedene Netzbetriebssysteme im Einsatz sind, ist das zu wählen, das sich am einfachsten integrieren lässt, sofern die gewünschte Faxserver-Applikation dies zulässt.

**Kommunikationskomponente**

Die Kommunikationskomponenten stellen die Verbindung zwischen dem Server und dem öffentlichen Telefonnetz her. Die Kommunikation wird auf der

Grundlage des T.30 Protokolls abgewickelt. Durch dieses Protokoll wird u. a. der Verbindungsaufbau, der Austausch der Absender-Faxnummer und die Übertragung und die Quittierung des Dokuments geregelt. Die Übertragung im Gruppe-3-Standard erfolgt hauptsächlich bei 9.600 bps und 14.400 bps. Außerdem sind die Kompressionsverfahren Modified Huffmann, Modified Read und Modified Modified im Einsatz. Der Gruppe-3-Standard ist am weitesten verbreitet. Daneben gibt es noch den Gruppe-4-Standard, der allerdings ISDN voraussetzt. Hier werden Übertragungsgeschwindigkeiten von 64 kBit pro Sekunde erreicht. Der Standard Gruppe 4 hat sich gleichwohl in den vergangenen Jahren nicht durchsetzen können, da entsprechende Stand-alone-Geräte relativ teuer sind. Es besteht außerdem keine Kompatibilität zwischen dem Gruppe-3- und dem Gruppe-4-Standard.

Bei Beginn der Kommunikation wird zwischen den Geräten sowohl die Übertragungsgeschwindigkeit als auch das Kompressionsverfahren ausgehandelt. Es wird die höchste Geschwindigkeit und das bestmögliche Kompressionsverfahren gewählt, das von beiden Geräten unterstützt wird.

Folgende Kommunikationskomponenten sind beim Einsatz eines Faxservers denkbar:

**a) Faxmodem**

Faxmodems sind recht preisgünstig verfügbar. Sie sind aber u. U. nicht ausreichend manipulationsresistent und werden zudem nicht von allen Faxserver-Applikationen im Dauereinsatz unterstützt. Daher sollte ihr Einsatz auf den privaten Gebrauch und auf einzelne Arbeitsplätze beschränkt bleiben.

**b) passive ISDN-Karten**

Passive ISDN-Karten sind einfach aufgebaut und damit preiswert. Die Hauptlast der Kommunikation trägt der Rechner. Dies ist bei starker Inanspruchnahme des Faxservers (z. B. Serien-Faxsendungen) problematisch. Bei passiven ISDN-Karten ist - ein entsprechendes Gerät auf Empfängerseite vorausgesetzt - generell auch die Übertragung nach dem Gruppe-4-Standard möglich. Müssen Faxdaten nach dem Gruppe-3-Standard übertragen werden, so sind die Daten entsprechend zu konvertieren. Wie beim Faxmodem gilt auch hier, dass das Hauptanwendungsgebiet auf einen einzelnen Arbeitsplatz oder auf den privaten Bereich beschränkt bleiben sollte.

**c) aktive ISDN-Karten**

Aktive ISDN-Karten, auch ISDN-Controller genannt, verfügen über einen eigenen Prozessor. Sie können daher das ISDN-Protokoll weitestgehend eigenständig abwickeln. Gemäß der Spezifikation des Common-ISDN-API (CAPI) müssen die Faxdaten im Structured Fax File (SFF)-Format an die ISDN-Karte übergeben werden. Die Konvertierung muss auf dem Faxserver erfolgen. Genau wie Modems unterstützen aktive ISDN-Karten im Gruppe-3-Standard nur die Übertragungsgeschwindigkeiten 9.600 und 14.400 bps unter Benutzung des Kompressionsverfahrens Modified Huffmann.

Ein wesentlicher Nachteil sowohl von Faxmodems als auch von aktiven und passiven ISDN-Karten ist, dass diese auch zu anderen Zwecken als der Faxübertragung benutzt werden können, z. B. im Modembetrieb oder als Remote-Access-Komponente. Dies ist aber bei einem Faxserver aus Gründen der Netzsicherheit gerade nicht erwünscht. Aktive ISDN-Karten können bis zu 30 ISDN-Kanäle zur Verfügung stellen. Beim Einsatz von aktiven ISDN-Karten sind auch die ISDN-Signalisierungsmöglichkeiten für das automatische Fax-

Routing verfügbar. Trotz der Verwendbarkeit für nicht-Fax-Betrieb sind aktive ISDN-Karten für den Einsatz in Faxservern durchaus empfehlenswert.

**d) Faxkarten (ggf. mit ISDN-Schnittstelle)**

Spezielle Faxkarten sind auf die Abwicklung des T.30-Protokolls optimiert. Sie übernehmen den Verbindungsaufbau und das "Aushandeln" der Kommunikationsparameter. Die Konvertierung der Daten und die Kompression können auf der Karte erfolgen. Der Faxserver wird damit deutlich entlastet. Es gibt Faxkarten, die die Übertragung von Faxdaten mit 9.600 und 14.400 bps und Anwendung aller drei Kompressionsverfahren bieten. Vorteil dieser Karten ist auch, dass sie im Regelfall nur das T.30-Protokoll beherrschen und daher nicht für den Modembetrieb oder als Remote-Access-Komponente einsetzbar sind. Teilweise werden Faxkarten um eine ISDN-Schnittstelle erweitert. Der Vorteil davon ist, dass die Signalisierungsmöglichkeiten von ISDN für das Fax-Routing nutzbar werden.

Zusammenfassend folgt, dass in Faxservern im Regelfall nur aktive ISDN-Karten und Faxkarten zum Einsatz kommen sollten. Die Karte muss kompatibel zur Applikationssoftware sein, da nicht jede Karte durch alle Faxserver-Applikationen unterstützt wird. Die Anzahl der notwendigen Karten hängt von der Auslastung des Faxservers ab. Je Stunde und Leitung bzw. je Kanal ist die Übertragung von ca. 40-50 Seiten Faxdaten möglich.

**Faxserver-Applikation**

Bei der Auswahl der Applikationssoftware ist sowohl das Faxvolumen, das über den Faxserver abgewickelt werden soll, als auch die Anzahl der Benutzer zu berücksichtigen.

Ist in der Organisation bereits ein E-Mail- bzw. Workflow-System vorhanden, so sollte eine Integration der Applikationssoftware mit diesen Systemen möglich sein. Es ist dann z. B. denkbar, dass Faxeingänge und Fax-Ausgänge zwischen dem Arbeitsplatzrechner des Benutzers und dem Faxserver über das bereits bestehende Workflow- bzw. E-Mail-System ausgetauscht werden. Interessant ist in diesem Zusammenhang auch, ob und wie ggf. bestehende Adressbücher bzw. Verteilerlisten mit den Adressbüchern des Faxservers synchronisiert werden können. Außerdem sollte die Archivierung von ein- und ausgehenden Faxsendungen in bestehenden Workflow-Systemen möglich sein.

Auch ist in die Überlegungen mit einzubeziehen, wie Faxsendungen vom Arbeitsplatz des Benutzers zum Faxserver gelangen und wo eine Umwandlung der Daten in ein für den Faxserver kompatibles Datenformat erfolgt. Die Konvertierung der Faxdaten am Arbeitsplatz erfolgt beim Senden im Regelfall mittels eines Druckertreibers oder einer besonderen Faxclient-Applikation.

Die konvertierten Daten können dann entweder über E-Mail oder auch mittels der Faxclient-Applikation an den Faxserver übermittelt werden. Denkbar ist auch, dass der Benutzer die konvertierten Daten in ein spezielles Verzeichnis auf dem Faxserver kopiert. Schließlich gibt es Faxserver, bei denen eine Druckerwarteschlange im Netz eingerichtet wird, in die die Faxdaten von der Anwendungssoftware, z. B. einem Textverarbeitungsprogramm, geschrieben werden. Außerdem ist es möglich, dass die Daten auf dem Faxserver komplett konvertiert werden. In diesem Fall erstellt der Benutzer mit einer entsprechenden Anwendungssoftware, z. B. einem Textverarbeitungsprogramm, die als Fax zu versendende Datei, die dann dem Faxserver übergeben werden muss. Dies kann mittels E-Mail, einer entsprechenden Faxclient-Applikation

oder durch Kopieren in ein auf dem Faxserver freigegebenes Verzeichnis erfolgen. Zu bedenken ist, dass die Konvertierung der Faxdaten am Arbeitsplatz dort Ressourcen verbraucht. Dies kann in der Regel vernachlässigt werden, wenn nur wenige Faxe am Tag versendet werden. Gerade bei Serien-Faxsendungen kann es aber passieren, dass der Arbeitsplatzrechner für längere Zeit blockiert wird. Andererseits verlangt eine Konvertierung auf dem Faxserver bei hoher Inanspruchnahme entsprechend leistungsfähige Hard- und Software.

Schließlich sollten bei der Auswahl geeigneter Applikationssoftware auch die Protokollierungmöglichkeiten am Faxserver mit berücksichtigt werden. Neben den Fehlerprotokollen sind auch die Sendeprotokolle von Interesse. Zunächst sollten den Benutzern durch den Faxserver die Sendeprotokolle zu den jeweiligen Faxsendungen zur Verfügung gestellt werden. Nur so können die Benutzer kurzfristig z. B. auf Verbindungsfehler reagieren. Weiterhin sollte die Möglichkeit bestehen, die anfallenden Gebühren mittels der Sendeprotokolle zu ermitteln und auf die entsprechenden Kostenstellen zu verteilen.

Ein weiterer Einflussfaktor für die Auswahl der Applikationssoftware ist die Frage, wie Faxeingänge den Empfänger erreichen. Die digitale Weiterleitung von Faxeingängen über das Netz wird auch als Fax-Routing bezeichnet.

Die technisch am einfachsten zu realisierende Möglichkeit ist natürlich der Ansatz, Faxeingänge an zentraler Stelle (Fax-Poststelle) auszudrucken und den Ausdruck an den Empfänger weiterzuleiten. Der Vorteil dieser Lösung ist, dass die Faxeingänge für die Akten zentral ausgedruckt werden. Zudem können die eingehenden Faxsendungen sowohl digital als auch manuell archiviert werden. Außerdem sind bestehende Vertretungsregelungen problemlos zu übernehmen. Nachteilig an diesem Verfahren ist die u. U. daraus entstehende Arbeitsbelastung der Fax-Poststelle. Außerdem stehen die Faxdaten dann nicht in elektronischer Form an den Arbeitsplätzen zur Verfügung.

Eine weitere Möglichkeit besteht darin, dass von der Fax-Poststelle Faxeingänge per E-Mail an den Empfänger gesandt werden. Der Nachteil dieses Verfahrens besteht ebenfalls in der Arbeitsbelastung der Fax-Poststelle. Dabei wird nicht automatisch von jedem Eingangs-Fax ein Ausdruck gefertigt. Wenn ein solcher Ausdruck aus organisatorischen oder sonstigen Gründen gewünscht wird, müssen entsprechende Regelungen getroffen werden.

Für die automatische Weiterleitung von Eingangs-Faxsendungen an den Empfänger über das Netz gibt es folgende Möglichkeiten:

**a) Linerouting**

Hier wird jeder Leitung ein fester Empfänger zugeordnet. Die Anzahl der direkt erreichbaren Empfänger ist auf die Anzahl der zur Verfügung stehenden Leitungen begrenzt.

**b) Auswertung der Absenderkennung**

Ein weiteres Verfahren stellt auf die übermittelte Absenderkennung eines Faxeingangs (CSID - Call Subscriber ID) ab. Hierbei wird auf dem Faxserver festgelegt, dass Faxeingänge bestimmter Absender jeweils an einen bestimmten Empfänger weitergeleitet werden. Der Nachteil dieses Verfahrens besteht darin, dass nur Faxeingänge bereits bekannter Absender automatisch weitergeleitet werden. Alle anderen Faxeingänge müssen manuell an die Empfänger weitergeleitet werden. Problematisch ist zudem, dass Absenderkennungen vom Absender frei gewählt werden können und daher unter Umständen nicht zuverlässig sind.

**c) Signalisierung mittels ISDN**

Sofern ISDN zum Einsatz kommt, gibt es weitere Möglichkeiten des automatischen Fax-Routings. Hierbei muss allerdings zwischen dem so genannten Mehrgeräteanschluss und dem Anlagenanschluss unterschieden werden.

Bei einem Mehrgeräteanschluss stehen 2 Leitungen und bis zu maximal 10 Rufnummern je Anschluss zur Verfügung. Die Rufnummern werden durch die jeweilige Telefongesellschaft vergeben. Sofern im Faxserver eine ISDN-Karte oder eine Faxkarte mit ISDN-Schnittstelle vorhanden ist, kann anhand der durch den Sender benutzten Rufnummer der Empfänger bestimmt werden. Aufgrund der Begrenzung auf 10 Rufnummern ist es somit auch nur möglich, an maximal 10 Empfänger Faxeingänge automatisch zu verteilen.

Beim ISDN-Anlagenanschluss ist zwischen dem öffentlichen Telefonnetz und dem organisationsinternen Telefonnetz eine Telekommunikationsanlage geschaltet. Auch bei dieser Anschlussart kann der Faxserver die durch den Sender benutzte Rufnummer erkennen und einen Faxeingang anhand dieser Nummer automatisch zum entsprechenden Empfänger routen. Die maximal mögliche Anzahl der Empfänger ist dabei deutlich höher. Die Realisierung erfolgt dadurch, dass jeder Mitarbeiter, der vom Faxserver Faxeingänge erhalten soll, eine zweite Durchwahlnummer erhält. Die Telefonanlage leitet Eingänge, die auf dieser zweiten Nummer erfolgen, direkt an den Faxserver weiter. Einziger Nachteil dieses Verfahrens ist, dass der Rufnummernpool einer Organisation stärker belastet wird. Die Telekommunikationsanlage muss also entsprechend leistungsfähig sein.

**d) Auswertung des Empfängers mittels optischer Zeichenerkennung**

Ein weiteres, aber wenig verbreitetes Verfahren zum automatischen Routing von Faxeingängen ist die optische Zeichenerkennung (OCR). Dabei wird versucht, im Faxeingang z. B. im Anschriftenfeld, Namen oder Nummern zu erkennen. Dieses Verfahren setzt leistungsfähige OCR-Software und entsprechende Rechenleistung sowie möglichst genormte Adressfelder bei Faxeingängen voraus.

**e) weitere Verfahren**

Es gibt zwei weitere Verfahren zur automatischen Weiterleitung von Faxeingängen, das Dual Tone Multi Frequency Verfahren und das Direct Inward Dialing Verfahren. Da beide Verfahren in Deutschland nicht anwendbar sind, werden sie hier nur aus Gründen der Vollständigkeit erwähnt.

Die automatische Weiterleitung von eingehenden Faxsendungen hat den Vorteil, dass das Personal der Fax-Poststelle entlastet wird. Zudem erreichen eingehende Faxsendungen den Empfänger schneller. Nachteilig ist insbesondere bei der Signalisierung mittels ISDN, dass der Rufnummernpool entsprechend belastet wird. Dafür ist die automatische Weiterleitung von Eingangs-Faxsendungen hiermit am besten zu realisieren. Bei einem hohen Aufkommen an eingehenden Faxsendungen sollte dieser Lösung der Vorzug gegeben werden. Sofern eingehende Faxsendungen nur für wenige Arbeitsplätze bzw. Gruppen bestimmt sind und überwiegend immer von den gleichen Absendern kommen, ist die Auswertung der Absenderkennung auch eine praktikable Lösung. Bei nur geringem Aufkommen an Eingangs-Faxsendungen kann die manuelle Verteilung eine sinnvolle Alternative darstellen.

Prüffragen:

- Werden bei der Auswahl eines Faxservers die Anforderungen an das IT-System einschließlich Betriebssystem, Kommunikationskomponenten und Applikationssoftware erhoben und berücksichtigt?
- Sind bei der Auswahl eines Faxservers die Integrationsmöglichkeit in ein bestehendes Netz und in ein E-Mail- bzw. Workflow-System berücksichtigt?
- Kommen in den Faxservern nach Möglichkeit nur aktive ISDN-Karten bzw. Faxkarten zum Einsatz und sind diese zur Applikationssoftware kompatibel?
- Bietet die Applikationssoftware des Faxservers ausreichende Möglichkeiten für Fehler- und Sendeprotokolle?

# M 2.182 Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen. Alle wesentlichen Inhalte wurden in die Maßnahme M 2.199 *Aufrechterhaltung der Informationssicherheit* überführt.

# M 2.183 Durchführung einer RAS-Anforderungsanalyse

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.415 *Durchführung einer VPN-Anforderungsanalyse* integriert.

# M 2.184 Entwicklung eines RAS-Konzeptes

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.416 *Planung des VPN-Einsatzes* und M 2.417 *Planung der technischen VPN-Realisierung* integriert.

# M 2.185 Auswahl einer geeigneten RAS-Systemarchitektur

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.416 *Planung des VPN-Einsatzes* und M 2.419 *Geeignete Auswahl von VPN-Produkten* integriert.

# M 2.186 Geeignete Auswahl eines RAS-Produktes

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.419 *Geeignete Auswahl von VPN-Produkten* integriert.

# M 2.187 Festlegen einer RAS-Sicherheitsrichtlinie

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.418 *Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung* integriert.

# M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Werden in einer Institution Mobiltelefone verwendet, ist dafür eine Sicherheitsrichtlinie zu erstellen, die alle umzusetzenden Maßnahmen beschreibt. Darüber hinaus sollte es für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von Mobiltelefonen geben. Falls technisch möglich, sollten die Anleitung für das Mobiltelefon und die Sicherheitshinweise zusätzlich auf dem Mobiltelefon gespeichert sein. Der Mitarbeiter ist auf den Speicherort hinzuweisen.

### Anfallende Datenarten

Sobald ein Mobiltelefon eingeschaltet wird, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Bei diesem werden Daten der SIM-Karte, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Das erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

Die bei der Telekommunikation anfallenden Datenarten lassen sich grob in drei Gruppen untergliedern:

- Bestandsdaten (oder auch Stammdaten) sind diejenigen Daten, die in einem Dienst oder Netz dauerhaft gespeichert und bereit gehalten werden. Hierzu gehören die Rufnummer und gegebenenfalls der Name und die Anschrift des Teilnehmers, Informationen über die Art des Endgerätes, gegebenenfalls für den Anschluss jeweils verfügbare Leistungsmerkmale und Berechtigungen sowie Daten über die Zuordnung zu Teilnehmergruppen.
- Inhaltsdaten sind die eigentlichen "Nutzdaten", d. h. die übertragenen Informationen und Nachrichten.
- Verbindungsdaten geben Auskunft über die näheren Umstände von Kommunikationsvorgängen. Hierzu gehören Angaben über Kommunikationspartner (z. B. Rufnummern des rufenden und des angerufenen Anschlusses), Zeitpunkt und Dauer der Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse, Leitungen und sonstige technische Einrichtungen, Dienste und - bei mobilen Diensten - die Standortkennungen der mobilen Endgeräte.

Im Folgenden werden Empfehlungen gegeben, wie diese Daten vor Missbrauch geschützt werden können.

### Schutz vor Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Dazu gehören:

- der Zugriff auf die SIM-Karte,
- der Zugriff auf das eigentliche Endgerät, also das Mobiltelefon,

- der Zugriff auf bestimmte Funktionen des Mobiltelefons, z. B. das Telefonbuch,
- der Zugriff auf die Mailbox, also die Anrufbeantworterfunktion, oder andere Dienstleistungen des Netzbetreibers,
- der Zugriff auf Daten beim Netzbetreiber (bei Fragen an die Hotline wegen der Abrechnung muss unter Umständen ein Kennwort genannt werden).

Alle diese Sicherheitsmechanismen sollten auch genutzt werden (siehe auch M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*). Am wichtigsten ist dabei sicherlich der Schutz der SIM-Karte, da deren Missbrauch zu hohen finanziellen Schäden führen kann. Die persönliche Geheimzahl (PIN) darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden ebenso wenig der PUK.

Bei Smartphones ist auch der Schutz des Endgerätes durch PIN oder Passwörter von entscheidender Bedeutung, da hier die Applikationen vertrauliche Daten, wie zum Beispiel Authentisierungstoken oder Passwörter, enthalten können. Daher muss ein solcher Schutz bei allen Geräten eingerichtet sein und darf sich nicht deaktivieren lassen. Ferner muss sich das Gerät automatisch (zum Beispiel nach zehn Minuten Untätigkeit) selbst sperren.

Bei Verlust der SIM-Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch und damit auch einen finanziellen Schaden abzuwehren (siehe M 2.189 *Sperrung des Mobiltelefons bei Verlust*).

Um die missbräuchliche Benutzung der SIM-Karte rechtzeitig zu bemerken, sollte in jedem Fall der Einzelverbindungsnachweis auf unerklärliche Gebühren und Zielrufnummern geprüft werden.

**Einzelverbindungsnachweis**

Der Netzbetreiber speichert die Anrufdaten für die Abrechnung. In Deutschland darf er sie nur bis zur Rechnungsstellung speichern, maximal aber 80 Tage gemäß TDSV (Telekommunikationsdienstunternehmen-Datenschutzverordnung - Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen). Es kann aber für den Kunden sinnvoll sein, dem Netzbetreiber zu erlauben, die Anrufdaten länger zu speichern, falls nachträglich Probleme mit der Rechnung auftreten.

Jeder Kunde sollte einen Einzelverbindungsnachweis verlangen, um die Mobiltelefon-Nutzung kontrollieren zu können. In Deutschland haben die Kunden das Recht auf einen kostenlosen Einzelverbindungsnachweis. Aus diesem können z. B. folgende Daten entnommen werden:

- Rechnungsdatum,
- angerufene Rufnummer (vollständig bzw. die letzten Ziffern unkenntlich),
- Beginn, Ende oder Dauer der Verbindung,
- Kosten des Gesprächs.

Alle Mitbenutzer des Telefons müssen darüber informiert werden, dass ein Einzelverbindungsnachweis beantragt wurde und welche Daten dadurch erfasst werden.

Wenn in einer Behörde bzw. einem Unternehmen zur Kostenkontrolle Einzelverbindungsnachweise geführt und ausgewertet werden, ist das Verfahren mit dem Betriebs- bzw. Personalrat und dem Datenschutzbeauftragten abzustimmen und den Benutzern bekannt zu geben.

Immer nach Erhalt der Einzelverbindungsnachweise sollte überprüft werden, ob sie korrekt sind. Hierdurch lässt sich auch ersehen, wo eventuell Kosten reduziert werden können.

**Weitergabe der Rufnummer**

Es kann gewählt werden, ob und welche Daten zu dem Mobiltelefon-Anschluss in öffentliche Telefonbücher eingetragen werden beziehungsweise für Abfragen über Telefonauskünfte zur Verfügung stehen. Ein solcher Eintrag ist jedoch nicht immer sinnvoll, zum Beispiel bei Mobiltelefonen aus einem Pool oder wenn die Zahl der Anrufer klein gehalten werden soll.

Wenn die Rufnummernanzeige aktiviert ist, können die Gesprächspartner (je nach Ausstattung) sehen, von welcher Telefonnummer sie angerufen werden. Dieser Dienst kann vom Netzbetreiber generell für ein Mobiltelefon an- oder abgeschaltet werden.

**Rufnummernunterdrückung**

Im Mobilfunk-Netz können den beteiligten Kommunikationspartnern die jeweiligen Rufnummern signalisiert werden. Wenn dies nicht gewünscht ist, sollte M 5.79 *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung* beachtet werden.

**Schutz vor Abhören von Telefonaten**

Der einzige wirksame Schutz gegen das Abhören von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Da diese Verschlüsselung nur bei wenig handelsüblichen Geräten realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potenziell abgehört werden. Die Kommunikation zwischen Mobiltelefon und Basisstation wird aber in Deutschland und den meisten anderen Ländern verschlüsselt. Diese Verschlüsselung in Mobilfunknetzen ist jedoch mit entsprechendem Aufwand zu brechen und bietet daher nur mittelmäßigen Schutz.

Folgende Maßnahmen werden zum Schutz vorm Abhören empfohlen:

- Es sollte nicht immer und überall telefoniert werden. Zum Telefonieren sollte ein ungestörter Bereich aufgesucht werden (dadurch werden auch andere weniger gestört).
- Grundsätzlich sollten keine Telefongespräche mit vertraulichem Inhalt geführt werden.
- Manche Mobiltelefone zeigen auf dem Display an, wenn die Übertragung zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird. Wenn diese Anzeige vorgesehen ist, sollten die Benutzer darüber informiert werden. Ab und zu sollten sie sich durch einen Blick auf das Display davon überzeugen, dass tatsächlich verschlüsselt wird. So gibt es z. B. einige Länder, in denen die Kommunikation zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird.
- Es gibt auch einige wenige und verhältnismäßig teure Mobiltelefone, mit denen die Kommunikation von Ende zu Ende verschlüsselt werden kann. Dafür müssen aber beide Gesprächspartner kompatible Geräte einsetzen. Wenn häufiger hochsensitive Informationen über Mobiltelefon weitergegeben werden sollen, kann dies sinnvoll sein.
- Bei der Datenübertragung zum Beispiel von einem Laptop über ein Mobilfunknetz sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Programmen, die dies einfach ermöglichen. Alternativ kann für die Datenübertragung ein verschlüsselter VPN-Tunnel etabliert werden.

- Wenn Mobiltelefone bzw. SIM-Karten gewechselt werden, ist es enorm aufwendig, gezielt Telefonate abzuhören. Dies kann daher bei der Übertragung hochsensitiver Information bzw. Daten zweckmäßig sein.
- Es sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden. Fehlende Gebühren für bestimmte Verbindungen können darauf hindeuten, dass abgehört wurde ebenso wie Gebühren für nicht bewusst getätigte Verbindungen.

**Sensibilisierung der Benutzer**

Die Benutzer von Mobiltelefonen sollten regelmäßig für die speziellen Gefährdungen der Informationssicherheit sensibilisiert werden (siehe M 2.558 *Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs*).

**Regelungen zur Nutzung privater Mobiltelefone**

Werden private Mobiltelefone für dienstliche Zwecke benutzt, sind folgende Aspekte vorher zu regeln:

- Wer bezahlt dienstliche Gespräche und wie werden sie abgerechnet?
- Moderne Mobiltelefone beinhalten Terminkalender, Adressbücher, E Mail-Unterstützung und mehr. Um diese Funktionen sinnvoll einzusetzen, ist im Allgemeinen eine Synchronisation mit einem PC oder einem Internetdienst erforderlich. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird, beziehungsweise, ob dienstliche Daten mit diesen Internetdiensten verarbeitet und dort gespeichert werden dürfen.

**Regelungen zur Nutzung dienstlicher Mobiltelefone**

Notwendige Regeln für die Nutzung von dienstlichen Mobiltelefonen:

- Es muss geklärt werden, ob bzw. in welcher Menge Privatgespräche mit dienstlichen Mobiltelefonen geführt werden dürfen.
- Es sollte überlegt werden, die Nutzung der Mobiltelefone auf bestimmte Kommunikationspartner zu begrenzen, um zum Beispiel unnötigen Kosten vorzubeugen oder auch um die Informationsweitergabe einzuschränken (siehe M 2.42 *Festlegung der möglichen Kommunikationspartner*). Hierzu kann eine organisatorische Vorgabe erfolgen, es kann aber auch technisch geregelt werden, wie weiter unten unter den Stichworten "Anrufsperrungen" und "Geschlossene Benutzergruppe" beschrieben.
- Auch bei dienstlichen Mobiltelefonen sollten die Benutzer über die Tarifstruktur, Roaming-Abkommen und Kosten informiert werden, damit sie beispielsweise im Ausland die günstigsten Netzbetreiber auswählen können, wobei die sichersten Netzbetreiber Priorität haben.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den Mobiltelefonen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von Mobiltelefonen sollte geregelt werden. Hierzu empfiehlt sich die Einrichtung eines Mobiltelefon-Pools (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).
- Bei jedem Benutzerwechsel müssen alle benötigten PINs gesichert weitergegeben werden (siehe M 2.22 *Hinterlegen des Passwortes*).

**Generelle Regelungen**

Unabhängig davon, ob privat oder dienstlich angeschaffte Mobiltelefone genutzt werden, sollte der Arbeitgeber schriftlich regeln,

- dass der Fahrer in dienstlich genutzten Fahrzeugen während der Fahrt nicht ohne Freisprecheinrichtung telefonieren darf, da sonst bei einem Unfall Mithaftung droht,
- welche Daten auf dem Mobiltelefon gespeichert werden dürfen und ob für die Daten eine Datenverschlüsselung einzurichten ist,
- dass Dienstgeheimnisse nicht über das Mobiltelefon weitergegeben werden dürfen, weil Gespräche auch akustisch durch Personen in der unmittelbaren Umgebung mitgehört werden können,
- dass der Benutzer sich von der Identität seiner Gesprächspartner überzeugen sollte.

Für Endgeräte mit Zugriffsschutz sollte es eine Passwortrichtlinie geben, die die Art des Zugriffschutzes (siehe M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*) festlegt und die gegebenenfalls Regelungen zur Ausgestaltung enthält (Länge des Passwortes etc.). Es wird meistens als unkomfortabel empfunden, nach wenigen Minuten Untätigkeit immer wieder ein langes Passwort einzugeben. Daher sollten Institutionen einen angemessenen Kompromiss zwischen Sicherheit und Komfort wählen und nicht lediglich die Passwortrichtlinie für den Arbeitsplatz-PC übernehmen.

Wird das Mobiltelefon in fremden Büroräumen vor Ort benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten. Ein Mobiltelefon sollte möglichst nicht unbeaufsichtigt bleiben. Falls es in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein und ausgeschaltet werden (Power Off). Auch in fremden Räumlichkeiten wie Hotelzimmern sollte ein Mobiltelefon bei Abwesenheit nicht ungeschützt herumliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden., bevor das Gerät ausgeschaltet wird (Power Off) und in den Safe oder zumindest an einen nicht sichtbaren Ort gebracht wird (z. B. Koffer).

Im Übrigen sollten Regelungen bei Verlust des Mobiltelefons (M 2.189 *Sperrung des Mobiltelefons bei Verlust*) getroffen und den Mitarbeitern bekannt gegeben werden. Werden für moderne Mobiltelefone besondere Programme zum Orten, Löschen und Sperren des Endgerätes angeschafft, so sind die Mitarbeiter in der Bedienung dieser Programme zu schulen. Ferner müssen Regelungen geschaffen werden, wie mit zeitweise verlorenen und dann wieder gefundenen Geräten zu verfahren ist, da diese manipuliert sein könnten. Es empfiehlt sich, solche Geräte komplett zu löschen und alle relevanten Daten und Programme neu aufzuspielen.

**Benutzungsverbot von Mobiltelefonen**

Es sollte überlegt werden, ob es in allen oder bestimmten Bereichen einer Institution verboten werden sollte, Mobiltelefone zu benutzen oder mitzuführen (siehe M 5.80 *Schutz vor Abhören der Raumgespräche über Mobiltelefone* über Mobiltelefone). Dies kann zum Beispiel für Besprechungsräume sinnvoll sein. Wenn die Sicherheitsleitlinie der Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

Durch Mobiltelefone können unter Umständen auch andere technische Geräte in ihrer Funktion beeinträchtigt werden. So können beispielsweise empfindliche IT Systeme in Serverräumen oder auch auf Intensivstationen durch Mobil-

telefone gestört werden. Mögliche Störungen sind umso unwahrscheinlicher, je geringer die Sendeleistung des Mobiltelefons ist beziehungsweise je weiter dieses entfernt ist.

Bei IT Systemen, auf denen sensitive Daten verarbeitet werden oder die an ein Rechner-Netz angebunden sind, sollten Verbindungen über ein Mobilfunknetz nur mit VPN-Techniken zugelassen werden (siehe M 5.81 Sichere Datenübertragung über Mobiltelefone).

**Telefonbuch**

Im Telefonbuch eines Mobiltelefons können Rufnummern und zugehörige Namen oder weitere Details gespeichert werden, und zwar im Endgerät, also dem Mobiltelefon, einer eventuell vorhandenen zusätzlichen Speicherkarte oder auf der SIM-Karte. Das Telefonbuch auf dem Endgerät beziehungsweise der Speicherkarte hat für gewöhnlich eine größere Kapazität und erlaubt mehr Zusatzdaten als der Speicher der SIM-Karte, zum Beispiel Anschrift, Faxnummer, E-Mail-Adresse und weitere Notizen, sodass die Inhalte aus SIM-Karte und Endgerät nicht übereinstimmen müssen. Wo die Telefonnummern bevorzugt gespeichert werden sollen, hängt von verschiedenen Faktoren ab, beispielsweise wie einfach die Daten auf anderen Medien gesichert werden können (siehe M 6.72 *Ausfallvorsorge bei Mobiltelefonen*) oder wie hoch der Schutzbedarf der Informationen ist. Denn je nach Speicherort sind die Daten durch unterschiedliche Mechanismen geschützt: Liegen sie auf der SIM-Karte, kann auf die Informationen nur durch die korrekte PIN zugegriffen werden. Werden die Daten auf dem Endgerät oder einer externen Speicherkarte im Endgerät gespeichert, liegen sie in der Regel im Klartext vor und können nur durch zusätzliche Verschlüsselung geschützt werden. In diesem Fall bietet es sich an, den Passwortschutz für das Endgerät mit einer Verschlüsselung zu kombinieren.

Im Telefonbuch sollten alle wichtigen Rufnummern gespeichert werden, damit diese jederzeit verfügbar sind. Die gespeicherten Rufnummern sollten gelegentlich kontrolliert werden, ob sie noch korrekt beziehungsweise notwendig sind. Alle Rufnummern sollten so gespeichert werden, dass sie weltweit angerufen werden können, das heißt inklusive Landes- und Ortsvorwahl. Da nur der Ländercode international abgestimmt ist, nicht die Null, sollte dazu jede Rufnummer mit einem "+" am Anfang, gefolgt vom Ländercode (zum Beispiel +49 für Deutschland), Ortsvorwahl ohne führende Null und dann Telefonnummer eingegeben werden. Ein Eintrag könnte also wie folgt aussehen: +4922895825369 GS-Hotline.

Wenn das Mobiltelefon von mehreren Benutzern eingesetzt wird, sollte das Telefonbuch vor der Übergabe gelöscht und das Telefonbuch des neuen Benutzers aufgespielt werden. Die Telefonbücher aller Benutzer müssen dafür zentral vom Verwalter des Mobiltelefon-Pools gespeichert werden (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).

**Anrufbeantworter**

Über die Netzbetreiber kann im Allgemeinen zu einem Mobiltelefon eine Anrufbeantworter-Funktionalität aktiviert werden. Eingehende Anrufe werden dabei beim Netzbetreiber in einer so genannten Mail- oder Mobilbox gespeichert, die vom Benutzer jederzeit abgerufen werden kann. Dies kann sehr sinnvoll sein, verursacht aber in der Regel zusätzliche Kosten.

Der Zugriff auf die Mailbox sollte durch eine PIN geschützt werden. Auch wenn die Mailbox nicht genutzt wird, sollte die voreingestellte PIN schnell geändert werden, um eine Fremdnutzung zu verhindern.

Eingegangene Aufzeichnungen sollten regelmäßig abgehört werden. Alle Benutzer müssen darüber informiert werden, wie dies funktioniert.

**Rufumleitung**

Mit der Funktion Rufumleitung können eingehende Anrufe auf die Mailbox oder auf eine andere Rufnummer weitergeleitet werden. Dafür gibt es mehrere Varianten:

- Es können alle eingehenden Anrufe weitergeleitet werden.
- Anrufe werden nur dann weitergeleitet, wenn besetzt ist.
- Anrufe werden nur dann weitergeleitet, wenn der Anschluss nicht erreichbar ist, z. B. wegen eines Funklochs oder weil das Mobiltelefon ausgeschaltet ist.
- Es können bestimmte Arten von Anrufen weitergeleitet werden, z. B. Sprach-, Daten- oder Faxanrufe.
- Viele Smartphones gestatten sogar eine telefonnummerngenaue Einrichtung von Weiterleitungen auf andere Anschlüsse oder den Anrufbeantworter.

Dabei sollte allerdings berücksichtigt werden, dass Rufumleitungen auf Festnetzanschlüsse hohe Kosten verursachen können, da der Angerufene die Weiterleitungskosten selbst tragen muss.

**Anrufsperrungen**

Über Anrufsperrungen können Gespräche zu oder von einer Rufnummer gesperrt werden. Diese Funktionen werden über den Netzbetreiber zur Verfügung gestellt und können über das Mobiltelefon geändert werden. Dafür ist im Allgemeinen ein Passwort erforderlich. Viele Smartphones können Anrufsperrungen ohne Unterstützung des Netzbetreibers durch lokale Software realisieren, die in der Regel viel feinteiliger konfiguriert werden kann.

Anrufsperrungen können sinnvoll sein, wenn das Mobiltelefon an Dritte weitergegeben werden soll. Es gibt verschiedene Möglichkeiten von Anrufsperrungen:

- Sperren aller abgehenden Anrufe (Notrufnummern sind davon ausgenommen)
- Sperren aller abgehenden internationalen Anrufe
- Sperren aller abgehenden internationalen Anrufe außer ins Heimatland
- Sperren aller ankommenden Anrufe
- Sperren aller ankommenden Anrufe bei Aufenthalt im Ausland
- Sperren bestimmter ankommender oder abgehender Anrufe

Ob und welche Art von Anrufsperrungen gewählt werden sollte, hängt von der Einsatzart des jeweiligen Mobiltelefons ab.

**Geschlossene Benutzergruppe**

Über den Dienst "Geschlossene Benutzergruppe" kann die Kommunikation auf die Mitglieder dieser Gruppe beschränkt werden (siehe auch M 5.47 *Einrichten einer Closed User Group*).

Die Gruppenmitglieder müssen beim Netzbetreiber eingetragen werden. Die Option "Geschlossene Benutzergruppe" kann am Mobiltelefon aktiviert wer-

den. Geschlossene Benutzergruppen sind beispielsweise sinnvoll, um die Datenübertragung über Mobilfunk einzuschränken. Auf vielen Smartphones können solche Benutzergruppen in der Regel auch lokal, ohne Einbindung des Netzbetreibers, umgesetzt werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Mobiltelefon-Nutzung?
- Wie wird die Einhaltung der Sicherheitsrichtlinie für die Mobiltelefon-Nutzung überprüft?
- Besitzt jeder Mobiltelefon-Benutzer ein Exemplar dieser Mobiltelefon-Richtlinie oder ein Merkblatt mit einem Überblick über die wichtigsten Sicherheitsmechanismen?
- Ist die Sicherheitsrichtlinie für die Mobiltelefon-Nutzung Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen?
- Wurden die Benutzer von Mobiltelefonen auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer von Mobiltelefonen auf deren geeignete Aufbewahrung hingewiesen?

# M 2.189 Sperrung des Mobiltelefons bei Verlust

**Verantwortlich für Initiierung:** Benutzer, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Bei Verlust der SIM-Karte bzw. des Mobiltelefons trägt der Inhaber der SIM-Karte die Kosten für eine missbräuchliche Nutzung des Mobiltelefonanschlusses. Daher sollte die SIM-Karte beim Netzbetreiber sofort gesperrt werden, um einen eventuellen Missbrauch, und damit einen zusätzlichen finanziellen Schaden, abzuwehren.

Darüber hinaus sollte die PIN-Abfrage der SIM-Karte stets aktiviert sein (siehe M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*). Bei einem Diebstahl oder Verlust verhindert dies, dass die SIM-Karte von einem Unbefugten benutzt oder ausgewertet werden kann. Bei deaktivierter SIM PIN kann ein nicht legitimierter Nutzer die SIM PIN aktivieren oder die SIM durch mehrfache Falscheingaben unbrauchbar machen. Die PIN wird allerdings nur abgefragt, wenn das Mobiltelefon eingeschaltet wird (Power On). Wird ein eingeschaltetes Mobiltelefon gestohlen, kann hiermit zumindest solange missbräuchlich telefoniert werden, bis der Akku leer ist.

Für Smartphones gibt es auf dem Markt Software zum Diebstahlschutz, die es erlaubt, das Mobiltelefon per GPS-Empfänger oder Mobilfunkzellen zu orten, die Daten auf dem Gerät zu löschen oder das Gerät vollständig zu sperren. Gegebenenfalls können sogar automatisierte Nachrichten an den IT-Betrieb über die Sperrung oder den Aufenthaltsort eines Gerätes versandt werden, wenn beispielsweise die SIM-Karte ausgetauscht wurde. Viele dieser Programme gestatten es auch Nachrichten an das Telefon zu senden oder aktivieren lediglich eine Displayanzeige, die den Finder bitten, die Telefonnummer des IT-Betriebs anzurufen oder das Gerät an einer bestimmten Adresse abzugeben. Die Anschaffung einer solchen Software kann sich schnell bezahlt machen, wenn ein verloren gegangenes Smartphone schneller zurückgegeben werden kann und die Daten besser vor Dieben geschützt sind. Auf der anderen Seite muss permanent das GPS aktiviert und eine Mobilfunk-Verbindung aufgebaut sein. Dies kann zu einem erhöhen Akkuverbrauch führen, zusätzlichen kann die notwendige Geräteortung durch Dritte missbraucht werden (siehe M 5.78 *Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung* und M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen*).

Um rechtzeitig zu bemerken, dass die SIM-Karte womöglich missbräuchlich genutzt wurde, sollte der Einzelverbindungsnachweis immer auf unerklärliche Gebühren und Zielrufnummern überprüft werden.

Alle Daten, die für die Sperrung der SIM-Karte bzw. des Mobiltelefons benötigt werden, sollten griffbereit, aber getrennt vom Mobiltelefon aufbewahrt werden. Das sind

- die Rufnummer des Mobilfunkanschlusses sowie die zugehörige SIM-Kartennummer,
- die Seriennummer des Mobiltelefons (GSM-USSD-Code *#06#),
- die Servicenummer des Netzbetreibers, unter der der Sperrwunsch gemeldet werden kann sowie
- das Servicenummer-Passwort und die Kundennummer, also die Daten, die für die Authentikation gegenüber dem Netzbetreiber benötigt werden.

Prüffragen:

- Ist sichergestellt, dass Mobiltelefone nach einem Verlust zeitnah gesperrt werden?
- Sind alle notwendigen Informationen für die Sperrung eines Mobiltelefons bei einem Verlust jederzeit griffbereit?

# M 2.190 Einrichtung eines Mobiltelefon-Pools

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

**Einrichtung eines Mobiltelefon-Pools**

Sind in einer Behörde bzw. einem Unternehmen eine Vielzahl von Mobiltelefonen im Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Mobiltelefone in einer Sammelaufbewahrung (Pool) zu halten.

Für alle Mobiltelefone ist die Stromversorgung sicherzustellen, damit die Akkus dieser Geräte den sofortigen Einsatz erlauben. Dabei ist zu beachten, dass sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird. Wenn die Mobiltelefone häufiger über längere Zeiträume eingesetzt werden, sollten zusätzlich Ersatzakkus vorrätig gehalten werden, insofern die Akkus austauschbar sind.

Hinweis: Die Ladegeräte sollten den Mobiltelefonen eindeutig und leicht erkennbar zugeordnet werden. Die Ladegeräte sehen sich zwar alle sehr ähnlich, sind aber leider meist nicht austauschbar. Ferner sollten auch die zugehörigen Datenkabel eindeutig den jeweiligen Mobiltelefonen zugeordnet und gemeinsam mit dem Ladegerät aufbewahrt werden.

Zusätzlich müssen die Rücknahme und die Ausgabe von Mobiltelefonen dokumentiert werden, sodass jederzeit nachvollziehbar ist, wer welche Geräte einsetzt bzw. zu einer bestimmten Zeit eingesetzt hat. Jeder Benutzer sollte mit Namen, Organisationseinheit, Datum und Uhrzeit in das Übergabejournal eingetragen werden.

Bei der Übergabe und Rücknahme von Mobiltelefonen sind außerdem folgende Punkte zu beachten:

**Übergabe:**
- Der neue Benutzer erhält alle benötigten PINs und Passwörter für die Nutzung des Mobiltelefons. Wenn diese auf selbst gewählte Werte geändert werden, müssen die neuen Werte bei der Rückgabe dokumentiert werden.
- Außerdem erhält er die Rufnummer des Mobiltelefons.
- Es sollten alle vom neuen Benutzer benötigten Telefonnummern und gegebenenfalls Programme aufgespielt werden. Ebenso sollten alle Konfigurationseinstellungen vorgenommen werden.
- Dem neuen Benutzer wird ein Merkblatt für den sicheren Umgang mit dem Mobiltelefon übergeben. Der Benutzer sollte außerdem die Bedie¬nungsanleitung des Mobiltelefons bekommen. Neben der normalen Bedie¬nung seines Telefons sollte der Benutzer vor allem in der Lage sein, etwaige Warnanzeigen (wie Piktogramme im Display) zu interpretieren.
- Das Mobiltelefon sollte geladen und zusammen mit dem passenden Ladegerät und falls vorhanden dem Datenkabel übergeben werden. Wenn das Mobiltelefon über längere Zeitspannen einsetzbar sein soll, sollte ein geladener Ersatzakku mit übergeben werden.

**Rücknahme bzw. Weitergabe:**

- Der Benutzer gibt die zuletzt benutzten PINs und Passwörter bekannt. Es muss überprüft werden, ob diese korrekt sind. Sie müssen notiert (und sicher verwahrt) werden.
- Der Benutzer muss das Mobiltelefon vollständig, mit allem Zubehör sowie der Dokumentation zurückgeben. Dies ist zu kontrollieren. Das Gerät sollte zudem auf Defekte, Schadsoftware und gegebenenfalls auch auf Manipulationen der Hardware überprüft werden. Um eventuelle Hardwaremanipulationen aufzudecken, kann das Gewicht des Mobiltelefons bei Rückgabe mit dem Gewicht bei der Übergabe zu verglichen werden. Haben Angreifer das Endgerät mit einem Abhörmikrofon präpariert, so ist es in der Regel messbar schwerer.
- Der Benutzer muss sicherstellen, dass vor Rückgabe des Gerätes sämtliche Daten (SMS, Fax, E-Mail, Telefonnummern oder sonstige Daten), die der Benutzer noch benötigt, auf ihm zugängliche Datenträger (z. B. seinen PC) übertragen werden.
- Das Gerät sollte komplett auf den Werkszustand zurückgesetzt und alle Daten vom Endgerät und von der Speicher- und SIM-Karte gelöscht werden. Nur so wird wirkungsvoll der Befall durch Schadsoftware und ein unbewusster Datenabfluss vermieden. Danach können wieder alle benötigten Programme und Daten auf das Gerät aufgespielt werden.

Prüffragen:

- Werden die Benutzer bei der Ausgabe von Mobiltelefonen auf die Regelungen und Sicherheitsmaßnahmen hingewiesen, die von ihnen einzuhalten sind?
- Wird das Mobiltelefon nach Rückgabe auf den Werkszustand zurückgesetzt?
- Wird das Mobiltelefon bei Übergabe an einen neuen Benutzer für ihn konfiguriert und mit den nötigen Programmen und Daten ausgestattet?
- Werden die Benutzer bei der Ausgabe von Mobiltelefonen informiert, wie die Geräte aufzubewahren sind?
- Wird die Ausgabe und Rücknahme der Mobiltelefone dokumentiert?

# M 2.191 Etablierung des IT-Sicherheitsprozesses

Diese Maßnahme ist mit Version 2006 entfallen.

# M 2.192 Erstellung einer Leitlinie zur Informationssicherheit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Die Leitaussagen zur Sicherheitsstrategie sollten in einer Leitlinie zur Informationssicherheit zusammengefasst werden, um die zu verfolgenden Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter zu dokumentieren. Mit der Sicherheitsleitlinie bekennt sich die Behörden- bzw. Unternehmensleitung sichtbar zu ihrer Verantwortung für Informationssicherheit.

Bei der Erstellung der Leitlinie zur Informationssicherheit müssen folgende Punkte beachtet werden:

### Verantwortung der Behörden- bzw. Unternehmensleitung

Wichtig ist, dass die Behörden- bzw. Unternehmensleitung in vollem Umfang hinter der Leitlinie zur Informationssicherheit und den darin festgehaltenen Zielen steht. Daher muss die Sicherheitsleitlinie von der Behörden- bzw. Unternehmensleitung unterschrieben und in deren Namen veröffentlicht werden. Selbst wenn einzelne Aufgaben im Rahmen des Sicherheitsprozesses an Personen oder Organisationseinheiten delegiert werden, verbleibt die Gesamtverantwortung für die Informationssicherheit immer bei der Behörden- bzw. Unternehmensleitung.

### Festlegung des Geltungsbereichs

In der Informationssicherheitsleitlinie muss beschrieben werden, für welche Bereiche diese gelten soll. Der Geltungsbereich kann die gesamte Institution umfassen oder aus Teilbereichen dieser bestehen. Wichtig ist jedoch, dass die betrachteten Fachaufgaben und Geschäftsprozesse im Geltungsbereich komplett enthalten sind.

### Festlegung von Sicherheitszielen

Zu Beginn des Sicherheitsprozesses muss die Behörden- bzw. Unternehmensleitung die Sicherheitsziele festlegen, abstimmen und dokumentieren. Diese lassen sich aus den Geschäftsprozessen und Fachaufgaben, gesetzlichen Rahmenbedingungen und allgemeinen Behörden- oder Unternehmenszielen ableiten. Die Sicherheitsziele dienen als Grundlage für die Erstellung der Leitlinie zur Informationssicherheit.

### Inhalt der Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit sollte kurz und bündig formuliert sein, da sich mehr als 20 Seiten in der Praxis nicht bewährt haben. Sie sollte dabei aber mindestens die folgenden Aspekte enthalten:

- Der Stellenwert der Informationssicherheit und die Bedeutung der wesentlichen Informationen, Geschäftsprozesse und IT für die Institution müssen dargestellt werden.
- Die Sicherheitsziele und der Bezug der Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution müssen dabei erläutert werden.
- Die Kernelemente der Sicherheitsstrategie sollten genannt werden.

- Die Leitungsebene muss allen Mitarbeitern aufzeigen, dass die Sicherheitsleitlinie von ihr getragen und durchgesetzt wird. Ebenso muss es Leitaussagen zur Erfolgskontrolle geben.
- Die für die Umsetzung des Sicherheitsprozesses etablierte Organisationsstruktur muss beschrieben werden (siehe M 2.193 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit*).

**Bekanntgabe der Leitlinie zur Informationssicherheit**

Sicherheitsmaßnahmen und organisatorische Regelungen werden erfahrungsgemäß nur dann von allen Mitarbeitern befolgt, wenn diese ihren Sinn erkennen. Die Sicherheitsleitlinie muss daher veröffentlicht werden, um die Strategie des verantwortlichen Managements zu dokumentieren. Dies sollte so erfolgen, dass der Stellenwert der Informationssicherheit deutlich wird. Es ist wichtig, dass alle Mitarbeiter die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können. Neue Mitarbeiter sollten auf die Leitlinie zur Informationssicherheit hingewiesen werden, bevor sie Zugang zu geschäftsrelevanten Informationen erhalten. Müssen alle Mitarbeiter die Kenntnis der Sicherheitsleitlinie schriftlich bestätigen, wird deren Bedeutung unterstrichen. Generell sollte die Leitlinie zur Informationssicherheit so allgemein gehalten sein, dass sich alle Mitarbeiter aus den verschiedenen Organisationsbereichen einer Institution davon angesprochen fühlen. Es ist aber auch möglich, die Sicherheitsleitlinie für spezielle Anwendungen oder Bereiche innerhalb einer Institution um Inhalte zu ergänzen, die nur für einen eingeschränkten Personenkreis relevant oder die vertraulich sind. Es empfiehlt sich, diese Abschnitte in eine Anlage zur Leitlinie zu verlagern, um so flexibler und zeitnah auf erforderliche Änderungen reagieren zu können, ohne dass der allgemeine Teil der Leitlinie angepasst werden muss. Falls erforderlich, kann die Anlage separat als vertraulich gekennzeichnet und besonders geschützt werden.

**Aktualisierung der Sicherheitsleitlinie**

Die Leitlinie zur Informationssicherheit sollte in regelmäßigen Abständen auf ihre Aktualität hin überprüft und gegebenenfalls angepasst werden. Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder der Sicherheitsstrategie sollten einfließen. Bei den häufig rasanten Entwicklungen sowohl im Bereich der IT als auch im Bereich der Sicherheit empfiehlt es sich, die Sicherheitsleitlinie alle zwei Jahre zu überarbeiten.

Prüffragen:

- Gibt es eine von der Leitungsebene verabschiedete Leitlinie zur Informationssicherheit?
- Ist ein klarer Geltungsbereich für die Sicherheitsleitlinie festgelegt?
- Beschreibt die Sicherheitsleitlinie den Stellenwert der Informationssicherheit, die Sicherheitsziele, die Kernelemente der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit?
- Sind alle Mitarbeiter auf die Leitlinie zur Informationssicherheit hingewiesen worden?
- Ist die Sicherheitsleitlinie aktuell?

# M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

### Planung und Einrichtung der Informationssicherheitsorganisation

Um einen Sicherheitsprozesses erfolgreich planen, umsetzen und aufrechterhalten zu können, muss eine geeignete Organisationsstruktur für Informationssicherheit vorhanden sein. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der Sicherheitsziele wahrnehmen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Zu Beginn eines Sicherheitsprozesses kann sich herausstellen, dass innerhalb der Institution zwar bereits Verantwortliche für verschiedene Aspekte der Informationssicherheit benannt sind, es aber keine übergreifende Struktur für die Informationssicherheit gibt. In diesem Fall muss eine geeignete, übergreifende Organisationsstruktur für die Informationssicherheit aufgebaut werden.

Ist bereits eine IS-Organisation etabliert, sollte regelmäßig überlegt werden, ob diese noch angemessen ist oder an neue Rahmenbedingungen angepasst werden muss.

### Funktion des IT-Sicherheitsbeauftragten

Die Art und Ausprägung einer Informationssicherheitsorganisation hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. Die Funktion des IT-Sicherheitsbeauftragten muss allerdings in jeder Institution eingerichtet werden, da er für alle Belange der Informationssicherheit zuständig ist. Die Aufgaben des IT-Sicherheitsbeauftragten sind unter anderem:

- den Informationssicherheitsprozess zu steuern und zu koordinieren,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren, sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- den Realisierungsplan für die Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- der Leitungsebene und dem IS-Management-Team über den Status Quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen Bereichs-IT-, Projekt- sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu steuern.

Der IT-Sicherheitsbeauftragte muss bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt werden, damit sichergestellt ist, dass sicherheitsrelevante Aspekte ausreichend beachtet werden.

Dazu gehören z. B. die Beschaffung von IT-Systemen oder die Gestaltung von IT-gestützten Geschäftsprozessen.

Um den direkten Zugang zur Behörden- bzw. Unternehmensleitung sicherzustellen, ist es empfehlenswert, diese Rolle als Stabsstelle einzurichten.

In kleinen Institutionen kann die Funktion des IT-Sicherheitsbeauftragten auch von einem qualifizierten Mitarbeiter neben anderen Aufgaben wahrgenommen werden. Maßgeblich ist, dass dem IT-Sicherheitsbeauftragten ausreichend Zeit für seine Aufgaben zugebilligt wird. Vor allem bei der erstmaligen Einrichtung des Sicherheitsprozesses müssen hierfür hinreichende zeitliche Ressourcen eingeplant werden. Auch sollte schon bei der Planung der Informationssicherheitsorganisation ein qualifizierter Vertreter des IT-Sicherheitsbeauftragten benannt werden.

**Auswahl des IT-Sicherheitsbeauftragten**

Der IT-Sicherheitsbeauftragte sollte Wissen und Erfahrung in den Gebieten Informationssicherheit und Informationstechnik besitzen. Weiterhin sollte er über die folgenden Qualifikationen und Eigenschaften verfügen:

- Überblick über Aufgaben und Ziele der Institution
- Identifikation mit den Zielsetzungen der Informationssicherheit
- Kooperations- und Teamfähigkeit (wenige andere Aufgaben erfordern so viel Fähigkeit und Geschick im Umgang mit anderen Personen)
- Fähigkeit zum selbstständigen Arbeiten
- Durchsetzungsvermögen
- Erfahrungen im Projektmanagement

Ein IT-Sicherheitsbeauftragter alleine kann nicht für angemessene Sicherheit in allen Bereichen einer Institution sorgen. Daher sind Kommunikations- und Präsentationsfähigkeiten wichtig. Die Leitungsebene muss in zentralen Fragen des Sicherheitsprozesses immer wieder eingebunden werden, außerdem müssen Entscheidungen eingefordert werden. Die Zusammenarbeit mit den Mitarbeitern ebenso wie mit Externen verlangt viel Geschick, da diese von der Notwendigkeit der (für sie manchmal etwas lästigen) Sicherheitsmaßnahmen überzeugt werden müssen. Mindestens genauso heikel ist die Befragung der Mitarbeiter nach sicherheitskritischen Vorkommnissen und Schwachstellen. Um bei diesen Befragungen verwertbare Ergebnisse zu erzielen, müssen die Mitarbeiter davon überzeugt sein, dass ehrliche Antworten nicht gegen sie selbst verwendet werden.

**Aufbau eines Informationssicherheitsmanagement-Teams**

In größeren Institutionen ist es sinnvoll, ein IS-Management-Team aufzubauen, das den IT-Sicherheitsbeauftragten unterstützt und sämtliche übergreifende Belange der Informationssicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet.

Die Größe und die Zusammenstellung des IS-Management-Teams sollten in Abhängigkeit vom Umfang des Sicherheitsprozesses und der dafür benötigten Ressourcen und Expertisen definiert werden. In BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise* sind verschiedene Varianten dargestellt, wie eine Aufbauorganisation des Informationssicherheitsmanagements aussehen kann.

**Auswahl des IS-Management-Teams**

Um die verschiedenen Sichten der Informationssicherheit in einer Institution zu berücksichtigen, sollten im IS-Management-Team folgende Vertreter zusammenarbeiten:

- IT-Sicherheitsbeauftragter
- IT-Verantwortliche
- Vertreter der Anwender
- Datenschutzbeauftragte

Bei Bedarf sollten Vertreter der Revision, des Justiziariats und der Personalvertretung der Institution hinzugezogen werden.

**Benennung eines verantwortlichen Managers**

Auf Leitungsebene sollte die Aufgabe Informationssicherheit eindeutig einem verantwortlichen Manager zugeordnet sein, an den der IT-Sicherheitsbeauftragte direkt berichtet. In kleinen Institutionen kann auch ein Geschäftsführer diese Aufgabe übernehmen.

**Überprüfung der Informationssicherheitsorganisation**

Eine einmal aufgebaute IS-Organisation ist nicht statisch. Geschäftsprozesse und Umfeldbedingungen ändern sich permanent, so dass auch die IS-Organisation immer wieder überdacht werden muss. Dabei sollte beispielsweise beleuchtet werden, ob die Aufgaben und Kompetenzen innerhalb des Sicherheitsprozesses ausreichend klar definiert waren, aber auch, ob vorgesehene Aufgaben wie geplant wahrgenommen werden konnten. Wichtig sind vor allem die folgenden Punkte:

- Überwachung von Verantwortlichkeiten im laufenden Betrieb
  Es muss regelmäßig überprüft werden, ob alle Verantwortlichkeiten und Zuständigkeiten eindeutig zugewiesen wurden und diese praxistauglich sind.
- Überprüfung der Einhaltung von Vorgaben
  Es muss regelmäßig geprüft werden, ob alle Prozesse und Abläufe der IS-Organisation wie vorgesehen angewendet und durchgeführt werden. Gleichzeitig sollte sichergestellt werden, dass die aufgebauten Organisationsstrukturen für Informationssicherheit den Anforderungen gerecht werden.
- Beurteilung der Effizienz von Prozessen und organisatorischen Regelungen
  Es muss regelmäßig überprüft werden, ob Prozesse und organisatorische Regelungen des Sicherheitsmanagements praxistauglich und effizient sind.
  Sobald Prozesse oder Regelungen, die aus Sicherheitsgründen eingerichtet wurden, zu kompliziert oder zeitaufwendig sind, werden sie trotz der Gefahr von Sicherheitsvorfällen häufig nicht beachtet oder bewusst umgangen.
- Managementbewertungen
  Das Management ist über die Ergebnisse der oben genannten Überprüfungen regelmäßig zu informieren. Die Berichte sind nicht nur notwendig, um dringende oder zeitkritische Probleme zu lösen, sondern enthalten wichtige Informationen, die das Management für die Steuerung des Sicherheitsprozesses benötigt.

**Anpassung und Verbesserung der Informationssicherheitsorganisation**

Die IS-Organisation muss regelmäßig in Bezug auf Effizienz und Effektivität optimiert werden. Haben sich Schwächen in den Prozessen oder Regelungen für die IS-Organisation gezeigt, müssen diese abgestellt werden.

**Dokumentation**

Die Aufgaben, Verantwortungen und Kompetenzen im Sicherheitsmanagement müssen nachvollziehbar dokumentiert sein. Dazu gehören auch die wesentlichen Arbeitsanweisungen und organisatorischen Regelungen.

Prüffragen:

- Ist ein IT-Sicherheitsbeauftragter benannt?
- Ist der IT-Sicherheitsbeauftragte ausreichend qualifiziert?
- Stehen dem IT-Sicherheitsbeauftragten (und der IS-Organisation) ausreichend Ressourcen zur Verfügung?
- In größeren Institutionen: Wird der IT-Sicherheitsbeauftragte durch ein Informationssicherheitsmanagement-Team unterstützt?
- Sind die Aufgaben und Kompetenzen innerhalb des Sicherheitsprozesses klar definiert?

# M 2.194 Erstellung einer Übersicht über vorhandene IT-Systeme

Diese Maßnahme ist mit Version 2005 entfallen.

# M 2.195 Erstellung eines Sicherheitskonzepts

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Ein Informationssicherheitskonzept dient der Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss ein Sicherheitskonzept sorgfältig geplant und umgesetzt sowie regelmäßig überprüft werden. Die einzelnen, im Folgenden kurz angerissenen Aspekte werden ausführlich im BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise* behandelt.

Nicht alle Bereiche einer Institution müssen durch ein einziges Sicherheitskonzept abgedeckt werden. Stellt die Umsetzung des IT-Grundschutzes in einem großen Schritt eine unübersichtliche Aufgabe dar, kann es sinnvoll sein, zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen. Von dieser Basis ausgehend sollte sich dann der Sicherheitsprozess auf die Gesamtorganisation ausweiten. Vor allem bei großen Behörden und Unternehmen kann es mehrere Sicherheitskonzepte geben, die verschiedene Organisationsbereiche abdecken. Dann muss jedoch gewährleistet sein, dass alle Bereiche einer Institution durch angemessene Sicherheitskonzepte abgedeckt werden.

Komplexe Geschäftsprozesse oder Anwendungen können in eigenen Sicherheitskonzepten behandelt werden. Dies empfiehlt sich vor allem bei der Einführung neuer Aufgaben oder Anwendungen.

Der festgelegte Geltungsbereich wird im Weiteren als Informationsverbund bezeichnet und stellt detailliert den Bereich dar, für den das Sicherheitskonzept umgesetzt werden soll. Ein Informationsverbund kann sich somit auf Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten beziehen. Er umfasst alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.

Der Informationsverbund muss so festgelegt sein, dass die betrachteten Geschäftsprozesse und Informationen diesem Bereich vollständig zugeordnet werden können. Die Abhängigkeiten aller sicherheitsrelevanten Prozesse sind zu berücksichtigen. Die Schnittstellen zu den anderen Bereichen müssen klar definiert werden, sodass der Informationsverbund im Gesamtunternehmen eine sinnvolle Mindestgröße einnimmt.

Das Sicherheitsmanagement muss eine Methode zur Risikobewertung auswählen, die es ermöglicht, potentielle Schäden durch Sicherheitsvorfälle zu analysieren und zu bewerten. Es können auch mehrere, aufeinander aufbauende Verfahren zur Risikobewertung gewählt werden.

In der Vorgehensweise nach IT-Grundschutz wird implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt.

In bestimmten Fällen, beispielsweise wenn der betrachtete Informationsverbund Komponenten mit hohem oder sehr hohem Schutzbedarf enthält, muss

jedoch eine ergänzende Sicherheitsanalyse und gegebenenfalls eine explizite Risikoanalyse durchgeführt werden. Die hierfür notwendigen Arbeitsschritte sind in den BSI-Standards 100-2 und 100-3 erläutert.

Basis jeder Risikobewertung ist die Beschreibung der zu schützenden Informationen und Geschäftsprozesse. Um einen Überblick über die für die Geschäftsprozesse wichtigen organisatorischen oder technischen Strukturen zu bekommen, ist der Informationsverbund strukturiert zu erfassen. Neben den technischen Komponenten, den Anwendungen und den verarbeitenden Informationen sind auch die räumliche Infrastruktur und die Vernetzung aufzunehmen. Dabei müssen auch die Abhängigkeiten der verschiedenen Komponenten untereinander festgehalten werden.

In der Schutzbedarfsfeststellung sind folgende Schritte enthalten:

- Es wird analysiert, welche Gefährdungen bzw. Risiken für die Institution als Folge unzureichender Informationssicherheit bestehen.
- Mögliche Schäden durch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit werden identifiziert.
- Die potentiellen Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch Sicherheitsvorfälle und andere Sicherheitsrisiken werden analysiert und bewertet.

Anhand dieser Betrachtungen lässt sich das Risiko für das Unternehmen bzw. die Behörde abschätzen und der Schutzbedarf für Informationen, Anwendungen und IT-Systeme festlegen.

Aus den allgemeinen Sicherheitszielen, dem identifizierten Schutzbedarf und der Risikobewertung werden konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet. Hierfür müssen konkrete Bausteine der IT-Grundschutz-Kataloge für die Sicherheitsanforderungen eines Informationsverbundes ausgewählt werden, um so ein spezifisches Paket von Sicherheitsmaßnahmen als Soll-Vorgabe zu erhalten.

Um zu ermitteln, welche der Sicherheitsmaßnahmen bereits umgesetzt und an welchen Stellen noch Lücken sind, wird ein Basis-Sicherheitscheck durchgeführt.

Die Umsetzung der nach IT-Grundschutz vorgeschlagenen Maßnahmen ist in der Regel für typische Geschäftsprozesse, Anwendungen und Komponenten mit normalem Schutzbedarf ausreichend. Jedoch ist eine ergänzende Sicherheitsanalyse erforderlich für Elemente des Informationsverbunds, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen der IT-Grundschutz-Kataloge nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (z. B. in Umgebungen oder mit Anwendungen) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Ziel der ergänzenden Sicherheitsanalyse ist, eine Management-Entscheidung darüber vorzubereiten und herbeizuführen, für welche dieser Elemente eine explizite Risikoanalyse durchzuführen ist.

Auf der Grundlage der Gefährdungslage werden im Rahmen der Risikoanalyse gegebenenfalls Ergänzungen oder Korrekturen am Sicherheitskonzept vorgenommen. Risiken, für deren Minderung keine geeigneten oder wirtschaftlichen Gegenmaßnahmen ergriffen werden können, werden identifiziert und ebenfalls einer systematischen Risikobehandlung zugeführt.

Vor der Fertigstellung eines Sicherheitskonzeptes müssen die in der Risikoanalyse zusätzlich identifizierten Maßnahmen mit den IT-Grundschutz-Maßnahmen konsolidiert werden. Dabei ist für alle neu ermittelten Sicherheitsmaßnahmen zu überprüfen, ob sie die vorhandenen Maßnahmen ersetzen, ergänzen oder in ihrer Wirkung beeinträchtigen. Anschließend müssen die Ergebnisse des Basis-Sicherheitschecks vervollständigt und auf den neuesten Stand gebracht werden.

Ein Sicherheitskonzept ist nur wirksam, wenn die darin vorgesehenen Maßnahmen auch zeitnah in die Praxis umgesetzt werden. Dies muss geplant und kontrolliert werden.

Dafür ist festzuhalten, in welchem Zeitraum die einzelnen Maßnahmen umzusetzen sind und welche passend kombiniert gemeinsam umgesetzt werden können. Außerdem müssen die Maßnahmen nach der Dringlichkeit der Umsetzung priorisiert werden. Die Umsetzungsplanung sollte entweder im Sicherheitskonzept oder in einem beigefügten Realisierungsplan festgehalten werden. Hierin sollten unbedingt Umsetzungsreihenfolge und Verantwortlichkeiten enthalten sein:

- Festlegung von Prioritäten (Umsetzungsreihenfolge): Alle Sicherheitsmaßnahmen sollten nach Wichtigkeit und Effektivität priorisiert werden. Grundsätzlich sollten Maßnahmen gegen besonders schwerwiegende Gefährdungen vorrangig umgesetzt werden. Dies ist besonders wichtig, wenn gegen diese Gefährdungen bisher nur wenig Schutz besteht. Können z. B. aus finanziellen Gründen nicht alle Maßnahmen sofort umgesetzt werden, sollten die Maßnahmen mit der größten Breitenwirkung zuerst umgesetzt werden.
- Bei der Umsetzungsreihenfolge sollten mögliche Zusammenhänge zwischen Maßnahmen berücksichtigt werden.
- Verantwortlichkeiten: Für jede Maßnahme ist festzulegen, wer für deren Initialisierung, Umsetzung und Kontrolle (z. B. Audit) oder Revision verantwortlich ist.

Bei der Auswahl von Sicherheitsmaßnahmen ist ebenfalls deren Angemessenheit und Wirtschaftlichkeit zu beachten. Es muss nachvollziehbar sein, warum die ausgewählten Maßnahmen geeignet sind, die Sicherheitsziele und -anforderungen zu erreichen. Die Dokumentation sollte daher konkrete Angaben über Verantwortlichkeiten und Zuständigkeiten sowie geplante Aktivitäten zur Kontrolle, Revision, Überwachung enthalten.

Die Reihenfolge für die Umsetzung offener Aktivitäten ist festzuhalten. Außerdem sind die geplanten bzw. eingesetzten Ressourcen für die Umsetzung der einzelnen Sicherheitsmaßnahmen zu dokumentieren.

Da Informationssicherheit ein kontinuierlicher Prozess ist, genügt es nicht, die Sicherheitsmaßnahmen einmal umzusetzen. Die Informationssicherheit muss kontinuierlich verbessert werden. Im Rahmen des Sicherheitsprozesses muss daher auf neue technische Entwicklungen reagiert werden. Schwachstellen sowie neu aufgedeckte Sicherheitslücken müssen berücksichtigt werden. Der Sicherheitsprozess ist daher regelmäßig zu überprüfen, zu aktualisieren und alle Änderungen sind zu dokumentieren. Wichtige Verfahren sind dabei die Einführung von regelmäßigen Berichten (siehe M 2.200 *Management-Berichte zur Informationssicherheit*) und Meldeprozesse.

Eine Zertifizierung des Sicherheitsprozesses dokumentiert die Einhaltung einer definierten Vorgehensweise und kann als unabhängiges Review-Verfahren in den Sicherheitsprozess integriert werden.

Das Sicherheitskonzept wird in der Praxis häufig herangezogen, um konkrete Sicherheitsmaßnahmen bezüglich ihrer Umsetzung oder ihrer Aktualität zu überprüfen. Daher sollte es so strukturiert sein, dass

- spezifische Bereiche schnell gefunden werden können, und
- es mit minimalem Aufwand aktualisiert werden kann (hierfür bietet sich die Nutzung eines Tools an).

Außerdem sollten die einzelnen Sicherheitsmaßnahmen ausreichend konkret beschrieben sein, damit im Vertretungsfall ein Dritter sicherheitsspezifische Aufgaben übernehmen kann.

Ein Sicherheitskonzept kann vertrauliche Informationen beinhalten, wie z. B. Angaben über noch nicht beseitigte Schwachstellen oder Informationen zu Maßnahmen, die helfen, diese Maßnahmen zu umgehen oder zu überwinden. Solche vertraulichen Informationen dürfen ausschließlich an die zuständigen Personen weitergegeben werden. Das Sicherheitskonzept sollte daher so gegliedert werden, dass die Bereiche, die einen breiten Adressatenkreis betreffen, von denen getrennt werden, die nur eingeschränkt weitergegeben werden dürfen.

Es ist wichtig, ein gemeinsames Verständnis für Informationssicherheit in einer Institution herzustellen. Dazu gehört auch die Verwendung einheitlicher und klarer Begriffe. Daher sollte frühzeitig ein Glossar mit den wichtigsten Begriffen rund um Informationssicherheit erstellt werden. Dieses Glossar hilft bei der Erstellung aller sicherheitsrelevanten Dokumente. Es kann im Sicherheitskonzept oder auch einzeln veröffentlicht werden.

Prüffragen:

- Wird der festgelegte Geltungsbereich (Informationsverbund) durch ein angemessenes Sicherheitskonzept abgedeckt?
- Gibt es eine strukturierte Beschreibung der betrachteten Informationen und Geschäftsprozesse?
- Ist die Schutzbedarfsfeststellung nachvollziehbar?
- Sind die ermittelten Sicherheitsmaßnahmen angemessen, umsetzbar und effizient?
- Gibt es eine klare Realisierungsplanung der noch umzusetzenden Maßnahmen?
- Ist das Sicherheitskonzept aktuell?
- Ist jeder Mitarbeiter zumindest über die ihn unmittelbar betreffenden Teile des Sicherheitskonzeptes informiert?

# M 2.196 Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan

Diese Maßnahme ist mit Version 2006 entfallen.

# M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und qualitätsbewusstes Handeln mithelfen, Schäden zu vermeiden und zum Erfolg der Institution beizutragen. Zur Integration der Mitarbeiter in den Sicherheitsprozess gehören folgende Aufgaben:

**Motivation und Arbeitsbedingungen**

Die Behörden- oder Unternehmensleitung muss ein positives Arbeitsklima schaffen und das Engagement der Mitarbeiter für die Informationssicherheit fördern. Dazu gehören unter anderem folgende Aspekte:

- Es müssen angemessene und bedienungsfreundliche Sicherheitsprodukte eingesetzt werden.
- Sicherheitskonzepte und -richtlinien müssen realistisch sein.
- Informationssicherheit muss von der Leitungsebene praktiziert werden, um eine hohe Akzeptanz bei den Mitarbeitern zu gewährleisten.

**Schulung und Sensibilisierung**

Eine weitere Aufgabe, die den gesamten Sicherheitsprozess begleiten muss, ist die Organisation und Durchführung von Schulungs- und Sensibilisierungsmaßnahmen. Das Unternehmen oder die Behörde sollte ein Schulungs- und Sensibilisierungskonzept erarbeiten. Eine ausführliche Behandlung dieses Themas ist im Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit* genauer nachzulesen.

**Beteiligung von Mitarbeitern**

Mitarbeiter müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden. Außerdem sollten Mitarbeiter frühzeitig bei der Planung von Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt werden.

**Personelle Sicherheitsmaßnahmen**

Es gibt eine Vielzahl von personellen Sicherheitsaspekten, die bei dem gesamten in einem Unternehmen oder einer Behörde tätigen Personal berücksichtigt werden sollten. Sicherheitsmaßnahmen betreffen nicht nur die eigenen Mitarbeiter, sondern ebenso Externe wie Mitarbeiter von Dienstleistern oder Kooperationspartnern. Beginnend mit der Einstellung von Mitarbeitern, über die Einarbeitung neuer Mitarbeiter bis hin zu deren Weggang ist eine Vielzahl von Maßnahmen notwendig. Die erforderlichen Sicherheitsmaßnahmen sind in Baustein B 1.2 *Personal* beschrieben.

Prüffragen:

- Werden die Mitarbeiter frühzeitig bei der Planung von Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt?
- Werden die Mitarbeiter bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen ausreichend informiert?
- Gibt es Schulungs- und Sensibilisierungskonzepte?

# M 2.198 Sensibilisierung der Mitarbeiter für Informationssicherheit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Viele Sicherheitsvorfälle werden durch unsachgemäßes Verhalten hervorgerufen: Mitarbeiter können Sicherheitslücken durch Unkenntnis, Fehlverhalten oder auch leichtfertige Weitergabe von Informationen verursachen. Daher sollte sichergestellt werden, dass alle Mitarbeiter die für ihren Arbeitsplatz erforderlichen Informationssicherheitskenntnisse haben, Zwischenfälle frühzeitig als solche erkennen können und eigenverantwortlich sinnvolle Maßnahmen bei Sicherheitsproblemen ergreifen können. Eine der wichtigsten Aufgaben des Informationssicherheitsmanagements besteht darin, die Mitarbeiter für das Thema Informationssicherheit zu sensibilisieren.

**Sensibilisierungsinhalte**

Um dies zu erreichen, muss den Mitarbeitern plausibel und nachvollziehbar dargestellt werden, warum und in welchem Maß Informationssicherheit für die Institution, aber auch speziell für ihren Arbeitsplatz wichtig ist. Sie müssen Gefährdungen und Auswirkungen von Sicherheitsvorfällen genauso kennen wie die erforderlichen Maßnahmen und die relevanten Regelungen in den Sicherheitsdokumenten (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*).

Folgende Themen sollten vermittelt werden:

- Grundprinzipien der Informationssicherheit,
- Überblick über zu schützende Informationen, Gefährdungen und Maßnahmen der Sicherheit von Informationen, mit und ohne IT-Einsatz,
- Inhalte der Richtlinien zur Informationssicherheit der Institution,
- Ziel und Inhalt des Sicherheitskonzeptes,
- Aufgaben, Ziele und Werte der Institution: Hierbei umfasst der Begriff Werte sowohl Vermögenswerte (z. B. Informationen, Produktionsanlagen, Mitarbeiter, spezielle Kenntnisse) als auch ideelle Werte (z. B. Philosophie, Verhaltenskodex).

Diese Themen sollten zum besseren Verständnis mit Beispielen untermauert werden und sich möglichst eng auf das Arbeitsumfeld der Mitarbeiter beziehen. Die hier genannten Themen sind lediglich eine Auswahl. Sensibilisierungsmaßnahmen sollten stets den individuellen Gegebenheiten der Institution angepasst sein. Um wirkungsvoll das Bewusstsein für Informationssicherheit zu schärfen und eingeschliffene Verhaltensweisen dauerhaft zu ändern, ist ein fortwährender Lernprozess erforderlich. Sinnvolle kontinuierliche Sensibilisierungsmaßnahmen müssen dabei auf das Arbeitsumfeld und die Zielgruppe abgestimmt sein.

**Materialien zur Informationssicherheit**

Um Mitarbeiter für Informationssicherheit zu sensibilisieren, müssen sie immer wieder auf verschiedenen Wegen und Plattformen angesprochen werden. Dazu kann auf Plattformen zurückgegriffen werden, die bereits in der Institution vorhanden sind, aber auch neu gestaltete genutzt werden. Zur Sensibilisierung können auch attraktive Werbematerialien bzw. -aktionen beitragen. Hierzu gehören zielgerichtete Mitteilungen und Slogans zur Informationssicherheit. Damit sie lange im Blickfeld der Mitarbeiter verbleiben, können kurze Informationssicherheitshinweise beispielsweise auf Kalendern oder Kaffee-

tassen untergebracht werden. Über Plakate können Verantwortliche ebenfalls Botschaften effektiv vermitteln. Diese sollten sie an auffälligen Stellen aufhängen, z. B. in der Kantine, im Aufzug und in Besprechungsräumen, und regelmäßig auswechseln. Poster zu Informationssicherheitsthemen gibt es beispielsweise von diversen Herstellern von Sicherheitsprodukten und Werbemittelherstellern. Merksprüche zur Informationssicherheit sollten einfach und einprägsam sein und können je nach Organisationskultur auch unterhaltend sein, beispielsweise "Die Sicherung ist null und nichtig, nimmt man das Passwort nicht so wichtig!" oder "Verzichte auf den Mailversand, ist der Inhalt sehr brisant!"

Für die Vermittlung von Themen rund um die Informationssicherheit bieten sich z. B. folgende Medien an:

- Flyer und Newsticker mit den wichtigsten Informationen und Grundsatzaussagen der Institutionsleitung zur Informationssicherheit
- Informationsbroschüren für ausgewählte Situationen, wie z. B. Arbeitsplatz, Besprechungsräume, Verhaltenstipps für Geschäftsreisen
- Plakate und Bildschirmschoner
- Tassen, Mousepads oder ähnliche Gegenstände mit Hinweisen zur Informationssicherheit
- E-Mails vom Sicherheitsmanagement-Team, um über aktuelle Vorfälle zu informieren und immer wieder Sicherheitsregeln ins Gedächtnis zu rufen
- Videoclips zu ausgewählten Sensibilisierungsthemen, wie z. B. Umgang mit organisationsfremden Personen ohne Besucherausweis
- Kurzvorträge zur Informationssicherheit auf internen Veranstaltungen, wie Abteilungstreffen oder bestehenden Schulungsmaßnahmen
- Publikation von Artikeln in Mitarbeiterzeitschriften zu aktuellen Gefährdungssituationen, zu sicherheitsrelevanten Vorfällen (wenn kein Nachahmungsrisiko besteht), zur Vorstellung von Sicherheitsmaßnahmen, etc.

Darüber hinaus bieten sich auch interaktive Formen der Sensibilisierung wie Workshops und Rollenspiele (siehe M 3.47 *Durchführung von Planspielen zur Informationssicherheit*) an. Bei der Sensibilisierung der Mitarbeiter sollte berücksichtigt werden, welche Medien und Formen der Kommunikation für die Institution geeignet sind und als akzeptable Kanäle angesehen werden.

Umsetzung der Sensibilisierungsmaßnahmen

Sensibilisierungsmaßnahmen zur Informationssicherheit können auch durch Schulungsprogramme unterstützt werden. Sie sind daher im Sensibilisierungskonzept zu berücksichtigen. Detaillierte Informationen zu den Schulungen sind in M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit* beschrieben.

Damit alle Mitarbeiter ein Bewusstsein für Informationssicherheit entwickeln, ist ein langfristiger Lern- und Entwicklungsprozess zu etablieren. Eine weitere Vertiefung der Themen rund um Informationssicherheit muss aufgebaut und auf einem aktuellen Stand gehalten werden sowie dauerhaft präsent sein. Inhalte und Medien sollten so aufeinander abgestimmt sein, dass sie die Mitarbeiter mit der Informationssicherheit vertraut machen und ihnen die erforderlichen Hintergründe und individuellen Voraussetzungen geben.

Nachfolgend werden vier Bereiche (Sensibilisierung, Schulung, Verstärkung und Öffentlichkeitsarbeit) einer Sensibilisierungskampagne beschrieben. Diese Bereiche hängen bei der Ausgestaltung in sinnvoller Weise voneinander ab, müssen aber nicht zwingend in einer strengen zeitlichen Reihenfolge durchgeführt werden.

**Sensibilisierung**

Im Bereich Sensibilisierung sollen den Mitarbeitern Hintergrundinformationen gegeben werden, um zu verstehen, warum sich die Institution für bestimmte Sicherheitsvorgaben entschieden hat, welche aktuellen Gefährdungen vorliegen, wie sich diese auf die Institution auswirken und was dies für die Mitarbeiter bedeuten würde. Durch diese Hintergrundinformationen sollen die Mitarbeiter sowohl für das Thema als auch für die Schulungen sensibilisiert werden.

Medienbeispiele für Hintergrundinformation: Infoveranstaltungen, Flyer, Broschüren, Plakate, Bildschirmschoner, Mousepads, Videos, etc.

**Schulung**

Der Bereich Schulung unterstützt den Mitarbeiter dabei, sich entsprechend den Vorgaben aus dem Sicherheitskonzept zu verhalten und so Gefahren für die Informationssicherheit abzuwenden. Der jeweilige zielgruppenspezifische Schulungsbedarf leitet sich dabei aus dem Sicherheitskonzept und einer darauf folgenden Zielgruppenanalyse ab (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*).

Medienbeispiele Schulung: Präsenzschulungen, Ergänzung bestehender Schulungen, Webkurse, Infotainment, Videos, etc.

**Verstärkung**

Im Bereich Verstärkung soll dafür gesorgt werden, dass die Lernkurve nach durchgeführten Schulungen möglichst lange auf einem hohen Niveau gehalten wird und dass die Mitarbeiter das Thema Informationssicherheit dauerhaft wahrnehmen (siehe M 3.95 *Lernstoffsicherung*).

Medienbeispiele Verstärkung: Newsletter, Foren, Gewinnspiele, Auffrischungsschulungen, etc.

**Öffentlichkeitsarbeit**

Durch Öffentlichkeitsarbeit kann der Reifegrad des Sensibilisierungsprozesses nach innen und außen dargestellt werden. Beiträge für z. B. Kongresse, Fachmedien oder Arbeitskreise über die durchgeführten Sensibilisierungsmaßnahmen können der Institution und den Mitarbeitern zu einem positiven Sicherheitsimage verhelfen und einen wertvollen Beitrag zur Sensibilisierung leisten.

Medienbeispiele Öffentlichkeitsarbeit: Mitarbeiterzeitungen, Fachzeitschriften, Pressemitteilungen, Kongressbeiträge, Arbeitskreise, etc.

Prüffragen:

- Ist sichergestellt, dass die Mitarbeiter kontinuierlich und ausreichend für Informationssicherheit sensibilisert und geschult werden?

# M 2.199 Aufrechterhaltung der Informationssicherheit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Im Sicherheitsprozess geht es nicht nur darum, das angestrebte Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um das bestehende Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, sollten alle Sicherheitsmaßnahmen regelmäßig überprüft werden.

Sowohl die korrekte Umsetzung als auch die Umsetzbarkeit eines Sicherheitskonzepts müssen regelmäßig überprüft werden. Dabei ist zu unterscheiden zwischen der Prüfung, ob bestimmte Maßnahmen geeignet und effizient sind, um die gesteckten Sicherheitsziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), und der Kontrolle, inwieweit Sicherheitsmaßnahmen in den einzelnen Bereichen umgesetzt wurden (Revision der Informationssicherheit).

Die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen müssen gemäß des Realisierungsplans umgesetzt werden. Der Umsetzungsstatus muss dokumentiert werden. Zieltermine und Ressourceneinsatz müssen überwacht und gesteuert werden. Die Leitungsebene ist dazu regelmäßig zu informieren.

Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens jährlich) durchgeführt werden und können auch zwischendurch erfolgen. Insbesondere Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden Sicherheitsmaßnahmen. Die in den einzelnen Überprüfungen ermittelten Ergebnisse sollten dokumentiert werden. Es muss zudem festgelegt sein, wie mit den Überprüfungsergebnissen zu verfahren ist, da die Informationssicherheit nur dann wirksam aufrechterhalten werden kann, wenn aufgrund der Überprüfungsergebnisse auch die erforderlichen Korrekturmaßnahmen ergriffen werden.

Es sollten auch gelegentlich unangekündigte Überprüfungen durchgeführt werden, da angekündigte Kontrollen häufig ein verzerrtes Bild des Untersuchungsgegenstands ergeben.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass die Kontrollen nicht den Charakter von Schulmeisterei haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Es sollte in der Behörde bzw. im Unternehmen festgelegt werden, wie die Tätigkeiten im Zusammenhang mit diesen Überprüfungen zu koordinieren sind. Dazu ist zu regeln, welche Sicherheitsmaßnahmen wann und von wem zu überprüfen sind, auch damit Doppelarbeit vermieden wird und keine Bereiche innerhalb einer Institution ungeprüft verbleiben.

Die vorhandenen Sicherheitsmaßnahmen sollten mindestens einmal im Jahr überprüft werden. Darüber hinaus sind sie immer dann zu prüfen, wenn

- neue Geschäftsprozesse, Anwendungen oder IT-Komponenten aufgebaut werden,

- größere Änderungen der Infrastruktur vorgenommen werden (z. B. Umzug),
- größere organisatorischen Änderungen anstehen (z. B. Outsourcing),
- die Gefährdungslage sich wesentlich ändert,
- wenn gravierende Schwachstellen oder Schadensfälle bekannt werden.

**Einhaltung des Sicherheitskonzeptes (Sicherheitsrevision)**

Hierbei muss geprüft werden, ob Sicherheitsmaßnahmen tatsächlich so umgesetzt sind und eingehalten werden wie im Sicherheitskonzept vorgegeben. Hierbei ist auch zu untersuchen, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob alle vorgesehenen Detektionsmaßnahmen (z. B. Auswertung von Protokolldateien) tatsächlich durchgeführt werden.

Dabei kann sich zeigen, dass Sicherheitsmaßnahmen nicht umgesetzt worden sind oder dass sie in der Praxis nicht greifen. In beiden Fällen sollten die Ursachen für die Abweichungen ermittelt werden. Als mögliche Korrekturmaßnahmen kommen - je nach Ursache - in Frage:

- organisatorische Maßnahmen sind anzupassen,
- personelle Maßnahmen, z. B. Schulungs- und Sensibilisierungsmaßnahmen, sind zu ergreifen oder disziplinarische Maßnahmen einzuleiten,
- infrastrukturelle Maßnahmen, z. B. bauliche Veränderungen, sind zu initiieren,
- technische Maßnahmen, z. B. Änderungen an Hardware und Software oder Kommunikationsverbindungen und Netzen, sind vorzunehmen,
- Entscheidungen des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene) sind einzuholen.

Auf jeden Fall sollte für jede Abweichung eine Korrekturmaßnahme vorgeschlagen werden. Außerdem sollten auch hier der Zeitpunkt und die Zuständigkeiten für die Umsetzung der Korrekturmaßnahme festgelegt werden.

Kontrollen sollen helfen, Fehlerquellen abzustellen. Es ist für die Akzeptanz von Kontrollen extrem wichtig, dass dabei keine Personen bloßgestellt werden oder als "Schuldige" identifiziert werden. Wenn die Mitarbeiter dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen.

Im Vorfeld sollten aber auch die Reaktionen auf Verletzung der Sicherheitsvorgaben festgelegt werden. Es müssen angemessene Maßnahmen ergriffen werden, die dazu beitragen, dass sich Sicherheitsvorfälle nicht wiederholen. Dazu könnte beispielsweise die Einschränkung von Zugriffsrechten gehören.

Falls unzulässige Aktivitäten von Mitarbeitern entdeckt werden, sollte der jeweilige Vorgesetzte informiert werden, damit angemessene Konsequenzen angestoßen werden können.

**Kontinuierliche Verbesserung des Sicherheitskonzeptes (Vollständigkeits- bzw. Aktualisierungsprüfung)**

Das Sicherheitskonzept muss regelmäßig aktualisiert, verbessert und an neue Rahmenbedingungen angepasst werden. Es muss regelmäßig geprüft werden, ob die ausgewählten Sicherheitsmaßnahmen noch geeignet sind, die Sicherheitsziele zu erreichen. Dabei kann direkt untersucht werden, ob die eingesetzten Sicherheitsmaßnahmen effizient sind oder ob die Sicherheitsziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten.

Deshalb ist es wichtig, externe Wissensquellen, wie Standards oder Fachpublikationen, im Hinblick auf neue technische und regulatorische Entwicklungen auszuwerten. Auch Kontakte zu Gremien und Interessengruppen, die sich mit Sicherheitsaspekten beschäftigen, helfen dem IS-Management-Team, das vorhandene Wissen über sicherheitsrelevante Methoden und Lösungen zu erweitern und zu aktualisieren. Außerdem werden dabei auch wertvolle Kontakte zu anderen IT-Sicherheitsbeauftragten geknüpft, um Lösungen anderer Institutionen kennenzulernen und Praxiserfahrungen auszutauschen. Es entstehen dadurch auch Wege, über die frühzeitig Warnungen über aufkommende Sicherheitsprobleme ausgetauscht werden können. Das IS-Management-Team sollte einen Überblick über thematisch passende Gremien und Interessengruppen haben und festlegen, wo sich aktive Mitarbeit anbietet und wo nur die Ergebnisse regelmäßig beobachtet und ausgewertet werden sollten.

**Durchführung der Prüfungen**

Entsprechend dem Prüfungszweck sind Umfang und Tiefe der Überprüfungen festzulegen. Als Grundlage für alle Überprüfungen dient das Sicherheitskonzept und die vorhandene Dokumentation des Sicherheitsprozesses.

Eine Überprüfung muss von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen jedoch nicht an der Erstellung der Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Auditoren müssen möglichst unabhängig und neutral sein.

Jede Überprüfung ist sorgfältig zu planen. Alle relevanten Feststellungen und Ergebnisse sind in einem Bericht festzuhalten. Dieser sollte neben einer Auswertung auch Korrekturvorschläge enthalten. Der Bericht sollte dem Leiter des überprüften Bereiches sowie dem IS-Management-Team übergeben werden, die auf dieser Basis die weiteren Schritte konzipieren müssen. Schwerwiegende Probleme sollten direkt der Leitungsebene kommuniziert werden, damit weitreichende Entscheidungen zeitnah getroffen werden können.

Werden bei der Prüfung spezielle Audit- oder Diagnosewerkzeuge eingesetzt, muss ebenso wie bei der Ergebnisdokumentation sichergestellt sein, dass nur autorisierte Personen darauf Zugriff haben. Diagnose- und Prüftools sowie die Prüfergebnisse müssen daher besonders geschützt werden.

Wenn Externe an Prüfungen beteiligt sind, muss sichergestellt werden, dass keine Informationen der Institution missbräuchlich verwenden (z. B. durch entsprechende Vertraulichkeitsvereinbarungen) und dass sie nur auf die benötigten Informationen zugreifen können (z. B. durch Zugriffsrechte oder Vier-Augen-Kontrolle). Sollten sie Prüftools einsetzen, muss deren Nutzung genau geregelt werden.

**Korrekturmaßnahmen**

Erkannte Fehler und Schwachstellen müssen zeitnah abgestellt werden. Der identifizierte Optimierungsbedarf bei Effizienz und Effektivität von Sicherheitsmaßnahmen muss umgesetzt werden.

Aufgrund der Überprüfungsergebnisse sind Entscheidungen über das weitere Vorgehen zu treffen. Insbesondere sind alle erforderlichen Korrekturmaßnahmen in einem Umsetzungsplan festzuhalten. Die Verantwortlichen für die Umsetzung der Korrekturmaßnahmen sind zu benennen und mit den notwendigen Ressourcen auszustatten.

Prüffragen:

- Werden regelmäßig Vollständigkeits- bzw. Aktualisierungsprüfungen des Sicherheitskonzeptes durchgeführt?
- Werden regelmäßig Sicherheitsrevisionen durchgeführt?
- Ist geregelt, welche Sicherheitsmaßnahmen wann und von wem zu überprüfen sind?
- Werden die Prüfungen von qualifizierten und unabhängigen Personen durchgeführt?
- Sind die ermittelten Ergebnisse der Überprüfungen nachvollziehbar dokumentiert?

# M 2.200 Management-Berichte zur Informationssicherheit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es, die Behörden- oder Unternehmensleitung bei der Wahrnehmung ihrer Gesamtverantwortung für die Informationssicherheit zu unterstützen. Eine wichtige Grundlage für die zu treffenden Entscheidungen sind übersichtlich und aussagekräftig aufbereitete Informationen zur aktuellen Lage der Informationssicherheit in der Institution.

Um den Sicherheitsprozess zu steuern und aufrecht zu erhalten, muss regelmäßig seine Wirksamkeit und Effizienz überprüft werden und diese Ergebnisse auf Leitungsebene bewertet werden. Ziel hierbei ist, das weitere Vorgehen im Sicherheitsprozess mit der Leitungsebene abzustimmen. Daher sind alle erforderlichen Änderungen am Sicherheitsprozess, beispielsweise in den Sicherheitszielen oder der Sicherheitsleitlinie, aufzuzeigen. Die Ergebnisse müssen dokumentiert und die bisherigen Aufzeichnungen gepflegt werden.

**Regelmäßige Management-Berichte**

Damit die Unternehmens- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Informationssicherheitsprozesses treffen kann, benötigt sie Eckpunkte über den Stand der Informationssicherheit. Diese Eckpunkte sollten in Management-Berichten aufbereitet werden, die unter anderem folgende Punkte abdecken:

- Ergebnisse von Audits und Datenschutzkontrollen
- Berichte über Sicherheitsvorfälle
- Berichte über bisherige Erfolge und Probleme beim Informationssicherheitsprozess

Die Leitungsebene muss vom IS-Management-Team regelmäßig in angemessener Form über die Ergebnisse der Überprüfungen und den Status des IS-Prozesses informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden.

Ein Management-Bericht sollte kurz und übersichtlich sein. Die folgenden Punkte können dabei, je nach aktueller Situation, relevant sein. Allerdings sollten nicht alle gleichzeitig in einem Management-Bericht zur Informationssicherheit betrachtet werden, um diesen nicht zu überfrachten. Es ist also zu überlegen, aufzeigen

- inwieweit die Vorgaben des Sicherheitskonzepts im Unternehmen oder in der Behörde bereits abgedeckt sind,
- an welchen Stellen noch Lücken - und damit Restrisiken - bestehen,
- welche Sicherheitsvorfälle aufgetreten sind, welche Schäden entstanden sind und welche Schäden verhindert werden konnten,
- welche Ergebnisse interne Überprüfungen und Audits erbracht haben (siehe M 2.199 *Aufrechterhaltung der Informationssicherheit*),
- inwieweit das Sicherheitsniveau den Sicherheitsanforderungen und der Bedrohungslage der Institution genügt,
- ob sich Rahmenbedingungen geändert haben, so dass weitere Maßnahmen erforderlich sind,

- ob die Aktivitäten im Rahmen der Informationssicherheit Erfolg hatten,
- ob sich die Sicherheitsmaßnahmen zur Erreichung der Sicherheitsziele als geeignet erwiesen haben oder ob Maßnahmen geändert oder ergänzt werden müssen,
- welche Rückmeldungen es von Kunden, Geschäftspartnern, Mitarbeitern oder der Öffentlichkeit zu Sicherheitsaspekten gab,
- welche Ressourcen für Informationssicherheit aufgewendet wurden,
- ob und wie die bisherigen Management-Entscheidungen umgesetzt wurden und ob die Aktivitäten im Rahmen der Informationssicherheit Erfolg hatten.

Daneben sollte sowohl ein Ausblick auf die zu erwartende Weiterentwicklung der organisationsweiten Informationssicherheit gegeben werden, als auch auf technische Entwicklungen und Verfahrensweisen, die eventuell zur Verbesserung des Sicherheitsprozesses beitragen könnten.

**Anlassbezogene Management-Berichte**

Neben den regelmäßigen Management-Berichten kann es notwendig sein, bei überraschend auftretenden Sicherheitsproblemen oder aufgrund von Risiken, die aus neuen technischen Entwicklungen resultieren, anlassbezogene Management-Berichte zu erstellen. Dies ist vor allem dann der Fall, wenn diese Probleme nicht auf Arbeitsebene gelöst werden können, weil z. B. materielle Ressourcen außerhalb des bewilligten Rahmens benötigt werden oder weitergehende personelle Regelungen getroffen werden müssen.

Immer wieder erregen Sicherheitsvorfälle wie globale Computer-Virenattacken die Aufmerksamkeit der Massenmedien. Es hat sich als sinnvoll erwiesen, auch in diesen Fällen Management-Berichte zu erstellen, um aufzuzeigen, inwieweit die eigene Institution von diesen Sicherheitsvorfällen betroffen wurde. Auch wenn sich die Sicherheitslage ändert (z. B. durch neue Bedrohungen, neue Technologien, neue Gesetze) kann ein anlassbezogener Management-Bericht sinnvoll sein.

Bei der Abfassung der Management-Berichte sollte berücksichtigt werden, dass sich der Leserkreis in der Regel nicht aus technischen Experten zusammensetzt. Entsprechend sollte sich der Text durch größtmögliche Verständlichkeit und Knappheit auszeichnen, indem gezielt die wesentlichen Punkte, wie beispielsweise bestehende Schwachstellen, aber auch erreichte Erfolge, herausgearbeitet werden.

Am Schluss jedes Management-Berichts, vor allem bei anlassbezogenen Berichten, sollten immer klar priorisierte und mit realistischen Abschätzungen des zu erwartenden Umsetzungsaufwands versehene Maßnahmenvorschläge stehen. Damit wird sichergestellt, dass eine notwendige Entscheidung der Leitungsebene ohne unnötige Verzögerungen herbeigeführt werden kann.

Der Management-Bericht zur Informationssicherheit sollte der Leitungsebene durch ein Mitglied des IS-Management-Teams persönlich präsentiert werden. So können wesentliche Schwerpunkte wie beispielsweise bestehende oder drohende Sicherheitsmängel betont werden. Das Mitglied des IS-Management-Teams steht auch direkt für Rückfragen und weitergehende Erläuterungen zur Verfügung, was erfahrungsgemäß zu einer Beschleunigung des Entscheidungsvorgangs führt.

Darüber hinaus ist der persönliche Kontakt auch wichtig, um Leitungsentscheidungen besser vorbereiten und Probleme schon im Voraus entschärfen zu können. Hilfreich wäre es auch, wenn ein Mitglied der Leitungsebene mit entsprechendem fachlichem Hintergrund und Interesse als Ansprechpartner zur

Verfügung steht. Der persönliche Kontakt bietet die Möglichkeit, einen "kleinen Dienstweg" zu etablieren, dessen Existenz sich in dringenden Notfällen als vorteilhaft erweisen kann.

**Management-Entscheidungen**

Das Management entscheidet auf Grundlage des Management-Berichts über die weitere Vorgehensweise im Sicherheitsprozess. Dabei wird die Behörden- oder Unternehmensleitung bei Bedarf vom IT-Sicherheitsbeauftragten unterstützt. Alle Entscheidungen müssen dokumentiert werden. Dazu gehören insbesondere folgenden Punkte:

- Erforderliche Aktionen zur Verbesserungen der Effektivität des Sicherheitskonzepts sowie die dafür benötigten Ressourcen
- Höhe des Schutzbedarfs sowie die Behandlung von Restrisiken, die bei einer an eine ergänzende Sicherheitsanalyse angeschlossene Risikoanalyse identifiziert wurden
- Veränderungen von sicherheitsrelevanten Prozessen, um internen oder externen Ereignissen zu begegnen, die Einfluss auf das Sicherheitskonzept haben könnten, z. B. in Hinsicht auf Änderungen bei
    - Geschäftszielen
    - Sicherheitsanforderungen
    - Geschäftsprozessen
    - externen Rahmenbedingungen (wie dem gesetzlichen Umfeld oder vertraglichen Verpflichtungen)

Zur kontinuierlichen Verfolgung des Sicherheitsprozesses sollten sämtliche Management-Berichte und Management-Entscheidungen zur Informationssicherheit in geordneter Weise archiviert werden. Diese Dokumentation sollte den Verantwortlichen bei Bedarf kurzfristig zugänglich sein (siehe M 2.201 *Dokumentation des Sicherheitsprozesses*).

Da die Management-Berichte zur Informationssicherheit im Allgemeinen sensitive Informationen über bestehende Sicherheitslücken und Restrisiken enthalten, ist deren Vertraulichkeit zu schützen. Es müssen angemessene Schutzvorkehrungen getroffen werden, damit keine unbefugten Personen Kenntnis über den Inhalt der Management-Berichte erlangen.

Prüffragen:

- Enthalten die Management-Berichte die wesentlichen relevanten Informationen über den Sicherheitsprozess?
- Sind die Management-Entscheidungen über erforderliche Aktionen, Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen dokumentiert?
- Werden die Management-Berichte aussagekräftig bewertet und unterschrieben?
- Werden die Management-Berichte und Management-Entscheidungen archiviert?

# M 2.201 Dokumentation des Sicherheitsprozesses

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Der Ablauf des Sicherheitsprozesses, wichtige Entscheidungen und die Arbeitsergebnisse der einzelnen Phasen sollten dokumentiert werden. Eine solche Dokumentation ist eine wesentliche Grundlage für die Aufrechterhaltung der Informationssicherheit und damit entscheidende Voraussetzung für die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist, dass nicht nur die jeweils aktuelle Version kurzfristig zugänglich ist, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird. Erst durch die kontinuierliche Dokumentation können die Entwicklungen und Entscheidungen im Bereich Informationssicherheit nachvollziehbar zurückverfolgt werden.

Neben Dokumenten zum Sicherheitsmanagement und dem Sicherheitsprozess gibt es weitere für das Sicherheitsmanagement relevante Dokumente. Abhängig vom Gegenstand und vom Verwendungszweck sind folgende Arten von Dokumentationen zu betrachten:

**Berichte an die Leitungsebene**

Damit die oberste Leitungsebene einer Behörde oder eines Unternehmens die richtigen Entscheidungen treffen kann, um Informationssicherheit auf einem angemessenen Niveau zu gewährleisten, benötigt sie die dafür notwendigen Informationen. Hierfür sollte der IT-Sicherheitsbeauftragte bzw. das IS-Management-Team regelmäßig sowie anlassbezogen Management-Berichte zum Status der Informationssicherheit (siehe auch M 2.200 *Management-Berichte zur Informationssicherheit*) erstellen.

**Dokumente zum Sicherheitsprozess**

Folgende Arten von Dokumentationen zum Sicherheitsprozess sollten erstellt werden:

- Die oberste Leitungsebene muss die Leitlinie zur Informationssicherheit der Behörde bzw. des Unternehmens festlegen und veröffentlichen. Diese enthält unter anderem die Sicherheitsziele und die Sicherheitsstrategie.
- Im Sicherheitskonzept werden die erforderlichen Sicherheitsmaßnahmen beschrieben und deren Umsetzung festgelegt.
- Auf der Sicherheitsleitlinie aufbauend gibt es bereichs- und systemspezifische Sicherheitsrichtlinien und Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz.
- Die wesentlichen Arbeiten des IS-Management-Teams sollten ebenfalls dokumentiert sein, dazu gehören z. B. Sitzungsprotokolle und Beschlüsse.
- Ergebnisse von Audits und Überprüfungen (z. B. Prüflisten und Befragungsprotokolle).

**Dokumentation von Arbeitsabläufen**

Arbeitsabläufe, organisatorische Vorgaben und technische Sicherheitsmaßnahmen müssen so dokumentiert werden, dass Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden.

Es muss bei Störungen oder Sicherheitsvorfällen möglich sein, den gewünschten Soll-Zustand der Geschäftsprozesse und der IT wiederherzustellen. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.

**Dokumentation von Sicherheitsvorfällen**

Sicherheitsrelevante Vorfälle müssen so aufbereitet werden, dass alle damit verbundenen Vorgänge und Entscheidungen nachvollziehbar sind. Ebenso soll es die Dokumentation ermöglichen, Verbesserungen an den Notfallstrategien vorzunehmen und bekannte Fehler zu vermeiden. Zur Bearbeitung von Sicherheitsvorfällen sind außerdem technische Unterlagen, wie Protokolle oder für den Vorfall besonders relevante System-Meldungen, zu speichern und zu archivieren. Die Regelungen des Datenschutzes müssen eingehalten werden.

**Technische Dokumentation**

Zu dieser Art von sicherheitsrelevanten Dokumentationen gehören:

- Installations- und Konfigurationsanleitungen,
- Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall,
- Dokumentation von Test- und Freigabeverfahren und
- Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen.

**Anleitungen für Mitarbeiter**

Sicherheitsmaßnahmen müssen für die Mitarbeiter verständlich dokumentiert werden. Den Mitarbeitern müssen also

- die geltenden Sicherheitsrichtlinien,
- übersichtliche Merkblätter für den verantwortungsvollen Umgang mit internen Informationen, für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheitsvorfällen,
- Handbücher und Anleitungen für die eingesetzten IT-Systeme und Anwendungen

zur Verfügung stehen.

Es kann in seltenen Fällen vorkommen, dass ein Verstoß gegen eine Sicherheitsrichtlinie sinnvoll und notwendig ist. Ein solcher Verstoß muss aber auf jeden Fall zuvor durch eine autorisierte Stelle genehmigt werden. Ausnahmegenehmigungen dürfen nur nach gründlicher Prüfung und in den seltensten Fällen erteilt werden. Anschließend muss eine schriftliche Begründung verfasst werden, die vom Verantwortlichen zu unterzeichnen ist.

**Informationsfluss und Meldewege**

Wichtig für die Aufrechterhaltung des Sicherheitsprozesses ist die Beschreibung und zeitnahe Aktualisierung der Meldewege und der Vorgehensweise für den Informationsfluss.

**Dokumentationswesen**

Es ist Aufgabe des IT-Sicherheitsbeauftragten bzw. des IS-Management-Teams, stets aktuelle und aussagekräftige Dokumentationen zur Informationssicherheit vorzuhalten. Für alle Dokumentationen im Rahmen des Si-

cherheitsprozesses sollte es daher eine geregelte Vorgehensweise geben. Dazu gehören z. B. folgende Punkte:

- Dokumentationen müssen verständlich sein. Das bedeutet auch, dass sie zielgruppengerecht gestaltet werden müssen. Berichte an die Leitungsebene haben andere Anforderungen als technische Dokumentationen für Administratoren.
- Dokumentationen müssen aktuell sein. Es muss festgelegt werden, wer sie pflegt. Sie müssen so bezeichnet und abgelegt werden, dass sie im Bedarfsfall schnell gefunden werden können. Es müssen Angaben zu Erstellungsdatum, Version, Quellen und Autoren vorhanden sein. Veraltete Unterlagen müssen sofort aus dem Umlauf genommen und archiviert werden.
- Es sollte ein definiertes Verfahren existieren, um Änderungsvorschläge (inklusive der Erstellung neuer Dokumente) einzubringen, zu beurteilen und gegebenenfalls zu berücksichtigen.
- Neben der schnellen Informationsweitergabe an Berechtigte ist andererseits die Vertraulichkeit von organisationsinternen Details sicherzustellen. Vertrauliche Inhalte müssen als solche klassifiziert werden und die Dokumente sicher verwahrt und bearbeitet werden (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Bei der Pflege der Vielzahl sicherheitsrelevanter Dokumente kann ein Dokumentenmanagement hilfreich sein (siehe auch M 2.259 *Einführung eines übergeordneten Dokumentenmanagements*).

Dokumentationen müssen nicht immer in Papierform vorliegen. Das Dokumentationsmedium kann je nach Bedarf gewählt werden. Zur Dokumentation können Übersichtsdiagramme (z. B. Netzplan), kurze Sitzungsprotokolle (z. B. jährliche Sitzung der Geschäftsführung zur Diskussion der Sicherheitsstrategie), handschriftliche Notizen oder Software-Tools (z. B. zur Dokumentation des Sicherheitskonzepts) genutzt werden.

Prüffragen:

- Sind für alle Phasen des Sicherheitsprozesses ausreichende Dokumentationen vorhanden?
- Gibt es eine geregelte Vorgehensweise für die Erstellung und Archivierung von Dokumentationen im Rahmen des Sicherheitsprozesses?
- Existieren Regelungen, um die Vertraulichkeit der Dokumentationen zu wahren?
- Sind die vorhandenen Dokumente auf dem neuesten Stand?

# M 2.202 Erstellung eines Handbuchs zur IT-Sicherheit

Diese Maßnahme ist mit Version 2006 entfallen.

# M 2.203 Aufbau einer Informationsbörse zur IT-Sicherheit

Diese Maßnahme ist mit Version 2005 entfallen.

# M 2.204 Verhinderung ungesicherter Netzzugänge

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Revisor

Jeder ungesicherte Zugang zu einem Netz stellt eine enorme Sicherheitslücke dar. Daher muss jede Kommunikation in das interne Netz ausnahmslos über einen gesicherten Zugang geführt werden. Dies kann beispielsweise eine Firewall sein (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Es müssen Regelungen getroffen werden, dass keine weiteren externen Verbindungen unter Umgehung der Firewall geschaffen werden dürfen. Alle Benutzer müssen darauf hingewiesen werden, welche Gefahren mit der Schaffung "wilder" Zugänge, z. B. über mitgebrachte Modems, verbunden sind.

Sämtliche externen Netzzugänge sollten zentral erfasst werden (siehe Baustein B 4.1 *Lokale Netze*). Weiterhin sollte durch Stichproben überprüft werden, ob über Modems oder anderweitig zusätzliche Netzzugänge geschaffen wurden. Dafür können z. B. automatisiert vorgegebene Rufnummerbereiche getestet werden, ob sich dort Datenübertragungseinrichtungen melden.

Die Datenübertragung sollte in allen Institutionen klar geregelt sein. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen. Dies betrifft z. B. nicht nur Router, Modems oder UMTS-Karten, sondern auch Infrarot- oder Funk-Schnittstellen. Insbesondere sollten die folgenden Punkte festgelegt sein:

- Festlegung des Benutzerkreises und der Nutzungsberechtigungen
- Vorgaben und Sicherheitsmaßnahmen für die Benutzung
- Sichere Konfiguration der Datenübertragungseinrichtungen
- Zuständigkeiten für Installation, Wartung und Betreuung
- Festlegung der möglichen Kommunikationspartner
- Nutzungszeiten
- Protokollierung

Beispiele hierfür finden sich in M 2.61 *Regelung des Modem-Einsatzes* oder M 2.179 *Regelungen für den Faxserver-Einsatz*.

Prüffragen:

- Wird die Einhaltung der Regelungen für Netzzugänge und Netzanbindungen regelmäßig überprüft?

# M 2.205 Übertragung und Abruf personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Leiter IT

Erfolgt eine Übertragung personenbezogener Daten vom Standort des Arbeit- bzw. Auftraggebers zu einem "entfernten" Arbeitsplatz (z. B. eines Telearbeiters), so müssen die datenschutzrechtlichen Bestimmungen Beachtung finden. Gemäß § 9 BDSG muss in solchen Fällen insbesondere verhindert werden, dass Unbefugte mit Hilfe von Einrichtungen zur Datenübertragung IT-Systeme nutzen (Benutzerkontrolle). Weiterhin ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle).

Der Transportweg bzw. die Übertragungsmethode sollte so gewählt sein, dass sowohl die Vertraulichkeit und Integrität als auch die Authentizität (Herkunftsnachweis) der personenbezogenen Daten gewährleistet werden kann.

Erfolgt die Übertragung personenbezogener Daten im Rahmen eines automatisierten Abrufverfahrens, sind die besonderen Zulässigkeitsvoraussetzungen in den einschlägigen Gesetzen zu beachten:

**Allgemeine Aspekte**

- Anlass und Zweck sowie beteiligte Stellen am Abrufverfahren sind festzulegen.
- Abrufberechtigungen sind festzulegen und zu kontrollieren.
- Art und Umfang der bereitgehaltenen Daten sind festzulegen.
- Sperr- und Löschfristen für Daten sind zu definieren.
- Es ist festzulegen, in welchen Fällen die speichernde Stelle von der abrufenden Stelle zu informieren ist.
- Der Transportweg ist festzulegen, z. B. Zugriff über ISDN-Wählleitung, gesichert über Callback basierend auf CLIP bzw. COLP (siehe M 5.49 *Callback basierend auf CLIP/COLP*).
- Es sollten geeignete kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) eingesetzt werden, um Verletzungen des Datenschutzes beim Transport schutzwürdiger Daten zu verhindern. Wie entsprechende Verfahren und Produkte ausgewählt werden können, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.
- Werden über einen Transportweg regelmäßig oder dauerhaft personenbezogene Daten ausgetauscht, sollte die Übertragung mit Hilfe eines virtuellen privaten Netzes (VPN) gesichert werden (siehe M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation* und M 5.83 *Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN*

**Maßnahmen gegen unbefugten Abruf**

Der Abruf von Daten durch nicht Abrufberechtigte ist durch geeignete Vorkehrungen zu verhindern:

- Jeder Benutzer muss sich gegenüber den IT-Systemen, von denen die personenbezogenen Daten abgerufen werden, eindeutig identifizieren und authentisieren.
- Nach einer festgelegten Anzahl von Fehlversuchen bei Anmeldungen an IT-Systemen oder Anwendungen ist die Berechtigung zu sperren.

- Passwörter müssen in regelmäßigen Abständen gewechselt werden. Soweit möglich, ist dies durch die entsprechenden Programme zu erzwingen.
- Art und Umfang der Protokollierung müssen festgelegt werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).
- Es sollten zufallsgesteuerte Stichprobenkontrollen oder eine Dauerprotokollierung durchgeführt werden. Zur Überprüfung der Protokolldateien sollten programmgesteuerte Prüfungsverfahren eingesetzt werden.
- Es ist festzulegen, an welcher Stelle die Protokollierungen durchgeführt werden (abrufende und/oder speichernde Stelle).
- Die Protokollierung muss so konzipiert sein, dass nachträglich festgestellt werden kann, aufgrund wessen Abrufberechtigung Daten abgerufen wurden.
- Die Gründe des Abrufs müssen protokolliert werden. Beim Abruf von Daten sollte protokolliert werden, über welchen Anschluss und welche Endgeräte die Übertragung stattfindet.

**Maßnahmen zur Organisationskontrolle**

- Alle Mitarbeiter, insbesondere die der abrufenden Stelle, sind auf das Datengeheimnis zu verpflichten. Eine Weitergabe von Daten an Dritte ist vertraglich zu untersagen.

Prüffragen:

- Werden bei Übertragung und Abruf personenbezogener Daten die datenschutzrechtlichen Bestimmungen beachtet?
- Wird wirksam verhindert, dass Unbefugte auf die personenbezogenen Daten zugreifen können?
- Wird regelmäßig überprüft, an welche Stellen personenbezogene Daten übermittelt werden können?
- Sind Transportweg und Übertragungsmethode so gewählt, dass Vertraulichkeit, Integrität und Authentizität der personenbezogenen Daten gewährleistet werden können?
- Wurden die umgesetzten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten bei Übertragung und Abruf dokumentiert?
- Liegt ein Konzept zur Überprüfung und Feststellung der Zulässigkeit der im Rahmen automatisierter Abrufe erfolgten Datenübertragungen vor?

# M 2.206 Planung des Einsatzes von Lotus Notes/Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Der Einsatz von Lotus Notes/Domino muss sorgfältig geplant werden. Dabei sollte der Planungsprozess als kontinuierlicher Prozess umgesetzt werden und nicht nur als einmalige Tätigkeit bei Ersteinführung. Der Detaillierungsgrad der Planung und der Umfang der Dokumentation, die im Planungsprozess zu erstellen ist, richtet sich unter anderem nach dem Schutzbedarf der jeweiligen Lotus Notes/Domino-Umgebung. Bei der Planung müssen außerdem auch Angemessenheitskriterien wie Größe und Ressourcen der Institution berücksichtigt werden. Zusätzlich ist der Umfang der Nutzung der unterschiedlichen Dienste der Lotus Notes/Domino-Plattform und der Komplexität der Architektur zu berücksichtigen.

So erfordert ein alleiniger Einsatz von Lotus Notes/Domino als interne und externe E-Mail-Plattform und Plattform für institutionsweite Zusammenarbeit (Workgroup-Unterstützung) aufgrund der einfacheren Architektur in der Regel eine weniger aufwendige Planung als bei einem Einsatz, der zusätzlich zu den E-Mail- und Workgroup-Diensten Extranet- und Internet-Schnittstellen vorsieht und eine breite Palette von Internet-Diensten einschließlich Instant Messaging und Web Services bereitstellt.

Grundsätzlich müssen bei der Einsatzplanung von Lotus Notes/Domino folgende Aspekte betrachtet werden:

- Architekturplanung unter Berücksichtigung von Sicherheitsaspekten,
- Planung der Rolle von Lotus Notes/Domino im institutionsweiten Identitätsmanagement,
- Planung der Domänen- und Zertifikatshierarchie,
- Planung administrativer Tätigkeiten im Umfeld Lotus Notes/Domino,
- Festlegen der Relevanz der Lotus Notes/Domino-Plattform für die institutionsweite Geschäftsfortführungs- und Notfallplanung,
- Planung der Kommunikationssicherheit für die Lotus Notes/Domino-Umgebung.

Die Lotus Notes/Domino-Plattform kann unter Verwendung von Servervirtualisierungstechniken oder Terminalserver-Technologie eingesetzt werden. In diesen Fällen ist eine entsprechende Planung des Zusammenspiels der Lotus Notes/Domino-Plattform mit der eingesetzten Virtualisierungsplattform zu erstellen.

Abhängig vom Schutzbedarf der von Lotus Notes/Domino unterstützten Geschäftsprozessen kann die Hochverfügbarkeit von Lotus Notes/Domino-Diensten erforderlich sein. Das Zusammenspiel der Lotus Notes/Domino-Plattform mit der eingesetzten Technologie zur Abbildung der Hochverfügbarkeitsanforderungen bzw. die Konfiguration der Lotus Notes/Domino-eigenen Mechanismen für Hochverfügbarkeit (Clustering) sind in diesen Fällen über eine entsprechende Planung abzubilden.

**Architekturplanung unter Berücksichtigung von Sicherheitsaspekten**

Es ist sicherzustellen, dass neben den fachlichen und funktionalen Anforderungen an die Lotus Notes/Domino-Plattform und den Anforderungen, die aus IT-strategischen Vorgaben einfließen, auch Sicherheitsaspekte bei der Architekturplanung beachtet werden. Dies kann über die Berücksichtigung allge-

meiner Sicherheitsleitlinien erfolgen oder auch über das Einbeziehen konkreter Vorgaben der Institution zur hauseigenen Sicherheitsarchitektur.

Die für die Lotus Notes/Domino-Architekturplanung relevanten Sicherheitsleitlinien bzw. Elemente der Sicherheitsarchitektur sind in konkrete Elemente der Architekturplanung zu überführen. So sind z. B. die Sicherheitsvorgaben der Institution zur Planung und Absicherung von Netzübergängen bei der Positionierung und Absicherung der Lotus Domino Server, die als Übergang zu Extranets oder zum Internet vorgesehen sind, zu berücksichtigen.

Die Entscheidung, wie viele Lotus Domino Server an welchen Punkten eingesetzt werden, sollte sich primär an dem Schutzbedarf der Lotus Domino Dienste orientieren. Grundsätzlich ist eine selektive und restriktive Installation der Lotus Domino Dienste auf Basis des Schutzbedarfs anzustreben. Wo möglich, sind bereits auf Ebene der Architektur hoch schutzbedürftige Dienste von Diensten mit niedrigem Schutzbedarf zu trennen, sodass eine Beeinträchtigung der hoch schutzbedürftigen Dienste durch Schwachstellen der Dienste mit niedrigem Schutzbedarf möglichst vermieden wird. So ist z. B. bei entsprechend hohem Schutzbedarf der zentrale E-Mail-Dienst der Institution redundant auszulegen und auf Servern zu betreiben, die möglichst keine weiteren und in Bezug auf Schwachstellen "risikobehaftete" Dienste beinhalten.

**Planung der Rolle von Lotus Notes/Domino im institutionsweiten Identitätsmanagement**

Die Lotus Notes/Domino-Plattform bietet umfangreiche Funktionalitäten zum Aufbau eines institutionsweiten Identitätsmanagements. Es ist grundsätzlich möglich, Lotus Notes/Domino als führendes System des Identitätsmanagements einzusetzen und andere Systeme über Schnittstellen (z. B. LDAP-Schnittstellen) mit Informationen über elektronische Identitäten und ihren Rechteumfang zu versorgen. Umgekehrt kann aber auch Lotus Notes/Domino als nachrangiges System diese Informationen von einer entsprechenden Schnittstelle eines anderen, führenden Systems erhalten.

Es ist erforderlich, dass für die Institution eindeutig festgelegt wird, welches das führende System zum Identitätsmanagement ist und wie die Information zu elektronischen Identitäten in der IT-Landschaft propagiert wird. Damit kann die Rolle von Lotus Notes/Domino entsprechend geplant werden. Diese Rolle wirkt sich maßgeblich auf den Schutzbedarf der Lotus Domino Dienste und der Lotus Notes/Domino-Infrastrukturkomponenten aus.

**Planung der Domänen- und Zertifikatshierarchie**

Der Einsatz der Lotus Notes/Domino-Plattform erfordert die Planung der Domänen- und Zertifikatshierarchie. Dies muss erstmalig bei der Einführung von Lotus Notes/Domino erfolgen und bei relevanten Änderungen der Organisationsstruktur, der genutzten Dienste, der angebundenen Partner etc. entsprechend angepasst werden. Dadurch, dass viele sicherheitsrelevante Einstellungen auf Domänenebene wirksam sind (z. B. Sperrungen, sicherheitsrelevante Replikationsparameter), ist die Berücksichtigung der Sicherheitsthemen bei der Planung der Domänenhierarchie zwingend erforderlich.

Während für kleine Institutionen ein Ein-Domänen-Konzept ausreichend sein kann (bezogen auf die Produktivdomänen), wird in der Regel für komplexe Strukturen, wie z. B. bei Konzernen oder größeren Institutionen, ein Mehr-Domänen-Konzept erforderlich sein. Bestandteile der Domänenhierarchie sind alle Elemente, die zur Festlegung der Lotus Domino Infrastruktur zur Verfügung stehen. Das sind neben den Lotus Domino Domänen auch die Lotus

Domino Organisationen und die Lotus Domino Netze (DNNs, *Lotus Domino Named Networks*) sowie das genutzte hierarchische Namenssystem (basierend auf dem X.500-Standard).

Die sicherheitstechnische Abbildung der Domänenhierarchie (die unter anderem regelt, zwischen welchen Servern und Benutzern Kommunikation erfolgen kann) geschieht über eine Zertifikatshierarchie (PKI). Die Planung der Zertifikatshierarchie ist abhängig von der Rolle von Lotus Notes/Domino im institutionsweiten Identitätsmanagement zu gestalten. Wesentliche Änderungen im Identitätsmanagement sollten immer eine Anpassung der Planung der Zertifikatshierarchie zur Folge haben und nicht durch technische Umgehungen (Workarounds) abgebildet werden. Es ist zu berücksichtigen, dass sowohl Lotus Notes eigene als auch Internet-Zertifikate (X.509-Zertifikate) verwaltet werden müssen.

Die erforderlichen Strukturen und Prozesse (wie z. B. in den X.509-Standards beschrieben) müssen in der Planung der Zertifikatshierarchie definiert werden. Dazu gehört beispielsweise die Festlegung der Zertifizierungsstelle (Certificate Authority), der Registrierungsstelle (Registration Authority) und des Zertifizierungsprozesses (CA-Prozess). Dabei ist zu entscheiden, ob eine Fremdanbieter-Zertifizierungsstelle genutzt wird oder ob eine Lotus Domino Zertifizierungsstelle eingerichtet wird.

Alle technischen Einstellungen wie auch die administrativen Vorgänge und Prozesse im Umfeld der Zertifikatshierarchie müssen sehr sorgfältig geplant, konzeptionell im Detail ausgearbeitet und ausreichend dokumentiert werden. Es ist zu berücksichtigen, dass ab Lotus Notes/Domino 8.5 eine Überprüfung zurückgezogener Zertifikate über OCSP (Online Certificate Status Protocol, RFC 2560 der IETF) möglich ist. Eine entsprechende Aktualisierung der Planung der Zertifikatshierarchie ist vorzunehmen.

**Planung administrativer Tätigkeiten im Umfeld Lotus Notes/Domino**

Es ist erforderlich, administrative Tätigkeiten im Umfeld Lotus Notes/Domino detailliert zu planen und in Form verbindlicher Anweisungen (wie z. B. eines verbindlichen Administrationsleitfadens) festzuschreiben. Der Detaillierungsgrad der Planung und der Umfang der Dokumentation sind abhängig vom festgelegten Schutzbedarf der Lotus Notes/Domino-Plattform.

Insbesondere kritische administrative Tätigkeiten, beispielsweise im Umfeld des Zertifizierungsprozesses, aber auch bei der Benutzeradministration, bei der Datenbankadministration, bei der Installation und Konfiguration von Komponenten und Diensten, müssen mit entsprechender Sorgfalt und Sachkenntnis durchgeführt werden.

Die ausreichende Dokumentation kritischer Administrationstätigkeiten muss in den Anweisungen zur Administration gefordert und entsprechend überprüft werden.

Unsachgemäße, auf Zuruf durchgeführte oder nicht ausreichend dokumentierte Administrationstätigkeiten stellen genauso wie vorsätzliche Angriffe unter Missbrauch administrativer Rechte erhebliche Gefährdungen dar. Diese haben, obwohl nicht Lotus Notes/Domino-spezifisch, wesentliche Auswirkungen auf die Erreichung der Schutzziele für die Lotus Notes/Domino-Plattform haben.

Aufgrund der technischen Komplexität der Lotus Notes/Domino-Plattform ist es in der Regel nicht ausreichend, allgemeine Anweisungen zur Administration umzusetzen, ohne plattformspezifische Ausprägungen vorzunehmen.

Bei der Planung der administrativen Tätigkeiten für Lotus Notes/Domino ist auch festzulegen, dass eine Überwachung und Kontrolle dieser Tätigkeiten unter Einsatz der technischen Möglichkeiten der Lotus Notes/Domino-Plattform zu erfolgen hat.

**Festlegen der Relevanz der Lotus Notes/Domino-Plattform für die institutionsweite Geschäftsfortführungs- und Notfallplanung**

Die Planung der Betriebsabläufe und der tief mit den Betriebsabläufen verzahnten Sicherheitsmaßnahmen der Lotus Notes/Domino-Plattform, wie z. B. der Maßnahmen zur Datensicherung und Wiederherstellung (*Backup/Recovery*), erfordert die Einstufung der Plattform im Gesamtkontext der Geschäftsfortführungs- und Notfallplanung. Ist dies nicht bereits in entsprechenden Aktivitäten der Institution erfolgt, sollte die Einstufung der Lotus Notes/Domino-Plattform im Hinblick auf die Geschäftsfortführungs- und Notfallplanung im Rahmen der Planung für die Einführung oder Migration von Lotus Notes/Domino stattfinden. Nur so lassen sich eine Reihe erforderlicher Sicherheitsmaßnahmen, wie z. B. Maßnahmen zur Sicherstellung der Verfügbarkeit der Plattform oder einzelner Dienste, angemessen planen.

**Planung der Kommunikationssicherheit für die Lotus Notes/Domino-Umgebung**

Aufgrund der verteilten Architektur typischer Lotus Notes/Domino-Umgebungen kommt der Planung der Kommunikationssicherheit eine tragende Rolle in der Sicherheitsplanung zu. Dabei sind folgende, für die Kommunikationssicherheit relevante, Themen abzudecken:

- Server-zu-Server-Kommunikation von Lotus Domino-Servern (sowohl unter Verwendung von Lotus Notes Protokollen, Internet-Protokollen wie auch bei der Datenbankreplikation),
- Client-zu-Server-Kommunikation für Lotus Notes Clients zu Lotus Domino Servern (für alle Lotus Notes Clienttypen inklusive administrativer Clients),
- Client-zu-Server-Kommunikation für fremde Clients zu Lotus Domino Servern (unter Verwendung der POP3 und IMAP-Protokolle),
- Remote Access Zugänge und spezifische Einwahlzugänge der Lotus Domino Server,
- Nutzung von Push-Diensten für mobile Endgeräte,
- Deinstallation (bzw. nicht installieren) unsicherer bzw. nicht benötigter Kommunikationsprotokolle (z. B. WebDAV),
- Restriktive Einrichtung von Vertrauensbeziehungen zwischen Servern,
- Nutzung oder Bereitstellung von Diensten/Schnittstellen außerhalb der Lotus Notes/Domino-Umgebung, wie z. B. LDAP-Schnittstellen.

Es ist zu berücksichtigen, dass Lotus Notes/Domino aus der Historie heraus noch Modem-Verbindungen zwischen Servern vorsieht, die in heutigen Umgebungen nicht mehr zeitgemäß sind und Sicherheitsrisiken induzieren können. Die Planung der Kommunikationssicherheit muss eine Entfernung dieser Verbindungen (falls vorhanden) und eine Deaktivierung der entsprechenden Schnittstellen bzw. Verbindungsdokumente vorsehen.

Prüffragen:

- Werden bei der Architekturplanung für die Lotus Notes/Domino-Plattform Sicherheitsaspekte berücksichtigt?
- Ist die Rolle von Lotus Notes/Domino im institutionsweiten Identitätsmanagement festgelegt?
- Ist die Planung der Domänen- und Zertifikatshierarchie ausreichend dokumentiert?

# M 2.207 Sicherheitskonzeption für Lotus Notes/Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Wie für jedes in einer Institution eingesetzte Software-Produkt muss auch für den Einsatz von Lotus Notes/Domino eine geeignete Sicherheitskonzeption erstellt werden. Abhängig von der Größe, den Ressourcen und der organisatorischen Struktur der Institution kann die Sicherheitskonzeption für Lotus Notes/Domino in ein Ergebnisdokument (z. B. eine Sicherheitsrichtlinie) oder eine Reihe von Ergebnisdokumenten einfließen. Eine modulare Dokumentation der Sicherheitskonzeption erleichtert die zielgruppenspezifische Verteilung der Dokumente, beispielsweise könnte eine Richtlinie für die Anwendungsentwicklung nur an die Anwendungsentwickler für die Lotus Notes/Domino-Plattform bzw. an Administratoren verteilt werden.

Die im Folgenden genannten Punkte der Sicherheitskonzeption sind dabei abzuarbeiten und die Ergebnisse zu dokumentieren. Sind Teile der Sicherheitskonzeption für den speziellen Einsatz der Lotus Notes/Domino-Plattform in der Institution nicht relevant (z. B. wenn keine Anwendungsentwicklung für die Lotus Notes/Domino-Plattform stattfindet), ist dies in der Sicherheitsrichtlinie zu dokumentieren.

**Sicherheitsrichtlinie für Lotus Notes/Domino**

Im Rahmen der Sicherheitsrichtlinie sind folgende Aspekte zu berücksichtigen:

- Die Sicherheitsrichtlinie muss konform zu den geltenden Sicherheitsrichtlinien der Institution sein (siehe M 2.192 *Erstellung einer Leitlinie zur Informationssicherheit*).
- Es müssen die jeweiligen Zielgruppen und die für sie relevanten Konzepte/Richtlinien der Lotus Notes/Domino-Sicherheitskonzeption genannt werden.
- Die im Weiteren genannten Konzepte sind entweder als Bestandteil der Sicherheitsrichtlinie aufzunehmen oder zu referenzieren. Es ist dabei sicherzustellen, dass über die Referenzen die jeweils aktuelle Version der Konzepte verfügbar ist.
- Die Verbindlichkeit der Richtlinie für alle Zielgruppen (zum Beispiel Lotus Notes Benutzer, Lotus Domino Administratoren, Führungskräfte, Projektleiter, Softwareentwickler, Softwarearchitekten) ist sicherzustellen, falls nicht bereits für alle Richtlinien der Institution eine entsprechende allgemeine Regelung zur Verbindlichkeit besteht.
- Sind in der Institution mehrere Lotus Notes/Domino-Umgebungen (Installationen) im Einsatz, müssen umgebungsspezifische Besonderheiten der Sicherheitskonzeption dokumentiert sein.
- Die Sicherheitsrichtlinie für die Nutzung von Lotus Notes/Domino muss institutionsweit abgestimmt sein und allen Benutzern bekannt gegeben worden sein. Hierbei empfiehlt es sich, die wichtigsten Inhalte für die jeweiligen Zielgruppen in einer kurzen und prägnanten Form aufzubereiten, z. B. in Form eines Faltblattes oder einer Webseite. Wenn sich Sicherheitsvorgaben verändern, müssen alle Benutzer hierüber informiert werden.

**Konzept zur Domänen- und Zertifikatshierarchie von Lotus Notes/Domino**

Das Konzept zur Domänen- und Zertifikatshierarchie von Lotus Notes/Domino ist das Ergebnis der in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* beschriebenen Planungstätigkeit. Das Konzept ist vom Verantwortlichen stets aktuell zu halten und muss bei Veränderungen angepasst werden. Bei größeren Änderungen der Lotus Notes/Domino-Infrastruktur erfolgt dies in der Regel durch die zuständigen Projektleiter, System- und Softwarearchitekten. Änderungen an diesem hoch sicherheitsrelevanten Konzept bedürfen einer Abnahme durch das Informationssicherheitsmanagement.

**Konzept zur Nutzung der Lotus Notes/Domino-eigenen Sicherheitsmechanismen: Verschlüsselung, Umgang mit Zertifikaten und Lotus Notes IDs**

Lotus Notes/Domino stellt unterschiedliche Verschlüsselungsmechanismen sowohl zur Verschlüsselung beweglicher Daten (Kommunikationsverbindungen, Kommunikationsinhalte) als auch zur Verschlüsselung der Datenbestände (z. B. Datenbankverschlüsselung, E-Mail-Verschlüsselung) bereit. Es ist zu definieren, welche Lotus Domino-eigenen Mechanismen genutzt werden sollen. Die Konformität zu einem institutionsweiten allgemeinen Verschlüsselungskonzept bzw. die durch proprietäre Lotus Notes/Domino-Mechanismen bedingten Abweichungen sind zu dokumentieren. Das Schlüsselmanagement für Lotus Notes/Domino ist gemäß den Vorgaben des institutionsweiten Verschlüsselungskonzepts zu gestalten und muss dem Schutzbedarf der Lotus Notes/Domino-Plattform Rechnung tragen.

Der Umgang mit Zertifikaten, z. B. bei Rezertifizierung wegen Ablauf, Erstellung von Cross-Zertifikaten etc. ist gleichfalls in diesem Konzept zu regeln. Gefordert sind konkrete Regelungen und kein Verweis auf die grundsätzlich in Lotus Notes/Domino vorhandenen Mechanismen. So ist z. B. festzulegen, wann ein Versand per E-Mail zur Rezertifizierung an die Administratoren zulässig ist und wann nicht.

Da Lotus Notes IDs aufgrund der "Portabilität" ein Sicherheitsrisiko darstellen, muss geregelt werden, wo Kopien dieser IDs zu Wiederherstellungszwecken vorzuhalten sind und wie Prozesse im Umgang mit Lotus Notes IDs (z. B. Rezertifizierung, Wiederherstellung) ablaufen sollen.

Ab Lotus Notes 8.5 steht mit der Lotus Notes ID Vault ein Werkzeug zum Management von Lotus Notes IDs zur Verfügung, das u. a. die Wiederherstellung verlorener Lotus Notes IDs, verlorener Passwörter, Synchronisation von Kopien von IDs mit nativen Mitteln der Lotus Notes/Domino-Plattform ermöglicht bzw. bereits vorhandene Funktionalität der Plattform erweitert oder vereinfacht. Die Nutzung des Werkzeugs wird empfohlen. Der Einsatz ist jedoch zu planen und das Konzept zur Nutzung der Lotus Notes/Domino-eigenen Sicherheitsmechanismen entsprechend anzupassen.

**Passwortrichtlinien für Lotus Notes/Domino**

Lotus Notes/Domino besitzt seit jeher eigene Mechanismen zur Bewertung der Passwortgüte. Es ist daher erforderlich, die institutionsweiten Passwortrichtlinien mit entsprechenden Anmerkungen zu übernehmen oder aber speziell für Lotus Notes/Domino eine Anpassung der Passwortrichtlinie an die Lotus Notes Mechanismen vorzunehmen. Die Lotus Notes/Domino-Passwortrichtlinien sollten möglichst Teil der Sicherheitsrichtlinie von Lotus Notes/Domino sein. Wenn eine Anmeldung über Single-Sign-On erfolgt, ist dies in der Sicherheitsrichtlinie entsprechend zu vermerken. Die für den Single-Sign-On genutz-

te Passwortgüte muss den kumulierten Anforderungen der angeschlossenen Anwendungen bzw. Systeme genügen.

**Protokollierungs- und Auswertungskonzept für Lotus Notes/Domino**

Konform zu der institutionsweit gültigen Richtlinie zur Protokollierung und Auswertung sicherheitsrelevanter Daten/Ereignisse ist ein konkretes Konzept für die Lotus Notes/Domino-Plattform zu erstellen. Abstimmvorgänge mit Datenschutzbeauftragten, Betriebsrat, Personalrat und anderen in diese Konzepte einzubindenden Stellen sind dann erforderlich, wenn keine entsprechende allgemeingültige Richtlinie zur Protokollierung und Auswertung vorliegt oder diese nicht den erforderlichen Detaillierungsgrad aufweist.

Bei der Erstellung der Sicherheitsrichtlinie ist zu berücksichtigen, dass die Vorgaben im Hinblick auf die auszuwertenden Datenvolumina realistisch sind und eine Umsetzung im Betrieb mit den vorhandenen Ressourcen möglich ist. Werden in der Institution bereits Werkzeuge zur zentralen Protokollierung und automatischen Protokollauswertung eingesetzt, ist zu prüfen, ob die Lotus Notes/Domino-Protokollierung und -Auswertung mit deren Hilfe erfolgen kann.

**Archivierungskonzept für Lotus Notes/Domino**

Die Lotus Notes/Domino-Plattform kann unterschiedliche archivierungspflichtige Daten beinhalten: E-Mails, archivierungspflichtige Workflow-Elemente, Datenbanken archivierungspflichtiger Lotus Notes-Anwendungen und Dienste usw. Bei der Nutzung von Lotus Notes/Domino als zentrales System zum Identitätsmanagement fallen auch hier archivierungspflichtige Daten an. Es ist daher erforderlich, ein fachliches und technisches Archivierungskonzept für die Lotus Notes/Domino-Plattform zu erstellen und entsprechend umzusetzen oder das vorhandene institutionsweite Archivierungskonzept an die Anforderungen der Lotus Notes/Domino-Umgebung anzupassen.

**Konzepte zur Absicherung aller genutzter Lotus Domino Dienste**

In der Regel wird die Absicherung aller Dienste (oft auch auf der Ebene installierter Module) in der Sicherheitsrichtlinie gefordert. Die Dokumentation der Maßnahmen zur Absicherung der Dienste muss nicht zwingend in der Sicherheitsrichtlinie für Lotus Notes/Domino erfolgen, da sie sich schwerpunktmäßig nur an die Zielgruppe der Administratoren und an das Informationssicherheitsmanagement richtet, sondern kann auch im Rahmen des Betriebskonzeptes erfolgen. Es sollten sowohl die technischen Maßnahmen an der Lotus Notes/Domino-Plattform (Härtung, Konfiguration server- und clientseitiger Komponenten) als auch organisatorische Maßnahmen und genutzte zusätzliche Sicherheitskomponenten zur Absicherung aller Dienste beschrieben werden.

Konzept zum Umgang mit sicherheitsgefährdenden Altanwendungen und für deren Betrieb benötigten sicherheitsgefährdenden Konfigurationen der Lotus Notes/Domino-Plattform

Ältere Lotus Domino-Anwendungen, die nicht migriert werden können, erfordern eventuell "unsichere" Einstellungen, um auf neueren Plattformen betrieben werden zu können. Wenn auf diese nicht verzichtet werden kann, ist es erforderlich, konzeptionell festzuhalten, wie diese betrieben und überwacht werden können, um das entstehende Sicherheitsrisiko zu minimieren. Insbesondere ist darauf zu achten, dass "unsichere" Parametrisierungen der Plattform nur punktuell zum Einsatz kommen und nicht aus Gründen der Kompatibilität mit den Altlagen zum institutionsweiten Standard erhoben werden.

**Richtlinie für die Anwendungsentwicklung für die Lotus Notes/Domino-Plattform**

Lotus Notes/Domino bietet sowohl die Möglichkeit der Anwendungsentwicklung unter den bisherigen, proprietären Technologien als auch die Anwendungsentwicklung unter einer Eclipse-basierten Java-Entwicklungsumgebung. Für jede der beiden Möglichkeiten ist, falls sie genutzt wird, eine entsprechende Richtlinie für die Anwendungsentwicklung zu erstellen. Diese Richtlinien müssen sowohl Coding-Standards für die nutzbaren Programmiersprachen als auch Best Practice der Entwicklung wie auch eine Beschreibung des Anwendungsentwicklungsprozesses beinhalten.

**Richtlinie für die Anwendungsintegration mit der Lotus Notes/Domino-Plattform**

Lotus Notes/Domino wird zunehmend als Plattform für server- und clientseitige Anwendungsintegration positioniert, sowohl durch den neuen Lotus Notes Client, der in der strategischen Positionierung des Herstellers als "universeller" Client gesehen wird, als auch durch die Möglichkeit der SAP-Integration. Um Anwendungsintegration nicht zu einer Quelle von sicherheitstechnischen Schwachstellen werden zu lassen, ist es erforderlich, eine plattformspezifische Richtlinie zur Anwendungsintegration mit der Lotus Notes/Domino-Plattform zu erstellen.

**Schutz vor Schadprogrammen für Lotus Notes/Domino**

Der Schutz vor Schadprogrammen für Lotus Notes/Domino ist die konzeptionelle Umsetzung der allgemeinen, institutionsweit gültigen Vorgaben zum Schutz vor Schadprogrammen. Dazu gehört sowohl der Schutz vor Schadprogrammen an Netzübergängen, an denen Lotus Domino als Web- oder E-Mail-Gateway zum Einsatz kommt, als auch der "nachgelagerte" Schutz vor Schadprogrammen der Lotus Domino Datenbanken (einschließlich der E-Mail-Datenbanken). Das Zusammenspiel der standardmäßig installierten server- oder clientseitigen Schutzprogramme mit den installierten Lotus Notes/Domino-Komponenten ist gleichfalls in diesem Konzept zu beschreiben.

**Härtungskonzept und Konfigurationsvorgaben für Lotus Notes/Domino**

Die zu installierenden Komponenten von Lotus Notes/Domino sind entsprechend dem Schutzbedarf und ihrem Einsatzszenario zu härten und zu konfigurieren. Es ist neben den im Konzept zur Absicherung der genutzten Dienste beschriebenen Absicherungsmaßnahmen auf Ebene der Dienste auch eine "Basishärtung" des Servers konzeptionell zu beschreiben. Zudem ist zu beschreiben, welche Dienste nicht genutzt werden und wie sie entsprechend deinstalliert (bzw. nicht installiert) werden können. Für alle genutzten Clienttypen (auch browserbasierte Clients) sind die clientseitig erforderlichen Härtungs- bzw. Konfigurationsvorgaben konzeptionell zu beschreiben.

**Konzept zur Nutzung von Push-Diensten**

Die Nutzung des Lotus Domino E-Mail-Dienstes in Verbindung mit Push-Diensten kann über die Anbindung fremder Push-Dienste (wie z. B. bei der Einbindung von Smartphones) oder über die Nutzung der Komponente *Lotus Notes Traveler* erfolgen. Es ist erforderlich, dass bei der Nutzung von Push-Diensten die anfallenden sicherheitsrelevanten Themen konzeptionell beschrieben werden.

Prüffragen:

- Existieren aktuelle Sicherheitsrichtlinien für die Nutzung von Lotus Notes?
- Sind alle relevanten Sicherheitsvorgaben der Institution auf Lotus Notes abgebildet?
- Werden alle Benutzer über neue oder veränderte Sicherheitsvorgaben zu Lotus Notes informiert?

# M 2.208 Planung der Domänen und der Zertifikatshierarchie von Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* integriert.

# M 2.209 Planung des Einsatzes von Lotus Notes im Intranet

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* integriert.

# M 2.210 Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* integriert.

# M 2.211 Planung des Einsatzes von Lotus Notes in einer DMZ

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* integriert.

# M 2.212 Organisatorische Vorgaben für die Gebäudereinigung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Innerer Dienst

Mit der Durchführung von Reinigungsarbeiten werden fast ausschließlich externe Unternehmen beauftragt. Das nicht zur eigenen Institution gehörende Reinigungspersonal muss alle Räume und Bereiche des Gebäudes betreten, auch Gebäudeteile, wie Technikräume oder Vorstandsetagen, zu denen nur bestimmte Mitarbeitergruppen Zutritt haben. Desweiteren benutzen die externen Reinigungskräfte häufig eigenes Arbeitsgerät und bringen je nach Vertrag auch Reinigungsmittel und andere Verbrauchsstoffe mit. Damit werden Schwachstellen geschaffen, da beispielsweise so auch internes Material auf dem Rückweg mitgenommen werden könnte.

Neben allgemeinen Merkmalen eines Leistungsverzeichnisses für Reinigungsarbeiten wie Art, Name und Lage des Objektes sind Raumnutzungsgruppen, aktuelle Raumverzeichnisse sowie die einzelnen Leistungsarten detailliert zu beschreiben. Leistungsarten können z. B. die Reinigung nichttextiler und textiler Beläge, die Reinigung und Pflege von Gegenständen der Raumausstattung und Einrichtung sowie Entsorgungsaufgaben sein. Darauf aufbauend werden die einzelnen Anforderungen mit Angabe des Umfanges in den einzelnen Räumen beschrieben.

Um den Arbeitsprozess nicht zu stören, werden Reinigungsarbeiten oft in die arbeitsfreien Zeiten verlegt. Damit muss aber auch geklärt werden, ob das Reinungspersonal beaufsichtigt werden sollte. Vorstellungen zu den Reinigungszeiten sowie die Sonderbehandlung einzelner besonders schutzbedürftiger und nicht unkontrolliert begehbarer Bereiche sind in der Leistungsbeschreibung aufzuführen.

Reinigungspersonal sollte vor Aufnahme ihrer Tätigkeit in die Aufgaben eingewiesen werden. Hierzu gehört vor allem eine Einweisung, welche Bereiche unter welchen Voraussetzung betreten werden dürfen, wie IT-Systeme zu reinigen sind bzw. was in der Umgebung von IT-Systemen zu beachten ist und wie sie mit vertraulichen Informationen umzugehen haben, die sie während ihrer Arbeit erhalten. Dies können z. B. Unterlagen sein, die sich auf Schreibtischen oder in Papierkörben finden, oder mitgehörte Gespräche.

Der Zutritt von Reinigungspersonal kann insbesondere in Bereichen mit höheren Sicherheitsanforderungen wie Rechenzentren, Serverräumen, Technikräumen oder Kommunikationszentralen problematisch sein und daher zusätzliche Sicherheitsmaßnahmen erfordern. In solchen Bereichen kann es sinnvoll sein, die Vertrauenswürdigkeit des Reinigungspersonals zu überprüfen oder diese während ihrer Tätigkeit zu beaufsichtigen.

Wenn Vertrauen in die Reinigungsfirma besteht, sollte der Zutritt der Reinigungskräfte über die vorhandene Zutrittskontrolle bzw. das Schließsystem geregelt werden. Das kann jedoch nur dann einewirksame Sicherungsmaßnahmen sein, wenn z. B. Ausweis oder Schlüssel gegen Unterschrift und nur zeitlich begrenzt an benannte bzw. bekannte Mitarbeitern der Reinigungsfirma ausgegeben werden. Bei der Vereinbarung über die Verwendung von Stammpersonal kann über das Ausweissystem eine wirksame Kontrolle der Vertragseinhaltung erreicht werden.

Für die Koordination, aber auch bei auftretenden Problemen ist vom Auftragnehmer ein Objektverantwortlicher zu benennen, der jederzeit ansprechbar ist. Er muss Entscheidungsbefugnis über das einzusetzende (vor allem auch über nicht mehr einzusetzendes, weil unerwünschtes) Personal haben.

Bereits in der Ausschreibung und der Vertragsformulierung ist die Sonderbehandlung sensitiver Bereiche einzubeziehen. Zum Beispiel sind bei Rechenzentren stichprobenartige Kontrollen von Taschen oder Transportgut im Zugangs- oder Zufahrtsbereich für betriebsfremdes Personal in den Verträgen festzuschreiben.

Da bei Reinigungskräften IT-Kenntnisse nicht vorausgesetzt werden können, sollten diese daher in allen Bereichen mit geschäftskritischen IT-Systemen dahingehend eingewiesen werden, welche Tätigkeiten zu Schäden an IT-Einrichtungen oder Problemen beim IT-Betrieb führen können. Beispiele für solche Problemfelder sind:

- Bei der Reinigung von Tastaturen können unbeabsichtigt Eingaben an Servern oder anderen zentralen Komponenten erfolgen, die den IT-Betrieb beeinträchtigen.
- IT-Systeme können versehentlich ausgeschaltet werden.
- Stromversorgungs- oder Kommunikationskabel können durch Staubsauger beschädigt oder aus den Endpunkten gerissen werden.
- Durch Wasser oder Reinigungsflüssigkeit können Kurzschlüsse in Hardware-Komponenten verursacht werden.

Bereiche mit einem erhöhten Sicherungsbedarf wie Maschinensaal oder Datenträgerarchiv sind nur unter Anwesenheit von Verantwortlichen des Auftraggebers oder in einigen Fällen auch unter Anwesenheit einer Vertrauensperson des Auftragnehmers, z. B. im Vier-Augen-Prinzip, zu reinigen.

Prüffragen:

- Wird kontrolliert, ob die Mitarbeiter der beauftragten Reinigungsfirma die ausgegebenen Schlüssel bzw. Ausweise vertragsgemäß verwenden?
- Sind die Reinigungskräfte über den Umgang mit der IT ausreichend informiert?
- Werden die Reinigungskräfte in besonders sensitiven Bereichen bei der Arbeit beaufsichtigt?

# M 2.213 Inspektion und Wartung der technischen Infrastruktur

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Die von Herstellern empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung der Komponenten der technischen Infrastruktur sollten unbedingt eingehalten und durch ausreichend geschultes Personal durchgeführt werden. Bei der Inspektion wird der Zustand der technischen Einrichtung festgestellt. Bei der Wartung werden vorbeugende Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit der technischen Einrichtungen vorgenommen, z. B. werden Verschleißteile vor dem Erreichen der Verschleißgrenze ausgetauscht.

Inspektionen und Wartungen sollten in lastschwachen Zeiten vorgenommen werden. Die Wahrscheinlichkeit, dass es durch Versagen von Bauteilen zu spontanen Ausfällen kommt, sinkt, wenn diese Arbeiten regelmäßig und gewissenhaft durchgeführt werden. Andernfalls kann das Versagen umfangreichere Reparaturarbeiten nach sich ziehen und dadurch zu größeren Betriebsunterbrechungen führen.

Die Wartungsarbeiten sichern neben der Verfügbarkeit auch den wirtschaftlichen Betrieb von Anlagen. So ist z. B. der regelmäßige Austausch oder die Reinigung von Filterelementen einer Klimaanlage wichtig für Leistungserhalt, Wirksamkeit und Betriebskosten der Klimatechnik.

Die Intervalle sollten über die vom Hersteller genannten Werte hinaus den tatsächlichen Umständen angepasst werden. Wird z. B. festgestellt, dass Verschleißteile deutlich früher die Verschleißgrenze erreichen, als laut Hersteller vorgesehen, müssen die Intervalle verkürzt werden. Zugleich sollten die Gründe für diese Verkürzung der Lebensdauer gesucht und nach Möglichkeit abgestellt werden. Besonders in Fällen einer vorübergehenden deutlichen Änderung der Einsatzbedingungen, z. B. Umbauarbeiten, sind zusätzliche Inspektionen dringend anzuraten.

Durchgeführte Inspektionen und Wartungsarbeiten an der technischen Infrastruktur sollten protokolliert werden, damit jederzeit nachvollziehbar ist, welche Arbeiten zu welchem Zeitpunkt durchgeführt wurden und wann die nächsten anstehen.

Prüffragen:

- Werden die Wartungsvorschriften eingehalten?
- Werden die Wartungsintervalle bei besonderen Beanspruchungen der Situation angepasst?
- Gibt es einen Überblick über durchgeführte sowie anstehende Inspektionen und Wartungsarbeiten an der technischen Infrastruktur?
- Wird den Ursachen ungewöhnlichen Verschleißes nachgegangen?

# M 2.214 Konzeption des IT-Betriebs

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um einen ordnungsgemäßen und sicheren IT-Betrieb gewährleisten zu können, ist eine übergreifende Konzeption unabdingbar. Es sollten Regelungen bzw. Vorgaben für den Einsatz von IT-Systemen und IT-Produkten in den verschiedenen Bereichen existieren, die gut aufeinander abgestimmt sind und die Sicherheitsziele der Behörde bzw. des Unternehmens widerspiegeln.

**Richtlinien für IT-Verfahrensabläufe und Sicherheitsprinzipien**

Alle an der IT-Planung und am IT-Betrieb beteiligten Organisationseinheiten müssen sich auf grundlegende Sicherheitsprinzipien verständigen, die auf alle Bereiche anzuwenden sind (z. B. Anforderungen an Passwörter). Es muss eine übergreifende Regelung der Authentisierung und Rechtevergabe (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*) erfolgen.

Die Verantwortlichkeiten für den Betrieb aller IT-Komponenten müssen klar festgelegt werden. Dazu gehört die Benennung von Administratoren und Ansprechpartnern für die Benutzer (siehe auch M 2.79 *Festlegung der Verantwortlichkeiten im Bereich Standardsoftware*).

Jeder Beschaffung von neuen IT-Komponenten sollte eine Konzeption für deren Einsatz zugrunde liegen. Dabei sollte auch deren Integration in den vorhandenen Informationsverbund betrachtet werden und welche Auswirkungen dies auf vorhandene Sicherheitsmechanismen hat, die eventuell angepasst werden müssen (siehe M 2.216 *Genehmigungsverfahren für IT-Komponenten*).

Ebenso wie der Ablauf bei der Bestellung von IT muss auch der Umgang mit den gelieferten IT-Komponenten geregelt sein (siehe M 2.90 *Überprüfung der Lieferung*). Bevor neue Hardware-Komponenten oder neue Software zum Einsatz kommen, müssen diese getestet werden (siehe M 4.65 *Test neuer Hard- und Software*).

Jede Installation von IT-Komponenten sollte den grundlegenden Sicherheitszielen der Behörde bzw. des Unternehmens folgen und auf geregelten Verfahren basieren. Abhängig von der jeweiligen IT-Komponente und deren Sicherheitsanforderungen müssen hierbei Zugriffsregelungen, Benutzerrechte und andere sicherheitsrelevante Konfigurationen eingerichtet werden. Grundsätzlich sollte jede Installation nachvollziehbar dokumentiert werden (siehe M 2.87 *Installation und Konfiguration von Standardsoftware*).

Um jederzeit die erforderlichen Ressourcen bereitstellen zu können, sind für den Betrieb der IT-Systeme und IT-Anwendungen die Kapazitätsanforderungen zu untersuchen. Es sollte regelmäßig abgeschätzt werden, ob die vorhandenen Kapazitäten für die vorhandenen oder geplanten Geschäftsprozesse und Anwendungen noch ausreichen.

**Richtlinien für den sicheren IT-Betrieb**

Um auch im laufenden Betrieb die Sicherheit aller IT-Systeme aufrechterhalten zu können, müssen eine Vielzahl von Faktoren berücksichtigt werden. Daher sollten alle zur Aufrechterhaltung eines ordnungsgemäßen und sicheren Be-

triebs notwendigen Aufgaben beschrieben und klar zugeordnet werden. Dies betrifft unter anderem die folgenden Aspekte:

- Die Informationsverarbeitung muss kontinuierlich in allen ihren Phasen, allen Anwendungen und allen Systemen dokumentiert werden (siehe M 2.219 *Kontinuierliche Dokumentation der Informationsverarbeitung*).
- Der Zugang zu allen IT-Systemen sollte geschützt sein, z. B. durch Passwörter.
- Die Funktionen derjenigen IT-Komponenten, die nicht zum Einsatz kommen sollen oder dürfen, sind - wenn möglich - zu sperren (siehe auch M 4.95 *Minimales Betriebssystem*).
- Die Protokollierungsdateien sind in regelmäßigen Abständen auf Anomalien (z. B. Ausführung von Funktionen, die nicht zum Einsatz kommen sollen) zu untersuchen.
- Nach Möglichkeit sollten die IT-Systeme in Abständen einem Integritätstest unterzogen werden, so dass unberechtigte Änderungen so früh wie möglich entdeckt werden können. Dies gilt insbesondere für Konfigurationsdaten.
- Für alle IT-Systeme sollten geeignete Verfahren zur Datensicherung eingesetzt werden.
- Die Einhaltung der Sicherheitsmaßnahmen muss regelmäßig kontrolliert werden (siehe M 2.199 *Aufrechterhaltung der Informationssicherheit*).

**Standardlösungen für verwendete Hard- oder Software-Komponenten**

Je größer eine Institution ist, desto wichtiger ist es, für die IT-Ausstattung und den IT-Betrieb möglichst einheitliche Komponenten zu verwenden. Dies betrifft sowohl Hardware-Komponenten, wie z. B. Router, Drucker und Grafikkarten, als auch Software-Produkte, wie Betriebssysteme, Textverarbeitungsprogramme und Tools. Anderenfalls besteht die Gefahr, dass das Gesamtsystem aufgrund von Interoperabilitätsproblemen und ausufernder Komplexität nicht mehr administriert werden kann.

Es sollten daher Hausstandards für Hardware- und Software-Komponenten festgelegt und dokumentiert werden, die bei der Beschaffung zu berücksichtigen sind. Dies erlaubt es, auf bewährte Lösungen zurückzugreifen und Interoperabilitäts- und Kompatibilitätsprobleme möglichst zu vermeiden. Weiterhin wird hierdurch der administrative Aufwand und das erforderliche Fachwissen verringert. In vielen Fällen können auch die Lagerkosten für Verbrauchsmaterial gesenkt werden. In Verbindung mit Rahmenverträgen oder Mengenrabatt können oft auch weitere finanzielle Einsparungen erreicht werden.

Aufgrund der schnellen technischen Fortentwicklung im Bereich der Informationsverarbeitung müssen Hausstandards für IT-Komponenten regelmäßig aktualisiert werden. Dies führt in der Regel dazu, dass ein Mischbetrieb zwischen verschiedenen "Generationen" von Hausstandards erforderlich ist. Daher ist bei der Überarbeitung der Hausstandards zu berücksichtigen, dass neue und alte IT-Komponenten bzw. Produkte kompatibel sind und gemeinsam verwendet werden können.

Ein besonders wichtiger Anwendungsfall für Hausstandards sind Arbeitsplatz-PCs. Hier sollte sowohl für die Hardware-Komponenten in den PCs, wie Prozessor, Arbeitsspeicher, Grafikkarte, usw., als auch für die installierte Software und deren Konfigurationen Hausstandards festgelegt werden. Anderenfalls besteht aufgrund der Vielzahl von Konfigurationsmöglichkeiten, die PCs bieten, die Gefahr, dass die eingesetzten Arbeitsplatz-PCs unüberschaubar und somit nicht mehr administrierbar werden. Allein die Pflege der notwendigen Hardware-Treiber für die Betriebssysteme ist in mittelgroßen Behörden und Unternehmen ohne verbindliche Festlegung von Hausstandards nicht

mehr leistbar. Durch Hausstandards für Arbeitsplatz-PCs wird auch der Einsatz von Systemmanagement-Produkten erleichtert.

**Hinweis:** Bei der Definition von Hausstandards für Hardware- oder Software-Komponenten sollte keinesfalls nur das marktgängigste Produkt in Betracht gezogen werden. Vielmehr sollte sich die Auswahl nach den funktionalen Anforderungen und den (IT-)Sicherheitsanforderungen richten. Eine "Monokultur", d. h. die weitgehende Dominanz eines einzelnen Produktes am Markt, kann unter Umständen sogar zu Sicherheitsproblemen führen. In diesem Fall sind nämlich auch die in dem Produkt evtl. vorhandenen Software-Schwachstellen besonders weit verbreitet und können daher, wenn sie ausgenutzt werden, zu hohen Gesamtschäden führen. Computer-Viren, Trojanische Pferde und andere Gefährdungen durch vorsätzliche Handlungen richten sich in vielen Fällen auf weit verbreitete Produkte.

**Konventionen für Namens-, Adress- und Nummernräume**

Innerhalb einer Institution existieren meist eine ganze Reihe unterschiedlicher Namens- und Nummernräume nebeneinander. Besonders populär sind diejenigen, die auch außerhalb der Behörde bzw. des Unternehmens verwendet werden, beispielsweise E-Mail-Adressen, DNS-Namen, Telefonnummern und Bezeichnungen von Organisationseinheiten. Aber auch rein interne Bezeichnungskonventionen, wie Inventarnummern, IP-Adressen und Ausweisnummern, spielen oft eine wichtige Rolle für die Organisation und das IT-Management.

Für einen reibungslosen Ablauf der Informationsverarbeitung und für die Administrierbarkeit der eingesetzten IT ist es erforderlich, dass ein übergreifendes Konzept für die verwendeten Namens- und Nummernräume erstellt wird. Bei der Konzeption sollten folgende Aspekte berücksichtigt werden:

- Möglichst wenig unterschiedliche Namens- und Nummernräume sollten parallel verwendet und gepflegt werden.
- Das Konzept muss Vergabe, Entzug, gegebenenfalls Sperrung von Namen und Nummern sowie das Zusammenspiel der einzelnen Namens- und Nummernräume regeln.
- Namen und Nummern, die nur für Teilbereiche (Organisationseinheiten, Teilnetze, Liegenschaften, usw.) benötigt werden, sollten möglichst aus allgemeinen, behörden- bzw. unternehmensweiten Namens- bzw. Nummernräumen abgeleitet werden.
- Die Struktur der verwendeten Namens- und Nummernräume sollte möglichst einfach, allgemein und ohne unnötige Ausnahmen sein, auch wenn dies bedeutet, dass die Bezeichnungen länger werden (z. B. mehr Ziffern enthalten). Anderenfalls besteht die Gefahr, dass die Bezeichnungen fehlinterpretiert oder von gängigen Produkten nicht verarbeitet werden können.
- Bei der Konzeption ist das absehbare mittelfristige Wachstum zu berücksichtigen, das durch den Namens- bzw. Nummernraum versorgt werden muss. In jedem Fall sind großzügige Reserven einzuplanen. Nachträgliche Erweiterungen oder Migrationen auf größere Namens- oder Nummernräume sind oft zeit- und kostenintensiv.
- Wenn Kollisionen, d. h. mehrfache Vergabe des gleichen Bezeichners oder der gleichen Nummer, durch das generelle Vergabesystem möglich sind, so ist im Konzept festzulegen, wie diese aufgelöst werden. Ein wichtiges Beispiel ist die Konvention *Vorname.Nachname* für E-Mail-Adressen. Hier muss im Konzept definiert werden, welche Adressen ersatzweise vergeben werden, wenn in der Behörde bzw. im Unternehmen zwei oder mehr Mitarbeiter mit gleichen Vor- und Nachnamen beschäftigt werden.

**Schnittstellendefinitionen für das Zusammenspiel der Komponenten**

Die Informationsverarbeitung geschieht in der Regel durch eine Vielzahl kleiner Verarbeitungsschritte, die durch geeignete Hardware- oder Software-Komponenten unterstützt werden. Der Datentransfer zwischen diesen Komponenten erfolgt in der Regel über Dateien, Datenbanken oder Netze.

Um einen reibungslosen IT-Betrieb gewährleisten zu können ist es daher erforderlich, die Schnittstellen für das Zusammenspiel der einzelnen Komponenten klar zu definieren. Alle Schnittstellendefinitionen sollten dokumentiert werden, sofern sie nicht von den verwendeten Komponenten her selbstverständlich sind.

Wichtige Aspekte von Schnittstellendefinitionen zwischen IT-Komponenten sind beispielsweise Datei- und Datenformate sowie Netzprotokolle. Um bei Bedarf einzelne Komponenten möglichst problemlos austauschen zu können (Investitionsschutz) und um auf praxisbewährte Lösungen zurückgreifen zu können, sollten so weit wie möglich Standardformate und Standardprotokolle verwendet werden, beispielsweise EDI, XML und HTTP.

Alle Änderungen an Schnittstellendefinitionen zwischen den verwendeten IT-Komponenten müssen dokumentiert und in Bezug auf Auswirkungen auf die Sicherheit des Informationsverbunds geprüft werden. Falls erforderlich ist das Sicherheitskonzept entsprechend zu ergänzen bzw. anzupassen.

Prüffragen:

- Sind grundlegende Sicherheitsprinzipien unter Beteiligung aller an IT-Planung und -Betrieb beteiligten Stellen definiert?
- Existieren dokumentierte Hausstandards für Hard- und Software?
- Werden bei der Überarbeitung des Hausstandards Kompatibilitätsaspekte mit älterer Hard- und Software berücksichtigt?
- Existiert ein übergreifendes Konzept für die verwendeten Namens- bzw. Nummernräume?
- Verfügt das übergreifende Konzept für die verwendeten Namens- bzw. Nummernräume über ausreichende Reserven für künftiges Wachstum?
- Existieren dokumentierte Schnittstellendefinitionen für die verwendeten IT-Komponenten?
- Sind die Zuständigkeiten für den Betrieb aller IT-Komponenten geregelt?
- Werden für Schnittstellen soweit möglich Standardformate bzw. -protokolle genutzt?

# M 2.215 Fehlerbehandlung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Alle Fehler, die IT-Systeme oder Kommunikationsverbindungen betreffen, müssen gemeldet und protokolliert werden. Hiervon sind natürlich alle Fehlermeldungen ausgenommen, die aufgrund von Plausibilitätsprüfungen angezeigt werden, also z. B. durch fehlerhafte Benutzereingaben hervorgerufen werden. Es muss gewährleistet sein, dass die gemeldeten Fehler schnellstmöglich behoben werden.

Die Untersuchung und Beseitigung von Fehlern sollte nur von entsprechend geschultem Personal durchgeführt werden. Alle Benutzer sollten darüber informiert sein, wer beim Auftreten von Fehlern oder Problemen mit IT-Systemen zu benachrichtigen ist. Außerdem sollten die Benutzer über Fehler, die das Arbeiten mit IT-Systemen beeinträchtigen können, informiert werden, ebenso über deren Behebung.

Die Protokolle über gemeldete Fehler sollten folgende Angaben enthalten:

- Bezeichnung und Versionsnummer der betroffenen IT-Systeme und Software,
- den Zeitpunkt der Meldung,
- eine Beschreibung, ob bzw. inwiefern die Nutzung der betroffenen IT-Systeme eingeschränkt ist,
- den Namen des für die Behebung Verantwortlichen sowie
- den Zeitpunkt der Fehlerbehebung.

In einigen Fällen kann es sinnvoll oder notwendig sein, aufgetretene Fehler nicht zu beheben, z. B. wenn kein zuverlässiger Patch vorhanden ist oder ein Ersatzteil nicht beschafft werden kann. Dann sollte im Protokoll vermerkt werden, ob die betroffene IT-Komponente mit Funktionseinschränkungen weiter betrieben werden kann.

Diese Protokolle sollten regelmäßig daraufhin überprüft werden, ob sie aktuell sind und ob alle gemeldeten Fehler behoben wurden.

Fehler sollten nur von den dafür benannten Verantwortlichen korrigiert werden. Die Fehlerbeseitigung muss im Rahmen der Sicherheitsrichtlinien der jeweiligen Institution erfolgen. Wenn für die Fehlerbehebung Patches oder Updates benötigt werden, sollten diese direkt vom Hersteller oder von vertrauenswürdigen Stellen bezogen werden (siehe auch M 4.107 *Nutzung von Hersteller- und Entwickler-Ressourcen*). Größere Korrekturmaßnahmen müssen zunächst auf vom Wirknetz getrennten Systemen getestet werden, da diese auch unerwünschte Nebeneffekte haben können. Nach der Fehlerbeseitigung müssen eventuell die geänderten IT-Systeme bzw. Komponenten erneut abgenommen und freigegeben werden (siehe M 2.62 *Software-Abnahme- und Freigabe-Verfahren*).

Prüffragen:

- Werden Fehler, die IT-Systeme oder Kommunikationsverbindungen betreffen, protokolliert und an die zuständige Stelle gemeldet?
- Wird eine schnellstmögliche Fehlerbehebung durch entsprechend benanntes und geschultes Personal gewährleistet?

- Falls ein Fehler nicht behoben werden kann: Wird im Protokoll vermerkt, ob und mit welchen Einschränkungen die betroffene IT-Komponente weiterbetrieben werden kann?
- Bei größeren Korrekturmaßnahmen: Werden Änderungen in einer gesonderten Testumgebung vorab getestet?

# M 2.216 Genehmigungsverfahren für IT-Komponenten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die Beschaffung, die Installation und der Betrieb von IT-Komponenten **aller Art** muss koordiniert und genehmigt sein. Es muss geregelt sein, wie IT-Komponenten abgenommen, freigegeben, installiert bzw. benutzt werden. Dies betrifft beispielsweise den Einsatz von Modems, Diskettenlaufwerken, Software und Mobiltelefonen. Eine entsprechende Vorgehensweise für den Bereich Standardsoftware ist in Baustein B 1.10 *Standardsoftware* beschrieben. Dabei wird der gesamte Lebenszyklus von Standardsoftware betrachtet: Erstellung eines Anforderungskataloges, Vorauswahl eines geeigneten Produktes, Test, Freigabe, Installation, Lizenzverwaltung und Deinstallation. Um eine analoge Vorgehensweise für andere IT-Komponenten zu entwickeln, kann sich ebenfalls an diesem Baustein orientiert werden.

Im Rahmen des Genehmigungsverfahrens von neuen IT-Komponenten müssen

- die generelle Funktionstüchtigkeit untersucht werden (siehe auch M 4.65 *Test neuer Hard- und Software*),
- deren Sicherheitseigenschaften bewertet werden,
- mögliche Sicherheitsrisiken, die durch diese IT-Komponenten entstehen könnten, untersucht und bewertet sowie weitestgehend behoben werden,
- alle ihre Sicherheitseigenschaften (sowohl die positiven als auch die negativen) sorgfältig dokumentiert werden,
- auf dieser Basis Installationsanweisungen erarbeitet werden.

Während des Genehmigungsverfahrens sollten außerdem Installations- bzw. Konfigurationsanleitungen erarbeitet werden, in denen auch alle sicherheitsrelevanten Einstellungen dokumentiert sind. Auch nach der Erstinstallation von IT-Komponenten müssen diese weitergepflegt werden (siehe auch M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Vor der Inbetriebnahme neuer IT-Komponenten sind (sofern erforderlich) die Administratoren bzw. die Benutzer in deren Anwendung zu schulen.

Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.

Prüffragen:

- Gibt es einen Prozess zur Koordination und Genehmigung bei Beschaffung, Installation und Betrieb von IT-Komponenten aller Art?
- Liegen aktuelle Installations- bzw. Konfigurationsanleitungen mit allen sicherheitsrelevanten Einstellungen vor?

# M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Grundsätzlich sollten Mitarbeiter natürlich sorgfältig mit allen Informationen umgehen. Darüber hinaus gibt es aber in vielen Bereichen Daten, die einen höheren Schutzbedarf haben oder besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten. Für diese gelten je nach ihrer Kategorisierung unterschiedliche Beschränkungen im Umgang mit ihnen. Daher ist es wichtig, alle Mitarbeiter auf die für diese Daten geltenden Restriktionen hinzuweisen (siehe auch M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Der Schutzbedarf von Daten wirkt sich natürlich unmittelbar auf alle Medien aus, auf denen diese gespeichert oder verarbeitet werden. Daten mit besonderem Schutzbedarf können in den unterschiedlichsten Bereichen anfallen, z. B. bei Fax oder E-Mail. Es sollte also in allen Bereichen Regelungen geben, in denen beispielsweise auch festgelegt ist, wer solche Daten lesen, bearbeiten bzw. weitergeben darf (siehe z. B. M 2.42 *Festlegung der möglichen Kommunikationspartner*). Dazu gehört auch die regelmäßige Überprüfung auf Korrektheit und Vollständigkeit der Daten (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).

Viele Informationen, aber auch Anwendungen, unterliegen Copyright-Vermerken oder Weitergaberestriktionen ("Nur für den internen Gebrauch"). Alle Mitarbeiter müssen darauf hingewiesen werden, dass weder Dokumente, noch Dateien oder Software ohne Berücksichtigung evtl. Copyright-Vermerke oder Lizenzbedingungen kopiert werden dürfen.

Ein besonderes Augenmerk muss auch auf alle Informationen gelegt werden, die die Grundlage für die Aufgabenerfüllung bilden. Dazu gehören alle geschäftsrelevanten Daten, also z. B. diejenigen Daten, bei deren Verlust die Institution handlungsunfähig wird, die die wirtschaftlichen Beziehungen zusammenarbeitender Unternehmen beeinträchtigen können oder aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann. Jede Behörde und jedes Unternehmen sollte eine Übersicht darüber haben, welche Daten als geschäftskritisch einzustufen sind. Neben den allgemeinen Sorgfaltspflichten können auch hier für diese Daten bei der Speicherung, Verarbeitung, Weitergabe und Vernichtung besondere Vorschriften und Regelungen gelten. Geschäftskritische Informationen müssen vor Verlust, Manipulation und Verfälschung geschützt werden. Längerfristig gespeicherte oder archivierte Daten müssen regelmäßig auf ihre Lesbarkeit getestet werden. Nicht mehr benötigte Informationen müssen zuverlässig gelöscht werden (siehe auch B 1.15 *Löschen und Vernichten von Daten*).

Prüffragen:

- Werden die Mitarbeiter regelmäßig auf den sorgfältigen Umgang mit Informationen hingewiesen?
- Werden alle Informationen entsprechend ihrem Schutzbedarf eingestuft?

# M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die IT-Komponenten, die innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind im Allgemeinen durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Häufig sollen aber IT-Systeme oder Datenträger auch außer Haus eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Um auch diese ausreichend schützen zu können, muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden.

Dabei muss festgelegt werden,

- welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten bzw. Datenträger außer Haus mitnehmen darf,
- welche grundlegenden IT-Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung sensitiver Daten, Aufbewahrung, etc.).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für extern eingesetzte IT-Komponenten hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollte für alle IT-Komponenten, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Bei größeren Institutionen, bei denen der Zutritt zu den Liegenschaften durch Pförtner bzw. Wachdienste kontrolliert wird, sollte überlegt werden, ob diese angewiesen werden sollten, in Stichproben zu überprüfen, inwieweit die Regelungen für die Mitnahme von Datenträgern und IT-Komponenten eingehalten werden.

Außerhalb der organisationseigenen Liegenschaften sind die Benutzer für den Schutz der ihnen anvertrauten IT verantwortlich. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen. Dazu gehören folgende Regeln:

- IT-Systeme müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden (siehe auch M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*).
- IT-Systeme wie Laptops oder Mobiltelefone und deren Anwendungen können im Allgemeinen durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten auch genutzt werden.
- IT-Systeme oder Datenträger, die sensitive Daten enthalten, sollten möglichst komplett verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*). Wenn IT-Systeme eine Verschlüsselungsfunktion ohne weitere Hilfsmittel ermöglichen, ist es

empfehlenswert, das diese Funktionen auch genutzt werden, wenn lediglich weniger sensitive Daten auf den IT-Systemen enthalten sind.
- Die Verwaltung, Wartung und Weitergabe von extern eingesetzten IT-Systemen sollte geregelt werden. Hierzu können beispielsweise Pools eingerichtet werden (siehe auch M 1.35 *Sammelaufbewahrung tragbarer IT-Systeme* bzw. M 2.190 *Einrichtung eines Mobiltelefon-Pools*).
- Es sollte protokolliert werden, wann und von wem welche IT-Komponenten außer Haus eingesetzt wurden.

Prüffragen:

- Gibt es Regelungen für die Mitnahme von Datenträgern und Komponenten?
- Werden die Benutzer von extern eingesetzten IT-Komponenten auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Hoher Schutzbedarf bezüglich Vertraulichkeit: Werden mobile IT-Systeme oder Datenträger durch vollständige Verschlüsselung der Datenträger geschützt?
- Werden die angebotenen Authentisierungsmechanismen genutzt, wenn IT-Komponenten extern eingesetzt werden?

# M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die Informationsverarbeitung muss kontinuierlich in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden, um einen ordnungsgemäßen IT-Betrieb gewährleisten zu können. Dazu gehören:

- eine aktuelle Dokumentation aller vorhandenen IT-Systeme und deren Konfiguration (siehe M 2.25 *Dokumentation der Systemkonfiguration*),
- die Dokumentation der auf den jeweiligen IT-Systemen eingerichteten Benutzer und deren Rechteprofile (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*), dies umfasst auch eine Beschreibung und Begründung aller Einschränkungen bei der Nutzung von IT-Systemen (Rechte und Ressourcen),
- die neu hinzugekommenen Hard- und Softwarekomponenten müssen in der Systemdokumentation aufgeführt werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*),
- die Dokumentation aller sicherheitsrelevanten Abläufe wie der Datensicherung (siehe M 6.37 *Dokumentation der Datensicherung*) oder der Vernichtung von Datenträgern,
- die Dokumentation der Wartungsmaßnahmen (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*),
- eine Beschreibung aller gefundenen und behobenen Fehler (siehe M 2.215 *Fehlerbehandlung*).

Die Benennung der Systemverantwortlichen (siehe M 2.26 *Ernennung eines Administrators und eines Vertreters* sollte ebenfalls schriftlich erfolgen und den Benutzern bekannt gegeben werden.

Für Problemfälle sollte dokumentiert sein, wer helfen kann und wo Informationen zu finden sind (M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*).

Prüffragen:

- Wird die Informationsverarbeitung in allen Phasen, allen Anwendungen und allen Systemen dokumentiert?
- Gibt es Regelungen für die Dokumentation der Informationsverarbeitung?

# M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Um IT-Systeme bzw. System-Komponenten und Netze nutzen zu können bzw. um dort gespeicherte Informationen abrufen zu können, muss die Zugriffs- bzw. Zugangskontrolle geregelt sein. Neben den an den einzelnen IT-Komponenten einzurichtenden Zugriffs- bzw. Zugangskontrollen sollte eine übergreifende Richtlinie hierzu existieren, in der die Grundsatzfragen geregelt sind. Die Regelungen zur Zugriffs- bzw. Zugangskontrolle müssen den Schutzbedarf der Behörde bzw. des Unternehmens widerspiegeln. Insbesondere ist hier auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z. B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen, zu verweisen.

Es empfiehlt sich, dabei Standard-Rechteprofile für nutzungsberechtigte Personen aufgrund ihrer Funktionen und Aufgaben festzulegen (siehe auch M 2.8 *Vergabe von Zugriffsrechten*). Die Benutzerrechte für Zugriffe auf Dateien und Programme müssen abhängig von der jeweiligen Rolle, dem Need-to-Know und der Sensitivität der Daten definiert sein. Falls Rechte vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden.

Die Richtlinien für die Zugriffs- bzw. Zugangskontrolle sollte allen Verantwortlichen für IT-Anwendungen vorliegen. Darauf aufbauend können dann Zugriffsregelungen für die einzelnen IT-Systeme abgeleitet und eingerichtet werden.

Für jedes einzelne IT-Systeme und jede IT-Anwendung sollten schriftliche Zugriffsregelungen und die Dokumentation der Einrichtung von Benutzern und der Rechtevergabe vorhanden sein (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*). Hierbei müssen die system- bzw. anwendungsspezifischen Besonderheiten und Sicherheitsanforderungen berücksichtigt werden. Verantwortlich für die Erstellung und Aktualisierung der system- bzw. anwendungsspezifischen Vorgaben sind die IT-Verantwortlichen.

Werden an Mitarbeiter besonders weitgehende Rechte vergeben (z. B. an Administratoren), so sollte dies möglichst restriktiv erfolgen. Hierbei sollte zum einem der Kreis der privilegierten Benutzer möglichst eingeschränkt werden und zum anderen nur die für die Durchführung der Arbeit benötigten Rechte vergeben werden (siehe auch M 2.38 *Aufteilung der Administrationstätigkeiten*). Für alle Aufgaben, die ohne erweiterte Rechte durchgeführt werden können, sollten auch privilegierte Benutzer unter Accounts mit Standard-Rechten arbeiten.

Der Zugriff auf alle IT-Systeme oder Dienste muss durch Identifikation und Authentikation des zugreifenden Benutzers oder IT-Systems abgesichert werden. Beim Zugriff aus externen Netzen sollten starke Authentisierungsverfahren eingesetzt werden, also solche die z. B. auf dem Einsatz von Einmalpasswörtern oder dem Besitz von Chipkarten basieren.

Beim Anmeldevorgang sollten keine Informationen über das IT-System oder den Fortschritt der Anmeldeprozedur angezeigt werden, bis dieser erfolgreich abgeschlossen ist. Es sollte dabei darauf hingewiesen werden, dass der Zugriff nur autorisierten Benutzern gestattet ist. Die Authentikationsdaten dürfen erst dann überprüft werden, wenn sie vollständig eingegeben wurden.

Weitere Anforderungen an die Authentikationsmechanismen finden sich in M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*.

Prüffragen:

- Existieren dem Schutzbedarf der Organisation angemessene Regelungen zur Zugangs- und Zugriffskontrolle?
- Existieren Standard-Rechteprofile, die den Funktionen und Aufgaben der Nutzer entsprechen?
- Existieren schriftliche Zugriffsregelungen sowie eine Dokumentation der Benutzereinrichtung und der Rechtevergabe?
- Wird der Zugriff auf alle IT-Systeme und Dienste durch Identifikation und Authentikation des zugreifenden Benutzers oder IT-Systems abgesichert?
- Werden Authentisierungsdaten erst nach vollständiger Eingabe überprüft?

# M 2.221 Änderungsmanagement

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Änderungsmanager, Fachverantwortliche

Bei der Komplexität heutiger IT-Systeme können bereits kleine Änderungen an laufenden Systemen zu Sicherheitsproblemen führen, z. B. durch unerwartetes Systemverhalten oder Systemausfälle.

In Bezug auf Informationssicherheit ist es Aufgabe des Änderungsmanagements, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen an IT-Systemen ergeben. Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, so sind die Auswirkungen auf die Sicherheit des Gesamtsystems zu untersuchen. Änderungen an einem IT-System dürfen nicht zu einer Verringerung der Effizienz von einzelnen Sicherheitsmaßnahmen und damit einer Gefährdung der Gesamtsicherheit führen.

Daher sollte es Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten geben (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten geplant, getestet, genehmigt und dokumentiert werden. Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Applikationen, neue Hardware, neue Netzwerkverbindungen, Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, Aufrüstung der Hardware, usw.),
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme, Benutzergruppen),
- räumliche Änderungen, z. B. nach einem Umzug.

Bevor Änderungen genehmigt und durchgeführt werden, muss durch Prüfung und Test der geplanten Aktionen sichergestellt werden, dass das Sicherheitsniveau während und nach der Änderung erhalten bleibt. Wenn Risiken, insbesondere für die Verfügbarkeit, nicht ausgeschlossen werden können, muss die Planung auch eine Rückfall-Lösung vorsehen und Kriterien vorgeben, wann diese zum Tragen kommen soll.

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind zu dokumentieren. Dies gilt sowohl in der Betriebs- als auch in einer Testumgebung.

Beim Änderungsmanagement ist das Berechtigungskonzept zur Durchführung von Änderungen ein wichtiger Punkt:

- Nur diejenigen, die Änderungen durchführen dürfen, sollten Zugriffsberechtigungen auf die dafür relevanten Systembereiche haben.
- Es sollte Mechanismen geben, die sicherstellen, dass alle wesentlichen Änderungen vorher abgestimmt wurden.

**Hinweis:** Bei der Durchführung von Änderungen sollte immer beachtet werden, dass Änderungen eines IT-Systems oder seiner Einsatzbedingungen

- Änderungen in der Umsetzung einzelner Sicherheitsmaßnahmen,
- die Erstellung eines neuen Sicherheitskonzepts oder sogar

- die Überarbeitung der organisationsweiten Leitlinie zur Informationssicherheit

erforderlich machen können. Bei größeren Änderungen sollte daher das Informationssicherheitsmanagement involviert werden.

Prüffragen:

- Gibt es Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten?
- Ist geregelt, dass bei der Durchführung von Änderungen auch Sicherheitsaspekte berücksichtigt werden müssen?
- Werden alle Änderungen geplant, getestet, genehmigt und dokumentiert?
- Werden Rückfall-Lösungen erarbeitet, bevor Änderungen durchgeführt werden?
- Wird bei größeren Änderungen das Informationssicherheitsmanagement beteiligt?

# M 2.222 Regelmäßige Kontrollen der technischen IT-Sicherheitsmaßnahmen

Diese Maßnahme ist mit Version 2006 entfallen.

# M 2.223 Sicherheitsvorgaben für die Nutzung von Standardsoftware

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

In den meisten Büroumgebungen wird für die typischen Büroaufgaben Standardsoftware eingesetzt. Dazu gehören z. B. Textverarbeitungsprogramme, Tabellenkalkulationen, Büro-Kommunikationssysteme, E-Mail-Programme und Datenbanken. Da diese häufig komplett von einem Anbieter gekauft werden, wird hier auch von Office-Paketen gesprochen. Durch die hohe Verbreitung gleichartiger Software können Sicherheitslücken in diesen Programmen große Auswirkungen haben, da sie an vielen IT-Systemen ausgenutzt werden können und sich Schadprogramme sehr schnell weiterverbreiten. Ein typisches Beispiel hierfür sind Makro-Viren (siehe G 5.43 *Makro-Viren*).

Um solche Probleme vermeiden bzw. reduzieren zu können, sollten daher Sicherheitsrichtlinien bei der Nutzung von Standardsoftware festgelegt werden.

Um den Einsatz von Standardsoftware wie Office-Pakten abzusichern, sind seitens IT-Betrieb und Sicherheitsmanagement die folgenden Punkte zu beachten:

- Sicherheit der Einsatzumgebung

Die Sicherheit aller Office-Pakete und anderer Standardsoftware hängt von der Sicherheit der eingesetzten Hardware und Betriebssysteme ab. Die meisten Hersteller von Office-Anwendungen bieten auf ihren Webseiten Empfehlungen für eine sichere Konfiguration des Produktes sowie Patches, um identifizierte Schwachstellen zu beheben. Diese sollten genutzt werden.

Außerdem werden Office-Programme auch von Cloud Computing Dienstleistern angeboten. Diese Programme laufen clientseitig in der Ausführungsumgebung des verwendeten Internet-Browsers ab. Grundlegend für die Sicherheit solcher Anwendungen ist neben der Sicherheit der Hardware und des Betriebssystems somit auch die Sicherheit der Internetumgebung und des externen Anbieters (siehe auch M 2.460 *Geregelte Nutzung von externen Dienstleistungen*).

- Add-Ins und Makros

Hierbei handelt es sich um Erweiterungen, die zum Teil von Drittanbietern stammen und von Office-Komponenten bei Bedarf ausgeführt werden, z. B. um Hypertextelemente richtig zu verarbeiten und auszugeben. Es sollten nur solche Add-Ins installiert werden, die von vertrauenswürdigen Herausgebern stammen und vom IT-Betrieb getestet und freigegeben wurden. Dabei ist darauf zu achten, dass die Konfigurationsoptionen in manchen Office-Anwendungen standardmäßig wenig restriktiv voreingestellt sind, sodass Add-Ins grundsätzlich als vertrauenswürdig gelten. Die Konfigurationen sind entsprechend anzupassen. Außerdem sollten alle Add-Ins fortlaufend von den Originalseiten der Anbieter aktualisiert werden, um sicherheitstechnisch auf dem neuesten Stand zu bleiben.

Makros erlauben die Automatisierung von Vorgängen in Anwendungen, stellen aber immer wieder eine Gefährdung dar, da sie Schadcode enthalten können. Ein typisches Ziel von Angriffen solcher Makroviren ist z. B. die Infektion der Standard-Dokumentvorlage, da sie beim Starten der entsprechenden Office-Anwendung automatisch geladen wird. Daher sollten Benutzer auf die Problematik hingewiesen und darüber informiert werden, wie sie Makro-Schad-

programmen vorbeugen können (siehe M 2.224 *Vorbeugung gegen Schadprogramme*). Dazu gehört insbesondere, dass Makros nicht automatisch ausgeführt werden sollten. ActiveX-Elemente sollten nach Möglichkeit deaktiviert werden.

**Sicherheitsmaßnahmen im laufenden Betrieb**

Office-Software und andere Standardsoftware sollte nie mit Administratorrechten gestartet werden. Es sollten nur solche Dateien direkt in den Anwendungen geöffnet werden, deren Herkunft als vertrauenswürdig eingeschätzt wird. Bevor Dateien aus externen Quellen geöffnet werden, müssen sie vorab durch ein aktuelles Virenschutzprogramm überprüft werden.

Für den Austausch von Dokumenten sollten diese möglichst digital signiert und/oder verschlüsselt werden.

Standardsoftware ist im Allgemeinen nicht auf ein hohes Sicherheitsniveau ausgelegt. Alle Mitarbeiter sollten daher darauf hingewiesen werden, dass besonders schutzbedürftige Informationen nicht ohne weitere Sicherheitsmaßnahmen auf einem Standard-Büroarbeitsplatz verarbeitet werden sollten. Einige der Standardprodukte bieten aber trotzdem eine Reihe von Sicherheitsfunktionen an, die aber meist deutlich weniger Sicherheit bieten als spezielle Sicherheitsprodukte. Die Benutzer sollten über diese Sicherheitsfunktionen und deren Wirksamkeit informiert werden (siehe auch M 4.30 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen). Dabei ist vor allen Dingen sicherzustellen, dass die Benutzer sich nicht in einer falschen, trügerischen Sicherheit wiegen und dass die Nutzung dieser Sicherheitsfunktionen keine Sicherheitslücken öffnet. Benutzer sollten darüber informiert werden, dass Office-Produkte nicht für jeden beliebigen Einsatzzweck geeignet sind.

Daneben bieten Office-Pakete häufig Funktionen, die den Austausch von Informationen erleichtern sollen, die aber häufig bereits in der Konzeption große Sicherheitsprobleme mit sich bringen.

**Beispiele:**

- Nutzung gemeinsamer Terminkalender
  Um die Koordination innerhalb von Arbeitsgruppen zu erleichtern, lassen sich die meisten elektronischen Terminkalender untereinander vernetzen. Neben vielen Vorteilen bringt dies aber auch einige Probleme mit sich. So will nicht jeder Mitarbeiter alle seine Termine den Kollegen offen legen. Darauf haben die Hersteller reagiert, in dem sie hier die Möglichkeit bieten, anderen nur die freien bzw. belegten Zeiten anzuzeigen. Viele Mitarbeiter glauben aber zum einen, dass es einen schlechten Eindruck macht, wenn hier viel freie Zeit angezeigt wird, und befürchten zum anderen, dass jede freie Minute von Kollegen mit Terminen besetzt wird. Dies führt dann dazu, dass große Zeiträume auf Vorrat blockiert werden.
  Daneben kann es auch zu anderen Problemen kommen, z. B. durch zu großzügige Rechtevergabe.
  Es sollte daher Richtlinien für die Verwendung vernetzter Terminkalender und die hierbei zu beachtenden Zugriffsrechte geben. Diese sollten frühzeitig mit dem Personal- bzw. Betriebsrat abgestimmt werden. Bei der Einführung von vernetzten Terminkalendern sollten außerdem alle Mitarbeiter in den richtigen Umgang damit eingewiesen werden.
- automatischer Start von CD-ROMs
  Unter allen neueren Windows-Betriebssystemen können CD-ROMs automatisch erkannt und gestartet werden. Dadurch können auch Schadpro-

gramme wie Viren oder Trojanische Pferde auf den Rechner gelangen werden. Die automatische CD-ROM-Erkennung sollte daher ausgeschaltet werden (siehe M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*).

- OLE (Object Linking And Embedding, Dienst zum Verknüpfen und Einbetten von Objekten)
  Über OLE-Funktionen können Objekte in Dateien eingebettet werden. Diese werden in vielen Office-Produkten benutzt, um Informationen anderen Programmen zur Verfügung zu stellen. Hierüber kann beispielsweise eine in Excel erstellte Tabelle in einem Word-Dokument eingebettet werden. Damit werden aber nicht nur die in dem Tabellenausschnitt dargestellte Informationen, sondern unter Umständen alle in der Excel-Datei enthaltenen Informationen in die Word-Datei übertragen. Wenn die Word-Datei dann weitergegeben wird, kann der Empfänger dann auch die Excel-Datei einsehen und sogar verändern, auch wenn diese durch ein Passwort lese- oder schreibgeschützt war.
  Um dies zu verhindern, sollte in diesem Beispiel die Tabelle als Text in die Word-Datei kopiert werden. Nur wenn die Ursprungs-Excel-Datei keine anderen Informationen enthält, als solche, die weitergegeben werden sollen, sollte sie in einer andere Datei eingebettet werden. Dies kann z. B. durch Anlegen einer neuen Excel-Datei erreicht werden (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).
- PostScript
  PostScript ist eine Seitenbearbeitungssprache, die beschreibt, wie Informationen exakt auf Papier oder in entsprechenden Anzeige-Programmen dargestellt werden sollen. Da der PostScript-Befehlssatz neben Anzeigeoptionen auch über (eingeschränkte) Anweisungen verfügt, um Dateien zu ändern, kann es zu Problemen ähnlich wie bei Makro-Viren kommen. Bei Anzeige-Programmen für PostScript handelt es sich um Interpreter, die die PostScript-Sprache abarbeiten. Ab Level 2.0 der PostScript-Spezifikation gibt es auch PostScript-Befehle, um Dateien zu schreiben. Dadurch ist es möglich, PostScript-Dateien zu erzeugen, die während der Bearbeitung durch einen Interpreter, auch bereits bei der Anzeige am Bildschirm, andere Dateien modifizieren, löschen oder umbenennen können.
  Viele der verfügbaren Anzeige-Programme können so aufgerufen werden, dass die Anweisungen aus den zu öffnenden PostScript-Dateien keine Informationen im Dateisystem nach sich ziehen können. Beispielsweise kann bei dem weitverbreiteten Programm *ghostscript* (*gs*) die Schreibmöglichkeiten auf Dateien im Dateisystem mit der Option *-dSAFER* abgeschaltet werden. Generell sollte darauf geachtet werden, dass die eingesetzten Anzeige-Programme nur so aufgerufen werden, dass keine ungewollten Änderungen im Dateisystem vorgenommen werden können.
- PDF (Portable Document Format)
  Auch PDF-Dateien können präpariert sein und Schadcode enthalten, der Sicherheitslücken ausnutzt. In PDF-Dateien lassen sich Funktionen wie Programmaufrufe einbetten, die ein Sicherheitsrisiko für die Dateien des lokalen IT-Systems darstellen. Häufig wird für solche Angriffe JavaScript verwendet. Vor allem ältere Versionen von PDF-Anwendungen sind für eine solche Infiltration anfällig. Häufig werden die Benutzer dafür auf eine manipulierte Webseite gelockt, wo dann eine präparierte PDF-Datei im Hintergrund geladen wird. Mit dem in der Datei versteckten Code wird Schadsoftware auf dem Rechner des Benutzers installiert. Dafür muss die Datei muss nicht einmal manuell geöffnet werden.
  Antiviren-Programme erkennen infizierte PDF-Datei in vielen, aber nicht in allen Fällen, da die Angreifer den Schadcode ständig variieren. Umso

wichtiger ist es, die eingesetzten Anwendungen regelmäßig auf Aktualität zu prüfen und Sicherheitsupdates schnell zu installieren.
Adobe hat im Adobe Reader ab Version Zehn (Adobe Reader X) eine Sandbox (oder "Geschützter Modus") integriert, um diesen Angriffen entgegen zu wirken. Daher sollten Anwender, die zur Betrachtung und Bearbeitung von PDF-Dokumenten Adobe Reader nutzen, mindestens Version Adobe Reader X einsetzen und den "Geschützten Modus" nutzen.

Aktive Inhalte in PDFs eröffnen Sicherheitsrisiken, werden aber nur selten tatsächlich benötigt. Daher sollte JavaScript in den PDF-Anzeige-Programmen deaktiviert werden.

Die am meisten verwendeten PDF-Betrachter sind Adobe Reader bzw. Acrobat. An Marktführern orientieren sich auch Schadsoftware-Entwickler. Daher kann es auch sinnvoll sein, weniger verbreitete PDF-Betrachter einzusetzen oder zumindest vorzuhalten, um bei akuten Warnmeldungen ausweichen zu können.

- Schnellspeicherung unter Word
  Word besitzt die Möglichkeit der Schnellspeicherung von erstellten Texten. Dies führt dazu, dass nur die aktuell vorgenommenen Änderungen an einem Dokument gespeichert werden. Dieser Vorgang nimmt nicht so viel Zeit in Anspruch wie ein vollständiger Speichervorgang, bei dem Word das vollständige überarbeitete Dokument speichert. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung.
  Der entscheidende Nachteil der Schnellspeicherung ist aber, dass die Datei unter Umständen Textfragmente enthalten kann, die der Verfasser nicht weitergeben möchte.
  Grundsätzlich sollte daher die Option "Schnellspeicherung zulassen" abgeschaltet werden. Des Weiteren sollte die Option "Erstellung einer Sicherungskopie" aktiviert sein. Das System sollte regelmäßig durch Löschen der nicht mehr benötigten Sicherungskopien gesäubert werden.
  Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:
- Sobald die Bearbeitung eines Dokuments abgeschlossen worden ist.
- Bevor eine Aufgabe ausgeführt wird, die viel Speicherplatz in Anspruch nimmt, z. B. die Suche nach Text oder das Kompilieren eines Indexes.
- Bevor der Dokumenttext in eine andere Anwendung übertragen wird.
- Bevor das Dokument in ein anderes Dateiformat konvertiert wird.

Um gegen Konzeptionsschwächen und bekannt gewordene Sicherheitslücken rechtzeitig Maßnahmen ergreifen zu können, sollte sich der Administrator bzw. das Sicherheitsmanagement regelmäßig über solche Probleme informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Prüffragen:

- Sind die Benutzer über die Möglichkeiten und Grenzen von Sicherheitsfunktionen der eingesetzten Software und der genutzten Speicherformate informiert?
- Werden Softwaremerkmale, die den Informationsaustausch vereinfachen sollen von den Sicherheitsvorgaben berücksichtigt?
- Gibt es Sicherheitsrichtlinien für die Nutzung von Standardsoftware?

# M 2.224 Vorbeugung gegen Schadprogramme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Einen absoluten Schutz gegen Schadprogramme gibt es nicht. Daher ist es besonders wichtig, alle Benutzer immer wieder über die Bedrohung durch Schadprogramme aufzuklären.

Weiterhin müssen im Sicherheitskonzept gegen Schadprogramme alle IT-Systeme erfasst werden, die innerhalb einer vernetzten Struktur gegen Schadprogramme geschützt werden müssen. Dabei sollten Viren-Schutzprogramme so platziert werden, dass alle möglichen Infektionswege abgedeckt sind (siehe auch M 2.154 *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme*).

Durch Beachtung einiger wichtiger Verhaltensregeln und Empfehlungen kann die Gefahr eines Befalls durch Schadprogramme reduziert werden:

- Es sollten regelmäßig aktualisierte Viren-Schutzprogramme eingesetzt werden.
- Alle von Dritten erhaltenen Dateien und Programme sollten vor der Aktivierung auf möglicherweise enthaltene Schadprogramme überprüft werden. Diese Überprüfung sollte möglichst automatisiert erfolgen.
- Schadprogramme können in aktive Inhalte von Web-Seiten (z. B. Java, JavaScript und besonders ActiveX) eingebettet sein. Eine Ausführung ist damit möglich, ohne dass der Benutzer dies bemerkt. Es sollte überlegt werden, den Internet-Browser so zu konfigurieren, dass beispielsweise aktive Inhalte gar nicht erst auf den eigenen Rechner geladen werden können oder nur von vertrauenswürdigen Seiten stammen dürfen.
- Schadprogramme verfolgen häufig den Zweck, Passwörter oder andere Zugangsdaten auszuspähen. Daher sollten Passwörter nie auf den IT-Systemen abgespeichert werden.
- Absender-Angaben in E-Mails ohne entsprechende zusätzliche Sicherheitsmechanismen sind nicht vertrauenswürdig. Absender-Namen oder Reply-Adressen lassen sich sehr einfach fälschen. Selbst wenn die Absender-Angaben korrekt sind und der Absender vertrauenswürdig ist, kann nicht davon ausgegangen werden, dass dieser wissentlich die E-Mail geschickt hat. Ein Schadprogramm auf seinem Rechner kann das Adressbuch ausgelesen und automatisch E-Mails generiert haben. Es sollten daher keine E-Mail-Anhänge oder andere empfangene Dateien geöffnet werden, wenn die E-Mail eine merkwürdige Betreffzeile oder einen ungewöhnlichen Nachrichtentext enthält. Im Zweifelsfall sollte bei den Kommunikationspartnern nachgefragt werden, ob sie die Nachrichten wirklich geschickt haben.
- Beim Austausch von E-Mails sollten möglichst digitale Signaturen eingesetzt werden, um die Echtheit und Korrektheit der E-Mail-Inhalte überprüfen zu können (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).
- Viele Daten und Programme sind über verschiedene Quellen verfügbar, z. B. über Mirror-Server im Internet oder über Zeitschriften-CD-ROMs. Daten und Programme sollten grundsätzlich nur von vertrauenswürdigen Quellen geladen werden, also insbesondere von den Original-Web-Seiten oder Original-Datenträgern des Erstellers (siehe auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

- Grundsätzlich sollten alle Programme vor Installation und Freigabe auf Testsystemen hinsichtlich der Funktionssicherheit und hinsichtlich eines Befalls durch Schadprogramme überprüft werden (siehe dazu auch M 4.65 *Test neuer Hard- und Software*).
- Bei CERTs bzw. anderen sicherheitsbezogenen Informationsdiensten sollte regelmäßig recherchiert werden, ob eingesetzte Programme dahingehend aufgefallen sind, dass sie Daten vom IT-System des Benutzers ohne dessen Wissen an andere IT-Systeme übertragen (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Von solchen Problemen waren in der Vergangenheit nicht nur einige Anwendungen, sondern auch bestimmte Programmbibliotheken betroffen. Den Programmierern, die diese Bibliotheken eingesetzt hatten, war teilweise nicht bekannt, dass dadurch Benutzerinformationen an Dritte weitergegeben wurden.
- Bei der Installation von Programmen sollten die Programmhinweise und Nutzungsbedingungen sorgfältig durchgelesen werden. Oftmals wird in diesen sogar (mehr oder weniger deutlich) darauf hingewiesen, dass bei der Verwendung des Programms bestimmte Benutzer- oder Systemdaten erhoben und weitergegeben werden.
- Die meisten modernen Betriebssysteme enthalten heute bereits integrierte Paketfilter. Diese Paketfilter-Funktionen sollten auf möglichst allen IT-Systemen aktiviert werden. Insbesondere für Windows-Betriebssysteme sind außerdem spezielle Personal-Firewalls erhältlich, die neben der reinen Paketfilter-Funktion auch weitere Sicherheitsfunktionen bieten, beispielsweise Registry- oder Prozess-Monitoring. Es sollte geprüft werden, auf welchen IT-Systemen der Einsatz einer zusätzlichen Personal-Firewall erforderlich ist.
- Die Benutzerrechte auf Clients und anderen Endgeräten sollten möglichst stark eingeschränkt werden. Dazu gehört auch, dass möglichst nur solche Anwendungen betrieben werden, für die keine Administratorrechte benötigt werden. Je mehr Rechte ein Anwender hat, desto höher ist die Wahrscheinlichkeit, dass ein auf diesem Weg eingedrungenes Schadprogramm funktioniert und sich tiefer im System einnisten kann.
- Die Absicherung eines Netzes darf sich nicht auf die Außengrenzen beschränken. Zum Schutz vertraulicher Daten müssen auch intern sichere Teilnetze gebildet werden, die möglichst gut gegen andere Netzbereiche abgeschottet sind. Eine geeignete Netzsegmentierung mit ausreichendem Schutz interner Netzgrenzen schränkt die Möglichkeiten von Schadprogrammen ein.
- Wenn die Abwehr eines Schadprogramms nicht gelungen ist und sich eine Schadfunktion aktivieren konnte, sollte sie möglichst schnell anhand ihres Verhaltens entdeckt werden. Die größten Chancen bestehen dabei durch eine genaue Beobachtung des Netzes.
  Netzaktivitäten und E-Mail-Verkehr sollten daher regelmäßig beobachtet und protokolliert werden. Häufig zeigt sich die Aktivität von Schadprogrammen durch unerwünschten Datenverkehr. In Frage kommen hier insbesondere ungewöhnlich große übertragene Datenmengen, wiederholte Übertragungen in bestimmten Zeitintervallen oder eine auffällig ansteigende Anzahl zu übertragender E-Mails. Intrusion Detection Systeme können hier die automatische Suche nach solchen Ungewöhnlichkeiten unterstützen.
- Im Hinblick auf vorbeugende Maßnahmen gegen Keylogger ist eine Besonderheit zu beachten. Da der Vertrieb von Keyloggern in vielen Ländern legal ist, nehmen Hersteller von Viren-Schutzprogrammen sie häufig nicht in ihre Signatur-Datenbank auf. Hinsichtlich der tatsächlichen Erkennung von Keyloggern durch das eingesetzte Viren-Schutzprogramm sollte Klar-

heit bestehen. Im Zweifelsfall sollte zusätzlich ein auf das Auffinden von Keyloggern spezialisiertes Programm eingesetzt werden.
- Nicht nur reguläre Programm-Dateien können Schadprogramme enthalten, sondern auch Dateien von Anwendungsprogrammen, die eine Makro-Sprache verwenden ("Makro-Viren"). Betroffen sind unter anderem die gängigen Office-Programme (wie Textverarbeitung oder Tabellenkalkulation) der meisten Hersteller. Viele Anwendungsprogramme bieten Einstellungsoptionen, die den Schutz vor Makro-Schadprogrammen erhöhen. Beispielsweise kann beim Öffnen von Dateien die Ausführung von Makros standardmäßig verhindert werden. Zu diesem Thema sollten die entsprechenden Empfehlungen der Hersteller von Anwendungsprogrammen geprüft und mit den eigenen Sicherheitsanforderungen abgeglichen werden. Als weitere Vorbeugung sollten Benutzer darauf hingewiesen werden, wie sie die automatische Ausführung möglicherweise vorhandener Makros verhindern können. Dies ist leider für fast alle Programme und Versionen unterschiedlich und auch nicht immer zuverlässig.

Prüffragen:

- Wird ein aktuelles Viren-Schutzprogramm eingesetzt und werden dessen Schadprogramm-Signaturen in kurzen Zeitabständen aktualisiert?
- Werden empfangene Daten und Programme vor deren Aktivierung auf Schadprogramme überprüft?
- Ist sichergestellt, dass Benutzer nur die Berechtigungen erhalten, die sie für ihre Arbeit tatsächlich benötigen?
- Werden Netzaktivitäten hinreichend beobachtet, um auffälliges Verhalten schnellstmöglich zu entdecken?
- Sind die Paketfilter-Funktionen auf allen gefährdeten IT-Systemen aktiviert?
- Ist ein ausreichender Schutz vor Keyloggern gewährleistet?
- Sind die Benutzer über die sie betreffenden Verhaltensregeln zum Schutz vor Schadprogrammen informiert?

# M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Mitarbeiter

Um zu einer umfassenden Gesamtsicherheit zu gelangen, ist die Beteiligung aller Mitarbeiter einer Organisation an der Umsetzung der erforderlichen Sicherheitsmaßnahmen erforderlich. Für alle Informationen, Anwendungen und IT-Komponenten muss daher festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Hierfür sollte immer eine konkrete Person (inklusive Vertreter) und keine abstrakte Gruppe benannt werden, damit die Zuständigkeit jederzeit deutlich erkennbar ist. Bei komplexeren Informationen, Anwendungen und IT-Komponenten sollten alle Verantwortlichen und deren Vertreter namentlich genannt sein.

Umgekehrt sollten natürlich alle Mitarbeiter wissen, für welche Informationen, Anwendungen und IT-Komponenten sie in welcher Weise verantwortlich sind.

Jeder Mitarbeiter ist dabei für das verantwortlich, was in seinem Einflussbereich liegt, es sei denn, es ist explizit anders geregelt. Beispielsweise ist die Leitungsebene der Organisation verantwortlich für alle grundsätzlichen Entscheidungen bei der Einführung einer neuen Anwendung, der Leiter IT zusammen mit dem Informationssicherheitsmanagement für die Ausarbeitung von Sicherheitsvorgaben für die IT-Komponenten,, die Administratoren für deren korrekte Umsetzung und die Benutzer für den sorgfältigen Umgang mit den zugehörigen Informationen, Anwendungen und Systemen.

Die Fachverantwortlichen als die "Eigentümer" von Informationen und Anwendungen müssen sicherstellen, dass

- der Schutzbedarf der Informationen, Anwendungen und IT-Komponenten korrekt festgestellt wurde,
- die erforderlichen Sicherheitsmaßnahmen umgesetzt werden,
- dies regelmäßig (z. B. täglich, wöchentlich, monatlich) überprüft wird,
- die Aufgaben für die Umsetzung der Sicherheitsmaßnahmen klar definiert und zugewiesen werden,
- der Zugang bzw. Zugriff zu den Informationen, Anwendungen und IT-Komponenten geregelt ist,
- die Informationssicherheit gefährdende Abweichungen schriftlich dokumentiert werden.

Die Fachverantwortlichen müssen zusammen mit dem Informationssicherheitsmanagement entscheiden, wie mit eventuellen Restrisiken umgegangen wird.

Prüffragen:

- Ist für alle Informationen, Anwendungen und IT-Komponenten klar geregelt, wer für diese und deren Sicherheit verantwortlich ist?

- Sind alle Mitarbeiter darüber informiert, für welche Informationen, Anwendungen und IT-Komponenten sie in welcher Weise verantwortlich sind?

# M 2.226 Regelungen für den Einsatz von Fremdpersonal

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter Personal, Leiter IT

Häufig wird in Behörden oder Unternehmen auf externe Unterstützung zurückgegriffen, falls die entsprechenden personellen Ressourcen nicht im eigenen Haus vorhanden sind. Dies kann im Extremfall dazu führen, dass Fremdpersonal über so lange Zeiträume im eigenen Haus eingesetzt wird, dass viele Mitarbeiter schon nicht mehr genau wissen, ob es sich um eigene oder externe Mitarbeiter handelt.

Externe Mitarbeiter, die über einen längeren Zeitraum in einer oder für eine Organisation tätig sind und eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten (siehe auch M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Beim Einsatz von externen Mitarbeiter muss außerdem auf jeden Fall sichergestellt sein, dass sie bei Beginn ihrer Tätigkeit - ähnlich wie eigene Mitarbeiter - in ihre Aufgaben eingewiesen werden (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*). Sie sind - so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist - über hausinterne Regelungen und Vorschriften zur IT-Sicherheit sowie die organisationsweite IT-Sicherheitspolitik zu unterrichten. Dies gilt in besonderem Maß, wenn sie innerhalb der Liegenschaften des Auftraggebers arbeiten.

Daneben sollte sichergestellt sein, dass auch für externe Mitarbeiter Vertretungsregelungen existieren (siehe M 3.3 *Vertretungsregelungen*). Ebenso sollte gewährleistet sein, dass sich diese mit den von ihnen eingesetzten IT-Anwendungen auskennen und auch die erforderlichen Sicherheitsmaßnahmen beherrschen.

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sollte der Ausscheidende explizit darauf hingewiesen werden, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt (siehe auch M 3.6 *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*).

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d. h. beispielsweise dass der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern der Behörde bzw. des Unternehmens erlaubt ist (siehe auch M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*).

Prüffragen:

- Werden externe Mitarbeiter mit längerfristigen Aufgaben schriftlich auf die Einhaltung der einschlägigen Gesetze, Vorschriften und interne Regelungen verpflichtet?
- Werden externe Mitarbeiter geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet?
- Existieren für externe Mitarbeiter Vertretungsregelungen?

- Existiert ein geregeltes Verfahren für die Beendigung des Auftragsverhältnisses mit externen Mitarbeitern?
- Wird kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal wie Besucher behandelt?

# M 2.227 Planung des Windows 2000 Einsatzes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.228 Festlegen einer Windows 2000 Sicherheitsrichtlinie

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.229 Planung des Active Directory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine grundlegende Voraussetzung für den sicheren Einsatz des Active Directory ist eine angemessene Planung im Vorfeld. Die Planung für ein Active Directory kann dabei in mehreren Schritten erfolgen. Es sollte zunächst ein Grobkonzept für die Struktur der Domäne erstellt und darauf aufbauend die einzelnen Teilaspekte konkretisiert werden. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können. Hinweise zum Aufbau und zur prinzipiellen Struktur eines Active Directory bietet die Maßnahme M 3.64 *Einführung in Active Directory*.

Im Rahmen der Active Directory Planung sind folgende Aspekte zu berücksichtigen:

- Welche Active Directory-Struktur im Sinne der Aufteilung in Domänen und welche Anordnung der Domänen in Bäume (Trees) und Wälder (Forests) soll gewählt werden?
- Welche Benutzer und Rechner sollen in welchen Domänen zusammengefasst werden?

Für jede Domäne muss entschieden werden,

- welche OU-Objekte existieren sollen, wie diese hierarchisch angeordnet werden und welche Objekte diese jeweils aufnehmen sollen,
- welche Sicherheitsgruppen benötigt werden und wie diese in OUs zusammengefasst werden,
- welches administrative Modell umgesetzt wird (zentrale/dezentrale Verwaltung),
- ob und an wen administrative Aufgaben delegiert werden sollen,
- welche Sicherheitseinstellungen für verschiedene Typen von Rechnern und Benutzergruppen gelten sollen,
- welche Einstellungen bei den Gruppenrichtlinien benötigt werden und nach welchem Konzept die Gruppenrichtlinien verteilt werden (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows* und M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*).
- welche Vertrauensstellungen von Windows-Server automatisch generiert werden und welche zusätzlichen Vertrauensstellungen (z. B. zu NT-Domänen oder externen Kerberos-Realms) eingerichtet werden müssen,
- auf welche Active Directory-Informationen über die verschiedenen Active Directory-Schnittstellen (z. B. ADSI, LDAP) von wem zugegriffen werden dürfen,
- welche Active Directory-Objekte in den so genannten Global Catalog übernommen werden sollen, auf den in einem Forest global zugegriffen werden kann,
- in welchem Modus die Domäne betrieben werden muss: müssen in einer Domäne noch Windows NT Backup-Domänen-Controller (BDCs) betrieben werden, so muss die Domäne im "Mixed-Mode" betrieben werden. Sind keine BDCs vorhanden, kann die Domäne im "Native-Mode" betrieben werden.

Generell muss die geplante Active Directory-Struktur dokumentiert werden, dies trägt maßgeblich zur Stabilität, konsistenten Administration und damit zur Systemsicherheit bei. Es empfiehlt sich insbesondere festzuhalten, welche

Schemaänderungen durchgeführt werden. Dabei sollten auch die Gründe für die Änderung dokumentiert sein.

Für jedes Active Directory-Objekt sollte dokumentiert sein:

- Name und Position im Active Directory-Baum (z. B. "StandortBerlin", Vater-Objekt: OU "Filialen-Deutschland")
- welchem Zweck das Objekt dient (z. B. Gruppe der Benutzer mit RAS-Zugang auf RAS-Server 1)
- welche administrativen Zugriffsrechte für das Objekt und dessen Attribute vergeben werden sollen (z. B. vollständig verwaltet von "Admin1")
- wie die Vererbung von Active Directory-Rechten konfiguriert werden soll, z. B. Blockieren der Rechtevererbung (siehe auch M 2.230 *Planung der Active Directory-Administration*, M 3.27 *Schulung zur Active Directory-Verwaltung*)
- welche Gruppenrichtlinienobjekte auf dieses Objekt wirken (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows*)

Der Planung der Active Directory-Administration und des benutzten administrativen Modells kommt eine wichtige Aufgabe zu. Empfehlungen dazu finden sich zusammengefasst in Maßnahme M 2.230 *Planung der Active Directory-Administration*.

Die sicherheitsrelevanten Kernaspekte der Active Directory-Planung sind zusammengefasst:

- Domänen begrenzen die administrative Macht von Administratoren. Administratoren können daher nur innerhalb einer Domäne verwaltend tätig werden, so dass ihre Verwaltungsbefugnis standardmäßig nicht über die Domänengrenze reicht. Dies gilt insbesondere im Verbund mit mehreren Domänen (Baum, Wald), so dass die oft geäußerten Bedenken, dass durch das standardmäßig transitive Vertrauensmodell auch administrative Berechtigungen über Domänengrenzen hinweg möglich sind, für normale Administratorenkonten ausgeräumt werden können (siehe jedoch *Organisations-Admins* unten).
- Domänenübergreifende Zugriffe setzen voraus, dass in der Ziel-Domäne explizit Zugriffsberechtigungen für den Zugreifer aus einer anderen Domäne eingerichtet werden. Standardmäßig sind daher keine domänenübergreifenden Zugriffe möglich.
  Dies bedeutet, dass in einem Baum oder Wald ein Administrator einer Domäne "A" nur dann administrativ auf eine beliebige andere Domäne "B" zugreifen kann, falls der Domänenadministrator von "B" dem Administrator der Domäne "A" explizit Berechtigungen dazu einräumt (siehe jedoch *Organisations-Admins*).
- Die Mitglieder der Gruppe *Organisations-Admins* genießen einen Sonderstatus, da sie im gesamten Forest Administratorrechte auf dem Active Directory besitzen. Insbesondere werden gesetzte Zugriffsrechte auf Active Directory-Objekte bei Zugriffen von Organisations-Admins ignoriert. Die Mitgliedschaft in der Gruppe der Organisations-Admins muss daher restriktiv vergeben und strikt kontrolliert werden. Es ist zu beachten, dass ein Organisations-Admin benötigt wird, um beispielsweise eine Subdomäne anzulegen.
- Administrative Delegation wird durch die Vergabe von Zugriffsrechten auf Active Directory-Objekte und deren Attribute erreicht. Die Verteilung der Zugriffsrechte muss gemäß dem administrativen Modell erfolgen. Durch die Mechanismen für Zugriffsrechte im Active Directory (Vererbung, Kontrolle der Vererbung, Wirkungsbereich von Zugriffseinstellungen) können sehr komplexe Berechtigungsstrukturen aufgebaut werden. Diese können sehr schnell unübersichtlich und nicht mehr administrierbar werden, so

dass sich durch Fehlkonfigurationen im Active Directory Sicherheitslücken ergeben können. Eine möglichst einfache Berechtigungsstruktur ist daher vorzuziehen.
- Schemaänderungen sind kritische Operationen und dürfen nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt werden.

Abschließend sei darauf hingewiesen, dass Fehler in der Active Directory-Planung und den zugrunde liegenden Konzepten nach erfolgter Installation nur mit beträchtlichem Aufwand zu berichtigen sind. Nachträgliche Veränderungen in der Active Directory-Struktur, wie z. B. die Anordnung von Domänen in Bäume und Forests, ziehen unter Umständen das komplette Neuaufsetzen von Domänen nach sich.

Prüffragen:

- Ist ein bedarfsgerechtes Active Directory-Berechtigungskonzept entworfen worden?
- Sind administrative Delegationen mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet?
- Ist die geplante Active Directory-Struktur einschließlich etwaiger Schemaänderungen nachvollziehbar dokumentiert worden?

# M 2.230 Planung der Active Directory-Administration

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Das Active Directory besteht aus verschiedenen Objekten, die baumartig organisiert sind. Jedes Objekt besteht aus bestimmten Attributen, die die Objektinformationen speichern. Durch Objekte geschieht die Verwaltung eines Windows-Systems ab Version 2000, die durch einen berechtigten Administrator erfolgen muss. Für alle Active Directory Objekte können Berechtigungen vergeben werden, die den Zugriff auf die Objekte steuern. Damit kann festgelegt werden, welche Objekte von welchen Benutzern in einer bestimmten Art und Weise verändert werden können, wie beispielsweise das Anlegen von Benutzern oder das Zurücksetzen von Benutzerpasswörtern.

Bei einer Standardinstallation der Serverbetriebssysteme Windows Server 2000 und Windows 2003 Server (im Folgenden unter dem Begriff Windows-Server zusammengefasst) besitzen nur Administratoren das Recht, Veränderungen an Objekten vorzunehmen und damit eine Domäne zu verwalten. Benutzer besitzen in der Regel maximal Leserecht.

Generell gilt auch unter Windows-Server, dass an der Domänengrenze auch die administrative Macht der Administratoren der Domäne endet. Lediglich die Mitglieder der Gruppe *Organisations-Admins* besitzen in jeder Domäne eines Forests Vollzugriff auf alle AD-Objekte, und zwar unabhängig von den für diese Objekte eingestellten Zugriffsrechten. Standardmäßig sind dies die Mitglieder der Administratorengruppe der Forest-Root-Domain (FRD).

In großen Domänen empfiehlt sich die Delegation administrativer Aufgaben, so dass die administrative Last auf mehrere Administratoren verteilt ist oder auch, unter Umständen zusätzlich, eine Rollentrennung umgesetzt werden kann. Die Delegation administrativer Aufgaben erfolgt im Active Directory durch die Vergabe von entsprechenden Zugriffsrechten auf Active Directory-Objekte für die jeweiligen Adminstratorengruppen. Dabei erlaubt die Active Directory-Rechtestruktur eine feingranulare Vergabe von Rechten. Auf diese Weise kann z. B. einem Administrator erlaubt werden, Benutzerkonten anzulegen und Benutzerpasswörter zurückzusetzen, jedoch nicht Benutzerkonten zu löschen oder in andere Organizational Units (OU, Organisationseinheiten) zu verschieben. Um die Vergabe gleichförmiger Rechte innerhalb eines kompletten Teilbaums zu vereinfachen, besteht zusätzlich die Möglichkeit, Rechte eines Objektes an Objekte im Unterbaum zu vererben. Da die Übernahme von vererbten Rechten durch bestimmte Objekte im Unterbaum unter Umständen nicht gewünscht ist, lässt sich die Übernahme für Objekte auch blockieren, so dass sich hier durchaus komplexe Szenarien für die Verteilung von Berechtigungen ergeben können (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*).

Aus Sicherheitssicht ergeben sich folgende Aspekte, die bei der Planung der Active Directory-Administration zu berücksichtigen sind:

- Wird Delegation eingesetzt, so sollten nur die unbedingt notwendigen Rechte vergeben werden, die zur Ausübung der delegierten administrativen Tätigkeiten erforderlich sind.
- Das Delegationsmodell und die daraus resultierenden Rechtezuordnungen müssen dokumentiert werden.

- Die administrativen Tätigkeiten sollten so delegiert werden, dass sich möglichst keine Überschneidungen ergeben. Ansonsten können durch zwei Administratoren sich widersprechende Veränderungen durchgeführt werden. Dies führt dann zu Replikationskonflikten, die von Windows-Server automatisch aufgelöst werden, so dass sich eine der Änderungen auf jeden Fall durchsetzt. Es gibt jedoch für diesen Fall keine Warnungen. Es empfiehlt sich daher, das Administrationsmodell so zu entwerfen, dass möglichst überschneidungsfreie Zuständigkeiten existieren. Auf diese Weise kann die Gefahr von Replikationskonflikten verringert werden. Sind Replikationskonflikte zu erwarten oder bereits aufgetreten, so sollte in regelmäßigen Abständen oder nach wichtigen Änderungen eine manuelle Überprüfung erfolgen, ob sich immer die korrekten Werte durchgesetzt haben. Ob das Führen einer Evidenzdatenbank mit den Active-Directory-Soll-Daten unter Umständen organisatorisch sinnvoll ist, muss im Einzelfall entschieden werden.
- Wird die Verwaltung des Active Directory delegiert, so wird dies durch die Vergabe von entsprechenden Zugriffsrechten innerhalb des Active Directory erreicht. Dabei wird in der Regel der Vererbungsmechanismus eingesetzt, um Berechtigungen auf Objekte in Teilbäumen zu verwalten. Komplexe Szenarien mit Delegation und damit Rechtevererbung sollten jedoch unbedingt vermieden werden, da sonst leicht Sicherheitslücken entstehen können. Beispielsweise kann der Fall eintreten, dass ein Benutzer zu wenig oder zu viele Rechte hat.
- Es muss ein Konzept für die Mitgliedschaft in den verschiedenen administrativen Gruppen entworfen werden. Dabei sind vor allem die Bedingungen und Verfahren zu definieren, die festlegen, ob, wann und wie lange ein Benutzer oder eine Benutzergruppe in eine administrative Gruppe aufgenommen wird. Es muss insbesondere dafür Sorge getragen werden, die Mitgliedschaft in der Gruppe der Organisations-Admins restriktiv zu handhaben und zu kontrollieren. Falls es der organisatorische Ablauf zulässt, kann erwogen werden, alle Mitglieder in dieser Gruppe nach Aufbau der Domänenstruktur zu entfernen und nur bei Bedarf und unter Einhaltung des Vier-Augen-Prinzips entsprechende Mitglieder hinzuzufügen. Es muss jedoch berücksichtigt werden, dass ein Mitglied der Gruppe der Organisations-Admins immer dann benötigt wird, wenn eine neue Domäne im Forest angelegt werden soll.
- Die Administratoren sind über die Active Directory-Struktur und die organisatorischen Abläufe im Rahmen ihrer administrativen Tätigkeit zu informieren und entsprechend zu schulen, um zu verhindern, dass nicht-konforme Änderungen zu Sicherheitslücken führen. Beispielsweise kann es erforderlich sein, beim Anlegen eines neuen Benutzers diesen in entsprechende Sicherheitsgruppen aufzunehmen oder sogar zusätzlich eine neue Sicherheitsgruppe mit einem speziellen Namen anzulegen. Wird dies vergessen, so erhalten Benutzer unter Umständen fehlerhafte Berechtigungen.
- Für große Domänen sollte darüber nachgedacht werden, deren Verwaltung mit geeigneten Werkzeugen zu unterstützen. Es gibt verschiedene kommerzielle und auch frei verfügbare Werkzeuge, die die Active Directory-Verwaltung erleichtern. Es sollte überlegt werden, diese einzusetzen. Werden solche Werkzeuge verwendet, so muss sichergestellt werden, dass die Active Directory-Verwaltung ausschließlich über diese Werkzeuge erfolgt.

Prüffragen:

- In großen Domänen: Sind die administrativen Aufgaben im Active Directory nach einem Delegationsmodell überschneidungsfrei verteilt?

- Sind alle administrativen Aufgabenbereiche und Berechtigungen dokumentiert?

# M 2.231 Planung der Gruppenrichtlinien unter Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Zur Konfiguration von Windows Rechnern steht ab Windows 2000 ein leistungsfähiger Mechanismus der so genannten Gruppenrichtlinien zur Verfügung. Schon unter Windows NT gab es mit den Gruppenrichtlinien ein ähnliches, aber deutlich weniger leistungsfähiges Instrument. Gruppenrichtlinien dienen im Active Directory dazu, einen Satz von Konfigurationseinstellungen, zu denen insbesondere auch Sicherheitseinstellungen gehören, auf eine Gruppe von Objekten anzuwenden. Durch ein so genanntes Gruppenrichtlinienobjekt (englisch *Group Policy Object, GPO*) wird ein vorgegebener Satz von Konfigurationsparametern (standardmäßig über 700) zusammengefasst. Für jeden Parameter kann ein konkreter Wert angegeben werden, der unter Umständen nur aus einem beschränkten Wertebereich stammt. Generell kann der Wert *nicht definiert* gewählt werden, so dass dann automatisch die Windows Standardeinstellungen für diese Parameter gelten. Die Standardeinstellungen sind in der Hilfedatei zu Gruppenrichtlinien, unter anderem im Windows 2000 Server Resource Kit, dokumentiert.

Die Parameter innerhalb eines Gruppenrichtlinienobjektes sind baumartig oder dateisystemartig thematisch zusammengefasst. Dabei ergibt sich eine generelle Zweiteilung auf oberster Ebene in Einstellungen für Rechner sowie für Benutzer. Aus Sicherheitssicht sind insbesondere die Einstellungen interessant, die sich unterhalb der folgenden "Pfade" finden:

- *Rechnereinstellungen\WindowsEinstellungen\Sicherheitseinstellungen*
- *Rechnereinstellungen\Administrative Einstellungen\Windows Komponenten\Windows Installer*
- *Rechnereinstellungen\Administrative Vorlagen\System\Gruppenrichtlinien*
- *Benutzereinstellungen\Administrative Vorlagen\Windows Komponenten\Microsoft Management Konsole*
- *Benutzereinstellungen\Administrative Einstellungen\Windows Komponenten\Windows Installer*

Die Server-Betriebssysteme Windows 2000 Server und Windows Server 2003 (im Folgenden unter dem Begriff Windows-Server zusammengefasst) berechnen generell für jeden an einer Domäne angemeldeten Rechner und für jeden angemeldeten Benutzer die jeweils gültigen Einstellungen für jeden Gruppenrichtlinienparameter. Diese Berechnung ist nötig, da die Vorgaben für die Parametereinstellungen durch unterschiedliche Gruppenrichtlinienobjekte definiert sein können, die sich gegenseitig überlagern können. Folgende Gruppenrichtlinienobjekte können definiert werden:

- Jeder Rechner besitzt ein lokal definiertes Gruppenrichtlinienobjekt. Dies erlaubt die Definition von Parametereinstellungen lokal auf dem Rechner, z. B. wenn keine Netzverbindung besteht.
- Gruppenrichtlinienobjekte können über Windows-Server Standorte (Sites) definiert werden. Damit können Einstellungen standortspezifisch adaptiert werden.
- Innerhalb der Active Directory Struktur können Gruppenrichtlinienobjekte für das Domänenobjekt definiert werden, so dass damit Parametereinstellungen für Rechner und Benutzer innerhalb der gesamten Domäne gesteuert werden können.

- Auf jedem OU-Objekt können Gruppenrichtlinien definiert werden, deren Einstellungen dann auf alle Rechner und Benutzer unterhalb dieses OU-Objektes wirken.

Für die Berechnung der jeweils für einen konkreten Rechner oder Benutzer geltenden Parametereinstellungen wird das folgende Berechnungs- bzw. Überdeckungsschema (Lokal <- Standort <- Domäne <- Organisationseinheit, LSDO) angewandt: Zunächst werden die lokalen Einstellungen berücksichtigt (L, Lokal). Dann werden diese Einstellungen durch die Einstellungen des Gruppenrichtlinienobjektes, das auf dem zugehörigen Standort definiert ist, überdeckt (S, Standort). Danach erfolgt die Überdeckung durch die auf dem relevanten Domänenobjekt definierten Gruppenrichtlinienobjekte (D, Domäne). Schließlich werden die Gruppenrichtlinienobjekte der OU-Objekte in der Reihenfolge angewandt, wie sie auf dem Weg vom Domänenobjekt zu dem OU-Objekt, das den jeweiligen Rechner oder Benutzer enthält, definiert sind (O, Organisationseinheit).

Die Überdeckung kann durch die Optionen *blockieren* bzw. *erzwingen* beeinflusst werden. Stehen die Einstellungen *blockieren* und *erzwingen* im Konflikt, so wird die Einstellung *erzwingen* durchgesetzt. Zusätzlich ist es auf OU-Ebene möglich, mehrere Gruppenrichtlinienobjekte für ein OU-Objekt zu definieren. Dabei erfolgt die Überdeckung gemäß der angegebenen Reihenfolge. Es ist dabei außerdem möglich, jedes einzelne Gruppenrichtlinienobjekt für ein OU-Objekt zu aktivieren oder zu deaktivieren.

Gruppenrichtlinienobjekte können im Active Directory nur auf OU-Objekten definiert werden, nicht jedoch auf einzelnen Rechnern oder Benutzerobjekten. Das lokal definierte Gruppenrichtlinienobjekt wird nicht im Active Directory gespeichert. Soll ein Gruppenrichtlinienobjekt, das auf einem OU-Objekt definiert ist, das Rechnerobjekte zusammenfasst, nicht auf alle enthaltenen Rechnerobjekte wirken, so besteht die Möglichkeit, durch die Vergabe von Zugriffsrechten auf das Gruppenrichtlinienobjekt die Anwendung auf ein konkretes Rechnerobjekt zu unterbinden. Hierzu ist diesem Rechnerobjekt das Zugriffsrecht *Anwenden* auf das Gruppenrichtlinienobjekt zu entziehen.

Die bisher benutzte Darstellung der Definition von Gruppenrichtlinienobjekten auf OU-Objekten war jedoch vereinfacht: Gruppenrichtlinienobjekte werden separat im Active Directory gespeichert und bilden einen Pool von Objekten. Jedes definierte Gruppenrichtlinienobjekt kann nun einem oder auch mehreren OU-Objekten assoziiert werden. Man spricht dann von einem *Link*. Durch das Kennzeichnen eines Links als aktiviert oder deaktiviert wird das jeweilige Gruppenrichtlinienobjekt bei der Berechnung für das OU-Objekt herangezogen oder nicht (siehe oben). Für jedes Gruppenrichtlinienobjekt kann über den Eigenschaftsdialog festgestellt werden, mit welchen OU-Objekten ein *Link* besteht, d. h. auf welche Objekte sie potentiell wirken.

Aus Sicherheitssicht sind bei der Planung und im Umgang mit Gruppenrichtlinienobjekten folgende Aspekte zu berücksichtigen:

- Das Gruppenrichtlinienkonzept muss so einfach wie möglich gehalten werden. Komplexe Strukturen aus Mehrfachüberdeckungen sind zu vermeiden. Insbesondere sollte auf die Möglichkeit der Vergabe von Zugriffsrechten auf Gruppenrichtlinienobjekte nur in Ausnahmefällen zurückgegriffen werden. Generell muss das Gruppenrichtlinienkonzept so dokumentiert sein, dass Ausnahmeregelungen einfach zu erkennen sind.
- Das Gruppenrichtlinienkonzept und die OU-Objektstruktur beeinflussen sich gegenseitig wesentlich, da Gruppenrichtlinienobjekte im Active Directory nur auf OU-Objekte angewandt werden können und nicht auf Rech-

ner- oder Benutzerobjekte. Beim Aufbau der OU-Gruppierungen ist daher darauf zu achten, dass nur Objekte, die mit gleichen GPO-Einstellungen versehen werden sollen, in einem OU-Objekt oder untergeordneten OU-Objekten zusammengefasst werden.
- Durch die Rechteberechnung ist es möglich, die Verwaltung der Parametereinstellungen auf unterschiedliche "Orte" (Lokal, Standort, Domänen-Objekt, OU-Objekte) zu verteilen. Es muss daher für jeden Parameter entschieden werden, wo er definiert wird. Es ist dabei zu beachten, dass einige Parameter nur dann wirksam werden, wenn sie an bestimmten "Orten" definiert werden. So können z. B. die Passworteinstellungen nur auf Domänen-Objekten definiert werden.
- Gruppenrichtlinienobjekte müssen vor unberechtigter Veränderung geschützt werden. Dazu müssen einerseits entsprechende Berechtigungen im Active Directory vergeben werden (siehe auch M 2.230 *Planung der Active Directory-Administration*, M 3.27 *Schulung zur Active Directory-Verwaltung*) und andererseits kann der Gebrauch von entsprechenden Verwaltungswerkzeugen, wie z. B. MMC-Gruppenrichtlinien-Snap-In oder Registrierungseditoren, für Benutzer unterbunden werden.
- Insbesondere für die sicherheitsrelevanten Parameter innerhalb eines Gruppenrichtlinienobjektes sind die Einstellungen festzulegen. Neben den oben angegebenen Einstellungen können je nach Anwendungsszenario auch weitere Parameter sicherheitsrelevant sein. Dazu zählen z. B. Internet-Explorer-Einstellungen.

Die Einstellungen der verschiedenen Gruppenrichtlinienobjekte müssen sich dabei generell an den Sicherheitsrichtlinien des Unternehmens bzw. der Behörde orientieren und diese umsetzen. Entsprechende Vorgaben für die Sicherheitseinstellungen, die als Ausgangsbasis innerhalb einer Gruppenrichtlinie dienen können, befinden sich im Dokument *Hilfsmittel zum Baustein Active Directory* im Abschnitt *Sicherheitseinstellungen für Gruppenrichtlinien*.

Prüffragen:

- Liegt ein Konzept vor, wie Gruppenrichtlinien unter Windows einzurichten sind?
- Wurden beim Gruppenrichtlinienkonzept Mehrfachüberdeckungen vermieden?
- Können durch die Dokumentation des Gruppenrichtlinienkonzepts Ausnahmeregelungen erkannt werden?
- Sind alle Gruppenrichtlinienobjekte durch restriktive Zugriffsrechte geschützt?
- Sind für die Parameter in allen Gruppenrichtlinienobjekten Vorgaben festgelegt?

# M 2.232 Planung der Windows-CA-Struktur ab Windows 2000

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Windows wird ab Windows 2000 mit eigenen PKI-Komponenten ausgeliefert, die den Aufbau einer unternehmensweiten Zertifikatshierarchie ermöglichen. Zertifikate dienen dazu, Identitäten von Personen und Systemen in kryptographischen Prozessen wie der Verschlüsselung, bei der ("zertifikatsbasierten") Authentisierung oder bei der elektronischen Signatur von Daten und Anwendungen zu bestätigen. Kernstück einer PKI (Public Key Infrastruktur) ist die so genannte Zertifizierungsstelle (Certificate Authority, CA), die Zertifikate ausstellen kann. Für den Betrieb von Windows ist der Betrieb einer CA zwar generell nicht notwendig, jedoch immer dann zwingend, wenn bestimmte Eigenschaften oder Funktionen genutzt werden sollen. Dazu gehört die Anmeldung mit Chipkarten oder anderen Token sowie abgesicherte Kommunikation zwischen Windows Systemkomponenten über SSL. Windows bietet zwei Ausprägungen einer CA an:

- Stand-alone-CA (alleinstehende Zertifizierungsstelle) und
- Enterprise-CA (organisationsweite Zertifizierungsstelle).

Der Hauptunterschied zwischen den beiden CA-Versionen ist, dass die Enterprise-CA im Active Directory integriert ist und damit vom Active Directory als Verzeichnisdienst profitiert. Beispielsweise werden Zertifizierungsstellen im Active Directory veröffentlicht, und Zertifikate können in großem Umfang automatisch ausgestellt und verteilt werden. Bei der Stand-alone-CA wird die Zertifikatsanforderung immer vom Administrator der CA geprüft. Die Zertifikatserzeugung muss durch den Administrator von Hand angestoßen werden. Die Stand-alone-CA kann auch auf einem nicht vernetzten Rechner installiert und betrieben werden, wohingegen die Enterprise-CA sinnvoll nur auf einem vernetzten Rechner ablaufen kann. Ab Windows Server 2003 Enterprise Edition können bei der Enterprise-CA die Zertifikatsvorlagen individuell angepasst werden.

Beide CA-Versionen eignen sich für den Aufbau von Zertifikatshierarchien und können daher auch als untergeordnete CA fungieren. Für viele infrastrukturelle Zwecke eines LANs ist die Enterprise-CA besser geeignet und sollte im Normalfall bevorzugt werden. In mehrstufigen Hierarchien empfiehlt es sich, die oberste Hierarchie (Wurzel-CA) offline zu betreiben, da deren Schlüssel als "Vertrauensanker" der gesamten Hierarchie besonders schützenswert ist und die CA nur selten zum Ausstellen der Zertifikate für die Sub-CAs benötigt wird.

Insbesondere bei der Planung einer behörden- oder unternehmensweiten PKI sollte darauf geachtet werden, dass alle Einsatzszenarien und die dadurch betroffenen Applikationen bekannt sind. Um die technische Machbarkeit abschätzen zu können, empfiehlt es sich, alle Komponenten, die eingesetzt werden sollen, im Vorfeld auf ihre Interoperabilität zu überprüfen.

Eine Auflistung struktureller Planungsaspekte ist auf den BSI-Webseiten unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe Hilfsmittel für die Planung der Windows 2000/2003 CA-Struktur). Generell gilt, dass alle für den Betrieb einer CA relevanten organisatorischen, technischen und auch sicherheitstechnischen Rahmenbedingungen in einem entsprechenden Konzept dokumentiert werden müssen.

**Planung des Einsatzes geeigneter Zertifizierungsstellen**

Organisatorische Aspekte:

- Die Planung einer PKI erfordert Zeit. In der Regel müssen insbesondere innerorganisatorische Zuständigkeiten geregelt und festgeschrieben werden.
- Die CA-Hierarchie sollte sich an den geplanten und zukünftig möglichen Einsatzszenarien orientieren. Unterschiedliche Einsatzzwecke sollten durch eigene CAs abgebildet werden, die unter einer gemeinsamen offline betriebenen Wurzel-CA zusammengeführt werden können.
- Der Verwendungszweck von Zertifikaten spielt bei der Planung der CA-Struktur eine wichtige Rolle. So bereitet der Aufbau einer generellen, organisationsweiten Zertifikatsinfrastruktur meist mehr Schwierigkeiten, als der Aufbau einer applikationsbezogenen PKI. Eine applikationsbezogene PKI kann beispielsweise eingesetzt werden, wenn im Rahmen einer netzbasierten Anwendung nur die betroffenen Mitarbeiter zuverlässig identifiziert werden müssen. Ein Beispiel hierfür ist das elektronische Einreichen und Bearbeiten von Urlaubsanträgen, wobei die Anträge nacheinander von verschiedenen Personen digital abgezeichnet, also signiert, werden müssen.
- Für den Betrieb der CAs und den Einsatz der ausgestellten Zertifikate ist eine CA-Richtlinie zu definieren und zu dokumentieren, typischerweise in der Form sogenannter Certification Practice Statements (CPS) und Certificate Policies (CP). Für deren Gliederung ist der Internet-Standard RFC 3647 international anerkannt.
- Für die Sperrung von Zertifikaten sind geeignete Prozesse einzuführen. Dabei sind die Aspekte Erreichbarkeit und Verfügbarkeit der Sperrstelle, Berechtigte zur Sperrung und deren zuverlässige Identifizierung sowie Dokumentation der Sperrung zu berücksichtigen.
- Bei Verlust oder Kompromittierung von Schlüsseln und entsprechender Sperrung benötigen die Mitarbeiter ein neues Zertifikat, um ihre Tätigkeit fortzusetzen. Hierfür sind insbesondere bei der Nutzung von Chipkarten oder Token als Schlüsselträger geeignete Verfahren zu definieren, wie in ausreichend kurzer Zeit die Arbeitsfähigkeit wiederhergestellt werden kann (z. B. durch sichere Vorhaltung und Ausgabe vorpersonalisierter Chipkarten an den einzelnen Standorten).

Technische Aspekte:

- Es muss geplant werden, welche kryptographischen Verfahren und Algorithmen und welche Schlüssellängen zum Einsatz kommen sollen (siehe auch M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*).
- Das Vertrauen in Zertifikate einer CA hängt wesentlich von deren Sicherheitsgrad ab. Daher ist für CAs, die sicherheitskritische Zertifikate erzeugen, besonders auf die physikalische und softwaretechnische Sicherheit zu achten. Sicherheitskritisch sind insbesondere solche Zertifikate, die einen großen Anwenderkreis haben oder von deren Korrektheit weitere sicherheitskritische Anwendungen abhängen.
- Für sensible Einsatzzwecke empfiehlt es sich, die privaten n Schlüssel durch die Speicherung in Kryptohardware (Chipkarten, Token) vor unbefugter Vervielfältigung und unbefugtem Zugriff zu schützen.
- Für Zertifikate mit unterschiedlichem Sicherheitsbedarf sollten unterschiedliche CAs eingesetzt werden.
- Beim Einsatz von Zertifikaten muss das Gültigkeitsmodell festgelegt werden ("Kettenmodell" versus "Schalenmodell"). Dabei ist festzulegen, wie

Zertifikate zu behandeln sind, wenn das Zertifikat der ausstellenden CA gesperrt wird oder abläuft.
- Für die verschiedenen Zertifikatstypen (z. B. Root-CA-Zertifikat, Benutzer-E-Mail-Zertifikat) muss jeweils die maximale Gültigkeitsdauer festgelegt werden. Bei der Prüfung von Zertifikaten nach dem Schalenmodell ist es sinnvoll, dass die Gültigkeitsdauer der Zertifikate nicht die Gültigkeitsdauer des Zertifikates der ausstellenden CA überschreitet.
- Die Möglichkeiten und Verfahren nach Ablauf der Gültigkeit eines Zertifikates sind festzulegen. Sind zum Beispiel Verlängerungen möglich oder müssen neue Zertifikate ausgestellt werden?
- Für die verschiedenen Einsatzzwecke sind geeignete Zertifikatsvorlagen einzurichten und anzuwenden. Dabei ist besonders auf die richtige Verwendung der Restriktionen, insbesondere der "Certificate Usage" im Zertifikat zu achten, um eine missbräuchliche Nutzung von Zertifikaten (z. B. zur Einrichtung von Sub-CAs) auszuschließen. Ab Windows Server 2008 stehen in den Zertifikatsvorlagen mehr Parameter als Vorgabe zur Verfügung, die jedoch nur genutzt werden können, wenn in derselben Hierarchie keine CAs auf älteren (Windows Server 2003) Systemen betrieben werden.
- Die Zertifikatsdatenbank der CA sollte in die Datensicherung einbezogen werden.

Neben der Planung einer PKI spielt insbesondere die Sicherheit im laufenden Betrieb der einzelnen PKI-Komponenten eine große Rolle. Die Absicherung einer Zertifizierungsstelle muss dem Schutzbedarf der jeweiligen Anwendung genügen, in der Zertifikate verwendet werden. Empfehlungen dazu finden sich in und unter den Hilfsmitteln zum IT-Grundschutz (siehe *Hilfsmittel für den Schutz der Zertifikatsdienste unter Windows Server 2003)*.

**Versionsspezifische Planungsaspekte für eine CA ab Windows Server 2003**

**Verteilung von Zertifikaten:**

Zertifikate können automatisch (ohne Benutzereingriff) oder manuell angefordert und ausgestellt (kurz: verteilt) werden). Die automatische Verteilung von Zertifikaten (*Auto-Enrollment*) basiert auf Active Directory und Gruppenrichtlinien (vergleiche M 1.1 *Einhaltung einschlägiger Normen und Vorschriften*). Auto-Enrollment vereinfacht die Verwaltung von Zertifikaten von Benutzern (ab Windows Server 2003 Enterprise Edition) und Computern für bestimmte Anwendungen im Organisationsumfeld. Häufiges Beispiel ist das Verteilen von Verschlüsselungszertifikaten für das *Encrypting File System* (EFS) auf Clients. Das Zertifikats-Enrollment wird nur für authentisierte Clients durchgeführt und ist mit entsprechenden Sicherheitsmechanismen und Berechtigungen versehen. Die Einstellungen sind im Gruppenrichtlinienobjekt-Editor unter

*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien öffentlicher Schlüssel* | *Eigenschaften* von *Einstellungen für die automatische Registrierung*

und

*Benutzerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien öffentlicher Schlüssel* | *Eigenschaften* von *Einstellungen für die automatische Registrierung*

zu finden. Standardmäßig fordern nur Domänencontroller automatisch ein Computerzertifikat an. Darüber hinaus rufen einige optionale Windows-Komponenten ebenfalls automatisch ein Zertifikat ab, so erhält jeder Client mit ak-

tiviertem EFS automatisch ein EFS-Zertifikat. Auto-Enrollment sollte jedoch nur im tatsächlich benötigten Umfang eingesetzt werden, da sonst die Verwaltung erschwert wird und unter anderem auch die Gefahr des Abfangens von Schlüsseln besteht.

Es sollte auf Grundlage der geplanten Applikationen oder Windows-Komponenten überlegt werden, welche Zertifikatstypen für welche Benutzer beziehungsweise Computer zugelassen sind und auf welche Weise die Verteilung stattfindet. Entsprechend sind die Gruppenrichtlinien und die Berechtigungen in den Zertifikatsdiensten zu planen.

**Archivierung von privaten Schlüsseln:**

Die Archivierung von privaten Schlüsseln in der Zertifizierungsstelle (ab Windows Server 2003 Enterprise Edition) ist nicht zu empfehlen. Sie sollte nur dann aktiviert werden, wenn ein geeignetes Konzept zur Rollentrennung der PKI-Verwaltung geplant und umgesetzt wurde. Die Archivierung kann die Gefahr des Schlüsselverlusts einzelner Benutzer verringern, allerdings wird das Risiko des Missbrauchs erhöht. Die geeignete Strategie ist abhängig von den eingesetzten Anwendungen und Komponenten und sollte durch die PKI-Planung und in einer Sicherheitsrichtlinie festgelegt werden.

**Rollentrennung:**

Rollentrennung bedeutet, dass die Konzentration mehrerer oder aller kritischer Verwaltungsrollen im Zusammenhang mit PKI auf eine Person oder ein Benutzerkonto verhindert wird. Dazu muss zunächst die Rollentrennung auf organisatorischer Ebene definiert sein, wie im oberen Absatz beschrieben. Auf technischer Seite kann die Rollentrennung durch das System erzwungen werden (ab Windows Server 2003 Enterprise Edition). Die vier Rollen sind:

- Zertifizierungsstellenadministrator
- Zertifikatsverwaltung
- Sicherungs-Operator
- Prüfer

Details zu den Rollen sind im Hilfethema *Rollenbasierte Verwaltung* der integrierten Windows-Hilfe zu finden.

Ein Benutzerkonto, das vorher zwei oder mehr der genannten Rollen inne hatte, wird durch die Rollentrennung von allen Verwaltungstätigkeiten an der CA ausgeschlossen. Die Rollen müssen durch einen Administrator neu zugeteilt werden. Bei einer fehlerhaften Konfiguration der Rollentrennung ist die CA nicht mehr nutzbar. Wenn diese Funktion eingesetzt werden soll, ist hierfür zunächst ein geeignetes Berechtigungskonzept zu erstellen, welches dann in einem Testszenario erprobt werden sollte.

Prüffragen:

- Sind die organisatorischen, technischen und sicherheitstechnischen Rahmenbedingungen für den Betrieb einer Certificate Authority (CA) unter Windows dokumentiert?
- Entsprechen die in der Windows CA eingesetzten kryptographischen Verfahren, Algorithmen und Schlüssellängen den Anforderungen der Organisation?
- Werden für Zertifikate mit unterschiedlichen Sicherheitsanforderungen unterschiedliche CAs eingesetzt?
- Sind Prozesse zur Laufzeitverlängerung und/oder zur rechtzeitigen Neu-Ausstellung von Zertifikaten bei Ablauf der Gültigkeit festgelegt?

- Entspricht die Absicherung der Zertifizierungsstelle dem Schutzbedarf der jeweiligen Anwendungen, in denen Zertifikate verwendet werden?
- Wurde bei der Planung einer behörden- oder unternehmensweiten PKI ab Windows 2000 darauf geachtet, dass alle Einsatzszenarien und die dadurch betroffenen Applikationen bekannt sind?
- Wird die Zertifikatsdatenbank regelmäßig gesichert?

# M 2.233 Planung der Migration von Windows NT auf Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 2.234 Konzeption von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Nach der Entscheidung, einen oder mehrere Internet-PCs für die Nutzung von Internet-Angeboten und -Diensten zur Verfügung zu stellen, sollte ein Konzept für die konkrete Realisierung erstellt werden. In diesem Konzept sollten die funktionale Anforderungen, Sicherheitsanforderungen, erforderliche Regelungen, Zuständigkeiten sowie Vorgaben für die technische Realisierung und Nutzung festgelegt werden.

Es wird empfohlen, bei der Konzeption mindestens die folgenden Teilaspekte zu berücksichtigen. Je nach den vorliegenden organisatorischen Randbedingungen müssen unter Umständen weitere Punkte in das Konzept aufgenommen werden. Hinweise hierzu können den Bausteinen B 3.301 *Sicherheitsgateway (Firewall)* und B 5.4 *Webserver* entnommen werden.

**Funktionale Anforderungen**

Als Erstes sollte festgelegt werden, welche im Internet angebotenen Dienste, z. B. World Wide Web (WWW), E-Mail, News oder Instant Messaging, genutzt werden sollen. Dies hat weitgehende Auswirkungen auf die zu installierende Software und die erforderlichen Sicherheitsmaßnahmen.

Um einen geeigneten Internet Service Provider (ISP) und eine zweckmäßige Anschlusstechnik auswählen zu können, sollten weiterhin die benötigten Bandbreiten und Antwortzeiten für die einzelnen Internet-Dienste dokumentiert werden.

Um Kriterien für die Aufstellungsorte der Internet-PCs zu erhalten, sollte anschließend im Konzept dokumentiert werden, wie hoch das voraussichtliche Nutzeraufkommen ist und welche Anforderungen hinsichtlich der räumlichen Nähe des Internet-PCs zum Mitarbeiter bestehen.

Weiterhin sollte festgelegt werden, wie mit Daten aus dem Internet, z. B. heruntergeladenen Dateien, umgegangen wird, ob diese z. B. auf anderen Systemen weiterverarbeitet werden dürfen oder archiviert werden müssen. Ein Datenaustausch zwischen Internet-PC und Hausnetz erfordert zusätzliche Sicherheitsmaßnahmen und Regelungen.

**Sicherheitsanforderungen**

Hinsichtlich der Sicherheitsanforderungen sollte im Konzept festgelegt werden, ob die Informationen, die aus dem Internet abgerufen oder an andere Computer im Internet gesendet werden, gegen unbefugtes Mitlesen oder unerlaubte Veränderung geschützt werden müssen.

Weiterhin ist im Konzept zu dokumentieren, ob auf dem Internet-PC schützenswerte Daten abgespeichert und längere Zeit vorgehalten werden müssen. Dies ist besonders dann relevant, wenn der Internet-PC auch für E-Mail verwendet wird.

Im Hinblick auf Zurechenbarkeit und Schutz vor unerlaubter Nutzung sollte festgelegt werden, ob sich Benutzer am Internet-PC authentisieren müssen, bevor sie den Internet-Zugang verwenden können.

Das Einsatzkonzept sollte auch Aussagen zu Anforderungen an die Verfügbarkeit enthalten. Es ist daher festzulegen, ob ein Ausfall des Internet-PCs für längere Zeit tolerabel ist oder ob für diesen Fall Ausweichlösungen geschaffen werden müssen.

**Erforderliche Regelungen**

Im Hinblick auf die Nutzung eines Internet-PCs müssen bestehende Regelungen angepasst oder neu festgelegt werden. Dazu gehören insbesondere das Sicherheitskonzept und die Benutzerrichtlinie (siehe auch M 2.235 *Richtlinien für die Nutzung von Internet-PCs*). Je nach Standort kann der Einsatz eines Internet-PCs aber beispielsweise auch Auswirkungen auf bestehende Zutrittsregelungen haben.

**Zuständigkeiten**

Auch Internet-PCs müssen durch fachkundiges Personal administriert und gewartet werden. Im Einsatzkonzept sollte daher festgelegt werden, welche Mitarbeiter bzw. Rollen für Administration und Betrieb des Internet-PCs zuständig sind und wer zu benachrichtigen ist, wenn der Internet-PC ausfällt oder wenn Anzeichen für einen Sicherheitsvorfall entdeckt werden.

Da sich das Nutzungsprofil und die Einsatzumgebung von Internet-PCs schnell ändern können, muss das Konzept fortgeschrieben werden. Es sollte dokumentiert werden, wer hierfür zuständig ist.

**Vorgaben für die technische Realisierung (Hardware)**

Im Konzept sollte vorgegeben werden, wie viele Internet-PCs zum Einsatz kommen und ob diese untereinander vernetzt und mit einer gemeinsamen Internet-Anbindung ausgestattet werden sollen. In diesem Fall sollte auch festgelegt werden, was für Komponenten zur Vernetzung verwendet werden.

Weiterhin sollte die Hardware-Ausstattung der Internet-PCs definiert werden. Dazu gehören z. B. die Hardware-Plattform, Laufwerke, Schnittstellen und Peripheriegeräte.

Falls eine Datensicherung des Internet-PCs erforderlich ist, sollte im Konzept festgelegt werden, über welche Medien oder Schnittstellen diese erfolgt.

**Vorgaben für die technische Realisierung (Software)**

Um die Administration zu vereinfachen, sollten alle Internet-PCs möglichst gleich ausgestattet sein. Die Software-Ausstattung sollte daher im Konzept weitgehend vorgegeben werden.

Das verwendete Betriebssystem sollte auf jeden Fall im Einsatzkonzept festgelegt werden. Falls eine Authentisierung der Benutzer erforderlich ist, sollten nur Betriebssysteme mit einer wirksamen Benutzertrennung, z. B. Windows NT/2000 oder Linux, eingesetzt werden. Windows 9x/ME sind in diesem Fall ungeeignet.

Weiterhin sollte dokumentiert werden, welche Client-Programme für Internet-Dienste zum Einsatz kommen sollen. In vielen Fällen wird zumindest ein WWW-Browser und ein E-Mail-Client benötigt. Weitere Beispiele sind News-Clients und Instant Messaging-Programme.

Um die Sicherheitsanforderungen erfüllen zu können, müssen meist zusätzliche Sicherheitstools installiert werden, z. B. für den Schutz vor Computer-Vi-

ren, zur Datensicherung oder zur Verschlüsselung. Im Konzept sollte festgelegt werden, welche Produkte hierfür ggf. verwendet werden.

**Vorgaben für die technische Realisierung (Internet-Anbindung)**

Das Einsatzkonzept sollte detaillierte Vorgaben zur technischen Realisierung der Internet-Anbindung machen, um die Anforderungen an Bandbreite, Antwortzeiten und Verfügbarkeit erfüllen zu können (siehe auch M 5.92 *Sichere Internet-Anbindung von Internet-PCs*). Hierzu gehört einerseits die Frage, über welchen oder welche Internet Service Provider (ISP) der Zugang zum Internet erfolgen soll (siehe auch M 2.176 *Geeignete Auswahl eines Internet Service Providers*).

Andererseits muss auch festgelegt werden, über welche Zugangstechnik, z. B. ISDN oder DSL, die Internet-Anbindung erfolgen soll und welche Schnittstelle des Internet-PCs, z. B. ISDN-Karte oder Netzwerkkarte, hierfür verwendet wird. Je nach verwendeter Zugangstechnik werden unter Umständen spezielle Programme oder Hardware-Komponenten, z. B. DSL-Modem bzw. Router, benötigt.

Prüffragen:

- Wurde ein Nutzungskonzept für den Einsatz von Internet-PCs erstellt, das auch die Sicherheitsanforderungen an den Internet-Zugang enthält?
- Ist in einem Konzept festgelegt, welche Internet-Dienste genutzt werden dürfen und welche Dienste an Internet-PCs zur Verfügung stehen?
- Ist der Umgang mit Daten aus dem Internet festgelegt, insbesondere hinsichtlich der Weiterverarbeitung auf anderen Systemen?
- Sind in dem Konzept die Anforderungen an die Verfügbarkeit von Internet-PCs festgelegt und ob für einen Ausfall Ausweichlösungen geschaffen werden müssen?
- Sind die Zuständigkeiten für Administration und Betrieb von Internet-PCs sowie Ansprechpartner benannt?

# M 2.235 Richtlinien für die Nutzung von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Für die sichere Nutzung von Internet-PCs ist es erforderlich, dass hierfür verbindliche Richtlinien festgelegt werden. Diese Richtlinien müssen allen beteiligten Mitarbeitern der Institution, d. h. mindestens den Benutzern des Internet-PCs und den zuständigen Administratoren, bekannt gemacht werden.

Es wird empfohlen, die Richtlinien für die Nutzung des Internet-PCs in einem Dokument zusammenzufassen und als Datei auf dem Internet-PC zur Verfügung zu stellen, z. B. auf dem Desktop. Dabei sollten mindestens folgende Teilaspekte berücksichtigt werden:

Die Benutzer sollten in kurzer, verständlicher Form über die Risiken informiert werden, die mit der Nutzung des Internet-PCs verbunden sind. Diese Information dient gleichzeitig als Motivation für die nachfolgenden Richtlinien.

Auch der Internet-PC muss durch fachkundiges Personal administriert und gewartet werden. Dies kann entweder durch die vorhandene Administration, z. B. für IT-Systeme im Hausnetz, oder durch andere Mitarbeiter erfolgen, die dann entsprechend geschult werden müssen. Die Zuständigkeit sollte in den Richtlinien dokumentiert werden.

In einigen Fällen kann es zweckmäßig sein, dass Benutzer bestimmte Konfigurationseinstellungen selbst vornehmen dürfen. Dies sollte in den Richtlinien vermerkt, anderenfalls sollte es untersagt werden.

In den Richtlinien sollte festgelegt werden, welche Personen den Internet-PC zu welchen Zeiten und für welche Zwecke benutzen dürfen. In diesem Zusammenhang ist insbesondere festzulegen, ob nur dienstliche oder auch private Nutzung - z. B. in der Mittagspause - zugelassen ist.

Weiterhin sollte dokumentiert werden, welche Programme für die Nutzung von Internet-Diensten verwendet werden dürfen und ob aktive Inhalte, wie z. B. Javascript, Java oder ActiveX, auf dem Internet-PC ausgeführt werden dürfen. Wichtig ist in diesem Zusammenhang auch, ob Benutzer selbständig Browser-Erweiterungen ("Plug-Ins") installieren und nutzen dürfen.

Falls das verwendete Betriebssystem eine Benutzertrennung unterstützt, sollten Client-Programme für die Nutzung von Internet-Diensten nicht unter dem Administrator-Benutzerkonto, z. B. *root* oder *Administrator*, gestartet werden. Auch von Administratoren sollten hierfür normale Benutzerkonten verwendet werden.

Es müssen Regelungen dafür festgelegt werden, welche persönlichen Daten und welche Informationen über die Behörde bzw. das Unternehmen, z. B. Postadressen, über den Internet-Zugang weitergegeben werden dürfen. Dazu gehört auch die Frage, ob Nachrichten mit einer dienstlichen Absenderadresse gesendet werden dürfen, falls der Internet-PC für E-Mail oder News genutzt wird.

Außerdem sollte in den Richtlinien vorgegeben werden, welche Daten auf dem Internet-PC abgespeichert werden dürfen und welche Verzeichnisse hierfür vorgesehen sind. Es muss auch geregelt werden, unter welchen Bedingungen

Daten vom Internet-PC in das Hausnetz oder umgekehrt transportiert werden dürfen.

In beiden Fällen ist mindestens eine Prüfung auf Computer-Viren durchzuführen. Für den Import von Daten und Programmen ins Hausnetz wird der Einsatz eines Schleusen-PCs empfohlen.

Falls eine lokale Datenhaltung auf dem Internet-PC vorgesehen ist, muss geregelt werden, ob die Benutzer für eine evtl. erforderliche Datensicherung selbst verantwortlich sind oder ob dies automatisch bzw. durch die Administration geschieht. Dies ist besonders wichtig, wenn der Internet-PC für E-Mail, Banking, elektronische Beschaffung oder ähnliche Aufgaben eingesetzt wird.

Die Benutzer müssen darüber belehrt werden, welche Angebote, z. B. illegale Inhalte, Pornographie oder Extremismus, auf keinen Fall genutzt werden dürfen. Außerdem müssen die Benutzer darüber belehrt werden, dass sie sich bei der Nutzung des Internets an geltende Rechtsvorschriften und die "Netiquette" halten müssen, da sie ja im Namen der Behörde bzw. des Unternehmens agieren.

Für die Einwahl beim Internet Service Provider oder für die lokale Anmeldung am Internet-PC werden meist Passwörter benötigt. In den Richtlinien sollte vorgegeben werden, welches Format und welche (Mindest-)länge diese Passwörter haben und wie oft sie geändert werden müssen.

Falls eine Benutzer-Authentisierung im Einsatzkonzept vorgesehen ist, sind die Benutzer darüber zu belehren, dass sie mit den Authentisierungsgeheimnissen sorgfältig umgehen und sich vom System abmelden müssen, wenn sie den Internet-PC verlassen.

Schließlich sollte festgelegt werden, ob das für die Einwahl beim Internet Service Provider benötigte Passwort abgespeichert werden darf oder ob es bei jeder Einwahl erneut eingegeben werden muss. Diese Entscheidung sollte auf einer Einschätzung beruhen, wie groß die Gefahr einer missbräuchlichen Nutzung der Internet-Anbindung im vorliegenden Einsatzumfeld ist. Ein doppelter Zugangsschutz (erst Benutzeranmeldung, dann Eingabe des Einwahlpasswortes) wird von Benutzern oft nicht akzeptiert.

Je nach Anwendungsfall und Einsatzumgebung müssen unter Umständen weitere Richtlinien oder Regelungen für den Internet-PC getroffen werden.

Prüffragen:

- Sind verbindliche Richtlinien für die Nutzung von Internet-PCs festgelegt?
- Sind die Richtlinien für die Nutzung von Internet-PCs den Benutzern sowie den zuständigen Administratoren bekannt?
- Sind die Benutzer von Internet-PCs über die damit verbundenen Risiken informiert?
- Ist festgelegt, welche Personen den Internet-PC zu welchen Zeiten und für welche Zwecke benutzen dürfen?
- Ist festgelegt, ob ausschließlich eine dienstliche oder auch eine private Nutzung des Internet-PCs zugelassen ist?
- Ist dokumentiert, welche Programme für die Nutzung von Internet-Diensten verwendet und ob aktive Inhalte auf dem Internet-PC ausgeführt werden dürfen?
- Ist sichergestellt, dass Client-Programme für die Nutzung von Internet-Diensten nicht unter dem Administrator-Benutzerkonto gestartet werden?

- Ist geregelt, welche persönlichen Daten und Informationen über die Organisation über den Internet-Zugang weitergegeben werden dürfen?
- Ist geregelt, welche Daten auf dem Internet-PC gespeichert und unter welchen Bedingungen in das Hausnetz oder heraus transportiert werden dürfen?
- Sind die Benutzer darüber belehrt, welche Internet-Angebote nicht genutzt werden dürfen und welche Rechtsvorschriften zu beachten sind?
- Sind Passwort-Kriterien für den Zugang zu Internet-Diensten festgelegt?

# M 2.236 Planung des Einsatzes von Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Grundsätzlich gibt es zwei Einsatzszenarien für eDirectory:

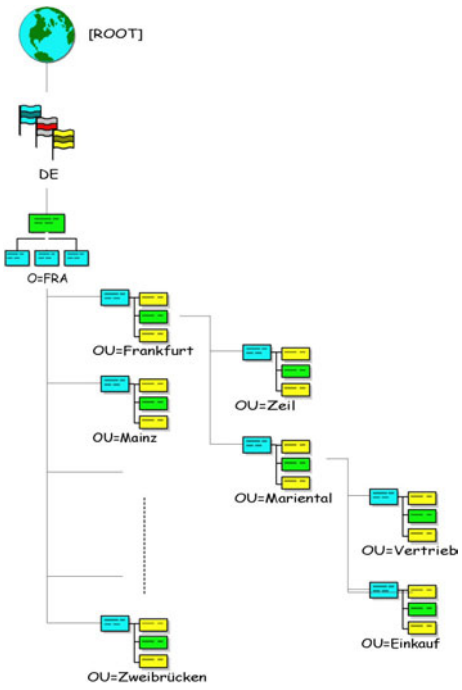
- der Einsatz als Managementprodukt für Ressourcen in einem gegebenen Netz oder
- die Verwendung als (Meta-)Verzeichnisdienst (LDAP-Server).

Abstrakt gesehen bildet das eDirectory eine hierarchisch und baumartig organisierte, Objekt-basierte Datenbank. Es ist an den Verzeichnisdienst-Standard X.500 angelehnt, von dem es die interne Struktur und den internen Aufbau entliehen hat. Es ist jedoch kein X.500-kompatibler Verzeichnisdienst, da das Zugriffsprotokoll auf dem proprietären NDAP(Novell Directory Access Protocol) basiert.

Das Baum-Konzept von eDirectory stellt sich auf folgende Weise dar: in einem Baum (*Tree*) werden Server, Benutzer und weitere Ressourcen abgebildet und können durch den Baum-Administrator verwaltet werden. Ein Baum bildet grundsätzlich eine administrative Grenze und limitiert auch den Wirkungsbereich von Berechtigungen.

Ein eDirectory-Verzeichnisbaum besteht aus verschiedenen Objekten. Jedes Objekt gehört einer ausgezeichneten Klasse an, z. B. Benutzerobjekt oder Serverobjekt, und ist gemäß dieser Klasse aus verschiedenen Attributen bzw. Eigenschaften zusammengesetzt. Die verschiedenen Objektattribute können unterschiedliche Werte aufnehmen, z. B. Telefonnummer oder IP-Adresse. Die Informationen über die bestehenden Objektklassen inklusive der darin vorkommenden Attribute werden im Directory-Schema gehalten. Durch Änderungen der Schemadefinition können neue Objektklassen erzeugt oder bestehende Objektklassen mit veränderten Attributsätzen versehen werden. Bei Veränderung des Schemas spricht man dann vom *Extended Schema*. eDirectory kennt verschiedene vordefinierte Objekttypen:

- *Tree-Objekt*: Dieses Objekt ist die Wurzel aller eDirectory-Objekte eines Verzeichnisbaums und enthält Informationen über diesen, z. B. Name des Baums. Unterhalb des Tree-Objekts können weitere Objekte angeordnet sein.
- *Container-Objekte*: Diese Objekte dienen dazu, andere Objekte zu gruppieren. Standardmäßig stehen die Objekte Land (Country, C), Organisation (Organization, O) und Organisations-Einheit (Organizational Unit, OU) zur Verfügung. Unterhalb eines OU-Objektes können weitere OU-Objekte enthalten sein, sowie so genannte Leaf-Objekte (siehe unten).
- *Leaf-Objekte*: Dies sind Server-, Benutzer-, Benutzer-Gruppen-, Rollen-, Drucker-, Druckerwarteschlangen-, Profil- sowie Applikations-Objekte. Weiterhin können auch Alias-Objekte zum Verweis auf bestehende Objekte in anderen Teilbäumen definiert werden.




In einem eDirectory-Baum gibt es immer eine ausgezeichnete Wurzel, die eine gewisse Sonderstellung besitzt: sie wird bestimmt durch den ersten Server, der in einem Baum installiert wird. Auf diesem Server läuft die Zertifizierungsstelle (CA) des Baums, der Voraussetzung für die Einbindung weiterer eDirectory-Server in den Baum ist. Die CA kann später auch auf einen anderen eDirectory-Server verschoben werden. Sämtliche weiteren eDirectory-Installationen müssen sich bei dem gegebenen eDirectory-Baum anmelden. Dabei muss der genaue Kontext, in dem der eDirectory-Server in einen bestehenden Baum eingebunden wird, angegeben werden. Ein späteres Verschieben der eDirectory-Server ist nur sehr schwer möglich, so dass der Server-Kontext im Voraus geplant werden muss.

Die ersten drei eDirectory-Server eines Baums erhalten automatisch eine vollständige Replica der Verzeichnisdaten, die weiteren nicht mehr - sofern dies nicht explizit so konfiguriert wird.

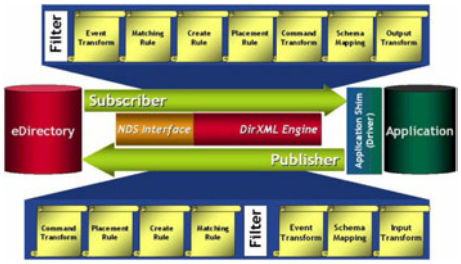
Nach einer Standardinstallation existiert eine zunächst einfache eDirectory-Struktur, die von eDirectory angelegt wird und dann entsprechend der Planung verändert werden kann. Da eDirectory primär der Verwaltung von IT-Ressourcen dient, sollte beim Aufbau der eDirectory-Baumstruktur darauf geachtet werden, dass die Struktur vornehmlich auf administrative Gegebenheiten abgestimmt wird. Wenn stattdessen zwanghaft die organisatorische Unternehmensstruktur bis ins Kleinste nachgebildet wird, kann dies zu Problemen in der Administration führen.

Es ist weiterhin darauf zu achten, dass die gewählte Baumstruktur nicht zu flach ist, damit sich die Replizierung zwischen den eDirectory-Servern nicht auf den gesamten Baum auswirkt. Der Ausfall eines einzelnen eDirectory-Servers oder der Verbindung dieses Servers zum Restsystem führt anderenfalls zu Fehlermeldungen sämtlicher in den Replizierungsring eingebundener Server.

Die möglichen Anordnungen von eDirectory-Objekten, d. h. welches Objekt welche anderen Objekte enthalten darf, welche Attribute existieren und aus

welchen Attributen Objekte zusammengesetzt werden, wird durch das so genannte eDirectory-Schema definiert. Das von eDirectory vorgegebene Schema kann verändert werden, dies stellt jedoch einen gravierenden Eingriff in die Verzeichnisstruktur dar, der nur nach sorgfältiger Planung durchgeführt werden darf.

Der eDirectory-Verzeichnisdienst bietet die Möglichkeit, mit anderen Verzeichnisdiensten über einen Synchronisationsmechanismus Daten im XML-Format abzugleichen. Als XML-Schnittstelle steht dazu das Produkt *DirXML* zur Verfügung. Diese besteht aus einem Kern (*engine*) und verschiedenen Treibern für diverse unterstützte Zielsysteme, z. B. Lotus Notes, SAP R/3, Windows 2000 Active Directory, Netscape (iPlanet), etc. Es gibt dabei zwei Kommunikationskanäle: Zum einen den so genannten *Publisher Channel*, unter dem fremde Verzeichnisdienste Änderungen ihres Datenbestandes dem eDirectory mitteilen können. Zum anderen gibt es den *Subscriber Channel*, mit dessen Hilfe eingeschriebene fremde Verzeichnisdienste von Änderungen im eDirectory erfahren.




Der Einsatz der *DirXML*-Schnittstelle bedarf auf jeden Fall einer genauen Planung, um später unerwünschte Seiteneffekte zu vermeiden, z. B. Endlosschleifen.

Im Rahmen der eDirectory-Planung sind folgende Aspekte zu berücksichtigen:

- Welche Gliederung in Organisations-, Organisationseinheit- und weitere Container-Objekte soll gewählt werden?
- Welche Objektklassen werden benötigt und welche Attribute sollen diese haben?
- Welche Benutzer und Server sollen in welchen Organisationseinheiten zusammengefasst werden?

Für jede Organisation muss entschieden werden,

- welche Administratorgruppen benötigt werden,
- welches administrative Modell umgesetzt wird (zentrale oder dezentrale Verwaltung),
- welche administrativen Rollen innerhalb der Baumstruktur existieren sollen,
- ob und an wen administrative Aufgaben delegiert werden sollen,
- welche Sicherheitseinstellungen für verschiedene Typen von Servern und Benutzergruppen gelten sollen,
- auf welche Informationen über die verschiedenen eDirectory-Schnittstellen (z. B. eDirectory-Clients, LDAP) von wem zugegriffen werden darf.

Generell muss die geplante eDirectory-Struktur dokumentiert werden. Dies trägt maßgeblich zur Stabilität, konsistenten Administration und damit zur Systemsicherheit bei. Es empfiehlt sich insbesondere festzuhalten:

- Welche Schemaänderungen werden durchgeführt? Dabei sollen auch die Gründe für die Änderung dokumentiert sein.

- Welche Objektklassen werden in welcher Weise verwendet, speziell welche Attribute werden für welche Inhalte genutzt?

Für jedes eDirectory-Objekt sollte dokumentiert sein:

- Name und Position im eDirectory-Baum (z. B. "StandortBerlin", Vater-Objekt: OU "Filialen-Deutschland"),
- welchem Zweck das Objekt dient,
- welche administrativen Zugriffsrechte für das Objekt und dessen Attribute vergeben werden sollen (z. B. vollständig verwaltet von "Admin1"),
- wie die Vererbung von eDirectory-Rechten konfiguriert werden soll, z. B. blockieren oder filtern der Rechtevererbung,
- welche Sicherheitsäquivalenzen zwischen Objekten bestehen sollen.

Die eDirectory-Administration und das benutzte administrative Modell muss auf jeden Fall geplant werden. Besonders auch die Einrichtung einer Rollen-basierten Administration und die Möglichkeit der Delegation von Administrationsaufgaben sind sicherheitskritisch. Bei sinnvoller, übersichtlicher und konsistenter Planung kann die Sicherheitsadministration durch diese Funktionalitäten transparenter und effizienter gestaltet werden.

Die Nutzung von eDirectory beinhaltet den Betrieb einer eigenen, eingebundenen Zertifizierungsstelle (CA). Auch hier muss sich die Planung nach den Anforderungen und besonders nach der zuvor aufgestellten Sicherheitsleitlinie richten.

Zusammengefasst ergeben sich folgende sicherheitsrelevante Kernaspekte bei der eDirectory-Planung:

- Bäume begrenzen die administrative Macht von Administratoren und den Verzeichnisdienst an sich.
- Standardmäßig ist bei der Erstinstallation von eDirectory der Benutzer *Admin* innerhalb des Organisationscontainers des eDirectory-Baums angelegt. Dieser besitzt das so genannte *Supervisor*-Recht auf den gesamten Baum.
- Administrative Delegation wird durch die Vergabe von Zugriffsrechten auf eDirectory-Objekte und deren Attribute erreicht. Die Verteilung der Zugriffsrechte muss gemäß dem administrativen Modell erfolgen. Die Mechanismen für Zugriffsrechte im eDirectory sind unter anderem Vererbung, Kontrolle der Vererbung, Wirkungsbereich von Zugriffseinstellungen und Sicherheits-Äquivalenz zwischen Objekten. Damit können sehr komplexe Berechtigungsstrukturen aufgebaut werden, die sehr schnell unübersichtlich und nicht mehr administrierbar werden, so dass sich durch Fehlkonfigurationen im eDirectory Sicherheitslücken ergeben können. Eine möglichst einfache Berechtigungsstruktur ist daher vorzuziehen.
- Schemaänderungen sind kritische Operationen und dürfen nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt werden.

Abschließend sei darauf hingewiesen, dass Fehler in der eDirectory-Planung und den zugrunde liegenden Konzepten nach erfolgter Installation nur mit beträchtlichem Aufwand zu berichtigen sind.

Prüffragen:

- Wurde für jeden geplanten eDirectory-Server sein genauer Kontext innerhalb des Verzeichnisbaumes festgelegt?
- Wurde eine eDirectory-Planung durchgeführt und dokumentiert?
- Wurde die Synchronisation der Verzeichnisdaten mit weiteren Verzeichnisdiensten geplant?

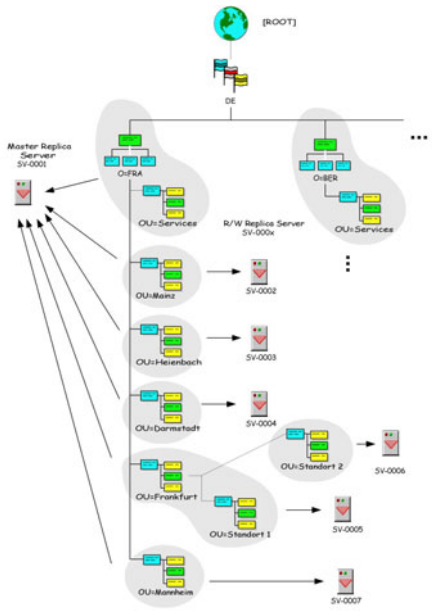
- Werden bei Schemaänderungen die Gründe für die Änderung dokumentiert?
- Wurde das Konzept der Rollen-basierten Administratoren konsistent geplant?
- Werden Schemaänderungen nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt?

# M 2.237 Planung der Partitionierung und Replikation im Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Als skalierbarer Verzeichnisdienst bietet eDirectory die Möglichkeit, Teile der Verzeichnisdatenbank in Partitionen zu zerlegen und auf verschiedene eDirectory-Server zu verteilen. Dies verkürzt die mittleren Zugriffszeiten, da die Suche sich unter Umständen nur auf eine spezielle Partition und nicht den gesamten Verzeichnisbaum erstrecken muss. Außerdem erhöht es die Ausfallsicherheit, da bei einem Serverausfall nur die dort befindliche Partition und nicht die gesamte Verzeichnisdatenbank betroffen ist. Weiterhin erlaubt es die Partitionierung, die Daten gemäß einer zuvor vorgenommenen Klassifizierung auf entsprechend gesicherte Server zu verteilen.

Bei der Planung der Partitionierung sind die vom eDirectory definierten Regeln für Partitionen zu berücksichtigen.




Partitionen können wiederum Unterpartitionen enthalten, welche gemäß den festgelegten Regeln gebildet wurden. Auf Partitionen können verschiedene Operationen ausgeführt werden, z. B. Erzeugen, Zusammenführen, Bewegen oder Annullieren einer der genannten Operationen.

Neben dem Mechanismus der Partitionierung des Verzeichnisbaums bietet eDirectory die Möglichkeit, Teile des Verzeichnisbaums auf andere eDirectory-Server zu replizieren. In der Terminologie von eDirectory wird dabei von *Replicas* gesprochen. In jeder Partition gibt es eine so genannte *Master-Replica*. Diese bildet den Mittelpunkt der jeweiligen Partition. Das Anlegen neuer Unterpartitionen oder neuer Replicas der aktuellen Partition ist von der Verfügbarkeit des *Master-Replica-Servers* abhängig. Es gibt verschiedene Möglichkeiten, die Verzeichnisdaten auf andere Server zu replizieren:

- *Read/Write Replica*: Auf Read/Write Replicas einer Partition kann genauso zugegriffen werden, wie auf die Master-Replica selbst. Insbesondere ist es in einer Read/Write Replica möglich, Modifikationen der Daten vorzunehmen. Die Informationen werden automatisch zwischen den einzel-

nen Replicas ausgetauscht. Sofern der Server, auf dem die Master-Replica gehalten wird, dauerhaft ausfällt, kann eine Read/Write Replica zur Master-Replica umkonfiguriert werden.
- *Read-Only Replica*: Diese Replicas empfangen lediglich Synchronisations-Updates von anderen Replicas. Clients können den Inhalt einer Read-Only Replica nicht ändern.
- *Filtered Read/Write Replica*: Auf diese Server wird lediglich ein Teil einer eDirectory-Partition repliziert. Die Auswahl des replizierten Inhaltes ist dabei sowohl auf der Ebene der Objektklassen als auch auf der Ebene einzelner Attribute möglich. Der Inhalt dieser Replica kann von Clients verändert werden. Bei einer Änderung des Informationsstandes wird der Inhalt automatisch mit den weiteren Replicas synchronisiert.
- *Filtered Read-Only Replica*: Dieser Typ einer Replica enthält nur eine Auswahl der gesamten Partition, die zudem nicht durch Clients verändert werden kann. Für die Auswahl des zu replizierenden Inhaltes bestehen die gleichen Möglichkeiten wie bei Filtered Read/Write Replicas.

Die oben beschriebenen Arten von Replicas werden manuell eingerichtet und konfiguriert. Die Replizierung selbst läuft automatisch ab. Ein weiterer Replikationstyp sind die *Subordinate-Reference-Replicas*. Diese werden vom eDirectory-System jedoch selbst angelegt und verwaltet. Sie enthalten lediglich Sprungadressen, um effizient Objektnamen über Partitionsgrenzen hinweg auflösen zu können (so genanntes *tree walking*).

Bei der Planung der Partitionen sollten folgende Punkte beachtet werden:

- Berücksichtigung des Schutzbedarfs: Die Informationen, die im Verzeichnis gehalten werden, sollten gemäß ihrem Schutzbedarf klassifiziert werden. Anhand dieser Klassifizierung sollte die Verteilung der Objekte auf entsprechend geschützte Server erfolgen. Dabei ist darauf zu achten, dass besonders der Inhalt des Security-Containers auf einem ausreichend abgesicherten Server gelagert wird, da es sich hierbei um sensitive Informationen handelt. Im Security-Container werden beispielsweise die *Key Management Objects* sowie die *Security Policies* gespeichert.
- geforderte Verfügbarkeit des Verzeichnisdienstes: Zur Verbesserung der Lastverteilung müssen hinreichend viele Repliken der Verzeichnisdaten auf eDirectory-Servern angelegt werden.
- Verteilung der Administrationsaufgaben: Damit eine Rollentrennung der Administrationsaufgaben mit der Trennung der Datenhaltung einhergeht, sollten die Administrationsaufgaben auf einzelne Partitionen verteilt werden.
- Einhaltung der eDirectory-Regeln zur Partitionierung. Die wesentlichen Regeln dabei sind:
    - Jede Partition beginnt hierarchisch mit einem einzelnen Container-Objekt.
    - Die Partition muss ein zusammenhängender Sub-Tree des eDirectory-Baums sein.
    - Verschiedene Partitionen dürfen sich nicht überschneiden.
    - Der Name der Partition muss der *Fully Qualified Distinguished Name* (*FQDN*) des Wurzelobjekts der Partition sein.
- Die genauen Kontexte der Server, welche Partitionen/Replicas halten. Ist die Struktur zu flach, so entsteht ein hoher interner Replizierungsaufwand. Darüber hinaus führen einzelne - momentan nicht verfügbare - Server zu entsprechenden Statusmeldungen bei sämtlichen weiteren in den Replizierungsring eingebundenen eDirectory-Servern.

Bei der Planung der Replicas sind folgende Punkte zu berücksichtigen:

- Aus den Anforderungen an Verfügbarkeit und Ausfallsicherheit des Verzeichnisdienstes müssen die Vorgaben für die Anzahl der anzulegenden Replicas abgeleitet werden.
- Die geforderte Systemperformance führt zur Planung der Lastverteilung.
- Es muss entschieden werden, ob durch die Definition von Filtern für Replicas ein Sicherheitsgewinn erzielt werden kann.
  Dieser liegt vor allem in der Möglichkeit einer getrennten Datenhaltung entsprechend einer zuvor vorgenommenen Klassifizierung der Daten. Es kann damit das Grundprinzip realisiert werden, dass jeder eDirectory-Server nur diejenigen Daten hält, welche er "benötigt" (bzw. welche die zugreifenden Nutzer oder Applikationen benötigen).
  Bei unbedachter Konfiguration kann dieser Sicherheitsgewinn allerdings wirkungslos bleiben. Ein möglicher Nachteil kann die Systemperformance sein. Sind gesuchte Daten auf einem eDirectory-Server nicht vorhanden bzw. nicht sichtbar, weil sie durch entsprechende Filterregeln ausgeblendet sind, so wird im Hintergrund weitergesucht (sofern dies zugelassen ist). Eine nicht bedarfsgerechte Konfiguration der Filterregeln kann also die Systemperformance negativ beeinflussen.
  **Beispiel:** Ein eDirectory-Server steht im Intranet einer Organisation und eine Teilmenge der dort gehaltenen Verzeichnisdaten soll auch im Internet verfügbar sein. Eine mögliche Lösung ist, einen weiteren eDirectory-Server in der demilitarisierten Zone (DMZ) zwischen Intranet und Internet mit einer gefilterten Replica aufzustellen, welche nur die im Internet tatsächlich benötigten Verzeichnisdaten hält.
- Die Datenhaltung muss geplant werden. Hier geht es um eine möglichst detaillierte Planung, welche Daten von wem und von wo aus zugreifbar sein sollen. Für die Durchsetzung der Vorgaben können beispielsweise gefilterte Replicas eingesetzt werden.

Prüffragen:

- Sind die Informationen, die im eDirectory-Verzeichnis gehalten werden, gemäß ihrem Schutzbedarf klassifiziert?
- Wurden aus den Anforderungen an Verfügbarkeit und Ausfallsicherheit des Verzeichnisdienstes die Vorgaben für die Anzahl der anzulegenden Replicas abgeleitet?
- Planung der Datenhaltung: Existiert eine möglichst detaillierte Planung, welche Daten von wem und von wo aus zugreifbar sein sollen?

# M 2.238 Festlegung einer Sicherheitsrichtlinie für Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Als eine der organisatorischen Hauptaufgaben bei der Planung des eDirectory-Einsatzes muss zunächst eine Sicherheitsrichtlinie fixiert werden. Durch die Sicherheitsrichtlinie wird festgelegt, welche Sicherheitsbestimmungen in einem eDirectory-System gelten sollen und wie diese bei der Installation umgesetzt werden müssen.

Durch die eDirectory-Sicherheitsrichtlinie sollten sämtliche sicherheitsbezogenen Themenbereiche eines eDirectory-Verzeichnisdienstes geregelt werden. Die folgende Liste gibt einen groben Überblick über die Bereiche, die durch eine solche Richtlinie geregelt werden sollten. Die Liste muss je nach Einsatzszenarien in der Behörde bzw. im Unternehmen entsprechend angepasst, ausgestaltet und erweitert werden.

**Allgemeines:**
- Wie sollen eDirectory-Server physikalisch abgesichert werden?
- Welche eDirectory-Komponenten, z. B. ConsoleOne und iMonitor, sollen genutzt werden?
- Welche Baumstruktur soll gewählt werden?
- Wie wird diese Baumstruktur partitioniert?
- Werden Schemaänderungen vorgenommen?
- Welche Objektklassen mit welchen Attributsätzen werden eingesetzt?
- Welche Repliken welchen Typs sollen angelegt werden?
- Welche Rechner sind eDirectory-Server und welche Rechner halten eine Replica?

**Rechtevergabe:**
- Welcher Benutzer darf welche Rechte ausüben?
- Welcher Administrator darf welche Rechte ausüben?
- Welche Authentisierungsverfahren sollen gewählt werden?
- Wie wird die Vererbung von Rechten innerhalb der Baumstruktur definiert?
- Welche Sicherheitsäquivalenzen zwischen Objekten oder Objektklassen werden definiert?

**Administration:**
- Welche Administratorrollen werden definiert?
- Wer darf Schemaänderungen vornehmen?
- Welche Administrationsaufgaben dürfen bzw. sollen delegiert werden?

**Datenkommunikation:**
- Welche Datenkommunikation ist abgesichert abzuwickeln?
- Mit welchen Mechanismen werden ggf. Vertraulichkeit, Integrität und Authentizität der Daten geschützt?

**Zertifikatsautorität:**
- Welche Parameter für die CA sind zu verwenden?
- Wer darf Einstellungen der CA ändern?
- Welche Objekte sind mit Zertifikaten zu versehen?
- Welche Zertifikate sind für SSL-Verbindungen einzusetzen?

**Dateisystem des unterliegenden Betriebssystems:**
- Welche Berechtigungen auf Systemdateien gelten für die verschiedenen Administratoren und Benutzer?
- Soll Verschlüsselung auf Dateisystemebene eingesetzt werden?

**LDAP:**
- Welche Benutzer dürfen unter welchen Bedingungen über LDAPauf das eDirectory zugreifen?
- Soll anonymer Login unterstützt werden?
- Welche Netzapplikationen dürfen via LDAP auf das eDirectory zugreifen?
- Soll die LDAP-Kommunikation generell über SSL laufen?
- Dürfen die Benutzerpasswörter im Klartext übertragen werden?

**Client-Zugriff auf den eDirectory-Verzeichnisdienst:**
- Welche Authentisierungsverfahren sollen eingesetzt oder erlaubt werden?
- Auf welchen Verzeichnisbaum darf vom Netz aus zugegriffen werden?
- Welche Ressourcen sind aus dem Netz von welchen Benutzern zugreifbar?

**Verschlüsselung von Attributen**
- Soll der *Secret Store* Mechanismus (verfügbar über das Zusatzmodul *Secure Login*) zur Verschlüsselung von Attributen genutzt werden?

**Fernzugriff zur Systemüberwachung und Administration:**
- Darf das Tool *iMonitor* genutzt werden?
- Wer darf das Tool *iMonitor* nutzen?
- Wie wird das Protokoll HTTPS zu diesem Zweck konfiguriert?

Diese komponentenspezifische Auflistung von Themengebieten kann in folgende zeitliche Abfolge gebracht werden:

**1. Definition der eDirectory-Baumstruktur**

Im ersten Schritt ist die logische Struktur des eDirectory-Baumes, die Aufteilung in Organisation und Organisationseinheiten sowie insbesondere auch die Zuordnung der Server und der zu verwaltenden Netz-Ressourcen festzulegen (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*).

Anschließend muss über die im Verzeichnisdienst gehaltenen Objekte und deren Attribute entschieden werden. Bei Bedarf sind hierzu Schemaänderungen am eDirectory vorzunehmen. Weiterhin sollte an dieser Stelle über die Partitionierung der Verzeichnisdaten und über die Einrichtung von Repliken entschieden werden (siehe M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*).

**2. Regelung der Verantwortlichkeiten**

Ein eDirectory-Verzeichnisdienst sollte von geschulten Netzadministratoren sicher betrieben werden. Dabei ist im Rahmen der Notfallvorsorge eine geeignete Stellvertreterregelung zu treffen. Generell sollte ein Konzept zur rollenbasierten Administration erstellt werden. Nur die berechtigten Sicherheits-Administratoren dürfen eDirectory-Sicherheitsparameter verändern.

Die Verantwortlichkeiten der einzelnen Benutzerdes eDirectory-Verzeichnisses sind unter Schritt 10 dargestellt.

**3. Festlegung von Namenskonventionen**

Um die Verwaltung des eDirectory-Verzeichnisbaums zu erleichtern, sollten eindeutige Namen für die Server, Applikationen, Drucker, Benutzer, Benutzergruppen und die weiteren eDirectory-Objekte verwendet werden.

**4. Festlegung der Regeln für Benutzerkonten**

Vor der Einrichtung von Benutzerkonten sollten die Restriktionen, die für alle oder nur für bestimmte Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge. Außerdem sollte das Erstellen der Login-Skripts geregelt werden.

**5. Einrichtung von Gruppen (Organizational Roles)**

Zur Vereinfachung der Administration sollten Benutzer-Objekte, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Die korrespondierenden eDirectory-Objekte heißen *Organizational Roles*. Benutzerrechte sowie Zugriffsrechte auf Verzeichnisobjekte und gegebenenfalls weitere vordefinierte Funktionen werden dann den Gruppen (Organizational Roles) und nicht einzelnen Benutzer-Objekten zugeordnet. Die Benutzer-Objekte erben die Rechte und Berechtigungen der Gruppen (Organizational Roles), denen sie angehören. So ist es z. B. denkbar, alle Mitarbeiter einer Abteilung in einer Gruppe (Organizational Role) zusammenzufassen. Benutzerberechtigungen sollten nur dann einzelnen Benutzern zugewiesen werden, wenn dies ausnahmsweise unumgänglich ist.

**6. Festlegung der Vorgaben für Protokollierung**

Hierbei ist festzulegen, welche vom eDirectory generierten Ereignisse zu protokollieren sind und bei welcher Ereigniskombination eine Benachrichtigung an den Sicherheits- bzw. Systemadministrator zu erfolgen hat. Weiterhin muss entschieden werden, wie lange die gesammelten Ereignisdaten aufzubewahren sind.

**7. Regelungen zur Datenspeicherung**

Es ist festzulegen, wo Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). Bei eDirectory werden Benutzerdaten nur auf eDirectory-Servern abgelegt. Eine Datenspeicherung auf den lokalen Festplatten der einzelnen Clients findet nicht statt. Die Frage nach der Datenspeicherung ist jedoch auf der Ebene einzelner Partitionen zu klären. Datenbestände sollten in Bezug auf ihren Schutzbedarf klassifiziert werden, und entsprechend sollte die Partitionierung des Verzeichnisses auf vertrauenswürdige und gesicherte Hosts vorgenommen werden. Dabei sind besonders die hochsensiblen Daten des Security-Containers zu berücksichtigen.

**8. Einrichtung von Projektverzeichnissen**

Um eine saubere Trennung von benutzer- und projektspezifischen Daten (Objekten) untereinander durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, die eine solche Objekthaltung unterstützt.

**9. Vergabe der Zugriffsrechte**

Für die Objekte des Verzeichnisdienstes ist festzulegen, welche Attribute für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind.

**10. Verantwortlichkeiten der Administratoren und Benutzer im Client-Server-Netz**

Neben der Wahrnehmung der Netzmanagement-Aufgaben (siehe Nr. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren im eDirectory-Verzeichnissystem übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Verwaltung des eDirectory-Baums oder einzelner Partitionen,
- die Verwaltung der Schemadefinition,
- die Verwaltung der CA und der Key Management Objekte (KMO),
- die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
- die Vergabe von Zugriffsrechten,
- das Hinterlegen und den Wechsel von Passwörtern und die Durchführung von Datensicherungen.

Auch die Benutzer müssen in einem eDirectory-Verzeichnisdienst mit Client-Zugriff bestimmte Verantwortlichkeiten übernehmen, insbesondere wenn ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden.

In der Regel beschränkt sich dies jedoch auf die Vergabe der eigenen Passwörter für das Login.

**11. Schulung**

Abschließend muss festgelegt werden, welche Benutzer zu welchen Teilaspekten geschult werden müssen. Erst nach ausreichender Schulung kann der Produktivbetrieb aufgenommen werden. Besonders die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit von eDirectory gründlich zu schulen.

Die so entwickelten Sicherheitsrichtlinien sind zu dokumentieren und im erforderlichen Umfang den Benutzern des eDirectory-Verzeichnisdienstes mitzuteilen. Bei der Definition der Sicherheitsrichtlinie für eDirectory ist zu beachten, dass sie sich an den bisher geltenden Sicherheitsrichtlinien der Behörde bzw. des Unternehmens orientieren muss, diesen nicht widersprechen (Konsistenz) und auch nicht im Widerspruch zu geltendem Recht stehen darf. In der Regel wird eine eDirectory-Sicherheitsrichtlinie existierende Regelungen spezifisch anpassen oder aber sinngemäß erweitern, z. B. durch zusätzliche Anforderungen für Komponenten. Dabei sind unter Umständen neue Regelungen für eDirectory-spezifische Funktionalitäten, z. B. iMonitor, zu treffen. Generell gilt, dass sich die Planung des eDirectory-Verzeichnisdienstes an den jeweiligen Sicherheitsrichtlinien orientiert, dabei jedoch auch Einfluss auf die Sicherheitsrichtlinien besitzt (Feedback-Prozess).

Prüffragen:

- Sind alle für den geplanten Einsatz von eDirectory relevanten Bereiche durch Sicherheitsrichtlinien abgedeckt?
- Ist die logische Struktur des eDirectory-Baumes festgelegt und dokumentiert worden?
- Ist eine geeignete Stellvertreterregelung für den eDirectory-Verzeichnisdienst getroffen worden?
- Werden eindeutige Namen für die Server, Applikationen, Drucker, Benutzer, Benutzergruppen und die weiteren eDirectory-Objekte verwendet?

- Gibt es Regelungen zur Einrichtung von Benutzern und Gruppen (Organizational Roles) im eDirectory?
- Ist die Protokollierung der vom eDirectory generierten Ereignisse geregelt?
- Werden Benutzerdaten entsprechend ihrer Schutzbedarf-Klassifizierung gespeichert?
- Ermöglicht die eDirectory-Verzeichnisstruktur eine Trennung von benutzer- und projektspezifischen Daten (Objekten)?
- Ist für die Objekte des eDirectory-Verzeichnisdienstes festgelegt, welche Attribute für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind?
- Sind alle Benutzer über die eDirectory-Sicherheitsrichtlinien informiert?

# M 2.239 Planung des Einsatzes von Novell eDirectory im Intranet

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

eDirectory ist als Management-Produkt für IT-Ressourcen einer Organisation geeignet. Dazu wird die Organisationshierarchie auf einen eDirectory-Baum abgebildet und der Zugriff auf die im Verzeichnis gehaltenen Objekte entsprechend vergeben. Dabei können Automatismen, wie die Vererbung von Zugriffsberechtigungen auf Teilbäume und das Einrichten von Benutzergruppen (Organizational Roles), die Administration des Verzeichnissystems erleichtern.

eDirectory kann auf verschiedenen Serverplattformen betrieben werden: Netware, Windows NT/2000, Linux sowie Sun Solaris.

Neben dem prinzipiell für alle Applikationen möglichen LDAP-Zugang zum eDirectory bietet Novell spezielle Client-Software an, die für bestimmte Systeme das Ressourcen- und Benutzermanagement im eDirectory erlaubt. Dabei handelt es sich um

- den *Novell Client für Windows* (derzeit - Februar 2002 - in der Version 4.83 für Windows NT/2000/XP und Version 3.31 für Windows 95/98/ME),
- die *Novell User Account Management Software* für Solaris sowie Linux auf Intel-Plattform.

Dabei kann eDirectory auch zur Authentisierung von Netware-Servern und zur Zugriffskontrolle auf dort gehaltene Volumes genutzt werden.

Folgende Aspekte sind bei der Einrichtung eines eDirectory-Verzeichnisdienstes im Intranet zu planen:

- der Verzeichnisbaum und Abbildung der IT-Ressourcen darin,
- die einzusetzenden Objektklassen sowie deren Attributsätze,
- gegebenenfalls Planung einer Schemaänderung,
- die Einrichtung von Benutzern und Benutzergruppen (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*),
- die Anbindung von Benutzern an das eDirectory (siehe M 4.157 *Einrichten von Zugriffsberechtigungen auf Novell eDirectory*),
- die Zugriffsrechte von Benutzern auf das eDirectory (siehe M 4.157 *Einrichten von Zugriffsberechtigungen auf Novell eDirectory*),
- das Administrationskonzept für das eDirectory (siehe M 3.29 *Schulung zur Administration von Novell eDirectory*),
- die Partitionierung und die Replizierung (siehe M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*),
- der Zertifikatsdienst (siehe M 4.155 *Sichere Konfiguration von Novell eDirectory*),
- die Client-Anbindung an das eDirectory (siehe M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*),
- der LDAP-Zugriff auf das eDirectory durch Netzapplikationen (siehe M 4.158 *Einrichten des LDAP-Zugriffs auf Novell eDirectory*),
- die Verschlüsselung des Netzverkehrs,
- die Datensynchronisation mit fremden Verzeichnisdiensten mittels *DirXML*,
- der Einsatzes des *Service Location Protocols* (SLP),
- Audits (siehe M 4.160 *Überwachen von Novell eDirectory*),

- ein automatisiertes und protokolliertes periodisches Backup (siehe auch M 6.81 *Erstellen von Datensicherungen für Novell eDirectory*),
- die Notfallvorsorge für den Systemausfall (siehe auch M 6.106 *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes*).

Prüffragen:

- Ist in der Planung zum Einsatz des eDirectory im Intranet festgelegt, wie die IT-Ressourcen der Institution im Verzeichnisbaum abgebildet werden?
- Wurden die einzusetzenden Objektklassen sowie deren Attributsätze des eDirectory-Verzeichnisdienstes im Intranet festgelegt?
- Ist geklärt, ob und wie der Netzverkehr des eDirectory-Verzeichnisdienstes verschlüsselt wird?

# M 2.240 Planung des Einsatzes von Novell eDirectory im Extranet

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

eDirectory lässt sich auch als E-Business-Plattform im Internet betreiben. In diesem Zusammenhang fungiert das eDirectory oft als LDAP-Server, der Daten für seine Benutzer in seinem Verzeichnisdienst bereithält. Die Benutzeranbindung erfolgt dabei über das LDAP-Protokoll, welches auf TCP/IP aufsetzt.

Prinzipiell können sich Benutzer auf drei verschiedene Arten via LDAP mit eDirectory verbinden:

- als [Public] Objekt (*Anonymous Bind*),
- als Proxy User (*Proxy User Anonymous Bind*),
- als NDS User (*NDS User Bind*).

Hier ist bei der Planung speziell zu berücksichtigen, ob ein *Anonymous Bind* zugelassen wird oder nicht. Standardmäßig hat das [Public] Objekt uneingeschränktes *Browse*-Recht auf den eDirectory-Baum.

Die Planung sollte eine Aufteilung der Verzeichnisdaten in drei Kategorien vorsehen:

- Daten, auf die über anonymen Login zugegriffen werden kann,
- Daten, auf die nach erfolgreicher Authentisierung zugegriffen werden darf, sowie
- Daten, auf die von außen prinzipiell nicht zugegriffen werden darf.

Die Verzeichnisdaten sollten entsprechend dieser Aufteilung in getrennten Bereichen gespeichert werden. Dies erleichtert unter anderem die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes. Ein eDirectory-Server mit direkter Internet-Anbindung sollte möglichst keine Daten halten, auf die von außen nicht zugegriffen werden braucht.

Weiterhin ist bei Bedarf der Einsatz von SSL für den LDAP-Zugriff auf das eDirectory zu planen. Es ist dann zu entscheiden, ob die Authentisierung über Passwörter oder Zertifikate erfolgen soll. Wird SSL nicht eingesetzt, so muss entschieden werden, ob Passwörter im Klartext übertragen werden können oder ob die Option *allowing cleartext passwords* ausgeschaltet wird.

Da der eDirectory-Server in diesem Einsatzszenario über eine direkte Internet-Anbindung verfügt, ist der Einsatz einer Firewall zu planen. Eine geeignete Vorgehensweise hierzu findet sich in Baustein B 3.301 *Sicherheitsgateway (Firewall)*.

Prüffragen:

- Erfolgt die Strukturierung des eDirectory im Extranet anhand der Verzeichnisdaten, auf die von außen anonym, nach erfolgreicher Authentisierung oder gar nicht zugegriffen werden darf?
- Ist die Form der Authentisierung für den Zugang zum eDirectory von außen festgelegt?
- Werden die für Zugriffe auf das eDirectory übertragenen Daten angemessen abgesichert, z. B. durch Verschlüsselung?

# M 2.241 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bevor ein Telearbeitsplatz eingerichtet wird, ist es sinnvoll, eine Anforderungsanalyse durchzuführen. Sinn dieser Anforderungsanalyse ist es, alle in Frage kommenden Einsatzszenarien zu bestimmen, um daraus die benötigten Hard- und Software-Komponenten für die Anbindung des häuslichen Arbeitsplatzes abzuleiten. Hierdurch können spezielle Anforderungen identifiziert werden, die den Einsatz bestimmter Systeme und/oder Software erforderlich machen (siehe hierzu z. B. Baustein B 4.4 *VPN* oder Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN*).

Die Ergebnisse einer solchen Anforderungsanalyse müssen dokumentiert und mit den IT-Verantwortlichen abgestimmt werden.

Im Rahmen dieser Anforderungsanalyse sind u. a. folgende Fragen zu klären:

- Bis zu welchem Vertraulichkeitsanspruch dürfen Daten im Rahmen der Telearbeit am Telearbeitsplatz, also außerhalb der "schützenden Mauern" der Behörde bzw. des Unternehmens, bearbeitet werden?
- Zu welchem Zweck wird der Zugang zur Institution genutzt (Abfragen von Informationen, Einstellen von Informationen, Programmnutzung)?
- Wie hoch ist der Datenverkehr zwischen dem häuslichen Arbeitsplatz und der Institution?
- Benötigt der Telearbeiter Zugriff auf das Intranet der Institution? Wenn ja, muss der Zugriff auf das gesamte Intranet, d. h. auf alle dort verfügbaren Daten und Dienste erfolgen oder nur auf Teilbereiche des Intranets?
- Ist für die Telearbeiter die Nutzung des Internets vorgesehen? Wenn ja, bekommt der Telearbeiter einen eigenen Internet-Zugang oder wird dieser Zugang über das Intranet der Institution realisiert?

Je nach dem Vertraulichkeitsanspruch der Daten kann es erforderlich sein, bestimmte Übertragungswege von der Organisation zum Telearbeitsplatz festzulegen. Dabei kann es sinnvoll sein, bestimmte Übertragungswege auszuschließen oder Mindestanforderungen dafür festzulegen. Beispielsweise könnte es vorgeschrieben sein, Papierdokumente mit vertraulichen Informationen nur auf direktem Weg von der Organisation zum Telearbeitsplatz in verschlossenen Transportbehältern zu transportieren. Ebenso könnten für verschiedene Vertraulichkeitsgrade unterschiedliche Verschlüsselungsverfahren für die Datenübertragung vorgesehen sein.

Ähnliche Überlegungen sollten angestellt werden, wenn die im Rahmen der Telearbeit zu verarbeitenden Informationen besonders vor Manipulation geschützt werden müssen.

Prüffragen:

- Wurde eine Anforderungsanalyse für den Telearbeitsplatz durchgeführt?
- Wurden die Anforderungen an den Telearbeitsplatz mit den IT-Verantwortlichen (Administratoren und anderem technischem Personal) abgestimmt?
- Wurde der Schutzbedarf der Informationen, die im Rahmen der Telearbeit verarbeitet werden, festgestellt und dokumentiert?

# M 2.242 Zielsetzung der elektronischen Archivierung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um eine elektronische Archivierung in einer Institution einzuführen, sind die Ziele festzulegen, die damit erreicht werden sollen. Dabei muss das Management der betreffenden Organisation einbezogen werden. Gegebenenfalls ist eine Koordinierung mit übergeordneten Organisationseinheiten notwendig. Insbesondere ist festzulegen,

- in welchen Bereichen welche Daten archiviert werden sollen,
- welches Sicherheitsniveau es zu erreichen gilt,
- welcher Funktions- und Leistungsumfang angestrebt ist und
- wer die Verantwortung hierfür trägt.

Die Ergebnisse sind im Archivierungskonzept (siehe Maßnahme M 2.243 *Entwicklung des Archivierungskonzepts*) zu fixieren.

**Welche Daten sind zu archivieren?**

Die Bestimmung der zu archivierenden Daten dient der Eingrenzung der technischen Anforderungen an das auszuwählende Archivsystem. Die Eingrenzung sollte aber so allgemein erfolgen, dass ausreichend Spielraum für die technische Ausgestaltung bleibt, wobei zu beachten ist, dass sich Anforderungen auch im Laufe der Zeit ändern können. Besonders auf Managementebene sind allgemeine Charakterisierungen sinnvoll wie:

- alle Daten/Dokumente der Abteilung,
- alle Daten/Dokumente der Geschäftsprozesse,
- alle Geschäftsdaten,
- alle Buchhaltungsdaten,
- alle Kundendaten, sowie
- alle Daten der Klassifikationsstufe.

Wenn Daten mit unterschiedlichem Schutzbedarf archiviert werden sollen, wird empfohlen, die Ziele und Anforderungen an die Archivierung anhand der jeweiligen Schutzbedarfskategorie zu definieren. Ein Beispiel hierfür ist die Archivierung von Dokumenten, die als offen, intern, geheim o. ä. klassifiziert worden sind.

**Welches Sicherheitsniveau soll erreicht werden?**

Das zu erreichende Sicherheitsniveau bei der Archivierung lässt sich auf Managementebene typischerweise wie folgt charakterisieren:

- Erfüllung gesetzlicher sowie organisationsinterner Anforderungen an den Schutz der Daten bei der Archivierung sowie darüber hinaus (z. B. nach Entsorgung der Datenträger),
- Widerstandsfähigkeit des Archivierungsprozesses gegen Manipulation,
- Widerstandsfähigkeit des verwendeten Archivsystems gegen interne und externe Angriffe auf die gespeicherten Daten sowie das IT-System selbst.

Wenn Daten und Dokumente klassifiziert werden, kann das Sicherheitsniveau auch anhand dieser Klassifikation detaillierter differenziert werden.

**Welcher Funktions- und Leistungsumfang soll erreicht werden?**

Der angestrebte Funktions- und Leistungsumfang elektronischer Archivierung kann je nach Organisation unterschiedlich ausfallen. Üblicherweise werden auf Managementebene die folgenden Anforderungen definiert:

- Integrationsfähigkeit in die bestehende IT-Systemlandschaft,
- Integrationsfähigkeit in bestehende IT- und Dokumentenmanagement-Prozesse,
- Einhaltung (gesetzlich sowie intern) vorgeschriebener Speicher- und Löschfristen für Daten,
- Aussonderungsmodalitäten und Beachtung der Anbietungspflicht.

Dies betrifft vor allem die öffentliche Verwaltung, da öffentliche Stellen unter Umständen dazu verpflichtet sind, Daten, die von besonderer Bedeutung sind, z. B. gesellschaftlicher, politischer oder historischer Art, einem dafür zuständigen Archiv nach Ablauf der Aufbewahrungsfrist anzubieten. Erst wenn dieses entscheidet, dass die entsprechenden Daten nicht archivwürdig sind, dürfen diese endgültig gelöscht werden. Über die Archivwürdigkeit von Daten kann in vielen Fällen erst nach Ablauf der Aufbewahrungsfrist entschieden werden, so dass die Daten am Ende der Aufbewahrungsfrist nicht immer automatisch bearbeitet werden können.

- Einhaltung des angestrebten Sicherheitsniveaus der Daten sowie
- Migrationsfähigkeit des Archivsystems, wenn sich Anforderungen und Einflussfaktoren ändern.

**Wer trägt die Verantwortung?**

Mit dem Aufbau bzw. dem Betrieb der elektronischen Archivierung müssen Verantwortliche benannt werden. Üblicherweise wird von Seiten des Managements eine Fachabteilung bzw. deren Leiter mit der Umsetzung der Archivierung beauftragt. Hiermit müssen auch Zielvorgaben, Befugnisse, personelle und finanzielle Ressourcen verknüpft werden. Die Delegation der Umsetzung ist entsprechend den organisationsinternen Richtlinien durchzuführen und im Archivierungskonzept zu fixieren.

Prüffragen:

- Werden die zu archivierenden Daten und ihre zugehörigen Sicherheitsniveaus ermittelt?
- Ist der Funktions- und Leistungsumfang der Archivierung festgelegt?
- Sind Verantwortliche für den Aufbau des Archivsystems und der Archivierung benannt?
- Gibt es Zielvorgaben und Befugnisse für Verantwortliche der Archivierung und sind der Archivierung personelle und finanzielle Ressourcen zugeordnet?
- Wurde die Aufgabenübertragung der Archivierung im Archivierungskonzept festgehalten?
- Sind die Planung und die Umsetzung der Archivierung im Archivierungskonzept fixiert?

# M 2.243 Entwicklung des Archivierungskonzepts

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Archivverwalter, IT-Sicherheitsbeauftragter

Der Aufbau eines Archivsystems sollte sorgfältig konzipiert werden. Dabei sind einerseits zahlreiche Einflussfaktoren (z. B. organisationsinterne oder rechtliche Vorgaben, technische und organisatorische Umgebungsbedingungen) zu beachten, andererseits bestehen vielfältige technische Möglichkeiten, um ein elektronisches Archiv aufzubauen. Daher sollte zunächst ein Konzept entwickelt werden, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines konkreten Archivierungssystems und der entsprechenden Produkte berücksichtigt werden und das gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Grundlage für das Archivierungskonzept ist die in M 2.242 *Zielsetzung der elektronischen Archivierung* festgelegte Zielsetzung.

Im Archivierungskonzept ist der technische bzw. organisatorische Einsatz des Archivsystems festzulegen, also z. B.

- die Zuständigkeiten und Verantwortlichkeiten,
- die Definition von Benutzerrollen (z. B. Archivverwalter, Administratoren, Benutzer, technische Benutzer),
- Definition von Zugriffsrechten und Modalitäten zur Rechtevergabe,
- Abgrenzung der zu archivierenden Daten,
- Schutz der archivierten Daten, z. B. durch Verschlüsseln und Signieren,
- die angestrebte Systemanbindung bzw. die Einsatzbedingungen für Archivierungskomponenten,
- die technische Ausgestaltung des Archivsystems,
- der Betrieb des Archivsystems (z. B. Beschreibung von Service Level Agreements).

Die Ergebnisse sollten aktualisierbar und erweiterbar schriftlich dokumentiert werden. Das Archivierungskonzept selbst sollte in allen umgesetzten Fassungen aufbewahrt werden. Die Mitarbeiter sind über den sie betreffenden Teil des Konzepts zu unterrichten. Die Unterrichtung sollte nachprüfbar dokumentiert werden. Ein möglicher Aufbau eines Archivierungskonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

**Inhaltsverzeichnis Archivierungskonzept**

- **Dokumentkontext**
  - Regelungsgegenstand
  - Regelmäßige Anpassung
  - Anordnung der Umsetzung
- **Definitionen**
  - Archivierung, Dokumentenbegriff
  - Langzeitarchivierung, Archivierung zu Revisionszwecken
  - Beschreibung der Einsatzart und des Archivsystems
- **Gefährdungslage zur Motivation**
  - Abhängigkeit der Institution vom Datenbestand
  - Typische Gefährdungen wie Datenverlust, Rekonstruktionsfehler, ...
  - Institutionsrelevante Schadensursachen

  - Beispiele zu Schadensfällen im eigenen Haus
- **Festlegung einer organisationsinternen Sicherheitsleitlinie**
  - Festlegung von Verantwortlichkeiten
  - Zielsetzung, Sicherheitsniveau
- **Beschreibung der Einflussfaktoren**
  - Identifikation der zu archivierenden Daten
  - Vertraulichkeitsbedarf der Daten
  - Integritätsbedarf der Daten
  - Authentizitätsbedarf der Daten
  - Verfügbarkeitsanforderungen an die Daten
  - Rechtliche Rahmenbedingungen
  - Archivierungsfristen (minimale, bei Bedarf auch maximale Speicherdauer)
  - Anforderungen an die Performance beim Einlesen bzw. Auslesen von Daten, Rekonstruktionsaufwand
  - Datenvolumen sowie Änderungsvolumen
  - Art der Daten (Formate)
  - Art der Zugriffe auf die archivierten Daten (lokal oder verteilt im LAN bzw. WAN)
  - Zu beachtende Normen und Standards
  - Erforderliche Funktionalität
  - Personalaufwand
  - Kosten inklusive Folgekosten (Wartung, Administration, Updates, etc.)
  - Kenntnisse und IT-spezifische Qualifikationen der Benutzer
- **Festlegung des Einsatzes**
  - Art des Archivsystems
  - Einsatzbedingungen an das Archivsystem
  - Zeitraum des Einsatzes
  - Benennung der Verantwortlichen
  - Festlegung von Service Level Agreements
  - Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
  - Dokumentation der Einsatzbedingungen und der Konfiguration
  - Interoperabilität, Standardkonformität, Investitionsschutz
  - Regelmäßige Datensicherung
  - Virenschutz
  - Einsatz kryptographischer Verfahren
- **Randbedingungen für die Archivierung**
  - Vertragsgestaltung
  - Refresh-Zyklen für die Speichermedien
  - Bestandsverzeichnis
  - Löschen von Daten
  - Vernichtung von unbrauchbaren Datenträgern
  - Vorhalten von arbeitsfähigen Lesegeräten
- **Sporadische Restaurierungsübungen**

Einzelne Punkte dieses Konzepts werden in den Maßnahmen

- M 2.242 *Zielsetzung der elektronischen Archivierung*,
- M 2.244 *Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung*,
- M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung*,

- M 2.246 *Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung*,

näher adressiert.

Bei der elektronischen Archivierung handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Archivierungskonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden.

Prüffragen:

- Existiert ein Archivierungskonzept, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines Archivierungssystems benannt sind?
- Sind der technische und der organisatorische Einsatz des Archivsystems im Archivierungskonzept festgelegt?
- Ist das Archivierungskonzept aktualisierbar und erweiterbar und wird schriftlich dokumentiert?
- Werden alle umgesetzten Fassungen eines Archivierungskonzepts aufbewahrt?
- Sind alle Mitarbeiter über die sie betreffenden Teile des Archivierungskonzepts unterrichtet und ist die Unterrichtung nachprüfbar dokumentiert?
- Elektronische Archivierung: Wird das Archivierungskonzept regelmäßig den aktuellen Gegebenheiten angepasst?

# M 2.244 Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Archivverwalter, IT-Sicherheitsbeauftragter

Bevor eine Entscheidung getroffen werden kann, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden sollen, müssen eine Reihe von technischen Einflussfaktoren ermittelt werden. Dazu sollten auch die Eigentümer der zu archivierenden Daten befragt werden, also beispielsweise die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen und die Systemadministratoren. Die Ergebnisse sind nachvollziehbar im Archivierungskonzept (siehe M 2.243 *Entwicklung des Archivierungskonzepts*) zu dokumentieren. Die für die elektronische Archivierung maßgeblichen technischen Einflussfaktoren sind unter anderem

- das zu erwartende Datenaufkommen,
- die Dateiformate der zu archivierenden Dokumente,
- das Änderungsvolumen und Versionierung,
- die Aufbewahrungsdauer der Dokumente,
- die Zahl und Art der Zugriffe,
- die vorhandene IT-Einsatzumgebung sowie
- zu beachtende Normen und Standards.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt:

**Zu erwartendes Datenaufkommen**

Ein wesentliches Kriterium für die Auswahl elektronischer Archivsysteme ist die Größe der zu archivierenden Dateien und das in Zukunft zu erwartende Datenaufkommen. Dies kann typischerweise nur großzügig abgeschätzt werden.

Die Dateigröße von Dokumenten hängt dabei auch sehr stark von der Wahl des Dateiformates und dem Umfang der Rendition (siehe weiter unten) ab.

**Dateiformate der zu speichernden Dokumente**

Je nach Wahl des Archivsystems können in diesem grundsätzlich alle verwendeten Dateiformate abgelegt werden, z. B. die in Büroumgebungen üblichen Formate (DOC, PDF, RTF, ASCII, ZIP, etc.) oder auch Bild- und Tondateien (JPG, GIF, WAV, MPEG, etc). Besondere Bedeutung erhalten bei der Archivierung jedoch Dateiformate, die eine langfristige Stabilität hinsichtlich der Syntax und Semantik der Daten bieten (wie z. B. SGML, XML oder auch HTML) oder Bilddateien, die ein exaktes Abbild des ehemals vorhandenen Papierdokuments darstellen können (z. B. TIFF). Die einzelnen Datenformate sind in Maßnahme M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten* detailliert beschrieben.

Bei der elektronischen Archivierung haben sich in der Vergangenheit mehrere Dateiformate etabliert, die eine unterschiedliche Eignung für künftige Verwendungszwecke der Daten aufweisen. Häufig kann oder soll jedoch der spätere Verwendungszweck nicht festgelegt werden. In so einem Fall ist aber nicht vorhersagbar, welches das beste Datenformat für die spätere Verwendung ist. Ebenso häufig bestehen bereits zum Zeitpunkt der Datenspeicherung konkur-

rierende Anforderungen an die Wahl des Dateiformates, die sich aus den unterschiedlichen Verwendungszwecken ergeben. Deshalb hat es sich, vor allem bei der Langzeitarchivierung, als vorteilhaft erwiesen, Dokumente in mehreren Dateiformaten gleichzeitig zu archivieren. Die Dokumente müssen dazu vorher konvertiert werden. Dieser Vorgang wird als Rendition bezeichnet. Bei der Rendition ist jedoch auf eine genaue Dokumentation der Verfahrensweise zu achten. Informationen über das Originalformat müssen mit archiviert werden.

Die Rendition von Dokumenten und anschließende Speicherung in mehreren Dateiformaten wirkt sich unmittelbar auf die für die Archivierung notwendige Speicherkapazität aus.

**Änderungsvolumen und Versionstiefe**

Bei der Archivierung von Dokumenten ist zu überlegen, welche Änderungen an den Dokumenten im Lauf der Zeit auftreten werden, wie häufig dies zu erwarten ist und wie damit zu verfahren ist. Wenn archivierte Dokumente geändert werden sollen, bestehen folgende Möglichkeiten:

- Das ursprüngliche Dokument wird durch die geänderte Version ersetzt.
- Die neue Version des Dokuments wird zusätzlich zur ursprünglichen Version archiviert (Versionierung), wobei unter Umständen nur eine maximale Anzahl von Versionen desselben Dokuments archiviert bleibt (Versionstiefe).

Durch organisationsinterne oder rechtliche Anforderungen kann eine Versionierung der Dokumente gefordert werden. Hier wird insbesondere auf die Maßnahmen M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung* und M 2.246 *Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung* verwiesen.

Eine Versionierung kann auch durch die Wahl des Speichermediums (z. B. WORM - Write Once Read Multiple) erzwungen werden.

Sofern eine Versionierung von Dokumenten vorgenommen wird, muss dies bei der Berechnung der notwendigen Speicherkapazität des Archivsystems berücksichtigt werden.

**Aufbewahrungsdauer der Dokumente**

Für die Kalkulation der notwendigen Speicherkapazität des Archivsystems ist eine Abschätzung der Aufbewahrungsdauer der archivierten Dokumente unerlässlich. Für die Aufbewahrungsdauer ergeben sich aufgrund rechtlicher oder organisationsinterner Vorgaben minimale, jedoch teilweise auch maximale Speicherfristen, die zu beachten sind.

Die Aufbewahrungsdauer hat jedoch nicht nur Einfluss auf die Speicherkapazität des Archivsystems, sondern auch auf die Auswahl des Speichermediums sowie dessen Entsorgung nach Ablauf der Aufbewahrungsdauer.

**Zahl und Art der Zugriffe**

Zugriffszahlen sowie die Art der Zugriffe auf das Archivsystem haben Auswirkungen auf die Konfiguration des Archivservers und die Auswahl der Speicherkomponenten.

Als Einflussfaktoren sind daher zu ermitteln:

- Wie viele Zugriffe werden innerhalb eines vorgegebenen Zeitraums auf das Archivsystem erfolgen?

- Wie hoch ist der Anteil von Schreibzugriffen gegenüber Lesezugriffen?
- Welche Antwortzeiten werden verlangt?
- Erfolgen die Zugriffe direkt von Benutzer- bzw. Clientsystemen auf das Archivsystem oder durch ein übergeordnetes Dokumentenmanagementsystem?
- Muss das Archivsystem zwischen Zugriffen verschiedener Benutzer unterscheiden oder erfolgt dies durch übergeordnete Komponenten?
- Muss das Archivsystem mehrere, voneinander getrennte Archive verwalten (Mandantenfähigkeit)?

**IT-Einsatzumgebung**

Archivsysteme sind typischerweise in komplexere IT-Landschaften eingebettet. Hierdurch ergeben sich technische Anforderungen, z. B. hinsichtlich

- der Netzanbindung,
- der verwendbaren Netzprotokolle (deren Definition z. B. bekannt sein muss, wenn die Kommunikationsverbindung über Firewalls geführt wird),
- Kompatibilität zu anderen Programmen oder IT-Systemen,
- der Einbindung in Systemmanagement-Umgebungen sowohl zur Administration als auch zur Überwachung des Archivsystems,
- der Administrations- und Nutzungsschnittstellen sowie
- der Antwortzeiten des Archivsystems.

**Zu beachtende Normen und Standards**

Die im Bereich der Archivierung bestehenden Standards konzentrieren sich auf die Bereiche

- Dateiformate und Kompressionsverfahren,
- Speichermedien und deren Aufzeichnungsverfahren sowie
- Dokumentenmanagement-Software.

Systemhersteller erhalten durch die Offenlegung von Schnittstellen, die im Rahmen der Standardisierung erfolgt, die Möglichkeit, eine Kompatibilität von Systemkomponenten, Schnittstellen und Datenformaten herzustellen. Deshalb kann durch die Berücksichtigung von Standards bei der Auswahl von Archivsystemen eine längerfristige Planungs- und Investitionssicherheit gewährleistet werden. Bei den in diesem Baustein empfohlenen Maßnahmen wird auf die derzeit gültigen Standards Bezug genommen.

Für den Anwender bedeutet die Orientierung an Standards eine Verringerung der Abhängigkeit von einzelnen Herstellern, Systemlieferanten und Dienstleistern. Bei den langen Zeiträumen, über die Archivsysteme typischerweise eingesetzt werden, ist dies besonders wichtig, da nicht absehbar ist, wie sich Produktlinien langfristig entwickeln. So könnte sich z. B. bei Insolvenz eines Herstellers proprietärer Speicherkomponenten das Problem ergeben, dass das Archivierungssystem nicht mehr in der bisherigen Art durch Zukauf neuer Speichermedien und -komponenten erweitert werden kann. In Behörden und Unternehmen mit hohem Archivierungsbedarf führt dies typischerweise kurzfristig den Eintritt in die Migrationsphase herbei. Bei Einsatz standardisierter Komponenten kann dagegen einfach ein anderer Lieferant für die betroffene Teilkomponente gewählt werden.

Hinsichtlich Standards ist allerdings zu beachten, dass auch diese mit der Zeit aufgrund neuer technologischer Entwicklungen an Relevanz verlieren und bei Bedarf durch neue Standards ersetzt werden. Diese unterscheiden sich gelegentlich inhaltlich grundlegend, äußerlich aber nur in der Versionsnummer. Zudem besteht auch ein Wettbewerb zwischen unterschiedlichen Standardisierungsgremien und Herstellern, die naturgemäß auf der Suche nach wirt-

schaftlichem Einfluss am Markt sind, wodurch es auch konkurrierende Standards gibt.

Prinzipiell ist die Archivierung jedoch auch ohne Beachtung von Standards unter Nutzung proprietärer Datei- und Speicherformate möglich, sofern über den Archivierungszeitraum eine ausreichende Wartung und Systembetreuung durch Hersteller und eine Anpassung der Schnittstellen an sich verändernde Anforderungen sichergestellt wird. Es wird jedoch aus obigen Gründen empfohlen, sich bei der Planung von Archivsystemen eng an geltenden Standards für Dateiformate und Schnittstellen zu orientieren.

Bereits bei der Planung eines Archivsystems sollte eine spätere Migration berücksichtigt werden, da sich bei der langfristigen Speicherung von Daten typischerweise zwischendurch die Technik oder die Anforderungen ändern. Besondere Sorgfalt sollte daher auf die Planung und Auswahl von Schnittstellen, Dateiformaten und Index-Datenbank verwendet und alle Entscheidungen nachvollziehbar dokumentiert werden.

Prüffragen:

- Sind die technischen Einflussfaktoren vor der Entscheidung für ein Archivierungssystem ermittelt und dokumentiert?
- Werden die Größe der zu archivierenden Daten und das in Zukunft zu erwartende Datenaufkommen abgeschätzt?
- Wird ermittelt, welche Änderungen, wie häufig an archivierten Dokumenten auftreten werden?
- Wird die Anzahl und Art der Zugriffe innerhalb eines vorgegebenen Zeitraums auf das Archivsystem ermittelt und die geforderten Antwortzeiten festgelegt?
- Wird ermittelt, ob das Archivsystem getrennte Archive verwalten und zwischen Benutzern unterscheiden können muss?
- Wird die Einsatzumgebung des Archivsystems ermittelt?
- Nutzung proprietärer Datei- und Speicherformate: Wird durch Verträge mit den Herstellern die Wartung, Systembetreuung und Anpassung sichergestellt?

# M 2.245 Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Archivverwalter, IT-Sicherheitsbeauftragter

Für die Aufbewahrung bestimmter Informationen bestehen verschiedene rechtliche Vorgaben, deren Nichteinhaltung zivil- oder strafrechtliche Konsequenzen haben kann. Daher sollten sich die Verantwortlichen informieren, welche rechtlichen Vorgaben in ihrem Fall anzuwenden sind. Hieraus ergeben sich Anforderungen für die Gestaltung des Archivierungskonzepts, die bei der Planung elektronischer Archivierung berücksichtigt werden müssen. Dies betrifft unter anderem

- die Mindestaufbewahrung aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen,
- Höchstaufbewahrungsdauer aus Datenschutzgründen,
- Zugriffsrechte für Externe, wie z. B. Steuerbehörden, sowie
- Qualität von digitalen Signaturen.

Die anzuwendenden rechtlichen Grundlagen sind im Einzelfall zu klären.

Im Folgenden werden einige Quellen genannt, die in Deutschland typischerweise zu berücksichtigen sind:

- Bürgerliches Gesetzbuch (BGB)
  Hier werden insbesondere Anforderungen an die Rechtsgültigkeit von Dokumenten im Zivilrecht gestellt. Das BGB definiert auch Verjährungsfristen, z. B. für Schadenersatz aus unerlaubter Handlung.
- Zivilprozessordnung (ZPO)
  Analog zum BGB wird durch die ZPO geregelt, welche Dokumente als Urkunde anerkannt werden müssen, beispielsweise aufgrund einer eigenhändigen Unterschrift oder einer qualifizierten digitalen Signatur.
- Handelsgesetzbuch (HGB)
  Hier werden Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit gestellt. Dies umfasst auch bestimmte Aufbewahrungsfristen für Geschäftsdokumente.
- Grundsätze ordnungsmäßiger Datenverarbeitung (GoDV)
  Die GoDV sind selbst keine gesetzliche Vorschrift, sondern hergeleitet aus den im HGB definierten Grundsätzen ordnungsmäßiger Buchführung. Sie sind als de facto-Standard für die DV-Revision in Unternehmen zu verstehen.
- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
  Das Bundesministerium der Finanzen hat die in den GoDV vorgesehenen Revisionsanforderungen im Rahmen der GDPdU präzisiert. Dies betrifft hauptsächlich alle steuerlich relevanten digital vorliegenden Dokumente.
  Hierbei wird u. a. gefordert, dass alle zur Auswertung der Daten notwendigen Informationen wie Dateistruktur, Datenfelder, interne und externe Verknüpfungen in maschinell auswertbarer Form zur Verfügung stehen müssen.
- Gesetze und Vorschriften zum Schutz personenbezogener Daten
  Sofern personenbezogene Daten archiviert werden, müssen die hierfür geltenden Gesetze und Vorschriften eingehalten werden. Dazu gehören

vor allem das Bundesdatenschutzgesetz (BDSG) und die entsprechenden Gesetze der Länder.

Weiterhin gibt es Gesetze und Vorschriften, die speziell für Behörden und in der Verwaltung zu beachten sind, beispielsweise:

- Bundesarchivgesetz und die entsprechen Landesarchivgesetze,
- Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien (RegR),
- Empfehlungen des Bundesarchivs zur Aussonderung elektronischer Akten im Konzept zur Aussonderung elektronischer Akten der Koordinierungs- und Beratungsstelle der Bundesregierung für Information in der Bundesverwaltung (Schriftenreihe der KBSt, Band 40).

Organisationsspezifisch gelten darüber hinaus zahlreiche weitere gesetzliche und organisationsinterne Regelungen (z. B. Vorschriften für Sozialversicherungsträger, Krankenhäuser, Pharmaindustrie, Militär oder Kreditwesen), die im Einzelfall ermittelt werden müssen. Wesentliche Regelungskriterien sind üblicherweise die Aufbewahrungsdauer sowie der Vertraulichkeits- und Integritätsbedarf, wobei bei letzteren neben der Stärke auch die Zeitdauer des Schutzbedarfs eingeht.

Für die öffentliche Verwaltung besteht darüber hinaus die gesetzliche Verpflichtung, auch in digitaler Form vorliegende Dokumente den zuständigen Archiven anzubieten (Anbietungspflicht).

Prüffragen:

- Sind die rechtlichen Vorgaben ermittelt und bei der Planung der elektronischen Archivierung berücksichtigt?
- Sind die Mindestaufbewahrungsdauer, die Höchstaufbewahrungsdauer und die Zugriffsrechte auf zu archivierende Dokumente ermittelt?
- Öffentliche Verwaltung: Werden digitale Dokumente den zuständigen Archiven angeboten (Anbietungspflicht)?

# M 2.246 Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Archivverwalter, IT-Sicherheitsbeauftragter

Für die elektronische Archivierung gibt es eine Reihe von organisatorischen Einflussfaktoren, die bei der Konzeption des Archivsystems berücksichtigt werden müssen. Dazu gehören unter anderem

- der Zeitraum des Einsatzes des Archivsystems,
- die Archivierungsfristen,
- der Vertraulichkeitsbedarf der Daten,
- der Verfügbarkeitsbedarf der Daten,
- der Integritätsbedarf der Daten,
- der Authentizitätsbedarf der Daten,
- die Festlegung akzeptabler Antwortzeiten,
- der Rekonstruktionsaufwand,
- der Personalaufwand,
- die Kenntnisse und IT-spezifischen Qualifikationen der Benutzer,
- die Ergonomie und Bedienfreundlichkeit des Archivsystems,
- die Einhaltung von Standards und
- die finanziellen Randbedingungen.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt.

### Einsatzzeitraum des Archivsystems

Die Einsatzdauer eines Archivsystems ist getrennt von der Zeitdauer der Archivierung zu kalkulieren. Es ist eine Abschätzung vorzunehmen, über welchen Zeitraum das konkret auszuwählende System betriebsbereit sein soll. Dies wirkt sich auf die Auswahl der Komponenten, speziell auf die geforderte Lebensdauer der Komponenten, aus.

Ein langer Zeitraum impliziert die Auswahl langlebiger IT-Komponenten sowie die Gestaltung entsprechender Service- und Lieferverträge, die typischerweise mit höheren Kosten verbunden sind.

Ein kurzer Zeitraum impliziert eine frühere Migration des Archivs auf ein neues Archivsystem.

### Archivierungsfristen

Für die Kalkulation der notwendigen Speicherkapazität des Archivsystems ist eine Abschätzung der Aufbewahrungsdauer der archivierten Dokumente unerlässlich. Für die Aufbewahrungsdauer ergeben sich aufgrund rechtlicher oder organisationsinterner Vorgaben minimale, jedoch teilweise auch maximale Speicherfristen, die zu beachten sind.

Die Aufbewahrungsdauer hat jedoch nicht nur Einfluss auf die Speicherkapazität des Archivsystems, sondern auch auf die Auswahl des Speichermediums sowie dessen Entsorgung nach Ablauf der Aufbewahrungsdauer.

**Vertraulichkeitsbedarf der Daten**

Bei der Bestimmung des Vertraulichkeitsbedarfs ist vor allem zu beachten, dass sich dieser Bedarf während der Archivierungsfrist ändern kann. Hierbei können wirtschaftliche und juristische Einflussfaktoren Geltung erlangen. Typischerweise ist davon auszugehen, dass der Vertraulichkeitsbedarf im Lauf der Zeit abnimmt.

Wenn ein langfristiger Schutz der Vertraulichkeit gefordert wird, so hat dies Einfluss auf die organisatorische Gestaltung des Archivierungskonzepts (siehe M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*) und die Auswahl technischer Komponenten.

**Verfügbarkeitsbedarf der Daten**

Die elektronische Archivierung wird typischerweise zur langfristigen Aufbewahrung von Daten und Dokumenten eingesetzt. Hierbei ist als wesentliche Anforderung in einem der vorigen Punkte bereits festgelegt worden, für welchen Zeitraum die betreffenden Dokumente zu archivieren sind.

Daneben ist festzulegen, welche weitergehenden Anforderungen an die Verfügbarkeit zu stellen sind, z. B. die Ausfallsicherheit des Archivsystems und die Stabilität der verwendeten Speichermedien.

**Integritätsbedarf der Daten**

Die Integrität elektronisch archivierter Dokumente muss typischerweise auch nach einer langen Aufbewahrungsdauer noch sichergestellt und prüfbar sein. Hierbei ist insbesondere davon auszugehen, dass Ursprungsdokumente und weitere Kontextinformationen zwischenzeitlich nicht mehr existieren, die Integritätsprüfung also unmittelbar vom Archivsystem bereitgestellt werden muss.

Es muss neben der Klassifizierung des Integritätsbedarfs (z. B. niedrig bis mittel, hoch oder sehr hoch) festgelegt werden, über welchen Zeitraum dies prüfbar sein soll.

**Authentizitätsbedarf der Daten**

Analog zur Integrität muss auch der Authentizitätsbedarf und der Zeitraum festgelegt werden, innerhalb dessen die Authentizität von Dokumenten prüfbar sein muss. Auch hier ist davon auszugehen, dass typischerweise nach einer längeren Archivierungsdauer die Ursprungsdokumente und Kontextinformationen nicht mehr beigebracht werden können. Die Authentizitätsprüfung muss also vom Archivierungsprozess bereitgestellt werden.

**Bestimmung akzeptabler Antwortzeiten**

Zwischen der Anfrage an ein Archivsystem und der Antwort ergibt sich eine Verzögerung (Antwortzeit). Die Anforderungen an diese Verzögerung werden typischerweise durch eine zu erzielende mittlere und eine maximal akzeptable Antwortzeit definiert.

Die Antwortzeit ist nach unterschiedlichen Faktoren zu charakterisieren, u. a.

- die Zeitdauer bis zur Reaktion des Archivsystems bei einer Anfrage,
- die Zeitdauer bis zur Speicherbestätigung des Archivsystems und
- die Zeitdauer bis zur vollständigen Übertragung des gewünschten Dokuments an das Clientsystem.

Die geforderte Antwortzeit hängt dabei sehr stark vom Einsatzszenario ab. So kann z. B. bei der Abfertigung von Passagieren auf Flughäfen eine Abfragezeit von wenigen Minuten eine sinnvolle Anforderung sein. Bei einer Recherche in Altdatenbeständen eines Grundbuchamtes können dagegen durchaus Reaktionszeiten im Stundenbereich innerhalb der Regelarbeitszeit akzeptabel sein.

Typischerweise ergeben sich auch subjektive Anforderungen an die Antwortzeiten. So kann z. B. eine hohe Reaktionszeit auf Suchanfragen oder beim Öffnen archivierter Dokumente als störender empfunden werden als eine gleich lange Zeitdauer bis zur Speicherbestätigung bei der Ablage von Dokumenten im Archiv.

Die Anforderungen an die Antwortzeit sind zu ermitteln und zu dokumentieren.

**Rekonstruktionsaufwand**

Es ist zu bestimmen, welcher zeitliche und technische Aufwand für das Wiederfinden und Bereitstellen archivierter Dokumente akzeptabel ist. Dies ist abhängig von der Art und Struktur der archivierten Daten und daher vom konkreten Einsatzszenario.

**Personalaufwand**

Der Personalaufwand für den Betrieb des Archivsystems stellt einen wesentlichen Einflussfaktor bei der Auswahl des Systems dar. Organisationsspezifisch ist zu ermitteln, welcher zusätzliche Personalaufwand und welche zusätzliche individuelle Belastung des Personals durch die Archivierung als tragbar angesehen werden.

Dies hat Auswirkungen auf die künftige Personalplanung, da gegebenenfalls zusätzliches Personal erforderlich ist. Die Rollen Archivverwalter, Archivadministrator und (technischer) Benutzer sind mindestens zu besetzen. Wenn im laufenden Betrieb zu wenig Personal verfügbar ist, muss die fehlende Personalkapazität durch externe Wartungs- und Serviceverträge kompensiert werden.

**Kenntnisse und IT-spezifische Qualifikationen der Benutzer**

Die Auswahl geeigneter Bedienschnittstellen des Archivsystems wird unter anderem von den Vorkenntnissen der vorgesehenen Benutzer beeinflusst. Hier sollte ermittelt werden, welche IT-spezifischen Fachkenntnisse vorliegen.

Dies hat auch Einfluss auf die Gestaltung von Dienstleistungen im Umfeld der Archivierung, etwa die Organisation einer Benutzerunterstützung (Helpdesk).

Alle Benutzer müssen in jedem Fall im Umgang mit dem Archivsystem geschult werden, damit Schäden durch Fehlbedienung möglichst vermieden werden. Die erforderliche Schulung muss in der Kalkulation der Gesamtkosten berücksichtigt werden.

**Ergonomie und Bedienfreundlichkeit des Archivsystems**

Die Bedienfreundlichkeit hat maßgeblichen Einfluss auf die Akzeptanz durch die Benutzer und dadurch auch auf die ordnungsgemäße Nutzung des Archivsystems.

Neben gesetzlichen Anforderungen zur Ergonomie an Arbeitsplätzen ist hierbei auch der subjektive Eindruck von Benutzern zu berücksichtigen. Die Ermittlung entsprechender Anforderungen kann z. B. über eine Befragung der

künftigen Benutzer erfolgen, es sollten jedoch auch Erfahrungen aus Pilot- und Testinstallationen der vorgesehenen Archivsystem-Komponenten einfließen.

**Einhaltung von Standards**

Für die Interoperabilität mit anderen Produkten und Organisationsprozessen sollte darauf geachtet werden, dass Archivsystem-Komponenten gewählt werden, die konform zu bestehenden Standards sind. Obwohl auch Standards nicht dauerhaft bestehen, sondern im Lauf der Zeit ebenfalls vom technischen Fortschritt überholt werden, wird die Einhaltung der maßgeblichen Standards typischerweise als Investitionsschutz angesehen.

Dies ist jedoch abhängig vom konkreten Einsatzzweck und der Einsatzumgebung. Es sollte daher individuell ermittelt werden, welche Standards maßgeblich sind. Einige relevante technische Standards sind in den Maßnahmen M 4.169 *Verwendung geeigneter Archivmedien* und M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten* beschrieben.

**Finanzielle Randbedingungen**

Die Einführung von Archivsystemen und die Gestaltung eines entsprechenden organisatorischen Rahmens werden typischerweise von den anfallenden Kosten beeinflusst:

- einmalige Investitionen,
- laufenden Kosten, inklusive Personalkosten,
- Lizenzgebühren.

Die technische Planung des Betriebs von Archivsystemen wird daher typischerweise von einer Finanzplanung begleitet. Hierbei sind die organisationsinternen Regelungen (Budgetplanung, Verteilung von Kostenstellen, etc.) zu berücksichtigen.

Die notwendigen Schulungen der Benutzer und Administratoren müssen in die Kalkulation der Gesamtkosten der Archivierung einbezogen werden.

Prüffragen:

- Wird der Zeitraum ermittelt, in dem ein konkret auszuwählendes Archivsystem betriebsbereit sein soll?
- Werden bei der Bestimmung des Vertraulichkeitsbedarfs mögliche Änderungen während der Archivierungsfristen bedacht?
- Sind die Anforderungen an die Verfügbarkeit des Archivsystems festgelegt?
- Wird der Integritätsbedarf und der Zeitraum der Prüfbarkeit festgelegt und durch das Archivsystem realisiert?
- Wird der Authentizitätsbedarf und der Zeitraum der Prüfbarkeit festgelegt und durch das Archivsystem realisiert?
- Sind die Anforderungen an die Antwortzeiten des Archivsystems ermittelt und dokumentiert?
- Sind die zeitlichen und technischen Grenzen für das Finden und Bereitstellen archivierter Dokumente ermittelt?
- Sind die Rollen Archivverwalter, Archivadministrator und (technischer) Benutzer besetzt?
- Sind die IT-spezifischen Fachkenntnisse der Benutzer für das Archivsystem ermittelt?
- Werden in Abhängigkeit der Einsatzumgebung des Archivsystems maßgebliche Standards ermittelt und ausgewählt?

# M 2.247 Planung des Einsatzes von Exchange und Outlook

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bei der Einsatzplanung von Exchange und Outlook müssen folgende Aspekte berücksichtigt werden:

- Microsoft Exchange-Systeme integrieren sich in das Active Directory (AD) einer Microsoft Windows-Netzinfrastruktur. Daher sollte die Microsoft Exchange Planung mit der Planung des Active Directory (siehe M 2.229 *Planung des Active Directory*) abgestimmt sein. Bei der Installation von Microsoft Exchange wird eine Schema-Erweiterung des Active Directory durchgeführt. Damit beeinflusst eine Exchange-Installation das Active Directory nachhaltig, so dass der Schema-Administrator des Schema-Master-Servers unbedingt beteiligt werden muss. Außerdem müssen die an der Planung beteiligten Personen ausreichende Kenntnisse über den generellen Aufbau des Windows-Netzes haben, insbesondere über die Verteilung der Domänen-Controller und die Erreichbarkeit des sogenannten Global Catalog Servers.
- Die Postfach-Datenbanken können auf verschiedene Exchange-Server verteilt werden. Damit lassen sich Informationen mit unterschiedlichem Schutzbedarf auf entsprechend physisch gesicherte Server aufteilen. Bei bedarfsgerechter Planung kann dies gleichzeitig die Performance und die Ausfallsicherheit erhöhen. Dies gilt auch für den Einsatz von weiteren Hochverfügbarkeitsfunktionen.
- Begleitend zur Planung des gewünschten Einsatzszenarios und der Verteilung der Exchange-Server ist eine Sicherheitsrichtlinie zu entwerfen, in der die für Exchange spezifischen Aspekte behandelt werden. Die dabei zu berücksichtigenden Gesichtspunkte sind in M 2.455 *Festlegung einer Sicherheitsrichtlinie für Groupware* zusammengefasst.
- Für die Anbindung eines Exchange-Systems an fremde Kommunikationssysteme stehen sogenannte Konnektoren zur Verfügung, die die Verbindung zwischen den verschiedenen Systemen herstellen. Der Einsatz dieser Konnektoren ist sorgfältig zu planen, um einen reibungslosen Kommunikationsablauf zu gewährleisten.
- Der Einsatz der Microsoft Outlook-Clients, deren Zugriffsmöglichkeiten auf den Microsoft-Exchange-Server und die Absicherung dieser Zugriffe müssen geplant werden. Es ist ferner zu klären, ob eine Anbindung als MAPI-Client gewünscht ist oder nicht. In der Vergangenheit wurde die MAPI-Schnittstelle häufig zur Verbreitung von Programmen mit Schadfunktionen (z. B. Viren, Würmer, usw.) missbraucht.
- Die Administration des Microsoft-Exchange-Systems muss geplant werden. Die Aufgaben reichen dabei von der Festlegung der Rollen und Verantwortlichkeiten inklusive Stellvertreterregelung in der Institution bis zur Definition geeigneter Administrationsrollen. In den entsprechenden Domänen müssen außerdem Benutzergruppen mit passenden Rechten eingerichtet werden.
- Die Benutzerkonten und die verwendeten Gruppen der Institution müssen geplant werden.
- Der Einsatz eines integrierten Viren-Schutzprogramms im Microsoft Exchange-System muss geplant werden. Dabei ist zu entscheiden, welche Viren-Schutzprogramme unter welchen Rahmenbedingungen Server- und Client-seitig eingesetzt werden.

Die Planung des Exchange-Systems darf nur dann als abgeschlossen betrachtet werden, wenn auch das sogenannte Roll-out im Detail geplant worden ist. Dabei wird unter anderem die Installationsreihenfolge der einzelnen Exchange-Server und aller Outlook-Clients festgelegt.

Um die Anforderungen aus dieser Maßnahme konkret umzusetzen, finden sich im Microsoft Technet Erläuterungen, beispielsweise wird für die Version 2010

- die Planung und Installation von Microsoft Exchange 2010 unter "Planning and Deployment: Exchange 2010 Help" und
- die Planung und Installation von Microsoft Outlook 2010 unter "Planning the deployment of Office 2010" behandelt.

Prüffragen:

- Wurde der Einsatz von Exchange und Outlook bedarfsgerecht geplant?
- Wurde der Schema-Administrator in die Planung des Exchange-Systems einbezogen?
- Existiert ein Plan zur Verteilung der Exchange und Outlook-Software?

# M 2.248 Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000

Diese Maßnahme ist mit der 13. Ergänzungslieferung entfallen. Die Inhalte wurden in M 2.455 *Festlegung einer Sicherheitsrichtlinie für Groupware* integriert.

# M 2.249 Planung der Migration von Exchange-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

In der Praxis wird häufiger ein bereits bestehendes Exchange-System migriert als dass eine vollständige Neuinstallation durchgeführt wird. Bei Exchange stellt daher die Migration von einer Vorgängerversion ein wichtiges Szenario dar.

Ein Versionswechsel bedeutet bei Microsoft Exchange-Systemen einen gravierenden Sprung in nahezu sämtlichen Teilaspekten. Es handelt sich deshalb nicht um ein Software-Update, sondern um einen weitreichenden Designwechsel. Bei diesem Wechsel ist nicht nur die Microsoft Exchange-Software betroffen, sondern auch das zugrundeliegende Windows Server-Betriebssystem.

Bei der Installation von Microsoft Exchange-Systemen wird eine sogenannte Schema-Erweiterung des Active Directories vorgenommen. Eine Schema-Veränderung ist ein grundlegender Eingriff in das Active Directory, die nicht rückgängig gemacht werden kann. Es ist deshalb unerlässlich, die Windows-Systemadministratoren und speziell die Active Directory-Schema-Administratoren in die Migrationsplanung einzubeziehen.

Die Migration muss in ihren einzelnen Schritten möglichst detailliert geplant, der angestrebte Migrationsprozess dokumentiert und allen Beteiligten zugänglich gemacht werden. Im Überblick sind folgende Schritte im Rahmen des Migrationsprozesses durchzuführen:

- Datensicherung aller Komponenten des bestehenden Groupware-Systems,
- Probelauf der neuen Software in einem Testszenario,
- Installation der neuen Rechner (für Microsoft-Exchange-Server) mit vorausgesetztem Windows Server-Betriebssystem,
- Neue Rechner (für Microsoft Exchange Server) Mitglied der gewünschten Domänen werden lassen,
- Installation der Microsoft-Exchange-Software auf den dafür vorgesehenen Windows-Servern,
- Verteilung und Anpassung der korrespondierenden Microsoft Outlook-Clients,
- Einrichten der Benutzerkonten inklusive der E-Mail-Funktionalität und
- Einspielen der alten E-Mail-Daten auf das migrierte System.

Folgende Aspekte sind aus Sicherheitssicht bei der Planung der Migration zu berücksichtigen:

- Welche Postfächer bzw. Objekte sind zu migrieren?
- Wird die bestehende Sicherheitsrichtlinie übernommen, geändert oder ergänzt?
- Ist das vorhandene Active Directory-Konzept berücksichtigt und, wo nötig, ergänzt worden?
- Welche E-Mail-Systeme müssen angebunden werden?
- Sind Funktionen in Benutzung, die mit der neuen Version abgekündigt oder nicht mehr unterstützt werden?
- Die neue Software sollte vor der Installation in einem separaten Testnetz getestet werden.

Allgemein ist zu beachten, dass sich die Terminologie der Objekte bei Microsoft Exchange mit Versionswechseln ändert.

Wie die Anforderungen aus dieser Maßnahme konkret umgesetzt werden können, ist beispielsweise für die Version 2010 in folgenden Dokumenten des Microsoft Technet aufgeführt:

- Eine Übersicht über ein Upgrade auf Microsoft Exchange Server 2010 bietet: "Upgrading to Exchange 2010: Exchange 2010 Help".
- Eine Übersicht der weggefallenen bzw. geänderten Funktionen älterer Microsoft Exchange-Server in Bezug auf Microsoft Exchange 2010 bietet: "Discontinued Features and De-Emphasized Functionality: Exchange 2010 Help".
- Die Koexistenz von versionsälteren Microsoft Exchange-Servern zusammen mit Microsoft Exchange 2010 muss geplant werden. Hierzu ist das veränderte Zugriffsmodell auf Exchange-Objekte zu beachten, wie in "Understanding Permissions: Exchange 2010 Help" beschrieben.
- Eine Migration von Lotus Notes wird unter "Migrating from Lotus Notes to the Microsoft Collaboration Platform" beschrieben.

Prüffragen:

- Wurden die einzelnen Schritte der Migration gründlich geplant und dokumentiert?
- Wurden die Windows-Systemadministratoren an der Planung der Migration von Exchange beteiligt?
- Wurden die vorzunehmenden Schema-Änderungen für Exchange am Active Directory dokumentiert?

# M 2.250 Festlegung einer Outsourcing-Strategie

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Fachverantwortliche

Die Bindung an einen Outsourcing-Dienstleister erfolgt auf lange Sicht, ist zunächst kostenintensiv und mit Risiken verbunden. Eine gute Planung des Outsourcing-Vorhabens ist daher wichtig. Dabei müssen neben den wirtschaftlichen, technischen und organisatorischen Randbedingungen auch die sicherheitsrelevanten Aspekte bedacht werden. Folgende Gesichtspunkte sollten betrachtet werden:

- Unternehmensstrategie (Flexibilität, Abhängigkeiten, zukünftige Planungen),
- Machbarkeitsstudie mit Zusammenstellung der Rahmenbedingungen,
- betriebswirtschaftliche Aspekte mit Kosten-Nutzen-Abschätzung.

Nach ersten strategischen Überlegungen muss zunächst geklärt werden, welche Geschäftsprozesse, Aufgaben oder Anwendungen generell für Outsourcing in Frage kommen.

Dabei darf die Bedeutung der rechtlichen Rahmenbedingungen nicht unterschätzt werden. Gesetze könnten beispielsweise das Auslagern bestimmter Kernaufgaben einer Institution generell verbieten oder zumindest weitreichende Auflagen enthalten und die Beteiligung von Aufsichtsbehörden vorschreiben. In der Regel bleibt der Auftraggeber weiterhin gegenüber seinen Kunden oder staatlichen Stellen voll verantwortlich für Dienstleistungen oder Produkte, unabhängig davon, ob einzelne Aufgabenbereiche ausgelagert wurden.

Die Informationssicherheit wird leider häufig zu Beginn der Planung vernachlässigt, obwohl ihr eine zentrale Bedeutung zukommt. Dies gilt sowohl für technische als auch organisatorische Sicherheitsaspekte, denen im Outsourcing-Szenario eine entscheidende Rolle zukommt. Generell ist nämlich zu bedenken:

- Die Entscheidung zum Outsourcing ist in der Regel nicht einfach zu revidieren. Die Bindung an den Dienstleister erfolgt unter Umständen sehr langfristig.
- Ein Dienstleister hat häufig Zugriff auf Daten und IT-Ressourcen des Auftraggebers. Der Outsourcing-Auftraggeber verliert dadurch die alleinige und vollständige Kontrolle über Daten und Ressourcen. Je nach Outsourcing-Vorhaben betrifft dies dann auch Daten mit hohem Schutzbedarf.
- Für die technische Umsetzung des Outsourcing-Vorhabens ist es notwendig, dass zwischen Auftraggeber und Dienstleister Daten übertragen werden. Dadurch ergibt sich automatisch ein erhöhtes Gefahrenpotential.
- In der Regel ist es erforderlich, dass Mitarbeiter oder Subunternehmer des Outsourcing-Dienstleisters (und damit Betriebsfremde) zeitweise in den Räumlichkeiten des Auftraggebers arbeiten müssen. Auch dadurch ergibt sich ein erhöhtes Gefahrenpotential.
- Im Rahmen eines Outsourcing-Vorhabens müssen neue Prozesse und Arbeitsabläufe entworfen, eingeführt und durchgeführt werden. Die Folgen der notwendigen Umstellungen müssen geklärt und abgeschätzt werden.
- Für jeden Outsourcing-Dienstleister besteht ein nicht zu unterschätzender Interessenskonflikt: Einerseits muss er die Dienstleistung möglichst kostengünstig erbringen, um seinen Gewinn zu maximieren, andererseits erwartet der Auftraggeber hohe Dienstleistungsqualität, Flexibilität und kun-

denfreundliches Verhalten. Dieser Punkt ist erfahrungsgemäß der am häufigsten unterschätzte. Während IT-Manager in der Regel sehr kritisch und kostenbewusst sind und Versprechungen von Herstellern und Beratern mit großer Skepsis begegnen, ist beim Outsourcing leider oft das Gegenteil zu beobachten. Allzu leicht verfällt hier der Auftraggeber den Werbeaussagen der Dienstleister in der frohen Erwartung, seine IT-Kosten signifikant senken zu können. Die Praxis lehrt jedoch, dass höchstens die Dienstleistungen in der Zukunft erbracht werden, die von Anfang an vertraglich fixiert worden sind. Stellt sich heraus, dass die Dienstleistungsqualität unzureichend ist, weil der Auftraggeber Leistungen erwartet, die er - im Gegensatz zum Outsourcing-Dienstleister - als selbstverständlich erachtet, sind Nachbesserungen in der Regel ohne hohe zusätzliche Kosten nicht zu erwarten. Jeder IT-Manager, der über Outsourcing nachdenkt, sollte sich die Mühe machen, nachzurechnen, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit Auftraggeber und Auftragnehmer beide von dem Vertragsverhältnis profitieren. Bei dieser Rechnung stellt sich vielleicht heraus, dass eine seriöse Leistungserbringung zu den versprochenen niedrigen Kosten höchst unwahrscheinlich ist.

Um die Outsourcing-Strategie festzulegen, muss daher immer eine individuelle Sicherheitsanalyse durchgeführt werden. Nur so kann letztendlich festgestellt werden, wie bestehende Geschäftsprozesse oder Informationsverbünde abgegrenzt und getrennt werden können, damit Teile davon ausgelagert werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten. Die Sicherheitsanalyse sollte nach der in der IT-Grundschutz-Vorgehensweise beschriebenen Methodik durchgeführt werden:

- Es sollte zunächst eine Strukturanalyse durchgeführt werden, um den aktuellen Ist-Zustand zu ermitteln.
- Danach erfolgt eine Schutzbedarfsfeststellung.
- Darauf aufbauend müssen geeignete Sicherheitsmaßnahmen ausgewählt und auf die jeweiligen Rahmenbedingungen des Outsourcing-Vorhabens angepasst werden. Dabei sind auch der Handlungsbedarf, die Prioritäten sowie die Kosten für die umzusetzenden Maßnahmen zu identifizieren. Die Ergebnisse können dann insbesondere in die Betrachtung der Wirtschaftlichkeit des Outsourcing-Vorhabens mit einbezogen werden.

Wenn der Schutzbedarf wichtiger Systeme oder Anwendungen hoch ist oder die Modellierung des Informationsverbunds nach IT-Grundschutz nicht möglich ist, muss eine ergänzende Sicherheitsanalyse (z. B. Risikoanalyse) durchgeführt werden. Sind die sicherheitsrelevanten Gefährdungen analysiert worden, kann festgelegt werden, ob und wie diesen begegnet werden soll.

Schlussendlich wird dennoch ein gewisses Restrisiko durch den Outsourcing-Auftraggeber zu tragen sein. Die Ergebnisse der Sicherheitsanalyse gehen unmittelbar in die Kosten-Nutzen-Abschätzung ein.

Das Management darf bei der Entwicklung einer erfolgversprechenden, langfristigen Outsourcing-Strategie den Blick nicht nur auf die Einsparung von Kosten richten. Die Auswirkungen eines Outsourcing-Vorhabens auf die Aufgabenerfüllung, das Geschäftsmodell und das Dienstleistungs- oder Produktportfolio müssen ebenfalls berücksichtigt werden. Sollen Standardabläufe oder Kerngeschäftsprozesse ausgelagert werden? Wichtig ist in diesem Zusammenhang, dass die Fähigkeit, Anforderungen an die IT selbst zu bestimmen und zu kontrollieren, in ausreichendem Maße erhalten wird. Insbesondere an die Weiterentwicklung und Pflege selbstentwickelter IT-Systeme und Anwendungen sollte gedacht werden.

Die nachfolgenden Hinweise beleuchten Vor- und Nachteile von Outsourcing mit Bezug zur Informationssicherheit.

- **Vorteil:** Es besteht die Möglichkeit, neue Dienstleistungen (z. B. durch Diversifikation oder Ausweitung der Produktpalette) zu etablieren. In der Folge muss das festgelegte Sicherheitsniveau jedoch auch für das ausgeweitete Angebot sichergestellt werden.
- **Vorteil:** Es besteht mehr Flexibilität, beispielsweise können Systeme, Ressourcen oder der Personalbedarf schneller angepasst bzw. erweitert werden, da dies vom Outsourcing-Dienstleister unter Umständen auch kurzfristig eingekauft werden kann. Fixe Kosten können so in variable umgewandelt werden. In Folge können sich jedoch durch die Erweiterungen (z. B. von IT-Systemen) auch neue Sicherheitsprobleme ergeben.
- **Vorteil:** Im Idealfall kann durch das Outsourcing-Vorhaben ein besseres Sicherheitsniveau erreicht werden, da der Dienstleister Spezialisten beschäftigt, so dass dadurch auch neue, sicherheitskritische Anwendungen betrieben werden können. Gerade in der Informationssicherheit ist es sehr zeitaufwendig und benötigt viel technisches Wissen, regelmäßig die Flut an Sicherheitshinweisen, Security-Bulletins, Updatemeldungen und Bug-Reports auszuwerten, ihre Relevanz zu erkennen und bei Bedarf rasch die richtigen Schritte einzuleiten. Zunehmende Komplexität der angebotenen Hard- und Softwarelösungen, immer kürzere Produktzyklen, steigende Vernetzung und steigende Anforderungen der Nutzer machen es zudem außerordentlich schwierig, immer wieder die richtige Balance zwischen Sicherheit und "mehr Funktionalität" zu finden.
- **Vorteil:** Gerade in Unternehmen oder Behörden mit kleiner IT-Abteilung haben einzelne Mitarbeiter oft einen hohen Stellenwert. Stehen sie einmal nicht zur Verfügung (Krankheit, Urlaub) oder verlassen die Institution, können sich gravierende Sicherheitsprobleme ergeben, weil es keinen gleichwertigen Vertreter gibt. Dienstleister hingegen können in der Regel auf mehrere gleich qualifizierte Experten zurückgreifen, die sich gegenseitig vertreten können.
- **Vorteil:** Von einigen Institutionen wird Outsourcing häufig als vielleicht einzige Möglichkeit gesehen, eine Neugestaltung ihrer Geschäftsprozesse und IT-Systeme gegen interne Widerstände durchzusetzen. Im Zuge des Outsourcing-Vorhabens soll eine heterogene Systemlandschaft aufgeräumt und standardisiert werden.
- **Nachteil:** Wenn das Know-how der vom Outsourcing-Dienstleister eingesetzten Spezialisten nicht angemessen ist, so können dadurch gravierende Sicherheitslücken entstehen. Ist zusätzlich intern nicht mehr das Fachwissen vorhanden, um das Sicherheitsniveau beim Outsourcing-Dienstleister zu kontrollieren, werden Sicherheitslücken womöglich nicht einmal entdeckt.
- **Nachteil:** Eine Ausweitung des Dienstleistungsangebots oder die Erweiterung von IT-Systemen ist nicht mehr allein eine Entscheidung des eigenen Managements. Der Outsourcing-Dienstleister muss immer an der Diskussion beteiligt werden. Dienstleister kompensieren nicht selten günstige Konditionen bei Vertragsabschluss durch hohe Forderungen bei späteren Sonderwünschen oder neuen Anforderungen des Auftraggebers. Der dann entstehende Kostendruck führt oftmals zu Einsparungen bei der Informationssicherheit.
- **Nachteil:** Der Aufwand für die Kontrolle der Dienstleistungsqualität darf nicht unterschätzt werden. Sollten hierbei Defizite festgestellt werden, können diese schwierig und zeitaufwendig zu beheben sein, vor allem wenn es zu Meinungsverschiedenheiten zwischen Auftraggeber und Dienstleister kommt. Wenn Fragen der Informationssicherheit dann nicht zeitnah gelöst werden, können sich Sicherheitslücken ergeben.

Eine umfassende Kosten-Nutzen-Analyse jedes Outsourcing-Vorhabens ist essentiell für den strategischen und wirtschaftlichen Erfolg. Es ist daher wichtig, alle Parameter zu kennen und auch richtig einzuschätzen.

Der strategische Wert der folgenden Ressourcen muss unter den Rahmenbedingungen des Outsourcing-Vorhabens eingeschätzt werden:

- Know-how
- Mitarbeiter
- IT-Systeme und Anwendungen

Bei der Kosten-Nutzen-Analyse können Studien und Erfahrungsberichte anderer Institutionen wertvolle Informationen liefern.

Abschließend ist die Outsourcing-Strategie zu dokumentieren. Die Ziele, Chancen und Risiken des Outsourcing-Vorhabens sollten eindeutig beschrieben werden. Es empfiehlt sich unter diesem Gesichtspunkt außerdem, die im Rahmen eines laufenden Outsourcing-Vorhabens gemachten Erfahrungen in die Dokumentation der Outsourcing-Strategie zu integrieren. Es sollte dabei auch auf Fehlentscheidungen und daraus abgeleitete Empfehlungen für die Zukunft hingewiesen werden.

Prüffragen:

- Berücksichtigt die Outsourcing-Strategie neben den wirtschaftlichen, technischen, organisatorischen und rechtlichen Randbedingungen auch die sicherheitsrelevanten Aspekte?
- Wird zur Festlegung der Outsourcing-Strategie eine für das Outsourcing-Vorhaben individuelle Sicherheitsanalyse nach der IT-Grundschutz-Vorgehensweise durchgeführt?
- Behält die auftraggebende Organisation im Outsourcing-Vorhaben ausreichende Fähigkeiten, Anforderungen an die Informationssicherheit zu bestimmen und zu kontrollieren?
- Sind in der Dokumentation zur Outsourcing-Strategie die Ziele, Chancen und Risiken des Outsourcing-Vorhabens beschrieben?

# M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Wenn eine Outsourcing-Strategie festgelegt wurde, müssen die Sicherheitsanforderungen so konkret ausgearbeitet werden, dass auf ihrer Basis der geeignete Dienstleister ausgesucht werden kann. Dabei sind Sicherheitsanforderungen an den Outsourcing-Dienstleister selbst, die benutzte Technik (inklusive Kommunikationswege und -dienste), aber auch an die eigene Organisation zu stellen. Die Erstellung eines detaillierten Sicherheitskonzeptes, das auf den hier formulierten Anforderungen aufbaut und nach Auswahl des Dienstleisters ausgearbeitet wird, wird in M 2.254 *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben* beschrieben.

Es ist zu bedenken, dass das Festlegen von Sicherheitsanforderungen ein iterativer Prozess ist:

- Zunächst werden die gewünschten Sicherheitsanforderungen durch den Auftraggeber spezifiziert.
- Danach wird in der Angebotsphase abgeglichen, wie und ob die gewünschten Sicherheitsanforderungen durch die anbietenden Dienstleister geleistet werden können (siehe auch M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters*).
- Ist ein Dienstleister ausgewählt, so muss mit diesem die weitere Verfeinerung der Sicherheitsanforderungen (z. B. basierend auf den eingesetzten Betriebssystemen oder Sicherheitsmechanismen) erarbeitet werden. In der Endphase dieses Abstimmungsprozesses müssen dann auch die Sicherheitsanforderungen für die konkrete Umsetzung definiert werden.

Generell ergeben sich für Outsourcing-Szenarien folgende Mindestsicherheitsanforderungen:

- Die Umsetzung des IT-Grundschutzes ist eine Minimalforderung an beide Outsourcing-Parteien. Zusätzlich müssen sowohl Outsourcing-Dienstleister als auch der Auftraggeber selbst ein Sicherheitskonzept besitzen und dieses umgesetzt haben.
- Es ist wichtig, die relevanten IT-Verbünde genau abzugrenzen (z. B. nach Fachaufgabe, Geschäftsprozess, IT-Systemen), so dass alle Schnittstellen identifiziert werden können. An die Schnittstellen können dann entsprechende technische Sicherheitsanforderungen gestellt werden.
- Es muss eine Ist-Strukturanalyse von IT-Systemen und Anwendungen (siehe auch M 2.250 *Festlegung einer Outsourcing-Strategie*) erfolgen.
- Es muss eine Schutzbedarfsfeststellung (z. B. von Anwendungen, Systemen, Kommunikationsverbindungen, Räumen) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit erfolgen (siehe auch M 2.250 *Festlegung einer Outsourcing-Strategie*).

Natürlich sind auch relevante Gesetze und Vorschriften zu beachten. Dies kann besonders in Fällen, in denen Auftraggeber oder Dienstleister länderübergreifend oder weltweit operieren, aufwendig sein.

Im Rahmen der Sicherheitsanforderungen ist festzulegen, welche Rechte (z. B. Zutrittsrechte, Zugriffsrechte auf Daten und Systeme) dem Outsourcing-Dienstleister vom Auftraggeber eingeräumt werden.

Die Anforderungen an Infrastruktur, Organisation, Personal und Technik müssen beschrieben werden. Es genügt hier oftmals die Verpflichtung auf ein Sicherheitsniveau, das IT-Grundschutz entspricht. Sollten darüber hinausgehende Anforderungen bestehen, müssen diese detailliert beschrieben werden. Dies hängt entscheidend von der Sicherheitsstrategie und bereits vorhandenen Systemen und Anwendungen ab. Beispielsweise könnten folgende Punkte in Abhängigkeit vom Outsourcing-Vorhaben detailliert werden:

**Organisatorische Regelungen und Prozesse**
- Anforderungen an sicherheitskritische organisatorische Prozesse (z. B. Zeitrestriktionen für den Alarmierungsplan) können spezifiziert werden.
- Spezielle Anforderungen an bestimmte Rollen können festgelegt werden. Es kann beispielsweise gefordert werden, dass ein IT-Sicherheitsbeauftragter mit speziellen Kenntnissen (z. B. Host-Kenntnissen) beim Outsourcing-Dienstleister benannt werden muss.

**Hard-/Software**
- Der Einsatz zertifizierter Produkte (z. B. gemäß Common Criteria oder ITSEC) beim Outsourcing-Dienstleister kann gefordert werden.
- Anforderungen an die Verfügbarkeit von Diensten und IT-Systemen können gestellt werden. Beispielsweise kann in diesem Zusammenhang der Grad und die Methode der Lastverteilung (z. B. für Web-Server mit Kundenzugriff bei sehr vielen Kunden) vorgegeben werden.
- Vorgaben an die Mandantenfähigkeit sowie die diesbezügliche Trennung von Hard- und Software können formuliert werden. Beispielsweise kann festgelegt werden, dass keine IT-Systeme des Auftraggebers in Räumen untergebracht werden dürfen, in denen bereits Systeme anderer Mandanten des Dienstleisters stehen.

**Kommunikation**
- Spezielle Verfahren zur Absicherung der Kommunikation zwischen Dienstleister und Auftraggeber wie Einsatz von Verschlüsselungs- und Signaturverfahren (siehe auch Bausteine B 4.4 *VPN* und B 1.7 *Kryptokonzept*) können fest vorgegeben werden.

**Kontrollen und QS**
- Allgemeine Anforderungen bezüglich Kontrolle und Messung von Sicherheit, Qualität oder auch Abläufen und organisatorischen Regelungen können festgelegt werden, z. B. Zeitintervalle, Zuständigkeiten.
- Gewünschte Verfahren oder Mechanismen für die Kontrolle und Überwachung, wie unangekündigte Kontrollen vor Ort, Audits (unter Umständen durch unabhängige Dritte) können spezifiziert werden.
- Anforderungen an die Protokollierung und Auswertung von Protokolldateien können festgelegt werden.

Generell bilden die festgelegten IT-Sicherheitsanforderungen eine der Grundlagen für die Wahl eines geeigneten Outsourcing-Dienstleisters. Spezielle IT-Sicherheitsanforderungen müssen jedoch eventuell an das von Dienstleistern umsetzbare IT-Sicherheitsniveau angepasst werden.

Prüffragen:

- Sind alle Sicherheitsanforderungen für das Outsourcing-Vorhaben auf Basis der Outsourcing-Strategie festgelegt?

- Wurden beide Outsourcing-Parteien auf IT-Grundschutz oder ein vergleichbares Schutzniveau vertraglich verpflichtet?
- Sind alle Schnittstellen zwischen Outsourcing-Auftraggeber und -nehmer identifiziert, so dass dafür entsprechende Sicherheitsanforderungen gestellt werden können?
- Ist in den Sicherheitsanforderungen festgelegt, welche Rechte (Zutrittsrechte, Zugangsrechte, Zugriffsrechte) dem Auftraggeber vom Outsourcing-Dienstleister einzuräumen sind?

# M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT

Bei der Wahl eines geeigneten Outsourcing-Dienstleisters sind ein möglichst detailliertes Anforderungsprofil und ein darauf basierendes Pflichtenheft entscheidende Erfolgsfaktoren. Nur so kann eine bedarfsgerechte Ausschreibung erfolgen, auf die sich auch geeignete Dienstleister bewerben.

Die Ausschreibung sollte die

- Beschreibung des Outsourcing-Vorhabens (Aufgabenbeschreibung und Aufgabenteilung) sowie
- Beschreibungen zum geforderten Qualitätsniveau, welches nicht zwangsläufig dem Niveau des Auftraggebers entsprechen muss, enthalten.

Weiterhin müssen den potenziellen Dienstleistern auch möglichst detailliert

- die Anforderungen an Informationssicherheit und
- die Kriterien zur Messung von Servicequalität und Sicherheit

mitgeteilt werden (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*). In Einzelfällen kann es notwendig sein, die Detailanforderungen bezüglich Sicherheit nur gegen eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement) an Dienstleister herauszugeben, da sich daraus Hinweise auf existierende oder geplante Sicherheitsmechanismen ableiten lassen.

Das Anforderungsprofil hängt stark von der Art des Outsourcing-Vorhabens ab. Als wichtige grundsätzliche Bewertungskriterien für Dienstleister und dessen Personal können gelten:

**Anforderungen an Outsourcing-Dienstleister**

- Bei ausländischen Dienstleistern müssen besondere Aspekte bedacht werden. Dazu gehören beispielsweise: fremde Gesetzgebung, andere Haftungsregelungen, Spionagerisiko, andere Sicherheitskultur, im Partnerunternehmen bzw. durch die landesspezifische Gesetzgebung zugelassene und verwendbare Sicherheitsmechanismen.
- Die Größe des Dienstleisters kann bei der Auswahl ein Argument sein. Bei kleinen Unternehmen könnte das Insolvenzrisiko höher sein. Bei großen Unternehmen ist zu bedenken, dass diese sehr viele Auftraggeber und Projekte haben, so dass ein einzelner Auftraggeber nur einer unter vielen ist und keine bevorzugte Stellung einnimmt.
- Der Dienstleister sollte Referenzen für ähnliche Outsourcing-Vorhaben aufweisen können. Dabei ist auf Interessenskonflikte durch Geschäftsbeziehungen zu Konkurrenten des Auftraggebers und auf die Unabhängigkeit von bestimmten Herstellern (z. B. Zulieferer, die Konkurrenten des Auftraggebers sind) zu achten.
- Die Referenzen sollten zumindest stichprobenartig auch hinterfragt werden. Es sollte also bei den aus den Referenzen erkennbaren Ansprechpartnern aus vergleichbaren Projekten Auskünfte über den Projektverlauf aus Sicht der Kunden eingeholt werden.
- Die Organisationsform eines Dienstleisters kann in Betracht gezogen werden, da dies z. B. die Haftungsgrenzen beeinflussen kann. Die Eigentü-

merstruktur sollte recherchiert werden, um mögliche Einflussfaktoren im Vorfeld abzuklären.
- Die Kundenstruktur sollte beachtet werden, da dies darauf hinweist, in welchem Wirtschaftssektor der Anbieter seine Stärken hat.
- Ein Qualitätsnachweis bzw. eine Zertifizierung, z. B. nach ISO 27001 auf Basis von IT-Grundschutz oder ISO 9000, ist eine sinnvolle Forderung.
- Auskünfte über die aktuelle wirtschaftliche Lage sowie Erwartungen an die zukünftige Geschäftsentwicklung der Dienstleister sollten eingeholt werden.

**Anforderungen an Mitarbeiter**

Auch an die Mitarbeiter eines Dienstleisters sind diverse Anforderungen zu stellen (siehe auch M 2.226 *Regelungen für den Einsatz von Fremdpersonal* und M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*).

- Die Qualifikation der Mitarbeiter muss in die Bewertung der Angebote einfließen. Es ist nach der Projektvergabe darauf zu achten, dass die im Angebot genannten Mitarbeiter auch später tatsächlich eingesetzt werden.
- Die Anzahl der verfügbaren Mitarbeiter muss bewertet werden. Dabei sollten auch die Vertretungsregelungen und die Arbeitszeiten hinterfragt werden.
- Bei der Wahl ausländischer Partner muss eine gemeinsame Sprache für die Kommunikation zwischen den eigenen Mitarbeiter und denen des Dienstleisters festgelegt werden. Hierbei sollte auch hinterfragt werden, ob die vorhandenen Sprachkenntnisse für die Klärung von Detailproblemen ausreichen. Die Erfahrungen zeigen, dass viele Personen aus Angst, sich zu blamieren, lieber zu wichtigen Fragen schweigen, wenn sie ihre Sprachfähigkeiten als nicht perfekt einschätzen.
- Entsprechend dem erforderlichen Sicherheitsniveau für das Outsourcing-Vorhaben sollte in die Bewertung der Angebote mit aufgenommen werden, ob eine Sicherheitsüberprüfung der Mitarbeiter vorliegt bzw. eine solche durchgeführt werden kann.

Prüffragen:

- Existiert zur Auswahl des Outsourcing-Dienstleisters ein Anforderungsprofil, das die Sicherheitsanforderungen für das Outsourcing-Vorhaben enthält?
- Sind Bewertungskriterien für den Outsourcing-Dienstleister und dessen Personal, basierend auf den Sicherheitsanforderungen des Outsourcing-Vorhabens, festgelegt?

# M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT

Nachdem ein Outsourcing-Dienstleister ausgewählt wurde, müssen alle Aspekte des Outsourcing-Vorhabens vertraglich in sogenannten Service Level Agreements (SLAs) festgehalten und geregelt werden. Die Aspekte, die im Folgenden beschrieben werden, sind als Hilfsmittel und Checkliste bei der Vertragsgestaltung zu sehen. Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen immer vom speziellen Outsourcing-Projekt ab. Je höher der Schutzbedarf der ausgelagerten IT-Systeme und Anwendungen ist, desto sorgfältiger und detaillierter muss der Vertrag zwischen Auftraggeber und Dienstleister ausgehandelt werden. Der Dienstleister sollte auf Einhaltung des IT-Grundschutzes und auf die vom Auftraggeber vorgegebenen Sicherheitsanforderungen verpflichtet werden (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*). Dazu gehört natürlich, dass der Outsourcing-Dienstleister sich verpflichtet, ein Sicherheitskonzept inklusive eines Notfallvorsorgekonzepts zu erstellen und Sicherheitsmaßnahmen sowie Systeme und Anwendungen zu dokumentieren.

Zusätzlich zur allgemeinen Leistungsbeschreibung empfiehlt es sich jedoch immer, auch eine genaue quantitative Leistungsbeschreibung vertraglich zu fixieren, z. B. zu Verfügbarkeitsanforderungen, Reaktionszeiten, Rechenleistung, zur Verfügung stehendem Speicherplatz, Anzahl der Mitarbeiter, Supportzeiten.

Generell wäre eine allgemeine Verpflichtung auf die Einhaltung des IT-Grundschutzes zwar zufriedenstellend, es empfiehlt sich jedoch immer, alle vereinbarten Leistungen so genau und eindeutig wie möglich vertraglich festzuhalten. Dadurch lassen sich später Streitigkeiten zwischen den Parteien vermeiden. Nachträgliche Konkretisierungen und Ergänzungen des Vertrages, die aufgrund unterschiedlicher Interpretationen der beschriebenen Leistungen notwendig werden, sind oftmals mit deutlichen Kostenerhöhungen für den Auftraggeber verbunden. Auch die Erstellung des Sicherheitskonzeptes selbst sollte Vertragsbestandteil sein. Insbesondere ist zu klären, wer für die fachlichen Inhalte verantwortlich ist und welche Mitwirkungspflichten dem Auftraggeber obliegen.

Im Folgenden findet sich eine Themenliste von Aspekten, die aus Sicherheitssicht geregelt werden sollten. Weitere Hinweise zu Details können den jeweiligen Maßnahmen der IT-Grundschutz-Kataloge entnommen werden:

**Infrastruktur**
- Absicherung der Infrastruktur des Dienstleisters (z. B. Zutrittskontrolle, Brandschutz, ...)

**Organisatorische Regelungen/ Prozesse**
- Festlegung von Kommunikationswegen und Ansprechpartnern
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
  - Verfahren zur Behebung von Problemen, Benennung von Ansprechpartnern mit den nötigen Befugnissen
  - regelmäßige Abstimmungsrunden

- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses)
- Zugriffsmöglichkeiten des Dienstleisters auf IT-Ressourcen des Auftraggebers: Wer greift wie auf welches System zu? Wie sind die Zuständigkeiten und Rechte?
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Dienstleisters zu den Räumlichkeiten und IT-Systemen des Auftraggebers
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Auftraggebers zu den Räumlichkeiten und IT-Systemen des Dienstleisters

**Personal**
- Gestaltung der Arbeitsplätze von externen Mitarbeitern (Einhalten von Computerarbeitsplatzrichtlinien)
- Festlegung und Abstimmung von Vertretungsregelungen
- Verpflichtung zu Fortbildungsmaßnahmen

**Notfallvorsorge**
- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit
- erforderliche Handlungen beim Eintreten eines Störfalls
- Reaktionszeiten und Eskalationsstufen
- Mitwirkungspflicht des Auftraggebers bei der Behebung von Notfällen
- Art und zeitliche Abfolge von regelmäßigen und adäquaten Notfallübungen
- Art und Umfang der Datensicherung
- Vereinbarung, ob bzw. welche Systeme redundant ausgelegt sein müssen
- Von besonderer Bedeutung können Regelungen im Fall höherer Gewalt sein. Es sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Dienstleisters die Verfügbarkeit von Daten und Systemen sichergestellt werden kann. Besonders wenn Dienstleister und Auftraggeber unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Auftraggeber von derartigen Vorkommnissen gänzlich überrascht werden.

**Haftung, juristische Rahmenbedingungen**
- Eine Verpflichtung auf die Einhaltung von geltenden Normen und Gesetzen sowie der vereinbarten Sicherheitsmaßnahmen und sonstigen Rahmenbedingungen ist vertraglich zu regeln. Ebenso sind Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) vertraglich zu fixieren.
- Die Einbindung Dritter, Subunternehmer und Unterauftragnehmer des Dienstleisters ist zu regeln. In der Regel empfiehlt es sich nicht, diese grundsätzlich auszuschließen, sondern sinnvolle Regelungen festzulegen.
- Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Es ist auch zu klären, ob der Dienstleister bereits bestehende Verträge mit Dritten (Hardwareausstattung, Serviceverträge, Softwarelizenzen etc.) übernimmt.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- Regelungen für das Ende des Outsourcing-Vorhabens, z. B. für einen Wechsel oder bei Insolvenz des Dienstleisters, können spezifiziert werden. Auf ein ausreichend flexibles Kündigungsrecht ist zu achten.
- Der Auftragnehmer ist zu verpflichten, nach Beendigung des Auftrags alle Hard- und Software inklusive gespeicherter Daten, die dem Auftraggeber gehören, zurückzugeben. Alle vorhandenen Daten inklusive Datensicherungen sind ebenfalls zurückzugeben oder (je nach Vereinbarung) zu vernichten.

- Die Aufteilung von Risiken zwischen Auftraggeber und Dienstleister muss bedacht werden.
- Haftungsfragen im Schadensfall sind zu klären.
- Sanktionen oder Schadensersatz bei Nichteinhaltung der Dienstleistungsqualität müssen festgelegt werden. Die Bedeutung von Schadensersatzzahlungen und juristischen Konsequenzen sollte dabei nicht überschätzt werden. Zu bedenken sind unter anderem die folgenden Punkte

  - **Quantifizierbarkeit des Schadens**

    - Wie wird beispielsweise ein Imageschaden gemessen?
    - Wie ist es zu bewerten, wenn gravierende Pflichtverletzungen aufgedeckt werden, die nur zufällig nicht zu einem größeren Schaden geführt haben?
  - **Insolvenz des Dienstleisters**

    - Das Recht auf Schadensersatzzahlungen ist wertlos, wenn diese die Zahlungsfähigkeit des Dienstleisters übersteigen und dieser Insolvenz anmeldet. Nachfolgend fallen dann mindestens Kosten für den Umzug zu einem neuen Dienstleister an.
  - **Katastrophale Schäden**

    - Eine Konventionalstrafe kommt zu spät, wenn der Auftraggeber durch das Ausmaß des Schadensereignisses seiner Geschäftsgrundlage beraubt wird und im schlimmsten Fall durch die Schadensfolgen die Zahlungsunfähigkeit eintritt.
  - **Beweisbarkeit**

    - Kann ein Schaden nachgewiesen bzw. der Verursacher überführt werden (z. B. Nachweis von Spionage oder Manipulationen)?

  Es ist immer zu bedenken, dass Schadensersatzzahlungen nur das allerletzte Mittel sind und nicht dazu führen dürfen, dass aus Kostengründen andere Sicherheitsmaßnahmen vernachlässigt werden. Sicherheit lässt sich nicht mit juristischen Mitteln erzielen.

**Mandantenfähigkeit**

- Die notwendige Trennung von IT-Systemen und Anwendungen verschiedener Kunden muss vereinbart werden.

  - Es ist sicherzustellen, dass Probleme bei anderen Kunden nicht die Abläufe und Systeme des Auftraggebers beeinträchtigen.
  - Es ist sicherzustellen, dass Daten des Auftraggebers unter keinen Umständen anderen Kunden des Outsourcing-Dienstleisters zugänglich werden.
- Es ist ein Mandantenkonzept durch den Outsourcing-Dienstleister zu erstellen, in dem beschrieben wird, wie sichergestellt wird, dass die IT-Systeme und Anwendungen mandantenfähig betrieben werden. Dies ist vom Kunden daraufhin zu überprüfen, ob durch die beschriebenen Maßnahmen für den jeweiligen Schutzbedarf eine ausreichende Trennung verschiedener Mandanten erreicht werden kann.
- Falls notwendig, muss die physikalische Trennung (d. h. dezidierte Hardware) vereinbart werden.
- Falls notwendig, muss vereinbart werden, dass die vom Dienstleister eingesetzten Mitarbeiter nicht für andere Auftraggeber eingesetzt werden. Es kann auch sinnvoll sein, diese auf Verschwiegenheit zu verpflichten, so dass die eingesetzten Mitarbeiter nicht mit anderen Mitarbeitern des Dienstleisters auftraggeberbezogene Informationen austauschen dürfen.

**Änderungsmanagement und Testverfahren**

- Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Auftraggeber immer in der Lage ist, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn beispielsweise gesetzliche Vorgaben geändert wurden. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert wird.
- In diesem Zusammenhang ist auch die Betreuung und Weiterentwicklung bereits vorhandener Systeme zu regeln. Nicht selten übernimmt der Dienstleister selbstentwickelte Systeme oder Software vom Auftraggeber, der damit die Fähigkeit verliert, diese in seinem Sinne weiterzuentwickeln. Der Evolutionspfad von Systemen muss daher geregelt werden.
- Eine kontinuierliche Verbesserung der Dienstleistungsqualität und des Sicherheitsniveaus sollte bereits in den SLAs festgeschrieben werden.
- Der Zeitrahmen für die Behebung von Fehlern ist festzulegen.
- Testverfahren für neue Soft- und Hardware sind zu vereinbaren. Dabei sind folgende Punkte einzubeziehen:
    - Regelungen für Updates und Systemanpassungen
    - Trennung von Test- und Produktionssystemen
    - Zuständigkeiten bei der Erstellung von Testkonzepten
    - Festlegen von zu benutzenden Testmodellen
    - Zuständigkeiten bei Auftraggeber und Dienstleister bei der Durchführung von Tests (z. B. Mitarbeit oder Hilfestellung des Auftraggebers, Abnahme- und Freigabeprozeduren)
    - Informationspflicht und Absprache vor wichtigen Eingriffen ins System (Negativbeispiel: Der Dienstleister spielt ein neues Betriebssystem auf dem Server ein. Durch unerwartete Fehler dabei werden wichtige Anwendungen gestört, ohne dass der Auftraggeber sich vorbereiten konnte.)
    - Genehmigungsverfahren für die Durchführung von Tests
    - Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit)

**Kontrollen**

- Dienstleistungsqualität und IT-Sicherheit müssen regelmäßig kontrolliert werden. Der Auftraggeber muss die dazu notwendigen Auskunfts-, Einsichts-, Zutritts- und Zugangsrechte besitzen. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies bereits im Vertrag geregelt sein.
- Allen Institutionen, die beim Auftraggeber Prüfungen durchführen müssen (z. B. Aufsichtsbehörden) müssen auch beim Outsourcing-Dienstleister die entsprechenden Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) eingeräumt werden.

Prüffragen:

- Sind alle Aspekte des Outsourcing-Vorhabens mit dem Outsourcing-Dienstleister schriftlich geregelt?
- Sind die Verantwortlichkeiten und Mitwirkungspflichten zur Erstellung des IT-Sicherheitskonzepts zwischen Outsourcing-Dienstleister und Auftraggeber geregelt?

# M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Für jedes Outsourcing-Vorhaben muss ein Sicherheitskonzept existieren. Dieses kann unter anderem auf Grundlage der IT-Grundschutz-Kataloge erstellt sein. Outsourcing-Projekte sind dadurch gekennzeichnet, dass sich viele technische und organisatorische Details erst im Laufe der Planung und bei Migration der Systeme ergeben. Das Sicherheitskonzept, das nach Beauftragung eines Dienstleisters erarbeitet wird, wird daher in den wenigsten Fällen gleich vollständig und endgültig sein und muss während der Migrationsphase von allen Beteiligten stetig weiterentwickelt und konkretisiert werden. Die Migrationsphase ist daher von entscheidender Bedeutung für den Erfolg des Gesamtprojektes und wird in Maßnahme M 2.255 *Sichere Migration bei Outsourcing-Vorhaben* ausführlich beschrieben.

Generell unterscheiden sich Sicherheitskonzepte für Outsourcing-Vorhaben nur wenig von Sicherheitskonzepten für selbstbetriebene IT-Systeme. Es ergeben sich jedoch folgende Besonderheiten, die berücksichtigt werden müssen:

- Am Outsourcing-Vorhaben sind aus technischer Sicht in der Regel drei Parteien beteiligt:

  - Outsourcing-Auftraggeber
  - Outsourcing-Dienstleister
  - Netzprovider

  Der Netzprovider stellt die Anbindung zwischen den Outsourcing-Parteien bereit. Die Zuständigkeit für die Netzanbindung fällt dabei in der Regel dem Outsourcing-Dienstleister zu.
- Jeder Beteiligte muss ein eigenes Sicherheitskonzept erstellen und umsetzen, welches auch das spezielle Outsourcing-Vorhaben umfasst. Damit sind Sicherheitskonzepte erforderlich:

  - für den Einflussbereich des Outsourcing-Dienstleisters,
  - für den Einflussbereich des Auftraggebers sowie
  - für die Schnittstellen und die Kommunikation zwischen diesen Bereichen.
- Zusätzlich zu den Einzelkonzepten ist ein Sicherheitskonzept für das Gesamtsystem zu erstellen, welches die Sicherheit im Zusammenspiel der Einzelsysteme betrachtet.
- Die verschiedenen Teil-Konzepte müssen zwischen Auftraggeber und Dienstleistern abgestimmt werden. Dabei ist der Auftraggeber am Sicherheitskonzept des Outsourcing-Dienstleisters nicht direkt beteiligt, sollte aber in einem Audit prüfen, ob es vorhanden und ausreichend ist. Für das Audit kann der Auftraggeber dabei auch auf externe Dritte zurückgreifen.

Die in M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben* und M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* genannten Sicherheitsanforderungen bilden dabei die Basis für das Sicherheitskonzept. Aufbauend auf den dort beschriebenen grundlegenden Anforderungen muss im Sicherheitskonzept die detaillierte Ausgestaltung erfolgen, wobei

beispielsweise die Maßnahmen konkretisiert und Ansprechpartner namentlich festgelegt werden.

Erfahrungsgemäß ist der Übergang (Migration) von Aufgaben und IT-Systemen vom Auftraggeber zum Outsourcing-Dienstleister eine Projektphase, in der verstärkt mit Sicherheitsvorfällen zu rechnen ist. Aus diesem Grund müssen im Sicherheitskonzept Regelungen und Maßnahmen zur Migration behandelt werden, die in M 2.255 *Sichere Migration bei Outsourcing-Vorhaben* genauer behandelt werden.

Im Folgenden sind einige Aspekte und Themen aufgelistet, die im Sicherheitskonzept im Detail beschrieben werden sollten. Da die Details eines Sicherheitskonzeptes direkt vom Outsourcing-Vorhaben abhängen, ist die Liste als Anregung zu verstehen und erhebt keinen Anspruch auf Vollständigkeit. Neben einem Überblick über die Gefährdungslage, die der Motivation der Sicherheitsmaßnahmen dient, und den organisatorischen, infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

**Organisation**
- Umgang mit Daten und schützenswerten Betriebsmitteln wie Druckerpapier und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und Löschen/Vernichten
- Festlegung von Aktionen, für die das "Vier-Augen-Prinzip" anzuwenden ist

**Hard-/Software**
- Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren
- Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen
- Einsatz von Datei-Integrität-Prüfungssystemen, um Veränderungen z. B. nach erfolgreichen Angriffen, zu erkennen
- Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen
- Einsatz kaskadierter Firewallsysteme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters
- sorgfältige Vergabe von Benutzer-Kennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters

**Kommunikation**
- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Auftraggeber, um sensitive Daten zu schützen
- Authentisierungsmechanismen
- Detailregelungen für weitere Netzanbindungen (siehe M 5.87 *Vereinbarung über die Anbindung an Netze Dritter*)
- Detailregelungen für den Datenaustausch (siehe M 5.88 *Vereinbarung über Datenaustausch mit Dritten*).

**Kontrollen und QS**
- Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messung von Sicherheit, Dienstqualität, Abläufen und organisatorische Regelungen

**Notfallvorsorge**
- Das Notfallvorsorgekonzept ist in M 6.83 *Notfallvorsorge beim Outsourcing* beschrieben.

Prüffragen:

- Existiert für jedes Outsourcing-Vorhaben ein Informations-Sicherheitskonzept basierend auf den zugehörigen Sicherheitsanforderungen?
- Besitzt jeder Beteiligte am Outsourcing-Vorhaben ein Sicherheitskonzept für seinen Einflussbereich und gibt es zusätzlich ein abgestimmtes Sicherheitskonzept für das Gesamtsystem?
- Wird das Sicherheitskonzept des Dienstleisters und seine Umsetzung durch den Auftraggeber oder unabhängige Dritte überprüft?

# M 2.255 Sichere Migration bei Outsourcing-Vorhaben

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Nach Beauftragung des Outsourcing-Dienstleisters muss zunächst ein vorläufiges Sicherheitskonzept entwickelt werden, in dem auch die Test- und Einführungsphase als Teilaspekt des Outsourcing-Vorhabens betrachtet wird. Zum einen sind in dieser Phase zahlreiche Betriebsfremde involviert, zum anderen müssen Abläufe etabliert, Aufgaben übertragen und Systeme neu eingerichtet bzw. angepasst werden. Einem sorgfältigen Testbetrieb kommt daher eine hohe Bedeutung zu. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die selten sehr sicher sind. Es ist daher beispielsweise sicherzustellen, dass produktive Daten nicht ohne besonderen Schutz als Testdaten verwendet werden. Dies muss durch das Sicherheitskonzept ausgeschlossen werden.

Vor der Erstellung eines Migrationskonzepts als Teil des Sicherheitskonzeptes für ein Outsourcing-Vorhaben muss ein Sicherheitsmanagement-Team speziell für die Migrationsphase beim Auftraggeber eingerichtet worden sein. Dieses muss während der Migrationsphase auf Sicherheitsbelange achten und durch geeignete Maßnahmen auch schon im Vorfeld der Migration dafür sorgen, dass ein sicherer IT-Betrieb während der Migration gewährleistet ist. Die Größe des Sicherheitsmanagement-Teams hängt dabei von Art und Größe des Outsourcing-Vorhabens ab, als Minimum kann es aus einem Sicherheitsexperten bestehen.

Dem Sicherheitsmanagement-Team kommen dabei folgende Aufgaben zu, aus denen sich Regelungen und Vorgaben ableiten, die im Migrationskonzept zu erfassen sind:

- Es ist ein gemischtes Team aus Mitarbeitern des Auftraggebers und des Outsourcing-Dienstleisters zu bilden. Dieses kann auch durch externe Experten verstärkt werden, um spezielles Know-how verfügbar zu machen.
- Für die Migrationsphase muss eine Sicherheitskonzeption erstellt werden.
- Die Verantwortlichkeiten und Hierarchien für die Migrationsphase sind festzulegen. Dabei ist es wichtig, dass klare Führungsstrukturen geschaffen und auf beiden Seiten eindeutige Ansprechpartner definiert werden. Zusätzlich ist darauf zu achten, dass auf beiden Seiten Verantwortlichkeiten auch auf hohen Ebenen definiert werden. Nur so kann sichergestellt werden, dass im Zweifelsfall mit entsprechendem Nachdruck gehandelt werden kann.
- Die erforderlichen Tests müssen geplant und durchgeführt werden, Abnahmeprozeduren erarbeitet und die Produktionseinführung geplant werden.
- Es sind geeignete interne Mitarbeiter für die Test-, Einführungsphase und den späteren Betrieb auszuwählen. Vertraglich kann sich ein Auftraggeber natürlich auch ein Mitspracherecht bei der Personalauswahl des Outsourcing-Dienstleisters einräumen lassen.
- Die Mitarbeiter des Auftraggebers sind zum Verhalten während und nach der Migrationsphase zu schulen. In der Regel sind die Mitarbeiter dabei mit neuen und unbekannten Ansprechpartnern konfrontiert. Dies birgt die Gefahr des Social Engineering (z. B. Anruf eines vermeintlichen Mitarbeiters des Sicherheitsteams des Dienstleisters).

- Der Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Auftraggebers genau kennen lernen und dahingehend eingewiesen werden.
- Der störungsfreie Betrieb ist durch genaue Ressourcenplanung und Tests sicherzustellen. Die produktiven Systeme dürfen dabei nicht vernachlässigt werden. Dazu ist im Vorfeld zu überprüfen, ob die vorgesehenen Mitarbeiter zur Verfügung stehen. Zusätzlich müssen Störungen durch notwendige Tests einkalkuliert werden.
- Anwendungen und IT-Systeme, die der Dienstleister übernehmen soll, müssen ausreichend dokumentiert sein. Die Prüfung der Dokumentation auf Vollständigkeit muss dabei ebenso bedacht werden wie das Anpassen der vorhandenen Dokumentation auf die veränderten Randbedingungen durch das Outsourcing-Vorhaben. Die Dokumentation neuer Systeme oder Teilsysteme muss dabei ebenfalls sichergestellt sein.
- Während der Migration muss ständig überprüft werden, ob die SLAs oder die vorgesehenen Sicherheitsmaßnahmen angepasst werden müssen.

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen eingestellt hat, sind verstärkt Mitarbeiter zu Bereitschaftsdiensten zu verpflichten.

Nach Abschluss der Migration muss sichergestellt werden, dass das Sicherheitskonzept aktualisiert wird, da sich erfahrungsgemäß während der Migrationsphase immer Änderungen ergeben. Dies bedeutet insbesondere:

- Alle Sicherheitsmaßnahmen müssen konkretisiert werden.
- Ansprechpartner und Zuständigkeiten werden mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert.
- Die Systemkonfigurationen ist zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.

Als letzte Aufgabe muss das Outsourcing-Vorhaben nach der Migrationsphase in den sicheren Regelbetrieb (siehe M 2.256 *Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb*) überführt werden. Dabei ist vor allem darauf zu achten, dass alle Ausnahmeregelungen, die während der Migrationsphase notwendig waren, wie z. B. erweiterte Zugriffsrechte, aufgehoben werden.

Prüffragen:

- Ist ein Sicherheitskonzept für die Migrationsphase erarbeitet, in dem auch die Test- und Einführungsphase betrachtet werden?
- Ist sichergestellt, dass produktive Daten in der Migrationsphase nicht ungeschützt als Testdaten verwendet werden?
- Sind die Mitarbeiter des Auftraggebers wie auch des Outsourcing-Dienstleisters auf die Migration vorbereitet?
- Werden alle Änderungen nach Abschluss der Migrationsphase im Sicherheitskonzept erfasst?
- Ist sichergestellt, dass alle Ausnahmeregelungen am Ende der Migrationsphase aufgehoben werden?

# M 2.256 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Nachdem ein Outsourcing-Vorhaben umgesetzt wurde, muss die Informationssicherheit auch im laufenden Betrieb gewährleistet werden. Dazu ist für das Outsourcing-Vorhaben ein Betriebskonzept zu planen, in dem auch die Sicherheitsaspekte berücksichtigt werden. Dabei unterscheiden sich die IT-bezogenen Einzelaufgaben generell nicht von denen, die zu planen und durchzuführen sind, wenn kein Outsourcing betrieben wird (siehe M 2.199 *Aufrechterhaltung der Informationssicherheit*).

Besonderheiten ergeben sich jedoch dadurch, dass die Aufgaben auf mehrere Parteien verteilt sind und daher zusätzliche Aufgaben (z. B. Abstimmungen und Kontrollen) anfallen. Diese sind unter anderem:

- Dokumentationen und Richtlinien müssen regelmäßig aktualisiert werden.
- Die geltenden Sicherheitskonzepte aller Beteiligten müssen daraufhin geprüft werden, ob sie noch aufeinander abgestimmt sind und das gewünschte Sicherheitsniveau gewährleisten. Insbesondere sollte der Outsourcing-Dienstleister den Auftraggeber über wichtige Änderungen in seinem Einflussbereich informieren.
- Regelmäßige Kontrollen zu folgenden Aspekten sind durchzuführen:
  - Durchführung der vereinbarten Audits
  - Umsetzungsstand der vereinbarten Sicherheitsmaßnahmen
  - Wartungszustand von Systemen und Anwendungen
  - Rechtezuweisung durch den Dienstleister (Missbrauch von Rechten)
  - Einsatz von Mitarbeitern, die dem Auftraggeber nicht gemeldet wurden, z. B. bei Vertretungen
  - Performance, Verfügbarkeit, Qualitätsniveau
  - Datensicherung
- Regelmäßige Abstimmungsrunden zu folgenden Punkten sind abzuhalten:
  - Informationen müssen zwischen den Partnern ausgetauscht werden (z. B. Personalnachrichten, organisatorische Regelungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen, die zu Beeinträchtigungen der Dienstleistungsqualität führen können).
  - Probleme müssen identifiziert und analysiert werden.
  - Wichtig sind gegenseitiges Feedback und das Aufspüren von Verbesserungspotentialen. Zur Motivation der Mitarbeiter können besonders positive Beispiele einer gelungenen Kooperation dargestellt werden.
  - Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) sollten frühzeitig besprochen werden.
- Es müssen regelmäßige Übungen und Tests zu folgenden Themen durchgeführt werden:
  - Reaktion auf Systemausfälle (Teilausfall, Totalausfall)

- Wiedereinspielen von Datensicherungen
- Beherrschung von Sicherheitsvorfällen

Prüffragen:

- Existiert ein Betriebskonzept für das Outsourcing-Vorhaben, das auch die Sicherheitsaspekte berücksichtigt?
- Werden die Sicherheitskonzepte der Outsourcing-Partner regelmäßig auf Aktualität und Konsistenz zueinander geprüft?
- Wird der Status der vereinbarten Sicherheitsmaßnahmen regelmäßig kontrolliert?
- Findet zwischen den Outsourcing-Partnern eine regelmäßige Kommunikation einschließlich Abstimmung zu Änderungen und Verbesserungen statt?
- Führen die Outsourcing-Partner regelmäßig gemeinsame Übungen und Tests zur Aufrechterhaltung des Sicherheitsniveaus durch?

# M 2.257 Überwachung der Speicherressourcen von Archivmedien

**Verantwortlich für Initiierung:** Archivverwalter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, Leiter IT

Die auf den Archivmedien vorhandene, freie Speicherkapazität ist kontinuierlich zu überwachen. Wenn die freie Speicherkapazität unter einen festzulegenden Schwellwert sinkt, sollte eine Benachrichtigung des Administrators sowie gegebenenfalls eine Signalisierung an eine Systemmanagement-Umgebung erfolgen. Sinkt die freie Speicherkapazität weiter unter einen kritischen Grenzwert, sollte eine Alarmierung ausgelöst werden. Bei der Alarmierung ist besonders darauf zu achten, dass sie rollenbezogen erfolgt, das heißt unabhängig von konkreten Personen. Damit ist sichergestellt, dass auch im Krankheitsfall oder bei Urlaub Alarmierungen wahrgenommen werden.

Der Schwellwert, der kritische Grenzwert sowie die Eskalationsprozeduren und -wege sind organisationsspezifisch festzulegen.

Für die Festlegung der Grenzwerte müssen die verwendeten Archivmedien und das durchschnittliche Volumen der zu archivierenden Daten zugrunde gelegt werden. Nach Auslösen des kritischen Alarms muss gewährleistet sein, dass für eine hinreichende Zeit weiterhin das durchschnittliche Datenaufkommen archiviert werden kann. Typischerweise wird für den Schwellwert eine Restkapazität von 15% der Gesamtkapazität des Speichermediums und für den kritischen Grenzwert eine Restkapazität von 10% zugrunde gelegt.

Um etwaige Lieferengpässe bei Speichermedien zu überbrücken, sollte eine ausreichende Zahl leerer Archivmedien an einem bekannten Ort gelagert werden. Dabei müssen die klimatischen und physikalischen Lagerbedingungen eingehalten werden (siehe M 1.60 *Geeignete Lagerung von Archivmedien*).

Für den Fall der Alarmierung ist zu dokumentieren, in welcher Weise und in welchem Zeitraum eine Reaktion auf die Alarme erfolgen soll. Dies ist z. B. in *Service Level Agreements* (SLAs) festzulegen, falls der Betrieb des Archivsystems durch Dritte erfolgt.

Neben dem Speicherplatz müssen ggf. noch betriebssystem- oder anwendungsspezifische Restriktionen überwacht werden. Die entsprechenden Programmdokumentationen müssen daraufhin geprüft werden. In Zweifelsfällen oder bei fehlenden Angaben in der Dokumentation sollte der jeweilige Hersteller zu Rate gezogen werden. Beispielsweise können die Anzahl der maximal zugelassenen Dateien pro Verzeichnis oder die maximal erlaubten Datenbankeinträge überschritten werden, so dass keine weiteren Daten auf dem Speichermedium angelegt werden können.

Prüffragen:

- Wird der freie Speicherplatz des Archivsystems kontinuierlich überwacht?
- Erfolgt eine rollenbezogene Alarmierung bei Unterschreiten von Grenzwerten der freien Speicherkapazität von Archivmedien?
- Werden genügend leere Archivmedien an einem bekannten Ort ordnungsgemäß gelagert?

# M 2.258 Konsistente Indizierung von Dokumenten bei der Archivierung

**Verantwortlich für Initiierung:** Archivverwalter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, Leiter IT

Beim Betrieb eines Archivs ist es wichtig, alle abgelegten Dokumente und Datensätze eindeutig zu referenzieren, um sie bei späteren Archivanfragen korrekt wiederfinden zu können. Zusätzlich bieten Archivsysteme die Möglichkeit von Suchanfragen. Da eine Volltextsuche abhängig von Art und Umfang der archivierten Daten sehr lange dauern kann, speichern Archivsysteme zu jedem Dokument einen separaten Datensatz mit Indexangaben in einer eigenen Suchdatenbank. Struktur und Umfang der Indexangaben sind in der Regel konfigurierbar und sollten die folgenden Eigenschaften aufweisen:

- Eindeutigkeit: Die Dokumentenbezeichner müssen eindeutig sein.
- Unterstützung zu erwartender Suchanfragen: Durch die Kontextangaben sollen spätere Suchanfragen beschleunigt werden. Da der spätere Suchkontext nicht feststeht, kann im Vorfeld nur eine Abschätzung späterer Suchanfragen vorgenommen und versucht werden, die Kontextangaben so aussagekräftig wie möglich zu gestalten.
- Geringer Umfang: Ein geringer Umfang an Indexdaten beschleunigt spätere Suchanfragen, jedoch kann ein zu geringer Umfang der Indexdaten Suchanfragen behindern bzw. das Auffinden von Dokumenten erschweren. Der Umfang der Kontextangaben ist letztlich in Abhängigkeit vom erwarteten Datenvolumen festzulegen.

Diese Parameter müssen grundsätzlich vor der Inbetriebnahme des Archivs festgelegt werden. Trotzdem kann es im Laufe der Zeit notwendig werden, die Eigenschaften zu ändern. Je nach Umfang und Art der Änderung der Indexdaten kann dies eine sehr aufwändige Neuindizierung der Archivdatenbestände erforderlich machen.

Der konkrete Kontext für einzelne zu archivierende Dokumente kann auf unterschiedliche Art und Weise erzeugt werden. Drei Verfahren werden dabei unterschieden:

- **manuelle Erstellung:**
  Auf der Ebene des Dokumentenmanagementsystems werden Indexangaben zu jedem Dokument über eine Eingabemaske manuell erzeugt. Hierdurch besteht besonders bei großen Datenmengen die Gefahr, dass inkonsistente Indexangaben erfasst werden.
- **halbautomatische Erzeugung:**
  Diese Verfahren automatisieren die Vergabe von Indexdaten, gestatten jedoch eine manuelle Kontrolle und Korrektur.
- **vollautomatische Erzeugung:**
  Hierbei werden Dokumentindizes vollautomatisch ohne manuelle Eingriffsmöglichkeit vergeben.

Die Wahl des Verfahrens ist abhängig vom erwarteten Datenvolumen. Werden in unregelmäßigen Abständen einzelne Dokumente archiviert, ist ein manuelles Verfahren auf der Grundlage konkreter Vorgaben zur Erstellung eines Kontextes ausreichend.

Werden regelmäßig große Datenvolumen archiviert, sollte ein halbautomatisches Verfahren zur Erzeugung der Indexdaten gewählt werden. Hier besteht die Möglichkeit, diese Informationen manuell zu kontrollieren und zu korrigie-

ren, bevor Dokument und Dokumentindex archiviert werden und dann gegebenenfalls nicht mehr nachträglich geändert werden können.

Bei der vollautomatischen Erzeugung der Indexdaten können Fehler nicht erkannt bzw. korrigiert werden. Eine eventuelle Fehlzuordnung von zu archivierenden Dokumenten, z. B. zu Geschäftsprozessen, kann dann nicht erkannt oder ausgeschlossen werden. Dieses Verfahren sollte deshalb nur dann angewandt werden, wenn alle Dokumente so strukturiert sind, dass alle Indexdaten in jedem Fall zweifelsfrei und zuverlässig extrahiert werden können.

Prüffragen:

- Sind alle abgelegten Dokumente und Datensätze beim Betrieb eines Archivs eindeutig referenziert?
- Wurde die Struktur und der Umfang der Indexangaben des Archivs vor Inbetriebnahme festgelegt?
- Regelmäßige Archivierung großer Datenvolumen und konfigurierbare Indexangaben: Wird ein halbautomatisches Verfahren zur Indexdatenerzeugung verwendet?
- Vollautomatische Indexdatenerzeugung: Können alle Indexdaten zuverlässig und zweifelsfrei extrahiert werden?

# M 2.259 Einführung eines übergeordneten Dokumentenmanagements

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Bei der elektronischen Archivierung müssen alle archivierten Dokumente eindeutig identifiziert und reproduziert werden können. Da dabei in der Regel große Datenbestände zu verwalten sind, wird der Einsatz eines übergeordneten Dokumentenmanagement-Systems (DMS), auch für kleine und mittlere Behörden bzw. Unternehmen, empfohlen.

**Dokumentenmanagement-System**

Ein Dokumentenmanagement-System (DMS) bildet die Schnittstelle zwischen Benutzer (-programmen) und Archivsystem und sorgt für eine konsistente Verwaltung, Versionierung und Zuordnung von elektronischen Dokumenten.

Das DMS übernimmt regelmäßig auch die Pflege der Index-Datenbank, in der die zu den elektronischen Dokumenten archivierte Kontextinformation verwaltet und eventuell um DMS-Bestandteile ergänzt wird.

Unterschieden werden dabei zum einen Systeme, die neben den Indizes auch die Dokumente selbst in einer Datenbank ablegen, und zum anderen Systeme, die in ihrer Datenbank ausschließlich Referenzdaten auf die eigentlichen Dokumente im jeweiligen Speichersystem ablegen. Die erstgenannten Systeme sind allerdings durch die Kapazität der Datenbank eingeschränkt und eignen sich damit nicht für die Archivierung großer Datenmengen.

Darüber hinaus muss ein Dokumentenmanagement-System die Festlegung von Zugriffsberechtigungen zu den archivierten Dokumenten sowie zur Index-Datenbank ermöglichen. Das DMS sollte auch eine Klassifikation von Dokumenten unterstützen. Es sollten Profile und Referenztabellen angelegt werden können, anhand derer Dokumente klassifiziert und verschlagwortet werden.

Die Eigenschaften des DMS müssen langfristig gewährleisten, dass die archivierten Dokumente eindeutig identifiziert, geschützt und reproduziert werden können.

**Organisatorische Einbettung**

Dokumentenmanagement-Systeme müssen in geeigneter Weise eingesetzt und in die Organisation eingebettet werden. Hierzu sind entsprechende Organisationsprozesse zu definieren, zu dokumentieren und in der Behörde bzw. im Unternehmen umzusetzen.

Regelungsbedarf besteht unter anderem hinsichtlich

- des Einstellens von Dokumenten ins DMS,
- der Nutzung des DMS beim Umgang mit Dokumenten,
- der Verantwortlichkeiten für Nutzung und Betrieb des DMS,
- der Rechtevergabe und der Zuständigkeit hierfür sowie
- der Anforderungen an den Betrieb des DMS (Service Level Agreements).

Letztlich soll durch die Organisationsprozesse sichergestellt werden, dass das Dokumentenmanagement auch in der vorgesehenen Weise benutzt und nicht

etwa umgangen wird. Nur so ist eine vollständige und konsistente Archivierung der in der Organisation genutzten elektronischen Dokumente und Informationen möglich.

**Standardisierung**

Die am Markt angebotenen Dokumentenmanagement- und Archivsysteme sind nicht alle miteinander kompatibel. Dies ist sowohl durch die verwendete Technologie als auch durch die verwendeten Medien- und Speicherformate verursacht.

Um diese Probleme zu beheben, arbeiten die am Markt operierenden DMS-Hersteller in verschiedenen Gremien an der Vereinheitlichung der dem Dokumentenmanagement zugrundeliegenden Technologien zum Speichern und Wiedergewinnen von Dokumenten. Bei der Auswahl des DMS sollten die betreffenden Standards berücksichtigt werden, damit DMS- und Archivkomponenten langfristig verträglich sind.

Die wichtigsten Gruppen bzw. Standards sind:

- ODMA
  Innerhalb der AIIM (**A**ssociation for **I**nformation and **I**mage **M**anagement) ist die ODMA-Gruppe (**O**pen **D**ocument **M**anagement **A**PI) als Standardisierungsgremium tätig. ODMA bezeichnet eine standardisierte Schnittstelle zwischen dem Dokumentenmanagement-System und den Benutzeranwendungen. Es vereinfacht an dieser Stelle die Einbindung der Anwendungen.
  Die meisten Anbieter unterstützen diesen Standard.
- DMA
  Die DMA (**D**ocument **M**anagement **A**lliance) ist als Projektgruppe innerhalb der AIIM gegründet worden. Sie ist aus einem Zusammenschluss von drei anderen Standardisierungsgremien, die ebenfalls im Umkreis der DMS gearbeitet haben, hervor gegangen:

  - ISO-Gruppe Document Filing and Retrieval - ISO 10166
  - Document Enabled Networking
  - Shamrock Document Management Coalition

  Die DMA etabliert einen Standard, mit dessen Hilfe Dokumentensammlungen und Dokumentenmanagement-Software über verschiedene Plattformen und Systeme hinweg einfach integriert werden können.
  Für den Benutzer ergibt sich so eine einheitliche Sicht auf alle Dokumenttypen, unabhängig vom Ort der Ablage oder der Erstellung.
  Nahezu alle führenden Hersteller halten diesen Standard ein. Im konkreten Einzelfall ist die Einhaltung der Standards allerdings zu prüfen.
- WfMC
  Die WfMC (**W**ork**f**low **M**anagement **C**oalition, Belgien) arbeitet als Standardisierungsorgan im Bereich der Workflows.
  Das Ziel ist, Software-Spezifikationen zu erstellen, mit deren Hilfe einheitliche Voraussetzungen für das Zusammenwirken unterschiedlichster Workflow-Produkte und -Komponenten in unterschiedlichsten Umgebungen geschaffen werden.
  Fast alle namhaften Hersteller arbeiten in diesem Gremium mit.

Prüffragen:

- Gewährleistet das Dokumentenmanagement-System (DMS) langfristig, dass alle archivierten Dokumente eindeutig identifiziert, geschützt und reproduziert werden können?

- Unterstützt das DMS die Vergabe und Kontrolle von Rollen und Zugriffsberechtigungen zu archivierten Dokumenten?
- Ist die Nutzung des DMS in der Organisation verpflichtend geregelt, so dass es nicht umgangen wird?
- Ist die Kompatibilität zwischen Benutzer-, DMS- und Archivkomponenten aufgrund einschlägiger Standards gewährleistet?
- Ist überprüft worden, ob der Einsatz eines Dokumentenmanagement-Systems sinnvoll ist?
- Ist die Verantwortung für Betrieb und Nutzung des DMS dokumentiert und bekannt?
- Ist die Nutzung des DMS in der Organisation verpflichtend geregelt und dokumentiert?
- Unterstützt das DMS die Vergabe und Kontrolle von Rollen und Zugriffsberechtigungen?

# M 2.260 Regelmäßige Revision des Archivierungsprozesses

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Revisor
**Verantwortlich für Umsetzung:** Archivverwalter, IT-Sicherheitsbeauftragter, Revisor

Der Prozess der Archivierung ist regelmäßig einer Revision zu unterziehen, um seine Korrektheit und Ordnungsmäßigkeit zu prüfen und daraus die Korrektheit und Authentizität der im Archivsystem abgelegten Dokumente abzuleiten.

Hierzu ist eine geeignete Vorgehensweise für die Revision entsprechend des in M 2.243 *Entwicklung des Archivierungskonzepts* beschriebenen Konzeptes zu entwickeln und in Form einer Checkliste zu dokumentieren.

Diese Checkliste sollte mindestens die folgenden Punkte umfassen:

**Fragen zu Verantwortlichkeiten**
- Sind die verantwortlichen Personen benannt und in ihre Aufgaben eingewiesen worden? Ist dies dokumentiert?
- Bestehen Vertretungsregelungen für alle verantwortlichen Personen?

**Fragen zum Organisationsprozess**
- Bestehen organisationsweite Regelungen zum Einsatz elektronischer Archivierung?
- Ist organisationsweit geregelt und dokumentiert, welche Dokumente zu archivieren sind? Ist diese Regelung umfassend und vollständig?
- Sind die Sicherheitsanforderungen an die Dokumente dokumentiert?
- Werden die organisationsweiten Regelungen regelmäßig an aktuelle Entwicklungen angepasst?
- Werden alle Anpassungen der Regelungen ordnungsgemäß dokumentiert und archiviert?

**Fragen zum Einsatz der Archivierung**
- Bestehen eindeutige Regelungen, welche Dokumente zu archivieren sind?
- Bestehen dokumentierte Regelungen, welche Kontextangaben zu archivierten Dokumenten vergeben werden, etwa die Angabe von Dokumentkategorien?
- Werden die zu archivierenden Dokumente vollständig und reproduzierbar archiviert?
- Werden die Anforderungen an die Vertraulichkeit der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Authentizität der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Integrität der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Verfügbarkeit der zu archivierenden Dokumente eingehalten?
- Werden die rechtlichen Vorgaben an die Archivierung eingehalten?
- Sind alle Benutzer und Administratoren entsprechend ihrer Rollen und Aufgaben geschult und eingewiesen? Ist dies dokumentiert?

**Fragen zur Redundanz der Archivdaten**

- Werden Archivdaten ausreichend redundant gespeichert und aufbewahrt, z. B. durch den Einsatz redundanter Archivsysteme oder alternativer Backup-Medien?
- Erfolgt eine regelmäßige Datensicherung der Archivsysteme sowie gegebenenfalls der Archivdaten?
- Sind die Datensicherungen den Vorgaben entsprechend durchgeführt worden?
- Sind die Datensicherungen der Archivdaten vollständig und lesbar?
- Gab es seit der letzten Revision Datenverluste?
  Wenn ja, wie häufig und wie schwer waren diese Vorfälle?
- Traten Fehler bei der Rekonstruktion archivierter Dokumente auf?
  Wenn ja, wie häufig waren diese Vorfälle und waren die Fehler behebbar?

**Fragen zur Administration**

- Wird der geforderte Refresh-Zyklus der Archivmedien eingehalten?
- Werden nicht mehr benötigte, beschriebene Archivmedien ordnungsgemäß vernichtet und entsorgt?
- Werden Lesegeräte und Speichermedien im geforderten Maße vorgehalten?

**Technische Beurteilung des Archivsystems**

Die Revision sollte auch eine technische Neubewertung der Archivsystem-Komponenten und der verwendeten Datenformate beinhalten. Hierdurch soll gewährleistet werden, dass technische Weiterentwicklungen frühzeitig erkannt werden und technische Änderungen am Archivsystem selbst durch den Hersteller im Vorfeld bekannt sind.

Bei dieser Prüfung kann sich herausstellen, dass technische Komponenten des Archivsystems geändert werden müssen. Dann muss sichergestellt werden, dass ausgetauschte Komponenten, z. B. Laufwerke, Speichermedien, Betriebssoftware, einwandfrei mit allen anderen Komponenten unter Beibehaltung der für den Betrieb notwendigen Funktionalität zusammenarbeiten.

Die Prüfergebnisse der Revisionen sind ebenfalls gemäß den Anforderungen an den Archivierungsprozess selbst zu archivieren.

Prüffragen:

- Wird der Prozess der Archivierung regelmäßig einer Revision unterzogen?
- Enthält die Checkliste zur Revision Fragen zu Verantwortlichkeiten, dem Organisationsprozess, Einsatz der Archivierung, Redundanz der Archivdaten, der Administration und der technischen Beurteilung des Archivsystems?
- Werden die Prüfergebnisse der Revision gemäß den Anforderungen des Archivierungsprozesses archiviert?

# M 2.261 Regelmäßige Marktbeobachtung von Archivsystemen

**Verantwortlich für Initiierung:** Archivverwalter, Leiter IT
**Verantwortlich für Umsetzung:** Archivverwalter, Leiter IT

Die geforderten Aufbewahrungszeiten für Archivdaten liegen normalerweise um ein Vielfaches höher als die durchschnittliche Lebenserwartung einzelner Bestandteile eines elektronischen Archivs. Dies betrifft sowohl Hardware- als auch Software-Komponenten.

Um den vollen Funktionsumfang über den gesamten Zeitraum der Archivierung dennoch sicher zu stellen, ist davon auszugehen, dass einzelne Hardware-Komponenten, ganze Baugruppen oder auch Software-Komponenten unter Umständen mehrfach ausgetauscht werden müssen.

Eine wichtige Voraussetzung dazu ist eine regelmäßige Marktbeobachtung. Diese dient dazu, sich abzeichnende Veränderungen rechtzeitig zu registrieren. Solche Veränderungen können z. B. sein:

- Änderung eines alten Standards oder Verabschiedung eines neuen Standards bei Speicherformaten,
- Veränderungen beim Hersteller des genutzten Archivsystems oder seiner Speicherkomponenten (Wechsel auf neue Systemplattformen, Beendigung einer Produktreihe und Einstellung des Supports, Einstellung der Produktion von Speichermedien, Insolvenz eines Herstellers),
- Bekanntwerden von Sicherheitslücken oder Schwachstellen, z. B. bei eingesetzten Verschlüsselungsalgorithmen.

Es wird empfohlen, einen regelmäßigen Kontakt zu allen beteiligten Herstellern aufzubauen, beispielsweise durch die Teilnahme an Informationsforen, z. B. Newsgroups und Mailinglisten, in denen aktuelle Informationen über das eingesetzte Archivsystem regelmäßig versandt werden.

Es sollte mindestens eine Person dafür verantwortlich sein, die oben beschriebenen Informationen regelmäßig aufzunehmen, nach ihrer Bedeutung für das verwendete Archivsystem auszuwerten und gegebenenfalls notwendige Aktivitäten zu empfehlen. Hierzu muss festgelegt werden, wie eine eventuell erforderliche Migration des Systems eingeleitet wird. Die hier gewonnenen Informationen fließen in die regelmäßige Revision des Archivierungsprozesses (siehe M 2.260 *Regelmäßige Revision des Archivierungsprozesses*) ein.

Prüffragen:

- Wird der Markt für Archivsysteme regelmäßig beobachtet, wobei erhaltene Informationen ausgewertet und notwendige Aktivitäten eingeleitet werden?

# M 2.262 Regelung der Nutzung von Archivsystemen

**Verantwortlich für Initiierung:** Archivverwalter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, Leiter IT

Durch entsprechende Regelungen ist sicherzustellen, dass das Archivsystem in der im Archivierungskonzept (siehe Maßnahme M 2.243 *Entwicklung des Archivierungskonzepts*) vorgesehenen Weise genutzt wird. Hierzu sollten Richtlinien für die Benutzung und die Administration des Archivsystems erstellt werden. Die Richtlinien sind entsprechend den organisatorischen Gepflogenheiten in der jeweiligen Institution zu verankern und bekanntzugeben. Beim Einsatz externer Personen sind diese auf die Beachtung dieser Richtlinien zu verpflichten.

Die Administrationsrichtlinien sollten mindestens die folgenden Punkte umfassen:

- Festlegung der Verantwortung für Betrieb und Administration des Archivsystems,
- Vereinbarungen über Leistungsparameter (Service Level Agreements) beim Betrieb des Archivsystems, insbesondere wenn die Administration oder der Betrieb durch Externe erfolgen soll,
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten zu den Komponenten des Archivsystems und den Archivmedien,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen für das Archivsystem und die verwendeten Archivmedien,
- Regelung zur Datensicherung der Software-Komponenten des Archivsystems selbst,
- Protokollierung der Aktivitäten am Archivsystem.

Die Benutzerrichtlinien sollten mindestens umfassen:

- Erläuterung der Zielsetzung der elektronischen Archivierung und der Archivierungsfristen für Dokumente,
- Festlegung der Verantwortung für Arbeiten mit dem Archivsystem,
- Festlegung, in welchem Umfang die Nutzung des Archivsystems verpflichtend ist,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Schulungsanforderungen an Benutzer, damit sie zur Nutzung des Archivsystems freigeschaltet werden dürfen,
- Regelung der Vergabe von Kontextinformationen zu den archivierten Dokumenten, siehe auch M 2.258 *Konsistente Indizierung von Dokumenten bei der Archivierung*,
- Verpflichtung zum sorgfältigen Umgang mit recherchierten Dokumenten unter Beachtung der eventuellen Zweckbindung der Informationen,
- Regelung zum Umgang mit Dokumenten nach Ablauf der festgelegten Archivierungsdauer,
- Regelung, dass Daten, deren Löschung nach einem festgelegten Zeitraum vorgesehen ist, nicht mehr verwendet werden dürfen, obwohl sie unter Umständen aus technischen Gründen noch vorhanden sind,
- Regelung zum Umgang mit personenbezogenen Daten,

- Nutzung der vom Archivsystem bereitgestellten Schutzmechanismen, um eine spätere Prüfung der Integrität und Authentizität der archivierten Dokumente zu ermöglichen, sowie zur Gewährleistung der erforderlichen Vertraulichkeit,
- Verpflichtung zur Überprüfung der Integrität und Authentizität recherchierter Dokumente vor der Weiterverwendung,
- Umgang mit Daten, deren Integrität sich nicht nachweisen lässt, z. B. bei fehlgeschlagener Signaturprüfung,
- Protokollierung der Benutzeraktivitäten am Archivsystem,
- Abrechnungsmodalitäten bei Nutzung des Archivsystems durch mehrere Organisationseinheiten.

Die Regelungen sowie deren Kenntnisnahme durch die Administratoren und Benutzer des Archivsystems sind zu dokumentieren.

Prüffragen:

- Wird überprüft, ob das Archivsystem laut dem Archivierungskonzept genutzt wird?
- Sind Richtlinien für die Benutzung und die Administration des Archivsystems erstellt?
- Werden externe Personen auf die Beachtung der Richtlinien verpflichtet?
- Legt die Administrationsrichtlinie die Verantwortung für Betrieb, Administration, Zugriffsrechte und Leistungsparameter des Archivsystems fest?
- Werden die Regelungen und die Kenntnisnahme durch Administratoren und Benutzer des Archivsystems dokumentiert?

# M 2.263 Regelmäßige Aufbereitung von archivierten Datenbeständen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Archivverwalter, Leiter IT

Für eine ordnungsgemäße Archivierung muss über den gesamten Archivierungszeitraum hinweg sichergestellt werden, dass

- das benutzte Datenformat dem Stand der Technik entspricht und von den verwendeten Anwendungen derzeit und zukünftig verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar sind und unter Beibehaltung der Semantik und der Nachweiskraft reproduziert werden können,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit physikalisch einwandfrei gelesen werden können,
- die verwendeten kryptographischen Verfahren zur Verschlüsselung und zur digitalen Signatur dem Stand der Technik entsprechen und
- für alle Komponenten der Speichereinheit (Speichermedien, Laufwerke, Jukeboxen sowie die Steuersoftware) Ersatz- und Wartungsmöglichkeiten bestehen.

Ist abzusehen, dass eine der geforderten Eigenschaften in naher Zukunft nicht mehr gegeben ist, müssen die betroffenen Systeme ausgetauscht werden. Dabei ist zu berücksichtigen, dass unter Umständen eine erhebliche Menge an archivierten Daten auf neue Datenträger kopiert werden muss.

Für die Aufbereitung verschlüsselter oder signierter Dokumente wird auf die Maßnahmen M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung* und M 2.265 *Geeigneter Einsatz digitaler Signaturen bei der Archivierung* verwiesen.

Prüffragen:

- Entspricht das benutzte Datenformat während des Archivierungszeitraums dem Stand der Technik und kann von den verwendeten Anwendungen verarbeitet werden?
- Sind die gespeicherten Daten während des Archivierungszeitraums lesbar und unter Beibehaltung der Semantik und Nachweisbarkeit reproduzierbar?
- Kann das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten während des Archivierungszeitraums verarbeitet werden?
- Können die Speichermedien während des Archivierungszeitraums jederzeit physikalisch einwandfrei gelesen werden?
- Entsprechen die verwendeten kryptographischen Verfahren zur Verschlüsselung und zur digitalen Signatur während des Archivierungszeitraums dem Stand der Technik?
- Werden Systeme, die in naher Zukunft nicht mehr den Leistungsanforderungen entsprechen, ausgetauscht?

# M 2.264 Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Informationssicherheitsmanagement, Leiter IT

Kryptographische Verfahren unterliegen einem technologischen Alterungsprozess, da im Laufe der Zeit durch mathematische oder technische Weiterentwicklungen Schwächen aufgezeigt werden können, die bei deren Auswahl noch nicht bekannt oder relevant waren.

Bei Aufbewahrungsfristen von 10 Jahren und länger ist davon auszugehen, dass verschlüsselte oder signierte Daten wiederholt mit neuen Schlüsseln und gegebenenfalls auf Basis neuer Algorithmen umgeschlüsselt werden müssen, um die Vertraulichkeit bzw. Integrität der Daten weiterhin zu schützen.

Um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist, sollten die Entwicklungen auf dem Gebiet der Kryptographie kontinuierlich beobachtet werden. Darüber hinaus sind einschlägige Informationsquellen laufend dahingehend auszuwerten, ob Möglichkeiten bekannt werden, bestehende Verfahren zu kompromittieren.

Wenn die verwendeten Kryptoverfahren nicht mehr zeitgemäß sind und daher die Vertraulichkeit oder Integrität der verschlüsselten Daten nicht mehr sichergestellt werden kann, müssen die Daten neu verschlüsselt bzw. signiert werden.

Folgende Aspekte sind bei der Neuverschlüsselung zu beachten (siehe auch Baustein B 1.7 *Kryptokonzept*):

- Es muss ein nach aktuellen Maßstäben sicherer Kryptoalgorithmus verwendet werden, von dem angenommen werden kann, dass er für einen langen Zeitraum sicher ist.
- Es muss ein Verfahren zur Verschlüsselung und Schlüsselverteilung gewählt werden, das den Anforderungen der Archivierungsanwendung gerecht wird.
- Die neu erzeugten Schlüssel müssen auf sicherem Weg an die Benutzer des Kryptoverfahrens verteilt werden.
- Eine Authentisierung der Kryptoschlüssel (z. B. durch ein elektronisches Zertifikat) ist vorzusehen.
- Die Ursprungsdatei muss nach erfolgreicher Verschlüsselung vernichtet werden, bei WORM-Medien der gesamte Datenträger.
- Wenn Datenträger im Rahmen der Neuverschlüsselung ausgesondert werden, sind auch diese sicher zu entsorgen.
- Neben den Haupt-Datenträgern sind auch Backup-Datenträger sicher zu entsorgen bzw. alte Dateien sicher zu löschen.

Die Verteilung der Schlüssel kann auf zwei unterschiedlichen Wegen erfolgen: Falls die Schlüsselerzeugung durch eine unabhängige, vertrauenswürdige Instanz erfolgen soll, ist sicherzustellen, dass die neuen Schlüssel ver-traulich und unverfälscht an den ursprünglichen Eigentümer des Dokuments übertragen werden.

Bei der Nutzung asymmetrischer Verfahren zur Verschlüsselung kann der Dokumenteneigentümer alternativ auf Verlangen selbst ein neues Schlüsselpaar erzeugen und den öffentlichen Schlüssel der archivierenden Instanz mitteilen.

In jedem Fall ist zu berücksichtigen, dass eine derartige Neuverschlüsselung einen gewissen Vorlauf braucht: Die Eigentümer der Daten bzw. der Schlüssel müssen benachrichtigt, die notwendigen Schlüssel generiert und verteilt werden. Bei einer großen Anzahl verschiedener Eigentümer und großen Datenmengen ist ein entsprechender Aufwand einzukalkulieren.

Bei der Auswahl eines möglichst langfristig zuverlässigen neuen Kryptoverfahrens sollte ein aktueller und anerkannter sicherer Algorithmus ausgewählt werden. Ist zum derzeit verwendeten Algorithmus keine wirklich gute Alternative verfügbar, sollte geprüft werden, ob eine Erhöhung der Schlüssellänge als Übergangslösung infrage kommt.

Nach der Neuverschlüsselung und erneuter Archivierung sind die alten Datenbestände zuverlässig zu vernichten. Falls die Ursprungsdaten auf WORM-Medien archiviert wurden, sind die Datenträger, auf denen die Daten in der bisherigen Verschlüsselung gespeichert wurden, sicher zu entsorgen. Auf wiederbeschreibbaren Medien müssen die Daten zuverlässig gelöscht werden (vergleiche dazu M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*). Es ist zu beachten, dass auch die auf Backup-Medien vorgehaltenen Daten neuverschlüsselt und alte Backup-Medien selektiv gelöscht oder vernichtet werden müssen (siehe hierzu M 6.84 *Regelmäßige Datensicherung der System- und Archivdaten*).

Prüffragen:

- Werden bestehende Kryptoverfahren kontinuierlich auf Kompromittierbarkeit untersucht und kryptographische Entwicklungen beobachtet?
- Werden unsichere Kryptoverfahren ausgetauscht und die mit ihnen verschlüsselten Daten mit einem sicheren Kryptoverfahren neu verschlüsselt?
- Werden alte Datenbestände nach der Neuverschlüsselung irreversibel vernichtet?

# M 2.265 Geeigneter Einsatz digitaler Signaturen bei der Archivierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, IT-Sicherheitsbeauftragter, Leiter IT

Digitale Signaturen sind für die elektronische Archivierung eine Herausforderung, da sie technisch bedingt eine begrenzte Lebensdauer haben, die vorher nicht immer bekannt ist. Andererseits sind sie aber auch erforderlich, wenn elektronische Dokumente wirklich beweissicher archiviert werden müssen. Die Aussagekraft digitaler Signaturen hängt sehr stark von deren Interpretation zum Zeitpunkt der Prüfung und damit vom so genannten Gültigkeitsmodell ab. Es bestehen derzeit auch noch keine langfristigen praktischen Erfahrungen mit der Archivierung digital signierter Dokumente, da digitale Signaturen erst seit wenigen Jahren praktisch eingesetzt werden.

### Gültigkeit und Beweiskraft

Diese beiden Eigenschaften einer digitalen Signatur werden üblicherweise wie folgt definiert: Eine digitale Signatur ist genau dann **gültig**,

- wenn sie mathematisch richtig ist und
- wenn zum *Zeitpunkt der Signaturausübung* der zugehörige Signaturschlüssel gültig war.

Eine digitale Signatur ist genau dann **beweiskräftig**,

- wenn sie zum *Zeitpunkt der Prüfung* entsprechend dem verwendeten Gültigkeitsmodell als gültig anerkannt wird und
- wenn der zugehörige Signaturschlüssel nicht kompromittiert ist.

### Aussagekraft digitaler Signaturen

Digitale Signaturen können zu unterschiedlichen Zwecken eingesetzt werden, unter anderem

- zum Nachweis der Integrität von Dateien,
- zur Beglaubigung der Authentizität von kryptographischen Schlüsseln oder elektronischen Dokumenten sowie
- zur Authentisierung.

Der Einsatz und die Aussagekraft digitaler Signaturen sind anwendungsspezifisch im Rahmen einer Sicherheitsrichtlinie (Policy) vorzugeben. In dieser Policy sollte unter anderem festgelegt werden,

- unter welchen Voraussetzungen digitale Signaturen erzeugt werden,
- von welcher Stelle digitale Signaturen erzeugt werden (bei Zertifikats-Signaturen z. B. in einem neutralen Trust Center),
- welches Gültigkeitsmodell für die Anwendung herangezogen wird,
- ob und wie digitale Signaturen gegebenenfalls widerrufen werden können sowie
- welche Aussage damit verbunden sein soll, d. h. was damit beglaubigt wird (bei einem Zeitstempel beispielsweise das Vorliegen eines Dokuments zu einem bestimmten Zeitpunkt).

Die Policy muss schriftlich dokumentiert und archiviert werden, damit bei einer späteren Prüfung der digitalen Signatur klar ist, was die Signatur aussagt (d. h. beweisen soll) und was nicht. Außerdem sollte sie auch in geeigneter Form veröffentlicht werden, damit alle, die auf die Signaturen vertrauen müssen bzw. wollen, sich darauf beziehen können.

**Lebensdauer digitaler Signaturen**

Die Lebensdauer digitaler Signaturen wird durch die technische Entwicklung von Hard- und Software sowie Fortschritte der Kryptographie beschränkt (siehe G 2.79 *Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung* und G 4.47 *Veralten von Kryptoverfahren*). Es muss davon ausgegangen werden, dass digitale Signaturen nach einem Zeitablauf von ca. 5 Jahren als veraltet gelten, da ihre Aussagekraft nachlässt. Schlüsselzertifikate und Zeitstempel sollten von einem Trust Center daher in der Regel für maximal 5 Jahre ausgestellt werden. Sie können aber auch kurzfristig für ungültig erklärt werden, wenn dies notwendig sein sollte. Dies wird als Sperrung bezeichnet.

**Sperrung von Schlüsselzertifikaten**

Wenn Schlüsselzertifikate durch die Zertifizierungsinstanz gesperrt werden, weil z. B. die Signaturschlüssel kompromittiert sind, muss schnell gehandelt werden. Alle ab diesem Zeitpunkt mit dem betreffenden Schlüssel erfolgten Signaturen haben ihre faktische Aussagekraft (z. B. Beweiskraft) verloren. Die Gültigkeit der Signaturen hängt jedoch auch vom Gültigkeitsmodell ab. Im Gegensatz zum Schalenmodell sind beim Kettenmodell im Grunde zunächst keine weiteren Aktionen bei der Kompromittierung von Schlüsseln erforderlich.

Dies kann unmittelbare Folgen für die Aussagekraft archivierter Dokumente haben. Wenn die betroffenen archivierten Dokumente nur mit dem nun ungültigen Schlüssel signiert sind, so ist diese Signatur je nach verwendetem Gültigkeitsmodell nicht mehr beweiskräftig.

**Empfehlung**

Für die Archivierung digital signierter Dokumente gibt es derzeit keine erprobten Standards, durch deren Anwendung eine langfristige Gültigkeit und Beweiskraft der Signaturen sichergestellt werden kann. Bis sich entsprechende Standards etablieren, sollten daher unter Berücksichtigung der bei der Langfristarchivierung auftretenden Gefährdungen folgende Empfehlungen beachtet werden:

- Die Aussagekraft der Signaturen und Zertifikate ist in einer Policy zu dokumentieren. Die Policy muss ebenfalls archiviert werden.
- Es sollte ein unabhängiges Trust Center zur Generierung von Schlüsselzertifikaten und Zeitstempeln eingebunden werden.
- Alle zu einem Dokument gehörenden Signaturen, Zeitstempel, Zertifikate und die für die Signatur- bzw. Zertifikatsprüfung benötigten Schlüssel müssen ebenfalls archiviert werden. Dies kann entweder lokal oder zentral durch das Trust Center erfolgen.
- Je nach Anforderungen an die Aussagekraft der Signaturen müssen u. U. weitere Kontextinformationen archiviert werden. Bei qualifizierten Signaturen gemäß Signaturgesetz gehören hierzu z. B. Verzeichnisdienstauskünfte des Zertifizierungsdiensteanbieters.
- Nach spätestens 5 Jahren, mindestens vor Ablauf der regulären Gültigkeit der Schlüsselzertifikate sollten die digitalen Signaturen und Zertifikate erneuert werden. Solange der Verzeichnisdienst integer verfügbar bleibt, ist dies eigentlich nur dann erforderlich, wenn die Eignung der Algorithmen nicht mehr gegeben ist. Da bei der Archivierung die Daten für einen längeren Zeitraum unbearbeitet vorgehalten werden, ist es sinnvoll, diese trotzdem vorsichtshalber alle 5 Jahre erneut zu signieren.
- Die Überprüfung einer digitalen Signatur schlägt fehl, sobald auch nur ein Bit im Dokument oder dessen Signatur geändert wird. Eine bitgenaue Ar-

chivierung ist deshalb unbedingt erforderlich, um die Gültigkeit der Signatur zu erhalten. Aus diesem Grund sollten entsprechende Fehlerkorrekturmaßnahmen bei der Speicherung der signierten Dokumente getroffen werden.
- Die Verantwortlichen für die elektronische Archivierung sollten sich regelmäßig über die Entwicklungen auf dem Gebiet der digitalen Signaturen informieren.

**Archivierungsmodelle**

Im Folgenden werden verschiedene Modelle für die Archivierung digital signierter Dokumente beschrieben. Dabei bleibt zunächst die Archivierung von Schlüsselverwaltungsinformationen, wie Zertifikaten oder Sperrlisten, unberücksichtigt.

Solange es bei den beschriebenen Modellen unwesentlich ist, ob das Originaldokument nur eine oder mehrere Signaturen enthält, wird von einer Originalsignatur gesprochen. Mehrere Originalsignaturen werden nur dann erwähnt, wenn die Funktionsweise der Archivierung sich dadurch ändert.

Die Beschreibungen der Modelle sind nach folgenden Punkten strukturiert:

- Notwendige Infrastruktur
- Ablauf der Archivierung eines signierten Dokuments
- Ablauf der Abfrage eines Dokuments aus dem Archiv
- Semantik der durch die Archivierung erfolgten zusätzlichen Signaturen, d. h. was wird durch diese Signaturen bestätigt?
- Vorgehensweise bei der Prüfung der Beweiskraft der Originalsignatur
- Notwendiges Vertrauen in die Instanzen, die an der Archivierung beteiligt sind

An die Beschreibung schließt sich eine kurze Diskussion der unterschiedlichen Modelle an.

**Modell 1: Archivierungsstelle mit Eingangsstempelung**

- Infrastruktur
  Vertrauenswürdige Archivierungsstelle, die auch Zertifizierungsdienste anbietet (Trust Center)
- Ablauf der Archivierung
  Das Dokument wird zusammen mit der Angabe des Zeitpunktes seines Eingangs bei der Archivierungsstelle archiviert.
- Ablauf der Abfrage
  Das Dokument zusammen mit der Zeitangabe seines Eingangs in die Archivierungsstelle wird durch die Archivierungsstelle zum Zeitpunkt der Abfrage digital signiert. Durch die Signatur der Archivierungsstelle wird die Authentizität des Dokuments nachgewiesen und dessen Integrität geschützt.
- Semantik der Signatur der Archivierungsstelle
  Durch die Signatur bei der Dokumentenabfrage bestätigt die Archivierungsstelle, dass das betreffende Dokument bei ihr zum angegebenen Zeitpunkt eingegangen und archiviert worden ist.
- Prüfung der Beweiskraft der Originalsignatur
  Um die Authentizität und Integrität des Dokuments zu verifizieren, wird zunächst die Signatur der Archivierungsstelle geprüft. Die Originalsignatur gilt genau dann als beweiskräftig, wenn sie zum angegebenen Zeitpunkt des Dokumenteneingangs bei der Archivierungsstelle beweiskräftig war. Diese Prüfung bleibt dem Benutzer überlassen. Die hierzu erforderlichen Zertifikate können ihm entweder von derselben Archivierungsstelle

zusammen mit dem Dokument bereitgestellt werden oder müssen von ihm bei einer anderen geeigneten Stelle angefordert werden.
- Vertrauensmodell
  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der signierten Dokumente und für die Korrektheit des Zeitpunkts des Dokumenteneingangs entgegengebracht.
  Gelingt es einem Angreifer, den Zeitpunkt des Dokumenteneingangs zu manipulieren, so kann er die Beweiskraft der Dokumente ändern. Durch Angabe eines späteren Zeitpunkts lässt sich die Beweiskraft eines Dokuments ausschalten. Andererseits kann bei einem archivierten Dokument mit gültiger, aber nicht beweiskräftiger Signatur die Beweiskraft durch Angabe eines früheren Eingangszeitpunkts vorgetäuscht werden.
  Die Korrektheit des gespeicherten Zeitpunkts des Dokumenteneingangs ist durch geeignete Schutzmaßnahmen sicherzustellen. Hierzu können digitale Signaturen verwendet werden, wie bei den Modellen 3 und 4.

**Modell 2: Archivierungsstelle mit Bestätigungsstempelung**
- Infrastruktur
  Vertrauenswürdige Archivierungsstelle, die auch Zertifizierungsdienste anbietet (Trust Center)
- Ablauf der Archivierung
  Beim Eingang des Dokuments bei der Archivierungsstelle wird die Beweiskraft der Originalsignatur des Dokuments geprüft. Das Dokument wird nur dann archiviert, falls die Beweiskraft zum aktuellen Zeitpunkt verifiziert werden kann. Bei mehreren Originalsignaturen wird deren Beweiskraft einzeln festgestellt. Das Dokument wird zusammen mit den Angaben über die Beweiskraft der einzelnen Signaturen archiviert, falls mindestens eine der Originalsignaturen beweiskräftig ist.
- Ablauf der Abfrage
  Zum Zeitpunkt der Abfrage wird das Dokument durch die Archivierungsstelle digital signiert, gegebenenfalls zusammen mit den Angaben über die Beweiskraft der Originalsignaturen. Durch die Signatur der Archivierungsstelle wird die Authentizität des Dokuments nachgewiesen und dessen Integrität geschützt.
- Semantik der Signatur der Archivierungsstelle
  Durch die Signatur der Archivierungsstelle wird die Beweiskraft der Originalsignatur bestätigt. Bei mehreren Originalsignaturen werden die mitgelieferten Angaben über deren Beweiskraft einzeln bestätigt.
- Prüfung der Beweiskraft der Originalsignatur
  Um die Authentizität und Integrität der Archivantwort zu verifizieren, wird die Signatur der Archivierungsstelle geprüft. Die Beweiskraft der Originalsignatur ergibt sich aus den mitgelieferten Angaben bzw. aus der Archivierung an sich.
- Vertrauensmodell
  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der signierten Dokumente und für die Prüfung der Beweiskraft der Dokumente vor der Archivierung entgegengebracht.
  Wenn es einem Angreifer unbemerkt gelingt, einen ehemals gültigen Signaturschlüssel zu brechen und Dokumente mit gefälschten Signaturen ins Archiv einzubringen, gelten diese als beweiskräftig. Durch geeignete Maßnahmen ist daher sicherzustellen, dass die Beweiskraft signierter Dokumente vor der Aufnahme ins Archiv geprüft und der Datenbestand vor unberechtigtem Hinzufügen von Daten geschützt wird.

**Modell 3: Trust Center mit Zeitstempeldienst**
- Infrastruktur

Rollentrennung zwischen einer Archivierungsstelle und einem vertrauenswürdigen Zeitstempeldienst (Trust Center), die miteinander kommunizieren.

- Ablauf der Archivierung
  Beim Eingang des Dokuments bei der Archivierungsstelle wird die Beweiskraft der Originalsignatur durch einen Zeitstempel des Trust Centers für die Dauer der Beweiskraft dieses Stempels bestätigt.
  Regelmäßig vor dem Ablauf der Beweiskraft des letzten Zeitstempels wird das Gesamtdokument, d. h. das Dokument inklusive aller Signaturen, mit einem neuen Zeitstempel des Trust Centers versehen.
- Struktur eines archivierten Dokuments
  Ein archiviertes Dokument enthält mindestens das signierte Originaldokument und einen Zeitstempel über dieses Dokument. Im Laufe der Zeit verlängert es sich durch zusätzliche Zeitstempel, die jeweils über das signierte Originaldokument inklusive aller bisherigen Zeitstempel ausgeführt werden.
- Ablauf der Abfrage
  Das Dokument inklusive aller Zeitstempel wird im aktuellen Zustand ausgeliefert.
- Semantik eines Zeitstempels
  Bei einer Zeitstempelung wird durch eine speziell für diesen Zweck vorgesehene Signatur des Trust Centers bestätigt, dass das Dokument zu dem im Zeitstempel angegebenen Zeitpunkt vorlag.
- Prüfung der Beweiskraft der Originalsignatur
  Die Beweiskraft des letzten Zeitstempels wird direkt verifiziert. Jeder andere Zeitstempel wird geprüft, indem seine Beweiskraft zum Zeitpunkt des jeweils nachfolgenden Zeitstempels verifiziert wird (rekursive Verifikation).
  Die Prüfung der Beweiskraft der Originalsignatur erfolgt zu dem Zeitpunkt, der im ersten Zeitstempel angegeben ist.
- Vertrauensmodell
  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der Dokumente entgegengebracht. Beim Trust Center wird dem Zeitstempeldienst vertraut.
  Anhand der Kette von Zeitstempeln ist die Beweiskraft der Originalsignatur lückenlos nachweisbar.

**Modell 4: Trust Center mit Archivstempeldienst**

- Infrastruktur
  Rollentrennung zwischen einer Archivierungsstelle und einem vertrauenswürdigen Archivstempeldienst (Trust Center), die miteinander kommunizieren.
- Funktionsweise einer Archivstempelung
  Wird ein Dokument zum ersten Mal einer Archivstempelung unterzogen, entspricht dieser Vorgang der Zeitstempelung: Das Dokument wird mit einem Zeitstempel versehen.
  Falls ein Dokument bereits genau einmal den Archivstempeldienst durchlief und somit schon einen Zeitstempel enthält, wird bei der erneuten Archivstempelung zunächst dieser Zeitstempel geprüft. Nur falls der Zeitstempel beweiskräftig ist, wird das Dokument inklusive Zeitstempel mit einer speziellen Archivsignatur signiert.
  Enthält ein Dokument bereits eine Archivsignatur, wird bei einer erneuten Archivstempelung zunächst die Archivsignatur geprüft. Nur falls die bisherige Archivsignatur beweiskräftig ist, wird sie durch eine aktuelle Archivsignatur ersetzt.
- Ablauf der Archivierung

Beim Eingang des Dokuments bei der Archivierungsstelle wird die Beweiskraft der Originalsignatur durch die Archivstempelung des Trust Centers für die Dauer der Beweiskraft des hinzugefügten Zeitstempels bestätigt. Regelmäßig vor dem Ablauf der Beweiskraft des Zeitstempels oder der letzten Archivsignatur muss eine Archivstempelung durch das Trust Center erfolgen.

- Struktur eines archivierten Dokuments
  Ein archiviertes Dokument besteht mindestens aus dem signierten Originaldokument und einem Zeitstempel darüber. Nach Ablauf der Beweiskraft des Zeitstempels enthält es zusätzlich genau eine Archivsignatur. Diese Signatur ist über das signierte Originaldokument und den Zeitstempel gebildet.
- Ablauf der Abfrage
  Das Dokument inklusive aller Signaturen wird im aktuellen Zustand ausgeliefert.
- Semantik der Archivsignatur
  Die Archivsignatur bestätigt die Beweiskraft des Zeitstempels. Der Zeitstempel wiederum bestätigt das Vorliegen des Originaldokuments zum angegebenen Zeitpunkt.
- Prüfung der Beweiskraft der Originalsignatur
  Zunächst wird die Beweiskraft der Archivsignatur und anschließend die Beweiskraft der Originalsignatur zum im Zeitstempel angegebenen Zeitpunkt verifiziert.
- Vertrauensmodell
  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der Dokumente entgegengebracht. Beim Trust Center ist ein vertrauenswürdiger Archivstempeldienst notwendig.
  Der Archivstempeldienst muss die Beweiskraft einer vorhergehenden Signatur prüfen. Gelingt es einem Angreifer, diese Prüfung zu unterdrücken und gefälschte, signierte Dokumente mit einer Archivsignatur zu versehen, gelten diese als beweiskräftig. Durch geeignete Maßnahmen muss daher sichergestellt werden, dass die Beweiskraft der bisherigen Signatur vor der Erneuerung oder dem Hinzufügen einer Archivsignatur geprüft wird.

**Diskussion der Modelle**

Je geringer das Vertrauen der Benutzer in die Archivierungsstelle ist, desto höher ist der Aufwand für die beweiskräftige Archivierung digital signierter Dokumente.

Bei vollem Vertrauen in die Archivierungsstelle ist Modell 2 anwendbar. Es ist für einen Benutzer das "bequemste" Modell, da dieser bei der Abfrage des archivierten Dokuments über die Beweiskraft der Originalsignatur informiert wird. Der Benutzer vertraut darauf, dass die Angaben der Archivierungsstelle stimmen. Über diese hinaus hat er keine Kontrollmöglichkeit. Will er einen Dritten von der Beweiskraft der Originalsignatur überzeugen, kann er lediglich auf die Antwort der Archivierungsstelle verweisen und auf deren durch Archivierungsrichtlinien belegte Vertrauenswürdigkeit.

In Modell 1 muss der Benutzer selbst die Beweiskraft der Originalsignatur des abgefragten Dokuments prüfen. Die Archivierungsstelle liefert ihm lediglich den Zeitpunkt, an dem das Dokument bei ihr einging. Ein Dritter kann ebenso wie der Benutzer die Prüfung der Beweiskraft durchführen, muss allerdings der Zeitangabe der Archivierungsstelle vertrauen.

Beide Modelle haben den Vorteil, dass der organisatorische Aufwand der Archivierungsstelle minimal ist: Nach der Archivierung ist keine weitere Behandlung des Dokuments erforderlich. Die Archivierung selbst dient als Versiege-

lung der Originalsignatur für die gesamte Archivierungsdauer. Entsprechend kritisch ist die Integrität des Datenbestandes des Archivs. Unberechtigtes Hinzufügen von Daten kann dazu führen, dass gefälschte Signaturen als beweiskräftig anerkannt werden.

In den Modellen 3 und 4 sind archivierte Daten selbst wiederum durch digitale Signaturen integritätsgeschützt. Dadurch wird verhindert, dass gefälschte signierte Dokumente als beweiskräftig anerkannt werden, wenn sie unberechtigt in das Archiv eingebracht werden.

Eine weitere vertrauensfördernde Maßnahme in den Modellen 3 und 4 ist die Möglichkeit, die Zuständigkeiten für die Dokumentenspeicherung einerseits und die Signaturversiegelung andererseits auf unterschiedliche Stellen zu verteilen: Archivierungsstelle und Trust Center.

Das notwendige Vertrauen in die Archivierungsstelle beschränkt sich dabei, wie es üblicherweise bei der Archivierung der Fall ist, auf die Speicherung von Dokumenten. Darüber hinaus erfordert die erfolgreiche Archivierung digital signierter Dokumente die regelmäßige Kommunikation mit dem Trust Center. Zunächst muss jedes eingehende Dokument durch das Trust Center zeitgestempelt werden, da der Zeitpunkt des Dokumenteneingangs bei der Archivierungsstelle für die nachträgliche Prüfung der Beweiskraft entscheidend ist.

In Modell 4 bestätigt das Trust Center regelmäßig die ordnungsgemäße Archivierung bis zum aktuellen Zeitpunkt, indem es die Beweiskraft der bisherigen Archivsignatur des Dokuments verifiziert und diese Signatur durch eine neue Archivsignatur ersetzt. Der zeitliche Abstand zwischen dem Ende der Beweiskraft des Zeitstempels und dem Zeitpunkt der letzten Archivstempelung vergrößert sich dadurch laufend. Die Archivsignatur bestätigt daher die Beweiskraft des Zeitstempels nur, solange die Archivstempelung im Trust Center ordnungsgemäß verläuft. Insbesondere betrifft dies die Überprüfung der Beweiskraft der bisherigen Archivsignatur. Ohne diese Prüfung kann die Archivierungsstelle gefälschte signierte Dokumente zur Archivstempelung vorlegen, die dann Beweiskraft erhalten. Der Benutzer muss also der ordnungsgemäßen Ausführung der Archivstempelung durch das Trust Center vertrauen.

Bei Modell 3 kann der Benutzer den zeitlich lückenlosen Ablauf der regelmäßigen Signaturversiegelung kontrollieren. Als Dienstleistung des Trust Centers ist lediglich eine Zeitstempelung erforderlich. Diese Zeitstempelung ist nicht spezifisch für die Archivierung und umfasst keine Überprüfungen. Ein vorliegendes Dokument wird ohne vorhergehende Betrachtung, sozusagen "blind" mit der aktuellen Zeit versehen und signiert. Eine vertrauenswürdige Realisierung einer Zeitstempelung ist daher im Allgemeinen einfacher als eine vergleichbar vertrauenswürdige Realisierung einer Archivstempelung.

Die Modelle 3 und 4 bieten zwar im Vergleich zu den Modellen 1 und 2 eine höhere Vertrauenswürdigkeit, hierbei ist es jedoch für die Benutzer komplizierter, die Beweiskraft der Originalsignatur zu überprüfen. Zusätzlich zur Beweiskraft der Originalsignatur zum Zeitpunkt des ersten Zeitstempels ist in Modell 3 eine ganze Kette von Zeitstempeln auf Beweiskraft zu prüfen, in Modell 4 hingegen nur die Beweiskraft der Archivsignatur.

Für die Langzeitarchivierung digitaler Signaturen gibt es noch keine erprobten Standards. Hier müssen sich noch einheitliche Konzepte und Standards durchsetzen, daher sollten sich die Verantwortlichen für die elektronische Archivierung regelmäßig über die Entwicklungen auf diesem Bereich informieren. Die zuvor beschriebenen Modelle sind somit als Beispiele zu verstehen,

zur Archivierung digital signierter Dokumente sind durchaus auch andere Verfahren denkbar.

Prüffragen:

- Wird der Einsatz und die Aussagekraft digitaler Signaturen bei der Archivierung in einer Sicherheitsrichtlinie (Policy) festgehalten und in geeigneter Form veröffentlicht?

# M 2.266 Regelmäßige Erneuerung technischer Archivsystem-Komponenten

**Verantwortlich für Initiierung:** Archivverwalter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, Leiter IT

Archivsysteme müssen über lange Zeiträume auf aktuellem technologischen Stand gehalten werden. In der Informationstechnik haben Standards für Hard- und Software sowie Datenformate zur digitalen Speicherung in der Vergangenheit im Vergleich zu den avisierten Zeiträumen einer Archivierung nur kurzzeitigen Bestand gehabt. Es ist davon auszugehen, dass dies auch künftig so bleibt, da die Standards in hohem Maße vom technischen Fortschritt geprägt werden.

Hardware-Komponenten unterliegen zudem Verschleißerscheinungen und müssen daher regelmäßig gewartet sowie gegebenenfalls ausgetauscht werden. Zusätzlich ist damit zu rechnen, dass Hersteller unvorhergesehen die Unterstützung bestehender Systeme einstellen oder, z. B. aufgrund von Insolvenz, nicht mehr in der Lage sind, langfristige Unterstützung zu gewährleisten.

Es ist daher damit zu rechnen, dass die Komponenten des Archivs regelmäßig erneuert werden müssen und unter Umständen eine Migration des kompletten Datenbestands auf ein neues Archivsystem notwendig ist.

Dieser Prozess ist eng mit der Maßnahme M 2.261 *Regelmäßige Marktbeobachtung von Archivsystemen* verknüpft.

Neue Hard- und Software ist vor der Installation in ein laufendes Archivsystem grundsätzlich ausführlich zu testen, um die Stabilität des bestehenden Systems nicht zu gefährden (siehe auch M 4.65 *Test neuer Hard- und Software*). Bei der Installation neuer Datenträger und Laufwerke muss auf Kompatibilität mit bestehenden Systemen und Datenträgern geachtet werden. Vor der Inbetriebnahme neuer Komponenten oder der Einführung neuer Datenformate ist ein Migrationskonzept zu erstellen, in dem alle Änderungen und Tests beschrieben werden. Das Archivierungskonzept (siehe M 2.243 *Entwicklung des Archivierungskonzepts*) ist unter Umständen anzupassen. Bei größeren Änderungen muss die in der Bausteinbeschreibung beschriebene Planungsphase erneut durchlaufen werden.

Bei der Änderung von Formaten muss geprüft werden, ob bei der Konvertierung von Altdaten in die neuen Formate aufgrund rechtlicher Anforderungen zusätzlich die Daten in ihren ursprünglichen Formaten archiviert werden müssen.

Prüffragen:

- Werden Hardware-Komponenten des Archivsystems regelmäßig gewartet?
- Wird neue Hard- und Software von Archivierungssystemen vor der Installation ausführlich getestet?
- Wird vor der Inbetriebnahme neuer Komponenten des Archivierungssystems oder der Einführung neuer Datenformate ein Migrationskonzept erstellt, in dem alle Änderungen und Tests beschrieben werden?

- Wird bei Änderungen am Archivierungssystem das Archivierungskonzept angepasst?
- Wird bei größeren Änderungen am Archivierungssystem die Planungsphase des Archivsystems erneut durchlaufen?
- Rechtliche Anforderungen bezüglich des Archivierungsformats: Werden bei der Änderung von Formaten die Daten zusätzlich in ihren ursprünglichen Formaten archiviert?

# M 2.267 Planen des IIS-Einsatzes

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.268 Festlegung einer IIS-Sicherheitsrichtlinie

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.269 Planung des Einsatzes eines Apache Webservers

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.270 Planung des SSL-Einsatzes beim Apache Webserver

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.271 Festlegung einer Sicherheitsstrategie für den WWW-Zugang

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.272 Einrichtung eines Internet-Redaktionsteams

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Fachverantwortliche, Leiter IT

Ein Webangebot benötigt regelmäßige Pflege. Vor allem dann, wenn Inhalte oder Dienste angeboten werden, die sich häufiger ändern, wird der Pflegeaufwand relativ schnell anwachsen.

Im Konzept für das Webangebot (siehe M 2.172 *Entwicklung eines Konzeptes für Webangebote* ) werden Verantwortliche für verschiedene Aspekte der Pflege des Webangebots benannt. Überschreitet der Umfang des Angebots und der damit verbundene Pflegeaufwand ein bestimmtes Maß, so kann es sinnvoll sein, zur besseren Koordination eine eigenständige Internet-Redaktion einzurichten. Auf diese Weise werden die Verantwortlichkeiten noch einmal betont und sichtbar in der Organisationsstruktur abgebildet.

Die Einrichtung einer Internet-Redaktion bietet den Vorteil, dass ein zentraler Kontakt für alle Fragen, die das Webangebot betreffen, zur Verfügung steht. Innerhalb einer solchen Redaktion können meist einfacher effiziente Prozesse zur Sicherstellung der Aktualität und Korrektheit der Informationen im Webangebot (beispielsweise bestimmte Freigabeprozesse oder ein Vieraugenprinzip) etabliert werden, als wenn dies über verschiedene Organisationseinheiten hinweg geschehen müsste.

Die Redaktion sollte mindestens diejenigen Personen umfassen, die im Web-Konzept als Verantwortliche genannt wurden. Oft ist es sinnvoll, weitere Personen in die Redaktion einzubinden. Eine Internet-Redaktion sollte folgende Mitglieder umfassen:

- einen Chefredakteur, der die Gesamtverantwortung für die Inhalte und Dienste im Webangebot übernimmt,
- für die verschiedenen inhaltlichen Bereiche jeweils einen Fachredakteur,
- einen Verantwortlichen für das optische Erscheinungsbild (Webdesign) des Webangebots,
- einen "technischen Webmaster", der für die technischen Aspekte des Betriebs des Webservers zuständig ist.

Neben der inhaltlichen Betreuung der Inhalte eines Webservers können zu den Aufgaben der Internet-Redaktion auch die Aufbereitung von Newsbeiträgen, Newslettern, RSS-Feeds oder Beiträge für Video-Plattformen gehören. Falls umfangreichere Webanwendungen genutzt werden, so sollte auch für diese Anwendungen ein Ansprechpartner in der Webserver-Redaktion vertreten sein. Die Fachredakteure, der Webdesigner und der technische Webmaster dienen jeweils als Ansprechpartner (Schnittstelle) zu den jeweiligen Fachbereichen.

Innerhalb der Internet-Redaktion müssen neben den normalen Redaktionsprozessen auch Vorgehensweisen und Zuständigkeiten für den Fall von Problemen festgelegt werden, damit eine schnelle und effiziente Reaktion auf Sicherheitsvorfälle gewährleistet ist (siehe auch M 2.173 *Festlegung einer Webserver-Sicherheitsstrategie*).

Prüffragen:

- Enthält die Redaktion alle Personen, die im Konzept für Webangebote als Verantwortliche genannt werden, den Chefredakteur, Fachredakteure, Webdesign-Verantworlichen und den technischen Webmaster?
- Falls umfangreiche Webanwendungen betrieben werden: Gibt es einen Ansprechpartner in der WWW-Redaktion für Webanwendungen?
- Sind normale Redaktionsprozesse sowie Vorgehensweisen und Zuständigkeiten für den Fall von Problemen und Sicherheitsvorfällen definiert?

# M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Häufig werden Fehler in Produkten bekannt, die dazu führen können, dass die Informationssicherheit des Informationsverbundes, wo diese betrieben werden, beeinträchtigt wird. Entsprechende Fehler können Hardware, Firmware, Betriebssysteme und Anwendungen betreffen. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.

Die Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Schwachstellen informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Für jedes eingesetzte System oder Softwareprodukt muss bekannt sein, wo Sicherheitsupdates und Patches erhältlich sind. Außerdem ist es wichtig, dass Integrität und Authentizität der bereits installierten Produkte oder der einzuspielenden Sicherheitsupdates und Patches überprüft werden (siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*), bevor ein Update oder Patch installiert wird. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden. Dies sollte auch bei solchen Paketen gemacht werden, deren Integrität und Authentizität verifiziert wurde.

Sicherheitsupdates oder Patches dürfen jedoch nicht voreilig eingespielt werden, sondern müssen vor dem Einspielen getestet werden. Falls sich ein Konflikt mit anderen kritischen Komponenten oder Programmen herausstellt, kann ein solches Update sonst zu einem Ausfall des Systems führen. Nötigenfalls muss ein betroffenes System so lange durch andere Maßnahmen geschützt werden, bis die Tests abgeschlossen sind.

Vor der Installation eines Updates oder Patches sollte stets eine Datensicherung des Systems erstellt werden, die es ermöglicht, den Originalzustand wieder herzustellen, falls Probleme auftreten. Dies gilt insbesondere dann, wenn ausführliche Tests aus Zeitgründen oder mangels eines geeigneten Testsystems nicht durchgeführt werden können.

In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*). Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lassen, um beim Bekanntwerden von Schwachstellen schnell Klarheit darüber zu erhalten, ob das System dadurch gefährdet ist.

Falls festgestellt wird, dass ein Sicherheitsupdate oder Patch mit einer anderen wichtigen Komponente oder einem Programm inkompatibel ist oder Probleme verursacht, so muss sorgfältig überlegt werden, wie weiter vorgegan-

gen wird. Wird entschieden, dass auf Grund der aufgetretenen Probleme ein Patch nicht installiert wird, so ist diese Entscheidung auf jeden Fall zu dokumentieren. Außerdem muss in diesem Fall klar beschrieben sein, welche Maßnahmen ersatzweise ergriffen wurden, um ein Ausnutzen der Schwachstelle zu verhindern. Eine solche Entscheidung darf nicht von den Administratoren alleine getroffen werden, sondern sie muss mit den Vorgesetzten und dem IT-Sicherheitsbeauftragten abgestimmt sein.

Prüffragen:

- Sind Regelungen für das Patchmanagement definiert?
- Werden Software-Updates und Patches ausschließlich aus vertrauenswürdigen Quellen bezogen?
- Werden Software-Updates und Patches vor dem Roll-Out getestet?
- Ist sichergestellt, dass bei einem fehlgeschlagenem Update der ursprüngliche Systemzustand wieder hergestellt werden kann?
- Wird die Entscheidung, einen Patch aufgrund aufgetretener Probleme nicht zu installieren, dokumentiert?

# M 2.274 Vertretungsregelungen bei E-Mail-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Für die Bearbeitung von E-Mail ist - ebenso wie bei jeder anderen Aufgabe - für jeden Mitarbeiter ein Vertreter zu benennen. Bei geplanter Abwesenheit sollten die Mitarbeiter dann für den Vertreter eine E-Mail-Weiterleitung einrichten oder den Zugriff auf ihr Postfach freigeben. Bei spontaner Abwesenheit, z. B. wegen Krankheit, können andere Regelungen die zeitnahe E-Mail-Bearbeitung sicherstellen. Beispielsweise kann das Vorzimmer der betroffenen Abteilung die IT-Verantwortlichen informieren, die dann wiederum am E-Mail-Server eine Weiterleitung schalten. Dies ist allerdings nur dann zulässig, wenn klar geregelt ist, dass E-Mail nur dienstlich genutzt werden darf. Die Benutzer sollten außerdem per E-Mail über die Weiterleitung informiert werden. Sobald sie wieder im Haus sind, sollten sie den IT-Verantwortlichen mitteilen, dass die Weiterleitung aufgehoben werden kann.

Alternativ können grundsätzlich auch aufgabenbezogene E-Mail-Adressen eingerichtet werden. Auch hier muss natürlich sichergestellt sein, dass eingehende E-Mail jederzeit zeitnah bearbeitet wird.

Viele E-Mail-Clients bieten die Möglichkeit, vor einer längeren Abwesenheit einen Dienst zu aktivieren (*Autoreply*, unter Outlook *Abwesenheitsassistent*), der dafür sorgt, dass jeder Absender einer E-Mail während der vorgegebenen Abwesenheitszeiten eine Nachricht erhält, dass dieser Empfänger vorübergehend nicht zu erreichen ist. Dies hat oft Vorteile, führt aber häufig dazu, dass zu viele Informationen über den Benutzer und die Organisation breit gestreut nach außen gegeben werden.

Andererseits wird der Absender trotz einer solchen Benachrichtigung über die Abwesenheit meistens im Unklaren darüber gelassen, wie mit seiner E-Mail weiter umgegangen wird. Es stellt sich dann die Frage, ob die E-Mail also bis auf weiteres unbearbeitet bleibt oder an einen Vertreter weitergeleitet wurde.

Daher sollten alle Benutzer darauf achten, dass weder die genaue Zeit der Abwesenheit noch Informationen über Interna weitergegeben werden, wie Telefonnummern oder Organisationseinheiten. Diese lassen sich für Angriffe über Social Engineering weiterbenutzen (siehe G 5.42 *Social Engineering*). Die Mitarbeiter sollten darin eingewiesen werden, wie Abwesenheitsbenachrichtigungen einzurichten sind, z. B. über einen entsprechenden Intranet-Hinweis.

Auf jeden Fall sollten aber Vertreter für alle längeren Abwesenheitsphasen benannt werden. Dies kann auch Externen über solche Mechanismen wie den Abwesenheitsassistent mitgeteilt werden, so dass sie wissen, dass die E-Mail angekommen ist und bearbeitet wird.

**Hinweis:** Die meisten E-Mail-Programme mit Autoreply-Funktion bieten auch die Möglichkeit, die Benachrichtigung nach Kriterien, die die Benutzer selbst festlegen können, zu steuern. Damit kann dann beispielsweise voreingestellt werden, dass interne E-Mail-Absender andere Antworten erhalten als externe. Hierfür werden in der Regel aber tiefere Kenntnisse des E-Mail-Clients benötigt. Wenn daher Regeln zur Steuerung von Autoreply-Funktionen eingesetzt werden sollen, sollten die Administratoren dies entsprechend für die Benutzer vorbereiten.

Prüffragen:

- Gibt es Vertretungsregelungen für die Bearbeitung von E-Mails bei Abwesenheit des Benutzers?
- Gibt es Regelungen für die Verwendung von Autoreply-Funktionen im E-Mail-Programm?

# M 2.275 Einrichtung funktionsbezogener E-Mailadressen

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 2.276 Funktionsweise eines Routers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In großen Netzen kann kaum auf den Einsatz von Routern verzichtet werden. Router werden sowohl in lokalen Netzen als auch in Weitverkehrsnetzen eingesetzt (siehe auch Baustein B 4.4 *VPN*). Ohne den Einsatz von Routern wäre das Internet nicht funktionsfähig.

Router können gleichzeitig unterschiedliche Protokolle (z. B. IP, IPX) und Topologien (z. B. Ethernet, Token Ring, FDDI, ATM, Frame Relay, ISDN) unterstützen. Dadurch sind Router in der Lage, lokale Netze nahtlos mit Weitverkehrsnetzen zu verbinden. Nicht zuletzt diese Funktion von Routern hat mit dazu beigetragen, dass sich das Internet in der Vergangenheit so rasch entwickeln konnte.

Ein Router übernimmt im wesentlichen zwei Aufgaben. Zum einen wird eine geeignete Verbindung zwischen dem Quellsystem beziehungsweise Quellnetz und dem Zielsystem beziehungsweise Zielnetz ermittelt und zum anderen werden Datenpakete entlang dieser Verbindung transportiert. Wenn das Zielsystem (Zielnetz) direkt an dem Router angeschlossen ist - d. h. Router und Zielsystem befinden sich im selben Subnetz - wird das vom Quellsystem gesendete Datenpaket direkt an das Zielsystem gesendet.

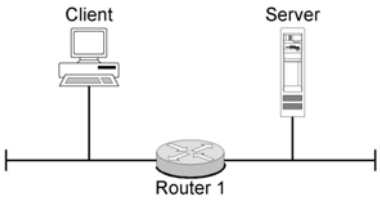



Abbildung: Routing

Wenn das Zielsystem (Zielnetz) nicht direkt am Router angeschlossen ist, sendet der Router das Datenpaket an einen benachbarten Router, der näher am Zielsystem (Zielnetz) angeschlossen ist, den sogenannten Next Hop. Der letzte Router in dieser Verbindungskette ist immer direkt am Zielnetz angeschlossen und sendet das Datenpaket zum Zielsystem.

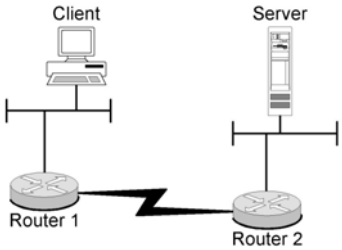



Abbildung: Routing

Die Aufgabe eines Routers ist es, eintreffende Datenpakete entweder direkt an den adressierten Empfänger zu übergeben, oder in das nächste Netz weiterzuleiten. In welches Netz das Datenpaket weitergeleitet wird, wenn es nicht direkt zugestellt werden kann, entscheidet die sogenannte Routing-Metrik. Die Metrik ist ein Maß für die Qualität der Verbindung zwischen dem Sender bzw. dem Router und dem Ziel des Paketes. Mit ihrer Hilfe entscheidet der Router, an welchen Next Hop er das Paket weitergibt. Routing-Metriken beziehen sich nicht ausschließlich auf die Länge des Weges zwischen Sender und Empfän-

ger, sondern können auch andere Merkmale, wie beispielsweise die Qualität der Leitungen, die Bandbreite oder die Auslastung in die Entscheidung mit einbeziehen. Welche Kriterien verwendet werden, ist von dem verwendeten Routing-Protokoll abhängig.

Die Routing-Informationen werden in sogenannten Routing-Tabellen verwaltet. Routing-Tabellen enthalten Informationen darüber, über welche benachbarten Router als Next Hop für bestimmte Zielnetze dienen können. Router treffen die Entscheidung, an welchen Next Hop ein empfangenes Datenpaket weitergegeben wird, ausschließlich auf Basis dieser Routing-Tabellen. Deswegen ist es besonders wichtig, diese Tabellen vor Manipulationen zu schützen. Es sind eine Reihe von Angriffen bekannt, welche die Manipulierbarkeit von Routing-Tabellen ausnutzen. In der folgenden Abbildung ist der Inhalt einer Routing-Tabelle beispielhaft dargestellt.

| **Ziel** | **Next Hop** | **Hop Count** |
|---|---|---|
| 210.23.125.98 | 210.23.122.4 | 3 |
| | 127.200.45.123 | 5 |
| | 203.2.67.187 | 8 |
| ... | ... | ... |

Tabelle: Beispielhafter Ausschnitt aus einer Routing-Tabelle

In diesem Beispiel würde der Router ein Paket mit der Zieladresse 210.23.125.98 an den Next Hop 210.23.122.4 weiterleiten. Der sogenannte Hop Count gibt an, wie viele Zwischenstationen das Paket noch passieren muss, um sein Ziel über den betreffenden Next Hop zu erreichen. Sind für ein bestimmtes Ziel mehrere benachbarte Router als Next Hops verfügbar, so kann der Hop Count als eine Routing-Metrik verwendet werden, um den "günstigsten" Next Hop zu bestimmen. Auch beim Routing Protokoll RIP wird der Hop Count als Routing-Metrik verwendet.

**Statisches und dynamisches Routing**

Es wird in bezug auf das Routing zwischen statischem und dynamischem Routing unterschieden. Diese beiden Methoden unterscheiden sich hinsichtlich der Verwaltung der Routing-Tabellen.

Beim statischen Routing werden diese Tabellen manuell mit Hilfe von Systembefehlen gepflegt.

Beim dynamischen Routing erfolgt die Pflege der Routing-Tabellen automatisiert. Dies geschieht mit Hilfe von Routing-Protokollen. Hier wird noch einmal zwischen den Interior Gateway Protokollen (IGP) und den Exterior Gateway Protokollen (EGP) unterschieden. IGP wird innerhalb von Netzen verwendet, die unter eigener Administrationsverantwortung stehen. Die Zusammenfassung der unter eigener Verantwortung betriebenen Netze wird auch als Routing-Domäne bezeichnet. Mit Hilfe von EGP werden Routing-Informationen zwischen unterschiedlichen Routing-Domänen ausgetauscht.

Die folgende Abbildung stellt diesen Zusammenhang dar.

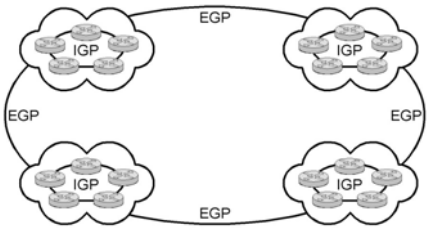



Abbildung: Austausch von Routing-Informationen

Die bekanntesten und standardisierten Routing-Protokolle sind das Routing Information Protocol (RIP), Open Shortest Path First (OSPF) und das Border Gateway Protocol (BGP), wobei es sich beim Border Gateway Protocol um ein Exterior Gateway Protokoll handelt. Erweitert werden diese Protokolle durch proprietäre Routing-Protokolle von unterschiedlichen Herstellern. Die bekanntesten Protokolle sind das Interior Gateway Routing Protocol (IGRP) und das Enhanced Interior Gateway Routing Protocol (EIGRP) des Herstellers Cisco.

Da Routing-Protokolle die Verwaltung von Routing-Tabellen automatisieren, haben Angreifer längst erkannt, Sicherheitslücken dieser Protokolle auszunutzen, um die Routing-Tabellen zu modifizieren und so Datenpakete umzuleiten oder ganze Netze außer Betrieb zu setzen (siehe G 5.51 *Missbrauch der Routing-Protokolle*).

Bei der Implementierung eines dynamischen Routings zwischen Netzen ist in erster Linie auf die Sicherheitsfunktionen der verwendeten Routing-Protokolle zu achten (siehe M 5.112 *Sicherheitsaspekte von Routing-Protokollen*). Der Administrator muss besonderen Wert auf die sichere Authentisierung der benachbarten Router beim Austausch von Routing-Tabellen legen. Es sollten nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung beim Austausch von Routing-Tabellen unterstützen.

Der Aufwand der manuellen Pflege von Routing-Tabellen ist zu groß, um in komplexen Netzen auf dynamisches Routing verzichten zu können. Der Einsatz von dynamischem Routing ist vor der Inbetriebnahme unter dem Gesichtspunkt der Sicherheit zu bewerten.

Allgemein sollte in Netzen mit hohem Schutzbedarf nach Möglichkeit kein dynamisches Routing verwendet werden. Kann auf dynamisches Routing aus wichtigen Gründen nicht verzichtet werden, so sollten zumindest nur solche Routing-Protokolle verwendet werden, die eine sichere Authentisierung der beteiligten Geräte und eine gesicherte Übertragung der Routing-Informationen bieten.

In M 2.278 *Typische Einsatzszenarien von Routern und Switches* ist ein weiteres Szenario beschrieben, in dem vom Einsatz von Routing-Protokollen abgeraten wird.

**Router als Paketfilter**

Viele Router können auch für die Filterung von Datenpaketen verwendet werden, d. h. der Router wird als Paketfilter eingesetzt (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Broadcast-Pakete werden von einem Router normalerweise nicht zwischen verschiedenen angeschlossenen Netzen transportiert. Hierdurch teilt der Router die angeschlossenen Netze in unterschiedliche Broadcast-Domänen auf.

Router verfügen allerdings meist noch über weitergehende Filterfunktionen. Beispielsweise können sogenannte Access Control Lists (ACL) konfiguriert werden. Der Router regelt anhand dieser Listen den Datenverkehr zwischen den beteiligten Netzen. Weitergehende Sicherheitsaspekte bei Access Control Lists sind in M 5.111 *Einrichtung von Access Control Lists auf Routern* zu finden.

Der Einsatz von Paketfiltern ist als alleinige Methode zur Kontrolle des Datenverkehrs zwischen Netzen mit einem unterschiedlichen Schutzbedarf meist nicht ausreichend. Mehr Informationen finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)* beispielsweise in M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways* und M 2.74 *Geeignete Auswahl eines Paketfilters*.

**Router als VPN-Gateway**

Einige am Markt verfügbare Router unterstützen die Funktion Virtual Private Network (VPN). Diese Router werden insbesondere dann eingesetzt, wenn sensitive Daten über ein Netz übertragen werden. Der Einsatz von Routern mit VPN-Funktionalität hat den Vorteil, dass anwendungsseitig keine Verschlüsselungsmechanismen vorhanden sein müssen. Die Verschlüsselung ist transparent für die Kommunikationspartner. Allerdings findet die Kommunikation auf der Strecke bis zum ersten verschlüsselnden Netzkoppelelement unverschlüsselt statt und birgt damit ein Restrisiko. Authentisierung ist hier nur zwischen den Koppelelementen möglich. Die eigentlichen Kommunikationspartner werden nicht authentisiert (M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

Prüffragen:

- Werden beim dynamischen Routing nur Routing-Protokolle verwendet, die eine verschlüsselte Authentisierung beim Austausch von Routing-Tabellen unterstützen?
- Ist der Einsatz von dynamischem Routing vor der Inbetriebnahme unter dem Gesichtspunkt der Sicherheit bewertet worden?
- Wird in Netzen mit hohem Schutzbedarf nach Möglichkeit kein dynamisches Routing verwendet?
- Ist das Restrisiko der unverschlüsselten Übertragung bis zum ersten Netzkoppelelement beim Einsatz von VPN analysiert und bewertet?

# M 2.277 Funktionsweise eines Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

**Einführung**

Ursprünglich arbeiteten Switches auf der OSI-Schicht 2, mittlerweile sind Switches mit unterschiedlichen Funktionen erhältlich. Hersteller kennzeichnen Switches meist mit dem OSI-Layer, der unterstützt wird. Dadurch entstanden die Begriffe Layer-2-, Layer-3- und Layer-4-Switch, wobei es sich bei Layer-3- und Layer-4-Switches eigentlich funktional bereits um Router handelt. Die ursprünglich unterschiedlichen Funktionen von Switches und Routern werden auf einem Gerät vereint. Dadurch wird die Abgrenzung der Gerätetypen (Switch oder Router) erschwert. Die wesentlichen Unterschiede dieser Geräte sind in der Einleitung zum Baustein B 3.302 *Router und Switches* aufgeführt.

Die ersten Switches entstanden aus den Bridges, die wie die modernen Switches heutzutage zur Auftrennung großer LAN-Segmente in mehrere kleine Segmente (Kollisionsdomänen) dienten. Bridges arbeiten in der Regel mit der Store-and-Forward-Technologie. Dabei wird jeder empfangene Ethernet-Frame eingelesen und dann anhand der Zieladresse entschieden, ob er an ein anderes LAN-Segment weitergegeben wird. Handelt es sich um lokalen Datenverkehr, erfolgt keine Weitergabe und der Frame gelangt nur zu den Stationen im lokalen Netz. Damit wird der lokale Verkehr auf einzelne Segmente begrenzt, was bei geeigneter Auslegung die Netzlast deutlich reduzieren kann. Bei kleineren Segmenten sinkt zudem der Anteil an Kollisionen und die Performance verbessert sich. Ist ein Frame an ein anderes Segment weiterzuleiten, wird er im Zwischenspeicher der Bridge abgelegt und anschließend an den Zielport übergeben. Zusätzlich kann beim Store-And-Forward die Integrität eines empfangenen Frames mit Hilfe von CRC-Prüfsummen überprüft werden. Korrupte Frames werden verworfen, was zu einer weiteren Verringerung der Netzlast beitragen kann.

Switches verfügen neben dem Store-and-Forward-Switching auch über den Mechanismus des Cut-Through-Forward-Switching, bei dem nur die Zieladresse - die ersten sechs Bytes eines Frames - gelesen wird. Hierdurch reduziert sich die Verzögerung zwischen dem Empfänger- und Sendeport erheblich. Allerdings ist es dabei nicht möglich, korrupte Frames auszufiltern. Durch das unnötige Weiterleiten fehlerhafter Frames kann eventuell ein Engpass entstehen. Abhilfe schafft ein adaptives Verhalten des Switches, bei dem der Frame während des Weiterreichens geprüft wird. Damit werden zwar korrupte Frames nicht ausgefiltert, aber der Switch kann die Qualität der Frames überwachen. Übersteigt der Prozentsatz der korrupten Frames einen vorher festgelegten Wert, so schaltet der Switch für diesen Port auf Store-and-Forward um, um in Zukunft zu filtern.

In der folgenden Abbildung ist beispielhaft eine sogenannte Switching-Tabelle dargestellt. In dieser Tabelle wird gespeichert, an welchem Port die Station mit der entsprechenden MAC-Adresse angeschlossen ist. Der Switch lernt diese Zuordnung dynamisch. Im Gegensatz zu einem Hub sendet der Switch einen Ethernet-Frame immer nur an den Port, an dem der Zielrechner angeschlossen ist.

Dadurch wird die Bandbreite, die einem Gerät zur Verfügung steht, nicht von der Kommunikation zwischen anderen angeschlossenen Stationen beein-

flusst. Ein weiterer Effekt ist, dass die Kommunikation zwischen zwei Stationen von keiner der anderen Stationen mitgelesen werden kann. Davon ausgenommen sind Broadcasts und Multicasts, die an alle angeschlossenen Stationen gesandt werden. Ebenso werden Frames, deren Ziel-MAC-Adresse noch unbekannt ist, an alle Ports weitergeleitet.

| **Ziel MAC Adresse** | **Ziel Switch Port** |
|---|---|
| 0001.02c4.fdca | Fast Ethernet0/4 |
| 0001.026d.d412 | Fast Ethernet0/8 |
| 0008.a345.12f3 | Fast Ethernet0/12 |
| 0060.97ac.de59 | Fast Ethernet0/16 |
| ... | ... |

Tabelle: Switching-Tabelle

Ein Frame, der an die Station mit der MAC-Adresse 0001.02c4.fdca gerichtet ist, wird vom Switch nur an den Port 01 weitergeleitet.

Da die Switching-Tabelle zur Steuerung des Datenflusses verwendet wird, muss sie vor Manipulationen geschützt werden. Es sind einige Angriffsmethoden bekannt, die die Integrität und Verfügbarkeit dieser Tabellen bedrohen (siehe G 5.112 *Manipulation von ARP-Tabellen*).

Layer-3- und Layer-4-Switches arbeiten analog auf einer entsprechend höheren OSI-Schicht.

Sind in einem lokalen Netz mit einer komplizierten Topographie mehrere Switches vorhanden, so kann es vorkommen, dass für die Verbindung zwischen zwei Geräten mehrere mögliche Wege existieren. Switching funktioniert aber nur dann, wenn zu jedem Zeitpunkt klar ist, an welchen Port ein Paket weitergeleitet werden muss. Andernfalls besteht die Gefahr, dass im Netz Schleifen (*Loops*) entstehen, auf denen Pakete immer im Kreis geschickt werden und niemals ihr eigentliches Ziel erreichen. Deswegen bieten Switches die Möglichkeit, automatisch untereinander eine logische Netzstruktur (einen sogenannten *Spanning Tree* des Netzes) "auszuhandeln", die eine reibungslose Funktion erlaubt. Zu diesem Zweck wird das sogenannte Spanning Tree Protocol (STP, IEEE 802.1d) verwendet. Überflüssige Verbindungen im Netz werden automatisch deaktiviert und nur dann wieder aktiviert, wenn die per STP ermittelte primäre Verbindung nicht verfügbar ist.

Hierzu muss jedem Switch eine Prioritätsinformation und eine eindeutige MAC-Adresse zugewiesen sein, es muss eine Multicast-Adresse für alle Switches existieren und jeder Port über eine ID eindeutig identifizierbar sein.

Um den Broadcast-Verkehr in einem "geswitchten" Netz einzuschränken, lassen sich virtuelle Netze (VLANs) bilden. Hierbei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, in dem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden. Die Gründe für den Zusammenschluss zu einem VLAN können organisatorischer oder technischer Art sein.

Unter dem Aspekt der Unternehmensorganisation ist es beispielsweise möglich, alle Mitarbeiter einer Abteilung in eine Netzgruppe zusammenzufassen, auch wenn sie auf verschiedenen Etagen verteilt sind. Unter dem Aspekt der Arbeitsorganisation können Mitarbeiter, die gemeinsam an einem Projekt ar-

beiten, zu einer Netzgruppe zusammengefasst werden, auch wenn sie zu verschiedenen Abteilungen gehören.

Jedes VLAN bildet eine separate Broadcast-Domäne. Ein VLAN braucht nicht auf einen einzelnen Switch beschränkt zu sein, sondern es kann sich über ein ganzes geswitchtes Netz erstrecken. Die Netzbenutzer bilden dann nicht mehr aufgrund ihres Standortes ein Netzsegment, sondern sie können innerhalb des Intranets standortunabhängig mit anderen Nutzern zu einer Gruppe zusammengefasst werden.

Es wird zwischen port- und hostbasierten VLANs unterschieden. Bei portbasierten VLANs werden einzelne Anschlüsse (Ports) an einem Switch direkt einem VLAN zugeordnet. Das bedeutet, dass der zugeordnete Anschluss unabhängig von der angeschlossenen Station fest einem bestimmtem VLAN zugeordnet ist. Bei hostbasierten VLANs wird die Zugehörigkeit eines VLANs beispielsweise über die MAC-Adresse oder IP-Adresse der angeschlossenen Station gesteuert. Bei hostbasierten VLANs hat der Anwender die Möglichkeit, sein Endgerät an jedem beliebigen Ort innerhalb des Netzes anzuschließen, ohne dass er die Zugehörigkeit zu seinem VLAN verliert.

Die Möglichkeit, VLANs über mehrere Switches auszudehnen, wird als Trunking bezeichnet. Hierbei wird pro Switch ein physischer Port für die Inter-Switch-Kommunikation reserviert, die logische Verbindung zwischen den Switches wird als Trunk bezeichnet. Trunking wird durch unterschiedliche, teils proprietäre Trunking-Protokolle realisiert. Der Ethernet-Rahmen wird beim Informationsaustausch zwischen den Switches in das Trunking-Protokoll gekapselt. Dadurch ist der Ziel-Switch in der Lage, die Information dem entsprechenden VLAN zuzuordnen. Als Standards werden IEEE 802.1q und beispielsweise die proprietären Protokolle ISL (Inter Switch Link) und VTP (VLAN Trunking Protokoll) des Herstellers Cisco verwendet.

Manchmal wird auch die Bündelung (Zusammenfassung) mehrerer physikalischer Verbindungen zwischen Switches zur Erzielung entsprechend höherer Durchsatzraten als Trunking bezeichnet. Diese Funktionalität wird andererseits auch als "Channel Bonding" oder "Channeling" bezeichnet. Wenn in einem Dokument der Begriff Trunking auftaucht, so muss deswegen stets darauf geachtet werden, in welcher Bedeutung der Begriff gerade verwendet wird. Hier wird unter Trunking stets die Möglichkeit verstanden, VLANs über mehrere Switches zu verteilen.

Die folgende Abbildung zeigt eine Konfiguration mit zwei Switches, die über einen Trunk-Port verbunden sind. Der Rechner, der am linken Switch ebenfalls an einem Trunk-Port angeschlossen ist, stellt ein potentielles Sicherheitsrisiko dar, da er Zugriff auf die Daten aus allen VLANs hat, die auf dem Switch konfiguriert sind.

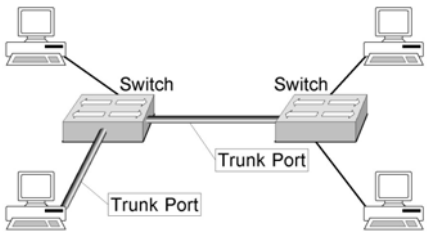



Abbildung: Trunking

Erstreckt sich ein VLAN über mehrere Switches, so steigt in der Praxis der Datenverkehr zwischen diesen Komponenten um den Anteil der mit Hilfe des

Trunking- Protokolls übertragenen Informationen. Die Kommunikation zwischen Teilnehmern unterschiedlicher VLANs erfolgt über OSI-Schicht 3, das heißt die Pakete werden VLAN übergreifend geroutet. Das Routing kann auf einem Switch durchgeführt werden, der Routing-Funktionen unterstützt (siehe auch den Abschnitt zu Layer-3-Switches in der Einleitung zum Baustein B 3.302 *Router und Switches*), oder auf einem angeschlossenen Router erfolgen, der die VLANs auf der OSI-Schicht 3 verbindet.

Die folgenden Abbildungen zeigen Beispiele für ein (port-basiertes) VLAN, das sich über drei verschiedene Etagen eines Gebäudes erstreckt und für eine Konfiguration mit zwei verschiedenen VLANs auf einem Switch.

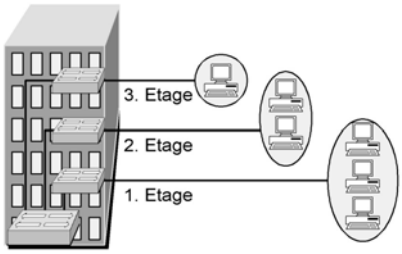



Abbildung: Beispiel für ein VLAN

Entgegen den Aussagen einiger Hersteller muss berücksichtigt werden, dass VLANs nicht entwickelt wurden, um Sicherheitsanforderungen bei der Trennung von Netzen zu erfüllen. VLANs bieten eine Vielzahl von Angriffspunkten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind. In der folgenden Beispiel-Abbildung kann nicht von einer sicheren Trennung zwischen dem VLAN 1 und VLAN 2 ausgegangen werden, da die beiden VLANs auf dem selben Switch realisiert sind.

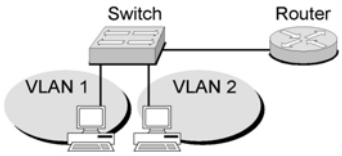



Abbildung: Zwei VLANs auf einem Switch

Auf einem Switch sollten keine VLANs mit unterschiedlichem Schutzbedarf konfiguriert sein. Soll dies aus wichtigen Gründen trotzdem geschehen, so müssen in jedem Fall zusätzliche Sicherungsmaßnahmen ergriffen werden, um ein angemessenes Sicherheitsniveau zu gewährleisten. Keinesfalls darf das Netz einer DMZ, die zwischen dem internen Netz und dem Internet steht, als VLAN auf dem selben Switch wie das interne Netz konfiguriert sein.

In der folgenden Abbildung wurde eine sichere Trennung von zwei VLANs mit unterschiedlichem Schutzbedarf realisiert, indem pro Switch lediglich ein VLAN konfiguriert wurde. Die Kopplung der Netze wird von einem Router übernommen, der als Paketfilter fungiert.

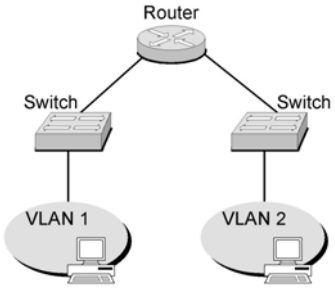



Abbildung: Sichere Trennung von VLANs

Prüffragen:

- Werden zusätzliche Sicherheitsmaßnahmen ergriffen, wenn interne VLAN mit unterschiedlichem Schutzbedarf auf einem Switch konfiguriert sind?
- Ist sichergestellt, dass das VLAN einer DMZ nicht auf dem selben Switch wie das interne Netz konfiguriert ist?

# M 2.278 Typische Einsatzszenarien von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Der Einsatzzweck von Routern bestimmt maßgeblich die Konfiguration der Systeme. Zudem bestimmt die Verwendung auch die zusätzlichen Funktionen, die von einem Router bereit gestellt werden müssen.

### Router im internen Netz

Router sind in vielen Installationen als reine LAN-to-LAN-Router im Einsatz, um Subnetze zu verbinden und die Nebeneffekte von rein "geswitchten" Netzen, beispielsweise sogenannte Broadcast-Stürme, zu verhindern. In dieser Funktion werden heute allerdings vermehrt Switches mit integrierter Routing-Funktion (Layer-3- oder Layer-4-Switches, siehe auch M 2.277 *Funktionsweise eines Switches*) eingesetzt. Bei diesem Einsatzszenario hängen die Sicherheitsanforderungen an den Router stark vom Schutzbedarf der Teilnetze ab, die über den Router verbunden sind.

### Router zur Anbindung an externe Netze

Wird ein Router zur Anbindung des eigenen Netzes einer Organisation an externe Netze eingesetzt, so spricht man von einem Border-Router. Oft sind Border-Router auch in ein Sicherheits-Gateway integriert und übernehmen in diesem die Funktion des externen Paketfilters (siehe unten). Bei Routern, die an fremde Netze angeschlossen sind, spielt die Sicherheit des Gerätes eine besonders wichtige Rolle, da sie Angriffen von außen direkt ausgesetzt sind.

### Router als Paketfilter

Router werden oft als Bestandteil von Sicherheits-Gateways zum Anschluss an öffentliche Netze (beispielsweise das Internet) verwendet. Im folgenden Beispiel besteht das Sicherheits-Gateway aus einem internen Paketfilter, einem externen Paketfilter und einem Applikations-Gateway. Statt Applikations-Gateways werden oft auch Stateful-Inspection-Systeme als zentrale Teile von Sicherheits-Gateways eingesetzt. Die festgelegten Filterregeln werden sowohl auf dem zentralen System als auch auf den Routern (intern und extern) konfiguriert. Auf den Routern wird das Regelwerk durch die Einrichtung von Access Control Lists (ACLs) etabliert.

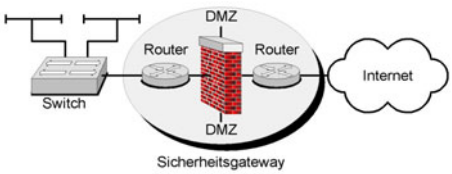



Abbildung 1: Router als Paketfilter

Die Funktion der Paketfilterung ist bei den meisten Routern bereits im Betriebssystem integriert. Es gibt auch Router, die bereits eine integrierte Stateful-Inspection-Firewall bereitstellen.

Es ist empfehlenswert, das Management der beteiligten Systeme (speziell die Einrichtung von Filterregeln) mit Hilfe einer einheitlichen Benutzeroberfläche durchzuführen. Dies hilft Konfigurationsfehler zu vermeiden, die beispielswei-

se Sicherheitslöcher im Sicherheits-Gateway öffnen oder zu Störungen des Netzbetriebs führen können.

Anforderungen an einen Router für diesen Einsatzzweck sind in M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways* zu finden.

Weiterhin sind bei der Konfiguration Vorgaben aus M 4.203 *Konfigurations-Checkliste für Router und Switches* als Mindestvoraussetzung zu berücksichtigen. Der äußere Paketfilter im aufgeführten Beispiel ist direkt an ein öffentliches Netz angeschlossen und damit einem erhöhten Risiko ausgesetzt. Deshalb muss dieser Router besonders restriktiv konfiguriert sein.

**Anbindung von Außenstellen**

Router können zur Anbindung von Außenstellen genutzt werden. In der nachfolgenden Abbildung dienen die dargestellten Router zur Kopplung von lokalen Netzen (LAN), die einen einheitlichen Schutzbedarf haben und unter einer einheitlichen Administrationsverantwortung stehen. In diesen Fällen werden zumeist keine oder nur schwache Filterregeln auf den Routern konfiguriert. In kleinen Netzen können statische Routen verwendet werden, während in mittleren oder großen Umgebungen Interior Gateway Protokolle als Routing-Protokolle eingesetzt werden. Die beteiligten Router sind somit Bestandteil einer abgeschlossenen Routing-Domäne. Als Verbindungstechnologien können ATM, Frame Relay, ISDN, DSL oder Standardfestverbindungen genutzt werden.

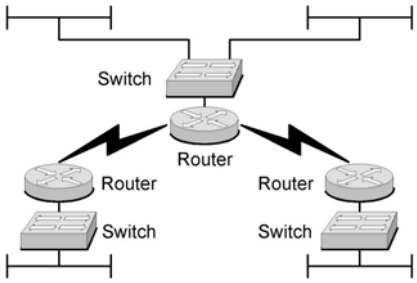



Abbildung 2: Anbindung von Außenstellen

**Remote Access**

In kleinen und mittleren Netzen werden Router oftmals auch zur Einwahl in lokale Netze (LAN) verwendet. Einwahlmöglichkeiten sollten jedoch nicht direkt in ein LAN integriert werden, sondern es sollte zumindest ein Einwahl-Router eingesetzt werden, der entsprechende Sicherheitsfunktionalität bietet, um das LAN vor Angriffen über die Einwahlzugänge zu schützen.

Ein möglicher Weg zur Absicherung einer Einwahl mit Hilfe eines Routers ist in der folgenden Abbildung dargestellt. Der Router wird in der DMZ eines Sicherheits-Gateways betrieben. Zusätzliche Sicherheit wird durch die Authentisierung mit Hilfe eines RADIUS-Servers erreicht. Der Router fungiert in diesem Fall als RADIUS-Client. Remote-User authentisieren sich nicht direkt am Router, sondern am RADIUS-Server. Dadurch können Benutzer zentral am RADIUS-Server verwaltet werden.

Durch die Verwendung eines One-Time-Passwort-Verfahrens (OTP) in Kombination mit einem Hardware-Token oder einer Smart-Card, wird eine starke Authentisierung erreicht. RADIUS-Server unterstützen in der Regel die Erweiterung von OTP-basierenden Verfahren durch die Installation von Plug-Ins oder durch die Kommunikation mit einem OTP-Server. Eine weitere Möglichkeit zur Erreichung einer starken Authentisierung ist die Einbindung der Remote-Access-Lösung in eine bestehende Public Key Infrastructure (PKI).

Der RADIUS-Server muss in diesem Fall für den Zugriff auf einen Verzeichnisdienst konfiguriert sein. Dadurch lässt sich in Kombination mit einer Smart-Card eine zertifikatsbasierende starke Verschlüsselung erreichen. Weiterführende Maßnahmen sind im Baustein B 4.4 *VPN* und B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* beschrieben.

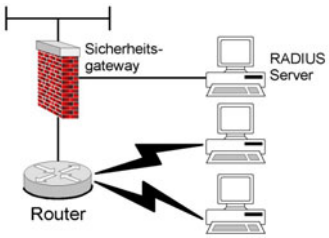



Abbildung 3: Remote Access

**VPN**

Eine weitere Möglichkeit Standorte sicher miteinander zu verbinden, ist die Nutzung von virtuellen privaten Netzen (VPN). Ein VPN ist ein gesicherter Tunnel, der über bestehende Netzinfrastrukturen geführt wird. Somit ermöglicht der Einsatz von VPNs eine sichere Übertragung von vertraulichen Informationen über unsichere Netze (z.B. das Internet). Der Datenverkehr zwischen zwei Endpunkten innerhalb eines VPN wird verschlüsselt. VPN-fähige Router sollten eine starke Verschlüsselung (z.B. 3DES, AES) unterstützen. Viele am Markt verfügbare Router unterstützen die VPN-Funktionalität.

IPSec ist ein Standard, der über eine Reihen von RFCs und Internet-Drafts der IEEE definiert wird. Auf der Basis von IPSec lassen sich VPNs zwischen Geräten unterschiedlicher Hersteller konfigurieren. IPSec stellt die Datenvertraulichkeit, Datenintegrität und die Authentisierung zwischen den Endpunkten des VPN sicher. IPSec basiert auf der Netzschicht des OSI-Referenzmodells. Es nutzt das Internet Key Exchange (IKE) zur Ausführung der Protokoll-Algorithmusvereinbarung entsprechend der lokalen Konfiguration und zur Erzeugung der Verschlüsselungs- und Authentisierungsschlüssel. Eine weitere VPN-Technologie, die auf einem Standard beruht, ist das sogenannte "SSL-VPN", bei dem der Datenverkehr über eine mit SSL/TLS gesicherte Verbindung geleitet wird.

Neben VPNs auf der Basis von IPSec und SSL existieren verschiedene andere, sowohl proprietäre, als auch Open Source Technologien. Dabei muss beachtet werden, dass diese meist untereinander nicht kompatibel und teilweise nur für bestimmte Plattformen verfügbar sind.

Falls die beteiligten Komponenten die Einbindung in eine bestehende PKI ermöglichen, kann dadurch die Verwaltung von VPNs (speziell das Schlüsselmanagement) wesentlich erleichtert und die Skalierbarkeit verbessert werden.

Es wird zwischen einem Site-to-Site-VPN und einem Client-to-Site-VPN unterschieden. Ein Site-to-Site-VPN dient zur Verbindung von Netzen. Dabei wird das VPN auf beiden Seiten durch entsprechend konfigurierte, VPN-fähige Router begrenzt. Diese Art von VPNs ist eine Alternative zur Verbindung von lokalen Netzen über Weitverkehrsstrecken.

Bei einem Client-to-Site-VPN wird ein VPN zwischen einem Client und einem VPN-fähigen Router aufgebaut. Dazu muss auf dem Client meist eine herstellerspezifische VPN-Client-Software installiert werden. Ein Client-to-Site-VPN

ist als eine weitere Alternative des Remote-Zugangs zu lokalen Netzen anzusehen.

In der folgenden Abbildung ist beispielhaft eine VPN-Architektur dargestellt.

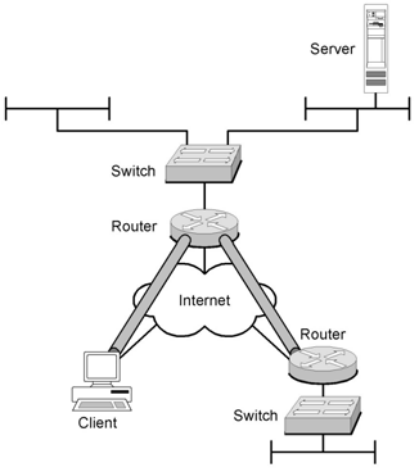



Abbildung 4: Beispiel für eine VPN-Architektur

**Switches**

Der Einsatzzweck eines Switches zur Bildung von VLANs ist in der Maßnahme M 2.277 *Funktionsweise eines Switches* beschrieben. Die folgende Abbildung zeigt ein typisches geswitchtes Netz.

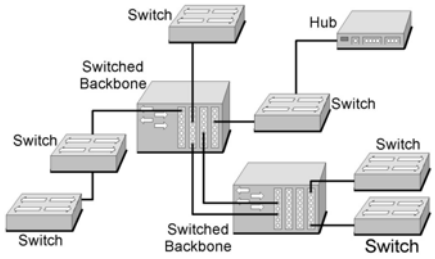



Abbildung 5: Geswitchtes Netz mit Backbone- und Access-Switches

In der Abbildung sind zwei Arten von Switches zu unterscheiden. Die Access-Switches, die sich durch eine hohe Anzahl von Anschlüssen (Ports) auszeichnen, stellen den unmittelbaren Anschluss der Endgeräte sicher. Die Access-Switches sind wiederum an zentrale Backbone-Switches angeschlossen.

Die Backbone-Switches bilden das so genannte Switched-Backbone. Ein Switched-Backbone bündelt die Bandbreite der angeschlossenen Switches, um eine hohe Durchsatzrate zwischen den Endgeräten sicherzustellen. Ein Switched-Backbone zeichnet sich also durch eine hohe Durchsatzrate aus. Der Durchsatz eines Switched-Backbones hängt von einigen Faktoren ab, die bei der Anschaffung von Geräten zu berücksichtigen sind. Die wichtigsten Faktoren sind der maximale Adresscache zur Vorhaltung der dynamisch erlernten MAC-Adressen, der Durchsatz der Backplane eines Backbone-Switches sowie die Leitungsgeschwindigkeit des Switched-Backbone.

Die beteiligten Switches müssen in einer Architektur ähnlich der Abbildung dynamisch erlernte Switching-Tabellen austauschen, um die Verbindung zwi-

schen Endgeräten, die an unterschiedlichen Switches angeschlossen sind, effizient herstellen zu können. Dies geschieht mit zumeist herstellerabhängigen (proprietären) Protokollen (z. B. Cisco Discovery Protocol CDP).

In großen geswitchten Netzen werden Switches typischerweise kaskadiert. Dies wird in der Praxis mit Hilfe des sogenannten Uplink-Ports erreicht.

Prüffragen:

- Ist der Einsatzzweck der vorhandenen Router und Switches dokumentiert?

# M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Da Router und Switches zentrale Elemente eines Netzes sind, ist der sichere und ordnungsgemäße Betrieb besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen (das zu erreichende Sicherheitsniveau) ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für Router und Switches formuliert werden, um die übergeordnet und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie bspw. IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb von Routern und Switches beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb von Routern und Switches treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Allgemeine Konfigurationsstrategie ("Liberal" oder "Restriktiv")
- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge werden müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vieraugenprinzip?
  - Nach welchem Schema werden Administrationsrechte vergeben?
- Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils
- Vorgaben für die Installation und Konfiguration
  - Vorgehen bei der Erstinstallation
  - Überprüfung der Default-Einstellungen hinsichtlich Sicherheitsgefährdungen
  - Regelungen zur physikalischen Zugriffskontrolle
  - Verwendung und Konfiguration von Konsole und sonstigen Zugriffsarten
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisie-

rung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Regelungen zur Einrichtung und Nutzung von VLANs und VPNs (beispielsweise: keine VLANs mit unterschiedlichem Schutzbedarf auf einem Switch)
  - Regelungen zu Erstellung und Pflege von Dokumentation, Form der Dokumentation: Verfahrensanweisungen, Betriebshandbücher
  - Falls allgemeine Vorgaben existieren: Zugelassene und nicht zugelassene Dienste, Protokolle und Netze
- Vorgaben für den sicheren Betrieb
  - Absicherung der Administration (beispielsweise: Zugriff nur über abgesicherte Verbindungen)
  - Einsatz von Verschlüsselung (Standards, Schlüsselstärken, Einsatzbereiche)
  - Vorgaben zu Passwortnutzung (Passwortregeln, durch Passwörter zu schützende Bereiche, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement
  - Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen
- Protokollierung
  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
- Datensicherung und Recovery (siehe auch M 6.91 *Datensicherung und Recovery bei Routern und Switches*)
  - Einbindung in das organisationsweite Datensicherungskonzept
- Störungs- und Fehlerbehandlung, Incident Handling
  - Regelungen für die Reaktion auf Betriebsstörungen und technische Fehler (lokaler Support, Fernwartung)
  - Regelungen für Sicherheitsvorfälle
  - Notfallvorsorge (siehe auch M 6.92 *Notfallvorsorge bei Routern und Switches*)
  - Einbindung in das organisationsweite Notfallvorsorgekonzept
- Revision und Audit (Verantwortlichkeiten, Vorgehen, Integration in ein übergreifendes Revisionskonzept)

Die Verantwortung für die Sicherheitsrichtlinie liegt beim Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Prüffragen:

- Berücksichtigt die Sicherheitsrichtlinie für Router und Switches die Vorgaben übergeordneter Sicherheitsrichtlinien?

- Werden die Inhalte und Umsetzungen der Sicherheitsrichtlinie für Router und Switches im Rahmen einer Revision regelmäßig geprüft?

# M 2.280 Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Aktive Netzkomponenten unterscheiden sich in ihrem Leistungsumfang, den angebotenen Sicherheitsmechanismen, Bedienkomfort und Wirtschaftlichkeit. Werden bei der Beschaffung Fehler gemacht, so kann dies schwerwiegende Folgen auf den sicheren Betrieb eines Netzes haben, da mit ungeeigneten Geräten das angestrebte Sicherheitsniveau unter Umständen nur schwer erreichbar ist.

Bevor Router und Switches beschafft werden, muss daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt.

Aus dem Blickwinkel der Informationssicherheit sind zentrale Anforderungen an aktive Netzkomponenten, dass diese die Administration über sichere Protokolle erlauben und dass die Benutzerverwaltung des Geräts es erlaubt, das organisationsweite Rollenkonzept entsprechend umzusetzen. Die Anforderung, dass Passwörter nur verschlüsselt im Gerät gespeichert werden dürfen, sollte eigentlich eine Selbstverständlichkeit sein, jedoch gibt es immer noch Geräte, bei denen Passwörter im Klartext in Konfigurationsdateien gespeichert werden müssen. Bei Neubeschaffungen sollten keine Geräte mehr berücksichtigt werden, die keine sichere Administrationsmöglichkeit bieten und bei denen es nicht möglich ist, Passwörter verschlüsselt abzuspeichern.

Auch rein funktionale Merkmale aktiver Netzkomponenten können Auswirkungen auf die Informationssicherheit haben. Meist ist dann der Grundwert Verfügbarkeit betroffen, beispielsweise wenn ein Gerät wegen unzureichender Speicherausstattung nicht die erforderlichen Durchsatzraten erreicht. Außerdem spielt die Unterstützung durch den Hersteller eine nicht zu vernachlässigende Rolle, wenn es beispielsweise darum geht, dass zeitnah Patches für Sicherheitslücken zur Verfügung gestellt werden.

Nachfolgend werden einige grundsätzliche Anforderungen bei der Beschaffung von Routern und Switches aufgelistet. Anschließend werden noch einige spezielle Anforderungen getrennt für Router und Switches beschrieben.

**Allgemeine Kriterien für Router und Switches**

- Grundlegende funktionale Anforderungen
  - Unterstützt das Gerät alle benötigten Protokolle und Verkabelungstypen?
- Sicherheit
  - Unterstützt das System sichere Protokolle zur Administration?
    Wenn Router und Switches nicht über ein eigenes Administrationsnetz administriert werden, müssen diese Geräte mit Hilfe von sicheren Netzprotokollen (beispielsweise SSH2) konfigurierbar sein.
  - Unterstützt das System die verschlüsselte Speicherung von Passwörtern?

Geräte, bei denen Passwörter unverschlüsselt gespeichert werden, sollten nicht mehr beschafft werden.

- Wartbarkeit
  - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches an?
    Es ist insbesondere wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.
  - Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?
    Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich.
  - Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
    Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Ansprüche an die Verfügbarkeit der Geräte abgedeckt werden können.
  - Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
    Dieser Punkt sollte Bestandteil des abgeschlossenen Wartungsvertrags sein. Beim Abschluss des Vertrags ist auf die Sprache der zur Verfügung gestellten Hotline des Herstellers zu achten.
- Zuverlässigkeit/Ausfallsicherheit
  - Wie zuverlässig und ausfallsicher ist das Produkt?
    Der Hersteller sollte Erfahrungswerte bezüglich der Zuverlässigkeit liefern können, beispielsweise Mean Time Between Failures (MTBF), Mean Time To Repair (MTTR).
  - Bietet der Hersteller Hochverfügbarkeitslösungen an?
    Wenn durch den Abschluss von Wartungsverträgen die Verfügbarkeitsanforderungen nicht abgedeckt werden können, muss das System Hochverfügbarkeitslösungen unterstützen.
- Benutzerfreundlichkeit
  - Lässt sich das Produkt einfach installieren, konfigurieren, und administrieren?
    Es sollten darüber hinaus Schulungen für das Produkt angeboten werden.
- Kosten
  - Wie hoch sind die Anschaffungskosten der Geräte?
  - Wie hoch sind die voraussichtlichen laufenden Kosten (Wartung, Betrieb, Support)?
    Diese Kosten sollten bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden (Reaktionszeiten, Hotline, Qualifikation des Personals, etc.).
  - Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal?
  - Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. RADIUS-Server, Netz-Management-System)?
    Diese Frage sollte bereits in der Planungsphase beantwortet werden. Wenn beispielsweise bereits ein Netz-Management-System im Einsatz ist, sollte die Kompatibilität mit den zu beschaffenden Geräten geprüft werden. Zudem sollte der Aufwand zur Integration der Geräte in eine bestehende Infrastruktur beachtet werden.

  - Wie hoch sind die Kosten für die Schulung von Administratoren?
- Funktionalität
  - Kann das System sicher in die bestehende Netz-Management-Architektur eingefügt werden?
    Der Aufwand zur Integration sollte berücksichtigt werden. Der Hersteller sollte MIB-Tables und Angaben zu den unterstützten NMS-Protokollen liefern.
  - Unterstützt das System NTP?
    NTP ist besonders im Hinblick auf die Protokollierung von Bedeutung, siehe auch M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*.
  - Unterstützt das System die Einbindung von Authentisierungsservern (beispielsweise RADIUS oder TACACS+)?
    Ist bereits ein Authentisierungsserver im Einsatz, so sollte das System diesen nutzen können.
- Protokollierung
  - Welche Möglichkeiten der Protokollierung sind vorhanden?
    Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:
    - Ist der Detailgrad der Protokollierung konfigurierbar?
    - Werden durch die Protokollierung alle relevanten Daten erfasst?
    - Unterstützt das System zentrale Protokollierung (z. B. syslog)?

    Router und Switches sollten eine zentrale Protokollierung unterstützen, um eine gezielte Auswertung der Log-Dateien sicherstellen zu können.
  - Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?
  - Werden Alarmierungsfunktionen unterstützt?
    Angriffe auf Router und Switches sollten durch Alarmierungsfunktionen der Geräte zentral und zeitnah gemeldet werden. Dies kann beispielsweise auf Basis eines Netz-Management-Systems geschehen.
- Infrastruktur
  - Abmessungen und Kompatibilität mit Schutzschränken
    Auch der Platzbedarf von Routern und Switches ist bei der Beschaffung zu berücksichtigen. Kann das Gerät in die vorgesehenen Schutzschränke eingebaut werden (Formfaktor, Gewicht, Befestigungselemente)?
  - Stromversorgung und Abwärme
    Vom Hersteller sollten Angaben zum Stromverbrauch und zu den Anforderungen an die Umgebungstemperatur verfügbar sein. Reicht die vorhandene Kapazität der Stromversorgung und der USV aus? Reicht die vorhandene Kühlleistung zur Abfuhr der Abwärme des Geräts aus?

**Besondere Kriterien für Switches**
- Performance und Skalierbarkeit
  - Kann das System den Ansprüchen an die Performance gerecht werden?
    Vom Hersteller sollten Angaben zum Datendurchsatz verfügbar sein, insbesondere sollte der Maximal-Durchsatz der Switch-Backplane

beachtet werden. Weitere Größen, die Einfluss auf die Performance haben können, sind die Größe des Adress-Cache und des Speichers.
  - Wie groß ist die Anzahl der bereitgestellten Ports?
    Ein Access-Switch sollte über eine ausreichende Anzahl von Ports zum Anschluss von Endgeräten verfügen. Oft lassen sich die Anschaffungskosten von unterschiedlichen Switches anhand der Kosten pro Port vergleichen.
  - Ist das System "stackable" oder (beispielsweise durch zusätzliche Einschubkarten) modular erweiterbar?
    Zusätzlich erforderliche Funktionen oder der Bedarf an einer höheren Portdichte sollten nicht dazu führen, dass Geräte vorzeitig ausgetauscht werden müssen.
- Funktionalität
  - Unterstützt der Switch Layer-3-Switching (Routing)?
    In lokalen Netzen kann diese Funktion im Hinblick auf die Performance (Datendurchsatz) vorteilhaft sein.
  - Unterstützt der Switch VLANs?
    Bei der Nutzung von VLANs sollte der Hersteller Angaben zum verwendeten Standard machen.
  - Unterstützt der Switch Cut Through oder/und Store and Forward?

**Besondere Kriterien für Router**
- Performance und Skalierbarkeit
  - Kann das System den Ansprüchen an die Performance gerecht werden?
    Vom Hersteller sollten Angaben zum Datendurchsatz verfügbar sein. Falls der Router als VPN-Endpunkt eingesetzt werden soll, sind auch die unterstützten Verschlüsselungsverfahren und die Performance beim Ver- und Entschlüsseln der Daten wichtige Performance-Kriterien.
  - Ist das Gerät modular erweiterbar?
    Die Anzahl der im Standardumfang bereitgestellten Interfaces, insbesondere die maximale Anzahl von unterstützten Interfaces sollte berücksichtigt werden.
- Funktionalität
  - Unterstützt der Router VPN-Funktionalität?
    Ein Router mit VPN-Funktionalität sollte den IPSec-Standard und starke Verschlüsselungsalgorithmen (3DES, AES) unterstützen.
  - Unterstützt der Router die Nutzung von ACLs?
    Die Filterfunktionen der zu beschaffenden Router sind zu berücksichtigen (siehe auch M 5.111 *Einrichtung von Access Control Lists auf Routern*,).
  - Welche Routing-Protokolle werden unterstützt?
  - Der Router sollte sichere Routing-Protokolle unterstützen (siehe auch M 5.112 *Sicherheitsaspekte von Routing-Protokollen*).

Prüffragen:

- Ist eine Anforderungsliste zur Bewertung der am Markt erhältlichen Produkte, vor der Beschaffung von Routern und Switches, erstellt worden?
- Sind bei der Neubeschaffung keine Geräte mehr berücksichtigt worden, die keine sichere Administrationsmöglichkeit bieten und bei denen es nicht möglich ist, Passwörter verschlüsselt abzuspeichern?

- Sind die Anforderungen für neue Switches und Router schriftlich dokumentiert?

# M 2.281 Dokumentation der Systemkonfiguration von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Die Konfiguration von Routern und Switches wird meist mittels Konfigurationsdateien vorgenommen, die auf dem Gerät gespeichert sind. Router und Switches besitzen eine Reihe von Konfigurationsoptionen, die für den sicheren Betrieb wichtig sind. Bei der Erstinstallation beziehungsweise im Auslieferungszustand sind diese Einstellungen mit Default-Werten belegt.

Die Konfiguration, die bei der Inbetriebnahme des Geräts vorgenommen wird, muss so dokumentiert werden, dass sie jederzeit vom Administrator oder seinem Vertreter nachvollzogen werden kann. Insbesondere dann, wenn eine Konfiguration von einem Default-Wert abweicht, sollte in einem Kommentar in der Konfigurationsdatei festgehalten werden, warum die Einstellung so gewählt wurde.

Jede Änderung der Konfiguration sollte vom Administrator nachvollzogen werden können. Es wird empfohlen, mindestens folgende Punkte zu dokumentieren:

- Welche Änderung wurde durchgeführt?
- Warum wurde die Änderung durchgeführt (Anlass)?
- Wann wurde diese Änderung durchgeführt (Uhrzeit, Datum)?
- Wer hat die Änderung durchgeführt?

Die Dokumentation der Änderungen kann ebenfalls durch Kommentare in der Konfigurationsdatei erfolgen. Dabei ist es jedoch in der Regel sinnvoll, zu jeder Option nur die jeweils letzte Änderung in der Datei selbst zu speichern.

Zusätzlich dazu sollten zumindest alle sicherheitsrelevanten Konfigurationsänderungen in einem Protokoll gespeichert werden, anhand dessen sich jederzeit nachvollziehen lässt, wie das Gerät zu einem bestimmten Zeitpunkt konfiguriert war. Dieses Protokoll sollte nicht auf dem Gerät selbst gespeichert werden.

Zur Erleichterung der Dokumentation und Protokollierung kann ein Revisions- und Versionskontrollsystem wie beispielsweise CVS eingesetzt werden. Ein solches System bietet den zusätzlichen Vorteil, dass notfalls eine frühere Konfiguration einfach wieder hergestellt werden kann. Netzmanagement-Systeme zur zentralen Administration bieten in der Regel ebenfalls eine integrierte Dokumentations- und Protokollfunktion.

Es ist empfehlenswert, die Dokumentation so zu gestalten, dass sie auch von einem Fachmann, der mit den konkreten Gegebenheiten der Systemlandschaft nicht vertraut ist, nachvollzogen werden kann.

Die Konfigurationsdateien sollten zur Notfallvorsorge zusätzlich zentral auf einem dafür vorgesehenen Server gespeichert werden. Für die zentrale Verwaltung von Konfigurationsdateien werden oft TFTP-Server verwendet. TFTP-Server sollten jedoch nur in einem abgesicherten Administrationsnetz betrieben werden, weil der Dienst TFTP eine Reihe von Schwachstellen beinhaltet (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*).

Eine Alternative dazu ist die Übertragung per SCP (siehe auch M 5.64 *Secure Shell*).

Prüffragen:

- Werden Konfigurationsänderungen an Routern und Switches nachvollziehbar dokumentiert?
- Werden alle sicherheitsrelevanten Konfigurationen in einem gesonderten Protokoll gespeichert, welches sich nicht auf dem betroffenen Gerät befindet?
- Werden die Konfigurationsdateien zur Notfallvorsorge zusätzlich zentral auf einem dafür vorgesehenen Server gespeichert?

# M 2.282 Regelmäßige Kontrolle von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zur Sicherstellung des ordnungsgemäßen Betriebs der aktiven Netzkomponenten und der Korrektheit aller Konfigurationsparameter ist ein regelmäßiger, möglichst automatisierter, Kontrollprozess zu etablieren. Hierzu gehören beispielsweiseregelmäßige Funktionstests, Veranlassen von Änderungen und Prüfung der Umsetzung sowie die Überprüfung der Logfiles und Alarme.

Um die im laufenden Betrieb entstehende große Menge an relevanten Daten effektiv verarbeiten zu können, ist meist der Einsatz geeigneter Werkzeuge für eine möglichst weit automatisierte Kontrolle erforderlich. Dies kann beispielsweise durch die Einbindung in ein Netzmanagementsystem (NMS) geschehen.

**Checkliste für die Kontrolle**

Für die Kontrolle kann die Checkliste in M 4.203 *Konfigurations-Checkliste für Router und Switches* verwendet werden. Als Basis sollte die erstellte Sicherheitsrichtlinie für Router und Switches dienen (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*). Zusätzlich sollten folgende Punkte im Rahmen des Kontrollprozesses berücksichtigt werden:

**Was** wird getestet bzw. kontrolliert?

- Die generelle Funktionsfähigkeit von Geräten wird im Normalfall regelmäßig durch den Administrator im laufenden Betrieb geprüft.
- Die Integrität von Konfigurationsdateien sollte in regelmäßigen Abständen geprüft werden. Die Sicherheitsrichtlinie für Router und Switches sollte eine regelmäßige Überprüfung mit Festlegung von Verantwortlichkeiten vorschreiben.
- Der Stand der Datensicherung (zentral gespeicherte Konfigurationsdateien) sollte regelmäßig vom Administrator geprüft werden.
- Die Systemdokumentation sollte laufend vom Administrator aktualisiert werden. Die Aktualität kann im Rahmen von Audits geprüft werden.

Hierzu sind auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.64 *Kontrolle der Protokolldateien* zu berücksichtigen.

**Wie** wird getestet?

- Durch die Einbindung der Komponenten in ein Netzmanagement-System kann eine regelmäßige Kontrolle sichergestellt werden. Sicherheitsverletzungen, Ausfälle und Fehlfunktionen können mit Hilfe von Alarmierungsfunktionen des NMS zeitnah erkannt werden.
- Im Rahmen von Audits erfolgt meist eine stichprobenartige Kontrolle von Komponenten. Als Basis für ein Audit dient die erstellte Sicherheitsrichtlinie für Router und Switches. Wichtiger Bestandteil einer solchen Untersuchung ist die Aktualität der Systemdokumentation, Stand der Datensicherung, Passwortwechsel, etc. Unter Zuhilfenahme der Checkliste aus M 4.203 *Konfigurations-Checkliste für Router und Switches* kann ein Großteil der sicherheitsrelevanten Einstellungen abgefragt werden.
- Es existiert eine Reihe frei verfügbarer Sicherheits-Tools (z. B. Nessus), welche die Sicherheitseinstellungen auf Routern und Switches prüfen können. Solche Tools können auf einem Rechner im Netz installiert sein. Es

sollte nach Möglichkeit die aktuellste Version verwendet werden. Als Betriebssystem ist oft Unix bzw. Linux notwendig. Von diesem System aus kann der Administrator entsprechende Router und Switches scannen, um somit eine Vielzahl von Einstellungen dieser Geräte zu prüfen. Kommerzielle Tools bieten teilweise recht komfortable Auswertungen und Möglichkeiten zur Historienverfolgung der durchgeführten Scans.
- Eine Vielzahl von Sicherheitsunternehmen bieten regelmäßige Überprüfungen von Routern und Switches an. Durch turnusmäßige Berichte und Auswertungen erhält der Betreiber einen Überblick über den Zustand der Komponenten.

**Wann** wird getestet?

- Der Administrator prüft laufend und meist automatisiert die Funktion der Geräte mit Hilfe eines NMS-Systems. Die Systemdokumentation ist vom Administrator laufend aktuell zu halten.
- Der Stand der Datensicherung, die Integrität der Konfigurationsdateien und weitere Daten zur Konfiguration sollten vom Administrator regelmäßig (wöchentlich) geprüft werden.
- Scans mit der Hilfe von Sicherheits-Tools sollten nach Installation regelmäßig (monatlich) durch den Administrator vorgenommen werden. Die Ergebnisse sind zu prüfen und zu archivieren.
- Die Prüfung der Einhaltung von Sicherheitsrichtlinien muss regelmäßig erfolgen (z. B. jährlich im Rahmen von Sicherheits- oder Grundschutzaudits).

**Wer** testet?

- Der Administrator sollte laufend Prüfungen durchführen (Funktion der Komponenten, Stand der Datensicherung, Integrität der Konfigurationsdateien, Scans, etc.).
- Die Einhaltung von Sicherheitsrichtlinien bzw. von Sicherheitsmaßnahmen im Rahmen von Sicherheits- bzw. Grundschutzaudits darf nicht durch den Administrator geprüft werden, sondern hat abhängig vom etablierten Sicherheitsmanagementprozess durch einen Auditor, IT-Sicherheitsbeauftragten oder Revisor zu erfolgen.

**Welche Informationen** bilden die Grundlage der Kontrolle?

- Sicherheitsrichtlinie für Router und Switches
- Protokolldateien von Routern und Switches
- Systemdokumentation (siehe M 2.281 *Dokumentation der Systemkonfiguration von Routern und Switches*)
- Sicherheitskonzept
- IT-Grundschutz-Kataloge
- Ergebnisse von durchgeführten Scans

**Überprüfung der Konfiguration**

Bei der Einrichtung der Router und Switches sind alle Default-Einstellungen zu prüfen und falls notwendig zu modifizieren. Hierbei werden beispielsweise nicht benötigte Dienste deaktiviert und Voreinstellungen den betrieblichen und sicherheitstechnischen Anforderungen angepasst. Eine Erläuterung der hierfür notwendigen Schritte findet sich in M 4.201 *Sichere lokale Grundkonfiguration von Routern und Switches* und M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches*.

Die Umsetzung der Vorgaben zum Umgang mit Default-Einstellungen sind im Rahmen von regelmäßigen Audits zu überprüfen. Hierdurch können versehentliche oder vorsätzliche Veränderungen festgestellt und die Umsetzung von aktuellen Empfehlungen der Hersteller verifiziert werden. Dies kann ausgehend von der für jeden Gerätetyp beziehungsweise für jede Betriebssystem-

version zu erstellenden Installationsanleitung erfolgen und sollte am jeweiligen Gerät verifiziert werden. Hierbei ist jedoch zu beachten, dass Betriebssystem-Kommandos bei manchen Herstellern nicht alle Default-Einstellungen anzeigen. Aus diesem Grund empfiehlt es sich, separate Software-Tools einzusetzen, um eine vollständige Analyse durchzuführen.

Für einen umfassenden Test aller Geräte können Softwareprodukte eingesetzt werden, die einen automatisierten Test mit konfigurierbaren Parametern ermöglichen.

**Mirror Port**

Zur Analyse des Datenverkehrs gibt es die Möglichkeit, einen Port des Routers oder des Switches als "Mirror Port" zu konfigurieren. Dabei wird der gesamte Datenverkehr eines beliebigen Ports auf den Mirror Port repliziert und kann mit entsprechenden Analyseprogrammen ausgewertet werden. Im Gegensatz zu anderen Analysemethoden wird der Datenverkehr dabei nicht unterbrochen oder beeinträchtigt.

Der Mechanismus bietet zwei Analysemethoden: Spiegelung des gesamten Datenverkehrs für einen definierten Port oder Spiegelung des Datenverkehrs für eine MAC-Adresse. Im zweiten Fall wird das gesamte Datenvolumen, welches mit einer definierten Quell- und/oder Ziel-MAC-Adresse über das Gerät läuft, auf den Mirror Port gespiegelt.

Der Mirror Port darf keinem produktiven VLAN und keiner Spanning Tree Group (STG) angehören. Standardmäßig muss "Port Mirroring" ausgeschaltet sein. Der Zugriff auf die Konfiguration des "Port Mirroring" ist zu schützen. Nach der Verwendung des Mirror Ports ist dieser wieder zu deaktivieren. Es ist regelmäßig zu prüfen, ob die Funktion Port Mirroring im Regelbetrieb deaktiviert ist.

Prüffragen:

- Wurde ein Kontrollprozess für die Sicherstellung des ordnungsgemäßen Betriebs der aktiven Netzkomponenten etabliert?
- Erfolgen Sicherheits- bzw. Grundschutzaudits durch einen Auditor, IT-Sicherheitsbeauftragten oder Revisor und nicht durch die zuständigen Administratoren?

# M 2.283 Software-Pflege auf Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Jeglicher Betrieb von Software macht es notwendig, Betriebssystem und Konfiguration regelmäßig zu überprüfen und zu pflegen. Router und Switches können hiervon nicht ausgenommen werden, um beispielsweise funktionale Erweiterungen zu ermöglichen, Softwarefehler zu beheben und Performance und Sicherheit zu verbessern.

Dabei ist zu beachten, dass in der Praxis zur Pflege des Betriebssystems bei Router und Switches oftmals ein kompletter Austausch der Betriebssystemsoftware erforderlich ist. Das Einspielen von Updates oder Patches ist in vielen Fällen nicht möglich. Wie bei allen Konfigurationsänderungen ist mit angemessener Sorgfalt vorzugehen, da eine unsachgemäße Durchführung Beeinträchtigungen der Funktion und der Sicherheit der Geräte zur Folge haben kann. Insofern gehört zur sorgfältigen Planung einer Änderung immer auch eine Fallback-Strategie.

**Einspielen neuer Software**

Bei der Vorbereitung von Updates sind folgende Punkte zu beachten:

- Es muss ein geeignetes Zeitfenster vorgesehen werden. Der benötigte Aufwand sollte nicht unterschätzt werden und vorsichtshalber eine ausreichende Down-Time eingeplant werden.
- Die vom Hersteller beigefügten Hinweistexte (Release Notes) des neuen Release sind sorgfältig zu lesen.
- Bei neuen Softwareversionen sind eventuell einzelne Features nicht mehr enthalten oder funktionieren nicht korrekt. Manchmal ändern sich auch Defaulteinstellungen.
- Neue Versionen eines Programmes und insbesondere eines Betriebssystems müssen vor der Inbetriebnahme sorgfältig getestet werden, um die volle Funktionalität sicher zu stellen.
- Neue Programme oder Betriebssysteme sind unter Umständen weniger performant, beispielsweise wegen zusätzlicher Features oder höherem Speicherbedarf. Dies kann zu Problemen führen, wenn ein Router oder Switch bereits vor dem Upgrade an der Auslastungsgrenze betrieben wurde.

Viele Hersteller bieten zur Planung der Erweiterung Konfigurationswerkzeuge an. Diese ermöglichen es, ausgehend vom benutzen Gerät eine Konfiguration zu planen und die benötigten Hardwarebestandteile wie Interfaces und Speicher auszuwählen.

Bei der Durchführung von Updates sollten folgende Schritte durchgeführt werden:

- Beschaffung des Updates aus vertrauenswürdiger Quelle. Normalerweise sollten Updates nur vom Hersteller bezogen werden. Falls der Hersteller für die Updates Prüfsummen zur Verfügung stellt oder die Update-Pakete digital signiert, so sollten die Prüfsummen oder Signaturen überprüft werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* und M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).
- Überprüfung der Integrität und Funktion des Updates

- Trennung des Gerätes vom produktiven Netz oder Deaktivierung aller Schnittstellen
- Nach Möglichkeit Sicherung der bestehenden Konfiguration und des Betriebssystems
- Einspielen des Updates
- Test
- Re-Aktivierung des Gerätes im Netz

**Änderung der Konfiguration**

Konfigurationsänderungen können sowohl direkt am Gerät an der System-Konsole (online) als auch auf einem eigenen Management-Rechner mit einem entsprechenden Konfigurationsprogramm oder einem Texteditor (offline) vorgenommen werden. Beide Vorgehen haben Vor- und Nachteile, generell ist jedoch die Offline-Konfiguration zu bevorzugen.

Die Online-Konfiguration kann in der Regel nur wenig komfortabel und ohne Zuhilfenahme von Tools erfolgen, beispielsweise ist das Einfügen von Kommentaren nicht immer möglich. Dafür wird die Syntax zeitnah überprüft.

Wenn die Erstellung von Konfigurationsdateien offline durchgeführt wird, stehen in der Regel komfortablere Werkzeuge zur Verfügung und es können Kommentare eingefügt werden. Nachteil bei dieser Vorgehensweise ist, dass oftmals Passworte im Klartext in die Konfigurationsdateien eingetragen werden müssen. Da die Passworte in der Konfigurationsdatei - und damit auch der bei Übertragung über das Netz auf das Gerät, sofern keine verschlüsselte Verbindung verwendet wird - lesbar sind, sollten diese sofort nach dem Einspielen der Konfigurationsdatei geändert werden. Eine andere Möglichkeit besteht darin, Passworte online zu setzen und die Konfiguration anschließend inklusive der verschlüsselten Passworte auszulesen.

Um sicher zu stellen, dass bei einem Boot-Vorgang aus dem Speicher die aktuelle Konfiguration eingelesen wird, muss die geänderte Konfiguration gespeichert werden, nachdem sie in das Gerät geladen wurde.

Bei manchen Geräten können Konfigurationsdateien für eine zentrale Administration auch auf separaten Servern gehalten und von dort geladen werden. Dies kann sowohl manuell als auch automatisiert - beispielsweise beim Bootvorgang - geschehen. Änderungen können somit automatisiert an die Geräte verteilt werden. Das Laden beim Bootvorgang ist jedoch wegen der Möglichkeit zur mutwilligen Störung, seiner Fehleranfälligkeit und der entstehenden Netzlast nicht empfehlenswert und wird nur selten genutzt. Die Sicherung und Verwaltung der Konfigurationsdateien hingegen sollte über einen derartigen zentralen Server erfolgen.

In jedem Fall muss der Administrationsrechner, auf dem die Offline-Konfiguration vorgenommen wird beziehungsweise auf dem die Konfigurationsdaten gehalten werden, vor unbefugtem Zugriff besonders geschützt werden.

Prüffragen:

- Sind für das Einspielen von Updates auf den Routern und Switches Wartungsfenster festgelegt?
- Werden die Updates für Router und Switches vor dem produktiven Einsatz getestet?
- Erfolgt die Beschaffung der Updates ausschließlich aus vertrauenswürdigen Quellen?
- Werden, sofern vom Hersteller angeboten, die Update-Prüfsummen verglichen bzw. die digitalen Signaturen überprüft?

- Ist sichergestellt, dass während der Aktualisierung die betroffenen Router und Switches vom produktiven Netz getrennt sind?

# M 2.284 Sichere Außerbetriebnahme von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auf aktiven Netzkomponenten gespeicherte Konfigurations- oder Log-Dateien enthalten eine Vielzahl von Informationen über das Netz, die Infrastruktur, die Organisation und eventuell auch über Personen im Unternehmen. Wenn ein Gerät an Externe weitergegeben wird (etwa an den Hersteller oder den Service bei einem Garantieaustausch oder an einen etwaigen Käufer), dann können diese Informationen ausgewertet werden.

Beispielsweise können folgende Informationen aus Konfigurationsdateien gewonnen werden:

- Verwendete Protokolle (insbesondere Routing-Protokolle), IP-Adressen und Subnetze
- VLAN-Konfiguration
- Access Control Lists
- Passwörter und SNMP Community Strings
- Name und Kontaktdaten des Administrators (Banner)

Wegen der Sensibilität dieser Informationen ist darauf zu achten, dass die Dateien vor der Außerbetriebnahme oder dem Austausch defekter oder veralteter Geräte gelöscht beziehungsweise unlesbar gemacht werden. Die Vorgehensweise hängt dabei stark vom Hersteller des Gerätes ab. In der Sicherheitsrichtlinie für Router und Switches sollten hierfür entsprechende Verantwortlichkeiten definiert werden.

Viele Geräte unterstützen die Funktion des "Factory-Resets". Durch einen Befehl oder durch das Betätigen eines Schalters werden die Komponenten auf die werksmäßigen Default-Einstellungen zurück gesetzt. Dabei ist allerdings zu beachten, dass dieser Reset nicht zwangsläufig alle gespeicherten Einstellungen auf den ursprünglichen Zustand zurücksetzt. Eine anschließende Kontrolle ist daher zwingend erforderlich. Auf anderen Geräten können Konfigurationsdateien durch entsprechende Befehle komplett gelöscht oder durch andere Dateien ersetzt werden. Sollten die eingesetzten Geräte über keine der erwähnten Funktionen verfügen, ist eine individuelle Umkonfiguration oder die physikalische Zerstörung des Speichers erforderlich.

Gespeicherte Protokolldateien können auf einigen Geräten ebenfalls mit Hilfe des "Factory-Resets" gelöscht oder überschrieben werden. Dies ist allerdings als Ausnahme zu betrachten. Häufig kann eine Protokolldatei mit einem entsprechenden Befehl gelöscht werden. Vor der Außerbetriebnahme eines Gerätes sollte daher besonders darauf geachtet werden, dass keine Log-Dateien mehr vorhanden sind. Sollten die eingesetzten Geräte über keine der erwähnten Funktionen verfügen, ist eventuell die physikalische Zerstörung des Speichers erforderlich.

Oft sind Router und Switches von außen mit IP-Adressen, Hostnamen oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftung sollte vor der Entsorgung entfernt werden.

Prüffragen:

- Ist sichergestellt, dass vor der Außerbetriebnahme oder dem Austausch von Routern und Switches die gespeicherten Daten sicher gelöscht werden?
- Sind in der Sicherheitsrichtlinie für Router und Switches Verantwortlichkeiten für die sichere Außerbetriebnahme definiert?
- Ist eine vollständige physikalische Zerstörung des Speichers gewährleistet, wenn eine sichere Löschung der Daten auf den Routern und Switches nicht möglich ist?
- Werden Beschriftungen wie z. B. IP-Adressen oder Hostnamen vor der Entsorgung der Router und Switches entfernt?

# M 2.285 Festlegung von Standards für z/OS-Systemdefinitionen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Festlegung von Standards für die z/OS-Systemdefinitionen ist eine der Voraussetzungen für ein funktionierendes System-Management. Standards unterstützen aber auch die Umsetzung von Sicherheitsregeln und deren Überwachung. Die folgenden Empfehlungen sollten dabei beachtet werden:

Vereinbarte z/OS-System-Standards müssen nachvollziehbar dokumentiert sein. Die Dokumentation muss für die Administratoren verfügbar sein.

Die Einhaltung der z/OS-System-Standards sollte regelmäßig überprüft werden.

Es sollte überlegt werden, eine Standardisierung für die folgenden Objekte zu vereinbaren:

- Account-Nummer in Jobs und für USER oder STCs
- ACS-Routinen
- Allokierungs-Regeln
- Application-ID (IMS)
- Assembler-Standards
- Benutzergruppen-Kennzeichen
  z. B. Netzadministration, Entwicklung, Test, Produktion und DB-Administration
- COBOL-Compiler-Optionen
- Command-Character (Console)
- Command-Character (Terminal)
- Coupling-Facility-Namen
- Dateien
  anzulegende Dateien sollten katalogisiert sein
- Datei-Namen
  evtl. mit Unterscheidungsmerkmalen für System, Entwicklung und Produktion. Der letzte Qualifier legt in der Regel die Dateiart fest. Kennzeichnung von Target- und DLIB-Dateien
- Datenbank-Namen
- DFSMS
  DATA-CLASS, STORAGE-CLASS, MANGEMENT-CLASS, STORAGE-GROUP, LLQ-Zuordnungen
- IMS-ID
- IMS-Start-Prozeduren
- Initiator-Klassen
- ISMF-Schutz-Festlegungen
- JES2
  Job-Klassen, Initiator, Parameter
- JOBCAT und STEPCAT sollten nicht verwendet werden (IBM hat im August 2004 angekündigt, den Support zu JOBCAT und STEPCAT ab z/OS 1.7 einzustellen.)
- Job-Namen
  evtl. mit Unterscheidungsmerkmalen für Entwicklung und Produktion
- Katalog-Namen
- LOGON-Prozeduren-Namen
- Member-Namen
  evtl. mit Unterscheidungsmerkmalen für Entwicklung und Produktion

- Output-Klassen
- PAGE-Datasets
- Parmlib-Member für JESx
- Prozeduren-Namen
- RACF-Resource-Klassen
- SMF-Belegung (System Management Facility)
- SMP/E-Datei-Namen
- SMP/E-Umgebungen für verschiedene Subsysteme
- SMP/E-Zonen-Datasets
- SMP/E-Zonen-Namen
- SMS-Datei-Namen
- SSID (Sub-System ID)
- Vermeidung von Standortkennzeichen
  Standortkennzeichen haben sich im Rahmen von Umstrukturierungen und Anwendungsverlagerungen nicht unbedingt als vorteilhaft erwiesen
- STC-Namen (Started Tasks)
- STEPCAT sollte nicht verwendet werden
- SVC-Belegung
- Sysplex-ID
- Systemdateien-Namen
- System-ID (mit Sysplex-Kennung)
- Table-Space-Namen
- TSO-LOGON-Prozeduren
- UNIT-Klassen
- USER-ID
- USERMODs
- Volume-Namen (System-Volumes, Anwendungs-Volumes)

In Abhängigkeit von den eingesetzten Subsystemen, Datenbanksystemen, Software-Produkten und Anwendungen kann diese Liste noch durch weitere Objekte ergänzt werden.

Prüffragen:

- Wurden die vereinbarten z/OS-Standards nachvollziehbar dokumentiert?
- Ist die Dokumentation der z/OS-Standards für die Administratoren verfügbar?
- Wird die Einhaltung der z/OS-System-Standards regelmäßig überprüft?

# M 2.286 Planung und Einsatz von zSeries-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

**Planung**

Vor der Anschaffung und Inbetriebnahme von zSeries-Systemen müssen verschiedene planerische Tätigkeiten durchgeführt werden. Für die Planung des Einsatzes der zSeries-Systeme sind folgende Empfehlungen bezüglich der Sicherheit zu beachten:

*Infrastruktur*

Der Standort der zSeries-Hardware muss in einem zutrittsgeschützten Rechenzentrum geplant werden. Empfehlungen für die Infrastruktursicherheit von Rechenzentren finden sich in Baustein B 2.9 *Rechenzentrum*.

*Hardware*

Die Hardware-Ressourcen, die für den Betrieb benötigt werden, müssen geplant und in ihrer Kapazität entsprechend den Anforderungen dimensioniert werden. Dies betrifft die gesamte Hardware-Ausstattung, von der Anzahl der Prozessoren, über Kanäle, Festplatten und Bandstationen bis hin zu Netz-Komponenten (inklusive Netzanschlüsse).

*Betriebssysteme*

Es ist zu klären, welches der möglichen Betriebssysteme (z/OS, zLinux ohne Trägersystem, zLinux unter dem Trägersystem z/VM, etc.) für die Anforderungen der Anwendung zum Einsatz kommen muss.

*Anforderung der Anwendungen*

Die Anforderungen der Anwendungen an die Hardware und das Betriebssystem müssen bei der Planung berücksichtigt werden:

- Wie viele Anwender werden auf die Anwendung gleichzeitig zugreifen?
- Wird ein *Single-System* oder ein *Parallel-Sysplex System* benötigt? (u. a. eine Frage der Verfügbarkeit)
- Welches Datenvolumen wird durch den Betrieb der Anwendung anfallen? (Festplatten, Magnetbandstationen)
- Welchen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit hat die Anwendung bzw. ihre Daten?
- Welche Netzanschlüsse werden benötigt bzw. von wo erfolgen Zugriffe (aus dem Internet, Intranet, eigene Netzumgebung)?

*Prozesse*

Es ist zu überprüfen, wie das neue System in die bestehenden Prozesse eingebunden werden kann. Dies betrifft z. B. das Change Management, Eskalations- und Meldeverfahren, Sicherheits-Audits und weitere Management-Disziplinen.

Die Einhaltung der Sicherheitsvorgaben und -richtlinien der Behörde oder des Unternehmens muss bei der Planung mit berücksichtigt werden.

*Personal*

Es ist zu überprüfen, wie viele Mitarbeiter mit welcher Ausbildung für den Betrieb des zSeries-Systems benötigt werden. Stehen nicht genügend ausgebildete Mitarbeiter mit Mainframe-Wissen zur Verfügung, müssen die Schulungsmaßnahmen rechtzeitig initiiert werden.

**Einsatzszenarien**

Im Folgenden werden exemplarisch einige typische Einsatzszenarien von zSeries-Systemen vorgestellt und Empfehlungen zur Trennung von Systemen mit unterschiedlichen Sicherheitsanforderungen beschrieben.

*Batch-Systeme*

Bei Batch-Systemen steht die Stapelverarbeitung im Vordergrund. Stapelverarbeitung bedeutet, dass vorgegebene Programme (*Batch-Jobs*) an Hand von durch JCL (*Job Control Language*) definierten Abläufen ohne Interaktion mit den Benutzern - in der Regel große - Datenbestände bearbeiten. Batch-Systeme können sowohl als Einzelsysteme als auch im Rahmen von *Parallel-Sysplex-Clustern* betrieben werden. Für Batch-Systeme ist zu überlegen, ob eine Scheduling-Funktion zur Kontrolle der Stapelverarbeitung eingesetzt werden soll (siehe M 2.287 *Batch-Job-Planung für z/OS-Systeme*). Die Verwaltung der Zugriffsrechte sollte durch RACF (*Resource AccessControl Facility*) abgedeckt werden. Anhand der Anforderungen an die Skalierbarkeit ist außerdem zu prüfen, ob ein *Parallel-Sysplex-Cluster* eingesetzt werden sollte.

*Online-Systeme*

Online-Systeme verarbeiten Transaktionen, die durch interaktive Arbeiten der Benutzer am Bildschirm ausgelöst werden. Hierbei kommen häufig sogenannte Transaktionsmonitore wie CICS (*Customer Information Control System*) oder IMS (*Information Management System*) zum Einsatz. Wie bei Batch-Systemen sollte RACF zur Verwaltung und Durchsetzung der Zugriffsrechte verwendet werden. Bei hohen Anforderungen an die Verfügbarkeit des Online-Systems sollte geprüft werden, ob diesen Anforderungen durch den Einsatz eines *Parallel-Sysplex-Clusters* Rechnung getragen werden kann. Weitere Empfehlungen finden sich in der Maßnahme M 2.296 *Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren*.

*Web-Server*

zSeries-Systeme werden auch als Web-Server für Internet- oder Intranet-Angebote eingesetzt. Als Betriebssystem kommt dabei z/OS oder auch zLinux (separat oder als Gast unter z/VM) zum Einsatz. Sicherheitsempfehlungen für den Betrieb von Linux auf zSeries-Systemen finden sich in der Maßnahme M 4.212 *Absicherung von Linux für zSeries*.

*Datenbank-Server*

z/OS-Systeme können auch als Datenbank-Server eingesetzt werden. Das System stellt dazu, häufig mit Hilfe der Datenbank-Software DB2, Services zur Verfügung, die es erlauben, Datenbankinformationen abzufragen oder deren Inhalte zu verändern. Datenbank-Server werden oft in Verbindung mit Transaktionsmonitoren (z. B. CICS) oder mit Webservern eingesetzt und liefern diesen den notwendigen Datenbank-Zugriff. Die Konzentration auf den reinen Datenbank-Service reduziert die Komplexität und verbessert die Performance des Systems gerade bei sehr großen Datenbanken. Wie bei den vorher be-

schriebenen Szenarien sollte RACF auch bei Datenbank-Servern zur Verwaltung und Durchsetzung der Zugriffsrechte verwendet werden. Weitere Empfehlungen zum Einsatz von DB2 finden sich in der Maßnahme M 2.296 *Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren*.

*Universelle Systeme*

Universelle Systeme sind Mainframes, die mehrere der oben beschriebenen Dienste erbringen. Sie verarbeiten sowohl Batch-Jobs als auch Online-Transaktionen und enthalten einen (oder mehrere) Datenbank-Server. Gegebenenfalls werden sie zusätzlich auch noch als Webserver im Internet oder Intranet eingesetzt. In allen Bereichen sollte RACF als Sicherheitssystem eingesetzt werden.

**System-Trennung**

Da für Produktions-Systeme unter z/OS in der Regel höhere Sicherheitsanforderungen gelten als für Test- und Entwicklungssysteme, muss zwischen beiden Systemumgebungen eine Trennung erfolgen. Um diese Trennung zu realisieren, sind folgende Empfehlungen zu berücksichtigen:

*Gemeinsame Festplatten-Zugriffe*

Die Festplatten sind den Test- und Produktions-Systemen so zuzuordnen, dass unberechtigte Zugriffe auf Produktions-Daten verhindert werden können. Dabei erfolgt die Definition der Adressen im HCD (*Host ConfigurationDefinition*). Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass Festplatten aus Test-Systemen an Produktions-Systemen (und umgekehrt) nicht *Online* gesetzt werden können und dass auf die gleichen Festplatten nicht gleichzeitig von Test- und Produktions-Systemen aus zugegriffen werden kann (*Shared DASD*).

*Einsatz von FTP*

Der Datenaustausch zwischen Produktions- und Test-Systemen sollte über FTP (*File Transfer Program*) erfolgen.

*Shared Sysplex*

Produktions- und Test-Systeme sollten nicht im selben *Parallel Sysplex*-Verbund betrieben werden. Ist eine solche Konstellation notwendig, muss eine logische Trennung über entsprechende Standards und RACF-Definitionen (*Resource Access ControlFacility*) sicherstellen, dass kein Missbrauch von Dateizugriffen entstehen kann.

*Shared RACF-Datenbanken*

Es sollte überlegt werden, für Produktions- und Test-Systeme keine *Shared-RACF*-Datenbanken zu verwenden.

Prüffragen:

- Wird der Standort der zSeries-Hardware in einem zutrittsgeschützten Rechenzentrum geplant?
- Werden die Hardware-Resourcen des zSeries-Systems, die für den Betrieb benötigt werden, geplant und in ihrer Kapazität entsprechend den Anforderungen dimensioniert?
- Wird bei der Planung des zSeries-Systems die Einhaltung der Sicherheitsvorgaben und -richtlinien berücksichtigt?

- Stehen für den Betrieb von zSeries-Systemen genügend ausgebildete Mitarbeiter mit Mainframe-Wissen zur Verfügung?
- Ist beim Einsatz von zSeries-Systemen sichergestellt, dass Test- und Produktions-Systeme nicht im gleichen Parallel-Sysplex-Verbund laufen?

# M 2.287 Batch-Job-Planung für z/OS-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Beim Einsatz eines z/OS-Systems als Stapelverarbeitungs-Systems ist es bei einer größeren Anzahl von Batch-Jobs unabdingbar, dass der Ablauf dieser Jobs geplant, überwacht und bearbeitet werden muss. Da diese Tätigkeit manuell ohne Fehler kaum noch realisierbar ist, sollte Automations-Software, sogenannte *Job-Scheduler*, zur Ablaufsteuerung der Batch-Jobs eingesetzt werden.

### Aufgaben der Job-Scheduler

Die Aufgabe der Job-Scheduler besteht im wesentlichen aus den Funktionen

- Starten der Batch-Jobs
- Überwachen des Betriebszustandes der Batch-Jobs (darüber hinaus sicherstellen, dass Ressourcen bereitstehen)
- Prüfen der Ergebnisse (über Returncodes) der Batch-Jobs
- Verfolgen der Abhängigkeiten von Batch-Jobs
- Verwalten des Status der Batch Jobs
- Korrektive Maßnahmen im Fehlerfall

Die Sicherheitsmechanismen, um den Job-Scheduler vor Missbrauch zu schützen, sollten durch ein Sicherheitssystem wie RACF (*Resource Access Control Facility*) realisiert werden.

Für den Einsatz des Job-Schedulers sind mindestens die folgenden Hinweise zu beachten:

### Attribut OPERATIONS

Der Einsatz des RACF-Attributes *OPERATIONS* für die Kennung der *Started Task* des *Job Schedulers* sollte vermieden werden. Anderenfalls besteht die Gefahr, dass Batch-Jobs, die unter dieser Kennung gestartet werden, Zugriff zu nahezu allen Produktionsdateien haben (siehe M 2.289 *Einsatz restriktiver z/OS-Kennungen* und M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Falls der Hersteller für den Betrieb des Job-Schedulers das Attribut *OPERATIONS* fordert, sollte mit dem Hersteller geklärt werden, ob es hierzu Alternativen gibt.

### Einsatz von RACF-SURROGAT-Kennungen

Um zu verhindern, dass die Batch-Jobs aus dem Job-Scheduler heraus unter der eventuell hoch autorisierten Kennung des Job-Scheduler laufen, sollte überlegt werden, ob RACF-SURROGAT-Kennungen als Verfahrenskennungen eingesetzt werden können. Dabei sind die Nachteile dieser Funktion zu berücksichtigen (siehe M 2.289 *Einsatz restriktiver z/OS-Kennungen*).

### Prozedurdateien

Die Prozedurdateien des Job-Schedulers müssen so über RACF geschützt werden, dass der Zugriff auf die Prozedurdateien nur Mitarbeitern möglich ist, die diesen Zugriff für ihre Tätigkeit auch benötigen. Dabei ist die Anzahl auf ein Minimum zu beschränken. Eine Stellvertreter-Regelung muss in jedem Fall vorgesehen sein.

Die Kennung des Job-Schedulers muss lesenden Zugriff auf alle Prozedurdateien besitzen, um die Batch-Jobs entsprechend starten zu können.

**Tool-Zugriff**

Der Job-Scheduler wird meist über einen ISPF-Dialog (*Interactive System Productivity Facility*) gesteuert. Der Zugang zum Job-Scheduler sollte nur Mitarbeitern zur Verfügung stehen, die ihn für ihre Arbeit benötigen, sowie deren Vertretern. Der Zugangs- und Zugriffsschutz sollte über RACF erfolgen. Falls dies nicht möglich ist, müssen interne Sicherheitsmechanismen des Schedulers genutzt werden.

**Systemadministration**

Die Verwaltung der Batch-Jobs im Job-Scheduler sollte, wenn immer möglich, so über RACF geschützt werden, dass jede Anwender-Gruppe, wie Systembetreuer, Space-Management oder RACF-Administration, nur ihre Batch-Jobs einsehen und bearbeiten kann.

Prüffragen:

- Werden bei Einsatz eines z/OS-Systems zur Ablaufsteuerung von Batch-Jobs sogenannte Job-Scheduler eingesetzt?
- Wird der Job-Scheduler auf dem z/OS-System durch ein Sicherheitssystem (z. B. RACF) vor Missbrauch geschützt?
- Ist bei z/OS-Systemen sichergestellt, dass die Kennung des Job-Schedulers ohne das RACF-Attribut OPERATIONS auskommt?
- Ist der Zugang und Zugriff zum Job-Scheduler-Programm bei z/OS-Systemen über RACF geschützt?

# M 2.288 Erstellung von Sicherheitsrichtlinien für z/OS-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Vor dem Einsatz von z/OS-Systemen müssen Sicherheitsrichtlinien für das z/OS-System und besonders auch für das Sicherheitssystem RACF (*Resource Access Control Facility*) geplant und festgelegt werden. Es sind folgende Empfehlungen zu berücksichtigen:

- Die z/OS-Systeme müssen in das unternehmens- bzw. behördenweite Sicherheitsmanagement eingebunden werden.
- Wie in Maßnahme M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen* beschrieben, ist ein Verfahren zur Verwaltung der Benutzer des z/OS-Systems und deren Kennungen zu erstellen.
- Es muss eine Richtlinie zum Gebrauch des Notusers erstellt werden (siehe Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme*).
- Eine Richtlinie zur Wiederherstellung der RACF-Datenbank unter z/OS muss erstellt werden (siehe Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme*).
- Ein Berechtigungsprozess für den Zugriff auf sicherheitskritische System-Ressourcen, wie z. B. APF-Dateien (*Authorized Programming Facility*), SVCs (*SuperVisor Calls*) usw., muss beschrieben und eingeführt sein.
- Ein Audit-Verfahren, wie in Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS* beschrieben, bzw. ein Monitoring-Verfahren, wie in Maßnahme M 2.292 *Überwachung von z/OS-Systemen* beschrieben, müssen etabliert sein.
- Ein Eskalations- und Meldeverfahren muss aufgebaut sein. In ihm muss festgelegt sein, wer Sicherheits-Verstöße erkennt, weitermeldet und welche Abwehrmaßnahmen zu ergreifen sind.
- Eine Dokumentation zu Aufbau und Funktion eines Notsystems, wie in Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme* beschrieben, muss erstellt sein (gilt nur für Einzel-Systeme).
- Es sollte eine Prüfliste mit Kontrollfragen erstellt werden, die alle wichtigen sicherheitsrelevanten Einstellungen des z/OS-Systems erfasst und deren Soll-Werte festlegt. Anhand dieser Prüfliste werden die Arbeitsanweisungen für die System- und RACF-Administratoren erstellt. Die Prüfliste dient dem Auditor als Basis für die Überprüfung der Systemsicherheit. In regelmäßigen Abständen muss die Prüfliste überarbeitet werden. Als Basis für eine solche Prüfliste können die Maßnahmen M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* und M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* dienen.

Prüffragen:

- Werden vor dem Einsatz von z/OS-Systemen Sicherheitsrichtlinien für das z/OS-System und besonders auch für das Sicherheitssystem RACF geplant und festgelegt?
- Existiert ein Eskalations- und Meldeverfahren für Sicherheitsvorfälle im Zusammenhang mit z/OS-Systemen?
- Existiert eine Prüfliste mit Kontrollfragen, die alle wichtigen sicherheitsrelevanten Einstellungen des z/OS-Systems erfasst und deren Soll-Werte festlegt?

# M 2.289 Einsatz restriktiver z/OS-Kennungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für die Verwaltung des Sicherheitssystems RACF (*Resource Access Control Facility*) werden u. a. Kennungen mit hoher Autorisierung benötigt. Zur Minimierung des Missbrauchsrisikos sind die folgenden Regeln zu beachten:

**SPECIAL, OPERATIONS, AUDITOR**

Attribute mit hoher Autorisierung im RACF, wie *SPECIAL*, *OPERATIONS* und *AUDITOR*, gelten systemweit und dürfen nur an Anwender vergeben werden, die für ihre Tätigkeit diese Rechte benötigen. Kennungen mit diesen besonders hohen Rechten sind auf ein Minimum zu begrenzen, und deren Vergabe ist zu dokumentieren.

**GROUP-SPECIAL, GROUP-OPERATIONS, GROUP-AUDITOR**

Sind hohe Rechte erforderlich, so ist zu überlegen, ob diese Rechte nicht auf Gruppenebene (*GROUP-SPECIAL*, *GROUP-OPERATIONS* und *GROUP-AUDITOR*) für die jeweilige Kennung eingeschränkt werden können. Auch die Vergabe der auf Gruppenebene eingeschränkten Rechte ist auf ein Minimum zu begrenzen und zu dokumentieren.

**Superuser (UID 0)**

Im optionalen Unix-Segment der User-Kennung (*OMVS Segment*) wird eine für *Unix System Services* (USS) gültige Userid (*UID*) vergeben, unter der die z/OS-Kennung im USS geführt wird. Die UID 0 (*Superuser*) oder die Berechtigung, das *su*-Kommando ausführen zu dürfen, darf nur an die Anwender vergeben werden, die diese Berechtigung für ihre Arbeit benötigen.

**SPECIAL und UID 0**

Hoch autorisierte Kennungen mit Attribut *SPECIAL* dürfen aus Sicherheitsgründen nicht gleichzeitig mit UID 0 als *Superuser* unter USS laufen. Es ist weiterhin zu überlegen, ob die Attribute *SPECIAL* und *OPERATIONS* an die gleiche Kennung vergeben werden sollten.

**Vergabe von UIDs**

UIDs sollten nicht doppelt vergeben werden (gleiche UID für verschiedene User). Viele Tätigkeiten, für die in bestimmten Unix-Betriebssystemen unbedingt *Superuser*-Rechte benötigt werden, können im RACF einzeln über spezielle RACF-Profile der Klasse *UNIXPRIV* autorisiert werden. Eine solche Autorisierung über RACF-Profile ist in jedem Fall sicherer als die Vergabe der *Superuser*-Rechte oder su-Kommando-Berechtigung (siehe auch Maßnahme M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

**Audit-Verfahren**

Um die Tätigkeit der Anwender mit hohen Berechtigungen auditieren zu können, muss ein entsprechendes Audit-Verfahren etabliert sein (siehe auch Maßnahme M 2.288 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*).

**IBMUSER bei Neuinstallationen**

Erfolgt eine Neuinstallation, so sind mit dem *IBMUSER* mindestens zwei Kennungen mit dem Attribut *SPECIAL* neu anzulegen. Ist dies erfolgt, so muss der *IBMUSER* gesperrt (*REVOKED*) werden und gesperrt bleiben. RACF-Definitionen sollten nicht mit der Kennung *IBMUSER* angelegt werden (siehe auch Maßnahme M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

**Notuser-Verfahren**

Für den Fall, dass z. B. alle Kennungen mit dem Attribut *SPECIAL* gesperrt wurden, oder kein Anwender mit dieser Berechtigung im Notfall verfügbar ist, ist ein Notuser-Verfahren zu etablieren (siehe auch Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme*).

Prüffragen:

- Werden hohe Berechtigungen im z/OS-System nur an Anwender vergeben, die für Ihre Tätigkeiten diese Rechte benötigen?
- Wird die Vergabe der Attribute mit hoher Autorisierung im RACF dokumentiert?
- Wird verhindert, dass hoch autorisierte z/OS-Kennungen mit Attribut SPECIAL gleichzeitig mit UID 0 als Superuser unter USS laufen?
- Ist ein Audit-Verfahren für die z/OS-Systeme etabliert?
- Werden nach einer Neuinstallation des z/OS-Systems mindestens zwei Kennungen mit dem Attribut SPECIAL angelegt und anschließend der IBMUSER gesperrt?
- Werden RACF-Definitionen unter z/OS nicht mit der Kennung IBMUSER angelegt?
- Ist für die z/OS-Systeme ein Notuser-Verfahren etabliert?

# M 2.290 Einsatz von RACF-Exits

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Neben den Anpassungsmöglichkeiten von RACF (*Resource Access Control Facility*) durch Kommandos und Parameter ist es darüber hinaus möglich, zusätzliche Sicherheitsregeln durch den Einsatz von RACF-*Exits* zu implementieren. *Exits* werden an verschiedenen Stellen der RACF-Funktionen durchlaufen und erlauben dort individuelle Eingriffe. Ihr Einsatz erfordert ein hohes Maß an Wissen und Erfahrung in der Assembler-Programmierung.

Die folgenden Empfehlungen sollten beim Einsatz von *Exits* beachtet werden:

### Wartung der Exits

Wenn *Exits* zur Erweiterung der RACF-Funktionalität notwendig sind, müssen diese per SMP/E (*System Management Program/Enhanced*) als *Usermod* eingebaut werden (siehe M 2.293 *Wartung von zSeries-Systemen*).

### DES-Algorithmus zur Authentisierung

RACF verschlüsselt die Kennung mit Hilfe des DES-Algorithmus (*Data Encryption Standard*), wobei als Schlüssel das eingegebene Passwort benutzt wird (das Passwort selbst wird dabei nicht gespeichert). Um sicherzustellen, dass der DES-Algorithmus (und nicht der schwächere *Masking*-Algorithmus) benutzt wird, darf der in der *SYS1.LINKLIB* mitgelieferte *ExitICHDEX01* nicht in der *Link Pack Area* eingesetzt werden. Es wird daher empfohlen, dieses Lade-Modul zu entfernen und den entsprechenden Eintrag in SMP/E zu deaktivieren (*Usermod*), damit zukünftige Wartungsaktivitäten dieses Lade-Modul nicht eventuell wieder installieren. Der DES-Algorithmus ist normalerweise die Standardeinstellung bei der Auslieferung von RACF unter z/OS.

### Änderungen von Exits

Es ist zu beachten, dass bei Änderungen von *Exits* ein IPL (*Initial Program-Load*) notwendig ist. Eine Ausnahme hiervon stellt *IRREVX01* dar; er lässt sich dynamisch nachladen.

### Erweiterte Passwortregeln

Es sollte überlegt werden, ob die über die SETROPTS-Funktion von RACF zur Verfügung gestellten Mechanismen der Passwortregeln ausreichen oder ob über den *New Password Exit ICHPWX01* erweiterte Passwortregeln eingeführt werden sollen.

### Verwendung von Tools

Beim Einsatz von Tools zur Passwort-Synchronsierung oder von Produkten zum Tape-Management ist zu überprüfen, ob RACF-*Exits* mit dem Produkt geliefert werden oder sogar Voraussetzung für das Funktionieren des jeweiligen Produktes sind.

### Exit-Kontrolle

Der Einsatz von *Exits* kann über die Funktion *DSMON* kontrolliert werden. Eine solche Kontrolle sollte regelmäßig im Rahmen von Audits erfolgen (siehe auch M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). Eine

Ausnahme stellt *IRREVX01* dar. Dieser *Exit* sollte jedoch ebenfalls kontrolliert werden, wenn er verwendet wird.

Prüffragen:

- Sind Exits zur Erweiterung der RACF-Funktionalität unter z/OS per SMP/E als Usermod eingebaut?
- Ist sichergestellt, dass der DES-Algorithmus oder ein stärkeres Verfahren zur Authentisierung in den z/OS-Systemen benutzt wird?
- Erfolgt regelmäßig im Rahmen von Audits eine Kontrolle zum Einsatz von Exits?

# M 2.291 Sicherheits-Berichtswesen und -Audits unter z/OS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Revisor

Zur Überwachung aller sicherheitsrelevanten Tätigkeiten muss ein Prozess eingerichtet werden. In diesem muss festgelegt sein, welche Sicherheitsreports regelmäßig erstellt werden und wie mit Abweichungen von den Vorgaben umgegangen wird. Diese Sicherheitsreports sollten als Information für den Auditor verwendet werden.

Darüber hinaus müssen zur Erhöhung der Betriebssicherheit eines z/OS-Systems regelmäßig Sicherheits-Audits durchgeführt werden. Durch solche Audits wird überprüft, ob die geforderten Sicherheitseinstellungen und Abläufe eingehalten werden. Vorgaben hierfür finden sich in M 2.288 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*.

**Sicherheits-Berichtswesen**

*SMF-Sätze (System Management Facility) als Quelle des Berichtswesens*

Für die Überwachung der Informationssicherheit von z/OS-Systemen sind die SMF-Sätze des Typs 80 von Bedeutung. Sie protokollieren alle Zugriffe auf Ressourcen, die durch RACF-Profile geschützt werden. In diesen Profilen kann durch RACF-Definitionen festgelegt werden, ob nur unerlaubte oder auch erlaubte Zugriffe protokolliert werden. Unerlaubte Zugriffe müssen in jedem Fall protokolliert werden. Bei systemkritischen Dateien sollten in einem Produktionssystem auch die erlaubten Zugriffe über SMF erfasst werden, wenn die Datei dabei geändert wird. Beim Protokollieren über SMF-Sätze sollte immer darauf geachtet werden, dass durch das Aktivieren von SMF-Funktionen nicht zu viele Logdaten entstehen. Die Kapazität und die Performance des Systems darf nicht zu stark beeinträchtigt werden.

Es muss sichergestellt werden, dass der SMF-Satz Typ 80 auch wirklich geschrieben wird. Dies wird im Member *SMFPRM00* in der *Parmlib* definiert. Der Schutz der *Parmlib* ist in Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* näher beschrieben.

*Einsatz von Tools*

- Einsatz des RACFICE-Tools
  Es ist zu überlegen, IBMs ICE-Tool (*RACFICE*) basierend auf IBMs *DFSORT* einzusetzen und dabei vorgefertigte Reports zu verwenden, vorhandene anzupassen oder neue zu erstellen.
  Bei den SMF-Sätzen können beispielsweise fehlgeschlagene Zugriffsversuche auf Ressourcen, erlaubte Zugriffe infolge besonderer Berechtigungen (*OPERATIONS*) und fehlgeschlagene Zugriffsversuche mit falschem Passwort als Reports erzeugt werden.
  Aus der RACF-Datenbank können zum Beispiel die Dateiprofile selektiert nach UACC (*Universal Access*), gesperrte Benutzerkennungen und Profile, die in den letzten 90 Tagen verändert wurden, als Reports erzeugt werden.
- Einsatz des RACF-Programms *DSMON*
  Es ist zu überlegen, das RACF-Programm *DSMON* als Basis für weitere Berichte zu benutzen. Dies ist in jedem Fall zu empfehlen, wenn kein *Re-*

*al-Time-Monitor* eingesetzt werden soll, um Veränderungen an vitalen z/OS-Definitionen kontrollieren zu können.

- Einsatz von Independent Vendor Tools
  Die Auswertung der in den SMF-Sätzen protokollierten Informationen erfordert besondere Systemkenntnisse, wie z. B. der SMF-Programmfunktion. Es ist deshalb zu überlegen, separate Tools zur Auswertung dieser Datensätze einzusetzen. Entsprechende Programme sind von verschiedenen ISVs (*Independent Software Vendors*) erhältlich.
- Einsatz eines Real-Time-Monitors
  Bei besonderen Sicherheitsanforderungen ist zu überlegen, ob ein Berichtswesen auf Stapelverarbeitungsbasis aktuell genug ist oder ob ein *Real-Time-Monitor* zur Erkennung bestimmter Sicherheitsverstöße nicht sinnvoller ist. Dabei werden die SMF-Sätze über *SMF-Exits* (IEF083, IEF084, IEF085) direkt abgefangen und zu einem Monitor-Programm geleitet, das die Analyse und Darstellung übernehmen kann (siehe auch Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
  Wichtige Informationen für eine Echtzeit-Überwachung sind z. B.:

  - Änderungen an APF-Dateien
  - Benutzung von Kennungen mit dem Attribut *SPECIAL* oder *OPERATIONS*
  - Erlaubte Zugriffe auf Grund des Attributes *OPERATIONS*
  - Mehrfache Zugriffsversuche mit falschem Passwort
  - Benutzung des Notusers

**z/OS-Sicherheits-Audits**

*Unabhängigkeit der Auditoren*

Die Durchführung der Audits muss durch unabhängige Auditoren erfolgen, d. h. das durchführende Personal darf sich und seine Arbeit nicht selbst auditieren.

Die Auditoren müssen z/OS-System- und RACF-Kenntnisse zur Durchführung ihrer Tätigkeit haben. Diese Kenntnisse sind durch regelmäßige Schulungen zu erwerben bzw. zu aktualisieren.

*Autorisierung der Auditoren*

Die Auditoren müssen Zugangsberechtigung zum System mit dem RACF-Attribut *AUDITOR* haben. Auch für die Files in HFS-Dateien muss dieses Attribut im jeweiligen FSP (*File Security Packet*) aktiviert sein.

*Kontrolle über SMF-Sätze*

Grundlage für das Audit sind die SMF-Sätze des Recordtyps 80. Die Informationen in der RACF-Datenbank legen dabei fest, welche Ereignisse in den SMF-Sätzen protokolliert werden. Es muss deshalb sichergestellt werden, dass diese SMF-Sätze geschrieben werden und für Auswertungen zur Verfügung stehen.

*Überprüfung von RACF-Profilen*

Die Auditoren sollten überprüfen, ob bei Neueinrichtungen und Veränderungen von RACF-Profilen

- Genehmigungen vorliegen,
- die Funktionen bzw. Attribute (*SPECIAL, OPERATIONS*) in ihrem Befugnisumfang begründet sind (gilt auch für *GROUP-SPECIAL* und *GROUP-OPERATIONS*).

*Gegenstand des Sicherheits-Audits*

Ein vollständiges Sicherheits-Audit ist sehr komplex und muss eine große Anzahl von sicherheitsrelevanten Funktionen überwachen. Die folgenden Funktionen sollten mindestens überwacht werden:

- Kritische System-Einstellungen:
  - Program Properties Table (PPT)
  - Kontrolle der APF-Dateien (Authorized Programming Facility)
  - Kontrolle der Dateien aus der Linklist
  - SVC-Einsatz (SuperVisor Call)
  - Tabelle ICHRIN03 (Started Task Table)
- Kritische RACF-Funktionen:
  - RACF Authorized Caller
  - Einsatz von RACF Exits
  - RACF Started Procedures (hier besonders die Attribute Privileged und Trusted)
  - RACF Global Access Table
- Kritische Aktionen:
  - Aktivitäten von Kennungen mit SPECIAL, OPERATIONS (gilt auch für GROUP-SPECIAL und GROUP-OPERATIONS) oder Notuser, IBMUSER
  - Veränderung von sensitiven RACF-Parametern durch den Einsatz des SETROPTS-Kommandos
  - Alle Aufrufe des RACDEF-SVC (SVC 133) und alle Veränderungen an RACF-Profilen, die durch diesen RACF-Befehl entstanden sind
- Hinweise auf potentielle Sicherheitsverstöße:
  - Ballung von fehlgeschlagenen Anmelde- oder Zugriffsversuchen
  - Veränderung von Audit-Attributen
  - Behauptete bzw. identifizierte Benutzeridentität
  - Art des versuchten Zugriffs (Erfolg oder Scheitern)

*Einsatz von Audit-Tools*

Zur Kontrolle der zu überwachenden Definitionen sollte mindestens der *DSMON* von RACF und das *RACFICE*-Paket eingesetzt werden. Es ist zu prüfen, ob ein zusätzliches Programm-Paket beschafft werden sollte, das die Auditoren bei ihrer Arbeit unterstützt.

Wichtig ist, dass ein Audit nur zur Feststellung von Tatsachen und nicht zur Ermittlung von Schuldigen dient, siehe auch M 2.199 *Aufrechterhaltung der Informationssicherheit*.

Prüffragen:

- Ist ein Prozess zur Überwachung aller sicherheitsrelevanten Tätigkeiten unter z/OS eingerichtet, in dem festgelegt ist, welche Sicherheitsreports regelmäßig zu erstellen sind?
- Werden regelmäßig Sicherheits-Audits des z/OS-Systems durchgeführt?
- Ist bei z/OS-Sicherheits-Audits gewährleistet, dass das durchführende Personal sich und seine Arbeit nicht selbst auditiert?
- Sind die Auditoren für die Auditierung von z/OS-Systemen ausgebildet und auf einem aktuellen Schulungsstand?
- Haben die z/OS-Auditoren eine Zugangsberechtigung zum System mit dem RACF-Attribut AUDITOR?

# M 2.292 Überwachung von z/OS-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um Fehlersituationen und Sicherheitsprobleme zeitnah erkennen und beheben zu können, ist es notwendig, den laufenden Betrieb von z/OS-Systemen zu überwachen. Dazu stehen verschiedene Datenquellen des Betriebssystems zur Verfügung. Diese können entweder manuell durch das *Operating* oder automatisiert durch Programme analysiert werden.

Die folgenden Empfehlungen sind bei der Überwachung von z/OS-Systemen zu berücksichtigen:

### MCS-Konsole

Die MCS-Konsole (*Multiple Console Support*) stellt wichtige System-Meldungen (Fehler, Sicherheitsverstöße usw.) dar, auf die der Operator auch sofort reagieren kann. Um aus der Flut der Nachrichten die wichtigen herauszufiltern, ist der Einsatz der MPF-Funktion (*Message Processing Facility*) unbedingt erforderlich. Dabei ist es empfehlenswert, die wichtigen Nachrichten auf eine spezielle Konsole zu leiten, während die Kommunikation mit dem Betriebssystem auf anderen Konsolen stattfinden sollte. Es sollte überlegt werden, Farben zum Herausheben von kritischen Nachrichten einzusetzen.

### SMF-Auswertung

Nahezu alle Aktivitäten des Betriebssystems werden über SMF-Sätze (*System Management Facility*) protokolliert. Diese Sätze sind in jedem Fall zur Analyse nach Sicherheitsverstößen heranzuziehen (siehe auch Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). Um auch Ereignisse der Vergangenheit analysieren zu können, muss ein entsprechendes Archivierungsverfahren für die SMF-Daten vorhanden sein. Da die SMF-Daten ebenso für Abrechnung und Performance-Analysen des z/OS-Systems herangezogen werden können, ist ferner zu überlegen, ob ein entsprechendes Berichtswesen aufgebaut werden soll.

### SYSLOG-Auswertung

Alle wesentlichen Ereignisse werden darüber hinaus vom Betriebssystem im sogenannten SYSLOG (*System Log*) mitgeschrieben, das über SDSF (*System Display and Search Facility*) für JES2 oder über *Flasher* für JES3 für manuelle Analysen zur Verfügung steht. Es ist zu überlegen, ob Auswertungsprogramme erstellt und eingesetzt werden sollen, die das SYSLOG nach kritischen Nachrichten durchsuchen und entsprechende Reports erstellen.

### Automation

Es ist zu überlegen, ob Automations-Programme eingesetzt werden sollen, die vordefinierte SYSLOG-Meldungen erkennen und entsprechende Reaktionen im System auslösen können. Hierzu gibt es eine Reihe von Produkten am Markt, auch MPF inklusive *Exit*-Programmierung kann benutzt werden.

### Anwendungs-Logs

Viele Anwendungen schreiben eigene Protokolldaten, so zum Beispiel auch das USS-Subsystem (*Unix System Services*). Diese Protokolle sind ebenfalls

auf Sicherheitsverstöße zu analysieren, wichtige Nachrichten sind den Operatoren zur Verfügung zu stellen.

**Zentrale Kontrolle**

In größeren Installationen mit verschiedenen Standorten sollte eine zentrale Stelle existieren (*Focal Point*), an die alle für den Betrieb wichtigen Informationen gemeldet werden. Der Einsatz von Programmen, die das Geschehen übersichtlich - eventuell grafisch - darstellen können, ist zu überlegen. darzustellen?

Prüffragen:

- Wird der laufende Betrieb von z/OS-Systemen überwacht?
- Wird unter z/OS die MPF-Funktion eingesetzt, um aus den Nachrichten der ABAP-Konsole die wichtigen Systemmeldungen herauszufiltern?
- Werden unter z/OS die SMF-Sätze zur Analyse von Sicherheitsverstößen herangezogen?
- Werden bei der Überwachung der z/OS-Systeme Protokolldaten von Anwendungen auf Sicherheitsverstöße analysiert, und wichtige Nachrichten den Operatoren zur Verfügung gestellt?
- Bei Installationen mit verschiedenen Standorten: Existiert eine zentrale Stelle, der alle für den Betrieb des z/OS-Systems wichtigen Informationen gemeldet werden?

# M 2.293 Wartung von zSeries-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Maintenance-Konzeption umfasst die Wartung der zSeries-Hardware, des z/OS-Betriebssystems, der verschiedenen Programm-Produkte und die Wartung des zSeries-Microcode (*Firmware*). Wartung betrifft den kompletten Lebenszyklus eines Produktes, von der Neuinstallation über die permanente Pflege bis hin zum Abbau.

**Wartung des zSeries-Hardware**

Es ist zu empfehlen, für die Wartung der zSeries-Hardware einen Wartungsvertrag mit dem Hersteller bzw. mit vom Hersteller autorisierten Partnerunternehmen abzuschließen. Wartung kann entweder auf regelmäßiger Basis erfolgen oder wird notwendig, wenn interne Prüfprogramme Fehler entdecken und über RSF (*Remote Support Facility*) den Hersteller oder seinen Vertreter informieren. Zur Sicherstellung der Funktionsfähigkeit der Hardware (und auch der Basis-Software) ist eine regelmäßige Überprüfung der EREP-Reports (*Environmental Record Editing and Printing Program*) zu empfehlen. Die im EREP-Report dargestellten Informationen über Hard- und Software-Probleme werden von der Hardware und dem z/OS-Betriebssystem geliefert.

**Wartung des z/OS-Betriebssystems**

Die Wartung eines z/OS-Systems inklusive aller Subsysteme ist äußerst komplex und bedarf deswegen einer sorgfältigen Planung. Unter den Begriff Wartung fällt:

- Inbetriebnahme eines neuen Systems
- Änderungen als Funktionserweiterung oder Nachrüstung von Funktionen
- Behebung von gemeldeten Fehlern durch sogenannte PTFs (*Program Temporary Fixes*)
- Einbau von PTFs als präventive Maßnahme (besonders wichtig sind hier PTFs gegen gemeldete Sicherheitslücken) auf Grund von Herstellerinformationen
- Abbau von Systemen

Die Wartung von z/OS-Betriebssystemen kann normalerweise nicht ohne Unterbrechung des Betriebs durchgeführt werden.

Bei der Wartung des z/OS-Betriebssystems sind die folgenden Empfehlungen zu berücksichtigen:

*Wartungspläne*

Es müssen Wartungspläne erstellt werden, in denen festgelegt wird, wann Änderungen am System durchgeführt werden dürfen. Es müssen IPL-Termine (*Initial Program Load*) festgelegt und Testszenarien erarbeitet werden. Dies muss mit allen Beteiligten abgesprochen werden. Um fehlgeschlagene Änderungen notfalls wieder rückgängig machen zu können, muss ein Rückfall-Konzept erstellt werden.

*Change Management*

Alle Änderungen an Definitionen des z/OS-Betriebssystems (auch dynamische Änderungen während des produktiven Betriebs) müssen über das

Change Management geplant und kontrolliert werden. Dies gilt auch für Neuinstallationen.

*Neuinstallation*

Eine Neuinstallation wird notwendig, wenn ein z/OS-Betriebssystem erstmalig in Betrieb gehen soll oder wenn eine neue Version (bzw. neues Release) die vorhandene Version ablösen soll. Der Hersteller bietet hier unter dem Begriff *CustomPac* verschiedene, weitgehend vorbereitete Produkt- und Systemlieferungen an, die teils kostenlos, teils im Rahmen von Wartungsverträgen zur Verfügung stehen.

*SystemPac* ist ein Teil des *CustomPac*-Angebotes und erlaubt es, eine weitgehend vorbereitete Lieferung des z/OS-Betriebssystems - gegebenenfalls einschließlich einiger Zusatzprodukte - zu installieren. Zur Neuinstallation ist eine separate Systemumgebung (siehe unten) erforderlich. Durch die Nutzung von *SystemPac* kann der Aufwand und dadurch auch die Wahrscheinlichkeit von Bedienungsfehlern bei der Neuinstallation erheblich reduziert werden. Es sollte deshalb überlegt werden, bei Neuinstallationen von z/OS auf den *SystemPac*-Mechanismen zurückzugreifen. Dabei sind auch die Zusatzkosten zu berücksichtigen, die dadurch eventuell anfallen.

*Permanente Pflege der Komponenten*

Das z/OS-Betriebssystem und seine Programm-Produkte müssen permanent gepflegt werden. Fast alle Hersteller stellen für ihre Programme *Patches* (im Mainframe-System als PTFs bekannt) zur Verfügung, die Fehler beheben sollen. IBM stellt diese PTFs für das z/OS-Betriebssystem über verschiedene Kanäle zur Verfügung:

- als Einzellieferung auf Anforderung des Kunden (z. B. auf Grund einer Fehlersituation): hier muss der Anwender die Rahmenbedingungen selbst überprüfen, z. B. die Abhängigkeiten
- als *RefreshPac* im Rahmen präventiver Wartung, angepasst an das Kundensystem (von IBM vorgeprüft) oder
- als OMIS-Lieferung (*Online Maintenance Information System*). OMIS basiert auf den Daten des Kundensystems und ist ebenfalls von IBM vorgeprüft.

Es ist zu überlegen, ob präventive Wartung zur Erhöhung der Betriebssicherheit notwendig ist, oder ob PTFs nur bei aktuellen Fehlern eingespielt werden sollen. Sicherheitsrelevante Patches sollten in jedem Fall präventiv und zeitnah nach dem Erscheinen eingespielt werden. Dies gilt besonders für Systeme mit Internetzugang. Informationen über sicherheitsrelevante Patches können von IBM angefordert werden.

*SMP/E-Wartung*

Als zentrales Wartungs-Tool ist SMP/E einzusetzen, das *System Modifikation-Program/Extended*. Durch die Bestandsführung der Software-Stände im CSI (*Consolidated Software Inventory*) wird sichergestellt, dass alle Informationen über Module, Versionen und Zusammenhänge des z/OS-Betriebssystems zur Verfügung stehen und damit Fehler bei der Installation der Patches möglichst vermieden werden.

*Independent Software Vendors*

Software-Produkte von ISVs (*Independent Software Vendors*) sollten möglichst ebenfalls über SMP/E installiert und gepflegt werden. Es ist zu überle-

gen, ob ISV-Produkte separat oder im Rahmen des *SystemPac*-Mechanismus installiert werden sollen.

*Consolidated Software Inventory*

Es sollte ein CSI für das z/OS-Betriebssystem existieren, bzw. im Falle einer *SystemPac*-Installation gemäß der Lieferung durch IBM sollte das (die) CSI(s), wie im Ablauf vorgesehen, angelegt werden. Pro Hersteller wird ein separates CSI empfohlen, um Problemen mit Namensgleichheit bei PTFs vorzubeugen.

*USERMODS*

Eigene Änderungen durch Anwender sollten nur mittels SMP/E installiert werden (als *USERMODS*). Dies stellt sicher, dass die eigenen Änderungen nicht durch Herstelleränderungen überspielt werden, ohne dass eine Information darüber vorliegt. Sie müssen nach jedem Releasewechsel des Systems bzw. der Module, auf denen die Änderungen aufsetzen, neu installiert und eventuell auch angepasst werden. *USERMODS* sollten auf ein Minimum begrenzt werden, da sie permanenten Pflegeaufwand nach sich ziehen.

*ACCEPT-Läufe*

Durch einen *ACCEPT*-Lauf wird ein PTF permanent im System abgelegt, d. h. es ist nicht mehr entfernbar. Ein *ACCEPT*-Lauf sollte daher erst stattfinden, wenn sichergestellt ist, dass die PTFs die festgestellten Probleme beseitigen und keine neuen erkennbaren Fehler hervorrufen.

*APPLY CHECK*

Es ist zu empfehlen, dass vor dem Einbau von PTFs über einen *APPLY CHECK SMP/E*-Lauf sichergestellt wird, dass die PTFs auch zur aktuell installierten Betriebssystem-Umgebung passen und keine zusätzlichen PTFserforderlich sind (sogenannte *Prerequisites* oder *Corequisites*).

*Test vor Produktion*

Die betriebliche Zuverlässigkeit der gelieferten PTFs sollte erst auf einem Testsystem überprüft werden, bevor die PTFs in ein Produktionssystem eingebaut werden. Bei größeren Wartungsarbeiten (z. B. ein sogenannter *Refresh* mit hunderten von PTFs) muss dieser Ablauf in jedem Fall vorgesehen werden.

*Kumulative Betriebssystemdateien*

Es sollten keine Betriebssystemdateien an SMP/E vorbei kopiert werden, da hierdurch die Sicherheit der Wartung beeinträchtigt werden kann. Kumulierte Dateien sind solche, die aus mehreren Dateien zusammengesetzt worden sind. Sollen kumulierte Dateien verwendet werden, muss entweder die Bestandsführung in SMP/E angepasst oder ein separates Verfahren eingesetzt werden, um die Bestandskontrolle gewährleisten zu können. Es ist daher zu überlegen, ob der Mehraufwand gerechtfertigt ist.

*Alternative Systemumgebung*

Zum Einbau von PTFs sollte eine zweite (alternative) Systemumgebung benutzt werden. Hierfür sollten separate Festplatten mit einer Kopie des Originalsystems verwendet werden. Dies ermöglicht ein problemloses Einbauen während der Betriebszeiten und erlaubt ein schnelles IPL (*Initial Program Load*) von der veränderten *System Residence* (der Festplatte, von der der Boot-Vor-

gang eingeleitet wird). Darüber hinaus unterstützt diese Vorgehensweise (Flip-Flop-Verfahren) den schnellen Fallback, da die Festplatten der vorher aktiven Betriebssystemkomponenten noch zur Verfügung stehen.

*System-Cloning*

Unter *System-Cloning* versteht man das Kopieren der Betriebssystem-Komponenten auf einen neuen Festplatten-Satz unter Berücksichtigung der zu ändernden Definitionen. Es ist zu überlegen, ob ein Verfahren zum *System-Cloning* etabliert wird, um alternative System-Umgebungen schnell und sicher aufbauen zu können.

Ein solches Verfahren muss eigenständig erstellt werden, z. B. in Form eines Batch-Jobs mit mehreren Schritten. Die Benutzung von System-Variablen hilft hier wesentlich.

*Einsatz symbolischer System-Variablen*

Bei den z/OS-Parameter-Dateien sollte, soweit möglich, mit symbolischen Variablen gearbeitet werden. Dies vereinfacht das *System-Cloning* erheblich und vermeidet vielfach auch Fehldefinitionen. Ab dem z/OS-Betriebssystem V1R4 stehen bis zu 800 Variablen zur Verfügung.

*Dokumentation*

Es ist zu überlegen, ob ein Berichtswesen, basierend auf SMP/E, aufgebaut werden sollte, um jederzeit den aktuellen Stand der gesamten Software des Betriebssystems darstellen zu können.

**Wartung des zSeries-Microcode (Firmware)**

Zur Behebung von Code-Fehlern in der Firmware, zum Firmware-Update auf neue Versionen und zur Aktivierung oder Deaktivierung von Hardware-Komponenten (z. B. Prozessoren, Krypto-Hardware) werden von den Herstellern Microcode-Updates durchgeführt. Hierfür müssen folgende Hinweise beachtet werden:

*Betreiberkontrolle*

Updates durch den Hersteller dürfen nur nach Absprache mit dem Betreiber der zSeries-Systeme und nur unter Kontrolle von Mitarbeitern des Betreibers durchgeführt werden.

*Hersteller-Erklärung*

Der Hersteller der Betriebssystem-Software sollte eine Vertraulichkeits-Erklärung ausstellen.

*Remote Wartung*

Der externe Zugang (*Remote Access*) ist, wie in Baustein B 4.4 *VPN* und speziell in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*beschrieben, zu schützen. Es muss sichergestellt werden, dass Änderungen an Firmware-Komponenten nur nach Abstimmung mit dem zSeries-Systembetreiber erfolgen.

**Abbau des z/OS-Betriebssystems**

Weiterführende Informationen zu dem Abbau eines z/OS-Betriebssystems sind unter M 2.297 *Deinstallation von z/OS-Systemen* zu finden.

Prüffragen:

- Existieren Wartungspläne mit festgelegten Zeitfenstern für Änderungen an zSeries-Systemen?
- Sind für die z/OS-Systeme IPL-Termine festgelegt und Testszenarien erarbeitet, die mit allen Beteiligten abgestimmt sind?
- Existiert ein Rückfall-Konzept, um fehlgeschlagene Änderungen des z/OS-Systems wieder rückgängig machen zu können?
- Werden alle, auch die dynamischen, Änderungen an Definitionen des z/OS-Betriebssystems über das Change Management geplant und kontrolliert?
- Wird SMP/E als zentrales Wartungs-Tool für z/OS-Systeme eingesetzt?
- Bei Nutzung des System-Cloning: Wird bei den z/OS-Parameter-Dateien, soweit möglich, mit symbolischen Variablen gearbeitet?
- Ist sichergestellt, dass Updates durch den Hersteller nur nach Absprache mit dem Betreiber der zSeries-Systeme und nur unter Kontrolle von Mitarbeitern des Betreibers durchgeführt werden?

# M 2.294 Synchronisierung von z/OS-Passwörtern und RACF-Kommandos

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In großen Mainframe-Verbünden kommunizieren oft viele z/OS-Betriebssysteme und ihre RACF-Datenbanken (*Resource Access Control Facility*) miteinander. Es besteht oftmals der Bedarf, Passwortänderungen oder RACF-Kommandos über mehrere z/OS-Systeme des Verbundes zu synchronisieren.

Bei der *Passwort-Synchronisation* werden die Passwörter der Anwender auf mehreren z/OS-Systemen automatisiert synchronisiert, so dass der Anwender nur ein Passwort verwenden muss.

Bei der *RACF-Kommando-Synchronisation* können RACF-Kommandos auf mehreren z/OS-Systemen parallel ausgeführt werden. Das entsprechende RACF-Kommando wird an einem System eingegeben und durch die zentrale RACF-Administration an alle anderen Systeme weitergeleitet. RACF unterstützt dies durch das Feature RRSF (*RACF Remote Sharing Facility*).

Solche Verbünde werden auch *Synchronisierungs-Verbund* genannt. Für einen *Synchronisierungs-Verbund* sind die folgenden Empfehlungen zu beachten.

### Standardisierung

Es muss sichergestellt werden, dass der Aufbau und die verwendeten Regeln der RACF-Datenbanken auf allen Systemen des *Synchronisierungs-Verbunds* möglichst identisch sind. Vor der Einrichtung eines Synchronisierungs-Verbunds sollte eine möglichst weitgehende Standardisierung durchgeführt werden (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).

### Sperren einer Benutzerkennung

Bei der Passwort-Synchronisation muss verhindert werden, dass das Sperren (*Revoke*) einer Benutzerkennung nach mehrmaliger Falscheingabe des Passwortes an alle anderen Systeme des Synchronisations-Verbundes weitergeleitet wird. Der Benutzer wäre sonst auf allen Systemen ausgesperrt. Ein Entsperren (*Resume*) kann beliebig oft übertragen werden.

### Weiterleiten von RACF-Kommandos

Bei der *RACF-Kommando-Synchronisation* muss mit äußerster Sorgfalt vorgegangen werden. Denn fehlerhafte RACF-Kommandos, die zu ungewollten Änderungen führen, werden sofort auf allen Systemen des Synchronisations-Verbundes ausgeführt. Es sollte deshalb überlegt werden, besonders sicherheitskritische RACF-Kommandos, welche die Stabilität der angebundenen Systeme beeinflussen können, von der Synchronisation auszuschließen.

### Absichern der Verwaltungsfunktion

Die Schnittstelle zu der Verwaltungs-Funktion des Synchronisations-Programmes (oft eine ISPF-Oberfläche - *Interactive System Productivity Facility*) darf nur autorisierten Mitarbeitern im Rahmen ihrer Tätigkeit zur Verfügung stehen.

**Schadensbegrenzung durch Aufteilen des Verbundes**

Zur Schadensbegrenzung bei der RACF-Kommando-Synchronisierung ist zu überlegen, einen großen Synchronisierungs-Verbund in zwei oder mehrere kleine Teilverbünde zu zerlegen.

Die Ausführung von fehlerhaften, sicherheitskritischen RACF-Kommandos kann dadurch auf den jeweiligen Teilverbund beschränkt werden. Ein Totalausfall aller Systeme, der auf fehlerhafte RACF-Kommandos zurückzuführen ist, kann auf diese Weise unter Umständen vermieden werden.

Die für den Betrieb notwendigen Festplatten der Systeme eines Teilverbundes müssen an die Systeme eines anderen Teilverbundes angeschlossen werden können. Dadurch können betriebswichtige Daten eines ausgefallenen Teilverbundes, wie die RACF-Datenbank, zumindest teilweise wieder hergestellt werden.

Die Aufteilung eines großen Synchronisierungs-Verbundes in mehrere kleinere Teilverbünde führt zu einem erhöhten Administrationsaufwand. Denn jeder Teilverbund muss separat administriert werden.

Prüffragen:

- Wird vor der Einrichtung des Synchronisierungs-Verbunds unter z/OS eine möglichst weitgehende Standardisierung durchgeführt, so dass der Aufbau und die verwendeten Regeln der RACF-Datenbank auf allen Systemen des Synchronisierungs-Verbunds möglichst identisch sind?
- Ist die Passwort-Synchronisation unter z/OS so eingerichtet, dass das Sperren (Revoke) einer Benutzerkennung nach mehrmaliger Falscheingabe des Passwortes nicht an alle anderen Systeme des Synchronisations-Verbunds weitergeleitet wird?
- Ist sichergestellt, dass die Schnittstelle der Verwaltungs-Funktion des Synchronisations-Programms für z/OS-Systeme nur autorisierten Mitarbeitern im Rahmen ihrer Tätigkeit zur Verfügung steht?

# M 2.295 Systemverwaltung von z/OS-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Systemverwaltung eines z/OS-Systems ist in verschiedene Bereiche aufgeteilt. Für viele Aufgaben gibt es in den Rechenzentren Spezialisten, die oft nur ganz bestimmte Tätigkeiten auf den z/OS-Systemen ausführen. Bei der Systemverwaltung sind nachfolgende Empfehlungen zu beachten:

**Unterteilung in Rollen**

Es sollte ein Rollenkonzept eingeführt werden. Dies ermöglicht die Zuordnung von System-Berechtigungen zu den Rollen und erleichtert hiermit die Arbeit der RACF-Administration.

Um die Vergabe von hohen Berechtigungs-Attributen im RACF zu reduzieren, sollte überlegt werden, die Administration in mindestens folgende Rollen zu unterteilen:

- Systemadministration
  Die Systemadministration (kein besonderes RACF-Attribut) ist für die Installation und Wartung der z/OS-Systeme verantwortlich. Ihre Berechtigungen dürfen nur die zu dieser Tätigkeit nötigen Arbeiten am System erlauben. Zugriffe auf Kundendaten sollten nur in Ausnahmefällen genehmigt werden (z. B. bei der Fehlersuche). Solche Zugriffe müssen mit dem jeweiligen Informationseigentümer abgestimmt werden.
- RACF-Administration
  Die RACF-Administration (RACF-Attribut *SPECIAL*) hat die folgende Aufgabe: Administration des Sicherheitsprogramms RACF sowie Anlegen und Löschen von Kennungen und Autorisierungen. Der RACF-Administrator vergibt und entzieht die Rechte auf Ressourcen im z/OS-System. Hieraus ergibt sich eine besondere Vertrauensstellung. Aus Sicherheitsgründen sollte die Zahl der Mitarbeiter, die dieser Rolle zugeordnet sind, auf ein Minimum begrenzt sein.
- Space-Management
  Das Space-Management (RACF-Attribut *OPERATIONS*) ist für die Verwaltung der Datenträger in z/OS-Systemen verantwortlich. Das Attribut *OPERATIONS* erlaubt den Zugriff auf alle Daten des Systems. Es sollte überlegt werden, Kennungen mit dem Attribut *OPERATIONS* in die ACCESS-Liste eines RACF-Profiles mit NONE aufzunehmen. Hierdurch wird der Zugriff über die *OPERATIONS*-Berechtigung verhindert. Allerdings können diese Dateien dann auch nur bedingt vom Space-Management verwaltet (z. B. Plattenverlagerung) werden.
- Operating
  Das Operating (kein besonderes RACF-Attribut) ist für den Betrieb der z/OS-Systeme verantwortlich. Da die Operatoren Zugang zu den Konsolen haben, muss das Operating in zutrittsgeschützten Räumen durchgeführt werden. Aus Gründen der Nachvollziehbarkeit sollten die Schichtpläne des Operating archiviert werden.
- Audits
  Der Auditor (RACF Attribut *AUDITOR*) kann alle sicherheitsrelevanten Systemeinstellungen einsehen, aber nicht ändern. Der Auditor gleicht die aktuellen Systemeinstellungen mit den vorgegebenen Systemeinstellungen ab.

**Stellvertreter-Regelungen**

Für alle wichtigen Rollen der Systemverwaltung müssen Stellvertreter-Regelungen vorhanden sein. Keinesfalls darf eine wichtige Rolle nur mit einer Person besetzt sein. Weitere Hinweise hierzu sind in M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* aufgeführt.

Prüffragen:

- Gibt es ein Rollenkonzept für z/OS-Systeme?
- Gibt es Stellvertreter-Regelungen für die wichtigen Rollen der Systemverwaltung von z/OS-Systemen?

# M 2.296 Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Einsatz von Transaktionsmonitoren muss detailliert geplant und durch geeignete Mechanismen abgesichert werden. Als Hilfestellung werden in dieser Maßnahme einige Empfehlungen im Überblick beschrieben, die sich aus Sicht der Informationssicherheit beim Betrieb von Transaktionsmonitoren bewährt haben. Je nach Einsatzszenario sind in der Regel weitere spezifische Planungen und Sicherheitsmechanismen erforderlich, die hier nicht dargestellt werden können. Insbesondere wird in dieser Maßnahme nicht der Datenbankteil von IMS betrachtet.

Transaktionsmonitore werden auf Mainframe-Systemen für den Online-Betrieb eingesetzt. Sie ermöglichen den Anwendern, im Dialogbetrieb auf die gewünschten Daten über nachgeschaltete Datenbanksysteme zuzugreifen. Dabei gehört es zu den Kernaufgaben des Transaktionsmonitors sicherzustellen, dass die folgenden Bedingungen erfüllt werden:

- Eine Transaktion muss immer komplett durchgeführt werden. Ist das nicht realisierbar, muss das System auf den vorherigen Stand zurückgesetzt werden (Roll-Back).
- Das System sollte sich vor und nach der Transaktion in einem konsistenten Zustand befinden, ansonsten muss das System zurückgesetzt werden.
- Jeder Anwender soll nur Zugriff auf seine Daten erhalten und sollte isoliert sein von allen anderen Daten.
- Nach Durchführung der Transaktion muss sichergestellt werden, dass der veränderte Zustand gespeichert wird und später in der gleichen Form zur Verfügung steht. Im Falle eines Systemausfalls müssen die noch nicht gespeicherten Transaktionen notfalls automatisch wiederholt werden.

Diese Bedingungen gelten sowohl für den Online-Betrieb, als auch für Transaktionen, die im Batch-Betrieb durchgeführt werden.

Transaktionsmonitore werden heute üblicherweise in einer sogenannten Drei-Tier-Konfiguration (Tier = Stufen) eingesetzt (Präsentation, Anwendungslogik, Datenhaltung) und decken normalerweise die folgenden Kernfunktionen ab:

- Message Queuing (Verwalten des Nachrichten-Flusses)
- Lock-Verwaltung (Verwaltung der Zugriffe und gegenseitige Absicherung)
- Logging (Verwaltung der Log-Funktionen)
- Roll-Back Funktionen (Zurückspringen auf den vorherigen Zustand)
- Laststeuerung (Load Balancing)
- Two-Phase Commit-Synchronisation (stellt sicher, dass eine Transaktion komplett durchgeführt wird oder ein Roll-Back erfolgt)

Als Transaktionsmonitor wird u. a. IMS TM (*Information Management System Transaction Monitor*) oder CICS (*Customer Information Control System*) eingesetzt. Als Datenbanksystem steht für IMS der IMS-eigene DB-Teil, VSAM-Datenbanken (*Virtual System Access Method*) oder DB2 (*Database 2*) zur Verfügung. Für CICS können VSAM, IMS DB oder DB2 als Datenbanksysteme eingesetzt werden.

Auch wenn die Transaktionsmonitore und Datenbanksysteme aus historischen Gründen eigene interne Schutzsysteme zum Teil noch anbieten, wird in der heutigen Zeit meistens ergänzend ein Sicherheitssystem wie RACF (*Re-*

*source AccessControl Facility*) eingesetzt. Mit RACF können die Authentisierung des Benutzers, der Schutz der Transaktionen und der Zugriffsschutz auf Datenelemente realisiert werden.

**Allgemeine Überlegungen**

Die Transaktionsmonitore IMS TM und CICS sind von der historischen Entwicklung her reine VTAM-Applikationen. Sie waren zu Beginn der Entwicklung für interne Netze konzipiert. Im Laufe der letzten Jahre sind jedoch durch die steigende Bedeutung des Internets erweiterte Schnittstellen bereitgestellt worden. Diese ermöglichen es, Zugriffe auf Anwendungen dieser Transaktionsmonitore auch vom Internet aus zu erlauben.

Die folgenden Empfehlungen gelten für den gesamten Bereich der Transaktionsmonitore und schließen die Datenbanken mit ein:

- Alle Sicherheitsmechanismen sollten möglichst durch RACF gesteuert werden. Die internen Sicherheitsmechanismen sind nur dort zu benutzen, wo es keine adäquaten RACF-Funktionen gibt.
- Es sollten vor Inbetriebnahme eines Transaktionsmonitors, wie IMS oder CICS, oder eines Datenbanksystems, wie DB2, Standards für alle relevanten Definitionen entwickelt werden. Die Standards sollten Transaktionsnamen, Tabellennamen, Resource Classes, etc. betreffen. Solche Standards helfen dabei, Fehler bei RACF-Definitionen zu vermeiden (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Es sollte überlegt werden, ob die Einführung von Rollen-Konzepten (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*) die Verwaltung der Benutzer erleichtert.
- Sicherheitsmechanismen sollten bei Transaktionsmonitoren immer so aktiviert werden, dass das entsprechende Regelwerk extern definiert werden kann. Der Einsatz externer Sicherheitsfunktionen, wie RACF-Definitionen, sollte immer eventuell vorhandenen internen Funktionen vorgezogen werden.

**IMS TM (*Transaction Monitor*, vorher *DC* genannt)**

Die folgenden Empfehlungen gelten für den IMS Transaktionsmonitor. Je nach Einsatzszenario sind in der Regel weitere Sicherheitsmechanismen erforderlich.

- IMS sollte über die Definition im *IMS Security Makro* so eingestellt werden, dass IMS RACF verwendet (Parameter *TYPE = RACFAGN / RACFTERM / RACFCOM*). Das IMS System muss durch die *RCLASS* Definition so definiert werden, dass dieser Name (die IMS-ID) in RACF als *Resource Class* geführt werden kann. Ist mehr als ein IMS im z/OS-System in Betrieb, sollte überlegt werden, ob die standardmäßig in RACF vorhandenen Namen benutzt werden sollen (z. B. AIMS, TIMS usw.) oder ob eigene (unterschiedliche) Namen vergeben werden sollten. Bei der Benutzung von eigenen Namen müssen diese als *Resource Classes* in RACF eingetragen werden.
  Über das IMS Security Makro können u. a. die folgenden Prüfungen aktiviert werden (Benutzung der Default IMS-ID IMS):
  - AGN Prüfung über RACF (über Klasse AIMS), Ablegen der gültigen User-IDs für IMS in RACF (RDEFINE)
  - Transaktions-Autorisierung (über Klasse TIMS oder GIMS und SECLVL=TRANAUTH im Security Makro)
  - Terminal Security (SECLVL=SIGNON / FORCSIGN im Security Macro und Resource Class TERMINAL in RACF)
  - Kommando Autorisierung (über Klasse CIMS oder DIMS)

Existiert ein Parallel Sysplex mit Datasharing, sollte als RCLASS Wert die IMS-ID des Master-IMS benutzt werden.
- Es sollte überlegt werden, ob zur Signon Verifizierung ein Exit (DFSSGNX0) eingesetzt werden sollte (falls die RACF Prüfung nicht ausreichend granular ist).
- Es müssen in RACF Standard Profile für die einzelnen Resource Classes eingerichtet werden, zu denen die Applikations-Anwender zugelassen werden können. Es ist empfehlenswert, vor Beginn der Definitionen Standards zu entwickeln, die die Definitionen erleichtern.

- Es sollte überlegt werden, ob die Sicherheitsanforderungen eine Terminal-Security über RACF notwendig machen (Class Terminal). Vorsicht ist geboten bei Einführung eines restriktiven Schutzes gegen nicht definierte Terminals, z. B. mit dem RACF Kommando SETROPTS TERMINAL(NONE): Es müssen mindestens einige Terminals für die Benutzung von RACF unter TSO freigeschaltet sein, da sich sonst niemand mehr auf dem System anmelden kann!
- Das Mapping von RACF-Resource Classes auf die internen IMS Security Regeln erfolgt über Definitionen, die über den SMU-Prozess (Security Management Utility) verarbeitet werden. Aus der Definitionsdatei wird über einen Preprocessor und nachfolgendem Assembly und Link ein Loadmodule erzeugt, das auf dem IMS Matrix Dataset gestellt wird und in dem u. a. die IMS Security Definitionen in Kontrollblockform zur Verfügung stehen. Die Datei des Quellcodes darf nur von Mitarbeitern zugreifbar sein, die diese Datei im Rahmen ihrer Tätigkeit benötigen.
- Zugriffe auf IMS aus dem TCP/IP-Netz (z. B. aus dem Internet) erfolgen über die OTMA-Schnittstelle (*OpenTransaction ManagerAccess*). Zur Absicherung dieser Verbindung muss über den Parameter *OTMASE=xxx* mindestens *CHECK* (besser *FULL*) sichergestellt werden, dass RACF zur Verifizierung eingesetzt wird. IMS Kommandos werden dabei gegen die Klasse *CIMS*, Transaktionen gegen *TIMS* geprüft. Die Gültigkeit der Verbindung sollte über Profile in der *FACILITY* Klasse in RACF sichergestellt werden.
- Es ist zu überlegen, ob die IMS Programme (Control Region, Message Processing Region, Utilities) zur Erhöhung der Sicherheit über die RACF Klasse *Program* geschützt werden sollen.
- Die IMS Dateien müssen über RACF Dataset Profile so geschützt werden, dass nur Mitarbeiter Zugriff zu den Dateien haben, die sie im Rahmen ihrer Tätigkeit auch benötigen. Anwender von IMS benötigen keinen Zugriff auf die IMS Dateien. Zu schützende Dateien sind z. B.

  - APF-Dateien (Authorized Programming Facility)
  - System-Dateien
  - Anwender-Dateien wie z. B. PSB-, DBD-, ACB- und PGM-LIB

  Der Zugriff auf APF- und System-Dateien darf nur für die STC-User-IDs (*Started Task Control*) und autorisierte Mitarbeiter freigegeben werden. Normale Anwender benötigen keinen Zugriff auf diese Dateien (siehe auch M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
  Der Zugriffsschutz von Anwender-Dateien muss durch RACF Definitionen erfolgen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- MVS Kommandos für IMS sollten über RACF geschützt werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Die Started Tasks sollten über die RACF Klasse *STARTED* abgesichert werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Bei besonders hohen Sicherheitsanforderungen an IMS kann auch der Zugang zur IMS Kontroll-Region generell durch die RACF *Resource Class* APPL auf der Basis des VTAM LU-Namens abgesichert werden. Da jeder

Anwender hierbei entweder als einzelner User oder in Gruppen definiert werden muss, ist zu beachten, dass dadurch ein erhöhter Administrationsaufwand entsteht. Dies gilt besonders für Installationen mit vielen Anwendern.

**CICS**

Die folgenden Empfehlungen gelten für den CICS Transaktionsmonitor. Je nach Einsatzszenario sind in der Regel zusätzliche Sicherheitsmechanismen erforderlich. Weitere Informationen sind in der IBM Dokumentation *CICS RACF Security Guide* zu finden:

- Sollen die CICS-Regions im Modus *Non-Swappable* laufen (PPT-Eintrag im SCHEDnn Parmlib-Member), muss sichergestellt werden, dass die Option *NOPASS* für das Modul DFHSIP im PPT-Eintrag (Program Property Table) **nicht** gesetzt wird. Die Option NOPASS umgeht Passwort- und RACF-Prüfungen.
- Die Started Task User-IDs müssen so definiert werden, wie M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben ist. Die User-IDs von CICS Started Tasks dürfen nicht das Attribut *OPERATIONS* besitzen.
- Die CICS Dateien müssen über RACF Dataset Profile so geschützt werden, dass nur Mitarbeiter Zugriff auf die Dateien haben, die sie im Rahmen ihrer Tätigkeit auch benötigen. Zu schützende Dateien sind z. B.
  - APF-Dateien (Authorized Programming Facility)
  - System-Dateien
  - Anwender-Dateien wie z. B. PSB-, DBD-, ACB- und PGM-LIB
- Der Zugriff auf APF- und System-Dateien darf nur für die STC-User-IDs (*Started Task Control*) und autorisierte Mitarbeiter freigegeben werden. Normale Anwender benötigen keinen Zugriff auf diese Dateien (siehe auch in M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
  Der Zugriff auf Anwender-Dateien muss im Rahmen der RACF Regeln erfolgen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- MVS Kommandos für CICS sollten über RACF geschützt werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Die Aktivierung von RACF für die CICS-Security erfolgt in der SIT (*System Initialization Table*) durch Setzen des Parameters SEC=*YES.* In der SIT kann auch definiert werden, ob Transaktionsschutz, Programmschutz oder Feldschutz von Eingabemasken über RACF aktiviert werden soll. Es muss sichergestellt werden, dass diese Modifikationen nur von autorisierten Mitarbeitern durchgeführt werden können. Dabei ist zu beachten, dass die Auswahl der SIT sowohl über *SYSIN* Eingabe als auch über einen Parameter im *EXEC Statement* der Prozedur (in der *Job Control Language*) definiert werden kann. Das SIT-Modul muss in eine APF-Bibliothek eingestellt und über RACF Profile so geschützt werden, dass nur die für diesen Bereich zuständigen Mitarbeiter Zugriff haben (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Auch die Quell-Datei der SIT darf nur zugreifbar sein für die dazu befugten Mitarbeiter und muss mit entsprechenden RACF Dateiprofilen geschützt werden.
- Die Kommando Security muss bei der Definition der Transaktionen eingeschaltet sein (*CMDSEC Parameter*). Es ist zu überlegen, ob durch SECPRFX=*YES* die Systeme voneinander unterschieden werden sollen. Dies ist empfehlenswert bei verschiedenen CICS-Jobs in einem System.
- Die Prozeduren der CICS Regions stehen auf einer (oder mehreren) Prozedur-Bibliothek(en). Diese müssen durch RACF so geschützt werden, dass nur Mitarbeiter diese Prozeduren verändern können, die im Rahmen ihrer Tätigkeit darauf Zugriff haben müssen. Es ist zu überlegen, ob eine separate *PROCLIB* (mit entsprechender Verknüpfung zu den ande-

ren *PROCLIBs*) das Sicherheitsniveau erhöht und das Missbrauchsrisiko durch getrennte Zugriffsdefinitionen dadurch verringert werden kann.
- Die Anmeldung an CICS muss über die Eingabe von RACF User-ID und Passwort erfolgen. Es ist zu empfehlen, eine Signon-Maske für die Anmeldung an CICS vorzusehen. Für jede CICS Region muss daher ein Default-User in RACF definiert sein. Die in der Default-User-ID im CICS-Segment definierten Vorgaben werden von CICS für alle Terminal Sessions verwendet, bis ein Signon mit der persönlichen User-ID durchgeführt wurde. Es wird empfohlen, die Default-User-ID nur mit sehr geringen Rechten auszustatten.
- Die *General Resource Classes* Txxxxxxx (*Member Class*) und Gxxxxxxx (*Group Class*) sollten für Transaktionssicherheit, die Klassen Cxxxxxxx (*Member Class*) und Vxxxxxxx (*Group Class*) für Kommando Sicherheit aktiviert werden (über das Kommando *SETROPTS*).
- Sicherheitsmechanismen in der Anwendung (Applikation) sollten nur dort implementiert werden, wo keine adäquaten Sicherheitsfunktionen von RACF oder anderen Sicherheitssystemen zur Verfügung stehen.
- Es ist zu überlegen, ob ein Terminalschutz auf Basis der VTAM-LU (Logical Unit) aktiviert werden soll. Diese Maßnahme erhöht den Schutz, bedeutet jedoch mehr Verwaltungsaufwand.
- Der Zugang zu der CICS Region kann über den VTAM ACB-Namen (*Access Control Block*) über RACF kontrolliert werden. Sollte diese Kontrolle eingesetzt werden, empfiehlt es sich, ein Gruppenkonzept aufzubauen, um den Verwaltungsaufwand möglichst gering zu halten.
- Für die CICS Transaktionen und System Kommandos sind unterschiedliche Gruppen zu bilden. Alle CICS Administrations-Transaktionen und alle kritischen CICS Kommandos sollten so geschützt werden, dass nur die Mitarbeiter Zugriff zu diesen Transaktionen haben, die sie im Rahmen von Administrationstätigkeiten auch benötigen. Eine Vertretungsregelung sollte vorhanden sein. Es ist zu überlegen, ob es erforderlich ist, weitere CICS *Resource Classes* einzusetzen (siehe *CICS RACF Security Guide*).
- CICS Systemdefinitionen können entweder über die RCT (*Resource ControlTable*) oder über die CSD (*CICS System Definitions*) vorgenommen werden. Während die ältere RCT noch als Loadmodule via *Assembly* und *Link* erstellt wird, wird die CSD durch den RDO Dialog (*Resource Definition Online*) über die Transaktionen CEDA, CEDB und CEDC als VSAM-Datei erstellt und von CICS eingelesen. In beiden Fällen müssen sowohl die relevanten Dateien als auch die Transaktionen durch RACF Profile so geschützt werden, dass nur CICS-Administratoren Zugriff auf diese Definitionen haben. Hier wird u. a. auch das CICS-DB2 Attachment über das Makro *DB2CONN* definiert, in dem z. B. der Name des DB2 Subsystems, die Berechtigungen auf bestimmte Kennungen oder Relationen zwischen Transaktion, DB2 Plan und Programm festgelegt werden.
  Es ist zu überlegen, ob CEDC (die nur lesende Aktionen durchführt) auch geschützt werden soll. Dies hängt vom Inhalt der Daten ab.

**DB2**

Die folgenden Empfehlungen gelten für das DB2-Datenbanksystem. Je nach Einsatzszenario sind in der Regel zusätzliche Sicherheitsmechanismen erforderlich. Weitere Informationen sind in der IBM Dokumentation *DB2 UDB Administration Guide* zu finden:

- Für jedes DB2-Subsystem muss ein Eintrag in der RACF *Router Table* vorgenommen werden, da diese Einträge standardmäßig nicht mit ausgeliefert werden.
- Die General Resource Class *DSNR* muss über das Kommando SETROPTS aktiviert werden. Die Profile müssen gemäß DB2 Dokumentati-

on definiert und Zugriffe dazu über *PERMIT* Kommandos eingerichtet werden. Vorher sollte ein Gruppenkonzept entwickelt werden, wie es beispielhaft in der IBM Dokumentation *DB2 UDB Administration Guide* beschrieben ist. Ist eine VTAM LU 6.2 Verbindung (*Virtual Telecommunication AccessManagement*) im Einsatz, sollte überlegt werden, ob ein zusätzlicher Schutz über die Klasse *APPCLU* zweckmäßig ist.

- Die DB2 Dateien müssen über RACF Dataset Profile so geschützt werden, dass nur Mitarbeiter Zugriff auf die Dateien haben, die sie im Rahmen ihrer Tätigkeit auch benötigen. Zu schützende Dateien sind z. B

  - System-Dateien
  - Anwender-Dateien als Datenbanken
  - APF-Dateien (Authorized Programming Facility)

  Der Zugriff auf APF- und System-Dateien darf nur für die STC-User-IDs (*Started Task Control*) und autorisierte Mitarbeiter freigegeben werden. Andere Anwender benötigen keinen Zugriff auf diese Dateien (siehe auch M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
  Der Zugriff auf Anwender-Dateien muss im Rahmen der RACF Regeln erfolgen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Der Zugriff auf die Prozedurbibliotheken der DB2 *Started Tasks* ist durch RACF Dateiprofile zu schützen (siehe M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
- MVS Kommandos für DB2 sollten über RACF geschützt werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Die DB2 Started Task User-IDs müssen in der RACF Klasse *STARTED* als *Protected User* definiert werden. Die User-IDs benötigen Zugriffe auf die Dateien der Started Task Prozeduren.
- Alle DB2 Dateien sollten über RACF *Dataset* Profile abgesichert werden, wobei normale Benutzer keinen direkten Zugriff auf die Datenbank haben sollten. Direkte Zugriffe sollten auf die Administratoren beschränkt bleiben.
- Es ist zu empfehlen, keine DB2 *GRANT PUBLIC* Genehmigung auf DB2-Katalog-Tabellen zu erteilen. Statt dessen sollten Zugriffsrechte auf der Ebene von Benutzergruppen vergeben werden.
- Es wird empfohlen, die internen System-Tabellen nur über DB2-Admin Kommandos (GRANT in DB2) zu schützen. Zugriffsrechte auf User-Tabellen sollten über RACF Gruppen vergeben werden. Dabei muss die RACF Gruppe in DB2 durch entsprechende GRANTs autorisiert werden. Die Autorisierung einzelner User-IDs oder (besser) ganzer Gruppen lässt sich durch das RACF Kommando *Permit* realisieren. Alle Sicherheitsdefinitionen sollten möglichst zu RACF verlegt werden.

Prüffragen:

- Wird bei den z/OS-Transaktionsmonitoren ergänzend ein Sicherheitssystem eingesetzt (z. B. RACF)?
- Werden alle Sicherheitsmechanismen für z/OS-Transaktionsmonitore möglichst durch RACF gesteuert und die internen Sicherheitsmechanismen nur dort genutzt, wo es keine adäquaten RACF-Funktionen gibt?
- Werden vor der Inbetriebnahme eines z/OS-Transaktionsmonitors oder eines Datenbanksystems Standards für alle relevanten Definitionen entwickelt?
- Sind die MVS Kommandos für z/OS-Transaktionsmonitore und Datenbanken über RACF geschützt?
- Werden alle DB2 Dateien unter z/OS über RACF Dataset Profile abgesichert?

- Haben nur die Administratoren einen direkten Zugriff auf die DB2-Datenbanken unter z/OS?

# M 2.297 Deinstallation von z/OS-Systemen

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wird ein z/OS-System nicht mehr benötigt, so reicht es nicht, das System einfach auszuschalten. Beim Abbau eines z/OS-Systems oder eines *Parallel-Sysplexes* sollten die folgenden Empfehlungen beachtet werden:

### Festplatten löschen

Alle Festplatten, die sensitive Daten wie Kundendaten enthalten, müssen so gelöscht werden, dass ihr Inhalt nicht mehr reproduziert werden kann. Hierfür kann ein Programm wie ICKDSF eingesetzt werden. Das Löschen kann u. U. auch durch die Herstellerfirma durchgeführt werden. Sind Festplatten, auch einzelne, defekt und müssen deshalb vom Hersteller ausgetauscht werden, ist sicherzustellen, dass die ausgetauschte Festplatte durch den Hersteller vernichtet wird. Dies sollte vertraglich vereinbart werden. Entsprechendes gilt auch für den Austausch eines kompletten Festplattenschranks. Vor der Weitergabe von Datenträgern an Dritte muss in jedem Fall geprüft werden, ob der Schutzbedarf der gespeicherten Daten dies zulässt (siehe auchM 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*).

### Kennungen löschen

Alle Kennungen des deinstallierten Systems müssen gelöscht werden, sofern dies nicht schon automatisch durch den Abbau erfolgt. Wenn ein System aus einem *Parallel-Sysplex* herausgelöst wird, so sind die Kennungen und Aliase auf den anderen Systemen des *Parallel-Sysplex* zu löschen.

Die betroffenen Kennungen müssen aus den Verwaltungssystemen (z. B. Benutzerverwaltung) entfernt werden.

### System-Namen entfernen

Die System-Namen (*SYSIDs*) müssen aus den System-Listen entfernt werden. Falls ein System aus einem *Parallel-Sysplex* genommen wird, muss der System-Name aus den *Sysplex*-Definitionen entfernt werden.

### System entfernen

Das System muss aus dem Passwort-Synchronisierungsverfahren entfernt werden, falls ein solches Verfahren in Betrieb ist (siehe M 2.294 *Synchronisierung von z/OS-Passwörtern und RACF-Kommandos*).

Das System muss aus allen Terminal-Monitor-Programmen, z. B. TPX (*Terminal Productivity Executive*) oder NV/AS (*NetView/Access*), entfernt werden.

Das System muss aus den NJE-Definitionen (*Network Job Entry*) des JES2/3 entfernt werden.

### Berichtswesen

Das Berichtswesen ist darauf zu überprüfen, ob Definitionen entfernt und eventuell Tabellen gelöscht werden müssen.

**Automation**

Vorhandene Automationsverfahren sind darauf zu untersuchen, ob Definitionen angepasst werden müssen.

**Lizenzschlüsselverwaltung**

Da sich durch den Abbau die Anzahl der Systeme reduziert hat, sollte geprüft werden, ob Software-Lizenzen nicht mehr benötigt werden und daher abbestellt werden können.

Prüffragen:

- Werden bei der Deinstallation eines z/OS-Systems alle Festplatten, die sensitive Daten enthalten, so gelöscht, dass ihr Inhalt nicht mehr reproduziert werden kann?
- Austausch defekter Festplatten eines z/OS-Systems beim Hersteller: Gibt es vertragliche Vereinbarungen zur Vernichtung der Festplatten durch den Hersteller?
- Ist sichergestellt, dass alle Kennungen von deinstallierten z/OS-Systemen gelöscht werden?
- Wird bei der Deinstallation von z/OS-Systemen das Berichtswesen darauf überprüft, ob Definitionen entfernt und eventuell Tabellen gelöscht werden müssen?

# M 2.298 Verwaltung von Internet-Domainnamen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Internet-Domainnamen (*Domains*) müssen bei Registrierungsstellen (*Registrars*) angemeldet werden. Eine Registrierungsstelle kann Namen für eine oder mehrere sogenannte Top-Level-Domains (beispielsweise die "klassischen" Domains *.com*, *.org*, *.gov* und die diversen Länder-Domains wie *.de* für Deutschland, *.at* für Österreich und *.ch* für die Schweiz) vergeben. Domains werden jeweils für einen bestimmten Zeitraum registriert. Ist dieser Zeitraum abgelaufen, so muss die Registrierung gegen Zahlung einer Gebühr verlängert werden. Wird die Verlängerung einer Registrierung vergessen, so kann dies unangenehme Folgen haben (siehe G 2.100 *Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen*). Es muss daher sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Organisation benutzt werden, regelmäßig und rechtzeitig verlängert werden. Dazu sollte in jeder Organisation eine Stelle festgelegt werden, die die Verwaltung der Domainnamen bei den verschiedenen Registrierungsstellen koordiniert.

Neben der Verwaltung der Domainnamen und der Sicherstellung der rechtzeitigen Verlängerung der Registrierungen sollten beim Management von Internet-Domainnamen auch folgende Punkte berücksichtigt werden:

**DNS Nameserver**

Bei der Registrierung eines Domainnamens müssen mindestens zwei DNS-Nameserver (*Primary Nameserver*) angegeben werden, die für die Zuordnung von Rechnernamen zu IP-Adressen zuständig sind. Ein Nameserver wird oft vom Internet-Zugangsprovider betrieben, kann aber auch von der Organisation selbst betrieben werden. Bei der Festlegung der Nameserver sollte zumindest darauf geachtet werden, dass die *Primary Nameserver* in verschiedenen Class-C Netzen liegen. Ist dies nicht der Fall, so kann ein Denial of Service Angriff auf den Router, mit dem dieses Netz ans Internet angebunden ist, die komplette Domain lahm legen, da keine Namen aus dieser Domain mehr aufgelöst werden können. Bei hohen Anforderungen an die Verfügbarkeit der Namensauflösung sollten die *Primary Nameserver* idealerweise in verschiedenen Netzen mit Anbindung über unterschiedliche Provider angesiedelt werden.

**Domainnamen**

Zu Anfang des "Internet-Zeitalters" reichte es meist aus, wenn eine Organisation eine einzige Internet-Domain betrieb. Mit der wachsenden Popularität des World-Wide-Web wurde es üblich, nicht nur eine Domain mit beispielsweise dem eigenen Institutionsnamen zu betreiben, sondern auch für bekannte Produkte Domains einzurichten.

Um zu verhindern, dass Domains mit dem Namen eigener Produkte und Dienstleistungen von Anderen registriert werden, die unter dieser Adresse dann eventuell pornographische oder andere anstößige Inhalte verbreiten, die von Besuchern dann mit der eigenen Organisation in Verbindung gebracht werden, sollten soweit möglich nicht nur der eigene Institutionsname und die Namen bekannter eigener Produkte in der korrekten Schreibweise registriert werden, sondern jeweils auch Varianten davon, etwa mit oder ohne Bindestrichen bei zusammengesetzten Namen. Diese Namen sollten unter den ver-

schiedenen "relevanten" Top-Level-Domains (etwa *.de*, *.com*, *.org*, *.info*) registriert werden. Außerdem sollte geprüft werden, ob nicht auch bestimmte falsch geschriebene Varianten (etwa bestimmte "Buchstabendreher") von Produkt- oder Institutionsnamen registriert werden sollten. Der dadurch entstehende Mehraufwand ist gering im Vergleich zu dem Aufwand, gegebenenfalls die "Herausgabe" einer Domain gerichtlich erzwingen zu müssen.

Für solche "sicherheitshalber" registrierten Domains sollte zumindest ein minimales Webangebot eingerichtet werden, das den Domainnamen nennt, auf dem das eigentliche Angebot eingerichtet ist und eine Weiterleitung dort hin anbietet. Gegebenenfalls kann auch einfach der Haupt-Webserver der Organisation über eine entsprechende Namensauflösung auch als Webserver für diese Domain agieren.

**Registrierungsstellen und Registrierungszeiträume**

Für mehrere Top-Level Domains (etwa *.com* und *.org*) existieren verschiedene Registrierungsstellen. Ein Wechsel der Registrierungsstelle ist jederzeit möglich, aber meist mit Kosten verbunden.

Es ist wichtig, für alle registrierten Domains einen Überblick über die jeweilige Laufzeit der Registrierung, den Preis für die Verlängerung und die Bankverbindung der Registrierungsstelle zu haben, um eine rechtzeitige Verlängerung der Registrierung sicher zu stellen.

**Vertragsgestaltung mit Internetdienstleistern**

Wenn die Domains der Organisation nicht in Eigenregie registriert und verwaltet werden, sondern dies über einen Internetdienstfeister geschieht, so muss bei der Vertragsgestaltung darauf geachtet werden, dass die Organisation selbst die Kontrolle über die Domains behält. Dies kann beispielsweise bei einem eventuellen Wechsel des Registrars oder bei der Auflösung von Namensstreitigkeiten von Bedeutung sein.

Für den Fall von Fehlern und Versäumnissen des Dienstleisters im Bezug auf die Verwaltung von Domainnamen sollten entsprechende Regelungen getroffen werden, da in solchen Fällen erheblicher Schaden entstehen kann (siehe G 2.100 *Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen*).

Falls die Nameserver nicht in der Organisation selbst betrieben, sondern bei einem Dienstleister gehostet werden, sollten in den Service-Level-Agreements insbesondere Vereinbarungen über die Anforderungen an die Verfügbarkeit der Nameserver und an Bearbeitungszeiten für Änderungen im DNS der Organisation getroffen werden.

Prüffragen:

- Gibt es eine Stelle, die die Registrierung für alle benutzten Domains regelmäßig und rechtzeitig verlängert?
- Wird dem Domain-Grabbing vorgebeugt?

# M 2.299 Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Da das Sicherheitsgateway für die Sicherheit des Netzes eine zentrale Rolle spielt, ist der sichere und ordnungsgemäße Betrieb besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen (das zu erreichende Sicherheitsniveau) ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für den Betrieb des Sicherheitsgateways formuliert werden, um die übergeordnet und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie beispielsweise IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb des Sicherheitsgateways beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb des Sicherheitsgateways treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Allgemeine Konfigurationsstrategie: Da das Sicherheitsgateway eine zentrale Rolle bei der Absicherung des Netzes spielt, muss es selbst (bzw. die einzelnen Komponenten) besonders sicher konfiguriert sein.
- Regelungen für die Arbeit der Administratoren und Revisoren:
    - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
    - Welche Vorgänge werden müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
    - Gilt für bestimmte Änderungen ein Vieraugenprinzip? Für besonders sicherheitskritische Änderungen an den Einstellungen des Sicherheitsgateway ist dies dringend empfohlen.
    - Nach welchem Schema werden Administrationsrechte vergeben?
- Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils
- Vorgaben für die Installation und Konfiguration einzelner Komponenten des Sicherheitsgateways
    - Vorgehen bei der Erstinstallation

  - Überprüfung der Default-Einstellungen hinsichtlich Sicherheitsgefährdungen
  - Regelungen zur physikalischen Zugriffskontrolle
  - Verwendung und Konfiguration von Konsole und sonstigen Zugriffsarten
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Regelungen zu Erstellung und Pflege von Dokumentation, Form der Dokumentation: Verfahrensanweisungen, Betriebshandbücher
- Vorgaben für den sicheren Betrieb
  - Absicherung der Administration (beispielsweise: Zugriff nur über abgesicherte Verbindungen)
  - Einsatz von Verschlüsselung (Standards, Schlüsselstärken, Einsatzbereiche)
  - Vorgaben zu Passwortnutzung (Passwortregeln, durch Passwörter zu schützende Bereiche, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement
  - Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen
- Protokollierung
  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
- Datensicherung und Recovery
  - Einbindung in das organisationsweite Datensicherungskonzept
- Störungs- und Fehlerbehandlung, Incident Handling
  - Regelungen für die Reaktion auf Betriebsstörungen und technische Fehler (lokaler Support, Fernwartung)
  - Regelungen für Sicherheitsvorfälle
- Notfallvorsorge
  - Einbindung in das organisationsweite Notfallvorsorgekonzept
- Revision und Audit (Verantwortlichkeiten, Vorgehen, Integration in ein übergreifendes Revisionskonzept)

Die Verantwortung für die Sicherheitsrichtlinie liegt beim Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Prüffragen:

- Existiert eine Sicherheitsrichtlinie zum Sicherheitsgateway, in der Anforderungen und Vorgaben zum sicheren Betrieb nachvollziehbar dokumentiert sind?

# M 2.300 Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sollen Komponenten des Sicherheitsgateway außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden. Dies gilt besonders dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben (beispielsweise verkauft) werden oder wenn ein Gerät im Rahmen eines Garantieaustausches oder einer Reparatur an den Hersteller oder eine Service-Firma übergeben wird, aber selbst dann, wenn die Geräte intern weiter verwendet oder verschrottet werden.

Je nach Einsatzzweck der Komponenten können beispielsweise folgende Informationen und Daten auf den Geräten gespeichert sein:

- Konfigurationsdateien, aus denen Informationen über die Netzstruktur der Organisation (wie IP-Adressen, Routing-Tabellen, SNMP-Community Strings, Access-Control-Lists oder ähnliches) entnommen werden können
- Passwortdateien
- Protokolldateien, die sicherheitsrelevante Informationen oder personenbezogene Daten enthalten
- Benutzerdaten, beispielsweise aus Web-Cache- oder E-Mail-Spool-Verzeichnissen
- potentiell gefährliche Dateien (Schadsoftware) aus "Quarantäne-Verzeichnissen"
- Zertifikate und Schlüssel (etwa SSL-Zertifikate bei SSL-Proxies oder Schlüssel für den Zugang per SSH)

Wegen der Sensibilität dieser Informationen ist darauf zu achten, dass die Dateien vor der Außerbetriebnahme oder dem Austausch defekter oder veralteter Geräte gelöscht beziehungsweise unlesbar gemacht werden. Nach dem Löschen der Daten muss überprüft werden, ob das Löschen auch erfolgreich war. Die Vorgehensweise hängt dabei stark von der Art und vom Verwendungszweck des Gerätes ab. In der Sicherheitsrichtlinie für das Sicherheitsgateway sollten hierfür entsprechende Verantwortlichkeiten definiert werden.

Die entsprechenden Dateien sind je nach Gerät und Einsatzzweck eventuell in mehreren unterschiedlichen Verzeichnissen gespeichert, beispielsweise befinden sich bei ALGs die verschiedenen Konfigurationsdateien meist an anderen Stellen als die Cache-Dateien, Spool- oder Quarantäneverzeichnisse. Vor der Außerbetriebnahme sollte daher geklärt werden, welche sicherheitsrelevanten Dateien an welchen Stellen gespeichert sind.

Bei "normalen" Rechnern, die als Komponenten des Sicherheitsgateway eingesetzt waren, sollten die Festplatten mit einem geeigneten Tool so gelöscht werden, dass keine Wiederherstellung der Dateien mehr möglich ist. Die kann beispielsweise dadurch geschehen, dass der Rechner von einem externen Boot-Medium gestartet wird und die Festplatten mit Zufallsdaten überschrieben werden. Dabei ist es empfehlenswert, den Überschreibvorgang mehrfach zu wiederholen.

Bei Appliances hängt die Vorgehensweise davon ab, ob in dem Gerät eine Festplatte eingebaut ist oder ob die Daten in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit

der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Sind auf dem Gerät besonders sicherheitskritische Informationen gespeichert und kann nicht mit hinreichender Sicherheit gewährleistet werden, dass die Daten wirklich gelöscht sind, so kann es erforderlich sein, die Speicherbausteine oder Festplatten physisch zu zerstören bzw. unbrauchbar zu machen.

Neben den Informationen, die auf dem Gerät selbst gespeichert sind sollte auch überprüft werden, ob auf den Backup-Medien sensitive Informationen enthalten sind. Falls es nicht aus anderen Gründen (beispielsweise Archivierung, Aufbewahrungspflicht aufgrund gesetzlicher Regelungen) erforderlich ist, die Backup-Medien aufzubewahren, so sollten die Medien nach der Außerbetriebnahme des Gerätes ebenfalls gelöscht werden.

Oft sind die Komponenten des Sicherheitsgateways von außen mit IP-Adressen, Hostnamen oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Prüffragen:

- Werden bei Außerbetriebnahme oder Ersatz des Sicherheitsgateways oder einer der Komponenten alle sicherheitsrelevanten Informationen auf den Geräten sicher gelöscht?
- Sind die Verantwortlichkeiten für den Ausmusterungsprozess des Sicherheitsgateways in der Sicherheitsrichtlinie definiert?
- Sofern die Backup-Medien von Komponenten des Sicherheitsgateways nicht mehr benötigt werden: Werden die sensitiven Informationen auf den Backup-Medien sicher gelöscht?
- Werden eventuell vorhandene Beschriftungen auf den Komponenten des Sicherheitsgateway vor der Ausmusterung entfernt?

# M 2.301 Outsourcing des Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Der Aufbau und Betrieb eines Sicherheitsgateway bedeutet einen nicht unerheblichen finanziellen und personellen Aufwand. Trotzdem kann auf ein Sicherheitsgateway nicht verzichtet werden, wenn LANs an nicht vertrauenswürdige Netze (insbesondere an das Internet) angeschlossen werden sollen. Oft wird daher überlegt, den Betrieb einer Sicherheitsgateway einem externen Dienstleister zu überlassen. Dabei sind verschiedene Varianten denkbar:

- **Betrieb vor Ort, Administration durch Externe**
  Das Sicherheitsgateway wird innerhalb der Räumlichkeiten des Auftraggebers betrieben und administriert. Damit wird ein externer Sicherheitsgateway-Administrator beauftragt.
  Diese Lösung bringt oft nicht einmal einen Kostenvorteil. Nachteilig ist hier, wie bei allen anderen Lösungen, dass Externe sicherheitsrelevante Aufgaben übernehmen und intern kein entsprechendes Wissen aufgebaut wird, so dass eine wirksame Kontrolle äußerst schwierig ist.
- **Remote Management**
  Das Sicherheitsgateway wird innerhalb der Räumlichkeiten des Auftraggebers aufgestellt und betrieben, aber über Fernzugriff administriert.
  Dabei ist eine starke Authentisierung sowie die Verschlüsselung der Verbindung unerlässlich. Die Dienstleister sollten nur auf die Sicherheitsgateway selber zugreifen dürfen, nicht auf weitere Daten und Verzeichnisse im LAN. Wie im Baustein B 4.4 *VPN* beschrieben, sollten weitere organisatorische Vorkehrungen getroffen werden, um einen möglichen Missbrauch einzudämmen. Dazu gehören beispielsweise

  - das Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
  - das Sperren des Fernwartungszugangs im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
  - Einschränkung der Rechte der externen Administratoren, so dass z. B. die Sicherheitsrichtlinien nicht niedriger eingestellt werden können,
  - "Zwangslogout" bei Leitungsunterbrechung; wird die Verbindung zwischen Fernwartungsstelle und PC-Gateway auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch ein "Zwangslogout" beendet werden.
- **Hosting**
  Bei dieser Lösung wird die Sicherheitsgateway beim Dienstleister aufgestellt und gepflegt. Vom internen LAN zum Sicherheitsgateway muss dabei eine feste, geschützte Verbindung vorhanden sein.
  Hierbei muss eine hohe Verfügbarkeit sowohl der Verbindung als auch des Sicherheitsgateway-Systems gewährleistet werden, da bei deren Ausfall keine externen Verbindungen mehr möglich sind.
  Im Allgemeinen sollen auch weitere Komponenten, die der Kommunikation zwischen geschütztem und externem Netz dienen, eingesetzt werden. Dazu gehören z. B. Informationsserver für die Bereitstellung von Informationen an interne oder externe Benutzer, Mailserver und DNS-Server. Diese werden üblicherweise in einer DMZ des Sicherheitsgateway aufgestellt (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway*). In diesem Fall müssten sie also beim externen Dienstleister betrieben werden. Dies kann die Kosten erheblich in die Höhe treiben.

Sowohl beim Remote Management als auch beim Hosting eines Sicherheitsgateways sollte eine Ausweich-Verbindung zum Dienstleister vorhanden sein, um bei einem Ausfall der Hauptanbindung die Administration bzw. die Internet-Anbindung zu gewährleisten. Für die Ausweich-Verbindung muss sichergestellt sein, dass für diese Verbindung mindestens das selbe Sicherheitsniveau gewährleistet ist, wie für die Hauptverbindung.

Bei den verschiedenen Dienstleistungsangeboten ist zu hinterfragen,

- wie viel technisches, aber auch wie viel sicherheitsrelevantes Wissen beim Anbieter vorhanden ist und wie dieses aktuell gehalten wird,
- ob und wie lange das Sicherheitsgateway-System unbeaufsichtigt betrieben wird,
- wie der Personaleinsatz gesteuert wird, da ja üblicherweise mehrere Kunden betreut werden.

Auch wenn die Betreuung des Sicherheitsgateways einem Dienstleister überlassen wird, muss trotzdem intern eine Sicherheitsgateway-Sicherheitspolicy erstellt werden, die mit den Sicherheitszielen der Organisation abgestimmt ist (siehe auch M 2.71 *Festlegung einer Policy für ein Sicherheitsgateway*). Beim Outsourcing eines Sicherheitsgateways sollte in den Service-Level Agreements insbesondere schriftlich fixiert werden,

- welche Reaktionszeiten bei Ausfällen oder Angriffen gewährleistet werden müssen,
- welche Verfügbarkeit zu gewährleisten ist (Performance, maximale Ausfallrate),
- was protokolliert werden darf bzw. muss,
- welche Sicherheitsmaßnahmen gewährleistet werden müssen. Dazu gehören insbesondere alle in Baustein B 3.301 *Sicherheitsgateway (Firewall)* aufgeführten Maßnahmen.

Für das Outsourcing einer so sicherheitskritischen Komponente wie dem Sicherheitsgateway muss in jedem Fall der Baustein B 1.11 *Outsourcing* angewandt werden. Beim Dienstleister sollte idealerweise ebenfalls ein vollständiges Informationssicherheitsmanagement-System z. B. basierend auf IT-Grundschutz existieren. Es wird empfohlen, beim Outsourcing des Sicherheitsgateways zumindest zu prüfen, ob das Sicherheitsmanagement des Dienstleisters den Anforderungen des Bausteins B 1.11 *Outsourcing* genügt.

Prüffragen:

- Betrifft das Remote Management des Sicherheitsgateways: Ist der Zugriff durch den Dienstleister lediglich auf die relevanten Komponenten des Sicherheitsgateway eingegrenzt?
- Betrifft das Hosting von Sicherheitsgateways: Wird ausschließlich eine geschützte Verbindung zum Sicherheitsgateway des Dienstleisters verwendet?
- Bestehen schriftliche Vereinbarungen über die Service-Level-Agreements für das Outsourcing des Sicherheitsgateways?

# M 2.302 Sicherheitsgateways und Hochverfügbarkeit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Sicherheitsgateway sollte immer die einzige Schnittstelle zwischen dem externen und dem zu schützenden Netz darstellen. Damit stellt natürlich das Sicherheitsgateway einerseits einen potentiellen Flaschenhals und zum anderen eine mögliche Bruchstelle für den gesamten Netzverkehr einer Organisation dar. Somit werden an die Verfügbarkeit von Sicherheitsgateways häufig hohe Anforderungen gestellt.

Die wichtigsten Komponenten eines Sicherheitsgateways sollten somit redundant ausgelegt werden. Dies sind vor allem diejenigen Komponenten, die zum Abruf oder zum Versand von Informationen unbedingt überquert werden müssen. In diese Kategorie fallen in der Regel Paketfilter, Application-Level-Gateway und evtl. VPN-Komponenten. Bei anderen Komponenten (z. B. Virenscanner oder Intrusion-Detection-System) muss die Bedeutung für die Sicherheit des zu schützenden Netzes im Einzelfall betrachtet werden.

Es gibt verschiedene Möglichkeiten, die Verfügbarkeit von Komponenten eines Sicherheitsgateways zu steigern:

**Cold-Standby:**

Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht in Betrieb ist. Wenn das erste System ausfällt, kann das Ersatzsystem manuell hochgefahren und ins das Sicherheitsgateway integriert werden.

| Vorteile einer Cold-Standby Lösung | Nachteile einer Cold-Standby Lösung |
|---|---|
| - Der Aufwand zur Neuinstallation bzw. zum Neuaufbau eines Sicherheitsgateways ist relativ gering.<br>- Die geringe Komplexität des Sicherheitsgateways erschwert Fehlkonfigurationen. | - Zum bestehenden System muss ein zweites System vorgehalten werden und ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden.<br>- Das Cold-Standby-System kann Fehlfunktionen nicht selbständig erkennen und muss manuell aktiviert werden. Es liegt in der Verantwortung der Administratoren, die Funktion des Wirksystems permanent zu überwachen und im Notfall einzuschreiten.<br>- Je nach eingesetztem Produkt erfordert das Hochfahren einer Komponente des Sicherheitsgateways die Anwesenheit eines Administrators, da manche Systeme ohne Benutzerinteraktion über Tastatur nicht in den Betriebszustand starten. Das Einschalten von Komponenten über eine web- |

| Vorteile einer Cold-Standby Lösung | Nachteile einer Cold-Standby Lösung |
|---|---|
| | gesteuerte Steckdose ist in diesem Fall ausgeschlossen. |

Tabelle 1: Vor- und Nachteile einer Cold-Standby Lösung

**Hot-Standby:**

Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem (meist mit der gleichen Konfiguration wie das im Regelbetrieb befindliche System) bereit. Dieses läuft aber ständig parallel mit, wobei eine Komponenten die andere überwacht. Bei einer Fehlfunktion kann dann das Ersatzsystem unmittelbar die Funktion des Wirksystems übernehmen. Dies kann automatisiert erfolgen oder auch nach Benutzerinteraktion. Eine Benutzerinteraktion kann verhindern, dass eine Umschaltung auf das Hot-Standby-System - die zusätzliche Komplikationen mit sich bringen kann - bei extrem kurzen Ausfällen erfolgt.

Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand der wichtigsten Komponenten beim Hot-Standby-Betrieb des Sicherheitsgateways in möglichst kurzen Zeitabständen überprüft werden.

| Vorteile einer Hot-Standby Lösung | Nachteile einer Hot-Standby Lösung |
|---|---|
| - Es ist keine Interaktion durch den Administrator an der Konsole notwendig.<br>- Da die Funktionen des ausgefallenen Systems von der Ersatzkomponenten automatisch übernommen wird, gibt es keine oder nur kurze Ausfallzeiten. | - Gegenüber Cold-Standby wird das Sicherheitsgateway sehr komplex, da alle beteiligten Komponenten durch zusätzliche Überwachungskomponenten ständig auf korrekte Funktion überprüft werden müssen.<br>- Für jede relevante Komponente des Sicherheitsgateways muss eine eigene Überwachungskomponente beschafft und betreut werden. |

Tabelle 2: Vor- und Nachteile einer Hot-Standby Lösung

**Parallelbetrieb:**

Bei einem Parallelbetrieb arbeiten zwei oder mehr Sicherheitsgateways ständig nebeneinander im Wirkbetrieb. Durch einen Parallelbetrieb wird nicht nur eine Lastverringerung und Performancesteigerung erreicht, vielmehr verringern sich auch die Probleme bei Ausfällen. Je nach gewählter Lastverteilungsmethode kann ein System im Fehlerfall die Aufgaben des gerade nicht zur Verfügung stehenden Systems übernehmen. Daraus resultiert natürlich ein kurzfristiger Performance-Verlust, aber die Funktionalität bleibt vollständig erhalten.

Dabei muss allerdings sichergestellt sein, dass alle Systeme konsistent gehalten werden. Bei Sicherheitsgateways muss hier vor allem auf korrekte Zeitsynchronisierung und die Konsistenz der Regelbasis geachtet werden. Außerdem muss gewährleistet sein, dass ein- und ausgehende Anfragen immer von den selben Komponenten bearbeitet werden, da sonst evtl. Verbindungen abgebrochen werden. Dies betrifft besonders Application-Level-Gateways und Paketfilter mit Stateful-Inspection-Funktion.

Beim Parallelbetrieb sind zwei Varianten zu unterschieden:

**Statischer Parallelbetrieb**

Bei dieser Variante ändert sich die Konfiguration (insbesondere die Routing-Informationen) der Komponenten des Sicherheitsgateways nicht. Eine Variante des statischen Parallelbetriebs könnte beispielsweise darin bestehen, dass über die parallelen Komponenten des Sicherheitsgateways unterschiedliche Dienste geleitet werden, also z. B. HTTP über einen Kommunikationsstrang und SMTP über einen parallelen Kommunikationsstrang. Diese Konfiguration erhöht zwar die Performance des Gesamtsystems, ist aber beim Ausfall einzelner Komponenten problematisch, da die Komponenten unterschiedlich konfiguriert sind und nicht ohne Weiteres durch die jeweils parallele Komponente ersetzt werden können. Aus diesem Grund ist von einer solchen Struktur und Konfiguration des Sicherheitsgateways in der Regel abzuraten.

**Dynamischer Parallelbetrieb/Loadbalancing**

Bei dieser Betriebsart wird die Konfiguration der Komponenten des Sicherheitsgateways den Performanceanforderungen im Betrieb angepasst. Ein Beispiel hierfür ist das Loadbalancing, bei dem Datenströme in Abhängigkeit von der Auslastung der an der Kommunikation beteiligten Komponenten geroutet werden.

Unbedingt zu beachten ist beim Loadbalancing, dass sich durch die automatischen Konfigurationsänderungen auf den beteiligten Komponenten keine Änderungen des Sicherheits-Regelwerks für das gesamte Sicherheitsgateway ergeben.

Loadbalancing kann Teil einer High-Availibility-Lösung (**HA-Lösung**) sein. Bei einer HA-Lösung wird die Verfügbarkeit von Komponenten des Sicherheitsgateways überwacht und es werden beim Ausfall ggf. Ersatzsysteme genutzt, die den Ausfall kompensieren sollen. Das oben angesprochene Loadbalancing dient in diesem Zusammenhang eigentlich nur der Performancesteigerung und führt alleine noch nicht zu Hochverfügbarkeit, es muss zusätzlich dafür gesorgt werden, dass bei einem Systemausfall die Ersatzsysteme den Ausfall automatisch ohne Zutun des Administrators auffangen. Eine ständige Überwachung der HA-Komponenten ist dabei ebenso wichtig wie ein automatisches Fail-Over im Bedarfsfall.

Vor- und Nachteile einer HA-Lösung sind mit denen eines Hot-Standby-Systems zu vergleichen. Vorteilhaft gegenüber Hot-Standby ist zusätzlich jedoch, dass sämtliche Komponenten des Sicherheitsgateways genutzt werden und sich somit eine Lastverteilung ergibt, die die Verfügbarkeit des Sicherheitsgateways sicherstellen kann.

**Anforderungen an HA-Lösungen:**

An eine HA-Lösung sollten folgende Forderungen gestellt werden:

- Auch nach einem automatischen Fail-Over muss das Sicherheitsgateway die Sicherheitsanforderungen der Sicherheitsleit- bzw. -richtlinie erfüllen ("Fail safe" bzw. "Fail secure").
- Die HA-Realisierung darf den Betrieb des Sicherheitsgateways bzw. dessen Sicherheitsfunktionen nicht behindern.
- Mindestens Paketfilter und Application-Level-Gateway sollten hochverfügbar ausgelegt werden, da eine Kommunikation bei einem Ausfall der Komponenten in der Regel nicht mehr möglich ist. Ähnliches gilt für VPN-Komponenten.

- Es sollten zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz bestehen, z. B. zwei Internetzugänge von unterschiedlichen Providern.
- Interne und externe Router müssen redundant ausgelegt sein, z. B. unter Verwendung von Protokollen wie "Virtual Router Redundancy Protocol" (VRRP) oder das proprietäre "Hot Standby Routing Protocol" (HSRP).
- Die Funktionsüberwachung sollte anhand einer Vielzahl von Parametern erfolgen und sich nicht auf ein einzelnes Kriterium verlassen (wie z. B. eine einfache Erreichbarkeitsprüfung durch Testen der Verfügbarkeit der Netzschnittstelle ("ping")). Ist eine Komponente mittels "ping" erreichbar, könnte beispielsweise überprüft werden, ob die konfigurierten Dienste in der intendierten Art und Weise arbeiten.
- Fehlkonfigurationen bei Inbetriebnahme oder Fehlfunktionen einer Komponente im Wirkbetrieb werden bei HA-Lösungen evtl. nicht sofort sichtbar, da Funktionen teilweise von der parallel installierten Komponente übernommen werden. So z. B. fällt es unter Umständen nicht sofort auf, wenn auf einem ALG die Filterung auf aktive Inhalte ausgeschaltet ist und die Anfragen vom korrekt konfigurierten System bearbeitet werden. Deshalb ist eine regelmäßige Kontrolle der Protokolldateien und der Warnmeldungen der HA-Lösung wichtig.

Besonders einfach ist eine HA-Lösung dann, wenn nur ein einstufiger Aufbau bestehend aus einem Paketfilter hochverfügbar ausgelegt werden soll. Viele kommerzielle Produkte bieten hierfür eine einfache Lösung, die im Wesentlichen in der Aktivierung einer entsprechenden HA-Option in der Administrationsoberfläche besteht.

Aufwändiger ist eine HA-Lösung bei mehrstufigen Sicherheitsgateways (z. B. zusammengesetzt aus Paketfiltern und Application-Level-Gateway). Hier muss jede Komponente hochverfügbar ausgelegt sein, was einen erheblichen Mehraufwand bedeutet. In der Regel müssen hier neben der Überwachungsfunktion noch dynamische Routingprotokolle (z. B. "Open Shortest Path First", OSPF) verwendet werden, die den Netzverkehr je nach Bedarf in die richtige Richtung lenken.

Dynamische Routing-Protokolle sind jedoch aus Sicht der Sicherheit nicht unproblematisch. Zu den Problemen siehe auch G 5.51 *Missbrauch der Routing-Protokolle* und M 5.112 *Sicherheitsaspekte von Routing-Protokollen*. Sollen zur Realisierung einer HA-Lösung dynamische Routing-Protokolle eingesetzt werden, so sollte im Rahmen einer ergänzenden Sicherheitsanalyse geprüft werden, ob das erforderliche Sicherheitsniveau noch erreicht wird.

In der P-A-P-Kette eines mehrstufigen Sicherheitsgateways muss eine Komponente die Überwachungsfunktion übernehmen. Diese Komponente entscheidet, ob der P-A-P-Strang funktionsfähig ist oder nicht. Für diese Aufgabe bietet sich eine eigenständige Überwachungskomponente an, die für nichts anderes als die Funktionskontrolle zuständig ist.

Ist die Integration einer eigenständigen Überwachungskomponente nicht möglich, so bietet es sich an, dem Application-Level-Gateway diese Aufgabe zu übertragen. Dies bietet zum einen den Vorteil, dass viele Funktionen des Sicherheitsgateways auf dem ALG implementiert sind, also von der Überwachungssoftware dann lokal ausgewertet werden können. Zum anderen ist das ALG oftmals an zentraler Stelle in das Sicherheitsgateway integriert, bietet also einen direkten Zugang zu den anderen Komponenten des Sicherheitsgateways.

Problematisch ist allerdings, dass ALGs oftmals das Aufspielen von Fremdsoftware zu verhindern versuchen, um eine Kompromittierung des Systems zu verhindern. Tatsächlich ist natürlich nicht auszuschließen, dass die eingesetzte Überwachungssoftware fehlerbehaftet ist und die Sicherheit des ALGs stark herabsetzt.

**Ergänzende Sicherheitsanalyse**

Hochverfügbarkeitslösungen sind immer auf spezielle Anforderungen zugeschnitten und Mischformen aus den oben beschriebenen Typen sind durchaus denkbar. Grundsätzlich wird für denn Fall, dass die Anforderungen an die Verfügbarkeit des Sicherheitsgateways eine Hochverfügbarkeitslösung notwendig erscheinen lassen, eine ergänzende Sicherheitsanalyse dringend empfohlen.

Prüffragen:

- Leitet sich die Entscheidung zur Erreichung der Hochverfügbarkeit aus der Sicherheitsrichtlinie der Organisation ab?
- Sind alle Komponenten des Sicherheitsgateways redundant ausgelegt?
- Ist der Anschluss des externen Netzes redundant ausgelegt?
- Erfolgt die Funktionsüberwachung der Systeme sowohl auf Verfügbarkeit der Netzwerkschnittstellen als auch auf die konfigurierten Dienste?
- Entspricht die Konfiguration der Ausweichsysteme der Konfiguration der Live-Systeme?
- Ist sichergestellt, dass bei einem automatischen Fail-Over das Sicherheitsniveau nicht sinkt?

# M 2.303 Festlegung einer Strategie für den Einsatz von Smartphones, Tablets oder PDAs

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Bevor in einer Organisation PDAs eingesetzt werden, muss festgelegt sein, welche generelle Strategie die Organisation im Hinblick auf die Nutzung der Geräte einnimmt. Insbesondere sind dafür die folgenden Fragen zu beantworten:

- Für welche Anwendungen sollen die PDAs eingesetzt werden?
- Werden den Mitarbeitern dienstliche PDAs zur Verfügung gestellt?
- Wird die Nutzung privater PDAs der Mitarbeiter erlaubt oder sogar offiziell unterstützt?

Insbesondere die Frage, für welche Zwecke PDAs eingesetzt werden sollen, ist für die späteren Entscheidungen wichtig, denn sie kann einen entscheidenden Einfluss auf die Auswahl anzuschaffender Geräte haben und muss in jedem Fall bei der Formulierung der Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung berücksichtigt werden.

### Klassifikation der Daten

Jeder Benutzer und jede Institution sollte sich Gedanken darüber machen, welche Daten auf einem PDA gespeichert werden dürfen und welchen Schutzbedarf diese haben. In einem Unternehmen oder einer Behörde sollte dies nicht nur für Daten auf PDAs, sondern generell geklärt werden. So gibt es in Anwendungsfeldern und Geschäftsprozessen Daten, die einen höheren Schutzbedarf haben oder die besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten.

Daher sollten in einer Institution alle Arten von Daten danach kategorisiert sein, wie schutzbedürftig sie sind und welche Beschränkungen im Umgang mit ihnen beachtet werden sollten (siehe hierzu auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Damit die Mitarbeiter mit diesen Einstufungen auch sinnvoll umgehen können, empfiehlt es sich, diesen hierzu leicht verständliche Tabellen und Beispiele an die Hand zu geben, in denen erläutert ist, welche Arten von Daten auf den verschiedenen IT-Systemen oder Anwendungen gespeichert oder verarbeitet werden dürfen und auch, an wen diese weitergegeben werden dürfen.

### Nutzung von privaten PDAs

Aufgrund einer unzureichenden Ausstattung oder eines hohen Benutzerdruckes kann es vorkommen, dass private PDAs für dienstliche Zwecke benutzt werden. Das Sicherheitsmanagement bzw. die IT-Verantwortlichen sollten aber auf jeden Fall sicherstellen, dass auch die private Nutzung innerhalb der Institution nicht "wild" erfolgt, sondern klar geregelt ist. Sollen PDAs nur für Anwendungen wie Termin- und Adressverwaltung oder für E-Mail-Kommunikation eingesetzt werden, so kann die Nutzung privater PDAs normalerweise erlaubt werden, wenn keine sonstigen Gründe dagegen sprechen.

Falls die PDAs für eine Anwendung eingesetzt werden sollen, aus der sich für die Geräte ein hoher Schutzbedarf ergibt, so ist es sehr fraglich, ob dafür die Nutzung privater PDAs zugelassen werden sollte. Der Grund dafür ist insbesondere, dass private Geräte weitgehend dem Einfluss der zentralen Konfiguration und Administration entzogen sind und es deswegen praktisch keine Möglichkeit gibt, für die Geräte ein akzeptables Sicherheitsniveau zu gewährleisten. Es wird dringend empfohlen, in diesem Fall keine Nutzung privater PDAs zuzulassen.

Bei der Entscheidung sollte auch berücksichtigt werden, dass die Entscheidung, private PDAs zuzulassen, auch Auswirkungen auf die spätere IT-Strategie einer Organisation haben kann.

**Beispiel:**

In einem Unternehmen wurden zwar keine PDAs für die Mitarbeiter angeschafft, die Mitarbeiter wurden aber dennoch bei der Beschaffung privater Geräte und der Anbindung an die Arbeitsplatz-PCs beraten. Als das Unternehmen die PCs von Windows NT nach Windows 2000 migrierte, stellte sich heraus, dass es unter Windows 2000 keine passenden Treiber für die vorhandenen PDAs existierten. Durch die massiven Benutzerbeschwerden stand das Unternehmen vor der Wahl, den Benutzern neue PDAs zu finanzieren oder diesen weiter NT-basierte PCs zur Verfügung zu stellen.

Wenn ein Verbot ausgesprochen wird, private PDAs für Dienstzwecke zu benutzen oder sie in das Büro mitzubringen, sollte immer bedacht werden, dass solche Verbote überwacht werden müssen und dass sie auch ineffektiv sein können.

Die Entscheidung sollte zusammen mit den Entscheidungsgründen dokumentiert und den Mitarbeitern auf geeignete Art und Weise kommuniziert werden.

Prüffragen:

- Gibt es eine generelle Strategie für die Nutzung von PDAs?
- Ist festgelegt, welche Daten auf PDAs gespeichert werden dürfen?
- Nutzung privater PDAs: Ist die private PDA-Nutzung innerhalb der Institution klar geregelt?
- Wird beachtet, dass Verbote bezüglich privater PDAs zu überwachen sind und Konsequenzen bei Nichteinhaltung folgen müssen?

# M 2.304 Sicherheitsrichtlinien und Regelungen für die Nutzung von Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Wenn in einer Institution entschieden wurde, PDAs einzusetzen, so müssen diese in die allgemeine Sicherheitsstrategie eingebunden werden.

Bei der Nutzung von PDAs gibt es eine Vielzahl von Möglichkeiten, diese vor Missbrauch zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben werden. Jede Institution sollte sich die Möglichkeiten und Risiken des PDA-Einsatzes bewusst machen. Hierbei sollten zwei Sicherheitsaspekte im Vordergrund stehen:

- die Sicherheit der auf PDAs gespeicherten Daten und
- die Auswirkung der PDA-Nutzung auf die Sicherheit anderer IT-Systeme innerhalb einer Institution.

Aufbauend auf die PDA-Sicherheitsrichtlinie sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von PDAs erstellt werden.

**Schutz vor Missbrauch**

Ein PDA hat nicht nur für den Besitzer den Vorteil, leicht zu transportieren und unauffällig zu verwahren zu sein, sondern auch für einen Dieb. Daher sollte auch ein PDA stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

Praktisch alle Varianten von PDAs und Organizern lassen sich durch PINs oder Passwörter gegen unbefugten Zugriff absichern. Leider sind nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher, wie es wünschenswert wäre. Daher sollten sich PDA-Benutzer informieren, wie zuverlässig die vorhandenen Sicherheitsmechanismen sind, z. B. über das Internet.

Solange keine besseren Sicherheitstools installiert sind, sollten aber auf jeden Fall die vorhandenen Sicherheitsmechanismen genutzt werden (siehe auch M 4.228 *Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs*). Alle Benutzer sollten sich aber über deren Wirkung und insbesondere deren Grenzen im Klaren sein. Dabei sollten die Passwörter und PINs sorgfältig ausgewählt werden, also auch lang genug sein, damit sie nicht einfach überwunden werden können. Die Passwörter dürfen keinesfalls zusammen mit dem PDA aufbewahrt werden.

**Sensibilisierung der Benutzer**

Alle PDA-Benutzer sollten nicht nur über die Vorteile von PDAs aufgeklärt werden, sondern auch über potentielle Risiken und Probleme bei der Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen.

Da auch für die Betriebssysteme von PDAs (beispielsweise Palm OS, Windows CE bzw. Windows Mobile, Symbian OS) immer wieder neue Sicherheitslücken offengelegt werden, sollte sich das Sicherheitsmanagement regelmä-

ßig über aktuelle Risiken informieren. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die neu bekanntgewordenen Gefahren zu informieren und damit auch zu sensibilisieren.

**Regelungen zur PDA-Nutzung**

**Allgemeine Regelungen**

Auf einem PDA sind Daten in der Regel schlechter geschützt als auf IT-Systemen innerhalb der Organisation. Unabhängig davon, ob privat oder dienstlich angeschaffte PDAs genutzt werden, sollte der Arbeitgeber daher schriftlich regeln,

- welche Daten nicht auf einem PDA gespeichert werden dürfen,
- dass Daten nicht überall eingegeben bzw. abgerufen werden sollten, da sie dabei unter Umständen mitgelesen werden können,
- wie, wann und durch wen Datensicherungen des PDAs durchzuführen sind,
- unter welchen technischen Einsatzbedingungen die PDAs eingesetzt werden dürfen. Hierzu gehören vor allem die Festlegung von Sicherheitsmaßnahmen, die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der betroffenen IT-Systeme.

Ein PDA sollte möglichst nicht unbeaufsichtigt bleiben. Falls ein PDA in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein PDA stellt einen Wert dar, der potentielle Diebe anlocken könnte.

Wird ein PDA in fremden Büroräumen benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten.

In fremden Räumlichkeiten wie Hotelzimmern sollte ein PDA nicht ungeschützt liegen gelassen werden. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

**Nutzung von privaten PDAs**

Bei der Nutzung von privaten PDAs in einer Behörde oder einem Unternehmen sind unter anderem die folgenden Punkte zu regeln:

- Die sinnvolle Nutzung von PDAs erfordert im Allgemeinen eine Synchronisation mit einem PC, beispielsweise für Terminkalender, Adressbücher, E-Mail-Unterstützung und mehr. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird, und wer die Installation vornimmt. Dies sollte nicht den Benutzern selbst überlassen werden.
- Es muss geklärt werden, inwieweit der Benutzer-Support bei Problemen, die sich aus der Nutzung von privaten PDAs ergeben, Hilfestellung leistet. Ebenso sollte im Vorfeld abgesprochen werden, wie private PDAs in die IT-Strategie der Institution eingebunden werden.

**Nutzung von dienstlichen PDAs**

Bei der Nutzung von dienstlichen PDAs sind unter anderem die folgenden Punkte zu regeln:

- Es muss geklärt werden, ob dienstliche PDAs auch mit privaten PCs synchronisiert werden dürfen. Dies erleichtert einerseits Terminabstimmun-

gen, andererseits könnte dadurch Schadsoftware in die dienstlichen Systeme eingeschleppt werden und interne Dokumente könnten auf die privaten PCs gelangen.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den PDAs umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von PDAs sollte geregelt werden.

**Einbindung in andere Sicherheitslösungen**

Bei der Benutzung von PDAs muss nicht nur überlegt werden, ob der Einsatz von Sicherheitssoftware zum Schutz des PDAs selber sinnvoll ist, sondern auch, wie der PDA mit der Sicherheitssoftware der Einsatzumgebung zusammenarbeitet. Dazu zwei Beispiele:

- Der Benutzer liest und schreibt auf seinem Desktop-PC häufig E-Mails, die verschlüsselt bzw. signiert sind. Außerdem möchte er seinen PDA nutzen, um unterwegs E-Mail zu bearbeiten. Mit verschlüsselten bzw. signierten Mails kann er aber aus verschiedenen Gründen Probleme bei der Weiter- verwendung auf dem PDA bekommen. So gibt es beispielsweise bisher nur sehr wenige Verschlüsselungs- bzw. Signaturanwendungen, die sowohl mit den einschlägigen Mailprogrammen auf Office-Systemen als auch auf PDAs kompatibel sind. Bei solchen Anwendungen werden außerdem oft Chipkarten oder andere Sicherheitstoken als sicherer Speicherplatz für die benötigten kryptographischen Schlüssel eingesetzt. Nur die wenigsten PDAs lassen sich aber um Chipkarten-Leseeinrichtungen erweitern. Viele PKI-Anwendungen arbeiten außerdem serverbasiert, benötigen also Zugriff auf einen Server, um beispielsweise Zertifikate überprüfen oder öffentliche Schlüssel von Kommunikationspartnern abrufen zu können.
- Im Unternehmen werden alle Daten, sowohl auf den Clients als auch den Servern, ausschließlich verschlüsselt gespeichert. Wenn Benutzer nun interne Daten auf PDAs transferieren wollen, kann zum einem passieren, dass sie unterwegs feststellen, dass sie zugriffsgeschützte Dateien geladen haben, die sie auf dem PDA nicht lesen können. Dies ist der für die Vertraulichkeit der Daten bessere Fall. Typischerweise werden die auf den PDA übertragenen Daten dort nämlich nicht oder nur schwach verschlüsselt, so dass sie weniger stark geschützt sind als auf den internen Systemen.

Auch solche Fälle, also die Einbindung von PDA-Applikationen in andere Sicherheitssoftware im Unternehmen, muss daher unbedingt in der PDA-Sicherheitsrichtlinie geregelt werden, um zu vermeiden, dass durch die PDA-Nutzung das festgelegte Sicherheitsniveau reduziert wird.

**Wo nötig: Nutzungsverbot von PDAs**

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von PDAs in allen oder bestimmten Bereichen einer Behörde oder eines Unternehmens eingeschränkt werden sollte. Dies kann z. B. dort sinnvoll sein, wo das Mitschneiden von Gesprächen oder das Fotografieren unterbunden werden soll.

Wenn die Sicherheitsrichtlinie der Institution es nicht zulässt, dass fremde IT-Systeme wie beispielsweise PDAs mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmä-

ßig kontrolliert werden. Für die Besucher sollte in diesem Fall eine Möglichkeit geschaffen werden, mitgebrachte Mobiltelefone, PDAs oder Notebooks sicher aufzubewahren. Beispielsweise können an den Eingängen Schließfächer zur Verfügung gestellt werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für Smartphones, Tablets und PDAs, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind?
- Sind Passwörter und PINs für die Nutzung von Smartphones, Tablets und PDAs ausreichend komplex und werden nicht zusammen mit dem jeweiligen Gerät aufbewahrt?
- Informiert sich das Sicherheitsmanagement regelmäßig über aktuelle Risiken der Nutzung von Smartphones, Tablets und PDAs und informiert erforderlichenfalls die Mitarbeiter?
- Bei Nutzung dienstlicher Smartphones, Tablets und PDAs: Ist die Verwaltung, Wartung und Weitergabe der betroffenen Geräte geregelt?
- Ist die Einbindung der auf Smartphones, Tablets und PDAs installierten Applikationen in andere Sicherheitssoftware in der entsprechenden Sicherheitsrichtline geregelt?

# M 2.305 Geeignete Auswahl von Smartphones, Tablets oder PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle, Leiter IT

Smartphones, Tablets oder PDAs gibt es in verschiedenen Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihren Abmessungen und im Leistungsumfang, sondern auch bei Sicherheitsmechanismen und Bedienkomfort. Zudem stellen sie unterschiedliche Anforderungen an Hard- und Software-Komponenten im Einsatzumfeld.

Aufgrund der Vielzahl von Modellen mit den unterschiedlichsten Betriebssystemen sind Kompatibilitätsprobleme mit anderer Hard- und Software wahrscheinlich.

Wenn einmal beschlossen worden ist, innerhalb einer Institution Smartphones, Tablets oder PDAs einzusetzen, sollte zunächst eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten und in einer Liste zu dokumentieren.

Anhand dieser Anforderungsliste sind dann die am Markt erhältlichen Produkte zu bewerten und die zu beschaffenden Geräte auszuwählen. Werden in einer Institution private Smartphones, Tablets oder PDAs dienstlich genutzt, dürfen nur solche private Geräte erlaubt werden, die diese Anforderungen erfüllen. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, verschiedene Gerätetypen anzuschaffen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden.

Außerdem ist sicherzustellen, dass die mobilen Endgeräte und die darauf verwendete Software zentral und effektiv verwaltet werden können (siehe M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs*). Auch sollte die notwendige Serverinfrastruktur einen möglichst geringen administrativen Aufwand erfordern.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

**Allgemeine Kriterien**

**Wartung**
- Lässt sich das Produkt einfach warten?
- Bietet der Hersteller regelmäßige Software-Updates an?
- Können für das Produkt Wartungsverträge abgeschlossen werden?

**Zuverlässigkeit/Ausfallsicherheit**
- Wie zuverlässig und ausfallsicher ist das Produkt?
- Ist das Produkt im Dauerbetrieb einsetzbar?
- Gibt es einen im Produkt integrierten Backup-Mechanismus?
- Kann eine automatische Datensicherung durchgeführt werden?

- Lässt sich das Produkt sicher löschen?

**Benutzerfreundlichkeit**
- Können Benutzer die Systeme ohne größere Schulungsmaßnahmen effektiv, sicher und fehlerfrei nutzen?
- Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
- Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit?

**Kosten**
- Wie hoch sind die Anschaffungskosten der Hard- und Software?
- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen Personalkosten (Administrator/Support)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

**Funktion**

**Installation und Inbetriebnahme**
- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
- Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden?
- Können wichtige Konfigurationsparameter vor Veränderungen durch unbefugte Benutzer geschützt werden?
- Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?

**Administration**
- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Können die Smartphones, Tablets oder PDAs über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?

**Protokollierung**
- Bietet das Produkt Protokollierung an?
- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?

**Kommunikation und Datenübertragung**
- Unterstützt das Smartphone, Tablet oder der PDA alle benötigten Datenübertragungstechniken (z. B. WLAN, Bluetooth, GSM, UMTS, LTE oder Infrarot)?

**Sicherheit**

**Kommunikation, Authentisierung und Zugriff**
- Hat das Smartphone, Tablet oder der PDA geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden? Gilt dies für alle Schnittstellen, also z. B. auch für drahtlose Verbindungen?
- Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Virenschutzprogramme) genutzt werden?

- Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
- Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?

Trotz einer Produktauswahl durch das IT-Management sollte immer damit gerechnet werden, dass Mitarbeiter andere Smartphones, Tablets oder PDAs bevorzugen und versuchen, diese im Betrieb einzusetzen und eventuell sogar Unterstützung dafür einfordern. Hierfür sollte eine geeignete Vorgehensweise definiert werden.

Manche Funktionen von Smartphones, Tablets oder PDAs sind nur in Verbindung mit externen Dienstleistern nutzbar. Über einen externen Dienstleister sollten jedoch keine internen Daten ausgetauscht werden, wenn die Vertraulichkeit und Integrität der Daten nicht gewährleistet ist. So ist beispielsweise die Übertragung über ein Mobilfunknetz meist zunächst verschlüsselt ("Luftschnittstelle"), die Daten werden dann aber oft innerhalb des Netzes des Mobilfunkanbieters unverschlüsselt übertragen und auf dem Server des Dienstbetreibers unverschlüsselt gespeichert. Im Zweifelsfall sollen solche Dienste daher nicht genutzt werden.

Prüffragen:

- Wurde die Beschaffungsentscheidung mit den Administratoren und dem technischen Personal abgestimmt?
- Wurde eine Bewertung der relevanten Geräte anhand der Anforderungsanalyse durchgeführt?
- Wurde eine Anforderungsanalyse durchgeführt?

# M 2.306 Verlustmeldung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Bei Ausfall, Defekt, Zerstörung, Verlust oder Diebstahl eines dienstlich genutzten IT-Systems, sollte dies umgehend gemeldet werden. Das gilt auch für private Geräte, die dienstlich genutzt werden, und für mobile Datenträger. Hierfür sollte es in jeder Organisation klare Meldewege und Ansprechpartner geben.

Auch Defekte bei geringpreisigen Datenträgern sollten gemeldet werden, damit das IT-Management erkennen kann, ob hiervon größere Lieferungen betroffen sind. Insbesondere bei Datenträgern, die für Datensicherungen und Archivierung eingesetzt werden, ist eine hohe Verlässlichkeit und eine lange Lebensdauer wichtig. Bei einem Verlust oder Diebstahl wiederum muss schnell gehandelt werden, da es hier nicht nur um die Wiederbeschaffung der Geräte geht, sondern auch darum, potenziellen Missbrauch der betroffenen Informationen zu verhindern.

Auf Laptops, Smartphones, Tablets, PDAs und ähnlichen Geräten, aber auch auf mobilen Datenträgern wie USB-Sticks können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten im eventuell betroffenen IT-System müssen umgehend geändert werden.
- Als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden, etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Bei Verlust von mobilen Endgeräten mit einer Funkverbindung sollten Maßnahmen zum Sperren, Löschen und Lokalisieren der mobilen Endgeräte genutzt werden. Die meisten Mobile-Device-Management-Lösungen bieten diese Funktionen an. Dafür sind im Vorfeld klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen (siehe M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*).

Wenn verlorene Geräte oder Datenträger wieder auftauchen, sollten sie auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme auf den wiedererlangten Geräten befinden, müssen die Geräte zumindest neu installiert werden (siehe M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops*). Wiedergefundene Datenträger sollten mit derselben Vorsicht behandelt werden, da sich hierauf Schadsoftware befinden könnte.

Prüffragen:

- Wissen die Benutzer, wie und wo sie Verlustmeldungen abgeben können?

# M 2.307 Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Fachverantwortliche

Die Empfehlungen dieser Maßnahme lassen sich in der Regel nur umsetzen, wenn bereits im Vertrag mit dem Outsourcing-Dienstleister beziehungsweise dem Cloud-Diensteanbieter alle relevanten Themen zum Vertragsende geregelt wurden.

Wird das Dienstleistungsverhältnis beendet, müssen die betroffenen Dienstleistungen, wie beispielsweise der IT-Betrieb, geordnet zurück in eigene Verantwortung oder auf einen anderen Dienstleister übergehen. Es müssen Vorkehrungen getroffen werden, dass durch das Vertragsende des Dienstleistungsvertrags die Geschäftstätigkeit der Institution nicht beeinträchtigt wird.

- Der Übergang auf einen anderen Dienstleister ist ein neues Outsourcing- oder Cloud-Nutzungs-Vorhaben. Die Maßnahmen des Outsourcing- Bausteins beziehungsweise die des Bausteins Cloud-Nutzung sind entsprechend anzuwenden.
- Beim Insourcing sind die relevanten Maßnahmen des Outsourcing-Bausteins analog anzuwenden. Entsprechendes gilt für den Baustein Cloud-Nutzung, sofern es sich um die Nutzung eines Cloud Services handelt. Für Strategie, Sicherheitskonzept für Insourcing, Migration und Notfallvorsorge gelten die gleichen Anforderungen wie bei einem "klassischen" Outsourcing- oder Cloud-Nutzungs-Verfahren.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- IT-Systeme, IT-Anwendungen und Arbeitsabläufe müssen ausreichend dokumentiert sein.
- Alle notwendigen Daten müssen vom Dienstleister an den Auftraggeber übertragen beziehungsweise übergeben werden.
- Alle Datenbestände beim Dienstleister müssen sicher gelöscht werden.
- Interne oder externe Mitarbeiter, die Aufgaben des Dienstleisters übernehmen, müssen eingewiesen und geschult werden.
- Es ist empfehlenswert, vertraglich eine Übergangsfrist zu vereinbaren, in der der ehemalige Dienstleister noch für Rückfragen und Hilfestellungen zur Verfügung steht.

Prüffragen:

- Regelt der Vertrag mit dem Outsourcing-Dienstleister oder dem Cloud-Diensteanbieter auch alle Aspekte der Beendigung des Dienstleistungsverhältnisses?
- Ist sichergestellt, dass eine Beendigung des Dienstleistungsverhältnisses mit dem Outsourcing-Dienstleister oder Cloud-Diensteanbieter die Geschäftstätigkeit des Auftraggebers nicht beeinträchtigt?

# M 2.308 Auszug aus Gebäuden

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Innerer Dienst, Mitarbeiter

Wenn ein Gebäude ganz oder teilweise wegen Auszug geräumt wird, sind folgende Dinge zu beachten:

- Im Vorfeld des Auszugs ist ein Bestandsverzeichnis aller für die Informationssicherheit relevanten Dinge (Hardware, Software, Datenträger, Ordner, Schriftstücke etc.) zu erstellen.
- Jeder Beschäftigte ist schriftlich darüber zu informieren, für welche Dinge er zuständig ist. Dadurch wird vermieden, dass sich ein Mitarbeiter sehr wohl um seine eigenen Dinge kümmert, Dinge für die vermeintlich jemand anderer zuständig ist, hingegen liegen bleiben.
- Nicht mehr benötigte Alt-Geräte, Datenträger etc. sind vor dem Auszug entsprechen der Maßnahme M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* Betriebsmitteln zu entsorgen. Keinesfalls dürfen alte Betriebsmittel einfach zurückgelassen werden, auch wenn der Vermieter, Nachmieter oder Käufer deren weitere Verwendung wünscht oder eine Entsorgung zusagt.
- Nach absolviertem Auszug sind **alle** Räume daraufhin zu überprüfen, ob auch tatsächlich keine sicherheitskritischen Dinge zurückgelassen wurden. Besonders in entlegenen Abstellbereichen wie Keller und Dachböden werden häufig Dinge vergessen.
  Alle Gegenstände der dienstlichen Nutzung sind konsequent einzusammeln, zu entfernen und gegebenenfalls nachträglich einer sicheren Entsorgung zuzuführen.

Die Empfehlungen aus M 2.177 *Sicherheit bei Umzügen* sollten berücksichtigt werden.

Prüffragen:

- Werden für den Auszug Bestandsverzeichnisse erstellt und verteilt?
- Wird das Gebäude nach erfolgtem Auszug nach zurückgelassenen Dingen durchsucht?

# M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

IT-Systeme, die außerhalb der eigenen Institution eingesetzt werden, sind mehr Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Trotzdem gibt es eine Vielzahl von Möglichkeiten, mobile IT-Systeme unterwegs zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind. Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von mobilen IT-Systemen erstellt werden.

### Sensibilisierung der Benutzer

Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten Mitarbeiter für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Da es bei mobilen IT-Systemen eine große Bandbreite von Varianten und Kombinationsmöglichkeiten gibt (von Handy über PDA zu Laptop mit WLAN-Schnittstelle), sollten sie vor allem über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und dies unterwegs auch nicht in Hör- und Sichtweite von Externen machen sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*).

### Regelungen zur Nutzung mobiler IT-Systeme

Ebenso sind bei der Nutzung von mobilen IT-Systemen diverse Punkte zu regeln:

- Die Benutzer müssen darüber informiert sein, welche Informationen mit mobilen IT-Systemen unterwegs verarbeitet werden dürfen. Die Daten sollten dementsprechend klassifiziert sein, um Einschränkungen den Benutzern transparent zu machen (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*). Dienstgeheimnisse dürfen nur dann auf mobilen IT-Systemen verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- Daten, die ein hohes Maß an Sicherheit verlangen (z.B. Angebote, Konstruktionsdaten, Wirtschaftsdaten des Unternehmens) sollten stets verschlüsselt auf dem mobilen IT-System abgelegt werden.
- Beim Einsatz mobiler IT-Systeme ist zu klären, ob mobile Mitarbeiter von unterwegs Zugriff auf interne Daten ihrer Institution erhalten.
  Falls dies vorgesehen ist, muss dieser Zugriff angemessen geschützt werden (siehe hierzu auch M 5.121 *Sichere Kommunikation von unterwegs* und M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*).
- Es muss geklärt werden, ob diese auch für private Zwecke benutzt werden dürfen, beispielsweise für private Schreiben oder ein Spielchen nach Feierabend.

- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen IT-Systemen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von mobilen IT-Systemen sollte geregelt werden.
- Bei jedem Benutzerwechsel müssen alle benötigten Passwörter gesichert weitergegeben werden (siehe M 2.22 *Hinterlegen des Passwortes*).

Mobile IT-Systeme sollten möglichst nicht unbeaufsichtigt bleiben. Falls ein mobiles IT-System in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein mobiles IT-System stellt einen Wert dar, der potentielle Diebe anlocken könnte.

Werden mobile IT-Systeme in fremden Büroräumen vor Ort benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten.

In fremden Räumlichkeiten wie Hotelzimmern sollten mobile IT-Systeme nicht ungeschützt ausliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

**Entsorgung von Datenträgern und Dokumenten**

Auch unterwegs gibt es häufiger Material, das entsorgt werden soll, schon alleine, damit das Gepäck noch tragbar bleibt. Während es aber innerhalb der eigenen Institution eingeübte Verfahren gibt, wie alte oder unbrauchbare Datenträger und Dokumente entsorgt werden (siehe auch M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*), ist dies unterwegs nicht immer möglich. Daher ist vor der Entsorgung ausgedienter Datenträger und Dokumente genau zu überlegen, ob diese sensible Informationen enthalten könnten. Ist dies der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zurück transportiert werden. Dies ist auch dann der Fall, wenn die Datenträger defekt sind, da Experten auch hieraus wieder wertvolle Informationen zurückgewinnen können. Auch Shredder-Einrichtungen in fremden Institutionen sollten mit Vorsicht betrachtet werden, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt bzw. wie zuverlässig diese ist.

**Nutzungsverbot von mobilen IT-Systemen**

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von mobilen IT-Systemen in allen oder bestimmten Bereichen einer Behörde oder Institution eingeschränkt werden sollte.

Dies kann z. B. für Besprechungsräume sinnvoll sein (siehe dazu beispielsweise M 5.80 *Schutz vor Abhören der Raumgespräche über Mobiltelefone*). Wenn die Sicherheitsrichtlinie der Institution es nicht zulässt, dass mobile IT-Systeme mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die mobile Nutzung von IT-Systemen?
- Wurden die Benutzer hinsichtlich des Schutzbedarfs mobiler IT-Systeme sowie der darauf befindlichen Daten sensibilisiert?

- Wurden die Benutzer hinsichtlich der spezifischen Gefährdungen bzw. entsprechender Maßnahmen bei der Nutzung mobiler IT-Systeme sensibilisiert?
- Sind die Benutzer darüber informiert, welche Art von Informationen auf mobilen IT-Systemen verarbeitet werden dürfen?

# M 2.310 Geeignete Auswahl von Laptops

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle, Leiter IT

Laptops gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihrem Abmessungen und Leistungsmerkmalen, sondern auch den Sicherheitsmechanismen und Bedienkomfort. Zudem stellen sie unterschiedliche Voraussetzungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener Laptop-Modelle mit den unterschiedlichsten Betriebssystemen, sind Kompatibilitätsprobleme bei Hardware, Software auf Laptop und PC sowie Schnittstellen naheliegend.

Wenn einmal beschlossen worden ist, innerhalb einer Institution Laptops einzusetzen, sollte daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung sollten dann die zu beschaffenden Produkte ausgewählt werden. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, mehrere Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden.

Zunächst sollte eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

**Allgemeine Kriterien**

- Wartbarkeit
  - Ist das Produkt einfach wartbar?
  - Bietet der Hersteller regelmäßige Software-Updates an?
  - Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?
- Zuverlässigkeit/Ausfallsicherheit
  - Wie zuverlässig und ausfallsicher ist das Produkt?
  - Ist das Produkt im Dauerbetrieb einsetzbar?
  - Gibt es einen im Produkt integrierte Backup-Mechanismus? Kann eine automatische Datensicherung durchgeführt werden?
- Benutzerfreundlichkeit
  - Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
  - Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
  - Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit?

- Kosten
  - Wie hoch sind die Anschaffungskosten der Hard- und Software?
  - Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
  - Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal (Administrator/Support)?
  - Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

**Funktion**
- Installation und Inbetriebnahme
  - Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
  - Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
  - Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?
- Administration
  - Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
  - Können die Laptops über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?
- Protokollierung
  - Bietet das Produkt Protokollierung an?
  - Ist der Detailgrad der Protokollierung konfigurierbar? Werden durch die Protokollierung alle relevanten Daten erfasst?
  - Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen?
  - Bietet das Produkt die Möglichkeit an, die Protokolldaten nicht nur lokal zu speichern, sondern auch auf entfernten Rechnern (zentrales Protokoll)?
- Kommunikation und Datenübertragung
  - Unterstützt der Laptop alle benötigten Datenübertragungstechnologien (z. B. Infrarot, Bluetooth oder GSM)?
- Sicherheit: Kommunikation, Authentisierung und Zugriff
  - Hat der Laptop geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
  - Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden?
  - Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Virensuchprogramme) genutzt werden?
  - Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
  - Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?
  - Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Produkte dahin gehend untersucht werden,

inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen mit Gewichten versehen werden, die reflektieren, wie wichtig die Erfüllung der jeweiligen Anforderung ist. Aufgrund der durchgeführten Produktbewertung (gemäß dem erstellten Anforderungskatalog) kann dann eine fundierte Kaufentscheidung getroffen werden.

Prüffragen:

- Wurde eine Anforderungsanalyse für die Auswahl von Laptops durchgeführt?
- Enthält die Anforderungsanalyse auch zusätzlich benötigte Hardware wie z. B. Dockingstations und Monitore?
- Wurde eine Bewertung der in Frage kommenden Geräte anhand der Kriterien aus der Anforderungsanalyse durchgeführt?
- Wurde die Beschaffungsentscheidung mit den Administratoren und dem technischen Personal abgestimmt?

# M 2.311 Planung von Schutzschränken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Beschaffung, Leiter IT
**Verantwortlich für Umsetzung:** Beschaffungsstelle, Haustechnik

Der Einsatz von Schutzschränken kann aus verschiedenen Gründen sinnvoll sein, z. B. als Ersatz für einen Serverraum oder um die Schutzwirkung eines Serverraums zu erhöhen. Da die Kosten für Schutzschränke nicht unerheblich sind, sollte zunächst ein Konzept erstellt werden, das auf den Anforderungen aus den geplanten Einsatzszenarien beruht. Dafür ist unter anderem zu hinterfragen, welche Komponenten durch den Schutzschrank gegen welche Bedrohungen geschützt werden sollen, also z. B. ob sie ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten Zugriff schützen sollen.

Außerdem ist ein Kostenvergleich dringend empfehlenswert. Zu vergleichen sind die Kosten, die die Beschaffung und der Unterhalt eines Schutzschrankes verursachen, mit den Kosten für die Errichtung eines Serverraums bzw. Datenträgerarchivs und dessen Unterhalt.

Bei der Planung des Raumes, in dem der Schutzschrank aufgestellt wird, ist durch Maßnahmen zum Brandschutz bis hin zur Installation einer Gefahrenmeldeanlage, gegebenenfalls innerhalb des Schutzschranks, dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach Möglichkeit keine wasserführenden Leitungen vorhanden sein sollten, da Undichtigkeiten größere Schäden verursachen können, gegen die nicht jeder Schutzschrank ausreichend abgesichert ist. Soll der Schutzschrank als Serverschrank eingesetzt werden, sind je nach Schutzbedarf zusätzliche Maßnahmen wie Überspannungsschutz, Not-Aus-Schalter, Klimatisierung, USV und eventuell auch eine Fernanzeige von Störungen vorzusehen.

Prüffragen:

- Sind die Anforderungen an Schutzschränke, unter Berücksichtigung des Schutzbedarfs seiner Inhalte, analysiert?
- Sind die Schutzschränke (gegen Feuer, Wasser, Einbruch) ausreichend abgesichert?
- Einsatz des Schutzschrankes als Serverschrank: Sind zusätzliche Maßnahmen, wie Klimatisierung, Not-Aus Schalter, Überspannungsschutz und USV berücksichtigt worden?

# M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Die Mitarbeiter sind wesentliche Erfolgsfaktoren, um Informationssicherheit in einer Institution zu etablieren und aufrechtzuerhalten. Sie sind es, die technische Schutzsysteme nutzen oder administrieren, die Richtlinien und Vorgaben mehr oder weniger sorgfältig beachten und die aus Unkenntnis oder Vorsatz sicherheitsrelevante Fehler machen können.

Die im Rahmen eines Sicherheitskonzeptes realisierten technischen und organisatorischen Maßnahmen wirken sich in vielfältiger Weise auf die einzelnen Mitarbeiter aus. So könnten sie zu regelmäßigen Passwortwechseln gezwungen sein, bestimmte Bereiche der Institution ohne Genehmigung nicht betreten dürfen, ihre Mitarbeiterausweise gut sichtbar tragen oder regelmäßig Sicherheitsschulungen besuchen müssen.

Ziel jeder Institution sollte es daher sein, dass alle Mitarbeiter den Wert und die Notwendigkeit einer angemessenen Informationssicherheit zur Erfüllung ihrer Aufgaben und den Fortbestand der Institution erkennen, akzeptieren und aktiv unterstützen. Sie sollten die bestehenden Regelungen und Maßnahmen beachten und durch ihr Verhalten dazu beitragen, die Informationssicherheit aufrechtzuerhalten und weiterzuentwickeln. Auch sollten sie sicherheitskritische Situationen möglichst frühzeitig erkennen und darauf richtig reagieren.

Dies setzt eine systematische Sensibilisierung der Mitarbeiter voraus, die durch einen kontinuierlichen Prozess in der Institution zu verankern ist. Aufbauend auf der Sensibilisierung sollten die Mitarbeiter durch ergänzende Schulungen alle erforderlichen Informationen und Fähigkeiten vermittelt bekommen (siehe M M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit*). Sensibilisierungs- und Schulungsprogramme sind somit eng verwandte Themengebiete, denen auf allen Organisationsebenen eine hohe Bedeutung zugemessen werden sollte. Damit das besondere Gewicht von Sensibilisierungsmaßnahmen erkennbar ist und die benötigten Ressourcen zur Planung, Umsetzung und Aufrechterhaltung verfügbar sind, muss das Management die Maßnahmen unterstützen (siehe M 3.96 *Unterstützung des Managements für Sensibilisierung und Schulung*).

Nachfolgend sind die Schritte aufgeführt, mit denen ein Sensibilisierungsprogramm erstellt werden kann:

**Ziel der Sensibilisierung festlegen**

Sensibilisierung für Informationssicherheit bedeutet, dass bei Mitarbeitern die Wahrnehmung von Informationssicherheit geschärft und ihr Sicherheitsbewusstsein entsprechend den Anforderungen der Institution geschult wird.

Zu Beginn der Sensibilisierung sollte ein Ziel definiert und im weiteren Verlauf dieser Maßnahme zielgruppenbezogen verfeinert werden. So können später Inhalte passgenau entwickelt und der Erfolg der Maßnahmen gemessen wer-

den. Bei der Zieldefinition sollte die Frage im Vordergrund stehen, warum Informationssicherheit für die Institution und ihre Mitarbeiter wichtig ist.

Beispiel für eine Zieldefinition:

- Die Mitarbeiter erkennen die Bedeutung von Informationssicherheit für die Institution und ihren Arbeitsplatz.
  Sie kennen die relevanten Gefährdungen und können die Auswirkungen von Sicherheitsvorfällen und Verstößen gegen geltende Regelungen beurteilen. Sie akzeptieren die Maßnahmen zur Informationssicherheit und sind bereit, diese zu beachten und in ihrem Arbeitsumfeld aktiv an deren Aufrechterhaltung und Weiterentwicklung mitzuarbeiten.

**Zielgruppenanalyse durchführen**

Durch die Zielgruppenanalyse werden Mitarbeiter mit vergleichbaren Merkmalen in Bezug auf die Informationssicherheit identifiziert, wie z. B. ¿Administratoren", "Mitarbeiter der Personalabteilung" oder "externe Mitarbeiter". Weiterhin sollten hier auch Entwicklungen der Mitarbeiterlaufbahn betrachtet werden, die für die Institution charakteristisch sind, z. B. Abteilungs-, Funktions- oder Standortwechsel.

Durch die Zielgruppenanalyse können die Sensibilisierungsmaßnahmen an spezielle Anforderungen und unterschiedliche Hintergründe der Mitarbeiter angepasst werden (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*).

**Sensibilisierungsziel pro Zielgruppe detaillieren**

Die Sensibilisierungsmaßnahmen sind zielgruppengerecht aufzubereiten. Als Ergebnis können z. B. Auswirkungen von Sicherheitsvorfällen für die jeweiligen Mitarbeiter so praxisnah wie möglich beschrieben werden. Weiterhin hat es sich auch als äußerst wirksam erwiesen, Beispiele aus dem privaten Umfeld der Mitarbeiter in Sensibilisierungsprogramme mit aufzunehmen, wie der Verlust der Digitalfotos aus dem letzten Urlaub oder ein verlorenes Smartphone.

**Inhalte der Sensibilisierung festlegen**

Sensibilisierungskampagnen können alle Themen beinhalten, die begründen, warum Informationssicherheit für die Institution und ihre Mitarbeiter wichtig ist. Hierzu zählen z. B. relevante Gefährdungen oder beispielhafte wie auch reale Sicherheitsvorfälle, an denen richtiges Verhalten trainiert werden kann. Dabei sollte darauf geachtet werden, dass genügend Inhalte einen engen Bezug zur Institution und der angesprochenen Zielgruppe haben. Zusätzlich können Beispiele aus vergleichbaren Institutionen oder aussagekräftigen Publikationen die Inhalte untermauern.

**Medien und Methoden auswählen**

Es sind solche Medien und Methoden auszuwählen, die sich eng an der herrschenden Kultur der Institution orientieren. Ziel ist es, die Mitarbeiter mit vertretbaren Kosten möglichst eindrucksvoll und nachhaltig zu erreichen und für Informationssicherheit zu sensibilisieren. Das heißt, die Wahrnehmungen, Emotionen und Fähigkeiten der Mitarbeiter für Schwachstellen und Vorfälle in ihrer Arbeitsumgebung müssen gestärkt werden, damit sie diese frühzeitig erkennen, bewerten und richtig darauf reagieren. Dabei sollte auf reine Anweisungstexte, ausführliche und detaillierte schriftliche Regelungen sowie auf eine für die Zielgruppe unverständliche Fachsprache zugunsten einer kurzen

und prägnanten Kommunikation verzichtet werden (siehe auch M 3.47 *Durchführung von Planspielen zur Informationssicherheit*).

**Sensibilisierungsmaßnahmen umsetzen**

Sensibilisierung und Schulung sind eng verwandte Themen, die sich in der Umsetzung ergänzen und aufeinander aufbauen. Sensibilisierung soll die Mitarbeiter zum Handeln motivieren (siehe M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*). Die richtigen Verhaltensweisen werden anschließend durch entsprechende Schulungsmaßnahmen weiter unterstützt (siehe M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit*). Es ist in der Praxis eine große Herausforderung, Mitarbeiter für Informationssicherheit zu interessieren und das richtige Verhalten aufrechtzuerhalten. Bekanntermaßen fallen Lernkurven nach Schulungen ohne unterstützende Maßnahmen schnell wieder ab. Deshalb muss der Lernstoff durch geeignete Maßnahmen, z. B. durch regelmäßige Wiederholungen, gefestigt werden (siehe M 3.95 *Lernstoffsicherung*).

**Erfolg von Sensibilisierung messen**

Der Erfolg der festgelegten Sensibilisierungsziele ist zu messen und auszuwerten. Dafür sollte der Sensibilisierungsstand der Teilnehmer vor, während und nach der Maßnahme anhand geeigneter Kennzahlen oder Kriterien erfasst werden. So lässt sich verfolgen, ob die Kampagne erfolgreich ist und wie sich die Sensibilisierung entwickelt. Weitere Informationen sind in Maßnahme M 3.94 *Messung und Auswertung des Lernerfolgs* dargestellt.

**Sensibilisierungsprogramm aktualisieren**

Informationssicherheit ist in einer Institution permanenten Veränderungen unterworfen. IT-Systeme, Prozesse, Leistungsspektren, Wettbewerbssituationen wandeln sich und damit einhergehend auch Gefährdungslagen, Risikobewertungen und erforderliche Sicherheitsmaßnahmen. Zusätzlich müssen die Ergebnisse der bisherigen Sensibilisierungsmaßnahmen betrachtet werden, insbesondere notwendige Veränderungen aufgrund der Messung und Auswertung des Lernerfolgs.

Diese Veränderungen müssen daher sorgfältig analysiert werden. Das Sensibilisierungsprogramm ist regelmäßig zu aktualisieren.

Prüffragen:

- Liegt ein zielgruppenorientiertes Sensibilisierungsprogramm vor?
- Wird das Sensibilisierungsprogramm regelmäßig überprüft und aktualisiert?

# M 2.313 Sichere Anmeldung bei Internet-Diensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Bei vielen Internet-Diensten müssen Benutzer sich anmelden, um diese nutzen zu können. Dazu ist in der Regel mindestens die Angabe eines Benutzernamens und eines Passwortes erforderlich, häufig werden aber auch mehr Informationen erfragt, wie z. B. Vor- und Familienname, Arbeitgeber, E-Mail-Adresse, etc. Werden Internet-Dienste für dienstliche Zwecke genutzt, sollten die Regelungen der Institution zur Internet-Nutzung beachtet werden, in der unter anderem beschrieben sein sollte, welche Angaben bei der Registrierung und Nutzung der Dienste gemacht werden dürfen (siehe dazu M 2.458 *Richtlinie für die Internet-Nutzung*).

Jeder Benutzer sollte sich genau überlegen, welche Angaben hier gemacht werden, da dies zum Beispiel unerwünschte Werbeaktionen auslösen kann. Um dies zu vermeiden, sollten möglichst wenig detaillierte Informationen weitergegeben und die Datenschutz-Hinweise genau gelesen werden. Die Benutzer sollten bei jeder Angabe personenbezogener Daten überlegen, inwieweit sie diese wirklich an den Dienstleister weitergeben möchten und welcher weiteren Verwendung sie dabei zustimmen. Falls eine funktionierende E-Mail-Adresse benötigt wird, aber die Weitergabe der dienstlichen oder privaten E-Mail-Adresse als Absenderadresse nicht erwünscht ist, kann hierbei auf Wegwerf-E-Mail-Adressen zurückgegriffen werden, die über kostenfreie Internet-Dienste erzeugt werden können.

Falls bestimmte Internet-Dienste regelmäßig beruflich genutzt werden, sollten von der Institution möglichst Vorgaben für die Mitarbeiter erarbeitet werden, wie die einzelnen Felder beim Anmeldevorgang auszufüllen sind.

Das Passwort für den jeweiligen Internet-Dienst sollte angemessen sorgfältig ausgesucht werden (siehe dazu auch M 2.11 *Regelung des Passwortgebrauchs*). Vor allem sollten solche Passwörter nicht mit einem Passwort übereinstimmen, das wichtige Daten schützen soll, also z. B. den Büro-Rechner.

Falls bei der Anmeldung personenbezogene Daten angegeben werden müssen, so sollte dies möglichst nur SSL-gesichert erfolgen (siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS*). Wenn die Nutzung eines Angebots die Angabe sensitiver Daten über eine ungesicherte Verbindung erfordert, so sollte sorgfältig abgewogen werden, ob dieses Angebot wirklich genutzt werden soll.

Viele Internet-Dienste bieten eine Recovery-Funktion für Passwörter an, also eine Rettungsmöglichkeit, wenn ein Benutzer sein Passwort vergisst. Hierfür müssen im Vorfeld oft einige Fragen beantwortet werden. Die Antworten werden vom Dienstleister gespeichert und der Benutzer wird danach gefragt, wenn er sein eigentliches Passwort vergessen hat. Die Fragen sind häufig vorgefertigt, oft wird z. B. nach dem Namen der Mutter oder des Haustieres, der Lieblingsfarbe oder des Geburtsortes gefragt. Leider bieten nur wenige Dienstleister die Möglichkeit, die Frage selbst vorzugeben.

**Hinweis:** Bei vielen Angriffen über Social Engineering oder Phishing wird nicht plump nach Passwörtern gefragt, sondern anscheinend unverfänglich nach dem Haustier oder der Lieblingsfarbe. Daher ist es sinnvoll, bei Recove-

ry-Funktionen keine wahrheitsgemäßen Antworten zu geben, sondern solche, auf die kein Angreifer kommt, die man sich aber selbst merken kann.

Prüffragen:

- Ist sichergestellt, dass die bei Internet-Diensten genutzten Passwörter von anderen Passwörtern verschieden sind?

# M 2.314 Verwendung von hochverfügbaren Architekturen für Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Verfügbarkeit von Geschäftsprozessen, Anwendungen und Diensten hängt oft von der Funktion eines zentralen Servers ab. Je mehr Anwendungen aber auf einem Server laufen, desto ausfallsicherer muss dieser sein. Ein Server enthält in der Regel verschiedene potentielle Fehlerquellen ("Single Points of Failure"), also Komponenten, deren Ausfall den Ausfall des Gesamtsystems auslösen kann: IEC, Festplatten, Stromversorgung, Lüfter, Backplane, etc. Die Wiederherstellung des Gesamtsystems kann in diesem Fall erhebliche Zeit in Anspruch nehmen. Neben der Vorhaltung von Ersatzteilen können zusätzlich folgende Möglichkeiten zur Steigerung der Verfügbarkeit eingesetzt werden:

- Cold-Standby
- Hot-Standby (manuelles Umschwenken)
- Cluster (automatisches Umschwenken)
  - Load balanced Cluster
  - Failover Cluster

Jede einzelne dieser Techniken bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel mit unterschiedlichen Kosten verbunden.

**Cold-Standby**

Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht aktiv ist. Wenn das erste System ausfällt, kann das Ersatzsystem manuell hochgefahren und ins Netz integriert werden.

Nach der Vorhaltung von einzelnen Ersatzteilen ist dies die einfachste Redundanz-Lösung, die mit den entsprechenden Vorteilen und Nachteilen verbunden ist:

| **Vorteile einer Cold-Standby Lösung** | **Nachteile einer Cold-StandbyLösung** |
|---|---|
| - Cold-Standby Lösungen bringen keine Komplexitätserhöhung für das Gesamtsystem mit sich.<br>- Die Kosten für ein Cold-Standby System belaufen sich lediglich auf die Kosten der zusätzlichen Hardware und sind so mit am geringsten unter den vorgestellten Möglichkeiten.<br>- Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbußen möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Cold-Standby System umgelegt. | - Zum bestehenden System muss ein zweites System vorgehalten werden.<br>- Das Ersatzsystem muss ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden.<br>- Da das Ersatzsystem manuell aktiviert werden muss, müssen Administratoren das System kontinuierlich überwachen und im Notfall einschreiten.<br>- Wenn die Applikationsdaten nicht auf einem externen Speichersystem liegen, so dass der Zugriff direkt aus dem Ersatzsystem möglich ist, dann müssen diese |

| Vorteile einer Cold-Standby Lösung | Nachteile einer Cold-StandbyLösung |
|---|---|
| | auf das Cold-Standby System migriert werden. |

Tabelle: Vor-und Nachteile einer Cold-Standby Lösung

Der Einsatz eignet sich gut für Server mit Anwendungen, bei denen kurze bzw. begrenzte Ausfallzeiten, bis der Eingriff des Administrators möglich ist, unkritisch sind. Beispiele dafür sind:

- Server in kleineren Netzen (Intranet)
- Wenig frequentierte Server im Internet

**Hot-Standby (manuelles Umschwenken)**

Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem bereit, das aber neben dem Produktivsystem parallel in Betrieb gehalten wird. Die Funktion des Produktivsystems wird überwacht, bei Ausfall wird das Ersatzsystem aktiv. Der Wechsel kann automatisch erfolgen oder auch manuell. Für den automatischen Wechsel sind zusätzliche Funktionalitäten im Gesamtsystem erforderlich z. B. die automatische Erkennung von Ausfällen. Dieser Fall wird im nächsten Abschnitt unter "Cluster" behandelt.

Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand des Ersatzsystems kontinuierlich überprüft werden.

| Vorteile einer Hot-Standby Lösung | Nachteile einer Hot-Standby Lösung |
|---|---|
| - Die Ausfallzeiten sind im Vergleich zu Cold-Standby geringer.<br>- Wie beim Cold-Standby ist diese Lösung auch relativ kostengünstig, verglichen mit höherwertigen Hochverfügbarkeitslösungen, die im Folgenden beschrieben werden.<br>- Das Ersatzsystem ist in Betrieb und kann auch zu Datenreplikation benutzt werden.<br>- Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbuße möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Hot-Standby System umgelegt. | - Es wird auch hier immer nur die Hälfte der vorhandenen Hardware genutzt.<br>- Das Ersatzsystem muss ständig auf dem aktuellen Stand gehalten werden.<br>- Im Falle der manuellen Aktivierung des Hot-Standby Systems ist eine kontinuierliche Überwachung von einem Systemverantwortlichen erforderlich. |

Tabelle: Vor- und Nachteile einer Hot-Standby Lösung

Der Einsatz von Hot-Standby Systemen eignet sich für Anwendungen, bei denen kurze Ausfallzeiten unkritisch sind. Die Problematik der Systemüberwachung und der Aktivschaltung des Hot-Standby Servers muss dabei mitbedacht werden. Mögliche Einsatzbereiche sind z. B. für:

- Webserver mit oft variierendem Content
- Server in kleineren Netzen (Application-Server, Mailserver)
- Datenbank-Server und Fileserver (z. B. sekundärer Server repliziert primären Server ständig und wird im Fehlerfall als primärer Server geschaltet).

**Cluster (automatisches Umschwenken)**

Ein Cluster besteht aus einer Gruppe von zwei oder mehreren Rechnern, die zur Steigerung der Verfügbarkeit oder auch der Leistung einer Anwendung oder eines Dienstes parallel betrieben werden. Die Anwendung oder der Dienst kann dabei auf einem der Rechner aktiv durchgeführt werden oder auf mehreren verteilt (Performance-Steigerung).

Cluster werden je nach Funktionsart in

- Load balanced Cluster
- Failover Cluster und

unterschieden.

**Load balanced Cluster**

Beim Load balanced Cluster werden Instanzen einer Anwendung oder eines Dienstes in Abhängigkeit von der Auslastung unter den Servern verteilt. Wenn dies für eine Anwendung oder einen Dienst möglich ist, dann kann damit nicht nur eine Lastverteilung (Load balancing) und somit eine Performancesteigerung erreicht werden, sondern auch die Probleme bei Ausfällen werden verringert.

Eine der Voraussetzungen für den Einsatz von Load balancing ist, dass die jeweiligen Anwendungen oder Dienste keinen schreibenden Datenzugriff benötigen dürfen.

Eine Redundanz kann in diesem Fall geschaffen werden, indem Systeme mit ähnlicher Leistung mit Hilfe eines Load-Balancing Prozesses "nebeneinander" gestellt werden und dafür gesorgt wird, dass beim Ausfall eines Servers die anderen Server diesen Ausfall auffangen.

| **Vorteile eines Load balanced Clusters** | **Nachteile eines Load balanced Clusters** |
|---|---|
| - Es können damit sowohl Verfügbarkeitssteigerung als auch Leistungssteigerung erreicht werden.<br>- Alle verfügbare Ressourcen werden dauerhaft genutzt.<br>- Die Lösung ist hochgradig skalierbar.<br>- Die Komplexität des Gesamtsystems ist geringer als bei einem Failover Cluster. | - Der Einsatz ist nicht für alle Arten von Anwendungen möglich. Insbesondere Anwendungen, die keine reinen Lesezugriffe verwenden und zugleich den Zugriff aller Server auf die gleichen Speicherressourcen verlangen, sind für Load Balancing nicht geeignet. |

Tabelle: Vor- und Nachteile eines Load balanced Clusters

Wenn neben der Verfügbarkeit die Performance hohen Stellenwert hat und die Applikation einen verteilten Einsatz erlaubt, bietet ein Load balanced Cluster eine optimale Lösung. Das kann z. B. der Fall sein für:

**Web-Server, für Front-end Applikationen mit ausschließlichen Lesezugriffen (z. B. Web-Server-Farmen) Failover Cluster**

Als Failover Cluster wird hier ein Cluster bezeichnet, wenn bei Ausfall eines der Cluster-Systeme automatisch der aktive Betrieb der Anwendung oder des Dienstes von einem anderen Teil des Clusters übernommen wird (Takeover). Die automatische Übernahme von Diensten beim Ausfall einer Systemkom-

ponente durch eine funktional äquivalente Komponente wird Failover genannt. Für die Failover-Funktionalität ist eine dedizierte "heartbeat" (Herzschlag) Verbindung üblich, die die Kommunikation zwischen den Cluster-Servern gewährleistet. Die Cluster-Server müssen neben der Verbindung mit dem Client-Netz auch mit dem Administrationsnetz dediziert verbunden sein, um einen direkten Zugriff im Notfall zu gewähren.

Ein automatisches Failover setzt voraus, dass alle Software- und Hardware-Komponenten geeignet überwacht werden. Daher ist es wichtig sicherzustellen, dass der Failover Mechanismus auf keinen falschen Annahmen basiert.

Folgende Punkte müssen beim Einsatz eines Failover-Clusters berücksichtigt werden:

- **Zugriff auf gemeinsamen Speicher:**
  Neben den servereigenen Festplatten, die das Betriebssystem und die für den Betrieb notwendigen Daten enthalten, ist es in einem Cluster ratsam, die Anwendungsdaten auf gemeinsamen Speicher zu verwalten.
  Der Zugriff auf diese Festplatten wird dem Teil des Clusters gewährt, der gerade aktiv ist. Es ist auch möglich, statt gemeinsamen Festplatten replizierte Festplatten zu verwenden. Dies ist dann sinnvoll, wenn das Failover von einem entfernten Standort aus stattfindet. Bei einem lokalen Failover sollte überlegt werden, ob die durch die Replikation erzeugte Komplexität und entstandene Abhängigkeiten nicht eine zusätzliche Bedrohung für die Verfügbarkeit darstellen.
- **Portabilität der Anwendung:**
  Die Installation und Inbetriebnahme einer Anwendung auf zwei oder mehreren Servern parallel erfordert in den meisten Fällen den Einsatz zusätzlicher Lizenzen. Darüber hinaus muss überprüft werden, ob die Applikation eine Failover-Funktionalität erlaubt.
- **NSPoF (No Single Points of Failure):**
  Wenn die Failover-Funktionalität des Clusters durch den Ausfall einer einzigen Komponente gestört werden kann, widerspricht dies dem eigentlichen Zweck der Cluster-Architektur. Um Single Points of Failure zu vermeiden, muss das Gesamtsystem analysiert werden und der Ausfall einzelner Komponenten (Netzteile, Systemspeicher, Hauptspeicher, Netzwerkkarten, Switche, Hubs etc.) in Betracht gezogen werden.
- **Betriebssystem und Konfiguration der Cluster-Server:**
  Die Cluster-Server sollten mit gleichen Betriebssystemversionen, Patches, Libraries und Applikationsversionen ausgestattet sein. Eine möglichst identische Hardware- und Software-Konfiguration kann ein möglichst identisches Verhalten im Falle eines Failovers gewährleisten. Darüber hinaus reduziert sich im Falle von identischen Systemen die Komplexität des Gesamtsystems (Einsatz der gleichen Failover Software, Netz-Schnittstellen, Kompatibilität der gemeinsamen Speichersystems, Administration, Service).
- **Dedizierte und redundante Verbindung zwischen den Servern:**
  Die Kommunikation zwischen den Cluster-Servern muss unabhängig von der Netzlast, möglichst verzögerungsfrei erfolgen, damit das Failover schnellstmöglichst stattfinden kann. Die Redundanz ist aufgrund der hohen Verfügbarkeitsanforderungen ebenfalls erforderlich.
- **Einsatz von ausgereiften Software-Produkten für das Failover Management:**
  Die Entscheidung, ob ein Failover stattfinden muss oder nicht, ist eine sehr komplexe. Neue oder selbstentwickelte Tools können Fehler enthalten und dadurch letztendlich die Verfügbarkeit des Gesamtsystems reduzieren.

- **Ausführliches Testen aller möglichen Failover-Aspekte:**
  Ein ausführliches Testen ist unter anderem auch dazu notwendig, um festzustellen, dass keine unerwarteten Fehlerquellen (Single Points of Failure) vorhanden sind. Insbesondere muss das Monitoring der Server und das Failover-Management auf alle möglichen Fehler getestet werden.

| Vorteile eines Failover Clusters | Nachteile eines Failover Clusters |
|---|---|
| - Durch das automatische Takeover kann die Verfügbarkeit erheblich gesteigert werden.<br>- Es sind keine manuellen Eingriff nötig. | - Diese Lösung ist hoch komplex.<br>- Failover Cluster sind nicht gut skalierbar.<br>- Es wird immer nur ein Teil der Ressourcen genutzt.<br>- Es entstehen hohe Kosten aufgrund zusätzlicher Hardware und Software |

Tabelle: Vor- und Nachteile eines Failover Clusters

Wie aus der Gegenüberstellung der Vorteile und Nachteile hervorgeht, ist der Einsatz eines Failover Clusters nur dann sinnvoll, wenn eine oder mehrere Applikationen sehr hohe Verfügbarkeitsanforderungen haben. Neben dem hohen Kostenaufwand sind sehr gute Kenntnisse des verantwortlichen Personals sowohl über die eingesetzten Betriebssysteme und Applikationen als auch über die Failover-Funktionalität erforderlich. Der Einsatz von Failover Lösungen für Server macht zudem nur dann Sinn, wenn auch alle Abhängigkeiten wie beispielsweise Netzanbindung oder Verfügbarkeit der Clients auch mit den entsprechenden Redundanzen ausgelegt sind.

Bereiche, für die typischerweise bei hohen Verfügbarkeitsanforderungen Failover Cluster eingesetzt werden, sind z. B.:

- Datenbank Anwendungen
- File Storage
- Anwendungen mit dynamischem Inhalt
- Mail Server

Wenn Geschäftsprozesse, Anwendungen oder Dienste hohe Anforderungen an die Verfügbarkeit haben, sollte auf jeden Fall überlegt werden, wodurch diese Anforderungen abgedeckt werden können. Die IT-Veranstwortlichen und das Sicherheitsmanagement sollten für die entsprechenden Server ein Konzept erarbeiten und angemessene Architekturen auswählen.

Prüffragen:

- Berücksichtigt die gewählte Server-Architektur die Verfügbarkeitsanforderungen?

# M 2.315 Planung des Servereinsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine grundlegende Voraussetzung dafür, dass ein Server sicher betrieben werden kann ist ein angemessenes Maß an Planung im Vorfeld.

Die Planung für den Einsatz eines Servers kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben soll das zu planende System erfüllen? Welche Dienste sollen von dem Server bereitgestellt werden? Gibt es besondere Anforderungen an die Verfügbarkeit des Systems oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
  Diese Vorgaben kommen aus der übergreifenden Planung und werden von den allgemeinen Zielvorgaben bestimmt. Je genauer die Rahmenbedingungen bekannt und je präziser die Vorgaben formuliert sind, desto einfacher werden die folgenden Planungsschritte.
- Sollen in dem System bestimmte Hardwarekomponenten eingesetzt werden? Dies kann beispielsweise für die Auswahl des Betriebssystems wichtig sein.
- Welche Anforderungen an die Hardware (CPU, Arbeitsspeicher, Kapazität der Festplatten, Kapazität des Netzes etc.) ergeben sich aus den allgemeinen Anforderungen?
- Handelt es sich bei dem eingesetzten Netz um einen homogenen oder heterogenen Rechnerverbund?
- Ersetzt das System ein altes, vorhandenes? Sollen von dem alten System Datenbestände oder Hardwarekomponenten übernommen werden?
- Sollen auf dem Rechner weitere Betriebssysteme mittels Multiboot installiert werden?

Die folgenden Teilkonzepte sollten bei der Planung des Servereinsatzes berücksichtigt werden:

- **Authentisierung und Benutzerverwaltung:** Welche Arten der Benutzerverwaltung und Benutzerauthentisierung sollen auf dem System genutzt werden? Werden Benutzer nur lokal verwaltet oder soll ein zentrales Verwaltungssystem genutzt werden? Soll das System auf einen zentralen, netzbasierten Authentisierungsdienst zugreifen, oder wird nur eine lokale Authentisierung benötigt? Mehr Informationen dazu finden sich in M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*.
- **Benutzer- und Gruppenkonzept:** Ausgehend vom organisationsweiten Benutzer-, Rechte- und Rollenkonzept müssen entsprechende Regelungen für das System erstellt werden (siehe auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

- **Administration:** Wie soll das System administriert werden? Werden alle Einstellungen lokal vorgenommen oder der Server in ein zentrales Administrations- und Konfigurationsmanagement integriert?
- **Partitions- und Dateisystem-Layout:** In der Planungsphase sollte eine erste Abschätzung des benötigten Plattenplatzes durchgeführt werden. Zur einfacheren Administration und Wartung ist es empfehlenswert, so weit wie möglich eine Trennung von Betriebssystem (Systemprogramme und -konfiguration), Anwendungsprogrammen und -daten (beispielsweise Datenbank-Server und Daten) und gegebenenfalls Benutzerdaten vorzunehmen. Verschiedene Betriebssysteme bieten hierfür unterschiedliche Mechanismen an (Aufteilung in Laufwerke unter Windows, Filesysteme unter Unix). Oft kann es sinnvoll sein, bestimmte Daten sogar auf einer eigenen Festplatte oder einem eigenen Plattensystem zu speichern. Dies erlaubt es beispielsweise, bei einer Neuinstallation oder einem Update des Systems die Daten auf den anderen Partitionen ohne Umkopieren zu übernehmen.
  Falls auf dem Server Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so wird der Einsatz verschlüsselter Dateisysteme dringend empfohlen. Dabei brauchen nicht notwendigerweise alle Dateisysteme verschlüsselt zu werden, sondern es wird oft ausreichend sein, für den Teil des Dateisystems eine Verschlüsselung vorzusehen, auf dem die Daten selbst gespeichert werden. Dies wird durch eine entsprechende Planung des Partitions- und Dateisystemlayouts erleichtert. Bei der Auswahl einer Verschlüsselung von einzelnen Dateien und Verzeichnissen sollte den Anwendern die Auswahl abgenommen werden, ob die Dateien verschlüsselt werden oder unverschlüsselt abgelegt werden.
  In der Planungsphase sollte die vorgesehene Aufteilung der Partitionen und deren Größe dokumentiert werden.
- **Netzdienste und Netzanbindung:** In Abhängigkeit von den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, die auf dem Server gespeichert oder verarbeitet werden sollen, muss die Netzanbindung des Servers geplant werden.
  Generell wird empfohlen, einen Server nicht direkt im selben IP-Subnetz zu platzieren wie die Clients, die auf den Server zugreifen sollen. Wenn der Server zumindest durch einen Router von den Clients getrennt ist, dann bestehen wesentlich besser Möglichkeiten zur Steuerung des Zugriffs und zur Erkennung von Anomalien im Netzverkehr, die auf mögliche Probleme hindeuten.
  Ein Server, der Daten mit einem hohen Schutzbedarf bezüglich Vertraulichkeit oder Integrität speichert oder verarbeitet, sollte in einem eigenen IP-Subnetz angesiedelt werden und zumindest durch einen Paketfilter vom Rest des Netzes getrennt werden. Bei einem sehr hohen Schutzbedarf sollte ein Application Level Gateway eingesetzt werden.
  Bei normalem Schutzbedarf kann ein Server, der ausschließlich von Clients aus dem internen Netz genutzt wird, ausnahmsweise auch im selben Teilnetz angesiedelt werden. Es wird jedoch empfohlen, auch in diesem Fall den Server bei anstehenden Umstellungen in der Netzstruktur in ein eigenes Teilnetz zu verlegen.
  Abhängig vom festgelegten Einsatzzweck des Rechners wird außerdem eventuell der Zugriff auf bestimmte Dienste im Netz (etwa Web-, File-, Datenbank-, Druck-, DNS oder Mailserver) benötigt. Dies muss bereits im Rahmen der Planung berücksichtigt werden, damit nicht zu einem späteren Zeitpunkt Schwierigkeiten beispielsweise durch zu geringe Übertragungskapazitäten oder Probleme mit zwischengeschalteten Sicherheitsgateways entstehen.
  Neben dem eigentlichen Dienst, für den ein Server aufgesetzt wird, werden oft noch andere Dienste benötigt, um den Server effizient nutzen und

administrieren zu können. Beispielsweise wird für eine Administration über das Netz ein sicherer Zugang (beispielsweise SSH, siehe auch M 5.64 *Secure Shell*) benötigt, oder die Dateien für ein Webangebot können über das Netz auf den Webserver übertragen werden. Wenn die dadurch entstehende Netzkommunikation über unsichere Netze stattfindet, so müssen geeignete sichere Protokolle benutzt werden. Außerdem dürfen die Dienste nur autorisierten Benutzern und Rechnern zur Verfügung gestellt werden. Dies kann durch eine Passwortvergabe, durch den Einsatz eines Paketfilters (siehe beispielsweise M 4.238 *Einsatz eines lokalen Paketfilters* oder Baustein B 3.301 *Sicherheitsgateway (Firewall)*) oder anderer Mechanismen realisiert werden. Kein Dienst sollte in einem unsicheren Netz wie dem Internet bereitgestellt werden, wenn dies nicht ausdrücklich vorgesehen ist.

In der Planungsphase sollte eine Übersicht über die vorgesehenen und benötigten Netzdienste sowie über die in diesem Zusammenhang nötigen Netzverbindungen erstellt werden. Allgemein ist es wichtig, bereits in der Planungsphase zu überlegen, wie groß die Abhängigkeit eines Systems vom Funktionieren der Netzanbindung sein darf.

- **Tunnel oder VPN:** Falls bereits in der Planungsphase absehbar ist, dass auf das System über unsichere Netze zugegriffen werden muss, sollten frühzeitig geeignete Lösungen untersucht werden. Beispielsweise kann der Zugriff über ein VPN erfolgen.
- **Monitoring:** Um die Verfügbarkeit und Auslastung des Systems und der angebotenen Dienste zu beobachten, kann ein Monitoring-System eingesetzt werden. Dafür wird auf einem weiterem Server ein Monitoring-Daemon installiert, dem ein lokal installierter Agent die zu überwachenden Daten sendet. Im weiterem besteht die Möglichkeit, die Aktivitäten von Netzdiensten, die von externen Systemen angeboten werden, zu überwachen. Bei Problemen kann zum Beispiel automatisch ein Administrator alarmiert werden.
- **Protokollierung**: Die Protokollierung von Meldungen des Systems und der eingesetzten Dienste spielt eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen, und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf dem System oder auf einem zentralen Logserver im Netz gespeichert werden sollen.

  Sinnvoller Weise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Daten ausgewertet werden sollen.
- **Hochverfügbarkeit**: Falls an die Verfügbarkeit des Systems und seiner Dienste besondere Anforderungen gestellt werden, so sollte bereits in der Planungsphase überlegt werden, wie diese Anforderungen erfüllt werden können (siehe auch M 6.43 *Einsatz redundanter Windows-Server*).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

Prüffragen:

- Wird ein Servereinsatz im Vorfeld grundlegend nach dem Prinzip des Top-Down-Entwurfs geplant?
- Sind in einem Grobkonzept alle Anforderungen an Dienste, IT-Sicherheitsziele, Aufgaben und Funktionalitäten berücksichtigt?

# M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Die Sicherheitsvorgaben für jeden Server ergeben sich aus der organisationsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für den Server oder eine Gruppe von Servern zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen zum Betrieb des Servers treffen. Zur Verbesserung der Übersichtlichkeit kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Server, die lediglich Daten mit normalem Schutzbedarf speichern und verarbeiten, kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei einem Server, auf dem Daten mit hohem Schutzbedarf gespeichert oder verarbeitet werden, wird grundsätzlich eine restriktive Strategie empfohlen. Für Server mit besonderem Schutzbedarf bezüglich eines der drei Grundwerte sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Regelungen zur physikalischen Zugriffskontrolle: Ein Server sollte grundsätzlich in einem abschließbaren Rechnerraum oder Serverschrank aufgestellt oder eingebaut werden. Dabei ist zu regeln, wer Zutritt zu dem Raum beziehungsweise Zugriff auf den Server selbst erhält.
- Regelungen für die Arbeit der Administratoren und Revisoren:
    - Nach welchem Schema werden Administrationsrechte vergeben? Welcher Administrator darf welche Rechte ausüben und wie erlangt er diese Rechte?
    - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole,

über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vier-Augen-Prinzip?
- Vorgaben für die Installation und Grundkonfiguration
  - Welche Installationsmedien werden zur Installation verwendet?
  - Soll ein zentraler Authentisierungsdienst genutzt werden oder erfolgt die Benutzerverwaltung und -authentisierung nur lokal?
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Vorgaben für die zu installierenden Softwarepakete.
  - Falls bei der Planung für den Server festgelegt wurde, dass Teile des Dateisystems verschlüsselt werden sollen, so ist es empfehlenswert, an dieser Stelle festzulegen, wie dies zu geschehen hat:
    - Welche Teile des Dateisystems sollen verschlüsselt werden?
    - Welcher Mechanismus zur Einbindung des verschlüsselten Dateisystems soll verwendet werden?
    - Welche Kryptoalgorithmen und Schlüssellängen sollen verwendet werden?
    - Welche Daten sollen in den verschlüsselten Dateisystemen gespeichert werden?
    - Wie werden die verschlüsselten Dateisysteme in das Backup einbezogen?

    Es empfiehlt sich, beim Einsatz verschlüsselter Dateisysteme hierfür ein eigenes Konzept zu erstellen und die Details der Konfiguration besonders sorgfältig zu dokumentieren, da im Fall von Problemen (Verlust des Schlüssels oder der Passphrase zum Schlüssel, inkorrekte Konfiguration oder ähnliches) die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein können.
  - Regelungen zu Erstellung und Pflege von Dokumentation
- Vorgaben für den sicheren Betrieb
  - Welcher Benutzerkreis darf sich lokal auf dem System anmelden?
  - Welche Benutzer erhalten Zugriff über das Netz? Welche Protokolle dürfen verwendet werden?
  - Auf welche Ressourcen dürfen die Benutzer zugreifen?
- Vorgaben für die Passwortnutzung (Passwortregeln, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Wer darf das System herunterfahren?
- Netzkommunikation und -dienste
  - Soll ein lokaler Paketfilter aufgesetzt werden?
  - Welche Netzdienste werden von dem Server angeboten?
  - Welche Authentisierungsverfahren sollen für die angebotenen Dienste gewählt werden?
  - Auf welche externen Netzdienste soll von dem Rechner aus zugegriffen werden können?
  - Soll ein verteiltes Dateisystem eingebunden werden?
    Verteilte Dateisysteme, bei denen die Nutzdaten unverschlüsselt übertragen werden, sollten nur im internen Netz verwendet werden.

Soll ein verteiltes Dateisystem über ein unsicheres Netz hinweg genutzt werden, so muss es durch zusätzliche Maßnahmen (kryptographisch geschütztes VPN, Tunneling) gesichert werden.

- Protokollierung

  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert? Werden sie lokal gespeichert oder soll ein zentraler Server eingesetzt werden, an dem die einzelnen Systeme im Netz ihre Protokollierungsinformationen schicken?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
  - Wer hat Zugriff auf die Logdateien?
  - Ist gewährleistet, dass personenbezogene Informationen nicht an unbefugte Personen gelangen?
  - Wie lange sollen die Logdateien gespeichert werden?

Anhand der oben genannten Punkte kann eine Checkliste erstellt werden, die bei Audits oder Revisionen hilfreich sein kann.

Die Verantwortung für die Sicherheitsrichtlinie liegt beim Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Prüffragen:

- Existiert eine Sicherheitsrichtlinie mit dem definierten Sicherheitsniveau für den Betrieb des Servers?
- Berücksichtigt die Sicherheitsrichtlinie des Servers alle zur Erreichung des angestrebten Sicherheitsniveaus notwendigen Strategien, Vorgaben und Regelungen?
- Werden die Inhalte und die Umsetzung der Sicherheitsrichtlinie regelmäßig aktualisiert und technisch überprüft?

# M 2.317 Beschaffungskriterien für einen Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Beschaffer

Die Beschaffung eines Servers betrifft sowohl die Hard- als auch die Software, aus der der Server aufgebaut werden soll. Werden bei der Beschaffung eines Servers Fehler gemacht, so kann dies schwerwiegende Folgen auf den sicheren Betrieb eines Netzes haben, da mit ungeeigneter Hard- und Software das angestrebte Sicherheitsniveau unter Umständen nur schwer erreichbar ist.

Bevor ein Server beschafft wird, muss daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass der Server im praktischen Betrieb den Anforderungen genügt.

Auch rein funktionale Merkmale von Servern können Auswirkungen auf die Informationssicherheit haben. Meist ist dann der Grundwert Verfügbarkeit betroffen, beispielsweise wenn ein Server wegen unzureichender Speicherausstattung nicht die geforderten Antwortzeiten oder Durchsatzraten erreicht. Außerdem spielt die Unterstützung durch den Hersteller eine nicht zu vernachlässigende Rolle, wenn es beispielsweise darum geht, dass zeitnah Patches für Sicherheitslücken zur Verfügung gestellt werden.

Aus dem Blickwinkel der Informationssicherheit sind zentrale Anforderungen an Server, dass

- Hard- und Software so ausgelegt sind, dass die Anforderungen an die Verfügbarkeit des Servers und die Integrität der Daten erfüllt werden können,
- die Administration über sichere Protokolle möglich ist,
- die Benutzerverwaltung es erlaubt, das organisationsweite Rollenkonzept entsprechend umzusetzen, und
- dass es gegebenenfalls möglich ist, besonders sensitive Daten zu verschlüsseln.

Nachfolgend werden einige Anforderungen aufgelistet, die bei der Beschaffung von Servern berücksichtigt werden sollten:

- Grundlegende funktionale Anforderungen
  - Unterstützt das Gerät alle benötigten Hardwareschnittstellen?
  - Unterstützt die Software alle benötigten Protokolle und Datenformate?
- Sicherheit
  - Unterstützt das System sichere Protokolle zur Administration?
    Wenn Server nicht über ein eigenes Administrationsnetz administriert werden, muss die Administration mit Hilfe von sicheren Netzprotokollen möglich sein.
- Wartbarkeit
  - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches für die Software an?
    Es ist insbesondere wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.
  - Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?

Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich.

- Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
  Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Ansprüche an die Verfügbarkeit der Geräte abgedeckt werden können.
- Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
  Dieser Punkt sollte Bestandteil des abgeschlossenen Wartungsvertrags sein. Beim Abschluss des Vertrags ist auf die Sprache der zur Verfügung gestellten Hotline des Herstellers zu achten.

- Zuverlässigkeit/Ausfallsicherheit

  - Gibt es verlässliche Informationen zur Zuverlässigkeit und Ausfallsicherheit von Hard- und Software?
  - Bietet der Hersteller gegebenenfalls Hochverfügbarkeitslösungen an?
    Wenn die Verfügbarkeitsanforderungen nicht über Wartungsverträge abgedeckt werden können, sollte das System Hochverfügbarkeitslösungen unterstützen.

- Benutzerfreundlichkeit

  - Lässt sich das Produkt einfach installieren, konfigurieren, administrieren und benutzen?
    Es sollten darüber hinaus Schulungen für das Produkt angeboten werden.

- Kosten

  - Wie hoch sind die Anschaffungskosten für Hard- und Software?
  - Wie hoch sind die voraussichtlichen laufenden Kosten (Wartung, Betrieb, Support)?
    Diese Kosten müssen bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden (Reaktionszeiten, Hotline, Qualifikation des Personals, etc.).
  - Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal?
  - Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden?
    Diese Frage sollte bereits in der Planungsphase beantwortet werden. Wenn beispielsweise bereits ein Netz-Management-System im Einsatz ist, sollte die Kompatibilität mit den zu beschaffenden Geräten geprüft werden.
    Zudem sollte der Aufwand zur Integration in eine bestehende Infrastruktur beachtet werden.
  - Wie hoch sind die Kosten für die Schulung von Administratoren?
  - Mit welchen Kosten muss gerechnet werden, wenn wegen erhöhter Kapazitätsanforderungen ein Upgrade der Hardware notwendig ist?
    Die Kosten können in diesem Fall erheblich höher ausfallen, als die Kosten für die Hardware selbst, da in etlichen Lizenzmodellen von Softwareanbietern der Lizenzpreis von der Anzahl der Prozessoren oder dem Prozessortakt abhängt, so dass bei einem Hardwareupgrade auch gleichzeitig eine neue Programmlizenz erforderlich sein kann.

- Protokollierung
    - Welche Möglichkeiten der Protokollierung sind vorhanden?
      Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:
    - Ist der Detailgrad der Protokollierung konfigurierbar?
    - Werden durch die Protokollierung alle relevanten Daten erfasst?
    - Unterstützt das System zentrale Protokollierung (z. B. Syslog)?
    - Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?
    - Werden Alarmierungsfunktionen unterstützt?
- Infrastruktur
    - Abmessungen und Kompatibilität mit Schutzschränken
      Auch der Platzbedarf eines Servers ist bei der Beschaffung zu berücksichtigen. Kann das Gerät in die vorgesehenen Schutzschränke eingebaut werden (Formfaktor, Gewicht, Befestigungselemente)?
    - Stromversorgung und Abwärme
      Vom Hersteller sollten Angaben zum Stromverbrauch und zu den Anforderungen an die Umgebungstemperatur verfügbar sein. Reicht die vorhandene Kapazität der Stromversorgung und der USV aus? Reicht die vorhandene Kühlleistung zur Abfuhr der Abwärme des Geräts aus?

Die Anforderungen und die auf ihrer Basis getroffenen Auswahlentscheidungen sollten so dokumentiert werden, dass zu einem späteren Zeitpunkt nachvollziehbar ist, wie die Entscheidung zu Stande gekommen ist.

Prüffragen:

- Existiert eine Anforderungsliste, die alle erforderlichen Merkmale zur Beschaffung von Servern berücksichtigt?

# M 2.318 Sichere Installation eines IT-Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem die Planung eines neuen IT-Systems (siehe M 2.315 *Planung des Servereinsatzes* beziehungsweise M 2.321 *Planung des Einsatzes von Client-Server-Netzen*) abgeschlossen und eine Sicherheitsrichtlinie (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server* beziehungsweise M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*) erstellt wurde, kann mit der Installation des Systems begonnen werden.

Es ist empfehlenswert, zunächst ein kurzes Installationskonzept entsprechend den funktionalen Anforderungen aus der Planung und den Vorgaben der Sicherheitsrichtlinie zu erstellen. Prinzipiell ist es vorteilhaft, die Installation in zwei Phasen vorzunehmen: Zunächst wird ein Grundsystem installiert und konfiguriert, anschließend werden die weiteren benötigten Dienste und Anwendungen eingerichtet. Die Installationsprogramme der meisten Betriebssysteme unterstützen diese Vorgehensweise mehr oder weniger gut.

Die beschriebenen Schritte brauchen nicht notwendigerweise alle für jedes IT-System erneut durchgeführt zu werden. Dies könnte sogar insofern kontraproduktiv sein, als die ständige Wiederholung die Gefahr von Fehlern erhöht. Es wird daher empfohlen, die beschriebenen Schritte einmal besonders sorgfältig auf einem Referenz-System durchzuführen, die nötigen Konfigurationen genau zu dokumentieren und so ein angepasstes Installationskonzept für das betreffende Betriebssystem zu erhalten. Dabei muss beachtet werden, dass dieses Installationskonzept auch bei Änderungen am Betriebssystem, die kein komplett neues Release darstellen (Service-Packs, Update-Releases oder ähnliches) überprüft und gegebenenfalls angepasst werden muss.

Bei virtuellen IT-Systemen wird in den seltensten Fällen für jede Instanz ein abgeändertes Betriebssystem installiert, hier wird in der Regel ein Grundsystem erstellt, dass in die Instanz kopiert und als eigenständiger Klon gestartet wird. In dieser Instanz werden im nächsten Schritt die benötigten Serverdienste oder Anwendungsprogramme installiert und zu jedem späteren Zeitpunkt kann ein neuer Klon generiert werden, um beispielsweise mehrere Instanzen mit identischen Serverdiensten oder Anwendungsprogrammen zu erhalten. Damit können sich aber auch Fehlentscheidungen und falsche Einstellungen, die bei der Erstellung des Grundsystems getroffen wurden, bei der Installation der Klone auf zahlreiche weitere Instanzen vererben. Für jeden einzelnen Klon sollten daher alle Empfehlungen dieser Maßnahme ebenfalls sorgfältig umgesetzt werden.

### Installation

Diese Maßnahme beinhaltet nur Empfehlungen für die ersten Schritte einer Installation und nicht für die endgültige Konfiguration für den geplanten Einsatzzweck. Die weitergehenden Konfigurationsschritte sind sehr stark vom jeweiligen System und Einsatzgebiet abhängig und werden in eigenen Maßnahmen behandelt.

Während der Installation und der späteren Konfiguration sollten zumindest die wichtigen Schritte so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Beispielsweise kann eine Checkliste für

die Installationerstellt werden, auf der beendete Schritte abgehakt und vorgenommene Einstellungen vermerkt werden können. Eine entsprechende Dokumentation ist für eine Fehleranalyse oder spätere Neuinstallation hilfreich. Dabei sollte beachtet werden, dass neben dem Autor auch weitere, auf diesem Gebiet eventuell weniger spezialisierte, Administratoren auf die Dokumentation zurückgreifen müssen. Daher ist es wichtig, dass die Dokumentation gut strukturiert und verständlich ist.

Wird das IT-System von Datenträgern wie DVDs oder anderen Speichermedien installiert, wird empfohlen, die Installation und Grundkonfiguration offline oder zumindest in einem sicheren Netz (Installations- oder Administrationsnetz) durchzuführen. Generell sollte verhindert werden, dass andere IT-Systeme während der Installation auf das zu installierende IT-System zugreifen können. Dies ist wichtig, weil während der Installation meist noch keine Passwörter vergeben wurden und keine Schutzmechanismen aktiv, aber eventuell schon Zugriffe möglich sind. Falls die Installation mehrerer IT-Systeme teilweise über das Netz erfolgen soll (beispielsweise Nachladen von Paketen), so wird empfohlen, einen Installationsserver im Administrationsnetz zu nutzen.

Insbesondere beim Betriebssystem selbst ist es wichtig, dass die installierte Version aus einer vertrauenswürdigen Quelle stammt. Dies ist besonders wichtig, wenn beispielsweise CD-Images aus dem Internet heruntergeladen wurden. In diesem Fall sollte unbedingt geprüft werden, ob digitale Signaturen der Pakete verfügbar sind, die zur Verifikation von Integrität und Authentizität der Pakete verwendet werden können (siehe auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*). Pakete und CD-Images, für die keine digitalen Signaturen oder wenigstens Prüfsummen existieren, sollten möglichst nicht eingesetzt werden.

Bei der Einrichtung der Festplattenpartitionen muss das in der Planungsphase (siehe M 2.315 *Planung des Servereinsatzes* bzw. M 2.321 *Planung des Einsatzes von Client-Server-Netzen*) erstellte Konzept umgesetzt werden. Wenn ein verschlüsseltes Dateisystem eingesetzt werden soll, so muss es meist initialisiert werden, bevor Daten hineinkopiert werden können, denn oft lässt sich ein Dateisystem nicht im Nachhinein verschlüsseln. Auch einige RAID-Systeme und -Level erfordern eine Konfiguration, die abgeschlossen sein muss, bevor die betreffenden Dateisysteme eingerichtet werden können.

**Einrichtung der Hardware und des Bootloaders**

Während der ersten Installationsphase braucht prinzipiell nur derjenige Teil der Hardware konfiguriert zu werden, der für das Booten des Systems (beispielsweise RAID-Laufwerke, verschlüsselte Dateisysteme oder ähnliches) und die Fortführung der Installation (gegebenenfalls Netzkarten) benötigt wird. Die restliche Hardware kann in der zweiten Phase der Installation eingerichtet werden.

Am Ende der Grundinstallation steht meist die Installation und Konfiguration eines Bootloaders, der dafür sorgt, dass beim Starten des Systems das Betriebssystem geladen wird. Meist bietet der Bootloader ein Auswahlmenü, das die Auswahl zwischen verschiedenen installierten Betriebssystemen oder Konfigurationen erlaubt. Bei der Konfiguration des Bootloaders muss mit entsprechender Sorgfalt vorgegangen werden, damit das System überhaupt starten kann. Die vorgenommene Konfiguration sollte dokumentiert werden. Manche Systeme bieten zu diesem Zeitpunkt der Installation auch die Möglichkeit, ein

Bootmedium zu erstellen, mit dem das System im Notfall gestartet werden kann.

Bei Clients und bei Servern, die nicht physisch gegen unautorisierten Zugriff geschützt sind, sollte der Bootloader nach Möglichkeit mit einem Passwort abgesichert werden.

Sofern dies nicht bereits automatisch geschehen ist, sollte spätestens beim Abschluss der Grundinstallation auch die Protokollierung der Systemereignisse aktiviert werden. Die Protokolldaten können bei Problemen bei der weiteren Installation und Konfiguration wertvolle Informationen liefern.

**Aktualisierung**

Wird das System von einer CD, DVD oder einem anderen "Offline-Medium" installiert, so sollte nach der Grundinstallation überprüft werden, ob zwischenzeitlich Aktualisierungen oder Sicherheitspatches vom Hersteller oder Distributor veröffentlicht wurden (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* und M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

**Installation der jeweiligen Serverdienste und Anwendungsprogramme**

Nachdem das Betriebssystem installiertund Grundkonfiguration und Aktualisierung abgeschlossen wurde, können die jeweiligen Serverdienste installiert und konfiguriert werden. Sowohl auf Clients als auch Servern werden in der Regel Serverdienste zur Fernadministration benötigt. Bei Servern kommen die eigentlichen Serverdienste hinzu, bei Clients müssen in der Regel grafische Benutzeroberflächen und Anwendungsprogramme installiert und eingerichtet werden. Hierfür wird ein analoges Vorgehen wie für das Betriebssystem selbst empfohlen.

Prüffragen:

- Liegt ein Installationskonzept vor, das die funktionalen Anforderungen und sicherheitsrelevanten Vorgaben berücksichtigt?
- Existiert im Installationskonzept eine Regelung zur Dokumentation der Installation und Konfiguration?
- Existiert im Installationskonzept eine Regelung zur Offline-Installation, sowie zur Verwendung von vertrauenswürdigen Installationsquellen und -medien?

# M 2.319 Migration eines Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sollen die Dienste des Servers von einem anderen System übernommen werden, so muss der Übergang geplant werden. Insbesondere dann, wenn besondere Anforderungen an die Verfügbarkeit der Dienste bestehen, ist eine besonders sorgfältige Planung erforderlich.

In den meisten Fällen ist es empfehlenswert, den "Funktionsübergang" auf das Ersatzsystem außerhalb der normalen Betriebszeiten durchzuführen. Falls dies nicht möglich ist müssen Maßnahmen getroffen werden, die sicher stellen, dass weder Daten beim Funktionsübergang verloren gehen, noch untragbare Ausfallzeiten entstehen.

Für die Migration wichtiger Server muss deswegen vorab ein entsprechendes Migrationskonzept erstellt werden. Dabei sollten insbesondere folgende Punkte mit berücksichtigt werden:

- Migration der Daten und Konfiguration
  Nach der Übertragung der Daten auf das neue System muss überprüft werden, ob die Daten vollständig und korrekt übertragen wurden.
  Wenn auf dem neuen System eine neue Version der Serversoftware eingesetzt werden soll, so muss sichergestellt sein, dass die neue Version mit den vorhandenen Datenbeständen korrekt umgehen kann. Dies betrifft nicht nur die Aufgabe, Daten der alten Version korrekt einzulesen, sondern insbesondere auch, diese Daten zu modifizieren oder neue Datensätze hinzuzufügen. Gerade in solchen Fällen tauchen oft Probleme auf, so dass gründliche Tests empfohlen werden.
  Außerdem ist es wichtig, dass die Konfiguration des alten Dienstes auf dem neuen System korrekt übernommen oder zumindest "funktional äquivalent nachgebaut" werden kann.
- Kompatibilität des Dienstes
  Es muss sichergestellt sein, dass der Dienst auf dem Ersatzsystem mit dem ursprünglichen Dienst kompatibel ist. Dies ist insbesondere dann von Bedeutung, wenn im Rahmen der Migration auf dem neuen System eine neue Version des Serverprogramms eingesetzt werden soll, auf die jedoch weiter mit Clients der alten Version zugegriffen wird. Selbst dann, wenn ein Hersteller Berichte von Referenzkunden über erfolgreiche Migrationen vorlegt oder "problemlose Abwärtskompatibilität", "vollständige Rückwärtskompatibilität mit früheren Versionen" oder ähnliches zusichert, wird dingend empfohlen, vorab entsprechende Tests durchzuführen.
- Kryptographische Schlüssel
  Falls Teile der Daten oder der Dateisysteme eines Servers verschlüsselt sind, so kommt der Sicherung oder Übertragung der entsprechenden Schlüssel besondere Bedeutung zu: Oft sind diese an einer anderen Stelle auf dem System gespeichert als die Nutzdaten selbst. Beispielsweise dann, wenn die Daten mit Hilfe systemnaher Programme blockweise direkt kopiert werden oder die Festplatten aus dem alten in das neue System umgebaut werden, muss sichergestellt sein, dass auch die Schlüssel mit übertragen werden, da sonst kein Zugriff mehr auf die verschlüsselten Daten möglich ist.
- Umstellung von Namen und Adressen
  Falls auf einen Server nur über seine IP-Adresse oder einen DNS-Namen zugegriffen wird, so ist eine Migration meist relativ unproblematisch, da in diesem Fall einfach das Ersatzsystem die IP-Adresse des alten Sy-

stems übernehmen kann. Problematischer wird es beispielsweise, wenn das neue System den selben DNS-Namen bekommen soll, aber nicht die IP-Adresse übernehmen kann. Denn es dauert eine gewisse Zeit, bis die Änderung der Adresse bei allen Clients "angekommen" ist. Solche Latenzzeiten müssen bei der Planung der Migration berücksichtigt werden.
Falls auf das System anders zugegriffen wird (beispielsweise wenn die Adresse von einem anderen Verzeichnisdienst aufgelöst wird), so muss berücksichtigt werden, dass auch die Änderung auf diesem Weg eventuell ebenfalls eine gewisse Latenzzeit hat, bevor sie wirksam wird.
Das größte Problem entsteht dann, wenn Clients auf den Servern über eine Anwendung zugreifen, bei der die IP-Adresse oder der Name des Servers in einer lokalen Konfigurationsdatei oder -datenbank gespeichert sind. Falls eine größere Anzahl Clients manuell umkonfiguriert werden müssen, so kann dies eine erhebliche Zeit in Anspruch nehmen und muss vorab geplant werden.

- Dauerhafte Verbindungen
  Falls es Clients gibt, die länger bestehende oder gar dauerhafte Netzverbindungen zu dem Dienst aufbauen, der auf einen neuen Rechner migriert werden muss (dies ist beispielsweise bei manchen Datenbankanwendungen er Fall), so muss dies bei der Migration berücksichtigt werden. Gegebenenfalls müssen diese Verbindungen auf den betreffenden Clients manuell beendet werden. Auch hierfür ist eine entsprechende Planung erforderlich.

Für die Durchführung der Migration ist es empfehlenswert, im Rahmen der Erarbeitung des Migrationskonzeptes eine Checkliste zu erstellen, die bei der Umstellung Schritt für Schritt durchgegangen werden kann. Bei der Planung der Migration und der Erstellung der Checkliste muss darauf geachtet werden, dass jeder Schritt nur von den vorhergehenden Schritten abhängig ist.

Bei hohen Anforderungen an die Verfügbarkeit des Dienstes sollte der gesamte Übergang vorab in einer Testumgebung unter möglichst realistischen Bedingungen geprobt werden, um mögliche Probleme frühzeitig zu identifizieren und zu beseitigen.

Prüffragen:

- Gibt es ein Migrationskonzept, das unter anderem die Verfügbarkeit von Funktionen, Diensten und Daten berücksichtigt?

# M 2.320 Geregelte Außerbetriebnahme eines Servers

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Soll ein Server außer Betrieb genommen werden, so darf dies nicht unvorbereitet und ohne Ankündigung für die Benutzer geschehen, sondern es muss eine Reihe von Maßnahmen ergriffen werden, um sicher zu stellen, dass

- keine wichtigen Daten verloren gehen,
- keine Dienste oder Systeme beeinträchtigt werden, die von dem Server abhängen, und dass
- keine sensitiven Daten auf den Datenträgern des Servers zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf dem System gespeichert sind und von wo aus darauf zugegriffen wird. Ausgehend von diesen Informationen sollte eine Planung für die Außerbetriebnahme des Servers erfolgen. Dabei sollten die folgenden Punkte berücksichtigt werden:

- Datensicherung
  Vor der Außerbetriebnahme des Servers müssen Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert (beispielsweise auf Magnetbändern, CD- oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.
- Ersatzsystem
  Wenn die von dem Server bereitgestellten Dienste weiter benötigt werden, so muss rechtzeitig ein angemessenes Ersatzsystem bereitgestellt werden. Für die entsprechende Planung, Beschaffung und Inbetriebnahme müssen entsprechende Ressourcen zur Verfügung stehen, siehe auch M 2.319 *Migration eines Servers*.
- Information der Benutzer
  Falls das System ersatzlos abgeschaltet wird, so müssen die Benutzer rechtzeitig über die bevorstehende Abschaltung informiert werden und gegebenenfalls die Gelegenheit erhalten, eigene Daten zu sichern.
- Entfernen von Verweisen auf das System
  Im Zuge der Außerbetriebnahme eines Systems müssen auch Verweise auf das System gelöscht werden. Dazu gehört beispielsweise das Löschen des DNS-Eintrags und der Einträge in sonstigen Verzeichnisdiensten sowie in Abhängigkeit vom Einsatzzweck weitere Verweise. Wird beispielsweise ein Webserver außer Betrieb genommen, so sollten Verweise auf diesen Server, die noch in eigenen Webseiten enthalten sind, gelöscht werden.
- Löschen der Daten auf dem abzuschaltenden System
  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder das logische Löschen mit den Löschfunktionen des Betriebssystems noch das Neuformatieren der Platten die Daten tatsächlich von den Festplatten entfernt. Mit geeigneter Software können Daten in solchen Fällen, oft sogar ohne großen Aufwand, wieder rekonstruiert werden. Weitere Hinweise

finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*.

- Löschen von Datensicherungsmedien
  Nach der Außerbetriebnahme eines Systems müssen gegebenenfalls auch die entsprechenden Datensicherungsmedien gelöscht oder unbrauchbar gemacht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.
- Entfernen sonstiger Informationen
  Oft enthalten Serversysteme weitere Daten (beispielsweise Konfigurationsdaten), die in einem nichtflüchtigen Speicher abgelegt sind, oder sind von außen beschriftet (beispielsweise mit dem Rechnernamen, der IP-Adresse und weiteren technischen Informationen). Diese Informationen sollten nach Möglichkeit vor der Weitergabe des Gerätes entfernt werden, da ein Angreifer auch aus solchen Informationen eventuell Hinweise für mögliche Angriffe ziehen kann.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden.

Prüffragen:

- Erfolgt die Außerbetriebnahme eines Servers unter Berücksichtigung der Verfügbarkeit von Funktionen, Diensten und Daten?
- Existiert eine Planung für die Vorgehensweise zur Außerbetriebnahme des Servers?

# M 2.321 Planung des Einsatzes von Client-Server-Netzen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine grundlegende Voraussetzung dafür, dass Clients sicher betrieben werden können, ist ein angemessenes Maß an Planung im Vorfeld.

Die Planung des Einsatzes kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben sollen die Clients erfüllen? Auf welche Dienste muss von den Clients zugegriffen werden können? Gibt es besondere Anforderungen an die Verfügbarkeit der Systeme oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Sollen in dem System bestimmte Hardware-Komponenten eingesetzt werden? Dies kann beispielsweise für die Auswahl des Betriebssystems wichtig sein.
- Welche Anforderungen an die Hardwareausstattung (CPU, Arbeitsspeicher, Kapazität der Festplatten, Kapazität des Netzes etc.) ergeben sich aus den allgemeinen Anforderungen?
- Handelt es sich bei dem Netz, in dem die Clients eingesetzt werden sollen, um einen homogenen oder heterogenen Rechnerverbund?
- Dienen die Clients als Ersatz für vorhandene Systeme? Sollen von den alten Systemen Datenbestände oder Hardware-Komponenten übernommen werden?
- Sollen auf den Rechnern weitere Betriebssysteme mittels Multiboot installiert werden?

Es wird empfohlen, ein oder mehrere generische Anforderungsprofile (beispielsweise "Allgemeiner Büro-PC", "Entwicklungsrechner" oder "Administrations-Client") zu erstellen, die bei konkreten Planungen als Grundlage dienen können.

Die folgenden Teilkonzepte sollten bei der Planung berücksichtigt werden:

- **Authentisierung und Benutzerverwaltung:** Welche Arten der Benutzerverwaltung und Benutzer-Authentisierung sollen genutzt werden? Werden Benutzer nur lokal verwaltet oder soll ein zentrales Verwaltungssystem genutzt werden? Soll das System auf einen zentralen, netzbasierten Authentisierungsdienst zugreifen oder wird nur eine lokale Authentisierung benötigt? Mehr Informationen dazu finden sich in M 4.133 *Geeignete Auswahl von Authentikationsmechanismen* und M 4.250 *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*.
- **Benutzer- und Gruppenkonzept:** Ausgehend vom organisationsweiten Benutzer-, Rechte- und Rollenkonzept müssen entsprechende Regelungen für die Clients erstellt werden (siehe auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

- **Administration:** Wie sollen die Systeme administriert werden? Werden alle Einstellungen lokal vorgenommen oder werden die Clients in ein zentrales Administrations- und Konfigurationsmanagement integriert?
- **Partitions- und Dateisystem-Layout:** In der Planungsphase sollte eine erste Abschätzung des benötigten Plattenplatzes durchgeführt werden. Zur einfacheren Administration und Wartung ist es empfehlenswert, so weit wie möglich eine Trennung von Betriebssystem (Systemprogramme und -konfiguration), Anwendungsprogrammen und -daten (beispielsweise Datenbank-Server und Daten) und gegebenenfalls Benutzerdaten vorzunehmen. Verschiedene Betriebssysteme bieten hierfür unterschiedliche Mechanismen an (Aufteilung in Laufwerke unter Windows, Dateisysteme unter Unix). Oft kann es sinnvoll sein, bestimmte Daten sogar auf einer eigenen Festplatte oder einem eigenen Plattensystem zu speichern. Dies erlaubt es beispielsweise, bei einer Neuinstallation oder einem Update des Systems die Daten auf den anderen Partitionen ohne Umkopieren zu übernehmen.
  In der Planungsphase sollte die vorgesehene Aufteilung der Partitionen und deren Größe dokumentiert werden.
  Falls auf den Clients Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so wird der Einsatz verschlüsselter Dateisysteme dringend empfohlen. Dabei brauchen nicht notwendigerweise alle Dateisysteme verschlüsselt zu werden, sondern es wird oft ausreichend sein, für den Teil des Dateisystems eine Verschlüsselung vorzusehen, auf dem die Daten selbst gespeichert werden. Dies wird durch eine entsprechende Planung des Partitions- und Dateisystemlayouts erleichtert.
  Bei besonderen Anforderungen an die Vertraulichkeit der Daten, die auf den Clients gespeichert sind, kann es erforderlich werden, die Systeme mit einem Verschlüsselungsprogramm auszustatten, das die gesamte Festplatte verschlüsselt und bereits vor dem Start des Betriebssystems eine Benutzer-Authentisierung (beispielsweise über eine Chipkarte) durchführt ("Pre-Boot-Authentication").
- **Netzdienste und Netzanbindung:** In Abhängigkeit von den Sicherheitsanforderungen der Daten, auf die von den Clients aus zugegriffen werden muss, muss die Netzanbindung der Clients geplant werden.
  Abhängig vom festgelegten Einsatzzweck der Rechner wird außerdem eventuell der Zugriff auf weitere Dienste im Netz benötigt. Dies muss bereits im Rahmen der Planung berücksichtigt werden, damit nicht zu einem späteren Zeitpunkt Schwierigkeiten beispielsweise durch zu geringe Übertragungskapazitäten oder Probleme mit zwischengeschalteten Sicherheitsgateways entstehen.
- **Monitoring:** Falls besondere Anforderungen an die Verfügbarkeit der Clients bestehen, so kann ein Monitoring-System eingesetzt werden. Dafür wird auf einem Server ein Monitoring-Daemon installiert, dem ein lokal installierter Agent die zu überwachenden Daten, beispielsweise zur Systemauslastung oder zum verbleibenden freien Speicherplatz, sendet. Bei Problemen kann zum Beispiel automatisch ein Alarm generiert werden.
- **Protokollierung:** Auch bei Clients spielt die Protokollierung eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen, und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf den Systemen oder auf einem zentralen Logserver im Netz gespeichert werden sollen.
  Sinnvollerweise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Protokolldaten ausgewertet werden sollen.

- **Hochverfügbarkeit:** Falls an die Verfügbarkeit der Clients besondere Anforderungen gestellt werden, so sollte bereits in der Planungsphase überlegt werden, wie diese Anforderungen erfüllt werden können.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

Prüffragen:

- Existieren ein Grob- bzw. die notwendigen Teilkonzepte zur Einsatzplanung von Client-Server-Netzen?
- Sind die Aufgaben der Clients und darauf aufbauend die benötigten Dienste definiert?
- Wurde für jeden Client-Typ unterschiedliche Anforderungsprofile erstellt?
- Wird bei der Betriebssystemauswahl die Nutzung spezieller Hardware berücksichtigt?
- Existieren Vorgaben zur Authentisierung und Benutzerverwaltung?
- Existieren Vorgaben zu den eingesetzten Netzdiensten und der Netzanbindung, die die Anforderungen der Einsatzprofile berücksichtigen?
- Werden in den Konzepten Anforderungen bzgl. Monitoring und Protokollierung definiert, die sich mit den Anforderungen und Schutzzielen decken?
- Werden die Einsatzkonzepte regelmäßig den aktuellen Erfordernissen angepasst?

# M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Die Sicherheitsvorgaben für alle Clients ergeben sich aus der organisationsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für die jeweilige Gruppe von Clients zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internet-Nutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Anwendern und anderen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen treffen. Zur Verbesserung der Übersichtlichkeit kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Clients mit normalem Schutzbedarf kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei Clients mit einem hohen Schutzbedarf wird grundsätzlich eine restriktive Strategie empfohlen. Für Clients mit besonderem Schutzbedarf bezüglich eines der drei Grundwerte sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Regelungen für die Arbeit der Benutzer der Clients:
  - Soll ein Client nur von jeweils einem einzelnen Benutzer genutzt werden, oder ist ein Betrieb mit wechselnden Benutzern vorgesehen?
  - Dürfen Benutzer bestimmte Konfigurationseinstellungen selbst ändern (beispielsweise Bildschirmhintergrund, Bildschirmschoner oder ähnliches) oder werden alle Einstellungen zentral vorgegeben?
  - Dürfen Benutzer auf bestimmte Bereiche des Systems keinen Zugriff haben? Diese Vorgaben haben in der Regel sowohl Auswirkungen auf die Rechtevergabe im System selbst als auch auf die Vorgaben für die Installation und Grundkonfiguration.
  - Welche Informationen dürfen die Benutzer lokal auf den Clients abspeichern? Generell sollten alle geschäftsrelevanten Informationen

zentral auf einem Server abgelegt werden, auf dem sie regelmäßig gesichert werden. Andernfalls muss dafür gesorgt werden, dass alle Informationen der Benutzer, die lokal auf den Clients abgespeichert sind, im Datensicherungskonzept des Clients berücksichtigt werden.
  - Sind die Benutzer gehalten, den Rechner abends herunterzufahren und auszuschalten, oder muss er rund um die Uhr in Betrieb sein? Für das Ausschalten von Client-Rechnern bei Arbeitsschluss sprechen beispielsweise Brandschutz und Stromersparnis. Darüber hinaus sind etwa Festplatten, die in Client-Computern eingesetzt werden, meist nicht für einen Dauerbetrieb geeignet. Ein durchgehender Betrieb der Rechner kann dennoch erwünscht sein, beispielsweise wenn über Nacht automatische Datensicherungen laufen oder die Rechner für andere Anwendungen genutzt werden.
- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Nach welchem Schema werden Administrationsrechte vergeben? Welcher Administrator darf welche Rechte ausüben und wie erlangt er diese Rechte?
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen?
  - Welche Vorgänge und Ereignisse müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vier-Augen-Prinzip?
- Vorgaben für die Installation und Grundkonfiguration:
  - Welche Installationsmedien werden zur Installation verwendet?
  - Soll ein zentraler Authentisierungsdienst genutzt werden oder erfolgt die Benutzerverwaltung und -authentisierung nur lokal?
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden. Es dürfen keine Sammelkonten, die verschiedene Benutzer mit derselben Kennung nutzen, verwendet werden.
  - Vorgaben für die zu installierenden Softwarepakete
  - Falls bei der Planung für die Clients festgelegt wurde, dass Teile des Dateisystems verschlüsselt werden sollen, so sollte an dieser Stelle festgelegt werden, wie dies zu geschehen hat.
  - Beim Einsatz verschlüsselter Dateisysteme sollte hierfür ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden, da im Fall von Problemen (Verlust des Schlüssels oder der Passphrase zum Schlüssel, inkorrekte Konfiguration oder ähnliches) die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein können.
  - Regelungen zu Erstellung und Pflege von Dokumentation
- Vorgaben für den sicheren Betrieb:
  - Welcher Benutzerkreis darf sich auf dem System anmelden?
  - Wie können sich die Benutzer gegenüber dem IT-System authentisieren? Generell sollte auf eine automatische Anmeldung, bei der die Benutzer ohne eine aktive Authentisierung beim Hochfahren des Clients angemeldet werden, verzichtet werden.
  - Erhalten Benutzer Zugriff auf ein oder mehrere LANs oder das Internet? Welche Protokolle dürfen verwendet werden? Bei Clients, die als Arbeitsplatzrechner in einer Organisation genutzt werden, ist es in der Regel nicht notwendig und oft auch nicht wünschenswert,

dass normale Benutzer über das Netz auf einen anderen Arbeitsplatzrechner zugreifen.
- Auf welche Ressourcen dürfen die Benutzer zugreifen?
- Es müssen Vorgaben für die Passwortnutzung erstellt werden (Passwortregeln, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern).
- Wer darf das System herunterfahren?
- Soll das System mit einer Boot-Sperre versehen werden, die ein Starten von externen Medien wie Disketten, CD-ROMs oder USB-Sticks verhindert?
  Es wird empfohlen, für den Normalbetrieb eine solche Sperre vorzusehen, die nur im Rahmen einer Störungssuche und -beseitigung vom Administrator aufgehoben werden kann, wenn er das System mit dem Notfall-Bootmedium (siehe M 6.24 *Erstellen eines Notfall-Bootmediums*) startet.

- Netzkommunikation und -dienste:
  - Soll ein lokaler Paketfilter aufgesetzt werden?
  - Auf welche externen Netzdienste soll von dem Rechner aus zugegriffen werden können?
  - Soll ein verteiltes Dateisystem eingebunden werden?
  - Verteilte Dateisysteme, bei denen die Nutzdaten unverschlüsselt übertragen werden, sollten nur im internen Netz verwendet werden. Soll ein verteiltes Dateisystem über ein unsicheres Netz hinweg genutzt werden, so muss es durch zusätzliche Maßnahmen (kryptographisch geschütztes VPN, Tunneling) gesichert werden.
- Protokollierung:
  - Welche Daten werden protokolliert? Wie und in welchen Intervallen werden die Protokolldaten ausgewertet? Wer führt die Auswertung durch?

Anhand der oben genannten Punkte kann eine Checkliste erstellt werden, die bei Audits oder Revisionen hilfreich sein kann.

Die Verantwortung für die Sicherheitsrichtlinie liegt beim Sicherheitsmanagement. Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Im Bezug auf Regelungen für die Benutzer sollte jedoch beachtet werden, dass diese nur so weit sinnvoll sind, wie sie im normalen Arbeitsalltag anwendbar sind, aber auch wie sie überwacht und durchgesetzt werden können. Beispielsweise ist es bei Zugriffsbeschränkungen nicht zielführend, den Benutzern nur in der Sicherheitsrichtlinie den Zugriff auf bestimmte Verzeichnisse zu verbieten, diese aber nicht auch durch eine entsprechende Rechtevergabe tatsächlich vor dem Zugriff zu schützen. Zugriffsbeschränkungen, die bei der Erstellung der Sicherheitsrichtlinie festgelegt wurden, sollten daher immer so weit wie möglich über entsprechende Vorgaben für die Installation und Konfiguration der Rechner umgesetzt werden.

Bei der Formulierung der Sicherheitsrichtlinie für Clients ist es auch wichtig, eine Balance zwischen Sicherheit (durch Einschränkungen der Funktionalität und restriktive Vergabe von Benutzerrechten) und Benutzerfreundlichkeit zu finden. Werden die Benutzer durch Regelungen, die für sie nicht transparent sind und die eventuell sogar als Schikane empfunden werden, zu sehr eingeschränkt, so kann sie dies im Gegenzug dazu verleiten, diese Beschränkungen mit besonderer Kreativität zu umgehen.

Dies unterscheidet die Sicherheitsrichtlinie für Clients von den entsprechenden Richtlinien etwa für Server oder aktive Netzkomponenten, bei denen in der Regel nur technisch versierte Anwender und Administratoren angesprochen sind, denen viele Einschränkungen eher plausibel gemacht werden können.

Prüffragen:

- Ist eine Client-Sicherheitsrichtlinie vorhanden, die das zu erreichende Sicherheitsniveau beschreibt?
- Wird die Client-Sicherheitsrichtlinie regelmäßig den aktuellen Erfordernissen angepasst?

# M 2.323 Geregelte Außerbetriebnahme eines Clients

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Außerbetriebnahme eines Clients muss vor allem sichergestellt werden, dass

- keine wichtigen Daten, die eventuell auf dem Client gespeichert sind, verloren gehen, und dass
- keine sensitiven Daten auf den Datenträgern des Rechners zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf dem System gespeichert sind.

- **Datensicherung**
  Vor der Außerbetriebnahme des Rechners müssen lokal gespeicherte Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert (beispielsweise auf Magnetbändern, CD- oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden.
  In diesem Zusammenhang kann es sinnvoll sein, den Benutzern für die Sicherung eventuell gespeicherter lokaler Daten ein geeignetes Laufwerk, beispielsweise einen externen CD- oder DVD-Brenner, zur Verfügung zu stellen.
  Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.
- **Austragen des Systems aus Verzeichnisdiensten und Datenbanken**
  Etwaige Berechtigungen im Netz, die an den Client-Rechner selbst (und nicht an einen Benutzer) gekoppelt sind, müssen gelöscht werden. Beispiele hierfür sind Einträge auf Proxyservern am Sicherheitsgateway oder Zugriffsrechte auf Netzdienste, die anhand der IP-Adresse gewährt werden. Ist der Client in netzweiten Verzeichnisdiensten oder Datenbanken eingetragen (etwa in einer Windows Domäne, Active Directory, NIS oder ähnlichen), so müssen die zugehörigen Einträge gelöscht oder zumindest die entsprechenden Konten deaktiviert werden.
- **Löschen der Daten auf dem System**
  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder das logische Löschen mit den Löschfunktionen des Betriebssystems noch das Neuformatieren der Platten die Daten tatsächlich von den Festplatten entfernt. Mit geeigneter Software können Daten in solchen Fällen, oft sogar ohne großen Aufwand, wieder rekonstruiert werden. Weitere Hinweise finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*.
- **Löschen von Datensicherungsmedien**
  Nach der Außerbetriebnahme eines Systems müssen gegebenenfalls auch die entsprechenden Datensicherungsmedien gelöscht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.
- **Entfernen sonstiger Informationen**

Sind auf einem Rechner noch an anderen Stellen als auf der Festplatte (etwa in einem nichtflüchtigen Speicher) potentiell sensitive Daten gespeichert (beispielsweise bestimmte Konfigurationsdaten), so müssen auch diese vor der Weitergabe des Geräts entfernt werden.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden.

Prüffragen:

- Existiert ein dokumentiertes Verfahren zur Außerbetriebnahme von Clients?
- Wird sichergestellt, dass alle evtl. noch auf dem Client vorhandenen Daten gesichert und anschließend vom Client sicher gelöscht werden?

# M 2.324 Einführung von Windows auf Clients ab Windows XP planen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Die geregelte und sichere Einführung von Windows-Clients ab Windows XP setzt eine umfangreiche Planung voraus. In der Planungsphase werden die notwendigen Voraussetzungen für einen sicheren Betrieb von Windows Client-Betriebssystemen geschaffen.

Die einzelnen Planungsschritte sind abhängig von den geplanten Einsatzszenarien der Windows-Client-Systeme. Die Einführung muss in ihren einzelnen Schritten möglichst detailliert geplant werden. Hierbei sind nicht nur die Inhalte, sondern auch interne Prozesse und Abläufe der Institution zu berücksichtigen. Alle Inhalte und Prozesse müssen definiert, in einer Richtlinie dokumentiert und allen Beteiligten zugänglich gemacht werden.

Generell muss ausreichend Zeit für die Einführung von eines neuen Windows-Client-Betriebssystems eingeplant werden. Dabei ist ein Zeitraum von einem halben Jahr für größere Unternehmen und Behörden durchaus realistisch. Im Laufe der Planung muss der Zeitplan erfahrungsgemäß mehrfach angepasst werden.

Die im Folgenden genannten sicherheitsrelevanten Aspekte müssen bei der Einführung ab Windows XP berücksichtigt werden.

**Neuinstallation oder Migration/Upgrade**

Für die Einführung von Windows-Clients ab Windows XP stehen verschiedene Verfahren zur Verfügung. Zum einen kann die Einführung durch einen parallelen Aufbau der zu migrierenden Windows Infrastruktur (neue Clients werden parallel zu bestehenden eingeführt) erfolgen. Zum anderen kann dies durch eine Migration oder ein Update vorhandener Client-Systeme geschehen.

Eine generelle Empfehlung für die Einführung kann nicht gegeben werden, da dies von den individuellen Rahmenbedingungen abhängt. Das Verfahren ist immer auf das Unternehmen oder die Behörde zuzuschneiden.

In erster Linie muss entschieden werden, ob bei der Einführung der neuen Windows-Version die Client-Systeme komplett neu installiert oder durch ein Update migriert werden. In der Praxis werden häufiger bestehende Client-Systeme migriert, statt eine vollständige Neuinstallation durchzuführen. Bei Neuinstallationen können an die individuellen Anforderungen angepasste Installationsmedien, sogenannte Baseline Images, für eine strukturierte Migration angelegt werden. Bei der Migration von älteren Windows-Clients auf neuere Versionen des Betriebssystems bedarf es einer angemessenen Planung, insbesondere, wenn auch die Domänen-Controller migriert werden (z. B. von Windows Server 2008 auf Windows Server 2012). Dazu sind zusätzliche Migrationsaspekte auf Seiten des Servers zu beachten (z. B. M 4.424 *Sicherer Einsatz älterer Software ab Windows 7*). Die Migration muss in ihren einzelnen Schritten möglichst detailliert geplant werden, da durch Planungsdefizite in der Zeit der Umstellung leicht Sicherheitslücken entstehen können.

Ein Upgrade des Betriebssystems auf Windows Vista ist nur von Windows XP mit Service Pack 2 oder höher möglich. Windows 7 kann nur von Win-

dows Vista migriert werden. Eine Upgrade-Kette von Windows XP über Windows Vista auf Windows 7 wird vom Hersteller nicht unterstützt und sollte nicht durchgeführt werden. Ein direktes Upgrade von Windows 7 auf Windows 8 und Windows 8.1 ist unter Beibehaltung von Windows-Einstellungen, persönlichen Dateien und Anwendungen möglich. Ein Upgrade von Windows 8 auf Windows 8.1 ist sowohl mittels Datenträger als auch über den Windows-Store möglich. Bei einem Update auf Windows 8.1 besteht die Einschränkung, dass ein Update nur mit derselben Version durchgeführt werden kann, also von Windows 8 Pro auf Windows 8.1 Pro. Bei der Verwendung von Datenträgern ist allerdings ein Wechsel der Versionen möglich. Für Volumen-Lizenzversionen von Windows 8 und Windows 8.1 Enterprise kann das Update nicht über den Windows-Store durchgeführt werden. Hierfür werden Datenträger benötigt. Bei Nutzung älterer Versionen von Windows, wie Windows 2000, muss eine Neuinstallation ab Windows Vista erfolgen. Grundsätzlich sollte auch bei einer upgradefähigen Betriebssystemversion eine Neuinstallation des Clients in Betracht gezogen werden.

Aufgrund der verschiedenen Editionen bei Windows-Clients ab Windows Vista stehen im Gegensatz zu früheren Versionen von Windows mehrere Migrationspfade zur Verfügung. Es muss festgelegt werden, welche Edition von Windows in der Institution genutzt werden soll (siehe M 2.440 *Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista*). Anhand dieser Festlegung ist unter Berücksichtigung der gegenwärtig eingesetzten Version der entsprechende Migrationspfad zu wählen, sofern von einer kompletten Neuinstallation abgesehen wird.

Bei jeder Neuinstallation und bei jedem Upgrade müssen die Anforderungen an die Aktivierung der Windows-Clients berücksichtigt werden (siehe M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* und M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

Es ist zu beachten, dass in der Migrationsphase unter Umständen erweiterte Zugriffsberechtigungen (z. B. für ein spezielles Migrationsteam) und schwächere Sicherheitseinstellungen wegen potenzieller Kompatibilitätsprobleme gewählt werden müssen. Diese Einstellungen müssen nach dem Abschluss der Migration wieder auf das höchstmögliche Sicherheitsniveau gebracht werden. Die zusätzlichen migrationsspezifischen Berechtigungen sind nach der Migration zu entziehen. Generell gilt, dass nach der erfolgten Migration dasselbe Sicherheitsniveau erreicht werden muss, wie bei einer Neuinstallation. Nach Abschluss der Migration hat ein Soll-Ist-Abgleich aller Sicherheitseinstellungen wie beispielsweise Berechtigungen und Gruppenmitgliedschaften stattzufinden.

Die Zeitspanne für die Migration muss festgelegt und eingehalten werden. Die Migration darf nicht zu einem Normalzustand werden. Dies hat insbesondere sicherheitsrelevante Auswirkungen, da die Sicherheit während der Migration üblicherweise abgeschwächt ist.

**Software Kompatibilitätsprüfung beim Wechsel zu einer höheren Windows-Version**

Es ist festzulegen, welche Software auf den Windows-Clients installiert werden soll. Für bereits vorhandene Software ist zu prüfen, ob sie unter der neuen Windows-Version lauffähig ist (siehe M 2.441 *Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista*). Dies gilt auch für geplante Neubeschaffungen von Software nach einer erfolgten Migration.

Für vorhandene Software, die nicht die Kompatibilitätsanforderungen der zu nutzenden Windows-Version erfüllt, müssen Übergangslösungen definiert werden, z. B. der Betrieb von virtuellen Clients mit alten Windows-Versionen in besonders abgesicherten Umgebungen.

Entsprechende Hardwareausstattung vorausgesetzt, kann auch über den Einsatz von Virtualisierung nachgedacht werden. Dazu wird auf dem Windows-Client eine Virtualisierungssoftware installiert. Diese stellt virtuelle Hardware zur Verfügung, auf der ein anderes Betriebssystem mit der benötigten Anwendungssoftware installiert werden kann. In der Enterprise und Ultimate Edition von Windows 7 ist die Microsoft Virtualisierungssoftware *VirtualPC* bereits enthalten. Windows 7 Professional, Enterprise und Ultimate verfügen zusätzlich über den *Windows XP Mode* mit einer Lizenz für eine virtuelle Windows-XP-Maschine. Mit der Einführung von Windows 8 hat Microsoft die Virtualisierungslösung Hyper-V in die Professional- und Enterprise-Versionen integriert. Der XP-Mode ist unter Windows 8 nicht mehr verfügbar. Beim Einsatz einer Virtualisierungssoftware muss das virtuelle Betriebssystem ebenfalls abgesichert werden.

**Einsatz in gemischten Windows-Umgebungen planen**

Beim Einsatz von Clients in gemischten Windows-Umgebungen können Abschwächungen der Sicherheitseinstellungen notwendig sein. Diese sind bei der Planung zu berücksichtigen. Insbesondere muss dafür Sorge getragen werden, dass nach der Realisierung einer homogenen Umgebung, das heißt wenn ausschließlich Clients, Domänencontroller und Server mit aktuellen Windows-Versionen verwendet werden, die Sicherheitseinstellungen auf das höhere Niveau anzuheben sind.

**Active Directory-bezogene Planung**

Bei der Einführung von Clients ab Windows XP in einer Active-Directory-Umgebung ist es nicht ausreichend, ausschließlich die Clients zu betrachten. Auch die Server sind zu berücksichtigen. Hierbei müssen vor allem die Änderungen im Active Directory geplant werden sowie ein Abgleich der Sicherheitseinstellungen auf Client- und Server-Seite erfolgen.

So sind beispielsweise entsprechende Gruppen- und OU-Strukturen (Organisationseinheit, Organisational Unit) im Active Directory zu entwerfen. Eine geeignete OU-Struktur begünstigt einen einfacheren und wegen der größeren Transparenz einen sichereren Betrieb unterschiedlicher Windows- Client-Systeme.

Wenn Window Client Versionen ab Windows Vistain einer Active Directory-Umgebung betrieben werden sollen, muss auf allen Domänen-Controllern mindestens Windows Server 2003 mit Service Pack 1 (SP1) oder höher ausgeführt werden. Sofern der Betrieb eines Windows-8-Clients in einer Windows-2003-Domäne erfolgt, besteht die Möglichkeit, dass einige Funktionalitäten nicht verfügbar sind oder einer zusätzlichen Konfiguration bedürfen. So wäre für die Speicherung von BitLocker- und TPM-Informationen in einer Windows-2003-Domäne ein Schema-Update notwendig.

Wenn eine ältere Serverversion als Windows Server 2008 auf den Domänen-Controllern ausgeführt wird, muss die Konfiguration der Gruppenrichtlinien auf einem Client ab Windows Vista erfolgen, da sich die Gruppenrichtlinien ab Windows Vista nicht mit der Group Policy Management Console von Windows Server 2003 verwalten lassen.

Auf dem Client muss ein Domänenadministrator mit dem Tool *GPOAccelerator* die notwendigen Konfigurationen der Gruppenrichtlinien erstellen. Im Anschluss müssen diese auf den Domänen-Controller übertragen werden. Alternativ können hierfür auch die Remote Server Administration Tools (RSAT) genutzt werden, da hier ein Programm zur Gruppenrichtlinienverwaltung integriert ist, mit dem sich die Gruppenrichtlinien ab Windows Vista konfigurieren und mit einem Objekt im Active Directory von einer Arbeitsstation verknüpfen lassen. Der Security Compliance Manager bietet auch die Möglichkeit, Sicherheitsvorlagen für Windows-Systeme zu erstellen und diese als Gruppenrichtlinienobjekt auf dem Domänencontroller zu importieren.

Entsprechende Sicherheitsvorlagen für verschiedene Windows-Versionen sind mit den Hilfsmitteln für die IT-Grundschutz-Kataloge auf der Webseite des BSI verfügbar.

Des Weiteren ist die Gruppenrichtlinien-Struktur im Active Directory zu planen. Über den Einsatz von Gruppenrichtlinien-spezifischen Mechanismen wie etwa das Blockieren der Vererbung oder das sogenannte Security Filtering muss in der Planungsphase entschieden werden. Dabei ist die Verarbeitungsreihenfolge für Gruppenrichtlinien zu berücksichtigen. Die Maßnahmen im Zusammenhang mit der Planung von Gruppenrichtlinien sind in M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* beschrieben.

Die generellen Active Directory-Planungsmaßnahmen sind unter anderem in M 2.229 *Planung des Active Directory* zusammengefasst.

**Sicherheitskonzept und Sicherheitsrichtlinie**

Das Planen und Erstellen eines Sicherheitskonzeptes beziehungsweise einer Sicherheitsrichtlinie im Vorfeld der Einführung von Clients ab Windows XP ist immens wichtig. In der Sicherheitsrichtlinie sind alle sicherheitsrelevanten Aspekte des Betriebs von Cient-Systemen ab Windows XP zu berücksichtigen. Weitere Anforderungen an das Sicherheitskonzept sind in der Maßnahme M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP* zusammengefasst.

**Secure Boot**

Windows-8-kompatible Hardware muss nach den Richtlinien von Microsoft mit aktiviertem "Secure Boot" ausgeliefert werden. Diese Funktion des BIOS-Nachfolgers UEFI soll sicherstellen, dass eine Manipulation des zu bootenden Betriebssystems, z. B. durch Schadsoftware, unterbunden wird. Secure Boot verhindert auch das Starten von Live-Betriebssystemen von mobilen Datenträgern. Der Einsatz von Secure Boot ist grundsätzlich zu empfehlen.

**TPM-Nutzung ab Windows 8**

Bei einem Trusted Platform Module (TPM) handelt es sich um einen Kryptochip, der u. A. Sicherheitsfunktionen (Zufallszahlenerzeugung, Hashfunktionen), ein sicheres Messen des Plattformzustandes sowie einen sicheren Speicher für Schlüsselmaterial (z. B. für Festplattenverschlüsselung) von Anwendungen und für das Betriebssystem bereit stellt. Bei einigen Rechnern muss dieser TPM-Chip über das Setup im BIOS eingeschaltet werden. Standardmäßig übernimmt Windows ab der Version Windows 8 die Oberhoheit über ein vorhandenes, nicht initialisiertes TPM während des Betriebssystemstarts. Die Nutzung des TPMs in Windows 8 ist wegen des damit verbundenen Kontrollverlustes umstritten. So könnten durch die Nutzung von Betriebssystemfunktionen Schadprogramme im TPM Schlüssel vor dem Zugriff Dritter (ein-

schließlich der Administratoren, Auditoren oder Forensiker) schützen und damit z. B. die Nutzerdaten verschlüsseln, was einen Zugriff auf die Daten durch Drittsoftware ausschließt. Der Einsatz eines TPMs muss daher vorab in der Institution abgewogen und eine entsprechende Festlegung getroffen werden.

**Benutzerkonzept**

Bei der Planung des Benutzerkonzepts muss der Umgang mit lokalen und domänenweiten Benutzerkonten geregelt werden. Hierbei muss auch über den Einsatz von servergespeicherten Benutzerprofilen (Roaming User Profile) entschieden werden. Die Nutzung von servergespeicherten Benutzerprofilen hat vor allem Auswirkungen auf die Backup-Strategie, sowie auf den Einsatz des Windows Encrypting File System (EFS).

Seit der Einführung von Windows 8 besteht die Möglichkeit, dass Benutzer sich auch mit einer Windows Live-ID am System anmelden oder das Benutzerkonto mit einer Live-ID verknüpfen. Dies soll dem Benutzer ermöglichen, Cloud-Dienste wie z. B. OneDrive (ehemals SkyDrive) zu nutzen oder Daten wie Einstellungen für Apps oder Favoriten automatisch zwischen Systemen zu synchronisieren. Hierdurch besteht allerdings die Möglichkeit, dass sensible oder personenbezogene Daten bewusst und unbewusst das Unternehmen verlassen und ein Verlust der Kontrolle über diese Daten eintritt.

Da durch die Anmeldung an einem Windows-System mittels Live-ID die Möglichkeit besteht, dass vertrauliche Daten mit Geräten synchronisiert werden, die sich nicht unter der Kontrolle der Institution befinden, sollte die Live-ID-Anmeldung durch die Aktivierung der Gruppenrichtlinie *Benutzer können keine Microsoft-Konten hinzufügen oder sich damit anmelden* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Konten: Microsoft-Konten blockieren* unterbunden werden. Allerdings muss hierbei beachtet werden, dass die Richtlinie gesetzt werden muss, bevor sich ein Benutzer mit einer Live-ID anmeldet. Wurde bereits ein Profil mit einer Live-ID angelegt, so ist mit dieser auch weiterhin die Anmeldung möglich, wenn die Richtlinie schon in Kraft ist.

Sofern die Nutzung von Microsofts Cloud-Diensten gewollt ist, besteht unter Windows 8 auch die Möglichkeit, ein Domänenkonto mit einer Live-ID zu verknüpfen, wodurch weiterhin die Anmeldung an der Domäne erfolgt, aber auch die Nutzung des Windows Stores möglich ist. Die Konfiguration der Synchronisierungseinstellungen erfolgt über eine Gruppenrichtlinie, die regelt, welche Cloud-Funktionen genutzt und welche Daten darüber synchronisiert werden können. Diese Synchronisationseinstellungen sind unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Einstellungen synchronisieren* konfigurierbar.

Sofern die Nutzung des Cloud-Speicherdienstes OneDrive nicht erforderlich ist, sollten die Cloud-Speicher-Funktionen komplett deaktiviert werden, damit Dateien nicht unbemerkt das Unternehmen verlassen können. Die Deaktivierung von OneDrive ist über die Einstellung *Verwendung von SkyDrive für die Dateispeicherung verhindern* unter der Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *SkyDrive* möglich. Für die Nutzung von Cloud-Speicherdiensten in einem Unternehmenskontext mit Kollaborationsfunktion bietet Microsoft OneDrive Pro, einen Onlinespeicher für geschäftliche Zwecke an. Die Administration der Dokumentenbibliothek erfolgt durch die Administratoren der Institution.

Bei der Planung des Benutzerkonzepts ab Windows Vista muss der Umgang mit der Benutzerkontensteuerung (User Account Control, UAC) geregelt wer-

den (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*). Es wird empfohlen, die Einstellungen so zu wählen, dass für Standardbenutzer keine Privilegienerhöhung möglich ist.

**Administrationskonzept**

Im Vorfeld der Einführung von Windows-Clients ab Windows XP ist ein Administrationskonzept zu erstellen. Es sind grundsätzlich zwei verschiedene Konten für administratives Personal vorzusehen. Soweit möglich, sollten die Administratoren für ihre Arbeit ein Konto mit den Privilegien eines Standardbenutzers verwenden. Nur wenn diese Privilegien nicht mehr ausreichend sind, sollte ein Konto mit administrativen Privilegien genutzt werden. Nach der Erfüllung der Aufgaben sollte sich der Administrator wieder vom Konto mit administrativen Privilegien abmelden und mit dem Standardbenutzerkonto weiterarbeiten.

Welche Konfiguration für die Benutzerkontensteuerung vorzunehmen ist, sollte im Administrationskonzept dokumentiert werden.

Weiterhin muss die Fernadministration der Clients und der Umgang mit lokalen administrativen Konten geregelt werden. Die Fragen der personellen und organisatorischen Zuständigkeiten müssen ebenfalls im Konzept Berücksichtigung finden. Verantwortlichkeiten sind zu trennen (Segregation of Duties) und im Administrationskonzept zu verankern. Die entsprechende Umsetzung ist sowohl auf der organisatorischen als auch der technischen Ebene zu planen.

Werden Windows Client-Systeme ab Windows XP in einer Active Directory-Umgebung eingesetzt, so müssen die administrativen Zuständigkeiten und Grenzen, sowie die Vergaberichtlinien für administrative Berechtigungen auf Client- und Benutzerobjekte im Active Directory geklärt werden.

Mit der Einführung von Windows 8 wurde auch das Konzept von Apps eingeführt, die eine Ergänzung zu den klassischen Desktop-Anwendungen sind. Apps sind Anwendungen, die über einen Microsoft-eigenen Onlineshop ("Windows Store") im Internet durch den Benutzer bezogen werden können. Der Vorteil von Apps ist die simple Handhabung bei der Installation. Für die Nutzung des Windows Stores ist die Anmeldung mit einem Windows-Konto (Live-ID) oder mit einem Anmeldekonto, das mit einer Live-ID verknüpft ist, notwendig. Grundsätzlich ist es im Unternehmenseinsatz empfehlenswert, Standard-Apps, die nicht benötigt werden, vom System zu entfernen und nur die Installation freigegebener Apps aus dem Store zu erlauben. Ebenfalls besteht die Möglichkeit, einen eigenen Unternehmens-App-Store zu betreiben, um Apps auszurollen. Weiterhin bietet Windows 8 einen Mechanismus namens Sideloading, mit dem Apps ohne einen App-Store direkt auf Zielcomputern installiert werden können. Voraussetzung zur Nutzung des Sideloadings ist allerdings eine Windows-8-Enterprise-Lizenz und eine Anbindung des Zielsystems an die Domäne.

Die Nutzung des Windows Stores ist entsprechend den Sicherheitsrichtlinien der Institution und den Vorgaben aus dem Datenschutz zu konfigurieren. Einstellungen für den Zugriff auf den Windows Store sind per Gruppenrichtlinie unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Store*konfigurierbar. Unter Windows 8 ist es ebenfalls möglich zu steuern, ob Apps Zugriff auf den Standort, den Namen des Benutzers und dessen Profilbild haben dürfen.

**Protokollierungs-/Audit-Konzept**

Um die Sicherheit von Windows-Clients ab Windows XP gewährleisten zu können, muss überwacht werden, ob die festgelegten Sicherheitsrichtlinien (siehe M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*) eingehalten werden. Insbesondere ist auf organisatorischer und technischer Ebene zu regeln, wie die gesammelten Daten regelmäßig ausgewertet werden. Werden Windows-Clients ab Windows Vista eingesetzt, sollten die Protokollierungen der Windows Firewall mit einbezogen werden. Die Sicherheitsaspekte, die bei der Protokollierung zu beachten sind, sind in M 4.148 *Überwachung eines Windows 2000/XP Systems* und M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*-Systemen aufgeführt.

**Datenablage, Datensicherung und Verschlüsselung**

Es ist festzulegen, wo die Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). Es wird grundsätzlich empfohlen, keine Daten auf Client-Systemen abzulegen. Daher muss eine geeignete serverseitige Speicherinfrastruktur vorhanden sein. Nach welcher Strategie verfahren werden soll, ist anhand der konkreten Umstände im Einzelfall festzulegen. In bestimmten Einsatzszenarien, wie beispielsweise bei der Verwendung mobiler IT-Systeme, ist die Datenablage auf diesen notwendig und erwünscht. In solchen Fällen muss die Client-seitige Datenablage und ihr (kryptographischer) Schutz geplant werden (siehe M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*). Die Umsetzung der technischen Maßnahmen, die die Sicherheit der lokalen Datenablage gewährleisten, wie Festplattenverschlüsselung, EFS oder Verschlüsselung der Offline-Dateien, muss vor der Einführung geplant werden.

Microsoft liefert mit Windows auch das eigene Verschlüsselungsprodukt BitLocker aus. Vertiefende Informationen zu BitLocker sind in M 4.337 *Einsatz von BitLocker Drive Encryption* zu finden.

Ab Windows 8 wird betriebssystemseitig das Unified Extensible Firmware Interface (UEFI) unterstützt, das den Nachfolger des klassischen PC-BIOS darstellt. UEFI ist für die Nutzung von Secure Boot notwendig, welches das Booten auf vorher signierte Bootloader beschränkt. Dies erhöht die Sicherheit beim Starten des Systems, da das Starten von Schadsoftware und anderen Betriebssystemen nicht möglich ist. Mittels Secure Boot werden nur Betriebssysteme mit korrekter Signatur gebootet. Der Einsatz von Secure Boot wird auf UEFI-basierten Systemen dringend empfohlen.

Um eine saubere Trennung von benutzer- und projektspezifischen Daten, sowie von Programmen und Daten des Betriebssystems durchzusetzen, muss eine geeignete Verzeichnisstruktur geplant werden. So können beispielsweise zwei Hauptverzeichnisse *\Projekte* und *\Benutzer* angelegt werden, unter denen die Dateien und Verzeichnisse der Projekte bzw. Benutzer in jeweils eigenen Unterverzeichnissen abgelegt werden.

Bei der Einführung von Windows-Versionen ab Windows XP muss auch eine entsprechende Datensicherungsstrategie festgelegt werden. Die Verfahrensweise ist für jedes IT-System und für jede Datenart zu bestimmen. Die Umsetzung hängt vor allem von der Art der Daten ab, die auf einem Client abgelegt sind. Werden auf einem Client keine Daten abgelegt, nur Standard-Software eingesetzt und haben die Benutzer servergespeicherte Profile, so kann unter Umständen auf Client-seitige Datensicherung verzichtet werden. Werden dagegen auf Windows-Clients Daten abgelegt, müssen sie bei Sicherun-

gen berücksichtigt werden. Weitere Informationen zu diesem Thema werden in M 6.32 *Regelmäßige Datensicherung* und M 6.33 *Entwicklung eines Datensicherungskonzepts* gegeben.

Die Verwendung von EFS oder einer anderen, clientseitigen Festplattenverschlüsselung muss beim Festlegen der Backup-Strategie berücksichtigt werden. Wird EFS eingesetzt, ist generell die Maßnahme M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren* zu beachten. Insbesondere sollte das Backup-Konzept den Umgang mit dem Schlüsselmaterial bei Wiederherstellungsoperationen regeln (siehe dazu auch M 4.147 *Sichere Nutzung von EFS unter Windows*).

Windows unterstützt den auf heute praktisch jedem PC vorhandenen Kryptochip TPM (Trusted Platform Module), um darin Schlüssel und Zertifikate sicher zu speichern. Dies erhöht einerseits die Sicherheit der kryptographischen Anwendungen, schränkt andererseits aber auch den Zugriff des Benutzers bzw. der Administratoren ein, da auch für diese nur eingeschränkter Zugriff auf TPM-Inhalte besteht. Beim Einsatz des TPM müssen daher zusätzliche Vorkehrungen für den Verlust kryptographischer Geheimnisse durch Ausfälle Fehler getroffen werden.

**Roll-out**

Die Abläufe bei der Installation, also die Roll-out-Phase, müssen bei der Planung berücksichtigt werden. Unter anderem sind die personellen Zuständigkeiten beim Roll-out eindeutig zu definieren. Es ist zusätzlich ein Roll-out-Notfallkonzept zu erstellen. Durch dieses Notfallkonzept muss sichergestellt werden, dass bei einer fehlgeschlagenen Umstellung der produktive Zustand schnell wiederhergestellt werden kann. Wenn neben Clientbetriebssystemen auch Server migriert werden, sollte die Migration der Server zuerst durchgeführt werden. Neu erstellte oder geänderte Gruppenrichtlinien, Active Directory-Einstellungen oder Berechtigungskonzepte können anschließend für zu migrierende Clients übernommen werden.

**Weitere Konzepte**

Neben den oben aufgeführten Konzepten können je nach Einsatzszenario weitere Konzepte notwendig werden, zum Beispiel ein Namenskonzept (Namenskonventionen für die Rechner, Benutzergruppen und die Benutzer), ein Softwareverteilungskonzept oder ein Konzept zur Anwendungsmigration. Insbesondere die Anwendungsmigration kann Auswirkungen auf die Sicherheit eines Windows-Systems haben (z. B. Abschwächung der Zugriffsrechte auf die Registrierung) und ist daher sorgfältig zu planen.

Die weiteren Konzepte sind ebenfalls in der Planungsphase zu berücksichtigen.

In der Regel bestehen hier bereits entsprechende Konzepe im Unternehmen oder in der Institution, die jedoch auf ihre Eignung im Umfeld des eingesetzten Windows-Betriebssystems geprüft werden müssen.

Nicht zuletzt sollte geplant werden, welche Benutzer und Administratoren geschult werden müssen und wann dies zu erfolgen hat. Insbesondere die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit der eingesetzten Windows-Versionen gründlich zu schulen. Erst nach dieser Schulung sollte der Betrieb dieser Windows-Systeme aufgenommen werden.

Prüffragen:

- Gibt es Richtlinien für die Neuinstallation bzw. Migration/Upgrade von Windows-Systemen und werden diese allen Beteiligten zugänglich gemacht?
- Werden wegen der Migration erweiterte Zugriffsberechtigungen und gelockerte Sicherheitseinstellungen der Domäne nach Abschluss der Migration wieder auf das höchstmögliche Sicherheitsniveau gebracht?
- Falls die Domänen-Controller bei einem Einsatz von Windows-Clients ab Windows Vista nicht unter Windows Server 2008 laufen: Erfolgt die Konfiguration der Gruppenrichtlinien von einem Windows-Client mit den entsprechenden Werkzeugen wie z. B. RSAT?
- Gibt es ein Benutzer- und Administrationskonzept für Windows-Client-Betriebssysteme?
- Gibt es Regelungen zur Überwachung, ob die festgelegten Sicherheitsrichtlinien eingehalten werden?
- Gibt es für Windows Versionen ab Windows XP ein Konzept zur Datenablage, Datensicherung und Verschlüsselung der Benutzerdaten?
- Gibt es Vorgaben für die Installation von Apps aus dem Windows-Store und deren Nutzung? Sind die Vorgaben und Anforderungen entsprechend in der Planung berücksichtigt?
- Ist die Nutzung von Cloud-Diensten wie z. B. OneDrive in der Sicherheitsrichtlinie für Client-Systeme geregelt, und in der Einführungsplanung berücksichtigt?
- Ist eine begründete Entscheidung zum Einsatz des TPM getroffen worden, und bestehen adäquate Konzepte für den Verlust dort gespeicherter kryptographischer Informationen?

# M 2.325 Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine der wichtigsten organisatorischen Aufgaben bei der Einführung von Windows-Clients ab Windows XP ist es, eine entsprechende Sicherheitsrichtlinie zu planen und zu definieren. Diese Richtlinie legt die später umzusetzenden Sicherheitsbestimmungen für Windows-Systeme fest.

Die in der Windows-Sicherheitsrichtlinie definierten Anforderungen werden durch die entsprechenden Sicherheitseinstellungen auf Betriebssystemebene oder durch organisatorische Maßnahmen umgesetzt. In Fällen, in denen technische Maßnahmen nicht ausreichen, ist eine Kombination notwendig, so dass eine technische Umsetzung durch zusätzliche organisatorische Maßnahmen begleitet und unterstützt wird. Nach Möglichkeit sollte immer eine technische Lösung gegenüber einer organisatorischen bevorzugt werden.

Die zu erstellende Sicherheitsrichtlinie hat sich an den bisher geltenden Sicherheitsrichtlinien der Organisation zu orientieren und darf diesen nicht widersprechen. Häufig werden existierende Regelungen für frühere Windows-Versionen angepasst oder sinngemäß erweitert. Dabei sind insbesondere spezifische Technologien der jeweils neuen Windows-Version zu berücksichtigen. Generell gilt, dass sich die Planung der Windows-Infrastruktur an der jeweiligen übergreifenden Sicherheitsrichtlinie orientiert, jedoch über einen Feedback-Prozess Einfluss auf diese übergreifende Sicherheitsrichtlinie besitzt. Nicht zuletzt sind beim Erstellen der Windows-Sicherheitsrichtlinie geltende rechtliche Bestimmungen zu beachten. Die Sicherheitsrichtlinie für Windows-Clients ist zu dokumentieren und im erforderlichen Umfang den Benutzern des Client-Server-Netzes mitzuteilen. Alle Administratoren sollten sie kennen und umsetzen.

Die folgenden Themenbereiche bieten einen groben Überblick über die abzudeckenden Bereiche einer solchen Richtlinie. Je nach Unternehmen oder Behörde und umzusetzenden Einsatzszenarien müssen noch weitere Aspekte in Betracht gezogen werden.

### Physische Sicherheit

Die Aspekte der physischen Sicherheit müssen bei der Planung der Windows-Sicherheitsrichtlinie berücksichtigt werden, da Windows auch auf mobilen Rechnern zum Einsatz kommen kann. Es müssen die generellen Empfehlungen zur physischen Sicherheit aus B 3.201 *Allgemeiner Client* und B 3.202 *Allgemeines nicht vernetztes IT-System* umgesetzt werden.

### Verantwortlichkeiten

Die Verantwortlichkeiten für den Betrieb der Systeme müssen in der Sicherheitsrichtlinie geregelt werden.

Es ist festzulegen, welche Verantwortung die einzelnen Administratoren zu übernehmen haben. Dies können zum Beispiel Verantwortlichkeiten sein für:

- Änderungen der Sicherheitsparameter (lokal),

- Änderungen der Sicherheitsparameter im Active Directory,
- die Verwaltung der Systeme im Active Directory,
- die Auswertung der Protokolldaten,
- die Vergabe von Zugriffsrechten und Systemberechtigungen,
- die Freigabe und das Durchführen von Konfigurationsänderungen sowie das Installieren von Software,
- das Hinterlegen und den Wechsel von Passwörtern und
- die Durchführung von Datensicherungen und Datenwiederherstellungen.

Auch die Endbenutzer müssen in einem Client-Server-Netz Verantwortlichkeiten übernehmen, sofern sie administrative Tätigkeiten ausführen sollen. In der Regel beschränken sich diese Verantwortlichkeiten auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese Rechte explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.

Die Administration der Systeme sollte durch geschulte Administratoren erfolgen, wobei im Rahmen der Notfallvorsorge für eine geeignete Stellvertreterregelung zu sorgen ist.

**Benutzerkonten**

Vor der Einrichtung von Benutzerkonten muss die Entscheidung getroffen werden, welche Konten lokal oder im Active Directory angelegt werden.

Active Directory oder ähnliche Lösungen sollten eingesetzt werden, da diese prinzipbedingt stärkere Authentisierungsverfahren und die effektive Steuerung der Konten ermöglichen. Der Verwendungsrahmen für lokale Konten ist auf bestimmte Anwendungen einzugrenzen. Des Weiteren sollten die Restriktionen, die für Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf Anmelde-Fehlversuche.

Mit Windows 8 wurde zusätzlich die Anmeldung mit einem Microsoft-Konto (Windows-Live ID) eingeführt, die es den Nutzern erlaubt, sich an jedem Windows-8-PC anzumelden. Mit der Live ID wird auch die Nutzung von Cloud-Diensten und die Synchronisation von Apps und Einstellungen zwischen mehreren PCs ermöglicht. Aufgrund des erhöhten Risikos eines unkontrollierten Datenverlustes sollte die Anmeldung mit einer Live-ID oder die Verknüpfung einer Live-ID mit einem Active-Directory-Konto im Unternehmensumfeld nicht genutzt werden.

**Berechtigungskonzept**

Die Sicherheitsrichtlinie muss unter anderem ein Berechtigungskonzept enthalten. Das Berechtigungskonzept legt Rechte von normalen und administrativen Benutzern fest.

Problematisch ist die Tatsache, dass Windows-Clientbetriebssysteme nicht rollenfähig sind. Daher muss ein entsprechendes Gruppenkonzept geplant und lokal oder in der Domäne umgesetzt werden. Dies erfordert im Wesentlichen eine Abbildung der Organisationshierarchie und der existierenden Rollen auf die jeweiligen Gruppen.

Durch die Vergabe entsprechender Berechtigungen an diese Gruppen sowie gegebenenfalls die Definition entsprechender Richtlinien (z. B. Software Restriction Policies) wird das Berechtigungskonzept umgesetzt. Dies erfordert eine entsprechende Planung und die Erfassung der Verantwortlichkeiten und Prozesse.

Folgende Bereiche müssen durch das Berechtigungskonzept abgedeckt sein:

- Systemberechtigungen und Benutzerrechte (z. B. lokale oder entfernte Anmeldung auf einem Rechner, das Herunterfahren eines Systems),
- Zugriffsberechtigungen auf Netzwerkfreigaben,
- Zugriffsberechtigungen auf Dateien (Anwendungs- und Systemdateien),
- Zugriffsberechtigungen auf Registry-Einträge.
- Ausführungsberechtigungen von Anwendungen und Apps

Benutzerrechte müssen sorgfältig geplant werden, da sie Vorrang vor anderen Rechten haben, insbesondere vor Datei- und Verzeichnisberechtigungen. Benutzerrechte beziehen sich auf das gesamte Windows-System. Die Vergabe der Benutzerrechte erfolgt über Gruppenrichtlinien, die bei Mitgliedern einer Active Directory-basierten Domäne im Active Directory und bei anderen Systemen lokal definiert werden (siehe M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*). Bei der Vergabe ist darauf zu achten, dass Berechtigungen und Rechte vorzugsweise Gruppen und nicht einzelnen Benutzern zugewiesen werden.

Ab Windows Vista muss das Berechtigungskonzept auch auf den Einsatz der Benutzerkontensteuerung (User Account Control, UAC) eingehen (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*).

**Kommunikationssicherheit**

Auch Anforderungen an die Sicherheit bei der Datenübertragung müssen ein Bestandteil der Sicherheitsrichtlinie sein. Es ist empfehlenswert, Grundanforderungen an die Übertragungssicherheit in der Sicherheitsrichtlinie zu formulieren (Sollzustand) und anschließend Ausnahmen zu erfassen, die aufgrund lokaler Gegebenheiten notwendig sind. Bei der Definition von Anforderungen und zugehörigen Ausnahmen sind vor allem die Fragen der erforderlichen Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit zu berücksichtigen.

Die technische Umsetzung der Anforderungen kann auf unterschiedliche Art und Weise erfolgen. Zwei der möglichen Umsetzungen werden in M 5.123 *Absicherung der Netzkommunikation unter Windows* und M 5.90 *Einsatz von IPSec unter Windows* beschrieben.

Bei der Umsetzung der Anforderungen ist die Windows-eigene Firewall gegen die Firewall-Funktionalität von separater Schutzsoftware abzuwägen. Erst ab Windows Vista genügt die Windows-eigene Firewall den normalen Sicherheitsanforderungen in den meisten Fällen. Falls bereits eine zentral verwaltete Schutzsoftware vorhanden ist, ist dessen Firewall-Funktionalität oft besser in die Sicherheitsfunktionen der gesamten Schutzsoftware eingebunden als die Windows-eigene Firewall unterschiedlicher Windows-Versionen. Besonders in gemischten Umgebungen empfiehlt es sich, die notwendigen Sicherheitsniveaus entsprechend solcher Abwägungen für jeden Systemtyp einzeln zu formulieren und auf die technische Verträglichkeit, die Anschaffungskosten und die zentrale Steuerung zu achten.

Ab Windows 7 können Daten von eingebauten Sensoren wie GPS-Sensoren gesammelt werden. Die Daten werden von Applikationen und Diensten genutzt, insbesondere von Internet-basierenden Diensten. Sensordaten sind standardmäßig von allen installierten Applikationen sowie Dienst- und Benutzerkonten abrufbar. Daher sollten sie im Normalfall deaktiviert werden, um die informationelle Selbstbestimmung der Nutzer des IT-Systems zu gewährleisten.

Wenn Sensoren benötigt werden, sollte vorab eine konkrete Regelung für die jeweilige Anwendung definiert werden. Es sind die Software sowie Dienst- und Benutzerkonten festzulegen, welche Sensordaten abfragen dürfen. Weiterhin sollten die Mitarbeiter auf Art und Nutzung der gesammelten Daten hingewiesen werden. Es muss geprüft werden, ob eine gesonderte Einverständniserklärung des Nutzers notwendig ist. Außerdem sollte das System verschlüsselt und mit Zugriffsschutz versehen werden, da sonst unter Umständen ein Dritter die Sensordaten extrahieren und für Social Engineering missbrauchen könnte.

**Anwendungen und Apps**

Mit der Einführung von Windows 8 wurde alternativ zur Nutzung klassischer Desktop-Programme zusätzlich ein neues App-Konzept realisiert. Apps können über den Microsoft-eigenen Windows Store im Internet bezogen werden. Der Windows Store bietet dem Anwender die Möglichkeit, nach Apps zu Suchen und diese auf dem System zu installieren. Da die Apps für bestimmte Funktionen Zugriff auf unterschiedliche Ressourcen wie z. B. den Kalender, das Adressbuch oder den GPS-Sensor benötigen und dadurch auf potenziell kritische Daten zugreifen können, muss bei der Planung der Sicherheitsrichtlinie auch die Installation und die Nutzung von Apps aus dem Windows Store entsprechend geplant und geregelt werden. Bei der Auswahl von Sicherheitsprodukten wie z.B. dem Virenschutz sollte zusätzlich darauf geachtet werden, dass das einzusetzende Produkt auch in der Lage ist, schädliche oder modifizierte Apps zu erkennen, da nie ganz ausgeschlossen werden kann, dass schadhafte Dateien trotz entsprechender Qualitätskontrollen und Vorgaben an Windows-8-Apps auch in den Windows Store gelangen können. Wie die Freigabe von Apps oder deren Absicherung in einem Unternehmenskontext zu erfolgen hat, muss in einer entsprechenden App-Richtlinie geregelt werden. Weitergehende Hinweise finden sich im Hilfsmittel *Einsatz von Apps unter Windows 8*.

**Protokollierung**

Sämtliche Windows-Versionen ab Windows 2000 und XP stellen sehr ausführliche Möglichkeiten zur Protokollierung sicherheitsrelevanter Ereignisse (erfolgreiche und/oder fehlgeschlagene Versuche) zur Verfügung.

Diese sind jedoch bei vollständiger Nutzung in der Lage, das System weitgehend mit der Protokollierung auszulasten und große Mengen an Speicherplatz zu verbrauchen. Bei der Definition der Protokolleinstellungen ist das Gesamtkonzept der Systemüberwachung (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems* und M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*) zu berücksichtigen.

**Einsatzszenarien-spezifische Aspekte**

Je nach Einsatzszenario entstehen weitere, für dieses Szenario spezifische Aspekte, die bei der Planung berücksichtigt sein müssen. Insbesondere durch die Verwendung von Peer-to-Peer entstehen neue Sicherheitsaspekte, die durch die Sicherheitsrichtlinien abgedeckt sein müssen (siehe auch M 5.152 *Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste*). Auf die Verwendung von Peer-to-Peer sollte nach Möglichkeit verzichtet werden, da es die Sicherheit des Client-Server-Netzes beeinträchtigen können.

Die für den mobilen Betrieb eines Windows-Client-Systems zu berücksichtigenden Aspekte werden in M 2.328 *Einsatz von Windows XP auf mobilen*

*Rechnern* bzw. M 2.442 *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen* beschrieben.

Ein weiteres Beispiel für szenariospezifische Sicherheitsaspekte ist die Verwendung von EFS, das zusätzliche sicherheitsrelevante Anforderungen aufwirft (siehe M 4.147 *Sichere Nutzung von EFS unter Windows*). Analog ist ab Windows Vista die mögliche Verwendung der BitLocker Festplattenverschlüsselung zu berücksichtigen (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*).

**Microsoft Baseline Security Analyzer (MBSA)**

Der Microsoft Baseline Security Analyzer (MBSA) ist ein kostenloses Tool, das eine Windows-Installation auf typische Sicherheitsprobleme hin untersucht. Der Einsatz des MBSA kann die Gestaltung einer sicheren Windows-Konfiguration daher unterstützen, indem er auf den entsprechenden Systemen initial und ggf. regelmäßig ausgeführt wird.

Prüffragen:

- Orientiert sich die Sicherheitsrichtlinie zu Windows-Clients ab Windows XP an den geltenden Sicherheitsrichtlinien des Unternehmens bzw. der Behörde?
- Wurde allen Benutzern des Client-Netzes die Sicherheitsrichtlinie zum mobilen Einsatz von Windows im erforderlichen Umfang bekannt gegeben?
- Werden die Verantwortlichkeiten für den Betrieb der Windows-Clients in der Sicherheitsrichtlinie geregelt?
- Beinhaltet die Sicherheitsrichtlinie ein Berechtigungskonzept, in dem Rechte sowohl normaler als auch administrativer Benutzer geregelt werden?
- Wird der Einsatz von Apps aus dem Windows Store auf Clients ab Windows 8 berücksichtigt?
- Ist der Einsatz der User Account Control (UAC) im Berechtigungskonzept geregelt?
- Werden in der Sicherheitsrichtlinie auch Anforderungen an die Sicherheit bei der Datenübertragung geregelt?
- Liegen der Planung der Sicherheitsrichtlinien die unterschiedlichen Einsatzszenarien der Windows-Clients zugrunde?

# M 2.326 Planung der Gruppenrichtlinien für Clients ab Windows XP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Gruppenrichtlinien repräsentieren eine Vielzahl von Benutzer- und Konfigurationseinstellungen, die mit Computern, Standorten, Domänen oder Organisationseinheiten (OUs) verknüpft werden. Bei der Anwendung einer oder mehrerer Gruppenrichtlinien werden im Grunde Änderungen in der Registry der betroffenen Systeme vorgenommen.

Gruppenrichtlinien bieten eine einfache Möglichkeit, um das Verhalten von Clients zu steuern und zudem Sicherheitseinstellungen sowie An- und Abmeldeskripte zu definieren. Durch Gruppenrichtlinien lässt sich das Verhalten von Betriebssystemen bestimmen und der Zugriff von Benutzern mittels Gruppenrichtlinienobjekten, auf bestimmte Funktionalitäten des Systems einschränken. Ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) fasst dabei einen vorgegebenen Satz von Konfigurationsparametern zusammen. Für jeden Parameter kann ein konkreter Wert angegeben werden, der unter Umständen nur aus einem beschränkten Wertebereich stammt. Generell kann auch der Wert *nicht definiert* gewählt werden. Dann gelten automatisch die Standardeinstellungen für diesen Parameter.

Seit der Einführung unter Windows 2000 wurden die Richtlinien ständig um neue Inhalte erweitert. Unter Windows 8 ist die Anzahl der möglichen Einstellungen auf über 3.600 angestiegen.

Die Planung und Einführung von Client-Gruppenrichtlinien sollte anhand eines standardisierten Prozesses wie dem Folgenden durchgeführt werden:

- Anforderungen der Clientanwendungen und Sicherheitseinstellungen ermitteln und die Client-Konfiguration definieren
- Entscheidung, welche Einstellungen zentral verwaltet werden sollen
- Testinstallation
- Dokumentation der per Gruppenrichtlinie verwalteten Einstellungen (einschließlich Checkliste), Client-Bereitstellungskonzept anpassen
- Export der Einstellungen
  a. auf Clients mittels *gpedit.msc, rsop.msc* oder *gpresult*
  b. oder mittels Domaincontroller Eventlog-Filter für GPO-Events setzen und regelmäßig kontrollieren, ob GPO-Objekt(e) keine Fehler verursachen und wirksam sind. Dazu können:
- Events ggf. auf einen Verwaltungs-Server umgeleitet und überwacht (z. B. *System Center-Server*) oder
- auf Clients mittels *GPLogView.exe* (separat von Microsoft erhältlich) ausgewertet werden.

Die Gruppenrichtlinien sind der primäre Mechanismus zur Umsetzung, der in der Maßnahme M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*, empfohlenen Sicherheitseinstellungen. Sie können als lokale GPO zur Einstellung von Parametern für ein konkretes IT-System oder einen konkreten Benutzer verwendet werden. Beim Betrieb in einer Active Directory-basierten Umgebung lassen sich GPOs zusätzlich auf der Standort- und Domänenebene und auf der Ebene einzelner Organisationseinheiten einsetzen.

Die Parameter innerhalb eines Gruppenrichtlinienobjektes sind baumartig oder dateisystemartig thematisch zusammengefasst. Auf der obersten Ebene ergibt sich eine generelle Zweiteilung in Einstellungen für IT-Systeme und für Benutzer. Dies ermöglicht sowohl die Definition von IT-System- als auch von benutzerbasierten Einschränkungen. Durch die im Benutzerteil definierten Einstellungen werden auch anwendungsspezifische Einschränkungen festgelegt. Werden zusätzliche administrative Vorlagen importiert, lassen sich weitere Anwendungen wie Microsoft Office über die Gruppenrichtlinien zentral konfigurieren. Es sollten benutzerspezifische und anwendungsspezifische Gruppenrichtlinien eingesetzt werden.

Die Benutzer- und die IT-Systemteile einer Gruppenrichtlinie lassen sich einzeln deaktivieren, so dass der jeweils deaktivierte Teil bei der Anwendung der Gruppenrichtlinie nicht ausgewertet wird. Dies schafft in einigen Einsatzszenarien Geschwindigkeitsvorteile. Über die Deaktivierung eines nicht genutzten Teils einer Gruppenrichtlinie sollte in Abhängigkeit von den individuellen Anforderungen entschieden werden.

Beim Einsatz einer Windows-Version ab Windows Vistavereinfacht die Benutzerkontensteuerung (*User Account Control, UAC*) den Einsatz lokaler Administratorrechte für normale Benutzer. Die Administratorrechte sind zwar immer zweckgebunden und zeitlich eingeschränkt, jedoch könnten Benutzer auch sicherheitsrelevante Systemeinstellungen ändern. Daher sollten sicherheitsrelevante Einstellungen nur via Gruppenrichtlinien des Active Directory konfiguriert werden. Dadurch können sie nicht mehr lokal geändert werden.

**Planung lokaler Gruppenrichtlinien**

Werden Gruppenrichtlinien festgelegt, muss auf die Unterschiede zwischen lokalen Gruppenrichtlinien und Richtlinien im Active Directory geachtet werden. Nicht alle Einstellungen, die in einer Active Directory-basierten GPO vorgenommen werden, können auch in einer lokalen Gruppenrichtlinie definiert werden. So fehlen in der lokalen Gruppenrichtlinie zum Beispiel die Kerberos- und die Systemdienst-Richtlinien. Einzelne Richtlinien wie *Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung* speichern sind nur beim Einsatz in einer Domäne wirksam. Bei der Festlegung einzelner Parameter muss folglich der Geltungsbereich einzelner Richtlinien berücksichtigt werden.

Windows XP unterstützt pro Computer nur eine lokale Gruppenrichtlinie. Die Gruppenrichtlinien werden in folgender Reihenfolge verarbeitet:

- Lokale Gruppenrichtlinien
- Standort-GPOs
- Domänen-GPOs
- GPOs der Organisationseinheiten

Ab Windows Vista wird dieselbe Bearbeitungsreihenfolge verwendet, bietet allerdings drei Ebenen an, um lokale Gruppenrichtlinien (sog. Mehrfachgruppenrichtlinienobjekte, kurz MLGPOs) in folgender Reihenfolge zu verarbeiten:

- Richtlinien für lokale Computer
- Richtlinien für Administratoren und Nicht-Administratoren (nur Benutzerrichtlinien)
- Benutzerspezifische lokale Gruppenrichtlinien (nur Benutzerrichtlinien)

Es ist zu beachten, dass die Richtlinien für Administratoren und Nicht-Administratoren sowie die benutzerspezifischen lokalen Gruppenrichtlinien nur die Benutzerrichtlinien enthalten. Eine lokale Konfiguration der Computerrichtlinien ist nur über die lokale Computerrichtlinie gegeben.

**Gruppenrichtlinien-Bereiche**

Folgende Bereiche existieren im Computer-Teil einer Gruppenrichtlinie: *Softwareeinstellungen, Windows-Einstellungen, Administrative Vorlagen*.

Die Softwareeinstellungen sind vor allem beim Einsatz in einer Domäne relevant. Mit ihrer Hilfe kann über die Gruppenrichtlinien Software installiert, aktualisiert oder deinstalliert werden. Es sollte darüber nachgedacht werden, Software Deployment Tools für diese Funktion einzuführen. Über Skript-Richtlinien können Skripte spezifiziert werden, die beim Starten oder Herunterfahren des Systems ausgeführt werden. Diese Methode sollte genutzt werden, da die Benutzerkontensteuerung alte Netlogon-Skripte blockt.

Für die toolgesteuerte Verteilung von Software bietet Microsoft beispielsweise das Tool Microsoft System Center Configuration Manager an. Die Softwareverteilung mit einem Tool sollte aufgrund einer höheren Effizienz und Effektivität im Vergleich zur manuellen Verteilung bevorzugt werden.

Sicherheitsrelevante Einstellungen werden als Unterbereich der Windows Einstellungen über die *Sicherheitseinstellungen* verwaltet. Die *Sicherheitseinstellungen* unterteilen sich in weitere Bereiche wie *Kontorichtlinien (Kennwortrichtlinien, Kontosperrungsrichtlinien, Kerberos-Richtlinie), Lokale Richtlinien (Überwachungsrichtlinien, Zuweisen von Benutzerrechten, Sicherheitsoptionen), Richtlinien öffentlicher Schlüssel, Richtlinien für Softwareeinschränkung, IP-Sicherheitsrichtlinien*. Bei der Festlegung von Richtlinien für Sicherheitseinstellungen ist zu beachten:

- Kontorichtlinien werden in einer Active Directory-Umgebung nur auf Domänenebene durchgesetzt.
- Die Verwendung von Richtlinien für eingeschränkte Gruppen verhindert nicht, dass Modifikationen an Gruppenmitgliedschaften durchgeführt werden können. Die unerlaubten Modifikationen werden aber bei der nächsten Anwendung der Richtlinien rückgängig gemacht.

Hervorzuhebende Neuerungen bei den Sicherheitseinstellungen ab Windows Vista sind die Konfigurationsmöglichkeiten für die lokale Firewall sowie für die Benutzerkontensteuerung (User Account Control, UAC).

Der Bereich *Administrative Vorlagen* wird für die Konfiguration der Windows Komponenten, des Systems, des Netzes sowie weiterer Anwendungen verwendet.

**Anwendungsspezifische Richtlinien**

Anwendungsspezifische Richtlinien werden im Bereich *Computerkonfiguration* | *Administrative Vorlagen und Benutzerkonfiguration* | *Administrative Vorlagen* definiert. Dabei können nicht nur Windows Komponenten wie NetMeeting, Internet Explorer, Windows Explorer und Windows Messenger konfiguriert werden, sondern auch Anwendungen, die ihre eigenen administrativen Vorlagen mitbringen, wie es bei Microsoft Office der Fall ist. Solche zusätzlichen administrativen Vorlagen müssen durch Administratoren explizit in eine Gruppenrichtlinie importiert werden.

Für die meisten Behörden und Unternehmen ist es empfehlenswert, alle vorhandenen Möglichkeiten zur zentralisierten anwendungsspezifischen Konfiguration auszunutzen. Durch die zentralisierte Vorgabe von sicherheitsrelevanten Einstellungen lassen sich viele Sicherheitsrisiken beseitigen. Welche Komponenten und/oder Anwendungen zentral durch GPOs konfiguriert werden, ist in Abhängigkeit von den individuellen Anforderungen festzulegen. Auch an

dieser Stelle sollte die Grundsatzregel umgesetzt werden, dass alle nicht benötigten Anwendungen und Komponenten zu deaktivieren sind (z. B. Windows Messenger). Die erforderlichen Anwendungen und Komponenten sind so restriktiv wie möglich zu konfigurieren. Wird zum Beispiel Microsoft NetMeeting benötigt, jedoch kein Desktop Sharing verwendet, so ist dieses Merkmal durch die Definition entsprechender Richtlinien zu deaktivieren.

Ab Windows Vista werden im Bereich *Administrative Vorlagen* wesentlich mehr Konfigurationsmöglichkeiten geboten, die bei der Planung zu betrachten sind, als bei früheren Versionen. Insbesondere sind seit Windows Vista folgende sicherheitsrelevante Neuerungen der anwendungsspezifischen Richtlinien hervorzuheben:

- Erweiterte GPO-Konfigurationsmöglichkeiten für den Internet Explorer.
  Die Erweiterungen betreffen insbesondere den Phishing Filter, die zentrale Aktivierung des geschützten Modus (Protected Mode) und die Behandlung von ActiveX-Steuerelementen. Diese anwendungsspezifischen Richtlinien werden im Bereich *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Internet Explorer und Benutzerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Internet Explorer* konfiguriert. Unter Windows 8 ist der Enhanced Protected Mode standardmäßig aktiviert. Weitere Neuerungen im Internet Explorer sind Do Not Track (DNT) und der standardmäßig integrierte Flash-Player.
- GPO-Konfigurationsmöglichkeiten für die BitLocker-Laufwerkverschlüsselung.
  Diese anwendungsspezifischen Richtlinien werden im Bereich *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *BitLocker-Laufwerkverschlüsselung* konfiguriert.
  TPM-spezifische Richtlinien sind im Bereich *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Trusted Plattform Module-Dienste* konfigurierbar.
- GPO-Konfigurationsmöglichkeiten für Windows Defender.
  Da Windows Defender vorwiegend für den Privatbereich entworfen wurde und nur ein geringes Sicherheitsniveau aufweist, ist vom alleinigen Einsatz des Windows Defender zur Identifizierung und Behandlung von Schadsoftware im professionellen Umfeld abzusehen. Der parallele Einsatz von Windows Defender mit einer Sicherheitslösung oder Lösung zum Schutz vor Schadsoftware eines Drittherstellers muss zuvor in einer Produktivumgebung getestet werden. Potenzielle Probleme können bei Bedarf durch Deaktivierung des Windows Defender über die anwendungsspezifische Richtlinie Windows Defender deaktivieren im Bereich *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Defender* vermieden werden.

**Benutzerspezifische Richtlinien**

Windows-Versionen ab Windows XP ermöglichen die Definition benutzerspezifischer Gruppenrichtlinien, die auf Benutzerbasis angewandt werden. Speziell beim Einsatz in einer Active Directory-Umgebung kann dies Sicherheitsvorteile bringen, indem Einschränkungen in Abhängigkeit vom Benutzertyp definiert werden und beispielsweise zwischen normalen und administrativen Benutzern unterschieden wird. Jede Differenzierung lässt sich durch eine geeignete OU-Struktur und die Definition entsprechender Gruppenrichtlinien umsetzen. Durch die ab Windows Vista erweiterte lokale Gruppenrichtlinie um Mehrfachgruppenrichtlinienobjekte (siehe Abschnitt: Planung lokaler Gruppenrichtlinien), lässt sich eine entsprechende Differenzierung auch ohne Active Directory implementieren.

Die Arbeitsumgebung eines Benutzers kann ab Windows XP durch die Verwendung von Gruppenrichtlinien in ihrer Funktionalität eingeschränkt werden. Insbesondere sollte durch die Definition der geeigneten Parameterwerte die Konfiguration der Microsoft Management Console (MMC), des Startmenüs, der Taskleiste, des Desktops, der angezeigten Systemsteuerungskomponenten sowie der zugelassenen Windows-Anwendungen und unter Windows 8 die Verwendung von Apps aus dem Windows Store vorgenommen werden.

Für die Arbeitsumgebung eines normalen Benutzers sollten nach Möglichkeit folgende Einschränkungen vorgenommen werden:

- Ausschließlich Anzeige zugelassener Systemsteuerungskomponenten,
- Sperren der meisten MMC Snap-ins (das *Zertifikate* Snap-in sollte zugelassen bleiben, wenn Zertifikate zum Einsatz kommen),
- Einschränkungen des Taskplaners,
- Deaktivierung oder Einschränkung des Active Desktops,
- Einschränkungen im Bereich der Start- und Taskleiste,
- Einschränkungen bei der Installation und Nutzung von Wechselspeichergeräten (z. B. USB-Flash-Speicher, USB-Festplatten, CDs und DVDs) ab Windows Vista.
- Ab Windows 8 besteht die Möglichkeit, sich mit einem Microsoft-Konto am System anmelden zu können, um Apps aus dem Windows Store herunterzuladen oder Microsoft Cloud-Dienste (z. B. Skydrive) zu nutzen. In einem Unternehmensumfeld sollten aus Sicherheitsgründen stattdessen zentral verwaltete Domänenkonten genutzt werden.

Bei der Definition der Richtlinien *Nur zugelassene Windows-Anwendungen ausführen* und *Angegebene Windows-Anwendungen nicht ausführen* ist zu beachten, dass diese Einschränkungen nur für den Start der Anwendungen mit dem Windows Explorer gelten. Der Start einer "verbotenen" Anwendung durch den Taskmanager, von der Kommandozeile oder aus einem anderen Programm heraus, wird damit nicht verhindert. Hierfür stehen je nach Notwendigkeit andere Mittel wie Richtlinien für Softwareeinschränkung (englisch Software Restriction Policy) oder beispielsweise unter Windows 7 Ultimate/Enterprise AppLocker zur Verfügung.

Außerdem sollten die anwendungsspezifischen Richtlinien zur Einschränkung der Anwendungen/Systemkomponenten auf Benutzer- bzw. Gruppenbasis verwendet werden.

**Einsatz außerhalb von Active Directory-basierten Umgebungen**

Beim Einsatz von Windows-Clients als Stand-alone-System oder in einer Windows-NT-Domäne sind die zentralen Konfigurationsmöglichkeiten mittels globaler Gruppenrichtlinien nicht verfügbar. In diesem Fall müssen die lokalen Gruppenrichtlinien jedes IT-Systems zur Umsetzung der definierten sicherheitsrelevanten Parametereinstellungen benutzt werden. Grundlage ist der, in der Planungsphase festgelegte, Mechanismus zur Pflege von lokalen Gruppenrichtlinien auf mehreren IT-Systemen. Um dennoch eine einheitliche Konfiguration von Stand-alone-Systemen erzielen zu können, kann der Microsoft Security Compliance Manager genutzt werden, um ein Konfigurationstemplate zu erstellen, welches dann mittels dem mitgelieferten Werkzeug LocalGPO auf die einzelnen Systeme appliziert werden kann.

**Einsatz in Active Directory-basierten Umgebungen**

Beim Einsatz von Windows-Clients in Active-Directory-basierten Umgebungen ist der Einsatz lokaler Gruppenrichtlinien auf einzelnen Systemen ebenfalls möglich. In diesem Fall werden jedoch die Vorteile der zentralen Administrati-

on nicht genutzt. Folglich sollten, die Active Directory-basierten Gruppenrichtlinien auf der Standort und Domänenebene bzw. auf Ebene einzelner Organisationseinheiten für die Umsetzung der Sicherheitseinstellungen benutzt werden.

Lokale Gruppenrichtlinien auf einzelnen Systemen sollten aufgrund ihrer schlechten zentralen Verwaltbarkeit nach Möglichkeit nicht eingesetzt werden, sofern eine zentrale Verwaltung nicht durch entsprechende Werkzeuge unterstützt wird. Ist jedoch der gemeinsame Einsatz lokaler und Active Directory-basierter Gruppenrichtlinien aus bestimmten Gründen erforderlich, so müssen die Parametereinstellungen aller Gruppenrichtlinien aufeinander abgestimmt werden, um Konflikte in der Vererbungshierarchie zu vermeiden.

Die Verwendung von Active-Directory-basierten Gruppenrichtlinien macht die Planung ihres Einsatzes in der Domäne erforderlich. Weitere Informationen zu Active-Directory-basierten Gruppenrichtlinien sind in der Maßnahme M 2.231 *Planung der Gruppenrichtlinien unter Windows* zusammengefasst. Im Allgemeinen müssen folgende Aspekte der Verwendung von Active-Directory-basierten Gruppenrichtlinien bedacht werden:

- OU- und Gruppenstruktur im Active Directory,
- Hierarchie der GPOs im Active Directory und generell das GPO-Konzept,
- Vererbung der Gruppenrichtlinien,
- Blockieren und Erzwingen der GPO-Überdeckung,
- Priorisierung bzw. die Festlegung der Reihenfolge bei Abarbeitung mehrerer GPOs,
- Berechnung der jeweils gültigen Einstellungen für einen Gruppenrichtlinienparameter und die GPO-Abarbeitungsreihenfolge,
- Steuerung der Abarbeitung von Gruppenrichtlinien,
- Verlinken der Gruppenrichtlinien,
- GPO-Schutz.

Ab Windows Vista wurden die Gruppenrichtlinien-Standard-Snap-ins *Gruppenrichtlinienverwaltung* und *Gruppenrichtlinienobjekt-Editor* zur Erstellung und Verwaltung von Gruppenrichtlinienobjekten überarbeitet. Versions-spezifische Richtlinien können nur von den in den jeweiligen Windows-Versionen enthaltenen, neuen Versionen dieser Verwaltungswerkzeuge dargestellt werden. Die Verwaltung der Versions-spezifischen Richtlinien im Active Directory sollte ausschließlich von einem Domänenmitglied mit der passenden Betriebssystemversion aus erfolgen.

Die computerspezifischen Gruppenrichtlinien werden während des Boot-Vorgangs angewandt, die benutzerspezifischen Gruppenrichtlinien erst bei der Benutzeranmeldung. Dabei besitzt die benutzerspezifische Gruppenrichtlinie den Vorrang und überschreibt gegebenenfalls Einstellungen, die in der Computer-Richtlinie definiert sind. Für Active-Directory-basierte Gruppenrichtlinien bietet sich der sogenannte Loopback-Verarbeitungsmodus an. Dieser stellt sicher, dass eine Computer-Richtlinie nicht von benutzerspezifischen Gruppenrichtlinien ausgehebelt werden kann. Dieser Verarbeitungsmodus sollte aktiviert werden, wenn sich die Einstellungen ausdrücklich auf den Computer beziehen und von Benutzern unabhängig sein sollen wie beispielsweise bei einem System im Kiosk-Betrieb. Es gibt zwei Varianten der Loopback-Verarbeitung: *Ersetzen* und *Zusammenführen*. Im *Ersetzen*-Modus werden keine benutzerspezifischen Einstellungen beachtet und die computerspezifische Gruppenrichtlinie wird angewandt. Der *Zusammenführen*-Modus führt die Einstellungen der Benutzer-GPO mit den Einstellungen der Computer-GPO zusammen. Ob eine Gruppenrichtlinie im Loopback-Verarbeitungsmodus und in welcher Variante eingesetzt werden soll, hängt immer vom jeweiligen Einsatzsze-

nario und den Anforderungen der bestehenden Umgebung ab. Je nach Szenario kann dieser Modus sicherheitsrelevante Vorteile bringen, eine allgemeine Empfehlung ist an dieser Stelle nicht möglich.

Wird eine GPO gleichzeitig auf Windows-Clients verschiedener Versionen in einer Domäne angewandt, muss auf die Anwendbarkeit der Parametereinstellungen auf diese unterschiedlichen Systeme geachtet werden. Teilweise können sich Unterschiede auch bereits zwischen verschiedenen Service Packs derselben Windows-Version ergeben. Grundsätzlich gilt, dass spezifische Parametereinstellungen für neuere Windows-Versionen von älteren Systemen ignoriert werden. Das unterschiedliche Verhalten verschiedener Betriebssysteme bei gleichen Einstellungen, wie EFS-Richtlinien (siehe M 4.147 *Sichere Nutzung von EFS unter Windows*), ist ebenfalls zu berücksichtigen. Es ist wesentlich zu wissen, ab welcher Betriebssystemversion die zu definierenden Einstellungen angewandt werden, um potenzielle Probleme zu vermeiden. Diese Information ist meist bei der Beschreibung der jeweiligen Richtlinie dokumentiert.

Die beiden Mechanismen *Sicherheitsfilter* (englisch *Security Filtering*) und *WMI Filter* ermöglichen es, Gruppenrichtlinien differenziert anzuwenden. Der *Security Filtering* Mechanismus gibt Sicherheitsgruppen an, für die die jeweilige Gruppenrichtlinie gilt. Standardmäßig wird eine Gruppenrichtlinie auf *Authentifizierte Benutzer* angewandt. *WMI Filter* steuern die Anwendung einer Gruppenrichtlinie in Abhängigkeit von der Beschaffenheit des IT-Systems (z. B. Betriebssystem, Service Pack Version, Festplattenplatz). Beide Mechanismen ermöglichen im Allgemeinen eine flexible Steuerung der Anwendung einer Gruppenrichtlinie auf ein Benutzer- oder Computer-Objekt im Active Directory. Ihr Einsatz erfordert jedoch genaue Planung und ausreichendes Testen im Vorfeld.

**Sicherheitsvorlagen**

Die Parametereinstellungen in Gruppenrichtlinien können nicht nur direkt mit dem entsprechenden MMC Snap-in, sondern auch durch den Import einer Sicherheitsvorlage vorgenommen werden. Sicherheitsvorlagen werden zur Konfiguration der Sicherheitseinstellungen verwendet. Sie werden in textbasierter Form in Richtliniendateien gespeichert (INF-Dateien) und können mit dem MMC Snap-in *Sicherheitsvorlagen* oder mit einem gewöhnlichen Texteditor bearbeitet werden. Eine Vielzahl definierter Sicherheitsvorlagen sind sowohl von Microsoft als auch von Drittanbietern frei verfügbar. Microsoft bietet hierbei unter Anderem die Sicherheitsrichtlinien Enterprise Client (EC) und Specialized Security Limited Functionality (SSLF).

Als grundsätzliche Vorgehensweise wird folgendes vorgeschlagen:

- Eine bestehende Sicherheitsvorlage wird ausgewählt (z. B. von Microsoft). Die Wahl einer Vorlage mit einem höheren Sicherheitsniveau wie Highly Secure (hisec*.inf) wird dabei empfohlen, da es aus Sicherheitssicht vorteilhafter ist, "sicherere" Einstellungen bei Notwendigkeit abzuschwächen als umgekehrt.
- Die Vorlage muss an lokale Anforderungen angepasst werden, die vorgenommenen Änderungen sind dabei zu begründen und zu dokumentieren.
- Die erstellte Vorlage wird in die entsprechende Gruppenrichtlinie importiert. Um beim Import einer Sicherheitsvorlage in eine Gruppenrichtlinie sicherzustellen, dass alle Einstellungen überschrieben werden, sollte die Verwendung der Option *Datenbank vor dem Importieren aufräumen* genutzt werden.

Eine weitere Verwendungsmöglichkeit finden die Sicherheitsvorlagen bei der Sicherheitsanalyse vorgenommener Einstellungen. Die aktuell auf einem Computer gültigen Einstellungen können mit denjenigen innerhalb einer INF-Datei verglichen werden. Dies kann entweder mittels des Sicherheitskonfiguration und -analyse Snap-ins der MMC oder mittels des Kommandozeilenwerkzeugs secedit erfolgen.

Durch das Anwenden der Sicherheitsvorlage *secsetup.inf*, die sich im Verzeichnis *%SystemRoot%\repair* befindet, können die Standardeinstellungen von Windows XP wiederhergestellt werden.

Eine weitere Möglichkeit, Sicherheitsvorlagen für unterschiedliche Windows-Versionen zu erstellen, bietet der Security Compliance Manager von Microsoft. Mit dem Security Compliance Manager (SCM) erstellte Sicherheitsvorlagen können in die Gruppenrichtlinie importiert werden. Zusätzlich wird mit dem Security Compliance Manager noch das Werkzeug LocalGPO ausgeliefert, welches die Absicherung von Stand-alone-Systemen, unter Nutzung der mit dem Compliance Manager erstellten Sicherheitsvorlage erlaubt. Von Microsoft bereitgestellte Baselines sind für unterschiedliche Systemrollen verfügbar und können mit dem SCM gemäß den Unternehmensvorgaben angepasst werden. Bei den Hilfsmitteln für den IT-Grundschutz finden sich Vorlagen für Windows 7 und Windows Server 2008, die die Anforderungen der IT-Grundschutz-Kataloge berücksichtigen und anhand der beigefügten Dokumentation auf das jeweilige Einsatzumfeld angepasst werden können.

**Definition eigener administrativer Vorlagen**

Die sicherheitsrelevanten Einstellungen in Gruppenrichtlinien sind nicht nur im Bereich Windows-Einstellungen, sondern auch im Bereich der administrativen Vorlagen zu finden. Administrative Vorlagen bestehen aus einzelnen Parametern, die die Einstellungen zugehöriger Registry-Schlüssel konfigurieren. Die entsprechenden ADM-Dateien bestimmen die einzelnen Parameter, die sich innerhalb der administrativen Vorlagen konfigurieren lassen. Windows XP enthält standardmäßig mehrere ADM-Dateien, die beispielsweise Konfigurationsmöglichkeiten für den Internet Explorer beinhalten. Es ist zu beachten, dass die administrativen Vorlagen lediglich Einstellungsparameter und keine Einstellungen definieren und somit nicht zum Speichern und Verteilen der Einstellungen verwendet werden. Ab Windows Vista wurden die ADM-Dateien durch ADMX-Vorlagedateien ersetzt, die eine neue Syntax auf XML-Basis für die Registry-basierten Richtlinien verwenden. ADMX-Dateien bieten den Vorteil, dass sie, im Gegensatz zu ADM-Dateien, sprachneutral sind und in Verbindung mit sprachspezifischen ADML-Dateien auf beliebige Sprachversionen angewendet werden können.

In Unterschied zu ADM-Dateien werden ADMX-Dateien nicht mehr einzeln in jedes Gruppenrichtlinienobjekt geladen, sondern in einem zentralen Speicher verwaltet. Da sich die Gruppenrichtlinien Snap-ins *Gruppenrichtlinienverwaltung* und *Gruppenrichtlinienobjekt-Editor* standardmäßig mit dem PDC-Emulator verbinden, sollte in einer Active Directory-basierten Umgebung die zentrale Speicherung der ADMX/ADML-Dateien im SYSVOL-Verzeichnis auf diesem Betriebsmaster erfolgen.

Es ist auch möglich, eigene administrative Vorlagen zu definieren. Diese Vorgehensweise empfiehlt sich vor allem, wenn in einem Unternehmen bzw. einer Institution reger Gebrauch von direkten Registry-Einstellungen gemacht wird. Durch die einmalige Definition einer administrativen Vorlage können die entsprechenden Registry-Einstellungen komfortabel über den Gruppenrichtli-

nien-Mechanismus verteilt werden. Dies stellt unter anderem sicher, dass die Registry-Einstellungen tatsächlich auf allen Zielsystemen umgesetzt werden.

**Testen der festgelegten Gruppenrichtlinien**

Die festgelegten Gruppenrichtlinien müssen getestet werden, bevor sie in einer Produktivumgebung eingesetzt werden. Die Tests müssen gewährleisten, dass einerseits die benötigte Funktionalität für die Mitarbeiter nicht eingeschränkt wurde und dass andererseits alle sicherheitsrelevanten Einschränkungen korrekt umgesetzt werden.

**Verwaltung von Gruppenrichtlinien mittels Microsoft PowerShell**

Seit Windows 7 gibt es die Möglichkeit, Gruppenrichtlinien mittels PowerShell-Befehlszeile zu verwalten. Es ist möglich, während der Anmeldung und des Starts PowerShell-Skripts auszuführen. Zur Absicherung der PowerShell-Laufzeitumgebung ist M 4.421 *Absicherung der Windows PowerShell* zu berücksichtigen.

Prüffragen:

- Erfolgt eine geeignete Verteilung der Sicherheitseinstellungen auf mehrere Gruppenrichtlinienobjekt (GPO)?
- Ist sichergestellt, dass auf allen Rechnern die richtigen Gruppenrichtlinienobjekte für die jeweils eingesetzte Windows-Version angewandt werden?
- Sind die Gruppenrichtlinien (Gruppen, anwendungsspezifische, benutzerspezifische) bedarfsgerecht konfiguriert?
- Wurden alle sicherheitsrelevanten Einstellungen in den Gruppenrichtlinien konfiguriert?
- Sind alle nicht benötigten Anwendungen und Komponenten mittels Gruppenrichtlinien oder durch die Nutzung einer Software zur Anwendungskontrolle deaktiviert worden?
- Ist eine für die Windows-Clients bedarfsgerechte Arbeitsumgebung für die Benutzer eingerichtet worden?
- Werden die Gruppenrichtlinien getestet, bevor sie in einer Produktivumgebung eingesetzt werden?
- Wurden die Konfigurationsempfehlungen des Herstellers zur Absicherung der Systeme herangezogen?
- Werden Werkzeuge eingesetzt, welche eine zentrale und einheitliche Konfiguration der Sicherheitseinstellungen ermöglichen?

# M 2.327 Sicherheit beim Fernzugriff auf Clients ab Windows XP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Mit Windows XP wurden zwei neue Mechanismen zur Fernsteuerung eines Rechners eingeführt: der Remote-Desktop und die Remote-Unterstützung. Der Remote-Desktop basiert auf der Technologie der Terminaldienste (RDP-Protokoll) und macht eine Anmeldung am System über ein Netz möglich. Die Remote-Unterstützung erweitert den Remote-Desktop um die Möglichkeit, innerhalb einer bestehenden Sitzung auf die Bildschirminhalte eines entfernten Rechners zuzugreifen und gegebenenfalls auch die Steuerung des Rechners zu übernehmen. Von Windows Vista,Windows 7 und Windows 8 werden diese Mechanismen zur Fernsteuerung ebenfalls unterstützt.

Der Remote-Desktop wird primär für Wartungsarbeiten auf Windows- Rechnern oder für den Zugriff auf virtuelle Maschinen über ein Netz eingesetzt. Hierzu können auch eine Vielzahl von Tools von Fremdanbietern eingesetzt werden. Der Einsatz der Remoteunterstützung ist bei Unternehmen und Behörden vor allem in Szenarien denkbar, wo Mitarbeiter eines internen oder externen Support-Zentrums einem Benutzer die notwendige Hilfestellung geben sollen. Bei einem aktivierten Remote-Zugriff via *mmc.exe*-Tools, telnet und Kommandozeilentools ist immer ein Timeout zu setzen. Ein Timeout sorgt für eine automatisierte Abmeldung des Nutzers vom Fernzugriff bei Inaktivität nach einer festzulegenden Zeitspanne.

Bei der Benutzung des Remote-Desktops ist zu beachten, dass immer nur genau ein Benutzer auf dem Zielrechner angemeldet sein kann. Der Remote-Desktop ist nicht als Ersatz für Terminaldienste zu verstehen.

Bei Windows-Versionen, bei denen der Remote-Desktop standardmäßig aktiviert ist, ist diese Einstellung zu deaktivieren. Remote-Desktop und Remote-Unterstützung können mittels der folgenden Gruppenrichtlinienobjekte aktiviert oder deaktiviert werden: *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste* sowie *Benutzerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste* und *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Remoteunterstützung* oder lokal über die Systemsteuerung (bei Windows XP unter *System* | *Remote* und bei Windows Vista unter *System* | *Erweiterte Systemeinstellungen* | *Remote*) erfolgen.

Unter Windows 7 und 8 ist die Remote-Unterstützung mittels der folgenden Gruppenrichtlinienobjekte zu aktivieren: *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Remoteunterstützung*

Die Konfiguration für den Remote-Desktop ab Windows 7 ist mittels des folgenden Gruppenrichtlinienobjektes zu aktivieren: *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Remotedesktopdienste.*

Ab Windows 7 lautet der Pfad für die lokale Einstellung über die Systemsteuerung *System und Sicherheit* | *System* | *Remoteeinstellungen.*

Beim Einsatz dieser beiden Technologien muss auf folgendes geachtet werden:

- Es ist starke Verschlüsselung (128-bit, Einstellung *Höchste Stufe*) zu verwenden. Diese muss in der Richtlinie *Verschlüsselungsstufe der Clientverbindung* (für Windows XP festzulegen unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Terminaldienste* | *Verschlüsselung und Sicherheit* und für Windows Vista unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste* | *Terminalserver* | *Sicherheit*) aktiviert werden. In Windows 7 und Windows 8 findet sich die Einstellung unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Remotedesktopdienste* | *Remotedesktopsitzungs-Host* | *Sicherheit*. Unter *Verschlüsselungsstufe der Clientverbindung festlegen* ist auch die *Höchste Stufe* auszuwählen.
- Es sollte keine automatische Kennwortanmeldung benutzt werden. Dies muss für Windows XP durch die Aktivierung der Richtlinie *Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Terminaldienste* | *Verschlüsselung und Sicherheit* ausgeschaltet werden. Das gilt auch für den XP-Mode unter Windows 7. In Windows Vista ist die Einstellung unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste* | *Terminalserver* | *Sicherheit* zu aktivieren. In Windows 7 und Windows 8 muss die Einstellung *Bei der Verbindungsherstellung immer zur Kennworteingabe auffordern* unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Remotedesktopdienste* | *Remotedesktopsitzungs-Host* | *Sicherheit* aktiviert werden.
- Die Umleitungen von Zwischenablage, Drucker, Dateiablagen und Smartcard-Anschlüssen, die für Windows XP unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Terminaldienste* | *Client/Server-Datenumleitung* aktiviert und deaktiviert werden, sollten nach Möglichkeit vermieden. werden. Unter Windows Vista lauten die entsprechenden Pfade *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste* | *Terminalserver* | *Druckerumleitung* bzw. *Geräte- und Ressourcenumleitung* bzw. *Temporäre Ordner*. In Windows 7 und Windows 8 sind die Optionen unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Remotedesktopdienste* | *Remotedesktopsitzungs-Host* | *Geräte- und Ressourcenumleitung* bzw. *Temporäre Ordner* zu finden.
- Zusätzlichen Schutz bei der Nutzung von Remote-Desktop bietet die Funktion der Netzauthentifizierung (*Benutzerauthentifizierung mit Authentifizierung auf Netzwerkebene ist für Remoteverbindungen erforderlich*), die seit Windows Vista und Windows Server 2008 zur Verfügung steht. Mit dieser Funktion authentifizieren Remotedesktopclients den Benutzer, der eine Verbindung herstellen will, zuerst über das Netz, bevor die eigentliche Remotedesktopverbindung aufgebaut wird. Unbefugte, welche kein Domänenkonto besitzen, können somit keine Remotedesktopverbindung starten. Bei der Nutzung dieser Funktion muss sichergestellt werden, dass im Unternehmen Remotedesktopclients eingesetzt werden, welche die Netzauthentisierung unterstützen. Unter Windows Server 2012 und Windows 8 wird die Authentisierung auf Netzebene standardmäßig erzwungen.

Die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff wird entweder über die Zuweisung entsprechender Benutzerrechte in den Richtlinien (*Anmeldung über Terminaldienste zulassen*, *Anmeldung über Terminaldienste verweigern*) oder über die Systemsteuerung spezifiziert. Standardmä-

ßig ist der entfernte Zugriff für die Gruppe der Administratoren sowie für die Gruppe *Remotedesktopbenutzer*, die nach der Installation leer ist, möglich.

Für den Aufbau einer Remote-Unterstützungssitzung gibt es die folgenden Möglichkeiten:

- "Eine vertrauenswürdige Person zur Unterstützung einladen"
- "Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten"

Der aktuell angemeldete Benutzer muss dem Aufbau einer Sitzung explizit zustimmen. Der Benutzername des Helfers stellt wegen fehlender Authentisierung die Schwachstelle beim Verbindungsaufbau dar. Aus diesem Grund erfordert der Remote-Unterstützungsmechanismus einen sorgfältigen Einsatz.

Es gibt zwei Möglichkeiten eine Remote-Sitzung zu starten. Die erste Option ist die Einwahl mittels Einladungsdatei. Soll eine Remote-Sitzung über diese Option aufgebaut werden, muss sich der Kommunikationspartner stets, bei jeder neuen Sitzung, mit einem entsprechenden Kennwort authentisieren. Dieses Kennwort muss durch den anderen Kommunikationspartner über einen gesonderten Kanal erfragt werden.

Die zweite Option ist die Verwendung von EasyConnect. Hierbei muss sich der Kommunikationspartner einmalig per Kennwort authentisieren. Da bei späteren Sitzungen der gleichen Kommunikationspartner eine weitere Authentisierung nicht notwendig ist, sollte EasyConnect grundsätzlich im Unternehmen nicht eingesetzt werden. Die Option der Einwahl mittels Einladungsdatei ist zu bevorzugen.

Durch die Definition entsprechender Richtlinien ist beim Einsatz der Remote-Unterstützung folgendes zu gewährleisten:

- Eine Sitzung sollte nur nach einer expliziten Einladung aufgebaut werden. Soll das Anbieten der Remote-Unterstützung möglich sein, darf der Verbindungsaufbau nur bestimmten Benutzergruppen erlaubt werden (z. B. Support-Mitarbeiter). Die Definition erfolgt hierbei in Form von:
  <Domänenname>\<Benutzername>
  <*Domänenname*>\<*Gruppenname*>
  <*Benutzername*>@<*Domain*>.<*TopLevelDomain*>.
  Eine Auswahl aus vorhandenen Benutzern bzw. Gruppen ist nicht möglich.
- Die maximale Gültigkeitsdauer der Einladung muss auf eine, für das Unternehmen oder die Institution annehmbare Größe, eingestellt werden. Die maximale Gültigkeitsdauer sollte fünf Minuten nicht überschreiten.
- Wird eine Einladung zur Remote-Unterstützung in einer Datei abgespeichert, so sollte ein Kennwort vergeben werden, um die Gefahr einer unautorisierten Verwendung der Einladung zu verringern.
- Die Steuerungsart (*Helfer dürfen den Computer nur ansehen* bzw. *Helfer dürfen den Computer remote steuern*) sollte nach Möglichkeit restriktiv (*Helfer dürfen den Computer nur ansehen*) gesetzt werden.

Beim Einsatz von Remote-Desktop und/oder Remote-Unterstützung sind die Auswirkungen auf die Konfiguration und Verwaltung von Firewalls zu berücksichtigen. Grundsätzlich wird empfohlen, keine Remote-Desktop- oder Remote-Unterstützungsverbindungen von außerhalb des eigenen Netzes zuzulassen.

Zusammengefasst gilt, dass der Einsatz von Fernsteuerungsmechanismen sehr sorgfältig abgewogen werden muss. Insbesondere aufgrund der bestehenden Unterschiede bei der Benutzerauthentisierung sollten die Vor- und Nachteile des jeweiligen Mechanismus in Betracht gezogen werden. Wird in einem Unternehmen oder einer Behörde kein Gebrauch von Remote-Desktop

bzw. Remote-Unterstützung gemacht, so sind diese unbedingt zu deaktivieren.

**Basiseinstellungen für GPOs**

Die nachfolgenden Einstellungen gelten nur für den Einsatz beider Fernsteuerungsmechanismen. Soll einer der beiden oder beide Mechanismen nicht verwendet werden, so ist dieser zu deaktivieren. Hierfür ist die Modifikation der unten angegebenen Richtlinieneinstellungen notwendig.

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Computer ab Windows 7 auf, die für die Benutzung von Remote-Desktop und Remote-Unterstützung konfiguriert werden sollten.

| Richtlinie | Status | Einstellung |
|---|---|---|
| Computerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Remotedesktopdienste \| Remotedesktopsitzungs-Host \| Sicherheit \| Bei der Verbindungsherstellung immer zur Kennworteingabe auffordern | Aktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Remotedesktopdienste \| Remotedesktopsitzungs-Host \| Sicherheit \| Benutzerauthentifizierung mit Authentifzierung auf Netzwerkebene ist für Remoteverbindungen erforderlich | Aktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Remotedesktopdienste \| Remotedesktopsitzungs-Host \| Sicherheit \| Verschlüsselungsstufe der Clientverbindung festlegen | Aktiviert | Höchste Stufe |
| Computerkonfiguration \| Administrative Vorlagen \| System \| Remoteunterstützung \| Remoteunterstützung anbieten konfigurieren | Deaktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| System \| Remoteun- | Aktiviert | Helfer dürfen den Computer remote steuern. |

| Richtlinie | Status | Einstellung |
|---|---|---|
| terstützung \| Angeforderte Remoteunterstützung konfigurieren | | Maximale Gültigkeitsdauer: 5 Minuten |

Tabelle: Gruppenrichtlinieneinstellungen für Computer (Windows 7 und Windows 8)

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Benutzer ab Windows 7 auf, die für die Benutzung von Remote-Desktop und Remote-Unterstützung konfiguriert werden sollten.

| Richtlinie | Status | Einstellung |
|---|---|---|
| Benutzerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Remotedesktopdienste \| Remotedesktopverbindungs-Client \| Speichern von Kennwörtern nicht zulassen | Aktiviert | |
| Benutzerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Remotedesktopdienste \| Remotedesktop-sitzungs-Host \| Verbindungen \|Regeln \| für Remotesteuerung von Remotedesktopdienste-Benutzersitzungen festlegen | Aktiviert | Vollzugriff mit Erlaubnis des Benutzers |

Tabelle: Gruppenrichtlinieneinstellungen für Benutzer (Windows 7 und Windows 8)

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Computer unter Windows Vista auf, die für die Benutzung von Remote-Desktop und Remote-Unterstützung konfiguriert werden sollten.

| Richtlinie | Status | Einstellungen |
|---|---|---|
| Windows Vista: Computerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Terminalserver \| Sicherheit \| Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern | Aktiviert | |
| Windows Vista: Computerkonfiguration \| Administrative Vorlagen \| Win- | Aktiviert | Höchste Stufe |

| Richtlinie | Status | Einstellungen |
|---|---|---|
| dows-Komponenten \| Terminaldienste \| Terminalserver \| Sicherheit \| Verschlüsselungsstufe der Clientverbindung festlegen | | |
| Computerkonfiguration \| Administrative Vorlagen \| System \| Remoteunterstützung \| Remoteunterstützung anbieten | Deaktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| System \| Remoteunterstützung \| Angeforderte Remoteunterstützung | Aktiviert | Helfer dürfen den Computer remote steuern. Maximale Gültigkeitsdauer: 5 Minuten |

Tabelle: Gruppenrichtlinieneinstellungen für Computer (Windows Vista )

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Benutzer unter Windows Vista auf, die für die Benutzung von Remote-Desktop und Remote-Unterstützung konfiguriert werden sollten.

| Richtlinie | Status | Einstellungen |
|---|---|---|
| Windows Vista: Benutzerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Remotedesktopverbindungs-Client \| Speichern von Kennwörtern nicht zulassen | Aktiviert | |
| Windows Vista: Benutzerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Terminalserver \| Verbindungen \| Regeln für Remoteüberwachung von Terminaldienste-Benutzersitzungen festlegen | Aktiviert | Vollzugriff mit Erlaubnis des Benutzers |

Tabelle: Gruppenrichtlinieneinstellungen für Benutzer (Windows Vista) Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Computer unter Windows XP auf, die für die Benutzung von Remote-Desktop und Remote-Unterstützung konfiguriert werden sollten.

| Richtlinie | Status | Einstellung |
|---|---|---|
| Computerkonfiguration \| Administrative Vorlagen | Aktiviert | Höchste Stufe |

| Richtlinie | Status | Einstellung |
|---|---|---|
| \| Windows-Komponenten \| Terminaldienste \| Verschlüsselung und Sicherheit \| Verschlüsselungsstufe der Clientverbindung festlegen | | |
| Computerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Verschlüsselung und Sicherheit \| Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern | Aktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Client/Server-Datenumleitung \| * | Aktiviert / Deaktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| System \| Remoteunterstützung \| Remoteunterstützung anbieten | Deaktiviert | |
| Computerkonfiguration \| Administrative Vorlagen \| System \| Remoteunterstützung \| Angeforderte Remoteunterstützung | Aktiviert | Helfer dürfen den Computer remote steuern. Maximale Gültigkeitsdauer: 5 Minuten |

Tabelle: Gruppenrichtlinieneinstellungen für Computer (Windows XP)

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Benutzer unter Windows XP auf, die für die Benutzung von Remote-Desktop und Remote-Unterstützung konfiguriert werden sollten.

| Richtlinie | Status | Einstellungen |
|---|---|---|
| Benutzerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Regeln für Remoteüberwachung von Terminaldienste-Benutzersitzungen festlegen | Aktiviert | Vollzugriff mit Erlaubnis des Benutzers |
| Benutzerkonfiguration \| Administrative Vorlagen \| Windows-Komponenten \| Terminaldienste \| Client \| Speichern von | Aktiviert | |

| Richtlinie | Status | Einstellungen |
|---|---|---|
| Kennwörtern nicht zulassen | | |

Tabelle: Gruppenrichtlinieneinstellungen für Benutzer (Windows XP)

Prüffragen:

- Ist die automatische Kennwortanmeldung bei Windows-Client-Versionen ab Windows XP deaktiviert?
- Ist die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff über die Zuweisung entsprechender Benutzerrechte oder in den Richtlinien festgelegt worden?
- Sind die Gruppenrichtlinien sicher und bedarfsgerecht konfiguriert worden?
- Kann eine Remote-Unterstützung nur nach einer expliziten Einladung über EasyConnect oder eine Einladungsdatei erfolgen?
- Ist die maximale Gültigkeitsdauer der Einladung auf eine annehmbare Größe eingestellt worden?
- Wird bei der Speicherung einer Einladung in einer Datei ein Kennwort auf die Datei vergeben?
- Werden die Auswirkungen auf die Konfiguration der Firewall bei der Planung der Remote-Unterstützung berücksichtigt?
- Wurden die Fernsteuerungsmechanismen vollständig deaktiviert, wenn deren Einsatz nicht vorgesehen ist?

# M 2.328 Einsatz von Windows XP auf mobilen Rechnern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Beim Einsatz von Windows XP auf mobilen Rechnern ist wie für alle anderen mobilen PCs der Baustein B 3.203 Laptop zu beachten.

**Datenverschlüsselung**

Mobile Computer befinden sich häufig in Umgebungen, die deutlich niedrigere Sicherheit als geschützte Büroumgebungen bieten. Daher sollten die auf dem mobilen Rechner befindlichen schützenswerten Daten verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*. Neben einer Reihe von Drittprodukten können zur Verschlüsselung auch die integrierten Windows XP Mechanismen eingesetzt werden:

- Das verschlüsselnde Dateisystem (EFS, Encrypting File System),
- Verschlüsselung der Offlinedateien.

Informationen zur sicheren Nutzung von EFS sind in der Maßnahme M 4.147 *Sichere Nutzung von EFS unter Windows* zu finden.

Das Konzept der Offlinedateien wurde mit Windows 2000 eingeführt. Offlinedateien sind im Grunde genommen Kopien von Dokumenten, die sich auf einer Netzwerkfreigabe befinden. Sie werden auf dem lokalen Computer in einer Datenbank gespeichert, so dass der Zugriff auf Dokumente auch dann erhalten bleibt, wenn die Netzwerkfreigabe nicht erreichbar ist.

Die Möglichkeit, diese Offlinedateien zu verschlüsseln, wurde unter Windows XP eingeführt. Der gesamte Speicher für Offlinedateien, der Dateien aller Benutzer beinhaltet, wird mit einem computerspezifischen Schlüssel verschlüsselt. Die Verschlüsselung ist transparent für Benutzer und kann nur von Administratoren aktiviert bzw. deaktiviert werden. Die Aktivierung kann durch die Ordner-Eigenschaften im Windows Explorer unter *Extras* | *Ordneroptionen* | *Offlinedateien* | *Offlinedateien verschlüsseln, um Daten zu schützen* oder in Gruppenrichtlinien unter *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Offlinedateien* | *Offlinedateicache verschlüsseln* erfolgen. Die Aktivierung der Offlinedateien-Verschlüsselung empfiehlt sich insbesondere für den Fall, wenn zu synchronisierende Originaldokumente verschlüsselt sind und die lokalen Offline-Kopien in entschlüsselter Form vorliegen können.

Die Strategie zum Schutz der auf einem mobilen Rechner befindlichen Daten (Windows XP EFS, Offlinedateien-Verschlüsselung oder Verschlüsselung mit einem Drittprodukt) ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen.

**Lokale Firewall**

Im Gegensatz zu stationären organisationsinternen Desktops, besteht bei mobilen Clients die Möglichkeit, dass sie direkt an das Internet angeschlossen werden. Schutz durch eine lokal installierte Firewall ist in diesem Fall unabdingbar.

Mit Windows XP wurde eine neue Funktionalität eingeführt - die Internet Connection Firewall (ICF), die mit dem Service Pack 2 in Windows-Firewall umbenannt wurde. Die Windows-Firewall ist ein zustandsbehafteter Paketfil-

ter, der jedes TCP/IP oder UDP Paket analysiert und entsprechend der Konfiguration abarbeitet.

Windows XP Service Pack 2 enthält unter anderem folgende Verbesserungen für die ICF/Windows-Firewall:

- Standardmäßig aktiviert für alle Interfaces
- Schutz schon beim Booten
- Zentrale Konfiguration über GPOs
- Quell-Adresseneinschränkung für Port
- Kommandozeilenunterstützung
- Lock-Down Modus
- Ausnahmelisten für Applikationen
- Mehrere Policy Profile möglich
- RPC Unterstützung
- Rücksetzen auf Herstellerkonfiguration
- Unterstützung der unbeaufsichtigten Installation

Die Windows-Firewall filtert ausschließlich eingehende Verbindungen. Ausgehende Pakete werden hingegen keinen Restriktionen unterworfen. Dies bedeutet, dass z. B. eine Einschränkung der zugreifbaren Internetserver mit der Windows-Firewall nicht möglich ist. Programme, die für den Internet-Zugriff berechtigt sein sollen, können nicht festgelegt und kontrolliert werden. Daher bietet die Windows-Firewall keinen Schutz vor Trojanischen Pferden, die sich bereits auf dem Rechner befinden.

Der Einsatz von der ICF (vor Service Pack 2) im Unternehmens- oder Behördenkontext ist durch die fehlenden zentralen Konfigurationsmöglichkeiten nur schwer möglich. Durch die Gruppenrichtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Netzwerkverbindungen* | *Verwendung des Internetverbindungsfirewalls im eigenen DNS-Domänennetzwerk nicht zulassen* lässt sich die ICF lediglich komplett deaktivieren. Die Konfiguration der ICF erfolgt für jede Netzschnittstelle gesondert lokal auf dem Windows XP System.

Mit Einführung von Service Pack 2 besteht für Administratoren jetzt auch die Möglichkeit zur zentralen Verwaltung der Windows-Firewall durch Gruppenrichtlinien unter *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* |*Netzwerkverbindungen* | *Windows-Firewall*. Bei der Konfiguration der Windows-Firewall können verschiedene Profile angelegt werden, so dass die Windows-Firewall je nach aktueller Umgebung (organisationsinternes Netz oder mobiler Einsatz) unterschiedlich konfiguriert werden kann. Denkbar ist an dieser Stelle, dass in einem organisationsinternen Netz gewisse Ausnahmen für den eingehenden Verkehr zugelassen werden (z. B. für den Fernzugriff auf den Rechner). Hingegen für den mobilen Einsatz sollte die Windows-Firewall keine Ausnahmen zulassen und den gesamten eingehenden Verkehr blockieren. Ist ein Domain Controller in der Reichweite des Clients, so wird das Domänenprofil angewandt, ansonsten wird das mobile Profil aktiviert.

Die Windows-Firewall wird nach der Installation des Service Packs 2 standardmäßig auf allen vorhandenen Netzschnittstellen aktiviert. Dies kann, je nach vorhandenem Kontext im jeweiligen Unternehmen oder in der Behörde, unter Umständen auch zu Problemen führen (siehe auch M 2.329 *Einführung von Windows XP SP2*).

Sowohl die ICF als auch die Windows-Firewall bieten die Möglichkeit der Protokollierung an. Diese ist nach der Firewall-Aktivierung standardmäßig deaktiviert und muss explizit aktiviert werden. Dabei ist die Aktivierung der Protokollierung getrennt für angenommene und verworfene Pakete möglich, so dass die Protokollierung den individuellen Bedürfnissen angepasst werden kann.

Die Protokollierung erfolgt im vom W3C standardisierten Extended Log File Format. Ist die maximale Größe der Protokolldatei erreicht, so wird eine Kopie der Datei mit der angehängten Dateinamenerweiterung *old* erzeugt. Erreicht die Protokolldatei erneut die Maximalkapazität, werden die gesicherten Protokolldaten überschrieben und gehen verloren. Aus diesem Grund ist auf die ausreichende Größe der Protokolldatei zu achten. Da die Protokollierungsdaten lokal abgelegt werden, muss ein Mechanismus zum Sammeln der Daten realisiert werden. Windows XP stellt in dieser Hinsicht keinen eigenen Mechanismus zur Verfügung.

Sollen Windows XP Rechner vor Angriffen aus dem lokalen Netz oder Internet (mobiler Einsatz) geschützt werden, ist der Einsatz einer Personal Firewall eines Drittanbieters in der Regel empfehlenswerter, da diese meist einen erweiterten Funktionsumfang besitzt (z. B. Filtern ausgehender Verbindungen oder Einschränkung berechtigter Programme für den Internet-Zugriff).

Ist keine Personal Firewall installiert und aktiviert, so sollte bei einem mobilem IT-System zumindest die Windows-Firewall (bzw. ICF vor SP2) eingerichtet werden (siehe auch Maßnahmen M 5.91 *Einsatz von Personal Firewalls für Clients* ).

Prüffragen:

- Werden die schützenswerten Daten auf allen mobilen Windows-Systemen verschlüsselt?
- Wurde auf allen mobilen Windows-Systemen eine Personal Firewall oder die Windows-Firewall (bzw. ICF vor SP2) installiert bzw. aktiviert?

# M 2.329 Einführung von Windows XP SP2

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Seit August 2004 ist das Windows XP Service Pack 2 von Microsoft erhältlich. Am 12. April 2005 endete der Zeitraum, in dem die Installation von SP2 mit einem speziellen Tool von Microsoft trotz aktivierten internetbasierten Windows-Update-Dienstes verhindert werden kann. Nur Organisationen, die einen eigenen Update-Server betrieben, können die Installation von SP2 weiterhin verhindern.

Das Service Pack 2 enthält neben Fehlerkorrekturen und Verbesserungen an vorhandenen Mechanismen auch einige sicherheitsrelevante Änderungen oder Erweiterungen. Zu nennen sind hier beispielsweise:

- Insgesamt mehr als 600 neue Sicherheitsrichtlinien (Windows-Firewall, Security Center, Internet Explorer usw.)
- Verbesserungen in der Windows-Firewall (früher Internet Connection Firewall, ICF), vor allem die Möglichkeit zur zentralen Administration.
- Verbesserungen im Internet Explorer: Add-on Management, Pop-up Blocker, Zone Elevation Blocking, konsistente MIME-Verarbeitung, Restriktivere Behandlung von ActiveX-Steuerelementen.
- Integration von Virenschutzsoftware von Drittherstellern in das sogenannte "Sicherheitscenter", das zur zentralen Verwaltung und Überwachung von Windows Sicherheitseinstellungen gedacht ist.
- Speicherschutz gegen Buffer Overflows: Der Systemkern und die Bibliotheken wurden mit spezifischen Compiler-Flags übersetzt, das einen Schutz gegen Buffer Overflows gewährleisten soll. Dieses "No Execute" Flag (NX) wird von einigen aktuellen Prozessoren benutzt.
- Markierung von heruntergeladenen Dateien und Anhängen auf NTFS-Laufwerken (Attachment Execution Service).
- Die Benutzung von Raw-Sockets und die direkte Manipulation von IP-Paketen wurden deutlich eingeschränkt, Denial-of-Service Vorkehrungen sind in den TCP/IP Stack integriert.
- USB-Schreibschutz wurde implementiert, so dass mit einer geeigneten Konfiguration nur lesender Zugriff auf USB-Speichergeräte wie USB-Sticks und USB-Platten möglich ist (so wird ein unberechtigter Datenexport auf USB-Medien verhindert).

Die Konfiguration neuer Einstellungen und insbesondere Gruppenrichtlinieneinstellungen muss im Vorfeld der SP2-Installation festgelegt werden. Änderungen in Gruppenrichtlinien können weitreichende Auswirkungen in Unternehmen und Behörden mit Windows XP Clients haben und müssen daher von Administratoren unbedingt sorgfältig durchgeführt werden.

**Problemen vorbeugen**

Aufgrund der umfangreichen Veränderungen besteht insbesondere bei größeren Installationen in Unternehmen oder Behörden die Gefahr, dass die Installation des Service Packs 2 zu Problemen führen kann. Dies ist besonders dann kritisch, wenn Anwendungen nicht mehr lauffähig sind oder Firewall- und Antivirus-Programme betroffen werden. Um diese Probleme zu vermeiden, muss die Einführung von SP2 genauestens geplant und zunächst ausgiebig getestet werden. Vor allem die Funktionsfähigkeit der Anwendungssoftware muss im Vorfeld überprüft werden.

Folgende Probleme können durch die Installation von Service Pack 2 verursacht werden:

- Probleme bei der Verwaltung der GPOs mit alten Werkzeugen, da neue administrative Vorlagen lange Zeichenketten enthalten
- MMC Snap-In *Gruppenrichtlinienergebnissatz* funktioniert bei Remote-Anfragen nicht mehr aufgrund der standardmäßig nach der Installation aktivierten Firewall
- Probleme bei DCOM-Anwendungen, da ein neues DCOM-Authentisierungsmodell eingeführt wurde (z. B. bei Delegation von Gruppenrichtlinienergebnissatz-Aufgaben an nicht-administrative Benutzer)
- Anwendungsprobleme aufgrund der standardmäßig aktivierten Firewall
- Anwendungsprobleme aufgrund der Änderungen am TCP/IP-Stack (Einschränkung der Benutzung von Raw-Sockets)
- Skript- und ActiveX-Fehlermeldungen, Bilddarstellungsprobleme beim Öffnen gespeicherter Web-Seiten in Anwendungen (unter anderem auch in Microsoft Office Produkten)
- Zusatzsoftware wird automatisch mit installiert (Windows Movie Maker). Diese muss unter Umständen wieder entfernt werden.

Zu den genannten Problemen gibt es mittlerweile im Internet und Fachzeitschriften eine Vielzahl von Lösungsvorschlägen, über die sich die Administratoren vor dem Aufspielen von SP 2 informieren sollten.

Prüffragen:

- Wird die Konfiguration neuer Einstellungen und der Gruppenrichtlinien im Vorfeld der Windows XP SP2-Installation festgelegt?
- Wird jede neue Konfiguration vor dem Roll-out getestet?

# M 2.330 Regelmäßige Prüfung der Sicherheitsrichtlinien und ihrer Umsetzung bei Windows-Clients ab Windows XP

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Um Verstöße gegen die geltenden Sicherheitsrichtlinien für Clients ab Windows XP feststellen zu können, sind regelmäßige Überprüfungen notwendig. Diese Prüfungen sollten ein fester Bestandteil eines organisatorischen Prozesses sein. Die Ergebnisse der Überprüfungen sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.

Folgende Aspekte sind dabei zu berücksichtigen:

- Die existierenden Sicherheitsrichtlinien müssen auf ihre Aktualität und Konsistenz überprüft werden. Im Laufe der Zeit werden natürlich neue Erkenntnisse über sicherheitsrelevante Aspekte von Windows Betriebssystemen gewonnen. Diese sind bei der Überprüfung der Sicherheitsrichtlinien angemessen zu berücksichtigen. Die Sicherheitsrichtlinien müssen gegebenenfalls angepasst und neu umgesetzt werden.
- Die Sicherheitsrichtlinien von Windows Systemen müssen sorgfältig umgesetzt werden. Auch die Umsetzung ist regelmäßig zu prüfen. Zur Ermittlung aktuell umgesetzter Einstellungen und ihrer etwaigen Unterschiede von den in Sicherheitsrichtlinien definierten Parameterwerten, können automatisierte Tools wie *secedit* oder der *Microsoft Security Compliance Manager* eingesetzt werden (siehe auch M 4.243 *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen*).
- Zugriffsberechtigungen in Dateisystem, Registry und Netzfreigaben müssen auf ihre Konsistenz geprüft werden. Benutzer dürfen nur die benötigten Berechtigungen besitzen.
- Benutzerberechtigungen (Systemberechtigungen) sind ebenfalls zu überprüfen.
- Änderungen, die sich aus der Installation neuer und dem Entfernen alter Software (Windows-Komponenten oder Anwendungssoftware von Drittherstellern) ergeben, sind angemessen zu berücksichtigen. Die dadurch resultierenden Änderungen der Sicherheitseinstellungen (Gruppenrichtlinienobjekte, Zugriffsberechtigungen usw.) sind umzusetzen, wobei für kritische Änderungen eine Sicherheitsanalyse durchzuführen ist.

Des Weiteren ist M 2.10 *Überprüfung des Hard- und Software-Bestandes* bei Überprüfungen zu beachten, um die Nutzung von nicht freigegebener Software fest- und abstellen zu können.

Prüffragen:

- Werden die Sicherheitsrichtlinien und ihre Umsetzung bei Windows-Clients ab Windows XP regelmäßig geprüft?

# M 2.331 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter Organisation
**Verantwortlich für Umsetzung:** Leiter Organisation, Mitarbeiter

Von der geplanten Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen hängt nicht nur die Wahl der Ausstattung, sondern auch die erforderlichen Sicherheitsmaßnahmen ab. Daher sollte zunächst dokumentiert werden, welche Nutzungsarten für welche Räume vorgesehen sind und basierend auf den Anforderungen aus den geplanten Einsatzszenarien die Einrichtung auszuwählen und organisatorische und technische Nutzungsregelungen festzulegen.

Die Lage von Besprechungs-, Veranstaltungs- und Schulungsräumen sollte möglichst so gewählt werden, dass Fremde nicht unnötig durchs Haus laufen müssen, also möglichst nah zu/zum

- Eingang
- Sanitären Einrichtungen
- Kantine

Der Weg zu einem Besprechungs-, Veranstaltungs- und Schulungsraum sollte möglichst nicht in die Nähe von oder gar durch besonders sicherheitsrelevante Bereiche führen. Ebenso sollten Besprechungs-, Veranstaltungs- und Schulungsräume so ausgewählt und eingerichtet sein, dass sie zu möglichst geringen Störungen des normalen Betriebs führen.

Die Wege zu einem Besprechungs-, Veranstaltungs- und Schulungsraum, zu den sanitären Einrichtungen und zur Kantine sollten gut erkennbar markiert sein. Dadurch wird es vermieden, dass sich Personen auf der Suche danach verlaufen. Ebenso entzieht es Personen, die sich absichtlich "versehentlich" verlaufen, die Argumentationsgrundlage.

Es sollte ein Raumbuchungssystem eingesetzt werden, aus dem auch nachträglich ersichtlich ist, wer die Räume genutzt hat. Dadurch können auch Ausweichmöglichkeiten leicht erkannt werden.

Prüffragen:

- Ist dokumentiert, welche Nutzungsarten für welche Räume vorgesehen sind?
- Führt der Weg zu Besprechungs-, Veranstaltungs- und Schulungsräumen möglichst nicht in die Nähe oder gar durch sicherheitsrelevante Bereiche?
- Sind die Wege zu Besprechungs-, Veranstaltungs- und Schulungsräumen, zu den sanitären Einrichtungen und zur Kantine gut erkennbar markiert?
- Existiert ein Raumbuchungssystem, aus dem auch nachträglich ersichtlich ist, wer die Räume genutzt hat?

# M 2.332 Einrichtung von Besprechungs-, Vortrags- und Schulungsräumen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter Organisation
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Leiter Organisation

Besprechungs-, Veranstaltungs- und Schulungsräume sind entweder für einen der genannten Zwecke fest einzurichten oder (bei wechselnder Nutzung) so zu möblieren, dass sie der jeweils aktuellen Nutzung optimal angepasst werden können.

In Schulungsräumen sind die Arbeitsplätze hinsichtlich Zahl und Anordnung der IT-Geräte sowie Platzangebot so zu gestalten, dass gegenseitige Störungen vermieden werden und dass an jedem Platz ausreichend Fläche vorhanden ist, um Unterlagen, Schreibblöcke etc. problemlos handhaben zu können.

Die Besprechungs-, Veranstaltungs- und Schulungsräume müssen geeignet ausgestattet werden. Dazu gehören beispielsweise Kommunikations- und Medienunterstützung wie Beamer oder Flipcharts. Für die Einrichtung sollten unter anderem folgende Aspekte berücksichtigt werden:

- Es sollten sich sinnvollerweise dort Stromanschlüsse befinden, wo Beamer, Laptops oder andere Verbraucher aufgestellt werden sollen. Sie sollten auch in genügender Anzahl für typischerweise mitgebrachte IT-Systeme wie Laptops vorhanden sein. Dies dient auch der Informationssicherheit, da sonst IT-Geräte durch wilde Verkabelung und Unachtsamkeit hinunterfallen oder anderweitig Schaden nehmen können.
- Die Stromversorgung eines Besprechungs-, Veranstaltungs- und Schulungsraums ist aus der letzten Unterverteilung heraus getrennt von anderen Räumen aufzubauen. Dadurch wirken sich Beeinträchtigungen der Energieversorgung nicht auf andere Räume aus. Optimal ist eine eigene Unterverteilung im Besprechungs-, Veranstaltungs- und Schulungsraum. Damit entfällt die Notwendigkeit, nach dem Ansprechen eines Sicherungselements die irgendwo anders im Gebäude befindliche Unterverteilung zu suchen.
- Es sollte mindestens ein Festnetz-Telefonanschluss vorhanden sein, um die Erreichbarkeit auch während Veranstaltungen zu gewährleisten. Dies ist insbesondere wichtig, wenn Mobiltelefone während Veranstaltungen ungenutzt bleiben sollen oder sogar ein Handy-Verbot ausgesprochen wurde. Für interne Verbindungen ist er dauerhaft freizuschalten. Für externe kommende und gehende Verbindungen ist er zum Schutz gegen Missbrauch nur bei Bedarf durch befugte Personen freizuschalten.
- Es muss überlegt werden, ob Netzsteckdosen für den Anschluss ans Internet oder interne Netze eingerichtet werden sollen. Da dies für interne Netze eine Vielzahl von Gefährdungen mit sich bringen kann, müssen solche Netzzugänge entsprechend abgesichert sein (siehe auch M 2.204 *Verhinderung ungesicherter Netzzugänge*). Wenn ein Internet-Zugang erforderlich ist, sollte überlegt werden, diesen nicht über das Intranet, sondern getrennt zu führen.
- Bei der Einrichtung eines WLANs in Besprechungs-, Veranstaltungs- und Schulungsräumen müssen alle erforderlichen Sicherheitsmaßnahmen eingesetzt werden.

Prüffragen:

- Sind Besprechungs-, Veranstaltungs- und Schulungsräume so eingerichtet, dass sie eine optimale und sichere Umgebung für Gespräche mit Externen bieten?
- Befinden sich Stromanschlüsse dort, wo Beamer, Laptops oder andere Verbraucher aufgestellt werden sollen?
- Ist die Stromversorgung eines Besprechungs, Veranstaltungs- und Schulungsraums aus der letzten Unterverteilung heraus getrennt von anderen Räumen aufgebaut?
- Falls Netzsteckdosen in Besprechungs, Veranstaltungs- oder Schulungsräumen für den Anschluss ans Internet oder interne Netze vorhanden sind, sind sie entsprechend abgesichert?
- Falls WLAN in Besprechungs, Veranstaltungs- oder Schulungsräumen vorhanden ist, ist es entsprechend abgesichert?

# M 2.333 Sichere Nutzung von Besprechungs-, Vortrags- und Schulungsräumen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Organisation
**Verantwortlich für Umsetzung:** Benutzer, Leiter Organisation

Für die Nutzung dieser Räume sollte es in jeder Organisation feste Regeln geben. Diese sollte unter anderem Verhaltenshinweise genereller Art für die Benutzer umfassen, aber auch solche zur Benutzung sowohl fest installierter als auch mitgebrachter Geräte.

Dabei sollten unter anderem folgende Aspekte berücksichtigt werden:

- Externe Teilnehmer von Besprechungen oder Schulungen sollten außerhalb der Besprechungs- und Schulungsräume nicht unbeaufsichtigt bleiben (siehe auch M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*).
- Es muss geklärt werden, unter welchen Rahmenbedingungen Externe mitgebrachte IT-Systeme wie Handys oder Laptops einsetzen dürfen.
- Vorhandene Festnetz-Telefonanschlüsse müssen vor Missbrauch geschützt werden, beispielsweise indem die Anwahl externer Nummern nur nach einer Passwort-Eingabe möglich ist.
- Im Raum sollten die Telefonnummern von Ansprechpartnern für Probleme wie IT-Support oder Schlüsselverwaltung ausgehängt oder ausgelegt sein. Die Ansprechpartner müssen jederzeit während der üblichen Bürozeiten erreichbar sein.
- Wenn im Raum ein Beamer und weitere Geräte fest eingerichtet sind, müssen die erforderlichen Sicherheitsmaßnahmen zum Schutz dieser Geräte vor Diebstahl getroffen werden. Beispielsweise können diese mit Diebstahlsicherungen wie Stahlkabeln versehen werden. Auch verschließbare Schränke für Materialen sind sinnvoll.
- Nach Ende jeder Veranstaltung sollte alles Material entfernt werden, das sensitive Informationen enthalten könnte. Daher sollte z. B. benutztes Flipchart-Papier mitgenommen und Tafeln gesäubert werden. Auch im Papierkorb gelandete Entwürfe dürfen nicht vergessen werden.
- In Besprechungs-, Veranstaltungs- und Schulungsräumen sind häufig fest installierte IT-Systeme wie z. B. Schulungsrechner vorhanden. Hierfür ist folgendes zu beachten:
  - Die IT in Besprechungs- und Schulungsräumen muss entsprechend den Erfordernissen konfiguriert und administriert werden (siehe auch M 4.225 *Einsatz eines Protokollierungsservers in einem Sicherheitsgateway*). Es ist festzulegen, wer für die Administration der Schulungsrechner zuständig ist. Außerdem müssen Ansprechpartner für immer wieder gerne auftretende Probleme benannt sein. Diese müssen auch kurzfristig helfen können.
  - In Räumen mit Schulungsrechnern sollte nichts mitgebracht werden dürfen, was die Funktionsfähigkeit der IT-Systeme beeinträchtigen könnte, also weder Getränke noch klebrige Pausenriegel. Das heißt dann auch, dass Kaffeepausen außerhalb des Raumes stattfinden müssen.
- Es muss klare Regelungen für Zugriffe auf LAN- und TK-Schnittstellen aus Besprechungs- und Schulungsräumen geben.

- Außerdem sollten Hinweise auf Fluchtwege und das richtige Verhalten bei Bränden nicht vergessen werden (siehe M 1.6 *Einhaltung von Brandschutzvorschriften*).

Bei aufgetretenen Problemen wie fehlendem Papier für Flipcharts oder defekten Geräten sollten die zuständigen Ansprechpartner informiert werden, damit diese zeitnah behoben werden können.

Bei Besprechungs-, Veranstaltungs- und Schulungsräumen stehen grundsätzlich zwei Lösungen für den Verschluss solcher Räume im Widerspruch. Wird der Raum außer bei Benutzung ständig verschlossen gehalten, ist zwar die darin befindliche IT gut gegen eine Reihe von Gefährdungen geschützt, eine spontane Nutzung des Raumes ist allerdings nicht möglich. Ständig offene Besprechungs-, Veranstaltungs- und Schulungsräume hingegen sind zwar jederzeit nutzbar, zugleich ist aber das Risiko für die IT deutlich höher. Sie abzuschließen hat außerdem den Vorteil, dass die Einrichtung der Schulungsräume sich eher in dem gewünschten Zustand befindet. Aus Sicht der Informationssicherheit sind Besprechungs-, Veranstaltungs- und Schulungsräume also außerhalb der Nutzungszeit verschlossen zu halten. Gleichzeitig ist natürlich sicherzustellen, dass der Zutritt bei Bedarf angemessen rasch und einfach zu realisieren ist. Die Schlüssel für die Besprechungs-, Veranstaltungs- und Schulungsräume sollten von einer zentralen Stelle verwaltet werden (z. B. Pforte oder innerem Dienst).

In Besprechungs-, Veranstaltungs- und Schulungsräume gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

Prüffragen:

- Ist festgelegt, unter welchen Bedingungen Externe mitgebrachte IT-Systeme einsetzen dürfen?
- Sind die in den Räumen vorhandenen Gerätschaften ausreichend gegen Diebstahl gesichert?
- Ist sichergestellt, dass in Besprechungs-, Veranstaltungs- und Schulungsräumen keine sensitiven Informationen zurückgelassen werden?
- Ist festgelegt, wer für die Administration von IT-Systemen zuständig ist, die in Besprechungs-, Veranstaltungs- und Schulungsräumen sind häufig fest installiert sind?
- Sind Regelungen für die Zugriffe auf LAN- und TK-Schnittstellen aus Besprechungs- und Schulungsräumen definiert?
- Werden die Schlüssel für die Besprechungs-, Veranstaltungs- und Schulungsräume von einer zentralen Stelle verwaltet?

# M 2.334 Auswahl eines geeigneten Gebäudes

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Innerer Dienst

Neben der Standortplanung (siehe M 1.16 *Geeignete Standortauswahl*), die das Umfeld eines Gebäudes betrachtet, muss ein Gebäude hinsichtlich seiner inneren Eignung beurteilt werden. Grundsätzlich ist natürlich schon bei der Gebäudeauswahl zu prüfen, ob alle für die spätere Nutzung relevanten Maßnahmen dann auch umgesetzt werden können.

Für einige dieser Maßnahmen können die Voraussetzung nachträglich jedoch nur mit extrem hohem Aufwand oder gar nicht geschaffen werden. Diese Maßnahme soll daher bei der Auswahl eines bestehenden Gebäudes helfen, typischerweise erst später auftretende Probleme im Vorfeld so weit wie möglich zu vermeiden. Sie kann aber auch bei der Planung eines Neubaus hilfreich sein.

Einzelne Aspekte sind je nachdem, ob das Gebäude gekauft oder gemietet wird, unterschiedlich relevant. Aus Sicht der Informationssicherheit ist unter anderem Folgendes hinsichtlich des Zustandes der Bausubstanz zu beachten:

- Ermöglicht die Statik (maximale Deckentraglast, tragende Wände) die Einrichtung von Räumen mit hoher Flächenlast (Serverraum, RZ, USV etc.) dort, wo sie arbeitsökonomisch und aus Sicht der Informationssicherheit sinnvoll anzuordnen wären (siehe auch M 1.13 *Anordnung schützenswerter Gebäudeteile* sowie für ein RZ M 1.47 *Eigener Brandabschnitt*)?
- Lassen sich die vorhandenen oder zusätzlich erforderlichen Erschließungswege (Flure, Treppenhäuser, Aufzüge) so nutzen und einrichten, dass Maßnahmen wie z. B. M 2.17 *Zutrittsregelung und -kontrolle* auch sinnvoll umzusetzen sind?
- Ist es auf Grund der Erschließungswege möglich, Bereiche mit hohen Sicherheitsanforderungen von solchen mit niedrigen zu trennen, so dass z. B. Schulungsräume außerhalb von sensitiven Bereichen wie der Produktentwicklung liegen?
- Lassen sich die vorhandenen oder zusätzlich erforderlichen Erschließungswege (Flure, Treppenhäuser, Aufzüge) jederzeit für den Transport auch größerer IT-Komponenten nutzen? Ist dies nicht gewährleistet, kann der Wiederanlauf nach einem Hardwareschaden unter Umständen stark verzögert werden.
- Gibt es (Bau-)Auflagen (Wegerechte, Denkmalschutz etc.), die einer bedarfsgerechten Nutzung des Gebäudes hinderlich sein können? Besonders auf Wegerechte Dritter ist hier zu achten, da diese mit erforderlichen zutrittsgeschützten Bereichen kollidieren können.
- Ist eine Raumverteilung möglich, so dass die Maßnahmen M 1.8 *Raumbelegung unter Berücksichtigung von Brandlasten* und M 1.51 *Brandlastreduzierung* umgesetzt werden können?
- Lassen sich die Maßnahmen M 1.3 *Angepasste Aufteilung der Stromkreise* und M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen* umsetzen?
- Gibt es einen äußeren Blitzschutz? Wenn ja, hat das Einfluss auf Details der Umsetzung der Maßnahmen M 1.25 *Überspannungsschutz* und M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen*.

Bei Mietobjekten sind zusätzlich folgende Aspekte zu berücksichtigen:

- Erhält der Mieter alle für die geeignete Herrichtung des Gebäudes erforderlichen Rechte? Welche Rechte und Einspruchsmöglichkeiten behält sich der Vermieter vor?
- Müssen Sicherheitseinrichtungen nach Ende des Mietverhältnisses zurückgebaut werden? Es muss in der Planungsphase sichergestellt werden, dass wegen solcher Zusatzkosten nicht auf erforderliche Sicherheitsmaßnahmen verzichtet wird.
- Wenn das Gebäude gleichzeitig von Dritten genutzt wird, ist zu klären, in wie weit dadurch die Umsetzung von Maßnahmen erschwert oder gar verhindert wird.
- Erhält man als Mieter ein Mitspracherecht bei einer späteren Neuvermietung dritt-genutzter Gebäudeteile? Es kann durchaus sein, dass ein neuer Mitnutzer des Gebäudes als sicherheitskritischer angesehen werden muss als der bisherige.
  Beispiel: Die Personalabteilung eines kleinen Schulbuch-Verlages zieht aus und als Nachmieter richtet dort eine politisch oder gesellschaftlich sehr umstrittene Organisation ein Büro ein.

Es sollte dokumentiert werden, welche Sicherheitsanforderungen bei der Gebäudeauswahl betrachtet wurden. Vor allem sollten eventuell vorhandene Sicherheitsrisiken und die ergriffenen Maßnahmen, um diesen vorzubeugen oder Auswirkungen zu reduzieren, festgehalten werden.

Prüffragen:

- Sind für jedes Gebäude die vorhandenen Gefährdungen und die erforderlichen schadensvorbeugenden oder -reduzierenden Maßnahmen dokumentiert?

# M 2.335 Festlegung der Sicherheitsziele und -strategie

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Informationssicherheit ist ein wichtiger Erfolgsfaktor, um die Ziele und Aufgaben eines Unternehmens bzw. einer Behörde erfüllen zu können. Informationssicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess, der auch als solcher in allen Geschäftsprozessen und den Köpfen aller Mitarbeiter verankert werden muss. Der Sicherheitsprozess muss durch die Behörden- bzw. Unternehmensleitung initiiert und etabliert werden. Zunächst müssen angemessene Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt werden. Neben den strategischen Leitaussagen müssen konzeptionelle Vorgaben erarbeitet und die organisatorischen Rahmenbedingungen geschaffen werden, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller Geschäftsprozesse des Unternehmens oder der Behörde zu ermöglichen.

Die Sicherheitsziele sollten zu Beginn jedes Sicherheitsprozesses sorgfältig bestimmt werden. Anderenfalls besteht die Gefahr, dass Sicherheitskonzepte erarbeitet werden, die nicht den Informationssicherheitsanforderungen der Behörde bzw. des Unternehmens entsprechen. Die methodische Planung der Informationssicherheit hilft, die grundlegenden Ziele und Aufgaben eines Unternehmens bzw. einer Behörde zu erreichen. Die Grundlage für die Definition der Sicherheitsziele bilden daher die generellen Ziele der Institution sowie die wesentlichen Geschäftsprozesse und Informationen. Angemessene und erreichbare Sicherheitsziele sind Voraussetzung für alle weiteren Schritte im Sicherheitsprozess. Die Ziele müssen realistisch, praxisorientiert, überzeugend und verständlich sein. Hieraus lässt sich dann im Rahmen der Sicherheitskonzeption ableiten, welchen Schutzbedarf die einzelnen Informationen, Geschäftsprozesse, Anwendungen, IT-Komponenten und Netze haben und welche Sicherheitsmaßnahmen daher umzusetzen sind.

Bei der Umsetzung von Sicherheitsmaßnahmen muss in der Regel immer ein Kompromiss zwischen Kosten und Aufwand gefunden werden. Es sollte daher transparent sein, welche Informationen und Geschäftsprozesse zur Aufgabenerfüllung beitragen und welcher Wert diesen beigemessen wird, um daraus angemessene Sicherheitsziele zu formulieren.

Die Sicherheitsziele müssen von der Unternehmens- oder Behördenleitung getragen und verantwortet werden. Sie sollten vom Informationssicherheitsmanagement-Team unter Beteiligung der Leitungsebene erarbeitet und dokumentiert werden. Je nach Organisationsstruktur ist es ratsam, die Leiter von größeren Geschäftsbereichen (z. B. Abteilungsleiter oder Bereichsleiter) in die Beratungen einzubeziehen.

Eine detaillierte Beschreibung, wie und in welcher Beschreibungstiefe Sicherheitsstrategie und -ziele festgehalten werden sollten, findet sich im BSI-Standard 100-2 *Vorgehensweise nach IT-Grundschutz*.

Sicherheitsziele und -strategie sollten regelmäßig daraufhin beleuchtet werden, ob sie noch aktuell und angemessen sind. Insbesondere bei Änderungen von Rahmenbedingungen, von Geschäftsprozessen oder des IT-Umfel-

des müssen die Sicherheitsziele und -strategie überprüft und eventuell angepasst werden.

Der Sicherheitsprozess kann nur dann langfristig erfolgreich sein, wenn die Wirksamkeit und Effizienz der Sicherheitsstrategie regelmäßig von der Leitungsebene überprüft wird. Die daraus resultierenden Verbesserungen gehen in die Anpassung des Sicherheitsprozesses ein.

Prüffragen:

- Sind die Sicherheitsstrategie und -ziele von der Behörden- bzw. Unternehmensleitung unterschrieben und werden von ihr getragen und verantwortet?
- Sind Sicherheitsziele und -strategie aktuell und angemessen?
- Ist ein adäquater Sicherheitsprozess etabliert?

# M 2.336 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung

Die Führung und Lenkung eines Unternehmens oder einer Behörde und die damit verbundenen Leitungsaufgaben beinhalten eine hohe Verantwortung. Diese Verantwortung bezieht sich nicht nur auf den Grad der Zielerreichung wie beispielsweise den Geschäftserfolg, sondern auch auf die Früherkennung und Minimierung von möglichen Risiken für den Betrieb. Dazu gehören neben anderen Risiken auch solche, die aus unzureichender Informationssicherheit entstehen.

Es ist eine komplexe Aufgabe, dauerhaft ein angemessenes Sicherheitsniveau zu gewährleisten. Dies erfordert ein systematisches Vorgehen, einen kontinuierlichen und zielgerichteten Sicherheitsprozess. Es ist Aufgabe der Leitungsebene jeder Institution, diesen Prozess zu initiieren, zu steuern und zu kontrollieren. Bei kleineren Institutionen wird dies häufig durch ein Mitglied der Leitungsebene persönlich übernommen. In mittleren und großen Institutionen wird die Aufgabe "Informationssicherheit" an eine dedizierte Person, den IT-Sicherheitsbeauftragten, delegiert. Je nach Größe und Art der Institution werden noch weitere Personen mit Sicherheitsaufgaben betraut, die diese ausschließlich oder zusätzlich zu anderen Aufgaben wahrnehmen. Hierfür ist es sinnvoll, eine geeignete Organisationsstruktur aufzubauen, um die verschiedenen Teilaufgaben im Bereich Sicherheit adäquat zu steuern. Dabei verbleibt die Gesamtverantwortung immer bei der Leitungsebene, unabhängig davon, an wie viele Personen Sicherheitsaufgaben delegiert wurden.

Die Geschäftsführung sollte regelmäßig über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufgeklärt werden. Dazu ist es empfehlenswert, die Leitungsebene auf folgende Punkte aufmerksam zu machen (siehe auch M 3.44 *Sensibilisierung des Managements für Informationssicherheit*):

- Darstellung der Sicherheitsrisiken und der damit verbundenen Auswirkungen und Kosten
- Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse
- Gesetzliche und vertragliche Sicherheitsanforderungen
- Übersicht über Standard-Vorgehensweisen zur Informationssicherheit für die Branche

Auch wenn die Leitungsebene für die Erreichung der Sicherheitsziele verantwortlich ist, muss der Sicherheitsprozess von allen Beschäftigten in einer Institution mitgetragen und mitgestaltet werden. Daher sollten folgende Prinzipien eingehalten werden:

- **Übernahme der Gesamtverantwortung für Informationssicherheit**
  Die Initiative für Informationssicherheit geht von der Behörden- bzw. Unternehmensleitung aus. Die Aufgabe "Informationssicherheit" wird durch die Behörden- bzw. Unternehmensleitung aktiv unterstützt.
- **Informationssicherheit integrieren**

Informationssicherheit muss in alle Prozesse und Projekte integriert werden. Darüber hinaus müssen alle Beteiligten über den Sicherheitsprozess ausreichend informiert und motiviert werden, damit sie diesen auch einhalten.

- **Zuständigkeiten definieren**
  Die Behörden- bzw. Unternehmensleitung benennt die für Informationssicherheit zuständigen Mitarbeiter und stattet sie mit den erforderlichen Kompetenzen und Ressourcen aus.
- **Lenken und Überwachen**
  Die Leitungsebene muss aktiv den Sicherheitsprozess initiieren, lenken und überwachen. Dazu muss das Management die Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit kennen, Sicherheitsziele vorgeben und Rahmenbedingungen schaffen, die es ermöglichen, diese Ziele zu erreichen.
- **Angemessene Ziele setzen**
  Absolute Informationssicherheit gibt es nicht. Deswegen ist es wichtig, die Sicherheitsziele so zu setzen, dass sie einerseits mit einem vertretbaren Aufwand (Personal, Zeit, Finanzmittel) erreichbar sind und andererseits die Sicherheitsrisiken auf ein akzeptables Maß reduziert werden.
- **Vorbildfunktion**
  Die Leitungsebene übernimmt auch im Bereich Informationssicherheit eine Vorbildfunktion. Dazu gehört unter anderem, dass auch die Leitungsebene alle vorgegebenen Sicherheitsregeln beachtet.
- **Kontinuierliche Verbesserung**
  Die Angemessenheit und Wirksamkeit aller Elemente des Sicherheitsmanagements muss ständig überprüft werden. Identifizierte Schwachstellen und Verbesserungsmöglichkeiten müssen konsequent behoben bzw. umgesetzt werden. Wichtig ist auch, zukünftige Entwicklungen, veränderte Rahmenbedingungen und potentielle Gefährdungen frühzeitig zu erkennen.
- **Kommunikation und Wissen**
  Die Leitungsebene und das IS-Management-Team müssen die Mitarbeiter motivieren und für ausreichende Schulungs- und Sensibilisierungsmaßnahmen sorgen. Mitarbeiter müssen vor allem über Sinn und Zweck sowohl von technischen Sicherheitsmaßnahmen als auch von organisatorischen Vorgaben aufgeklärt werden. Anwender sollten in die Umsetzungsplanung von Maßnahmen mit einbezogen werden. Damit können sie Ideen einbringen und die Praxistauglichkeit von Sicherheitsmaßnahmen beurteilen.

Prüffragen:

- Hat die Behörden- bzw. Unternehmensleitung deutlich sichtbar die Verantwortung für Informationssicherheit übernommen?
- Lässt sich die Leitungsebene regelmäßig über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen beraten?
- Hat die Behörden- bzw. Unternehmensleitung Sicherheitsverantwortliche benannt?
- Wird Informationssicherheit von der Leitungsebene vorgelebt?

# M 2.337 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Informationssicherheit muss in alle Geschäftsprozesse integriert werden. Es muss dabei gewährleistet sein, dass nicht nur bei neuen Projekten, sondern auch bei laufenden Anwendungen alle erforderlichen Sicherheitsaspekte berücksichtigt werden.

Vor allem in größeren Institutionen existiert häufig bereits ein übergreifendes Risikomanagementsystem. Dabei sind operationelle Risiken inklusive der IT-Risiken integraler Bestandteil des Risikomanagements. Informationssicherheit ist ebenso eine grundlegende und prozessübergreifende Anforderung an Institutionen. Daher sollten die Methoden zum Management von Risiken aus dem Bereich der Informationssicherheit mit den bereits etablierten Methoden zum Risikomanagement abgestimmt werden. Wichtig ist, dass Arbeitsanweisungen oder Dienstvereinbarungen aus unterschiedlichen Bereichen einer Institution sich nicht widersprechen dürfen.

Der BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise sowie die Bausteine der IT-Grundschutz-Kataloge enthalten ausführliche und konkrete Maßnahmenempfehlungen zur Organisation des Sicherheitsprozesses. Im Folgenden werden daher nur beispielhaft wichtige übergreifende Sicherheitsmaßnahmen kurz genannt:

**Definition von Zuständigkeiten (Funktionstrennung)**

Zuständigkeiten und Kompetenzen innerhalb der Informationssicherheitsorganisation (oder kurz IS-Organisation) müssen klar definiert und zugewiesen werden. Für alle wichtigen Funktionen sind zudem Vertretungsregelungen sicherzustellen.

**Festlegung von Kommunikationswegen**

Kommunikationswege müssen geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es muss für alle Aufgaben und Rollen festgelegt sein, wer wen informiert, wer bei welchen Aktionen informiert werden und in welchen Umfang dies geschehen muss.

**Zuweisung der Verantwortung für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme**

Für alle wesentlichen Geschäftsprozesse, Informationen, IT-Systeme und Anwendungen, aber auch für Gebäude und Räume müssen verantwortliche Personen benannt werden. Je nach Bereich und Sprachgebrauch werden diese verantwortlichen Personen z. B. als Informationseigentümer, Geschäftsprozessverantwortliche oder Fachverantwortliche bezeichnet. Die Fachverantwortlichen müssen die Erarbeitung und Umsetzung der Sicherheitsstrategie unterstützen. Die Maßnahme M 2.225 *Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten* gibt weitere Hinweise.

**Integration der Mitarbeiter in den Sicherheitsprozess**

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und qualitätsbewusstes Handeln mithelfen, Schäden zu vermeiden, und zum Erfolg beitragen. Dies betrifft nicht nur die festangestellten Mitarbeiter, sondern alle, die innerhalb der Institution beschäftigt sind, also beispielsweise auch Pförtner und Praktikanten.

Ebenso sollten auch Personen einbezogen werden, die von außerhalb auf Geschäftsprozesse, Anwendungen oder IT-Systeme zugreifen, also z. B. mobile Mitarbeiter. Wichtige Sicherheitsmaßnahmen, die beim Personalmanagement zu beachten sind, also beginnend bei der Personalauswahl und Einstellung bis hin zum Wechsel in andere Bereiche oder dem Weggang aus der Institution, sind im Baustein B 1.2 *Personal* beschrieben.

Darüber hinaus müssen alle Mitarbeiter innerhalb ihres Aufgabenbereiches in die erforderlichen Sicherheitsmaßnahmen eingewiesen werden. Sie sollten regelmäßig für Sicherheitsaspekte sensibilisiert werden, um das Bewusstsein für Risiken und Schutzvorkehrungen im alltäglichen Umgang mit Informationen zu schärfen. Auch das Management muss in das Sensibilisierungskonzept einbezogen werden. Vertiefende Ausführungen hierzu finden sich im Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit*.

**Einbindung externer Dienstleister in den Sicherheitsprozess**

Das Sicherheitsmanagement sollte einen Überblick besitzen über alle Arten von Dienstleistern, die Aufgaben für die Institution wahrnehmen. Dies können Dienstleistungen sein, die unmittelbar die Verarbeitung geschäftsrelevanter Informationen betreffen, wie der Betrieb eines Rechenzentrums, aber auch allgemeine Unterstützungsdienstleistungen wie Wachdienst. Hierbei spielt es keine Rolle, an welchem Standort die Dienstleistung erbracht wird (Institution oder Dienstleister).

Das Sicherheitsmanagement sollte für jeden Dienstleister einschätzen, ob dessen Tätigkeit sicherheitsrelevante Auswirkungen haben kann und welche Sicherheitsvorkehrungen in diesem Rahmen zu treffen sind. Werden IT-Systeme, Anwendungen oder Geschäftsprozesse zu einem externen Dienstleister ausgelagert, ist der Baustein B 1.11 *Outsourcing* anzuwenden. In die Sicherheitskonzeption müssen außerdem auch Mitarbeiter von Dienstleistern einbezogen werden, die über längere Zeit in den Räumlichkeiten der Institution Aufgaben wahrnehmen.

**Einbeziehung von Sicherheitsaspekten in alle Geschäftsprozesse**

Das Management muss einen Überblick über die geschäftskritischen Informationen, Fachaufgaben und Geschäftsprozesse haben. Die zuständigen Fachverantwortlichen und das Informationssicherheitsmanagement-Team müssen konkrete Regeln zum Umgang mit den relevanten Sicherheitsaspekten aufstellen (z. B. Schutzmaßnahmen, Klassifizierung und Kennzeichnung von Informationen).

**Rechte und Berechtigungen**

Zum Schutz der Werte müssen der Zutritt zu Räumen, der Zugang zu IT-Systemen und Anwendungen sowie der Zugriff auf Informationen geregelt werden. Nähere Informationen finden sich z. B. in den Maßnahmen M 2.6 *Vergabe von Zutrittsberechtigungen*, M 2.7 *Vergabe von Zugangsberechtigungen*,

M 2.8 *Vergabe von Zugriffsrechten* und M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*.

**Änderungsmanagement**

Änderungsmanagement beschäftigt sich mit der Planung von Änderungen an Hard- und Software sowie Prozessen. Es muss durch organisatorische Vorgaben sichergestellt werden, dass dabei Aspekte der Informationssicherheit berücksichtigt werden. Näheres findet sich z. B. in der Maßnahme M 2.221 *Änderungsmanagement*.

**Konfigurationsmanagement**

Konfigurationsmanagement umfasst alle Maßnahmen und Strukturen, die erforderlich sind, um den Zustand der betrachteten Objekte zu überwachen, beginnend von der Identifikation, über die Bestandsführung und Aktualisierung bis hin zur Außerbetriebnahme.

Betrachtete Objekte (Konfigurationselemente) können dabei ganze Infrastrukturbereiche, konkrete Anwendungen und IT-Systeme, aber auch einzelne Komponenten davon (beispielsweise Dokumentationen) sein.

Im Rahmen des Konfigurationsmanagements müssen Prozesse und Regelungen eingeführt werden, die beschreiben, wie Informationen über die Eigenschaften der eingesetzten Konfigurationselemente sowie Informationen über sicherheitsrelevante Störungen, Probleme und Änderungen im Zusammenhang mit Konfigurationselementen verwaltet werden. Typische Tätigkeiten sind beispielsweise die Aktualisierung der Liste der IT-Systeme oder die Anpassung von sicherheitsrelevanten Dokumentationen nach Änderungen von Geschäftsprozessen oder Anwendungen. Empfehlungen zum Konfigurationsmanagement finden sich in Baustein B 1.9 *Hard- und Software-Management*.

Prüffragen:

- Wird der IT-Sicherheitsbeauftragte bzw. das Informationssicherheitsmanagement-Team an sicherheitsrelevanten Entscheidungen ausreichend beteiligt?
- Ist geregelt, dass das Sicherheitsmanagement in alle Prozesse und Entwicklungen eingebunden ist, die für die Informationssicherheit relevant sind?
- Sind Zuständigkeiten und Kompetenzen innerhalb der Organisationsstrukturen für Informationssicherheit klar definiert und zugewiesen?
- Gibt es für alle wichtigen Funktionen der IS-Organisation wirksame Vertretungsregelungen?

# M 2.338 Erstellung von zielgruppengerechten Sicherheitsrichtlinien

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

### Zielgruppengerechte Vermittlung von Sicherheitsthemen

Ein wichtiger Erfolgsfaktor für die Erreichung eines angemessenen Sicherheitsniveaus sind verantwortungsbewusste und kompetente Mitarbeiter, die koordiniert zusammenarbeiten. Dabei bringen Management, IT-Benutzer, Administratoren und Sicherheitsexperten sehr individuelle fachliche Voraussetzungen mit und nehmen unterschiedliche Aufgaben wahr. Während die Unternehmens- bzw. Behördenleitung die Gesamtverantwortung trägt, Ziele vorgibt und Rahmenbedingungen definiert, müssen Administratoren technisch hochqualifiziert sein und Detailwissen besitzen, um Systeme bedienen und sicher konfigurieren zu können.

Sicherheitsverantwortliche sind mit den IT-Grundschutz-Katalogen in der Lage, ein ganzheitliches Sicherheitskonzept zu erstellen. Dieses wird oftmals viele Seiten umfassen, wenn alle Bereiche der Informationssicherheit damit abgedeckt werden sollen. Die zielgruppengerechte Aufbereitung und Vermittlung der Inhalte des Sicherheitskonzepts ist eine wichtige Aufgabe des Sicherheitsmanagements. Das Ziel ist, dass alle Mitarbeiter die sie und ihren Arbeitsbereich betreffenden Sicherheitsaspekte kennen und beachten.

Es empfiehlt sich daher, unterschiedliche Sicherheitsrichtlinien oder ausführliche Teilkonzepte zu erstellen, die einzelne Sicherheitsthemen bedarfsgerecht darstellen. Damit erhalten Mitarbeiter genau die Informationen, die sie zu einem bestimmten Thema wirklich benötigen.

Separate Sicherheitsrichtlinien für IT-Systeme oder Dienstleistungen, die sich in einem sicherheitskritischen Bereich befinden, deren Konfiguration kompliziert ist oder deren Anwendung komplex ist, können technische Anweisungen für Administratoren enthalten, die nicht allgemein verständlich sind. In den Dokumenten für die Mitarbeiter sollten Sicherheitsthemen dagegen angemessen aufbereitet und nicht mit unnötigen Details versehen sein.

### Hierarchischer Aufbau von Richtlinien

Bei der Formulierung von Richtlinien hat es sich bewährt, auf verschiedenen Ebenen zu arbeiten.

Zunächst sollten in der ersten Ebene kurz und prägnant die allgemeinen Sicherheitsziele und die Sicherheitsstrategie in einer Leitlinie zur Informationssicherheit formuliert werden (siehe M 2.192 *Erstellung einer Leitlinie zur Informationssicherheit*). Die Strategie enthält keine technischen Details und wird vom Management verabschiedet. In der nächsten Ebene sollten hieraus grundlegende technische Sicherheitsanforderungen abgeleitet werden.

Zur allgemeinen Sicherheitskonzeption gehören Dokumente, die verschiedene Aspekte der Informationssicherheit beschreiben (z. B. eine Richtlinie zur Internetnutzung oder ein Virenschutzkonzept), ohne auf konkrete Produkte einzugehen.

In der dritten Ebene werden technische Details, konkrete Maßnahmen und produktspezifische Einstellungen beschrieben. Sie enthält viele Dokumente, die regelmäßig geändert und typischerweise nur von den zuständigen Experten gelesen werden.

Die nachstehende Abbildung stellt den hier beschriebenen Aufbau graphisch dar.


Abbildung: Hierarchischer Aufbau von Richtlinien

**Inhalt von speziellen Sicherheitsrichtlinien**

Folgende Themen eignen sich beispielsweise zur zielgruppengerechten Aufbereitung in spezielle Sicherheitsrichtlinien:

- Verhaltensregeln und Sicherheitshinweise für IT-Benutzer
- Verhaltensregeln und Sicherheitshinweise für Administratoren
- Sicherheitsgateways (siehe auch M 2.70 *Entwicklung eines Konzepts für Sicherheitsgateways*)
- Virenschutz (siehe auch M 2.154 *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme*)
- Notfallvorsorge (siehe auch M 6.3 *Erstellung eines Notfall-Handbuches*)
- Datensicherung (siehe auch M 6.33 *Entwicklung eines Datensicherungskonzepts*)
- Archivierung (siehe auch M 2.243 *Entwicklung des Archivierungskonzepts*)
- Einsatz von Groupware (siehe M 2.455 *Festlegung einer Sicherheitsrichtlinie für Groupware*)
- Outsourcing (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*)

**Sicherheitsrichtlinie zur IT-Nutzung**

Oft empfiehlt es sich, die allgemeinen Zielvorgaben der Leitlinie zur Informationssicherheit in einer Sicherheitsrichtlinie zur IT-Nutzung zu konkretisieren und die wichtigsten organisationsweiten Maßnahmen des Sicherheitskonzeptes allgemeinverständlich, ohne technische Details, in einer Richtlinie zusammenzufassen. Diese Richtlinie beschreibt die Grundzüge der organisationsweiten IT-Nutzung und führt die Mitarbeiter durch das Sicherheitskonzept.

Folgende Themen könnten in einer allgemeinen Sicherheitsrichtlinie zur IT-Nutzung behandelt werden:

- Umgang mit schützenswerten Informationen (Festlegung von Informationseigentümern, Pflicht zur Klassifizierung von Informationen nach Schutzbedürftigkeit)
- relevante Gesetze und Vorgaben
- Kurzbeschreibung wichtiger Rollen (z. B. IT-Sicherheitsbeauftragter, Administrator, Benutzer)
- Ausbildung des Personals

- Pflicht zur Einrichtung von Vertretungsregelungen
- Anforderungen an die Verwaltung von IT (Beschaffung, Einsatz, Wartung, Revision und Entsorgung)
- grundlegende Sicherheitsmaßnahmen (Zutritt zu Räumen und Zugang zu IT-Systemen, Verschlüsselung, Virenschutz, Datensicherung, Notfallvorsorge)
- Regelungen für spezifische IT-Dienste (Datenübertragung, Internetnutzung)

Das BSI stellt auf seinen Webseiten im Bereich IT-Grundschutz verschiedene Musterrichtlinien und -konzepte als Beispiele zur Verfügung.

Prüffragen:

- Sind Sicherheitsrichtlinien zielgruppenorientiert erstellt, indem sie bedarfsgerecht die relevanten Sicherheitsthemen darstellen?

# M 2.339 Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Damit die gesteckten Sicherheitsziele erreicht werden können, müssen dafür angemessene Ressourcen bereitgestellt werden.

**Bereitstellung von Ressourcen für Informationssicherheit**

Informationssicherheit erfordert ausreichende finanzielle und personelle Ressourcen sowie eine geeignete Ausstattung. Diese müssen dem Informationssicherheitsmanagement-Team von der Behörden- bzw. Unternehmensleitung in angemessenem Umfang bereitgestellt werden.

Es ist zu empfehlen, dass das IS-Management-Team anhand der Sicherheitsziele die für die Umsetzung aller identifizierten Maßnahmen benötigten Ressourcen aufzeigt. Dies dient einerseits als Grundlage für Management-Entscheidungen über die Zuteilung der Ressourcen und andererseits zur Festlegung der Projektpläne und der Umsetzungszeiträume.

**Zugriff auf externe Ressourcen**

Die internen Sicherheitsexperten sind häufig mit ihren Routinetätigkeiten so ausgelastet, dass sie bei neuen Aufgaben oder Entwicklungen nicht alle sicherheitsrelevanten Einflussfaktoren analysieren oder Sicherheitslösungen umsetzen können. Hierzu gehören beispielsweise geänderte gesetzliche Anforderungen, die Einführung neuer IT-Systeme sowie die Verfolgung der aktuellen technischen Entwicklungen. Um Arbeitsspitzen bewältigen zu können, müssen entweder intern zusätzliche Mitarbeiter eingesetzt oder auf externe Experten zurückgegriffen werden. Der Bedarf muss von den internen Sicherheitsexperten kommuniziert werden, damit die Leitungsebene die erforderlichen Ressourcen bereit stellt.

Es ist sicherzustellen, dass alle erforderlichen Sicherheitsmaßnahmen umgesetzt werden, sei es durch den Rückgriff auf externe oder interne Kräfte.

**Ressourcen für den IT-Sicherheitsbeauftragten**

Ohne eine funktionierende Organisationsstruktur für Informationssicherheit nützen die teuersten technischen Lösungen nichts. Die Erfahrung zeigt, dass die Berufung eines IT-Sicherheitsbeauftragten die effektivste Sicherheitsmaßnahme ist. Nach der Bestellung eines Sicherheitsbeauftragten geht in den meisten Institutionen die Anzahl an Sicherheitsvorfällen signifikant zurück. Damit der IT-Sicherheitsbeauftragte eine tatsächliche Verbesserung des Sicherheitsniveaus erreichen kann, muss er

- ausreichend Zeit für seine Arbeit haben,
- ausreichend in alle Geschäftsprozesse, Fachaufgaben und Projekte integriert sein,
- genügenden Zugriff auf alle erforderlichen Ressourcen haben.

In kleineren Institutionen ist es möglich, dass ein Mitarbeiter die Aufgaben des IT-Sicherheitsbeauftragten in Personalunion neben seinen eigentlichen Tätigkeiten wahrnimmt.

**Ressourcen für das Informationssicherheitsmanagement-Team**

Ein IS-Management-Team sollte immer dann eingerichtet werden, wenn der IT-Sicherheitsbeauftragte alleine nicht mehr alle Geschäftsprozesse und Projekte betreuen kann, also die Institution eine gewisse Größenordnung überschritten hat.

Die erstmalige Einrichtung des Sicherheitsprozesses ist meist mit einem erhöhten Aufwand verbunden. Häufig ist es deshalb zweckmäßig, dem IS-Management-Team für diese Phase zusätzliche personelle Ressourcen zur Verfügung zu stellen.

**Bereitstellung von Ressourcen für den IT-Betrieb**

Grundvoraussetzung für einen sicheren IT-Betrieb ist, dass dieser reibungslos funktioniert, also vernünftig geplant und organisiert ist. Für den IT-Betrieb müssen ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des IT-Betriebs (knappes Budget, überlastete Administratoren und eine unstrukturierte oder schlecht gewartete IT-Landschaft) müssen in der Regel gelöst werden, damit die eigentlichen Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können. Ob die bereitgestellten Ressourcen ausreichen, zeigt sich beispielsweise daran, ob die IT-Benutzer angemessen betreut werden oder ob alle Hard- und Software wie vorgesehen getestet wird.

**Wirtschaftlichkeitsaspekte in der Sicherheitsstrategie**

Die Sicherheitsstrategie sollte von Beginn an auch Wirtschaftlichkeitsaspekte berücksichtigen. Bei der Auswahl der umzusetzenden Sicherheitsmaßnahmen sollten die zur Verfügung stehenden Ressourcen berücksichtigt werden. Wenn für bestimmte Maßnahmen keine ausreichende technische oder personelle Unterstützung vorhanden ist, muss die Strategie geändert werden. In vielen Fällen lassen sich andere Maßnahmen finden, die zu einem ähnlichen Sicherheitsniveau führen. Wenn aber die formulierten Sicherheitsziele und die vorhandenen finanziellen, technischen oder personellen Möglichkeiten zu weit auseinander liegen, müssen sowohl die Sicherheitsziele als auch die Geschäftsprozesse grundsätzlich überdacht werden. In diesem Fall muss auch die Leitungsebene über diese Diskrepanz informiert werden, damit sie gegebenenfalls Korrekturmaßnahmen veranlassen kann.

Bei der Festlegung von Sicherheitsmaßnahmen sollten immer die für die Umsetzung benötigten personellen und finanziellen Ressourcen konkret genannt werden. Hierzu gehört die Benennung von Verantwortlichen und anderen Ansprechpartnern, aber auch die Festlegung genauer Terminpläne und der zu beschaffenden Materialien. Es empfiehlt sich außerdem, bei allen geplanten Sicherheitsmaßnahmen zu dokumentieren, ob die für Informationssicherheit eingeplanten Ressourcen termingerecht bereitgestellt wurden und was die Gründe für Projektabweichungen waren. Nur so lassen sich nachhaltige Verbesserungen erreichen und Störungen vermeiden.

**Ressourcen für die Überprüfung der Informationssicherheit**

Alle Sicherheitsmaßnahmen müssen regelmäßig auf ihre Wirksamkeit und Eignung geprüft werden. Auch hierfür müssen ausreichende Ressourcen bereitgestellt werden. Generell sollten nicht diejenigen, die Sicherheitsmaßnah-

men konzipiert haben, deren Wirksamkeit und Eignung prüfen. Hierfür kann auch externer Sachverstand hinzugezogen werden, um Betriebsblindheit zu vermeiden.

Die Frage, ob ausreichende Ressourcen für Informationssicherheit bereitgestellt werden, ist wesentlich schwieriger zu beantworten als die Überprüfung von rein technischen Aspekten.

Prüffragen:

- Sind die finanziellen und personellen Ressourcen für die Informationssicherheit angemessen?
- Wurden bei der Festlegung von Sicherheitsmaßnahmen die für die Umsetzung erforderlichen Ressourcen beziffert?
- Wurden für Informationssicherheit eingeplante Ressourcen tatsächlich termingerecht bereitgestellt?
- Haben der IT-Sicherheitsbeauftragte bzw. das Informationssicherheitsmanagement-Team genügend Zeit für ihre Sicherheitsaufgaben?
- Gibt es ausreichend Ressourcen für einen ordnungsmäßigen IT-Betrieb?

# M 2.340 Beachtung rechtlicher Rahmenbedingungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Leiter Organisation, Vorgesetzte

Bei der Verarbeitung von Informationen sind eine Vielzahl von gesetzlichen oder vertraglichen Rahmenbedingungen zu beachten. Diese variieren sehr stark in Abhängigkeit von der Art der Institution, der Branche und den Geschäftsprozessen.

Typische Bereiche der Informationsverarbeitung, die besonderen gesetzlichen Regelungen unterliegen, sind:

- Schutz personenbezogener Daten,
- Einsatz von kryptographischen Verfahren,
- Schutz von geistigem Eigentum,
- ordnungsgemäßer Betrieb von IT-Systemen.

Abhängig von dem Land, in dem die Informationen verarbeitet werden und ihrem speziellen Einsatzzweck können noch eine Vielzahl von weiteren rechtlichen Regelungen existieren. Diese einzeln zu nennen, würde den Rahmen der IT-Grundschutz-Kataloge sprengen. In diversen Bereichen des IT-Grundschutzes werden länder- oder branchenspezifische Gesetze angesprochen, wie z. B. zu Kryptographie, Outsourcing oder Archivierung. Dies sind aufgrund der Vielzahl möglicher gesetzlicher Rahmenbedingungen jeweils nur Beispiele ohne Anspruch auf Vollständigkeit oder Aktualität.

Alle für die Geschäftsprozesse und Informationsverarbeitung, den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben müssen identifiziert und dokumentiert werden. Es ist dabei zu beachten, dass gesetzliche Vorschriften sich häufig auf Landes- und Regionalebene unterscheiden. Als Konsequenz müssen für jede Lokation jeweils die dort gültigen Gesetze eingehalten werden. Ebenso ist zu berücksichtigen, dass je nach Art der Geschäftsprozesse und dem Einsatzzweck der IT-Systeme (z. B. Büroumgebung, Prozesssteuerung) verschiedene Vorschriften gelten können.

Insbesondere müssen

- alle angewandten betrieblichen Praktiken und Vorgehensweisen,
- alle im Rahmen der geschäftlichen Tätigkeiten verarbeiteten Informationen,
- alle installierten IT-Systeme (Hardware- und Software) sowie
- die zum Betrieb der Geschäftsprozesse und IT-Systeme notwendige physikalische Infrastruktur

die gültigen gesetzlichen Vorschriften erfüllen. Alle Änderungen gesetzlicher Auflagen müssen erfasst und die für die Institution relevante Änderungen berücksichtigt werden.

Führungskräfte, welche die rechtliche Verantwortung für die Institution vor Ort tragen, müssen für die Identifizierung und Dokumentation der anzuwendenden gesetzlichen Vorschriften sorgen. Hiermit sollte ein Jurist oder Rechtsexperte beauftragt werden. Falls innerhalb der Institution das erforderliche Wissen oder die nötigen Ressourcen nicht zur Verfügung stehen, sollte externe Rechtsberatung eingeholt werden. Da nicht alle Mitarbeiter sämtliche Gesetze und Regelungen kennen müssen, sollten dabei die für die einzelnen Be-

reiche der Institution relevanten gesetzlichen und vertraglichen Vorgaben herausgearbeitet werden. Um deren Einhaltung zu überwachen, können in den einzelnen Bereichen Verantwortliche benannt werden. So ist der betriebliche Datenschutzbeauftragte dafür verantwortlich, auf die Einhaltung der gültigen Datenschutzvorschriften sowie für die Erstellung und Einhaltung eines institutionsweit gültigen Regelwerks zum Schutz personenbezogener Daten hinzuwirken. Die IT-Leitung muss für die Definition und Dokumentation des Lizenzmanagements sorgen.

Natürlich ist auch jeder einzelne Mitarbeiter und insbesondere das Führungspersonal für die Umsetzung der Regelungen zu rechtlichen Aspekten und für die Überwachung der Einhaltung verantwortlich (siehe auch M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Prüffragen:

- Gibt es ein Dokument mit dem Überblick über alle für die Institution relevanten rechtlichen Vorgaben?
- Sind die Verantwortlichkeiten und Zuständigkeiten für die Einhaltung rechtlicher Vorgaben definiert?

# M 2.341 Planung des SAP Einsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Vor der Installation und Inbetriebnahme eines SAP Systems müssen umfangreiche Planungen erfolgen. Eine sorgfältige Planung ist nicht nur unter Sicherheitsgesichtspunkten notwendig. Auch die Geschäftsprozesse und -abläufe, die durch das SAP System automatisiert und unterstützt werden sollen, müssen vollständig, korrekt und im notwendigen Detailgrad erfasst werden. Nur so ist eine erfolgreiche Umsetzung innerhalb eines SAP Systems möglich. Selbst eine Planungsphase von mehreren Monaten kann für große Systeme bei Neuplanung knapp bemessen sein.

Schon in der Konzeptionsphase sollten der Datenschutzbeauftragte und der Personal- oder Betriebsrat beteiligt werden. Zum einen werden mit SAP-Systemen in der Regel auch immer personenbezogene Daten verarbeitet, z. B. mit dem Modul HR oder im Rahmen der Protokollierung (siehe unten). Zum anderen sollte die notwendige Umstellung von Geschäftsprozessen und Arbeitsabläufen begleitet werden.

Planungen sind für jedes SAP System individuell durchzuführen, da sich jedes SAP System im Einsatzszenario unterscheidet. Auch für das Test- und Abnahme-System und das Entwicklungs-System, die einem Produktiv-System zugeordnet sind, sollte aufgrund der unterschiedlichen Verwendungszwecke eine individuelle Planung erfolgen. Es ist dabei zu beachten, dass jeweils auch die Abhängigkeiten zwischen SAP Systemen berücksichtigt werden müssen. Dies gilt besonders für die verschiedenen Ausprägungen (Entwicklung, Test und Abnahme, Produktion) eines SAP Systems, aber auch für unterschiedliche SAP Systeme in einem Verbund. Insofern muss eine auf die Zusammenarbeit der individuellen Systeme abgestimmte Gesamtplanung erfolgen.

Im Folgenden ist eine Liste von SAP Sicherheitsteilkonzepten angegeben, die im Hinblick auf die Sicherheit eines SAP Systems in der Planungsphase zu erstellen sind und die auch kontinuierlich gepflegt werden müssen. Die Liste ist nicht vollständig und muss auf die lokalen Gegebenheiten und Anforderungen angepasst werden, mindestens erforderlich sind aber die folgenden SAP Sicherheitsteilkonzepte:

- Planung der technischen Konfiguration
- Administrationskonzept
- Konzept zur Benutzerverwaltung
- Berechtigungskonzept
- Ressourcen-Planung
- Planung der SAP Systemlandschaft
- Audit- und Logging-Konzept
- Änderungsmanagement-Konzept
- Backup-Konzept
- Notfallvorsorge-Konzept

Generell sind bei der Konzeption die bestehenden Sicherheitskonzepte der Behörde oder des Unternehmens zu berücksichtigen.

**Planen der technischen Konfiguration**

Aufbauend auf den vorstehend genannten Konzepten muss die technische Umsetzung durch die SAP Systemkonfiguration (Customizing) erfolgen. Dazu sind für den ABAP-Stack die notwendigen technischen Konfigurationsschrit-

te im Rahmen eines projektbezogenen Implementation Guide (IMG) festzulegen. Die notwendigen Schritte für die gewünschte Konfiguration werden in der Regel aus dem SAP Referenz-IMG ausgewählt (siehe M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*). Für den Java-Stack existiert der IMG-Mechanismus nicht, trotzdem sind die erforderlichen Konfigurationsschritte zu planen, um die gewünschten Konfiguration zu erhalten (siehe auch auch M 4.266 *Sichere Konfiguration des SAP Java-Stacks*).

Bei der Planung der technischen Konfiguration ist zu berücksichtigen, dass Rückkopplungsprozesse notwendig sind, um auf Änderungen reagieren zu können, die sich im Rahmen der Implementierung ergeben. In der Planungsphase können die SAP Systemdokumentationen herangezogen werden, um die notwendigen technischen Konfigurationen zu bestimmen und zu planen. Diese sind über das SAP Help Portal help.sap.com zugreifbar. Nach der Installation kann die technische Konfiguration, sofern notwendig, angepasst werden.

**Administrationskonzept**

Ein gutes Konzept für die Administration eines SAP Systems trägt wesentlich zur Sicherheit bei. Im Administrationskonzept ist festzulegen, wer welche administrativen Aufgaben wahrnimmt. Die technische Umsetzung muss dann dafür Sorge tragen, dass jeder nur die ihm zugeordneten Aufgaben wahrnehmen kann. Generell sollten dabei die nachfolgend beschriebenen Empfehlungen und Aspekte berücksichtigt werden.

Es muss immer ein Konzept für die Stacks (ABAP, Java) erstellt werden, die für ein SAP System installiert sind. Es muss ausgeschlossen sein, dass ein Stack installiert ist und kein Administrationskonzept vorliegt.

In großen Unternehmen und Behörden empfiehlt sich, die Administration auf mehrere Personen aufzuteilen und so eine Funktionstrennung herbeizuführen. Generell sollte immer eine Trennung der Basis-Administration und der Administration auf Applikations- und Modul-Ebene umgesetzt werden.

Weiterhin empfiehlt sich mindestens eine Aufteilung in Administratoren für Benutzerverwaltung, Berechtigungsverwaltung, Verwaltung der System-Protokollierung, Backup und Änderungsmanagement. Je nach personeller Ausstattung kann die Trennung auch weiter fortgesetzt werden, etwa auf Basis einzelner Schnittstellen (z. B. RFC, ICF, SOAP) oder Dienste (z. B. Batch-Verarbeitung). Bei der Planung des Konzeptes sollten auch die relevanten Verantwortlichen für Geschäftsprozesse und Informationen einbezogen werden. Nur so ist sichergestellt, dass das Konzept auf die Anforderungen zugeschnitten ist, die sich aus den Geschäftsprozessen ergeben.

Bei der Aufteilung der administrativen Tätigkeiten ist jedoch zu bedenken, dass weder für den ABAP-Stack noch für den Java-Stack eine solche detaillierte Trennung vorkonfiguriert ist.

Daher muss mit erhöhtem Konfigurationsaufwand gerechnet werden, wenn eine feinere Trennung erreicht werden soll.

In kleinen Unternehmen und Behörden, die oft nur einen einzigen Administrator beschäftigen, ist eine Funktionstrennung schon aufgrund fehlender personeller Alternativen nicht möglich. In diesem Fall sollten die Folgen eines internen Angriffs oder mangelnder Systemkenntnis jedoch sorgsam bedacht und abgeschätzt werden. Hier kann eine regelmäßige externe Sicherheitsprüfung helfen, die Systemsicherheit aufrecht zu erhalten. Generell müssen auch in-

terne Sicherheitskontrollen definiert werden, um das Risiko zu vermindern. Es ist dabei zu berücksichtigen, dass diese Kontrollen sowie deren Umsetzung und Durchführung auch verwaltet werden müssen.

Der ABAP-Stack eines SAP Systems darf nicht durch einen Benutzer mit SAP_ALL Berechtigungen administriert werden. Diese Administrationsvariante birgt zu viele Sicherheitsrisiken. Erfolgt die Basis-Administration durch genau einen Administrator, so kann folgendes Vorgehen sinnvoll sein:

- Dem zur Administration genutzten Konto werden die Berechtigungsobjekte aus dem Profil SAP_ALL über eine Profil-Kopie zugeordnet.
- Alle Berechtigungsobjekte, die nicht für die Basis-Administration benötigt werden - dies sind in der Regel Berechtigungen, die in Applikationen oder Modulen Verwendung finden - werden aus der Profil-Kopie gelöscht.

Damit besitzt der Administrator nicht automatisch alle Applikationsberechtigungen. Auch wenn nur ein Administrator genutzt wird, empfiehlt es sich, im Rahmen des Administrationskonzeptes festzulegen, welche administrativen Aufgaben der Administrator wahrnehmen darf und welche nicht. Die verbleibenden Berechtigungsobjekte sind dann entsprechend anzupassen. Auf diese Weise können bestimmte administrative Operationen durch den Administrator nur dann ausgeführt werden, wenn beispielsweise eine Genehmigungskette durchlaufen wurde.

Im Administrationskonzept sind auch Verfahrens- und Vorgehensweisen für die Notfall-Administration festzulegen.

**Konzept zur Benutzerverwaltung**

Die Komplexität des Benutzerverwaltungskonzeptes wird dadurch bestimmt, ob nur ein einziges oder mehrere SAP Systeme verwaltet werden sollen. Muss nur ein System verwaltet werden, so ist durch das Benutzerverwaltungskonzept Folgendes festzulegen:

- Welche Konventionen für die Benutzernamen werden eingesetzt, so dass Benutzernamen eindeutig sind?
- Wer besitzt innerhalb der Benutzerverwaltung welche Rechte?
- Welche Benutzertypen werden wie eingesetzt?
- Wie werden die Benutzer in Gruppen aufgeteilt?
- Wie werden privilegierte Standardbenutzer geschützt?
- Welche Benutzer sind Mitglied der Gruppe SUPER?
- Welche Prozesse sind für die Benutzerverwaltung (z. B. Beantragung, Genehmigung, Anlegen, Verändern, Löschen) vorgesehen?

Es ist darauf zu achten, dass für alle anfallenden Verwaltungsarbeiten Prozesse definiert werden (z. B. Anlegen von Benutzern, Ändern oder Zuordnen von Rollen) und diese vollständig spezifiziert sind. Zusätzlich sind die jeweiligen Verantwortlichkeiten vollständig festzulegen. So wird verhindert, dass sich durch unklare Verantwortlichkeiten oder unvollständig definierte Prozesse Sicherheitslücken einschleichen.

Für den Java-Stack besteht zwar die Möglichkeit, unterschiedliche Benutzerspeicher einzusetzen, generell kann jedoch der Einsatz der "User Management Engine" (UME) empfohlen werden, da diese die größte Flexibilität in der Konfiguration anbietet. In der Regel sollte die UME dann so konfiguriert werden, dass der zugehörige ABAP-Stack als Benutzerspeicher genutzt wird. So wird sichergestellt, dass gleiche Benutzerkonten mit gleichem Namen durch den Java- und ABAP-Stack auf den gleichen Benutzerstammsatz abgebildet werden.

Müssen mehrere SAP Systeme verwaltet werden, so wird durch das Konzept zur Benutzerverwaltung der mit der Benutzerverwaltung einhergehende Administrationsaufwand maßgeblich bestimmt. Es muss entschieden werden, ob eine dezentrale oder zentrale Benutzerverwaltung eingesetzt wird. Die Entscheidung ist dabei abhängig vom Einsatzszenario für das SAP System und den Anforderungen der dabei insgesamt eingesetzten Systeme.

Neben den oben beschriebenen Aspekten sind dann außerdem durch das Benutzerverwaltungskonzept folgende Aspekte zu behandeln:

- Auf welchem System werden welche Benutzerkonten verwaltet (Definition des führenden Systems)?
- Wie erfolgt die Verteilung der Benutzerkonten auf die einzelnen Systeme?
- Welche Systeme benötigen oder verlangen eine separate Benutzerverwaltung?

Eine zentrale Benutzerverwaltung ist sinnvoll, wenn es sich um eine möglichst homogene Art von Benutzern (z. B. behörden- oder unternehmensinterne Benutzer) handelt, die auf mehrere SAP Systeme zugreifen. Dabei sollten die Sicherheitsanforderungen in den Zugriffsszenarien nicht stark differieren. Ist die Benutzermenge inhomogen (z. B. behörden- oder unternehmensinterne Benutzer, Benutzer von Partnerunternehmen oder -behörden, Kunden mit loser Behörden- bzw. Unternehmensbindung), so kann es sinnvoll sein, mehrere Verwaltungsinseln (d. h. Systeme mit jeweils einer zentralen Benutzerverwaltung) einzurichten, die die Benutzer der unterschiedlichen Einsatzszenarien verwalten.

Bei der Entscheidung für oder gegen eine zentrale Benutzerverwaltung müssen auch technische Randbedingungen bedacht werden. Soll beispielsweise die Zentrale Benutzer Verwaltung (ZBV, Central User Administration, CUA) eines SAP Systems verwendet werden, wird eine funktionierende ALE-Landschaft vorausgesetzt (siehe auch M 5.128 *Absicherung der SAP ALE (IDoc/ BAPI) Schnittstelle*).

Dann ist es auch möglich die Zuordnung von Berechtigungen zu Benutzern zentral zu verwalten und in andere SAP Systeme zu transportieren.

Weitere Hinweise zur Sicherheit bei der Benutzerverwaltung finden sich in M 4.259 *Sicherer Einsatz der ABAP-Stack Benutzerverwaltung* und M 4.267 *Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung*.

Hinweise auf weitere Dokumentationen zur Benutzerverwaltung in SAP Systemen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Berechtigungskonzept**

Berechtigungen steuern, wer auf Funktionen und Daten zugreifen darf. Das Berechtigungskonzept ist daher wichtig für die Sicherheit beim Zugriff auf Funktionen und Daten eines SAP Systems. Eine bedarfsgerechte Planung der Berechtigungen durch ein ausgereiftes Berechtigungskonzept ist darum unerlässlich. Maßnahme M 2.342 *Planung von SAP Berechtigungen* enthält die Informationen, die dabei zu beachten sind.

**Ressourcen-Planung**

Ein SAP System kann ein Unternehmen oder eine Behörde nur dann optimal unterstützen, wenn die Rechner-Ressourcen auf das Einsatzszenario und auf die dabei benötigte SAP Software und deren Ressourcen-Anforderungen abgestimmt sind.

Im Ressourcen-Plan ist daher die Hardware-Ausstattung genau zu planen. Themen sind unter anderem:

- Anzahl der benötigten Rechner
- CPU- und Speicher-Ausstattung der Rechner
- benötigte Festplattenkapazitäten
- erforderliche Netz-Bandbreite
- notwendige Netzsegmente und Netzkoppelelemente

Die relevante SAP Dokumentation zur Ressourcen-Planung wird in M 2.346 *Nutzung der SAP Dokumentation* genannt.

**Planen der SAP Systemlandschaft**

Ein SAP System besteht immer aus mehreren Komponenten mit unterschiedlichen Aufgaben, die miteinander über die Netzinfrastruktur kommunizieren. Die Sicherheit eines SAP Systems kann schon durch die genutzte Architektur der Systemlandschaft positiv beeinflusst werden. Umgekehrt kann eine nicht hinreichend geplante und aufgebaute Systemlandschaft zu Sicherheitsproblemen führen.

Da die aus Sicherheitssicht günstigste Systemlandschaft sehr vom Einsatzszenario eines SAP Systems und dem Schutzbedarf der gespeicherten Daten abhängt, können in einem IT-Grundschutz-Baustein nur grundsätzliche Empfehlungen gegeben werden. SAP bietet jedoch in der Regel für verschiedene Produkte und Einsatzszenarien Empfehlungen für den günstigsten Systemaufbau an.

Allgemein sollte die Planung so erfolgen, dass nur die unbedingt benötigten Zugriffe auf und zwischen Komponenten möglich sind. Insbesondere ist eine Trennung von Produktiv-System, Test- und Abnahme-System sowie

Entwicklungs-System vorzusehen. Durch entsprechende Planung ist sicherzustellen, dass Produktivdaten eines SAP Systems nicht unverändert in Systeme für Tests und Abnahmen oder für die Entwicklung übertragen und dort genutzt werden. Kann dies nicht sichergestellt werden, müssen die Test- und Abnahme-Systeme so geschützt sein, dass auch dort die Vertraulichkeit der Daten gewährleistet ist.

Durch die Definition der Systemlandschaft muss unter anderem Folgendes festgelegt werden:

- Auf welchen Rechnern sind die einzelnen Komponenten zu installieren?
- Wo sind die einzelnen Rechner und Komponenten netztechnisch angesiedelt?
- Welche Komponenten müssen vor Zugriffen (intern, extern) durch entsprechende Firewalls oder Router geschützt werden?
- Auf welche Komponenten müssen Benutzer (intern, extern) direkt zugreifen? (Die entsprechenden Komponenten können daher nicht vollständig durch Firewalls oder Router geschützt werden.)
- Welche Komponenten müssen aufgrund des Zugriffsverhaltens in der DMZ (De-Militarisierte Zone) angesiedelt werden?
- Wie kann die Verfügbarkeit des gesamten SAP Systems gewährleistet werden?

Weitere Hinweise für spezielle Einsatzszenarien finden sich M 2.343 *Absicherung eines SAP Systems im Portal-Szenario* und M 2.344 *Sicherer Betrieb von SAP Systemen im Internet*.

SAP Dokumentationen mit detaillierten Hinweisen zur empfohlenen Systemlandschaft finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Audit- und Logging-Konzept**

Das Audit- und Logging-Konzept muss festlegen, welche Aktivitäten des SAP Systems und welche Aktivitäten der Benutzer zu protokollieren sind. Außerdem müssen folgende Aspekte berücksichtigt werden:

- Wer hat die Berechtigung, die Audit- und Protokoll-Einstellungen zu verändern?
- Wo werden die Protokolldaten abgelegt?
- Wer hat Zugriff auf die erstellen Protokolldaten?
- Wie erfolgt die Auswertung der erstellten Protokolldaten?
- Durch wen und in welchem Umfang erfolgen Sicherheitsprüfungen (Audits) und in welchen Abständen?

Ein SAP System besitzt umfangreiche Möglichkeiten, um interne Abläufe und Benutzeraktivitäten zu protokollieren. Die hier wichtigen Aspekte werden in M 4.270 *SAP Protokollierung* thematisiert.

Neben der reinen Systemüberwachung, die durch die Protokollierung erreicht werden soll, ist im Rahmen von Audits die Sicherheit des SAP Systems regelmäßig zu prüfen. Audits können dabei sowohl durch Administratoren (Selbstkontrolle) als auch durch andere Prüfer erfolgen. Die Prüfer können dabei aus anderen Abteilungen stammen (Informationssicherheit, Revision) oder aber von externen Dritten (IT-Auditoren, Wirtschaftsprüfer, Aufsichtsorganisationen). Weitere Informationen dazu finden sich in M 2.347 *Regelmäßige Sicherheitsprüfungen für SAP Systeme*. Es ist zu beachten, dass Selbstkontrollen durch Administratoren nicht ausreichen, um die Sicherheit von SAP Systemen zu beurteilen.

**Änderungsmanagement-Konzept**

Die Aktualisierung eines SAP Systems durch Patches, Hot-Fixes und Updates ist wichtig, um die Sicherheit des Systems zu erhalten. Fehler in der Programmierung können nur behoben werden, wenn das System regelmäßig aktualisiert wird. Da sich die Änderungsmanagement-Prozesse von ABAP- und Java-Stack technisch unterscheiden, sind zwei separate Konzepte zu entwerfen. Folgende Fragestellungen sind jeweils durch das Konzept zu klären:

- Nach welchem Prozess erfolgt die Systemaktualisierung über die Systemvarianten Entwicklung, Test und Abnahme, Produktion?
- Wie wird sichergestellt, dass die eingespielten Updates den Betrieb nicht negativ beeinflussen?
- In welchen Zeitabständen erfolgt die Aktualisierung?
- Wer besitzt die Berechtigung, Aktualisierungen im Produktivsystem durchzuführen?
- An welchen Stellen des Änderungsmanagement-Prozesses müssen Kontrollschritte erfolgen?
- Wie wird sichergestellt, dass Aktualisierungen nicht durch eine einzelne Person durchgeführt werden können?
- Wie ist der Zugriff auf die Werkzeuge und Funktionen einzuschränken, die für die Aktualisierung benötigt werden?
- Wie werden Veränderungen protokolliert und dadurch nachvollziehbar gemacht?

Änderungen werden in den ABAP-Stack über das so genannte Transportsystem eingespielt. Dabei können mehrere SAP Systeme zu einem Transportverbund (Transportdomäne genannt) zusammengeschaltet werden. Im Rah-

men der Planung des Änderungsmanagement-Konzeptes ist daher ein Transportkonzept zu erstellen. Hier sind unter anderem folgende Fragestellungen und Aspekte zu klären:

- Wer darf Transporte erzeugen?
- Der Freigabeprozess für Transporte muss klar definiert werden, es müssen Qualitätsziele definiert sein, die eingehalten werden, bevor neue Transporte oder Patches eingespielt werden.
- Wer darf Transporte einspielen?
- Wie kommen die Transporte (technisch) von einem System zum anderen?
- Wie ist die Prozessreihenfolge zu definieren, so dass unterschiedliche Personen involviert werden, damit die benötigten Kontrollschritte durchgeführt werden?
- Es dürfen keine direkten Transporte durch Entwickler von der Entwicklung in Test und Abnahme oder die Produktion möglich sein.
- Welcher Integritätsschutz von Transportdateien soll eingesetzt werden?
- Wie ist die Nachvollziehbarkeit sicherzustellen? (Frage: Wer hat wann was gemacht?)
- Die Transportlandschaft muss geplant werden: Welche Instanzen und Mandanten sind jeweils involviert? Von welcher Quelle darf in welches Ziel transportiert werden?

Weitere Informationen und Empfehlungen finden sich in M 2.221 *Änderungsmanagement*, M 4.272 *Sichere Nutzung des SAP Transportsystems* und M 4.273 *Sichere Nutzung der SAP Java-Stack Software-Verteilung*.

Hinweise aus SAP Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Backup-Konzept**

Bezüglich des Backup-Konzeptes bestehen keine außergewöhnlichen Anforderungen für ein SAP System (siehe M 6.97 *Notfallvorsorge für SAP Systeme*).

Das SAP Backup-Konzept sollte sich in ein bestehendes Backup-Verfahren integrieren, so dass keine speziellen Ausnahmeprozeduren notwendig werden. Im Vordergrund sollte stehen, die Verantwortlichkeiten und Prozessabläufe für die Datensicherungen zu definieren und umzusetzen.

**Notfallvorsorge-Konzept**

Für geschäftskritische Notfälle muss ein Notfallvorsorge-Konzept für SAP Systeme und zugehörige Notfall-Prozeduren festgelegt werden (siehe auch M 6.97 *Notfallvorsorge für SAP Systeme*).

Prüffragen:

- Sind die Personalvertretung, der Datenschutzbeauftragte und die IT-Sicherheitsverantwortlichen ausreichend in alle Planungen zum SAP Einsatz mit einbezogen?
- Liegt eine auf die Zusammenarbeit der individuellen SAP Systeme abgestimmte Gesamtplanung vor?
- Stehen die erstellten SAP Sicherheitsteilkonzepte im Einklang mit bestehenden Sicherheitskonzepten?
- Wurde die Funktionstrennung für administrative Aufgaben (Basis-Administration und Administration auf Applikations- und Modul-Ebene) korrekt umgesetzt?

- Werden im Rahmen des Notfallvorsorge-Konzeptes für SAP Systeme regelmäßig Notfallübungen durchgeführt und die Prozesse anhand der dabei gemachten Erfahrungen angepasst?
- Ist der SAP Einsatz umfassend geplant worden?

# M 2.342 Planung von SAP Berechtigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

**Erklärung der wichtigsten Begriffe**

Berechtigungen in einem SAP System steuern die Zugriffsmöglichkeiten seiner Benutzer. Die Sicherheit der Geschäftsdaten hängt daher direkt von den eingestellten Berechtigungen ab. Aus diesem Grund muss die Vergabe von Berechtigungen sorgfältig geplant und durchgeführt werden, um die gewünschte Sicherheit zu erreichen.

Die Funktionen eines SAP Systems (z. B. Programme oder Reports, generell Applikationen im SAP System) werden über Transaktionen aufgerufen, die dabei unterschiedliche Operationen oder Aktivitäten (z. B. Schreiben, Lesen, Löschen) auf Daten ausführen können. Die über Transaktionen gestarteten Applikationen prüfen beim Aufruf, ob der aufrufende Benutzer über die notwendigen Berechtigungen verfügt, die angeforderte Operation auf den durch die Applikation angesprochenen Daten auszuführen.

Der Prüfmechanismus baut auf so genannten Berechtigungsobjekten auf, die Autorisierungsfelder besitzen. Eine konkrete Berechtigung kann als Ausprägung eines Berechtigungsobjektes mit ausgefüllten Autorisierungsfeldern verstanden werden. Beim Start einer Transaktion prüft der SAP Kern zunächst, ob der Benutzer die Berechtigung zum Start der Transaktion besitzt. Nach dem Start kann die Transaktion auch weitere Berechtigungsprüfungen durchführen. Geprüft wird, ob der zugreifende Benutzer eine Berechtigung besitzt, die vom benötigten Berechtigungsobjekt abgeleitet ist. Ist dies der Fall, werden die Autorisierungsfelder der Berechtigung daraufhin geprüft, ob sie die benötigten Werte oder Wertekombinationen enthalten. Eine Transaktion kann dabei auf mehrere Berechtigungen prüfen. Welche dies sind, wird im Programm-Code festgelegt. Beim Start einer Transaktion wird vom SAP Kern immer auf das Berechtigungsobjekt S_TCODE geprüft. Beim Start von Applikationen wird auf das Berechtigungsobjekt S_PROGRAM geprüft. Die eigentliche Prüfung erfolgt also immer durch den Kern des SAP Systems, auch wenn diese durch den Programm-Code der Transaktion angestoßen wird.

Aus Applikationssicht sind insbesondere diejenigen Autorisierungsfelder von Berechtigungsobjekten wichtig, die als so genannte Organisationsebenen ausgeprägt werden müssen. Sie berechtigen dann eine Rolle, eine bestimmte Transaktion, beispielsweise für den angegeben Buchungskreis (oftmals eine zusammenhängende Geschäftseinheit eines Unternehmens, z. B. Tochterunternehmen) durchzuführen.

Berechtigungen werden Benutzern dadurch zugeordnet, dass ihnen so genannte Rollen zugeordnet werden. Rollen geben an, welche Transaktionen durch den Benutzer ausgeführt werden sollen, dem eine Rolle zugeordnet wurde. Da jede Transaktion auf bestimmte, durch den Programm-Code festgelegte Berechtigungsobjekte prüft, kann für jede Rolle ein Berechtigungsprofil (d. h. Menge von Berechtigungen) abgeleitet werden, in dem alle Berechtigungsobjekte enthalten sind, die zur Ausführung der Transaktionen generell benötigt werden. Der Prozess, das Berechtigungsprofil für eine Rolle und die darin enthaltenen Transaktionen zu erstellen, wird über den Profilgenerator (Transaktion PFCG) automatisiert.

Über Prüfkennzeichen für Transaktionen kann gesteuert werden, für welche Berechtigungsobjekte, auf die eine Transaktion prüft, der SAP Kern tatsächlich eine Prüfung ausführt. Über die Prüfkennzeichen können folglich Berechtigungsobjekte beim Aufruf einer Transaktion von der Prüfung ausgeschlossen werden. In diesem Fall wird durch den Profilgenerator auch keine Berechtigung im generierten Berechtigungsprofil erzeugt. Die Prüfkennzeichen werden über die Transaktion SU24 gepflegt, hier werden auch für die einzelnen Autorisierungsfelder der Berechtigungsobjekte die Werte gepflegt, die durch den Profilgenerator in die generierten Berechtigungen der Profile eingetragen werden. Es handelt sich dabei um Vorschlagswerte. Die Profile, die durch den Profilgenerator erzeugt werden, müssen unter Umständen noch manuell nachbearbeitet werden.

**Planungsschritte bei der Vergabe von Berechtigungen**

Die Vergabe von Berechtigungen in einem SAP System ist also ein mehrstufiger Prozess. Zunächst müssen die benötigten Rollen definiert werden. Wichtig ist dabei, dass die Rollen letztendlich Arbeitsplätze oder Positionen im Unternehmen oder der Behörde beschreiben. Sie sollten nicht auf einzelne Mitarbeiter bezogen sein, sonst wird die Anzahl an Rollen unübersichtlich und unbeherrschbar. Ein gutes Berechtigungskonzept steht und fällt damit, ob die definierten Rollen sorgfältig spezifiziert wurden.

Sind die Rollen definiert, müssen die zugehörigen Berechtigungsprofile durch den Profilgenerator erzeugt werden. Der Umfang der erzeugten Berechtigungen in den Rollenprofilen wird durch die Konfiguration der Prüfkennzeichen beeinflusst. Auch dies muss sorgfältig geplant werden, da abgeschaltete Prüfungen immer auch einen gewissen Grad an Sicherheitsverlust bedeuten. Die erzeugten Profile und enthaltenen Berechtigungen sind zu prüfen und gegebenenfalls anzupassen.

Abschließend werden die Berechtigungen Benutzern dadurch zugewiesen, dass einem Benutzer eine Rolle zugeordnet und der so genannte Benutzerabgleich angestoßen wird. Dadurch werden im Benutzerstammsatz die im Berechtigungsprofil der Rolle enthaltenen Berechtigungen gespeichert.

**Berechtigungskonzept**

Das Berechtigungskonzept für ein SAP System muss in zwei Ausprägungen erstellt werden: für den ABAP-Stack und für den Java-Stack. Es gilt dabei zu beachten, dass sich das Berechtigungssystem des Java-Stacks fundamental von dem des ABAP-Stacks unterscheidet. Konzeptionell sind jedoch die gleichen Fragestellungen zu betrachten. Dies sind unter anderem:

- Welche Rollen werden benötigt?
- Welche Rolle darf welche Funktionen des SAP Systems aufrufen (z. B. Transaktionen, Programme oder Reports)?
- Welche Rolle darf auf welche Daten des SAP Systems zugreifen?
- Welche administrativen Rollen mit welchen Berechtigungen werden benötigt, um das geplante Administrationskonzept umzusetzen?
- Nutzen Applikationen neben dem SAP Standardberechtigungssystem noch weitere Berechtigungen? Diese sind entsprechend im Konzept zu berücksichtigen und zu planen.
- Welche Prozesse für die Berechtigungsverwaltung sind mit den zugehörigen Verantwortlichkeiten zu definieren (z. B. Beantragung, Genehmigung, Anlegen, Verändern, Löschen)?

- Sind Funktionstrennungsaspekte im Berechtigungskonzept ausreichend beachtet? Hier spielen insbesondere auch rechtliche Anforderungen eine Rolle.
- Wird beim Änderungsmanagement auch das Risikopotential betrachtet, welches durch eine Berechtigungshäufung entstehen kann?

Es ist darauf zu achten, dass für alle anfallenden Vorgänge im Kontext von Berechtigungen Prozesse definiert werden und die Prozesse vollständig spezifiziert sind. Zusätzlich sind die jeweiligen Verantwortlichkeiten vollständig festzulegen. So wird verhindert, dass sich durch unklare Verantwortlichkeiten oder unvollständig definierte Prozesse Sicherheitslücken einschleichen.

Die Definition der Rollen und der zugeordneten Berechtigungen muss sich einerseits an den Erfordernissen der Institution orientieren, andererseits müssen hier auch die Anforderungen einbezogen werden, die sich aus den rechtlichen Rahmenbedingungen ergeben, wie beispielsweise dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontrAG), der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) oder dem Bundesdatenschutzgesetz (BDSG). Eine ausführliche Planung ist daher unumgänglich. Je detaillierter die Erfordernisse der Rollen bekannt sind, desto besser können später die Berechtigungen vergeben werden. Dabei ist auf die notwendige Trennung zwischen Rollen zu achten. Es ist empfehlenswert, die Rollen, und damit die Berechtigungen, an die interne Organisationshierarchie und die darin existierenden Positionen und Stellen anzupassen. So kann beispielsweise erreicht werden, dass bei Positionswechseln von Mitarbeitern deren alte Berechtigungen nicht mehr verfügbar sind.

Wichtig ist außerdem, dass im Unternehmen oder in der Behörde Verantwortliche für Informationen und Prozesse ernannt werden (Informationseigentümer bzw. Verfahrensverantwortliche), die einen bestimmten Datenbestand der Organisation verantworten. Beispielsweise ist der Leiter der Finanzabteilung (Chief Financial Officer, CFO) für den Finanz- und Controllingbereich verantwortlich. Die Verantwortlichen aller Bereiche sind unbedingt in die Planung der benötigten Rollen, Berechtigungen und Prozesse einzubeziehen, da nur sie die dazu notwendigen Kenntnisse auf fachlicher Ebene besitzen. Administratoren sind in der Regel nicht in der Lage, die Rollen und Berechtigungen auf Applikationsebene alleine zu planen.

Im Rahmen der Berechtigungsplanung ist auch Folgendes festzulegen:

- Welche Berechtigungen sind als kritisch zu betrachten (d. h. erlauben kritische Operationen im SAP System unter administrativen, rechtlichen oder betriebswirtschaftlichen Aspekten)?
- Welche Rollen dürfen welche kritischen Berechtigungen, Profile oder Rollen erhalten?
- Welche Rollen dürfen welche Werte für kritische Berechtigungsfelder erhalten?

Weitere Hinweise zur Definition von kritischen Berechtigungen finden sich in M 4.261 *Sicherer Umgang mit kritischen SAP Berechtigungen*.

Im Detail unterscheiden sich die Konzepte für den ABAP- und Java-Stack sehr. Für den ABAP-Stack muss die Berechtigungsverwaltung über den Profilgenerator und nicht manuell erfolgen. Generell muss von der manuellen Verwaltung dringend abgeraten werden, da dies häufig zu Fehlkonfigurationen der Berechtigungen führt. Durch den Profilgenerator wird sichergestellt, dass die Benutzer nur die Berechtigungen erhalten, die zum Ausführen derjenigen Transaktionen notwendig sind, die ihnen über die Rollen zugeordnet wurden.

Daher ist wichtig, dass insbesondere die Konzepte, Prozesse und Abläufe auf die Verwendung des Profilgenerators abgestimmt sind.

Für den JAVA-Stack besteht hingegen keine Wahlmöglichkeit, da der Berechtigungsmechanismus der Spezifikation der Java 2 Enterprise Edition (J2EE) genutzt werden muss. Es ist dabei zu beachten, dass die "User Management Engine" (UME) über diesen Standard hinausgehende Optionen anbietet.

Weitere Informationen finden sich in M 4.260 *Berechtigungsverwaltung für SAP Systeme*, in M 4.262 *Konfiguration zusätzlicher SAP Berechtigungsprüfungen* sowie in M 4.268 *Sichere Konfiguration der SAP Java-Stack Berechtigungen*.

Hinweise auf SAP Dokumentationen, die bei der Planung des Berechtigungskonzeptes genutzt werden können, finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Planen der Berechtigungsverwaltung**

Die Verwaltung der Berechtigung muss geplant und das gewünschte Verwaltungskonzept muss definiert werden. Im Wesentlichen ist dabei zu berücksichtigen, welche Aufgaben in der Berechtigungsverwaltung durch wen erledigt werden. Hier empfiehlt sich ein rollenbasierter Ansatz (siehe auch M 4.260 *Berechtigungsverwaltung für SAP Systeme*), so dass den definierten Rollen später konkrete Benutzer und damit Personen zugeordnet werden können. Dabei ist zu beachten, dass unvereinbare Rollen (Funktionstrennung) nicht derselben Person zugeordnet werden. Da in einer Organisation auch für die Berechtigungsverwaltung schon eine Vielzahl an Rollen impliziert sind, müssen diese entsprechend abgebildet werden.

So gibt es beispielsweise in der Regel keine einzelne Administrator-Rolle, vielmehr sind Rollen wie Benutzer-Administrator, Rollen-Administrator, Berechtigungs-Administrator, Entwickler, Help-Desk-Mitarbeiter oder Transport-Manager zu betrachten. Folglich sind die von SAP vordefinierten Rollen in der Regel nicht ohne Anpassungen zu benutzen.

Prüffragen:

- Sind die Rollen und Berechtigungen im SAP System adäquat geplant worden?
- Werden die vom Profilgenerator erzeugten Profile und enthaltenen Berechtigungen im SAP System geprüft und gegebenenfalls angepasst?
- Wird das Berechtigungskonzept in den beiden ABAP-Stack und Java-Stack gleichwertig umgesetzt?
- Wird darauf geachtet, dass für alle anfallenden Vorgänge im Kontext von SAP-Berechtigungen Prozesse definiert und vollständig spezifiziert werden?
- Ist die Verwaltung der Berechtigungen im SAP System mit allen Prozessen geplant und wurden die Verantwortlichkeiten vollständig definiert?

# M 2.343 Absicherung eines SAP Systems im Portal-Szenario

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Entwicklung, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

SAP Systeme werden immer häufiger auch in Portal-Szenarien eingesetzt. Im Folgenden wird davon ausgegangen, dass es sich um ein internes Behörden- oder Unternehmensportal handelt, über welches auf ein SAP System zugegriffen wird. Diese Maßnahme behandelt nicht die Sicherheit des Behörden- oder Unternehmensportals, sondern die Sicherheit eines SAP Systems im Umfeld des Portales. Für SAP Systeme in Internetszenarien finden sich entsprechende Maßnahmen in M 2.344 *Sicherer Betrieb von SAP Systemen im Internet*. Der Zugriff in Portal-Szenarien erfolgt in der Regel über HTTP, und Benutzer setzen dafür einen Browser ein.

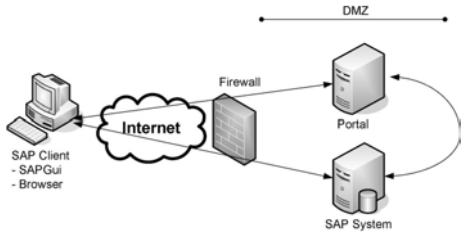



Abbildung: SAP System im Portal-Szenario

In Portalszenarien wird oft fälschlich angenommen, dass das eingesetzte Portal auf das "nachgelagerte" SAP System zugreift. Ein direkter Benutzerzugriff auf das SAP System wäre dann nicht notwendig. In der Regel erfolgt jedoch im Portal nur eine Umleitung auf das SAP System, so dass die Benutzeranfragen direkt an das SAP System erfolgen. Dies ist oft sogar transparent für den Benutzer, da die im Browser angezeigten Daten innerhalb der aufgerufenen Portalseite in einem Rahmen eingeblendet werden. Insofern ist auch in Portal-Szenarien die Maßnahme M 2.344 *Sicherer Betrieb von SAP Systemen im Internet* relevant.

Generell sind für SAP Systeme in Portal-Szenarien folgende grundsätzliche Aspekte wichtig:

- Architektur des Netz- und Systemaufbaus (siehe auch M 2.341 *Planung des SAP Einsatzes*)
- Kommunikationsabsicherung (siehe auch M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*)
- Sicherheit von Anwendungen im Internet-Einsatz
- Erkennen von Angriffen (Intrusion Detection Systeme)
- Schutz vor Viren beim Hoch- oder Herunterladen von Dateien (siehe auch M 4.271 *Virenschutz für SAP Systeme*)

Folgende Aspekte, die sich direkt aus dem Portal-Szenario ableiten, sind besonders zu berücksichtigen:

**Systemzugriff einschränken**

Alle SAP Systeme, die durch Browser-Umleitungen angesprochen werden, müssen für Benutzer zugreifbar sein. Dieser Umstand ist in der Risikobetrachtung zu berücksichtigen und hat Auswirkungen auf die Position des SAP Sy-

stems im Netz, da es beispielsweise in der DMZ (Demilitarisierte Zone) angesiedelt werden muss.

Der Zugriff auf die betroffenen SAP Systeme muss durch eine Firewall auf die Ports beschränkt werden, über die HTTP bzw. HTTPS abgewickelt wird. Je nach Szenario sollte der Zugriff auf das SAP System über einen Reverse Proxy geleitet werden, so dass auf das SAP System nicht direkt zugegriffen wird.

**Dialogzugriff einschränken**

In der Regel darf der SAPGui-Zugang für die über das Portal angesprochenen SAP Systeme nur eingeschränkt zugelassen werden. Insbesondere für Benutzer, die nur über das Portal mittels Browser zugreifen, muss der SAP-Gui-Zugang unterbunden werden. Hier können beispielsweise Benutzer vom Typ "Internetbenutzer" eingesetzt werden, wenn der Port-Zugang nicht durch die Firewall beschränkbar ist. Es ist generell zu bedenken, dass der SAP-Gui-Zugang für Administratoren möglich sein muss, so dass die Firewall entsprechend zu konfigurieren ist. Alternativ kann auch eine separates Administrationsnetz genutzt werden.

Wird der Internet Transaction Server (ITS) zum Zugriff auf das SAP System nicht genutzt, sollte der ITS Zugang deaktiviert werden, da dieser einen SAP-Gui-ähnlichen Zugang zum SAP System bietet. Die ITS Komponente muss vor der Version 6.40 des SAP Web Application Servers als separate Komponente (WGate, AGate) installiert werden. In diesem Fall sollten diese Komponenten nicht installiert oder aber deinstalliert werden.

Ab Version 6.40 ist der ITS integriert, so dass die entsprechenden Dienste im ABAP-Stack (z. B. webgui) und Java-Stack (z. B. mi oder me) deaktiviert werden müssen. Dies erfolgt im ABAP-Stack dadurch, dass der ICF-Dienst "webgui" deaktiviert ist (siehe auch M 5.127 *Absicherung des SAP Internet Connection Framework (ICF)*). Im Java-Stack (siehe auch M 4.266 *Sichere Konfiguration des SAP Java-Stacks*) sind die Applikationen "mi" und "me" über den Deploy-Dienst zu deaktivieren.

**Authentisierung/Single Sign-On**

In der Regel ist Single Sign-On zwischen dem Portal und dem SAP System konfiguriert. Daher ist sicherzustellen, dass Konten mit gleichen Namen in beiden Systemen der gleichen Person zugeordnet sind. Kann dies nicht sichergestellt werden, so muss der so genannte Benutzer-Mapping-Mechanismus des Portals genutzt werden.

Beim Zugriff auf das SAP System werden dann die hinterlegten Konten-Informationen genutzt. In diesem Fall ist dann auf die Konsistenz der Benutzer-Mapping-Informationen zu achten.

**Berechtigungen**

In Portal-Szenarien kann der Fall auftreten, dass Applikationen, die im Portal ablaufen (Frontend-Applikation), selbst direkt auf das SAP System zugreifen. Je nach Applikationsdesign wird dann ein technisches Konto oder das Konto des angemeldeten Benutzers zum Zugriff genutzt. Für dieses Konto darf im SAP System dann nur der Aufruf derjenigen ABAP-Funktionsgruppen erlaubt sein, die für die Portalanwendung benötigt werden.

Generell ist darauf zu achten, dass die Berechtigungen der im SAP System gehaltenen Benutzer minimal gestaltet werden. Bei den Planungen sollte davon

ausgegangen werden, dass die Berechtigungsprüfung der Frontend-Applikation auch unterlaufen werden kann. Wird der Benutzer vom Portal lediglich umgeleitet, so greift er direkt auf das SAP System zu. Daher sollten die Berechtigungen im SAP System immer so eingerichtet sein, dass nur die Funktionen aufgerufen werden können, die durch die Portal-Applikation möglich sind. Dies ist insbesondere dann wichtig, wenn der Dialog-Zugriff von Portal-Benutzern nicht ausgeschlossen ist.

**Sitzungsmanagement der Applikationen**

Alle Applikationen des ABAP- und des Java-Stacks, die über das Portal genutzt werden, sollten ein sicheres Sitzungsmanagement implementieren. Insbesondere ist durch die Programmierung der Applikationen sicherzustellen, dass Sitzungsinformationen bei der Benutzerabmeldung vom Portal ungültig werden.

Es ist zu bedenken, dass die Abmeldung vom Portal nicht automatisch zur Abmeldung am SAP System führt. Dies ist immer dann ein Problem, wenn ein Client-Rechner von mehreren Personen genutzt wird, da dann ein nachfolgender Benutzer unter Umständen auf die Daten des vorherigen Benutzers im SAP System zugreifen kann.

SAP stellt Programmier-Frameworks (z. B. Business Server Pages, BSP) zur Verfügung, die eine automatisierte Abmeldung am SAP System anbieten. Bei Eigenentwicklungen sollte dies bei der Entscheidung, welche Technologie bzw. Framework zur Implementierung genutzt wird, berücksichtigt werden.

Prüffragen:

- Sind SAP Systeme, die durch Browser-Umleitungen angesprochen werden und für Benutzer zugreifbar sein müssen, in der Risikobetrachtung berücksichtigt worden?
- Wird der Zugriff auf die betroffenen SAP Systeme im Portal-Szenario durch eine Firewall auf HTTP bzw. HTTPS Ports beschränkt?
- Ist der Dialogzugriff auf das SAP System unterbunden, wenn dieser nicht benötigt wird?
- Ist sichergestellt, dass Konten mit gleichen Namen in Portal und SAP System den gleichen Personen zugeordnet sind?
- Sind die Berechtigungen im SAP System minimal gehalten, so dass nur die Funktionen aufgerufen werden können, die durch die Portal-Applikation möglich sind?
- Sind die eingesetzten Applikationen mit einem sicheren Sitzungsmanagement ausgerüstet, das auch in Portal-Szenarien funktioniert?

# M 2.344 Sicherer Betrieb von SAP Systemen im Internet

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Entwicklung, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

SAP Systeme werden immer häufiger auch in Internet-Szenarien eingesetzt. In der Regel sind dann entsprechende Zusatzapplikationen installiert, oder sie werden im Rahmen von Internet-Portal-Szenarien (siehe auch M 2.343 *Absicherung eines SAP Systems im Portal-Szenario*) als "Backend-Systeme" eingesetzt. Der Zugriff in Internet-Szenarien erfolgt in der Regel über HTTP, und Benutzer setzen dafür einen Browser ein.

Daher sind in Internet-Szenarien folgende Aspekte zu berücksichtigen:

### Systemzugriff nach Risikobetrachtung einschränken

Alle SAP Systeme, die direkt aus dem Internet angesprochen werden, sind einem erhöhten Risiko ausgesetzt. Dies ist in der Risikobetrachtung zu berücksichtigen. Der Zugriff auf die betroffenen SAP Systeme muss durch eine Firewall auf die Ports beschränkt werden, über die HTTP bzw. HTTPS abgewickelt wird.

Generell gelten für den Zugriff auf ein SAP System aus dem Internet die gleichen Anforderungen, wie für jedes andere System, beispielsweise einen Web-Server (siehe auch B 5.4 *Webserver*). Daher sind die allgemeinen, relevanten Maßnahmen für vernetzte Systeme mit Internetanschluss zu berücksichtigen. So kann es beispielsweise sinnvoll sein, auf das SAP System über einen Reverse Proxy oder eine Applikationsfirewall (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*) zuzugreifen.

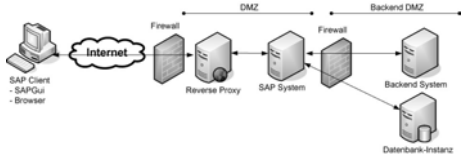



Abbildung: SAP System im Internet

### Kommunikationsschnittstelle prüfen und absichern

Über die HTTP-basierten Schnittstellen werden Applikationen angeboten. Sowohl für die System-Applikationen als auch für normale Applikationen muss eine Risikobetrachtung erfolgen. Weiterhin ist eine Sicherheitsprüfung der Web-Schnittstelle sinnvoll, um die Gefährdung gegenüber typischen Web-basierten Angriffen einschätzen zu können.

Generell ist zu bedenken, dass über die HTTP-Schnittstelle auch RFC-Zugriffe möglich sind. Daher dürfen nur die Dienste aktiviert werden, die benötigt werden und die sorgfältig auf ihre Eignung zum Betrieb im Internet hin geprüft wurden.

### Dialogzugriff einschränken

Der direkte SAPGui-Zugriff auf SAP Systeme über das Internet sollte ausgeschlossen werden und durch eine Firewall auf die Protokolle HTTP und HTTPS beschränkt sein.

**Internet Transaction Server**

Wird der Internet Transaction Server (ITS) zum Zugriff auf das SAP System nicht genutzt, so sollte der ITS Zugang deaktiviert werden, da dieser einen SAPGui-ähnlichen Zugang zum SAP System bietet.

Die ITS Komponente muss vor der Version 6.40 des SAP Web Application Servers als separate Komponente (WGate, AGate) installiert werden. In diesem Fall sollten diese einfach nicht installiert sein. Ab Version 6.40 ist der ITS integriert, so dass die entsprechenden Dienste im ABAP-Stack (z. B. Webgui, siehe M 5.127 *Absicherung des SAP Internet Connection Framework (ICF)*) und Java-Stack (z. B. mi oder me, siehe M 4.266 *Sichere Konfiguration des SAP Java-Stacks*) deaktiviert werden müssen.

Wird der ITS genutzt, so muss in Hinblick auf die Berechtigungen im SAP System sorgfältig geprüft werden, ob nur die jeweils erlaubten Funktionen aufgerufen werden können. Stichprobenprüfungen reichen in diesem Fall nicht aus. Die Prüfung ist unter Umständen mit erheblichem Aufwand verbunden. Insbesondere sollten alle Transaktionen, auf die nicht zugegriffen werden soll, deaktiviert werden, um auszuschließen, dass diese durch kritische Berechtigungskombinationen aufgerufen werden können. Da ein SAP System mehrere tausend Transaktionen enthalten kann, ist dies ein zeitintensiver Konfigurationsprozess, der in der Regel nicht geleistet werden kann. Daher muss die Gefährdung durch ein sorgfältig durchdachtes Berechtigungskonzept möglichst gering gehalten werden.

**Authentisierung/Single Sign-On**

Single Sign-On Zugriffe aus dem Internet sollten nur zwischen den für den Internet-Zugriff freigegebenen Systemen aktiviert sein.

Für externe Systeme sollten keine Vertrauensstellungen konfiguriert werden, da die Sicherheit für diese nicht kontrolliert werden kann.

**Berechtigungen**

Es ist darauf zu achten, dass die Berechtigungen der im SAP System gehaltenen Benutzer minimal gestaltet werden. Es empfiehlt sich, für Benutzer, die keinen SAPGui-Zugriff benötigen, Konten vom Typ Kommunikations- oder Internet-Benutzer einzusetzen.

**Validieren von Daten aus SAP Systemen mit Internet-Zugriff**

Daten, die von SAP Systemen mit Internetzugriff an Systeme ohne Internetzugriff weitergegeben werden - etwa durch Anfragen oder durch Datentransport - müssen validiert werden, bevor sie an das Backend-System weitergesendet werden.

**Verfügbare Daten**

Werden Daten aus internen SAP Systemen über SAP Systeme mit Internet-Zugriff bereitgestellt, so sollte Folgendes geprüft werden:

- Es sollte geprüft werden, ob es tatsächlich erforderlich ist, dass die Daten über direkte Zugriffe auf die internen Systeme bereitgestellt werden oder ob periodische Datenexporte und -importe möglich sind. Dies verhindert den Zugriff auf interne Systeme von außen.
- Beim Exportieren von Daten sollte geprüft werden, ob alle Informationen exportiert werden müssen oder ob tatsächlich nur ein Teil der Informatio-

nen benötigt wird. Dies beschränkt die auf dem SAP System mit Internetzugriff gespeicherten Daten.

Bei Export-/Import-Lösungen ist zu beachten, dass dies die direkte Applikationsintegration (etwa für CRM oder SRM Systeme) unterbindet, so dass die Vorteile der direkten Integration nicht mehr genutzt werden können. Zusätzlich muss der Datentransport konfiguriert und verwaltet werden. Daher bietet sich diese Lösung in der Regel nur für einfache Szenarien an.

Prüffragen:

- Sind SAP Systeme, die direkt aus dem Internet angesprochen werden, in der Risikobetrachtung berücksichtigt worden?
- Wird bei Nutzung von ITS geprüft, ob nur die jeweils erlaubten Funktionen aufgerufen werden können?
- Ist sichergestellt, dass im SAP-System Single Sign-On Zugriffe aus dem Internet nur zwischen den für den Internet-Zugriff freigegebenen Systemen aktiviert sind?
- Ist sichergestellt, dass im SAP-System für externe Systeme keine Vertrauensstellungen konfiguriert sind?
- Werden Daten, die von SAP Systemen mit Internetzugriff an Systeme ohne Internetzugriff weitergegeben werden validiert, bevor sie an das Backend-System weitergesendet werden?
- Wird beim Exportieren von Daten geprüft, das nur der erforderliche Teil der Informationen exportiert wird?

# M 2.345 Outsourcing eines SAP Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Beim Outsourcing von SAP Systemen ist Folgendes zu beachten:

- Die Maßnahmen des Bausteines B 1.11 *Outsourcing* sind beim Outsourcing-Partner umzusetzen.
- Besonderes Augenmerk verdient die reibungslose Prozessintegration, damit beispielsweise auch Rückmeldungen vom Outsourcing-Partner zum Outsourcing-Auftraggeber erfolgen. Dies trifft auch auf die Prozesse im Kontext der Benutzer- und Berechtigungsverwaltung zu.
- Es empfiehlt sich, eine Tabelle mit allen Aufgaben, die für ein SAP System anfallen, aufzustellen. In dieser Tabelle sollte vermerkt werden, welche Aufgaben durch Mitarbeiter des Outsourcing-Partners und welche durch eigene Mitarbeiter durchgeführt werden. Die verantwortlichen Personen sind zu dokumentieren. Die nachfolgende Tabelle ist als unvollständiges Beispiel zu verstehen und muss auf die lokalen Gegebenheiten angepasst werden. Die Aufgaben müssen in der Regel in Unteraufgaben verfeinert werden.

| **Aufgabe** | **Verantwortlich** |
|---|---|
| Planung des SAP Systems | Unternehmen/Behörde (Outsourcing-Partner jedoch einbeziehen) |
| Definition des Berechtigungskonzeptes | Unternehmen/Behörde |
| Installation des SAP Systems | Outsourcing-Partner |
| Basis-Konfiguration des SAP Systems | Outsourcing-Partner (mit Vorgaben durch das Unternehmen bzw. der Behörde aus der Planungsphase) |
| Konfiguration auf Ebene von Modulen oder Applikationen | Unternehmen/Behörde (entsprechend der Vorgaben aus der Planungsphase) |
| Basis-Administration - Anlegen von Benutzern | Outsourcing-Partner (nach Auftrag durch Unternehmen bzw. Behörde, bei Rollentrennung beim Outsourcing-Partner) |
| Basis-Administration - Verwalten von Berechtigungen | Outsourcing-Partner (nach Auftrag durch Unternehmen bzw. Behörde, bei Rollentrennung beim Outsourcing-Partner) |
| Applikationsadministration - Anlegen von Benutzern | Unternehmen/Behörde (nach internem Genehmigungsprozess) |
| Applikationsadministration - Verwalten von Berechtigungen | Unternehmen/Behörde (nach internem Genehmigungsprozess) |
| Einspielen von Updates und Patches | Outsourcing-Partner |

**Erläuterungen:**

- In der Regel erfolgt der Betrieb der Rechner und die Basis-Administration des SAP Systems durch den Outsourcing-Partner. Die Applikationsverwaltung und -administration erfolgt in der Regel durch den Outsourcing-Auftraggeber. Es ist zu beachten, dass der Outsourcing-Partner über die applikationsspezifischen (Sicherheits-) Anforderungen informiert wird. Nur so kann eine adäquate Basis-Administration erfolgen.
- Es sollten regelmäßige Abstimmungen für den Bereich Sicherheit erfolgen. Dabei können geänderte Anforderungen des Outsourcing-Auftraggebers und Vorschläge des Outsourcing-Partners zum Erhöhen der Sicherheit diskutiert werden.
- Im Rahmen der Risikobetrachtung ist zu bedenken, dass der Outsourcing-Partner volle Kontrolle über die Daten des betriebenen SAP Systems hat. Dies ist aus Sicherheitssicht für alle Behörden und Unternehmen kritisch zu betrachten. Die Verfügbarkeit entsprechender Kontrollen wird beispielsweise auch im Sarbanes Oxley Umfeld geprüft.
- Werden sensitive Daten verarbeitet, die eine besondere Sorgfaltspflicht implizieren, die sich auch aus gesetzlichen Vorgaben ableiten oder explizit gefordert sind, so muss auch der Outsourcing-Partner entsprechend in die Pflicht genommen werden. Der Outsourcing-Partner muss dann durch eine entsprechende Geheimhaltungsverpflichtung rechtlich gebunden werden.
- Für die Benutzer- und Berechtigungsverwaltung ist es sinnvoll, dass ein Mitarbeiter des Outsourcing-Auftragnehmers in den Prozess der Berechtigungsplanung eingebunden ist, denn nur so kann der Outsourcing-Partner beispielsweise den applikationsbezogenen Sicherheitsansprüchen Rechnung tragen. Outsourcing-Szenario keine Berechtigungen angesammelt werden können?

Prüffragen:

- Liegt ein adäquates Outsourcing-Konzept für das SAP System vor?
- Sind alle Aufgaben und Verantwortlichkeiten beim Outsourcing von SAP Systemen für Auftraggeber und -nehmer klar festgelegt?
- Ist der Outsourcing-Partner über die applikationsspezifischen (Sicherheits-) Anforderungen informiert?
- Werden regelmäßige Abstimmungen für den Bereich Sicherheit zwischen dem Outsourcing-Auftraggeber und dem Outsourcing-Partner durchgeführt?
- Ist gewährleistet, dass der Outsourcing-Auftragnehmer in den Prozess der Berechtigungsplanung eingebunden ist?

# M 2.346 Nutzung der SAP Dokumentation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler, Leiter IT

SAP stellt eine Vielzahl von Dokumenten und Informationen zur Verfügung. Die verfügbare Dokumentation muss insbesondere Administratoren bekannt sein und regelmäßig auf Aktualisierungen geprüft werden.

SAP stellt Informationen zentral über den SAP Service Marketplace (http://service.sap.com) zur Verfügung. Es ist zu beachten, dass zum Zugriff JavaScript im Browser aktiviert sein muss und meist eine Authentisierung erfolgen muss. Eine Ausnahme bildet das SAP Help Portal, über das die Produkt-Dokumentationen erhältlich sind.

Der SAP Service Marktplatz verweist auf weitere Informationsquellen. Im Folgenden werden einige Beispiele genannt:

- Über den SAP Service Marktplatz werden SAP Hinweise oder zusätzliche Software angeboten. Wichtig sind hier auch die sicherheitsrelevanten Informationen, die unter dem Quicklink "/security" zu finden sind. Hier kann auch der SAP Security Newsletter abonniert werden, über den sicherheitsrelevante Informationen per E-Mail verteilt werden. Wichtig sind außerdem die SAP Produkt-Sicherheitsleitfäden, die unter dem Quicklink "/securityguide" angeboten werden. Im vorliegenden Kontext ist insbesondere der SAP NetWeaver Sicherheitsleitfaden relevant.
- Über das SAP Help Portal (http://help.sap.com) sind für alle Produkte Anleitungen und umfangreiche Dokumentationen verfügbar.
- Das SAP Developer Network (http://sdn.sap.com) ist als Informationsquelle für Entwickler gedacht. Hier ist eine kostenfreie Registrierung notwendig.

Im Folgenden sind die relevanten SAP Dokumente für die einzelnen Maßnahmen des vorliegenden Bausteines angegeben. Die Dokumente finden sich, wenn nicht anders angegeben, im SAP Help Portal.

### M 2.341 Planung des SAP Einsatzes

Detailinformationen zur Benutzerverwaltung in SAP Systemen finden sich im SAP Dokument "Identity Management", Kapitel "Benutzer und Rollen (BC-Sec-USR)", in den Abschnitten "Benutzerpflege" und "Zentrale Benutzerverwaltung" sowie im Abschnitt "User Management Engine".

SAP bietet zum Thema Ressourcen-Planung (auch "Sizing" genannt) umfangreiche Informationen auf dem Service Marktplatz an. Unter dem Stichwort "Solution Life-Cycle Management" finden sich unter anderem die Themen "Quick Sizer Tool" und "Sizing Guidelines". Diese Informationen helfen, die Ressourcen-Planung durchzuführen.

SystemlandschaftDetaillierte Hinweise zur empfohlenen Systemlandschaft finden sich in der Regel in den Sicherheitsleitfäden zu den einzelnen SAP Produkten, die auf dem SAP Service Marktplatz unter dem Kürzel "securityguide" zu finden sind.

Detailinformationen zum Transportsystem finden sich im SAP Dokument "SAP NetWeave Technical Operations Manual" in den Abschnitten "Software Change Management" der ABAP- und Java-Stack-Beschreibungen.

**M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme**

Detaillierte Informationen zum Audit Information System (AIS) finden sich im SAP Hinweis 451960.

**M 2.342 Planung von SAP Berechtigungen**

Detailinformationen, die bei der Planung des Berechtigungskonzeptes genutzt werden können, finden sich im SAP Dokument "Identity Management", Kapitel "Benutzer und Rollen (BC-Sec-USR)", im Abschnitt "SAP Berechtigungskonzept".

**M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme**

Weitere Hinweise zu Debugging-Berechtigungen finden sich in den SAP Hinweisen 13202 und 65968.

**M 4.256 Sichere Installation von SAP Systemen**

Weitere Detail-Informationen zur Betriebssystemabsicherung sind im SAP Dokument "SAP NetWeaver Security Guide" in den Abschnitten "SAP System Security Under UNIX/LINUX" und "SAP System Security Under Windows" enthalten.

**M 4.258 Sichere Konfiguration des SAP ABAP-Stacks**

Im SAP Dokument "Customizing (BC-CUS)" findet sich im Abschnitt "Einführungsleitfaden (IMG)" die IMG Dokumentation, die beim Einführungsleitfaden zu beachten ist.

Detailinformationen zum Umgang mit Profilen finden sich im SAP Dokument "Konfiguration" im Abschnitt "Profile".

Detaillierte Informationen zum Thema Systemänderbarkeit finden sich im SAP Dokument "Transport Organizer (BC-CTS-ORG)" im Abschnitt "Systemänderbarkeit einstellen".

Administratoren müssen sich mit den Auswirkungen der Mandanten-Konfiguration sehr genau vertraut machen. Entsprechende Detail-Dokumentation findet sich im SAP Dokument "Transport Organizer (BC-CTS-ORG)" im Abschnitt "Mandantensteuerung".

Detailbeschreibungen zum Absichern der Betriebssystemkommandos finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "Logical Operating System Commands" sowie im Dokument "Konfiguration" im Abschnitt "Externe Betriebssystem-Kommandos: Inhalt".

Weitere Detailinformationen zu Single Sign-On finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "User Authentication and Single Sign-On" sowie im Dokument "Verwendung von Anmeldetickets".

Weitere Informationen zu SNC finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "Transport Layer Security".

**M 4.259 Sicherer Einsatz der ABAP-Stack Benutzerverwaltung**

Weitere Hinweise zur Benutzerverwaltung in SAP Systemen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Vorgehen bei der Erstinstallation".

Detailhinweise zum Umgang mit Standardbenutzern finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "Protecting Standard Users".

**M 4.260 Berechtigungsverwaltung für SAP Systeme**

Detailhinweise zum Aufbau der Berechtigungsverwaltung und zu relevanten Berechtigungen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Organisation der Berechtigungsverwaltung".

Detailhinweise zur Berechtigungsverwaltung mit dem Profilgenerator finden sich im SAP Dokument "Identity-Management" im Abschnitt "Rollenpflege".

**M 4.261 Sicherer Umgang mit kritischen SAP Berechtigungen**

Allgemeine Hinweise zu Berechtigungsprüfungen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Berechtigungsprüfungen". Bei der Identifikation kritischer Berechtigungen ist entsprechendes Wissen über die zugrunde liegenden Berechtigungsprüfungen notwendig.

Weitere Informationen zu SAP Systemberechtigungen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Schutzmaßnahmen für besondere Profile".

**M 4.262 Konfiguration zusätzlicher SAP Berechtigungsprüfungen**

Weitere Informationen zum Deaktivieren von Berechtigungsprüfungen finden sich im SAP Dokument "Identity-Management" in den Abschnitten "Berechtigungsprüfungen" und "Umfang der Berechtigungsprüfungen verringern".

Weitere Informationen zur Konfiguration von Berechtigungsgruppen finden sich im SAP Dokument "ALV Grid Control (BC-SRV-ALV)" im Abschnitt "Berechtigungsgruppen pflegen und zuordnen".

**M 4.263 Absicherung von SAP Destinationen**

Weitere Detailinformationen zur Zugriffssteuerung auf Destinationen finden sich im SAP Dokument "RCF/ICF Security Guide" im Abschnitt "Controlling Access to RFC Destinations".

**M 4.264 Einschränkung von direkten Tabellenveränderungen in SAP Systemen**

Detailinformationen zu Parameter-Transaktionen finden sich an folgenden Stellen:

- SAP Dokument "RFC Security Guide", Abschnitt "Authorization Object S_TABU_DIS (Table Maintenance)"
- Dokumentation des Einführungsleitfadens (IMG, Transaktion SPRO) unter "SAP Web Application Server/ Systemadministration/ Benutzer und Berechtigungen/ Zeilenbezogene Berechtigungen"
- SAP Dokument "Berechtigungen in mySAP HR" im Abschnitt "Anwendungsübergreifende Berechtigungsobjekte"

Weitere Informationen zu Parametertransaktionen und Berechtigungen im Zusammenhang mit Transaktion SE93 finden sich in folgenden SAP Dokumenten:

- SAP Dokument "ABAP-Programmierung (BC-ABA)", Abschnitt "Parametertransaktion"

- SAP Dokument "Identity-Management", Abschnitt "Berechtigungsprüfungen"

**M 4.265 Sichere Konfiguration der Batch-Verarbeitung im SAP System**

Weitere Details zur Batch-Verarbeitung finden sich im SAP Dokument "Hintergrundverarbeitung" im Abschnitt "Berechtigungen für die Hintergrundverarbeitung".

**M 4.266 Sichere Konfiguration des SAP Java-Stacks**

Hinweise zu den Java-Stack-Diensten und deren Funktion finden sich in den jeweiligen Handbüchern, wie etwa dem SAP Dokument "Technisches Betriebshandbuch für SAP NetWeaver" im Abschnitt "Administration des SAP Web Application Server (JAVA)" sowie in den zugehörigen Dokumenten "Architekturhandbuch", "Administrationshandbuch" und "Entwicklerhandbuch".

Der SAP Hinweis 606733 bietet zur HTTP PUT Problematik weitere Detailinformationen an.

**M 4.269 Sichere Konfiguration der SAP System Datenbank**

Die SAP Empfehlungen zur Absicherung der Datenbank finden sich im SAP Dokument "Operating System and Database Platform Security Guides" im Abschnitt " Database Access Protection". Die Empfehlungen erfolgen für die unterschiedlichen Datenbankprodukte.

**M 4.270 SAP Protokollierung**

Detailbeschreibungen zu den Systemüberwachungsfunktionen finden sich im SAP Dokument "Werkzeuge zur Systemüberwachung".

Weitere Informationen zur Änderungsverfolgung sind im SAP Hinweis 1916 und den darin referenzierten Hinweisen zu finden.

**M 4.271 Virenschutz für SAP Systeme**

Weitere Detailinformationen zur Schnittstelle für Computer-Viren-Schutzprogramme finden sich im SAP Dokument "Viren-Scan-Schnittstelle". Hinweise zu Produkten, die über die Schnittstelle angebunden werden können, finden sich auf dem SAP Service Marktplatz unter dem Quicklink "securitypartners" unter "Partners for Virus Scan interface (NW-VSI)".

**M 4.272 Sichere Nutzung des SAP Transportsystems**

Detailinformationen zum Transportmanagementsystem finden sich im SAP Dokument "Change and Transport System - Überblick (BC-CTS)" und "Transport Management System (BC-CTS-TMS)".

**M 4.273 Sichere Nutzung der SAP Java-Stack Software-Verteilung**

Weitere Detailinformationen zur Software-Verteilung im SAP Java-Stack finden sich im SAP Dokument "SAP NetWeaver Java Development Infrastructure".

**M 5.125 Absicherung der Kommunikation von und zu SAP Systemen**

Detailhinweise zur SNC-Konfiguration finden sich in den SAP Dokumenten "Administration Manual" im Abschnitt "Configuring SNC (SAP J2EE Engine to ABAP Engine)". Weitere Hinweise finden sich im SAP Dokument "Network

and Transport Layer Security" im Abschnitt "Secure Network Communications (SNC)".

Detaillierte Anleitung zur Installation und Konfiguration von SSL finden sich im SAP Dokument "Systemsicherheit" im Abschnitt "SAP Web AS für SSL-Unterstützung konfigurieren" und im SAP Dokument "Administration Manual" im Abschnitt "Configuring the Use of SSL on the SAP J2EE Engine". Informationen über den SSL-Schutz bei internen LDAP Zugriffen des Java-Stacks sind im Dokument "Configuring SSL Between UME and LDAP Directory (SAP NW`04)" beschrieben.

**M 5.126 Absicherung der SAP RFC-Schnittstelle**

Detailhinweise zur RFC-Kommunikation finden sich im SAP Dokument "RFC/ ICF Security Guide" im Abschnitt "RFC Scenarios".

Weitere Informationen zum Thema "Trusted Systems" finden sich in den SAP Dokumenten "RFC/ICF Security Guide" im Abschnitt "Authorization Object S_RFCACL" und im Dokument "Komponenten der SAP Kommunikationstechnologie" im Kapitel "RFC" im Abschnitt "Trusted System: Vertrauensbeziehungen zwischen SAP Systemen".

Weitere Detailinformationen zur sideinfo Datei finden sich im SAP Dokument "Komponenten der SAP Kommunikationstechnologie" im Abschnitt "Introduction to RFC Client Programs" und im Dokument "SAP Gateway" im Abschnitt "Side-Information-Tabellen".

Detailinformationen zu externen RFC-Servern finden sich im SAP Dokument "RFC/ICF Security Guide" in den Abschnitten "Security Measures - Overview (RFC)" und "RFC Communication between SAP Systems and External (Non-SAP) Systems". Informationen zum RFC SDK finden sich im Dokument "Komponenten der SAP Kommunikationstechnologie" im Abschnitt "The RFC API" und im Abschnitt "Contents of the RFC SDK".

Nähere Informationen zum SAP Gateway finden sich im SAP Dokument "SAP Gateway" im Abschnitt "Sicherheitseinstellungen beim SAP Gateway".

**M 5.127 SAP Internet Connection Framework (ICF) absichern**

Weitere Detailinformationen zum ICF finden sich im SAP Dokument "Komponenten der SAP-Kommunikationstechnologie" im Kapitel "Internet Communication Framework" im Abschnitt "Administration: HTTP Kommunikation mit dem SAP-System als Server" und im SAP Dokument "RFC/ICF Security Guide" im Abschnitt "ICF Scenarios".

**M 5.128 Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle**

Weitere Informationen zur Absicherung der ALE-Schnittstelle finden sich im SAP Dokument "Security Guide ALE (ALE Applications)".

**M 5.129 Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen**

Weitere Detailinformationen zur SOAP-Schnittstelle finden sich im SAP Dokument "Komponenten der SAP-Kommunikationstechnologie" im Abschnitt "SOAP Framework" des Kapitels "Internet Communication Framework".

Weitere Hinweise zur Content-Server-Schnittstelle finden sich im SAP Dokument "SAP Content-Server Security Guide" und im Dokument "Knowled-

ge Provider (BC-SRV_KPR)" im Abschnitt "SAP Content Server HTTP 4.5 Schnittstelle".

**M 6.97 Notfallvorsorge für SAP Systeme**

Detaillierte Hinweise zum Backup finden sich im "SAP NetWeaver Technical Operations Manual". Für den ABAP-Stack in den Abschnitten "Sicherung und Wiederherstellung" sowie "Erstellen einer homogenen Systemkopie", für den Java-Stack im Abschnitt "Sicherung und Wiederherstellung des SAP Web Application Server (Java)".

Prüffragen:

- Sind den Administratoren die von SAP zur Verfügung gestellten Dokumente bekannt?
- Werden die von SAP zur Verfügung gestellten Dokumente regelmäßig auf Aktualisierungen geprüft?

# M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Revisor

Die Sicherheit eines SAP Systems kann nur dann auf Dauer gewährleistet werden, wenn dieses regelmäßig geprüft wird. Auf diese Weise können Fehlkonfigurationen und Schwachstellen aufgedeckt und behoben werden.

Sicherheitsprüfungen sollten in regelmäßigen Abständen durch unterschiedliche Personen erfolgen. So sollten beispielsweise Administratoren in relativ kurzen Abständen (etwa monatlich) Kurzprüfungen durchführen. Es empfiehlt sich dabei, eine Prüfliste aufzubauen, damit ein definierter Prüfumfang gewährleistet ist. Festgestellte kleinere Probleme können meist sofort durch die Administratoren korrigiert werden, größere Probleme sind entsprechend der Prozessvorgaben weiterzumelden. In mittleren Zeitabständen (mehrere Monate) sollten Sicherheitsprüfungen durch andere, interne Rollen (z. B. Informationssicherheit, IT-Revision) erfolgen. In längeren Zeitabständen können dann auch Prüfungen durch externe Prüfer sinnvoll sein. Folgende Aspekte sind bei Prüfungen zu berücksichtigen:

### Regelmäßige Recherche von sicherheitsrelevanten Informationen

Generell müssen sich Administratoren und für die Informationssicherheit verantwortliche Personen regelmäßig über Neuerungen und Änderungen informieren, die die verantworteten Systeme betreffen. Dazu sind insbesondere die SAP Informationsquellen regelmäßig zu sichten.

Siehe dazu auch M 2.346 *Nutzung der SAP Dokumentation*.

### Berechtigungen für Revisionsbenutzer

Für das SAP Benutzerkonto, das zur Prüfung der Systemkonfiguration durch externe Personen genutzt wird, sollten nur lesende Berechtigungen vergeben sein. Veränderungen dürfen durch den Revisionsbenutzer nicht durchgeführt werden. Im ABAP-Stack darf dem Revisionsbenutzer nicht das Profil SAP_ALL zugeordnet werden.

Können die Berechtigungen des Revisionsbenutzers nicht auf den lesenden Zugriff beschränkt werden, so darf der Zugriff nur im 4-Augen-Prinzip erfolgen.

SAP bietet ein eigenes Audit System (Audit Information System, AIS) an, das es Revisoren ermöglicht, ein SAP System zu untersuchen. Dabei sind bereits unterschiedliche Rollen und Berechtigungen verfügbar, die dem Benutzerkonto des Revisionsbenutzers zugeordnet werden können. Die verfügbaren Rollen sind in der Regel so gestaltet, dass nur lesender Zugriff besteht. Die Rollen können im Profilgenerator (Transaktion PFCG) über die Suche "SAP*AUDITOR*" eingesehen werden.

### Zugriff auf AIS konfigurieren

Für die Prüfung kann das Audit Information System (AIS) eingesetzt werden. Das AIS liegt in unterschiedlichen Versionen vor: als Transaktion SECR und in der rollenbasierten Version.

Über die Transaktion SECR können Prüfungen teilweise automatisiert erfolgen. Das AIS erlaubt es außerdem, das Prüfergebnis zu dokumentieren und den Prüfstatus (Ampel-Status: rot, gelb, grün) vorzuhalten.

Es empfiehlt sich, eine Untermenge der angebotenen Prüfmöglichkeiten zu definieren (Top 10 Security Reports) und diese abzuarbeiten. Dabei ist die festgestellte Ist-Konfiguration gegen die Soll-Konfiguration zu prüfen.

Es ist zu bedenken, dass das AIS kritische Systeminformationen preisgibt. Der Zugriff muss daher auf die berechtigten Prüfer eingeschränkt werden (S_TCODE, Transaktion SECR).

Im Gegensatz zur Transaktion SECR besteht das rollenbasierte AIS aus vorgefertigten Rollen, Berechtigungen und Programmen, die es ermöglichen, einem Benutzer die für ein Audit notwendigen Berechtigungen auf System- und Modul-Ebene zu erteilen. Im Fokus stehen dabei vornehmlich kaufmännische Audits. Das rollenbasierte AIS muss entsprechend eingerichtet und konfiguriert werden.

Detaillierte Informationen dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Prüfen der Veränderungen der Systemänderbarkeit**

Die Einstellungen zur Systemveränderbarkeit sind regelmäßig zu prüfen. Dazu kann die Transaktion SE03 "Administration/Systemänderbarkeit" genutzt werden. Zu prüfen sind die globalen Einstellungen und die Einstellungen für jeden Mandanten. Informationen zur Systemänderbarkeit finden sich auch in M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*.

Für den Java-Stack besteht nicht die Möglichkeit, die Systemänderbarkeit durch Systemeinstellungen zu konfigurieren.

**Security Auditlog**

Das Security Auditlog enthält sicherheitsrelevante Protokoll-Einträge. Eine regelmäßige Auswertung muss daher erfolgen. Für die Auswertung können die Transaktionen SM20, SM20N oder RZ27_Security eingesetzt werden, wobei die Transaktion SM20N aufgrund der besseren Benutzungsschnittstelle zu bevorzugen ist. Um die Transaktionen SM20 und SM20N verwenden zu können, muss vorher mit der Transaktion SM19 der Auswerteumfang definiert und das Auditlog aktiviert werden (siehe auch M 4.270 *SAP Protokollierung*).

**Profilparameter**

Die eingestellten Profilparameter sind gegen die geplanten Soll-Werte zu prüfen (siehe auch M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*). Die gültigen Profilparameter lassen sich auch direkt über die Transaktion SM20N anzeigen. Alternativ kann der Report RSPARAM über die Transaktion SE38 ausgeführt werden.

**Benutzerinformationssystem**

Über das Benutzerinformationssystem (Transaktion SUIM) sollten regelmäßig Prüfungen erfolgen. Folgende Informationen sind dabei sicherheitsrelevant:

- Benutzer mit Falschanmeldungen
  Dies kann auf Angriffsversuche hindeuten.
- Benutzer mit Anmeldedaten und Kennwortänderungen

So lassen sich Benutzer identifizieren, die nie angemeldet sind oder ihr Passwort nicht geändert haben, sofern dies nicht automatisch erzwungen wird.
- Benutzer mit kritischen Kombinationen von Berechtigungen für den Transaktionsstart
  Es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen.
- Benutzer mit kritischen Berechtigungen
  Es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen.
- Änderungsbelege für Benutzer, Rollenzuordnungen, Rollen, Profile und Berechtigungen
  Hierbei ist insbesondere auf Änderungen an administrativen Objekten zu prüfen.

**Erreichbare SAP Gateways**

Über die Transaktion RSGWLST können die von einem SAP System erreichbaren SAP Gateways anderer SAP Systeme bestimmt werden. Dies zeigt die Verbindungs- und Zugriffsmöglichkeiten auf. Es können die Einstellungen der Datei "secinfo" der entfernten Gateways eingesehen werden, über die die Autorisierungen zum Ansprechen und Registrieren des entfernten SAP Gateways definiert werden. Zusätzlich können die Destinationen und die registrierten RFC-Server-Programme der ansprechbaren entfernten SAP Gateways abgeprüft werden.

Die Auswertung erfordert jedoch entsprechende technische Kenntnisse. Da über die Transaktion RSGWLST auch sensitive Systeminformationen erlangt werden können, muss die Transaktion zugriffsbeschränkt werden.

Der Status des SAP Gateways des lokalen Systems kann über die Transaktion SMGW (Gateway Monitor) geprüft werden.

**Prüfen der Single Sign-On (SSO) Möglichkeiten**

Benutzer können sich an einem SAP System zunächst mit gültigen Authentisierungsinformationen (z. B. Benutzername/Passwort, Zertifikat) anmelden und dann über den SSO Mechanismus ohne erneute Eingabe von Authentisierungsinformationen auf andere SAP Systeme zugreifen.

Über die Transaktion STRUST können die Zertifikate anderer SAP Systeme eingesehen werden, die das lokale SAP System bei SSO-Zugriffen akzeptiert. Hier sollten nur vertrauenswürdige Systeme eingetragen sein. Alternativ kann die Prüfung auch über die Transaktionen SSO2 oder SSO2_ADMIN erfolgen.

**Regelmäßige Prüfung der Berechtigungen**

Das vollständige Prüfen von Berechtigungen ist in der Regel aufgrund des Mengengerüstes nicht manuell möglich. Daher ist ein gutes Berechtigungskonzept unbedingt notwendig. Aber auch dann müssen die Berechtigungen regelmäßig auf Konsistenz mit dem Berechtigungskonzept geprüft werden. Hier können Stichproben (siehe auch "Benutzerinformationssystem" oben) für wichtige Benutzergruppen durchgeführt werden. Das Berechtigungskonzept muss sicherstellen, dass Prozesse aufgesetzt sind, die verhindern, dass Berechtigungen angesammelt werden.

Zusätzlich können Werkzeuge zum Einsatz kommen, die ein integriertes Änderungs- und Risikomanagement anbieten, so dass beispielsweise die Möglichkeit des Betrugs durch Benutzer aufgrund von Berechtigungsproblemen verringert werden kann. SAP bietet dazu den so genannten "SAP GRC Access Control" an, der die konfigurierten Berechtigungen dahingehend prüft,

ob Benutzer Berechtigungen besitzen, die aus Sicherheitssicht als kritisch zu betrachten sind. Solche Prüfungen finden typischerweise auch im Sarbanes-Oxley-Umfeld statt, sind generell jedoch für jede Behörde oder jedes Unternehmen sinnvoll. Die Prüfung muss die unter diesen Gesichtspunkten kritischen Berechtigungen für Transaktionen (wie etwa SE80, SE16, SQVI oder kritische Autorisierungsobjekte für Benutzer, beispielsweise S_PROGRAM, S_USER_GRP, S_TABU_DIS, S_RFC, S_USR_RFC) erkennen und anzeigen. Ähnliche Prüfwerkzeuge sind auch von Drittherstellern erhältlich.

**Aktualität der Updates prüfen**

Für das SAP System ist die Aktualität der installierten Updates zu prüfen. Dazu kann die Transaktion SPAM eingesetzt werden. Der aktuelle Patch-Stand des Systems muss dann mit den verfügbaren Patches verglichen werden. Dies erfordert, dass dem Prüfer die von SAP verfügbaren Patches bekannt sind.

Die Prüfung muss auch auf Fehler oder Warnungen bei Updates erfolgen. Dabei ist zu beachten, dass Warnungen auch dann existieren können, wenn der Update-Status auf "grün" steht.

**Sicherheit der Kommunikationsschnittstellen prüfen**

Die Sicherheit der unterschiedlichen Kommunikationsschnittstellen (siehe auch M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*) sollte geprüft werden. Dies betrifft beispielsweise die RFC-, ICF- und ALE-Schnittstellen des ABAP-Stack und die Schnittstellen des Java-Stacks.

Hier ist insbesondere zu prüfen, wer administrative Berechtigungen besitzt und welche Dienste und Funktionen verfügbar sind.

Prüffragen:

- Werden im SAP System in regelmäßigen Abständen Sicherheitsprüfungen mit definiertem Prüfumfang durchgeführt?
- Werden im SAP System die Einstellungen zur Systemänderbarkeit (globale Einstellungen, Einstellungen für jeden Mandanten) regelmäßig geprüft?
- Erfolgt eine regelmäßige Auswertung des Security Auditlog im SAP System?
- Werden die eingestellten Profilparameter im SAP System gegen die geplanten Soll-Werte geprüft?
- Erfolgt im SAP System regelmäßig eine Prüfung zum Benutzerinformationssystem?
- Werden im SAP System die Berechtigungen regelmäßig auf Konsistenz mit dem Berechtigungskonzept geprüft?
- Wird für das SAP System die Aktualität der installierten Updates geprüft?
- Werden im SAP System die Kommunikationsschnittstellen (z. B. RFC, ICF und ALE) geprüft, insbesondere wer administrative Berechtigungen besitzt und welche Dienste und Funktionen verfügbar sind?

# M 2.348 Sicherheit beim Customizing von SAP Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Im Rahmen des Customizings wird ein SAP System so konfiguriert und angepasst, dass es die gewünschte Unterstützung für die Institution anbieten kann. Diese Aufgabe ist in der Regel zeitaufwendig. Folgendes ist daher zu bedenken:

- Für das Customizing ist ein entsprechendes Konzept zu erstellen, das den gewünschten Soll-Zustand des SAP Systems möglichst genau beschreibt und auch die Prozesse definiert, nach denen das Customizing durchgeführt wird.
- Für das Konzept ist eine Anforderungsanalyse notwendig. Dabei muss festgelegt werden, welche Anpassungen durch das Customizing erfolgen müssen, damit das gewünschte System-Verhalten erreicht wird (siehe auch M 2.341 *Planung des SAP Einsatzes*.
- Im Rahmen des Customizing-Prozesses sind Rückmelde-Prozesse einzusetzen, die Anpassungen des Konzeptes während der Umsetzung (siehe auch M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*) erlauben.
- Das Customizing darf nur von sachkundigen und vertrauenswürdigen Personen durchgeführt werden.
- Anpassungen der Konfigurationen sollten nicht im Produktiv-System erfolgen, sondern über das Transportsystem kontrolliert eingespielt werden.

Prüffragen:

- Ist für das Customizing ein Konzept erstellt worden, das den gewünschten Soll-Zustand des SAP Systems beschreibt und auch die Prozesse definiert, nach denen das Customizing durchgeführt wird?
- Wird das Customizing von SAP Systemen von sachkundigen und vertrauenswürdigen Personen durchgeführt?
- Werden am SAP System Anpassungen der Konfiguration über das Transportsystem kontrolliert eingespielt?

# M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Um ein SAP System an die spezifischen Bedürfnisse eines Unternehmens oder einer Behörde anzupassen, kann die Funktion des Systems durch Eigenentwicklungen verändert oder erweitert werden. Folgendes muss aus Sicherheitssicht bei der Software-Entwicklung für SAP Systeme beachtet werden:

### Software-Entwicklungsprozess

Für den Software-Entwicklungsprozess sollten als Grundlage die Empfehlungen aus M 2.378 *System-Entwicklung* umgesetzt werden.

### Entwickler in Produktiv-Systemen

Da Produktiv-Systeme schützenswerte System- und Geschäftsdaten enthalten, dürfen Entwickler keinen Zugriff auf die Produktiv-Systeme erhalten. Insbesondere darf kein Debugging im Produktiv-System erfolgen. Fehleranalysen müssen im Entwicklungssystem durchgeführt werden. Dies bedeutet für den ABAP-Stack, dass kein Benutzer mit der Berechtigung S_DEVELOP ausgestattet werden darf. Die Werkzeuge CATT und eCATT (ABAP-Stack) oder Remote-Debugging der Engine (Java-Stack) dürfen in Produktiv-Systemen nicht genutzt werden. Dies ist durch die Mandanten- bzw. Java-Stack-Konfiguration auszuschließen.

In besonders begründeten Ausnahmefällen, in denen Entwickler Fehleranalysen nur in Produktiv-Systemen durchführen können, dürfen diesen temporär Anzeigeberechtigungen und Debugging-Berechtigungen ohne Modifikationsmöglichkeiten eingeräumt werden. Die Sicherheit ist durch zusätzliche organisatorische Maßnahmen entsprechend zu unterstützen.

Weitere Hinweise zu diesem Thema finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Direktes Einspielen neuer Software in das Produktiv-System durch Entwickler muss durch ein mehrstufiges Software-Freigabe-Konzept unterbunden werden (siehe M 4.272 *Sichere Nutzung des SAP Transportsystems* und M 4.273 *Sichere Nutzung der SAP Java-Stack Software-Verteilung*).

### Sicherheitsvorgaben bei Eigenentwicklungen

Die Entwickler sollten durch geeignete Sicherheitsvorgaben unterstützt werden. Nur wenn konkrete Anforderungen oder Rahmenbedingen bekannt sind, kann ein Entwickler diese in der Programmierung berücksichtigen. Empfehlenswert sind unter anderem die folgenden Vorgaben:

- ABAP-Code muss immer Berechtigungen prüfen.
- Die eigenen und verwendeten Berechtigungsobjekte im ABAP-Code sind zu dokumentieren und müssen über die Transaktion SU24 für den Profilgenerator eingepflegt werden (siehe auch M 2.342 *Planung von SAP Berechtigungen*).
- Für Java-Code sind die benutzten Dienste zu dokumentieren.
- Die verwendeten Rollen und Vorgaben an die so genannten "Security Constraints" (d. h. welche Rollen für den Zugriff auf Applikationsfunktionen notwendig sind) sind für Java-Applikationen zu dokumentieren.

- Für ABAP-Programme sollte der ABAP Code Inspector (Transaktion SCI) eingesetzt werden, um eigene Programme unter anderem auf Sicherheit und das Einhalten der SAP Namenskonventionen zu prüfen. Dies gilt insbesondere dann, wenn keine anderen Werkzeuge genutzt werden, um sicherheitsrelevante Kontrollen von ABAP-Programmen durchzuführen.

**Sicherheit bei Fremdanwendungen**

Software, die durch Dritte entwickelt wurde, darf nur nach einem sorgfältigen Abnahmeprozess im SAP System installiert werden. Im Abnahmeprozess sind auch Sicherheitsprüfungen durchzuführen. Die Sicherheitsanforderungen sind im Pflichtenheft detailliert zu beschreiben. Nur so kann die gewünschte Sicherheit der Anwendung umgesetzt werden.

Prüffragen:

- Ist sichergestellt, dass die Entwickler keinen Zugriff auf das SAP Produktiv-System haben?
- Existiert ein mehrstufiges Software-Freigabe-Konzept, das ein direktes Einspielen neuer Software in das SAP Produktiv-System durch Entwickler unterbindet?
- Existieren für die Entwicklung von SAP Programmen geeignete Sicherheitsvorgaben (konkrete Anforderungen und Rahmenbedingungen), die den Entwickler unterstützen?

# M 2.350 Aussonderung von SAP Systemen

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wird entschieden, ein SAP System nicht weiter zu betreiben, weil es beispielsweise durch eine neuere Systemversion auf neuer Hardware abgelöst wird, so sind die nachfolgend beschriebenen Punkte zu beachten. Die Maßnahmen sollen verhindern, dass ein Angreifer die freigewordene Identität des SAP Systems missbrauchen kann. Der Aussonderungsprozess muss also dafür Sorge tragen, dass die Identität des SAP Systems gelöscht und unbrauchbar wird.

### Löschen/Entsorgen der Speichermedien

Die Speichermedien aller betroffenen Rechner sind vor der Wiederverwendung sicher zu löschen (siehe M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*). Wird die Hardware entsorgt, so muss dies ebenfalls auf sichere Weise geschehen (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*).

### System aus dem SAP Verbund löschen

In der Regel ist ein SAP System in einen SAP Verbund eingebunden. Andere Systeme besitzen daher Referenzen auf das auszusondernde System.

Alle Referenzen auf das ausgesonderte System in anderen SAP Systemen oder Komponenten müssen gelöscht werden. Dies betrifft unter anderem

- Identitäten (d. h. technische Benutzer), unter denen das ausgesonderte System zugreift,
- Vertrauensstellungen,
- Destinationen,
- Konfigurationen des Transportsystems,
- Konfigurationen der zentralen Benutzerverwaltung,
- Konfigurationen der Systemüberwachung (Monitoring).

Es muss beachtet werden, dass dabei auch Referenzen in Systemen externer Partner betroffen sein können. Der Aussonderungsprozess muss daher auch dafür sorgen, dass entsprechende Prozesse bei betroffenen externen Partnern angestoßen werden.

### System aus dem Netzverbund löschen

Alle Referenzen auf Netz- und Betriebssystem-Ebene sind zu löschen. Dies betrifft unter anderem

- DNS-Einträge,
- Firewall-Regeln,
- SAPGui/SAPLogon-Konfiguration (Systemlisten),
- Einträge in "host" und "services" Dateien.

Für die Listen verfügbarer Systeme für das SAP Logon - diese werden in der Datei saplogon.ini gespeichert - empfiehlt es sich, eine zentrale Verwaltung zu nutzen und die Datei auf die Clients zu verteilen.

Prüffragen:

- Werden die Speichermedien aller betroffenen Rechner von SAP Systemen vor der Wiederverwendung oder Aussonderung sicher gelöscht?
- Sind bei der Aussonderung von SAP Systemen alle Referenzen auf das ausgesonderte System in anderen SAP Systemen oder Komponenten gelöscht?
- Werden bei der Aussonderung von SAP Systemen auch alle Referenzen auf Netz- und Betriebssystem-Ebene gelöscht?

# M 2.351 Planung von Speicherlösungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die grundsätzliche Entscheidung, welche Art von Speicherlösung angemessen für die Institution ist, muss durch eine Anforderungsanalyse getroffen werden. Zunächst ist festzustellen, welche Anwendungen von der Speicherlösung zukünftig unterstützt werden sollen und welche vorhandene Hardware durch eine neue Speicherlösung unterstützt oder abgelöst werden soll.

Maßgebliche Kenngrößen sind die Anforderungen an Verfügbarkeit, Performance und Kapazität. Bei normalen Verfügbarkeitsanforderungen sollte zudem geprüft werden, welche Komplexität für die Institution tragbar ist. Die Einführung von SAN-Lösungen bedeutet, dass eine neue Basistechnik eingeführt wird. Damit ist ein entsprechender Aufwand zur Planung und Einführung dieser Technik zu kalkulieren. Beim geplanten Einsatz von Speicherlösungen in virtualisierten Serverumgebungen sind beispielsweise zusätzliche Aspekte wie die Gewährleistung einer eineindeutigen WWN- oder Netzadressvergabe zu beachten, deren Umsetzung zusätzlichen Aufwand generiert.

NAS-Lösungen sind besonders auf die einfache Integration in etablierte IT-Umgebungen und auf den dateiorientierten Zugriff ausgerichtet. Ihr Einsatz ist daher dann angezeigt, wenn Dateien und dateiorientierte Anwendungen auf zentrale hochwertigere, aber dennoch eher einfach zu administrierende Speicherlösungen konsolidiert werden sollen.

Wenn kurzfristig Speicherplatz auf Servern durch zentralen Speicher ersetzt werden soll, langfristig jedoch höhere Verfügbarkeitsanforderungen zu erwarten sind, kann auch der Einsatz von Speicherlösungen erwogen werden, die eine Mischform von SAN und NAS darstellen. Sogenannte Hybrid-Speicherlösungen lassen sich in erster Ausbaustufe als (sehr hochwertige) NAS-Lösungen betreiben. Durch Aufrüstung interner Komponenten können sie zu SAN-Lösungen für weitere Server und bei Bedarf zu redundanten Speichernetzen ausgebaut werden.

Wenn die Schutzbedarfsfeststellung für eines dieser betrachteten Systeme sofort oder in absehbarer Zukunft ergibt, dass hoher oder sogar sehr hoher Schutzbedarf in Bezug auf Verfügbarkeit vorliegt, sodass eine redundante Datenspeicherung an verschiedenen Standorten erforderlich ist, dann sollte SAN-Technik eingesetzt werden. In diesem Fall sollte dringend darauf geachtet werden, dass die Speicherlösung SAN-Protokolle unterstützt. Mit dieser Technik lassen sich vollständig redundante und hochverfügbare Speicherlösungen aufbauen.

Die Entscheidung für den Einsatz einer bestimmten Speicherlösung, beispielsweise NAS oder SAN, ist auf geeignete Weise zu dokumentieren. Innerhalb der Institution empfiehlt sich daher bereits im Verlauf der Planungs- und Konzeptionsphase einer Speicherlösung die Erstellung eines fachlichen Grobkonzeptes. Dieses sollte alle Aspekte betrachten, die Gegenstand dieser Maßnahme sind, also unter anderem die Anforderungen an die Speicherlösung, die Auswahl von Hardware und Lieferanten, Planung der Infrastruktur etc. Darüber hinaus ist ein Sicherheitskonzept für den Einsatz von Speicherlösungen zu erstellen.

Es ist ebenfalls im Rahmen der Planung zu regeln, wie die aufzubauende Speicherlösung in die bestehenden Betriebsprozesse integriert werden kann. Auf diesem Weg ist bereits zu einem frühen Zeitpunkt erkennbar, wie bestehende Prozesse angepasst und verändert werden müssen. Verzögerungen in der Umsetzungs- und Betriebsphase können damit vermieden oder zumindest reduziert werden.

Sofern nicht bereits an einer übergeordneten Stelle erfolgt, sollte im Rahmen der Planungsaktivitäten einer Speicherlösung auch festgehalten werden, wie mit der Versionierung eingesetzter Software zu verfahren ist. Dies verhindert spätere Verstöße gegen bestehende Kompatibilitätsmatrizen und bietet der Institution bei Bekanntwerden von Schwachstellen oder kritischen Fehlern die Möglichkeit, schnell zu erkennen, ob Handlungsbedarf besteht.

**Auswahl der Hardware**

Entscheidende Kenngrößen bei der Auswahl der Speicherlösung sind:

- der derzeitige und der prognostizierte Bedarf an Speicherplatz, der durch Anwendungen definiert wird (Kapazitätsanforderungen),
- die Anforderungen der Anwendungen an die Geschwindigkeit der Speicherzugriffe (Performanceanforderungen),
- die Anforderungen an die Ausfallsicherheit für die Anwendungen (Verfügbarkeitsanforderungen),
- die Anforderungen an die Vertraulichkeit und Integrität der zu verarbeitenden Daten als Entscheidungsgrundlage für den möglichen Einsatz hardwarenaher Verschlüsselungsmechanismen (Sicherheitsanforderungen)
- Möglichkeit zum Einsatz von Secure Operating Systemen. Solche speziellen Betriebssysteme können die Komplexität von Sicherheitskonfigurationen reduzieren und zudem dazu beitragen, den manuellen Verwaltungsaufwand und die Fehlerwahrscheinlichkeit zu senken.

Es ist für die Planung von Speicherlösungen zu erfassen, welche Geschäftsprozesse und Anwendungen in der Institution die Speicherlösung sofort und in Zukunft nutzen werden und welche Anforderungen bezüglich des Wachstums des Speicherbedarfs, der Performance und der Ausfallsicherheit dadurch gestellt werden. Bei einer solchen Prognose sollte beachtet werden, dass eine solche Schätzung stets sehr großzügig erfolgen sollte. Es zeigt sich immer wieder, dass auch großzügige Schätzungen des zukünftigen Speicherbedarfs in kurzer Zeit von den tatsächlichen Anforderungen übertroffen werden.

Bei der Planung von Speicherlösungen muss auch die erforderliche Datensicherung mit einbezogen werden, denn die Abschätzung des Speicherbedarfs bestimmt auch, wie die Datensicherungsumgebung ausgelegt werden muss. Hierbei muss sichergestellt werden, dass auch nach Ausbau der Speicherlösung mit den angeschlossenen Datensicherungsgeräten die Zeiten für Datensicherung und auch für das Wiedereinspielen einer Datensicherung eingehalten werden können, die den Verfügbarkeitsanforderungen der betroffenen Organisationseinheiten genügen.

**Anforderung der Anwendungen**

Speicherlösungen dienen üblicherweise einer Vielzahl von Servern und damit von Anwendungen zur Speicherung ihrer Daten. Die Anforderungen an die Speicherlösung in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit werden durch die Anwendung mit dem höchsten Schutzbedarf definiert.

Bei der internen technischen Auslegung eines SANs ist zu prüfen, ob die Verfügbarkeitsanforderungen der Institution an das SAN nahelegen, eine desastertolerante Auslegung (M 2.354 *Einsatz einer hochverfügbaren SAN-Lösung*) zumindest in die Planungen einzubeziehen.

Wenn die Institution Anwendungen betreibt, die besonders hohe Anforderungen an die Vertraulichkeit der Daten stellen, so ist in die Planungen einzubeziehen, dass die Daten sowohl während des Transports im SAN als auch auf den Speichermedien durch Verschlüsselung geschützt werden. Dies ist im Rahmen der ergänzenden Sicherheitsanalyse und Risikoanalyse zu betrachten.

**Auswahl von Produkten/Herstellern/Lieferanten**

Der Einsatz von Produkten verschiedener Generationen oder von verschiedenen Herstellern erhöht im Allgemeinen die Komplexität des Gesamtsystems und kann unter Umständen zu Problemen führen. Daher ist es ratsam, eine Homogenität der Systeme anzustreben. Auch bei der Auswahl der Vertragspartner sollte berücksichtigt werden, dass Probleme, die beim Aufbau, Test und Betrieb entstehen können, in der Regel schneller und effektiver beseitigt werden, wenn nur ein Anbieter involviert ist.

Auf der anderen Seite kann eine starke Abhängigkeit von bestimmten Herstellern oder Lieferanten auch Probleme verursachen. Meistens spielen außerdem auch wirtschaftliche Aspekte bei der Auswahl der Produkte eine wichtige Rolle. Alle diese Faktoren sollten bei der Planung von Neubeschaffungen berücksichtigt werden. Als weiterer Punkt muss beachtet werden, dass Hersteller meistens die einwandfreie Funktion ihrer Lösungen nur für bestimmte Zusammenstellungen von Hard- und Software garantieren und durch Supportleistungen unterstützen. Daher ist es ratsam, auf die Interoperabilitätszertifizierung der Hersteller im Hinblick auf die Einsatzumgebung ihrer Produkte und auf weitergehende verbindliche Aussagen zur Kompatibilität und Interoperabilität von Produkten zu achten. Oft veröffentlichen Hersteller in diesem Zusammenhang sogenannte Kompatibilitätsmatrizen.

Hersteller von Speicherkomponenten erbringen Supportleistungen häufig auch über einen Fernwartungszugang. Bei der Auswahl eines Herstellers sollten die Vorgaben des Herstellers hinsichtlich erforderlicher Wartungsarbeiten ermittelt werden. Ist eine Fernwartung vorgesehen, besteht für die Institution die Notwendigkeit zur Absicherung des Zugangs (M 5.33 *Absicherung von Fernwartung*). Insbesondere sollten die rechtlichen Randbedingungen des Landes beachtet werden, aus dem die Fernwartung erbracht wird, da es sein kann, dass Sicherheitsbehörden wie Nachrichtendienste die Zugangsdaten erhalten können, ohne dass dies dem SAN-Betreiber mitgeteilt wird. Bei weitergehenden Fragen zur Spionageabwehr sollte der Kontakt zu den Verfassungsschutzämtern des Bundes oder der Länder aufgenommen werden.

**Einsatz zentraler Managementsysteme**

Der Einsatz einer gemeinsamen Managementapplikation für die zentrale und einfache Überwachung und Verwaltung von Ressourcen vereinfacht die Administration der Speicherlösung. Insbesondere für größere Speicherlösungen ist der Einsatz eines zentralen Verwaltungssystems für eine effiziente Speicherverwaltung unumgänglich. Der Einsatz von proprietären Verwaltungsmechanismen bei den verschiedenen Produkten machte es bisher schwierig, ein zentrales Management in heterogenen Speicherumgebungen umzusetzen.

Die Verabschiedung des SMI-S (Storage Management Initiative Specification) Standards durch die SNIA (Storage Network Industry Association) bietet Herstellern von Storagekomponenten die Möglichkeit, ihre Produkte auf einfache Weise an zentrale Verwaltungssysteme anzubinden. Daneben bietet SMI-S einen Weg, über heterogene Netze hinweg, Basisfunktionen wie beispielsweise Storage-Provisionierung oder LUN Masking einzusetzen.

Die Version 1.6 von SMI-S beinhaltet zahlreiche Sicherheitsvorgaben, die sich hauptsächlich auf die Gewährleistung von Authentisierungsmechanismen und die Sicherstellung der Vertraulichkeit beziehen. Die Betrachtung weiterer Sicherheitsziele befindet sich in Entwicklung. Die SNIA stellt jeweils detaillierte technische Dokumentationen aller bisherigen Versionen von SMI-S zur Verfügung.

Die SNIA stellt weiterhin Informationen darüber bereit, wie ein gewählter Hersteller SMI-S-konforme Hard- oder Software anbieten kann. Diese Angaben sollten entsprechend bei der Planung der Speicherlösung berücksichtigt werden.

Bei der Planung des Einsatzes von SMI-S sollten mindestens folgende Sicherheitsmechanismen für die Kommunikation zwischen Managementsystem und Speicherlösung eingesetzt werden:

- Verschlüsselung: Einsatz sicherer Verschlüsselungsmechanismen zur vollständigen Verschlüsselung der Kommunikation (siehe Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*)
- Authentisierung: Empfohlen wird der Einsatz von HTTP Digest Access Authentication. HTTP Basic Authentication sollte nur eingesetzt werden, wenn die Authentisierung bereits über HTTPS oder eine andere Verschlüsselungsmethode geschützt wird.

**Planung des Netzanschlusses**

Die interne Vernetzung der SAN-Komponenten und die Anbindung an die Server erfolgen üblicherweise durch ein eigenes Fibre-Channel-Netz. Auch wenn iSCSI genutzt wird, ist aus Gründen der Betriebssicherheit hierfür ein eigenes Netz aufzubauen.

Wenn zur Verwaltung und Kontrolle von NAS-Lösungen oder SAN-Komponenten (Speichergeräte, SAN-Switches etc.) der Anschluss dieser Geräte an ein LAN erforderlich ist, sollte dieses LAN als separates Administrationsnetz betrieben werden. Damit werden folgende Schutzziele verfolgt:

- Administrative Daten und Aktionen können nicht von beliebigen Benutzern belauscht werden.
- Es können Protokolle (insbesondere SNMP Version 1) eingesetzt werden, die bekannt unsicher sind, aber mangels verfügbarer Alternativlösungen zur Überwachung des Betriebs eingesetzt werden müssen.
- Die Rechteverwaltung innerhalb eines solchen Netzes wird übersichtlicher.
- Besondere Kontrollmaßnahmen wie Intrusion-Detection-Systeme können übersichtlicher und effizienter gestaltet werden.

Der Einsatz unsicherer Protokolle sollte vermieden werden und stattdessen SNMP ab Version 3 eingesetzt werden. In der Praxis werden jedoch noch immer Systeme eingesetzt, die Version 3 nicht unterstützen und die daher auf ältere Protokollversionen angewiesen sind. In diesem Fall entstehen zusätzliche Risiken, denen sich die Verantwortlichen bewusst sein müssen. Diese unsicheren Protokolle sollten nur innerhalb eines separaten abgeschotteten Administrationsnetzes eingesetzt werden. Dies sollte aber höchstens eine mit-

telfristige Übergangslösung darstellen, langfristig sollten nur noch Geräte eingesetzt werden, die SNMP-Protokolle ab Version 3 unterstützen.

**Infrastruktur**

Bevor ein SAN angeschafft und in Betrieb genommen wird, müssen verschiedene infrastrukturelle Aspekte in die Planungsmaßnahmen mit aufgenommen werden.

Der Standort der Komponenten eines SANs muss in einem zutrittsgeschützten Serverraum oder einem Rechenzentrum geplant werden. Empfehlungen für die Infrastruktursicherheit von Serverräumen finden sich in Baustein B 2.4 *Serverraum*, die Anforderungen an Rechenzentren in Baustein B 2.9 *Rechenzentrum*.

Neben der allgemein geschützten Aufstellung sollte auch überprüft werden, ob die Klimatisierung des gewählten Standorts und die Stromversorgung dort den technischen Anforderungen und der angestrebten Verfügbarkeit der Speicherlösung entsprechen. Die Stationierung der einzelnen Komponenten des SAN-Systems ist sorgfältig zu planen. So sollte sorgfältig geprüft werden, wo Sicherungsgeräte, die regelmäßige oder gelegentliche manuelle Eingriffe erfordern (z. B. Entnahme oder Wechsel von Bandkassetten) zweckmäßig und unter Beachtung aller Sicherheitsanforderungen aufgestellt werden können.

Ebenso ist bei räumlich verteilten SAN-Konfigurationen zu prüfen, ob alle Geräte permanent mit Strom versorgt werden können. Es kann nötig sein, einen SAN-Switch in einem normalen Verteilerraum zu installieren, um extern stationierte Server anzuschließen. Dieser Raum ist dann, ebenso wie die Server, in die Energieversorgung über USV und Netzersatzanlage einzubinden. Weitere Maßnahmen zur Notfallvorsorge bei SAN finden sich in Maßnahme M 6.98 *Notfallvorsorge und Notfallreaktion für Speicherlösungen*.

**Prozesse**

Die Speicherlösung ist als zentrale IT-Komponente in alle Steuerungsprozesse der IT zu integrieren. Insbesondere Überwachungs- und Eskalationsverfahren sind innerhalb der vorhandenen Betriebsabläufe auf den NAS- oder SAN-Betrieb anzupassen. Leistungen des Herstellers zur Überwachung und Betriebssicherung sind in eigene Abläufe einzubeziehen. Dabei sind stets die Vorgaben der Sicherheitsleitlinie und weiterer Ausführungsbestimmungen der Institution zu beachten.

**Personal**

Es ist zu überprüfen, wie viele Mitarbeiter mit welcher Ausbildung für den Betrieb der Speicherlösung benötigt werden. Stehen nicht genügend ausgebildete Mitarbeiter zur Verfügung, müssen die erforderlichen Schulungsmaßnahmen rechtzeitig initiiert werden.

Prüffragen:

- Wurde eine Anforderungsanalyse zur Ermittlung der derzeitigen und zukünftigen Anforderungen an Verfügbarkeit, Performance und Kapazität durchgeführt?
- Wurde die Entscheidung für den Einsatz einer bestimmten Speicherlösung, beispielsweise NAS oder SAN, auf geeignete Weise dokumentiert?
- Wurde ein Sicherheitskonzept für den Einsatz von Speicherlösungen erstellt?

- Wurde die Infrastruktur für die Aufstellung von Speichersystemen geprüft und angepasst?
- Wurden die Überwachungs- und Eskalationsverfahren innerhalb der vorhandenen Betriebsabläufe auf den NAS- oder SAN-Betrieb angepasst?

# M 2.352 Erstellung einer Sicherheitsrichtlinie für NAS-Systeme

Diese Maßnahme ist 2014 mit der 14. Ergänzungslieferung entfallen. Alle wesentlichen Inhalte wurden in die Maßnahme M 2.525 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen* überführt.

# M 2.353 Erstellung einer Sicherheitsrichtlinie für SAN-Systeme

Diese Maßnahme ist 2014 mit der 14. Ergänzungslieferung entfallen. Alle wesentlichen Inhalte wurden in die Maßnahme M 2.525 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen* überführt.

# M 2.354 Einsatz einer hochverfügbaren SAN-Lösung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Haben Systeme und Anwendungen, deren Daten im SAN gespeichert werden sollen, einen sehr hohen Schutzbedarf in Bezug auf die Verfügbarkeit aufzuweisen, so muss der Einsatz einer hochverfügbaren SAN-Lösung in Betracht gezogen werden.

Der Begriff "hochverfügbar" bezeichnet hier eine hohe Widerstandsfähigkeit gegen Schadensereignisse. Hochverfügbare Lösungen werden allgemein auch als "Desaster-tolerant" bezeichnet. Bezogen auf die gespeicherten Daten einer Institution bedeutet dies, dass mithilfe von SAN-Komponenten ein Speichersystem derart aufgebaut wird, dass

- alle Daten an zwei Standorten vorgehalten werden,
- die SAN-Komponenten der Speicherlösung an den beiden Standorten gekoppelt, aber nicht abhängig voneinander sind
- jede einzelne Komponente redundant konfiguriert ist,
- ein Schadensereignis an einem Standort die Funktionalität der Komponenten am zweiten Standort nicht beeinträchtigt.

Kenngrößen, die anzeigen, ob eine solche Architektur nötig und angemessen ist, sind:

- Die maximale Wiederanlaufzeit (engl. RTO: Recovery Time Objective) gibt die Zeitspanne an, die vergehen darf, bis nach einem Schadensereignis IT-Systeme wieder in hinreichender Funktionalität zur Unterstützung von Geschäftsprozessen zur Verfügung stehen.
- Der maximal tolerierbare Datenverlust (engl. RPO: Recovery Point Objective): Aus dem Alter des letzten verfügbaren konsistenten Datenbestandes lässt sich die Menge an "verloren gegangener Arbeit" nach dem Eintritt eines Schadensereignisses bemessen. Der maximal tolerierbare Datenverlust beschreibt im Grunde die Menge oder auch die Komplexität an Arbeit, die mit einem für die Institution tragbaren Aufwand verbunden ist, ohne dass geschäftskritische Verluste zu verzeichnen sind.
- Das betroffene Umfeld umfasst den räumlichen Umfang des Schadensereignisses. Nur wenn ein Standort mit seinen Systemen außerhalb der Wirkung des Ereignisses liegt, bleibt er nützlich.

SAN-Speicherlösungen sind eine Schlüsseltechnik, um sehr hohe Anforderungen an die Verfügbarkeit der IT zu erfüllen:

- Sie können bei Erhalt einer leistungsfähigen Kopplung so weit räumlich getrennt werden, dass auch gegen umfassend wirkende Ereignisse Vorsorge möglich ist.
- Die mögliche leistungsfähige Kopplung kann genutzt werden, um den maximalen Datenverlust zu minimieren oder gänzlich auszuschließen.

Die maximale Ausfallzeit einer Anwendung kann jedoch nur in Teilen durch die Konfiguration der Speicherlösung beeinflusst werden. Da die Ausfallzeit ausschließlich aus Sicht der Anwender gemessen werden darf, hängt sie nicht nur von der Verfügbarkeit der gespeicherten Daten ab, sondern genauso von der Verfügbarkeit der übrigen IT-Infrastruktur (Server, Netz, PCs, ...), die von SAN-Komponenten mit Daten versorgt werden. Des Weiteren sind auch Zeiten bis zur Alarmierung und Rüstzeiten zur Beseitigung der Störung zu betrachten.

**Möglichkeit der Konfiguration**

Es existieren verschiedene Möglichkeiten, eine Speicherlösung hochverfügbar zu konfigurieren.

**Spiegelung durch den Server**

Die einfachste Möglichkeit des hochverfügbaren SAN-Einsatzes ist dann gegeben, wenn ein Server, der seine Daten auf einem SAN-Speicher ablegt, an ein zweites, räumlich abgesetztes Speichersystem angeschlossen wird.

Jeder Schreibzugriff des Servers wird auf beiden Speichersystemen durchgeführt. Nachteilig an dieser Lösung ist, dass die Konfiguration und Administration der Instanz "Speicher" auf dem Server stattfindet.

Der Vorteil einer zentralen Speicherlösung, an der auch zentral administriert werden kann, bleibt auf diese Weise ungenutzt. Zudem muss die Verkabelung komplexer angelegt werden, da jeder Server mit beiden Speichersystemen verbunden wird. Vereinfacht dargestellt muss in Ergänzung der Verbindung zwischen Server und Speichersystem eine zweite Leitung von Server direkt zum abgesetzt stationierten zweiten Speichersystem verlegt werden.

**Replikation**

Replikation kann durch den Server oder durch das Speichersystem erfolgen. Serverbasierte Replikation wird in der Regel über eine eigene Software, die Applikation oder das Betriebssystem realisiert. Allerdings geht dieser Ansatz meistens mit einer hohen Belastung von CPU, Hauptspeicher und Bandbreite einher.

Bei der Replikation durch das Speichersystem werden die Server mit einem Speichersystem verbunden, dieses Speichersystem gleicht seinen Datenbestand komplett oder entsprechend seiner Konfiguration mit einem weiteren Speichersystem an einem abgesetzten Standort ab.

Wenn die Standorte nah genug beieinander liegen, ist synchrone Datenreplikation möglich. "Synchrone Datenreplikation" bedeutet, dass jeder Schreibzugriff des Servers von seiner direkt angeschlossenen Speicherplatte erst dann als fertig gemeldet wird, wenn das zweite, abgesetzte Speichersystem dem ersten Speichersystem das erfolgreiche Schreiben ("Acknowlege") bestätigt hat.

Damit werden Festplattenzugriffe aus Sicht der Anwendung langsamer, da zum einen zwei Plattensysteme schreiben und zum anderen die Signallaufzeit (Latenz) zwischen dem Speichersystem an Standort A und dem an Standort B hinzukommt.

Bei der asynchronen Datenreplikation sorgt besondere Replikationssoftware auf den Speichersystemen dafür, dass das Speichersystem an Standort A seine veränderten Daten regelmäßig an das Speichersystem an Standort B übermittelt. Dies geschieht häufig über IP-Verbindungen. Daher ist die Entfernung zwischen Hauptstandort und Replikationsstandort nicht begrenzt und kann sich sogar über Kontinente hinweg erstrecken.

Damit hat die Anwendung ein ungebremstes Speichersystem zugeordnet. Ein weiterer Vorteil an dieser Stelle ist, dass eine Institution nicht mehr gezwungen ist, die exakt identischen Speichersysteme für die Notfallvorsorge an zwei Orten bereitzuhalten. Am Hauptstandort kommt dann ein hochleistungsfähiges System zum Einsatz. Am zweiten Standort kann dagegen ein günstigeres

System installiert werden, sodass dennoch die Hauptaufgaben in einem Notfallszenario gewährleistet werden.

Der Nachteil bei der asynchronen Replikation ist, dass das zweite Speichersystem stets einen älteren, zeitlich versetzten Datenbestand hat. Wie groß der Datenverlust bei Ausfall des primären Systems ist, hängt von der eingesetzten Technik und der Konfiguration der asynchronen Spiegelung ab.

Synchrone Datenreplikation von Speichersystemen ist meist dann sinnvoll, wenn auch redundante Serversysteme bereitstehen, die den Betrieb direkt weiterführen können. Ein Szenario, bei dem an einem Standort das Speichersystem komplett ausfällt, die angeschlossenen Server und Netzkomponenten aber nicht (z. B. die des SANs), ist eher selten.

Weitere Informationen zur Replikation finden sich in M 3.92 *Grundlegende Begriffe beim Einsatz von Speicherlösungen*.

Bei der Planung einer hochverfügbaren Speicherlösung muss zunächst das gesamte Notfallvorsorgekonzept der Institution, zumindest aber der IT-Notfallvorsorgeteil dieses Konzeptes, geprüft werden. Die Verfügbarkeitsanforderungen müssen schriftlich festgelegt werden.

Angepasst an die Anforderungen und die Risikopolitik der Institution ist die Planung einer hochverfügbaren Speicherlösung nur der erste Schritt in Richtung Hochverfügbarkeit. Gleichzeitig muss die Planung der Weiterentwicklung der gesamten IT-Umgebung und der Notfallplanung für die Institution erfolgen.

Eine hochverfügbare Speicherlösung ist nur dann sinnvoll, wenn auch Server für den Wiederanlauf bereitstehen und wenn die Anwender an intakten Arbeitsplätzen über ein funktionierendes Netz auf Anwendungen und Daten zugreifen können.

Es ist zu beachten, dass ein Test- und Konsolidierungssystem ergänzt werden muss. Konfigurationsänderungen und Software-Updates dürfen bei Aufbau einer hochverfügbaren Konfiguration nie direkt am Produktivsystem vorgenommen werden. Von der Institution sind Systeme vorzuhalten, an denen sämtliche Änderungen getestet werden können. Nur so lässt sich sicherstellen, dass der Betrieb nicht durch fehlerhafte Konfiguration, Software oder administrative Eingriffe gefährdet wird.

**Hochverfügbarkeitsanbindung über den Einsatz von Speicher-Virtualisierung**

Eine hochverfügbare Speicher-Virtualisierung ermöglicht durch ihre Funktionen den Aufbau einer komplett hochverfügbaren Speicherlösung, die in der Lage ist, auf Ausfallszenarien automatisch zu reagieren.

Die Grundlage einer hochverfügbaren Speicher-Virtualisierung stellt die Virtualisierungs-Appliance dar. Sie ermöglicht die zentrale Verwaltung aller Speicherbereiche und wird für eine hochverfügbare Speicherlösung als sogenannter Cluster ausgeführt. Die Verteilung der Cluster und der Storagesysteme erfolgt dabei auf zwei unterschiedliche Brandabschnitte.

Die gewählte Architektur sollte in der Lage sein, zu gewährleisten, dass die Daten immer konsistent auf beiden Storagesystemen vorhanden sind (Spiegelung). Die Speicher-Virtualisierungslösung ist wiederum in sich redundant aufgebaut, und bei Ausfall eines Speichersystems arbeiten die Appliances weiter.

Die Funktionalität einer solch hochverfügbaren Speicherlösung mit Speicher-Virtualisierung sollte im Rahmen von Tests und Übungen im Rahmen des Notfallmanagements (siehe Baustein B 1.3 *Notfallmanagement*) getestet und geübt werden, um sicherzustellen, dass sie auch in Notfällen die geforderte Leistung erbringt. Bei den Tests und Übungen ist das Risiko des Datenverlusts durch die Tests und Übungen selbst besonders zu beachten. Die Tests und Übungen sind entsprechend auszugestalten, damit es nicht durch sie zu einem Schaden für die Daten der Institution kommt.

Prüffragen:

- Sind die Verfügbarkeitsanforderungen an die Speicherlösung schriftlich festgehalten?
- Entsprechen die Replikationsmechanismen den Verfügbarkeitsanforderungen?
- Wird die hochverfügbare Konfiguration der Speicherlösung den Verfügbarkeitsanforderungen gerecht?
- Ist ein Test- und Konsolidierungssystem vorhanden?

# M 2.355 Auswahl von Lieferanten für eine Speicherlösung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT

Nachdem die Anforderungen für eine Speicherlösung spezifiziert wurden, ist ein geeigneter Lieferant zu identifizieren. Die Auswahl möglicher Lieferanten muss dabei mehr Kriterien berücksichtigen als die reine Hardwarelösung und deren Preis. Mögliche Auswahlkriterien sind:

- Technische Anforderungen
- Kaufmännische Anforderungen (Kauf, Leasing, Storage-on-Demand-[SoD-] Modelle)
- Bestehende Lieferantenbeziehungen
- Bestehende Rahmenverträge mit Lieferanten
- Flächendeckende Serviceerbringung

Es ist davon auszugehen, dass die Unterstützung des Lieferanten mindestens bei der Lösung von Problemen im Betrieb und erst recht bei Hardwareausfällen benötigt wird. Entsprechend sind neben Preisen und Konditionen für die Beschaffung der Speicherlösung und deren Inbetriebnahme auch die Konditionen und der Leistungsumfang der angebotenen Unterstützung zu bewerten.

Die Aspekte der Wartung und Instandhaltung werden schriftlich im Vertrag im Rahmen von sogenannten Service Level Agreements (SLAs) definiert. Entsprechend sollte das Angebot eines möglichen Lieferanten neben den Hardware- und Softwarepreisen auch die Preise für denkbare SLAs beinhalten, sodass der Kunde die Gesamtpakete vergleichen kann, wenn verschiedene Hersteller oder Lieferanten in Betracht kommen.

Wichtig ist in diesem Zusammenhang auch die Bewertung von zusätzlichen Kriterien wie der Servicefähigkeit eines Anbieters, die beispielsweise von der Verteilung einzelner Servicestützpunkte abhängt. Darüber hinaus kann eine zentrale Hotline, die durch den Anbieter zur Verfügung gestellt wird, oder der Nachweis der Leistungsfähigkeit durch eine signifikante Anzahl entsprechend zertifizierter Mitarbeiter für das gewünschte System ein ausschlaggebender Aspekt sein. Institutionen sollten dazu weiterhin M 2.356 *Vertragsgestaltung mit Dienstleistern für Speicherlösungen* beachten.

Wenn eine Speicherlösung nicht gekauft, sondern z. B. geleast wird, muss auch vertraglich festgehalten werden, wie bei Vertragsende der Datentransfer auf Nachfolgesysteme, die Datenlöschung und andere technische und organisatorische Fragen gehandhabt werden und welche Kosten hierfür entstehen.

Generell ist festzustellen, dass gerade bei komplexen Systemen eine Lösung aus einer Hand Vorteile haben kann und daher präferiert werden sollte: In der Regel können Probleme, die beim Aufbau, Test und Betrieb entstehen, schneller und effektiver beseitigt werden, wenn nur ein Anbieter involviert ist.

Bei Lösungen aus Komponenten verschiedener Anbieter können in der Anschaffung preisliche Vorteile erzielt werden. Es ist aber wichtig zu prüfen, ob dieser Vorteil auch bestehen bleibt, wenn die Kosten der Umsetzung (Grundkonfiguration, Probebetrieb, Datenmigration) und des Betriebs (Wartung, Unterstützung bei Problemen) mit betrachtet werden.

Prüffragen:

- Enthält der Vertrag eindeutige und quantifizierbare Leistungsbeschreibungen?
- Sind die Auswahlkriterien und die Auswahl des Lieferanten nachvollziehbar dokumentiert?
- Sind genaue Regelungen für das Laufzeitende des Vertrages getroffen worden?

# M 2.356 Vertragsgestaltung mit Dienstleistern für Speicherlösungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT

Nur wenige Institutionen werden die technische Betreuung der Speicherlösung im Normalbetrieb und in Notfallsituationen selbst vollumfänglich leisten können und wollen. In diesem Fall müssen sie auf geeignete Hersteller und Lieferanten zugreifen, im Weiteren kurz als Dienstleister bezeichnet.

Die Aspekte, die im Folgenden beschrieben werden, sind als Hilfsmittel und Checkliste bei der Vertragsgestaltung zu sehen. Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen von den Verfügbarkeitsanforderungen des Auftraggebers und auch von der Komplexität der konkreten Speicherlösung ab.

Grundsätzlich sollte der Dienstleister auf die Einhaltung aller relevanten Gesetze und Vorgaben, vor allem aber des Datenschutzes nach dem Bundesdatenschutzgesetz (BDSG) und auf den Einsatz von organisatorischen und technischen Maßnahmen zur Informationssicherheit verpflichtet werden. Diese sollten mindestens dem Niveau des IT-Grundschutzes entsprechen und gegebenenfalls um weitere, vom Auftraggeber vorgegebene, Sicherheitsanforderungen ergänzt werden.

Neben diesen allgemeinen Verpflichtungen empfiehlt es sich, alle vereinbarten Leistungen messbar und prüfbar im Vertrag schriftlich zu fixieren. So kann es z. B. angemessen sein zu vereinbaren, dass ein qualifizierter Mitarbeiter des Dienstleisters bei bestimmten Problemfällen innerhalb von vier Stunden vor Ort sein muss. Eine solche konkrete, an den Anforderungen der Institution festgemachte Aussage kann eventuell sinnvoller sein als ein Pauschalangebot ("Gold-Support"), das möglicherweise ungünstige Ausnahmen (beispielsweise "Sonntags nur telefonische Unterstützung") von der geforderten Qualität beinhaltet.

Auch die Erstellung des Notfallvorsorgekonzeptes für die Speicherlösung sollte Vertragsbestandteil sein. Insbesondere ist zu klären, wer für die fachlichen Inhalte verantwortlich ist und welche Mitwirkungspflichten dem Auftraggeber obliegen.

Es ist dringend anzuraten, dass der Auftraggeber genügend Vorbereitung in die Zusammenstellung der eigenen Anforderungen investiert. Nachträgliche Konkretisierungen und Ergänzungen des Vertrages, die aufgrund unterschiedlicher Interpretation von ungenau beschriebenen Leistungen notwendig werden, sind oftmals mit deutlichen Kostenerhöhungen für den Auftraggeber verbunden.

Insbesondere wenn es sich bei dem Dienstleistungsverhältnis um Outsourcing handelt, ist der Baustein B 1.11 *Outsourcing* zusätzlich anzuwenden, bei Cloud-Speicherlösungen der Baustein B 1.17 *Cloud-Nutzung* und insbesondere die Maßnahme M 2.541 *Vertragsgestaltung mit dem Cloud-Dienstean-bieter*. Die folgende Themenliste sollte in diesen Fällen der Konkretisierung

der grundlegenden Anforderungen an die Vertragsgestaltung aus diesen Bausteinen in Bezug auf Speicherlösungen dienen.

**Organisatorische Regelungen und Prozesse**
- Festlegung von Kommunikationswegen und Ansprechpartnern
- Festschreibung von Zeiten (z. B. Tagbetrieb, Nachtbetrieb, was zählt als Wochenende, Feiertage)
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
- Verfahren bei Störungen, Notfällen, Krisen und sonstigen Sicherheitsvorfällen, Benennung von Ansprechpartnern mit den nötigen Befugnissen
- Zugriffsmöglichkeiten des Dienstleisters auf IT-Ressourcen des Auftraggebers
- Datenübertragung von Wartungs- bzw. Statusinformationen zum Dienstleister oder Hersteller
- Zutritts- und Zugangsberechtigungen für Mitarbeiter des Dienstleisters zu den Räumlichkeiten und IT-Systemen des Auftraggebers
- Übergabe von Datenbeständen bei Beendigung des Vertragsverhältnisses, Datenlöschung bei Rücknahme von Speichermedien durch den Auftragnehmer

**Personal**
- Gegebenenfalls Gestaltung der Arbeitsplätze von externen Mitarbeitern
- Festlegung und Abstimmung von Vertretungsregelungen
- Planung von Fortbildungsmaßnahmen

**Notfallvorsorge**
- Erforderliche Handlungen beim Eintreten eines Ereignisses mit dem Potenzial zum Sicherheitsvorfall, zum Notfall oder zur Krise
- Reaktionszeiten und Eskalationsstufen für solche Ereignisse
- Mitwirkungspflicht des Auftraggebers bei der Behebung von Notfällen
- Vereinbarung zur Bereitstellung von Ersatz- oder Ausweichsystemen
- Von besonderer Bedeutung können Regelungen im Fall höherer Gewalt sein. Es sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Dienstleisters die Verfügbarkeit dieses durch z. B. weiteres externes Personal sichergestellt werden kann.

**Haftung, juristische Rahmenbedingungen**
- Eine Verpflichtung der einzelnen Mitarbeiter des Auftragnehmers auf die Einhaltung von geltenden Normen und Gesetzen sowie besonderer vereinbarter Sicherheitsmaßnahmen ist vertraglich zu regeln. Gegebenenfalls sind besondere Geheimhaltungsvereinbarungen vertraglich zu fixieren.
- Die Einbindung Dritter, Subunternehmer und Unterauftragnehmer des Dienstleisters ist zu regeln. In der Regel empfiehlt es sich nicht, diese grundsätzlich auszuschließen, sondern sinnvoll zu regeln.
- Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Es ist zu klären, ob der Dienstleister bereits bestehende Verträge mit Dritten (Hardwareausstattung, Serviceverträge, Softwarelizenzen etc.) übernimmt.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsvertrags zu regeln.
- Regelungen für das Ende des Vertragsverhältnisses, z. B. für einen Wechsel oder bei Insolvenz des Dienstleisters, sollten spezifiziert werden.
- Auf ein ausreichend flexibles Kündigungsrecht ist zu achten.
- Der Auftragnehmer ist zu verpflichten, nach Beendigung des Auftrags alle vom Auftraggeber im Rahmen des Vertragsverhältnisses angeschaffte

Hard- und Software inklusive gespeicherter Daten zurückzugeben sowie alle gespeicherten Informationen sicher zu löschen.
- Haftungsfragen im Schadensfall sind zu klären. Sanktionen oder Schadensersatz bei Nichteinhaltung der Dienstleistungsqualität dürfen aus Sicht des Auftraggebers dabei nicht überschätzt werden.
- Zunächst ist stets zu fragen, wie ein Schaden nachgewiesen bzw. der Verursacher überführt werden kann.
- Wie wird beispielsweise ein Reputationsschaden quantifiziert?
- Wie ist es zu bewerten, wenn gravierende Pflichtverletzungen aufgedeckt werden, die nur zufällig nicht zu einem größeren Schaden geführt haben?
- Das Recht auf Schadensersatzzahlungen ist wertlos, wenn diese die Zahlungsfähigkeit des Dienstleisters übersteigen und dieser Insolvenz anmeldet.
- Auf der anderen Seite sollten aber "Sanktionen" in Form von kostenloser Bereitstellung des Dienstes oder Dienstleistung oder eine kostenlose höhere Dienstgüte kritisch bewertet werden. Wenn ein Schaden geschäftskritisch oder sogar ruinös ist, dann bieten diese kostenlosen Dienste keinen Mehrwert.

**Änderungsmanagement und Testverfahren**
- Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Auftraggeber in der Lage ist, sich neuen Anforderungen anzupassen. Es ist festzulegen, wie geänderte Anforderungen des Auftraggebers behandelt werden.
- Testverfahren für neue Soft- und Hardware sind zu vereinbaren. Dabei sind folgende Punkte einzubeziehen:
    - Regelungen für Updates und Systemanpassungen
    - Zuständigkeiten bei Auftraggeber und Dienstleister bei der Erstellung von Testkonzepten und bei der Durchführung von Tests
    - Abnahme- und Freigabeprozeduren. Es ist immer wieder zu beobachten, dass der Auftragnehmer explizit oder implizit eine Freigabe von Änderungen für den produktiven Betrieb vornimmt, obwohl gegebenenfalls beachtliche Risiken und Verantwortung beim Auftraggeber liegen.

**Kontrolle des Auftragnehmers**
- Die Dienstleistungsqualität muss regelmäßig (z. B. monatlich) kontrolliert werden. Der Auftraggeber muss die dazu notwendigen Auskunfts-, Einsichts- und Zugangsrechte besitzen. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies bereits im Vertrag geregelt sein.

Prüffragen:

- Wurde der Dienstleister auf die Einhaltung aller relevanten Gesetze und Vorgaben und auf den Einsatz von organisatorischen und technischen Maßnahmen zur Informationssicherheit verpflichtet?
- Sind alle vereinbarten Leistungen im Vertrag messbar und prüfbar schriftlich fixiert?
- Wird die Dienstleistungsqualität regelmäßig kontrolliert?
- Sind die Schnittstellen zwischen Anwender und Dienstleister klar definiert und deckt dies auch Sonderfälle wie z. B. Sicherheitsvorfälle oder Notfälle ab?

# M 2.357 Aufbau eines Administrationsnetzes für Speichersysteme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Verwaltung und Überwachung von Ressourcen wie SAN- oder NAS-Komponenten, an die hohe Sicherheitsanforderungen gestellt werden, muss angemessen umgesetzt werden. Der Aufbau eines eigenen LANs, das ausschließlich administrativen Aufgaben dient, ist oft der übersichtlichste, effektivste und wirtschaftlichste Weg, um diesen Anforderungen zu genügen. In diesem Administrationsnetz werden PCs stationiert, die ausschließlich zur Verwaltung kritischer Komponenten dienen.

Grundsätzlich sollen auch innerhalb dieses Netzes nur sichere Protokolle (SSH statt Telnet, HTTPS statt HTTP) zur Administration genutzt werden. Die zumindest logische, wenn nicht gar physische Trennung dieses Administrationsnetzes von Produktionsnetz macht jedoch den Einsatz unsicherer Protokolle, insbesondere des in vielen Produktionsumgebungen immer noch fast unvermeidlichen SNMP Version 1, tolerierbar.

**Konzeption/Planung**

- Ein sehr einfacher Aufbau eines solchen Netzes kann damit starten, dass ein separater Switch in Betrieb genommen wird.
- Alle Clients der Administratoren werden mit ihrem Netzanschluss an das Administrationsnetz gebunden.
- Alle Server und Systeme mit erhöhtem Sicherheitsbedarf (aktive Netzkomponenten, Speichersysteme) erhalten einen zusätzlichen Netzanschluss und werden damit an das Administrationsnetz gebunden.
- Auf den Servern wird der Administrationszugang der Betriebs- und Anwendungssoftware, wo immer das möglich ist, exklusiv an die Netzadresse im Administrationsnetz gebunden.

Im Administrationsnetz sollten private (wie in RFC-Standard 1918 beschrieben) Adressen benutzt werden. Solche Adressen werden in "offiziellen" Netzen nicht geroutet, so dass ein Anschluss an offizielle Netze, wenn er denn nötig werden sollte, stets NAT (Network Address Translation) und weitere Schutzmaßnahmen, die durch eine Firewall realisiert werden, erfordert.

Im Administrationsnetz sollte auf allen IT-Komponenten durch Nutzung oder Einsatz eines NTP-Servers eine einheitliche Uhrzeit sichergestellt werden. Damit wird die Auswertung von Protokollen erleichtert und die Bewertung von Vorfällen, die Wirkung auf mehreren Komponenten zeigen, ermöglicht.

Die verfügbaren Ressourcen für den gesamten Aufbau eines Speichersystems sind zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür notwendigen finanziellen Ressourcen.

Die Ergebnisse sind entsprechend zu dokumentieren.

Es ist zudem zu prüfen, ob im Administrationsnetz zusätzliche Überwachungsmaßnahmen etabliert werden sollten. Zum Beispiel kann durch Einsatz von netzbasierten IDS zusätzlich überwacht werden, ob unzulässige Aktivitäten im Netz zu beobachten sind.

Ebenso könnte in einem solchen Netz auch eine zentrale Protokollierung etabliert werden, in der eine zentrale Instanz als Protokollserver die Logdaten aller Server und Speichersysteme verwaltet. Es ist zu beachten, dass solche besonderen Maßnahmen gegebenenfalls mit der Personalvertretung abgestimmt werden müssen.

Falls das Administrationsnetz einen komplexen Aufbau aufweist, sollte der Baustein B 4.1 *Lokale Netze* für Aufbau und Prüfung herangezogen werden.

**Umsetzung**

Zunächst ist zu untersuchen, wie ein Produktionsnetz und die darin stationierten Server und sonstigen Geräte (aktive Netzkomponenten, Speichersysteme) um ein Administrationsnetz erweitert werden können.

Zunächst sind die Maßnahmen M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und M 2.140 *Analyse der aktuellen Netzsituation* zu bearbeiten. Anschließend sind die Anforderungen an die Netzkommunikation des neu aufzubauenden Administrationsnetzes zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

Die Schutzbedarfsanforderungen des Administrationsnetzes sind aus den bestehenden IT-Verfahren, die über dieses Netz administriert werden sollen, abzuleiten.

**Betrieb**

Mit Aufnahme des Testbetriebes muss eine Prüfung stattfinden, die die Sicherheitsvorkehrungen testet und zur Grundlage der Betriebsdokumentation dieses Netzes wird. Typische Prüffragen sind:

- Ist eine durchgängige Trennung des Administrationsnetzes vom Produktionsnetz gegeben?
- Werden, wo immer möglich, sichere Dienste (secure shell, https) genutzt? Sind die unsicheren Varianten dieser Dienste (telnet, http) auf den administrierten Geräten deaktiviert?
- Ist überschaubar und dokumentiert, wo auf den Einsatz unsicherer Dienste nicht verzichtet werden kann?
- Sind alle Default-Kennungen und -Passwörter auf PC, Servern und aktiven Netzkomponenten etc. geändert?

Anschließend kann der produktive Betrieb gestartet werden.

**Aussonderung**

Wenn PCs oder andere Hardware ausgesondert oder auch nur zur Reparatur zeitweise aus dem Netz genommen werden, ist sicherzustellen, dass keine internen Informationen (Passwörter, Protokolldateien, Dokumente zu Interna etc.) darauf gespeichert sind.

**Notfallvorsorge**

Es muss eine Notfallplanung geben, so dass der Betrieb des produktiven Netzes sichergestellt wird, wenn das Administrationsnetz ausfällt.

Prüffragen:

- Wird die Verwaltung und Überwachung des Speichersystems den Sicherheitsanforderungen des Speichersystems gerecht?

- Ist für alle Komponenten des Administrationsnetzes eine einheitliche Uhrzeit sichergestellt?
- Werden während des Testbetriebs des Administrationsnetzes die Sicherheitsvorkehrungen getestet und der Test sowie die Ergebnisse dokumentiert?
- Gibt es eine Notfallplanung, so dass bei Ausfall des Administrationsnetzes das produktive Netz weiterbetrieben werden kann?

# M 2.358 Dokumentation der Systemeinstellungen von Speichersystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Dokumentation der Systemeinstellungen zum Speichersystem weist die Umsetzung von technischen und organisatorischen Vorgaben nach und beschreibt die individuelle Konfiguration der Institution. Die Dokumentation ist Grundlage für die Administration im Normalbetrieb und für die Planung und Durchführung von Änderungen. Zudem ist eine aktuelle und korrekte Dokumentation Grundlage der Notfallvorsorge.

Daten, die im Notfall relevant sind, müssen in allen Notfallszenarien zugreifbar sein. Dabei muss jedoch beachtet werden, dass Informationen zu den Systemeinstellungen vertraulich sind und daher ausreichend vor unberechtigtem Zugriff geschützt werden müssen.

Dokumentiert werden sollten insbesondere folgende Informationen:

Zur Organisation:

- Eine Beschreibung der definierten Rollen und der zugehörigen Rechteprofile
- Die administrativen Benutzer des Speichersystems mit zugeteilter Rolle
- Der Zeitpunkt der Einrichtung von Benutzerkennungen und -rechten sowie gegebenenfalls die Befristung und weitere Erläuterungen
- Die Kontaktdaten des Benutzers und dessen organisatorische Einbindung
- Vorgaben zu Datensicherung und Notfallvorsorge

Zur Technik:

- Die Aufstellung aller Speichergeräte mit Angaben zu Typ, Zweck und Anwenderkreis
- Die logischen und physischen Zuordnungen der Speichergeräte zu den Servern
- Sämtliche Anbindungen der Speichergeräte an die Netze (SAN, LAN, gegebenenfalls WAN zur Fernüberwachung)
- Eine Aufstellung, welche Geräte über eine NAS-Schnittstelle Daten exportieren
- Eine Aufstellung aller Management-Schnittstellen (In-Band und Out-Band). Diese sollte auch eine Übersicht enthalten, welche Schnittstellen aktiv sind und welche Dienste darüber erreichbar sind.

Zur Administration:

- Eine grafische Darstellung der Netze (SAN, LAN, gegebenenfalls WAN) und der konfigurierten Verbindungen zwischen Speichersystemen, Servern und Administrations-PC.
- Alle erforderlichen Angaben zur Aktivierung und Deaktivierung von Schnittstellen und Diensten.
- Die notwendigen Einstellung für die Datensicherung
- Die Einstellungen zur Protokollierung
- Empfehlenswert ist eine kurze Darstellung ("Kochbuch") der Handhabung von wichtigen oder regelmäßig durchzuführenden Administrationstätigkeiten.

Die Dokumentation zur Organisation sollte regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht.

Die technische Dokumentation sollte noch häufiger zumindest stichprobenartig überprüft werden, da sie die Grundlage der Notfallvorsorge ist.

Prüffragen:

- Entspricht die Dokumentation der Systemeinstellungen den technischen und organisatorischen Vorgaben und beschreibt sie die spezifische Konfiguration der Speichersysteme der Organisation?
- Sind die im Notfall relevanten Daten in allen Notfallszenarien verfügbar?
- Sind vertrauliche Daten aus der Dokumentation der Systemeinstellungen vor dem Zugriff Unberechtigter geschützt?
- Sind die Vorgaben zu Datensicherung und Notfallvorsorge für Speichersysteme dokumentiert?
- Wurde die Dokumentation zu Speichersystemen (insbesondere der Rechtevergabe) mindestens alle 6 Monate überprüft?

# M 2.359 Überwachung und Verwaltung von Speicherlösungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um Fehlersituationen und Sicherheitsprobleme zeitnah erkennen und beheben zu können, ist es notwendig, den laufenden Betrieb von Speicherlösungen zu überwachen. Voraussetzung für eine solche Überwachung ist die Möglichkeit, Daten von verschiedenen Quellen (Server, Switches, Speichersysteme usw.) auszuwerten.

Eine Speicherlösung besteht aus einer Vielzahl von Komponenten, die zu überwachen sind:

- Daten über den Zustand der Hardware der Speicherlösung,
- Daten zur Auslastung der Speicherlösung und
- Daten über die Netzinfrastruktur (IP und FC)

Alle Daten sollten dabei vorrangig daraufhin geprüft werden, ob die Vorgaben des Betriebshandbuchs umgesetzt bzw. eingehalten werden.

Eine effiziente Analyse der Daten ist in der Regel nur realisierbar, indem spezielle Anwendungen zum automatisierten Monitoring und Reporting eingesetzt werden. Dabei muss eine Vielzahl von Daten gesammelt und ausgewertet werden. Daher sollte unter anderem durch Einsatz oder Nutzung eines NTP-Servers eine einheitliche Datums-/Uhrzeiteinstellung auf allen Geräten erzwungen werden. Wichtige Nachrichten, die auf Basis von SNMP gesendet werden, können durch den Einsatz von Nachrichtenfiltern herausgefiltert und somit schneller erkannt werden.

Spezielle Produkte zur Überwachung ermöglichen je nach Ausprägung sowohl eine Statusüberwachung als auch die Anpassung von Einstellungen in Echtzeit. Der Netzadministrator kann bei auftretenden Problemen automatisch gewarnt werden, bevor diese zu Ausfällen führen.

Die Überwachung von Ereignissen der gesamten Speicherlösung (FC/IP-Ports, Netz- und Speichersysteme) und Umgebungsparameter gestattet eine frühzeitige Fehlererkennung und -isolierung sowie eine Indikation der Verfügbarkeit und Leistungsfähigkeit der gesamten Umgebung.

In diesem Zusammenhang müssen folgende Komponenten überwacht werden:

- Die Anwendungen, die in einer Speicherlösung Daten verarbeiten oder eine Hilfsfunktion haben. Dazu gehören die Sicherungssoftware und auch Antiviren-Software
- Die Menge der Nutzdaten, die von Anwendungen verarbeitet und dann über das Speichernetz vom Server auf Speichersysteme transportiert werden (Kapazitätsmanagement)
- Die Netzhardware, die für den Transport der Daten benötigt wird
- Die Speicherhardware (Plattensysteme, Bandlaufwerke), die zur Speicherung der Daten benötigt wird
- Das Netz - Bei einem NAS-System ist das TCP/IP-Netz zu überwachen, bei einem SAN das speicherinterne Netz und zudem das zusätzlich zur Steuerung und Verwaltung genutzte lokale Netz.

Eine erweiterte Möglichkeit der Überwachung von Speicherlösungen bietet der Einsatz sogenannter Security Information and Event Management-Lösungen

(SIEM). Diese sind in der Lage, Ereignis-, Bedrohungs- und Risikodaten zusammenzufassen. Auf dieser Basis können sie Sicherheitsinformationen liefern und schnelle Reaktionen auf Sicherheitsvorfälle sowie die Protokollverwaltung und Erzeugung von Compliance-Berichten sicherstellen.

Neben der Überwachung der Ressourcen sollte auch die Verwaltung einzelner Komponenten und des Gesamtsystems von zentraler Stelle aus möglich sein. Systeme, die eingesetzt werden, um die Speicherlösungen zu steuern oder zu kontrollieren, werden oft als Speichermanagementsysteme bezeichnet. Idealerweise verfügen Managementsysteme über die Möglichkeit, auf eine Reporting-Historie zuzugreifen. Auf diesem Weg können Ereignisse und Störungen, die in der Vergangenheit liegen, nachträglich untersucht werden und entsprechende Erkenntnisse der Stabilisierung des Gesamtsystems dienen.

**NAS-Management**

Die Überwachung von reinen NAS-Lösungen ist häufig besonders einfach gestaltet. Auch wenn das System scheinbar "wartungsfrei" erscheint, ist es nötig, technische und/oder organisatorische Überwachungsmaßnahmen zu etablieren. Nach Möglichkeit sollte die NAS-Lösung in ein einfaches Netzmanagementsystem eingebunden werden, um mindestens zu kontrollieren, ob die NAS-Lösung verfügbar ist und hinreichend Speicherkapazität aufweist.

**SAN-Management**

Bei der Überwachung von SAN-Lösungen stehen die Mechanismen des "In-Band-Managements" und des "Out-of-Band-Managements" zur Verfügung.

In-Band-Management findet auf den Schnittstellen und Netzen statt, die dem Datentransport zwischen den SAN-Geräten dienen. Die Möglichkeiten der Konfiguration und der Überwachung sind beim In-Band-Management häufig weitreichender und komfortabler, da die zugrunde liegende Software produktnah ist und Hersteller hier Alleinstellungsmerkmale suchen.

Das Out-of-Band-Management benutzt dagegen zusätzliche Schnittstellen, üblicherweise TCP/IP-Netzanschlüsse. Als Protokoll zur Informationsgewinnung ist SNMP weit verbreitet. Out-of-Band-Management bietet die üblichen Standards und erleichtert die Kombination von Produkten unterschiedlicher Hersteller.

Da als Protokoll beim Out-of-Band-Management oft noch die wenig sichere SNMP Version 1 genutzt wird, ist ein separates abgeschottetes Management-LAN zu betreiben (siehe M 2.357 *Aufbau eines Administrationsnetzes für Speichersysteme*). Grundsätzlich sollen auch innerhalb dieses Netzes nur sichere Protokolle (SSH statt telnet, HTTPS statt HTTP) zur Administration genutzt werden. Die zumindest logische, wenn nicht gar physische Trennung dieses Administrationsnetzes vom Produktionsnetz macht jedoch den Einsatz unsicherer Protokolle tolerierbar.

Bei höheren Anforderungen an die Verfügbarkeit der Managementlösung sollte eine Kombination der beiden dargestellten Varianten gewählt werden. Wenn sowohl In-Band- als auch Out-of-Band-Management und Überwachung im Einsatz sind, erleichtert und beschleunigt die zusätzliche Netzanbindung die Überwachung und Diagnose von Problemen, erhöht jedoch auch den Betriebsaufwand.

**Zentrale Kontrolle**

In größeren Installationen, vor allem bei Speicherlösungen mit verschiedenen Standorten der Komponenten, sollte eine zentrale Stelle existieren, an die alle für den Betrieb wichtigen Informationen gemeldet werden. Der Einsatz von Programmen, die das Geschehen übersichtlich grafisch darstellen können, ist ratsam.

Ein solches Managementsystem stellt die Schnittstelle zu einem komplexen System dar. Es kann nur von hinreichend geschultem Personal effizient genutzt werden.

Sofern eine Speicherlösung durch einen externen Dienstleister betrieben wird, sind in Abhängigkeit der Vertragsgestaltung Service Level Agreements (SLAs) geschlossen worden. In diesem Fall sollte eine Institution Festlegungen treffen, wie die Einhaltung dieser vertraglichen Regelungen überwacht werden kann (z. B. durch regelmäßiges Reporting und Kontrolle) bzw. welche Informationspflichten für den Dienstleister mit diesen einhergehen.

Prüffragen:

- Gibt es dokumentierte Festlegungen und Prozesse zur Überwachung und Verwaltung der Speicherlösung?
- Gibt es eine zentrale Stelle, an die Informationen unterschiedlicher Speicherlösungen gemeldet werden?
- Sind Nachrichtenfilter im Einsatz, um die wesentlichen Nachrichten herauszufiltern und besser darzustellen?
- Sind Festlegungen getroffen und dokumentiert wurden, die die Überwachung vertraglich vereinbarter SLAs mit dem Dienstleister regeln?

# M 2.360 Sicherheits-Audits und Berichtswesen bei Speichersystemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Revisor

Umfang und Häufigkeit von Sicherheitsüberprüfungen auf Speichersystemen werden durch die Daten, die auf dem jeweiligen Speichersystem verarbeitet werden, bestimmt. Bei komplexen Systemen, in denen eine Vielzahl von Anwendungen ihre Daten auf dem Speichersystem ablegen, muss eine Analyse der Geschäftsprozesse und eine darauf abgestimmte Feststellung des Schutzbedarfs vorgenommen werden. Dabei ist für Anwendungen und Daten, die die wesentlichen Geschäftsprozesse unterstützen, der Schutzbedarf festzustellen, um Anforderungen an die Häufigkeit und Tiefe von Sicherheits-Audits zu erhalten. Wie üblich geben die strengsten Anforderungen einer einzelnen Anwendung die Vorgabe für das Gesamtsystem.

Zur Überwachung aller sicherheitsrelevanten Tätigkeiten muss ein Prozess eingerichtet werden. In diesem muss festgelegt sein, welche Sicherheitsreports regelmäßig erstellt werden. Da Speichersysteme komplex zusammengesetzt sein können, müssen Sicherheitsreports relevante Beobachtungen aus verschiedenen Quellen zusammenstellen und bewerten. Zudem muss festgelegt werden, wie mit Abweichungen von den Vorgaben umgegangen wird. Die Sicherheitsreports sollten als Information für den Auditor verwendet werden.

### Inhalt eines Audits

Ein Audit gleicht die Sicherheitsvorgaben mit den aktuellen Einstellungen und Daten ab. Durch ein solches Audit wird überprüft, ob die geforderten Sicherheitseinstellungen und Abläufe eingehalten werden.

### Ziel des Sicherheitsaudits

Wichtig ist, dass ein Audit nur zur Feststellung von Tatsachen und nicht zur Ermittlung von Schuldigen dient, siehe auch M 2.199 *Aufrechterhaltung der Informationssicherheit*.

### Sicherheits-Berichtswesen

Das Resultat eines Audits kann als eine einfache Soll-Ist-Gegenüberstellung gehalten werden. Der Bericht soll in gebotener Kürze die Vorgaben z. B. aus der Sicherheitsrichtlinie darstellen und die Feststellungen des Audits zu den einzelnen Vorgaben darstellen. Wenn Abweichungen vom Soll gefunden werden und Maßnahmen zur Besserung bekannt sind, so sollten diese direkt in den Report geschrieben werden.

### Unabhängigkeit der Auditoren

Die Durchführung der Audits muss durch unabhängige Auditoren erfolgen, d. h. das durchführende Personal darf sich und seine Arbeit nicht selbst auditieren.

Auch wenn die Tätigkeit der Auditoren durch die Administratoren des Speichersystems unterstützt wird, benötigen sie tiefere Kenntnisse über das Speichersystem zur Durchführung ihrer Tätigkeit. Diese Kenntnisse sind durch regelmäßige Schulungen zu erwerben bzw. zu aktualisieren.

**Autorisierung der Auditoren**

Wenn die Auditoren selbstständig und ohne Unterstützung durch die Administratoren tätig werden sollen, so ist eine Rolle "Auditor" für alle Komponenten des Speichersystems zu definieren. Die Rechte zu dieser Rolle sollten als "Nur Lesen" aller Einstellungen und Logdateien des Speichersystems definiert werden.

Wenn keine konkreten Vorgaben der Institution vorliegen, so sollte der Auditor mindestens die folgenden Bereiche prüfen:

- Es gibt ein Sicherheitskonzept für die technische Ausgestaltung und organisatorische Regelungen des Speichersystems.
- Der Schutzbedarf der gespeicherten Daten in Bezug auf Verfügbarkeit und Vertraulichkeit wurde nach Vorgaben der Anwender festgelegt und dokumentiert.
- Bei Inbetriebnahme wurden in allen Komponenten (Speicher, Sicherungsgeräte, gegebenenfalls SAN-Switche), Administrations-PC und zusätzlicher Software die Standardpasswörter ersetzt.
- Alle Komponenten (Speicher, Sicherungsgeräte, gegebenenfalls SAN-Switche) sind in zutrittsgeschützten Räumen mit angemessener Infrastruktur (Stromversorgung, Klimatisierung) stationiert.
- Administrative Zugriffe auf Speichersysteme erfolgen ausschließlich über ein separates Administrationsnetz.
- Das Administrationsnetz ist durch Firewall, Anti-Viren-Software und gegebenenfalls ein IDS abgesichert.
- Zur Administration werden nur gesicherte Verbindungen (z. B. über https, ssh) genutzt.
- Der Zugriff auf die Speichersysteme und ihre Daten ist ausreichend geschützt und vom restlichen Institutionsnetz geeignet abgetrennt.
- Die Daten werden verschlüsselt transportiert bzw. gespeichert, wenn dies aufgrund ihres Schutzbedarfs erforderlich ist.
- Das Logging ist so eingestellt, dass Fehlersituationen und Missbrauchsversuche protokolliert werden. Die Protokolldateien werden regelmäßig kontrolliert.
- Grundkonfiguration und folgende relevante Änderungen der Konfiguration sind schriftlich dokumentiert. Ein Netzplan der Topologie der Speichersysteme und ihrer Verbindungen zum LAN ist vorhanden und aktuell. Diese Dokumentation ist auch im Notfall verfügbar.
- Nach Änderungen werden sicherheitsrelevante Einstellungen des Speichersystems erneut überprüft.
- Der störungsfreie Ablauf von Datensicherungen und die Brauchbarkeit von Sicherungsmedien werden regelmäßig kontrolliert.

Prüffragen:

- Gibt es einen Überwachungsprozess für alle sicherheitsrelevanten Tätigkeiten und Quellen eines Speichersystems, in dem festgelegt ist, welche Sicherheitsreports regelmäßig erstellt werden?
- Ist geregelt, wie mit Abweichungen von Vorgaben umgegangen wird?
- Werden Umfang, Tiefe und Häufigkeit der Sicherheits-Audits auf Speichersystemen von den darauf verarbeiteten Daten und dem Schutzbedarf ihrer Anwendungen bestimmt?

# M 2.361 Außerbetriebnahme von Speicherlösungen

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Werden Speicherlösungen, einzelne Komponenten oder einzelne Datenträger aus einer Speicherlösung nicht mehr benötigt, so ist zunächst sicherzustellen, dass alle Daten, die auf dieser Speicherlösung gespeichert sind, in geeigneter Weise auf andere Speicherlösungen übertragen werden.

Anschließend ist sicherzustellen, dass alle Nutzdaten und Konfigurationsdaten sicher gelöscht werden.

### Austausch von Systemkomponenten und Speichermedien

Sind einzelne Speichermedien oder Systemkomponenten defekt und müssen deshalb ausgetauscht werden, ist sicherzustellen, dass die ausgetauschten Speichermedien und Komponenten durch Externe, wie z. B. durch den Hersteller, so behandelt werden, dass die Daten nicht reproduziert werden können.

Wenn hoher oder sehr hoher Schutzbedarf der Daten festgestellt wurde, sollte mit dem Hersteller oder Händler vereinbart werden, dass die betreffenden Platten physisch vernichtet werden. Ein Nachweis des Herstellers oder des Lieferanten ist gegenüber der Institution zu führen.

### Festplatten löschen

Wenn intakte Festplatten ausgetauscht werden, die gegebenenfalls weiterverwendet werden können oder sollen, müssen die darauf gespeicherten Daten so gelöscht werden, dass ihr Inhalt nicht mehr reproduziert werden kann (siehe auch M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*).

Für SAN- und NAS-Festplatten in komplexen Speicherlösungen sind spezielle Löschprogramme des Herstellers erforderlich. Das Löschen kann dann durch das mit der Wartung beauftragte Unternehmen durchgeführt werden. Dazu muss eine vertragliche Vereinbarung mit einer entsprechenden Verpflichtung des Dienstleisters vorgenommen werden. Auch hierzu ist gegenüber der Institution ein Nachweis zu führen.

Das nachweisliche sichere Löschen einzelner Speichermedien (z. B. Festplatten) innerhalb einer Speicherlösung kann in der Regel problemlos umgesetzt werden. Weitere Informationen zur Frage, wie nicht nur bestimmte Speichermedien, sondern bestimmte Daten in Speicherlösungen gelöscht werden, sind nicht in dieser Maßnahme enthalten. Siehe dazu die Maßnahme M 2.527 *Sicheres Löschen in SAN-Umgebungen*.

### Abbau einer Speicherlösung

Wenn eine Speicherlösung außer Betrieb genommen werden soll, ist zunächst ein Vorgehen zur Migration der Daten zu entwerfen. Es muss sichergestellt sein, dass alle Daten der Speicherlösung in geeigneter Form in andere Speicherlösungen überführt werden. In geeigneter Form heißt, dass alle Anforde-

rungen, die sich aus der Tätigkeit der Institution ergeben, aber auch gesetzliche Anforderungen zu Aufbewahrungsfristen und dergleichen erfüllt werden.

Es empfiehlt sich, eine Übergangsphase einzuplanen. In dieser Zeit werden bereits die Daten aus der neuen Speicherlösung im aktiven Betrieb genutzt, jedoch ist es noch möglich, auf die Daten der alten Speicherlösung zuzugreifen. So wird erreicht, dass auch spät erkannte Probleme noch behoben werden können.

Erst wenn die Transitionsphase als abgeschlossen erklärt wird, können die Nutzdaten gelöscht werden. Dazu sollte mit dem Hersteller bzw. Lieferanten ein effizientes, an den Schutzbedarf der Daten angepasstes Verfahren ausgewählt werden. Im Zweifel ist für alle Platten der Speicherlösung das Verfahren wie bei Austausch einzelner Platten zu wählen. Gerade ab höherem Schutzbedarf bezüglich Vertraulichkeit kann es sinnvoller sein, alle Platten physisch zu zerstören, da der Wiederverkaufswert in keinem Verhältnis zum Schaden durch möglichen Vertraulichkeitsverlust steht.

**Verwaltungsinformationen entfernen**

Die IP-Adressen bei NAS-Systemen bzw. LUNs und ähnliche Angaben bei SAN-Komponenten müssen aus der Konfiguration entfernt werden. Ebenso ist sicherzustellen, dass sonstige Verwaltungsinformationen zuverlässig entfernt werden. Dazu gehören beispielsweise Informationen, die z. B. von einem Webserver, der als Administrationswerkzeug auf dem System läuft, gespeichert werden.

Wegen der Sensibilität dieser Informationen ist darauf zu achten, dass die Dateien vor der Außerbetriebnahme oder dem Austausch defekter oder veralteter Komponenten gelöscht beziehungsweise unlesbar gemacht werden. Die Vorgehensweise hängt dabei stark vom Hersteller der Komponenten ab. In der Sicherheitsrichtlinie für Speicherlösungen sollten hierfür entsprechende Verantwortlichkeiten definiert werden.

Viele Komponenten unterstützen einen sogenannten Factory Reset. Dieser führt häufig jedoch nicht zur Löschung aller sicherheitsrelevanten Informationen, sodass weiterhin Restinformationen vorhanden sein können. Eine anschließende Kontrolle ist daher zwingend erforderlich. Auf anderen Komponenten können Konfigurationsdateien durch entsprechende Befehle komplett gelöscht oder durch andere Dateien ersetzt werden. Sollten die eingesetzten Komponenten über keine der erwähnten Funktionen verfügen, ist eine individuelle Umkonfiguration oder die physische Zerstörung des Speichers erforderlich.

**Lizenzschlüsselverwaltung**

Es muss geprüft werden, ob Softwarelizenzen (z. B. für Antiviren-Software) nicht mehr benötigt und daher abbestellt werden können.

**Dokumentation**

Eine Abschlussdokumentation über die Datenmigration und die Datenlöschung ist anzulegen.

Die Dokumentation zur Notfallplanung ist zu kontrollieren und zu aktualisieren. Auch funktionale Abhängigkeiten in Planungen zum Wiederanlauf nach Störungen müssen an die neue Konfiguration angepasst werden. In der Notfall-

dokumentation und der Betriebsdokumentation dürfen keine Verweise mehr auf die außer Betrieb genommene Speicherlösung existieren.

Prüffragen:

- Wird sichergestellt, dass alle Nutzdaten und Konfigurationsdaten sicher gelöscht werden, wenn diese nicht mehr benötigt werden?
- Wurde eine Übergangsphase für die Einführung einer neuen Speicherlösung eingeplant?
- Werden Verweise auf die außer Betrieb genommene Speicherlösung aus allen relevanten Dokumenten entfernt?

# M 2.362 Auswahl einer geeigneten Speicherlösung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um fundiert zu entscheiden, welche Speicherlösung im jeweiligen Anwendungsfall angemessen ist, sind die technischen Grundlagen unterschiedlicher Techniken detailliert zu beleuchten und deren Auswirkungen auf den möglichen Einsatz in der Institution zu prüfen. Die Entscheidungsgrundlagen müssen dabei nachvollziehbar dokumentiert werden.

### Network Attached Storage

NAS-Systeme sind spezielle Speichersysteme, die dem Client Speicherplatz als nutzbares Dateisystem zur Verfügung stellen. Als Dateisystem werden hierfür meistens Windows (SMB/CIFS) oder Unix (NFS) zur Auswahl gestellt. NAS-Systeme sind sehr einfach in eine bestehende Netzinfrastruktur zu integrieren. Sie können wie Server an das Netz der Institution angeschlossen werden. Entsprechend sind NAS-Systeme oft als "Appliance" ausgeführt. Sie werden betriebsfertig ausgeliefert und können nach einigen elementaren Konfigurationen (z. B. der Netzeinstellungen) in Betrieb genommen werden. Basissoftware eines NAS-Systems ist üblicherweise eine für diesen Einsatzfall minimierte und optimierte Version eines Standard-Betriebssystems (häufig Unix oder Linux, gegebenenfalls auch Windows).

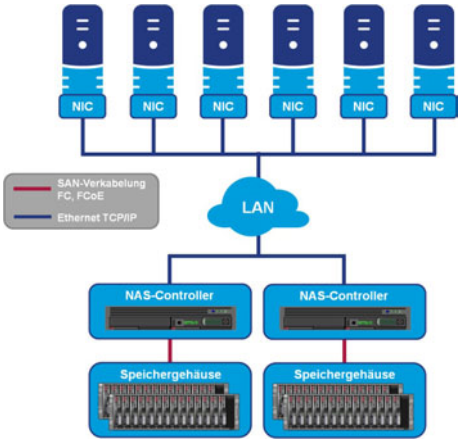



Abbildung: Schematische Darstellung eines Network Attached Storage

Die einfache Anbindung erweist sich gleichzeitig als ein Nachteil von NAS, da die NAS-Systeme über Ethernet-Technik mit den Servern beziehungsweise Clients verbunden sind. Die darunter liegenden TCP/IP-Protokolle haben einen relativ geringen Durchsatz und verwenden dabei einen relativ großen Protokoll-Overhead. So sind sie im Grunde nicht für den schnellen Zugriff auf Massenspeicher ausgelegt. Werden NAS-Systeme eingesetzt, kann daraus eine hohe Belastung des LANs folgen. In vielen Anwendungsfällen ist jedoch festzustellen, dass eine Gigabit-Ethernet-Anbindung im Realbetrieb hinreichend schnell ist und durch eine geeignete Architektur des LANs Engpässe de facto nicht zu beobachten sind.

Durch die Verwendung von Standardnetzen und Standardprotokollen besitzen NAS-Systeme die gleichen Schwachstellen, die auch Unix- oder Windows-Server betreffen.

Weniger geeignet sind Standard-NAS-Systeme als Speicherlösung für Anwendungen, die nicht dateiorientiert arbeiten. Darunter fallen alle größeren Datenbanken und zum Beispiel auch Microsoft Exchange-Server. Wenn eine solche Anwendung auf einem NAS-System betrieben werden soll, ist zu überprüfen, ob Produkte am Markt verfügbar sind, die spezifisch für den Betrieb des Produktes und das Einsatzszenario optimiert sind.

Ein NAS-System kann oft für eine Reihe von Servern zum Einsatz kommen. Obwohl die reinen Hardwarekosten meistens deutlich höher sind als der Ausbau der einzelnen Server mit mehr und/oder größeren Festplatten, kann dadurch die Verfügbarkeit erheblich verbessert werden. Deutliche Vorteile liegen in der oft vorhandenen Möglichkeit, durch Konfiguration des Geräts oder Hardwareerweiterungen im laufenden Betrieb Kapazitätsanforderungen ohne Stillstand zu erfüllen. Verbesserungen sind auch bei der Datensicherung zu erzielen. Mit direkt angeschlossenen Datensicherungsgeräten (Bandlaufwerken, Optical Discs, Jukeboxen zur Archivierung) ausgestattet, kann eine Vereinfachung, Beschleunigung und Stabilisierung bei der Sicherung von Datenbeständen, die über gewachsene Serverlandschaften verteilt sind, erzielt werden.

Ein Nachteil von einfachen NAS-Systemen ist, dass ein Ausfall oft weiter reichende Folgen hat als der Ausfall eines einzelnen Servers und dass ein Ausfall nicht einfach durch ein in der Institution kurzfristig verfügbares Ersatzsystem kompensiert werden kann.

**Storage Area Networks**

SANs bestehen aus Plattensubsystemen, Datensicherungssystemen und einer eigenen Netzinfrastruktur. Plattensubsysteme fassen intern eine Menge von Festplatten zusammen. Hier wird unterschieden, ob diese Zusammenfassung lediglich durch ein gemeinsames Gehäuse und eine gemeinsame Stromversorgung geschieht (JBOD = Just a Bunch of Disks) oder ob ein spezielles Schaltgerät, der sogenannte RAID-Controller mithilfe der RAID-Technik (RAID = Redundant Array of Independent Discs) die physischen Festplatten zu virtuellen Festplatten zusammenfasst. Darüber hinaus gibt es intelligente RAID-Controller, die weitere Dienste zur Verfügung stellen können.

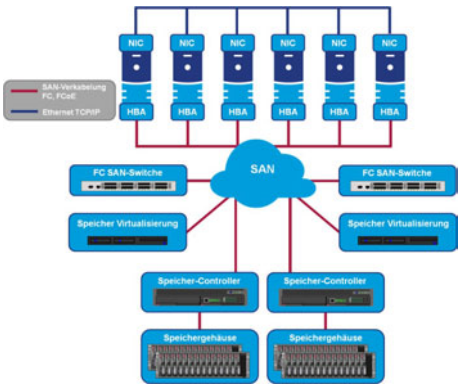



Abbildung 2: Schematische Darstellung eines Storage Areas Networks

Durch die Zusammenfassung mehrerer physischer Festplatten zu virtuellen Einheiten (Pools), auch "Speichervirtualisierung durch Pooling" genannt, kann

durch geschicktes Kombinieren von physischen Festplatten die Ausfallsicherheit oder die Performance des Gesamtsystems oder beides erhöht werden. Der Speicher-Controller zeigt nach außen nur die zusammengefassten Festplatten (virtuelle Festplatte oder logisches "Volume") und verteilt die Daten, die er auf einer solchen Festplatte schreiben soll, auf die einzelnen physischen Festplatten.

Diese Funktionalität kann auch im Server mithilfe einer speziellen Applikation, dem "Volume Manager", umgesetzt werden, wobei dann der Server stärker belastet wird.

Es existieren verschiedene Algorithmen, nach denen die Datenverteilung geregelt wird, die sogenannten RAID-Level. Wenn das RAID-Level die Speicherung von redundanten Informationen unterstützt, bleiben die gespeicherten Informationen selbst nach dem Ausfall einer Festplatte intakt und können rekonstruiert werden. Oft können einzelne Festplatten des Plattensubsystems im laufenden Betrieb ausgetauscht werden ("hot swap").

Plattensubsysteme bieten die Möglichkeit, alle Teilkomponenten redundant auszulegen und können somit zur Erhöhung der Verfügbarkeit eingesetzt werden. Ein weiterer Vorteil ist, dass durch passende Konfigurationsmechanismen der einer Anwendung zugeordnete Speicherplatz an ihren Platzbedarf angepasst werden kann.

Ein Plattensubsystem stellt lediglich Speicher für die Anwendungen zur Verfügung. Selbst bei redundanter Speicherung der Daten ist eine zusätzliche Datensicherung notwendig, da z. B. logische Fehler beim Datenbestand durch Hardwareredundanz im Speichersystem nicht korrigiert werden können. Als Systeme zur Datensicherung sind Bandlaufwerke, optische Medien, aber auch wiederum spezielle Festplattensysteme nutzbar. Auch diese Geräte werden direkt in das Speichernetz integriert.

SANs verwenden eine eigene Netzhardware und eigene, für den Anwendungsfall geeignete schnelle Netzprotokolle. Meistens sind Glasfaserkabel im Einsatz (Systembezeichnung: Fibre Channel, kurz FC). Ein einfaches Storage Area Network besteht aus einem Fibre-Channel-Switch oder -Director (größere Switches, die mit mehr Funktionalität ausgestattet sind, werden oft als Director bezeichnet), einem oder mehreren Plattensubsystemen und den Servern, die über sogenannte Host Bus Adapter, kurz HBA, mit dem Fibre-Channel-Switch verbunden werden.

Fibre-Channel-Netze verwenden ein spezielles, an die Anforderung von Massenspeichernutzung angepasstes Protokoll, das hohe Übertragungsraten ermöglicht und deshalb für Speichersysteme sehr geeignet ist. Ebenfalls möglich ist der Einsatz von iSCSI-Geräten. iSCSI nutzt hierbei das IP-Netz und "verpackt" Speicherprotokolle, also Steuerbefehle für Massenspeicher und zugehörige Daten, in IP-Pakete. iSCSI wird eingesetzt, um über eine virtuelle Ende-zu-Ende-Verbindung den Zugriff von Servern mittels iSCSI Host Bus Adapter auf das Speichernetz zu ermöglichen, ohne dass eigene Speichernetze betrieben werden müssen. Vorhandene Netzkomponenten (LAN-Switches) können genutzt werden, es muss keine neue oder von der vorhandenen Netztechnik verschiedene Hardware für die Verbindungen zwischen Servern und Speichergeräten eingesetzt werden. Der Begriff SAN wird im Folgenden für beide Techniken verwendet. Wenn eine Unterscheidung notwendig sein sollte, wird "Fibre Channel SAN" oder FC-SAN und entsprechend iSCSI-SAN oder IP-SAN verwendet.

Ein großer Vorteil von SANs ist ihre Desaster-Toleranz. Das Konzept des Multi-Pathings, das im SAN konsequent verfolgt wird, spielt dabei eine wesentliche Rolle: Falls es einem Server möglich ist, ein Plattensubsystem über mehrere Host Bus Adapter und über unterschiedliche Netzverbindungen zu erreichen, so kann der Datentransfer zwischen beiden Systemen auf mehrere Datenwege verteilt werden. Durch den Einsatz mehrerer Host Bus Adapter in den Servern und die Präsentation der virtuellen Festplatten auf mehreren Schnittstellen eines Plattensubsystems lassen sich somit die mögliche Übertragungsgeschwindigkeit und Verfügbarkeit des Speichersystems effektiv steigern. Wenn zwei oder mehr Host Bus Adapter in einem Server genutzt werden, so wird bei Ausfall eines Adapters die Last auf den oder die verbleibenden HBAs verlagert. Dieses für Betriebssystem und Anwendungen transparente "Failover" verbessert somit die Verfügbarkeit des Servers. Entsprechend kann durch eine redundante Auslegung aller Teilkomponenten eines SANs eine sehr hohe Ausfallsicherheit erreicht werden. Die Maßnahme M 2.354 *Einsatz einer hochverfügbaren SAN-Lösung* beschreibt dieses Thema ausführlicher.

So wäre es in einem kleinen Storage Area Network denkbar, dass sich an zwei möglichst weit auseinander liegenden Orten auf dem Betriebsgelände jeweils ein baugleiches Speichersystem befindet. Jedes dieser Speichersysteme ist mit einem von zwei wiederum getrennt installierten Switchen verbunden. Um eine redundante Verbindung zum SAN zu gewährleisten, verfügen die Server zumindest über zwei Host Bus Adapter, sodass jeder Host Bus Adapter mit einem der beiden SAN-Switches verbunden ist. Somit wäre ein Ausfall einzelner Leitungen, eines HBAs, eines Switches oder sogar eines Speichersystems ohne Beeinträchtigung der Gesamtsystemleistung denkbar.

Beim Design eines SANs ist es leicht möglich, Redundanzen zu schaffen, sodass ein Ausfall einzelner Komponenten wie Kommunikationsleitungen, Switchen oder sogar eines Plattensubsystems, keine Beeinträchtigung der Gesamtsystemleistung bewirkt.

Bei höchsten Anforderungen an die Verfügbarkeit kann dieser Ausbau so erweitert werden, dass in zwei oder mehr räumlich weit auseinander liegenden (bis zu 100 km) und technisch autarken Rechenzentren jeweils in allen Komponenten redundante SANs aufgebaut werden. So kann im Extremfall der Ausfall eines kompletten Rechenzentrums ohne Betriebsunterbrechung oder Kapazitätsverlust für die Anwender kompensiert werden.

Weitere Redundanz lässt sich durch "Cluster"-Server erreichen, die eine logische Maschine auf zwei oder mehr physische Server verteilen. Dabei wird eine Anwendung auf zwei oder mehr Servern installiert. Diese Server arbeiten mit denselben Anwendungsdaten. Falls ein Server eine Störung erleidet, übernimmt der zweite Server automatisch die Arbeit der ausgefallenen Hardware.

Erkauft werden die positiven Eigenschaften einer SAN-Lösung durch Preis und Komplexität. Die selbe Menge Speicher ist in der Realisierung durch ein SAN um ein Vielfaches teurer als in der Ausführung als Direct Attached Storage oder NAS.

Zudem ist auch die Planung und der Aufbau eines SANs sehr komplex, sodass die Institution speziell geschultes Personal einstellen muss oder externe Unterstützung benötigt.

### Zusammenfassung

Kurz dargestellt ist NAS eine Speicherlösung mit dateibasiertem Zugriff, SAN eine Speicherlösung mit blockbasiertem Zugriff. SAN setzt also "tiefer" an und bietet alle technischen Möglichkeiten, die für die Datenspeicherung angeboten werden. NAS ist als Erweiterung der Serverlandschaft einer Institution anzusehen.

### Hybrid-Storage

Eine Speicherlösung, die eine Kombination zwischen NAS und SAN darstellt, wird oftmals unter der Bezeichnung Hybrid-Storage oder kombinierte Speicherlösung (Unified Storage) geführt.

Der interne Aufbau solcher Systeme erfüllt alle Kriterien eines SANs. Nach außen können sie jedoch sowohl als NAS als auch als SAN betrieben werden. Dieser Mischbetrieb wird durch den Einsatz entsprechender Systemkomponenten und eine entsprechende Konfiguration ermöglicht. So kann sich ein Speichersystem sowohl für einige Anwendungen per Ethernet-Anschluss als "Filer" präsentieren und somit Fileservices über CIFS und NFS zur Verfügung stellen als auch für andere Server per Fibre Channel oder iSCSI Speicherkapazität zugänglich machen.

In der Praxis können NAS- und Storage-Controller entweder in einem IT-System zusammengefasst werden oder als physisch getrennte Komponenten vorliegen. Neben klassischen Fibre-Channel-SAN-Switchen können auch sogenannte Converged oder Unified Switches zum Einsatz kommen, die neben FC auch Fibre Channel over Ethernet (FCoE) und IP bedienen.

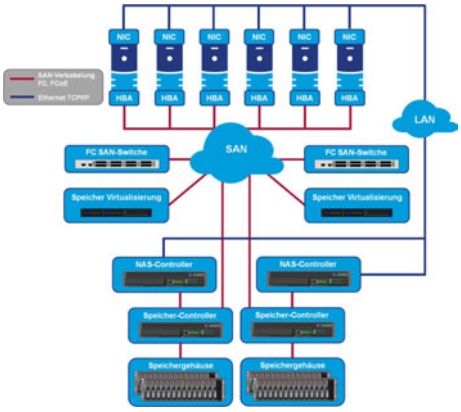



Abbildung 3: Schematische Darstellung eines Hybrid-Storage

### Objekt-Storage

Objekt-Storage (oftmals auch als "Object-based Storage" bezeichnet) ermöglicht gegenüber den traditionellen blockbasierten und filebasierten Zugriffsmethoden einen objektbasierten Zugriff.

Objektbasierende Speicherlösungen speichern Daten in Verbindung mit den zugehörigen Metadaten auf einem Datenträger in Form von Objekten und nicht in Form von Dateien. Mittels der Vergabe einer eindeutigen Objekt-ID (Hash-Wert), die in den Metadaten des Objekts festgehalten wird, kann das Objekt eindeutig identifiziert werden. Der Zugriff auf einen objektbasierenden Speicher erfolgt über eine führende Anwendung. Die Anwendung greift hierbei über eine spezielle API und deren mögliche Kommandos oder direkt per IP auf den

Objekt-Storage zu. Im Falle eines Zugriffs per API muss die führende Applikation die herstellerspezifische API des gewählten Objekt-Storage unterstützen.

Objekt-Storage wird vor allem im Bereich Archivierung, Dokumentenmanagement und beim Ablegen von Objekten in einer Cloud eingesetzt.

**Cloud-Storage**

Im Zusammenhang mit Weiterentwicklungen im Storageumfeld etabliert sich zunehmend auch der Begriff des Cloud-Storage. Hierunter ist Storage für die Cloud-Nutzung zu verstehen. Die Speicherlösung an sich bleibt dabei weitgehend unverändert, jedoch liegt eine von klassischen SAN- oder NAS-Architekturen abweichende Art des Zugriffs auf die gespeicherten Daten vor. Dieser wird in der Regel mittels Web-Services realisiert.

Prüffragen:

- Sind bei der Planung der Speicherlösung die Möglichkeiten und Grenzen der verschiedenen Arten von Speicherlösungen für die Verantwortlichen der Institution transparent gemacht worden?
- Sind die Entscheidungskriterien für die Auswahl einer geeigneten Speicherlösung nachvollziehbar dokumentiert worden?
- Ist die Entscheidung für die Auswahl der Speicherlösung nachvollziehbar dokumentiert?

# M 2.363 Schutz gegen SQL-Injection

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Anwendungsentwickler

Um die Ausnutzung von SQL-Injections (siehe G 5.131 *SQL-Injection*) zu verhindern oder zumindest zu erschweren, sind eine Reihe von Maßnahmen zu ergreifen. Diese erstrecken sich über alle Komponenten einer Anwendung, von der Applikation selbst über den Server bis hin zum Datenbank-Managementsystem (DBMS).

**Maßnahmen bei der Programmierung von Applikationen**

Eine der wichtigsten Maßnahmen zur Vermeidung von SQL-Injection ist die sorgfältige Überprüfung und Filterung von Eingaben und Parametern durch die Applikation. Überprüft werden sollte, ob die übergebenen Daten dem erwarteten Datentyp entsprechen. Wird z. B. ein numerischer Parameter erwartet, kann man diesen in PHP ("PHP: Hypertext Preprocessor") mit der Funktion *is_numeric()* prüfen. Die Filterung hingegen muss dafür sorgen, dass Sonderzeichen wie das Quote-Zeichen ('), das Semikolon (;) und doppelte Bindestriche (--) ignoriert werden.

Sicherer ist der Einsatz von *Stored Procedures* beziehungsweise *Prepared SQL-Statements*. Diese werden von vielen Datenbank-Managementsystemen (DBMS) angeboten und sind ursprünglich dazu gedacht, häufiger auftretende Abfragen zu optimieren. Der Vorteil dieser parametrisierten Statements ist, dass Parameter nicht mehr direkt in ein SQL-Statement eingebunden werden. Vielmehr werden diese getrennt vom SQL-Statement separat an die Datenbank übergeben. Das Zusammenführen von Statement und Parametern erfolgt durch das DBMS selbst, wobei die oben genannten Sonderzeichen **automatisch** maskiert werden.

Um potentiellen Angreifern keine Anhaltspunkte für Angriffe zu liefern, sollte besonderes Augenmerk darauf gelegt werden, dass Applikationen möglichst keine Fehlermeldungen nach außen ausgeben, die Rückschlüsse auf das verwendete System oder auf die Struktur der dahinterliegenden Datenbank zulassen.

**Serverseitige Maßnahmen**

Die wichtigste Sicherheitsmaßname auf dem Server ist das Härten des Betriebssystems. Um so wenig Angriffspunkte wie möglich zu bieten, werden dabei Maßnahmen ergriffen wie:

- das Deaktivieren nicht benötigter Dienste,
- das Löschen nicht benötigter Benutzerkonten,
- das Einspielen relevanter Patches und
- das Löschen aller für die Funktion des Servers unnötigen Bestandteile.

Darüber hinaus sollte der Einsatz eines Application-Level-Gateways (ALG) (siehe M 5.117 *Integration eines Datenbank-Servers in ein Sicherheitsgateway*) erwogen werden. ALGs können auf Applikationsebene die Daten überwachen, die zwischen Webbrowser und Anwendung ausgetauscht werden, und verhindern, dass schädliche Daten den Server erreichen.

Eine weitere zusätzliche Sicherheitsmaßnahme stellt der Einsatz von Intrusion-Detection-Systemen (IDS) und Intrusion-Prevention-Systemen (IPS) dar. IDS analysieren den über ein Netz übertragenen Datenverkehr und erkennen potentiell gefährliche Daten. Die dazu eingesetzten Analysetechniken unter-

teilen sich in *Misuse* und *Anomaly Detection*. Die Misuse Detection versucht, bereits bekannte Angriffsmuster zu erkennen. Die Anomaly Detection verfolgt den Ansatz, die zulässigen Verhaltensmuster zu lernen und Abweichungen davon als Angriff zu identifizieren. Während ein IDS in der Lage ist, Angriffe zu erkennen und Warnungen auszugeben, ist ein IPS in der Lage, entsprechende Reaktionen auszuführen. Die Reaktion kann beispielsweise darin bestehen, die Verbindung zu blockieren, Daten zu verwerfen oder zu ändern.

Bei erhöhten Sicherheitsanforderungen sollte geprüft werden, ob der Einsatz von IDS beziehungsweise IPS zweckmäßig ist.

**Datenbankseitige Maßnahmen**

Ebenso wie beim Betriebssystem sollte auch eine Härtung der Datenbank erfolgen. Im Falle der Datenbank bedeutet dies z. B.:

- das Entfernen nicht benötigter Stored Procedures,
- das Deaktivieren nicht benötigter Dienste,
- das Löschen nicht benötigter Benutzerkonten und Default Accounts und
- das Einspielen relevanter Patches.

In diesem Zusammenhang sollte auch ein speziell für den Datenbankzugriff vorgesehener Account angelegt werden, der mit möglichst eingeschränkten Zugriffsrechten auskommen sollte.

Darüber hinaus sollten sensitive Daten, wie z. B. Passwörter, in der Datenbank soweit möglich nur verschlüsselt gespeichert werden.

Von vielen Herstellern werden mittlerweile sogenannte Schwachstellen-Scanner angeboten, die sowohl Applikationen als auch Datenbanken auf Sicherheitslücken, wie beispielsweise mögliche SQL-Injections, überprüfen können.

**Beispiel für prinzipielles Vorgehen zur Erstellung von sicherem Code bei Verwendung von PHP und MySQL:**

In PHP verhindert die Funktion mysql_real_escape_sting() die Übergabe von Sonderzeichen an eine MySQL-Datenbank. Die Funktion maskiert die in dem übergebenen String enthaltenen Sonderzeichen wie z. B. Quotes und verhindert so SQL-Injections.

Anstatt der folgenden Syntax:

```
$query = "SELECT * FROM users
WHERE username=
'" . $_POST['username'] . "'
AND password=
'" . $_POST['password'] . """;
```

sollte also diese Syntax verwendet werden:

```
$query = "SELECT * FROM users
WHERE username=
'" . mysql_real_escape_string($_POST['username']) . "'
AND password=
'" . mysql_real_escape_string($_POST['password']) . """;
```

**Beispiel für sicheren Code bei Verwendung von ASP mit ADO und SQL-Server:**

Die Verwendung eines prepared Statements für das obige Beispiel sieht in diesem Fall folgendermaßen aus:

```
$query = "SELECT * FROM users WHERE username=?
AND password=?"
Set cmd = Server.CreateObject("ADODB.Command")
cmd.CommandText = query
cmd.CommandType = adCmdText
Set param = cmd.CreateParameter("",adVarChar, adParamInput,
nMaxUsernameLength, strUsername)
cmd.Parameters.Append
Set param = cmd.CreateParameter("",adVarChar, adParamInput,
nMaxUsernameLength, strPassword)
cmd.Parameters.Append
Set rs = cmd.Execute()
```

Hierbei ist zu beachten, dass die oben aufgeführten Code-Beispiele nur den grundsätzlichen Ansatz zur Vermeidung von SQL-Injection veranschaulichen sollen.

Prüffragen:

- Werden Eingaben und Parameter durch die Applikation vor Weiterleitung an das Datenbanksystem sorgfältig überprüft und gefiltert?
- Werden Stored Procedures beziehungsweise Prepared SQL Statements eingesetzt?
- Ist gewährleistet, dass keine Fehlermeldungen nach außen ausgeben werden, welche Rückschlüsse auf das verwendete System oder auf die Struktur der dahinterliegenden Datenbank zulassen?

# M 2.364 Planung der Administration ab Windows 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Vor der Einführung eines Windows-Servers ab der Version 2003 sind umfangreiche Planungen durchzuführen, damit er geregelt und sicher eingeführt sowie anschließend sicher betrieben werden kann. Aus der Beschreibung des Einsatzszenarios und der Definition des Einsatzzwecks ergeben sich Anforderungen an die Administration. Sie muss anhand der Vorgaben der Sicherheitsrichtlinie erfolgen (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*) und dokumentiert werden. Darin sollte unter anderem darauf hingewiesen werden, dass die Verwendung des Servers in der Rolle einer Arbeitsstation eines Benutzers zu unterlassen ist. Administrative Änderungen, die im laufenden Betrieb durchgeführt werden, können sicherheitsrelevante Nebeneffekte hervorrufen und sollten daher nur mit besonderer Sorgfalt durchgeführt werden.

Die Administration kann vor Ort mit dem Zugang zur Konsole des Servers, von einem anderen Computer innerhalb des LAN oder von außerhalb, zum Beispiel über VPN erfolgen. Bei der Planung der Aufgaben und Berechtigungen der Administratoren sind Regelungen zuer Zutrittsberechtigung zu treffen (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*). Dabei ist die vorher erarbeitete Funktionstrennung (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) zu beachten. Unnötige Zutritts- und Zugriffsrechte zum Server sind zu vermeiden. Die Aufgabenbereiche der Windows Server-Administratoren müssen schriftlich festgehalten und mit den Sicherheitsrichtlinien der Institution abgestimmt werden.

**Typische administrative Aufgaben**

Administration müssen regelmäßig diverse Aktionen durchführen, um die IT-Systeme zu aktualisieren, pflegen und betriebsbereit zu halten. Hierzu gehören unter anderem folgende Tätigkeiten:

- Ereignisanzeige überwachen
- Software installieren, warten und deinstallieren
- Windows-Komponenten hinzufügen/ändern/entfernen
- Aktualisierungen (Windows Update)
- Auslastung kontrollieren
- Funktion der Hardware überwachen
- Funktion von Applikationen und Diensten überwachen
- Dateisystem warten
- Rechte entsprechend neuer Anforderungen anpassen
- Benutzer/Gruppenverwaltung, neue Benutzer/Gruppen anlegen, verschieben oder löschen
- Anpassungen am OU Design vornehmen
- Änderungen oder Anpassungen am Active Directory vornehmen
- Daten sichern
- Netzkonnektivität prüfen
- Virenschutz prüfen und warten
- Registrierdatenbank warten
- Datum/Uhrzeit/Zeitzonen administrieren

**Eingebaute Standardgruppen für die Administration**

Die Administration eines Windows-Servers erfordert weitreichende Berechtigungen und somit ein geeignetes Berechtigungskonzept. Folgende lokale Sicherheitsgruppen für die Administration sind nach einer Standardinstallation vorhanden:

**Systemdefinierte Sicherheitsgruppen**

| Gruppe | Server 2003 | Server 2008 | Beschreibung |
|---|---|---|---|
| Administratoren | X | X | Vollzugriff auf alle Bereiche, sehr sicherheitskritisch |
| Hauptbenutzer | X | X | umfangreicher Zugriff auf Systemeinstellungen, mit einigen Einschränkungen: Hauptbenutzer können z. B. nicht den Besitz von Dateien übernehmen, Gerätetreiber laden oder entladen, Sicherheits- und Systemprotokolle verwalten, Dienste installieren |
| Sicherungs-Operatoren | X | X | Lese- und Schreibzugriff auf alle Dateien |
| Remoteunterstützungsanbieter | X | X | nur in Active Directory-Umgebung vorhanden, dürfen von Ferne an einer Konsolensitzung teilnehmen ("Shared Desktop"), erhalten somit die Rechte des angemeldeten Benutzers. Für Fernadministration ungeeignet, besser geeignet ist *Remotedesktop* |
| Hilfedienstgruppe | X | | mit Hilfe dieser Gruppe können Administratoren gemeinsame Rechte für alle Supportan- |

| Gruppe | Server 2003 | Server 2008 | Beschreibung |
|---|---|---|---|
| | | | wendungen festlegen, kann hohes Sicherheitsrisiko verursachen |
| Netzwerkkonfigurations-Operatoren | X | X | Eigenschaften von Verbindungen im Ordner *Netzwerkverbindungen* administrieren |
| Druck-Operatoren | X | | Administration von Druckern und Druckerwarteschlangen |
| Leistungsprotokollbenutzer | X | X | Administration der Konsole *Leistung* (*perfmon.exe*) |
| Distributed COM-Benutzer | X | X | Administration der Konsole *Komponentendienste* |
| Systemmonitorbenutzer | X | X | lesender Zugriff auf Leistungszähler und -protokolle |
| Benutzer | X | X | erlaubt Anmeldung an Mitgliedsservern und alleinstehenden Servern |
| Remotedesktopbenutzer | X | X | Gruppe zur Steuerung der Remote-Desktop-Einwahlmöglichkeit |
| TelnetClients | X | | Gruppe zur Steuerung der Telnet-Einwahlmöglichkeit |
| Replikations-Operator | X | X | vom Betriebssystem verwendete Gruppe, darf nicht für Benutzer verwendet werden |
| Gäste | X | X | Steuerung des Ressourcenzugriffs für Benutzer ohne Anmeldung, darf nicht für Benutzer verwendet werden |
| Kryptographie-Operatoren | | X | Mitglieder dieser Gruppe sind auto- |

| Gruppe | Server 2003 | Server 2008 | Beschreibung |
|---|---|---|---|
| | | | risiert, kryptographische Vorgänge auszuführen. |
| IIS_IUSRS | | X | hierbei handelt es sich um eine integrierte Gruppe, die von Internetinformationsdienste (Internet Information Services, IIS) verwendet wird. |

Hinweis:

Die Standardgruppen auf einem Domänencontroller unterscheiden sich zum Teil von den hier genannten.

Für die Aufgabenerfüllung der Administration gibt es im Betriebssystem Sicherheitsgruppen, wie die Gruppe *Administratoren*, die vollen administrativen Zugriff auf alle Bereiche des Servers haben und somit die Sicherheit erheblich beeinflussen können. Für definierte Einsatzzwecke, zum Beispiel *Dateiserver*, sind Sicherheitsgruppen mit nicht vollen administrativen Rechten einzuplanen. So können administrative Aufgaben wie das Erstellen einer Datensicherung unter Verwendung der Gruppe *Sicherungsoperatoren*, sowie die damit einhergehenden Gefährdungen auf ihre Teilbereiche im Server beschränkt werden. Für Benutzergruppen und deren Mitglieder ist immer das Prinzip der minimal nötigen Berechtigungskombination einzuhalten. So sollte betrachtet werden, ob es ausreicht, die Administrationsaufgaben mit den geringeren Rechten der Sicherheitsgruppe *Hauptbenutzer* durchzuführen (siehe M 5.10 *Restriktive Rechtevergabe*). Bei einem bestehenden Netz ist zu berücksichtigen, ob für die festgelegten Aufgaben mit den vorhandenen Sicherheitsgruppen aus dem Active Directory oder dem lokalen Server gearbeitet werden kann (zu berücksichtigen ist G 2.115 *Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen ab Windows Server 2003*).

Die Installation von zusätzlichen Komponenten erweitert die Auswahl von Standardgruppen, die für die Administration in Frage kommen. Ein Beispiel hierfür ist die Sicherheitsgruppe *Terminalserverbenutzer* bei installierten Terminalserverdiensten oder *DHCP-Administratoren* bei installiertem DHCP-Dienst. Die Festlegung auf vorhandene Sicherheitsgruppen ist jedoch nicht immer geeignet, da deren Rechte nicht angepasst werden können. Daher ist eine für die festgelegten Administrationsaufgaben angepasste Sicherheitsgruppe zu nutzen.

Um Fehler zu vermeiden, ist genau festzulegen, für welche administrativen Aufgaben die Berechtigungen der Gruppe *Administratoren* wirklich erforderlich sind. Zum Beispiel können Änderungen des Vollzugriffs im Dateisystem standardmäßig nur durch die Gruppe *Administratoren* erfolgen (für weitere Informationen siehe M 4.149 *Datei- und Freigabeberechtigungen unter Windows*), andererseits hat die Gruppe *Administratoren* immer Zugriff via Remotedesktop auf jeden Server, unabhängig von der Gruppe *Remotedesktopbenutzer*. In größeren Umgebungen sollten immer die Gruppen mit dem niedrigsten administrativen Zugriffsniveau bevorzugt werden. Bei Bedarf können Berechtigungen um Gruppen mit höherem Zugriffsniveau ergänzt werden.

**Selbstdefinierte Gruppen**

Weiterhin können selbstdefinierte Sicherheitsgruppen entworfen werden, welche die Berechtigungen für eine definierte administrative Aufgabe enthalten. Eigene Gruppen können entsprechend ihres Zugriffsniveaus in der oben genannten Auflistung ergänzt werden.

Bei der Planung muss geprüft werden, ob Programme ungewollt mit zu weitreichenden administrativen Berechtigungen aufgerufen werden, um zu verhindern, dass die Programme dadurch Zugriff auf kritische Bereiche des Servers erhalten und die Sicherheit des Servers gefährden können.

**Benutzerkonten für die Administration**

Bei der Betrachtung der Arbeitsaufgaben, die eine Person mit einem autorisierten Benutzerkonto in einer IT-Umgebung durchführt, muss für Administratoren eine grundlegende Abgrenzung gefunden werden:

- Welche Aufgaben betreffen die Nutzung des IT-Systems?
- Welche Aufgaben betreffen die Administration des IT-Systems?

Es ist sehr zu empfehlen, diese Betrachtungsweise in zwei separaten Konten für eine Person abzubilden. Da die eingebauten Standardgruppen von Windows-Servern keine spezielle Nutzung als Administrator oder Benutzer erzwingen, sollten ein normales Benutzerkonto für das tägliche Arbeiten und ein administratives Konto für administrative Aufgaben vorhanden sein und dementsprechend genutzt werden.

Es ist wichtig, einen definierten und dokumentierten Prozess für die Einrichtung und Entfernung von Benutzerkonten zu implementieren. Dies ist besonders wichtig für administrative Konten.

Das Ziel ist immer, die Anmeldung einer Benutzersitzung auf einem Windows-Server oder Windows-Verwaltungscomputer mit so geringen Berechtigungen wie möglich durchzuführen, am besten mit normalen Benutzerrechten. Mehrere grundlegende Ansätze sind hierfür denkbar:

- **Sekundäre Anmeldung auf dem Server**
  Auf dem zu administrierenden Server wird eine normale Benutzersitzung mit eingeschränkten Rechten angemeldet, Administrationswerkzeuge werden mit Hilfe der sekundären Anmeldung (*Ausführen als*... oder *runas*) mit dem entsprechenden administrativen Benutzerkonto auf dem Server ausgeführt. In diesem Fall ist zu überlegen, ob normalen Benutzern die lokale Anmeldung auf einem Server erlaubt wird (Standardeinstellung) oder ob hierfür eine separate Sicherheitsgruppe entworfen wird.
- **Einrichten einer Verwaltungsstation**
  Für den Betrieb einer Verwaltungsstation ist *Active Directory* zu empfehlen (M 2.229 *Planung des Active Directory*). Die Anmeldung an der Verwaltungsstation erfolgt mit einem Benutzerkonto, das auf diesem Computer nur geringe Berechtigungen besitzt (z. B. Benutzer). Von der Verwaltungsstation aus wird auf die zu administrierenden Server mit entsprechenden Werkzeugen (siehe unten) zugegriffen. Entweder hat das Benutzerkonto dort die erforderlichen Berechtigungen, oder der Zugriff erfolgt mit Hilfe der sekundären Anmeldung. Dadurch ist in den meisten Fällen keine komplette Anmeldung mit administrativen Berechtigungen nötig.
- **Lokales Anmelden mit erweiterten Berechtigungen**
  In diesem Szenario sollte das lokale Anmelden an Servern generell unterbunden und nur für ausgewählte administrative Benutzerkonten freigeschaltet werden. Diese Benutzerkonten sollten genau für die vorgesehene

Aufgabe angepasst sein. Weitere Einschränkungen dieser Konten, zum Beispiel durch festgelegte Anmeldezeiten, sind zu empfehlen. Ab Windows Server 2008 werden die Risiken bei dieser Vorgehensweise durch die Benutzerkontensteuerung begrenzt (siehe hierzu M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*).

Es empfiehlt sich, die jeweiligen Strategien in einer Richtlinie für die Windows-Server-Umgebung zu vermerken.

**Konfigurationsänderungen**

Es muss bei der Planung beachtet werden, dass administrative Änderungen im laufenden Betrieb hinsichtlich Verfügbarkeit und Zuverlässigkeit als kritisch zu betrachten sind (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Bei der Planung der administrativen Aufgaben muss also unterschieden werden, welche Aufgaben während des laufenden Betriebs und welche Aufgaben nur in speziellen Wartungsfenstern durchgeführt werden können. Dies ist stark von der Konfiguration des Servers, den zusätzlichen Serverapplikationen und den Verfügbarkeitsanforderungen abhängig. Konfigurationsänderungen sollten vorzugsweise nur in speziellen Wartungsfenstern durchgeführt werden, da unter Umständen Neustarts des Servers im laufenden Betrieb provoziert werden können.

**Administrationswerkzeuge**

Ein wichtiger Aspekt ist die Auswahl der geeigneten Administrationswerkzeuge für den jeweiligen Server. Die mitgelieferten Werkzeuge bieten eine sehr gute Integration in die Sicherheitsmechanismen des Betriebssystems und ein einheitliches Bedienkonzept. Eingesetzte Werkzeuge müssen den Anforderungen der Sicherheitsrichtlinie der Institution entsprechen.

Die zentralen mitgelieferten Komponenten für die Administration sind:

- *Microsoft Management Console* **(MMC):**
  Fast alle Komponenten sind über ein eigenes MMC-Snap-in zu administrieren. Mit der MMC können Komponenten auf entfernten Servern von einer Verwaltungsstation aus administriert werden. Viele Werkzeuge von Drittherstellern benutzen die MMC als Administrationsoberfläche.
- ***Server Manager*:**
  Ab der Version Windows Server 2008 sind die zentralen Verwaltungsfunktionen im Tool *Server Manager* gebündelt. Für den *Server Manager* steht auch eine Server-Manager-Konsole als MMC-Snap-In zur Verfügung.
- **Fernadministration per Remotedesktop**
  Die Verwendung von Remotedesktops kann die Sicherheit des Servers hinsichtlich Integrität und Vertraulichkeit verringern, siehe G 5.132 *Kompromittierung von RDP-Benutzersitzungen ab Windows Server 2003*. Außerdem entstehen erhöhte organisatorische Anforderungen.
- **Konsolen, die *Internet Information Services* (IIS) erfordern**
  Diese werden für die Administration des Anwendungsservers sowie zum Teil für die Zertifizierungsdienste benötigt. Außerdem setzen viele Werkzeuge von Drittherstellern auf Web-basierte Konsolen. Hierbei entstehen zusätzliche Risiken, so dass gegebenenfalls weitere Maßnahmen umzusetzen sind (siehe M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003*).
- **Kommandozeilenbefehle**
  Viele Komponenten von Windows-Servern können mit Kommandozeilenbefehlen administriert werden. Die Syntax der Kommandos ist teilweise kompliziert, so dass ein erhebliches Risiko für falsche Bedienung und Fehlkonfiguration besteht. Die Verwendung sollte sich auf Fälle konzentrieren,

bei denen GUI-basierte Werkzeuge nicht im erforderlichen Maß zur Verfügung stehen zum Beispiel beim Einsatz eines *Windows Server Core* ab Windows Server 2008).
Einige Einstellungen sind jedoch nur durch entsprechende Kommandozeilenbefehle zu realisieren. Meist ist der konkrete Anwendungsfall explizit dokumentiert, beispielsweise in Artikeln der *Microsoft Knowledge Base*, in der Windows-Hilfe oder in anderen vom Hersteller online bereitgestellten Dokumenten. Es wird empfohlen, die Gewährleistung und den Umfang der Herstellerunterstützung für den konkreten Anwendungsfall vorab mit dem Hersteller zu klären.
Die Verwendung von Kommandozeilenwerkzeugen ist geeignet, wenn eine sehr flexible Automation von Vorgängen erforderlich ist, zum Beispiel mit Hilfe von Skripten. Die Skripte müssen vor Verwendung auf einem Testsystem erprobt werden (siehe M 2.367 *Einsatz von Kommandos und Skripten ab Windows Server 2003*).
Bestimmte Konfigurationsroutinen und Administrationsprogramme von Drittherstellern können weitere Konfigurationsänderungen erfordern, unter anderem wenn diese IIS-Komponenten oder das .NET-Framework voraussetzen. Dadurch kann die Sicherheit des Servers beeinträchtigt werden. Bei der Festlegung ihrer Verwendung ist auf ihre Eignung zu achten (siehe B 1.10 *Standardsoftware*).
Die Verwendung von 16-Bit-Programmen für Administrationszwecke ist generell zu vermeiden.

- **Fernadministration**

  - **Zugriff aus dem LAN**
    Die mitgelieferten Remote-Werkzeuge bieten innerhalb des LAN einen effizienten Zugriff auf Windows-Server. Sofern die Sicherheitsrichtlinie für Windows-Server erfüllt ist, sind für ein normales Sicherheitsniveau keine weiteren Maßnahmen erforderlich. Die Nutzung der im LAN zugelassenen Remote-Werkzeuge, zum Beispiel von Remote-Desktop-Verbindungen, sollten in einer Sicherheitsrichtlinie definiert sein.
  - **Zugriff über Sicherheits-Gateways**
    Der Zugriff über Sicherheits-Gateways sollte auf Grundlage der RAS-Sicherheitsrichtlinie erfolgen. Remote-Werkzeuge können von einem anderen Computer innerhalb des LAN, aber auch von außerhalb, beispielsweise über das Internet, verwendet werden. Für einen Fernzugriff von außerhalb der durch Sicherheits-Gateways geschützten IT-Umgebung müssen der Authentisierungsvorgang und die Datenübertragung verschlüsselt werden. Hierfür ist HTTPS oder ein VPN zu empfehlen. Weiterhin ist zu beachten, dass der Zugriff von externen Clients auf wenige Computer beschränkt wird. Hierfür müssen jedoch alle beteiligten Komponenten in das Administrationskonzept einbezogen werden, zum Beispiel Sicherheits-Gateways, VPN-Gateways und Windows Server 2003-Zertifizierungsdienste.
    Im Rahmen der Planung der Fernadministration muss auch für den entfernten Zugang eine Sicherheitsrichtlinie festgelegt werden. Die durch die organisationsweiten Sicherheitsrichtlinien geltenden Vorschriften sind dazu entsprechend anzupassen und zu erweitern.

**Externe Dienstleister**

Die speziellen Anforderungen beim Outsourcing (siehe B 1.11 *Outsourcing*) sowie vertragliche Vereinbarungen mit externen Dienstleistern müssen in das oben beschriebene Berechtigungskonzept einfließen. Für externe Dienstleister sollten separate Sicherheitsgruppen entworfen werden, die nur in den notwendigen Bereichen über Berechtigungen verfügen. Die vorhandenen Stan-

dardgruppen sind meist nicht geeignet. Beispielsweise ist zu prüfen, ob für einen reinen Datensicherungsdienstleister die Berechtigungen der Gruppe *Sicherungsoperatoren* schon zu weitreichend sind.

Die Übergabe von Anmeldedaten von administrativen Konten sowie die Durchsetzung von Kennwortrichtlinien gestaltet sich besonders schwierig, wenn die beauftragte Person des Dienstleisters nicht vor Ort arbeitet (siehe auch G 2.111 *Kompromittierung von Anmeldedaten bei Dienstleisterwechsel*). Kommt Active Directory zum Einsatz, ist es erst ab Windows Server 2008 möglich, innerhalb einer Domäne unterschiedliche Kennwortrichtlinien für externe Dienstleister zu erzwingen. Dies muss beim Einsatz von Windows Server 2003 daher auf organisatorischer Ebene geregelt und in einer IT-Richtlinie definiert werden.

**Einspielen von Patches und Updates**

Windows-Server ermöglichen das regelmäßige automatische Einspielen von Aktualisierungen. Das Risiko von Diensteunterbrechungen durch automatische Neustarts und von Inkompatibilitäten mit installierten Programmen ist hierbei gegenüber der zeitnahen Schließung von Sicherheitslücken abzuwägen.

Für Server mit hohem Schutzbedarf sollte diese Funktion deaktiviert werden. Bei Servern mit normalem Schutzbedarf ist die Entscheidung für automatische Updates im Einzelfall zu treffen.

Automatische Updates sollten nicht direkt aus dem Internet bezogen werden, sondern über ein Software-Verteilungssystem wie *Windows Server Update Service*, WSUS verwaltet und zum Installieren freigegeben werden (siehe M 4.417 *Patch-Management mit WSUS ab Windows Server 2008*). Hier sind Regeln zu definieren, welche Arten von Updates und Patches automatisch installiert werden und welche der Freigabe durch einen Administrator bedürfen. In jedem Fall ist M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* umzusetzen und zu gewährleisten.

Vor dem Einspielen von Service Packs sollte eine Ausroll-Strategie (Reihenfolge der Server, mögliches Rollback) festgelegt werden. Hierbei ist auch zu berücksichtigen, dass Service Packs bestimmte neue Funktionen enthalten können, die auf Servern mit bestimmten Rollen vorrangig installiert werden müssen. Ein Beispiel hierfür ist die Sicherheitsgruppe *Distributed COM-Benutzer,* die mit Service Pack 1 von Windows Server 2003 neu hinzukam.

**Dokumentation**

Zur Planung der Administration gehört auch der Entwurf eines geeigneten Dokumentationskonzeptes. Es sollte eng an das Änderungsmanagement (M 2.221 *Änderungsmanagement*) angelehnt sein.

Die definierten Aufgaben der Administratoren eines Servers, die entsprechenden Berechtigungen (auch Ressourcenberechtigungen) und die verwendeten Administrator-Werkzeuge sind in die Dokumentation aufzunehmen, um bei Personalausfall den weiteren Betrieb zu ermöglichen (siehe G 1.1 *Personalausfall* und M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).

Es ist ein geeignetes Konzept zur Dokumentation der Kennwörter von Dienstkonten zu entwickeln. Diese Kennwörter sind hochkritisch und müssen einer

strikten Zugriffskontrolle unterliegen, zum Beispiel über einen Tresor, Mehrfachverschlüsselung und Vier-Augen-Prinzip).

Bei der Verwendung von administrativen Skripten muss eine erweiterte Dokumentation angefertigt werden. Die zu dokumentierenden Konfigurationen und Einsatzszenarien können aus der Dokumentation der Testumgebung für Skripte verwendet werden (siehe M 4.240 *Einrichten einer Testumgebung für einen Server*).

Prüffragen:

- Sind die Anforderungen zur Administration von Windows Servern mit den Vorgaben der Sicherheitsrichtlinie der Organisation abgestimmt und dokumentiert?
- Sind die Aufgabenbereiche der Windows Server-Administratoren schriftlich festgehalten und mit den Sicherheitsrichtlinien der Organisation abgestimmt?
- Sind die auf den Windows Servern eingetragenen Benutzergruppen, deren Mitglieder und die sich darauf ergebenen Berechtigungen auf das minimal erforderliche Maß reduziert?
- Werden die Windows Server über angepasste administrative Konten administriert?
- Wird unterschieden, welche Systemänderungen während des laufenden Betriebs und welche Aufgaben nur in speziellen Wartungsfenstern durchgeführt werden können?
- Entsprechen die eingesetzten Administrationswerkzeuge von Windows Server den Anforderungen der Sicherheitsrichtlinie der Organisation?
- Ist das Verfahren zur Fernadministration von Windows Server mit den Sicherheitsanforderungen der Organisation abgestimmt?
- Wurden Regeln definiert, welche Arten von Updates und Patches automatisch installiert werden und welche der Freigabe durch einen Administrator bedürfen?
- Wird der Umgang mit den Kennwörtern der Dienstkonten dokumentiert?

# M 2.365 Planung der Systemüberwachung unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Revisor

Beim Betrieb von Windows Server 2003 werden vielfältige und umfangreiche Ereignisprotokolle erzeugt. Diese Protokolle dienen vorrangig dem Nachweis und der Aufrechterhaltung eines ordnungsgemäßen Betriebes, aber auch der Fehleranalyse. Sie sind oft auch Grundlage von Revisionen oder weiteren Auswertungen.

Aus den Inhalten der Protokolle ergeben sich Aufbewahrungsfristen und zu berücksichtigende datenschutzrechtliche Aspekte. Die Grundsätze zur Protokollierung sollten den gesetzlichen Anforderungen entsprechen und den Missbrauch von Protokolldaten sowie damit verbundene Gefährdungen und Risiken minimieren. (siehe M 5.9 *Protokollierung am Server*, M 2.64 *Kontrolle der Protokolldateien*, M 2.110 *Datenschutzaspekte bei der Protokollierung*).

**Grundsätze der Überwachung und Protokollierung**

- Protokolle sind nur im notwendigen Umfang zu erzeugen. Ihre Erzeugung verursacht Ressourcen- und Speicherplatzverbrauch. Es gilt das Vermeidungsprinzip.
- Höhere Sicherheitsanforderungen erfordern allgemein eine umfangreichere Überwachung.
- Protokolle werden für begründete, festgeschriebene Zwecke erzeugt und unterliegen dieser Zweckbindung.
- Die Überwachung und Protokollierung unterliegt den Interessen der Organisation und muss mit der Personalvertretung und dem Datenschutzbeauftragten abgestimmt sein.
- Protokolle sind vor unberechtigtem Zugriff, vor Manipulation und nachträglicher Änderung zu schützen.
- Protokolle sind regelmäßig und ausreichend zeitnah auszuwerten.
- Für die korrekte Auswertung von Protokollen sind exakte und synchrone Zeiteinträge sowie definierte Formate, Schnittstellen und Verfahren erforderlich.
- Bei der Auswertung von Protokollen sind die Grundsätze des Bausteins B 1.8 *Behandlung von Sicherheitsvorfällen* zu berücksichtigen.
- Protokolle sind nach Überschreiten ihrer maximalen Aufbewahrungsfrist zu löschen.

**Überwachungsrichtlinie**

Auf Grundlage der Sicherheitsrichtlinie für den zu überwachenden Windows Server 2003 muss eine Überwachungsrichtlinie für den Server abgeleitet und umgesetzt werden. In der Überwachungsrichtlinie wird definiert, welche Ereignisse durch wen zu überwachen sind, welche Aktionen auf bestimmte Ereignisse innerhalb einer festgelegten Reaktionszeit erfolgen müssen und wie mit den Protokolldaten umzugehen ist. Die bei Windows Server 2003 mitgelieferten Sicherheitsvorlagendateien befinden sich im Ordner *%SystemRoot%\Security\Templates*. Sie können mit der Managementkonsole MMC (Snap-In *Sicherheitsvorlagen*) eingesehen werden und dienen der Übersicht und Orientierung.

Welche Benutzer und Ereignisse überwacht werden sollen, wird im *Gruppenrichtlinien*-Snap-In festgelegt. Es sollte dokumentiert sein, ob und - wenn ja - aus welchem Grund zu folgenden Kategorien Erfolgs- und/oder Fehlerereignisse protokolliert werden:

- Anmeldeversuche
- Anmeldeereignisse
- Kontenverwaltungsereignisse
- Active Directory-Zugriffe
- Objektzugriffe
- Rechteverwendungen
- Prozessnachverfolgungen
- Systemereignisse
- Richtlinienänderungen

**Objektüberwachung**

Für die Überwachung der Objektzugriffe (z. B. Dateien) ist zu beachten, dass diese sowohl in der Überwachungsrichtlinie des Servers als auch in den Eigenschaften der ausgewählten Objekte aktiviert sein muss. Zum Beispiel erlaubt Windows Server 2003 für Administratoren sowohl die Übernahme des Besitzes von Dateien als auch deren Übergabe an Dritte und damit auch an den ursprünglichen Besitzer. Dieser ist somit nur eingeschränkt in der Lage, eine solche Aktion zu erkennen. Deshalb sollten solche Ereignisse für überwachte Objekte zuverlässig ausgewertet werden.

**Ereignisprotokolle**

Mit der *Ereignisanzeige* können die Protokolle manuell eingesehen und verwaltet werden. Jeder einzelne Eintrag besitzt ergänzende Details und eine eindeutige Ereignis-ID, zu der ausführliche Beschreibungen existieren. Die Konfiguration der Ereignisanzeige muss definiert sein. Dazu sind die folgenden Aspekte zu beachten:

- **Rollentrennung**
  Der Speicherort für die Ereignisprotokolle kann gegebenenfalls vom Standard *%SystemRoot%\system32\config* abweichen, wenn z. B. deren Auswertung nicht von der Administration beeinflusst werden darf. In diesem Ordner befindet sich auch die Registry. Daher ist es nicht sinnvoll, dem Administrator den Zugriff auf diesen Ordner zu entziehen. Seit Windows Server 2003 ist eine Beschränkung der Berechtigungen auf die Protokolle der Ereignisanzeige möglich. Die gewünschten Zugriffsberechtigungen (*Access Control List*, ACL) werden mittels einer Sicherheitsbeschreibungssprache (*Security Descriptor Definition Language*, SDDL) im Registry-Wert *CustomSD* für die separaten Protokolle definiert.
  Alternativ kann eine gewünschte Trennung von Administration und Überwachung mit einem Systemmanagementwerkzeug realisiert werden, auf das der betreffende Administrator keinen Einfluss besitzt.
- **Protokollgröße und -aufbewahrung**
  Die maximale Größe der Protokolldateien muss mit dem Verhalten beim Überschreiben, der erwarteten Anzahl möglicher Ereignisse und dem zu protokollierenden Überwachungszeitraum harmonieren. Falls "*Ereignis nie überschreiben*" konfiguriert wird, ist zu gewährleisten, dass die Protokolldatei nicht zu groß wird und so das System beeinträchtigt. Ansonsten könnte der Server stoppen und herunterfahren, sofern die Sicherheitseinstellungen so konfiguriert sind. Die geforderte Verfügbarkeit wäre unter Umständen nicht gegeben.
- **Relevante Protokolle**
  Die Ereignisprotokolle umfassen mindestens die Protokolle

- System,
- Anwendung und
- Sicherheit.

Abhängig von der Rolle und Funktion des Servers und können zusätzlich die Protokolle
Verzeichnisdienst,
DNS-Server und
Dateireplikationsdienst
geführt werden.
Weitere dateibasierte Protokolle, die in Abhängigkeit der Rolle und Funktion des Servers berücksichtigt werden sollten, sind:

- IIS-Protokolle
- RRAS-Protokolle
- RADIUS-Protokolle

- **Ereignistypen**
  In den Protokollen können folgende Ereignistypen enthalten sein:

  - Fehler
  - Warnung
  - Information
  - Erfolgsüberwachung
  - Fehlversuchsüberwachung

**Instrumente zur Überwachung protokollierter Ereignisse**

Protokolle können je nach Bedarf manuell (z. B. über die Ereignisanzeige), mittels benutzerdefinierter Skripte (z. B. *Eventlg.pl*, *Eventquery.vbs*), mit speziellen Werkzeugen (z. B. *Dumpel.exe*, *Auditusr.exe*, *EventCombMT*) oder mit vollautomatisierten Managementwerkzeugen (z. B. *Microsoft Operations Manager 2005,* MOM 2005) ausgewertet werden. Darüber hinaus existieren auch Produkte von Drittanbietern.

Quellenhinweise:

| **Werkzeug** | **Quelle** |
|---|---|
| *Eventlg.pl* | Windows 2000 Resource Kit, Supplement 1 |
| *Eventquery.vbs* | Windows 2000 Resource Kit, Supplement 1 |
| *Dumpel.exe* | Windows 2000 Server Resource Kit, Supplement 1 |
| *Auditusr.exe* | Bestandteil Windows Server 2003 mit SP1 |
| *EventCombMT* | Microsoft Windows Server 2003 Resource Kit Tools |

Diese Produkte decken auch Anforderungen an eine Überwachung ab, welche mit den Bordmitteln eines Windows Server 2003 nicht ausreichend realisiert werden können. Dazu zählt z. B. die Benachrichtigung per SMTP, echtzeitnahe Reaktion auf Ereignisse oder ansatzweise eine forensische Analyse, zur Feststellung verdächtiger Vorfälle und Ermittlung der Verursacher.

Bei der Überwachung der Verfügbarkeit eines Windows Server 2003 oder seiner Dienste ist zu berücksichtigen, dass eine zuverlässige Überwachung und

automatische Eskalation nur von einem unabhängigen Drittsystem gewährleistet werden kann.

Die Art der Überwachung sollte ebenfalls in der Überwachungsrichtlinie dokumentiert sein.

- **Automatisierte Überwachung**
  Manuelle Überwachungen und Auswertungen sind potenziell fehlerbehaftet und subjektiv, unterliegen individuellen Schwankungen und sind nur eingeschränkt verfügbar. Die automatisierte Überwachung und Auswertung ist manuellen Verfahren vorzuziehen. Der Grundsatz der Angemessenheit ist zu berücksichtigen.
  Details zur empfohlenen Vorgehensweise sind von Microsoft im Planungshandbuch für die Sicherheitsüberwachung und Angriffserkennung beschrieben.
  Auch wenn für die Sicherheitsüberwachung eines Windows Server 2003 das Sicherheitsprotokoll der Ereignisanzeige höchste Priorität besitzt, darf nicht übersehen werden, dass weitere Ereignisse und somit deren Aufzeichnung sicherheitsrelevant sind. Eine regelmäßige Korrelation der Daten der Ereignisprotokolle mit anderen Daten wie beispielsweise Urlaubstagen, Feiertagen, Uhrzeiten etc. sollte durchgeführt werden, um Abweichungen von "normaler" Nutzung festzustellen.
- **Systemmonitor**
  Der Systemmonitor mit seinen Leistungsprotokollen und Warnungen liefert zuverlässig Informationen über die aktuelle Verfügbarkeit von Ressourcen wie Hauptspeicher, Prozessor, Netzwerk und Festplattenplatz. Er kann automatisch beim Überschreiten definierter Grenzwerte warnen. Damit kann die Sicherstellung der Verfügbarkeit eines Servers unterstützt werden. Die statistischen Auswertungen der Leistungsprotokolle über einen längeren Zeitraum gestatten Trendanalysen und eine rechtzeitige bedarfsgerechte Erweiterung oder Modernisierung erforderlicher Hardware. Auch Druckerwarteschlangen lassen sich mit dem Systemmonitor überwachen.
- **Hardware**
  Hardwarekomponenten, welche speziell zur Verbesserung der Verfügbarkeit beschafft wurden (z. B. Unterbrechungsfreie Stromversorgung, Temperaturüberwachung), produzieren Ereignisse oder Protokollinformationen, die in die Überwachung einzubeziehen sind.
- **Anwendungen**
  Anwendungen können sicherheitsrelevante Informationen im Anwendungs-Protokoll der Ereignisanzeige oder in eigenen Protokollen dokumentieren. Diese Informationen und/oder Protokolle sollten ebenfalls in die Überwachung einbezogen werden.

**Dokumentation**

Als Dokumentation dient die Überwachungsrichtlinie. Weiterhin sollten Sicherheitsvorlagen (.inf-Dateien) für die effektive Überwachungsrichtlinie des Windows-Server-2003 Systems erstellt werden. Bei zusätzlichen Tools sind die überwachten Objekte und die protokollierten Ereignis-Typen zu dokumentieren.

Prüffragen:

- Existiert eine Überwachungsrichtlinie für Windows Server 2003 zum Umgang mit Ereignissen in den Protokolldaten und ist deren Umfang mit den Anforderungen der Sicherheitsrichtlinie der Organisation abgestimmt?

- Entsprechen sowohl der für die Protokolldateien zur Verfügung stehende Speicherplatz als auch die auditierten Protokolle den Sicherheitsanforderungen der Organisation?
- Erfüllen die Instrumente zur Überwachung protokollierter Ereignisse unter Windows Server 2003 die Sicherheitsanforderungen der Organisation?
- Werden die Ergebnisse der Überwachung von Windows Server 2003 auch zur Identifikation von unerkannten Schwachstellen und Schulungsbedarf genutzt?

# M 2.366 Nutzung von Sicherheitsvorlagen unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sicherheitsrelevante Einstellungen können in Windows Server 2003 durch *Sicherheitsvorlagen* festgelegt werden. Da die meisten Bereiche des Systems sicherheitsrelevante Aspekte aufweisen, sind Vorlagen ein wichtiges und mächtiges Administrationswerkzeug. Mit ihrer Hilfe können Einstellungen standardisiert und zentral administriert werden. Die wichtigsten Werkzeuge für Vorlagen sind Sicherheitskonfigurationseditor (englisch Security Configuration Editor, SCE) und Sicherheitskonfigurations-Assistent (englisch Security Configuration Wizard, SCW, erst ab Service Pack 1 enthalten). Eine kurze Beschreibung ist unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Im Unterschied zu administrativen Vorlagen (M 2.368 *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*) enthalten Sicherheitsvorlagen für alle Einstellungsoptionen konkrete Werte. Das Aktivieren einer Sicherheitsvorlage in der lokalen Sicherheitsrichtlinie verändert unmittelbar die Systemkonfiguration. Sämtliche Einstellungen der Vorlage werden sofort aktiviert und mit dem konkreten Wert konfiguriert.

Der Vorlagentyp von Windows NT 4.0 (Dateien mit der Erweiterung *.pol*) sollte auf Windows Server 2003 nicht mehr angewendet werden. Vorhandene Sicherheitsvorlagen mit diesem Typ sollten als Gruppenrichtlinienobjekte neu erstellt werden. Das Programm *Gpolmig.exe* aus dem *Windows Server 2003 Ressource Kit* kann den Aufwand hierfür verringern.

### Allgemeine Vorsichtsmaßnahmen für Sicherheitsvorlagen

In G 3.81 *Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003* sind einige Gefährdungen aufgezählt. Durch eine sorgfältige Planung und Umsetzung und durch Beachtung von Grundregeln kann sichergestellt werden, dass Sicherheitsvorlagen die gewünschte Wirkung auf dem Zielsystem haben.

Zu Beginn sollte der Aufwand für das Entwickeln und Testen abgeschätzt werden. Dies ist abhängig von der Anzahl der unterschiedlich konfigurierten Zielsysteme, Art und Anzahl der Einstellungen in einer Vorlage sowie der vorgesehenen Verteilungsstrategie von Vorlagen auf die Zielsysteme. Dies sollte vorab in einer Anforderungsanalyse geklärt werden, in welcher auch vorhandene Sicherheitsrichtlinien für den IT-Verbund zu berücksichtigen sind.

Eine Test- und Entwicklungsumgebung oder zumindest ein vorübergehend isolierter Testserver ist in jedem Fall zu empfehlen. Je höher die Anzahl von Einstellungen und Zielkonfigurationen ist, desto größer der Aufwand für die Testumgebung. Je mehr sich die Konfiguration eines Testservers in einem bestimmten Bereich der tatsächlichen Konfiguration von potenziellen Zielservern annähert, desto besser kann die Wirkung der Vorlage für diesen Bereich vorhergesagt werden.

Der technische Aufwand für einzelne Einstellungen, wie beispielsweise die Kennwortlänge, ist klein und mit geringerem Risiko verbunden (eine Testumgebung ist hier nicht unbedingt nötig). Dies gilt insbesondere, wenn sie als Gruppenrichtlinie automatisch auf alle relevanten Server und Clients übertragen werden.

Das Verteilen und Aktivieren der Sicherheitsvorlagen in der Produktivumgebung (nachfolgend *Ausrollen* genannt) stellt ein nicht unerhebliches Risiko dar, insbesondere, wenn sich beim Test nicht hinreichend nachvollziehen lässt, wie sich kritische Einstellungen auf dem Zielserver auswirken werden. Dann ist es erforderlich, das Ausrollen zunächst auf einzelne, weniger kritische Server zu beschränken und erst bei entsprechendem Erfolg weiter auszudehnen. Des Weiteren sollten so genannte Rollback-Szenarien eingeplant und getestet werden. Rollback bedeutet, dass die Konfiguration des Servers bei Problemen wieder in den vorherigen Zustand zurückversetzt werden kann. Die Sicherung des Systemstatus und die zuverlässige Wiederherstellung sollten bei den Rollout- und Rollback-Szenarien berücksichtigt werden.

In vielen Fällen ist es sicherer, eine große Anzahl von Einstellungen auf mehrere Sicherheitsvorlagen zu verteilen und dann stufenweise auszurollen. Es kann zum Beispiel Vorlagen für bestimmte Windows Server 2003 Komponenten, für bestimmte Behörden- oder Unternehmensbereiche oder für bestimmte Sicherheitsstufen (z. B. Basissicherheit und hohe Sicherheit) geben. Dieses Vorgehen ist deutlich flexibler für die Entwicklung weiterer Vorlagen, da gezielt spezifische Vorlagen ersetzt werden können, während bewährte Grundeinstellungen erhalten bleiben. Beim stufenweisen Ausrollen kann es zu Konflikten kommen, wenn zwei Vorlagen dieselbe Einstellung definieren. Die Ausrollstrategie entscheidet darüber, welche Vorlage dominiert.

Sicherheitsvorlagen können manuell auf einem Server oder automatisiert auf mehreren Servern ausgerollt werden. Das manuelle Ausrollen erfolgt mittels der Konsolen des SCE bzw. des SCW und empfiehlt sich für einzelne Server mit sehr hohem Schutzbedarf, da mögliche unerwünschte Effekte so am schnellsten erkannt und behoben werden können. Die Automatisierung erfolgt mittels Skripten oder durch Active Directory. Letzteres ist für das stufenweise Ausrollen am besten geeignet, da mit geringem Aufwand eine Reihe von Vorlagen zugewiesen und die jeweils dominierende Vorlage festgelegt werden kann.

Es wird deutlich, dass eine geeignete Strategie für den jeweiligen IT-Bereich konzeptionell festgelegt werden muss, bevor Sicherheitsvorlagen produktiv eingesetzt werden. Sicherheitsvorlagen können den Freigabeprozess für Konfigurationsänderungen in Windows Server 2003 sowie die Bereitstellungskonzepte (M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003*) deutlich transparenter gestalten. Sie sollten in einen Freigabeprozess im Rahmen von M 2.221 *Änderungsmanagement* eingebunden sein.

**Sicherheitskonfigurations-Editor (SCE)**

Der SCE besteht nach einer Standardinstallation aus den Konsolen:

- *Lokale Sicherheitsrichtlinie* (unter *Start* | *Systemsteuerung* | *Verwaltung*): führt Sicherheitseinstellungen direkt auf lokalem Server durch
- *Sicherheitsvorlagen*: erstellt und verwaltet Sicherheitsvorlagen (*.inf*-Dateien) führt keine Konfigurationsänderungen am Server durch
- *Sicherheitskonfiguration und -analyse:* Modellierung von Sicherheitseinstellungen und Analyse des Systems mit Hilfe einer zwischengeschalteten Konfigurationsdatenbank, Export und Import von Sicherheitsvorla-

gen, Überprüfen der Richtlinienkonformität, Aktivieren einer modellierten Sicherheitskonfiguration

Die Konsolen *Sicherheitsvorlagen* und *Sicherheitskonfiguration und -analyse* werden über die *Microsoft Management Console* (MMC) aufgerufen.

Mittels der Werkzeuggruppe SCE werden alle Aspekte der Authentisierung und Signierung von Netzverkehr zwischen Windows-Computern eingestellt. Außerdem werden hier alle zentralen Sicherheitseinstellungen für einen Server eingestellt, unter anderem die Überwachungsrichtlinien und Berechtigungen im Dateisystem und in der Registrierdatenbank. In Domänen enthalten die SCE-Konsolen zusätzliche Einstellungen für Kerberos und andere domänenweite Einstellungen. Alle diese Einstellungen können in Sicherheitsvorlagen gespeichert werden. Es ist zu empfehlen, immer die aktuellsten vom Hersteller angebotenen Einstellungen einzuspielen (siehe Hilfsmittel zum IT-Grundschutz, *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Bei Windows Server 2003 werden einige Sicherheitsvorlagen für unterschiedliche Sicherheitsanforderungen mitgeliefert. Sie befinden sich im Verzeichnis *C:\WINDOWS\security\templates*. Vom Hersteller sind weitere dokumentierte Vorlagen erhältlich.

Die Einstellungen unter *Eingeschränkte Gruppen*, *Systemdienste*, *Registrierung* und *Dateisystem* können nicht mittels Rollback rückgängig gemacht werden. Solche Einstellungen können durch das Anwenden einer anderen Sicherheitsvorlage neu gesetzt werden. Eine Rollback-Variante stellt das parallele Entwickeln von Rollback-Vorlagen dar, welche die Einstellungen aus den eigentlichen Sicherheitsvorlagen im Notfall mit unkritischeren Werten überschreibt. Besonders kritisch sind Ressourcenberechtigungen (ACL) und Objekt-Überwachungseinstellungen (SACL). Berechtigungskonzepte, die in Sicherheitsvorlagen abgebildet werden, können vorhandene Berechtigungsstrukturen durch Anwenden der Vorlage unwiederbringlich zerstören. Hier muss M 2.370 *Administration der Berechtigungen ab Windows Server 2003* berücksichtigt werden.

Für jeden Server sollte eine verbindliche Festlegung aller Einstellungen unter *Kontorichtlinien*, *Lokale Richtlinien* und *Ereignisprotokoll* getroffen werden. Hierzu sind die Sicherheitsrichtlinien und Sicherheitskonzepte für den betrachteten Informationsverbund und die Maßnahmen des IT-Grundschutzes heranzuziehen. Ferner können die Standardeinstellungen von Windows Server 2003 sowie die mitgelieferten Sicherheitsvorlagen als Referenz verwendet werden. Es sollte für jeden Server eine gültige Sicherheitsvorlage bzw. ein Satz Sicherheitsvorlagen existieren. Die Sicherheitskonfiguration des Servers sollte dem letzten dokumentierten Stand der Sicherheitsvorlagen entsprechen.

Die Konformitätsanforderungen sollten in einer Sicherheitsrichtlinie für den betrachteten Informationsverbund vorgeschrieben werden.

Der Sicherheitskonfigurationsassistent (SCW) stellt eine Erweiterung und zum Teil eine Vereinfachung des SCE dar. Es gelten dieselben Grundsätze. Hinweise und Empfehlungen zur Bedienung des SCW finden sich in den Hilfsmitteln zum IT-Grundschutz (siehe *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

**Dokumentation**

Für eine minimale Dokumentation von Sicherheitsvorlagen genügt es, für jeden Server die verwendeten Vorlagendateien (Dateien mit der Erweiterung *.inf* oder *.xml*), deren Version und bei selbsterstellten Vorlagen auch deren Inhalt in die Systemdokumentation aufzunehmen. Durch entsprechendes Versionsmanagement und Zugriffskontrolle auf die Vorlagen sollte nachvollziehbar sein, wer wann welche Vorlagen editiert hat. Wird die Vorlage über Active Directory bereitgestellt, sind alle weiteren Faktoren zu dokumentieren, welche die Wirksamkeit der Einstellungen für den oder die Server bestimmen, z. B. *Organizational Unit* (OU), Sicherheits- und WMI-Filter. Es muss immer nachvollziehbar sein, woher eine einzelne Sicherheitseinstellung stammt.

Auf dieser Basis sollten Dokumentationen und gegebenenfalls Konzepte für Tests, eigene Skripte sowie Bereitstellungs- und Rollbackszenarien im Zusammenhang mit Sicherheitsvorlagen erstellt werden. Die Dokumentation sollte ebenfalls zur Planung der regelmäßigen Auswertung von System- und Sicherheitsprotokollen herangezogen werden.

Für die Sicherheitsvorlagen des SCW werden Transformations- und Stylesheet-Dateien für Anzeige und Ausdruck der Vorlagen mitgeliefert (*C:\WINDOWS\security\msscw\transformfiles*). Für die Basisdokumentation der Serverrollen im Rahmen einer Systemdokumentation ist dies ausreichend.

Zur Dokumentation von aktiven Einstellungen ist die GPMC-Konsole (*Group Policy Management Console*) gut geeignet, sofern Active Directory zum Einsatz kommt. Für die Gruppenrichtlinienobjekte, Richtlinienergebnissätze und Gruppenrichtlinienmodellierungen können Berichte in druckbarem Format in eine HTML-Datei exportiert werden (gewünschtes Objekt markieren | Menü *Aktion* | *Bericht speichern...*).

Prüffragen:

- Werden Sicherheitsvorlagen unter Windows Server 2003 verwendet und in den Test- und Freigabeprozess des Änderungsmanagements eingebunden?
- Wurden Rollout- und Rollback-Strategien für Sicherheitsvorlagen unter Windows Server 2003 bzw. Rollbackvorlagen geplant und getestet?
- Basieren die Einstellungen in den Sicherheitsvorlagen unter Windows Server 2003 auf aktuellen Sicherheitsempfehlungen des Herstellers?
- Sind die in den Sicherheitsvorlagen unter Windows Server 2003 vorgenommenen Einstellungen nachvollziehbar dokumentiert?
- Unterliegen die Sicherheitsvorlagendateien einer Versions- und Zugriffskontrolle?

# M 2.367 Einsatz von Kommandos und Skripten ab Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In der Praxis werden häufig Kommandos und Skripte für kleine Aufgaben eingesetzt, zum Beispiel um bestimmte Parameter zu setzen oder anzuzeigen. Skripte ermöglichen es, Kommandos automatisiert ablaufen zu lassen. Fehlbedienung und Unkenntnis können das Risiko bei einem einzelnen Kommando in einem Skript vervielfachen. Deshalb müssen Skripte mit Bedacht eingesetzt werden, damit ihre Auswirkungen kontrollierbar und nachvollziehbar bleiben. Wird der Aufwand für Planung, Entwurf und Wartung in Kauf genommen, können administrative Aufgaben mittels Skripten vereinheitlicht und standardisiert werden.

### Kommando

Mit Kommandos wird der Aufruf von Programmen mittels des Feldes "*Ausführen"* oder über die Befehlszeile der Eingabeaufforderung bezeichnet. Während unter DOS der Befehlszeileninterpreter *command.com* agierte, steht unter Windows die wesentlich leistungsfähigere *CMD.exe* zur Verfügung. Alles, was in dieser CMD-Shell aufgerufen werden kann, wird als Kommando bezeichnet. Es muss zwischen den impliziten Kommandos und Steuerungskonstrukten der CMD-Shell, , Kommandos des Betriebssystems und Kommandos von Drittherstellern unterschieden werden. Kommandos können in einer lesbaren Datei (Batch-Datei, spezielle Skript-Datei) zusammengestellt werden.

### Skript

Ein Skript ist eine Klartext-Datei, die mit einem beliebigen Editor wie *notepad.exe* erstellt werden kann. Die in einem Skript enthaltenen Anweisungen werden beim Aufruf durch einen entsprechenden Interpreter ausgeführt. Skripte werden unter Windows hauptsächlich eingesetzt, um die Administration zu automatisieren. Sie können vor allem die Ausführung sich ständig wiederholender Administrationsaufgaben sehr erleichtern. Werden sie automatisch ausgeführt, zum Beispiel über *Geplante Tasks*, arbeiten sie auch in Abwesenheit eines Administrators. Die Wiederverwendung von Skripten gewährleistet die Nachvollziehbarkeit und einheitliche Qualität der durchgeführten Aufgaben.

### Anforderungen

Für Skript-Interpreter, mitgelieferte Skripte und Skripte aus Zusatzpaketen des Herstellers (z. B. *MBSA*, *Support Tools*, *Ressource Kit*) sowie eigenentwickelte Skripte sollten die gleichen Anforderungen gelten wie für eine Standardsoftware (siehe B 1.10 *Standardsoftware*). Es handelt sich letztlich um Standardsoftware für die Administration. Die Anforderungen und Bedingungen, um Skripte zu erstellen und anzuwenden, sind zu analysieren und daraus verbindliche Festlegungen zu treffen. Ebenso sind alle eigenentwickelten Skripte sowie Werkzeuge oder Skripte von Drittherstellern angemessen zu dokumentieren und zu testen (siehe M 2.83 *Testen von Standardsoftware*).

Skripte im Umfeld eines betriebskritischen IT-Systems dürfen nur von administrativem Personal geschrieben und gepflegt werden, das für die Programmierung von Skripten ausreichend geschult ist und über genug Erfahrung verfügt

(siehe G 2.67 *Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten*). Es muss ganz besonders im Umfeld der Administration und deren Automatisierung sichergestellt werden, dass keine unerlaubte oder nicht freigegebene Software in Form von Werkzeugen oder komplexen Skripten angewendet wird. Auf den Einsatz von Software ohne nachvollziehbare Herkunft ist zu verzichten. Ebenso sollte die Umgebung, in der Skripte ausgeführt werden dürfen, ausreichend gegen Missbrauch und Schadsoftware geschützt sein.

Der Rahmen für den Einsatz von Skripten sollte in einer Sicherheitsrichtlinie festgelegt werden. Es ist mindestens festzulegen, für welchen Einsatzzweck und aus welcher Herkunft Skripte verwendet und welche Skriptumgebungen und Skriptsprachen benutzt werden dürfen. Weiterhin ist festzulegen, welche Anforderungen an die Entwicklung und Freigabe für Skripte in bestimmten Einsatzbereichen gelten sollen. Wenn nichts anderes festgelegt wird, sind immer die Maßnahmen aus B 1.10 *Standardsoftware* anzuwenden. Es ist allerdings zu berücksichtigen, dass diese unter Umständen nicht für jeden Einsatzbereich effektiv und praktikabel sind, zum Beispiel bei Anmeldeskripten.

Es sollte überlegt werden, generell keine unsignierten Skripte zuzulassen. Die Signaturen basieren auf Sicherheitszertifikaten. Skripte des Herstellers sind bereits signiert. Es empfiehlt sich, die eigenen Zertifikate aus Vorlagen einer Windows Server 2003-Zertifizierungsstelle zu erstellen. Zum Signieren werden spezielle Programmier-Objekte der Krypto-API von Windows verwendet, auf die mittels Skripte zugegriffen werden kann. Nähere Informationen sind für Windows Server 2003 dem *Platform Software Developement Kit* (Platform SDK) oder ab Windows Server 2008 dem *Windows SDK* zu entnehmen. Die Richtlinie kann ab Windows XP/Server 2003 mit Hilfe einer Softwareeinschränkungsrichtlinie administrativ umgesetzt werden.

**Grundsätze**

Für alle Skripte sollte beachtet werden, dass sie in der Regel zwar aufwärts, aber oft wegen ihrer Weiterentwicklung bei der Nutzung neuer Funktionen nicht abwärts kompatibel sind.

Skripte werden immer im Sicherheitskontext der aufrufenden Benutzersitzung ausgeführt, sie verfügen während des Ablaufs über die Berechtigungen dieses Sicherheitskontextes. Wird ein Skript durch einen Dienst oder einen laufenden Prozess gestartet, dann gilt der Sicherheitskontext dieses Dienstes oder Prozesses auch für das Skript. Für viele Funktionen, auf die mittels Skript zugegriffen wird, werden administrative Berechtigungen auf einzelne Objekte oder auf dem gesamten Server benötigt.

Werden Skripte für Benutzer (z. B. An-/Abmeldeskripte) oder Dienste (z. B. im Zusammenhang mit Datensicherung) bereitgestellt, dürfen innerhalb des Skriptablaufs keine unerlaubten erweiterten Berechtigungen vergeben.

Häufig werden Skripte bei Domänenanmeldungen oder über Gruppenrichtlinien des Active Directory automatisch verteilt und ausgeführt.

Es sollte dafür gesorgt werden, dass den Benutzern Quelltexte von administrativen Skripten verborgen bleiben und dass die Skriptausführung den Betrieb nicht beeinträchtigt. Entsprechende Einstellungen befinden sich zum Beispiel in den mitgelieferten administrativen Vorlagen unter *Administrative Vorlagen* | *System* | *Skripts*.

Ab Windows Server 2008 ist zu beachten, dass auch Skripte der Benutzerkontensteuerung unterliegen (siehe M 4.340 *Einsatz der Windows-Benutzer-*

*kontensteuerung UAC ab Windows Vista*). Dies kann zur Folge haben, dass für frühere Windows-Versionen entwickelte Skripte zunächst nicht mehr funktionieren, weil ihnen administrative Berechtigungen fehlen.

**Systemeigene Mittel für Skripts:**

Unter Windows Server 2003 und höher stehen nach einer Standardinstallation umfangreiche Möglichkeiten zur Verfügung, um Skripte zu erstellen und auszuführen:

Es handelt sich um eine Skriptumgebung des Herstellers, die auch eine Dokumentation beinhaltet. Die Möglichkeiten der Batch-Programmierung waren in älteren Versionen eingeschränkt, sind aber inzwischen sehr mächtig, es steht zum Beispiel eine *FOR*-Anweisung zur Verfügung. Es ist keine Installation erforderlich.

VBScript ist eine einfache Skriptsprache. Sie besitzt keine eingebauten Funktionen zur Administration. Diese werden erst in der Kombination mit *Windows Scripting Host* (WSH) und den Schnittstellen zur *Windows Management Instrumentation* (WMI), *Active Directory Service Interface* (ADSI) und anderen Schnittstellen des Betriebssystems erschlossen. Dazu müssen Objekte in das Skript eingebunden werden, die über diese Schnittstellen bereitgestellt werden. Ohne gute Kenntnisse der entsprechenden Objektmodelle ist deren Nutzung zwar mit Hilfe von umfangreichen Vorlagen und Beispielen möglich, jedoch nicht zu empfehlen (z. B. wegen ähnlicher Methoden wie GetObject versus CreateObject). JScript ist mit VBScript hinsichtlich des Einsatzzwecks gleichzusetzen. Der Unterschied besteht in der an die Programmiersprache Java angelehnten Syntax. VBScript und JScript werden seit dem Erscheinen von Windows Server 2003 nicht mehr weiterentwickelt und sind daher unter dem Aspekt der Zukunftssicherheit kritisch zu bewerten.

Skripte (z. B. in Form von *.vbs*- oder *.js*-Dateien) werden über *CScript.exe* (Kommandozeilenausgabe) oder *WScript.exe* (grafisches Ausgabefenster) aufgerufen und abgearbeitet. Durch diese beiden Programme wird der WSH in Ausführung gebracht. WSH ist die standardmäßige Umgebung zur Skriptverarbeitung. Er besitzt eigene Programmfunktionen und kann Erweiterungen für WSH-kompatible Sprachen nachladen (VBScript, JScript). Der WSH ist ein Interpreter. Er kann COM-Objekte verwenden und hat Zugriff auf eine Reihe von Systemschnittstellen (siehe oben). *WScript.exe* und *CSript.exe* enthalten einen rudimentären Debugger zum Testen von Skripten.

Im Zusammenhang mit WSH sind eine Reihe von Aktualisierungen und Fehlerkorrekturen für Windows NT/2000/XP/2003 erschienen, die Sicherheitsprobleme behoben und zum Teil die Überarbeitung bestehender Skripte erforderlich gemacht haben. Dies sollte bei der Entwicklung von Skripten für den WSH berücksichtigt werden.

WMI (*Windows-Verwaltungsinstrumentation*) ist als zentrale Verwaltungstechnologie ab Windows Server 2003 integriert. WMI ermöglicht einen einheitlichen Zugriff auf die Konfiguration, Verwaltung und Überwachung fast aller Windows-Ressourcen. WMI gibt es bereits seit 1998 (Windows NT 4.0 SP4). Die WMI-Architektur ist komplex, sie besteht aus drei Schichten (Ressourcen, Infrastruktur, Nutzer) und ist objektorientiert aufgebaut. Sie wurde über DLLs für die Anbieterbeschreibungen (*%SystemRoot%\system32\wbem*) und den WMI-Dienst (*winmgmt.exe*) implementiert. Für den Zugriff mittels Windows-Skripten werden kompatible Skriptumgebungen wie WSH oder ActivePerl verwendet. Mit dem Snap-in *wmimgmt.msc*, dem WMI-Testprogramm *wbemtest.exe* oder dem Befehlszeilen-Werkzeug *wmic.exe* können WMI-Kon-

figurationen vorgenommen und verfügbare Klassendefinitionen untersucht werden.

Mit ADSI wird eine skriptbasierte Verwaltung des Verzeichnisdienstes Active Directory analog der WMI-Technologie ermöglicht.

**Neuerungen mit Windows Server 2008**

Mit Windows PowerShell wird eine weiterentwickelte Kommandozeilen- und Skriptingumgebung für die Windows-Plattform angeboten, welche VBScript, JScript und den WSH ablöst. PowerShell übernimmt einige aus der Unix-Welt bekannte Konzepte (z. B. Pipes) und setzt auf dem .NET-Objektmodell auf. Ab Windows Server 2008 ist PowerShell optional verfügbar, ab Server 2008 R2 ist sie im Standardlieferumfang enthalten. :

Mit Scriptomatic wird ein Werkzeug zum Generieren von Skripten bereitgestellt. Das Werkzeug unterstützt WMI und ADSI. Eine Version für die PowerShell ist ebenfalls verfügbar.

Für viele Werkzeuge und Skripte, die von Microsoft bereitgestellt werden, gibt es keine generelle Produktunterstützung. Dies ist im Einzelfall mit dem Hersteller zu klären. Teilweise wurden die Werkzeuge zu Lehrzwecken bereitgestellt, besitzen keine oder nur unzureichende Fehlerbehandlungen und sind nicht leistungsoptimiert.

**WSH abschalten**

Die Skript-Fähigkeiten von Windows werden leider auch zur Verbreitung von Schadsoftware () missbraucht. Auf Clients werden Skripte daher häufig eingeschränkt oder unterbunden. In einer Client/Server-Umgebung kann der administrative und organisatorische Nutzen von Skripten das erhöhte Risiko und den entsprechenden Sicherheitsaufwand rechtfertigen. Werden nur Kommandozeilenskripte benötigt, sollte der WSH auf dem Server blockiert werden, um die Sicherheit zu erhöhen.

Der WSH kann auf verschiedene Weise blockiert werden:

- Erstellen des Registrierschlüssels (ab Windows 2000/XP/Server 2003)
  *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\ Settings\Enabled*
  *(Format Reg_DWORD)*
  Der Wert wird auf Null gesetzt. Die geänderte Registrierungseinstellung sollte in einer administrativen Vorlage abgebildet werden.

**Alternative Skriptumgebungen**

Alternative Skriptumgebungen wie Perl, KiXtart und andere verringern die Angriffsfläche nicht automatisch. Sie greifen genauso auf Betriebssystemfunktionen zu und können eigene Sicherheitslücken enthalten. Es gelten die oben genannten Anforderungen und Grundsätze.

**Dokumentation**

Für die Entwicklung sowohl von eigenentwickelten als auch von Skripten von Fremdherstellern sind die in der Software-Entwicklung gängigen Dokumentationsgrundsätze einzuhalten. Mindestens sollten ein Anforderungskatalog, eine Funktionsbeschreibung und Benutzerhilfe, die Ausführungsbedingungen sowie eine Versionskontrolle vorliegen. In der Dokumentation der jeweiligen Windows-Komponente oder des jeweiligen Betriebskonzeptes muss anhand

von Skriptname und Versionsnummer erkennbar sein, welches Skript eingesetzt wird.

Prüffragen:

- Ist die Umgebung, in der Skripte ausgeführt werden dürfen, ausreichend gegen Missbrauch und Schadsoftware geschützt?
- Wird für die Programmierung von Skripten ausschließlich ausreichend geschultes Personal eingesetzt?
- Werden nur freigegebene Skripte und Werkzeuge eingesetzt?
- Ist in der Sicherheitsrichtlinie festgelegt, für welchen Einsatzzweck und aus welcher Herkunft Skripte verwendet und welche Skriptumgebungen bzw. Skriptsprachen benutzt werden dürfen?
- Ist sichergestellt, dass in den Quelltexten der Skripte keine administrativen Kennungen hinterlegt werden?
- Ist der Windows Scripting Host (WSH) auf den Servern deaktiviert, sofern dieser nicht benötigt wird?
- Sind alle eigenentwickelten Skripte sowie Werkzeuge oder Skripte von Drittherstellern angemessen dokumentiert und getestet?

# M 2.368 Umgang mit administrativen Vorlagen unter Windows ab Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Windows-Gruppenrichtlinien sind ein effektives und vielseitiges Mittel zur Konfiguration von diversen Windows-Systemen, unter anderem Windows Server 2003 oder Windows Server 2008. Notwendige Vorüberlegungen für den Einsatz von Gruppenrichtlinien sind den Maßnahmen M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* und M 2.231 *Planung der Gruppenrichtlinien unter Windows* zu entnehmen.

### Zusammenhang von Gruppenrichtlinien und der Registry

Die meisten Einstellungen in den Gruppenrichtlinien führen zu Änderungen in der Registry eines Windows-Systems. Die Registry gehört zu den kritischen Kernkomponenten eines Windows-Servers und benötigt besonderen Schutz und besondere Sorgfalt. Die Aspekte "Test", "Sicherheitsüberwachung", "Rückführung" und "Dokumentation" sollten immer berücksichtigt werden. Hierzu müssen geeignete Werkzeuge verwendet werden der Registrierungseditor von Windows allein deckt die genannten Aspekte nicht ab.

Gruppenrichtlinien können durch Vorlagen von Microsoft und durch benutzerdefinierte Vorlagen, zum Beispiel von anderen Softwareherstellern, erweitert werden. Diese so genannten administrativen Vorlagen stellen einen Satz von Einstellungsoptionen bereit, die gezielt und automatisiert Registrierungsschlüssel in die Registry schreiben. Im Zusammenspiel mit der ab Windows Server 2003 mitgelieferten Gruppenrichtlinienverwaltung (*Group Policy Management Console*, GPMC) und den umfangreichen netzbasierten Bereitstellungsmechanismen (Active Directory) von Gruppenrichtlinien sind administrative Vorlagen ein geeignetes Mittel zum sicheren Umgang mit der Registry von Windows-Server-Systemen.

Es wird empfohlen, Änderungen an Schlüsseln in der Registrierungsdatenbank ausschließlich über administrative Vorlagen vorzunehmen und auf manuelle Änderungen vollständig zu verzichten. Im Rahmen des Änderungsmanagements sollten zumindest manuell durchgeführte Änderungen an Registrierungsschlüsseln zeitnah in einer benutzerdefinierten administrativen Vorlage implementiert werden.

### Kompatibilität von administrativen Vorlagen

Jede Version von Windows-Betriebssystemen ab Windows 2000 und fast jedes Service-Pack enthält administrative Vorlagen des Herstellers, die um neue Einstellungsoptionen erweitert worden sind und alle Optionen der Vorgänger-Versionen beinhalten. Dies gilt auch für Windows Server 2003 und höher. Die Abwärtskompatibilität der neuen Einstellungsoptionen ist in den Vorlagen dokumentiert und wird in der GPMC-Konsole angezeigt. Die mit neu eingeführten Betriebssystemversionen hinzugefügten Einstellungsoptionen haben auf einer inkompatiblen Windows-Version keine Wirkung. Beispielsweise bleiben beim Öffnen einer in Windows Server 2003 enthaltenen Vorlage auf einem Windows 2000 Server-System die inkompatiblen Einstellungsoptionen unsichtbar und unwirksam.

Eine Gruppenrichtlinie sollte immer basierend auf der administrativen Vorlage der neuesten Windows-Version erstellt werden, auf welcher die Richtlinie voraussichtlich verwendet wird. Die jeweiligen Vorlagen sind auf den Internetseiten von Microsoft als sogenannte *administrative Templates* in Form von ***adm-*** oder ***admx-***Dateien verfügbar. Wenn eine benutzerdefinierte administrative Vorlage für Windows Server 2003 erstellt wird, so sind Kompatibilität und Wirkung auf frühere Windows-Versionen ausreichend zu testen und in der Vorlage zu dokumentieren.

**Neuerungen ab Windows Server 2008**

Die mit Windows 2000 eingeführten administrativen Vorlagen vom Typ *adm* bieten die Möglichkeit, neben Basiseinstellungen des Systems, wie zum Beispiel Parametern des Netzes, auch Konfigurationen an Office-Produkten vorzunehmen. Allerdings zeigten die *adm*-Dateien in der Praxis auch Nachteile:

- Es sind keine mehrsprachigen Anpassungen verfügbar.
- Jede *adm*-Datei ist bedingt durch das Format einige Kilobyte groß, bei Einsatz vieler *adm*-Dateien innerhalb einer Domäne werden diese Dateien immer repliziert. Dies kann erheblichen Datenverkehr verursachen.
- Administrative Vorlagen können nicht zentral gespeichert werden.

Aufgrund dieser Restriktionen wurde ab Windows Server 2008 und Windows Vista das Format der Vorlagendateien geändert. Das neue, XML-basierte Format *admx* mindert die oben genannten Nachteile. Die Größe der einzelnen Vorlagen wurde durch das XML-Format erheblich verringert. Durch die Einführung eines zentralen Speicherortes können die Vorlagendateien zentral gespeichert und verwaltet werden. Der lokale Pfad zu den Vorlagendateien findet sich unter *%systemroot%\PolicyDefinitions*.

Gleichzeitig wurden angepasste Sprachpakete in Form von *adml*-Dateien eingeführt. Diese Dateien werden grundsätzlich unterhalb des Ordners *PolicyDefinitions* gespeichert. Auf einem Windows Server 2008 mit deutscher Sprachumgebung sind neben den sprachneutralen *admx*-Dateien mindestens die beiden sprachspezifischen Ordner *de-DE* und *en-US* vorhanden. Innerhalb dieser Ordner werden die erwähnten *adml*-Dateien gespeichert.

**Neuerungen ab Windows Server 2008 R2**

Innerhalb des Gruppenrichtlinienverwaltungs-Editors werden die administrativen Vorlagen unterhalb des Pfades *Administrative Vorlage*n des Knotens *Computer* und des Knotens *Benutzerkonfiguration* angezeigt.

Mit Windows Server 2008 R2 wurden die folgenden Neuerungen eingeführt:

- Die neue Bedienoberfläche bietet erweiterte Konfigurationseinstellungen der Eigenschaften. Alle verfügbaren Informationen oder Kommentar-Felder sind nun innerhalb einer Registerkarte verfügbar.
  Mehrteilige Zeichenfolgen und QWORD-Werttypen werden nun unterstützt. Durch die Möglichkeit REG_MULTI_SZ-Registrierungswerttypen anzulegen, kann unter anderem die Eingabe eines mehrzeiligem Text erfolgen.
  Die beschriebenen Neuerungen gelten auch für Windows 7-Systeme mit installierten Remoteserver-Verwaltungstools (*RSAT*).

**Arbeiten mit administrativen Vorlagen ab Windows Server 2008**

Innerhalb einer Domänen-Umgebung werden die Vorlagen in der Regel nicht lokal bearbeitet oder angewendet. Üblicherweise werden ein zentraler Ablageort und ein zentrales Verwaltungswerkzeug genutzt.

Dieser sogenannte Central Store ist ein neu zu erstellender Ordner unterhalb der Struktur *\SYSVOL\domain\Policies.* Nachdem der Ordner erstellt wurde, werden der Inhalt der lokalen *PolicyDefinitions* oder neue Vorlagen aus *msi*-Paketen in dieses Verzeichnis kopiert.

Die Vorlagen können über den Aufruf des Editors zur Gruppenrichtlinienverwaltung-bearbeitet werden. Dieser zeigt alle in den zentralen Speicherort kopierten Vorlagen an. Da der Editor nur diesen Pfad auswertet, ist es wichtig, die von Microsoft vorgegebenen Pfade beizubehalten.

**Migration bestehender *adm*-Vorlagen**

Grundsätzlich werden alte *adm*-Vorlagen auch von Windows Server 2008 unterstützt. Oft ist jedoch die vollständige Migration aller alten *adm*-Vorlagen schon aus Gründen der Konsistenz die sinnvollere Alternative. Neben verschiedenen Drittprodukten bietet Microsoft mit dem *ADMX Migrator* ein kostenloses *MMC*-integriertes Werkzeug zur Migration der *adm*-Vorlagen an.

**Aktualisieren oder Hinzufügen neuer Vorlagen**

Für die effektive Nutzung der Vorlagen in bestehenden Umgebungen werden durch Microsoft für aktuelle Systeme angepasste oder für neue Systeme oder Service-Packs neu erstellte Vorlagen (*Templates*) zur Verfügung gestellt. Aktualisierte Vorlagen werden in Form von installierbaren *msi*-Paketen angeboten. Abhängig von der Nutzung der Vorlagen, lokal oder als Domänen-Vorlage, unterscheiden sich die Speicherorte für den Import.

Soll die Konfiguration der administrativen Vorlagen (*admx*) der Windows-Server von einem Client-System aus erfolgen, so muss es sich mindestens um ein Windows Vista-System mit installierten Verwaltungswerkzeugen handeln (*Remote Server Administration Tools, bzw. aktuelle GPMC*).

Weiterführende Informationen bezüglich des Zusammenspiels von Vorlagen und Gruppenrichtlinien finden sich in M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*.

**Aktualisierung des Betriebssystems**

Nach einer Aktualisierung des Betriebssystems bleiben alle Einstellungen erhalten und können mit den gegebenenfalls erneuerten administrativen Vorlagen des Betriebssystems verwaltet werden. Benutzerdefinierte Vorlagen samt aktivierten Einstellungen bleiben unverändert erhalten und können in den zugehörigen Gruppenrichtlinienobjekten ("Group Policy Objects", GPO) verwaltet werden.

**Anwenden benutzerdefinierter administrativer Vorlagen**

Das Anwenden einer benutzerdefinierten administrativen Vorlage schreibt für jede aktivierte Einstellungsoption den entsprechenden Registrierungsschlüssel dauerhaft -wie bei den Windows NT 4-Systemrichtlinien -in die Registry. Zum Entfernen ist dann manuelles Editieren der Registry erforderlich. Der Effekt heißt in Windows 2000 Server, Windows Server 2003 und höher "nicht verwaltbare Richtlinieneinstellung" und wird auch "Registry Tattooing" genannt. Danach kann in der GPMC-Konsole nur noch der Wert des Schlüssels geändert werden, beispielsweise von 1 auf 0 für "ja" oder "nein" , jedoch nicht mehr der Schlüssel selbst.

Der "Tattooing-Effekt" tritt nicht bei mitgelieferten administrativen Vorlagen einiger Microsoft-Produkte auf, zum Beispiel Windows 2000/XP/Server 2003

und Office XP/2003. Sie heißen in Windows XP/Server 2003 "voll verwaltbare Vorlagen", die resultierenden Einstellungen heißen kurz "Richtlinien" (engl. "True Policies"). Diese Richtlinieneinstellungen werden zusätzlich in den Registrierungsschlüsseln

HKEY_LOCAL_MACHINE\Software\Policies

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\Policies

HKEY_CURRENT_USER\Software\Policies

HKEY_CURRENT_USER
\Software\Microsoft\Windows\CurrentVersion\Policies

verwaltet und als *.pol*-Dateien im Dateisystem abgelegt. Die Policies-Schlüssel sollten nicht durch benutzerdefinierte administrative Vorlagen manipuliert werden.

Vor der Anwendung sollte der Systemstatus (englisch "System State") gesichert werden (siehe M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server*). Die Registrierung zu sichern genügt allein nicht, um bei Komplikationen mit einer Vorlage den Ursprungszustand wiederherstellen zu können. Außerdem müssen Funktionalität und Wirkung der Einstellungen unbedingt auf einem isolierten Testsystem erprobt werden. Hierbei sind alle Windows-Versionen zu berücksichtigen, mit denen die Vorlage verwendet werden soll.

Werden die Einstellungen auf mehrere Server angewendet, so ist der Ausroll-Prozess in einem unkritischen Bereich der Produktivumgebung zu beginnen. Der Bereich ist unter ständiger Beobachtung und Erfolgskontrolle sukzessive auf kritischere Schichten der Produktivumgebung auszuweiten. Zur Erfolgskontrolle dient in einer Active Directory-Umgebung die GPMC-Konsole oder auf einem allein stehenden Server die Richtlinienergebnissatz-Konsole (RSOP-Konsole).

Für jeden so erstellten Schlüssel sind im Sicherheitsprotokoll mindestens Schreibzugriffe zu erfassen. Die Einstellung der Objektüberwachung mittels Sicherheitsprotokoll wird in M 2.365 *Planung der Systemüberwachung unter Windows Server 2003* beschrieben. Die Schreibberechtigung für normale Benutzerkonten ist zu deaktivieren. Beides kann manuell mit dem Registrierungseditor, skriptgesteuert (siehe M 2.367 *Einsatz von Kommandos und Skripten ab Windows Server 2003*) oder mittels einer Windows-Sicherheitsvorlage (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*) geschehen.

**Entfernen benutzerdefinierter administrativer Vorlagen**

Das Entfernen administrativer Vorlagen erfordert einen ähnlich hohen administrativen Aufwand wie das Einspielen. Wenn einige oder alle Einstellungsoptionen einer administrativen Vorlage nicht mehr verwendet werden sollen, dann wird sie üblicherweise aus der GPMC-Konsole entfernt und gegebenenfalls durch eine modifizierte Version ersetzt. Jedoch werden dadurch Registrierungsschlüssel weder entfernt noch wenigstens zurückgesetzt. Daher müssen vor dem Entfernen der Vorlage aus der GPMC-Konsole alle aktiven Einstellungen, die in der GPMC-Konsole sichtbar sind, dokumentiert und anschließend auf einen unkritischen Wert gesetzt werden. Unkritisch sind solche Werte, die zur Unwirksamkeit eines Registrierungsschlüssels führen. Die Vorlage

sollte erst nach entsprechender Erfolgskontrolle mittels GPMC- oder RSOP-Konsole entfernt werden. Das erneute Hinzufügen einer versehentlich entfernten Vorlage zeigt in der GPMC-Konsole nicht die vorhandenen Registry-Einstellungen an, auch wenn der oder die Registrierungsschlüssel noch gesetzt und wirksam sind.

Um die Gefahr des Missbrauchs solcher verwaisten Registrierungsschlüssel auszuschließen, müssen anschließend alle nicht mehr verwendeten Registrierungsschlüssel vor ungewollter Verwendung geschützt werden. Dies ist im Normalfall nur durch Löschung möglich. Die Löschung kann manuell mit dem Registrierungseditor oder skriptgesteuert erfolgen. Alternativ können durch eine Windows-Sicherheitsvorlage der Zugriff auf die Schlüssel verweigert und die Überwachungseinstellungen verschärft werden, wodurch sich allerdings die Eintragungshäufigkeit im Sicherheitsprotokoll erhöht und der Aufwand für die Auswertung steigt.

**Dokumentation**

Für eine minimale Dokumentation von administrativen Vorlagen genügt es, für jeden Server die verwendeten Vorlagendateien (Dateien mit der Erweiterung "*.adm*"), deren Version und bei benutzerdefinierten Vorlagen auch deren Inhalt in die Systemdokumentation aufzunehmen. Durch entsprechendes Versionsmanagement und Zugriffskontrolle auf die Vorlagen sollte nachvollziehbar sein, wer wann welche Vorlagen editiert hat. Weiterhin müssen jede aktivierte Einstellungsoption, ihr aktueller Wert und die zugrunde liegende Vorlage erfasst werden. Wird die Vorlage über Active Directory bereitgestellt, sind alle weiteren Faktoren zu dokumentieren, welche die Wirksamkeit der Einstellungen für den oder die Server bestimmen, z. B. Organizational Unit (OU), Sicherheits- und WMI-Filter. Es muss immer nachvollziehbar sein, woher der einzelne Registrierungsschlüssel stammt.

Auf dieser Basis sollten Dokumentationen und gegebenenfalls Konzepte für Tests, eigene Skripte und Bereitstellungs- und Rückführungsszenarien im Zusammenhang mit administrativen Vorlagen erstellt werden. Die Dokumentation sollte ebenfalls zur Planung der regelmäßigen Auswertung von System- und Sicherheitsprotokollen herangezogen werden.

Zur Dokumentation von aktiven Einstellungen ist die GPMC-Konsole gut geeignet, sofern Active Directory zum Einsatz kommt. Für die Gruppenrichtlinienobjekte, Richtlinienergebnissätze und Gruppenrichtlinienmodellierungen können Berichte in druckbarem Format in eine HTML-Datei exportiert werden (gewünschtes Objekt markieren | Menü *Aktion* | *Bericht speichern*...).

Prüffragen:

- Erfolgen Änderungen an Schlüsseln in der Registrierungsdatenbank ausschließlich über administrative Vorlagen und wird auf manuelle Änderungen vollkommen verzichtet?
- Wird die Funktionalität und Wirkung der in der Registrierungsdatenbank vorgenommenen Einstellungen auf einem isolierten Testsystem im Vorfeld erprobt?
- Werden alle administrativen Vorlagen ausschließlich in den vordefinierten Ordnern gespeichert und konfiguriert?
- Ist sichergestellt, dass es keine manuell hinzugefügten Schlüssel in der Registry gibt, die nicht durch eine administrative Vorlage oder ein geeignetes Werkzeug verwaltet werden?
- Sind alle aktivierten Einstellungen der administrativen Vorlagen in die Systemdokumentation des Servers aufgenommen worden?

# M 2.369 Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Wartung dient der Werterhaltung eines Windows Server 2003 bzw. der Aufrechterhaltung seiner Funktionen und vorgesehenen Verwendbarkeit. Sie darf nur von fachkundigem sowie autorisiertem Personal ausgeführt werden und kann Bestandteil einer Gewährleistung sein. Bei der Durchführung von Wartungen sind insbesondere beim Einsatz von externem Personal die Forderungen der Maßnahme M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten* zu berücksichtigen.

Eine Wartung wird regelmäßig und geplant auf Grundlage eines Wartungsplanes, in der Regel außerhalb des Normalbetriebes, durchgeführt. Werden Cluster für den Netzwerklastenausgleich eingesetzt (*Network Load Balancing,* NLB), ist auch eine Wartung ohne Unterbrechung des Normalbetriebs möglich. Die Wartung umfasst Konfigurationsarbeiten, Reinigungen, die Begutachtung und Erneuerung von Verschleißteilen, Hardware-Erweiterungen sowie das Beheben kleiner Defekte. Herstellerangaben sind dabei zu beachten (siehe M 2.213 *Inspektion und Wartung der technischen Infrastruktur*).

Somit werden erkannte Fehler behoben, Anpassungen und Aktualisierungen umgesetzt und gegebenenfalls über Erweiterungen neue Funktionen und Anwendungen bereitgestellt. Die Erweiterungen dürfen nur nach ausreichendem Testen und vorliegender Genehmigung vorgenommen werden. Änderungen am Server sind zu dokumentieren.

Wartungsanforderungen und deren Durchführung sind vom Verantwortlichen für die Wartung, meist der zuständige Administrator, zu koordinieren (siehe Baustein B 1.9 *Hard- und Software-Management*) und zu dokumentieren (Maßnahme M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

**Vorbereitung der Wartung**

Anhand der Teilkonzepte für die Rollen und Komponenten des Servers sollten die bei der Wartung abzuarbeitenden Bereiche identifiziert werden. Für wartungsrelevante Aspekte können die spezifischen Grundschutzmaßnahmen konsultiert werden. Anhaltspunkte für weitere wartungsrelevante Aspekte in verschiedenen Anwendungsszenarien sind in der Dokumentationsbibliothek *Microsoft Operations Framework* (MOF) für Windows Server 2003 zu finden.

Bestimmte wartungsrelevante Systemeigenschaften lassen sich nur im Normalbetrieb feststellen. Deshalb sind entsprechende Informationen aus dem *Systemmonitor, Netzwerkmonitor,* Taskmanager und rollenspezifischen Konsolen rechtzeitig zu ermitteln und zu berücksichtigen. Besonderes Augenmerk ist dabei auf die Seitenfehler in Verbindung mit der Auslagerungsdatei und auf den Ressourcenverbrauch von Prozessen zu richten (siehe M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*).

Mit dem *Windows Systemressourcen Manager* (WSRM) besteht für Enterprise- oder Datacenter-Editionen die Möglichkeit, den Ressourcenverbrauch für

Anwendungen, Prozesse und Dienste mittels Richtlinien zu definieren und zu steuern.

Es sollte ein Protokoll zu den während der Wartung abzuarbeitenden Schritten geführt werden, das auch Datum und einen Verantwortlichen enthält. Nach der Wartung sollte es aufbewahrt werden, um später eventuelle Unregelmäßigkeiten nachvollziehen zu können, z. B. bei der Auswertung der Ereignisanzeige.

Das Systemprotokoll aus der Ereignisanzeige ist auf Fehler und Warnungen zu prüfen. Es ist auf jeden Fall zu beurteilen, in wie weit der sichere Betrieb des Servers durch diese Ereignisse gefährdet ist.

Wenn durch Wartungsarbeiten ein stark erhöhtes Aufkommen von bestimmten Ereignistypen zu erwarten ist, dann sollte dies vorher angekündigt werden, um Fehlalarme zu vermeiden. Unter Umständen kann dies auch für andere Protokolle sinnvoll sein, soweit sie betroffen sind.

Darüber hinaus kann die Serverhardware mit anderen Werkzeugen überwacht werden. Viele Hersteller bieten für ihre Hardware eigene Überwachungssoftware an, die auch Warnmeldungen senden und verarbeiten kann. Je nach Ausstattung werden z. B. die Festplatten, die Lüfterdrehzahl, die Spannungen des Netzteiles und die unterbrechungsfreie Stromversorgung überwacht. Häufig bieten hochwertige Festplatten eine so genannte Fehlerfrüherkennung. Dadurch ist es möglich, rechtzeitig vor dem Ausfall der Festplatte diese zu wechseln. Es ist zu gewährleisten, dass diese Informationen bei der Wartung berücksichtigt werden, siehe hierzu auch M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*.

**Regelmäßige Wartungsarbeiten**

Es ist zu prüfen und zu gewährleisten, dass die Serverhardware vollständig ist und keine in der Organisation nicht zugelassenen Komponenten beinhaltet. Für den sicheren Betrieb des Servers müssen alle Geräte und Dienste ohne Störung in Betrieb sein. Deshalb ist ihr ordnungsgemäßer Betrieb in der *Computerverwaltung (Gerätemanager* und *Dienste)* zu kontrollieren.

Die aktuellen *Systemeigenschaften* des Servers sind mit den dokumentierten Konfigurationsvorgaben abzugleichen. Dabei sind besonders die Einstellungen unter *Erweitert*, *Systemwiederherstellung* und *Automatische Updates* zu beachten. Falls Sicherheitsvorlagen verwendet werden, ist die Konformität des Servers zur aktuellen Version der Vorlagen zu prüfen.

**Patches**

Bei einer Wartung ist zu überprüfen, ob aktuell verfügbare Sicherheits-Patches eingepflegt sind. Für diese Aufgabe kann der Microsoft Security Baseline Analyser (MBSA) genutzt werden. Zuvor sollte jedoch geprüft werden, ob der MBSA alle relevanten Patches detektieren kann und welche der verfügbaren Patches tatsächlich für den Server relevant sind. Normalerweise werden erforderliche Sicherheitsaktualisierungen zeitnah ausgeführt.

Da unter Umständen einzelne Patches für deren Wirksamkeit einen Neustart von Geräten, Diensten oder gar des Servers erforderlich machen, können diese Aktualisierungen nur während einer Wartung ausgeführt werden. Abweichungen sind zu begründen.

**Konten und Passwörter**

Die Organisationsrichtlinien für den Umgang mit Konten und Passwörtern gelten auch für lokale Konten des Servers und die Dienstkonten (siehe M 4.48 *Passwortschutz unter Windows-Systemen*). Im Rahmen von Wartungs- und Integritätsprüfungen des Windows-Server-2003-Systems sollte geprüft werden, ob die Organisationsrichtlinien für den Umgang mit Konten und Passwörtern bzw. die Regelungen des Berechtigungskonzeptes eingehalten werden. Insbesondere sollte hierbei geprüft werden, ob unbenutzte lokale Konten vorhanden sind oder leere Passwörter bzw. Passwörter, die nicht den Organisationsrichtlinien entsprechen, vergeben wurden. Hierbei können Tools bzw. Scripte des MBSA genutzt werden. Besonderes Augenmerk ist auch auf temporäre Konten zu richten, also solche, die nur für einen begrenzten Zeitraum vorgesehen waren oder sind.

Dienstkonten verfügen häufig über erweiterte Rechte und bedürfen deshalb eines besonderen Schutzes. Bei der Kennwortänderung der Dienstkonten muss das neu vergebene Kennwort zusätzlich in den Eigenschaften des betroffenen Dienstes auf dem Reiter *Anmelden* eingetragen werden. Anschließend ist ein Neustart der betroffenen Dienste notwendig. Werden diese Dienste während des Normalbetriebes benötigt, können solche Maßnahmen nur während der Wartung durchgeführt werden, siehe auch Maßnahme M 4.284 *Umgang mit Diensten ab Windows Server 2003*.

**Datenträger und Datenbestände**

Die Datenbestände des Servers sind auf nicht erlaubte Datentypen und Software zu prüfen. Abweichungen sind gemäß Vorgaben der Organisation zu behandeln. Dabei sind auch verschlüsselte Datenbestände zu erfassen, welche den Vorgaben der Verschlüsselungsrichtlinie der Organisation nicht entsprechen. Unerwünschte EFS-Verschlüsselungen können z. B. mit dem Werkzeug *EFSInfo* lokalisiert werden (siehe auch M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*).

Vorgaben für die Speicherplatznutzung (z. B. maximale Verzeichnisgröße oder Auslagerung alter Daten) sind auf deren Einhaltung zu kontrollieren und gegebenenfalls umzusetzen. Datenträgerkontingente unterstützen diese Aufgabe, erlauben jedoch für Windows Server 2003 (bis einschließlich SP1) nur eine Beschränkung pro Benutzer und Partition. Mit dem Windows Server 2003 R2 stehen mit der erweiterten Kontingentverwaltung und der Dateiprüfung umfangreiche und komfortable Werkzeuge mit Berichtsfunktion zur Verfügung.

Die aktuellen Berechtigungen für Daten, Freigaben, Registrierung und Drucker sind auf Unregelmäßigkeiten sowie Abweichungen von Vorgaben zu prüfen. Für relativ statische Datenbestände und für Systemdaten wird die Dokumentation und Überprüfung der vergebenen Berechtigungen mittels *.inf*-Dateien (*Sicherheitsvorlagen*) und *Sicherheitskonfiguration und -analyse* empfohlen.

Die Wartung für Datenträger umfasst die Überwachung des freien Speicherplatzes auf der Partition, die Datenträgerbereinigung und die Defragmentierung. Für deren Durchführung ist ausreichend Zeit einzuplanen.

Erhebliche Inkonsistenzen zwischen der Summe der gespeicherten Dateien, dem erwarteten und dem noch verfügbaren Speicherplatz auf der Festplatte können auf unerwünschte versteckte Datenströme (*Alternate Data Streams*, ADS) auf NTFS-Partitionen hinweisen. Falls es Hinweise auf versteckte Datenströme gibt, sollte darauf geachtet werden, dass die eingesetzte Antivirensoftware versteckte Datenströme untersucht (siehe M 2.157 *Auswahl eines*

*geeigneten Viren-Schutzprogramms*). Ist die Festplattenbelegung durch vermutete versteckte Datenströme erheblich, sollte eine Analyse mit geeigneten Werkzeugen von Drittherstellern erfolgen (siehe G 2.116 *Datenverlust beim Kopieren oder Verschieben von Daten ab Windows Server 2003*).

**Visuelle Kontrolle**

Durch die visuelle Kontrolle ist das äußere Umfeld des Servers zu begutachten. Dabei sind Kabel und Verbindungen, sowie die Befestigung von Baugruppen zu kontrollieren. Weiterhin ist eine Überprüfung der Sauberkeit und gegebenenfalls eine Reinigung der Lüftungskanäle, der Ventilatoren und der Kühlkörper durchzuführen.

**Spezielle Wartungsarbeiten**

Sollen Datenträger im Zuge von Wartungsarbeiten zuverlässig gelöscht werden, kann das nur mit Werkzeugen von Drittanbietern durchgeführt werden. Hierzu sind geeignete Produkte auszuwählen, siehe B 1.15 *Löschen und Vernichten von Daten*.

Ist Hardware redundant ausgelegt, wie z. B. durch RAID 5, doppelte Netzteile und Cluster, muss beim Ausfall einer redundanten Komponente diese umgehend ersetzt werden, da ansonsten die Ausfallsicherheit nicht mehr gegeben ist.

Alle Hardware-Hersteller bieten aktuelle Informationen, Firmware und Treiber für ihre Produkte an. Es wird empfohlen, diese Angebote regelmäßig zu prüfen und bei wesentlichen Änderungen deren Umsetzung innerhalb der Wartung zu berücksichtigen.

**Garantie- und Wartungsverträge**

Die Einhaltung von Garantie- und Wartungsverträgen ist zu überwachen, damit erforderliche Wartungen durch Vertragspartner durchgeführt werden und keine unnötigen Ausfälle oder Kosten entstehen. Die Beschaffung ist rechtzeitig über notwendige Aktivitäten zu unterrichten.

Prüffragen:

- Beinhalten die regelmäßigen Wartungsarbeiten unter Windows Server 2003 neben der Überprüfung des Patch-Levels auch eine regelmäßige Überprüfung der Hardware?
- Wurde für jeden Windows Server 2003 ein Wartungsplan erstellt und mit den Anforderungen der Sicherheitsrichtlinien abgestimmt?
- Werden durchgeführte Wartungsarbeiten angemessen dokumentiert?
- Sind die erforderlichen Garantie- und Wartungsverträge noch gültig und entsprechen den aktuellen Anforderungen?

# M 2.370 Administration der Berechtigungen ab Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Leiter IT

**Übersicht der zur Verfügung stehenden Berechtigungskonzepte**

Das Sicherheitsmodell von Windows mit Konten, Gruppen und Zugriffsberechtigungen beschränkt sich keineswegs auf Objekte im Dateisystem NTFS. Vielmehr können in fast allen Bereichen des Betriebssystems Berechtigungen für jede Art von authentisierbaren Konten fein granuliert werden. Daher ist ein eigenes Berechtigungskonzept für Windows Server zu erstellen.

Aspekte des Berechtigungsmodells von Windows-Servern ab Server 2003 sind:

- Benutzerkonten und Computerkonten
- Systemkonten
- vordefinierte Standardgruppen
- Gruppenmitgliedschaften
- Verschachtelung von Gruppen (nur Active Directory)
- Zugriffsberechtigungen am Objekt (*Access Control List*, ACL)
- Systemzugriffskontrollen-Einstellung am Objekt (*System Access Control List*, SACL)
- Vererbung

Folgende Berechtigungseinstellungen sind nicht Teil des oben genannten Berechtigungsmodells:

- ressourcenbasierte Berechtigungsmechanismen in den *Internet Information Services* (IIS)
- Systemrechte (engl. rights/privileges)
- rollenbasiertes Zugriffsmanagement (*Role Based Access Control*, RBAC)

Die Möglichkeiten dieser Berechtigungseinstellungen werden unter den Hilfsmitteln zum IT-Grundschutz (siehe *Administration der Berechtigungen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) erläutert.

**Schulung**

Das Verständnis der oben aufgezählten Mechanismen und der dahinter stehenden Philosophien muss den Administratoren durch Schulungen und Bereitstellung von Fachbüchern vermittelt werden. Ansonsten ist ein sicherer Betrieb der jeweils eingesetzten Mechanismen und damit des Windows-Servers insgesamt nicht zu gewährleisten.

Je nach Aufgabenbereich der Administratoren sollten sie auch zu den entsprechenden Komponenten geschult werden, um die Auswirkung von Berechtigungskonfigurationen einschätzen und vorausplanen zu können.

Details zu einzelnen Berechtigungen in den verschiedenen Bereichen des Betriebssystems können aus der Online-Hilfe von Windows und der Microsoft-Technet-Dokumentation für Administratoren entnommen werden.

**Grundregeln**

Die Administration von Berechtigungen für Benutzerkonten und administrative Konten erfordert ein Grundverständnis der Berechtigungs- und Sicherheitsmechanismen und die Einhaltung gewisser Grundregeln. Vor allem Berechtigungsänderungen im laufenden Betrieb ohne vorherige Tests müssen besonders sorgfältig durchgeführt werden, um die Verfügbarkeit des IT-Systems nicht zu gefährden.

Bei allen Tätigkeiten und Planungen im Zusammenhang mit dem Einräumen von Berechtigungen sollte immer das Prinzip der geringsten Berechtigungen (englisch *Least Privileges*) gelten. Danach sollten einem Konto nicht "vorsorglich" weitreichende Berechtigungen eingeräumt werden, sondern es sollte nur solche Berechtigungen erhalten, die zur Abdeckung der für das Konto definierten Anforderungen notwendig sind. Berechtigungen können Schritt für Schritt auf ein höheres Niveau angehoben werden, wenn die Anforderungen dies rechtfertigen. So sollte ein Konto nicht Vollzugriff auf eine Ressource bekommen, wenn der Benutzer des Kontos keine administrativen Tätigkeiten auf der Ressource auszuführen braucht.

Eine generelle Schwierigkeit besteht in der Vorhersage der Auswirkungen einer bestimmten Berechtigungskonfiguration. Windows-Server bieten verschiedene Simulationswerkzeuge zur Vorhersage der Auswirkungen von Berechtigungskonfigurationen an:

- Die Registerkarte *Effektive Berechtigungen*
  In den Sicherheitseinstellungen eines Objektes, zum Beispiel einer Datei, ist die Option zur Simulation unter *Erweitert* | *Effektive Berechtigungen* | *Auswählen* zu erreichen. Simulationen sollten sowohl mit der konfigurierten Sicherheitsgruppe als auch stichprobenartig mit Benutzerkonten durchgeführt werden, welche die Rechte ausüben sollen.
- Die Konsolen *Richtlinienergebnissatz* (Resultant Set of Policies, RSOP)
  *Start* | *Ausführen* | *rsop.msc* eintippen
  Kommt Active Directory zum Einsatz, kann dieser Prozess über die Gruppenrichtlinienverwaltungs-Konsole auch auf entfernten Computern im Netz gestartet und ausgewertet werden.

Von den Simulationswerkzeugen sollte bei der Modellierung von Berechtigungen und bei der Administration im laufenden Betrieb intensiv Gebrauch gemacht werden. Es ist zu empfehlen, dies beim Freigabeprozess für Konfigurationsänderungen in einer entsprechenden Sicherheitsrichtlinie zu formulieren.

**Account Sharing, vergessene Kennwörter**

Benutzerkonten dürfen nicht von mehreren Personen verwendet werden (so genanntes Account Sharing). Dies gilt für administrative wie für normale Benutzerkonten. Falls der Administrator aus zwingenden organisatorischen Gründen ein geteiltes Konto zur Verfügung stellen muss, ist dies für den Einzelfall zu begründen und zu dokumentieren. Das verwendete Konto, das Verfahren für die Durchsetzung der Kennwortrichtlinie, die Berechtigungen (ACL) und Überwachungseinstellungen (SACL) sowie der berechtigte Personenkreis sind zu dokumentieren. Der Missbrauch kann hier nur auf organisatorischem Weg vermieden werden. Geteilte Benutzerkonten sind ähnlich administrativen Konten als kritische Konten einzustufen und bei der Systemüberwachung zu berücksichtigen.

Der Forgotten Password Wizard dient ab Windows XP und Server 2003 zum Zurücksetzen vergessener lokaler Kennwörter, ohne dass lokal gespeicherte private Schlüssel dabei gelöscht werden. In einer Umgebung mit zentra-

lisierter Authentisierung sollte dieser Wizard nicht verwendet werden, da er die Sicherheit eines solchen Konzeptes unterläuft. Datenträger, mit denen das Passwort zurückgesetzt werden kann ("Password Reset Disc"), dürfen nicht erstellt werden. Dies muss in der Sicherheitsrichtlinie festgehalten werden und kann beispielsweise mittels Gruppenrichtlinien durchgesetzt werden.

Prüffragen:

- Gibt es für Windows Server ein eigenes Berechtigungskonzept?
- Werden die Administratoren zu den Berechtigungskonzepten von Windows Server geschult?
- Werden unter Windows Server vorsorglich Simulationswerkzeuge bei der Modellierung von Berechtigungen und bei der Administration im laufenden Betrieb benutzt?
- Wird unter Windows Server Account Sharing unterbunden bzw. auf ein Mindestmaß begrenzt?

# M 2.371 Geregelte Deaktivierung und Löschung ungenutzter Konten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Personalabteilung, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Soll ein Benutzerkonto deaktiviert oder gelöscht werden, muss anhand der Dokumentation der Zugriffsberechtigungen überprüft werden, welche Berechtigungen das Konto in der IT-Umgebung hat und für welche Authentisierungsvorgänge es benötigt wird.

### Konten deaktivieren

Ungenutzte Benutzerkonten können ein Sicherheitsrisiko darstellen. Aus diesem Grunde ist eine Empfehlung, die Angriffsoberfläche zu reduzieren und diese ungenutzten Konten zu deaktivieren. Dies ist umso wichtiger, je höher die Privilegien dieser Konten sind (administrative Konten). Aus diesem Grunde ist die Infrastruktur regelmäßig auf aktive Benutzer- und administrative Konten zu untersuchen, die nicht mehr verwendet werden. Es ist ebenfalls wichtig, dass solche Konten nicht von verschiedenen Personen verwendet werden. Es muss immer nachvollziehbar sein, wer wann welches Konto verwendet hat.

### Konten löschen

Muss ein Benutzerkonto gelöscht werden, ist anhand der Dokumentation zu überprüfen, welche Zugriffsrechte das Benutzerkonto hat. Vor dem Löschen des Kontos muss geprüft werden, auf welche Objekte (zum Beispiel Dateifreigaben) die Berechtigungen gesetzt sind. Nach dem Löschen ist sicherzustellen, dass die Konten bzw. deren Sicherheitskennung aus den Zugriffsberechtigungslisten (Access Control List, ACL) entfernt worden sind.

Dabei darf Windows Server 2003 in seiner Lauffähigkeit nicht eingeschränkt werden, z. B. durch gelöschte Dienstkonten. Bei der Löschung administrativer Konten sollte eine Stellvertreterregelung greifen, sofern die administrativen Aufgaben bestehen bleiben. Hierfür muss bereits vor der Löschung ein entsprechendes Ersatzkonto existieren und in Betrieb genommen worden sein. Wird hierbei nicht sorgfältig vorgegangen, dann kann es sehr schwierig werden, die Administrierbarkeit einer Ressource bzw. den Zugriff auf Ressourcen wiederherzustellen. Daher kann es sich als notwendig erweisen, das Konto zunächst zu deaktivieren und erst nach einem Test zu löschen. Beim Löschen von Benutzerkonten sollte vorher ein Verfahren definiert sein, das den Verbleib und gegebenenfalls die Weiterverwendung der vom Benutzer erzeugten Daten regelt. Ansonsten können die Daten unter Umständen nur mit erhöhtem Aufwand (Objektbesitz übernehmen durch Administratoren) oder gar nicht mehr lesbar gemacht werden. Dies gilt in besonderem Maße für hochvertrauliche bzw. verschlüsselte Daten (siehe Maßnahme M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*). Es sollte dementsprechend vor der Löschung auch ermittelt werden, in welchen Gruppen der Benutzer Mitglied war, um zu prüfen, ob er möglicherweise bislang das einzige Mitglied einer Gruppe mit administrativen Rechten oder Ressourcenberechtigungen war.

Die genannten Schritte stellen auch eine Herausforderung an die zugrunde liegenden organisatorischen Prozesse dar. Dies ist unter anderem in der Maßnahme M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* beschrieben.

Die geregelte Deaktivierung oder Löschung von Benutzerkonten sowie damit verbundene Fristen sollte in einer Sicherheitsrichtlinie für den IT-Verbund dokumentieren werden.

Prüffragen:

- Werden Windows-Systeme regelmäßig auf ungenutzte administrative und Benutzerkonten überprüft?
- Werden bei Windows-Systemen ungenutzte Benutzerkonten sofort deaktiviert?
- Wird bei Windows-Systemen vor dem Löschen von Benutzerkonten überprüft, auf welche Objekte die Berechtigungen gesetzt sind?
- Existieren für Windows-Systeme Verfahren für den Verbleib bzw. die Weiterverwendung von Daten nach der Löschung von Benutzerkonten?
- Bestehen bei Windows-Systemen administrative Ersatzkonten?

# M 2.372 Planung des VoIP-Einsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine grundlegende Voraussetzung für den sicheren Einsatz von VoIP ist eine angemessene Planung im Vorfeld. Die Planung für den Einsatz von VoIP kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Soll vollständig oder partiell auf VoIP umgestiegen werden? Soll VoIP nur für die Kommunikation der leitungsvermittelnden TK-Anlagen untereinander eingesetzt?
- Gibt es besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinformationen?
- Welche Signalisierungs- und Medientransportprotokolle sollen eingesetzt werden?
- Wie vielen Benutzern soll die Kommunikation über VoIP ermöglicht werden?
- Wie soll die Anbindung ans öffentliche Telefonnetz erfolgen? Sollen VoIP-basierte Kommunikationsverbindungen direkt aus dem öffentlichen Datennetz gestattet werden?
- Kann die Sicherheit des vorhandenen LANs durch VoIP beeinträchtigt werden? Ist das vorhandene LAN für die Nutzung von VoIP ausreichend dimensioniert? Müssen Änderungen an der Netzarchitektur vorgenommen werden?

Die folgenden Teilkonzepte sollten bei der Planung des VoIP-Einsatzes berücksichtigt werden:

- **Umfang der Verschlüsselung:** Es muss festgelegt werden, was verschlüsselt werden soll. Beispielsweise kann entschieden werden, dass die gesamte Kommunikation im LAN nicht verschlüsselt, aber alle externen Gespräche vor der Einsicht und Manipulation durch Dritter geschützt werden sollen (siehe Maßnahme M 2.374 *Umfang der Verschlüsselung von VoIP*). Im Weiterem muss entschieden werden, ob die Multimediadaten und/oder die Signalisierung verschlüsselt werden sollen.
- **Verschlüsselungsmechanismen:** Wenn für einzelne Kommunikationsstrecken die Verschlüsselung festgelegt wurde, muss entschieden werden, wie der Schutz integriert werden kann. Die Verschlüsselung kann sowohl
  auf der Anwendungsschicht, wie beispielsweise über H.235 oder SRTP (siehe M 5.134 *Sichere Signalisierung bei VoIP* und M 5.135 *Sicherer Medientransport mit SRTP*), als auch auf tieferen Schichten, wie über SSL/TLS, IPSec oder VPNs, erfolgen.
- **Komponentenauswahl:** Um die getroffenen Entscheidungen umsetzen zu können, müssen die einzusetzenden Geräte diese auch unterstützen. Können keine entsprechenden Geräte beschafft werden, weil beispielsweise nicht alle Anforderungen erfüllt werden können, muss die Planung

korrigiert werden. Hierdurch entstehende Änderungen müssen mit dem Sicherheitsmanagement abgestimmt und dokumentiert werden.

- **Notfallvorsorge:** Nicht nur für die Geschäftsprozesse ist die Verfügbarkeit der Telefonie eine wichtige Voraussetzung. Bei einem Ausfall der Telefonie kann keine Hilfe in Notfällen gerufen werden. Daher müssen entsprechende Vorkehrungen getroffen werden. Weitere Informationen hierzu sind in der Maßnahme M 6.100 *Erstellung eines Notfallplans für den Ausfall von VoIP* zu finden.
- **Netztrennung:** In einigen Fällen kann die logische oder physikalische Trennung des VoIP-Netzes vom Datennetz sinnvoll sein (siehe Maßnahme M 2.376 *Trennung des Daten- und VoIP-Netzes*). In der Planungsphase ist zu entscheiden, ob eine Segmentierung notwendig ist.
- **Leistungsmerkmale:** Sehr oft bieten VoIP-Komponenten zusätzliche Leistungsmerkmale. Diese können den Betrieb einer zusätzlichen Middleware-Komponente erfordern oder besitzen andere sicherheitsrelevante Nachteile. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und das Wechselsprechen. Während der Planung ist zu entscheiden, welche Leistungsmerkmale verwendet werden soll.
- **Administration und Konfiguration:** Es ist frühzeitig festzulegen, wer die Administration und Konfiguration vornehmen soll. Hierfür sollte ein für VoIP zuständiger Administrator benannt werden. Im weiterem ist zu entscheiden, wie die Administration erfolgen soll (siehe M 4.287 *Sichere Administration der VoIP-Middleware* und M 4.288 *Sichere Administration von VoIP-Endgeräten*).
- **Protokollierung:** Die Protokollierung von Meldungen der einzelnen VoIP-Komponenten spielt eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf dem System oder auf einem zentralen Logserver im Netz gespeichert werden sollen.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass diese Informationen meist von anderen Personen als dem Autor ausgewertet werden müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

Prüffragen:

- Sind für den VoIP-Einsatz die Anforderungen an die Integrität, Vertraulichkeit und Verfügbarkeit festgelegt?

# M 2.373 Erstellung einer Sicherheitsrichtlinie für VoIP

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Bei der Telefonie werden hohe Erwartungen in deren Verfügbarkeit gesetzt. Ebenso wichtig ist aber deren Vertraulichkeit. Daher ist der sichere und ordnungsgemäße Betrieb von Telekommunikationseinrichtungen besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen an VoIP sowie das zu erreichende Sicherheitsniveau ergeben sich aus der organisationsweiten Sicherheitsleitlinie. Sie sollten in einer spezifischen Sicherheitsrichtlinie für VoIP formuliert werden, um die übergeordnete und allgemein formulierte Sicherheitsleitlinie zu konkretisieren und umzusetzen. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie beispielsweise IT-Richtlinien, Passwortrichtlinien, Richtlinien zu den IT-Systemen, auf denen die VoIP-Komponenten betrieben werden, oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die VoIP-Sicherheitsrichtlinie muss allen Personen und Gruppen, die an Planung, Beschaffung und Betrieb der VoIP-Komponenten beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb von VoIP treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten.

**Allgemeine Regelungen für die VoIP-Nutzung**

Alle VoIP-Benutzer sollten über potentielle Risiken und Probleme bei der VoIP-Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgeklärt sein.

Da für die VoIP-Komponenten immer wieder neue Sicherheitslücken offen gelegt werden, sollte sich der IT-Sicherheitsbeauftragte regelmäßig über aktuelle Risiken informieren. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die neu bekannt gewordenen Gefahren zu informieren und damit auch zu sensibilisieren.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese sollten anschließend zwischen allen Beteiligten abgestimmt werden und auf Machbarkeit überprüft werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

In der Sicherheitsrichtlinie muss klar geregelt sein,

- ob und wo VoIP-Komponenten eingesetzt werden dürfen,

- unter welchen technischen Einsatzbedingungen VoIP eingesetzt wird. Hierzu gehören vor allem die Festlegung von Sicherheitsmaßnahmen, die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der betroffenen IT-Systeme,
- welche Informationen nicht über VoIP kommuniziert werden dürfen und
- welche Leistungsmerkmale und Funktionen unterstützt werden sollen.

Mitarbeiter müssen darüber informiert sein, unter welchen Bedingungen sie VoIP außerhalb der eigenen Institution benutzen dürfen, da hier unter Umständen andere Sicherheitsregelungen gelten.

**VoIP-Middleware**

Für den Betrieb von VoIP-Middleware muss unter anderem folgendes geregelt werden:

- Die Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils (siehe auch M 2.375 *Geeignete Auswahl von VoIP-Systemen*) müssen erstellt werden.
- Es müssen Regelungen für die Arbeit der Administratoren und Revisoren getroffen werden. Folgende Fragen sollten hierfür beantwortet werden:
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen das Vier-Augen-Prinzip?
  - Kann der Aufgabenbereich des Administrators für die IT-Systeme von dem Verantwortlichen für die VoIP-Applikation getrennt werden?
- Die Verantwortlichkeiten müssen festgelegt und geregelt werden.
- Vorgaben für die Installation und Konfiguration müssen festgelegt und dokumentiert werden, wie
  - das Vorgehen bei der Erstinstallation,
  - die Überprüfung der Default-Einstellungen hinsichtlich ihrer Sicherheitsgefährdungen und
  - die Verwendung und Konfiguration
- Eine Benutzer- und Rollenverwaltung muss eingeführt, beziehungsweise erweitert werden. Hierzu gehören:
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigungen für Installation, Updates, Konfigurationsänderungen etc.),
  - ein Rollenkonzept für die Administration und
  - eine Konzeption der Benutzerverwaltung. Die Benutzer müssen angelegt und Telefonnummern zugewiesen werden. Den Benutzern können bestimmte Privilegien, wie der Möglichkeit kostenpflichtige Servicenummern anzurufen, zuwiesen werden.
- Ein sicherer Betrieb erfordert Regelungen
  - zur Erstellung und Pflege von Dokumentation, Form und Umfang der Dokumentation, z. B. Verfahrensanweisungen, Betriebshandbücher,
  - dazu, welche Dienste und Protokolle zugelassen bzw. nicht zugelassen werden,

  - zu den erlaubten Kommunikationsverbindungen, wie zum Beispiel sollte ein direkter Verbindungsaufbau von internen VoIP-Systemen in öffentliche Netzen vermieden werden,
  - für die Durchführung von Softwareaktualisierungen und
  - zu den Vorgaben in der Sicherheitsrichtlinie der IT-Systeme, auf denen die VoIP-Middleware betrieben wird.
- Die Vorgaben für den sicheren Betrieb sollten Informationen dazu beinhalten, wie

  - die Administration abzusichern ist (beispielsweise sollte ein Administrationszugriff nur über abgesicherte Verbindungen erfolgen),
  - verschlüsselnde Signalisierungs- und Medientransport-Protokollen einzusetzen sind,
  - welche Werkzeuge für Betrieb und Wartung einzusetzen sind,
  - Berechtigungen zu vergeben sind und welche Vorgehensweisen bei Software-Updates und Konfigurationsänderungen zu beachten sind und
  - welche Sicherheitsmaßnahmen auf dem Betriebssystem umzusetzen sind, auf dem die Middleware betrieben wird.
- Für die Protokollierung ist zu entscheiden,

  - welche Ereignisse protokolliert,
  - wo die Protokolldateien gespeichert und
  - wie und in welchen Abständen die Protokolle ausgewertet werden sollen.
- Für die Datensicherung und Wiederherstellung bei VoIP-Komponenten muss das organisationsweite Datensicherungskonzept erweitert werden.
- Es müssen Regelungen für die Reaktion auf Betriebsstörungen, technische Fehler (lokaler Support, Fernwartung) und Sicherheitsvorfälle getroffen werden.

**VoIP-Endgeräte**

Im Folgenden werden Vorgaben für den Betrieb von VoIP-Endgeräten vorgestellt, die in der Sicherheitsrichtlinie ergänzt werden sollten.

- Es müssen Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils gemacht werden.
- Es müssen Regelungen für die Arbeit der Administratoren und Revisoren getroffen werden. Ein Beispiel hierfür wäre die Trennung der Administration des einzusetzenden Softphones von der Administration des IT-Systems.
- Vorgaben für die Installation und Konfiguration müssen in der Sicherheitsrichtlinie aufgenommen werden. Hierzu sollten folgende Fragen beantwortet werden:

  - Ist eine Konfiguration bei der Auslieferung der Hardphones ausreichend oder soll im Betrieb eine Konfiguration möglich sein?
  - Wie werden bei einer hohen Anzahl von Endgeräten die Änderungen der Konfiguration im Betrieb durchgeführt?
  - Über welche Zugangswege dürfen Administratoren auf die Endgeräte zugreifen?
  - Welche Arten von Konfigurationen der Leistungsmerkmale, wie beispielsweise Weiterleitungen, dürfen die Benutzer durchführen?
- Vorgaben für den sicheren Betrieb spielen eine wichtige Rolle. Hierzu gehören

  - die Absicherung der Administration (beispielsweise Zugriff nur über abgesicherte Verbindungen),

- der Einsatz von verschlüsselnden Signalisierungs- und Medientransport-Protokollen,
- Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement,
- Berechtigungen und Vorgehensweisen bei Software-Updates und Konfigurationsänderungen,
- Vorgaben für Maßnahmen bei der Abwesenheit des Benutzers, wie beispielsweise Rufumleitungen und Sperren des Telefons und
- der sichere Betrieb des Betriebssystems, auf dem ein Softphone betrieben wird.
- Für die Notfallvorsorge müssen in der Sicherheitsrichtlinie Regelungen für die Bereitstellung von alternativen Kommunikationswegen aufgenommen werden.

Die Verantwortung für die Umsetzung der VoIP-Sicherheitsrichtlinie liegt beim IT-Betrieb, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsbeauftragten erfolgen.

Prüffragen:

- Existiert für den Bereich VoIP eine Sicherheitsrichtlinie, in der allgemeine sicherheitstechnische Vorgaben konkretisiert werden?
- Werden in der VoIP-Richtlinie Vorgaben für den Betrieb und die Nutzung von VoIP Komponenten geregelt?
- Ist die VoIP-Sicherheitsrichtlinie allen beteiligten Personen und Gruppen zugänglich und bekannt?

# M 2.374 Umfang der Verschlüsselung von VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Gelingt es einem Angreifer, sich an einer geeigneten Stelle Zugang zu einem internen Netz zu verschaffen, kann er die gesamte Netzkommunikation im LAN protokollieren. Falls die VoIP-Nutzlast nicht verschlüsselt ist, kann der Angreifer sämtliche Informationen mitlesen. Beispielsweise kann er durch die Auswertung der Signalisierungsinformationen ermitteln, wer wie lange mit wem telefoniert hat. Allerdings könnte ein Angreifer auch die Nachrichten auswerten, die über das Medientransport-Protokoll ausgetauscht werden und dadurch die Telefongespräche mithören. Daher sollte überlegt werden, dass die VoIP-Nutzdaten verschlüsselt werden. Eine Verschlüsselung müssen aber alle beteiligten TK-Systeme unterstützen.

Bei der Überlegung, ob die Kommunikation über VoIP verschlüsselt werden soll, ist es häufig zweckmäßig, zwischen interner und externer Kommunikation zu unterscheiden.

Für VoIP-Telefonate innerhalb eines LANs kann überlegt werden, ob auf eine Verschlüsselung verzichtet werden kann. Dabei muss sichergestellt werden, dass auf diese Informationen nicht über einen unsicheren Netzbereich, wie einem WLAN, durch einen Außentäter zugegriffen werden kann. Um die internen Gespräche vor dem Zugriff durch Innentätern zu schützen, kann der Einsatz einer Verschlüsselung aber sinnvoll sein. Hierfür ist der Betrieb der VoIP-Endgeräte als VPN-Endpunkte oder die Nutzung eines verschlüsselten Medientransportprotokolls, wie SRTP, denkbar.

Wenn alle eingesetzten VoIP-Geräte verschlüsselte Signalisierungsprotokolle unterstützen, wird empfohlen, diese zu nutzen. Hierdurch wird unter anderem verhindert, dass ein Angreifer Passwörter mitlesen und sich als ein anderer Benutzer beispielsweise am SIP-Registrar anmelden kann.

Verlassen Pakete mit VoIP-Inhalten das gesicherte LAN, müssen sie mit entsprechenden Verfahren geschützt werden. Für den Schutz der VoIP-Kommunikation ist eines oder mehrere der folgenden Verfahren auszuwählen:

- Nutzung verschlüsselnder Medientransportprotokolle, wie SRTP (Secure Realtime Transport Protocol).
- Verschlüsselung der Signalisierungsprotokolle, beispielsweise mit TLS (Transport Layer Security)
- **Virtual Private Networks (VPNs):**
  Durch den Einsatz von VPN-Gateways können Informationen verschlüsselt zwischen entfernten LANs übertragen werden. Einzelne Geräte können als VPN-Endpunkte betrieben werden. Dies hat den weiteren Vorteil, dass ein Innentäter ebenfalls keinen Zugriff auf die Informationen erhält. Ohne eine direkte Unterstützung von verschlüsselnden Signalisierungs- und Medientransportprotokollen kann auf dieser Weise eine protokollunabhängige Verschlüsselung eingesetzt werden.
  Werden, beispielsweise für eine Kommunikation zwischen verschiedenen Liegenschaften, mehrere VoIP-Vermittlungseinheiten (Middleware) benötigt, sollten diese ebenfalls in einen VPN zusammengefasst werden, wenn keine anderen Verschlüsselungsmechanismen aktiviert werden können. Wird die Verbindung, beispielsweise zwischen mehreren Middleware-Komponenten in unterschiedlichen Liegenschaften, nicht ausreichend

geschützt, könnte ein Angreifer unter Umständen alle Gespräche zwischen den Liegenschaften abhören. Wird die Middleware auf einem IT-System betrieben, kann in der Regel eine VoIP-protokollunabhängige VPN-Unterstützung problemlos nachinstalliert werden.

- **Verschlüsselung des Funknetzes:**
  Auf ein ungesichertes Funknetz innerhalb einer Institution könnte auch von außerhalb der Liegenschaft auf das Netz zugegriffen werden. Sind die VoIP-Gesprächsteilnehmer über ein WLAN miteinander verbunden, muss ein qualifizierter Schutz für das WLAN, wie WPA2, genutzt werden (siehe hierzu Baustein B 4.6 *WLAN*). Da sich diese Verschlüsselung auf das Funknetz beschränkt, ist zu beachten, dass die Informationen im restlichen LAN ungeschützt übertragen werden. Verlassen die VoIP-Informationen nicht über andere Wege das LAN, gelten bei einer qualifizierten Verschlüsselung die gleichen Bedingungen wie bei einer internen Kommunikation, bei der unter Umständen auf eine Verschlüsselung verzichtet werden kann.

Soll ein Gespräch zu einem Telefonteilnehmer über ein öffentliches Telefonnetz aufgebaut werden, kann die Verbindung zwischen dem VoIP-Endgerät und dem Gateway, der zwischen dem IP-Netz und dem öffentlichen leitungsvermittelnden Netz eingesetzt wird, gegebenenfalls mit VPNs oder verschlüsselnden Signalisierung- und Medientransportprotokollen geschützt werden. Da nur sehr wenige Telefone für leitungsvermittelnde Netze Schutzmechanismen bereitstellen und deren Einsatz vom jeweiligen Empfänger abhängig ist, ist eine Verschlüsselung zwischen VoIP-Gateway und dem Gesprächspartner meist nicht realistisch.

Ist eine verschlüsselte Kommunikation, beispielsweise zu externen Gesprächspartnern, nicht möglich, müssen die Benutzer hierüber informiert und sensibilisiert werden. Vertrauliche Gespräche sollten bei einer fehlenden Verschlüsselung nicht über das Telefon geführt werden.

Bei der Beschaffung von VoIP-Komponenten muss darauf geachtet werden, dass diese verschlüsselnde Signalisierungs- und Medientransportprotokolle wie z. B. TLS und SRTP unterstützen (siehe M 2.375 *Geeignete Auswahl von VoIP-Systemen*).

Prüffragen:

- Werden VoIP-Datenpakete, die das gesicherte LAN verlassen, durch geeignete Sicherheitsmechanismen geschützt?
- Werden VoIP-Verbindungen zwischen Middleware-Komponenten in unterschiedlichen Liegenschaften dem Schutzlevel entsprechend geschützt?
- Werden Benutzer über Gefährdungen bei der VoIP-Kommunikation informiert und sensibilisiert?
- VoIP im WLAN: Ist ein qualifizierter Schutz des WLAN gewährleistet?

# M 2.375 Geeignete Auswahl von VoIP-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle, Leiter IT

Die verschiedenen Hersteller von TK-Produkten bieten zahlreiche Lösungen zur Telefonie an. Neben reinen Geräte für VoIP und für analoge und digitale Telefonie können auch Produkte, die beide Architekturen unterstützen, erworben werden. Beispiele sind TK-Anlagen für leitungsvermittelnde Netze, die über einen IP-Anschluss verfügen und Gateways, die zwischen eine VoIP-Architektur und ein öffentliches, leitungsvermittelndes Telefonnetz geschalten werden können. Für die Auswahl sind neben der Grundfunktionalität, wie der Unterstützung der benötigten Signalisierungs- und Medientransportprotokolle, zahlreiche sicherheitstechnische Aspekte zu berücksichtigen.

Bevor VoIP-Komponenten beschafft werden, muss eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt.

**Allgemeine Anforderungen**

Nachfolgend werden einige allgemeine Anforderungen aufgelistet, die bei der Beschaffung von VoIP-Endgeräten und der Middleware berücksichtigt werden sollten:

**1. Allgemeine Kriterien**

- Soll eine VoIP-Appliance oder eine Lösung, die auf einem Standard-PC betrieben werden kann, beschafft werden?
  In jedem Fall muss das meist komplexe Betriebssystem so konfiguriert werden, dass nur die wirklich benötigten Funktionen aktiviert sind, die Zugriffsrechte restriktiv vergeben und Schwachstellen systematisch beseitigt werden.
- Unterstützt das Produkt alle benötigten Protokolle?
- Werden Schulungen von dem Hersteller oder einem unabhängigen Anbieter zu dem Produkt angeboten?
- Gibt es verlässliche Informationen zur Zuverlässigkeit und Ausfallsicherheit von Hard- und Software?
- Können die VoIP-Komponenten den Ansprüchen an die Performance gerecht werden?
- Ist das Produkt nach formalen Methoden, wie den Common Criteria, evaluiert?
- Ist die VoIP-Komponente interoperabel zu bestehenden Produkten?
- Unterstützen die VoIP-Komponenten eine sichere Anmeldung und eine sichere Benutzerverwaltung?
- Enthält die mitgelieferte Produktdokumentation eine genaue Beschreibung aller technischen und administrativen Details?
- Wird für die VoIP-Komponenten die Möglichkeit des Abschlusses von Wartungsverträgen angeboten? Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich. Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden? Bietet der

Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
- Lässt sich das Produkt einfach installieren, konfigurieren, und administrieren?

**2. Protokollierung**

Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:

- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?
- Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen?
- Unterstützt das System zentrale Protokollierung? Eine zentrale Protokollierung erleichtert eine gezielte Auswertung der Protokolldaten.
- Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?

**3. Updates**

- Werden regelmäßig Updates und Patches für das Produkt angeboten? Werden Sicherheitspatches zeitnah nach Bekanntwerden einer Sicherheitslücke angeboten?
- Können durch eine Aktualisierung der Software auch neuere Versionen der Signalisierungs- und Medientransportprotokolle, in denen Sicherheitsprobleme beseitigt wurden und die zusätzliche Sicherheitsmechanismen bereitstellen, verwendet werden?
- Berücksichtigen die Updates tiefere Schichten der VoIP-Komponente, wie Updates im Betriebssystem oder Dienste, die nicht in unmittelbaren Zusammenhang zu VoIP stehen? Um bestehende Schwachstellen im Betriebssystem der Appliance oder im IT-System zu beseitigen, sollten diese Bestandteile ebenfalls aktualisiert werden.
- Werden Updates und Patches so abgesichert, dass ausgeschlossen werden kann, dass bei der Übertragung der Updates diese gegen manipulierte Versionen ausgetauscht werden können?

**4. Administration**

- Unterstützen die VoIP-Komponenten sichere Protokolle zur Administration?
- Können die VoIP-Komponenten so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
- Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
- Können die VoIP-Komponenten über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?

**5. Verschlüsselung**

Um über VoIP verschlüsselt kommunizieren zu können, müssen die beteiligten Geräte entsprechende Funktionalitäten beinhalten. Je nach Schutzbedarf kann aber während der Planung entschieden worden sein, auf eine Verschlüsselung der internen VoIP-Kommunikation zu verzichten. Dennoch sollten auch dann VoIP-Komponenten angeschafft werden, die über die Möglichkeit zur

Verschlüsselung verfügen oder bei denen diese nachgerüstet werden kann. Folgende Aspekte sollten berücksichtigt werden:

- Unterstützen die VoIP-Komponenten die Verschlüsselung der Medientransport- und Signalisierungsinformationen oder kann die Unterstützung nachträglich eingebunden werden?
- Können die VoIP-Komponenten als VPN-Endpunkte betrieben werden?

**Auswahl von Vermittlungssystemen (Middleware)**

Telefonie stellt oft einen essentiellen Geschäftsprozess dar. Daher werden unter anderem hohe Anforderungen an die Verfügbarkeit gestellt. Folgende Kriterien sollten bei der Beschaffung berücksichtigt werden:

- Kann die VoIP-Middleware redundant ausgelegt werden?
- Bietet der Hersteller gegebenenfalls Hochverfügbarkeitslösungen an?
- Sollen ein oder mehrere, zentrale Geräte die VoIP-Gesamtfunktionalität bereitstellen oder sollen mehrere einzelne, von einander abhängige Geräte beschafft werden?
  Einzelne, voneinander abhängige Geräte sind zum Beispiel SIP-Registrare, Proxy-Server und Location Server. Systeme, die alle VoIP-Funktionalitäten in einer Gesamtlösung bereitstellen, lassen sich oft leichter konfigurieren. Mehrere, verteilte Systeme können dagegen besser skaliert werden. Da die Administration bei mehreren Geräten oft aufwendiger ist, sind dadurch Fehlkonfigurationen wahrscheinlicher.

**Auswahl der aktiven Netzkomponenten**

Falls für den Umstieg auf VoIP neue Netzkomponenten wie Switches beschafft werden, müssen diese ebenfalls besondere Voraussetzungen erfüllen. Soll VoIP über ein bestehendes Datennetz genutzt werden, müssen die Geräte VoIP-Pakete erkennen und bevorzugt weiterleiten können. Soll zwischen zwei lokalen Netzen über ein unsicheres Datennetz, wie dem Internet, telefoniert werden können, müssen weitere Anforderungen gestellt werden. Wenn bisher keine Maßnahmen zur Verschlüsselung ergriffen wurden, sollten beispielsweise die am unsicheren Netz angeschlossenen Gateways als VPN-Endpunkte eingesetzt werden können.

Prüffragen:

- Berücksichtigt die Anforderungsliste Merkmale der IT-Sicherheit zur Erreichung des angestrebten Sicherheitsniveaus?
- Existiert eine Regelung, um die am Markt erhältlichen Produkte von Hard- und Software gemäß der Anforderungsliste zu bewerten?
- Existiert eine Regelung, um die Kaufentscheidung anhand der Bewertungsgrundlage durchzuführen?

# M 2.376 Trennung des Daten- und VoIP-Netzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik, Leiter IT

IP-Telefonie ermöglicht das Telefonieren über existierende IP-Datennetze. Jedoch können zur Erhöhung von Skalierbarkeit, Dienstqualität (QoS), Administrierbarkeit und Sicherheit die Datennetze von den Sprachnetzen auch logisch getrennt werden. Es muss überprüft werden, ob eine Trennung von Daten- und VoIP-Netz erforderlich ist. Eine Trennung ist sinnvoll, wenn Daten- und VoIP-Netz einen unterschiedlichen Schutzbedarf haben.

### Trennung der Netze über VLANs

Lokale Netze können physikalisch durch aktive Netzkomponenten oder logisch durch eine entsprechende VLAN-Konfiguration, also über virtuelle lokale Netze (Virtual Local Area Networks), segmentiert werden. Eine logische Trennung kann mit VLAN-Technologie auf der Ebene 2 mit VLAN-fähigen Switches aufgebaut werden (siehe auch M 2.277 *Funktionsweise eines Switches*). VLANs alleine bieten jedoch keinen Schutz vor Angreifern, die sich mit ihrem IT-System (PC, Laptop oder Server) physikalisch an ein VLAN anschließen. Da die Netzdose, also der VLAN-Port, des Telefons jedem unmittelbar zugänglich ist, könnte ein Angreifer direkt die Telefone im VLAN angreifen, indem er z. B. anstatt eines Telefons seinen PC mit dem VLAN verbindet.

Aus diesem Grunde sollten weitere, über die logische Netztrennung hinausgehende Maßnahmen getroffen werden, um derartigen Angriffe zu begegnen.

### Physikalische Trennung der Netze

Bei erhöhten Sicherheitsanforderungen kann eine komplette physikalische Trennung des Sprachnetzes vom Datennetz sinnvoll sein. Die physikalische Trennung von Daten- und Sprachnetzen verringert deutlich die Angriffsmöglichkeiten. Außerdem kann bei dem Ausfall eines Netzes, beispielsweise durch den Ausfall der aktiven Netzkomponenten oder einem Kabelbruch, weiterhin über das verbleibende Netz kommuniziert werden. Durch die Trennung hat die Auslastung des Datennetzes keinen Einfluss auf die Auslastung des Sprachnetzes.

### Probleme einer Trennung

Bei einer konsequenten Trennung des VoIP-Netzes vom IP-Datennetz können in der Praxis allerdings anderswo zusätzliche Aufwände entstehen:

- Die VoIP-Komponenten benötigen Zugriff auf Benutzerdatenbanken, wie LDAP-Verzeichnisse, die sich typischerweise bereits im Datennetz befinden, aber bei einer Netztrennung eventuell doppelt gepflegt werden müssten.
- Die Verwaltung des VoIP-Netzes, wie die Namensauflösung über DNS, erfordert in der Regel den Zugriff auf das Datennetz.
- Die Administration der VoIP-Komponenten kann bei einer konsequenten Trennung der Netze aufwendiger sein, beispielsweise da Software-Aktualisierungen der VoIP-Komponenten dann nicht mehr über ein Datennetz übertragen werden können, beispielsweise über SFTP, sondern vor Ort eingespielt werden müssen. Auch eine Remote-Konfiguration von VoIP-Komponenten, beispielsweise über SSH oder SHTTP, setzt einen An-

schluss an ein Datennetz oder separate IT-Systeme zur Konfiguration voraus.

Diese Probleme können aber durch entsprechende Gateways zwischen dem Daten- und Sprachnetz gelöst werden. Für viele Dienste könnte ein Proxy-Server im Sprachnetz betrieben werden, von dem die Anfragen aus dem Sprachnetz in das Datennetz weitergeleitet werden.

- Weitere Probleme bei der Netztrennung stellen die Nutzung von Multifunktionsgeräten, wie VoIP-Telefone mit integrierten Mail-Client, oder die weit verbreiteten Softphones dar. Diese Endgeräte benötigen sowohl Zugriff auf das Sprach- als auch auf das Datennetz.
  Ein Ansatz zur Lösung wäre, diese Geräte in einem dafür angelegten logischen Netz zu betreiben. Eine physikalische Trennung ist hier nicht möglich.
- Um den Aufwand der Verkabelung zu verringern, besitzen viele Hardphones einen integrierten "Miniswitch". Dabei wird das Telefon direkt an die Netzdose angeschlossen und ein weiteres IT-System, wie der Arbeitsplatzrechner, wird mit dem Telefon verbunden.
  Diese Anordnung verhindert die physikalische Trennung des Sprach- vom Datennetz. Für eine logischen Trennung muss der Access-Switch die beiden an einem Switchport angeschlossenen Geräte unterscheiden können. Dies ist beispielsweise über die MAC-Adresse oder durch eine IEEE 802.1X-Anmeldung möglich.

**Schutz der Ports**

Sollen Hardphones oder andere VoIP-Endgeräte, über die nur telefoniert werden soll, eingesetzt werden, ist darauf zu achten, dass von den Netzanschlüssen, mit denen diese Geräte verbunden sind, ausschließlich die vorgesehen VoIP-Verbindungen aufgebaut werden können. Anderenfalls könnte ein Angreifer ein mobiles IT-System an die Netzdose für das TK-Endgerät anschließen und Zugriff auf nicht für ihn bestimmte Informationen und Dienste erhalten. Ein Beispiel hierfür ist ein Telefon in einer nicht dauerhaft beaufsichtigten Umgebung, wie einer Tiefgarage. Dieser Schutz kann durch entsprechende Filterregeln an den aktiven Netzkomponenten erfolgen.

Je nach Schutzbedarf können zusätzliche Maßnahmen, wie Authentisierung nach IEEE 802.1X, eingesetzt werden, um einen sichereren Betrieb zu gewährleisten. Es muss aber berücksichtigt werden, dass eine dynamische oder statische Zuordnung der MAC-Adresse zu einem (Switch) Port oder einer VLAN-Zugriffsliste keinen ausreichenden Schutz darstellt, da MAC-Adressen leicht gefälscht werden können.

Prüffragen:

- Erfordert der Schutzbedarf eine Trennung des Daten- und VoIP-Netzes?
- Haben Geräte, die für VoIP und Datendienste genutzt werden Zugriff auf das Datennetz und das VoIP-Netz?
- Können von Netzanschlüssen für VoIP-Endgeräte nur VoIP-Verbindungen aufgebaut werden?

# M 2.377 Sichere Außerbetriebnahme von VoIP-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sollen VoIP-Komponenten, beispielsweise Endgeräte oder Middleware, außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden. Dies gilt nicht nur, wenn Geräte an Hersteller, Service-Unternehmen, Entsorgungsunternehmen oder sonstige Dritte weitergegeben werden. Auch bei Verschrottung, Umzug oder Weitergabe an andere Benutzer müssen entsprechende Maßnahmen ergriffen werden. Neben der endgültigen Außerbetriebnahme betrifft dies insbesondere auch Reparaturen, Wartung und Garantieaustausch.

In vielen Fällen ist es erforderlich, frühzeitig mit Herstellern, Händlern beziehungsweise Service-Unternehmen zu klären, welche Maßnahmen zur Löschung sicherheitsrelevanter Informationen mit den Vertrags- und Garantiebedingungen vereinbar sind. Oft können hier gemeinsam sinnvolle Vorgehensweisen festgelegt werden.

Je nach Einsatzzweck der Komponenten können beispielsweise folgende Informationen auf den Geräten gespeichert sein:

- Auflistungen, wer mit wem telefoniert hat,
- Zeitpunkt und Dauer der Anrufe,
- Benutzernamen und Passwörter für die Anmeldung an der VoIP-Infrastruktur,
- Rechte und Privilegien der einzelnen Benutzer,
- E-Mail-Adressen der einzelnen Benutzer für Voice-Mails,
- Ansagen für den Anrufbeantworter,
- hinterlassene Nachrichten für die Benutzer,
- IP-Adressen und weitere Informationen, die auf den Netzaufbau schließen lassen,
- Protokolldateien,
- Zertifikate und Schlüssel,
- Konfigurationsdateien,
- persönliche Telefonbücher,
- organisationsweite Telefonverzeichnisse mit allen Mitarbeitern,
- Passwörter, um private Gespräche abzurechnen,
- Informationen über weitere Dienste für die Benutzer, wie Terminerinnerungen und
- in Ausnahmefällen die vollständige Aufzeichnung der eigentlichen Telefongespräche.

Aufgrund des Schutzbedarfs dieser Informationen ist darauf zu achten, dass die Daten gelöscht beziehungsweise unlesbar gemacht werden, bevor defekte oder veraltete Geräte außer Betrieb genommen oder ausgetauscht werden. Nach dem Löschen der Daten muss überprüft werden, ob das Löschen auch erfolgreich war. Die Vorgehensweise hängt dabei stark von der Art und vom Verwendungszweck des Gerätes ab.

Bei "normalen" Rechnern, die als VoIP-Komponenten eingesetzt waren, sollten die Festplatten mit einem geeigneten Tool so gelöscht werden, dass keine Wiederherstellung der Dateien mehr möglich ist. Die kann beispielsweise dadurch geschehen, dass der Rechner von einem externen Boot-Medium gest-

artet wird und die Festplatten mit Zufallsdaten überschrieben werden. Dabei ist es empfehlenswert, den Überschreibvorgang mehrfach zu wiederholen.

Bei Appliances hängt die Vorgehensweise davon ab, ob in dem Gerät eine Festplatte eingebaut ist oder ob die Daten in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Neben den Informationen, die auf dem Gerät selbst gespeichert sind, sollte auch überprüft werden, ob auf den Backup-Medien sensitive Informationen enthalten sind. Falls es nicht aus anderen Gründen (beispielsweise Archivierung, Aufbewahrungspflicht aufgrund gesetzlicher Regelungen) erforderlich ist, die Backup-Medien aufzubewahren, so sollten die Medien nach der Außerbetriebnahme des Gerätes ebenfalls gelöscht werden.

Oft sind die Komponenten von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Prüffragen:

- Existiert im Rahmen der (temporären) Außerbetriebnahme eine Regelung, um die Daten auf den abzuschaltenden IT-Komponenten sicher zu löschen?
- Existiert im Rahmen der Außerbetriebnahme eine Regelung, um die Datensicherungsmedien der abzuschaltenden IT-Komponenten sicher zu löschen?

# M 2.378 System-Entwicklung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Leiter IT

System-Entwicklung findet im Sinne dieser Maßnahme statt, wenn Hardware, Software oder ein komplexes System, das aus mehreren Software- und Hardware-Komponenten besteht, erstellt, geändert oder ergänzt werden soll.

In allen diesen Fällen muss dieses Vorhaben vor der Durchführung mit der IT-Leitung und den betroffenen Fachabteilungen abgestimmt werden. Hierfür muss eine erste Übersicht der benötigten Leistungen und Anforderungen formuliert werden. Das Sicherheitsmanagement ist schon zu diesem frühen Zeitpunkt über das Vorhaben einer System-Entwicklung zu informieren, damit die relevanten Sicherheitsaspekte schon bei der Konzeption mit berücksichtigt werden können. Neben den Leistungen, die das System erbringen soll, müssen auf jeden Fall die möglichen Auswirkungen auf die Geschäftsprozesse und auf die Informationssicherheit in der Organisation betrachtet werden.

Die Anforderungen an die Sicherheit eines IT-Systems sollten bereits vor Beginn der Entwicklung ermittelt und abgestimmt werden. Eine nachträgliche Implementierung von Sicherheitsmaßnahmen ist bedeutend teurer und bietet im Allgemeinen weniger Schutz als Sicherheit, die von Beginn an in den Systementwicklungsprozess oder in den Auswahlprozess für ein Produkt integriert wurde. Sicherheit sollte daher integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

Die hier aufgeführten Empfehlungen orientieren sich am "Planung und Durchführung von IT-Vorhaben in der Bundesverwaltung" (V-Modell) sowie teilweise an den Vorgaben der "Information Technology Security Evaluation Criteria" (ITSEC) und den "Common Criteria for Information Technology Security Evaluation" (CC).

Für die Erstellung der Anforderungen ist die Maßnahme M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* zu beachten. Dort werden die wesentlichen Punkte erläutert, die zur Festlegung der funktionalen und der sicherheitsrelevanten Anforderungen berücksichtigt werden müssen.

Der Anforderungskatalog muss mit dem Sicherheitsmanagement abgestimmt werden. Falls sich im Laufe der System-Entwicklung Änderungen der Anforderungen ergeben, muss ebenfalls das Sicherheitsmanagement diesen zustimmen und der Anforderungskatalog aktualisiert werden. Der Anforderungskatalog bildet die Grundlage für die Abnahme und Freigabe des Produktes.

**Vorgehensmodell**

Die System-Entwicklung muss nach einem durchgängigen, einheitlichen und verbindlichen Vorgehensmodell durchgeführt werden. Diese müssen die strikte Einhaltung des Vorgehensmodell sicherstellen. Das Vorgehensmodell muss sicherheitsspezifische Rollen, Aktivitäten und Ergebnisse umfassen, durch die die Angemessenheit und Umsetzung sicherheitsbezogener Systemeigenschaften kontrolliert werden können.

Vor der Freigabe müssen mindestens die in den ITSEC/CC definierten Phasen

- Anforderungsdefinition,
- Architektur- oder Fach-Entwurf,
- Fein-Entwurf und

- Realisierung durchlaufen werden.

**Sicherheitsrelevante Phasenergebnisse der Anforderungsdefinition**

In der Anforderungsdefinitionsphase müssen die Bedrohungen, Schwachstellen und Risiken für die Informationssicherheit der jeweiligen Anwendung, die Sicherheitsaspekte der Einsatzumgebung, die externen Vorgaben und das Projektumfeld untersucht werden. Im Rahmen einer Schutzbedarfsfeststellung wird daraus der Sicherheitsbedarf abgeleitet, der zur Formulierung von Sicherheitsanforderungen führt. Die Sicherheitsanforderungen müssen auf Konsistenz und Vollständigkeit geprüft werden (siehe auch M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*).

**Sicherheitsrelevante Phasenergebnisse des Architektur-Entwurfs**

In der Architektur-Entwurfsphase müssen die internen Kontrollen für die Anwendung, die Grundfunktionen der Informationssicherheit und die organisatorischen und technischen Sicherheitsmaßnahmen auf fachlicher Ebene spezifiziert werden.

Es muss geprüft werden, dass die Sicherheitsanforderungen durch die Spezifikationen des Architektur-Entwurfs konsistent und ausreichend detailliert dargestellt werden. Hierbei sollte eine klare logische Trennung zwischen Sicherheitskomponenten und anderen Komponenten vorgenommen werden.

**Sicherheitsrelevante Phasenergebnisse des Fein-Entwurfs**

In der Phase des Fein-Entwurfs müssen die Sicherheits-Spezifikationen des Fach-Entwurfs so weit verfeinert werden, dass sie als Basis für die Realisierung dienen können, ohne dass ein weiterer Interpretationsbedarf besteht. Alle Module, in denen Kontrollfunktionen durchgeführt werden, sicherheitsempfindliche Verarbeitungs- und Kommunikationsabläufe erfolgen und auf sensitive Daten zugegriffen wird oder von denen sensitive Daten übertragen werden, müssen identifiziert werden.

Es muss geprüft werden, ob der Fach-Entwurf durch den Fein-Entwurf konsistent verfeinert wird. Die für die Gewährleistung der Sicherheitsanforderungen notwendigen internen Kontrollen müssen durch die Definition von Programm-Schnittstellen (API, Application Program Interfaces) spezifiziert werden. Für eine bessere Handhabung sollten die Sicherheits-APIs klar strukturiert und von den übrigen Modulen getrennt sein.

**Sicherheitsrelevante Phasenergebnisse der Realisierung**

In der Realisierungsphase müssen die spezifizierten Sicherheitsanforderungen durch Nutzung der entsprechenden Sicherheits-APIs adäquat umgesetzt werden. Es muss geprüft und getestet werden, ob die Implementation ihrer Spezifikation, insbesondere der Sicherheitsspezifikation genügt.

**Mindestanforderungen an die Entwicklungsumgebung**

Eine integrierte Entwicklungsumgebung (Integrated Development Environment, IDE) ist ein Anwendungsprogramm zur Entwicklung von Software. Die integrierte Entwicklungsumgebung erleichtert das Entwickeln von IT-Systemen, da alle wesentlichen Bestandteile wie zum Beispiel der Compiler, Debugger oder der Editor zu einer Einheit zusammengefasst sind.

Es muss eine einheitliche und verbindliche Bibliotheksstruktur für die gesamte Entwicklung zugrunde gelegt werden. Namenskonventionen müssen sowohl für den Programmcode als auch für die Benennung von Modulen definiert und

vorgeschrieben werden. Ziel ist dabei, wichtige Informationen wie z. B. Entwicklungsstadium und -ort, Dokumentationstyp etc. durch geeignete Bezeichnung hervorzuheben.

Es sind Methoden, Werkzeuge und Rollen zu definieren und einzusetzen, die es erlauben,

- Systeme (Hard- und Software) sowie deren Bestandteile und Eigenschaften festzulegen und zu identifizieren,
- die systematische und kontrollierte Bearbeitung der notwendigen Änderungen und Verbesserungen zu steuern,
- unbeabsichtigte, unkontrollierte oder ungesteuerte Veränderungen zu verhindern,
- alle Zwischen- und Endergebnisse zu archivieren und zu verwalten,
- Entwicklungen dezentral, d. h. in verschiedenen Entwicklungseinheiten nach einem einheitlichen (Sicherheits-)Standard durchzuführen,
- alle Benutzer der Entwicklungswerkzeuge und der Entwicklungsdatenbank eindeutig zu identifizieren,
- den Zugriff von Benutzern der Entwicklungswerkzeuge auf die Entwicklungsdatenbank in Abhängigkeit von der Benutzerrolle (need-to-know) zu kontrollieren,
- die Integrität der Entwicklungsdaten zu gewährleisten,
- Modifikationen der Entwicklungsdaten feststellen und zu Personen zuordnen zu können.

Es muss möglich sein, geprüfte und abgenommene Entwicklungsergebnisse festzuschreiben, so dass sie als Basis für die weitere Entwicklung dienen können. Insbesondere muss es möglich sein, an definierten Punkten des Vorgehensmodells die Entwicklung an unterschiedliche Entwicklungseinheiten zur Weiterführung zu vergeben.

Die eingesetzten Entwicklungswerkzeuge müssen es unterstützen, dass alle aufgrund von Modifikationen oder aufgrund von negativen Testergebnissen nötigen Änderungen nachgehalten, durchgeführt und qualitätsgesichert werden.

Auch die physische Umgebung, in der die System-Entwicklung stattfinden soll, muss bei der frühen Planung anhand der Sicherheitsanforderungen festgelegt werden. Dazu gehören unter anderem auch die Anforderungen an Zutritts- und Zugangskontrollmechanismen.

**Qualitätssicherung (QS)**

Die Qualitätssicherung muss bei Beginn der Entwicklung geplant werden. Dabei müssen geeignete Maßnahmen zur Einhaltung der Sicherheitsanforderungen festgelegt und in konstruktiver und analytischer Weise im Entwicklungsprozess verankert sein.

Neben der Kontrolle, ob das System die Funktionalitäten gemäß Spezifikation und Anforderungskatalog erfüllt, muss auch das Verhalten des Systems im Fehler- oder Missbrauchsfall überprüft werden.

Es muss QS-Maßnahmen zu definierten Reviewterminen, mindestens am Ende jeder Entwicklungsphase, geben. Darüber hinaus können im Bedarfsfall zusätzlich interne Reviews einberufen werden.

Während der Anforderungsdefinition und der Entwurfsphasen sind Testspezifikationen und Testfälle zu entwerfen und zu dokumentieren, die zur Prüfung der System-Qualität und der Einhaltung der Sicherheitsanforderungen geeig-

net sind. Während der Realisierungsphase und bei der Abnahme müssen entsprechende Tests durchgeführt werden.

Die Durchführung der Tests ist zu dokumentieren. Automatische Wiederholbarkeit und automatischer Abgleich der Testergebnisse (Regressionstest) sind anzustreben. Praxisdaten als Testdaten sind grundsätzlich nur in anonymisierter Form zulässig (siehe auch M 2.82 *Entwicklung eines Testplans für Standardsoftware* bzw. M 2.83 *Testen von Standardsoftware*).

**Überführung in Produktion und Software-Wartung**

Es muss einheitliche Richtlinien für die Überführung in die Produktion und für die System-Wartung geben.

**Überführung in die Produktion**

Die strikte Trennung von Entwicklung und Produktion, speziell der Verarbeitung von Testdaten und Echtdaten, muss gewährleistet werden. Es muss ein klar definiertes Freigabeverfahren für entwickelte Systeme und Anwendungen geben. Erst nach der Freigabe darf der Transfer aus der Test- in die Produktionsumgebung erfolgen. Sämtliche Programmteile, die lediglich Testzwecken dienen, sind vor der Freigabe zu entfernen. Mindestvoraussetzung für eine Freigabe ist das vollständige und erfolgreiche Durchlaufen einer Abnahme mit umfangreichen Tests in der Zielumgebung am Ende des Entwicklungsprozesses. Im Rahmen der Abnahme muss insbesondere festgestellt werden, ob sich die IT-Systeme und IT-Anwendungen in der Zielumgebung gemäß den Sicherheitsanforderungen verhalten.

Es muss sichergestellt sein, dass nur ordnungsgemäß freigegebene Programme bzw. Module zum Einsatz kommen (siehe auch M 2.85 *Freigabe von Standardsoftware*).

- Es muss Verfahren zur sicheren Verteilung von Entwicklungsergebnissen geben (siehe auch M 2.86 *Sicherstellen der Integrität von Standardsoftware*).
- Es muss einheitliche und verbindliche Verfahren zur Installation und Konfiguration der ausgelieferten Anwendungen geben (siehe auch M 2.84 *Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware* bzw. M 2.87 *Installation und Konfiguration von Standardsoftware*).
- Zu keinem Zeitpunkt dürfen Entwickler in der Lage sein, unautorisiert und unkontrolliert IT-Systeme oder Anwendungen während der Entwicklung zum Produktionseinsatz zu bringen oder bereits in der Produktion befindliche IT-Systeme oder Anwendungen nach der Abnahme bzw. Freigabe zu modifizieren (siehe auch M 2.88 *Lizenzverwaltung und Versionskontrolle von Standardsoftware*).
- Es muss ein Verfahren geben, die Übernahme in Abhängigkeit von zeitlichen und lokalen Bedingungen vorzusehen.

**Wartung und Problemmanagement**

Jegliche unautorisierte Veränderung eingesetzter IT-Systeme muss verhindert werden. Autorisierte Modifikationen müssen durch ein geeignetes Änderungs- und Konfigurationsmanagement nachvollziehbar sein. Im Rahmen des Änderungs- und Konfigurationsmanagements müssen auch Aufbewahrungsfristen für alle System-Komponenten definiert werden.

Auch nicht mehr im Einsatz befindliche Systemkomponenten, wie Programm-oder Modulversionen, Konfigurationsdaten und deren Dokumentation müssen für die Dauer der Aufbewahrungsfrist nachvollziehbar bleiben. Es

muss ein klar definiertes Verfahren und eindeutig festgelegte Kompetenzen für die Rückmeldung von Systemproblemen an die zuständige Instanz geben.

Jede autorisierte Modifikation im System aufgrund festgestellter Mängel oder zur Erweiterung der Funktionalität muss gemäß dem gewählten Vorgehensmodell in der einheitlichen Entwicklungsumgebung mit einer kontrollierten Wieder-Überführung in die Produktion erfolgen. Es muss zusätzlich ein klar definiertes Verfahren für den Umgang mit Notfällen geben.

**Software-Entwicklung durch Endbenutzer**

Standardsoftware ermöglicht oft den Endbenutzern die Entwicklung und Nutzung von eigenen Programmen, um Routinetätigkeiten zu erleichtern (z. B. über Makroprogrammierung). Der unkontrollierte Einsatz solcher selbstentwickelter Programme kann allerdings ein Sicherheitsrisiko darstellen. Daher sollte in jeder Organisation die Grundsatz-Entscheidung getroffen werden, ob solche Eigenentwicklungen erwünscht sind oder nicht und wer diese erstellen darf (siehe M 2.379 *Software-Entwicklung durch Endbenutzer*). Eigenentwicklungen müssen ebenfalls getestet und freigegeben werden, bevor sie in der Produktivumgebung eingesetzt werden dürfen. Ebenso muss geklärt werden, wer diese Programme wartet und Probleme damit behebt. Die Regelungen für den Einsatz von selbstentwickelten Programmen sollte in einer Sicherheitsrichtlinie festgehalten werden.

Prüffragen:

- Ist ein Prozess vorhanden, der sicherstellt, dass relevante Aspekte der Informationssicherheits schon bei der Konzeption einer System-Entwicklung berücksichtigt werden?
- Existiert ein Vorgehensmodell zur Systementwicklung, welches sicherheitsspezifische Rollen, Aktivitäten und Ergebnisse berücksichtigt?
- Werden bei der System-Entwicklung die Risiken für die Anwendung und die Einsatzumgebung idenfiziert und berücksichtigt?
- Werden entwickelte Komponenten einem sicherheitstechnischem Test nach der Sicherheitsspezifikation unterzogen?
- Sind die Anforderungen an die Entwicklungsumgebung definiert?
- Sind für die System-Entwicklung angemessene Qualitätssicherungsmaßnahmen definiert?
- Existieren für die System-Entwicklung Richtlinien zur Überführung von Anwendungen in die Produktion und zur Wartung?
- Ist die Trennung von Test- und Echtdaten gewährleistet?
- Sind Aufbewahrungsfristen für alle System-Komponenten definiert?

# M 2.379 Software-Entwicklung durch Endbenutzer

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Leiter IT

Viele Standardprogramme ermöglichen es den Benutzern, selbst Programme zu entwickeln, z. B. um sich Routinetätigkeiten zu erleichtern. Ein typisches Beispiel dazu ist die Makroprogrammierung unter Microsoft Word oder Access oder auch die Bereitstellung von Programmierschnittstellen bei Microsoft Outlook.

Die Kreativität und Einsatzbereitschaft, die Mitarbeiter hierbei an den Tag legen, ist grundsätzlich zu begrüßen, allerdings sollte trotzdem in jeder Institution überlegt werden, wie mit der Makro- bzw. Software-Entwicklung durch Endbenutzer umgegangen werden soll.

Es ist zu bedenken,

- dass die Makro- bzw. Programmersteller im allgemeinen keine geschulten Programmierer sind,
- dass die Sicherheitsrichtlinien des Hauses beachtet werden sollten,
- wie andere Benutzer davon profitieren können (und wer dann die Benutzerbetreuung übernimmt) und
- wie die meist spontan erstellten Programme gepflegt und dokumentiert werden.

Zunächst sollte in jeder Institution die Grundsatz-Entscheidung getroffen werden, ob solche Eigenentwicklungen erwünscht sind oder nicht. Dies ist in jedem Fall in den Sicherheitsrichtlinien zu dokumentieren.

Wenn Eigenentwicklungen unerwünscht sind, sollte sinnvollerweise bereits bei der Installation von Standardprogrammen die Möglichkeit dazu deaktiviert werden (soweit dies möglich ist).

Sind Eigenentwicklungen dagegen notwendig, sollten hierfür entsprechende Benutzerrichtlinien entwickelt werden, um Mindestanforderungen an Sicherheit, Dokumentation und Qualität sicherzustellen.

In einer solchen Richtlinie sollte insbesondere festgehalten werden, dass

- die bestehenden Vorschriften zum Datenschutz und zur Informationssicherheit eingehalten werden,
- die Eigenentwicklungen sorgfältig dokumentiert werden,
- für Eigenentwicklungen nur die dafür freigegebenen Software-Produkte (z. B. die Makro-Funktionalität eines bestimmten Office Paketes) verwendet werden. Die Installation weiterer Anwendungen oder Entwicklungsumgebung ohne Genehmigung der IT-Abteilung ist nicht zulässig.

Auch in Eigenentwicklungen wird einiges an Arbeitszeit investiert. Deswegen sollte sichergestellt sein, dass Eigenentwicklungen auch anderen Benutzern zu Gute kommen und dann auch dauerhaft gepflegt werden. Weiterhin sollte ein Ansprechpartner für Probleme mit diesen Eigenentwicklungen vorhanden sein. Eigenentwicklungen sollten auch allen Benutzern in der aktuellen Version zur Verfügung stehen. Daher ist es sinnvoll, alle Eigenentwicklungen, die für weitere Mitarbeiter interessant sein könnten, an die IT-Abteilung weiterzuleiten. Diese kann dann prüfen, ob eine weitere Verbreitung sinnvoll ist, und

kann im weiteren eventuell notwendige Anpassungen vornehmen und Benutzersupport anbieten.

Die Makro-Programmierungen müssen gegen unerlaubte Veränderung geschützt werden. Auch dürfen nur vertrauenswürdige Makros eingesetzt werden. Außerdem sollte die Weitergabe von Entwicklungsergebnissen an Unbefugte verhindert werden. Makro-Erweiterungen sollten erst dann im Produktivsystem verwendet werden, nachdem diese in einer isolierten Testumgebung getestet und für sicher erachtet wurden.

Prüffragen:

- Gibt es ein Verfahren für den Umgang mit Software oder Makros, die durch Endbenutzer entwickelt wurde?
- Ist sichergestellt, dass Eigenentwicklungen gut dokumentiert sind?
- Ist sichergestellt, dass Eigenentwicklungen allen Benutzern in der aktuellen Version zur Verfügung stehen?

# M 2.380 Ausnahmegenehmigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

In Einzelfällen kann es sinnvoll und notwendig sein, Ausnahmen von den in einer Sicherheitsrichtlinie getroffenen Regelungen zuzulassen. Ausnahmen sollten zwar möglichst vermieden werden, es ist aber auf jeden Fall besser, eine Ausnahme zuzulassen, als unnachgiebig auf Vorgaben zu bestehen, die im konkreten Einzelfall nicht einzuhalten sind. Sollten sich Ausnahmen häufen, ist dies ein Zeichen dafür, dass die vorhandenen Sicherheitsvorgaben überdacht und eventuell angepasst werden müssen.

Ausnahmen müssen aber in jedem Fall durch eine autorisierte Stelle genehmigt werden. Bei dem Genehmigungsverfahren sind sowohl Fachverantwortliche als die "Eigentümer" von Informationen und Anwendungen, als auch das Sicherheitsmanagement zu beteiligen. Für alle Ausnahmefälle muss gründlich überprüft werden, ob diese die Sicherheitsvorgaben nicht untergraben. Dafür ist eine Risikobewertung vorzunehmen. Ausnahmen dürfen nur genehmigt werden, wenn dass ermittelte Risiko als tragbar eingestuft wurde.

Ausnahmegenehmigungen sollten zeitlich klar befristet werden. Es muss regelmäßig überprüft werden (spätestens alle 12 Monate), ob die Ausnahmegenehmigungen noch erforderlich sind und ob zeitlich befristete Ausnahmegenehmigungen wieder aufgehoben oder nach Ablauf verlängert wurden.

Anschließend muss eine schriftliche Begründung verfasst werden, die von den Verantwortlichen zu unterzeichnen ist.

Für die Erteilung von Ausnahmegenehmigungen sollte ein dokumentiertes Verfahren existieren. Es sollte mindestens folgendes dokumentiert werden:

- Begründung, warum eine Abweichung von den Sicherheitsvorgaben erforderlich ist und welche Regelung betroffen ist,
- Beschreibung der Ausgestaltung der Ausnahmegenehmigungen sowie Darstellung der Auswirkungen und Abgrenzung des betroffenen Bereichs, inklusive der Risikobewertung,
- Zeitpunkt der Einrichtung,
- Antragsteller und Genehmigender,
- Zeitraum der Befristungen.

Über Abweichungen von den geltenden Sicherheitsvorgaben sind alle betroffenen Mitarbeiter zu informieren.

Prüffragen:

- Gibt es ein Genehmigungs- und Dokumentationsverfahren für Ausnahmegenehmigungen?
- Gibt es eine Übersicht über alle erteilten Ausnahmegenehmigungen?
- Sind alle Ausnahmen nachvollziehbar begründet?
- Werden die möglichen Konsequenzen von Ausnahmen analysiert und wurde das ermittelte Risiko als tragbar eingestuft?
- Ist sichergestellt, dass alle Ausnahmegenehmigungen aufgehoben werden, sobald sie nicht mehr erforderlich sind?

# M 2.381 Festlegung einer Strategie für die WLAN-Nutzung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Bevor in einer Organisation WLANs eingesetzt werden, muss festgelegt sein, welche generelle Strategie die Organisation im Hinblick auf die WLAN-Nutzung einnimmt. Insbesondere ist hierfür zu klären, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen hierüber kommuniziert werden dürfen. Dabei sollte auch festgelegt werden, in welchen räumlichen Bereichen WLANs aufgebaut werden sollen (sinnvoll kann dies also beispielsweise in Umgebungen sein, in denen sich die Benutzer häufig innerhalb bestimmter Bereiche bewegen) und in welchen Bereichen auf keinen Fall WLANs vorhanden sein dürfen (bis hin zur aktiven Abschirmung).

WLAN-Komponenten können beispielsweise eingesetzt werden, um

- eine Institution, eine einzelne Abteilung oder einen Produktionsbereich flächendeckend mit einem Funknetz zu versorgen,
- den Einsatz von mobilen Komponenten in einzelnen Räumen zu ermöglichen, also z. B. in Besprechungsräumen,
- ein WLAN für die Nutzung durch fremde Teilnehmer kommerziell anzubieten (Hotspots).

Funknetze können mit oder ohne Kopplung an andere Netze aufgebaut werden, was ebenfalls die Gefährdungslage deutlich beeinflusst und damit auch die zu ergreifenden Sicherheitsmaßnahmen. Je nach geplantem Einsatzzweck und Einsatzumgebung können die erforderlichen Sicherheitsmaßnahmen erheblich differieren. Dies muss in jedem Fall bei der Formulierung der Sicherheitsrichtlinien und Regelungen für die WLAN-Nutzung berücksichtigt werden. Die Entscheidung sollte zusammen mit den Entscheidungsgründen dokumentiert werden.

Beim Aufbau eines drahtlosen Netzes ist ein erheblicher Planungsaufwand notwendig, um die für einen professionellen Einsatz erforderliche Stabilität, Übertragungsqualität und Sicherheit zu erreichen (siehe auch M 2.383 *Auswahl eines geeigneten WLAN-Standards* und M 5.140 *Aufbau eines Distribution Systems*).

Die IT-Verantwortlichen sowie das Sicherheitsmanagement einer Institution sollten sich darüber im klaren sein, dass bei drahtlosen Kommunikationssystemen, insbesondere bei WLANs, viele technische Aspekte schnell weiterentwickelt und modifiziert werden. Dies bedeutet für die IT-Verantwortlichen und das Sicherheitsmanagement zum einen, dass für einen sicheren Betrieb von WLANs generell ein höherer Aufwand notwendig ist und zum anderen, dass die Sicherheitsmaßnahmen in kürzeren Abständen als bei anderen Systemen auf ihre Wirksamkeit getestet und an Veränderungen angepasst werden müssen.

Um drahtlose Netze und die damit verbundenen IT-Systeme sicher betreiben zu können, sind die folgenden Punkte wesentlich:

- Die Arbeitsweise und Technik der eingesetzten drahtlosen Kommunikationssysteme müssen von den für den Betrieb Verantwortlichen vollständig verstanden werden.

- Die Sicherheit der eingesetzten Technik sollte regelmäßig evaluiert werden. Ebenso sollten regelmäßig die Sicherheitseinstellungen der benutzten IT-Systeme (z. B. Access Points, Laptops, PDAs) untersucht werden.
- Die WLAN-Nutzung muss in der Sicherheitsrichtlinie der Institution verankert sein, jede Änderung der WLAN-Nutzung muss mit dem Sicherheitsmanagement abgestimmt werden.
- Um die übertragenen Daten auch zuverlässig zu sichern, müssen Vorgaben ausgearbeitet werden, die sich unter anderem mit der Auswahl adäquater Verschlüsselungs- und Authentikationsverfahren, deren Konfiguration und Schlüsselmanagement beschäftigen.
- Es ist zu definieren, welche WLAN-Standards, z. B. IEEE 802.11g, von den WLAN-Komponenten mindestens unterstützt werden sollten, um ein sicheres Zusammenspiel der einzelnen Komponenten zu gewährleisten und die erforderlichen Sicherheitsmechanismen flächendeckend nutzen zu können.

**Nutzung von WLAN-Komponenten**

Viele von Endbenutzern verwendete IT-Systeme wie Laptops oder PDAs enthalten WLAN-Funktionalitäten, die bei der Auslieferung meistens nicht deaktiviert sind. Es sollte sichergestellt sein, dass hierüber keine "wilde" WLAN-Nutzung erfolgt, sondern es muss klar geregelt sein, ob diese WLAN-Funktionalitäten genutzt werden dürfen, und wenn ja, unter welchen Rahmenbedingungen.

Prüffragen:

- Ist festgelegt, für welche Organisationseinheiten, für welche räumlichen Bereich und für welche Anwendungen die WLAN-Nutzung zugelassen ist?
- Ist in der Sicherheitsrichtlinie der Organisation der Einsatz von WLAN geregelt?
- Werden die Sicherheitsanforderungen an die eingesetzten WLANs regelmäßig durch Sicherheitsuntersuchungen überprüft?
- Werden Änderungen in der WLAN-Infrastruktur und/oder den Nutzungsbedingungen mit dem IT-Sicherheitsmanagement abgestimmt?

# M 2.382 Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Für den Einsatz von WLAN-Komponenten in Behörden und Unternehmen müssen geeignete Sicherheitsrichtlinien aufgestellt werden. Diese WLAN-spezifischen Sicherheitsrichtlinien müssen konform zum generellen Sicherheitskonzept und den allgemeinen Sicherheitsrichtlinien der Institution sein. Sie müssen regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Die WLAN-spezifischen Vorgaben können in den vorhandenen Richtlinien ergänzt oder in einer eigenen Richtlinie zusammengefasst werden.

Eine WLAN-Sicherheitsrichtlinie sollte unter anderem folgende Punkte umfassen:

- Es sollte beschrieben sein, wer in der Institution WLAN-Komponenten installieren, konfigurieren und benutzen darf. Dazu sind auch eine Vielzahl von Randbedingungen festzulegen wie z. B.
  - welche Informationen über WLAN-Komponenten weitergegeben werden dürfen,
  - wo die WLAN-Komponenten benutzt und wo Access Points aufgestellt werden dürfen,
  - an welche anderen internen oder externen Netze das WLAN gekoppelt werden darf.
- Für alle WLAN-Komponenten sollten Sicherheitsmaßnahmen und eine Standard-Konfiguration festgelegt werden.
- Bei einem Verdacht auf Sicherheitsprobleme muss ein Sicherheitsverantwortlicher hierüber informiert werden, damit dieser weitere Schritte unternehmen kann (siehe auch B 1.8 *Behandlung von Sicherheitsvorfällen*).
- Administratoren, aber auch Benutzer von WLAN-Komponenten sollten über die Gefährdungen durch WLAN-Komponenten und die zu beachtenden Sicherheitsmaßnahmen informiert bzw. geschult werden.
- Die korrekte Umsetzung der in der WLAN-Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen sollte regelmäßig kontrolliert werden.

**Benutzerrichtlinie für WLAN**

Um Benutzer nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene WLAN-Benutzerrichtlinie zu erstellen. In einer solchen Benutzerrichtlinie sollten dann kurz die Besonderheiten bei der WLAN-Nutzung beschrieben werden, wie z. B.

- an welche anderen internen und externen Netze der WLAN-Client gekoppelt werden darf,
- unter welchen Rahmenbedingungen sie sich an einem internen oder externen WLAN anmelden dürfen,
- ob und wie Hotspots genutzt werden dürfen,
- dass der Ad-hoc-Modus abzuschalten ist, damit kein anderer Client direkt auf den WLAN-Client zugreifen kann,
- welche Schritte bei (vermuteter) Kompromittierung des WLAN-Clients zu unternehmen sind, vor allem, wer zu benachrichtigen ist.

Wichtig ist auch, dass klar beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass

- keine sicherheitsrelevanten Konfigurationen verändert werden dürfen,
- stets ein Virenscanner aktiviert sein muss,
- eine vorhandene Personal Firewall nicht abgeschaltet werden darf (siehe auch M 5.91 *Einsatz von Personal Firewalls für Clients* ),
- dass alle Freigaben von Verzeichnissen oder Diensten deaktiviert oder zumindest durch gute Passwörter geschützt sind,
- für die Nutzung externer WLANs nur spezielle Benutzerkonten mit restriktiver Rechtevergabe verwendet werden sollten.

Außerdem sollte die Benutzerrichtlinie ein klares Verbot enthalten, ungenehmigt Access Points anzuschließen. Des Weiteren sollte die Richtlinie insbesondere im Hinblick auf die Nutzung von klassifizierten Informationen, beispielsweise Verschlusssachen, Angaben dazu enthalten, welche Daten im WLAN genutzt und übertragen werden dürfen und welche nicht. Benutzer sollten für WLAN-Gefährdungen sowie für Inhalte und Auswirkungen der WLAN-Richtlinie sensibilisiert werden.

**Richtlinie für Administratoren eines WLANs**

Daneben sollte eine WLAN-spezifische Richtlinie für Administratoren erstellt werden, die auch als Grundlage für die Schulung der Administratoren dienen kann. Darin sollte festgelegt sein, wer für die Administration der unterschiedlichen WLAN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Administratoren gibt, und wann welche Informationen zwischen den Zuständigen fließen müssen. So ist es durchaus üblich, dass für den Betrieb der aktiven Komponenten (Distribution System und Access Points) eine andere Organisationseinheit zuständig ist als für die Betreuung der WLAN-Clients oder für das Identitäts- und Berechtigungsmanagement.

Die WLAN-Richtlinie für Administratoren sollte des Weiteren die wesentlichen Kernaspekte zum Betrieb einer WLAN-Infrastruktur umfassen, wie z. B.

- Festlegung einer sicheren WLAN-Konfiguration und Definition von sicheren Standard-Konfigurationen
- Nutzung eines WLAN-Management-Systems
- Auswahl und Einrichtung von Kryptoverfahren inklusive Schlüsselmanagement
- Regelmäßige Auswertung von Protokolldateien, zumindest von Access Points
- Durchführung von WLAN-Messungen: Die Konfiguration und die Netzabdeckung von Access Points und Clients sollte regelmäßig mittels WLAN-Analysator und Netz-Sniffer kontrolliert werden. Hierbei sollte insbesondere auch nach nicht genehmigten WLAN-Clients und Access Points innerhalb der Organisationsgrenzen gesucht werden.
- Inbetriebnahme von Ersatzsystemen
- Maßnahmen bei Kompromittierung des WLANs

Auch wenn innerhalb einer Institution keine WLANs offiziell installiert sind, sollte trotzdem regelmäßig vom Sicherheitsmanagement veranlasst werden, dass nach ungenehmigt installierten WLAN-Komponenten gescannt wird.

Alle WLAN-Anwender, egal ob Benutzer oder Administratoren, sollten mit ihrer Unterschrift bestätigen, dass sie den Inhalt der WLAN-Sicherheitsrichtlinie gelesen haben und die darin definierten Anweisungen auch einhalten. Ohne diese schriftliche Bestätigung sollte niemand das WLANs nutzen dürfen. Die

unterschriebenen Erklärungen sind an einem geeigneten Ort, beispielsweise in der Personalakte, aufzubewahren.

Prüffragen:

- Ist festgelegt, an welchen internen oder externen Netzen das WLAN gekoppelt werden darf?
- Ist ein Prozess mit Handlungsanweisungen bei Sicherheitsproblemen im WLAN-Bereich definiert?
- Sind Administratoren und Benutzer über die Sicherheitsrisiken und die zu beachtenden Sicherheitsmaßnahmen im Bereich WLAN informiert?
- Ist festgelegt, wer für die Administration der WLAN-Komponenten zuständig ist?
- Erfolgt eine regelmäßige Auswertung der Protokolldateien?
- Erfolgt eine regelmäßige Prüfung auf unautorisierte WLAN-Komponenten?
- Wird die Kenntnisnahme von Anweisungen und Belehrungen durch die WLAN-Benutzer schriftlich bestätigt?
- Existiert eine Benutzerrichtlinie zur Zugriffsregelung auf Hotspots?
- Liegt eine Sicherheitsrichtlinie für den Einsatz von WLAN vor?

# M 2.383 Auswahl eines geeigneten WLAN-Standards

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Im Rahmen der WLAN-Planung ist zunächst eine Ist-Aufnahme durchzuführen, welche der von der Institution betriebenen Systeme in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen. Nachdem diese Ist-Aufnahme abgeschlossen wurde, kann daraus ermittelt werden, welcher WLAN-Standard genutzt werden kann. Dabei verwenden die WLAN-Standards IEEE 802.11, IEEE 802.11b und IEEE 802.11g das 2,4 GHz-Band, die Standards IEEE 802.11a und IEEE 802.11h das 5 GHz-Band. Durch die Auswahl des richtigen Frequenzbandes können Störungen des WLANs durch andere von der Institution betriebene Systeme vermieden werden. Nur in den Standards IEEE 802.11 und IEEE 802.11i sind Sicherheitsmechanismen beschrieben.

Neben dieser technischen Betrachtung müssen außerdem die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards gegeneinander abgewogen werden. Generell sollten zur Authentisierung und Verschlüsselung nur als allgemein sicher anerkannte Verfahren eingesetzt werden. Hierbei ist die Verwendung anerkannter kryptografischer Verfahren mit ausreichender Schlüssellänge sowie kollisionsfreier Hash-Verfahren sicherzustellen (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Bei Verwendung von WPA oder WPA2 wird die Nutzung von Authentisierungsverfahren mit gegenseitiger Authentisierung empfohlen. Hierbei muss sich der WLAN-Client gegenüber dem Access Point authentisieren und umgekehrt. Hierfür kann entweder ein geheimer Text, der sogenannte Pre-Shared Key, oder das EAP-Framework mit einem RADIUS-Server zur Authentisierung verwendet werden. Bei hohem Schutzbedarf empfiehlt sich die Nutzung von Geräte- und Benutzer-Authentisierung, sodass nur der Institution bekannte (und entsprechend der Sicherheitsrichtlinien konfigurierte) Clients im WLAN zugelassen werden.

So verwendet der Standard IEEE 802.11 das als unsicher eingestufte Wired Equivalent Privacy (WEP) mit statischen Schlüsseln. WLANs, in denen WEP zum Einsatz kommt, sollten somit nicht ohne zusätzliche Sicherheitsmaßnahmen in Bereichen eingesetzt werden, in denen vertrauliche Informationen übertragen werden sollen. Hier ist mindestens das von der Wi-Fi Alliance veröffentlichte Wi-Fi Protected Access (WPA) zu wählen. Besser ist die Ergänzung IEEE 802.11i bzw. WPA2 zur Sicherung der WLAN-Kommunikation. Hier wird unter anderem die Verwendung von Pre-Shared Keys mit dem Temporal Key Integrity Protocol (TKIP) zur sicheren Kommunikation im WLAN definiert. IEEE 802.11i selbst schreibt das Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) als zukunftsgerichtetes Verfahren der Authentisierung vor, das durch das Counter Mode Verfahren auch zusätzliche Vertraulichkeit gewährleistet. Ebenso verwendet CCMP den Advanced Encryption Standard (AES) zur Verschlüsselung der Informationen, im Gegensatz zu RC4 in WEP und WPA.

Eine sorgfältige Betrachtung der einzelnen WLAN-Standards, vor allem im Hinblick auf deren Sicherheitsfunktionen, ist unumgänglich und immer durchzuführen. Erst nach einer ausführlichen Bewertung der einzelnen Standards kann eine Festlegung auf einen bestimmten WLAN-Standard erfolgen. Die

Entscheidungsgründe müssen dokumentiert werden, damit sie später noch nachvollziehbar sind.

Prüffragen:

- Ist der zu verwendende WLAN-Standard innerhalb der Organisation festgelegt?

# M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Um einen sicheren Betrieb eines WLANs zu gewährleisten, ist es notwendig, die Kommunikation über die Luftschnittstelle komplett abzusichern. Ohne ausreichende Verschlüsselung besteht die Gefahr, dass unberechtigte Personen über das WLAN übertragene Daten mitlesen können. Ebenso bietet ein nicht ausreichend geschütztes WLAN einen Angriffspunkt auf ein eventuell damit verbundenes LAN. Darüber hinaus ist die Integrität der Daten sicherzustellen, damit Manipulationen an diesen Daten erkannt werden. Ebenso ist eine (gegenseitige) Authentisierung der WLAN-Komponenten untereinander wichtig.

In den WLAN-Standards IEEE 802.11 und 802.11i sind diverse Kryptoverfahren beschrieben, die zur Absicherung eines WLANs verwendet werden können. Diese sind je nach Einsatzgebiet, Schutzbedarf und Größe der Institution auszuwählen und anzuwenden.

### Wired Equivalent Privacy (WEP)

WEP ist der älteste und am weitesten verbreitete Verschlüsselungsstandard für WLANs und ist im Standard IEEE 802.11 beschrieben. WEP bietet nur das absolute Minimum an Schutz, um zufälliges Mitlesen oder zufälliges Einbuchen zu verhindern.

WEP gilt mittlerweile als veraltet und unsicher, da eine Vielzahl von Sicherheitslücken nachgewiesen wurden. WEP ist daher für die Absicherung von WLANs als ungenügend einzustufen und sollte nicht mehr eingesetzt werden.

Falls keinerlei anderen Kryptoverfahren außer WEP zur Verfügung stehen und die WLAN-Komponenten weiter betrieben werden sollen, sollte WEP aktiviert werden. Dann muss die maximale Schlüssellänge gewählt werden und die Schlüssel regelmäßig manuell gewechselt werden (mindestens einmal täglich). Eine solche Entscheidung ist zu dokumentieren und allen Benutzern des WLAN mitzuteilen. Ein solches ungenügend abgesichertes WLAN darf höchstens in einem unkritischen Bereich eingesetzt werden, beispielsweise zum reinen Zugriff auf das Internet. Es ist aber sicher zu stellen, dass über ein WLAN, dass nur durch WEP abgesichert wurde, keine sensiblen Daten übertragen werden oder über die beteiligten WLAN-Komponenten erreichbar sind.

### WPA, WPA2 und IEEE 802.11i

IEEE 802.11i gilt als neuer Sicherheitsstandard für WLANs, das in Teilen auch dem Wi-Fi Protected Access 2 (WPA2) der Wi-Fi Alliance entspricht. Im Gegensatz zu WPA, das dem Draft 3.0 von IEEE 802.11i entspricht und ebenfalls von der Wi-Fi Alliance veröffentlicht wurde, wird in WPA2 und IEEE 802.11i der Advanced Encryption Standard (AES) als Verschlüsselungsalgorithmus verwendet. In WPA, genauso wie in WEP, kommt weiterhin RC4 zum Einsatz. Sowohl WPA als auch WPA2 bzw. IEEE 802.11i bieten mit dem optional anzuwendenden Temporary Key Integrity Protocol (TKIP) durch eine dynamische Schlüsselgenerierung zusätzlichen Schutz.

Bei WPA2 und IEEE 802.11i ist darüber hinaus die Verwendung von CCMP als Implementierungsmethode für AES zur Integritätssicherung zwingend vorgeschrieben.

Nach Möglichkeit sollte ein WLAN flächendeckend einheitlich mit WPA2 unter Verwendung von CCMP (zumindest WPA mit TKIP) abgesichert werden, da hier stärkere Algorithmen zur Verschlüsselung und Integritätssicherung verwendet werden. Schwächere Verfahren sind nach dem Stand der Technik inakzeptabel.

Für die Authentisierung von Benutzern können Pre-Shared Keys (PSK) verwendet werden. Diese werden beim ersten Verbindungsaufbau zur Authentisierung gegenüber einer anderen WLAN-Komponente verwendet. Bei den Pre-Shared Keys sollte darauf geachtet werden, dass diese wesentlich länger sein sollten, als die üblichen sechs bis acht Zeichen, da davon die Sicherheit der Verschlüsselung abhängt. Dieses Verfahren ist allerdings nur für kleinere WLAN-Installationen praktikabel, für große WLANs sollte eine EAP-Methode nach IEEE 802.1X verwendet werden.

Zum besseren Überblick über die verschiedenen Sicherheitsmechanismen dient folgende Tabelle:

| | **WEP** | **WPA** | **802.11i (WPA2)** |
|---|---|---|---|
| Verschlüsselungs-Algorithmus | RC4 | RC4 | AES |
| Schlüssellänge | 40 bzw. 104 Bit | 128 Bit (64 Bit bei der Authentisierung) | 128 Bit |
| Schlüssel | statisch | dynamisch (PSK) | dynamisch (PMK) |
| Initialisierungsvektor | 24 Bit | 48 Bit | 48 Bit |
| Datenintegrität | CRC-32 | MICHAEL | CCMP |

**TKIP und CCMP**

Das Temporary Key Integrity Protocol (TKIP) basiert als abwärtskompatible Lösung auf WEP, es beseitigt jedoch dessen gröbsten Schwächen. Für TKIP ist in IEEE 802.11i das Problem der mangelhaften Integritätsprüfung in WEP durch den Einsatz des zusätzlichen Verfahrens MICHAEL (zum Message Integrity Check) gelöst worden. TKIP und MICHAEL sind als temporäre Lösung zu verstehen.

CCMP steht für CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code). Hierbei wird nicht direkt der Klartext mit AES verschlüsselt, sondern ein aus dem symmetrischen Schlüssel gebildeter Zähler. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartexts mit dem AES-verschlüsselten Zähler. Außerdem wird die Methode Cipher Block Chaining (CBC) zur Integritätssicherung der Daten verwendet.

Zur Schlüsselverwaltung und -verteilung wird wieder IEEE 802.1X vorausgesetzt. Die in IEEE 802.11i verwendete Schlüssellänge beträgt 128 Bit.

**Extensible Authentication Protocol (EAP)**

Als zusätzlicher Schutz der Authentisierung kann das Extensible Authentication Protocol (EAP) gemäß Standard IEEE 802.1X verwendet werden. EAP wird im RFC 3748 genau beschrieben. Der Benutzer meldet sich hier bei einer Authentisierungsinstanz, z. B. an einem RADIUS-Server, an und dieser prüft die Zugangsberechtigung, bevor der Sitzungsschlüssel ausgehandelt wird. EAP unterstützt eine Reihe von Authentisierungsmethoden, so dass auch Zertifikate und Zwei-Faktor-Authentisierungen genutzt werden können.

EAP-Methoden, die in einem WLAN verwendet werden können sind z. B.:

- EAP-TLS
  Bei EAP-TLS, definiert in RFC 2716, wird eine beidseitige Authentisierung anhand von X.509-Zertifikaten durchgeführt. Dazu muss der zu authentisierende Partner beweisen, dass er den privaten Schlüssel kennt, der zu dem öffentlichen Schlüssel gehört, welcher seinem Kommunikationspartner bekannt ist. Folglich müssen Verfahren etabliert werden, die entsprechende Zertifikate verteilen und verwalten können. Eine solche Public Key Infrastructure (PKI) einzurichten und zu betreiben setzt eine sorgfältige Planung voraus (siehe z. B. M 2.232 *Planung der Windows-CA-Struktur ab Windows 2000*). Der Schlüsselaustausch selbst findet über einen durch TLS gesicherten Tunnel statt.
- EAP-TTLS
  Bei EAP-TTLS wird im Gegensatz zu EAP-TLS auf darauf verzichtet, dass der WLAN-Client ein eigenes Zertifikat besitzen muss. Nur der Server benötigt bei EAP-TTLS ein gültiges Zertifikat. Über den durch TLS gesicherten Tunnel können dann andere, eventuell weniger sichere Verfahren zur Client- bzw. Benutzerauthentisierung benutzt werden. EAP-TTLS ist ebenso wie EAP-TLS ein schlüsselerzeugendes Verfahren, d. h. bei der Kommunikation wird jedes Mal ein neuer Session Key erzeugt, der dann für die Absicherung des Tunnels mittels TLS verwendet wird.
- EAP-PEAP
  Auch EAP-PEAP ist ein schlüsselerzeugendes Verfahren und erfordert, ähnlich wie EAP-TTLS, nur bei dem Authentisierungsserver ein gültiges X.509-Zertifikat. Im Gegensatz zu EAP-TTLS sind zur Client-Authentisierung im gesicherten Tunnel nur andere EAP-Methoden möglich, wie z. B. EAP-MSCHAPv2 oder EAP-TLS. Dabei ist die Kombination mit EAP-MSCHAPv2 für Netze interessant, die hauptsächlich Windows 2000 oder Windows XP als Client-Betriebssystem einsetzen, die diese Methode hier bereits fest enthalten ist.

Weitere EAP-Methoden sind im Standard IEEE 802.1X oder in der Technischen Richtlinie *Sicheres WLAN* des BSI beschrieben.

Generell ist es in größeren Installationen sinnvoll, zur Benutzerauthentisierung EAP gemäß IEEE 802.1X zu verwenden.

Aktuelle WLAN-Komponenten unterstützen IEEE 802.11i und damit WPA2 bereits. Bei der Beschaffung neuer WLAN-Komponenten ist auf jeden Fall vorher zu prüfen, ob diese auch entsprechende EAP-Methoden unterstützen.

**Schlüsselmanagement**

Die kryptographischen Schlüssel zum Schutz der Kommunikation oder zur Authentisierung müssen regelmäßig gewechselt werden (siehe M 2.388 *Geeignetes WLAN-Schlüsselmanagement*).

Bei allen WLAN-Komponenten muss darauf geachtet werden, dass diese beim Verbindungsaufbau mit anderen WLAN-Komponenten keine Kryptoverfahren mit geringerer Schutzwirkung als die ausgewählten akzeptieren. Verbindungen mit solchen Komponenten müssen abgelehnt werden.

Prüffragen:

- Wurde ein ausreichender Verschlüsselungsstandard implementiert?
- Einsatz von WEP: Entspricht die Güte der eingesetzten Passwörter dem Stand der Technik?
- Einsatz von WEP: Werden die verwendeten Passwörter/Schlüssel regelmäßig (mindestens einmal täglich) gewechselt?
- Einsatz von WEP: Ist die Entscheidung zum Einsatz von WEP dokumentiert?
- Einsatz von WEP: Erfolgt die Nutzung ausschließlich in unkritischen Bereichen?
- Einsatz von WEP: Ist sichergestellt, dass keine sensiblen Daten übertragen werden?
- Existiert eine Regelung zur Nutzung von Algorithmen und Verfahren die dem Stand der Technik entsprechen?
- Einsatz von Pre-Shared-Keys (PSK): Entspricht die Güte der eingesetzten Passwörter/Schlüssel dem Stand der Technik?
- Werden zur zusätzlichen Absicherung des WLANs EAP-Verfahren eingesetzt?

# M 2.385 Geeignete Auswahl von WLAN-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Zur Auswahl von WLAN-Geräten ist zunächst zu hinterfragen, ob diese in die WLAN-Sicherheitsstrategie hineinpassen. WLAN-Komponenten gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihrem Leistungsumfang, sondern auch in den Sicherheitsmechanismen und im Bedienkomfort. Zudem stellen sie unterschiedliche Voraussetzungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener WLAN-Komponenten sind Kompatibilitäts-probleme naheliegend. Wichtige Kriterien für die Auswahl von WLAN-Komponenten sind daher Sicherheit und Kompatibilität.

Wenn beschlossen wurde, innerhalb einer Institution ein WLAN aufzubauen, sollte eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung sollten dann die zu beschaffenden Produkten ausgewählt werden. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, mehrere Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden. Ein wichtiges Kriterium bei der Beschaffung von WLAN-Komponenten ist die Kompatibilität zu bereits vorhandenen Geräten.

Bei der Beschaffung sollte auch Datendurchsatz und Reichweite hinterfragt werden. Mit externen Antennen kann bei WLAN-Komponenten zusätzlich die Reichweite verbessert werden. Allerdings ist hier sicherzustellen, dass durch die größere Reichweite ein WLAN nicht in Bereiche abstrahlt, in denen es nicht genutzt werden soll oder darf.

Bei der Beschaffung von Access Points sollte unter anderem überprüft werden,

- wie viele Kanäle einstellbar sind,
- ob die SSID einstellbar ist,
- ob der SSID-Beacon deaktivierbar ist,
- welche kryptographischen Verfahren implementiert sind (WEP, WPA, WPA2 und weitere),
- ob bei der Authentisierung sowohl der Open System als auch der Shared Key Modus vorgegeben werden kann (letzteres ist leider nicht selbstverständlich),
- inwiefern EAP-Methoden nach IEEE 802.1X unterstützt werden,
- ob eine Administration über sichere Kommunikationswege, z. B. SSH oder SSL, möglich ist und unsichere Protokolle, wie z. B. HTTP oder Telnet, abgeschaltet werden können,
- ob eine IP- bzw. MAC-Adressfilterung möglich ist,
- ob ACLs für die Zugriffe über das WLAN, ein angeschlossenes LAN oder zur Konfiguration der Access Points eingerichtet werden können,
- ob ein Paketfilter integriert ist,
- ob weitere Mechanismen zur Zugriffssteuerung vorhanden sind (Filterung nach verschiedenen Kriterien wie Ports, Applikationen, URLs, etc.),
- ob Tunnel-Protokolle wie PPTP oder IPsec unterstützt werden.

Es sollte unbedingt getestet werden, ob die implementierten kryptographischen Verfahren nicht nur gleich benannt sind, wie bei anderen eingesetzten WLAN-Komponenten, sondern auch korrekt zusammenarbeiten.

Die korrekte Konfiguration der Access Points ist ein wesentlicher Sicherheitsaspekt. Bei einigen Access Points ist eine Konfiguration drahtlos direkt über das WLAN möglich, was von den Herstellern als komfortabel angepriesen wird. Dies birgt aber auch Sicherheitsprobleme, daher sollte darauf verzichtet werden, wenn eine solche Funktionalität aber vorhanden ist, sollte sie zumindest abschaltbar sein (und im Betrieb grundsätzlich abgeschaltet sein). Viele Access Points bieten zur bequemen Konfiguration auch die Möglichkeit, diese über eine serielle oder USB-Schnittstelle an eine Managementkonsole anzuschließen. Über HTTP oder Telnet können diese dann über das Intranet oder Internet administriert werden. Hierfür ist eine vernünftige Absicherung des Fernzugriffes notwendig, beispielsweise die Absicherung der Kommunikation über SSL oder SSH. Fernzugriffe über das Internet sollten generell kritisch hinterfragt werden.

Der Administrationszugriff auf WLAN-Komponenten sollte nur autorisierten Personen möglich sein. Daher sollte hinterfragt werden, wie dieser abgesichert ist. Wenn dies über Passwörter erfolgt, müssen diese möglichst komplex gewählt werden (siehe M 2.11 *Regelung des Passwortgebrauchs*). Besser ist es, für Administrationszugriffe starke Authentisierungsmethoden einzusetzen (siehe auch M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*).

Die Umsetzung der erforderlichen Sicherheitsregeln an Access Points ist häufig sehr aufwändig. Dazu gehören neben dem Schlüsselmanagement vor allem die notwendigen Einstellungen von verschiedenen Parametern und Optionen. Für einige Access Points gibt es daher mittlerweile Lösungen, um diese innerhalb einer Institution über einen zentralen Server zu steuern. Leider sind dies bisher noch proprietäre Lösungen und werden nur von den WLAN-Komponenten des jeweiligen Herstellers unterstützt.

Da es vor allem bei Netzkoppelelementen aufwendig sein kann, bis der Netzverwalter die korrekte Konfiguration herausgefunden hat, sollte es möglich sein, diese zu speichern.

Die Online-Hilfe und Dokumentation von WLAN-Komponenten sollten sprachlich so formuliert sein, dass zukünftige Benutzer bzw. Administratoren die technischen Beschreibungen nachvollziehen können.

**Zusammenwirken mit der zugehörigen Infrastruktur**

Im Rahmen der Beschaffung sollten auch das korrekte Zusammenwirken aller WLAN-Komponenten mit der zugehörigen Infrastruktur geprüft werden. Hierzu zählen beispielsweise:

- Die im WLAN genutzte Authentisierungsmethode muss sowohl von den Clients und den Access Points, als auch vom Authentisierungsserver unterstützt werden.
- Falls im WLAN die Authentisierung nach IEEE 802.1X erfolgt, müssen die Access Points die Authentisierungsmethode EAP unterstützen und die mitgeteilten Informationen innerhalb von IEEE 802.1X korrekt verarbeiten.
- Es ist zu prüfen, ob der Authentisierungsserver auf eine eigene Datenbank zur Benutzer-Authentisierung verzichten kann und stattdessen die Authentisierungsanfragen an eine zentrale Benutzerdatenbank mittels sicherer Abfragemethoden durchreichen kann.

Bei der Beschaffung einer größeren WLAN-Installation sind vor der endgültigen Beschaffung entsprechende Teststellungen durchzuführen. Mit Hilfe eines Prüfkatalogs kann die Erfüllung der technischen Anforderungen evaluiert werden. Diese Prüfungen erleichtern eine spätere Durchführung der WLAN-Installation und deren Abnahme.

Prüffragen:

- Wurde bei der Auswahl der WLAN-Geräte darauf geachtet, dass diese in die WLAN-Sicherheitsstrategie hineinpassen und kompatibel zu den Hard- und Software-Komponenten im Einsatzumfeld sind?
- Wurde eine Anforderungsliste für die WLAN-Komponenten erstellt?
- Wurde beim Einsatz von WLAN mit großer Reichweite darauf geachtet, dass nicht in Bereiche abgestrahlt wird, in denen es nicht genutzt werden soll oder darf?
- Wird beim beim Einsatz von kryptografischen Verfahren darauf geachtet, dass diese in der Organisation gleich benannt sind und korrekt zusammenarbeiten?
- Wenn die Konfiguration eines Access Points drahtlos direkt über das WLAN möglich ist, ist diese Konfiguration abschaltbar und im Betrieb grundsätzlich ausgeschaltet?
- Ist sichergestellt, dass der Administrationszugriff auf WLAN-Komponenten nur autorisierten Personen möglich ist und die Anmeldung nur mit möglichst komplexen Passwörtern erfolgt?
- Ist die korrekte Konfiguration der Netzkoppelelemente gespeichert und gesichert?
- Ist die Online-Hilfe und Dokumentation der WLAN-Komponenten leicht nachvollziehbar?
- Werden vor der endgültigen Beschaffung von WLAN-Komponenten Teststellungen durchgeführt und ein Prüfkatalog zur Prüfung der Erfüllung der technischen Anforderungen erstellt?

# M 2.386 Sorgfältige Planung notwendiger WLAN-Migrationsschritte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auf Grund der Schnelllebigkeit der WLAN-Technologie wird sich in der Praxis eine Migration einer bestehenden Installation hin zu neuen Protokollen, Techniken oder Produkten nur selten vermeiden lassen. Dabei ist generell zwischen zwei Migrationsarten zu unterscheiden:

- Migration der Übertragungstechnik (z. B. von IEEE 802.11g nach IEEE 802.11h)
- Migration der WLAN-Sicherheitsmechanismen (z. B. von WEP zu WPA-PSK oder IEEE 802.11i mit IEEE 802.1X)

Im ersten Fall muss der gesamte Planungsprozess für ein WLAN durchlaufen werden, angefangen bei Risikobewertung, bis hin zur Auswahl geeigneter Sicherheitsmaßnahmen.

Im zweiten Fall müssen vorübergehend gegebenenfalls unterschiedliche Sicherheitssysteme parallel betrieben werden und eine erweiterte Konfiguration der Access Points, des Distribution Systems und des Übergabepunktes zum WLAN durchgeführt werden. Die noch nicht migrierten WLAN-Komponenten oder WLAN-Bereiche sind durch entsprechende technische und organisatorische Festlegungen nötigenfalls auf eine eingeschränkte Nutzung zu reduzieren. So kann beispielsweise der Zugriff von noch nicht migrierten Komponenten auf sensible Daten verboten oder der nicht migrierte WLAN-Bereich durch eine zusätzliche DMZ vom restlichen WLAN und LAN abgesichert werden.

Während eines möglicherweise notwendigen Mischbetriebs zweier Sicherheitsmechanismen, z. B. von WPA-PSK bzw. WPA2-PSK und WEP, sind folgende Punkte zu beachten:

- Der Mischbetrieb sollte so kurz wie möglich dauern.
- Falls WEP und Pre-Shared Keys gleichzeitig verwendet werden, so ist verstärkt darauf zu achten, dass die Schlüsselinformationen häufiger (mindestens täglich) gewechselt werden und nur komplexe Passwörter benutzt werden (siehe M 2.388 *Geeignetes WLAN-Schlüsselmanagement*).
- Access Points müssen es erlauben, beide Mechanismen während der Migrationsphase simultan zu betreiben. Access Points, die maximal WEP unterstützen, sind so schnell wie möglich zu ersetzen und aus dem WLAN zu entfernen.
- WLAN-Clients, die lediglich WEP unterstützen (z. B. ein Drucker oder ein PDA) sollten nur eingeschaltet werden, wenn sie benötigt werden. Diese sollten schnellstmöglich durch Clients ersetzt werden, die WPA2 unterstützen.
- Die Konfiguration der WLAN-Komponenten wie einen WLAN-Drucker sollte, sofern möglich, nicht über die Luftschnittstelle erfolgen, sondern über den Konsolen-Port der Komponente.

In jedem Fall sind die einzelnen Migrationsschritte sorgfältig zu planen. Dabei sollte die Migration auch zur Konsolidierung einer gewachsenen WLAN-Infrastruktur genutzt werden und eine Nachschulung der WLAN-Administratoren und WLAN-Benutzer erfolgen. Sofern sich durch die Einführung neuer WLAN-Authentisierungsmechanismen der Anmeldevorgang für die WLAN-Benutzer

ändert, sind die Benutzer ebenfalls nachzuschulen. Des Weiteren sollte die WLAN-Benutzerrichtlinie an die neuen Abläufe angepasst werden.

Prüffragen:

- Wird bei der Migration der Übertragungstechnik der gesamte Planungsprozess für ein WLAN durchlaufen?
- Werden bei einer Migration der WLAN-Sicherheitsmechanismen, die noch nicht migrierten WLAN-Komponenten oder WLAN-Bereiche auf eine eingeschränkte Nutzung reduziert?
- Werden bei einem Mischbetrieb zweier WLAN-Sicherheitsmechanismen entsprechende Maßnahmen ergriffen?
- Wird bei einer Migration eine Konsolidierung der gewachsenen WLAN-Infrastruktur und eine Nachschulung der WLAN-Administratoren und Benutzer durchgeführt?
- Wird die WLAN-Benutzerrichtlinie bei einer migration an die neuen Abläufe angepasst?

# M 2.387 Installation, Konfiguration und Betreuung eines WLANs durch Dritte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Wenn ein WLAN durch einen externen Auftragnehmer installiert, konfiguriert oder betreut werden soll, so sind bei einem WLAN, neben den Empfehlungen in Baustein B 1.11 *Outsourcing*, die im Folgenden beschriebenen Punkte zu beachten:

- Es ist stets zu prüfen, ob eine WLAN-Installation nicht selbst durchgeführt werden kann oder ob dies auch durch die eigenen Mitarbeiter geleistet werden kann. Eine Machbarkeits- und eine Kostenprüfung sollte hierfür durchgeführt werden.
- Die Sicherheitsstrategie und auch die Sicherheitsrichtlinie sollte stets selbst erstellt werden und nicht durch Dritte. Dadurch wird verhindert, dass sich in der Institution niemand mehr ausführlich mit den Sicherheitsaspekten von WLANs auseinandersetzt und somit eventuell notwendige Sicherheitsmaßnahmen vergessen werden. Beratungen und Hilfestellungen durch Dritte in Anspruch zu nehmen ist aber dann sinnvoll, wenn keine internen Ressourcen dafür vorhanden sind.
- Bei der Vergabe einer WLAN-Installation ist ein detailliertes Pflichtenheft zu erstellen. Darin sind alle Mindestanforderungen an die WLAN-Komponenten und alle mit dem WLAN verbundenen Netzteile usw. genau zu definieren. Das Pflichtenheft sollte vertragliche Grundlage bei der Vergabe an einen externen Auftragnehmer sein und später als Prüfgrundlage bei der Abnahme dienen.
- Dem Auftragnehmer ist die Sicherheitsstrategie und die Sicherheitsrichtlinie für den Einsatz eines WLANs vorzulegen. Er muss vertraglich dazu verpflichtet werden, diese einzuhalten und umzusetzen. Dies ist bei der Umsetzung der vertraglich vereinbarten Leistungen regelmäßig zu überprüfen, um frühzeitig eventuelle Probleme zu erkennen. Die Sicherheitsstrategie und die Sicherheitsrichtlinie sollten fester Bestandteil des Pflichtenheftes sein.
- Der Auftragnehmer sollte weitreichende und am besten langjährige Erfahrungen im Aufbau und in der Absicherung eines WLANs haben. Entsprechende Referenzen sind vorzulegen und zumindest stichprobenweise zu prüfen.
- Der Auftragnehmer muss vertraglich dazu verpflichtet werden, die Konfiguration des WLANs und der WLAN-Komponenten, sowie Passwörter, Verbindungsschlüssel und Zugangskennungen und -mechanismen nicht an unbefugte Personen weiterzugeben. Ebenso sollte der Auftragnehmer dazu verpflichtet werden, die durch die Arbeit am übrigen Netz eventuell bekannt gewordenen Informationen und Daten nicht zwischenzuspeichern oder an unbefugte Personen weiterzugeben.
- Vor der Installation eines WLANs durch den Auftragnehmer sind entsprechende Teststellungen durchzuführen. Dabei sollten alle geplanten Sicherheitseinstellungen ausführlich getestet werden. In dieser Phase ist ein eventuell an das WLAN angeschlossene LAN besonders gefährdet und es sollte eine entsprechende Absicherung erfolgen.
- Während der Installation eines WLANs durch den Auftragnehmer sollte darauf geachtet werden, dass keine Hintertüren in das WLAN durch den Auftragnehmer eingebaut werden. Alle Einstellungen und Konfigurationen

sind durch den Auftragnehmer genau zu dokumentieren und mit Abschluss der Installation an den Auftraggeber vollständig zu übergeben.
- Nach Abschluss der Installation sollte anhand des Leistungsverzeichnisses eine Abnahme durchgeführt werden. Darüber hinaus können die im Pflichtenheft nach der Vergabe erstellten Ausführungsunterlagen als Prüfungsgrundlage dienen, da hierin beispielsweise Verfahren für Abnahmemessungen spezifiziert sein können.
- Die Abnahme der WLAN-Installation sollte mit Hilfe eines unabhängigen Experten erfolgen, um auch die technischen Details genau überprüfen zu lassen.
- Sofern auch ein Wireless IDS beschafft wurde, müssen entsprechende Testszenarien, die im Vorfeld der Ausschreibung festgelegt wurden, durchgeführt werden. Hier bietet es sich an, das WLAN zunächst in einem Probebetrieb zu fahren. Dabei sollte auch verifiziert werden, ob der gesamte Überwachungsbereich auch über die WLAN-Sensoren erfasst wird. Des Weiteren sollten verschiedene Störfälle simuliert werden.
- Als wesentlicher Schwerpunkt sollte bei der Abnahme zudem die Dokumentation auf Vollständigkeit und eventuelle Inkonsistenzen geprüft werden.
- Sollte das WLAN auch nach der Installation durch einen externen Auftragnehmer betreut werden, so muss der Auftragnehmer auch hier vertraglich verpflichtet werden, alle hierbei bekannt gewordenen Informationen, wie Passwörter, sensible Daten, Konfigurationseinstellungen usw., nicht an unbefugte Personen weiterzugeben. Ebenso sollte ein Notfallvorsorgeplan mit dem Auftragnehmer erstellt werden. Hierbei sollte für jedes möglicherweise im WLAN auftretende Problem der Schweregrad, die Reaktionszeit, die jeweiligen Arbeitsschritte und wer im Notfall informiert werden muss genau definiert werden.

Prüffragen:

- Ist dem Auftragnehmer die Sicherheitsstrategie und die Sicherheitsrichtlinie für den WLAN-Einsatz vorgelegt worden?
- Wurde mit dem Auftragnehmer ein Notfallvorsorgeplan für Probleme im WLAN erstellt?

# M 2.388 Geeignetes WLAN-Schlüsselmanagement

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Verwendung kryptographischer Sicherheitsmechanismen setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus (siehe auch M 2.46 *Geeignetes Schlüsselmanagement*). Bei der Verwendung von WEP bzw. WPA-PSK oder WPA2-PSK hängt die Sicherheit des WLANs wesentlich davon ab, dass die verwendeten WLAN-Schlüssel geeignet ausgewählt und nicht kompromittiert wurden. Daher muss ein geeignetes Verfahren zum Schlüsselmanagement ausgewählt werden, passend zu den vorhandenen Kryptomechanismen. Hierbei muss zunächst unterschieden werden zwischen statischem (manuellen) und dynamischem Schlüsselmanagement.

**WEP**

Bei WEP wird nur ein einziger, statischer Schlüssel verwendet, d. h. in jeder WLAN-Komponente in einem Netz muss derselbe WEP-Schlüssel eingetragen sein. Weiterhin sieht WEP kein dynamisches Schlüsselmanagement vor, so dass die Schlüssel manuell administriert werden müssen. Da WEP-Schlüssel in kürzester Zeit kompromittiert werden können, sollte WEP nicht mehr eingesetzt werden. Falls es aus irgendwelchen Gründen doch eingesetzt wird, müssen die Schlüssel regelmäßig manuell gewechselt werden (mindestens einmal täglich).

**WPA / WPA2 mit TKIP oder CCMP**

Bei WPA wird TKIP eingesetzt, das die Nutzung dynamischer kryptographischer Schlüssel statt ausschließlich statischer bei WEP erlaubt. Bei IEEE 802.11i (WPA2) kommt CCMP als kryptographisches Verfahren zur Integritätssicherung und zur Verschlüsselung der Nutzdaten hinzu.

TKIP und CCMP sind symmetrische Verfahren, alle Kommunikationspartner müssen daher einen gemeinsamen Schlüssel konfiguriert haben. Dieser Schlüssel wird als Pairwise Master Key (PMK) bezeichnet. Der Pairwise Master Key (PMK) kann über zwei verschiedene Wege auf die beteiligten WLAN-Komponenten gelangen:

- **Statische Schlüssel:** Der PMK kann (analog zu WEP) manuell als ein statischer Schlüssel, als Pre-Shared Key (PSK) bezeichnet, auf Access Points und Clients konfiguriert werden. Es besteht meist die Möglichkeit den gemeinsamen geheimen Schlüssel auch über Passwörter festzulegen. Diese Passwörter werden über Hash-Funktionen in den PMK umgerechnet. Hat ein solcher PSK eine zu geringe Komplexität (im Sinne der Länge des Schlüssels und der Zufälligkeit der Zeichen), ist er anfällig gegenüber Wörterbuch- bzw. Dictionary-Attacken. Daher sollten diese Passwörter eine hohe Komplexität und eine Länge von mindestens 20 Stellen besitzen. Ab einer gewissen Größe eines WLANs ist das Ausrollen eines neuen Schlüssels mit erheblichen Problemen verbunden.
  Die Nutzung der PSK ist in der Kombination mit WPA bzw. WPA2 möglich. Sollte WPA-PSK bzw. WPA2-PSK verwendet werden, ist zu empfehlen, die Schlüssel zum Schutz der Kommunikation oder zur Authentisierung mindestens alle drei bis sechs Monate zu wechseln.

- **Dynamische Schlüssel:** Eine höhere Sicherheit bietet ein Mechanismus zur dynamischen Schlüsselverwaltung und -verteilung, der dafür sorgt, dass regelmäßig und insbesondere nach einer erfolgreichen Authentifizierung des WLAN-Clients am Access Point ein neuer Schlüssel (PMK) bereitgestellt wird. Für diese Schlüsselverwaltung und -verteilung greift IEEE 802.11i auf einen anderen Standard zurück und zwar auf IEEE 802.1X. Dieser Standard ist zur portbasierten Netzzugangskontrolle in kabelbasierten Netzen entworfen worden. Grundsätzliche Idee in IEEE 802.1X ist, dass die Freischaltung eines Netzports erst dann erfolgt, wenn der Nutzer sich erfolgreich dem Netz gegenüber authentisiert hat. Die Authentisierung erfolgt also auf Schicht 2. Damit so etwas überhaupt funktioniert, spezifiziert IEEE 802.1X eine Schnittstelle zwischen Client, Netzelement und einem Authentisierungssystem. Diese Schnittstelle basiert auf dem Extensible Authentication Protocol (EAP) und einer Adaptierung dieses Protokolls für die Übertragung auf Layer 2 in LAN (als EAP over LAN, EAPOL bezeichnet). Hand in Hand geht damit die Festlegung einer Funktion zur Schlüsselverwaltung und -verteilung.

Generell sollten in regelmäßigen Abständen, mindestens jedoch vierteljährlich, die Schlüsselinformationen bei allen WLAN-Komponenten ausgetauscht werden. Bei größeren Installationen sollte hierfür eine geeignete Funktion in der zentralen WLAN-Management-Lösung enthalten sein, um den Arbeitsaufwand gering zu halten.

Der Wechsel der Schlüsselinformationen an allen WLAN-Komponenten sollte bereits während der Planungsphase genau getestet werden, um dadurch eventuell auftretende Schwierigkeiten zu erkennen.

Prüffragen:

- Werden die Passwörter/Schlüssel aller WLAN-Komponenten in regelmäßigen Abständen (mindestens vierteljährlich) gewechselt?
- Wird der Wechsel der Passwörter/Schlüssel an den WLAN-Komponenten im Vorfeld getestet?
- Existiert zur Minimierung des Arbeitsaufwandes und zur besseren Nachvollziehbarkeit eine zentrale Lösung für das WLAN-Management?

# M 2.389 Sichere Nutzung von Hotspots

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Bei Hotspots handelt es sich um einen räumlich begrenzten Funkbereich, der auf einen Raum, eine Halle oder eine Produktionsstätte begrenzt sein kann. Meistens werden Hotspots explizit für die Nutzung durch fremde Teilnehmer aufgebaut. Ihr Hauptzweck ist üblicherweise der drahtlose Zugang zum Internet. Häufig findet man solche Hotspots in Hotels, Flughäfen, Messehallen, Bahnhöfen und Kongresszentren.

Hotspots sollten immer als unsicheres Netz betrachtet werden, zum einem, da das dort vorhandene Sicherheitsniveau von außen nur schwer einzuschätzen ist und zum anderen, da die meisten Hotspots ihre Dienste in Form von Shared-Networks anbieten. Dadurch kann im Allgemeinen der Zugriff von jedem Endgerät auf jedes andere teilnehmenden Endgerät möglich sein. Ist das Risiko, das bei der Nutzung eines Hotspots entsteht, generell nicht abschätzbar, so ist es auch möglich, die Nutzung von Hotspots durch die WLAN-Sicherheitsrichtlinie vollständig zu verbieten. Dann ist aber auch technisch sicherzustellen, dass ein WLAN-Client nicht auf einen solchen Hotspot zugreifen kann.

Die Betreiber von Hotspots können viel für die Sicherheit der von ihnen angebotenen Funkstrecke und anderen Dienstleistungen tun (siehe M 4.293 *Sicherer Betrieb von Hotspots*), ohne Mitarbeit der Benutzer ist eine vernünftige Absicherung allerdings nicht zu erreichen. Hierzu gehören unter anderem folgende Maßnahmen:

- Die Benutzer sollten nachfragen, welche Sicherheitsvorkehrungen am Hotspot getroffen worden sind, um dessen Sicherheitsniveau und die Vertrauenswürdigkeit des Betreibers einschätzen zu können.
- Vor der Benutzung sollten sie sich nach der Preisgestaltung und der Art der Abrechnung erkundigen. Aus Sicht der Verbraucher ist interessant, wie viel personenbezogene Daten bekannt gegeben werden müssen und wie mit diesen umgegangen wird. Die Benutzer sollten außerdem darauf achten, dass ihre Authentisierungsdaten am Hotspot nicht gespeichert werden oder missbraucht werden können. Die Authentisierung sollte grundsätzlich verschlüsselt erfolgen.
- Jeder Benutzer eines Hotspots sollte sich über seine Sicherheitsanforderungen im Klaren sein und danach entscheiden, ob bzw. unter welchen Bedingungen für ihn eine Nutzung des Hotspots akzeptabel ist.
- Spätestens dann, wenn finanzrelevante, personenbezogene oder andere sensible Daten wie Kreditkartennummern, PINs, Passwörter oder auch E-Mails übertragen werden sollen, muss sichergestellt werden, dass alle notwendigen Sicherheitsmaßnahmen auf dem Client, vor allem Verschlüsselung, aktiviert sind. Als Beispiel wäre hier das sichere Bearbeiten von Emails über eine HTTPS-Webschnittstelle bzw. über die hierfür vorgesehenen sicheren Internetprotokolle (Secure POP, IMAPS, SMTP mit SSL/TLS) zu nennen.
- Wenn der Betreiber die Verschlüsselung auf der Funkstrecke gewährleistet, könnte prinzipiell auf Verschlüsselung auf der Applikationsebene verzichtet werden. Als zusätzliche Sicherheitsmaßnahme sollte diese aber weiter durchgeführt werden, auch da diese unter eigener Kontrolle steht. Insbesondere Passwörter sollten nie unverschlüsselt über fremde Netze übertragen werden.

- Zum Zugriff auf ein organisationsinternes Netz sollte generell vom WLAN-Client eine verschlüsselte Verbindung über den vertrauenswürdigen Access Point der Institution aufgebaut werden.
- Wenn man sich im Bereich eines Hotspots befindet, diesen aber nicht benutzen möchte, so sollte die WLAN-Schnittstelle am WLAN-Client abgeschaltet sein, um ein zufälliges Einbuchen zu vermeiden.
- Falls der Betreiber für die Authentisierung am Hotspot Zertifikate anbietet, sollten die Benutzer deren Korrektheit überprüfen. Auch wenn dies lästig ist, sollten Angaben wie Fingerprint, Gültigkeitsdauer, Inhaber sowie die Zertifizierungsinstanz des Zertifikates auf Plausibilität überprüft werden.
- Generell müssen bei allen mobilen Clients, die sich in verschiedene WLANs einbuchen können, weitere lokale Schutzmaßnahmen implementiert werden, wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc. Weitere Maßnahmen für einen WLAN-Client finden sich in der Maßnahme M 4.297 *Sicherer Betrieb der WLAN-Komponenten*.
- Für die Nutzung von Hotspots empfiehlt es sich außerdem, spezielle Benutzerkonten mit sicherer Grundkonfiguration und restriktiven Rechten anzulegen. Keinesfalls sollte sich ein Benutzer mit Administratorrechten von seinem Client aus an externen Netzen anmelden.

Prüffragen:

- Benutzung eines externen Hotspots: Entsprechen die Algorithmen und Sicherheitsverfahren des Hotspots dem aktuellen Stand der Technik?
- Benutzung eines externen Hotspots: Erfolgt die Übertragung sensibler Daten ausschließlich unter Verwendung entsprechender Sicherheitsmaßnahmen und sicherer Protokolle?
- Erfolgt der Zugriff auf ein internes Netz der Organisation nur über vertrauenswürdige Access Points und Verbindungen?
- Ist in der Sicherheitsrichtlinie der erlaubte Zugriff auf Hotspots definiert?
- Wird die Gültigkeit der Hotspot-Zertifikate bei der Authentisierung überprüft?
- Werden für die Nutzung an externen Hotspots separate Benutzerkonten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen verwendet?
- Wird die Anmeldung an externe Hotspots mit administrativen Benutzerkonten verhindert?

# M 2.390 Außerbetriebnahme von WLAN-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wenn WLAN-Komponenten außer Betrieb genommen werden, müssen alle sensiblen Informationen gelöscht werden. Hierbei müssen insbesondere die Authentikationsinformationen für den Zugang zum WLAN und anderer erreichbarer Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Dies bedeutet, dass beispielsweise kryptographische Schlüssel sicher gelöscht und Zertifikate für digitale Signaturen gesperrt werden müssen.

### Außerbetriebnahme von WLAN-Clients

Als WLAN-Clients findet eine Vielzahl verschiedener Geräte Verwendung. Hierzu zählen unter anderem:

- Laptops
- PDAs, Smartphones und ähnliche Geräte mit WLAN-Unterstützung
- WLAN-fähige Telefone, Drucker und Kameras

Die WLAN-Funktionalität ist typischerweise eine neben diversen anderen Funktionen bei diesen Endgeräten. Bei der Außerbetriebnahme dieser Endgeräte ist daher zu berücksichtigen, ob solche Geräte sicherheitskritische WLAN-Informationen beinhalten, die zu löschen, zu übertragen bzw. zu archivieren sind, z. B.:

- Informationen über den Benutzer des Endgerätes
- Zertifikate bzw. zugehörige private Schlüssel (für Benutzer oder Geräte)
- Kennwörter für WLAN-Zugänge
- Schlüsselmaterial von Authentikationsverfahren wie z. B. WPA-PSK-Schlüssel
- PIM-Daten, also Kontaktinformationen, Termine usw.

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung zu nutzen. Bei Zertifikaten ist beispielsweise ein Eintrag in die entsprechende CRL vorzunehmen, um das Zertifikat zu widerrufen.

Falls ein WLAN-Client gestohlen wird, sind mindestens alle oben aufgeführten Informationen zu berücksichtigen, und es ist dafür zu sorgen, dass die Informationen nicht länger zum Zugriff auf WLANs der betroffenen Institution genutzt werden können.

### Außerbetriebnahme von Access Points

Bei der Außerbetriebnahme von Access Points ist grundsätzlich das Gleiche zu beachten wie bei WLAN-Clients. Mindestens folgende sicherheitsrelevante Informationen sind, sofern zutreffend, zu löschen, zu übertragen bzw. zu archivieren:

- Pre-Shared Keys (PSK) von WPA bzw. WPA2
- RADIUS-Schlüssel (RADIUS Shared Secrets)
- IPSec-Schlüssel (PSKs bzw. private Schlüssel zu Zertifikaten)
- Benutzerdaten (insbesondere bei integrierten WLAN-Benutzerverwaltungen)
- Konfigurationsinformationen wie z. B. IP-Adressen und Namen von RADIUS-Servern, Name des Access Points selbst, IP-Adresse, SSID

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung zu nutzen. Die entsprechenden Verfahren müssen rechtzeitig ausgewählt und getestet werden.

Oft enthalten Access Points weitere Daten (beispielsweise Konfigurationsdaten), die in einem nichtflüchtigen Speicher abgelegt sind, oder sind von außen beschriftet (beispielsweise mit dem Rechnernamen, SSID, IP-Adresse und weiteren technischen Informationen). Diese Informationen sollten nach Möglichkeit vor der Weitergabe des Gerätes entfernt werden, da ein Angreifer auch aus solchen Informationen eventuell Hinweise für mögliche Angriffe ziehen kann.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann, damit kein Schritt vergessen wird.

Prüffragen:

- Existieren Vorgaben für die Außerbetriebnahme von WLAN-Komponenten?
- Ist sichergestellt, dass alle sensiblen Daten (z. B. Zertifikate, Passwörter, Benutzerkonten, Beschriftungen, etc.) auf den WLAN-Komponenten zuverlässig gelöscht werden?

# M 2.391 Frühzeitige Information des Brandschutzbeauftragten

**Verantwortlich für Initiierung:** Brandschutzbeauftragter, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter, Haustechnik

Bei allen Arbeiten an Rohr- und Kabeltrassen, die in irgendeiner Form Wanddurchbrüche sowie notwendige Flure, Flucht- und Rettungswege berühren, ist der Brandschutzbeauftragte zu informieren. Diese Information muss schon so deutlich im Vorfeld der eigentlichen Arbeiten erfolgen, dass der Brandschutzbeauftragte ausreichend Gelegenheit hat, alle Aspekte des baulichen vorbeugenden Brandschutzes in die Planung und Durchführung der beabsichtigten Arbeiten einzubringen.

Dem Brandschutzbeauftragten muss, auch während laufender Arbeiten, durch rechtzeitige Information die Gelegenheit gegeben werden, die ordnungsgemäße Ausführung von Brandschutzmaßnahmen zu kontrollieren, bevor diese durch den Baufortschritt nicht mehr zugänglich sind, z. B. weil eine abgehängte Decke bereits geschlossen worden ist.

Die Einbindung des Brandschutzbeauftragten ist durch entsprechende Organisationsanweisungen sicherzustellen und in den Planungs- und Abnahmeunterlagen der Baumaßnahme zu dokumentieren (siehe auch M 1.6 *Einhaltung von Brandschutzvorschriften*).

Prüffragen:

- Gibt es eine schriftlich festgelegte Handlungsanweisung zur Einbindung des Brandschutzbeauftragten in Arbeiten an Leitungstrassen?

# M 2.392 Modellierung von Virtualisierungsservern und virtuellen IT-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Um eine angemessene Gesamtsicherheit für den IT-Betrieb zu erreichen, müssen alle Virtualisierungsserver und alle virtuellen IT-Systeme systematisch im Sicherheitskonzept berücksichtigt werden. In Bezug auf die IT-Grundschutz-Vorgehensweise bedeutet dies insbesondere, dass alle virtuellen IT-Systeme in die Strukturanalyse und in die Modellierung einbezogen werden müssen.

Als Modellierung wird in der IT-Grundschutz-Vorgehensweise die Zuordnung von Bausteinen zu den vorhandenen Zielobjekten (IT-Systeme, Anwendungen, Räume, etc.) bezeichnet. Grundsätzlich erfolgt die Modellierung virtueller IT-Systeme nach den gleichen Regeln wie bei eigenständigen physischen IT-Systemen. Das heißt, es sind die Hinweise in Kapitel 2.2 der IT-Grundschutz-Kataloge zu beachten. Die Zuordnung der IT-Grundschutz-Bausteine richtet sich in erster Linie nach der Funktion des IT-Systems (Server, Client, etc.), nach dem verwendeten Betriebssystem (Unix, Windows, etc.) und nach den darauf betriebenen Applikationen (Datenbank, Webserver, etc..).

Um die Pflege des Sicherheitskonzepts zu erleichtern und die Komplexität zu reduzieren, sollte besonders sorgfältig geprüft werden, inwieweit die virtuellen IT-Systeme zu Gruppen zusammengefasst werden können. Prinzipiell können auch solche virtuellen IT-Systeme, die sich auf unterschiedlichen physischen Computern befinden, in einer Gruppe zusammengefasst werden. Dies muss jedoch im Einzelfall geprüft werden. Hinweise zur Gruppenbildung finden sich in der IT-Grundschutz-Vorgehensweise.

Falls unterhalb der Virtualisierungsschicht ein vollwertiges und eigenständiges Basis-Betriebssystem zum Einsatz kommt, muss dieses Betriebssystem unabhängig von den virtuellen IT-Systemen in die Modellierung einbezogen werden. Auch hier ist zu prüfen, ob eine Gruppierung vorgenommen werden kann.

**Beispiel-Szenario**

Als Beispiel wird ein physischer Server S1 betrachtet, auf dem mit Hilfe einer Virtualisierungssoftware die drei virtuellen Server VM1, VM2 und VM3 betrieben werden. Als Basis-Betriebssystem kommt auf dem physischen Server S1 eine Unix-Version zum Einsatz. Die Virtualisierungsschicht ist in diesem Beispiel eine Software-Komponente, die unter Unix läuft, also eine hostbasierte Servervirtualisierung (Typ 2). Die beiden virtuellen Server VM1 und VM2 werden mit Windows 2003 betrieben, auf VM3 ist hingegen Unix installiert. Applikationen können sowohl auf den drei virtuellen Servern als auch (unter Umgehung der Virtualisierungsschicht) direkt auf dem Basis-Betriebssystem des physischen Servers S1 ablaufen.

Die folgende Abbildung zeigt ein Schema dieser Beispiel-Konfiguration:

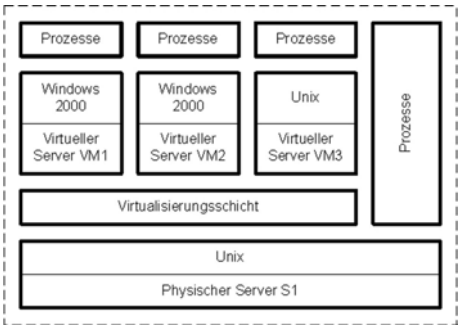



Abbildung: Schema der Beispiel-Konfiguration mit drei virtuellen Servern

**Hinweis:** Nicht bei allen Lösungen zur Virtualisierung kommt ein vollwertiges Basis-Betriebssystem unterhalb der Virtualisierungsschicht zum Einsatz.

Falls die Voraussetzungen für eine Gruppierung von VM1 und VM2 erfüllt sind, könnte die Modellierung für das oben dargestellte Beispiel-Szenario wie folgt aussehen (Auszug):

| **Baustein** | **Zielobjekt** |
|---|---|
| B 3.101 Allgemeiner Server | S1 |
| B 3.101 Allgemeiner Server | VM3 |
| B 3.101 Allgemeiner Server | Gruppe aus VM1 und VM2 |
| B 3.102 Server unter Unix | S1 |
| B 3.102 Server unter Unix | VM3 |
| B 3.108 Windows Server 2003 | Gruppe aus VM1 und VM2 |

Tabelle: Zuordnung Bausteine zu Zielobjekten

Prüffragen:

- Existiert eine Planung für den Einsatz von virtuellen IT-Systemen, in der die Ziele des Einsatzes sowie die Auswirkungen auf die IT-Risiken betrachtet werden?
- Steht der Einsatz von virtuellen IT-Systemen im Einklang mit den Sicherheitszielen der Organisation?
- Sind die Anforderungen an die virtuellen IT-Systeme hinsichtlich deren Isolation voneinander sowie Verfügbarkeit und Durchsatz definiert?
- Wird vor der Überführung von virtuellen IT-Systemen geprüft, ob ausreichende Antwortzeiten bzw. Verarbeitungsgeschwindigkeiten erzielt werden?
- Ist festgelegt, welche Anwendungen sich auf virtuelle IT-Systeme stützen?
- Sind die Auswirkungen auf administrative und betriebliche Prozesse auf den virtuellen IT-Systemen untersucht?
- Sind die Auswirkungen auf Anwender und Benutzer auf den virtuellen IT-Systemen untersucht?
- Werden alle virtuellen Systeme im IT-Sicherheitskonzept berücksichtigt?
- Wurden alle virtuellen Systeme in die IT-Strukturanalyse, die Schutzbedarfsfeststellung und die Modellierung mit einbezogen?
- Sind die Administratoren für Planung, Einrichtung und Betrieb von virtuellen IT-Systemen ausgebildet?
- Werden die Leistungsdaten der virtuellen IT-Systeme überwacht?

# M 2.393 Regelung des Informationsaustausches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Fachverantwortliche, Mitarbeiter

Informationen können in unterschiedlichen Formen vorliegen. Meistens werden im Bereich des IT-Grundschutzes in Papierform vorliegende Informationen bzw. elektronisch erfasste Informationen betrachtet. Generell müssen alle Informationen angemessen geschützt werden, angefangen von Gedanken und Ideen über geschriebene und gedruckte Darstellungen bis zu elektronischen Nachrichten, Sprach-, Bild oder Videoaufzeichnungen.

Sollen zwischen zwei oder mehreren Kommunikationspartnern Informationen ausgetauscht werden, so sind zu deren Schutz eine Reihe von unterschiedlichen Aspekten zu beachten. Bei jeder Art von Informationsaustausch ist zunächst zu klären,

- wie schutzbedürftig diese sind (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*),
- mit wem diese ausgetauscht werden dürfen (siehe M 2.42 *Festlegung der möglichen Kommunikationspartner*) und
- wie diese dabei zu schützen sind.

Hierfür sollten klare und verständliche Regelungen vorliegen, die alle Formen des Informationsaustausches abdecken, also zum Beispiel den mündlichen Austausch ebenso wie Datenaustausch per Datenträger, Mail, Fax, (Mobil-) Telefon oder Internet. Generell sollte sichergestellt sein, dass Informationen nicht in falsche Hände, Augen und Ohren gelangen können und sie nicht unbemerkt verändert werden können.

Allen Mitarbeitern sollte bewusst sein, dass sie dafür verantwortlich sind, interne Informationen angemessen zu schützen. Beispielsweise sollten Ideenskizzen auf Papier nicht in Besprechungsräumen liegengelassen werden, Projektplanungen nicht in öffentlichen Verkehrsmitteln oder im Restaurant diskutiert werden, Anrufern nicht ungeprüft Interna mitgeteilt werden. Schutzbedürftige Informationen sollten nicht unbeaufsichtigt an Druckern oder Faxgeräten ausgedruckt oder gar liegengelassen werden. Wandtafeln und Whiteboards in Besprechungs-, Schulungs- und Veranstaltungsräumen sollten am Ende der jeweiligen Sitzung gereinigt werden, benutzte Flipchart-Blätter sind gegebenenfalls zu entfernen. Mitarbeiter sollten regelmäßig auf solche Aspekte hingewiesen werden, beispielsweise über passende Erläuterungen und Veranschaulichungen im Intranet oder in der Hauszeitung.

Bei Kommunikationspartnern sollte regelmäßig überprüft werden, ob diese berechtigt sind, die jeweiligen Informationen zu erhalten. So könnte sich unter anderem die Firmenzugehörigkeit, die Post- oder E-Mail-Adresse oder die Faxnummer geändert haben und übermittelte Informationen so die Falschen erreichen. Bei einem Erstkontakt sollte zusätzlich die Identität des Gegenüber überprüft werden, da Visitenkarten auf beliebige Namen ausgestellt werden können. Daher ist es zu empfehlen, bei neuen Geschäftspartnern Rückfrage in deren Behörde oder Unternehmen zu halten oder Referenzen einzuholen.

Wie analoge und elektronische Informationen beim Informationsaustausch zu schützen sind, ist unter anderem ausführlich in den Bausteinen B 5.2 *Datenträgeraustausch* und B 5.3 *Groupware* beschrieben.

Prüffragen:

- Sind Regelungen erstellt und bekanntgegeben worden, was beim Informationsaustausch zu beachten ist?
- Sind alle Mitarbeiter für mögliche Gefährdungen beim Informationsaustausch ausreichend sensibilisiert?

# M 2.394 Prüfung elektrischer Anlagen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Haustechnik

Nach der Errichtung und anschließend in regelmäßigen Abständen müssen elektrotechnische Installationen überprüft werden.

Die Erstprüfung ist in der Norm DIN-VDE 0100-610 *"Errichten von Niederspannungsanlagen - Teil 6-61: Prüfungen - Erstprüfungen"* (Deutsche Fassung der IEC 60364-6-61) beschrieben. Die Prüfung muss durch einen staatlich anerkannten Sachverständigen erfolgen. Der Prüfer besichtigt die Installationen und ihre Ausführung vor Ort und führt Prüfmessungen durch. Hierbei wird geprüft, ob

- alle elektrischen Anlagen nach Herstellervorgaben errichtet worden sind,
- Brandschotts korrekt eingebaut wurden,
- eine richtige Auswahl der Leiter in Bezug auf Strombelastbarkeit, Auswahl und Einstellung der Schutzeinrichtungen und Übereinstimmung mit der Planung getroffen wurde,
- Schaltpläne vollständig und korrekt sind,
- Warnhinweise angebracht wurden,
- alle Leiter ordnungsgemäß verbunden sind,
- die Durchgängigkeit der Schutzleiter gegeben ist.

Zudem umfaßt die Erstprüfung die Messung des Isolationswiderstands der gesamten Anlage und die Prüfung und den Nachweis des Schutzes durch automatische Abschaltung.

Ergebnis der Erstprüfung ist die Feststellung der Betriebssicherheit und Wirksamkeit der elektrotechnischen Anlagen.

Elektrische Anlagen müssen auch danach regelmäßig durch einen Sachkundigen auf Betriebssicherheit überprüft werden. Dabei muss neben dem vorrangigen Schutzziel der Unfallverhütung vor allem die Auswirkung von Änderungen der Nutzung (z. B. durch eine stark angestiegene Anzahl von Verbrauchern) überprüft und dokumentiert werden. Die Prüfprotokolle mit den Ergebnissen der Prüfungen und Messungen sollten archiviert werden.

Prüffragen:

- Werden elektrotechnische Installationen nach der Errichtung durch einen Sachverständigen überprüft?
- Wird die elektrotechnische Installation regelmäßig durch einen Sachkundigen auf Betriebssicherheit überprüft?

# M 2.395 Anforderungsanalyse für die IT-Verkabelung

**Verantwortlich für Initiierung:** Planer, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Leiter IT, Planer

Bei der Analyse der Anforderungen, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der IT-Verkabelung haben, müssen verschiedene Fragestellungen bearbeitet werden.

Die meistens im Vordergrund stehende Frage ist die nach dem erforderlichen Daten-Durchsatz. In ihr wird zunächst die kurzfristig geplante Nutzung durch die Anwender in der Institution und darauf aufbauend die längerfristige Entwicklung der IT-Nutzung abgeschätzt.

Zwei Entwicklungen sind dabei zu berücksichtigen:

Zum einen wird Bandbreite stetig billiger. Die Folge ist, dass Dienste, die von Dritten angeboten und von diesen bezogen werden, immer höhere Anforderungen an die Kapazität der IT-Verkabelung stellen. Nach den IT-typischen Diensten wie E-Mail und WWW werden nun auch Sprach- und Bildübertragung bis hin zum digitalen Fernsehen zum Inhalt von IT-Netzdiensten. Der damit steigende Bedarf an Bandbreite muss bei der Auswahl der Qualität der IT-Verkabelung berücksichtigt werden.

Zum zweiten wird das IT-Netz zum Träger für immer weitere Anwendungen. Alle Anwendungen, die die Protokolle und Standards der IT-Welt nutzen können, werden sie voraussichtlich auch einsetzen. Das bedeutet, dass ein IT-Netz und damit die IT-Verkabelung zukünftig nicht mehr nur als Träger der Kommunikation zwischen Rechnern dient. Auch die Telefonie und Anwendungen, die bislang auf eigene, anwendungsspezifische Netztechnik angewiesen sind, werden zur Nutzung einheitlicher IT-Technik weiterentwickelt. Diese absehbaren Entwicklungen haben zur Folge, dass die Anzahl der Anschlüsse entsprechend zu planen ist und dass kein Teil eines Gebäudes mehr bei der Planung einer IT-Verkabelung ausgespart werden kann. Zudem ist die interne Verkabelung eines Gebäudes flexibel und erweiterbar auszulegen, weil eine Nutzungsänderung von Räumen oder Gebäudeteilen zugleich auch eine Änderung der Anforderungen an den Netzanschluss darstellen wird.

Trotz Vereinheitlichung der Technik ist es in einigen Fällen erforderlich, unterschiedliche oder separate Kabel für bestimmte Anwendungen einzuplanen. Gerade in besonders sicherheitsbedürftigen Anwendungsbereichen, wie Alarm gebender Technik oder bei der Steuerung von Maschinen und Anlagen, wird es angemessen oder sogar nötig sein, eigene Kabel und Vermittlungstechnik für solche Anwendungen zu verwenden. Besitzen die Anwendungsbereiche einen unterschiedlichen Schutzbedarf und können diese nicht auf einem anderen Weg geschützt werden (z. B. mit VPNs), sollte generell eine Trennung erfolgen.

**Verfügbarkeit**

Das Schutzziel Verfügbarkeit wird zunächst durch eine sorgfältig Planung und Ausführung der Kabeltrassen verfolgt. Wenn die Anforderungen der Nutzer so weit gehen, dass auch bei umfassenderen Vorfällen die Anbindung und die Netzinfrastruktur des Gebäudes nutzbar bleiben muss, so muss dies durch eine durchdachte redundante Trassenführung (siehe M 6.103 *Redundanzen für*

*die Primärverkabelung*, M 6.104 *Redundanzen für die Gebäudeverkabelung*) angestrebt werden.

**Integrität**

Um die Integrität der transportierten Daten sicherzustellen, ist die Abschirmung gegen äußere Einflüsse das oberste Gebot. Das bedeutet vor allem, dass die IT-Verkabelung getrennt von der elektrotechnischen Verkabelung zu führen ist. Zudem ist zu bestimmen, welche Kabeltypen für die Einsatzanforderungen angemessen sind (siehe M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*).

**Vertraulichkeit**

Wenn Vertraulichkeit der transportierten Daten, also Abhörsicherheit des Kabels, ein wesentlicher Aspekt ist, sind Lichtwellenleiter (LWL) die erste Wahl. Sie erfordern weitaus mehr technischen Aufwand für den potentiellen Lauscher an der Leitung als alle Kupfer-basierten Lösungen.

Wichtiger noch ist der Schutz von Verteilern und Anschlussdosen, um zu verhindern, dass normale IT-Geräte für Abhörversuche an das lokale Netz angeschlossen werden können. Das gilt natürlich auch für eine LWL-Verkabelung.

In vielen Fällen kann die Vertraulichkeit und Integrität der transportierten Daten alternativ oder ergänzend mit Hilfe von kryptographischen Verfahren geschützt werden, sofern die angeschlossenen Endgeräte und die genutzten Übertragungsprotokolle dies unterstützen. Zum Schutz der Verfügbarkeit tragen kryptographische Verfahren hingegen nur in Spezialfällen bei.

**Weitere Anforderungen**

Es ist zu beachten, dass auch die Energieversorgung von aktiven Komponenten, wie IP-Telefone oder WLAN-Access Points, durch die IT-Verkabelung stattfinden kann oder soll. Wo der Anschluss solcher Geräte zu planen ist, wird Kupferverkabelung obligatorisch, weil die Stromversorgung nur über Kupferkabel möglich ist.

Prüffragen:

- Existiert eine Anforderungsanalyse für die IT-Verkabelung, die unterschiedliche Anwendungsbereiche sowie die Aspekte der Verfügbarkeit, Integrität- und Vertraulichkeit berücksichtigt?

# M 2.396 Vorgaben zur Dokumentation und Kennzeichnung der IT-Verkabelung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Wenn eine Erneuerung oder Modernisierung der IT-Verkabelung geplant wird, ist zwischen Auftraggeber und den Auftragnehmern (Netzplaner, Lieferanten und Errichtern) zu vereinbaren, wie die Dokumentation der IT-Verkabelung auszuführen ist. Der Auftraggeber muss sicherstellen, dass er bei Inbetriebnahme eine interne und eine externe Dokumentation der Verkabelung besitzt.

Die interne Dokumention umfasst alle Aufzeichnungen, die die Errichtung und den Betrieb der IT-Verkabelung betreffen. Für die interne Dokumentation gilt, dass sie so umfangreich angefertigt und gepflegt werden sollte, dass der Betrieb und die zukünftige Weiterentwicklung bestmöglich unterstützt werden.

Die externe Dokumentation ist die Beschriftung von Anschlüssen zur Unterstützung des Betriebs. Im Sinne des Schutzes vor Sabotage und anderem böswilligen Eingriff gilt, dass die extern sichtbare Dokumentation der Verkabelung (z. B. die Beschriftung der Netzdosen und Kabelenden) so sparsam wie möglich ausfallen sollte. Hier gilt es, einem potentiellen Angreifer so wenig Hinweise wie möglich zu geben, jedoch gleichzeitig dem IT-Personal die notwendigen Kennzeichnungen bereitzustellen, die für ordnungsgemäße und nachvollziehbare Patch- und Vernetzungsarbeiten erforderlich sind.

Bei mittleren und großen Vorhaben zur Verkabelung ist der Einsatz von geeigneter Software zur Dokumentation zwingend. Bereits in der Planungsphase müssen deshalb Vorgaben über Dateiformate und damit über Programm und Version der einzusetzenden Software gemacht werden. So wird sichergestellt, dass der Auftragnehmer seine Dokumentation in einer Form liefern kann, die der Auftraggeber unmittelbar weiter nutzen kann. Ebenso sollten Vorgaben zur Namenskonvention für die Dateien selbst und auch für Elemente und Strukturen, die in den Dateien beschrieben sind, gemacht werden. Die Version einer Datei sollte möglichst schon am Dateinamen erkennbar sein, beispielsweise dadurch dass jeder Dateiname mit einer Datumsangabe der Form JJJJMMTT beginnt.

Auch für die Namenskonventionen und Kennzeichnungen in den Dokumenten sind klare Vorgaben zu machen. Beispielsweise ist zu vereinbaren, wie unterschiedliche Klassen von verlegten Kupferkabeln in Zeichnungen auszuzeichnen sind (Beispiel: L123-cu6a = Leitung 123, Kupfer, CAT 6a).

Ein Problem ergibt sich oft bei Raumnummern: der Architekt vergibt diese üblicherweise in der Planungsphase. Diese Raumnummern werden auch bei der Planung und Ausführung der IT-Verkabelung verwendet. Wenn der Nutzer nach Übernahme des Gebäudes eine andere Systematik für die Kennzeichnung und Beschriftung von Räumen einführt, kann dies zu Unklarheiten, zu Beeinträchtigungen des Betriebes oder zu anderen Sicherheitsproblemen führen.

Beispielsweise kann es passieren, dass durch Inkonsistenzen bei der Raumnummerierung Kabelverbindungen zu falschen Räumen und somit zwischen den falschen IT-Systemen hergestellt werden.

Erster Schritt der Dokumentation der IT-Verkabelung ist die Planungs- und Errichtungsdokumentation. Zu dokumentieren ist zunächst die geplante Topografie des Netzes. Dabei wird in die Gebäude- und Raumplanung zunächst der geplante Verlauf der Wege von Kabeln und Trassen und die Lage der Anschlussdosen eingezeichnet. Vom Errichter sind dann Dokumente zur Ausführung der Verkabelungsarbeiten zu erbringen.

Die Dokumentation der IT-Verkabelung besteht aus:

- Trassenverlauf und -nutzung im Gebäudeabschnitt,
- Trassenverlauf, Leitungsführung und Lage der Anschlussdosen pro Etage,
- Raumpläne für alle Technikräume der IT-Verkabelung mit Schrankaufstellung und eventuell Einspeisungspunkten von Fremdnetzen,
- Schrankansichtspläne mit Schrankeinbauten und Patchplänen,
- Konformitätsnachweise über die auftragsgerechte Ausführung,
- Lieferinformationen, Messprotokolle und Abnahmeprüfungen.

Diese Dokumentation ist Grundlage und wesentlicher Teil der Abnahme des Gewerkes durch den Bauherrn.

Für den späteren Netzbetrieb ist es zweckmäßig, getrennte Dokumente für die Ist-Beschreibung des Netzes und zur Fortschreibung anzufertigen. Die enge Anbindung an die Bauplanung und an typische Programme und Datenformate der Bauplanung (CAD) sind eher in der Errichtungsphase zweckmäßig.

Im laufenden Betrieb ist es oft zweckmäßiger, logische und IT-spezifische Strukturen des IT-Netzes in der Dokumentation zu betonen und bauliche Aspekte unterzuordnen. Zu diesem Zweck sind "IT-nahe" Software-Werkzeuge angemessener. Die Mitarbeiter sind mit der Bedienung solcher Programme meist besser vertraut, als im Umgang mit CAD-Software.

Prüffragen:

- Existieren Vorgaben zur Kennzeichnung der Verkabelung vor Ort (Verteiler und Dosen, externe Dokumentation) sowie zur Dokumentation der Verkabelung in Unterlagen und Plänen (interne Dokumentation)?

# M 2.397 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine grundlegende Voraussetzung für den sicheren Einsatz von Druckern, Kopierern und Multifunktionsgeräten ist eine angemessene Planung im Vorfeld. Der Einsatz von Druckern kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs geplant werden: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

Im Grobkonzept sollten beispielsweise folgende Schwerpunkte behandelt werden:

- Zunächst muss geregelt werden, wo Drucker und Kopierer aufgestellt werden sollen und wer in diese Räume bzw. auf die Geräte zugreifen darf (siehe M 1.32 *Geeignete Aufstellung von Druckern und Kopierern*).
- Als nächstes muss der Zugriff auf die Netzdrucker geregelt werden, also wer welche Zugriffsberechtigungen auf welche Drucker für welche Aufgaben erhält.
- Die Drucker und Kopierer müssen vor Angriffen geschützt werden.
    - Durch entsprechende Maßnahmen sollte physischen Manipulationen entgegengewirkt werden. Werden beispielsweise Schlösser oder Siegel an Wartungszugängen, wie Zugangsklappen angebracht, können unautorisierte Veränderungen erschwert oder zumindest erkannt werden.
    - Im Weiteren sollten Angriffe über Netze erschwert werden. Hierzu gehören beispielsweise unberechtigte Zugriffe auf Schnittstellen zur Fernadministration über das LAN (siehe Maßnahme M 4.301 *Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte*).
    - Außerdem müssen die elektronischen Informationen geschützt werden, sowohl bei der Übertragung zum Drucker als auch bei der weiteren Verarbeitung. Beispielsweise sollte überlegt werden, alle Dokumente, die auf den Festplatten der Drucker und Kopierer (eventuell nur temporär) abgespeichert werden, zu verschlüsseln.

Die folgenden Teilkonzepte sollten bei der Planung des Einsatzes von Druckern, Kopierern und ähnlichen Geräten berücksichtigt werden:

- **Allgemeine Aspekte:**
    - **Kauf oder Mieten:** In einigen Fällen kann es sinnvoll sein, die benötigten Drucker oder Kopierer nicht zu kaufen, sondern zu mieten. Werden die Geräte gemietet, muss sichergestellt werden, dass eventuell im Speicher abgelegte Dokumente sicher gelöscht werden, damit diese nicht vom nächsten Kunden, der das Gerät mietet, wieder hergestellt werden können. Hierbei muss vorab überprüft werden, ob die Speicherbereiche zuverlässig gelöscht werden können, ohne diese physisch zu zerstören.

- **Lokale oder netzfähige Drucker:** Es ist zu entscheiden, wo lokale Drucker, die nur einzelnen IT-Systemen zur Verfügung stehen oder netzfähige Drucker, die von mehreren Benutzern genutzt werden können, eingesetzt werden sollen. Häufig bietet auch eine Zwischenlösung Vorteile: Benutzer, die oft sensible Informationen ausdrucken müssen, erhalten für diese Ausdrucke einen lokalen Drucker. Für die Ausdrucke der restlichen Benutzer oder für Ausdrucke von Informationen mit einem geringeren Schutzbedarf stehen bei der Zwischenlösung leistungsfähigere, zentrale Drucker zur Verfügung.
- **Druckserver:** Netzdrucker können direkt von den Arbeitsplatzrechnern oder über einen (oder mehrere) Druckserver angesteuert werden. Ein Druckserver nimmt die Druckaufträge von den IT-Systemen an und leitet sie an die gewünschten Drucker weiter. Neben einer zentralen Verwaltung und Protokollierung können die Drucker so effizienter gegen Angriffe geschützt werden, wenn nur noch die Druckserver auf die Netzdrucker zugreifen dürfen. Es ist eine geeignete Lösung auszuwählen.
- **Richtlinien für die Nutzung:** Um Drucker, Kopierer, Scanner und Multifunktionsgeräte sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, müssen hierfür Sicherheitsvorgaben erstellt werden, die auf den vorhandenen Sicherheitszielen basieren sowie die Anforderungen aus den geplanten Einsatzszenarien einbeziehen. Diese spezifischen Sicherheitsvorgaben müssen mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein.
  Darauf aufbauend ist die sichere Nutzung dieser Geräte zu regeln, und es müssen Sicherheitsrichtlinien dafür erarbeitet werden (siehe M 2.398 *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*). Es ist darauf zu achten, dass Drucker, Multifunktionsgeräte und ähnliche Geräte in Sicherheitsaudits einbezogen werden und dass auch bei diesen Geräten regelmäßig die Umsetzung der Sicherheitsvorgaben kontrolliert wird.
- **Verteilung von Privilegien:** Es muss entschieden werden, ob bestimmte Funktionen eines Druckers auf ausgewählte Benutzer eingeschränkt werden sollen.
  Beispiele hierfür sind kostspieligere Funktionen wie Farbdrucke oder Papierdokumente auf besonderen Papierformaten, wie DIN A3. Die entsprechenden Benutzerrechte können die Verwaltung des Druckers und die Fehlersuche erschweren.
- **Nachfüllen von Verbrauchsgütern:** Bei Druckern und Kopierern müssen regelmäßig Verbrauchsgüter wie Toner und Papier nachgefüllt werden. Es sind Regelungen zu treffen, wer hierfür zuständig ist und welche Abläufe dabei eingehalten werden müssen (siehe M 2.52 *Versorgung und Kontrolle der Verbrauchsgüter* und M 2.2 *Betriebsmittelverwaltung*).

- **Regelungen des Dokumentenzugriffs:** Es müssen Maßnahmen ergriffen werden, die den Zugriff auf fremde Dokumente erschweren:

  - **Sicherheitskritische Informationen:** Werden an Netzdruckern häufig sicherheitskritische Informationen ausgedruckt, muss sichergestellt werden, dass nur befugte Personen auf die Ausdrucke zugreifen können. Hierfür können beispielsweise Netzdrucker und Kopierer eingesetzt werden, bei denen sich die Benutzer für einen Ausdruck direkt am Gerät authentisieren müssen (siehe M 4.299 *Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten*). Alternativ könnte auch der Zutritt zum Drucker auf wenige vertrauenswürdige Personen beschränkt werden, die die Ausdrucke an die jeweiligen Empfänger verteilen.

  - **Weitere Restriktionen:** Es ist zu klären, ob und welche Restriktionen für Druckerzugriffe gelten sollen. Beispielsweise ist es normalerweise nicht sinnvoll, dass Mitarbeiter, die sich von außerhalb ins Netz einwählen, auf entfernte Drucker ausdrucken können, da sie ihre Ausdrucke nicht direkt abholen können. Auch für die Zeiten, in denen normalerweise nicht gedruckt wird, können entsprechende Restriktionen umgesetzt werden.
- **Schutz der Netzdrucker:** Der Zugriff auf die Netzdrucker sollte beschränkt werden (siehe M 4.301 *Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte*):

  - **Administration:** Damit keine unberechtigten Personen Änderungen an den Druckereinstellungen vornehmen können, sind entsprechende Maßnahmen zum Schutz der Netzdrucker zu ergreifen.
  - **Physischer Schutz:** Es sollte überlegt werden, Maßnahmen gegen Manipulationen direkt am Gerät zu ergreifen.
  - **Netzspezifischer Schutz:** Beim Einsatz von netzfähigen Komponenten sind Mechanismen zum Schutz vor Angriffen aus dem Netz einzurichten. Wenn IEEE 802.1X oder ähnliche Verfahren zur netztechnischen Zugangskontrolle von den Netzdruckern und der Netzinfrastruktur unterstützt werden, sollten diese auch verwendet werden. Dies dient dem Schutz vor IT-Systemen, die unberechtigt an das Netz angeschlossen wurden. Weiterhin sollten Druckserver keine Verbindungen zu anderen IT-Systemen außer zu den voreingestellten Druckern aufbauen können.
- **Verfügbarkeit:** Es müssen Vorkehrungen gegen einen Ausfall der Druckserver oder einzelner Geräte getroffen werden. Durch entsprechende Wartungsverträge kann beispielsweise die Ausfallzeit reduziert werden, wenn technische Defekte auftreten (siehe M 6.105 *Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten*).
- **Verschlüsselung:** In der Maßnahme M 4.300 *Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten* werden unter anderem folgende Fragestellungen, die bei der Planung eine wichtige Rolle spielen, betrachtet:

  - **Festplattenverschlüsselung:** Viele Drucker und digitale Kopiergeräte besitzen eingebaute Speichermedien, auf denen Informationen abgelegt werden. Falls das Gerät hierfür eine Verschlüsselung unterstützt, sollte diese benutzt werden.
  - **Verschlüsselung der Kommunikation:** Es sollte überlegt werden, die Kommunikation zwischen den Arbeitsplatzrechnern und den Druckservern sowie zwischen den Druckservern und den Druckern zu verschlüsseln.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist auf eine passende Strukturierung und auf Verständlichkeit zu achten.

Prüffragen:

- Ist die sichere Nutzung von Druckern, Kopierern und Multifunktionsgeräten geplant?
- Ist geregelt, wo die Druckern, Kopierern und Multifunktionsgeräten aufgestellt werden dürfen?
- Wurde der Zugriff auf die Drucker, Kopierer und Multifunktionsgeräten geregelt?

- Wurden Vorkehrungen geplant, die Drucker, Kopierer und Multifunktionsgeräten vor Angriffen schützen sollen?

# M 2.398 Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, IT-Sicherheitsbeauftragter

Ein sicherer Einsatz von Druckern, Kopierern und Multifunktionsgeräten lässt sich nicht allein durch technische Maßnahmen erreichen. Zusätzlich müssen entsprechende Richtlinien für die Administratoren und die Benutzer festgelegt werden.

In der Administrationsrichtlinie sollten alle umzusetzenden Sicherheitsmechanismen für Drucker, Kopierer und Multifunktionsgeräte beschrieben sein. Dieses Dokument richtet sich an Fachpersonal.

Die Richtlinien für die Benutzer zur sicheren Nutzung von Druckern, Kopierern und Multifunktionsgeräten sollten in einem übersichtlichen Merkblatt zusammengefasst werden. Dieses Merkblatt sollte an allen Aufstellungsorten dieser Geräte aufgehängt werden.

Es sind folgende Aspekte zu berücksichtigen:

- **Zutritt zu den Kopier- und Druckerräumen:** Wenn möglich, sollte der Zutritt zu den Räumen mit den Druckern und Kopierern beschränkt werden (siehe auch M 1.32 *Geeignete Aufstellung von Druckern und Kopierern*). Es bietet sich an, den Zutritt beispielsweise auf die Mitarbeiter einer Abteilung oder die Nutzer einer Etage zu beschränken. Die Benutzer sind über die Zutrittsbeschränkungen und die zugelassenen Personenkreise zu unterrichten.
- **Behandlung nicht abgeholter Dokumente:** Häufig werden ausgedruckte Dokumente nicht abgeholt oder Fehldrucke nicht entsorgt. Alle Benutzer müssen darüber informiert sein, dass sie ihre Ausdrucke zeitnah abholen müssen. Dokumente, die keinem Benutzer zugeordnet werden können, sollten eingesammelt oder besser direkt mit einem Shredder vernichtet werden.
- **Umgang mit sensiblen Dokumenten:** Als hoch vertraulich klassifizierte Informationen sollten nicht an allgemein zugänglichen Druckern ausgedruckt bzw. Kopierern vervielfältigt werden. Amtlich geheim zu haltende Dokumente (Verschlusssachen) müssen gemäß der geltenden Vorschriften und Anweisungen geschützt werden.
- **Authentisierung am Gerät:** Soll eine Authentisierung direkt am Drucker, Kopierer oder Multifunktionsgerät erfolgen (siehe M 4.299 *Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten*), müssen die Benutzer in dieses Verfahren eingewiesen werden.
- **Verteilung von Ausdrucken:** Werden an Netzdruckern oft sicherheitskritische Informationen ausgedruckt, sollte überlegt werden, die Ausdrucke an die jeweiligen Empfänger durch vertrauenswürdige Personen verteilen zu lassen. Dieser Ansatz ist eine Alternative zur Authentisierung am Gerät und hat den Vorteil, dass nur diese Personen Zutritt zu den jeweiligen Druckern benötigen.
- **Auswahl eines Standarddruckers:** Bei mehreren verfügbaren Druckern können die Benutzer auf ihrem Client meist für alle Applikationen einen

Standarddrucker vorauswählen. Diese Funktion bietet für die Benutzer den Komfort, ohne zusätzliche Eingaben auf ihrem bevorzugten Drucker ausdrucken zu können. Durch zusätzliche Angaben kann der Ausdruck auf ein anderes Gerät umgeleitet werden.
Als Standarddrucker sollte ein logisches (virtuelles) Gerät, wie ein Druckvorschau-Programm oder ein PDF-Generator gewählt werden. Dies bietet einen gewissen Schutz davor, dass Informationen unbemerkt ausgedruckt werden, beispielsweise weil unbeabsichtigt die Drucken-Schaltfläche in einer Applikation betätigt wurde.

- **Löschen des Kopierspeichers:** Ein Vorteil von digitalen Kopierern ist, dass ein einmal eingescanntes Dokument beliebig oft ausgedruckt werden kann. Damit dadurch keine Informationen für Unbefugte zugreifbar werden, muss der hierfür verwendete temporäre Speicher nach der Benutzung gelöscht werden. Bei vielen Kopierern können die Benutzer dies nur manuell veranlassen, daher müssen entsprechende Hinweise und Anweisungen an den Geräten angebracht werden.

Jeder Benutzer sollte sich mit dem Merkblatt zur sicheren Nutzung von Druckern und Kopierern vertraut machen. Daher sollte das Merkblatt in jedem Kopierer- und Druckerraum aufgehängt sein.

Prüffragen:

- Gibt es eine Benutzer- und Administrationsrichtlinie für Drucker, Kopierer und ähnliche Geräte?
- Gibt es ein Merkblatt zur sicheren Nutzung von Druckern, Kopierern und Multifunktionsgeräten und ist dies allen Benutzern bekannt?

# M 2.399 Kriterien für die Beschaffung und geeignete Auswahl von Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle

Bei der Beschaffung neuer Drucker, Kopierer oder Multifunktionsgeräte besteht die Möglichkeit, diese von vornherein so auszuwählen, dass im späteren Betrieb mit geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann.

Viele Drucker und Kopierer sind modular aufgebaut. Das Grundgerät kann um zusätzliche Funktionen erweitert werden. Hierzu gehören beispielsweise auch zusätzliche Sicherheitsmechanismen, wie die Unterstützung einer Authentisierung über PINs oder Chipkarten. Bevor Drucker, Kopierer und ähnliche Geräte beschafft werden, sind daher neben den allgemeinen Anforderungen auch die Sicherheitsanforderungen festzulegen. Die Anforderungen und die auf dieser Basis getroffenen Entscheidungen sind zu dokumentieren. Nachfolgend werden einige grundsätzliche Anforderungen bei der Beschaffung von Druckern aufgelistet:

- Grundlegende funktionale Anforderungen
  - Sollen netzfähige Geräte beschafft werden?
  - Ist die Leistungsfähigkeit des Geräts der Größe des Benutzerkreises angemessen?
  - Was für ein Druckertyp mit welchem Druckverfahren soll angeschafft werden?
  - Kann das Gerät nachträglich durch zusätzliche Funktionen erweitert werden?
    Viele Geräte können durch entsprechendes Zubehör beispielsweise Netzfähigkeit, Duplexdruck, zusätzliche Papierschächte und eine Authentisierung nachgerüstet werden.
- Allgemeine Sicherheit
  - Unterstützt das System sichere Protokolle zur Administration?
    Damit die Geräte von zentraler Stelle aus administriert werden können, müssen netzfähige Geräte sichere Protokolle zur Administration unterstützen, bei einer Browser-basierten Konfiguration beispielsweise SSL/TLS.
  - Können Informationen verschlüsselt gespeichert werden?
    Um nach einem (unberechtigten) Ausbau der Festplatte den Zugriff auf die Daten zu verhindern, legen einige Geräte die Informationen verschlüsselt auf der Festplatte ab.
  - Ist eine Möglichkeit der Authentisierung direkt am Gerät vorgesehen (z. B. über Passwort- oder PIN-Eingaben oder Chipkarten) oder kann diese Funktion nachträglich eingebaut werden?
    Bei vielen Geräten ist eine Authentisierung vorgesehen, bei einigen allerdings nur für die Administration, um Zugriffe auf die Konfiguration abzusichern. Es gibt jedoch auch Geräte, bei denen sich alle Benutzerzugriffe absichern lassen, so dass Informationen erst ausgedruckt werden, wenn sich der Benutzer am Gerät authentisiert hat. Dies dient als Schutz davor, dass an einen Netzdrucker übertragene oder an einem Kopierer eingescannte Informationen von Unberech-

tigten ausgedruckt werden können. Eine solche Funktion kann auch für eine Kostenkontrolle verwendet werden.
  - Sind Ösen oder andere Möglichkeiten vorhanden, um die Geräte physisch vor Diebstahl zu schützen?
  - Können Manipulationen an der Hardware durch Gehäuseschlösser oder ähnliche Vorkehrungen erschwert werden?
    Häufig kommt es beispielsweise vor, dass Speichermodule aus Druckern oder Kopierern gestohlen werden.
- Sicheres Löschen
  - Kann nach jedem Kopiervorgang der Speicher durch die Benutzer gelöscht werden?
    In vielen Geräten sind Speicher, meist in der Form von Festplatten, eingebaut. Wenn Daten dort unverschlüsselt gespeichert werden, können diese unter Umständen von Unbefugten ausgelesen werden. Außerdem besteht die Gefahr, dass Angreifer die im Gerät gespeicherten Seiten erneut ausdrucken lassen. Einige Geräte bieten daher Funktionen zum Löschen des Speichers. Die Einstellungen sollten so vorgenommen werden, dass das Löschen automatisch nach jedem Kopiervorgang erfolgt.
  - Ist es möglich, die gesamte Festplatte zu löschen?
    Für eine spätere Entsorgung sollte die Möglichkeit bestehen, die gesamte Festplatte durch Überschreiben zu löschen. Das Löschen der gesamten Festplatte sollte nur nach Eingabe eines entsprechenden Löschbefehls durch einen Berechtigten möglich sein.
  - Werden Informationen zum Löschen auf dem Display angezeigt?
    Sowohl das Löschen der zuletzt gespeicherten Daten als auch das Löschen der gesamten Festplatte durch Überschreiben sollte möglichst auf dem Display des Geräts angezeigt werden.
- Netztechnische Sicherheit
  - Besitzt das Gerät netztechnische Schutzmechanismen, wie IP- und Portfilter?
  - Muss das Gerät WLAN- oder Bluetooth-fähig sein oder ist ein kabelgebundener Anschluss ausreichend?
    Der Einsatz von Funktechniken ist mit höheren Sicherheitsrisiken verbunden als der Anschluss über Kabel. Bei funkbasierten Lösungen müssen deshalb meist zusätzliche Sicherheitsmaßnahmen ergriffen werden.
  - Unterstützt das Gerät die Verschlüsselung der Druckerkommunikation?
    Damit die auszudruckenden Informationen bei der Übertragung über ein Netz nicht mitgelesen werden können, sollten Netzprotokolle eingesetzt werden, die eine Verschlüsselung der Informationen unterstützen. Ein Beispiel hierfür ist das Internet Printing Protokoll (IPP) in Verbindung mit SSL (Secure Sockets Layer).
  - Kann das Gerät in eine vorhandene IEEE 802.1X-Umgebung integriert werden?
    IEEE 802.1X ermöglicht die Authentisierung der Endgeräte am Netz. Dies schützt davor, dass IT-Systeme unerlaubt am LAN betrieben werden.
- Wartbarkeit
  - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches an?
    Es ist besonders wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.
  - Können für das Produkt Wartungsverträge abgeschlossen werden?

Oft ist der Zugriff auf Updates und Unterstützungsleistungen des Herstellers nur in Verbindung mit einem gültigen Wartungsvertrag möglich.

- Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
  Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Anforderungen an die Verfügbarkeit der Geräte abgedeckt werden können.
- Bietet der Händler oder Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
  Dieser Aspekt sollte Bestandteil eines Wartungsvertrags sein. Beim Abschluss des Vertrags ist darauf zu achten, dass die Hotline- bzw. Support-Mitarbeiter auch die Sprache der Personen, die in der Regel dort anrufen werden, sprechen.

- Kosten

  - Wie hoch sind die Anschaffungskosten der Geräte?
  - Wie hoch sind die voraussichtlichen laufenden Kosten, einschließlich Wartung, Betrieb und Support?
    Diese Kosten sollten bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden, beispielsweise im Hinblick auf Reaktionszeiten, Hotline und Qualifikation des Personals.

Prüffragen:

- Werden Anforderungen zur Beschaffung von Druckern, Kopierern und Multifunktionsgeräten definiert?
- Werden die Anforderungen dokumentiert?
- Werden bei der Beschaffung von Druckern, Kopierern und Multifunktionsgeräten Sicherheitsaspekte als Auswahlkriterien mit berücksichtigt?

# M 2.400 Sichere Außerbetriebnahme von Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sollen Drucker, Kopierer, Multifunktionsgeräte oder einzelne Komponenten solcher Geräte außer Betrieb genommen oder ersetzt werden, müssen alle sicherheitsrelevanten Informationen von den Geräten gelöscht werden. Dies gilt besonders dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben werden. Beispiele hierfür sind Verkauf, Rückgabe nach Leasing, Austausch durch den Hersteller und Reparatur durch eine Service-Firma. Aber selbst dann, wenn die Geräte intern weiter verwendet oder verschrottet werden, müssen alle schutzbedürftigen Informationen auf den Geräten gelöscht werden.

Je nach Einsatzzweck und Gerätetyp können beispielsweise folgende sicherheitsrelevante Informationen gespeichert sein:

- **"Zwischengespeicherte" Informationen:** Bei digitalen Kopierern wird in der Regel erst das gesamte Dokument eingescannt, bevor es ausgedruckt wird. Auch bei Druckern wird das Dokument erst zwischengespeichert. Zum Zwischenspeichern sind daher in den Geräten Speicherkomponenten eingebaut, meist in der Form von Festplatten. Unter Umständen können die zwischenzeitlich gelöschten Dokumente wieder hergestellt werden. Einige Geräte bieten eine Funktion, um den Inhalt des Speichers zu löschen.
- **Konfigurationseinstellungen:** Besonders bei netzfähigen Geräten geben die Konfigurationseinstellungen, wie IP-Adressen, unter Umständen Hinweise auf die Netzstruktur. Die Konfigurationseinstellungen sollten daher gelöscht oder in den Lieferzustand zurückgesetzt werden. Viele Geräte bieten hierfür entsprechende Funktionen.
- **Passwörter:** Bei vielen Geräten ist eine Passwort- oder Token-basierte Authentisierung vorgesehen, bei einigen allerdings nur für die Administration. Es gibt jedoch auch Geräte, bei denen für alle Benutzerzugriffe eine Authentisierung aktiviert werden kann. Alle Passwörter sollten auf den Lieferzustand zurückgesetzt werden.
- **Zertifikate:** Einige Geräte bieten die Möglichkeit, eine zertifikatsgestützte Authentisierung einzubinden, beispielsweise über IEEE 802.1X. Alle Zertifikate sollten auf den Lieferzustand zurückgesetzt werden.
- **Weitere Restinformationen:** Unter Umständen kann über Verbrauchsmaterialien, wie Toner-Trommeln, auf die ausgedruckten Dokumente geschlossen werden. Bei höherem Schutzbedarf sollte anhand einer Risikoabschätzung entschieden werden, ob benutzte Verbrauchsmaterialien vernichtet werden müssen.

Vor der Außerbetriebnahme oder Weitergabe von Geräten an Dritte muss der interne Speicher gelöscht werden. Wenn die Festplatte ausgebaut werden kann, wird empfohlen, diese separat zu löschen. Nach dem Löschen des Speichers muss überprüft werden, ob das Löschen auch erfolgreich war.

Die Vorgehensweise hängt dabei stark von der Art und vom Verwendungszweck des jeweiligen Gerätes ab.

Sind auf dem Gerät besonders sicherheitskritische Informationen gespeichert und kann nicht mit hinreichender Sicherheit gewährleistet werden, dass die

Daten wirklich gelöscht sind, so kann es erforderlich sein, den Speicher physisch zu zerstören bzw. unbrauchbar zu machen.

Prüffragen:

- Werden alle Informationen von Druckern, Kopierern und Multifunktionsgeräten vor der Entsorgung, Rückgabe oder Austausch sicher gelöscht?
- Wird überprüft, ob die Speicherinhalte von Druckern, Kopierern und Multifunktionsgeräten vor der Entsorgung tatsächlich gelöscht sind?

# M 2.401 Umgang mit mobilen Datenträgern und Geräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Über mobile Datenträger können je nach technischer Auslegung eine große Menge an Daten bei hohen Durchsatzraten ausgetauscht werden. Die Varianten von mobilen Datenträgern waren bis vor einigen Jahren auch noch durchaus überschaubar. Klassischerweise wurden nur auswechselbare Datenträger wie Disketten oder CDs für den Datenaustausch verwendet. Mittlerweile finden sich mobile Datenträger in einer Vielzahl von Varianten, die nicht immer auf den ersten Blick als solche zu erkennen sind. So gibt es beispielsweise Armbanduhren oder Musik-Abspielgeräte mit integriertem Datenspeicher. Die gängige Größe dieser integrierten Datenspeicher beginnt hier bei einigen hundert Megabyte und kann durchaus bis zu mehreren Gigabyte reichen.

Daher sollten für den Umgang mit Wechseldatenträgern und mobilen Geräten einige grundlegende Aspekte berücksichtigt werden. Es ist zu klären,

- welche mobilen Datenträger in der Institution genutzt werden sollen (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*),
- welche tatsächlich genutzt werden und wer diese einsetzt (z. B. über Bestandsverzeichnisse wie in M 2.2 *Betriebsmittelverwaltung* beschrieben),
- welche Daten auf mobilen Datenträgern gespeichert werden dürfen und welche nicht (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*),
- wie die auf diesen mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- mit welchen Externen Datenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind (siehe hierzu B 5.2 *Datenträgeraustausch*),
- wie verhindert wird, dass diese mobilen Datenträger für die unbefugte Weitergabe von Informationen benutzt werden,
- wie gegen die Verbreitung von Schadsoftware über die mobilen Datenträger vorgebeugt wird.

Es sollte außerdem geklärt werden, ob Mitarbeiter ihre privaten mobilen Datenträger und Geräte innerhalb der Institution benutzt werden dürfen, und auch umgekehrt, ob Mitarbeiter private Daten auf dienstlichen mobilen Datenträgern und Geräten speichern oder nutzen dürfen. Ebenso ist zu klären, ob die von Externen mitgebrachten mobilen Datenträger und Geräte innerhalb der Institution eingesetzt werden dürfen, beispielsweise um Dateien auszutauschen.

Je restriktiver die Sicherheitsvorgaben für den Umgang mit mobilen Datenträgern und Geräten sind, desto höher sind auch die Einschränkungen im Arbeitsalltag. Daher sollten alle Sicherheitsvorgaben daraufhin abgewogen werden, ob sie angemessen sind.

Die Vielzahl und Varianten von Datenträgern werden weiter zunehmen. Datenträger werden zunehmend "unsichtbar", da sie in anderen Geräten integriert werden. Es sollte regelmäßig überprüft werden, ob die Sicherheitsvorgaben für den Umgang mit mobilen Datenträgern und Geräten noch aktuell sind, angefangen damit, ob alle Varianten von derzeit gebräuchlichen Datenträgern noch erfasst sind.

Mobile Datenträger können leicht unterwegs verloren oder gestohlen werden. Daher sollten vertrauliche Informationen auf mobilen Datenträgern verschlüsselt werden. Am Besten sollten hierfür Produkte eingesetzt werden, die dafür sorgen, dass automatisch alle Daten, die auf mobilen Datenträger gespeichert werden, verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*).

Alle IT-Systeme sollten mit einer Boot-Sperre versehen werden, die ein Starten von externen Medien wie Disketten, CD-ROMs oder USB-Sticks verhindert, damit hierüber nicht unkontrolliert Software eingespielt oder Konfigurationsänderungen vorgenommen werden können. Weitere Hinweise hierzu finden sich in der Maßnahme M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*.

Die für die jeweilige Institution angemessene Vorgehensweise sollte dokumentiert und in einer Sicherheitsrichtlinie für die Mitarbeiter aufbereitet werden. Um die Risiken durch mobile Datenträger angemessen zu mindern, sind verschiedene technische Maßnahmen sinnvoll (siehe z. B. M 4.200 *Umgang mit USB-Speichermedien* oder M 4.232 *Sichere Nutzung von Zusatzspeicherkarten*), aber nicht ausreichend. Es ist unerlässlich, die Mitarbeiter hierfür entsprechend zu sensibilisieren.

Prüffragen:

- Ist die Nutzung privater mobiler Datenträger und IT-Komponenten geregelt?

# M 2.402 Zurücksetzen von Passwörtern

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Informationssicherheitsmanagement, Leiter IT

Solange Benutzer sich mit Passwörtern authentisieren müssen, wird es vorkommen, dass sie ihre Passwörter vergessen. Einerseits soll Benutzern in so einer Situation schnell geholfen werden, damit sie wieder arbeiten können. Andererseits muss verhindert werden, dass sich Unberechtigte durch unzureichende Berechtigungsprüfungen Zugriff auf IT-Systeme verschaffen können (siehe G 5.42 *Social Engineering*). Daher muss jede Institution für das Zurücksetzen von Passwörtern geeignete Vorgehensweisen auswählen.

Wichtig ist dabei, dass für das Zurücksetzen von Passwörtern flexible Richtlinien definiert werden. Eine starre Vorgehensdefinition ist in den meisten Fällen in der heutigen mobilen Arbeitswelt nicht praktikabel. Einerseits sollte das Vorgehen dem Schutzbedarf des jeweiligen Passwortes entsprechen und andererseits sollten die Zugriffsanforderungen der Anwender berücksichtigt werden.

Welche Vorgehensweise jeweils angemessen ist, hängt von vielen Faktoren ab, beispielsweise von der Größe der Institution, der Anzahl der Mitarbeiter, der geographischen Verteilung der Mitarbeiter (sind diese immer vor Ort, sind sie oft beim Kunden, wie sind diese dann erreichbar usw.) und natürlich vom Schutzbedarf der durch das Passwort geschützten Informationen und Geschäftsprozesse (Zugriff nur auf ein lokales IT-System, auf ein LAN, auf interne Netze von außerhalb, auf ein Internet-Postfach, usw.).

Hinweis: Das übliche Authentisierungsverfahren mit Hilfe von Benutzername und Passwort ist in der Regel für den normalen Schutzbedarf geeignet. Für höheren Schutzbedarf sollten stärkere Authentisierungsverfahren eingesetzt werden, beispielsweise durch die Kombination mit Chipkarte, USB-Token oder Einmalpasswort-Verfahren.

Im Folgenden werden die Vor- und Nachteile einiger Varianten zur Passwort-Rücksetzung dargestellt, aus denen die für den jeweiligen Anwendungsfall angemessenen Verfahren ausgewählt werden können.

**Schriftlich per Post oder Fax**

Hierbei wird für das Zurücksetzen eines Passworts ein Formular verwendet, in dem der Benutzer seinen Namen eintragen und unterschreiben muss. Dieses Formular muss dann per Post oder Fax dem Support gesendet werden. Dieses Verfahren ist gründlich, vor allem, wenn die Formulare archiviert werden. Nachteil ist allerdings, dass es je nach Organisationsgröße einige Zeit dauern kann, bis das Formular per (Haus-)Post beim Support ankommt. Um zu verhindern, dass sich ein Unberechtigter einfach im Namen eines berechtigten Benutzers ein Passwort zurücksetzen lässt, sollten bei dieser Variante Vergleichsunterschriften vorliegen. Der Bearbeiter beim Support muss dann die Unterschrift auf dem Formular mit der hinterlegten Unterschrift vergleichen.

Die Antwort mit dem neuen Passwort könnte der Bearbeiter ebenfalls per Post oder Fax übersenden.

Bei einem Fax kann aber im Allgemeinen nicht sichergestellt werden, dass wirklich nur der Benutzer das Passwort erhält. Bei der Postübertragung könn-

te ein versiegelter Umschlag verwendet werden. Nachteil ist aber wieder die Post-Laufzeit.

**Telefonisch ohne Zusatzmerkmale**

Die einfachste Variante ist, Passwörter per telefonischem Zuruf zurückzusetzen. Allerdings ist hierbei eine sichere Verifizierung des Benutzers aufwändig. Der Support muss in der Lage sein, an Hand der Stimme den Benutzer zu identifizieren. In Institutionen, deren Größenordnung es erlaubt, dass die Mitarbeiter sich telefonisch gegenseitig aufgrund der Stimme identifizieren können, ist diese Lösung möglich.

Eine Überprüfung der Telefonnummer ist auch nicht ausreichend. Diese könnte beispielsweise gefälscht sein. Ein Angreifer könnte auch die Abwesenheit eines Mitarbeiters nutzen, um aus dessen Büro heraus beim Support anzurufen. Genau dieses Szenario, also dass Passwörter alleine auf Grund eines Anrufs zurückgesetzt werden, steht sogar im Fokus von Social-Engineering-Angriffen. Auf diese Variante sollte also möglichst verzichtet werden.

**Telefonisch plus Wissensfrage**

Um einen Passwort-Wechsel per Telefon zu erleichtern, kann der Support auch zusätzliche Wissensmerkmale abfragen, die vorher hinterlegt wurden. Dies können beispielsweise Geburtstag oder Personalnummer des Mitarbeiters sein (dies sind allerdings Merkmale, die leicht in Erfahrung zu bringen sind). Es können Merkwörter sein, die sich zwar der Benutzer leicht merken kann, die aber schwer zu erraten ist. Hierfür empfiehlt es sich, nicht nur einen Begriff zu hinterlegen, sondern mehrere und eventuell zu jedem Begriff auch eine passende Frage zu hinterlegen. Beispielsweise könnte beim Support dann eine Frage wie "Wie hieß das Haustier, dass Sie mit 10 Jahren hatten?" mit der passenden Antwort hinterlegt sein.

Es sollten hierbei möglichst keine vorformulierten Wissensfragen wie "Wie ist der Vorname ihres Vaters?" verwendet werden, da die Antworten hierauf leicht herauszufinden sind.

**Identitätsüberprüfung mittels schon abgespeicherter Informationen**

Bei einer Anfrage per Telefon kann zur Identitätsüberprüfung auch auf andere, bei der Registrierung des Benutzers schon abgespeicherte Informationen zurückgegriffen werden. Dies könnte beispielsweise eine Mitarbeiter-Kennziffer, Geburtsdatum oder ähnliches sein. Ein Nachteil ist hierbei, dass die meisten solcher typischerweise vorab erfassten Informationen vielerorts bekannt sind und meist auch schnell über das Internet recherchiert werden können.

**Persönliche Vorsprache**

Hierbei muss der Benutzer direkt zu einer bestimmten Person gehen und den Passwort-Wechsel veranlassen. Diese Person kann, je nach Institutionsgröße, entweder ein Vorgesetzter, ein Fachverantwortlicher oder direkt ein Support-Mitarbeiter sein.

Diese Person sollte auf jeden Fall dazu berechtigt sein, die (Neu-)Vergabe von Zugriffsrechten zu genehmigen und deren Einrichtung zu beauftragen oder selbst durchzuführen.

**Beauftragung einer vertrauenswürdigen Person**

Bei dieser Variante könnte beispielsweise ein Kollege beauftragt werden, eine signierte E-Mail an den Support zu senden, in der er um die Zurücksetzung des Passwortes bittet. Durch die kryptographische Signatur kann überprüft werden, wer die Anfrage gestellt hat. Hat er hierfür keinen Auftrag erhalten, könnte ein Angriff nachträglich nachgewiesen werden.

Das neue Passwort könnte in einer verschlüsselten Mail der beauftragten Person übermittelt werden, das er dem betroffenen Benutzer mitteilt. Zusätzlich sollte der Benutzer über die Zurücksetzung informiert werden, damit ein möglicher Angriff entdeckt werden kann.

Dieser Ansatz hat allerdings die Nachteile, dass ein Angriff im Allgemeinen erst nachträglich festgestellt werden würde und dass ein Dritter das Rücksetzungspasswort erfahren würde.

**Zurücksetzen auf Einmal-Passwörter**

Generell sollte der Support bei der Rücksetzung von Passwörtern nur Einmal-Passwörter vergeben, so dass die Benutzer diese unmittelbar nach der erfolgreichen Anmeldung auf ein nur ihnen bekanntes Passwort ändern müssen. Dabei sollte der Support darauf achten, kein einheitliches Rücksetzungspasswort zu verwenden, da sich ein solches schnell herumspricht. Die Zeichenzusammensetzung des Passwortes sollte außerdem so komplex sein, dass es nicht leicht zu erraten ist.

Außerdem sollte der Support verifizieren, ob das Passwort wirklich zurückgesetzt werden muss.

**Mitteilung des Rücksetzungspasswortes**

Um dem betroffenen Mitarbeiter das neue Passwort mitzuteilen, können ebenfalls verschiedene Wege gewählt werden, beispielsweise:

- Der Support teilt dem Mitarbeiter das neue Passwort durch einen zweiten vordefinierten Weg mit, z. B. per Hauspost oder Rückruf auf eine vorher registrierte Telefonnummer (nicht, wenn von dieser die Rücksetzungsanfrage kam).
- Das Passwort kann einem Vorgesetzten, einem Sekretariat oder einer anderen vertrauenswürdigen Stelle mitgeteilt werden, die den Mitarbeiter kennt und diesen informiert.
- Das Passwort wird an eine vorab registrierte Adresse (physische oder E-Mail-Adresse) gesendet.
- Das Passwort wird per Kurier versendet, der den Ausweis des Empfängers überprüft.

**Schulung der Support-Mitarbeiter**

Wichtig ist auch, dass die Support-Mitarbeiter zum Berechtigungsmanagement ausreichend geschult werden. Sie sollten sowohl typische Social-Engineering-Methoden kennen, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen, als auch den Umgang mit Problemfällen und flexiblen Lösungsmöglichkeiten gelernt haben. Die Erfahrung zeigt, dass eine starre Vorgehensweise leichter zu hintergehen ist, vor allem, wenn sie einem Angreifer bekannt ist, als wenn Mitarbeiter mitdenken. Wenn beispielsweise festgelegt wurde, dass bei einer Passwort-Rücksetzung immer der Vorgesetzte zu informieren ist und dieser nicht greifbar ist, ist es besser, einen geeigneten Vertreter zu suchen als zu lange zu warten.

Wenn der Schutzbedarf des jeweiligen Passworts zu hoch ist und der Support-Mitarbeiter aufgrund fehlender sicherer Möglichkeiten die Verantwortung nicht übernehmen möchte, dann muss es dafür eine Eskalationsstrategie geben.

**Information der Mitarbeiter**

Alle Benutzer sollten darüber informiert sein, was sie veranlassen müssen, wenn sie ein Passwort vergessen haben. Außerdem sollten alle Benutzer aufmerken, wenn sie bei einem Anmeldeversuch feststellen, dass sie das korrekte Passwort nicht kennen. Neben purer Vergesslichkeit könnte dies auch ein Zeichen sein, dass sich ein Angreifer unbefugten Zugriff verschafft hat. Im Zweifelsfall sollte dies dem Sicherheitsmanagement gemeldet werden (siehe M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

Prüffragen:

- Wurde ein für die Organisation angemessenes Verfahren zum Zurücksetzen von Passwörtern definiert?
- Trägt das festgelegte Verfahren zum Zurücksetzen von Passwörtern dem Schutzbedarf der durch die Passwörter geschützten Ressourcen Rechnung?
- Wurden die Support-Mitarbeiter für das Berechtigungsmanagement speziell geschult?
- Bei höherem Schutzbedarf des Passwortes: Gibt es eine Eskalationsstrategie falls der Support-Mitarbeiter die Verantwortung nicht übernehmen kann?

# M 2.403 Planung des Einsatzes von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Fehler in der Konzeption eines Verzeichnisdienstes sind nach erfolgter Installation nur mit beträchtlichem Aufwand zu berichtigen. Daher muss der Einsatz von Verzeichnisdiensten sorgfältig geplant werden.

Bevor ein Verzeichnisdienst eingeführt wird, muss entschieden werden, für welche Einsatzzwecke er genutzt werden soll. Von der vorgesehenen Nutzungsart hängen unter anderem die erforderlichen Überlegungen zur Struktur des Verzeichnisdienstes ab. Auch die im Verzeichnisdienst zu speichernden Daten beeinflussen entscheidend die Art und den Umfang der notwendigen Planungen. Je nach Komplexität des Verzeichnisdienstes können die Planungen zur Konzeption des Verzeichnisdienstes mehrere Monate andauern, und auch ein Jahr überschreiten. Von dem geplanten Einsatzszenario hängen die festzulegenden Sicherheitsrichtlinien ab.

Beispiele für Nutzungsmöglichkeiten eines Verzeichnisdienstes sind:

- Adressbuch für Telefonnummern, Postadressen, usw.
- Einbindung in E-Mail-Systeme
- digitale Zertifikate, PKI (Public Key Infrastrukturen)
- netzweite Konfigurationsinformationen von IT-Systemen und Anwendungen
- einheitliches zentrales, ortsunabhängiges Benutzermanagement
- Authentikation von Menschen und Prozessen zur Anmeldung an IT-Systemen im Netz

Die genannten Beispiele zeigen eine Auswahl an möglichen Nutzungsarten eines Verzeichnisdienstes und variieren in Art, Größe und Ausprägung. Kombinationen von möglichen Anwendungszwecken sind nicht nur denkbar, sondern stellen sogar eine Stärke der Verzeichnisdienste dar. Gleichzeitig erhöht sich damit die Komplexität des Verzeichnisdienstes, was eine entsprechend sorgfältige Planung seines Einsatzes voraussetzt.

Weitergehende Fragestellungen in der Planung ergeben sich bei der Festlegung, ob der Verzeichnisdienst oder Teile davon außerhalb des Intranet einer Organisation erreichbar sein sollen.

- Wie wird der Zugang zum Verzeichnisdienst von außen abgesichert?
- Wie ist der Zugriff auf die Daten des Verzeichnisdienstes abzusichern?
- Welche Authentisierungsmechanismen werden benötigt?
- Welche Daten sollen von außen anonym erreichbar sein?
- Welche Daten sollen nach erfolgter Authentisierung erreichbar sein?
- Welche kryptographischen Verfahren sind erforderlich, um die Vertraulichkeit bzw. Integrität der übertragenen Daten sicherzustellen?

**Entwurf der Baumstruktur**

Die Anforderungen an den Verzeichnisdienst sind zunächst zu analysieren und zu dokumentieren. Neben der Festlegung der Nutzung des Verzeichnisdienstes ist ein Modell aus Objektklassen und Attributtypen zu entwickeln, das den Ansprüchen der vorgesehenen Nutzungsarten genügt.

Für den Entwurf der Baumstruktur im Directory Information Tree (DIT) ist zunächst ein oberstes Element, das Root-Element, zu wählen. Prinzipiell las-

sen sich alle weiteren Objekte direkt unterhalb dieser Wurzel anordnen. Für ein Verzeichnis der Mitarbeiter einer Organisation oder der Benutzer in einem Netz ist es allerdings sinnvoll, eine Strukturierung nach Abteilungen vorzunehmen. Die übliche Objektklasse zur Darstellung solcher Organisationseinheiten ist die "organizationalUnit".

Anschließend sind die einzelnen Personen bzw. Benutzer als Objekte im Verzeichnisbaum abzubilden. Dazu existieren bereits zahlreiche Schemata, die mit dem Verzeichnisdienst schon installiert wurden oder eingebunden werden können und je nach erforderlicher Informationstiefe unterschiedliche Klassen zur Verfügung stellen.

Die einfachste Objektklasse hierzu ist "person", die im Grunde nur Informationen über den Namen einer Person, Telefonnummer sowie über ein Passwort vorsieht.

Im Attribut "userPassword" sollten nie unverschlüsselte Passwörter gespeichert werden. Es empfiehlt sich, hier nur einen Hashwert zu speichern. Besser noch sollten aber weder die Passwörter noch deren Hashwerte in einem allgemein lesbaren Bereich des Verzeichnisdienstes, sondern in einer speziellen Bereich gespeichert werden, der ausschließlich für die Authentisierung vorgesehen ist.

Davon abgeleitet kann die "organizationalPerson" verwendet werden, die diverse Adressen und (Telefon-)Nummern sowie Abteilungszugehörigkeiten kennt, um die Organisationszugehörigkeit von Personen zu beschreiben. Die wiederum davon abgeleitete Klasse "inetorgPerson" aus dem gleichnamigen Schema bietet darüber hinaus Attribute für weitere Telefonnummern, Anschriften und E-Mail-Adressen bis hin zum Autokennzeichen. Diese Klasse kann benutzt werden, um Personen außerhalb ihrer internen Organisationszugehörigkeit zu beschreiben, z. B. für die Nutzung von Internet-Diensten.

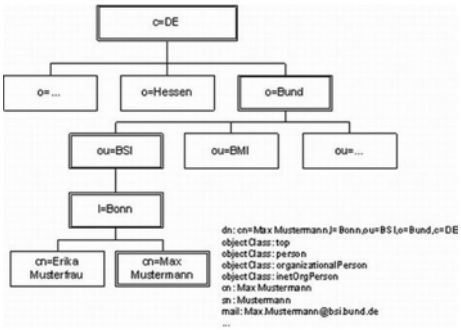



Abbildung: Beispiel einer Baumstruktur

Schemata, die typischerweise mit Verzeichnisdiensten geliefert werden, enthalten bereits rund tausend Objektklassen und Attribute. Daraus sind die geeigneten Elemente für den Einsatz eines Verzeichnisdienstes auf Grundlage der vorhergehenden Analyse der Anforderungen auszuwählen. Im Allgemeinen reichen die vordefinierten Klassen dazu aus. Dabei kann es auch praktikabel sein, ein vorhandenes Attribut in einem anderen Kontext zu benutzen und ihm so eine andere Bedeutung zu geben, ohne seinen Namen zu ändern. Von dieser Möglichkeit sollte nur Gebrauch gemacht werden, wenn sichergestellt ist, dass Verwechslungen vermieden werden können und Fehlanwendungen dieses Objektes damit ausgeschlossen sind.

Für den Fall, dass vorhandene Objektklassen und Attributtypen für den geplanten Einsatzzweck nicht ausreichend sind, ist es möglich, ein vorhandenes Schema zu erweitern. Dabei ist zu beachten, dass jedes Schemaobjekt

eine Objekt-ID (OID) besitzt, an der es eindeutig erkannt werden kann. OID-Namensräume werden durch die Internet Assigned Numbers Authority (IANA) verwaltet und fest einem Besitzer zugeordnet. Daher sollten Änderungen an einem bestehenden Schema eines fremden Besitzers grundsätzlich vermieden werden.

Für die Erstellung eigener Schemaobjekte besteht die Möglichkeit, unter www.iana.org einen eigenen Namensraum anzufordern. Unter der zugeteilten OID-Stammnummer dürfen eigene Verzweigungen definiert werden.

Wenn der Verzeichnisdienst primär der Verwaltung von IT-Ressourcen dient, sollte beim Aufbau der Baumstruktur ausreichend darauf geachtet werden, dass die Struktur auch auf administrative Gegebenheiten abgestimmt wird. Eine zu detaillierte Nachbildung der Organisationsstruktur in der Baumstruktur sollte vermieden werden, da dies Probleme in der Administration des Verzeichnisdienstes nach sich ziehen kann.

Die Baumstruktur sollte nicht zu flach gewählt werden, damit sich Teile des Verzeichnisbaumes in verschiedene Partitionen zerlegen lassen und so auf verschiedene Server im Netz verteilt werden können. Dies hat außerdem den Vorteil, dass sich eine Replizierung zwischen den Verzeichnisdienst-Servern nicht auf den gesamten Baum auswirkt. Weitere Aspekte zur Konzeption eines verteilten Verzeichnisdienstes sind in M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst* beschrieben.

Werden Verzeichnisdienste für verschiedene Nutzungsmöglichkeiten eingesetzt, sollten die Verzeichnisdaten möglichst entsprechend ihres Schutzbedarfs in getrennten Bereichen auf dem Verzeichnisdienst-Server gespeichert werden. Bei Bereichen mit unterschiedlichem Schutzbedarf erleichtert dies unter anderem die Durchführung von Datensicherungen und die Konfiguration des jeweiligen korrekten Zugriffsschutzes. Auf einem Verzeichnisdienst-Server mit direkter Internet-Anbindung sollten außerdem keine Daten gehalten werden, auf die von außen nicht zugegriffen werden soll.

Im Rahmen der Verzeichnisdienst-Planung sind folgende Aspekte zu berücksichtigen:

- Welche Einsatzzwecke und welche Aufgaben sollen erfüllt werden und welche Informationen sollen enthalten sein?
- Welche Gliederung in Standorte, Organisationen, Organisationseinheiten und weitere Objekte soll gewählt werden?
- Welche Objektklassen werden benötigt und welche verbindlichen oder optionalen Attribute sollen diese haben?
- Welche Zugriffsrechte auf die Informationen sollen über die verschiedenen Verzeichnisdienst-Schnittstellen den Benutzern gegeben werden?
- Welche Maßnahmen, z. B. das Signieren von LDAP-Pakete, sind geplant, um das unbefugte Sammeln von Daten aus dem Verzeichnisdienst wirksam zu unterbinden?

Generell ist die geplante Verzeichnisdienst-Struktur vollständig zu dokumentieren. Dies trägt maßgeblich zur Stabilität, konsistenter Administration und damit zur Systemsicherheit bei. Es sollte insbesondere festgehalten werden:

- Welche Objektklassen werden in welcher Weise verwendet, speziell welche Attribute werden für welche Inhalte genutzt?
- Welche Erweiterung des Schemas werden mit welcher Begründung durchgeführt?

Für jedes Verzeichnisdienst-Objekt sollte dokumentiert sein:

- Name und Position im Verzeichnisdienst-Baum, wie z. B. "StandortBonn", Vater-Objekt: OU "BSI",
- welchem Zweck das Objekt dient, wie z. B. Drucker im Netz,
- welche administrativen Zugriffsrechte für das Objekt und dessen Attribute vergeben werden sollen, wie z. B. vollständig verwaltet von "Admin1" und
- wie die Vererbung von Verzeichnisdienst-Rechten konfiguriert werden soll, wie z. B. blockieren oder filtern der Rechtevererbung.

**Personenbezogene Daten im Verzeichnisdienst**

Grundsätzlich sollte bei der Planung des Einsatzes eines Verzeichnisdienstes, der auch personenbezogene Daten enthält, der Datenschutzbeauftragte der Institution beteiligt werden, damit die Belange des Datenschutzes zur Wahrung des informationellen Selbstbestimmungsrechts frühzeitig berücksichtigt werden. Auch die Mitarbeitervertretung in Form des Personalrats oder Betriebsrats sollte rechtzeitig beteiligt werden.

Genauso wie für andere Daten im Verzeichnisdienst gilt für die personenbezogenen Daten, dass stets ein angemessener Schutz der Vertraulichkeit und der Integrität der Verzeichnisdienst-Einträge sowie ihrer Verfügbarkeit und Aktualität zu gewährleisten ist.

Über die grundlegenden Maßnahmen hinaus ist beim Einsatz von Verzeichnisdiensten Folgendes zu beachten:

- Personenbezogene Einträge im Verzeichnisdienst sollten auf die für den jeweiligen Nutzungszweck notwendigen Angaben beschränkt werden. Bei einem internen Verzeichnisdienst könnten das beispielsweise E-Mail-Adresse, Telefonnummer, Faxnummer oder öffentliche Schlüssel sein. In einem in externe Netze eingebundenen Verzeichnisdienst sollten keine Informationen wie z. B. Hinweise auf Aufgabenbereiche und, Arbeitszeiten von Personen sowie Örtlichkeiten sollten, soweit nicht für die Aufgabenerledigung notwendig, aufgenommen werden. Um Spam zu vermeiden, sollte auch gut überlegt werden, ob und in welcher Form E-Mail-Adresse in Verzeichnisdiensten angegeben werden.
- Grundsätzlich ist sicherzustellen, dass der Zugriff auf Informationen in Einträgen mit Personenbezug auf das für die jeweilige Aufgabenerledigung erforderliche Maß eingeschränkt wird.
- Soll der Verzeichnisdienst als Basis von Personalinformationssystemen genutzt oder ausgebaut werden, ist die Personalvertretung einzubeziehen.
- Sofern ein Verzeichnisdienst oder Teile davon außerhalb des Intranets einer Institution angeboten werden, um beispielsweise anderen Institutionen oder Geschäftspartnern Daten zur Verfügung zu stellen, müssen die allgemeinen datenschutzrechtlichen Bestimmungen berücksichtigt werden.

Die Planung der Verzeichnisdienst-Administration und des benutzten administrativen Modells ist eine wichtige Aufgabe. Empfehlungen dazu finden sich zusammengefasst in Maßnahme M 2.407 *Planung der Administration von Verzeichnisdiensten*.

Hinsichtlich der Planung des Personaleinsatzes ist zu überprüfen, wie viele Mitarbeiter mit welcher Ausbildung für den Aufbau und den Betrieb des Verzeichnisdienstes benötigt werden. Stehen nicht genügend ausgebildete Mitarbeiter zur Verfügung, müssen die erforderlichen Schulungsmaßnahmen (siehe M 3.62 *Schulung zur Administration von Verzeichnisdiensten*) rechtzeitig initiiert werden.

Prüffragen:

- Wurde eine sorgfältige Planung des Verzeichnisdienstes durchgeführt?
- Wurde für alle geplanten Objekte der genaue Kontext innerhalb des Verzeichnisbaums festgelegt?
- Wurden Personalvertretung und Datenschutzbeauftragte bei der Planung des Verzeichnisdienstes beteiligt?
- Ist ein bedarfsgerechtes Berechtigungskonzept zum Verzeichnisdienst entworfen worden?
- Existiert eine Dokumentation zur geplanten Verzeichnisdienst-Struktur?
- Sind Maßnahmen geplant, die das unbefugte Sammeln von Daten aus dem Verzeichnisdienst wirksam unterbinden?
- Ist der Umgang mit personenbezogenen Daten, die im Verzeichnisdienst gespeichert werden, geregelt?

# M 2.404 Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Es muss ein Sicherheitskonzept zum Verzeichnisdienst erstellt werden. Darin wird geregelt, welche Dienste, Komponenten, etc. in welcher Weise genutzt werden sollen und dürfen. Die folgende Liste gibt einen groben Überblick über Bereiche, die im Konzept geregelt werden sollten. Die Liste muss je nach Einsatzszenarien in der Institution entsprechend angepasst, ausgestaltet und erweitert werden. Diese spezifischen Sicherheitsvorgaben müssen mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein.

**Allgemeines:**
- Wie sollen die Verzeichnisdienst-Server physikalisch abgesichert werden?
- Welche Verzeichnisdienst-Komponenten dürfen genutzt werden?
- Welche Werkzeuge zur Administration sollen verwendet werden?
- Wie wird der Baum des Verzeichnisdienstes strukturiert und partitioniert?
- In welchem Ausmaß dürfen Schema Änderungen vorgenommen werden und zu welchem Zeitpunkt?
- Welche Objektklassen mit welchen Attributsätzen dürfen eingesetzt werden?
- Welche Replikationen welchen Typs sollen angelegt werden?
- Welche Rechner sind Verzeichnisdienst-Server und welche Rechner sollen eine Replikation halten?
- Welche Rechner sind als Root-Domäne besonders zu schützen?

**Rechtevergabe:**
- Welcher Benutzer soll welche Rechte ausüben können?
- Welcher Administrator soll welche Rechte ausüben können?
- Welche Authentisierungsverfahren sollen genutzt werden?
- Wie wird die Vererbung von Rechten innerhalb der Baumstruktur definiert?

**Administration:**
- Welche Administratorrollen werden definiert?
- Wer darf zu welchem Zeitpunkt Schema Änderungen vornehmen?
- Welche Administrationsaufgaben dürfen bzw. sollen delegiert werden?

**Datenkommunikation:**
- Welche Datenkommunikation ist abgesichert abzuwickeln?
- Mit welchen Mechanismen werden Verfügbarkeit, Vertraulichkeit und Integrität der Daten geschützt?

**Zertifikatsautorität:**
- Welche Parameter für die Zertifizierungsstelle sind zu verwenden?
- Wer darf Einstellungen der Zertifizierungsstelle ändern?
- Welche Objekte sind mit Zertifikaten zu versehen?
- Welche Zertifikate sind für SSL-Verbindungen einzusetzen?

**Dateisystem des unterliegenden Betriebssystems:**
- Welche Berechtigungen auf Systemdateien sollen für die verschiedenen Administratoren und Benutzer gelten?
- Soll Verschlüsselung auf Dateisystemebene eingesetzt werden?

**LDAP:**
- Welche Benutzer dürfen unter welchen Bedingungen über LDAP auf den Verzeichnisdienst zugreifen?
- Soll ein anonymer Login unterstützt werden?
- Welche Netzapplikationen dürfen via LDAP auf den Verzeichnisdienst zugreifen?
- Soll die LDAP-Kommunikation generell über SSL laufen?
- Dürfen die Benutzerpasswörter im Klartext übertragen werden?

**Client-Zugriff auf den Verzeichnisdienst:**
- Welche Authentisierungsverfahren sollen eingesetzt oder erlaubt werden?
- Auf welchen Verzeichnisbaum darf vom Netz aus zugegriffen werden?
- Welche Ressourcen sind aus dem Netz von welchen Benutzern zugreifbar?

**Verschlüsselung von Attributen:**
- Soll die Verschlüsselung von Attributen genutzt werden?

**Fernzugriff zur Systemüberwachung und Administration:**
- Darf ein Werkzeug zur Fernwartung genutzt werden?
- Wer darf solche Werkzeuge nutzen?
- Wie wird das Protokoll HTTPS zu diesem Zweck konfiguriert?

Die hier beschriebenen Punkte müssen in einer Sicherheitsrichtlinie für Verzeichnisdienste weiter konkretisiert werden (siehe M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*).

Prüffragen:

- Wurde ein Sicherheitskonzept für Verzeichnisdienste erstellt?
- Wurde dieses Sicherheitskonzept mit dem Sicherheitskonzept der gesamten Institution abgestimmt?

# M 2.405 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Als eine der nächsten organisatorischen Aufgaben bei der Planung des Verzeichnisdienst-Einsatzes muss aufbauend auf dem Sicherheitskonzept (siehe M 2.404 *Erstellung eines Sicherheitskonzeptes für Verzeichnisdienste*) eine Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten fixiert werden. Durch die Sicherheitsrichtlinie wird festgelegt, welche konkreten Sicherheitsbestimmungen in einem Verzeichnisdienst-System gelten sollen und wie diese bei der Installation und dem Betrieb umgesetzt werden müssen.

Durch die Verzeichnisdienst-Sicherheitsrichtlinie sollten sämtliche sicherheitsbezogenen Themenbereiche eines Verzeichnisdienstes geregelt werden. Diese komponentenspezifische Auflistung von Themengebieten kann in folgende zeitliche Abfolge gebracht werden:

**1. Definition der Verzeichnisdienst-Baumstruktur**

Im ersten Schritt ist die logische Struktur des Verzeichnisdienst-Baumes, die Aufteilung in die Organisation (die dem Root-Element und somit dem obersten Element des Baumes entspricht) und Organisationseinheiten (Organizational Units, abgekürzt mit OU) sowie insbesondere auch die Zuordnung der Server und der zu verwaltenden Netz-Ressourcen festzulegen (siehe M 2.403 *Planung des Einsatzes von Verzeichnisdiensten*).

Anschließend müssen Art und Umfang der im Verzeichnisdienst gehaltenen Objekte und deren Attribute festgelegt werden. Bei Bedarf sind hierzu Schema Änderungen am Verzeichnisdienst vorzunehmen. Weiterhin sollten an dieser Stelle die Partitionierung der Verzeichnisdaten und die Einrichtung von Repliken festgelegt werden (siehe M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst*).

**2. Regelung der Verantwortlichkeiten**

Ein Verzeichnisdienst sollte nur von geschulten Netzadministratoren betrieben werden. Dabei ist im Rahmen der Notfallvorsorge eine geeignete Stellvertreterregelung zu treffen. Generell sollte für den Verzeichnisdienst-Betrieb ein Konzept zur rollenbasierten Administration erstellt werden. Nur die berechtigten Administratoren dürfen Verzeichnisdienst-Sicherheitsparameter verändern. Die Verantwortlichkeiten der einzelnen Benutzer des Verzeichnisses sind weiter unten dargestellt.

**3. Festlegung von Namenskonventionen**

Um die Verwaltung des Verzeichnisbaums zu erleichtern, sollten Namenskonventionen festgelegt werden, damit eindeutige Namen für die Server, Applikationen, Drucker, Benutzer, Benutzergruppen und die weiteren Verzeichnisdienst-Objekte verwendet werden.

**4. Festlegung der Regeln für Benutzerkonten**

Vor der Einrichtung von Benutzerkonten sollten die Restriktionen, die für alle oder nur für bestimmte Konten gelten sollen, festgelegt werden.

Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Anmelde-Vorgänge. Außerdem sollte das Erstellen der Login-Skripts geregelt werden.

**5. Einrichtung von Gruppen**

Zur Vereinfachung der Administration sollten Benutzer-Objekte, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Benutzerrechte sowie Zugriffsrechte auf Verzeichnisobjekte und gegebenenfalls weitere vordefinierte Funktionen werden dann den Gruppen und nicht einzelnen Benutzer-Objekten zugeordnet. Die Benutzer-Objekte erben die Rechte und Berechtigungen der Gruppen, denen sie angehören. So ist es z. B. denkbar, alle Mitarbeiter einer Abteilung in einer Gruppe zusammenzufassen. Benutzerberechtigungen sollten nur dann einzelnen Benutzern zugewiesen werden, wenn dies ausnahmsweise unumgänglich ist.

**6. Festlegung der Vorgaben für Protokollierung**

Hierbei ist festzulegen, welche vom Verzeichnisdienst generierten Ereignisse zu protokollieren sind und bei welcher Ereigniskombination eine Benachrichtigung an die Administratoren zu erfolgen hat. Weiterhin muss entschieden werden, wie lange die gesammelten Ereignisdaten aufzubewahren sind.

**7. Regelungen zur Datenspeicherung**

Es ist festzulegen, wo Benutzerdaten gespeichert und wie diese geschützt werden (siehe M 2.138 *Strukturierte Datenhaltung*). Datenspeicherung auf den lokalen Festplatten der einzelnen Clients sollte nicht stattfinden. Die Frage nach der Datenspeicherung ist jedoch auf der Ebene einzelner Partitionen zu klären. Datenbestände sollten in Bezug auf ihren Schutzbedarf klassifiziert werden, und entsprechend sollte die Partitionierung des Verzeichnisses auf vertrauenswürdige und gesicherte Hosts vorgenommen werden. Dabei sind besonders die hochsensiblen Daten zu berücksichtigen.

**8. Einrichtung von Projektverzeichnissen**

Um eine saubere Trennung von benutzer- und projektspezifischen Daten (Objekten) untereinander durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, die eine solche Objekthaltung unterstützt.

**9. Vergabe der Zugriffsrechte**

Für die Objekte des Verzeichnisdienstes ist festzulegen, welche Attribute für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind.

**10. Verantwortlichkeiten der Administratoren und Benutzer im Client-Server-Netz**

Neben der Wahrnehmung der Netzmanagement-Aufgaben (siehe oben) müssen die Verantwortlichkeiten der einzelnen Administratoren im Verzeichnissystem festgelegt werden. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Verwaltung des Verzeichnisdienst-Baums oder einzelner Partitionen,
- die Verwaltung der Schemadefinition,
- die Verwaltung der Zertifizierungsstelle und der Schlüssel-Objekte,
- die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
- die Vergabe von Zugriffsrechten und

- das Hinterlegen und den Wechsel von Passwörtern und die Durchführung von Datensicherungen.

Auch die Benutzer müssen in einem Verzeichnisdienst mit Client-Zugriff bestimmte Verantwortlichkeiten übernehmen, insbesondere wenn ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In der Regel beschränkt sich dies jedoch auf den verantwortungsvollen Umgang mit den eigenen Passwörtern für den Verzeichnisdienst.

**11. Schulung**

Abschließend muss festgelegt werden, welche Benutzer zu welchen Teilaspekten geschult werden müssen. Erst nach ausreichender Schulung kann der Verzeichnisdienst in den Produktivbetrieb aufgenommen werden. Besonders die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit eines Verzeichnisdienstes gründlich zu schulen.

Die daraus entwickelten Sicherheitsrichtlinien sind zu dokumentieren und im erforderlichen Umfang den Benutzern des Verzeichnisdienstes mitzuteilen. Bei der Definition der Sicherheitsrichtlinie für Verzeichnisdienste ist zu beachten, dass sie sich an den vorhandenen Sicherheitsrichtlinien der Institution orientieren muss, diesen nicht widersprechen (Konsistenz) und auch nicht im Widerspruch zu geltendem Recht stehen darf. In der Regel werden mit einer Verzeichnisdienst-Sicherheitsrichtlinie existierende Regelungen spezifisch angepasst oder aber sinngemäß erweitert, z. B. durch zusätzliche Anforderungen für Komponenten. Dabei sind unter Umständen neue Regelungen für Verzeichnisdienst-spezifische Funktionalitäten zu treffen. Generell gilt, dass sich die Planung des Verzeichnisdienstes an den jeweiligen Sicherheitsrichtlinien orientiert, dabei jedoch auch Einfluss auf die Sicherheitsrichtlinien besitzt (Feedback-Prozess).

Prüffragen:

- Sind alle für den geplanten Einsatz von Verzeichnisdienst relevanten Bereiche durch die Sicherheitsrichtlinien abgedeckt?
- Sind alle Benutzer über die Verzeichnisdienst-Sicherheitsrichtlinien informiert?

# M 2.406 Geeignete Auswahl von Komponenten für Verzeichnisdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

In der Planungs- und Konzeptionsphase für einen Verzeichnisdienst wurden dessen Zweck und Einsatzszenarien definiert und Sicherheitsrichtlinien für den Einsatz festgelegt.

Nachdem die Anforderungen für den Einsatz eines Verzeichnisdienstes spezifiziert wurden, müssen geeignete Komponenten zu seiner Realisierung identifiziert werden. Dies gilt insbesondere für die zu beschaffende Software. Aber auch die dafür benötigte Hardware samt Betriebssystem sowie die Netz-Infrastruktur müssen den Anforderungen genügen.

**Auswahl der Software für den Verzeichnisdienst**

Software für Verzeichnisdienste wird von vielen Herstellern auf unterschiedlichen Plattformen angeboten. Es gibt kommerzielle Produkte, aber auch frei verfügbaren Varianten. Bekannte Verzeichnisdienste basieren heute praktisch alle auf dem LDAP-Standard. Einige Beispiele, ohne Wertung und Anspruch auf Vollständigkeit, sind:

- Active Directory in Microsoft Windows-2000-Server- oder Windows-Server-2003-Netzen
- eDirectory, ehemals NDS in Novell-Netzen
- Fedora Directory Server, unterstützt von Red Hat
- OpenLDAP (Open Source Software für diverse Betriebssysteme)
- Apple Open Directory in Mac OS X Server
- IBM Tivoli Directory Server
- Sun Java System Directory Server
- Network Information Service (NIS) in Unix-Netzen (nicht LDAP-basiert)

Verzeichnisdienste können sowohl bereits in ein Betriebssystem integriert sein, wie z. B. Active Directory in Windows Server ab Windows 2000, oder auch als eigenständige Software-Komponente für verschiedene Betriebssysteme, wie z. B. OpenLDAP, oder auf Java-Plattform, wie z. B. Sun Java System Directory Server, angeboten werden.

Ein wichtiges Kriterium bei der Beschaffung von Verzeichnisdienst-Software ist zunächst die Kompatibilität zu den Anwendungen, die gemäß der strategischen Entscheidung aus der Planungsphase den Verzeichnisdienst nutzen sollen. Hierbei sind insbesondere die Schnittstellen zu betrachten, die vom Verzeichnisdienst angeboten werden.

Der Standard LDAPv3 wird in seinem Kern von praktisch allen angebotenen Verzeichnisdiensten eingehalten. Produktspezifische Erweiterungen des LDAP-Standards sind jedoch möglich. Diese können sowohl funktionaler Natur sein als auch konkrete Sicherheitsmerkmale umfassen.

Werden LDAP-Erweiterungen benötigt, gilt es zu überprüfen, ob diese von der Verzeichnisdienst-Software auch bereitgestellt werden.

Darüber hinaus kann die Bereitstellung weiterer Schnittstellen ein Kriterium für die Beschaffung sein, wenn die effektive oder effiziente Nutzung des Ver-

zeichnisdienstes dadurch erst möglich wird. Beispiele für solche Schnittstellen eines Verzeichnisdienstes sind Extended Markup Language (XML), Directory Services Markup Language (DSML) und Simple Object Access Protocol (SOAP) sowie die proprietären Active Directory Service Interfaces (ADSI) und Novell Directory Access Protocol (NDAP).

Insgesamt sind die Anforderungen der Anwendungen und deren Benutzer an den Verzeichnisdienst zu ermitteln, um dessen Verfügbarkeit sicherzustellen. Je nach Anforderung ist beispielsweise sicherzustellen, dass der Verzeichnisdienst die Anzahl der Anfragen verarbeiten kann. Wenn auf Client-Seite hierzu weitere Komponenten erforderlich sind, müssen auch diese in den Prozess der Auswahl und Beschaffung einbezogen werden.

**Erfüllung der Sicherheitsanforderungen**

Im Rahmen der Planung und Konzeption des Verzeichnisdienstes wurden Anforderungen an dessen Sicherheit in Abhängigkeit vom Einsatzzweck formuliert. Folgende Fragestellungen sollten daher bei der Auswahl von Software-Komponenten zur Realisierung des Verzeichnisdienstes mindestens berücksichtigt werden:

- Können mit dem betrachteten Produkt die administrativen Aufgaben so delegiert oder verteilt werden, dass sie den Anforderungen, gegebenenfalls auch für zukünftige Planungen, genügen? Lassen sich die damit verbundenen Rechte der einzelnen Administrator-Gruppen so granular einstellen, dass sie auf die notwendigen Zugriffsrechte eingeschränkt werden können? Können die administrativen Tätigkeiten am Verzeichnisdienst angemessen hinsichtlich Vertraulichkeit und Integrität abgesichert werden?
- Werden ausreichend starke Mechanismen zur Authentisierung der Benutzer des Verzeichnisdienstes gemäß den Anforderungen der Institution zur Verfügung gestellt?
- Kann die Vertraulichkeit der Daten bei der Übertragung zwischen Standorten und zum Benutzer angemessen abgesichert werden?
- Bieten die Verzeichnisdienst-Komponenten genügend Unterstützung für den Fall, dass elektronische Zertifikate zur Authentisierung, Verschlüsselung, digitalen Signatur oder im Rahmen einer PKI benötigt werden?
- Ist, falls erforderlich, eine Multi-Master-Replikation des Verzeichnisdienstes möglich? Wird die Multi-Master-Replikation auf allen geforderten Ebenen durch die Verzeichnisdienst-Software unterstützt?
  Im Gegensatz zu einer Master-Slave-Installation existieren bei einer Multi-Master-Replikation mehrere Master-Server, die die Anfragen der Anwendungen bzw. deren Benutzer entgegennehmen und verarbeiten. Hierbei wird stets der Master-Server angesprochen, der dem Anfragenden am nächsten ist.
  Vor allem bei räumlich weit verteilten Verzeichnisdienst-Strukturen ist der Multi-Master-Betrieb empfehlenswert. In jedem Fall ist sicherzustellen, dass eine regelmäßige Replikation zwischen den Master- Servern stattfindet, da alle Master immer den vollen Datenbestand des Verzeichnisdienstes vorhalten müssen. Der Verwaltungsaufwand für einen Multi-Master-Betrieb ist daher höher.

**Schulung und weitere Unterstützung**

Für die sichere Installation, Konfiguration und Betrieb eines Verzeichnisdienstes muss eine ausreichende Kompetenz beim administrativen Personal vorhanden sein. Bei der Auswahl von Software-Produkten eines Verzeichnisdienstes ist daher zu beachten, ob für diese geeignete Schulungen vom Hersteller oder einem unabhängigen Anbieter angeboten werden.

Sollte es im laufenden Betrieb eines Verzeichnisdienstes zu komplexeren Problemen kommen, ist gegebenenfalls weitergehende Unterstützung durch den Hersteller oder einen Dritten erforderlich. Daher sollte bei der Beschaffung von Verzeichnisdienst-Komponenten an den Abschluss geeigneter Unterstützungsverträge bzw. Service Level Agreements (SLAs) gedacht werden.

Die notwendigen Schulungen und Unterstützungsleistungen müssen in die Kalkulation der Gesamtkosten für den Verzeichnisdienst einbezogen werden.

**Werkzeuge**

Für die Administration von Verzeichnisdiensten und die Verwaltung der Daten werden in der Regel eine Reihe von Werkzeugen angeboten. Bei der Auswahl eines Verzeichnisdienstes sollte also auch geklärt werden, ob es geeignete Werkzeuge gibt, um dessen Administration zu unterstützen. Außerdem ist zu hinterfragen, ob diese Werkzeuge die an sie gestellten Anforderungen erfüllen.

- Unterstützen die Werkzeuge die Verwaltung des Verzeichnisdienstes wie auch der Daten des Verzeichnisdienstes in ausreichendem Maße? Wird die Administration bei Installation, Konfiguration und Betrieb der Komplexität des Verzeichnisdienstes entsprechend angemessen unterstützt, um Fehler und Irrtümer weitestgehend zu vermeiden?
- Lassen sich die Schnittstellen und Zugänge zur Administration und Überwachung bei Verwendung dieser Werkzeuge ausreichend absichern?

**Skalierbarkeit**

Für die Verfügbarkeit des Verzeichnisdienstes ist auch die Leistungsfähigkeit der dahinter liegenden Datenbank von Bedeutung.

- Ist der Verzeichnisdienst hinreichend skalierbar? Kann der Verzeichnisdienst hinsichtlich seiner Strukturen und der Anzahl der möglichen Einträge auch noch zukünftigen Ansprüchen gerecht werden?

**Hardware**

Ist die für den Verzeichnisdienst vorgesehene Hardware oder das darauf laufende Betriebssystem bereits vorhanden oder aus anderen Gründen vorgegeben, so schränkt dies die Auswahl der geeigneten Software in aller Regel ein und ist zu berücksichtigen.

Wenn der Verzeichnisdienst andererseits in eine heterogene Landschaft von Hardware und Betriebssystemen zu integrieren ist, muss die Software des Verzeichnisdienstes dies unterstützen.

Für den Fall, dass Hardware und/oder Betriebssystem für den zu etablierenden Verzeichnisdienst neu zu beschaffen sind, müssen die Anforderungen hinsichtlich Leistung und Speicherplatz erfüllt werden, um letztlich die Verfügbarkeit des Verzeichnisdienstes und die Integrität seiner Daten zu gewährleisten (siehe auch M 2.317 *Beschaffungskriterien für einen Server*)

**Netze**

Entsprechendes gilt auch für die Netz-Infrastruktur. Sollen vorhandene Netze mit vorgegebenen Bandbreiten genutzt werden, müssen die Verzeichnisdienst-Komponenten so ausgewählt sein, dass die Netzlast bei Anfragen an den Verzeichnisdienst so verteilt werden kann, dass die Verfügbarkeit des Dienstes aufrecht erhalten bleibt.

Bei einer Neuplanung oder Erweiterung des Netzes müssen die Kommunikationsverbindungen so ausgelegt werden, dass sie den Anforderungen aus der Analyse des zu erwartenden Netzverkehrs mit dem Verzeichnisdienst gerecht werden können

Prüffragen:

- Existiert ein Kriterienkatalog, aufgrund dessen die Komponenten für den Verzeichnisdienst ausgewählt und beschafft werden?
- Wurden Sicherheitsanforderungen für die Komponenten des Verzeichnisdienstes gemäß ihres Einsatzzweckes formuliert?

# M 2.407 Planung der Administration von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Administration eines Verzeichnisdienstes erfordert eine sorgfältige Planung. Dabei sollte auf eine ausreichende Trennung der administrativen Aufgaben und der zugehörigen Administratorkonten geachtet werden. Grundsätzlich sollte die Verwaltung des Verzeichnisdienstes selbst von der Verwaltung der Daten im Verzeichnis getrennt werden, indem beispielsweise die administrativen Rollen Diensteverwaltung und Datenverwaltung mit unterschiedlichen Verantwortungsbereichen geschaffen werden.

Dienstadministratoren sollten sich um die Bereitstellung des gesamten Verzeichnisdienstes, verzeichnisweite Einstellungen, Installation und Wartung der Software sowie um die Installation des Betriebssystems auf den Verzeichnisdienst-Servern kümmern.

Datenadministratoren sollten hingegen für die Verwaltung der Daten zuständig sein, die im Verzeichnisdienst und damit auf den Servern des Verzeichnisdienstes gespeichert sind. Sie sollten den Verzeichnisdienst nicht konfigurieren und bereitstellen können. Datenadministratoren sollten außerdem möglichst nicht für die Gesamtheit aller Daten des Verzeichnisdienstes zuständig sein. Typischerweise verwalten sie eine Teilmenge der Objekte des Verzeichnisdienstes. Mit Hilfe von Einstellungen in den Access Control Lists für die im Verzeichnisdienst gespeicherten Objekte sollten zu diesem Zweck die Verwaltungsmöglichkeiten eines bestimmten Administratorkontos auf spezielle Bereiche des Verzeichnisdienstes beschränkt werden.

Einige Informationen, die zur Verwaltung oder Konfiguration des Verzeichnisdienstes erforderlich sind, werden von Objekten im Verzeichnisdienst selbst gesteuert. Obwohl diese Informationen, wie z. B. Vertrauensstellungen, Schemata oder Regeln zur Replikation, im Verzeichnisdienst gespeichert sind, sollten sie von den Dienstadministratoren verwaltet werden. Daher können Dienstadministratoren auch als Datenadministratoren fungieren, nicht jedoch umgekehrt.

Darüber hinaus kann auch ein weitergehendes administratives Modell für den Verzeichnisdienst geplant werden. Die Einrichtung einer Rollen-basierten Administration und die Möglichkeit der Delegation von Administrationsaufgaben beeinflussen die Sicherheit des Verzeichnisdienstes und verdienen daher eine besondere Beachtung. Bei sinnvoller, übersichtlicher und konsistenter Gestaltung der Sicherheitsadministration kann gleichzeitig auch eine erhöhte Transparenz und Effizienz geschaffen werden.

Im Rahmen der Planung der Administration von Verzeichnisdiensten müssen für jede Institution folgende Fragen beantwortet werden:

- Welche Administratorgruppen werden benötigt?
- Welches administrative Modell wird umgesetzt? Zentrale oder dezentrale Verwaltung?
- Welche administrativen Rollen sollen innerhalb der Baumstruktur existieren?
- Sollen administrative Aufgaben delegiert werden? An wen?
- Auf welche Objekte darf über die verschiedenen Verzeichnisdienst-Schnittstellen von welchen Administratoren zugegriffen werden?

Folgende sicherheitsrelevante Aspekte sollten bei der Planung der Verzeichnisdienst-Administration berücksichtigt werden:

- Eine Delegation wird durch die Vergabe von Zugriffsrechten auf die Verzeichnisdienst-Objekte und deren Attribute erreicht. Dabei wird in der Regel der Vererbungsmechanismus eingesetzt, um Berechtigungen auf Objekte in Teilbäumen zu verwalten. Komplexe Szenarien mit Delegation und damit Rechtevererbung sollten jedoch vermieden werden. Diese werden sonst sehr schnell unübersichtlich und sind kaum noch administrierbar, so dass leicht Sicherheitslücken durch Fehlkonfigurationen entstehen können.
- Standardmäßig ist im Allgemeinen bei der Erstinstallation eines Verzeichnisdienstes ein übergreifender Administrator angelegt, der auf alle Objekte des Verzeichnisdienstes volle Zugriffsrechte besitzt. Dies sollte bei der Erstinstallation geändert werden. Die Verteilung der Zugriffsrechte sollte gemäß dem zuvor festzulegenden administrativen Modell erfolgen.
- Im Fall der administrativen Delegation sollten nur die unbedingt notwendigen Rechte vergeben werden, die zur Ausübung der delegierten administrativen Tätigkeiten erforderlich sind.
- Der administrative Zugang zum ersten bzw. obersten Teil des Verzeichnisdienstes sollte aufgrund der weitreichenden Berechtigungen besonders geschützt werden. Bei entsprechend hohem Schutzbedarf ist zu überlegen, diesen Zugang nur im Vier-Augen-Prinzip, beispielsweise durch ein geteiltes Passwort, zu gewähren.
- Schema Änderungen sind überaus kritische Operationen und dürfen, wenn überhaupt, nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt werden. Sie müssen genau dokumentiert werden.
- Für den Fall, dass eine eigene Zertifizierungsstelle (Certification Authority, CA) in den Verzeichnisdienst eingebunden wird, ist deren Betrieb und Administration der zuvor aufgestellten Sicherheitsrichtlinie entsprechend zu planen.
- Die administrativen Tätigkeiten sollten so delegiert werden, dass sich möglichst keine Überschneidungen ergeben. Ansonsten könnten durch zwei Administratoren sich gegenseitig widersprechende Veränderungen durchgeführt werden, die dann zu Replikationskonflikten führen könnten. Durch ein Administrationsmodell mit überschneidungsfreien Zuständigkeiten kann die Gefahr von Replikationskonflikten verringert werden. Sind Replikationskonflikte zu erwarten oder bereits aufgetreten sollte in regelmäßigen Abständen und nach wichtigen Änderungen immer eine manuelle Überprüfung der Werte erfolgen.
- Das Modell der administrativen Delegation und die daraus resultierenden Rechtezuordnungen müssen dokumentiert werden.
- Für große Verzeichnisdienste sollte eine Werkzeug gestützte Verwaltung in Betracht gezogen werden. Für praktisch alle Verzeichnisdienste gibt es verschiedene kommerzielle und auch frei verfügbare Werkzeuge. Werden solche Werkzeuge verwendet, so müssen diese sicher konfiguriert und betrieben werden.

Prüffragen:

- Werden die administrativen Aufgaben für die Verwaltung des Verzeichnisdienstes selbst und für die Verwaltung der Daten strikt getrennt?
- Sind die Berechtigungen im administrativen Modell des Verzeichnisdienstes restriktiv und möglichst überschneidungsfrei?
- Sind alle administrativen Aufgabenbereiche und Berechtigungen ausreichend dokumentiert?

# M 2.408 Planung der Migration von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Oftmals wird ein Verzeichnisdienst nicht vollständig neu aufgebaut, sondern es existieren bereits einzelne Verzeichnisdienste im Institutionsnetz, die aber nur auf die Unterstützung bestimmter Anwendungen oder Fachverfahren abgestimmt sind oder ihren Dienst nur in einem Teilnetz zur Verfügung stellen. Letzteres trifft insbesondere zu, wenn ehemals autonome Teile einer Organisation in Folge von Zusammenlegungen zu einem Netz vereinigt werden. Die Migration eines Verzeichnisdienstes kann auch durch die Umstellung der Server-Landschaft auf eine neue Hardware, ein neues Betriebssystem oder durch den Wechsel von einer Betriebssystem-Version auf eine aktuellere begründet sein.

In jedem Fall erfordert die Migration von Verzeichnisdiensten eine sorgfältige Planung, da aufgrund der Umstellung Sicherheitslücken entstehen könnten.

- Die Integrität der Daten ist zu wahren. Die Daten der betroffenen Verzeichnisdienste dürfen keine unerwünschten Änderungen infolge der Migration erfahren. Soweit dies geplant ist, müssen alle Objekte der Verzeichnisdienste vollständig migriert werden.
- Die Vertraulichkeit der Daten ist zu gewährleisten. Es ist sicherzustellen, dass weder im Laufe der Migration noch nach deren Abschluss unautorisierte Zugriffe auf Daten erfolgen können.
- Letztlich ist als wesentlicher Bestandteil auch die Verfügbarkeit der Verzeichnisdienste während der Migration in erforderlichem Umfang aufrecht zu halten, bis der Verzeichnisdienst nach erfolgreicher Migration wieder in den normalen Betrieb übergeht.

Für die Migration eines Verzeichnisdienstes stehen verschiedene Migrationsverfahren zur Verfügung, die sich insbesondere im zusätzlichen Bedarf an Hardware unterscheiden:

- Aktualisierung des Verzeichnisdienstes: Bei dieser Umstellungsart wird ein Update des Verzeichnisdienstes auf die vorhandenen Rechner aufgespielt. Es ist keine zusätzliche Hardware notwendig. Nachteilig ist jedoch, dass der betroffene Rechner während der Umstellung nicht genutzt werden kann.
- Vollständige Neuinstallation: Die Migration geschieht durch einen parallelen Aufbau der Verzeichnisdienst-Infrastruktur. Nach Installation und Konfiguration geht der neue Verzeichnisdienst in den Wirkbetrieb über. Das existierende System wird dabei nicht beeinflusst und kann in dieser Zeit weiter genutzt werden. Allerdings entsteht bei dieser Variante ein hoher Bedarf an zusätzlicher Hardware.
- Rollende Migration: Diese Variante bietet sich an, wenn der Verzeichnisdienst in hierarchische Teilstrukturen (Partitionen) aufgeteilt ist. Für die jeweilige Partition wird zunächst eine parallele Struktur aufgebaut, die dann nach erfolgtem Aufbau genutzt wird.
  Die so frei gewordene Hardware kann anschließend für den parallelen Aufbau der nächsten Teilstruktur verwendet werden.

Eine generelle Empfehlung für eines der Verfahren zur Migration des Verzeichnisdienstes kann jedoch nicht gegeben werden, da das geeignete Verfahren stark von den jeweiligen Gegebenheiten abhängt und auf die Institution zugeschnitten werden muss.

Die Migration ist auch in zwei Phasen möglich. Zuerst werden die existierenden Verzeichnisdienst-Strukturen Eins-zu-Eins übernommen. Im eigentlichen Sinne wird dabei nur ein Update der Software bzw. des Betriebssystems auf den jeweiligen Verzeichnisdienst-Servern durchgeführt. Dies hat den Nachteil, dass Unzulänglichkeiten vielfach erhalten bleiben und eine Konfiguration des Verzeichnisdienstes unter Sicherheitsgesichtspunkten weiterhin erforderlich ist.

In einem zweiten Schritt erfolgt dann Restrukturierung des Verzeichnisdienstes. Dieses Vorgehen entspricht meist einem völligen Neuaufbau. Es bietet den Vorteil, dass hierbei alte und komplizierter administrierbare Strukturen durch neue ersetzt werden können. Außerdem lassen sich Veränderungen in der Organisation im Verzeichnisdienst entsprechend abbilden. Es ist dabei jedoch zu beachten, dass die Planung und Umsetzung der neuen Struktur meist mit großem Aufwand verbunden ist.

**Migrationskonzept**

Aufgrund der Komplexität der Migration eines Verzeichnisdienstes muss vorab ein entsprechendes Migrationskonzept erstellt werden. Dabei sollten insbesondere folgende Punkte berücksichtigt werden:

- Soll der Verzeichnisdienst im Rahmen der Migration in einer heterogenen Struktur mit verschiedenen Software-Versionen bzw. Betriebssystemen betrieben werden?
  Es sollte in diesem Fall festgelegt werden, ob dieser Mischbetrieb nur für einen definierten Übergangszeitraum oder dauerhaft aktiv sein soll. In einem Mischbetrieb ist darauf zu achten, dass die einzelnen Komponenten des Verzeichnisdienstes miteinander kompatibel sind, um die Verfügbarkeit zu gewährleisten. Weiterhin ist wichtig, dass die Sicherheitsmechanismen zur Authentisierung der Benutzer des Verzeichnisdienstes oder zur Sicherung der Vertraulichkeit und Integrität der Daten im Verzeichnis oder bei deren Abfrage ausreichend sind und den definierten Anforderungen an einen Verzeichnisdienst genügen.
- Sollen im Zuge der Migration auch Umstellungen auf Seiten der Clients durchgeführt werden?
  Je nach Umfang der Migration des Verzeichnisdienstes kann beispielsweise das Authentisierungsprotokoll der Clients gegenüber dem Verzeichnisdienst geändert werden. Um neue Sicherheitsmerkmale des Verzeichnisdienstes nutzen zu können, kann dabei eine Migration der Clients sogar erforderlich werden.
- Soll eine Änderung an der Partitionierung und der Replizierung des Verzeichnisdienstes vorgenommen werden?
  Für solche tiefgreifenden Änderungen ist eine bedarfsgerechte Planung des Restrukturierungsprozesses wesentlich, vor allem wenn eine Steigerung der Leistungsfähigkeit des Verzeichnisdienstes erreicht werden soll.

**Migration planen und dokumentieren**

Die Migration muss in ihren einzelnen Schritten möglichst detailliert geplant, der angestrebte Migrationsprozess dokumentiert und allen Beteiligten zugänglich gemacht werden. Im Überblick sind folgende Schritte im Rahmen des Migrationsprozesses durchzuführen:

- Es muss ein realistischer Zeitplan für die Migration erstellt werden. Im Laufe der Migrationsplanung muss mit Angleichungen des Zeitplanes gerechnet werden.

- Der Migrationsplan muss eine Strategie zur Umstellung der Verzeichnisdienst-Server festlegen (siehe auch Abschnitt *Aktualisierung, vollständige Neuinstallation, rollende Migration*).
- Die Reihenfolge, in der die Verzeichnisdienst-Server umgestellt werden sollen, muss festgelegt werden. Dabei ist die Rolle des Servers, der die Wurzel in der Verzeichnisdienst-Hierarchie bereitstellt, besonders zu berücksichtigen.
- Wenn die Migration gleichzeitig eine Umstellung der Client-Rechner umfassen soll, ist auch hier die Reihenfolge zu planen. Werden Clients vor Verzeichnisdienst-Servern umgestellt, sind in der Regel nach der Migration des Verzeichnisdienstes nochmalige Konfigurationsarbeiten an den Clients erforderlich. Andersherum ist auf die Kompatibilität der Clients mit dem Verzeichnisdienst zu achten, damit dessen Verfügbarkeit gewährleistet bleibt, aber trotzdem keine Sicherheitslücken entstehen.
- Stützt sich die Verwaltung von Benutzern und Benutzergruppen auf den Verzeichnisdienst, der migriert werden soll, so ist darauf zu achten, dass die Migration Einfluss auf die Zugriffsberechtigungen haben kann. Wenn durch die Migration die Authentisierungsattribute eines Benutzerkontos geändert werden, wie z. B. der Benutzername, ist sicherzustellen, dass die erlaubten Zugriffe weiterhin möglich sind. Andererseits muss verhindert werden, dass mit den alten Authentisierungsattributen weiter auf Ressourcen zugegriffen werden kann.
- Während der Migration ist darauf zu achten, dass die notwendigen Vertrauensstellungen zwischen verschiedenen Teilen des Verzeichnisdienstes korrekt erzeugt werden. Es ist zu planen, in welcher Phase der Migration welche Vertrauensbeziehungen bestehen sollen.
- Bei der Durchführung der Migration werden in der Regel diverse Migrationswerkzeuge eingesetzt. Vor der Migration muss daher auch der Werkzeugeinsatz geplant werden. Es ist festzulegen, welche Werkzeuge für welche Migrationsschritte zum Einsatz kommen sollen.
- Wenn zur Migration weitergehende Berechtigungen vergeben werden müssen, damit die benutzten Werkzeuge auf notwendige Informationen zugreifen können, ist zu beachten, dass dadurch potentielle Sicherheitslücken erzeugt werden können.
  Diese weitergehenden Berechtigungen sind daher sofort zu entziehen, nachdem sie nicht mehr benötigt werden. Ebenso empfiehlt es sich Zugriffe mit diesen Berechtigungen geeignet zu überwachen.
- Die für die Durchführung der Migration verantwortlichen Personen müssen benannt werden und mit ausreichenden Berechtigungen ausgestattet werden, die oft sehr weitreichend sind. Es ist daher in solchen Fällen darauf zu achten, dass nur vertrauenswürdige Personen mit diesen Aufgaben betraut werden. Im Migrationskonzept sollte außerdem festgelegt sein, welche Aufgaben nur im Vier-Augen-Prinzip erfolgen dürfen.
- In jeden Fall sollten für die Migration des Verzeichnisdienstes umfangreiche Analyse- und Test-Phasen eingeplant werden. Für die Tests selbst sollte ein isoliertes Test-Netz vorgesehen werden.
- Es sollte eine vollständige Datensicherung der Daten des Verzeichnisdienstes angefertigt werden, bevor die Migration beginnt.
- Es ist ein Notfallplan zu erstellen, der die Rückkehr zum Verzeichnisdienst im Zustand vor Beginn der Migration ermöglicht, so dass bei einem fehlgeschlagenen Migrationsversuch ein operatives System schnell wiederhergestellt werden kann.
- Nach Abschluss der Migration empfiehlt sich ein Soll-Ist-Vergleich aller Sicherheitseinstellungen, insbesondere der Zugriffsberechtigungen auf den Verzeichnisdienst und die dort abgelegten Daten.

**Meta-Verzeichnisdienst statt Migration**

Stellt sich bei der Planung zur Migration des Verzeichnisdienstes heraus, dass diese Migration zu aufwändig würde oder nicht innerhalb eines vorgegebenen Zeitrahmens zu realisieren wäre, kann der Einsatz eines sogenannten Meta-Verzeichnisdienstes in Betracht gezogen werden.

Ein Meta-Verzeichnisdienst dient dazu, die Daten von anderen, bereits existierenden Verzeichnisdiensten zusammenzufassen. Damit ist es möglich, mehrere unterschiedlich Verzeichnisdienste zu synchronisieren. Zur Realisierung gibt es verschiedene Ansätze:

- Das Meta-Verzeichnis stellt als Informationshändler alle angebundenen Verzeichnisse dar, als wäre es nur ein Verzeichnis. Es wird daher auch als virtuelles Verzeichnis bezeichnet. Der Meta-Verzeichnisdienst bietet lediglich eine einheitliche Sicht auf die zusammengefassten Informationen mehrerer angeschlossener Verzeichnisse, die weiterhin ihre eigenen Schemata und Namensräume benutzen können. Zu beachten ist, dass ein solches Meta-Verzeichnis auf die dauerhafte Existenz der angebundenen Verzeichnisse angewiesen ist und Kommunikationsverbindungen zu ihnen bereitgestellt werden müssen, die für die Zahl der Anfragen und zugehörigen Antworten geeignet sind.
- Ein Meta-Verzeichnisdienst, der als zentraler Informationsspeicher arbeitet, übernimmt die ausgewählten Informationen aus den angeschlossenen Verzeichnisdiensten in sein eigenes Verzeichnis. Es werden Metaobjekte erzeugt, welche die gesammelten Attribute der zugrunde liegenden Verzeichnisdienste umschließen.
  Um weiterhin eine Synchronisation zu ermöglichen, sind die Objekte des Meta-Verzeichnisdienstes mit den Ursprungsverzeichnissen assoziiert. Zu beachten ist, dass diese Synchronisation entweder ereignisgesteuert oder mit einer ausreichend hohen Synchronisationsfrequenz abläuft, damit die erforderliche Aktualität der Daten des Metaverzeichnisdienstes gewährleistet ist.

Die hier aufgeführten Aspekte dienen als Leitfaden für ähnliche und weitergehende Fragestellungen, die im Rahmen des Migrationskonzeptes adressiert werden müssen. Es ist zu beachten, dass ein Migrationsplan immer auf die konkrete Situation zugeschnitten sein muss und die jeweiligen lokalen Anforderungen an die Migration reflektiert.

Prüffragen:

- Existiert ein Konzept nach dem Verzeichnisdienst-Migrationen durchgeführt werden?
- Wurden die am Verzeichnisdienst vorgenommenen Schema-Änderungen dokumentiert?
- Wurden weitreichende Berechtigungen zur Durchführung der Migration des Verzeichnisdienstes nach deren Abschluss wieder zurückgesetzt?

# M 2.409 Planung der Partitionierung und Replikation im Verzeichnisdienst

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Ein skalierbarer Verzeichnisdienst bietet die Möglichkeit, Teile der Verzeichnisdatenbank in Partitionen zu zerlegen und auf verschiedene Verzeichnisdienst-Server zu verteilen. Dies verkürzt die mittleren Zugriffszeiten, da Suchabfragen sich unter Umständen nur auf eine spezielle Partition und nicht den gesamten Verzeichnisbaum erstrecken. Außerdem erhöht es die Ausfallsicherheit, da bei einem Serverausfall nur die dort befindliche Partition und nicht die gesamte Verzeichnisdatenbank betroffen ist. Weiterhin erlaubt es die Partitionierung, die Daten gemäß einer zuvor vorgenommenen Klassifizierung auf entsprechend gesicherte Server zu verteilen.

Bei der Planung der Partitionierung sind die vom Verzeichnisdienst definierten Regeln für Partitionen zu berücksichtigen. Partitionen können wiederum Unterpartitionen enthalten, welche ebenfalls gemäß den festgelegten Regeln gebildet werden müssen.

Neben dem Mechanismus der Partitionierung des Verzeichnisbaums bieten Verzeichnisdienste die Möglichkeit, Teile des Verzeichnisbaums auf andere Verzeichnisdienst-Server zu replizieren. In der Terminologie von Verzeichnisdiensten werden die replizierten Teilbereiche dabei als Repliken oder Reproduktionen bezeichnet. Bei der Planung der Replikation ist insbesondere eine Analyse des zu erwartenden Netzverkehrs zu machen, um hier die Erfordernisse an die Bandbreite der Kommunikationsverbindungen festzustellen oder bei vorgegebenen Netz-Parametern die Topologie der Repliken daran auszurichten.

Bei der Planung der Partitionen sollten folgende Punkte beachtet werden:

- **Berücksichtigung des Schutzbedarfs:** Die Informationen, die im Verzeichnis gehalten werden, sollten gemäß ihrem Schutzbedarf klassifiziert werden. Anhand dieser Klassifizierung sollte die Verteilung der Objekte auf entsprechend geschützte Server erfolgen. Dabei ist darauf zu achten, dass besonders Objekte mit schützenswerten Informationen wie beispielsweise kryptographischen Schlüsseln auf einem ausreichend abgesicherten Server gelagert werden.
- **Geforderte Verfügbarkeit des Verzeichnisdienstes:** Zur Verbesserung der Lastverteilung müssen hinreichend viele Repliken der Verzeichnisdaten auf Verzeichnisdienst-Servern angelegt werden.
- **Verteilung der Administrationsaufgaben:** Damit eine Rollentrennung der Administrationsaufgaben mit der Trennung der Datenhaltung einhergeht, sollten die Administrationsaufgaben auf einzelne Partitionen verteilt werden.
- **Verzeichnisdienst-Regeln zur Partitionierung**: Die Regeln zur Verzeichnisdienst-Partionierung müssen festgelegt und eingehalten werden. Die wesentlichen Regeln dabei sind:
  - Jede Partition beginnt hierarchisch mit einem einzelnen Container-Objekt.
  - Die Partition muss ein zusammenhängender Unterbaum (Sub-Tree) des Verzeichnisdienst-Baums sein.

- Verschiedene Partitionen dürfen sich nicht überschneiden.
- Der Name der Partition muss der Fully Qualified Distinguished Name (FQDN) des Wurzelobjekts der Partition sein.

Bei der Planung der Replikationen sind folgende Punkte zu berücksichtigen:

- Aus den Anforderungen an Verfügbarkeit und Ausfallsicherheit des Verzeichnisdienstes müssen die Vorgaben für die Anzahl der anzulegenden Replikationen abgeleitet werden.
- Die geforderte Systemperformance führt zur Planung der Lastverteilung.
- Es muss entschieden werden, ob durch die Definition von Filtern für Replikationen ein Sicherheitsgewinn erzielt werden kann.
  Dieser Sicherheitsgewinn liegt vor allem in der Möglichkeit einer getrennten Datenhaltung entsprechend einer zuvor vorgenommenen Klassifizierung der Daten. Es kann damit das Grundprinzip realisiert werden, dass jeder Verzeichnisdienst-Server nur diejenigen Daten hält, welche er "benötigt" (bzw. welche die zugreifenden Nutzer oder Applikationen benötigen). Bei unbedachter Konfiguration einer Replikation kann die Systemleistungsfähigkeit verringert werden. Sind gesuchte Daten auf einem Verzeichnisdienst-Server nicht vorhanden bzw. nicht sichtbar, weil sie durch entsprechende Filterregeln ausgeblendet sind, so wird im Hintergrund weitergesucht (sofern dies zugelassen ist). Eine nicht bedarfsgerechte Konfiguration der Filterregeln kann also die Leistungsfähigkeit des Systems negativ beeinflussen.

Die genauen Kontexte der Server, welche Partitionen bzw. Replikationen halten, beachtet werden. Ist die Struktur zu flach, so entsteht ein hoher interner Replizierungsaufwand. Darüber hinaus führen einzelne, momentan nicht verfügbare Server zu entsprechenden Statusmeldungen bei sämtlichen weiteren in diese Replizierung eingebundenen Verzeichnisdienst-Servern.

Prüffragen:

- Wurde bei der Partitionierung auf die Verfügbarkeit und den Schutzbedarf des Verzeichnisdienstes geachtet?
- Steht eine ausreichende Bandbreite zur Verfügung, um die Replikationen zeitgerecht auszuführen?

# M 2.410 Geregelte Außerbetriebnahme eines Verzeichnisdienstes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wird entschieden, einen Verzeichnisdienst nicht weiter zu betreiben, weil er beispielsweise durch eine neuere Version auf neuer Hardware abgelöst wird, so sind die nachfolgend beschriebenen Punkte zu beachten.

Die Außerbetriebnahme eines Verzeichnisdienstes ist sorgfältig zu planen und gewissenhaft durchzuführen, so dass beispielsweise berechtige Benutzer sich weiterhin anmelden können und der benötigte Zugriff auf Ressourcen im Netz sichergestellt ist und andererseits Daten und Rechte, die nicht mehr aufrecht erhalten werden sollen, sicher gelöscht bzw. dauerhaft entzogen werden.

Vor der Außerbetriebnahme ist zu überprüfen, ob eine Datensicherung des Verzeichnisdienstes verfügbar ist, mit deren Hilfe der Verzeichnisdienst wieder hergestellt werden kann, falls Probleme im Netz entstehen.

Dies betrifft auch verschlüsselte Daten, die auf anderen Rechnern im Netz der Institution gespeichert sind, aber deren relevante Schlüsselinformationen Bestandteil des Verzeichnisdienstes sind. Umfasst der Verzeichnisdienst eine Zertifizierungsstelle, sind möglicherweise kryptographische Schlüssel und Zertifikate von der Außerbetriebnahme betroffen. Dann ist zu überprüfen, ob eine explizite Sicherung des Schlüssel-Materials anzufertigen ist.

In dem Fall, in dem von dem auszusondernden Verzeichnisdienst Informationen bereitgestellt werden, die weiterhin für bestimmte Zwecke oder Anwendungen benötigt werden, muss dafür Sorge getragen werden, dass diese Informationen durch andere Quellen in ausreichendem Umfang zur Verfügung stehen.

### Löschen/Entsorgen der Speichermedien

Die Speichermedien aller betroffenen Rechner sind vor der Wiederverwendung sicher zu löschen (siehe M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*). Wird die Hardware entsorgt, so muss dies ebenfalls auf sichere Weise geschehen (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*).

### Partition aus dem Verzeichnisdienst löschen

Ist ein Verzeichnisdienst verteilt aufgebaut, halten einzelne Verzeichnisdienst-Server dabei oft nur einen Teil des gesamten Namensraums in einer Partition des Verzeichnisdienstes. Die anderen Teile des Verzeichnisdienstes verweisen mit Referenzen auf den auszusondernden Teil.

Bei der Außerbetriebnahme einer Partition des Verzeichnisdienstes muss darauf geachtet werden, dass keine anderen Partitionen in der Hierarchie des Verzeichnisdienstes unterhalb der der zu löschenden Partition vorhanden sind. Diese hätten dann ihren Bezug im Namensraum zu den übergeordneten Teilen des Verzeichnisdienstes verloren und wären somit völlig unbrauchbar.

Wird eine solche Partition oder der entsprechende Verzeichnisdienst-Server aus dem gesamten Verzeichnisdienst herausgenommen, müssen alle Refe-

renzen auf den ausgesonderten Teil in anderen Komponenten des Verzeichnisdienstes gelöscht oder angepasst werden. Dies betrifft unter anderem

- Verweise auf Objekte und ihre Attribute,
- Vertrauensstellungen,
- Indizes (Kataloge),
- Benutzerverwaltung,
- Systemüberwachung (Monitoring).

Es muss beachtet werden, dass dabei auch Referenzen in Verzeichnisdiensten externer Organisationen betroffen sein können. Im Rahmen der Planung der Außerbetriebnahme muss daher auch dafür gesorgt werden, dass entsprechende Anpassungen bei betroffenen externen Organisationen angestoßen werden.

Wenn die Partition, die außer Betrieb genommen werden soll, innerhalb des Verzeichnisdienstes eine ausgezeichnete Rolle innehatte, beispielsweise als Master oder Besitzer eines globalen Index, so muss diese Rolle zuvor auf einen anderen Teil des Verzeichnisdienstes übertragen werden, da ansonsten die Funktion des Verzeichnisdienstes nicht sichergestellt ist.

Prüffragen:

- Ist bei Außerbetriebnahme des Verzeichnisdienstes sichergestellt, dass weiterhin benötigte Rechte bzw. Informationen aus anderen Quellen zur Verfügung stehen, alle anderen aber gelöscht werden?
- Werden externe Nutzer darüber informiert, wenn ein Verzeichnisdienst außer Betrieb genommen werden soll?
- Wird bei der Außerbetriebnahme einzelner Partitionen eines Verzeichnisdienstes darauf geachtet, dass dadurch andere Partionen nicht beeinträchtigt werden?

# M 2.411 Trennung der Verwaltung von Diensten und Daten eines Active Directory

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die administrativen Tätigkeiten für Windows-Server-Betriebssysteme können grundsätzlich in die zwei Rollen "Diensteverwaltung" und "Datenverwaltung" mit unterschiedlichen Verantwortungsbereichen unterteilt werden.

Unter der "Diensteverwaltung" wird die Betreuung des Active-Directory-Dienstes selbst verstanden. Diensteadministratoren verwalten die Domänen-Controller, z. B. Einspielen von Updates auf Betriebssystemebene, und die Konfiguration des Active Directory, beispielsweise verzeichnisweite Einstellungen, wie Vertrauensstellungen oder Replikationsarchitektur.

Die Verwaltung der Daten im Active Directory bzw. auf den Mitgliedsrechnern der Active-Directory-Gesamtstruktur sollte von den Datenadministratoren durchgeführt werden. Dabei sollten die Datenadministratoren keine Veränderungen am Active-Directory-Dienst selbst, z. B. Änderungen an der Verzeichnisdienst-Replikation, durchführen dürfen. Mittels Zugriffskontrolllisten (Access Control Lists, ACLs) sollten die Berechtigungen soweit möglich auf einzelne Teilbereiche eingeschränkt werden.

Da Dienste-Administratoren für die Diensteverwaltung weitreichende Berechtigungen benötigen, sollten sie grundsätzlich auch administrative Tätigkeiten in Bezug auf die Datenverwaltung durchführen können. Umgekehrt sollten die Datenadministratoren jedoch nicht in der Lage sein, die Konfiguration des Active Directory zu ändern.

Um Missbrauch der administrativen Konten vorzubeugen, müssen die Benutzerkonten der oben genannten Rollen entsprechend abgesichert werden. Die hierzu erforderlichen Konfigurationen am Active Directory selbst sind in der Maßnahme M 4.318 *Umsetzung sicherer Verwaltungsmethoden für Active Directory* aufgeführt.

Prüffragen:

- Existiert eine Aufteilung der administrativen Benutzer bezüglich Diensteverwaltung und Datenverwaltung des Active Directory?

# M 2.412 Schutz der Authentisierung beim Einsatz von Active Directory

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Active Directory fungiert innerhalb des Netzes als zentrale Komponente. Um eine vertrauenswürdige Kommunikation zwischen den betroffenen Teilnehmern innerhalb des Netzes gewährleisten zu können, ist die Sicherheit und Zuverlässigkeit hinsichtlich der Authentisierung und Autorisierung beim Zugriff auf Netzressourcen erforderlich.

Um einen möglichst hohen Schutz der Active-Directory-Authentisierung zu erhalten, sollte die LAN-Manager-Authentisierung deaktiviert und der Server-Message-Block-Datenverkehr (SMB-Datenverkehr) zwischen Domänen-Controllern sowie zwischen Domänen-Controller und Computern der Domäne signiert werden. Ferner sollte der prä-Windows-2000-kompatible Zugriff deaktiviert, sowie die anonymen Zugriffe auf die Domänen-Controller eingeschränkt werden.

Ein hohes Maß an Sicherheit kann nur erreicht werden, wenn alle Domänen-Controller, Mitgliedsserver und Arbeitsstationen das Authentisierungsprotokoll NTLMv2 (NT LAN Manager Version 2) unterstützen. NTLMv2 steht standardmäßig ab Windows NT 4.0 SP4 zur Verfügung (siehe hierzu auch M 5.123 *Absicherung der Netzkommunikation unter Windows*). Ältere Authentisierungsprotokolle aus früheren Windows-Versionen bieten eine geringere Sicherheit. So werden beispielsweise bei dem LAN-Manager-Authentisierungsprotokoll (LM) die Kontokennwörter in einem unsicheren LM-Hashformat gespeichert. Die Kennwörter für das Windows-NT-Authentisierungsprotokoll NT LAN Manager (NTLM) und NT LAN Manager Version 2 (NTLMv2) werden im NTLM-Hashformat abgelegt. Der NTLM-Hash ist kryptografisch stärker als das LM-Hashformat.

Das SMB-Protokoll bildet die Grundlage für die Microsoft Datei- und Druckfreigabe sowie für viele andere Netzoperationen, wie z. B. die Remoteverwaltung von Windows. Um beispielsweise Man-in-the-Middle-Angriffe zu verhindern (siehe G 5.143 *Man-in-the-Middle-Angriff*), bei denen SMB-Pakete während der Übertragung geändert werden, unterstützt das SMB-Protokoll die digitale Signatur von SMB-Paketen.

Einige Betriebssysteme und Anwendungen, die für Windows-Betriebssysteme vor Windows 2000 entwickelt wurden, benötigen einen anonymen Zugriff auf andere Server und Domänen-Controller, z. B. setzt der Spooler-Dienst unter Windows NT 4.0 einen anonymen Zugriff auf Remotedrucker voraus. Auch werden anonyme Zugriffe für die Einrichtung von Vertrauensbeziehungen zwischen einer Windows-NT-4.0-Domäne und einer Windows-2000-Domäne benötigt. Für eine größtmögliche Sicherheit sollten anonyme Zugriffe auf Domänen-Controller sowie anonyme Zugriffe auf Active-Directory-Daten strikt unterbunden werden.

Diese Schritte können beim Einsatz von früheren Windows Client- und Server-Betriebssystemen, z. B. Windows 95, Windows 98, Windows Millennium Edition und Windows NT 4.0, zu Störungen im Betrieb des Netzes führen, da diese die oben genannten Schutzmaßnahmen nicht oder nur eingeschränkt unterstützen. Daher ist es aus Gründen der Verfügbarkeit nicht immer mög-

lich, die unsichere LAN-Manager-Authentisierung zu deaktivieren, den SMB-Datenverkehr zu signieren und anonyme Zugriffe auf Domänen-Controller zu unterbinden. In solchen Fällen sollten die entsprechenden Anforderungen von Diensten und Programmen, die für ihre Funktionen anonymen Zugriff benötigen, gegen die Sicherheitsvorteile abgewogen werden. Die getroffenen Entscheidungen müssen inklusive verbleibender Restrisiken dokumentiert und vom Leiter IT unterschrieben werden.

Sofern die Serverumgebung verschiedene Windows-Betriebssysteme umfasst, müssen die in Maßnahme M 4.314 *Sichere Richtlinieneinstellungen für Domänen und Domänen-Controller* beschriebenen Sicherheitsempfehlungen angepasst werden, so dass sie mit den früheren Versionen von Windows kompatibel sind.

Prüffragen:

- Wird in der Umgebung des Active Directory konsequent das Authentisierungsprotokoll NTLMv2 eingesetzt?
- Wurde die LAN-Manager-Authentisierung deaktiviert und wird der SMB-Datenverkehr signiert?
- Werden anonyme Zugriffe auf Domänen-Controller unterbunden?

# M 2.413 Sicherer Einsatz von DNS für Active Directory

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine Active-Directory-Installation besteht üblicherweise aus mehreren Servern mit unterschiedlichen Verzeichnispartitionen. Damit der Zugriff sowohl für die Clients als auch der Zugriff zwischen den Servern, z. B. bei der Replikation, erleichtert wird, verwendet Active Directory DNS (Domain Name System) für die Suche nach Active-Directory-Servern. Somit muss der DNS-Dienst als eine Grundlage des Active Directory angesehen werden.

Um die Integrität und Verfügbarkeit des Active Directory sicherzustellen, ist dafür Sorge zu tragen, dass DNS-Clientabfragen nicht durch unautorisierte Systeme im Netz fehlgeleitet werden können. In Windows-Umgebungen sollte der Schutz der DNS-Daten durch in Active Directory integrierte DNS-Zonen auf den Domänen-Controllern erhöht werden. Dabei werden die zonenspezifischen DNS-Daten in dem Container "MicrosoftDNS" des Active Directory gespeichert.

Die Konfigurationsdaten für in Active Directory integrierte DNS-Zonen werden in der Windows-Registry abgelegt. Der Zugriff auf die Konfigurationsdaten sollte nur auf administrative Konten beschränkt werden.

Im Folgenden wird ausschließlich auf in Active Directory integrierte DNS-Zonen und damit auf die Windows Server spezifischen Eigenschaften zur Unterstützung des sicheren Betriebs von Active Directory eingegangen. Darüber hinausgehende, allgemeine Maßnahmen zur Absicherung von DNS werden hier nicht beschrieben.

Zum Schutz der DNS-Infrastruktur sollten die DNS-Server geschützt werden sowie auf den DNS-Servern gespeicherte DNS-Daten ausreichend abgesichert werden und die Integrität der DNS-Antworten auf die Client-Anfragen bei der Übertragung gesichert werden. Wie dies umgesetzt werden kann, wird im Folgenden beschrieben.

Um die Integrität der auf dem Domänen-Controller zwischengespeicherten DNS-Daten zu gewährleisten, muss die Option "Zwischenspeicher vor Beschädigungen sichern" für den DNS-Server-Prozess aktiviert werden. Damit soll sichergestellt werden, dass ausschließlich autorisierte DNS-Einträge im Zwischenspeicher eingefügt werden können.

Der Zugriff auf den DNS-Dienst der Domänen-Controller sollte so weit wie möglich eingeschränkt werden. Dies kann z. B. dadurch erreicht werden, dass an den Sicherheitsgateways zwischen zwei Netzsegmenten der DNS-Dienst (UDP-Port 53) eingeschränkt wird. Der DNS-Dienst muss dabei für folgende Komponenten verfügbar sein:

- zwischen den DNS-Clients und dem entsprechenden DNS-Server,
- zwischen DNS-Servern, die Zonentransfers durchführen,
- zwischen DNS-Servern, die Client-Anfragen an die entsprechenden Zonen delegieren, und den für die jeweilige Zone verantwortlichen DNS-Servern,
- zwischen DNS-Servern, die Client-Anfragen weiterleiten und den DNS-Servern der übergeordneten Hierarchieebene.

Des Weiteren sollten die Netzaktivitäten in Bezug auf DNS-Anfragen überwacht werden, da ein ungewöhnlich hohes Aufkommen an DNS-Anfragen auf einen Denial-of-Service-Angriff (DoS-Angriff) gegen einen DNS-Server und damit unter Umständen auch gegen einen Domänen-Controller hindeuten kann. In diesem Falle sollte der Angreifer möglichst schnell identifiziert und entsprechende Gegenmaßnahmen eingeleitet werden (siehe auch M 6.106 *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes*).

Mittels IPsec (Internet Protocol Security) kann die Vertraulichkeit, Authentizität und Integrität des IP-Datenverkehrs im Netz sichergestellt werden. Bei einem IPsec-Verbindungsaufbau authentisieren sich Client und Server gegenseitig, so dass die Authentizität der Daten vom DNS-Client überprüft werden kann.

Die Integrität der DNS-Daten bei der Übertragung kann durch IPsec bei der Verwendung von Authentication Header (AH) bzw. durch Encapsulating Security Payload (ESP) sichergestellt werden.

Im Gegensatz zum Authentication Header des IPsec wird bei der Verwendung von ESP der Datenverkehr zusätzlich verschlüsselt. Durch ESP ist ebenfalls die Vertraulichkeit der DNS-Daten sichergestellt. ESP sollte daher verwendet werden.

Durch die Verwendung von IPSec erhöht sich das Datenaufkommen. Daher sollte vor dem Einsatz von IPsec sichergestellt werden, dass ausreichend Ressourcen vorhanden sind, damit bei aktivierter Verschlüsselung bzw. Signierung ein ausreichender Datendurchsatz im Netz möglich ist.

**Ausreichende Absicherung der gespeicherten DNS-Daten**

Für den Schutz der DNS-Daten auf dem Server sollten folgende Punkte berücksichtigt werden:

- Bei Windows-Server-Betriebssystemen wird ein DNS-Server mitgeliefert. Wird dieser verwendet, muss er so konfiguriert werden, dass nur Registrierungsanforderungen von autorisierten Clients der Active-Directory-Gesamtstruktur verarbeitet werden. Falls er nicht verwendet wird, ist er zu deaktivieren.
- Wird ein DNS-Server eines anderen Herstellers verwendet, so ist darauf zu achten, dass dieser die sichere dynamische Aktualisierung der DNS-Daten unterstützt und entsprechend konfiguriert wurde.
- Der Zugriff von Benutzern auf die DNS-Daten im entsprechenden Active-Directory-Container "MicrosoftDNS" sollte über ACLs so eingerichtet werden, dass nur Administratoren, Domänen-Administratoren, Organisations-Administratoren und DNS-Administratoren Vollzugriff auf die Domänendaten besitzen.
- Die Administration der DNS-Server und damit auch der DNS-Daten ist ebenso kritisch wie die Konfiguration des Active Directory.
  Daher ist bei der Vergabe der Administratorberechtigungen in gleicher Art und Weise vorzugehen wie bei der Vergabe der Berechtigungen für die Dienste-Administratorkonten (siehe M 2.411 *Trennung der Verwaltung von Diensten und Daten eines Active Directory*)
- Die Informationen sekundärer DNS-Zonen werden auf einem Domänen-Controller nicht im Active Directory, sondern in einer textbasierten Zonendatei gespeichert. Wenn möglich sollte auf eine verteilte DNS-Struktur zurückgegriffen werden, bei der jeder DNS-Server nur eine Zone verwaltet und entsprechende Client-Anfragen von den anderen Servern an den verantwortlichen DNS-Server weitergeleitet werden.

Können sekundäre DNS-Zonen auf diese Weise nicht vermieden werden, z. B. aufgrund des erhöhten Datenvolumens, so muss die Zonen-Datei mittels NTFS-Berechtigungen vor unbefugten Zugriffen geschützt werden. Lediglich die allgemeinen Administratoren, Domänen-Administratoren, Organisations-Administratoren und DNS-Administratoren sollten Vollzugriff auf die sekundären Domänen-Daten erhalten.

Weiterführende Informationen zur Konfiguration von DNS-Servern finden sich online in den Dokumenten "Best Practice Active Directory Design for Managing Windows Networks" und "Best Practice Active Directory Deployment for Managing Windows Networks" im Microsoft TechNet (http://technet.microsoft.com).

Prüffragen:

- Werden integrierte DNS-Zonen bzw. die sichere dynamische Aktualisierung der DNS-Daten verwendet, um DNS-Clientabfragen durch unautorisierte Systeme zu vermeiden?
- Ist der Zugriff auf die Konfigurationsdaten des DNS-Servers nur von administrativen Konten erlaubt?
- Ist der DNS-Cache auf DNS-Servern gegen unberechtigte Änderungen geschützt?
- Wird der Zugriff auf den DNS-Dienst der Domänen-Controller (z. B. am Sicherheitsgateway) auf das notwendige Maß beschränkt?
- Werden die Netzaktivitäten in Bezug auf DNS-Anfragen überwacht?
- Einsatz von IPSec zur Absicherung der DNS-Kommunikation: Ist ein ausreichender Datendurchsatz im Netz gewährleistet?
- Ist der Zugriff auf die DNS-Daten im Active Directory mittels ACLs auf Administratoren beschränkt?
- Werden sekundäre DNS-Zonen vermieden oder zumindest die Zonen-Datei vor unbefugtem Zugriff geschützt?

# M 2.414 Computer-Viren-Schutz für Domänen-Controller

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für einen ausreichenden Schutz gegen Computer-Viren und andere Schadprogramme muss in einer Institution ein umfassendes Computer-Viren-Schutzkonzept umgesetzt werden. Die entsprechende Vorgehensweise wird im Baustein B 1.6 *Schutz vor Schadprogrammen* beschrieben. In dem Computer-Viren-Schutzkonzept sollten grundsätzlich auch die Domänen-Controller einer Institution berücksichtigt werden.

Damit die Nutzung eines Viren-Schutzprogramms auf einem Domänen-Controller keine negativen Auswirkungen auf den laufenden Betrieb hat, sind jedoch für Domänen-Controller einige Besonderheiten zu beachten.

Die Hinweise in dieser Maßnahme sind als allgemeine Hinweise zu verstehen. Unter Umständen müssen zusätzlich die speziellen Anweisungen des Herstellers des jeweils eingesetzten Viren-Schutzprogramms berücksichtigt werden.

Bei der Auswahl der Viren-Schutz-Software muss darauf geachtet werden, dass der Einsatz auf einem Domänen-Controller explizit unterstützt wird. Entscheidend ist dabei, dass die Viren-Schutz-Software die vom Betriebssystem-Hersteller vorgesehenen Programmierschnittstellen (Application Programming Interface, API) verwendet.

Bei der Verwendung falscher Programmierschnittstellen werden unter Umständen die Metadaten der untersuchten Dateien durch den Zugriff der Viren-Schutz-Software verändert. In diesem Fall ist es möglich, das der File Replication Service (FRS) des Betriebssystems eine Replizierung der vermeintlich geänderten Datei innerhalb der Organisation veranlasst. Solche unnötigen Replizierungen können zu einer verminderten Systemleistung führen und sollten daher vermieden werden. Weitere Details bezüglich kompatibler Viren-Schutzprogramme sind im Microsoft-Knowledge-Base-Artikel mit der Artikel-ID 815263 zu finden.

Die korrekte Funktionsweise der Viren-Schutz-Software sollte in einer Testumgebung vor dem endgültigen Einsatz in einer Produktivumgebung ausgiebig auf korrekte Funktionalität getestet werden. Die Testumgebung sollte dabei den Gegebenheiten der Produktivumgebung möglichst nachempfunden werden, um Auswirkungen auf die Gesamtleistung des Domänen-Controllers festzustellen.

Um die Einführung von Schadsoftware zu vermeiden, sollte auf Domänen-Controllern ausschließlich die Active-Directory-Funktionalität des Betriebssystems verwendet und möglichst keine weiteren Dienste angeboten werden. Insbesondere darf ein Domänen-Controller nicht als herkömmlicher Arbeitsplatz genutzt werden. So sollten lokal auf einem Domänen-Controller angemeldete Benutzer nicht in der Lage sein, im Internet zu surfen, E-Mails zu empfangen oder auf externe Datenträger, wie z. B. USB-Speichermedien oder DVD-ROMs, zuzugreifen.

Ebenso sollte der Domänen-Controller nicht als Dateifreigabe-Server genutzt werden. Werden auf dem Domänen-Controller Dateien per Dateifreigaben im Netz verfügbar gemacht, so werden diese Dateien vom Viren-Schutzprogramm bei jedem Zugriff auf Schadsoftware untersucht, was zu Performan-

ce-Einbußen auf dem Domänen-Controller führen kann. Dateifreigaben auf dem Domänen-Controller sollten somit deaktiviert werden.

Grundsätzlich sollte das Viren-Schutzprogramm alle Dateizugriffe transparent im Hintergrund überwachen. Allerdings existieren auf den Windows-Server-Betriebssystemen einige Dateien, z. B. Verzeichnisdienst-Datenbank, Protokolldateien, Datenbank des Dateireplikationsdienstes, die bei einem Zugriff durch ein Viren-Schutzprogramm die Funktionen des Domänen-Controllers beeinträchtigen können. Um unnötige Dateisperrungen durch das Viren-Schutzprogramm zu verhindern und den einwandfreien Betrieb des Domänen-Controllers sicherzustellen, sollten daher die folgenden Punkte beachtet werden.

**Zugriff auf die Active Directory-Datenbank und Protokolldateien durch die Extensible Storage Engine (ESE)**

Die Verzeichnisdienst-Datenbank und Protokolldateien werden vom Active Directory mittels ESE für den exklusiven Dateizugriff geöffnet. Daher kann die ESE nur auf die Dateien zugreifen, die nicht durch die Viren-Schutz-Software blockiert werden. Gleichzeitig kann die Viren-Schutz-Software nur auf die Dateien zugreifen, die nicht durch die ESE blockiert werden.

Sowohl die Datenbankdateien als auch die Protokolldateien verwenden Active-Directory-interne Prüfsummen, die durch den Dateizugriff eines Viren-Schutzprogramms ungültig werden und zu inkonsistenten Datenbanken führen können. Eine inkonsistente Datenbank kann zu einem Ausfall des Active Directory führen.

Daher sind folgende Dateien aus der regelmäßigen Virenüberprüfung auszuschließen:

- Active-Directory Hauptdatenbank
- Active-Directory Transaktionsprotokolldateien
- Active-Directory Arbeitsordner

**Zugriff auf die Datenbank und Protokolldateien des Dateireplikationsdienstes (FRS) durch ESE**

Wie bereits beschrieben, können durch den unsachgemäßen Einsatz von Viren-Schutzprogrammen bei Datenbank- oder Protokolldateizugriffen konkurrierende Zugriffe des Replikationsdienstes auftreten. Ebenso kann eine Änderung der internen Prüfsummen dieser Dateien zu einem Ausfall des Active Directory führen. Daher sollten folgende Dateien aus der regelmäßigen Virenüberprüfung ausgeschlossen werden:

- Dateien im Arbeitsordner des Dateireplikationsdienstes
- Datenbankprotokolldateien des Dateireplikationsdienstes
- Staging-Ordner (Cache für neue und geänderte Dateien, die repliziert werden sollen) und Stammreplikat (Kopie des Distributed-File-System-Stamms und dessen untergeordnete Verknüpfungen) des Dateireplikationsdienstes
- Vorinstallationsordner des Dateireplikationsdienstes

Wird der Dateireplikationsdienst verwendet, um Windows-Freigaben zu replizieren, deren Verknüpfungsziel auf Windows Server Betriebssystemen liegt, so sind diese Dateien der SYSVOL-Ordner ebenfalls auszuschließen

**Dateireplikation durch den Dateireplikationsdienst (File Replication Service, FRS)**

Der Dateireplikationsdienst wird von den Windows-Server-Betriebssystemen für die Replizierung von Anmeldeskripten und Systemrichtlinien des SYSVOL-Ordners zwischen Domänen-Controllern verwendet. Werden die Metadaten (Sicherheitsinformationen oder Zeitstempel) einer Datei durch ein Viren-Schutzprogramm verändert, so wird die entsprechende Datei durch FRS zwischen den Domänen-Controllern erneut repliziert. Dieses Verhalten führt zu einer erhöhten Replizierung der SYSVOL-Dateien und damit zu

- einem erhöhten Bandbreitenverbrauch im Netz,
- einem erhöhten Ressourcenverbrauch auf den Domänen-Controllern und
- einer hohen Anzahl von Dateien im Staging-Ordner (dies gilt insbesondere für die Betriebssysteme Windows Server 2003 und Windows 2000 Server SP 3).

Um eine übermäßige Replikation zu verhindern, sollten folgende Punkte beachtet werden:

- Es ist ein Viren-Schutzprogramm auszuwählen, das die Metadaten der SYSVOL-Dateien nicht ändert.
- Sollte eine entsprechende Auswahl nicht möglich sein, so ist das SYSVOL-Verzeichnis inklusive aller Unterverzeichnisse aus der automatischen Überprüfung durch das Viren-Schutzprogramm zu entfernen. Dabei erhöht sich allerdings das Risiko für einen Virenbefall, da anders als bei den oben genannten Dateien in diesem Falle ausführbare Dateien, z. B. Anmeldeskripte, von der Viren-Schutz-Software nicht mehr erfasst werden. Daher sollten für den Fall, das die SYSVOL-Verzeichnisse nicht durch das Viren-Schutzprogramm abgesichert werden können, ausschließlich signierte Anmeldeskripte auf den Domänen-Controllern und Arbeitsstationen der Administratoren verwendet werden.

**Update-Funktion des Microsoft Betriebssystems**

Im Rahmen der Update-Funktion des Windows-Server-Betriebssystems ("Microsoft Update", "Windows Update" oder "Automatisches Update") kann das exklusive Zugriffsrecht für Dateien eines Viren-Schutzprogramms zu Problemen führen.

Um diese Probleme zu vermeiden, sollten folgende Dateien aus der regelmäßigen Virenüberprüfung ausgeschlossen werden:

- Datenbankdateien mit Bezug auf die Update-Funktionalität, wie z. B. im Ordner %windir%\SoftwareDistribution\Datastore die Datei "Datastore.edb"
- die im Ordner %windir%\SoftwareDistribution\Datastore\Logs abgelegten Transaktionsprotokolldateien

Weitere Details zu den auszuschließenden Dateien finden sich online im Dokument *Managing Domain Controllers* im Microsoft Windows Server TechCenter und im Microsoft-Knowledge-Base-Artikel mit der Artikel-ID 822158, welcher Empfehlungen für die Suche nach Viren auf einem Windows Server 2003-, Windows 2000- oder Windows XP-Computer beschreibt.

Hinweise zur Einführung von Skriptsignaturen können den Hilfsmitteln zum IT-Grundschutz (siehe *Virenprüfung durch Einführung von Skriptsignaturen* in *Hilfsmittel zum Baustein Active Directory*) entnommen werden.

Prüffragen:

- Werden die Domänen-Controller im Computer-Viren-Schutzkonzept berücksichtigt?
- Ist die eingesetzte Viren-Schutz-Software vom Hersteller für den Einsatz auf Domänen-Controllern freigegeben?
- Wurde die Viren-Schutz-Software vor dem produktiven Einsatz auf dem Domänen-Controller in einer Testumgebung ausreichend getestet?
- Werden Dateien, die bei Zugriff durch die Viren-Schutz-Software die Funktion des Domänen-Controllers beeinträchtigen können, (z. B. Datenbanken und Protokolldateien von Verzeichnisdienst und Dateireplikationsdienst) von der Viren-Prüfung ausgenommen?
- Werden Dateien, die von der Prüfung durch die Viren-Schutz-Software ausgenommen sind, ausreichend gegen Virenangriffe geschützt?

# M 2.415 Durchführung einer VPN-Anforderungsanalyse

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bevor eine VPN-Verbindung zwischen einzelnen IT-Systemen, verschiedenen Standorten einer Institution oder auch zu Kunden eingerichtet wird, sollte eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hardware- und Software-Komponenten abzuleiten. Durch das Aufstellen und Durchspielen von Nutzungsszenarien können spezielle Anforderungen an die VPN-Architektur oder die VPN-Komponenten aufgedeckt werden.

Im Rahmen dieser Anforderungsanalyse sind unter anderem folgende Punkte zu beachten:

- Festlegung der Geschäftsprozesse:
  Als erstes muss geklärt werden, für welche Geschäftsprozesse das Virtuelle Private Netz (VPN) genutzt und welche Informationen darüber kommuniziert werden sollen. Aus den Ergebnissen müssen die benötigten Anforderungen ermittelt und gemäß ihrer Bedeutung für das Unternehmen oder die Behörde priorisiert werden. Neben den Geschäftsprozessen müssen auch die Anwendungen, die die jeweiligen Prozesse unterstützen, betrachtet werden. Hierbei muss auch erfasst werden, welche der betroffenen Anwendungen zeitkritisch oder bandbreitenintensiv sind.
- Festlegung der Anwendungszwecke:
  Es gibt viele unterschiedliche Nutzungsszenarien für VPNs, wie die Durchführung von Fernwartungstätigkeiten, die Anbindung einzelner Mitarbeiter oder ganzer Standorte. Daher muss geklärt werden, welche Einsatzzwecke unterstützt werden sollen und welche VPN-Typen dafür eingesetzt werden (z. B. Site-to-Site-, End-to-End- und End-to-Site-VPNs).
- Festlegung der Benutzer:
  Es ist zu klären, welche Arten von Benutzern mit welchen Berechtigungen und welchen Vorkenntnissen das VPN nutzen sollen (z. B. Außendienstmitarbeiter, Mitarbeiter auf Dienstreise, Mitarbeiter einer Zweigstelle). Dabei ist auch zu klären, wie diese sicher identifiziert und authentisiert werden sollen.
- Regelung von Zuständigkeiten:
  Auch VPN-Komponenten müssen durch fachkundiges Personal administriert und gewartet werden. Bei der Durchführung einer VPN-Anforderungsanalyse sollte daher festgelegt werden, wer für die Administration und den Betrieb des VPNs zuständig ist - und zwar auf beiden Seiten des VPNs. Im Weiteren muss geklärt werden, wer zu benachrichtigen ist, wenn das VPN ausfällt oder wenn Anzeichen für einen Sicherheitsvorfall entdeckt werden. Hierfür muss Fachpersonal vorhanden sein, das über entsprechendes Wissen verfügt.
- Vertraulichkeit und Integrität:
  Je nach Schutzbedarf bezüglich der Vertraulichkeit und Integrität werden häufig besondere Anforderungen an das VPN gestellt, die im Allgemeinen durch zusätzliche Sicherheitsmaßnahmen abgedeckt werden können. In vielen Fällen existieren hierzu übergeordnete Regelungen oder Richtlinien, die bei der Beschaffung und beim Betrieb von VPN-Komponenten berücksichtigt werden müssen. Um Informationen mit hohem Schutzbedarf bezüglich Vertraulichkeit und/oder Integrität zu übertragen, empfiehlt es

sich, gemäß den Common Criteria zertifizierte VPN-Komponenten einzusetzen (siehe auch M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*). Ein Beispiel für zertifizierte VPN-Komponenten ist die SINA-Produktfamilie (Sichere Inter-Netzwerk-Architektur). Neben reinen Krypto-Gateways (SINA-Box) zum Aufbau von VPN-Verbindungen umfasst die SINA-Produktfamilie auch Endsysteme mit integrierten Kryptofunktionen (SINA-Client) sowie ein Managementsystem.

- Verfügbarkeit:
  Besonders bei einer Standortvernetzung wird häufig gewünscht, dass zu jeder Zeit ausreichend schnell Informationen über das VPN ausgetauscht werden können. Besitzen die betroffenen Anwendungen einen höheren Schutzbedarf bezüglich der Verfügbarkeit, sollte dies bei der Anforderungsanalyse berücksichtigt werden. Erhöhte Anforderungen an die Verfügbarkeit lassen sich bei VPNs nicht immer durch technische Sicherheitsmaßnahmen abdecken, da VPNs oft über Netze aufgebaut werden, die nicht unter der eigenen Kontrolle stehen und somit nicht beeinflusst werden können.
- Beschränkung der Netze:
  Mit VPNs können verschiedene Netze durch Nutzung einer sicheren Verbindung zu einem logischen Netz zusammengefasst werden. Je nach Konfiguration können dadurch alle IT-Systeme eines Netzes auf alle IT-Systeme oder nur auf bestimmte IT-Systeme der anderen Netze zugreifen. Bei der VPN-Anforderungsanalyse sollte entschieden werden, von wo über das jeweilige VPN auf welches Netz und auf welche IT-Systeme zugegriffen werden darf.
- Auswahl der genutzten Applikationen und -protokolle:
  Über ein VPN können unterschiedliche Arten von Informationen versendet und empfangen werden. Beispielsweise können E-Mails übertragen, Dateien kopiert oder auf einen Webserver zugegriffen werden. Neben diesen klassischen Diensten kann auch auf einem Terminalserver gearbeitet oder über VoIP telefoniert werden. Es sollte daher festgelegt werden, welche Applikationen über ein VPN genutzt werden dürfen und welche nicht. Es muss nicht nur entschieden werden, welche Applikationen eingesetzt werden dürfen, sondern auch die Protokolle, mit denen die Informationen übertragen werden können. Beispielsweise kann festgelegt werden, dass Netzfreigaben nur über SMB statt NFS eingebunden werden dürfen.
- Bandbreite und Verzögerung:
  Ein VPN ermöglicht es, auf Applikationen in einem entfernten Netz zuzugreifen. Da VPN-Verbindungen oft über ein WAN aufgebaut werden, müssen für zeitkritische Anwendungen spezielle Voraussetzungen berücksichtigt werden, besonders im Hinblick auf die verfügbare Bandbreite und Verzögerungen bei der Übertragung. Dies betrifft beispielsweise Zugriffe auf Terminalserver oder die Telefonie über VoIP. Für die VPN-Anforderungsanalyse sollten die benötigten Bandbreiten, die zulässige Verzögerung sowie gegebenenfalls weitere Qualitätsmerkmale des Netzes berücksichtigt werden.
- Geographische Beschränkungen:
  Ein VPN kann dazu dienen, dass sich mobile Mitarbeiter von beliebigen Orten unterwegs ins Institutions-LAN einwählen können. Wenn dies aber nicht gewünscht wird, sollte festgelegt werden, von wo auf das LAN zugegriffen werden darf. Dies kann auch technisch unterstützt werden. Beispielsweise könnte nur der IP-Adressbereich eines oder weniger Provider zugelassen werden. Bei einer Wählverbindung könnte anhand der Ländervorwahl gefiltert werden. Zu beachten ist jedoch, dass diese technischen Zugriffsbeschränkungen nicht absolut zuverlässig sind. Zusätzlich müssen also den Benutzern entsprechende organisatorische Vorgaben gemacht werden.

Diese Punkte müssen nicht zwangsläufig pauschal für die gesamte Institution betrachtet, sondern können auch differenziert auf einzelne Standorte oder Anwendungszwecke angewendet werden. Besonders bei der Vernetzung von mehreren Standorten kommt häufig nicht jeder Liegenschaft die gleiche Priorität zu. An kleine Vertriebsbüros werden beispielsweise meist andere Anforderungen bezüglich Verfügbarkeit gestellt als an Unternehmenszentralen. Ebenso bestehen an End-to-End-VPNs andere Anforderungen als an Site-to-Site-VPNs. Als Lösungsansatz könnten die verschiedenen Anwendungszwecke zum Beispiel bezüglich ihrer Anforderungen an Bandbreite, Verfügbarkeit, Vertraulichkeit, Integrität und Dienstgüte (Quality of Service oder kurz QoS) klassifiziert werden.

Die Ergebnisse der Anforderungsanalyse müssen dokumentiert und mit dem technischen Personal abgestimmt werden. Die fachlichen Anforderungen und die in der Leitlinie zur Informationssicherheit formulierten Sicherheitsziele fließen in die Konzeption des VPNs (siehe M 2.416 *Planung des VPN-Einsatzes* und M 2.417 *Planung der technischen VPN-Realisierung*) sowie dessen Realisierung ein.

Prüffragen:

- Ist festgelegt, für welche Geschäftsprozesse und Anwendungszwecke das jeweilige VPN genutzt und welche Informationen darüber kommuniziert werden dürfen?
- Ist festgelegt, welche Arten von Benutzern mit welchen Berechtigungen und welchen Vorkenntnissen das jeweilige VPN nutzen dürfen?
- Sind geeignete Verfahren zur Identifikation und Authentikation für die Nutzung jedes VPNs festgelegt?
- Sind die Zuständigkeiten und Meldewege für Betrieb und Nutzung von VPNs geklärt?
- Ist für jedes VPN festgelegt worden, von wo auf welches Netz zugegriffen werden darf?

# M 2.416 Planung des VPN-Einsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Da es sich bei der Einrichtung eines VPNs um eine komplexe Aufgabe handelt, ist eine strukturierte Vorgehensweise erforderlich. Daher sollte vor der Einführung eines VPNs in einer Institution unbedingt eine sorgfältige Planung erfolgen. Dieser Schritt folgt unmittelbar auf die Anforderungsanalyse (siehe M 2.415 *Durchführung einer VPN-Anforderungsanalyse*) und sollte auf den dort gewonnenen Erkenntnissen aufbauen.

Im Folgenden werden jeweils die wesentlichen Fragestellungen aufgezeigt, die im Rahmen eines **organisatorischen Konzepts** beantwortet werden müssen. Je nach konkreter Situation ergibt sich naturgemäß ein speziell auf die jeweiligen Gegebenheiten zugeschnittener zusätzlicher Regelungsbedarf.

- Es sollten die Verantwortlichkeiten für das jeweilige VPN festgelegt werden (Installation, Verwaltung, Überprüfung, Überwachung). Je nach organisatorischer Struktur müssen die Verantwortlichkeiten existierender Rollen erweitert oder neue Rollen geschaffen werden (siehe auch M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen*).
- Es muss festgelegt werden, wie und von wem die Benutzerkonten und die Zugriffsberechtigungen verwaltet und administriert werden (Berechtigungskonzept). Ein per Extranet angebundener Lieferant muss beispielsweise andere Zugriffrechte als eine angebundene Zweigstelle haben.
  Es empfiehlt sich, für den VPN-Zugang unterschiedliche Benutzergruppen mit verschiedenen Berechtigungen zu definieren. Die Gruppenzugehörigkeit von einzelnen Benutzern sollte durch ein entsprechendes Anforderungsprofil geregelt werden, das festlegt, welche Voraussetzungen für die Mitgliedschaft in einer Gruppe erfüllt werden müssen. Mögliche Voraussetzungen sind der Einsatzzweck (z. B. Telearbeit, Außendienst-Tätigkeiten, Wartungsarbeiten), Nachweis bestimmter Kenntnisse (z. B. Teilnahme an Schulungen) und eine Zustimmung durch Vorgesetzte. Wie die Erlaubnis zum entfernten Zugriff reglementiert werden soll, muss jeweils innerhalb der Institution entschieden werden. Oft existieren schon ähnliche Regelungen, z. B. für die Erlaubnis zur Nutzung von Internet-Zugängen, die dann adaptiert werden können.
  Die erteilten Zugangs- und Zugriffsberechtigungen müssen dokumentiert und bei Änderungen fortgeschrieben werden.
- Für feste entfernte Standorte (wie Telearbeitsplätze) müssen Anforderungen festgelegt werden, die beschreiben, welchen Ansprüchen (z. B. in Bezug auf Sicherheit und technischer Ausstattung) der entfernte Arbeitsplatz genügen muss, damit von dort VPN-Verbindungen in das LAN der Institution erlaubt werden können. Das Konzept kann eine anfängliche sowie eine periodisch wiederkehrende Überprüfung der Räumlichkeiten und dortigen Technik vorsehen und regeln, wie und durch wen diese erfolgt.
  Die Betriebsorte von VPN-Clients unterliegen häufig nicht der Kontrolle des LAN-Betreibers und besitzen daher auch ein besonderes Gefährdungspotential. Gegenüber stationären Clients kommen bei mobilen Clients weitere Gefährdungen hinzu. Nicht jeder Ort, an dem die technischen Voraussetzungen zum VPN-Verbindungsaufbau vorhanden sind, ist dafür geeignet. Daher müssen Regelungen getroffen werden, von welchen Standorten aus VPN-Verbindungen zum Ziel-LAN aufgebaut werden dürfen. Je nach geplantem Einsatzszenario kann es zweckmäßiger sein, eine Negativliste von besonders ungeeigneten Standorten zu führen. Da-

zu können z. B. Hotel-Foyers, Hotel-Business-Center oder öffentliche Verkehrsmittel gehören.

- Wird die Sicherheit von VPN-Zugängen verletzt, kann dies unter Umständen die Kompromittierung des gesamten LANs nach sich ziehen. Für die VPN-Administration sollten deshalb Verfahren festgelegt werden, die beschreiben, wie Änderungen an der VPN-Konfiguration durchzuführen sind (Beispiel: Beantragung, Überprüfung der geplanten Konfiguration, Durchführung, Überprüfung der durchgeführten Veränderung).
- Ein weiterer wichtiger Punkt bei der Konzeption ist die grundsätzliche Frage, ob eine Eigenrealisierung bzw. Eigenbetrieb des VPNs notwendig ist oder ob auf Fremdrealisierung bzw. -betrieb zurückgegriffen wird. Viele Dienstleister verfügen über hohe Kompetenz und Erfahrung in Bezug auf die Planung, Einrichtung und den Betrieb von VPNs. Allerdings ist es nicht immer vorteilhaft oder erwünscht, den kompletten Betrieb eines VPNs aus der Hand zu geben. Bei Fremdbetrieb eines VPNs müssen die Anforderungen des Bausteins B 1.11 *Outsourcing* beachtet werden.
- Der Schutzbedarf für das VPN muss ermittelt werden. Dieser leitet sich aus dem Schutzbedarf der darüber übertragenen Informationen sowie der damit verbundenen IT-Komponenten ab. In diesem Zusammenhang muss auch ermittelt werden, wie sich eine Nichtverfügbarkeit des Systems auswirkt und welche Ausfallzeiten hingenommen werden können.
  Die Anforderungen an die VPN-Sicherheitsmechanismen (z. B. Authentisierung und Integritätssicherung) müssen definiert werden. Hierbei muss hinterfragt werden, ob starke Kryptographie an allen beteiligten Standorten rechtlich eingesetzt werden darf.
- Haben externe Zulieferer oder Kunden eine Anbindung an das VPN, so müssen unterschiedliche Sicherheitszonen definiert werden. Aus den Sicherheitszonen heraus dürfen nur die Zugriffe erlaubt werden, die tatsächlich für die Benutzer erforderlich sind.
- Um einem Missbrauch vorzubeugen, müssen in der VPN-Sicherheitsrichtlinie die Rechte und Pflichten von VPN-Benutzern festgelegt werden. Diese müssen entsprechend verbindlich verpflichtet werden, die Sicherheitsregelungen einzuhalten.
- Da beim entfernten Zugriff auf ein LAN besondere Sicherheitsrisiken durch die meist ungesicherte Umgebung eines VPN-Clients bestehen, sollte jeder VPN-Benutzer eine besondere Schulung erhalten. Im Rahmen dieser Schulung sollen die Benutzer einerseits für die spezifischen VPN-Gefährdungen sensibilisiert und andererseits im Umgang mit den technischen Geräten und der Software unterrichtet werden. Falls Authentisierungstoken zum Einsatz kommen sollen, müssen die Benutzer über deren ordnungsgemäße Handhabung informiert werden.
  Ebenso müssen auch die Administratoren sowohl für die eingesetzten Produkte gründlich ausgebildet als auch über VPN-Sicherheitsrisiken und Sicherheitsmaßnahmen aufgeklärt werden.
- Den Administratoren muss nicht nur für den Betrieb des VPNs ausreichend Zeit zur Verfügung stehen, sondern auch für die Suche nach Informationen über aktuelle VPN-Sicherheitslücken, die Konzeption von Maßnahmen zur Steigerung der Informationssicherheit beim VPN-Betrieb und die Einarbeitung in neue Komponenten.

Die VPN-Planung muss der Leitungsebene zur Entscheidung vorgelegt werden. Alle Entscheidungen müssen nachvollziehbar dokumentiert werden.

Prüffragen:

- Sind die Verantwortlichkeiten für den VPN-Betrieb festgelegt?

- Ist festgelegt, wie und von wem die Benutzerkonten und die Zugriffsberechtigungen für den VPN-Betrieb verwaltet und administriert werden?
- Ist der Schutzbedarf jedes VPNs hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit bekannt?
- Sind alle VPN-Benutzer bezüglich der VPN-Nutzung hinreichend geschult und zur Einhaltung der Sicherheitsrichtlinien verpflichtet?
- Ist festgelegt, welche Zugriffsmöglichkeiten externen VPN-Benutzern eingeräumt werden?
- Werden die erteilten Zugangs- und Zugriffsberechtigungen dokumentiert und bei Änderungen angepasst?
- Ist festgelegt, welchen Ansprüchen entfernte Arbeitsplätze für VPN-Zugriffe genügen müssen?
- Ist ein Änderungsmanagement für das VPN eingerichtet?

# M 2.417 Planung der technischen VPN-Realisierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Neben den organisatorischen und personellen Planungen, die in M 2.416 *Planung des VPN-Einsatzes* behandelt werden, erfordert die Einführung eines VPNs auch Entscheidungen zu einer Reihe von technischen Aspekten. Diese Entscheidungen müssen in jedem Fall vor der Beschaffung getroffen werden und bilden die Grundlage für die spätere VPN-Realisierung. Bei der technischen Planung sind alle existierenden Rahmenbedingungen aus der aktuellen technischen Situation zu berücksichtigen, um Inkompatibilitäten zu vermeiden.

Im Folgenden werden jeweils die wesentlichen Fragestellungen aufgezeigt, die im Rahmen des **technischen Konzepts** beantwortet werden müssen. Je nach konkreter Situation ergibt sich naturgemäß ein speziell auf die jeweiligen Gegebenheiten zugeschnittener zusätzlicher Regelungsbedarf.

- Es sollte beschrieben sein, wie das VPN durch Hardware- und Software-Komponenten technisch realisiert ist. Die Komponenten werden lediglich durch ihre Funktion definiert. Im Rahmen einer nachgeschalteten Analyse vorhandener Systemkomponenten und am Markt beschaffbarer neuer Komponenten können die Elemente des Konzeptes tatsächlichen Geräten und Software-Produkten zugeordnet werden (siehe M 2.419 *Geeignete Auswahl von VPN-Produkten*).
- Alle potentiellen VPN-Endpunkte, die die Einwahl in das LAN ermöglichen, und die dafür verwendeten Zugangsprotokolle sind zu beschreiben.
- Im Rahmen der Sicherheitskonzeption sind alle VPN-Zugangspunkte zum lokalen Netz zu erfassen und es ist zu beschreiben, wie diese Zugangspunkte an das LAN angeschlossen werden (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*). Das Sicherheitskonzept muss aufbauend auf der aktuellen Netzstruktur analysieren, welche Teilnetze bei Nutzung eines VPN-Zugangs erreichbar sind. Es sollte überlegt werden, dedizierte Zugangsnetze (Access Networks) zu bilden, aus denen nur kontrolliert (über Router, Paketfilter bzw. interne Firewall) in das produktive Netz zugegriffen werden kann. Die Bildung von Zugangsnetzen erfordert dabei die Anschaffung und Wartung zusätzlicher Hard- und Software (siehe auch M 5.77 *Bildung von Teilnetzen*).
- Alle Dienste und Protokolle, die über den VPN-Zugang zugelassen werden, sowie die darüber zugreifbaren Ressourcen sind zu dokumentieren. Die Auswahl ist davon abhängig, welche Applikationen eingesetzt werden sollen. Für einen zeitkritischen Datenverkehr werden eventuell QoS (Quality of Service), MPLS (Multi Protocol Label Switching) oder dedizierte Leitungen benötigt.
- Es müssen geeignete Verschlüsselungsverfahren zum Schutz der Daten festgelegt werden. Relevant sind hier unter anderem:
  - Tunneling
    Die Kommunikation kann auf niedriger Protokollebene verschlüsselt werden (so genanntes Tunneling, siehe M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation*). Dazu muss ein geeignetes Verfahren ausgewählt werden. Die herkömmlichen VPNs stellen solche Verfahren standardmäßig, jedoch in unterschiedlicher Zahl und Ausprägung zur Verfügung.
  - TLS/SSL-Verschlüsselung

Zur Verschlüsselung kann auch TLS/SSL eingesetzt werden, wenn von der Verschlüsselung auf niedriger Protokollebene aus bestimmten Gründen kein Gebrauch gemacht werden kann. Dies gilt besonders für Zugriffe auf Webserver oder E-Mail-Server über Browser, die standardmäßig TLS/SSL-gesicherte Kommunikation unterstützen. Dazu sollte auch M 5.66 *Clientseitige Verwendung von SSL/TLS* beachtet werden.

- Verschlüsselung durch Netzkoppelelemente
  Neben der Absicherung der Kommunikation durch Software kann auch der Einsatz von verschlüsselnden Netzkoppelelementen (Router, Modems) erwogen werden. Diese sind besonders für den stationären Einsatz und zur Anbindung mehrerer Rechner sinnvoll, da die Verschlüsselung transparent erfolgt und die Endsysteme nicht belastet werden. Zu beachten ist jedoch, dass die Netzkoppelelemente sorgfältig konfiguriert und gewartet werden müssen.
  Auch bei direkten Einwahlverfahren beispielsweise über analoge Telefonnetze oder ISDN ist eine Verschlüsselung zum Schutz der Daten erforderlich.

- In M 3.65 *Einführung in VPN-Grundbegriffe* werden die verschiedenen Arten von VPNs vorgestellt. Anhand der Anforderungen muss entschieden werden, welcher VPN-Typ realisiert werden soll.
- Es muss entschieden werden, ob die Verbindung über dedizierte Carrier-Leitungen realisiert werden muss. Diese Entscheidung hat in der Regel erheblichen Einfluss auf die Kosten.
- Um einen stabilen Betrieb und eine kontinuierliche Verbesserung gewährleisten zu können, sollten geeignete Monitoring-Systeme eingeplant werden. Die aus den Monitoring-Systemen gewonnenen Erkenntnisse tragen wesentlich zur Feinabstimmung des VPN-Betriebs bei (siehe M 4.321 *Sicherer Betrieb eines VPNs*).

Die VPN-Planung muss der Leitungsebene zur Entscheidung vorgelegt werden.

Prüffragen:

- Ist die technische Realisierung des VPN dokumentiert?
- Ist festgelegt, welche Verschlüsselungsverfahren für das VPN genutzt werden sollen?
- Ist festgelegt, welche Anforderungen an das Trägernetz bestehen?
- Sind die VPN-Endpunkte und die erlaubten Zugangsprotokolle festgelegt?
- Sind die Dienste, Protokolle und Ressourcen, die über das jeweilige VPN zugelassen sind, definiert?
- Ist festgelegt, welche Teilnetze über das VPN erreichbar sind?
- Ist festgelegt, wie das Monitoring des VPN erfolgt?

# M 2.418 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Für den Einsatz von VPN-Komponenten in Behörden und Unternehmen müssen geeignete Sicherheitsrichtlinien aufgestellt werden. Diese VPN-spezifischen Sicherheitsrichtlinien müssen konform zum generellen Sicherheitskonzept und den allgemeinen Sicherheitsrichtlinien der Institution sein. Sie müssen regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Die VPN-spezifischen Vorgaben können in den vorhandenen Richtlinien ergänzt oder in einer eigenen Richtlinie zusammengefasst werden. Eine VPN-Sicherheitsrichtlinie sollte unter anderem folgende Punkte umfassen:

- Es sollte beschrieben sein, wer in der Institution VPN-Komponenten installieren, konfigurieren und benutzen darf. Dazu sind auch eine Vielzahl von Randbedingungen festzulegen wie z. B.
  - welche Informationen über VPNs übertragen werden dürfen,
  - wo die VPN-Komponenten benutzt werden dürfen,
  - auf welche anderen internen oder externen Netze oder IT-Systeme über ein VPN zugegriffen werden darf.
- Für alle VPN-Komponenten sollten Sicherheitsmaßnahmen und eine Standard-Konfiguration festgelegt werden.
- Alle VPN-Benutzer sollten darauf hingewiesen werden, dass bei einem Verdacht auf Sicherheitsprobleme ein Sicherheitsverantwortlicher hierüber informiert werden muss, damit dieser weitere Schritte unternehmen kann (siehe auch B 1.8 *Behandlung von Sicherheitsvorfällen*).
- Administratoren, aber auch Benutzer von VPN-Komponenten sollten über VPN-Gefährdungen und die zu beachtenden Sicherheitsmaßnahmen informiert bzw. geschult werden.

Die korrekte Umsetzung der in der VPN-Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen sollte regelmäßig kontrolliert werden.

**Benutzerrichtlinie für VPN**

Um Benutzer nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene VPN-Benutzerrichtlinie zu erstellen, z. B. in Form eines Merkblattes. In einer solchen Benutzerrichtlinie sollten dann kurz die Besonderheiten bei der VPN-Nutzung beschrieben werden, wie z. B.

- an welche anderen internen und externen Netze oder IT-Systeme der VPN-Client gekoppelt werden darf,
- unter welchen Rahmenbedingungen sie sich an einem internen oder externen VPN anmelden dürfen,
- welche Schritte bei (vermuteter) Kompromittierung des VPN-Clients zu unternehmen sind, vor allem, wer zu benachrichtigen ist.

Benutzer sollten darauf hingewiesen werden, dass VPNs nur von geeigneten Standorten und mit von der Institution dafür zugelassenen IT-Komponenten aufgebaut werden dürfen. Ungeeignete Standorte können je nach Einsatzzweck z. B. Hotel-Foyers, Hotel-Business-Center oder öffentliche Verkehrsmittel sein, fremd-administrierte IT-Systeme können ebenso ungeeignet sein (siehe M 4.251 *Arbeiten mit fremden IT-Systemen*). Wichtig ist auch, dass klar

beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass

- keine sicherheitsrelevanten Konfigurationen verändert werden dürfen,
- Passwörter nicht auf dem Client gespeichert werden dürfen, es sei denn mit von dafür freigegebenen Passwort-Speicher-Tools (siehe M 4.306 *Umgang mit Passwort-Speicher-Tools*),
- stets ein Virenscanner aktiviert sein muss,
- eine vorhandene Personal Firewall nicht abgeschaltet werden darf (siehe auch M 5.91 *Einsatz von Personal Firewalls für Clients* ),
- die Konfiguration der VPN-Clients nicht von den Benutzern verändert werden darf, nur durch die hierfür benannten Administratoren, und
- alle Freigaben von Verzeichnissen oder Diensten deaktiviert oder zumindest durch gute Passwörter geschützt sind.

Außerdem sollte die Benutzerrichtlinie Angaben dazu enthalten, welche Daten im VPN genutzt und übertragen werden dürfen und welche nicht. Hierzu gehört vor allem der Umgang mit klassifizierten Informationen, beispielsweise Verschlusssachen. Benutzer sollten für VPN-Gefährdungen sowie für Inhalte und Auswirkungen der VPN-Richtlinie sensibilisiert werden.

**Richtlinie für Administratoren eines VPNs**

Daneben sollte eine VPN-spezifische Richtlinie für Administratoren erstellt werden, die auch als Grundlage für die Schulung der Administratoren dienen kann. Darin sollte festgelegt sein, wer für die Administration der unterschiedlichen VPN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Administratoren gibt, und wann welche Informationen zwischen den Zuständigen fließen müssen. So ist es durchaus üblich, dass für den Betrieb der serverseitigen Komponenten eine andere Organisationseinheit zuständig ist als für die Betreuung der VPN-Clients oder für das Identitäts- und Berechtigungsmanagement. Die VPN-Richtlinie für Administratoren sollte weiterhin die wesentlichen Kernaspekte zum Betrieb einer VPN-Infrastruktur umfassen, wie z. B.

- Festlegung einer sicheren VPN-Konfiguration und Definition von sicheren Standard-Konfigurationen,
- geeignete Verwaltung aller VPN-Komponenten,
- Auswahl und Einrichtung von Kryptoverfahren inklusive Schlüsselmanagement,
- Regelmäßige Auswertung von Protokolldateien, zumindest auf den Servern,
- Inbetriebnahme von Ersatzsystemen,
- Maßnahmen bei Kompromittierung des VPNs.

Alle VPN-Anwender, egal ob Benutzer oder Administratoren, sollten mit ihrer Unterschrift bestätigen, dass sie den Inhalt der VPN-Sicherheitsrichtlinie gelesen haben und die darin definierten Anweisungen auch einhalten. Ohne diese schriftliche Bestätigung sollte niemand VPNs nutzen dürfen. Die unterschriebenen Erklärungen sind an einem geeigneten Ort, beispielsweise in der Personalakte, aufzubewahren.

Prüffragen:

- Existiert eine aktuelle VPN-Sicherheitsrichtlinie?
- Besitzt jeder VPN-Benutzer ein Exemplar der VPN-Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen?
- Wird die Sicherheitsrichtlinie für die VPN-Nutzung den Benutzern im Rahmen der Schulungen zu Sicherheitsmaßnahmen erläutert?

# M 2.419 Geeignete Auswahl von VPN-Produkten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Unternehmen und Behörden haben vielfältige Anforderungen an Netze, wie beispielsweise die Vernetzung unterschiedlicher Standorte und die Anbindung mobiler Mitarbeiter oder Telearbeitern an das interne Netz. Dementsprechend unterscheiden sich die Anforderungen der Institutionen und müssen bei der Auswahl von VPN-Produkten berücksichtigt werden. Die Ergebnisse der Maßnahmen M 3.65 *Einführung in VPN-Grundbegriffe* und M 2.416 *Planung des VPN-Einsatzes* sind ebenfalls einzubeziehen.

VPN-Produkte unterscheiden sich in ihrem Leistungsumfang, den angebotenen Sicherheitsmechanismen, dem Bedienkomfort und der Wirtschaftlichkeit. Zudem stellen sie unterschiedliche Voraussetzungen an Hardware- und Software-Komponenten im Einsatzumfeld.

Bevor ein VPN-Produkt beschafft wird, sollte eine Anforderungsliste für die Bewertung der am Markt erhältlichen Produkte erstellt werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen.

Wird ein Dienstleister beauftragt, ein VPN bereitzustellen, kann in der Regel die Auswahl der Produkte, die vom Dienstleister betrieben werden, nicht beeinflusst werden. Hinweise zur Auswahl von VPN-Dienstleistern sind in M 2.420 *Auswahl eines Trusted-VPN-Dienstleisters* zu finden.

Ein VPN besteht meistens aus der Kombination von mehreren Hardware- und Software-Komponenten. Zunächst kann grob zwischen LAN-seitigen und Client-seitigen Komponenten unterschieden werden. Die konkret zu beschaffenden Komponenten hängen von der gewählten VPN-Systemarchitektur ab. In großen Institutionen werden oft mehrere VPN-Verbindungen gleichzeitig für unterschiedliche Einsatzzwecke betrieben. Hierfür sind in der Regel besondere IT-Systeme (Hardware mit Software) erforderlich, die speziell für den Einsatz als VPN-Server konzipiert sind.

Verschiedene Hersteller bieten VPN-Komponenten als Appliances an. Dabei handelt es sich um vorkonfigurierte Geräte, die nur für einen genau vorgegebenen Einsatzzweck (hier: VPN-Endpunkt) hergestellt und konfiguriert werden. Gegenüber dem Aufbau einer zentralen VPN-Komponente aus Standard-IT-Komponenten, die (in Eigenregie oder durch einen Dienstleister) entsprechend konfiguriert werden, bieten Appliances oft den Vorteil einer einfacheren Konfiguration. Dem steht jedoch meist der Nachteil gegenüber, dass die Konfiguration weniger flexibel ist und weniger Möglichkeiten zur Anpassung an individuelle Bedürfnisse bietet.

Folgende Sicherheitsgrundfunktionen müssen bei der Auswahl von VPN-Produkten erfüllt werden:

- Identifikation, Authentisierung und Autorisierung:
  Hierunter fallen die Identifikation und Authentisierung von Systemen untereinander, von Systemen gegenüber Benutzern und von Benutzern gegenüber Systemen. Es muss möglich sein, verschiedene Benutzerkennungen mit unterschiedlichen Rechteprofilen einzurichten. Es sollten ausreichend starke anerkannte Authentisierungsverfahren vorhanden sein. Re-

mote-Zugriffe sollten durch eine starke Authentisierung abgesichert werden.
Es muss außerdem möglich sein, die festgelegten Zugriffsrechte auf den VPN-Komponenten abbilden zu können.

- Dienstgüte (Quality of Service, QoS):
  Im Zusammenhang mit Netzübergängen ist der Begriff Dienstgüte als Überwachung und Steuerung der Kommunikation zu verstehen, die über ein Sicherheitsgateway erfolgen darf. Ein geeignetes Produkt muss die bei der VPN-Konzeption ermittelten Anforderungen erfüllen können und eine Priorisierung von geschäftskritischen Applikationen ermöglichen.
- Übertragungssicherung:
  Zur Übertragungssicherung kommen Funktionen zum Einsatz, welche die Vertraulichkeit und Integrität der Daten sichern. Außerdem muss die Authentizität der Kommunikationspartner gewährleistet werden. Wichtig ist dabei, dass das Produkt sichere kryptographische Mechanismen bietet, die dem Stand der Technik entsprechend (siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Bei der Planung und Realisierung des VPNs muss außerdem die Integration der VPN-Endpunkte in ein Sicherheitsgateway berücksichtigt werden.
- Schlüsselmanagement:
  Zum Schlüsselmanagement müssen geeignete Funktionen vorhanden sein, um geheime und öffentliche Schlüssel für die kryptographischen Mechanismen verwalten, verteilen und eventuell auch erzeugen zu können. Die ausgewählten Produkte sollten dabei möglichst flexibel sein und eine nahtlose Integration verschiedenster Techniken ermöglichen.

Die nun folgende Liste gibt einen Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden. Neben den hier aufgeführten Kriterien müssen weitere spezifische Anforderungen erarbeitet werden, die aus den geplanten konkreten Einsatzszenarien resultieren (siehe Maßnahme M 2.415 *Durchführung einer VPN-Anforderungsanalyse*).

**Allgemeine Kriterien**

- Performance und Skalierbarkeit
  - Kann das Produkt den Ansprüchen an die Performance gerecht werden?
  - Bietet das Produkt Funktionen zur Lastverteilung?
  - Können die Produkte die zu übertragenen Informationen komprimieren und dekomprimieren?
  - Kann das Produkt einem zukünftigen Wachstumsbedarf gerecht werden (z. B. durch modularen Systemaufbau, einfaches Einbinden neuer VPN-Server, gemeinsame Benutzerverwaltung für alle VPN-Zugänge)?
- Wartbarkeit
  - Ist das Produkt einfach wartbar?
  - Bietet der Hersteller regelmäßige Software-Updates an?
  - Wird für das Produkt ein Wartungsvertrag angeboten?
  - Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
  - Bietet der Hersteller einen kompetenten technischen Kundendienst (Call-Center, Hotline) an, der in der Lage ist, bei Problemen sofort zu helfen?
- Zuverlässigkeit/Ausfallsicherheit
  - Wie zuverlässig und ausfallsicher ist das Produkt?

  - Bietet der Hersteller auch Hochverfügbarkeitslösungen an?
  - Ist das Produkt im Dauerbetrieb einsetzbar?
- Benutzerfreundlichkeit

  - Lässt sich das Produkt einfach installieren, konfigurieren und nutzen? Genügt das Produkt den geltenden Ergonomievorschriften?
  - Ist insbesondere für den VPN-Client die Benutzerführung so gestaltet, dass auch ungeübte Benutzer damit arbeiten können, ohne Abstriche in der Sicherheit in Kauf nehmen zu müssen (z. B. durch kontextsensitive Hilfen, Online-Dokumentation, detaillierte Fehlermeldungen)?
  - Ist die Nutzung des VPN-Clients so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?

**Funktion**
- Installation und Inbetriebnahme

  - Kann die Installation der VPN-Client-Software automatisiert mit vorgegebenen Konfigurationsparametern erfolgen?
  - Ist die Installation der VPN-Client-Software auch für weniger versierte Mitarbeiter durchführbar?
  - Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
  - Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Einsteckkarten , Treiber)?
  - Ist das VPN mit gängigen Systemmanagementsystemen kompatibel?
- Verhalten im Fehlerfall

  - Bleibt die Sicherheit des VPN-Zugangs auch nach einem kritischen Fehler gewährleistet?
  - Kann konfiguriert werden, wie sich das System nach einem kritischen Fehler verhalten soll? Kann z. B. eingestellt werden, dass nach einem kritischen Fehler automatisch ein Neustart durchgeführt oder der Administrator benachrichtigt wird?
- Administration

  - Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
  - Kann die Administration über eine graphische Benutzeroberfläche erfolgen, die sich intuitiv bedienen lässt? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?
  - Wird neben der graphischen Administrationsoberfläche auch eine kommandozeilenbasierte Schnittstelle angeboten?
  - Sind die administrativen Funktionen durch eine adäquate Zugriffskontrolle geschützt?
- Protokollierung

  - Bietet das Produkt geeignete Funktionen zur Protokollierung an?
  - Ist konfigurierbar, wie detailliert die Protokollierung erfolgt und welche Arten von Ereignissen aufgezeichnet werden? Werden durch die Protokollierung alle relevanten Daten erfasst?
  - Ist die Protokollierung in der Weise möglich, dass die Daten nach unterschiedlichen Kategorien erfasst werden können (z. B. verbin-

dungsorientiert, benutzerorientiert, protokollorientiert, dienstorientiert)?
  - Sind die Protokolldaten mit einem Zugriffsschutz versehen?
  - Können die Protokolldaten nicht nur lokal gespeichert werden, sondern auch auf entfernten Rechnern (zentrales Protokoll)? Werden für die entfernte Speicherung gängige Verfahren angeboten, so dass auch Fremdsysteme zur Protokollierung benutzt werden können (z. B. syslog)? Können die Protokolldaten abgesichert übertragen werden?
  - Bietet das Produkt leicht bedienbare Funktionen zur Auswertung der Protokolldaten an?
  - Kann die Protokollierung mit dem eingesetzten Systemmanagementsystem zusammenarbeiten, insbesondere hinsichtlich Übertragungsformat und Übertragungsprotokoll?
  - Bietet das Produkt die Möglichkeit an, beim Auftreten bestimmter Ereignisse den Administrator zu informieren oder auch geeignete Schutzmaßnahmen automatisch durchzuführen? Beispielsweise ist es oft sinnvoll, ein Benutzerkonto zu sperren, wenn mehrere fehlgeschlagene Authentisierungsversuche in Folge für das jeweilige Benutzerkonto festgestellt werden.
  - Kann die Protokollierung an die spezifischen Bestimmungen des Datenschutzes, die für und in der Institution gelten, angepasst werden?
- Kommunikation und Datenübertragung
  - Unterstützt das VPN-Produkt LAN-seitig alle relevanten Netzwerktechnologien (z. B. Ethernet, ATM)?
  - Unterstützt das VPN-Produkt WAN-seitig alle geplanten Zugangstechnologien (z. B. ISDN, Mobiltelefon, analoge Telefonleitung, X.25)?
  - Ist die Anzahl der VPN-Clients, die sich gleichzeitig in den VPN-Server einwählen können, ausreichend?
  - Unterstützt das VPN-Produkt die gängigen Protokolle für den entfernten Zugang über Telekommunikationsnetze (z. B. PPP, SLIP)?
  - Unterstützt das VPN-Produkt die gängigen Dienstprotokolle für den entfernten Zugriff (z. B. TCP/IP)?
  - Werden für den Internet-basierten Zugriff die gängigen Tunnel-Protokolle (z. B. PPTP, L2F, IPSec, SSL) unterstützt?
  - Bietet das VPN-Produkt je nach verwendeter Zugangstechnologie zusätzliche, technologieabhängige Mechanismen (z. B. Kanalbündelung für ISDN, Rückruf des VPN-Clients durch den VPN-Server) an?
- Sicherheit: Kommunikation, Authentisierung und Zugriff
  - Bietet das Produkt geeignete Funktionen zur gesicherten Datenübertragung an?
  - Erfolgt die Absicherung der Kommunikation durch standardisierte Mechanismen?
  - Sind alle verwendeten kryptographischen Verfahren etabliert, und entsprechen sie dem Stand der Technik?
  - Erlaubt die Produktarchitektur eine nachträgliche Installation neuer Sicherheitsmechanismen?
  - Bietet das Produkt geeignete Funktionen zur Authentisierung der Benutzer, bevor ihnen Zugang zu lokalen Ressourcen gewährt wird?
  - Können mehrere Authentisierungsmechanismen miteinander verknüpft werden?
  - Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?

- Erlaubt das VPN die Nutzung eines oder mehrerer gängiger externer Authentisierungsdienste, z. B. SecureID, TACACS+, RADIUS?
- Ist es möglich, zusätzliche externe Authentisierungsdienste einzubinden?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Produkte dahingehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen entsprechend ihrer Relevanz für die Institution gewichtet werden. Analog kann auch der Erfüllungsgrad einer Anforderung durch das jeweilige Produkt in mehrere Stufen eingeteilt werden. Auf der Grundlage der durchgeführten Produktbewertung kann dann eine fundierte Kaufentscheidung getroffen werden.

Vor der Installation muss überprüft werden, ob die ausgewählten Produkte tatsächlich die Anforderungen ausreichend erfüllen und kompatibel mit den vorgesehenen Technologien sind. Die Auswahl der VPN-Geräte stellt einen wesentlichen Aspekt für den reibungslosen Betrieb eines VPNs dar. Die Entscheidung muss daher gut überlegt sein, da spätere Änderungen oft mit hohen Kosten oder auch mit Sicherheitseinbußen verbunden sind.

Prüffragen:

- Werden die Anforderungen der Institutionen an die Vernetzung unterschiedlicher Standorte bzw. die Anbindung mobiler Mitarbeiter oder Telearbeitern bei der Auswahl von VPN-Produkten berücksichtigt?

# M 2.420 Auswahl eines Trusted-VPN-Dienstleisters

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Der eigenständige Betrieb eines VPNs erfordert oft ein hohes Fachwissen des zuständigen Administrators. Neben VPN-spezifischen Einstellungen müssen zusätzlich kryptographische Aspekte berücksichtigt und die Anbindung an öffentliche Netze optimiert werden. Werden alle Einstellungen bestmöglich gewählt, so kann die Vertraulichkeit und Integrität der Daten geschützt werden, die Verfügbarkeit hingegen kann nicht beeinflusst werden. Ausfälle im öffentlichen Netz, an das das VPN-Gateway angeschlossen ist, können weiterhin den Datenfluss zwischen den zu verbindenden Standorten unterbrechen.

Eine Alternative zu diesen eigenständig administrierten "Secure-VPNs" sind "Trusted-VPNs". Bei einem Trusted-VPN wird ein externer Dienstleister mit der sicheren Übermittlung der Informationen beauftragt. Durch vertragliche Vereinbarungen kann der Dienstleister verpflichtet werden, die übertragenen Informationen bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.

Anstatt über öffentliche Netze, wie dem Internet, werden die Informationen bei Trusted-VPNs in der Regel über dedizierte Leitungen des Anbieters (Carrier-Netz) übertragen. Da das Carrier-Netz unter der Kontrolle des Dienstleisters steht, kann dieser den Schutz der Informationen bis zu einem gewissen Grad garantieren.

Aus der Sicht des Kunden stellt der Dienstleister Geräte zur Verfügung, die an die zu verbindenden LANs des Kunden angeschlossen werden. Da die Daten vom Dienstleister oftmals nicht verschlüsselt werden und die gesamte Betreuung beim externen Dienstleister liegt, sollten Trusted-VPNs nur bei wenig schutzwürdigen Daten ohne zusätzliche Sicherheitsmechanismen des Kunden verwendet werden. Selbst in diesem Fall ist eine zusätzliche Verschlüsselung der Daten auf Kundenseite sehr empfehlenswert. Bei höherem Schutzbedarf muss vor Übertragung der Daten eine Verschlüsselung durchgeführt werden.

Ein großer Nachteil von Trusted-VPNs stellt die oft starke Abhängigkeit zum Dienstleister dar. Ein Wechsel zu einem anderen Dienstleister ist oft mit einem sehr hohen Aufwand verbunden.

Ein großer Vorteil von Trusted-VPNs ist, dass die entsprechenden Service-Provider oft länderübergreifend präsent sind. Gerade im internationalen Umfeld ist es für eine Institution nur eingeschränkt möglich, an allen Standorten qualifiziertes Personal und Prozesse für den Betrieb eines eigenen VPNs bereitzustellen.

Bei der Auswahl eines Trusted-VPN-Dienstleisters sowie den darauf folgenden Vertragsverhandlungen sollten die in M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters* und M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* beschriebenen Aspekte berücksichtigt werden. Für den Betrieb eines Trusted-VPNs sind darüber hinaus folgende Punkte zu beachten:

- Service Level Agreement

Aufgrund erhöhter Kosten ist es nicht wirtschaftlich, die Leistungen eines Dienstleisters mit der höchstmöglichen Qualität zu wählen. Vielmehr muss im Vorfeld entschieden werden, was genau mit welcher Qualität benötigt wird. Dies muss mittels Service Level Agreements (SLAs) ausgehandelt und dokumentiert werden. SLAs beinhalten die messbare Beschreibung einer zu erbringenden Dienstleistung, einschließlich der zu erreichenden Qualität und der anzuwendenden Messgrößen. Im Weiteren muss mit dem Dienstleister festgelegt werden, welche Konsequenz ein Verstoß gegen vereinbarte SLAs hat und wie ein entsprechendes Reporting durchgeführt wird.

- Globale Konnektivität
  Oft werden VPNs nicht nur zur Verbindung von Standorten genutzt, sondern auch um mobile Mitarbeiter in das LAN zu integrieren. Soll die Anbindung von mobilen Mitarbeitern über ein Trusted-VPN erfolgen, muss der Dienstleister Einwahlpunkte anbieten, zu denen die Mitarbeiter über eine der folgenden Lösungen eine Verbindung aufbauen können:

  - Datenverbindungen über öffentliche Netze:
    Hier wird eine Datenverbindung über ein öffentliches Netz, wie dem Internet, aufgebaut. Da die Übertragungsqualität von Datenverbindungen über öffentliche Netze nicht beeinflusst werden kann, können unter Umständen Störungen auftreten. Beispielsweise erfordern Terminalserver-Anwendungen oft eine hohe Bandbreite, die nicht überall zu Verfügung gestellt werden kann.
  - Wählverbindungen
    Bei Wählverbindungen können sich mobile Mitarbeiter direkt über eine Telefonverbindung, wie zum Beispiel über Mobilfunknetze, direkt in den Zugangspunkt des Dienstleisters einwählen. Besonders bei mobilen Mitarbeitern, die sich oft im Ausland befinden, kann dies zu Problemen führen, wenn eine Telefonverbindung über weite Strecken hinweg aufgebaut werden muss. Daher sollte bei Auswahl dieser Lösung darauf geachtet werden, dass der Dienstleister unterschiedliche Einwahlpunkte anbietet.
- Flächendeckung
  VPNs werden oft eingesetzt, um mehrere Standorte miteinander zu verbinden. Im Gegensatz zu mobilen Mitarbeitern verfügen die Anbindungen der verschiedenen Liegenschaften meist über eine größere Bandbreite, damit umfangreichere Informationen übermittelt werden können. Anstatt mit Wählverbindungen über Drittanbieter werden die Liegenschaften in der Regel mit Standleitungen an das Trusted-VPN angeschlossen. Besonders für weltweit arbeitende Unternehmen ist die Anbindung von ausländischen Standorten wichtig. Es muss daher geklärt werden, ob der Anbieter geeignete Anschlüsse bereitstellen kann und darf.
- Tarifstrukturen
  Neben den technischen Anforderungen sind auch die finanziellen Rahmenbedingungen wichtig. Neben Kostenmodellen für die bereitgestellte Bandbreite können oft zusätzliche Supportleistungen oder eine Garantie, beispielsweise für eine hohe Verfügbarkeit, hinzugekauft werden.
- Überwachung (Reports)
  In der Regel garantieren die Dienstleister dem Kunden eine bestimmte Qualität der Verfügbarkeit, Vertraulichkeit und Integrität. Ein leistungsfähiges Monitoring stellt dabei die Grundlage für die Überwachung der in den SLAs festgelegten Anforderungen dar. Der Kunde muss die Möglichkeit haben, die festgelegten Anforderungen entsprechend überprüfen zu können.
- Störungsbehandlung

Der Kunde muss wissen, an wen er sich bei Störungen wenden kann. Beispiele für Störungen können Übertragungsproblemen im Netz des Dienstleisters und defekte Gateways, die die Verbindung zwischen LAN und Netz des Dienstleisters bilden, sein.

Alle vereinbarten Leistungen müssen so genau und eindeutig wie möglich schriftlich festgehalten werden. Die Sicherheit des Trusted-VPNs muss regelmäßig kontrolliert werden, damit es auch ein vertrauenswürdiges Netz bleibt. Der Auftraggeber muss die dazu notwendigen Berechtigungen besitzen. Untersuchungsergebnisse von unabhängigen Dritten sollten dem Auftragnehmer mitgeteilt werden. Allen Institutionen, die beim Auftraggeber Prüfungen durchführen müssen (z. B. Aufsichtsbehörden) müssen auch beim VPN-Dienstleister die entsprechenden Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) eingeräumt werden.

Prüffragen:

- Sind alle Vereinbarungen mit Trusted-VPN-Dienstleistern schriftlich fixiert?
- Wird die Sicherheit von Trusted-VPNs regelmäßig kontrolliert?

# M 2.421 Planung des Patch- und Änderungsmanagementprozesses

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Änderungsmanager

Jede Institution sollte für das Patch- und Änderungsmanagement einen klar definierten Prozess eingerichtet haben und die Zuständigkeiten für die verschiedenen Aufgaben geregelt haben (siehe M 2.423 *Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement*). Alle Änderungen von Hard- und Softwareständen und Konfigurationen sollten über den Prozess Patch- und Änderungsmanagement gesteuert und kontrolliert werden. Um alle Änderungen erfassen und bewerten zu können, sollten alle vom Patch- und Änderungsmanagement betreuten IT-Systeme dem Änderungsmanager unterstellt sein. Änderungen an Konfiguration und Zustand der Systeme sollten damit nur noch über das Änderungsmanagement möglich sein.

Der Patch- und Änderungsmanagementprozesses kann, angelehnt an ITIL, wie folgt schematisch dargestellt werden:

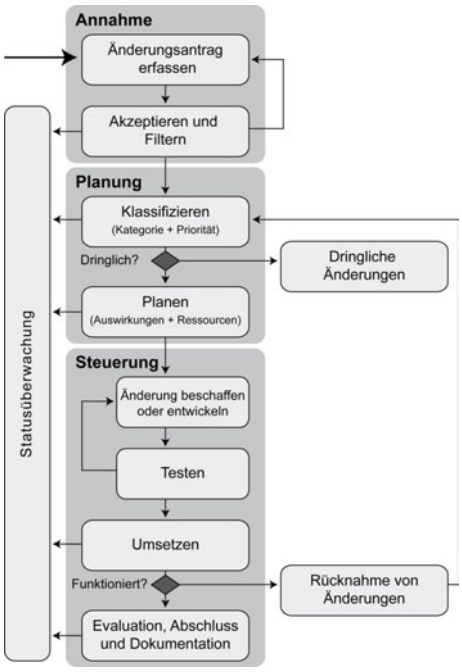



Abbildung: Überblick über den Patch- und Änderungsmanagementprozess

**Koordination**

Nachdem ein Request for Change (RfC), also eine Änderungsanforderung, eingereicht und akzeptiert wurde, muss er zunächst kategorisiert und priorisiert werden, bevor mit der eigentlichen Umsetzungsplanung und -koordination begonnen wird.

Wenn eine Änderungsanforderung (wie in M 2.422 *Umgang mit Änderungsanforderungen* beschrieben) eingereicht und akzeptiert wurde, muss sie zunächst klassifiziert, also kategorisiert und priorisiert werden, bevor mit der eigentlichen Umsetzungsplanung und -koordination begonnen wird. Im An-

schluss sollten weitere Punkte berücksichtigt werden, bevor der Patch oder die Änderung eingespielt werden kann.

- Beschaffung oder Entwicklung der Patches und Änderungen
  Viele Hersteller bieten die Möglichkeit, die nötigen Informationen über die Veröffentlichung neuer Hard- oder Software oder über aufgetretene Fehler und deren Behebung im Abonnement per E-Mail zu erhalten.
  Die Aktualisierungen und Patches werden in der Regel auf Internet-Servern zum Download bereit gestellt. Teilweise sind diese Quellen nur in Verbindung mit gültiger Registrierung oder Support-Verträgen zugänglich.
  Häufig bietet die installierte Software oder das installierte Betriebssystem dem Benutzer die Möglichkeit, Software-Änderungen direkt mittels der jeweiligen Anwendung oder dem jeweiligen System zu laden.
  Einige Hersteller stellen ihren Kunden spezielle Applikationen zur Verfügung, um die Produkte zu verwalten und zu aktualisieren. Zusätzlich gibt es auch immer mehr Anwendungen, die, wenn der Benutzer und die Sicherheitseinstellungen dies zulassen, selbsttätig über das Internet bei ihren Herstellern nach Aktualisierungen suchen und den Anwender gegebenenfalls informieren. Aus Sicherheitssicht hat das automatisierte Einspielen von Änderungen allerdings Nachteile. Daher sollte genau überlegt werden, ob solche Mechanismen in Anspruch genommen werden sollen.
  Eine interne Softwareentwicklung könnte eine weitere Möglichkeit sein, Software-Änderungen zu beziehen, falls aufgetretene Sicherheitslücken oder andere Anforderungen diese erforderlich machen. Allerdings muss dafür nicht nur das nötige Fachwissen vorhanden sein, sondern auch die Schnittstellen offen liegen.
- Testen
  Die Funktionalität der Systeme muss nach Einspielen der Änderung durch einen Test ermittelt werden. Dafür sind bei jeder Änderung, wenn möglich, eine repräsentative Auswahl an typischen Anwendungsszenarien mit der Fachabteilung festzulegen und zu testen. Die Ergebnisse sind zu dokumentieren und mit den erwarteten Ergebnissen zu vergleichen, um eventuelles Fehlverhalten festzustellen. Ferner müssen alle Protokoll-Dateien, die während des Tests angelegt werden, auf Hinweise von Fehlfunktionen untersucht werden.
- Integration in die Softwareverteilung, Test der Integration
  Oft müssen spezifische Paket- oder Dateiformate, in denen die Hersteller ihre Aktualisierungen zur Verfügung stellen angepasst werden, damit diese in einem automatischen Softwareverteil-System benutzt werden können. Dies gilt insbesondere dann, wenn während oder nach der Installation noch aktive Komponenten, wie beispielsweise Shell-Skripte ausgeführt werden müssen. Diese Anpassungen sind auf einem Testsystem auf ihre Wirksamkeit zu prüfen, bevor die Änderungen verteilt werden.

**Umsetzung**

Die vom Änderungsmanager bestimmten Mitarbeiter werden beauftragt, die Änderung umzusetzen. Das Änderungsmanagement überwacht dies. Bei Änderungen, die nur ungenügend getestet werden können, ist es in manchen Fällen sinnvoll, diese zunächst nur bei einer kleinen Anwendergruppe einzuspielen. Danach werden die Ergebnisse evaluiert, bevor die Änderung auf allen Systemen umgesetzt wird. Ist dies aufgrund der Gegebenheiten nicht möglich oder sinnvoll, beispielsweise weil vergleichbare Änderungen schon häufig ohne Probleme durchgeführt wurden, oder weil miteinander inkompatible Softwarestände eine Teil-Verteilung unmöglich machen, kann auch eine Komplett-Verteilung durchgeführt werden.

**Evaluation**

Durchgeführte Änderungen sollten anschließend evaluiert werden. Danach wird das Ergebnis vom Änderungsmanagement bzw. vom CAB (Change Advisory Board) anhand der folgenden Aspekte bewertet:

- Hat die Änderung bzw. der Patch das angestrebte Ziel erreicht?
- Sind die Auftraggeber und die Anwender mit dem Ergebnis zufrieden?
- Sind Seiteneffekte (Störungen bei nicht von der Änderung betroffenen Anwendungen) aufgetreten?
- Wurden die veranschlagten Kosten, der geplante Aufwand und der Zeitplan eingehalten?

Wurde die Änderung erfolgreich durchgeführt, kann die Änderungsanforderung (Request for Change) bzw. der Änderungsdatensatz geschlossen werden. Ist die Änderung fehlgeschlagen, muss entschieden werden, ob die durchgeführten Änderungen angepasst werden müssen. In machen Fällen empfiehlt es sich, die Änderung rückgängig zu machen und eine neue oder abgeänderte Änderungsanforderung auszuarbeiten. Bei einer fehlgeschlagenen Änderung kann es auch sinnvoll sein, die Ursachen zu beleuchten und davon ausgehend IT-Systeme oder Prozesse anzupassen. So können ähnliche Probleme zukünftig vermieden werden.

Je nach Art und Umfang der Änderung kann es sinnvoll sein, eine Evaluation direkt nach dem Einspielen durchzuführen. Andererseits kann es auch sinnvoll sein, einige Tage oder Wochen abzuwarten, bis die Auswirkungen der Änderung und die Zielerreichung abzusehen sind. Durchgeführte Änderungen sind erst dann erfolgreich abgeschlossen, wenn sie positiv evaluiert und dokumentiert wurden. Damit dies nicht vergessen wird, sollte sich der Änderungsmanager über eine zeitliche automatisierte Wiedervorlage daran erinnern lassen.

**Rücknahme von Änderungen**

Ob es notwendig ist, Hard- oder Software-Änderungen zurückzuziehen, ergibt sich direkt aus der Evaluation. Haben die Änderungen den gewünschten Erfolg nicht erreicht oder hat sich die Situation sogar verschlechtert, sollten die Änderungen zurückgenommen werden, wenn es technisch möglich und wirtschaftlich vertretbar ist.

Dies kann häufig durch die benutzte Patch- und Änderungsmanagementsoftware technisch unterstützt werden. Ist dies nicht der Fall, müssen die Patches und Änderungen manuell rückgängig gemacht werden.

**Abschluss und Dokumentation**

Es empfiehlt sich, alle Änderungsanforderungen, Hard- und Software-Änderungen, Testdurchführungen und -ergebnisse in einer Datenbank zu dokumentieren, unabhängig davon, ob sie erfolgreich waren oder nicht, (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*). Das Wissen um Fehler bei der Installation der Änderungen und deren Lösungen sollte als Wissen in der Institution für den Wiederholungsfall zur Verfügung stehen.

In vielen Institutionen ist es inzwischen Routine, Betriebssysteme und Anwendungen regelmäßig mit den verfügbaren Software-Updates zur Behebung von Schwachstellen und dem Schutz vor Schadsoftware zu versorgen. Dieses Verfahren ist jedoch auch für Hardware notwendig, was bei ordnungsgemäßer Funktionalität der Hardware oft in Vergessenheit gerät. In vielen IT-Geräten kommen kompakte Betriebssysteme zum Einsatz, die oft auf die jeweili-

ge Hardware zugeschnitten sind. Dazu gehören beispielsweise Router, Switches, Netzdrucker und Mobiltelefone. Daher muss sichergestellt sein, dass auch solche Geräte ins Änderungsmanagement einbezogen und mit sicherheitsrelevanten Updates versorgt werden.

Prüffragen:

- Existiert ein definierter Prozess für Patch- und Änderungsmanagement?
- Werden alle Änderungen von Hard- und Softwareständen und Konfigurationen vom Patch- und Änderungsmanagement gesteuert und kontrolliert?

# M 2.422 Umgang mit Änderungsanforderungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Änderungsmanager

Die Anträge für Patches und Änderungen sollten nach einem festgelegten Vorgehen eingereicht und bearbeitet werden.

**Einreichen und Erfassen von Änderungsanforderungen**

Zunächst müssen alle Änderungsanforderungen (Request for Changes, RfCs) erfasst werden. Damit alle notwendigen Informationen vorliegen, empfiehlt es sich, den Antragstellern ein Formular zur Verfügung zu stellen (siehe Muster einer Änderungsanforderung aus den Hilfsmitteln zum IT-Grundschutz).

Dieser Antrag dient ebenfalls dazu, die Änderung abzustimmen (siehe auch: M 2.427 *Abstimmung von Änderungsanforderungen*). Wenn beispielsweise eine Änderung beantragt wurde, um ein bestehendes Problem zu lösen, sollte auch eine entsprechende Referenz auf das Problem, meist eine Erfassungsnummer in einer Datenbank, mit dokumentiert werden.

Nicht jeder Änderungsantrag wird innerhalb des Patch- und Änderungsprozesses als normale Änderung behandelt. Einige routinemäßige Änderungen, die klar umschrieben sind, standardisiert durchgeführt werden und dennoch eine Änderung betreffen, können wie eine Serviceanfrage behandelt werden. Eine Serviceanfrage wäre zum Beispiel das Zurücksetzen eines Passworts und, bezogen auf das Patch- und Änderungsmanagement, eine Änderung am Login-Banner eines Dienstes (der Text mit dem sich der Dienst bei einem Verbindungsaufbau über die Netzwerkschnittstelle meldet).

**Änderungsanforderungen filtern und akzeptieren**

Nachdem eine Änderungsanforderung erfasst wurde, wird sie durch den Änderungsmanager (Change Manager) kontrolliert. Dabei sollen nicht durchführbare, unnötige oder doppelte Änderungsanforderungen ermittelt werden. Solche Anträge sollten unter Angabe des Grundes abgelehnt werden. Die Antragsteller haben damit die Möglichkeit, die Änderungsanforderung zu überdenken und umzuformulieren.

Wenn eine Änderungsanforderung akzeptiert wurde, werden die Informationen in einem Änderungsdatensatz aufgenommen, um die Änderung durchzuführen. Der Datensatz kann in einem Software-Werkzeug, auf Papier oder auch in einer selbst erstellten Datenbank erfasst werden. Im weiteren Verlauf werden dem Änderungsdatensatz noch die nachstehenden Informationen hinzugefügt:

- Ermittelte Priorität und Kategorie,
- Beurteilung der Auswirkungen und die erforderlichen Ressourcen,
- Empfehlungen des Änderungsmanagers bzw. des Änderungsberatungsausschusses (Change Advisory Boards, CABs),
- Datum und Uhrzeit der Autorisierung,
- Geplantes Datum für die Umsetzung der Änderung,
- Aktuelles Datum und aktuelle Uhrzeit der Änderung,
- Datum der Auswertung,
- Testergebnisse und aufgetretene Probleme,
- Begründung für eine eventuelle Ablehnung des Vorschlags bzw. des Antrags und

- Ablaufplan und Auswertungsdaten.

**Änderungsanforderungen klassifizieren (Priorität und Kategorie)**

Nachdem eine Änderungsanforderung akzeptiert worden ist, muss sie priorisiert und kategorisiert werden:

- Die Priorität beschreibt, wie wichtig eine Änderung ist und leitet sich von der Dringlichkeit und den Auswirkungen ab. Wenn es sich um die Korrektur eines bekannten Fehlers handelt, der schon einmal im Rahmen des Patch- und Änderungsmanagements eingestuft worden ist, wird die Priorität unter Umständen bereits mit übergeben. Dabei sollten die Priorität der Änderung jedoch immer noch einmal vom Änderungsmanager überprüft und gegebenenfalls korrigiert werden. Gleiches gilt für Sicherheitspatches oder Updates, die von der Informationssicherheit beantragt werden. Die endgültige Priorität wird jedoch innerhalb des Änderungsmanagements unter Berücksichtigung der anderen in Bearbeitung befindlichen Änderungsanforderungen festgelegt.
- Die Kategorie wird vom Änderungsmanager auf der Grundlage von den zu erwartenden Auswirkungen und benötigten Ressourcen bestimmt.

Die aus Priorität und Kategorie zusammengesetzte Klassifizierung legt die weitere Bearbeitung der Änderungsanforderung fest und beschreibt somit die Bedeutung der geplanten Änderung.

Prioritäten werden vom Änderungsmanager für eine Änderung vergeben und sind in unterschiedliche Prioritätsstufen eingeteilt, wobei das Sicherheitsmanagement ein Einspruchsrecht gegen zu niedrige bzw. falsche Priorisierung erhalten sollte. Es können beispielsweise die folgenden Prioritätsstufen vom Änderungsmanagement vergeben werden:

- höchste Priorität:
  Eine Änderungsanforderung mit höchster Priorität bezieht sich z. B. auf ein Problem, das für die Zielgruppe im Rahmen der Nutzung wichtiger IT-Dienste erhebliche Schwierigkeiten verursacht. Auch dringend benötigte Anpassungen der IT (z. B. um eine Sicherheitslücke zu schließen, für die ein Wurm im Internet kursiert) werden mit dieser Priorität versehen. Änderungen dieser Priorität werden auch "Urgent Changes" genannt. Diese Änderungen unterscheiden sich von denen mit hoher und normaler Priorität dadurch, dass in diesem Fall die benötigten Ressourcen sofort zur Verfügung gestellt werden sollten. Eine Dringlichkeitssitzung des CAB oder des Informationssicherheitsmanagement-Team kann ebenfalls erforderlich sein. Wenn Änderungen in diese Priorität eingestuft werden, können alle früheren Planungen Verzögerungen erfahren oder vorerst eingestellt werden.
- hohe Priorität:
  Diese Priorität beschreibt z. B. eine Änderung aufgrund einer schwerwiegenden Störung oder hängt mit anderen dringenden Aktivitäten zusammen. Diese Änderung erhält bei der nächsten Sitzung des CAB oberste Priorität bei der Zuordnung von Ressourcen für Test- und Durchführung.
- normale Priorität:
  Eine Änderung mit normaler Priorität hat keine besondere Dringlichkeit oder größere Auswirkung, darf aber nicht auf einen späteren Zeitpunkt verschoben werden. Im CAB erhält diese Änderung bei der Zuteilung von Ressourcen normale Priorität.
- niedrige Priorität:
  Eine Änderung mit niedriger Priorität ist erwünscht, hat jedoch Zeit, bis sich eine geeignete Gelegenheit ergibt (z. B. eine Folgeversion oder eine geplante Wartung).

Kategorien werden in der Regel vom Änderungsmanagement zugewiesen, wobei auch hier das Sicherheitsmanagement ein Einspruchsrecht gegen eine zu niedrige Kategorisierung erhalten sollte. Kategorien sollen eine Einschätzung darüber liefern, wie sich die Änderung auswirkt und wie die Institution durch den Änderungsprozess belastet wird. Beispielsweise können nachstehende Kategorien vergeben werden:

- geringfügige Folgen:
  Eine Änderung dieser Kategorie erfordert wenig Aufwand. Der Änderungsmanager kann diese Art von Änderungen genehmigen, ohne dass er sie dem CAB vorlegen muss.
- erhebliche Folgen:
  In diese Kategorie fallen Änderungen, die einen erheblichen Aufwand erfordern und weitreichende Auswirkungen auf die IT-Dienste zur Folge haben. Solche Änderungen werden im CAB besprochen, um den erforderlichen Aufwand zu definieren und das Risiko zu minimieren. Im Vorfeld und zur Vorbereitung der Sitzung wird zunächst die notwendige Dokumentation an die Mitglieder des CAB sowie gegebenenfalls auch an einige IT-Spezialisten und Entwickler verschickt.
- weitreichende Folgen:
  Eine Änderung dieser Kategorie erfordert einen großen Aufwand. Für eine solche Änderung benötigt der Änderungsmanager zunächst die Autorisierung durch das Sicherheitsmanagement-Team. Anschließend muss die Änderung dem CAB noch zur Beurteilung und weiteren Planung vorgelegt werden.

**Planung**

Die am Patch- und Änderungsmanagementprozess beteiligten Mitarbeiter planen die Umsetzung für alle angenommenen Änderungen. Bei Bedarf geschieht dies zusammen mit dem CAB. An dieser Stelle des Patch- und Änderungsmanagementprozesses ist es wichtig, die dazu benötigten technischen und personellen Ressourcen zu berücksichtigen und die Auswirkungen auf den Betrieb während der Durchführung der Änderung abzuschätzen. Die folgenden Aspekte sollten mindestens berücksichtigt werden:

- Verfügbarkeit der betroffenen IT-Systeme,
- Zuverlässigkeit und Wiederherstellbarkeit der betroffenen IT-Dienste,
- Planung des Notfallmanagements für die betroffenen IT-Dienste,
- Blackout-Pläne, also Notfallpläne für die Reaktion auf unerwünschte Effekte durch die Änderung,
- Datensicherungsverfahren,
- Mögliche Auswirkungen der Änderungen auf andere IT-Dienste (Seiteneffekte),
- benötigte technische und personelle Ressourcen und deren Kosten
- benötigte Genehmigungen wie
  - finanzielle Genehmigungen, wenn beispielsweise ein kostenpflichtiges Update eingespielt werden oder auf ein Folgeprodukt (Upgrade) gewechselt werden muss.
  - technische Genehmigungen, weil beispielsweise zusätzliche IT-Systeme beschafft werden müssen.
  - geschäftliche Genehmigungen, weil beispielsweise die Aktualisierung Auswirkungen auf Zulieferer hat.
- Anzahl und Verfügbarkeit der benötigten IT-Spezialisten,
- gewünschte zeitliche Umsetzung einer Änderung,
- Konsequenzen für die Nutzung der IT-Dienste und daraus resultierende Anpassungen an Service-Level-Vereinbarungen,
- eventuelle Konflikte mit anderen Änderungen.

Prüffragen:

- Gibt es ein festgelegtes Verfahren, wie Anträge für Patches und Änderungen eingereicht und bearbeitet werden?
- Werden alle Änderungsanforderungen (RfCs) erfasst und dokumentiert?
- Erfolgt eine Kontrolle der erfassten Änderungsanforderungen durch den Änderungsmanager?
- Wird jede Änderungsanforderung priorisiert und kategorisiert?
- Werden für die jeweiligen Prioritäten die benötigten Ressourcen zur Verfügung gestellt?

# M 2.423 Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Beim Aufbau des Patch- und Änderungsmanagements müssen eine Reihe von Verantwortlichkeiten geregelt werden. Es ist dabei sicherzustellen, dass für jeden Aufgaben- und Organisationsbereich exakt definiert ist, welche Verantwortlichkeiten im Patch- und Änderungsprozess ein Mitarbeiter besitzt und wie die Koordination zwischen den einzelnen Bereichen abzulaufen hat.

Teilweise ist es üblich, dass die Mitarbeiter verschiedener Bereiche einer Institution unterschiedliche Verantwortlichkeiten bezüglich der Durchführung von Änderungen besitzen. So kann beispielsweise ein Bereich für die Betreuung der Basis-Betriebssysteme zuständig sein und ein anderer Bereich die darauf installierten Dienste (z. B. E-Mail-Server, Fachanwendung, etc.) betreuen. Dies kann dann dazu führen, dass unterschiedliche Bereiche für das Patchen eines Gesamtsystems verantwortlich sein können. In solchen Fällen ist es besonders wichtig, dass die Zuständigkeiten sauber festgelegt worden sind.

Die so aufgeteilten Verantwortlichkeiten sollten sich auch im Berechtigungskonzept bei der Konfiguration der Werkzeuge für die Verteilung von Patch- und Änderungen und des IT-Systems wieder finden.

Es ist unbedingt ein koordinierter Ablauf von Änderungen erforderlich. Kein Mitarbeiter darf Änderungen durchführen, ohne diese vorher mit dem Änderungsmanagement abzusprechen. Auch alle Mitarbeiter des IT-Betriebs müssen relevante Änderungen grundsätzlich mit dem Änderungsmanagement absprechen. Damit wird sichergestellt, dass etwaige Änderungen sich nicht gegenseitig behindern oder gar zu einem Systemausfall führen.

Die zentrale Rolle, die die Koordination und Bewertung der Änderungen übernimmt, ist der Änderungsmanager (Change Manager). Hierfür muss in der Institution eine Person benannt sein, um ein effizientes und effektives Patch- und Änderungsmanagement zu betreiben. Der Änderungsmanager filtert, akzeptiert und klassifiziert sämtliche Änderungsanforderungen. Er ist zudem sowohl für die notwendigen Autorisierungen als auch die Planung, Koordinierung und Durchführung von Änderungen verantwortlich.

Bei einer Institution mindestens mittlerer Größe oder mit komplexen IT-Infrastrukturen sollte der Änderungsmanager bei seiner Arbeit durch ein Change Advisory Board (CAB) unterstützt werden. Es hat sich bewährt, neben den mit der technischen Umsetzung von Patch- und Änderungsaufgaben betrauten Personen auch eine Person aus jeder Fachabteilung als Mitglied in das CAB zu berufen. Das CAB wird regelmäßig zu bestimmten Zeiten einberufen, um Änderungen zu beurteilen und dem Änderungsmanager zu helfen, diese einzuschätzen, zu priorisieren und zu autorisieren. In der Regel wird dem CAB nur die Auswahl schwerwiegender Änderungen vorgelegt. Zu diesem Zweck kann das CAB hinsichtlich seiner Mitglieder unterschiedlich zusammengesetzt sein. Das komplette CAB könnte beispielsweise alle 3 Monate zusammenkommen und über kritische Änderungsanforderungen diskutieren.

Für unkritische regelmäßige Änderungen können die Absprachen direkt zwischen dem Änderungsmanager und den verantwortlichen Administratoren bzw. dem Test-Team erfolgen.

Damit das CAB seine Tätigkeiten angemessen durchführen kann, müssen seine Mitglieder die Bedeutung und Auswirkung von Änderungen sowohl aus Sicht der Geschäftsziele und -prozesse als auch vom technischen Standpunkt aus beurteilen können.

Prüffragen:

- Sind für alle Organisationsbereiche Verantwortliche für das Patch- und Änderungsmanagement benannt?
- Spiegeln sich die festgelegten Zuständigkeiten beim Patch- und Änderungsmanagement auch im Berechtigungskonzept wieder?
- Ist ein Änderungsmanager benannt worden?
- Sind alle mit der Umsetzung des Patch- und Änderungsmanagementprozesses betrauten Personen mit den Begriffen des Patch- und Änderungsmanagement, der Informationssicherheit und der kryptographischen Verfahren vertraut?

# M 2.424 Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Änderungsmanager, IT-Sicherheitsbeauftragter

Ein Patch- und Änderungsmanagement-Werkzeug spielt als zentrale Instanz zur Umsetzung des Patch- und Änderungsmanagementprozesses und zur Softwareverteilung für den sicheren und ordnungsgemäßen Betrieb der Institution eine wesentliche Rolle.

Das Patch- und Änderungsmanagement muss mit einem angemessenen organisatorischen und technischen Aufwand betrieben werden. Dabei ist unter anderem der Schutzbedarf der Geschäftsprozesse und damit der Schutzbedarf der Daten und Systeme zu berücksichtigen. Dafür sollte eine spezifische Sicherheitsrichtlinie für das Patch- und Änderungsmanagement erstellt werden. Diese muss mit dem Sicherheitskonzept der Institution und den daraus abgeleiteten Sicherheitsrichtlinien abgestimmt sein.

Aspekte, zu denen in dieser Sicherheitsrichtlinie Vorgaben formuliert werden müssen, sind:

**Vorgaben für die Planung:**
- Zur Skalierbarkeit der Serverapplikation des Werkzeugs müssen bereits im Vorfeld Anforderungen zum Einsatz von Replikation, Lastverteilung und der Möglichkeit, technische Redundanzen zu benutzen, formuliert werden.
- Für eine sichere Netzverbindung zu externen Bezugsquellen von Patches oder Änderungen z. B. bei Herstellern müssen geeignete Regelungen festgelegt werden. Beispielsweise könnte die Direktverbindung der Clients zu den Herstellern der eingesetzten Software durch entsprechende Regeln auf dem Sicherheitsgateway auf einen Proxy umgeleitet werden.
- Damit Integrität und Authentizität von Patches und Änderungen zuverlässig überprüft werden kann, müssen geeignete Konzepte und Komponenten festgelegt werden.
- Es müssen Anforderungen zum Bereitstellen der Dokumentation für Betrieb, Notfall und Wiederanlauf des Patch- und Änderungsmanagement-Werkzeugs formuliert werden. Zu den Anforderungen gehören unter anderem, dass die Dokumentation immer aktuell sein muss. Des Weiteren sollte definiert werden, wo die Dokumentation gelagert werden muss und wie viele Exemplare der Dokumentation vorhanden sein müssen.

**Vorgaben für die Administration**
- Es ist erforderlich, ein Rechtekonzept für Mitarbeiter im Patch- und Änderungsmanagement und auch für die Dienste, welche von der Patch- und Änderungsmanagementsoftware verwendet werden, zu erstellen.
- Für die Administratoren ist festzulegen, wie Rechte vergeben werden. welche sie bekommen oder welche sie verteilen dürfen.

**Vorgaben für die Installation**

Die Werkzeuge für das Patch- und Änderungsmanagement müssen sicher konfiguriert werden. Die jeweiligen konkreten Einstellungen hängen stark von den vorhandenen Anwendungen und IT-Systemen der Institution ab. Allge-

meine Hinweise hierzu finden sich in M 4.237 *Sichere Grundkonfiguration eines IT-Systems*.

- Es muss festgelegt werden, wie die für das Patch- und Änderungsmanagement-Werkzeug relevanten IT-Ressourcen, wie beispielsweise die Komponenten der Software zur Verteilung von Patches und Änderungen und der Betriebssysteme unter Berücksichtigung von Sicherheitsaspekten konfiguriert werden.
- Das Patch- und Änderungsmanagement-Werkzeug sollte angemessen im LAN separiert werden. Neue Änderungen und Patches sollten nicht im Produktivnetz getestet werden, sondern in einem separaten Testnetz.

**Vorgaben für den sicheren Betrieb**

- Für den Betrieb eines Patch- und Änderungsmanagement-Tools sind Vorgaben und Abläufe festzulegen, also beispielsweise, wer darauf zugreifen darf und wo Änderungen durchgeführt werden dürfen.
- Patches und Änderungen werden häufig über das Internet bezogen. Verbindungen in öffentliche oder weniger vertrauliche Netze sind grundsätzlich über Sicherheitsgateways abzusichern.
- Das Patch- und Änderungsmanagement-Werkzeug selbst muss in den Prozess des Patch- und Änderungsmanagements mit eingegliedert werden. In dem Zusammenhang ist zu definieren, wie Hard- und Software-Änderungen für das Patch- und Änderungsmanagement-Werkzeug selbst zu behandeln sind.

**Vorgaben für Protokollierung und Monitoring**

Die Art und Weise der Überwachung, Protokollierung und der Auswertung der vom Patch- und Änderungsmanagement-Werkzeug gelieferten Daten ist festzulegen

**Datensicherung**

Ein geeignetes Verfahren für die Datensicherung ist festzulegen. Bei der Datensicherung sollten mindestens folgende Komponenten in regelmäßigen Abständen gesichert werden:

- Die Konfiguration bzw. die Einstellungen der für das Patch- und Änderungsmanagement benötigten Werkzeuge
- Die Datenbanken mit den aktuellen Konfigurationen der IT-Systeme
- Bei selbstübersetzter Software die genauen Compiler-Einstellungen
- Die installierten Patches und Änderungen
- Die letzten Wiederherstellungspunkte der IT-Systeme
- Eventuell vorhandene ältere Versionsstände, beispielsweise weil die neuste Version einer Software noch nicht ausreichend getestet wurde oder nicht auf allen Systemen lauffähig ist
- Eine Übersicht über die Vergleichsprüfsummen der Softwarepakete, diese sollte eventuell auf einem Write Once Read Many - Medium (WORM) gesichert werden

Des Weiteren muss das Verfahren für das Patch- und Änderungsmanagement-Werkzeug in das übergreifende Datensicherungskonzept der Institution eingebunden werden (siehe auch M 6.32 *Regelmäßige Datensicherung*).

**Störung und Notfallvorsorge**

Für die Notfallvorsorge müssen die einzelnen Notfällplane der Anwendungen und IT-Systeme, die vom Patch- und Änderungsmanagement verwaltet werden, berücksichtigt werden.

In Abhängigkeit von den Verfügbarkeitsanforderungen an das Patch- und Änderungsmanagement-Werkzeugs sollte überlegt werden, ob für das Patch- und Änderungsmanagement-Werkzeug ein separater Notfallplan für unerwünschte Effekte bei und nach der Installation von Patches und Änderungen erstellt wird.

Prüffragen:

- Gibt es eine Sicherheitsrichtlinie für das Patch- und Änderungsmanagement-Werkzeug?
- Werden in der Sicherheitsrichtlinie alle relevanten Aspekte für den Einsatz eines Patch- und Änderungsmanagement-Werkzeugs berücksichtigt?

# M 2.425 Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement

**Verantwortlich für Initiierung:** Änderungsmanager, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, Änderungsmanager

Der Patch- und Änderungsmanagementprozess kann mit verschiedenen Produkten oder Produktkombinationen unterstützt werden. Es kann vielfältige Gründe geben, ein Werkzeug zur Umsetzung und Durchführung des Patch- und Änderungsprozesses einzusetzen. Häufig sind heterogene IT-Infrastrukturen und die effektivere Ausnutzung von Ressourcen bestimmend.

Vor der Beschaffung eines Werkzeugs für das Patch- und Änderungsmanagement sollten die Anforderungen und Rahmenbedingungen ermittelt werden, um ein für die jeweilige Institution geeignetes Werkzeug zu finden. Das Vorgehen für die Evaluation eines Produktes ist stets ähnlich und orientiert sich an der gültigen Patch-Strategie der Institution, unabhängig davon, ob ein Patch- und Änderungsmanagement als Werkzeug für ein Betriebssystem, für die Produktpalette eines Herstellers oder für ein großes heterogenes IT-Szenario benötigt wird.

Nachfolgend ist eine Auswahl der wichtigsten Ausstattungsmerkmale zu finden, welche bei der Produktwahl beachtet werden sollten und die die Basis für die Formulierung der Anforderungen an das Softwarewerkzeug sind.

- Plattformunterstützung:
  Unter diesem Begriff rangieren grundsätzlich zwei Aspekte. Einerseits wird hier betrachtet, welche Plattformen bezüglich Umsetzung des Patch- und Änderungsprozesses unterstützt werden und andererseits, auf welcher Plattform das Werkzeug lauffähig ist. Besonders der erste Aspekt sollte sehr detailliert betrachtet werden, da beispielsweise im Server-Client-Bereich die meisten Werkzeug-Hersteller Änderungsvorgänge bei Microsoft-Produkten unterstützen. Dies heißt jedoch nicht, dass auch die gesamte in der Institution vorhandene IT-Produktpalette von Desktop- und Server-Betriebssystem über Applikationsserver bis hin zu Einzelprodukten abgedeckt wird.
- Patchanalyse:
  Einige Hersteller konzentrieren sich auf die mit dem Verteilungsprozess verbundene Menge der Updates und ihrer raschen Verteilung sowie dem Reporting des "Auslieferungsstatus". Einige liefern mehr Informationen zu den Hintergründen bzw. Gründen eines Patches, teilweise mit Listen betroffener Dateien, genauer Beschreibung der Schwachstellen und eigenen Testberichten. Insbesondere für die Verwendung von Sicherheitspatches, welche in der Regel rasch verteilt werden sollten, können die Detailinformationen einen unverzichtbaren Hinweis für die interne Einstufung der Hard- oder Software-Änderung enthalten.
- Patchverifikation:
  Die meisten Hersteller liefern Hash-Summen, Fingerprints oder Signaturen mit den Patches und Änderungen, um deren Echtheit und Integrität zu bestätigen, jedoch prüfen nur wenige Werkzeuge diese Nachweise auch. Auf Grund dessen besteht die Gefahr, dass unerwünschte Software massenhaft in der Institution verteilt und erheblicher Schaden verursacht wird. Aus Sicherheitsgründen sollten daher keine Änderungswerkzeuge eingesetzt werden, bei denen diese Funktionalität fehlt.

- Patchstrategie:
  Das Werkzeug muss eine flexible Konfiguration ermöglichen, um möglichst viele Schritte der gewählten Patchstrategie automatisieren zu können. Diese kann, auf Grund unterschiedlicher Plattformen, stark differieren. Die abgearbeiteten Schritte des Änderungsprozesses sollten vom Tool nachvollziehbar, je nach Bedarf sogar revisionssicher, dokumentiert werden. Spätere Änderungen im Prozess müssen in das Werkzeug einfließen können.
- Verteilung:
  Nicht jeder Patch sollte auf jedes System ausgebracht werden. Das Werkzeug sollte die Gruppierung von Systemen und Applikationen nach frei definierbaren Attributen wie z. B. Schutzbedarf, Standort und Organisationseinheit ermöglichen. Aus diesen Attributen können IT-Systemprofile, entsprechend den standardisierten Systemtypen in der Institution, werden.
- Rollback:
  Keine Software ist perfekt. Deshalb kann trotz aller Vortests die Notwendigkeit entstehen, einen Patch-Prozess umzukehren. Die Automatisierung dieses Vorgangs spart im Fehlerfall Zeit und Geld! Wenn sich fehlerhafte Änderungen nicht zeitnah und mit geringem Aufwand zurücknehmen lassen, kann dies die Institution erheblich schädigen.
- Statusbewertung:
  Es muss ein Automatismus existieren, um die geänderte Hard- oder Software auf allen Systemen korrekt zu verteilen. Es könnten, wie bei Softwareverteilung im Allgemeinen, Probleme mit der Verbindung oder Verfügbarkeit eines Systems auftreten. Ein Patch kann dann vom System auf Grund anderer Systemzustände abgelehnt werden. Wichtig ist daher die Möglichkeit, dass das Änderungswerkzeug den Patch-Status aller Systeme erfasst. Je nach Strategie sollte das Werkzeug bei aufgetretenen Problemen den technischen Patch-Prozess bei den restlichen IT-Systemen fortsetzen oder bestimmte Systemgruppen überspringen oder den Patch-Prozess beenden.

Prüffragen:

- Sind die Anforderungen und Rahmenbedingungen für die Auswahl eines Werkzeugs für das Patch- und Änderungsmanagement bestimmt?

# M 2.426 Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse

**Verantwortlich für Initiierung:** Änderungsmanager, Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Änderungsmanager

Je nach Art der durchgeführten Änderungen kann es notwendig sein, dass eine Anwendung oder ein IT-System neu gestartet werden muss, was zur Folge hat, dass diese über einen kurzen Zeitraum nicht im Produktivbetrieb benutzt werden können. Darüber hinaus können auch sorgfältig durchgeführte Tests nicht immer vermeiden, dass es zu Schwierigkeiten bei der betroffenen Anwendung oder gar zum Stillstand und damit Ausfall eines Systems durch die Verteilung von Hard- oder Software-Änderungen kommen kann.

Aus diesem Grund ist, unabhängig von durchgeführten Tests, auch die aktuelle Situation der betroffenen Geschäftsprozesse zu berücksichtigen. Es kann z. B. durchaus sinnvoll sein, eine Hard- oder Software-Änderung ein paar Tage später durchzuführen, obwohl das betroffene System zum aktuellen Zeitpunkt als sicherheitskritisch eingestuft wird. Eventuell werden durch das System wichtige Dienstleistungen erbracht, auf die die Institution angewiesen ist. Die Leitungsebene könnte das Risiko einer Unterbrechung von Geschäftsprozessen durch das Patch- und Änderungsmanagement höher bewerten als das Risiko durch eine noch nicht geschlossene Schwachstelle.

Um Hard- und Software-Änderungen zu verteilen, ist es daher notwendig, alle Beteiligten bezüglich der kommenden Änderungen und der zu erwartenden Ausfallzeiten zu benachrichtigen. Zu den einzelnen Parteien gehören alle Fachabteilungen, die das System benötigen. Insbesondere Fachabteilungen, deren Aufgabenerfüllung von den betroffenen Anwendungen und IT-Systemen abhängig ist, müssen in die Priorisierung von Änderungen und in die Terminfindung einbezogen werden.

Es muss mindestens eine Eskalationsebene über dem Änderungsmanager und dem CAB existieren, welche notfalls die Entscheidung über die Priorisierung (siehe M 2.422 *Umgang mit Änderungsanforderungen*), übernimmt. Diese Eskalationsebene muss aus der Leitungsebene der Institution gewählt werden.

Prüffragen:

- Wird die aktuelle Situation der von geplanten Änderungen betroffenen Geschäftsprozesse berücksichtigt?
- Werden die relevanten Fachabteilungen über anstehende Änderungen informiert?
- Gibt es eine Eskalationsebene, deren Mitglieder aus der Leitungsebene der Institution sind, die in Zweifelsfällen Entscheidungen bezüglich der Priorität und Terminplanung einer Hard- oder Software-Änderung treffen kann?

# M 2.427 Abstimmung von Änderungsanforderungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Änderungsmanager

Der Erfolg des Patch- und Änderungsmanagementprozesses hängt von einer effektiven Kommunikation ab, da die einzelnen Prozessschritte, wie sie in M 2.421 *Planung des Patch- und Änderungsmanagementprozesses* und M 2.422 *Umgang mit Änderungsanforderungen* festgelegt wurden, oft nur weiter durchgeführt werden können, nachdem eine Reaktion der verantwortlichen Rollen vorliegt.

In den Abstimmungsprozess, um eine Hard- oder Softwareänderung durchzuführen, sind außer dem Change Advisory Board (CAB) eventuell weitere Zielgruppen einzubeziehen. Welche dies sind, hängt von der Größe und der Struktur der Institution ab. Typischerweise sollten der Antragsteller einer Hard- oder Softwareänderung, der IT-Helpdesk und der von den Auswirkungen der Änderung betroffene Endbenutzer bzw. ein Vertreter des Fachbereiches einbezogen werden.

Den Geschäftsprozess-Verantwortlichen muss das Antragsverfahren für Hard- oder Softwareänderungen bekannt sein, sowie welchen Prozess der Antrag durchläuft und welche Informationen im Verlauf des Antragsverfahrens bereit gestellt werden. Ein wesentlicher Aspekt ist die inhaltliche Qualität des Änderungsantrages (RfCs). Die notwendigen Angaben werden häufig als Formular oder über eine Eingabemaske in einer speziellen Anwendung erfasst. Welche Informationen benötigt werden und wie das Formular aufgebaut wird, sollte daher mit besonderer Sorgfalt, in Abstimmung mit den möglichen Zielgruppen, festgelegt werden.

Ferner muss durch den Patch- und Änderungsmanagementprozess sicher gestellt werden, dass bei schwerwiegenden Änderungen alle Fachverantwortlichen die Möglichkeit haben, sich zu dem Antragsinhalt zu äußern, um eine, aus Sicht einer Zielgruppe, unerwünschte Änderung zu verhindern.

Auf der anderen Seite darf das Antragsverfahren nicht zu lange dauern. Es muss außerdem möglich sein, wichtige Änderungen beschleunigt zu behandeln. Dabei muss es unter Umständen definiert erlaubt sein, den regulären Patch- und Änderungsmanagementprozess abzukürzen.

Prüffragen:

- Werden beim Abstimmungsprozess zur Durchführung einer Änderung alle betroffenen Zielgruppen berücksichtigt?
- Ist sichergestellt, dass sich alle von der Änderung betroffenen Zielgruppen, nachweisbar zu dieser äußern können?
- Gibt es ein festgelegtes Verfahren, durch das wichtige Änderungsanforderungen beschleunigt werden können?

# M 2.428 Skalierbarkeit beim Patch- und Änderungsmanagement

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Änderungsmanager

Bei der Beschaffung eines Patch- und Änderungsmanagement-Werkzeugs gelten oft andere Anforderungen als im späteren Betrieb. Die IT-Landschaft wächst und zusätzliche IT-Systeme, die vom Patch- und Änderungsmanagement berücksichtigt werden müssen, kommen hinzu. Daher ist es wichtig, dass das Patch- und Änderungsmanagement-Werkzeug skaliert werden kann. Welche Skalierbarkeit bei der Einführung des Systems benötigt wird, muss bereits während der Planungsphase ermittelt werden.

Die Hauptfaktoren, welche die Skalierbarkeit beeinflussen, sind die geforderte Umsetzungsgeschwindigkeit für das Verteilen der Hard- oder Software-Änderungen in Bezug auf die vorhandene IT-Infrastruktur und die Notwendigkeit, im Fehlerfall die IT-Systeme massiv parallel wiederherzustellen.

Für den Fall, dass fehlerhafte Hard- oder Software-Änderungen verteilt werden, müssen definierte Unterbrechungspunkte für die Verteilung definiert werden. Da diese Möglichkeit stark von der Umsetzungsgeschwindigkeit abhängig ist, muss festgelegt werden, wo, wie und zu welchem Zeitpunkt eine bewusste Unterbrechung der Verteilung möglich ist.

Um festzustellen, ob eine erwartete Umsetzungsgeschwindigkeit besteht, können zunächst Betriebswerte der IT-Infrastruktur wie Netzbandbreiten und Systemauslastung dienen. Die Umsetzungsgeschwindigkeit muss bei den Tests vor Inbetriebnahme des Systems jedoch sorgfältig praktisch überprüft werden. Auf eventuelle auftretende Engpässe in der IT-Infrastruktur muss rasch durch Erweiterung oder Konfigurationsänderung reagiert werden.

Zu den ermittelten Werten ist ein vermutliches Wachstum der IT-Infrastruktur in der direkten Zeit nach der Inbetriebnahme hinzuzurechnen, um nicht sofort in eine weitere Skalierungs- und Umbauphase des Systems überzugehen. Erst sollten weitere Erfahrungswerte aus dem Betrieb gesammelt werden, welche dann als zusätzlichen Anhaltpunkte für den weiteren Ausbau des Systems verwendet werden müssen.

In der Praxis hat sich der Ansatz bewährt, die Skalierbarkeit entsprechend der physischen und geografischen IT-Struktur der Institution umzusetzen. Wenn es die Patch-Strategie der Institution erlaubt, können, z. B. in den jeweiligen Niederlassungen der Institution, Verteilersysteme eingesetzt werden, die jeweils die Software-Änderungen nur für die IT-Systeme des jeweiligen Standortes erhalten und verarbeiten.

Ist die Patch-Strategie der Institution dagegen stark zentral orientiert oder werden die Patch- und Änderungsmanagement-Werkzeuge im Outsourcing betrieben, so ist es empfehlenswert, die Skalierung so zu wählen, dass pro Niederlassung dezidierte Systeme betrieben werden.

Werden Softwarewerkzeuge zur Unterstützung des Patch- und Änderungsmanagements eingesetzt, so ist darauf zu achten, dass diese den Anforderungen an die Skalierbarkeit genügen.

Prüffragen:

- Gibt es bei der Verteilung von Hard- oder Software-Änderungen definierte Unterbrechungspunkte, falls die Hard- oder Software fehlerhaft ist?
- Wird die Umsetzungsgeschwindigkeit vor der Inbetriebnahme eines Patch- und Änderungsmanagement-Werkzeugs sorgfältig geprüft?

# M 2.429 Erfolgsmessung von Änderungsanforderungen

**Verantwortlich für Initiierung:** Änderungsmanager, Leiter IT
**Verantwortlich für Umsetzung:** Änderungsmanager

Managementprozesse wie das Patch- und Änderungsmanagement müssen stetig verbessert, optimiert und an die sich verändernden Bedingungen in der Institution angepasst werden. Die Art und Weise, wie die vorliegende Maßnahme in der Institution umgesetzt wird, zeigt auch den Reifegrad des Patch- und Änderungsmanagement-Prozesses.

Die im Vorfeld von Hardware-, Software- oder Konfigurationsänderungen durchgeführten Tests dienen vorwiegend der Prüfung, ob die Änderungen in dem voraussichtlichen Einsatzfeld grundsätzlich funktionieren. Da Änderungen meistens eine Störung beheben sollen, ist es notwendig, von den Antragstellern der Änderungsanforderung nachträglich eine Auswertung über den Erfolg der Änderung einzuholen.

Dafür ist es unumgänglich, so genannte Nachtests durchzuführen. Als Voraussetzung dafür müssen Referenzsysteme als Qualitätssicherungssysteme ausgewählt werden. Außerdem muss sichergestellt werden, dass die Nachtests durch diejenigen Fachanwender, welche die Geschäftsprozesse der Institution kennen und eventuell vorhandene Fehler beurteilen können, durchgeführt werden.

Wurde die Änderung aus Sicherheitssicht nötig, müssen die Nachtests vom Änderungsmanager initiiert und von Fachanwendern durchgeführt werden.

Die Ergebnissen der Nachtests und Auswertungen werden im Rahmen des Patch- und Änderungsprozesses dokumentiert. Für den Änderungsmanager, das Change Advisory Board und das Sicherheitsmanagement werden somit Daten zur Verbesserung des Prozesses zur Verfügung gestellt.

Prüffragen:

- Werden Nachtests zur nachträglichen Überprüfung der Aktualisierung durchgeführt?
- Wurden Referenzsysteme als Qualitätssicherungssysteme ausgewählt?
- Werden die Ergebnisse der Nachtests und Auswertungen im Rahmen des Patch- und Änderungsprozesses dokumentiert?

# M 2.430 Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer, IT-Sicherheitsbeauftragter

Nicht nur innerhalb der Räumlichkeiten einer Institution müssen Informationen angemessen geschützt werden, dies ist natürlich auch außerhalb erforderlich. Mitarbeiter müssen mit sensiblen Informationen auch auf Geschäfts- oder Privatreisen sorgfältig umgehen.

Es sollte eine Sicherheitsrichtlinie erstellt werden, in der beschrieben ist, was Mitarbeiter bei Geschäfts- oder Privatreisen beachten müssen. Diese kann auch in der Richtlinie für die sichere Nutzung mobiler IT-Systeme integriert sein (siehe M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*). Zusätzlich sollte für die Mitarbeiter ein kurzes und übersichtliches Merkblatt für das richtige Verhalten unterwegs erstellt werden.

**Sensibilisierung der Benutzer**

Die Mitarbeiter sollten darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit fremden Personen austauschen dürfen. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*). Vertrauliche Informationen sollten auch nicht in Hör- und Sichtweite von Externen diskutiert oder weitergegeben werden.

Weiterhin müssen die Mitarbeiter darüber informiert sein, welche Informationen unterwegs bearbeitet werden dürfen. Hierzu sollten die Informationen entsprechend klassifiziert sein, damit die Benutzer eventuelle Einschränkungen klar erkennen können (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Mitarbeiter sollten unter anderem über folgende Aspekte informiert werden:

- Mitarbeiter müssen sich vor der Reise über die Sicherheitslage, Gebräuche und Gesetze des Reiselandes informieren. Hierbei sind beispielsweise die Länder- und Reiseinformationen des deutschen Auswärtigen Amts hilfreich.
- Auf Reisen sollten möglichst keine sensiblen Informationen mitgeführt werden, die nicht unbedingt benötigt werden. Falls dies doch notwendig ist, sollten diese im Handgepäck mitgeführt werden. Das Gepäck sollte nie unbeaufsichtigt bleiben.
- Sensible Informationen sollten nicht unbeaufsichtigt im Hotelzimmer, in Tagungs- oder fremden Büroräumen verbleiben. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe. Hochschutzbedürftige Informationen sollten allerdings auch nicht in einem hoteleigenen Safe verwahrt werden.
- Für die Kommunikation mit der eigenen Institution und Geschäftspartnern sollten nur gesicherte Verbindungen benutzt werden. Da E-Mails ebenso wie Festnetz- und Mobiltelefone überwacht sein könnten, sollte die Kommunikation möglichst mit einer Ende-zu-Ende-Verschlüsselung abgesichert werden, wenn hochschutzbedürftige Informationen weitergegeben werden. Auch bei fremden Faxanschlüsse ist Vorsicht geboten, da die zu

übertragenden Dokumente auf dem Faxgerät gespeichert und später ausgedruckt, also kopiert werden könnten.
- Mitarbeiter sollten misstrauisch werden, wenn sie sich unterwegs ungewöhnlich stark ausgefragt fühlen. Sie sollten niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.
- Geschenke, die digitale Speicher enthalten, z. B. USB-Sticks, sollten mit besonderer Vorsicht behandelt werden, da diese Schadsoftware enthalten könnten. Die Annahme von Geschenken von Geschäftspartnern kann ohnehin problematisch sein, da Gegenleistungen erwartet werden könnten.

**Entsorgung von Datenträgern und Dokumenten**

Auch unterwegs gibt es häufiger Material, das entsorgt werden soll, schon alleine, damit das Gepäck noch tragbar bleibt. Während es aber innerhalb der eigenen Institution eingeübte Verfahren gibt, wie alte oder unbrauchbare Datenträger und Dokumente entsorgt werden (siehe auch M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*), ist dies unterwegs nicht immer möglich. Daher ist vor der Entsorgung ausgedienter Datenträger und Dokumente genau zu überlegen, ob diese sensible Informationen enthalten könnten. Ist dies der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zurück transportiert werden.

Weiterhin ist zu beachten, dass Experten auch von defekten Datenträgern unter Umständen wertvolle Informationen zurückgewinnen können. Solche Datenträger dürfen deshalb ebenfalls nicht einfach weggeworfen werden, wenn darauf schützenswerte Daten gespeichert sein könnten.

Auch Akten- und Datenvernichter ("Shredder") in fremden Institutionen sollten mit Vorsicht betrachtet werden, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt bzw. wie zuverlässig diese ist.

Die Sicherheitsrichtlinie muss daher Regelungen enthalten, wie Mitarbeiter unterwegs mit ausgedienten Datenträgern und Dokumenten umgehen sollen.

Prüffragen:

- Existiert eine Sicherheitsrichtlinie für den Informationsschutz unterwegs?
- Ist jeder Mitarbeiter darüber informiert, was die wichtigsten Sicherheitsmaßnahmen bei Geschäfts- und Privatreisen sind?
- Ist geregelt, wie Mitarbeiter unterwegs mit ausgedienten Datenträgern und Dokumenten umgehen sollen?

# M 2.431 Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Das jeweils geeignete Vorgehen, Daten sicher zu löschen oder zu vernichten, hängt sowohl von der Art der Datenträger als auch vom Schutzbedarf dieser Informationen ab. Die Informationen sollten daher nach ihrem Schutzbedarf klassifiziert sein (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Aus vielerlei Gründen, beispielsweise im Rahmen von Partnerschaften oder Outsourcing-Dienstleistungen, werden sensible Informationen, sowohl auf elektronischen Datenträgern als auch in analoger Form an Dritte übergeben. Vorher ist vertraglich zu regeln, zu welchem Zeitpunkt und in welcher Weise diese Datenträger vollständig zurückzugeben oder zu vernichten sind.

Eine Vielzahl von Gesetzen, Vorschriften und Regelungen, die je nach Art der Institution und ihrer Geschäftsprozesse stark variieren können (siehe auch M 2.340 *Beachtung rechtlicher Rahmenbedingungen*), sind bei der Löschung oder Vernichtung von Daten einzuhalten. Die entsprechenden Speicher- und Löschfristen für die verschiedenen Arten von Daten müssen identifiziert und beachtet werden.

Für die unterschiedlichen Arten von Datenträgern müssen passende Methoden eingesetzt werden, um die darauf enthaltenen Informationen sicher zu löschen oder den gesamten Datenträger zu vernichten. Es ist für die Institution wichtig, einen Überblick über die Arten der eingesetzten Datenträger zu haben. Es kann zwischen analogen Datenträgern, wie beispielsweise Papier, Farbbändern von Schreibmaschinen und Faxgeräten sowie digitalen Datenträgern (elektronisch, magnetisch, optisch) unterschieden werden. In der Praxis werden analoge Datenträger oft unkontrolliert, zum Beispiel über Papierkörbe entsorgt, da sie als "Büromaterial" ohne besonderen Schutzbedarf betrachtet werden.

Die für die sichere Löschung oder Vernichtung von Informationen notwendige Vorgehensweise sollte für die Mitarbeiter in einer Sicherheitsrichtlinie festgelegt werden (siehe M 2.432 *Richtlinie für die Löschung und Vernichtung von Informationen*). Welche Verfahren und Geräte für die verschiedenen Datenträger ausgewählt werden sollten, ist in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* beschrieben. In größeren Institutionen kann es hilfreich sein, Formblätter anzubieten, auf denen alle wesentlichen Informationen und durchzuführende Aktionen (wie Mitarbeiter-Name, Art der gespeicherten Daten, Grund und Art der Entsorgung) abgefragt werden.

Da sich die Technik und Bauart der digitalen Datenträger ständig ändert und weiterentwickelt, müssen auch die Vorgehensweisen und Verfahren zum zuverlässigen Löschen und Vernichten stetig angepasst werden.

Falls für die Vernichtung von Datenträgern auf externe Dienstleister zurückgegriffen wird, muss die gesamte Entsorgung, von den Sammelstellen über den Transport bis zur Vernichtung beim Dienstleister angemessen abgesichert

sein (siehe M 2.436 *Vernichtung von Datenträgern durch externe Dienstleister*).

Zusätzlich ist es sinnvoll, die Mitarbeiter regelmäßig für den sorgfältigen Umgang mit sicherheitskritischen Informationen und IT-Komponenten zu sensibilisieren (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Um sensible Dateien selektiv zu löschen, muss darauf geachtet werden, dass nicht nur die aktuelle Version, sondern auch alle Vorgängerversionen, temporäre Dateien, Dateifragmente, etc. gelöscht werden. Die Verantwortlichen müssen wissen, wo Betriebssystem und Applikationssoftware Kopien der bearbeiteten Daten anlegen. Eine strukturierte Datenhaltung erleichtert es, die Informationen wieder zu finden (siehe M 2.138 *Strukturierte Datenhaltung*). Die Erfahrung zeigt allerdings, dass immer wieder Informationen übersehen werden, wenn Datenträger vor Weitergabe an Externe selektiv gelöscht werden. Es ist daher von dem selektiven Löschen abzuraten.

Müssen Datenträger repariert werden, können vertrauliche Daten in falsche Hände geraten, wenn die Datenträger vorher nicht sicher gelöscht wurden. Der externe Dienstleister muss sorgfältig ausgewählt werden (siehe M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters*). Es muss eine schriftliche Zusicherung erfolgen, dass die Informationen auf den entsprechenden Datenträgern weder gelesen noch kopiert werden, sofern dies nicht für die Durchführung des Reparaturauftrages notwendig ist.

Beim Löschen und Vernichten von Informationen ist auf die sichere Entsorgung von Datenträgern zu achten, auf denen sich Kopien der zu löschenden Daten befinden. Dazu gehören beispielsweise Backup-Datenträger aber auch RAID-Systeme. Nach der Außerbetriebnahme eines IT-Systems müssen auch die entsprechenden Datensicherungsmedien gelöscht oder unbrauchbar gemacht werden, sobald die darauf gespeicherten Daten nicht mehr benötigt werden.

Hinweis: Werden die Daten direkt bei der Speicherung auf digitale Datenträger durch ein geeignetes Verschlüsselungsprodukt verschlüsselt, entstehen viele der angesprochenen Probleme erst gar nicht. Bei Laptops ist eine vollständige Verschlüsselung der Daten grundsätzlich empfehlenswert. Bei Server-Architekturen ist eine Komplett-Verschlüsselung häufig nicht machbar. Je nach Technologie kann eine vollständige Verschlüsselung der Server-Festplatten mehr Aufwand und Kosten als eine spätere Vernichtung der Platten mit sich bringen. Dies betrifft insbesondere SAN/NAS-Architekturen.

Auch bei analogen Datenträgern finden sich häufig Kopien, so zum Beispiel Altakten in lange nicht benutzten Lagerräumen, die ebenfalls vernichtet werden müssen.

Bei einem hohen oder sehr hohen Schutzbedarf der Informationen ist die Löschung und die Vernichtung zu protokollieren, vor allem im Rahmen der Aussonderung von analogen und digitalen Datenträgern.

Prüffragen:

- Sind die Speicher- und Löschfristen für die in der Institution gebräuchlichsten Informationen bekannt? Werden sie beachtet?
- Sind geeignete Lösch- und Vernichtungsverfahren für alle Arten von in der Institution eingesetzten Datenträgern vorhanden?

- Ist beim Einsatz externer Dienstleister für die Entsorgung geregelt, wie die Datenträger intern gesammelt und bis zur Abholung aufbewahrt werden?
- Ist sichergestellt, dass bei der Löschung von Daten auch die Vorgängerversionen, temporären Dateien, Dateifragmente oder ähnliches gelöscht werden?
- Werden Löschung und Vernichtung von Datenträgern oder Informationen mit hohem oder sehr hohem Schutzbedarf protokolliert?

# M 2.432 Richtlinie für die Löschung und Vernichtung von Informationen

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Mitarbeiter

Informationen müssen sicher gelöscht werden, wenn Datenträger ausgesondert oder gesetzliche Aufbewahrungsfristen überschritten werden. Eine geregelte Vorgehensweise hilft dabei, den Missbrauch der gespeicherten Daten zu verhindern. Informationen auf Datenträgern müssen vor Weitergabe oder Aussonderung so gelöscht werden, dass eine Rekonstruktion der Informationen mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Auch nach Erhalt eines Datenträgers ist zu prüfen, ob die darauf enthaltenen Informationen zuverlässig gelöscht werden müssen, wenn sie entsprechend ihrem Verwendungszweck verarbeitet oder auf andere Datenträger übertragen wurden, beispielsweise zu Archivierungszwecken.

### Zielsetzung

Diese Richtlinie dient dazu, die Mitarbeiter für das Thema Löschen oder Vernichten von Daten zu sensibilisieren und zu motivieren. Sie soll Hilfe und Unterstützung bei der Auswahl der richtigen Verfahren und Werkzeuge zur Löschung oder Vernichtung von schutzbedürftigen Daten geben. Welches die am besten geeignete Vorgehensweise zur Löschung oder Vernichtung ist, hängt vom verwendeten Datenträger, dessen Speichertechnologie sowie der Schutzbedürftigkeit der Informationen ab. Die Einhaltung der Richtlinie sollte regelmäßig überprüft werden.

### Geltungsbereich

In der Richtlinie sollten die zurzeit gebräuchlichen und in der Institution eingesetzten Datenträger berücksichtigt werden. Unterscheidungen müssen zunächst zwischen analogen und digitalen Medien vorgenommen werden. Die digitalen Medien teilen sich in elektromagnetische (wie Festplatten, Disketten, Magnetbänder), optische (wie CDs oder DVDs), magneto-optische (MO-Disk) und Flash-EEPROM (wie USB-Sticks) auf.

Die anfallenden Daten müssen bezüglich ihres Schutzbedarfs bewertet werden. Weiterhin sind für jede Art von Datenträgern passende Löschverfahren auszuwählen und verbindlich festzulegen.

### Rechtsvorschriften und interne Regelungen

In diesem Überblick sollte dargestellt werden, welche gesetzlichen Regelungen wie z. B. Datenschutzgesetze für das Löschen von Daten und Vernichten von Datenträgern einzuhalten sind. Aber auch auf Regelwerke mit normativem Charakter wie ISO-Standards und institutionsinterne Vorgaben sollte verwiesen werden.

### Verantwortlichkeiten

In diesem Teil werden die Verantwortlichkeiten der Funktionsträger definiert. Dabei sind insbesondere die Rollen Mitarbeiter, Vorgesetzte, Administrator, Revisor, Datenschutzbeauftragter und IT-Sicherheitsbeauftragter zu unterscheiden.

**Ansprechpartner**

Die Richtlinie sollte Ansprechpartner und Kontaktinformationen (Telefon, E-Mail etc.) für die Mitarbeiter zu Fragen rund um das Löschen von Informationen enthalten oder aufzeigen, wo diese Informationen gefunden werden können. Dabei sollte beachtet werden, dass es häufig zu Verwirrung führt, wenn zu viele unterschiedliche Ansprechpartner genannt werden. Besser ist es meist, nur wenige Ansprechpartner zu benennen, die dann bei Bedarf die Benutzer an die richtige Stelle verweisen (Help-Desk-Konzept).

**Vorgehensweise**

In der Richtlinie muss festgehalten werden, welche Methoden zur sicheren Löschung existieren und in der Institution zum Einsatz kommen. Für jede Art von Speichermedien kommen dabei typischerweise andere Verfahren zum Einsatz. Es muss beschrieben werden, wie und wann die Benutzer die Informationen zu löschen haben.

Müssen andere, in der Richtlinie nicht erfasste Datenträger gelöscht werden, ist die Richtlinie soweit möglich sinngemäß anzuwenden.

**Aktualisierung**

Aufgrund der sich ändernden Technologien muss die Richtlinie regelmäßig überarbeitet werden, damit die beschriebenen Lösch- und Vernichtungsmethoden auch für neue Arten von Datenträgern geeignet sind. Dies gilt auch für bisher nicht betrachtete oder erfasste Datenträger. Eventuell sind neue Verfahren zu entwickeln und anzuwenden.

Prüffragen:

- Existiert eine Richtlinie für die Löschung oder Vernichtung von Daten?
- Wird die Einhaltung der Richtlinie für die Löschung oder Vernichtung von Daten regelmäßig überprüft?
- Ist die Richtlinie aktuell? Berücksichtigt sie alle zur Zeit eingesetzten Datenträgerarten?

# M 2.433 Überblick über Methoden zur Löschung und Vernichtung von Daten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation

Um Informationen auf Datenträgern zu löschen, stehen verschiedene Methoden zur Verfügung. Welche Methode gewählt werden sollte, hängt hierbei wesentlich vom Schutzbedarf der zu löschenden Daten ab, aber natürlich auch von der Art der Datenträger.

Bei analogen Datenträgern können Informationen beispielsweise geschwärzt (überschrieben), ausgeschnitten oder ausradiert werden. Bei digitalen Datenträgern können Daten mit Löschprogrammen gelöscht oder überschrieben werden.

Bei den im Folgenden beschriebenen Löschmethoden für elektronische Datenträger steigt der Schutz gegen die Wiederherstellung von Restdaten in der genannten Reihenfolge.

**Löschkommandos**

Löschkommandos sind vom Betriebssystem zur Verfügung gestellte Befehle wie "Delete" und "Erase", um Dateien oder Verzeichnisse zu löschen. Bei der Benutzung von Löschkommandos ist zu beachten, dass dabei in der Regel nicht tatsächlich die Datei-Informationen gelöscht werden, sondern nur der Verweis auf diese Informationen im "Inhaltsverzeichnis" des Datenträgers gelöscht wird. Die Datei selbst ist weiterhin vorhanden. Es gibt Methoden und Programme, mit denen die gelöscht geglaubten Informationen wiederhergestellt werden können. Von dieser Methode ist daher abzuraten, wenn sichergestellt sein muss, dass die Daten nicht rekonstruiert werden können.

Es sind also Verfahren und Mechanismen notwendig, die über die Standardlöschverfahren der Betriebssysteme hinausgehen und auch Daten mit hohem Schutzbedarf so löschen, dass sie nicht wiederhergestellt werden können.

**Überschreiben einzelner Dateien**

Neben den im Umfang der gebräuchlichen Betriebssysteme vorhandenen Löschkommandos gibt es zusätzliche softwarebasierte Werkzeuge, um einzelne Dateien zu überschreiben. Mit diesen Lösch-Tools (auch Wipe-Tools genannt) lassen sich einzelne Dateien oder Speicherbereiche durch vollständiges Überschreiben mit geeigneten Datenmustern löschen.

Dabei ist allerdings darauf zu achten, dass Informationen aus Dateien häufig teilweise oder sogar vollständig rekonstruierbar sind, obwohl die Dateien mit Wipe-Tools gelöscht wurden. Hauptsächlich liegt das daran, dass durch Betriebssystem oder Anwendungen Kopien der Daten an ganz unterschiedlichen Orten abgelegt wurden, die die Benutzer häufig weder kennen oder kontrollieren können.

So befinden sich gelöscht geglaubte Daten unter Umständen weiterhin auf dem Datenträger und lassen sich mit entsprechenden Verfahren auslesen.

Hierzu gehören beispielsweise:

- vom Betriebssystem bzw. Anwendungsprogramm erstellte und wieder gelöschte Zwischendateien (Cache-Dateien) oder temporäre Dateien,
- automatisch von einem Programm angelegte Sicherungskopien, wie diese beispielsweise von Office-Programmen häufig angelegt werden,
- Auslagerungsdateien (siehe auch M 4.325 *Löschen von Auslagerungsdateien*),
- Daten-Fragmente, die unter Windows-Betriebssystemen in der Registry oder in Index-Datenbanken vorhanden sein können,
- File-Slack (File-Slack oder Datenversatz bezeichnet das bei einigen Betriebssystemen übliche Abspeichern von "Auffülldaten" in unallozierte Bereiche von Datenträgern) bzw. Cluster-Tips-Fragmente.

Auf die Verarbeitung dieser Daten durch das Betriebssystem oder Anwendungsprogramm haben Administratoren oder Benutzer oft nur sehr geringen Einfluss. Auch Programme, die Wipe-Techniken verwenden, haben keine volle Kontrolle über alle diese Datenspuren. Daher muss der komplette Datenträger gelöscht oder ein anderes sicheres Löschverfahren gewählt werden, um sicherzustellen, dass sich keine weiteren Kopien der Informationen auf dem Datenträger befinden.

**Formatieren**

Durch das Formatieren wird ein elektronischer Datenträger zur Aufnahme von Daten vorbereitet.

Bei Festplatten wird zwischen der Low-Level-Formatierung (LLF), bei der Spuren und Sektoren auf der Platte neu erzeugt werden, und der logischen oder High-Level-Formatierung (HLF), die durch das Betriebssystem erfolgt, unterschieden.

Da bei der Low-Level-Formatierung die Struktur der Festplatte geändert und im Gegensatz zu einer High-Level-Formatierung auch die Aufteilung der Spuren und Sektoren gelöscht und anschließend neu geschrieben wird, kann unter Umständen nach der Formatierung die Festplatte nicht mehr genutzt werden. Falls Festplatten wiederverwendet werden sollen, sollte vorher geklärt werden, ob durch die Low-Level-Formatierung die Garantie für die Festplatte verloren geht.

Mit der Low-Level-Formatierung können Festplatten unabhängig vom Betriebssystem wieder in den "Urzustand" versetzt und damit auch vorhandene Informationen gelöscht werden. Über die Zuverlässigkeit der Löschung der vorhandenen Daten kann allerdings keine Aussage getroffen werden. Von der Nutzung als Löschverfahren wird deshalb abgeraten. Ein mehrfaches Überschreiben des Datenträgers ist auf jeden Fall zuverlässiger.

Bei der High-Level-Formatierung (HLF) wird lediglich die Dateisystemstruktur neu angelegt. Sie eignet sich daher nicht zum zuverlässigen Löschen von Informationen.

**Komplettes Überschreiben von Datenträgern**

Eine für den normalen Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger überschrieben wird. Mit speziellen Softwarewerkzeugen werden dabei die Datenträger einmal oder mehrfach mit vorgegebenen Zeichenfolgen oder Zufallszahlen überschrieben. Die Datenträger müssen intakt sein und sind auch nach dem Überschreiben weiterhin nutzbar.

Die Vertrauenswürdigkeit und Sicherheit dieses Löschverfahrens hängt dabei von folgenden Faktoren ab:

- Die Software muss durch die Benutzer richtig eingesetzt werden. Eine fehlerhafte Anwendung kann dazu führen, dass der Datenträger nicht oder nur teilweise überschrieben wird.
- Die Konfiguration der Löschtools hat wesentliche Auswirkungen darauf, dass die Datenträger vollständig und zuverlässig gelöscht werden. Daher muss sichergestellt sein, dass die Tools optimal konfiguriert sind und die Einstellungen nicht durch Unbefugte verändert werden können.
- Die Löschsoftware muss gewährleisten, dass alle Bereiche des Datenträgers, auch die geschützten oder schadhaften Sektoren, in der gewünschten Weise überschrieben werden. Wegen der Unterschiede in der Technologie der verschiedenen Datenträgerarten (beispielsweise gibt es alleine bei Festplatten bei verschiedenen Herstellern unterschiedliche Technologien) und der raschen Weiterentwicklung der Technologie ist nicht auszuschließen, dass dieses Ziel nicht von allen Softwareprodukten erreicht wird. Die Software muss nach Abschluss des Überschreibens eine Verifikation des erfolgreichen Überschreibens ermöglichen.

Es wird immer diskutiert, wie viele Durchläufe bei einer Überschreibprozedur nötig sind, damit die Daten sicher gelöscht sind. Untersuchungen von Forensik-Laboren haben gezeigt, dass bereits nach einem Durchlauf mit geeigneten Zeichenfolgen oder Zufallszahlen keine Daten mehr rekonstruiert werden konnten. Für den normalen Schutzbedarf ist also ein einmaliges Überschreiben mit einem zuverlässigen Werkzeug ausreichend.

Für den höheren Schutzbedarf sollte die Überschreibprozedur aus mindestens zwei Durchläufen und einer Verifikation des Überschreibvorgangs bestehen. Als Datenmuster werden Zufallsdaten empfohlen. Eine andere Möglichkeit ist, beim mehrfachen Überschreiben beim zweiten Durchlauf das zum ersten Durchlauf komplementäre Datenmuster (Bit-Folge) zu verwenden.

Um Datenträger zu löschen, auf denen Verschlusssachen (VS) gespeichert waren, dürfen nur vom BSI für den jeweiligen Geheimhaltungsgrad empfohlene bzw. zugelassene Produkte eingesetzt werden.

**Löschen mit Löschgeräten**

Die Aufgabe von Löschgeräten ist es, schutzbedürftige Daten, die auf magnetischen Datenträgern gespeichert sind, sicher und unwiederbringlich zu löschen. Dazu verfügen die Löschgeräte über einen starken Gleichfeld- oder Wechselfeldmagneten, mit dessen Hilfe die Datenträger vom Magnetfeld des Gerätes durchflutet werden ("Durchflutungslöschen"). Diese Geräte werden auch Degausser genannt. Da es sich beim Löschen mit Löschgeräten ausschließlich um eine magnetische Einwirkung handelt, können Löschgeräte auch nur bei magnetischen Datenträgern wie Magnetbändern, Disketten und Festplatten verwendet werden. Durch das Magnetfeld des Löschgerätes werden die aufgezeichneten magnetischen Domänen auf den Datenträgern zerstört. Bei Verwendung eines geeigneten Löschgerätes sind deshalb nach dem Löschen auf dem Datenträger keine Informationen mehr vorhanden. Geeignet heißt dabei, dass die magnetische Feldstärke des Löschgerätes deutlich größer sein muss als die des Datenträgers, um diesen vollständig zu entmagnetisieren. Dabei muss auf die sorgfältige Bedienung geachtet werden, unter anderem müssen die Datenträger korrekt positioniert und die richtige Zeitdauer der magnetischen Einwirkung ausgewählt werden. Die Bedienungsanleitung der Löschgeräte ist in jedem Fall zu beachten.

Der Vorteil beim Löschen mit einem Löschgerät besteht darin, dass mit geringem Zeitaufwand der gesamte Datenträger sicher gelöscht werden kann. Allerdings ist zu beachten, dass Festplatten und verschiedene Arten von Magnetbändern nach dem Löschen nicht mehr verwendet werden können, weil mit den aufgezeichneten Daten auch die Servospur, mit der der Schreib-/ Lesekopf gesteuert wird, gelöscht wird.

**Löschen von elektronischen Speichermedien**

RAM-Speicher (SRAM und DRAM) sind flüchtige Speicher, bei denen durch die Trennung von der Stromversorgung der Speicherinhalt gelöscht wird. Falls eine Pufferbatterie vorhanden ist, muss sie ebenfalls entfernt werden. Im Gegensatz dazu muss bei den nichtflüchtigen Speichern EEPROM und Flash-Memory zum Löschen des Speicherinhalts eine Spannung angelegt werden. EPROMs hingegen können nur mit einer UV-Licht Einstrahlung von bis zu 30 Minuten gelöscht werden. Die korrekte Vorgehensweise ist den Datenblättern der Hersteller zu entnehmen.

Es kann jedoch nicht ausgeschlossen werden, dass nach dem Löschen über "Spuren" in den Speicherzellen ein Rückschluss auf die vorher gespeicherten Daten möglich ist. Es wird deshalb empfohlen, die kompletten Speicher vor dem Löschen einmal vollständig mit Zufallszeichen zu überschreiben.

**Löschen von Flash-Disks**

Flash-Disks sind Halbleiterspeicher auf der Basis von Flash-EPROMs, die in Rechnern, insbesondere Notebooks, an Stelle der Festplattenlaufwerke verwendet werden.

Flash-Disks können wie Flash-EPROMs für normalen Schutzbedarf mit einem geeigneten Löschprogramm durch einmaliges, bei höherem Schutzbedarf durch bis zu dreimaliges Überschreiben zuverlässig gelöscht werden.

**Vernichten von Datenträgern**

Bei der Auswahl geeigneter Verfahren zum Vernichten sind sowohl analoge Datenträger wie Papier oder Mikrofilm als auch digitale Datenträger (elektronisch, magnetisch, optisch) zu betrachten. Die Vernichtung von Datenträgern kann beispielsweise durch Zerkleinern mit Messerwerken, Shreddern, Schneidmühlen, Stanzen und weiteren geeigneten Geräten oder auch durch Verbrennen oder Einschmelzen erfolgen.

**Vernichten von analogen Datenträgern**

Verfahren und Geräte, die für die Vernichtung von analogen Datenträgern, also z. B. Papier-Dokumenten oder Mikrofilmen, mit schutzbedürftigen Informationen geeignet sind, sind in M 2.435 *Auswahl geeigneter Aktenvernichter* beschrieben.

**Vernichten von digitalen Datenträgern**

Für digitale Datenträger sind geeignete Verfahren und Geräte in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* beschrieben.

Optische Datenträger wie CDs oder DVDs können nicht überschrieben oder durch magnetische Durchflutung zerstört werden. Sie müssen wie schreibgeschützte oder nicht mehrfach beschreibbare Datenträger (CD-ROMs oder CD-Rs) vernichtet werden.

Magnetische Datenträger, die nicht weiter verwendet werden, sollten mit geeigneten Geräten vernichtet werden. Defekte Festplatten, die nicht mehr überschrieben werden können, müssen vernichtet werden. Die Vernichtung kann durch Schreddern oder thermische Verfahren wie Verbrennen oder Einschmelzen erfolgen.

Geräte zur Vernichtung von Datenträgern sind häufig groß, komplex in der Bedienung und auch teuer. Daher ist die Vernichtung bei Dienstleistungsfirmen in räumlicher Nähe sinnvoller als die Anschaffung eigener Geräte. Werden Datenträger durch externe Dienstleistungsfirmen vernichtet, müssen die Sammelstellen, der Transport und die Vernichtung beim Dienstleister angemessen abgesichert sein (siehe M 2.436 *Vernichtung von Datenträgern durch externe Dienstleister*).

# M 2.434 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Beschaffungsstelle, IT-Sicherheitsbeauftragter, Leiter IT

Typischerweise werden in den meisten Institutionen für die verschiedenen Arten von Datenträgern unterschiedliche Werkzeuge zur Löschung oder Vernichtung der darauf gespeicherten Daten eingesetzt. Einige davon an den Arbeitsplätzen der Mitarbeiter, andere zentralisiert, beispielsweise beim IT-Support. Vor der Beschaffung eines Werkzeugs sollten die Anforderungen und Rahmenbedingungen ermittelt werden, um ein für den jeweiligen Anwendungsfall geeignetes Werkzeug zu finden. Bei der Auswahl von Geräten zur Löschung oder Vernichtung von Daten sind die Anforderungen zu berücksichtigen, die in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* festgelegt wurden.

Die Anforderungen an die jeweiligen Werkzeuge zur Löschung oder Vernichtung von Daten sollten dokumentiert werden, um auf Basis der Dokumentation regelmäßig prüfen zu können, ob die Anforderungen durch die ausgewählten Werkzeug erfüllt werden.

Die Anforderungen an Aktenvernichter sind in M 2.435 *Auswahl geeigneter Aktenvernichter* beschrieben. Die Anforderungen an Werkzeuge zur Löschung oder Vernichtung elektronischer Datenträger sind stark von deren Bauart und Einsatzzweck bestimmt. Im Vordergrund steht die Erfüllung der Sicherheitsanforderungen der Institution. Geklärt werden sollte unter anderem:

- Können die Daten entsprechend ihres Schutzbedarfs zuverlässig gelöscht werden?
- Hat eine unabhängige Institution wie das BSI das Produkt nach anerkannten Sicherheitskriterien wie den Common Criteria (CC) zertifiziert oder für den Einsatz im Geheimschutz-Bereich zugelassen?
- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
- Kann das Produkt so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
- Können wichtige Konfigurationsparameter vor Veränderungen durch unbefugte Benutzer geschützt werden?
- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Ist die Leistungsfähigkeit des Produktes der Größe des Benutzerkreises angemessen?
- Können Mitarbeiter die Werkzeuge ohne größere Schulungsmaßnahmen effektiv, sicher und fehlerfrei nutzen?
- Wie hoch sind die Anschaffungskosten der Produkte? Wie hoch sind die voraussichtlichen laufenden Kosten (Wartung, Betrieb, Support)?

Werden Daten unabsichtlich gelöscht, kann dies ganze Geschäftsprozesse stören. Daher sollte geklärt werden, ob sich die Schnittstellen und Zugänge zur Verwendung dieser Werkzeuge ausreichend absichern lassen.

Wie diese Anforderungen konkretisiert werden können, soll am Beispiel an einem Anforderungsprofil zum sicheren Löschen von Festplatten aufgezeigt werden.

**Beispiel:**

Um Festplatten zu löschen, gibt es eine Vielzahl auf dem Markt verfügbarer Werkzeuge. Die wesentlichen Unterscheidungsmerkmale sind hierbei:

- Anzahl der Überschreibvorgänge
- Überschreibmuster
- Wechsel der Überschreibmuster pro Durchlauf
- Berücksichtigung der Festplatten-internen Codierung
- Verifikationsdurchläufe

Bei der Auswahl von Löschwerkzeugen für Festplatten sollte darauf geachtet werden, dass die ausgewählte Lösung die folgenden Anforderungen erfüllt:

- Unterstützung der eingesetzten Betriebssysteme und Anwendungen: Sie sollte mit der vorhandenen Hardware und den eingesetzten Betriebssystemen problemlos zusammenarbeiten.
- Protokollierung: Löschvorgänge sollten protokolliert werden können. Um gesetzliche oder vertragliche Rahmenbedingungen zu erfüllen, kann es erforderlich sein, nachweisen zu können, dass Datensätze zu einem bestimmten Zeitpunkt gelöscht wurden.
- Korrektheit der Implementierung: Tests von Löschtools haben immer wieder ergeben, dass diese fehlerhaft implementiert werden und z. B.
  - falsche (also untaugliche) Überschreibmuster verwendet wurden,
  - Sektoren nicht überschrieben wurden,
  - nicht die angegebene Anzahl von Überschreibvorgängen durchgeführt wurde,
  - statt Zufallszahlen als Überschreibmuster Konstanten benutzt wurden.

Da es für Anwender schwierig ist, solche Implementierungsfehler festzustellen, sollten möglichst Produkte beschafft wurden, die von unabhängigen Stellen getestet wurden. Bevorzugt sollte auf Tests zurückgegriffen werden, bei denen alle Testkriterien offengelegt werden, wie z. B. Tests, die auf CC oder ISO- bzw. DIN-Normen basieren. Wenn hier keine aktuellen Prüfungen vorliegen, sollten ersatzweise IT-Fachzeitschriften vor einer Beschaffung gesichtet werden, die regelmäßig Tests von Lösch-Werkzeugen durchführen.

Prüffragen:

- Sind die Anforderungen an Werkzeuge zur Löschung oder Vernichtung von Informationen dokumentiert?
- Wurde überprüft, ob die Anforderungen durch die ausgewählten Werkzeuge erfüllt werden?

# M 2.435 Auswahl geeigneter Aktenvernichter

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Organisation
**Verantwortlich für Umsetzung:** Beschaffungsstelle, IT-Sicherheitsbeauftragter

Mit Aktenvernichtern können Papier-Dokumente, aber auch Chipkarten und CDs so zerschnitten werden, dass aus den Fragmenten die ursprünglichen Informationen nicht mehr ohne Weiteres ausgelesen werden können. Ob und mit welchem Aufwand die Informationen rekonstruiert werden können, hängt von der Güte des benutzten Geräts ab. In der Norm DIN 66399:2012 "Vernichten von Datenträgern" sind drei Schutzklassen und sieben Sicherheitsstufen definiert. Grundlage für die Zuordnung in eine Schutzklasse ist der Schutzbedarf der Daten. Die Norm benennt für jede Schutzklasse die zugehörigen Sicherheitsstufen und damit die Größe der von den Aktenvernichtern erzeugten Partikel. In den niedrigeren Sicherheitsstufen gibt es Aktenvernichter, die das Material in Streifen schneiden (Streifenschnitt). In den höheren Sicherheitsstufen solche, die durch eine andere Schnitttechnik Partikel erzeugen (z. B. Kreuzschnitt). Bei Streifenschnitt gibt es allerdings eine hohe Wahrscheinlichkeit, dass sich die Dokumente wieder zusammensetzen lassen. Vor allem bei einer geringen Durchmischung, also nur wenigen zerkleinerten Dokumenten, lassen sich selbst sehr schmal geschnittene Dokumente der Sicherheitsstufe P-3 wieder mit geringem Aufwand rekonstruieren. Um Dokumente mit schutzbedürftigen Informationen zu entsorgen, sollten daher Aktenvernichter mit Partikelschnitt (z. B. Kreuzschnitt ab Sicherheitsstufe P-4) verwendet werden.

Anforderungen an solche Geräte werden in der Norm DIN 66399:2012 Teil 2 "Anforderungen an Maschinen zur Vernichtung von Datenträgern" beschrieben. Den verschiedenen Arten von Datenträgern sind jeweils Sicherheitsstufen zugeordnet, die unterschiedliche Anforderungen an die Größe des vernichteten Materials stellen. In DIN 66399 werden Sicherheitsstufen durch eine Materialkennung und die Stufennummer angegeben, wie beispielsweise "Papier, Sicherheitsstufe 3 (P-3)". Ein Vernichter für Papier ist nicht unbedingt ausreichend für die Vernichtung von Chipkarten oder ähnlichen Datenträgern. Bei den im Folgenden genannten Werten für Partikelgrößen erfordert die DIN 66399 Teil 2 eine Einhaltung von 90 %, 10 % der Partikel in einer Stichprobe dürfen größer sein.

- Sicherheitsstufe 3: Für Akten (P-3) darf die Partikelgröße 320 Quadratmillimeter nicht überschreiten. Bei Streifenschnitt darf die Streifenbreite maximal 2 Millimeter betragen. Bei Mikrofilmen (F-3) sind 10 Quadratmillimeter und bei Chipkarten (E-3) 160 Quadratmillimeter gefordert. Die Reproduktion der Informationen ist nur mit erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich.
- Sicherheitsstufe 4: Die Partikelgröße darf für Akten (P-4) 160 Quadrat-millimeter nicht überschreiten, bei Mikrofilmen (F-4) 2,5 Quadrat-millimeter. Bei Chipkarten (E-4) darf die Partikelgröße 30 Quadrat-millimeter nicht überschreiten, der Chip muss hierbei mindestens einmal geteilt werden. Die Reproduktion der Informationen ist nur mit außergewöhnlich hohem Aufwand möglich.
- Sicherheitsstufe 5: Die Partikelgröße (P-5) darf 30 Quadratmillimeter nicht überschreiten, bei Mikrofilmen (F-5) 1 Quadratmillimeter. Bei Chipkarten (E-5) darf die Partikelgröße 10 Quadratmillimeter nicht überschreiten, der

Chip muss dabei mehrfach geteilt werden. Die Reproduktion der Informationen ist nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen möglich.

Für die Vernichtung von Datenträgern mit normalem Schutzbedarf sollten Vernichtungsgeräte der Sicherheitsstufen 3 (mit den oben genannten Einschränkungen), oder höher verwendet werden. Bei höherem Schutzbedarf sollten Geräte der Sicherheitsstufen 4, 5 oder höher eingesetzt werden.

Bei der Wahl der geeigneten Sicherheitsstufe sollten die Anwender folgendes beachten, um eine Optimierung von Kosten und Sicherheit zu erreichen:

- Je kleiner die Partikelgröße, umso größer ist die Sicherheit bei der Vernichtung. Entscheidend ist insbesondere bei Dokumenten, ob schon einzelne Partikel schützenswerte Information beinhalten, oder ob die schützenswerte Information erst durch Zusammensetzen mehrerer Partikel zur Verfügung steht. Es kann Situationen geben, in denen einzelne übergroße Partikel, welche nach Toleranzbereich der Norm durchaus zulässig sind, schon schützenswerte Information enthalten können und das Schutzziel mit einer gewählten Sicherheitsstufe eventuell nicht erreicht wird.
  In gewissem Maß kann die Sicherheit erhöht werden, wenn Aktenvernichter eine hohe Durchsatzleistung haben und deswegen schon beim Vernichtungsvorgang eine starke Vermischung der Partikel erfolgt. Aktenvernichter für den Büroeinsatz haben üblicherweise nur eine geringe Durchmischung. Die Sicherheit wird weiter reduziert, wenn Farbe oder andere Eigenschaften des Vernichtungsguts eine Rekonstruktion erleichtern.
- Bei kleinerer Partikelgröße wird die Durchsatzleistung des Gerätes geringer. Um eine gewünschte Durchsatzmenge zu erreichen, ist die Anschaffung eines leistungsmäßig größeren und damit teureren Aktenvernichters erforderlich. In diesem Fall ist zu prüfen, ob die Randbedingungen eine niedrigere Sicherheitsstufe und damit ein billigeres Gerät zulassen, wenn dadurch die Anforderungen aus dem Schutzbedarf eingehalten werden.

Das soll an zwei Beispielen verdeutlicht werden:

- Ein Unternehmen muss häufig Akten mit höchstem Schutzbedarf (Firmen-Vertraulich, Geheim) vernichten. Wegen des eher geringen Umfangs der Akten ist keine große Durchsatzleistung zu erwarten. In diesem Fall muss ein Aktenvernichter der Sicherheitsstufe P-6 oder P-7 eingesetzt werden.
- In einem Unternehmen fallen in der Masse offene Dokumente und Dokumente bis zu normalem Schutzbedarf (Nur für interne Verwendung) zur Vernichtung an. Dokumente mit höherem Schutzbedarf mit wenigen Seiten sind nur selten zu vernichten. Hier ist ein Aktenvernichter der Sicherheitsstufe P-5 vertretbar. Die Dokumente mit höherem Schutzbedarf sind dann zusammen mit anderen, z. B. offenen Unterlagen, zu vernichten, um eine ausreichende Vermischung der Partikel zu erreichen.

Datenträger mit Dokumenten in verkleinerter Darstellung (z. B. Mikrofilm, Mikrofiche) sowie Magnetstreifenkarten, Chipkarten, CDs und DVDs können grundsätzlich ebenfalls mit geeigneten Vernichtungsgeräten vernichtet werden. Um dieselbe Sicherheitsstufe zu erreichen, müssen diese aber in kleinere Partikelgrößen zerschnitten werden. In der Norm DIN 66399 Teil 2 sind auch für Mikrofilme Partikelgrößen vorgegeben. Derzeit sind aber keine Mikrofilmvernichter mehr am Markt erhältlich. Eine Vernichtung von Mikrofilmen ist deshalb nur durch Verbrennen oder Einschmelzen möglich.

Vernichtungsgeräte unterliegen durch die Nutzung einem normalen Verschleiß. Durch Vernichtung von Material, für dass das Vernichtungsgerät nicht geeignet ist, können Schäden entstehen. In beiden Fällen wird die Schneid-

qualität beeinträchtigt, sodass in regelmäßigen Abständen eine Prüfung des Vernichtungsgutes notwendig ist. Hier reicht zumeist ein Vergleich des Vernichtungsgutes mittels Sichtkontrolle gegen die Angaben aus der Gerätedokumentation.

Prüffragen:

- Entspricht die Partikelgröße dem Schutzbedarf der Informationen?
- Werden für die Vernichtung schutzbedürftiger Informationen Aktenvernichter mit Kreuzschnitt verwendet?
- Ist bei der Auswahl des Aktenvernichters die Durchsatzmenge beachtet worden?
- Wird das Vernichtungsgut regelmäßig kontrolliert, ob die Partikelgröße eingehalten wird?

# M 2.436 Vernichtung von Datenträgern durch externe Dienstleister

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter Organisation

Falls für die Vernichtung von Datenträgern auf externe Dienstleister zurückgegriffen wird, sind mit diesen detaillierte Regelungen zu treffen (siehe z. B. M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister*). Trotz Outsourcing sind interne Regelungen notwendig, um beispielsweise festzulegen, wie Datenträger eingesammelt und bis zur Abholung durch den Dienstleister verwahrt werden. In der DIN SPEC 66399:2012 Teil 3 "Prozess der Datenträgervernichtung" sind Kriterien für die Einbindung von Dienstleistern definiert. In vielen Fällen wird der Dienstleister für die Vernichtung auch mit dem Abtransport bereits vernichteter Datenträger oder auch dem Abtransport nicht vernichteter Datenträger mit dem Ziele der Vernichtung und der nachfolgenden Verwertung beauftragt. Hierbei sind die jeweils geltenden gesetzlichen Bestimmungen zu beachten.

### Absicherung beim Auftraggeber

Zu vernichtende Datenträger müssen vor unbefugtem Zugriff gesichert aufbewahrt werden, bis sie abgeholt werden. Zur Sammlung von Datenträgern können innerhalb einer Institution beispielsweise Container aufgestellt werden, die so abgesichert sein müssen, dass keine Datenträger wieder entnommen werden können. Diese Sammelcontainer sind besonders interessant für Angreifer, da sie eine konzentrierte Sammlung von sensiblen Informationen enthalten. Keinesfalls sollte eine Vielzahl an Containern auf allgemein zugänglichen Fluren aufgestellt werden. Jedoch sollten die Standorte der Sammelcontainer arbeitsplatznah gewählt werden, damit Mitarbeiter zu vernichtende Datenträger nicht ungesichert, beispielsweise in der Schreibtischschublade, verwahren, ehe sie diese einer Sammlung übergeben (vergleiche M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*). Werden die Mitarbeiter bei der Auswahl eines geeigneten Standortes für die Sammelcontainer beteiligt, erhöht dies die allgemeine Akzeptanz.

Außerdem müssen Transport und Vernichtung angemessen abgesichert werden. Dazu sind mit der Dienstleistungsfirma vertragliche Vereinbarungen zu treffen, siehe dazu den Mustervertrag zur Entsorgung von Datenträgern unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten. Es muss regelmäßig überprüft werden, dass diese Regeln auch eingehalten werden.

### Absicherung beim Transport

Es muss sichergestellt sein, dass nur die mit dem Transport beauftragten Personen die zu vernichtenden Datenträger ausgehändigt bekommen. Dafür sind zunächst beim Auftraggeber Personen zu benennen, die in den Entsorgungsprozess eingewiesen sind und die korrekte Ausführung der Abläufe überwachen können. Die beauftragten Transportboten müssen sich als solche ausweisen können, damit nicht die gesammelten vertraulichen Daten an einen Unbefugten herausgegeben werden. Die Übergabe der Datenträger ist schriftlich zu bestätigen, sowohl bei der Ein- als auch bei der Ablieferung. Auf der gesamten Transportstrecke muss gewährleistet sein, dass nur berechtigte Personen das Material transportieren. Auf der gesamten Transportstrecke sollten weder die Mitarbeiter der Transportfirma noch andere Personen auf das

Material Zugriff nehmen können. Beispielsweise könnten verschlossene oder verplombte Behälter eingesetzt werden.

**Absicherung beim Dienstleister**

Der Entsorgungsdienstleister muss einen funktionierenden Sicherheitsprozess aufgesetzt haben, so dass die zu vernichtenden Datenträger zuverlässig unlesbar gemacht werden und keine Unbefugten Informationen daraus gewinnen können. Der Dienstleister muss ein aktuelles, nachvollziehbares Datenschutz- und Sicherheitskonzept haben. Generelle Anforderungen an Dienstleister und deren Mitarbeiter sind in M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters* beschrieben.

Bei der Anlieferung ist die Vollständigkeit des Transportguts zu überprüfen, also z. B. die Anzahl der Behälter und deren Gewicht zu kontrollieren. Beim Dienstleister wird das zu entsorgende Material typischerweise zunächst zwischengelagert. Hier muss sichergestellt sein, dass es eine funktionierende Zutrittskontrolle gibt, damit Unbefugte auf die zu vernichtenden Datenträger oder auf die Geräte keinen Zugriff erhalten.

Die Geräte und Werkzeuge zur Vernichtung von Datenträgern dürfen nur von Mitarbeitern bedient werden, die in deren Handhabung eingewiesen wurden.

Prüffragen:

- Werden die zu vernichtenden Datenträger vor unbefugtem Zugriff gesichert aufbewahrt, bis sie abgeholt werden?
- Sind beim Auftraggeber Personen zur Kontrolle des Entsorgungsprozesses benannt und eingewiesen worden?
- Kontrolliert der Auftraggeber regelmäßig den Entsorgungsprozess?
- Sind Abholung und Transport der zu vernichtenden Datenträger angemessen abgesichert?
- Ist der Sicherheitsprozess beim Entsorgungsdienstleister zuverlässig, nachvollziehbar und dem Schutzbedarf der zu vernichtenden Datenträger angemessen?

# M 2.437 Planung des Einsatzes eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die vielfältigen Einsatzmöglichkeiten von Samba machen umfangreiche Planungen im Vorfeld notwendig, damit eine geregelte und sichere Einführung sowie in Folge ein sicherer Betrieb ermöglicht wird. Dabei ist zu gewährleisten, dass die für IT-Systeme festgelegten Sicherheitsrichtlinien (siehe vor allem M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*) eingehalten werden und so eine richtlinienkonforme Umsetzung erfolgt. In Abhängigkeit des Einsatzszenarios ist zu definieren, in welchem Szenario und in welcher Funktion Samba eingesetzt werden soll und welche Software hierfür gegebenenfalls zusätzlich installiert werden muss (beispielsweise OpenLDAP).

**1. Szenarienplanung**

Um die unterschiedlichen Aufgabenbereiche, in denen Samba eingesetzt werden kann, zu verstehen, ist es hilfreich sich die verschiedenen Szenarien vor Augen zu führen, die ein Rechner in einem Windows-Netz haben kann:

- Standalone-Rechner:
  Ein Standalone-Rechner kann ein einzelner Arbeitsplatzrechner oder ein Server sein, der zu keiner Domäne gehört. Ein solcher Rechner verwaltet seine eigene Benutzerdatenbank, die er auch nicht exportiert.
- Domänenmitglied:
  Ein Domänenmitglied kann ein Arbeitsplatzrechner oder ein Server sein, der Mitglied in einer Domäne ist. Er bezieht seine Benutzerdatenbank von einem Domänencontroller.
- Domänencontroller:
  Ein Server der seine Benutzerdatenbank exportiert, wird als Domänencontroller bezeichnet. Hier wird im NT4-Domänenmodell (auch bei Samba) zwischen Primary Domain Controller (PDC) und Backup Domain Controller (BDC) unterschieden. Im neueren Active Directory (AD)-Domänenmodell werden die Benutzerinformationen nicht mehr im Security Account Manager (SAM), sondern, neben vielen anderen zusätzlichen Informationen, im AD-Verzeichnis abgelegt. Ein wichtiger Unterschied ist, dass nicht mehr zwischen PDCs und BDCs unterschieden wird, sondern es nur noch Domänencontroller gibt. Jeder Domänencontroller hat Schreibzugriff auf das AD-Verzeichnis, da der Verzeichnisdienst den Abgleich mehrerer AD-Verzeichnisse unterstützt (Multimaster-Replikation). Des Weiteren kommen in einer AD-Domäne andere Protokolle zum Einsatz. Beispielsweise werden statt Network Basic Input/Output System (NetBIOS) die Protokolle Domain Name System (DNS) und Transmission Control Protocol (TCP)/ Internet Protocol (IP) eingesetzt).

Ein Samba-Server kann in den folgenden Szenarien eingesetzt werden. Dabei ist zu beachten, dass es für ein und dasselbe Szenario durchaus mehrere Möglichkeiten gibt, Samba einzusetzen:

- Als Mitglied einer NT4-Domäne (Domänenmitglied)
- Als Mitglied einer AD-Domäne (Domänenmitglied)
- Als PDC für eine NT4-kompatible Domäne (Domänencontroller)
- Als BDC eines Samba-PDCs in einer NT4-kompatiblen Domäne (Domänencontroller). Das Protokoll, das ein NT4 PDC verwendet um die SAM-Datenbank mit seinen BDCs abzugleichen, konnte noch nicht in Samba

implementiert werden. Daher kann ein Samba BDC nur mit einem Samba PDC eingesetzt werden.

**2. Funktionsplanung**

Wird Samba als Mitglied einer NT4-Domäne oder Mitglied einer AD-Domäne eingesetzt, so kann Samba folgende Funktionen ausüben:

- Datei-Server
- Druck-Server

Wird Samba als PDC für eine NT4-kompatible Domäne oder BDC eines Samba PDC in einer NT4-kompatiblen Domäne eingesetzt, so kann Samba folgende Funktionen ausüben:

- Anmelde-Server
- Datei-Server
- Druck-Server

**3. Winbind**

Damit die Benutzer Samba-Freigaben nutzen können, müssen sie sich auf dem Server authentisieren. Hierfür ist es erforderlich, dass auf dem Samba-Server für jeden Benutzer ein Windows- und ein Unix-Benutzerkonto vorhanden sind. Das Unix-Benutzerkonto wird unter anderem benötigt, damit Samba die Zugriffskontrolle im Dateisystem dem Kernel überlassen kann (siehe auch M 4.332 *Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server*).

Daher muss jeder Windows-Domänenbenutzer, mit all seinen Gruppenmitgliedschaften im Unix-Betriebssystem existieren. Theoretisch ist es möglich, alle Domänenbenutzer von Hand unter Unix nachzupflegen. Statt dieser Vorgehensweise sollte aber Winbind eingesetzt werden.

Winbind kann zu Windows-Benutzern und -Gruppen passende Unix-Benutzer und -Gruppen dynamisch erzeugen, falls diese unter Unix noch nicht existieren. Außerdem kann durch den Einsatz von Winbind in Verbindung mit Samba die Beanspruchung der Domänencontroller im Informationsverbund gesenkt und eine niedrigere Netzlast erreicht werden. Für eine ausführliche Beschreibung von Winbind wird auf M 4.333 *Sichere Konfiguration von Winbind unter Samba* verwiesen.

Bei der Planung des Einsatzes eines Samba-Servers ist im Bezug auf Winbind zu beachten, dass das ID-Mapping-Backend "ads" nur eingesetzt werden kann, wenn Samba im Security Mode "ads" betrieben wird (siehe M 4.328 *Sichere Grundkonfiguration eines Samba-Servers*).

Prüffragen:

- Wurde konkret geplant, welche Szenarien und Funktionen der Samba-Server übernehmen soll?
- Wenn der Einsatz von Winbind nötig ist, wurde dieser entsprechend geplant?

# M 2.438 Sicherer Einsatz externer Programme auf einem Samba-Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Viele Funktionen, wie das Anlegen eines neuen Benutzers im Unix System oder die Abfrage von Druckerstatusinformationen, sind nicht in Samba implementiert.

Samba nutzt zur Realisierung dieser Funktionen Programme des Systems, auf dem es installiert ist. Um beispielsweise einen neuen Benutzer im Unix System anzulegen, ruft Samba das über den Parameter "add user script" spezifizierte Programm auf. Alle Konfigurationsparameter, die Samba für den Aufruf externer Programme nutzt, enden auf die folgenden Zeichenketten:

- command
- script
- exec
- panic action
- program

In Samba 3 gibt es ungefähr 40 solcher Konfigurationsparameter. Mit dem Kommando:

testparm -vs | grep -E "(command =)|(script =)|(exec =)|\ (panic action =)|(program =)" | wc -l

kann die genaue Anzahl der Konfigurationsparameter für die momentan eingesetzte Samba-Version angezeigt werden. Falls Samba zur Kommunikation mit dem Drucksystem das Common Unix Printing System (CUPS) Application Programming Interface (API) nutzt, ist standardmäßig keiner dieser Parameter gesetzt, beziehungsweise wird keiner dieser Parameter verwendet. Ob Samba mit der CUPS-Bibliothek übersetzt und verlinkt wurde, kann mit folgendem Kommando überprüft werden:

root# ldd $(which smbd) | grep 'libcups'

Nutzt Samba nicht das CUPS API zur Kommunikation mit Druckern, so werden, je nach Wert des Konfigurationsparameters "printing" in der Konfigurationsdatei "smb.conf", einige der drucksystemspezifischen Konfigurationsparameter mit Standardwerten vorbelegt. Folgende Konfigurationsparameter sind davon betroffen:

- print command
- lpq command
- lprm command
- lppause command
- lpresume command
- queuepause command
- queueresume command

Viele, der über solche Konfigurationsparameter spezifizierten externen Programme, werden von Samba mit Root Rechten ausgeführt. Es ist daher sicherzustellen, dass nur Programme, die keine schadhafte Funktion besitzen, von Samba aufgerufen werden.

Mit dem Kommando

```
user> testparm -vs | grep -E "(command =)|(script =)|(exec =)|\ (panic action =)|(program =)"
```

werden alle Parameter ausgegeben, die für die Einbindung externer Programme in Samba verantwortlich sind. Zusätzlich zu den Parametern werden die momentan gültigen Werte angezeigt.

Prüffragen:

- Werden externe Programme auf schadhafte Funktionen überprüft, bevor diese Programme in Samba eingebunden werden?

# M 2.439 Konzeption und Organisation des Anforderungsmanagements

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Anforderungsmanager, Behörden-/Unternehmensleitung

Typischerweise gibt es in den verschiedenen Bereichen einer Institution Übersichten über die Anforderungen, die in diesen Bereichen und für deren Geschäftsprozesse relevant sind. Nicht immer sind dies formalisierte Übersichten, sondern oftmals Einzelinformationen in verschiedenen Strukturen und Wissen in den Köpfen von Experten. Durch die Komplexität vieler Geschäftsprozesse und Organisationsstrukturen sowie durch eine zunehmende Vielfalt an Vorgaben aus der internationalen Zusammenarbeit können sich hierbei schnell eine große Anzahl verschiedener Anforderungen ergeben.

Deswegen ist es sinnvoll, das vorhandene Wissen über die verschiedenen gesetzlichen, vertraglichen und sonstigen Vorgaben zusammenzutragen und, wenn nötig, zu ergänzen. Dafür müssen Verantwortliche benannt und deren Aufgaben im Bereich Anforderungsmanagement festgelegt werden. Die entsprechende Rolle wird häufig als "Anforderungsmanager" bezeichnet. Je nach Art und Größe der Institution kann es sinnvoll sein, einen oder mehrere Anforderungsmanager zu benennen.

In einigen Unternehmen wird auch die Bezeichnung "Compliance Manager" benutzt, dieser ist dann der zentrale Anforderungsmanager für die Institution. Sofern dies nicht durch andere Regelungen vorgeschrieben ist, muss hierfür aber keine neue Stelle geschaffen werden. Die Aufgabe kann beispielsweise vom Sicherheitsmanagement, der Revision, dem Controlling oder dem Justitiariat mit übernommen werden.

Die Benennung eines zentralen Anforderungsmanagers hat den Vorteil, dass dieser einen Überblick über die gesamte Institution hat, wodurch Doppelarbeiten und Konflikte frühzeitig erkannt und vermieden werden können. Mehrere Anforderungsmanager in den verschiedenen Bereichen einer Institution können andererseits meist besser die Bedürfnisse der von ihnen betreuten Zielgruppe abdecken. Im Folgenden wird der besseren Lesbarkeit wegen immer im Singular auf die Rolle des Anforderungsmanagers Bezug genommen.

Zu den Aufgaben eines Anforderungsmanagers (für die von ihm betreuten Bereiche) gehören:

- Alle für die wesentlichen Geschäftsprozesse und Informationen sowie für den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben müssen identifiziert und dokumentiert werden (siehe M 2.340 *Beachtung rechtlicher Rahmenbedingungen*).
- Die Anforderungen sind strukturiert zu erfassen und aus den verschiedenen Bereichen zusammenzuführen und zu konsolidieren.
- Um die einzelnen identifizierten Anforderungen zu erfüllen und angemessene Maßnahmen umzusetzen, müssen Verantwortliche benannt werden. Der Anforderungsmanager sollte regelmäßig überprüfen, ob die ergriffenen Maßnahmen geeignet sind, um die Anforderungen abzudecken.
- Häufig müssen Anforderungen auch zunächst interpretiert und auf die Gegebenheiten der jeweiligen Institution übersetzt werden, da die meisten Gesetze und Vorgaben eher Ziele und Erwartungen formulieren, nicht aber wie deren Umsetzung konkret auszugestalten ist.

- Alle Arten der genannten Anforderungen gehen auch jeweils auf eine bestimmte Zielgruppe zurück, die deren Einhaltung fordert oder prüft. Bei der Identifikation der Anforderungen sollte auch immer die Zielgruppe dokumentiert werden, um deren Bedürfnisse zu erfüllen. Dies erspart später viele Anpassungsarbeiten. Bei gesetzlichen Anforderungen ist es z. B. sinnvoll, festzuhalten, welche Instanz (also z. B. welche Aufsichtsstelle) deren Einhaltung prüft und in welcher Form hierfür die Informationen aufbereitet werden müssen.

In der folgenden Tabelle finden sich hierzu einige Beispiele:

| **Anforderungen** | **Zielgruppe** | **Verantwortlicher Anforderungsmanager** |
|---|---|---|
| Datenschutz-Gesetze | Datenschutz-Aufsicht | Behördlicher oder betrieblicher Datenschutzbeauftragter |
| Arbeitsrecht | Personalvertretung | Personalreferat |
| Strafrecht | Strafverfolgungsbehörden | Justitiariat / Hausjurist |
| Verträge | Dienstleister<br>Kunden | Einkauf<br>Vertrieb |
| Sonstige Anforderungen | Kooperationspartner | Fachabteilung |

Tabelle: Zuordnung von Anforderungen zu Zielgruppen und Anforderungsmanagern

**Zusammenarbeit mit Sicherheitsmanagement**

Die Informationssicherheit ist direkt oder indirekt ein zu beachtender Aspekt in fast allen Anforderungsbereichen. Dabei ist der IT-Sicherheitsbeauftragte nur in wenigen Fällen der Anforderungsmanager. Anforderungsmanager und IT-Sicherheitsbeauftragter müssen daher regelmäßig zusammenarbeiten, um einerseits die Sicherheitsanforderungen aus den verschiedenen Bereichen ins Anforderungsmanagement zu integrieren und andererseits die als sicherheitsrelevant identifizierten Anforderungen in Sicherheitsmaßnahmen zu überführen und deren Umsetzung zu kontrollieren.

Sicherheitsanforderungen ergeben sich in erster Linie durch die Auslegung allgemeiner Rechtsvorschriften, teilweise aus Spezialgesetzen sowie aus tätigkeits- oder branchenbezogenen Vorschriften, die die Sicherheit bestimmter Systeme, Dienstleistungen oder Tätigkeiten regeln. Dazu kommen zivilrechtliche Pflichten, deren (schuldhafte) Verletzung zu Haftung des Verantwortlichen führen kann. Beispiele sind

- Datenschutzgesetze
- KWG, KonTraG
- Urheberrechtsgesetz
- Verträge, Allgemeine Geschäftsbedingungen, etc.
- Lizenzmanagement

Die als sicherheitsrelevant identifizierten Anforderungen fließen typischerweise bei der Planung und Konzeption von Geschäftsprozessen, Anwendungen und IT-Systemen oder bei der Beschaffung neuer Komponenten ein. Typische Beispiele in den IT-Grundschutz-Katalogen sind Maßnahmen wie M 2.419 *Geeignete Auswahl von VPN-Produkten*.

Prüffragen:

- Gibt es in der Institution einen Überblick über die zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben?
- Ist sichergestellt, dass die Maßnahmen zur Erfüllung der spezifischen Anforderungen umgesetzt werden und geeignet sind?

# M 2.440 Geeignete Auswahl einer Windows-Version für Clients ab Windows Vista

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Client-Betriebssysteme ab Windows Vista gibt es in unterschiedlichen Versionen für Privatanwender sowie für Unternehmen, Behörden und andere Institutionen. Die Versionen unterscheiden sich hinsichtlich ihres Funktionsumfangs, des Preises und hinsichtlich der unterstützten Lizenzmodelle.

Für den Privatanwender hat Microsoft die folgenden Versionen von Windows-Clients konzipiert:

- Windows Vista Starter
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Ultimate
- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium
- Windows 7 Ultimate
- Windows 8
- Windows 8 Professional
- Windows 8 RT

Für den Einsatz in Unternehmen, Behörden und anderen Institutionen empfiehlt Microsoft eine der folgenden Versionen von Windows-Clients:

- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Professional (ersetzt die Business Edition von Windows Vista)
- Windows 7 Enterprise
- Windows 7 Ultimate
- Windows 8 Professional
- Windows 8 Enterprise

Ergänzend gibt es in Europa noch die so genannten Windows Vista und Windows 7 N Versionen. In diesen ist der Microsoft Media Player nicht enthalten. Der Microsoft Media Player kann genutzt werden, um digitale Medien wie Bilder, Audio und Video wiederzugeben.

**Windows Vista und Windows 7 Starter:**

Diese Version ist in Deutschland nicht einzeln erhältlich. Die Version ist für die Verwendung in Entwicklungs- und Schwellenländern vorgesehen oder wird mit leistungsreduzierten Notebooks, sogenannten Netbooks ausgeliefert. Der Funktionsumfang ist sehr stark reduziert und enthält nur Basisfunktionen. Diese Editionen unterstützen lediglich eine 32-Bit Betriebssystemarchitektur.

**Windows Vista und Windows 7 Home Basic:**

Diese Version ist für Privatanwender konzipiert. Windows Vista und Windows 7 Home Basic besitzen im Vergleich zu Windows Vista und Windows 7 Home Premium einen reduzierten Funktionsumfang. Der Privatanwender muss unter anderem auf die Aero-Glass-Oberfläche und auf das Windows Media Center

sowie integrierte Backup-Funktionen verzichten. Beide Editionen können keiner Domäne beitreten und sind auf dem deutschen Markt nicht erhältlich.

**Windows Vista und Windows 7 Home Premium:**

Diese Version ist für Privatanwender konzipiert. Die erweiterte Version von Windows Vista und Windows 7 Home bietet die Aero-Glass-Oberfläche in vollem Funktionsumfang sowie weit reichende Multimedia-Funktionen. So ist zum Beispiel das Windows Media Center komplett integriert. Der Betrieb des Systems in einer Domäne ist in dieser Version nicht verfügbar.

**Windows Vista und Windows 7 Ultimate:**

Diese Version ist sowohl für Privatanwender als auch für den Behörden- und Unternehmenseinsatz konzipiert. Die Version bietet alle Funktionen, die von sämtlichen Windows Vista und Windows 7 Versionen angeboten werden, zum Beispiel Festplattenverschlüsselung mit BitLocker und umfangreiche Netzunterstützung. Im Unterschied zu Windows Vista und Windows 7 Enterprise, sind die Windows Vista und Windows 7 Ultimate Lizenzen nicht als Volumenlizenzen erhältlich.

**Windows Vista und Windows 7 Business / Windows 7 Professional:**

Diese Version ist für den Einsatz in Unternehmen, Behörden und anderen Institutionen konzipiert, sie unterstützt beispielsweise Windows Domänen. In Windows Vista und Windows 7 Business / Windows 7 Professional steht ein großer Funktionsumfang in den Bereichen Netz, Backup und Sicherheit zur Verfügung. Multimedia-Funktionen stellt Windows Vista und Windows 7 Business nur eingeschränkt zur Verfügung. Einige Anwendungsfunktionen sowie die Sicherheitsfunktionen BitLocker Laufwerksverschlüsselung und AppLocker Anwendungssteuerung (ab Windows 7) sind nicht integriert.

**Windows Vista und Windows 7 Enterprise:**

Diese Version ist für den Einsatz in Behörden und Unternehmen konzipiert. Windows Vista und Windows 7 Enterprise sind nur über das Volumenlizenzangebot des Herstellers Microsoft erhältlich. Des Weiteren unterscheiden sich Windows Vista und Windows 7 Enterprise auch im Funktionsumfang gegenüber Windows Vista Business, Windows 7 Business und Windows 7 Professional. Windows Vista und 7 Enterprise stellen Funktionen zur Festplattenverschlüsselung, Virtualisierung, die Unterstützung für Unix-basierte Anwendungen (SUA) und eine mehrsprachige grafische Oberfläche (MUI) zur Verfügung.

Aus den aufgeführten Versionen von Windows Vista und Windows 7 sollten eine oder mehrere geeignete Versionen für den Einsatz in der Institution ausgewählt werden, die alle benötigten Funktionen für die geplante Einsatzumgebung enthalten. Diese Entscheidung muss begründet und dokumentiert werden.

Das Microsoft Lizenzmodell "Windows Anytime Upgrade" bietet nachträgliche Upgrades zwischen den verschiedenen Windows Editionen. Es sind Upgrades von der Windows Vista / Windows 7 Edition Home Basic zu Home Premium sowie von Home Premium, Professional und Business zu Windows Vista / Windows 7 Ultimate möglich. Ein Upgrade von 32-Bit-Editionen auf 64-Bit ist nicht möglich.

Unter Windows 8 sind insgesamt nur noch vier verschiedene Versionen erhältlich, die vom bisherigen Versionierungsschema für Windows Vista und Windows 7 abweichen:

**Windows 8:**

Diese Version von Windows ist speziell für den Privatgebrauch ausgelegt, da sie einen reduzierten Funktionsumfang aufweist. So fehlen zum Beispiel die Integration des BitLocker-Dienstes für die Verschlüsselung von Daten und Laufwerken, die Remotedesktopverbindung und die Option für den Domänenbeitritt in Unternehmensnetzwerken. Ein Upgrade von Windows 7 Professional oder Ultimate auf diese Windows-8-Version ist nicht möglich. Windows 8 ist nur als Einzelhandelspaket oder als OEM-Version erhältlich.

**Windows 8 Professional:**

Diese Version ist sowohl für den privaten als auch für den geschäftlichen Einsatz entwickelt und richtet sich an Umgebungen, in denen der Rechner in ein Netz eingebunden werden soll oder einer Domäne beitreten muss. Mit dieser Version ist die zentrale Verwaltung der Systeme mittels Gruppenrichtlinien möglich. Der BitLocker-Dienst ist ebenso integriert wie die Remotedesktopverbindung. Virtualisierungsfunktionen, die z. B. das Booten von einer virtuellen Festplatte erlauben, und ein integrierter Hyper-V-Client sind ebenfalls vorhanden. Windows 8 Professional kann als Einzelhandelspaket, als OEM-Version oder in einer Volumenlizenz bezogen werden.

**Windows 8 Enterprise:**

Die Enterprise-Version von Windows 8 ist nur für Firmenkunden erhältlich. Sie enthält alle Funktionen, welche auch unter Windows 8 Professional zu finden sind, bietet aber zudem weitere Funktionalitäten für den mobilen Unternehmenseinsatz an, wie z. B. Windows to Go und Direct Access. Windows to Go erlaubt es, eine Windows-8-Installation von einem USB-Stick zu booten, während die mit Windows 7 eingeführte Direct-Access-Funktion die Einwahl in das Firmennetzwerk über ein VPN ermöglicht. Das Anwendungssteuerungssystem AppLocker zur Unterbindung der Ausführung nicht standardmäßiger oder nicht genehmigter Software ist ebenfalls nur in dieser Version erhältlich. Windows 8 Enterprise bietet die Möglichkeit des Sideloadings, also der Installation von Windows-Store-Apps ohne Veröffentlichung im Store. Windows 8 Enterprise ist nur über ein Volumenlizenzprogramm erhältlich. Hierdurch ist auch die Nutzung der Windows-8-Enterprise-Version zeitlich begrenzt.

**Windows 8 RT:**

Windows RT 8 ist ein Windows-basiertes Betriebssystem, das nur auf bestimmten Tablets und PCs mit ARM-Prozessoren verfügbar ist. Die Installation von herkömmlichen x86- oder x64-Anwendungen ist mit dieser Version nicht möglich, und die Installation von Apps erfolgt nur über den Windows-Store. Windows 8 RT wird sowohl für den privaten als auch für die Integration in das Unternehmensumfeld beworben, verfügt aber über keine Funktion zum Beitritt zu einer Domäne. Mit Windows 8 RT und Windows Server 2012 R2 kann aber z. B. der Zugriff auf Unternehmensressourcen freigegeben werden. Windows 8 RT ist nur in einer OEM-Version verfügbar, da es nur als Betriebssystem für sog. Appliances (also Geräte, bei denen herstellerseitig keine Installation eines Betriebssystems durch den Kunden vorgesehen ist) angeboten wird.

**32-Bit oder 64-Bit**

Die 64-Bit-Versionen bieten einen höheren Schutz gegen Schadprogramme, da u. a. standardmäßig nur signierte Treiber geladen werden können und die höhere Entropie der verwendeten Speicherschutzmechanismen die Ausnutzung von Softwareschwachstellen erschwert. Zusätzlich schützt die Kernel

Patch Protection der 64-Bit-Versionen vor Manipulation des Windows-Kerns. Moderne Rechner sind mit 4 Gigabyte oder mehr Arbeitsspeicher ausgestattet, was ebenfalls erst mit den 64Bit-Versionen voll genutzt werden kann. Ab Windows 7 sollte daher die 64-Bit-Version eingesetzt werden. Die 64-Bit-Versionen von Vista sind aufgrund zu vieler Kompatibilitätsprobleme nicht für den flächendeckenden Einsatz geeignet.

Bei der Beschaffung ist in Abstimmung mit der Hard- und Softwareplanung zu prüfen, ob Lizenzen für 32-Bit, 64-Bit oder Kombinations-Lizenzen am günstigsten sind. Insbesondere müssen auch ältere Fachapplikationen und Spezialhardware berücksichtigt werden, die unter Windows-Clients ab Windows Vista möglicherweise nicht vom Hersteller unterstützt werden.

Prüffragen:

- Wurde eine geeignete Betriebssystem-Version für Windows-Clients ab Windows Vista ausgewählt, die alle benötigten Funktionen enthält?
- Werden in Abstimmung mit der Hardware- und Softwareplanung bevorzugt 64-Bit-Versionen eingesetzt?
- Wurde die Auswahl der geeigneten Windows Version begründet und dokumentiert?

# M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows für Clients ab Windows Vista

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Windows-Client-Versionen ab Windows Vista zeichnen sich gegenüber vorherigen Windows-Versionen durch neue Sicherheitsmechanismen und Betriebssystemeigenschaften aus. Deren Anforderungen werden nicht von jeder Software erfüllt. In der Folge wird Software, die auf Vorgängerversionen zu Windows Vista erfolgreich betrieben werden konnte, nicht ohne weiteres auch auf neueren Windows Versionen wie Vista, 7 oder 8 unterstützt. Der prägnanteste Unterschied zwischen Windows 7 und Windows 8 ist die Bedienoberfläche und das damit verbundene Bedienkonzept, das sich grundlegend verändert hat. Da in Windows 8 erhebliche Teile der Codebasis von Windows Vista und Windows 7 übernommen worden sind, können die meisten Anwendungen unter Windows 8 weiterhin verwendet werden. Eine Kompatibilitätsprüfung muss aber dennoch bei allen Versionen im Rahmen einer Beschaffung oder Migration erfolgen.

**Kompatibilitätsprüfung**

Vor einer beabsichtigten Beschaffung von Software für Windows-Clients ab Windows Vista muss deren Kompatibilität zu der eingesetzten Windows-Version in der vorliegenden Konfiguration überprüft werden. Das gleiche gilt für bereits verwendete Software vor einer geplanten Migration zu einem Windows-Client-Betriebssystem ab Windows Vista. Bei einer beabsichtigter Hardwareänderung oder bei einer Betriebssystemmigration ist die Treibersoftware für alle betreffenden Komponenten ebenfalls auf Kompatibilität und Verfügbarkeit zu prüfen.

Die Kompatibilitätsprüfung kann durch folgende Aktivitäten durchgeführt beziehungsweise unterstützt werden:

- Überprüfen der Kompatibilität von Anwendungen und Hardware für Windows 7 und Windows 8 im Windows Kompatibilitätscenter. Für Windows 8 muss auf das Logo "Windows 8 Compatible" geachtet werden.
- Der Windows Upgrade-Assisstent ist sowohl für Upgrades auf Windows 8 und Windows 8.1 verfügbar und prüft die bestehende PC-Hardware, installierte Desktop-Apps und angeschlossene Geräte auf deren Kompatibilität mit einer höheren Version von Windows. Der Windows Upgrade-Assisstent ist als Download unter http://windows.microsoft.com/de-de/windows-8/upgrade-assistant-download-online-faq verfügbar
- Prüfung der Angabe der Systemvoraussetzungen auf den Herstellerseiten
- Rechtsverbindliche Zusicherung der Kompatibilität durch den Hersteller der Software
- Überprüfung der Kompatibilität in einer Testumgebung
- Anfrage bei Microsoft, mit Bezug zu bekannten Kompatibilitäten oder Kompatibilitätsproblemen
- Austausch mit anderen Anwendern
- Recherche mit Bezug zu bekannten Kompatibilitäten oder Kompatibilitätsproblemen
- Untersuchung der Software mit unterstützenden Diagnose-Programmen wie *regmon, filemon* oder, unter Windows 7 und Windows 8, *procmon*

Die Kompatibilitätsprüfung sollte in das Test- und Freigabeverfahren der Software integriert werden.

Für die Behandlung von Problemen hinsichtlich der Software-Kompatibilität ab Windows 7 ist zusätzlich M 4.424 *Sicherer Einsatz älterer Software ab Windows 7* zu beachten.

Prüffragen:

- Wurde vorhandene oder zur Beschaffung anstehende Software für Windows-Clients ab Windows Vista auf Kompatibilität zu der eingesetzten Windows-Version überprüft?
- Wird vor einer beabsichtigter Hardwareänderung oder bei einer Betriebssystemmigration die Treibersoftware für alle betreffenden Komponenten auf Kompatibilität und Verfügbarkeit zur eingesetzten Windows-Version geprüft?
- Ist die Kompatibilitätsprüfung in das Test- und Freigabeverfahren der Software integriert?

# M 2.442 Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Der Einsatz eines mobilen Rechners ist mit typischen Gefährdungen verbunden, die sich aus dem mobilen Einsatz ergeben. Beim Einsatz von Windows ab Windows Vista auf mobilen Rechnern ist, wie für alle mobilen Rechner, der Baustein B 3.203 *Laptop* zu beachten. Für die Bereiche Datenverschlüsselung, Datensicherung und lokal installierte Firewall stellen Clients ab Windows Vista eigene Mechanismen zur Verfügung. Zu diesen werden nachfolgend Empfehlungen ausgesprochen.

Windows Phone 8 ist ein Betriebssystem für Smartphones. Es basiert auf dem Kernel von Windows 8 und beinhaltet somit auch Sicherheitsmechanismen von Windows 8 (z.B. Secure Boot, BitLocker). Die im Folgenden beschriebenen Maßnahmen sind damit z. T. auch für Geräte mit Windows Phone 8 anwendbar.

### UEFI Secure Boot

Einige Sicherheitsfunktionen des Betriebssystems können umgangen werden, wenn es einem Angreifer gelingt, auf dem System ein anderes Betriebssystem zu starten, das unter seiner Kontrolle steht. Hierzu kommen oft Live-Systeme zum Einsatz, die von mobilen Datenträgern gebootet werden. Mit "Secure Boot" verfügt der BIOS-Nachfolger UEFI über eine Funktion, die das Booten unautorisierter Betriebssysteme verhindert und beim Booten das eingerichtete Betriebssystem auf Manipulationen untersucht. Auf mobilen Systemen sollte Secure Boot zwingend zum Einsatz kommen. Nähere Ausführungen hierzu finden sich in Maßnahme M 4.49 *Absicherung des Boot-Vorgangs für ein Windows-System*.

### Datenverschlüsselung

Mobile Rechner befinden sich häufig in Umgebungen, die ein deutlich niedrigeres Sicherheitsniveau als geschützte Büroumgebungen bieten. Daher sollten die auf dem mobilen Rechner befindlichen schützenswerten Daten verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*). Neben einer Reihe von Drittprodukten können zur Verschlüsselung auch die in Windows Vista und Windows 7 integrierten Mechanismen eingesetzt werden:

- EFS (Encrypting File System) kann zur Verschlüsselung einzelner Dateien und/oder Verzeichnisse eingesetzt werden (siehe M 4.147 *Sichere Nutzung von EFS unter Windows*).
- Verschlüsselung der Offline-Dateien.
  Offline-Dateien sind im Grunde Kopien von Dokumenten, die sich auf einer Freigabe im Netz befinden. Sie werden auf dem lokalen Rechner in einer Datenbank gespeichert, so dass der Zugriff auf die Dokumente auch dann erhalten bleibt, wenn die Freigabe im Netz nicht erreichbar ist. Die Möglichkeit, diese Offline-Dateien zu verschlüsseln, wurde unter Windows XP eingeführt.
  Der gesamte Speicher für Offline-Dateien, der Dateien aller Benutzer beinhaltet, wird mit einem computerspezifischen Schlüssel verschlüsselt. Die

Verschlüsselung ist transparent für den Benutzer und kann nur von Administratoren aktiviert und deaktiviert werden.

Der zusätzliche Einsatz des EFS empfiehlt sich, wenn die zu schützenden Daten auf dem mobilen Rechner auch dann verschlüsselt sein sollen, wenn der mobile Rechner ab Windows Vista eingeschaltet ist. Wenn an den Dateien oder Laufwerken, die mittels EFS geschützt sind, gearbeitet wird, liegen auch hier die Daten unverschlüsselt vor.

Unter Windows Vista ohne SP1 empfiehlt sich der Einsatz der Verschlüsselung der Offline-Dateien , wenn der lokale Ordner für Offline-Dateien auf dem mobilen Rechner von der Bootpartition in eine andere Partition verschoben worden ist.

Die Strategie zum Schutz der auf einem mobilen Rechner befindlichen Daten ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen.

**Datensicherung**

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. Vertiefende Informationen hierzu sind in M 6.32 *Regelmäßige Datensicherung* zu finden.

Seit Windows Vista können einzelne Dateien gesichert oder komplette PC-Sicherungsabbilder (Images) von Partitionen erstellt werden (siehe M 6.78 *Datensicherung unter Windows Clients*).

Wenn Netzlaufwerke zur Aufnahme der Datensicherung konfiguriert sind, kann eine Sicherung nur erfolgen, wenn die mobilen Rechner mit dem Backup-Server untereinander vernetzt sind. Die Zeiten zur Datensicherung müssen daher entsprechend geplant werden.

Für die Datensicherung können Wechselmedien eingesetzt werden. Wenn dies beabsichtigt wird, müssen die entsprechenden Zugriffe auf die Wechselmedien zur Datensicherung und zur Datenrücksicherung möglich sein. Dies muss bei der technischen Durchsetzung von Zugriffsbeschränkungen auf Wechselmedien berücksichtigt werden (siehe M 4.339 *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*).

Die Strategie zur Datensicherung eines mobilen Rechners (Sicherung einzelner Dateien, Windows Complete PC-Sicherungsabbild oder Drittprodukt sowie Sicherungszeiten und -orte) ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen.

**Lokal installierte Firewall**

Im Gegensatz zu stationären institutionssinternen Desktops besteht bei mobilen Rechnern die Möglichkeit, dass sie direkt an das Internet angeschlossen werden. Der Schutz durch eine lokal installierte Firewall ist in diesem Fall unabdingbar.

Clients ab Windows Vista bieten mit der Windows Firewall eine Kombination aus "Personal Firewall" und IPSec-Gateway. Die Firewall kann über das Windows Sicherheitscenter konfiguriert werden. Seit Windows 7 kann die Firewall auch im Wartungscenter unter der Rubrik *Sicherheit* konfiguriert werden. Für eine deutlich feiner granulierte Konfigurationsmöglichkeit der Windows Firewall steht seit Windows Vista ein Snap-in für die Managementkon-

sole (*mmc.exe*) zur Verfügung. Ein Snap-in ist eine Ergänzungskomponente einer Konsole für bestimmte administrative Aufgaben.

Die Windows Firewall kann neben eingehenden auch ausgehenden Datenverkehr kontrollieren. In der Standardeinstellung wird der eingehende Datenverkehr bis auf die konfigurierten Ausnahmen blockiert (Whitelist-Ansatz) und der ausgehende Datenverkehr bis auf die konfigurierten Ausnahmen durchgelassen (Blacklist-Ansatz).

Die Standardeinstellung der Windows Firewall hängt von der zugrunde liegenden Windows Version ab. Unter Windows Vista und Windows 7 Enterprise sowie Windows Vista Business und Windows 7 Professional sind an der Windows Firewall nur wenige Ports geöffnet. Unter Windows Vista sowie Windows 7 Ultimate dagegen sind zahlreiche lokale Windows-Dienste von außen erreichbar.

Die Windows Firewall nutzt den Windows Dienst "Network Location Awareness" (NLA). Für jede Netzumgebung (auch Netztyp genannt) kann der Administrator eigene Richtlinien für die Windows Vista beziehungsweise Windows 7 Firewall konfigurieren. Dabei unterscheiden Clients ab Windows Vista die drei Netzumgebungen *Domäne* (bei Windows 7 *Domänennetzwerk)*, *Öffentlich* und *Privat*. Befindet sich ein Client erstmalig in einem Netz, dann erfragt Windows ab Windows Vista vom Benutzer, welche Netzumgebung gerade vorherrscht. Hierzu benötigt der Benutzer administrative Berechtigungen. Liegen diese nicht vor, dann wählt das Betriebssystem ab Windows Vista die Klassifikation *Öffentlich.* Ist das Netz eine Domäne mit dem Windows Client als Mitglied, dann wählt Windows automatisch die Netzumgebung *Domäne/Domänennetzwerk.*

Einmal klassifizierte Netze werden vom NLA-Dienst anhand verschiedener Kriterien wie der MAC-Adresse des Default-Gateways wiedererkannt. Nur ein Benutzer mit administrativen Berechtigungen kann eine andere Klassifikation vornehmen sowie das Verhalten der Windows Firewall für eine bestimmte Klassifikation ändern.

Das Standardverhalten der Windows Firewall gibt folgende Einstellungen für die Netzumgebungen *Domäne*, *Öffentlich* und *Privat* vor.

Für die Netzumgebung *Domäne* gilt:

- Die Windows Firewall wird aktiviert
- Die Windows Firewall bezieht die Richtlinieneinstellungen aus der Active Directory-Domäne.
- Die Konfiguration der Netzerkennung und der Datei- und Druckerfreigabe basiert auf den aus der Active Directory-Domäne herunter geladenen Gruppenrichtlinien.

Für die Netzumgebung *Öffentlich* gilt:

- Die Windows Firewall wird aktiviert.
- Die Netzerkennung (NLA) wird deaktiviert.
- Jegliche Datei- und Druckerfreigabe wird deaktiviert, inklusive der Freigabe von Wechselmedien.

Für die Netzumgebung *Privat* gilt:

- Die Windows Firewall wird aktiviert.
- Die Netzerkennung (NLA) wird aktiviert.
- Jegliche Datei- und Druckerfreigabe wird deaktiviert, inklusive der Freigabe von Medien

Aller Wahrscheinlichkeit nach werden mobile Rechner in unterschiedlichen Umgebungen einen Zugang zu einem Netz haben. Typische Netzumgebungen sind das LAN der eigenen Institution, ein LAN am Heimarbeitsplatz und ein Internetzugang an einem öffentlichen WLAN-Hotspot. Clients ab Windows Vista unterstützen die automatische Erkennung einer Netzumgebung und wenden unterschiedliche Firewall-Regelsätze in Abhängigkeit von der aktuellen Netzumgebung an. Soll der Benutzer diese Eigenschaft nutzen können, muss er zumindest beim ersten Zugang zu einem Netz über administrative Rechte verfügen. Der Benutzer muss dann mindestens in der korrekten Zuweisung einer Netzumgebung und gegebenenfalls auch in der Anpassung von Regelsätzen geschult werden.

Die Strategie zum Einsatz der lokalen Firewall auf einem mobilen Rechner (Netzumgebungs-abhängige Regelsätze, Möglichkeit der Zuordnung der Netzumgebung durch einen Benutzer) ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen. Dabei ist zu prüfen, ob die windowseigene Firewall auch in komplexeren Szenarien, wie im Zusammenspiel mit einem Virtual Private Network (VPN), die benötigte Schutzwirkung entfaltet oder ob auf ein Produkt eines Drittherstellers zurückgegriffen werden muss.

Prüffragen:

- Ist der Boot-Vorgang bei UEFI-basierten mobilen IT-Systemen mit Secure Boot abgesichert?
- Werden die Daten auf einem mobilen Client ab Windows Vista durch Verschlüsselung und Datensicherung geschützt?
- Wird die Strategie zum Einsatz der lokalen Firewall auf einem mobilen Rechner nach Bedarf anhand der konkreten Umstände und im Einzelfall festgelegt?

# M 2.443 Einführung von Windows Vista SP1

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

SP1 steht für Service Pack 1 und ist eine Zusammenstellung von Software-Korrekturen und -Ergänzungen für das Betriebssystem Windows Vista von Microsoft. Das SP1 gibt es für die 32-Bit-Version (x86) und die 64-Bit-Version (x64) von Windows Vista.

Microsoft unterstützt für den Bezug des SP1 die Vertriebswege *Stand-alone-Package*, *Windows Update* und *Integrated DVD*. Die nachfolgende Tabelle nennt zu jedem dieser Vertriebsweg wichtige Eigenschaften.

| **Vertriebsweg** | **Eigenschaften** |
|---|---|
| Standalone Package | - Erfordert keinen Internet-Zugang des Windows Vista Clients auf dem das SP1 eingespielt werden soll.<br>- Ein einmal bezogenes Standalone Package kann etwa über ein Programm zur Software Verteilung auf mehreren Windows Vista Clients eingespielt werden.<br>- Die Größe des Service Pack 1 RC variiert zwischen 400 MB und 900 MB, je nach dem, wie viele Sprachen unterstützt werden und ob die 32-Bit Version (x86) oder die 64-Bit Version (x64) gewählt wurde. |
| Windows Update | - Erfordert für die Verbindung zu den entsprechenden Update-Servern von Microsoft einen Internet-Zugang des Windows Vista Clients, auf den das SP1 eingespielt werden soll.<br>- Mit etwa 65 MB wesentlicher kleiner als ein Standalone Package. |
| Integrated DVD | - Beinhaltet das Betriebssystem Windows Vista auf dem Stand des SP1.<br>- Für die Installation von Windows Vista in Verbindung mit SP1.<br>- Im Anschluss an die Installation muss Windows Vista innerhalb von 30 Tagen aktiviert werden. |

Tabelle: Vertriebswege von Windows Vista SP1

Um das SP1 zu beziehen, ist die damit verbundene Netzauslastung für das LAN der Organisation zu berücksichtigen. Die Netzauslastung ergibt sich aus der Größe des SP1 und der Anzahl der Windows Vista Clients, die zeitgleich das SP1 beziehen.

Bevor das SP1 auf einem Windows Vista Produktivsystemen zum Einsatz kommt, muss das SP1 in einer Testumgebung auf mögliche Inkompatibilitäten getestet werden.

Des Weiteren muss vor der Installation des SP1 auf einem Windows Vista Client sichergestellt werden, dass der dafür notwendige Festplattenplatz vorhanden ist. Der benötigte Festplattenplatz hängt von einer Vielzahl von Faktoren ab. Zu diesen zählen beispielsweise der Vertriebsweg des SP1 auf dem Windows Vista Client sowie die Anzahl der zu unterstützenden Sprachen. Die Installationsroutine des SP1 ermittelt die präzisen Werte zum notwendigen Festplattenplatz. Zur Orientierung nennt Microsoft 4,5 GB im Fall eines Standalone-Package mit fünf unterstützten Sprachen für die 32-Bit-Version (x86). Im Bedarfsfall müssen vor einer Installation des SP1 genaue Angaben zum erforderlichen Festplattenplatz von Microsoft erfragt werden.

Vor der Installation des SP1 auf einem Windows Vista Client muss sichergestellt werden, dass zuvor die notwendigen Windows Vista Updates eingespielt worden sind. Dies sind laut Microsoft Knowledge Base Artikel 935509 das Update 935509 zu BitLocker, das Update 938371 zur Installation/Deinstallation des SP1 und das Update 937287 zur Windows Vista Installations-Software (Stand Frühjahr 2008).

Das Service Pack 1 verfügt neben Fehlerkorrekturen und Verbesserungen an vorhandenen Mechanismen auch über einige sicherheitsrelevante Änderungen oder Erweiterungen enthalten. Zu diesen zählen beispielsweise:

- Warnmeldungen anstatt des bisher drohenden RFM (Modus mit reduzierter Funktionalität, Reduced Functionality Mode), wenn gegen bestimmte Vorgaben im Zusammenhang der Aktivierung einer Windows Vista Lizenz tatsächlich oder vermeintlich verstoßen worden ist (siehe M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* und M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).
- EFS-verschlüsselte Dateien können mit dem Tool zur "Datensicherung und Wiederherstellung" gesichert werden. (siehe M 6.78 *Datensicherung unter Windows Clients*).
- APIs (Application Programming Interfaces) bieten verbesserte Möglichkeiten, Antivirensoftware von Drittanbietern in einer 64-Bit Umgebung neben der Kernel Patch Protection zu nutzen.
- Es wird eine Multifaktor Authentifizierung durch einen USB-Stick und einer PIN für BitLocker bei der Nutzung des TPM (Trusted Platform Module) unterstützt.
- Die Verschlüsselung weiterer Partitionen durch BitLocker (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*) ist möglich.
- SHA-256, AES-GCM und AES-GMAC für ESPESP (Encapsulating Security Payload) und AH (Authentication Header), ECDSA, SHA-256 und SHA-384 für Internet Key Exchange (IKE) und AuthIP werden unterstützt.
- Der NIST SP 800-90 Elliptical Curve Cryptography (ECC) Pseudozufallszahlengenerator (pseudo-random number generator = PRNG) steht bei der Auswahl der verfügbaren PRNG zur Verfügung.

Prüffragen:

- Ist festgelegt, welche Version des Service Pack 1 benötigt wird?
- Wurde das Service Pack 1 in einer Testumgebung auf mögliche Inkompatibilitäten getestet, bevor es in einer Produktivumgebung installiert worden ist?

- Steht genügend Bandbreite für den Bezug des Service Pack 1 über das Internet und die Installation des Service Pack 1 im LAN der Organisation zur Verfügung?
- Steht auf dem jeweiligen Windows Vista Client genügend Festplattenplatz für das Service Pack 1 zur Verfügung?
- Sind auf dem Windows Vista Client die notwendigen Updates gemäß dem Microsoft Knowledge Base Artikel 935509 vor der Service Pack 1 Installation installiert worden?

# M 2.444 Einsatzplanung für virtuelle IT-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für virtuelle IT-Systeme sind bei der Planung neben den schon in M 2.315 *Planung des Servereinsatzes* angegebenen Voraussetzungen für einen sicheren Serverbetrieb weitere Punkte zu beachten. Im Folgenden werden zusätzliche Vorgaben hinsichtlich der Planung virtueller IT-Systeme beschrieben.

**Herstellerunterstützung für virtuelle IT-Systeme**

Es ist zu prüfen, dass alle Anwendungen, die auf virtuellen IT-Systemen betrieben werden sollen, durch ihre Hersteller auf der gewählten Virtualisierungsplattform unterstützt werden. Die Hersteller geben Ihre Software in der Regel für eine bestimmte Kombination aus Betriebssystem und Hardwareplattform frei. Sie sichern nur dann Support für eventuell auftretende Probleme zu, wenn die Software gemäß diesen Vorgaben genutzt wird. Da die Hardwareplattform "virtuelles IT-System" bisher nicht standardisiert ist, sagen nicht alle Softwarehersteller eine pauschale Unterstützung virtueller IT-Systeme zu. Die Hersteller bieten meistens nur für eine bestimmte Kombination von Betriebssystem und Virtualisierungsprodukt Support an, z. B. bei der Fehleranalyse und -behebung.

**Lebenszyklus virtueller IT-Systeme**

Weiterhin ändern sich etablierte Verfahrensweisen für die Inbetriebnahme, Inventarisierung, den Betrieb und die Außerbetriebnahme von (virtuellen) IT-Systemen beim Betrieb in einer virtuellen Infrastruktur. Es ist daher detailliert zu planen und festzulegen, wie diese Prozesse angepasst werden. Folgende Punkte sind sicherzustellen:

- Es muss geprüft werden, ob die eingesetzten Betriebssysteme und Anwendungen für den Betrieb in virtualisierten IT-Systemen geeignet sind.
- Es ist zu gewährleisten, dass das Virtualisierungsprodukt für den Einsatzzweck der IT-Systeme geeignet ist.
- Es dürfen keine Virtualisierungsfunktionen wie z. B. Snapshots verwendet werden, die zu Problemen mit dem Applikationen führen können (Siehe auch M 4.347 *Deaktivierung von Snapshots virtueller IT-Systeme*).
- Für die Applikationen sollten keine Hardwarekomponenten wie z. B. Softwareschutzmodule (*Dongles*) oder ISDN-Karten benötigt werden, die den virtuellen IT-Systemen innerhalb der virtuellen Infrastruktur nicht zur Verfügung gestellt werden können.
- Alle virtuellen IT-Systeme müssen von der Inventarisierung des Informationsverbundes vollständig erfasst werden, damit beispielsweise eine Unterlizenzierung vermieden wird oder Systeme betrieben werden, deren Einsatzzweck unbekannt ist.
- Die für die Inbetriebnahme von physischen IT-Systemen üblichen Verfahrensweisen sowie Planungs- und Betriebsvorbereitungen sind auf angemessene Weise und ihrem Sinn nach auf die virtuellen IT-Systeme zu übertragen. Werden beispielsweise physische IT-Systeme mit einem Aufkleber versehen, auf dem Name und IP-Adresse dokumentiert werden, so ist dies bei virtuellen IT-Systemen nicht möglich. Diese Vorgaben können aber bei der Benennung dieser virtuellen IT-Systeme in der Verwaltungssoftware umgesetzt werden.

- Mit den Server- und Anwendungsbetreibern sind zusammen realistische und angemessene Performance- und Ressourcenanforderungen für die virtuellen IT-Systeme festzulegen, bevor die Systeme in Betrieb genommen werden. Werden die Performanceanforderungen bestimmt, ist zu prüfen, ob Leistungseinschränkungen bei gelegentlich auftretenden Lastspitzen hingenommen werden können: So sind beispielsweise Skripte zur automatisierten Verarbeitung von Datenbankinhalten häufig nicht zeitkritisch und müssen daher nicht mit maximaler Performance ausgeführt werden.
- Es ist zu regeln, wie Routinetätigkeiten während des Betriebs virtueller IT-Systeme auszuführen sind. Dabei muss sichergestellt werden, dass Tätigkeiten, wie das Starten und Stoppen virtueller IT-Systeme, das Anlegen und Löschen von sowie das Zurücksetzen auf Snapshots mit den Serverbetreibern und Applikationsbesitzern abgestimmt werden.
- Die Performance virtueller IT-Systeme ist zu überwachen. Es muss sichergestellt sein, dass ihre Performanceanforderungen ausreichend erfüllt werden.
- Es ist ein Prozess zu etablieren, mit dem Engpässe beim Verbrauch an Prozessorleistung, Hauptspeicher und Festplattenspeicher rechtzeitig erkannt werden und bei dem auf solche Engpässe angemessen reagiert wird.

**Test- und Entwicklungsumgebungen**

In Test- und Entwicklungsumgebungen, bei denen lediglich eine funktionale Analyse virtueller IT-Systeme durchgeführt werden soll, kann von den oben angegebenen Vorgaben abgewichen werden. Allerdings ist ein Prozess innerhalb der Organisation zu etablieren, der gewährleistet, dass die Konfiguration und die Ressourcenzuteilungen der virtuellen IT-Systeme überprüft und unter Umständen angepasst werden, bevor sie produktiv in Betrieb genommen werden. Beispielsweise sollten virtuelle IT-Systeme nicht einfach aus der Test- und Entwicklungsumgebung heraus kopiert oder geklont, sondern neu installiert werden. Wird das IT-System nicht neu installiert, muss für die zu kopierenden beziehungsweise zu klonenden virtuellen IT-Systeme sorgfältig geprüft werden, ob sie sich für den Produktivbetrieb eignen. Es ist insbesondere zu prüfen, ob bestimmte in Test- und Entwicklungsumgebungen verwendete Virtualisierungsfunktionen (wie z. B. Skripte in Gastwerkzeugen) noch aktiv sind. Die Tests sollten dabei in einer Umgebung durchgeführt werden, die die gleiche Virtualisierungslösung wie das Zielsystem verwendet. Dies soll gewährleisten, dass das Verhalten der virtuellen IT-Systeme in der Testumgebung nicht von der Produktivumgebung abweicht.

Prüffragen:

- Werden virtuelle IT-Systeme aus Test- und Entwicklungsumgebungen vor der Inbetriebnahme im Produktivnetz daraufhin geprüft, dass sie für den Produktiveinsatz geeignet sind?
- Ist eine Vorgehensweise für die Inbetriebnahme von Virtualisierungsservern und virtuellen IT-Systemen festgelegt worden?
- Ist für virtuelle IT-Systeme festgelegt worden, welche Virtualisierungsfunktionen (wie beispielsweise Snapshots) verwendet werden dürfen?
- Ist sichergestellt, dass die Performance der virtuellen IT-Systeme laufend überwacht wird?
- Sind alle virtuellen IT-Systeme des Informationsverbundes in der Inventarisierung erfasst?
- Ist eine Vorgehensweise für die Außerbetriebnahme von Virtualisierungsservern und virtuellen IT-Systemen festgelegt worden?

# M 2.445 Auswahl geeigneter Hardware für Virtualisierungsumgebungen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter Beschaffung

Die gängigen Betriebssystem- und Servervirtualisierungslösungen haben individuelle Anforderungen an die zugrunde liegende Hardwarearchitektur bzw. die Ausstattung des Virtualisierungsservers mit Hardwarekomponenten wie Netzschnittstellen oder Massenspeicherkarten. Diese Anforderungen müssen bei der Beschaffung von Serversystemen bedacht werden, wenn diese als Virtualisierungsserver eingesetzt werden sollen. Für die unterschiedlichen Arten der Virtualisierung (Betriebssystem-, hypervisorbasierte und hostbasierte Servervirtualisierung) bestehen einige grundsätzliche Unterschiede in den Hardwareanforderungen. Diese sind im Folgenden dargestellt.

### Anforderungen von Betriebssystemvirtualisierung und hostbasierter Servervirtualisierung

Systeme zur Betriebssystemvirtualisierung und so genannte hostbasierte Servervirtualisierungslösungen können meist auf eine umfangreiche Treiberunterstützung des Basisbetriebssystems, auf dem sie installiert werden, zurückgreifen. Ein Beispiel für eine Betriebssystemvirtualisierung ist *Sun Solaris Zones*, die in das Betriebssystem *Solaris* integriert ist. Hostbasierte Servervirtualisierungen sind beispielsweise *Microsoft Virtual PC, Sun VirtualBox,* oder *VMware Server*, die wie ein herkömmlicher Dienst auf einem kompatiblen Betriebssystem installiert werden können. In der Regel kann jede Hardwarekomponente (Netzschnittstellen, SCSI-Controller und ähnliches) verwendet werden, die vom gewählten Betriebssystem unterstützt wird. Üblicherweise ist in solchen Fällen eine Vielzahl an Komponenten nutzbar.

### Anforderungen von Hypervisorprodukten

Erheblich strengere Anforderungen an die Auswahl der in Kombination mit der Virtualisierungslösung einzusetzenden Hardwarekomponenten werden jedoch durch die Hypervisorprodukte gestellt. Hier sind z. B. *Microsoft Hyper-V, VMware ESX* oder *XEN* zu nennen. Diese stellen ein auf für die Virtualisierung reduziertes Betriebssystem dar und haben meist eine eingeschränkte Hardwareunterstützung beziehungsweise Treiberausstattung oder besondere Hardwareanforderungen an den verwendeten Prozessor. Z. B. kann die Virtualisierungslösung *XEN* nur dann ohne Einschränkungen genutzt werden, wenn der Prozessor Virtualisierungsfunktionen enthält (*Intel VT, AMD-V*). Gleiches gilt für *Microsoft Hyper-V.*

Unabhängig von der Wahl der zu nutzenden Virtualisierungslösung sind Kompatibilitäten bei der Planung der Virtualisierungsumgebung vorab zu prüfen. Untersucht werden muss bei Betriebssystemvirtualisierungslösungen und hostbasierten Servervirtualisierungslösungen die Lauffähigkeit der Virtualisierungssoftware unter dem entsprechenden Betriebssystem mit der gewählten Hardware.

### Auswahl der Hardware

Als Hardwareplattform für die Virtualisierungslösung sind geeignete physische Server auszuwählen. Die Hersteller der Virtualisierungslösungen veröffentlichen in regelmäßigen Abständen aktualisierte Kompatibilitätslisten, die bestimmte Hardwarekonfigurationen als tauglich für ihr Produkt zertifizieren, al-

so eine Gewähr für die Eignung der Hardware geben. Solche Listen sollten bei der Wahl der Hardware berücksichtigt werden, vor allem, wenn diese im Produktivbetrieb eingesetzt werden sollen.

Zudem werden die in Wartungsverträgen für die Virtualisierungssoftware vereinbarten Unterstützungsleistungen und Garantien häufig nicht oder nur eingeschränkt gewährt, wenn die verwendete Hardware vom Hersteller nicht zertifiziert ist. Bei bereits produktiv eingesetzten und problemlos funktionierenden Umgebungen ist zu prüfen, inwieweit der Hersteller Support für sein Virtualisierungsprodukt auch mit der vorhandenen Hardware gewährt, auch wenn diese nicht zertifiziert ist.

Prüffragen:

- Wurde die Kompatibilität der Virtualisierungslösung zur verwendeten Hardware überprüft?
- Ist sichergestellt, dass der Hersteller der eingesetzten Virtualisierungslösung Support für die betriebene physische Hardware gewährt?

# M 2.446 Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei Virtualisierungsinfrastrukturen kommen zusätzlich zu den üblichen Rollen und Administrationstätigkeiten (siehe M 2.38 *Aufteilung der Administrationstätigkeiten*) weitere administrative Aufgaben im Rechenzentrumsbetrieb hinzu.

Die Besonderheit der Rolle von Administratoren in einer virtuellen Infrastruktur besteht darin, dass diese potenziell eine sehr weitgehende Machtbefugnis über die virtuellen IT-Systeme, die in der virtuellen Infrastruktur betrieben werden, haben können. Dies schließt mit ein, dass sie

- die Kontrolle über die emulierte Hardwareausstattung haben,
- die virtuellen IT-Systeme mit Netzen verbinden können,
- den virtuellen IT-Systemen Speicherressourcen aus dem Speichernetz zuweisen können und
- meist Zugriff auf die Konsolen der virtuellen IT-Systeme

haben.

Eine Aufteilung der Administratorrolle ermöglicht die gegenseitige Kontrolle der unterschiedlichen Administratorengruppen in einem arbeitsteiligen Rechenzentrumsbetrieb.

So können bei einigen Virtualisierungsprodukten, wie z. B. *Citrix XENCenter, Microsoft System Center Virtual Machine Manager* oder *VMware vSphere*, Administratorrollen definiert werden, die bestimmten Benutzergruppen eine Auswahl von Rechten in der virtuellen Infrastruktur zuweisen. Hier können beispielsweise bestimmte Benutzergruppen daran gehindert werden, virtuelle IT-Systeme aus der virtuellen Infrastruktur zu exportieren. Des Weiteren können Berechtigungen zum Ein- und Ausschalten von virtuellen IT-Systemen oder zur Erzeugung von Snapshots erteilt oder entzogen werden.

Es ist zu prüfen, ob für die virtuell zu betreibenden IT-Systeme eine Aufteilung der Administratorrollen notwendig ist. Dies kann beispielsweise der Fall sein, wenn eine bestimmte Administratorengruppe keine Berechtigung für die Zuweisung von Netzen für ein virtuelles IT-System mit erhöhtem Schutzbedarf bezüglich Vertraulichkeit erhalten soll.

Wird die Aufteilung der Administratorrollen benötigt, so ist die Definition entsprechender Administratorrollen für die Virtualisierungsinfrastruktur zu nutzen. Einige Virtualisierungsprodukte bieten eine solche Möglichkeit nicht. In diesem Fall ist zu prüfen, ob eine Aufteilung der Administratorrollen ausschließlich organisatorisch, das heißt z. B. mittels einer Richtlinie ausreicht.

Prüffragen:

- Wurde geprüft, ob eine Aufteilung der Administratorrollen für die virtuelle Infrastruktur notwendig ist?
- Wurde die Aufteilung der Administratorrollen, wenn sie notwendig ist, organisatorisch oder, falls möglich, mit technischen Mitteln des Virtualisierungsproduktes umgesetzt?

# M 2.447 Sicherer Einsatz virtueller IT-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Bei der Inbetriebnahme virtueller IT-Systeme müssen einige Besonderheiten beachtet werden, die über die für physische IT-Systeme notwendigen Maßnahmen hinaus gehen (beispielsweise M 2.318 *Sichere Installation eines IT-Systems*). Dies resultiert aus der Dynamik und Flexibilität der virtuellen IT-Systeme sowie der Möglichkeit, dass mehrere virtuelle IT-Systeme, die unterschiedliche Daten verarbeiten, auf einem Virtualisierungsserver nebeneinander betrieben werden.

Virtuelle IT-Systeme sind zunächst genauso wie physische Computer gemäß ihrem Typ und Einsatzzweck (Anwendungsserver oder Client, aber auch beispielsweise Switch) in Betrieb zu nehmen. Daher sind die für physische Systeme einschlägigen und etablierten Maßnahmen bei der Installation und im späteren Betrieb ebenfalls für virtuelle IT-Systeme umzusetzen. Darüber hinaus muss berücksichtigt werden, dass für Applikationen, falls sie von eigenständigen physischen IT-Systemen auf virtuelle IT-Systeme verlagert werden, zusätzliche Gefährdungen entstehen können. Beispielsweise kann es unter Umständen zu Engpässen bei der Verarbeitungsgeschwindigkeit oder bei der Speicherkapazität kommen. Daher kann es erforderlich sein, eine bestehende Installationsdokumentation für ein in Betrieb zu nehmendes, virtuelles IT-System anzupassen.

Die Inbetriebnahme virtueller IT-Systeme muss deshalb sorgfältig vorbereitet werden (siehe auch M 2.444 *Einsatzplanung für virtuelle IT-Systeme*). Es sollten insbesondere folgende Punkte vor der unmittelbaren Inbetriebnahme beachtet werden:

- Es muss sichergestellt werden, dass nur die hierfür zuständigen Administratoren die Virtualisierungssoftware bezüglich der virtuellen IT-Systeme konfigurieren sowie virtuelle IT-Systeme einrichten oder löschen können.
- Die Zugriffsrechte auf die virtuellen IT-Systeme müssen gemäß den Anforderungen eingerichtet werden. Als Grundregel gilt auch hier, dass nur die tatsächlich erforderlichen Zugriffsmöglichkeiten erlaubt werden sollten. Dies gilt nicht nur für die Verwaltungssoftware des Virtualisierungsservers, sondern insbesondere auch für die Daten, mit denen das virtuelle IT-System auf dem Virtualisierungsserver repräsentiert wird.
- Es muss gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur zur Verfügung stehen.
- Die Auswirkungen der Virtualisierung (beispielsweise bei der Systemüberwachung oder der Nutzung virtueller Hardware-Ressourcen), die sich für die Administratoren des virtuellen IT-Systems selbst und der darauf betriebenen Applikationen ergeben, sind zu ermitteln und zu beachten.
- Abhängig vom Einsatzzweck müssen die einzelnen virtuellen IT-Systeme auf einem physischen Computer mehr oder weniger stark isoliert und gekapselt sein (siehe auch M 3.72 *Grundbegriffe der Virtualisierungstechnik* und M 3.70 *Einführung in die Virtualisierung*). Dies gilt insbesondere dann, wenn virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver betrieben werden sollen.

- Der Einsatz mehrerer virtueller IT-Systeme auf einem physischen Computer kann erhebliche Auswirkungen auf die Verfügbarkeit, den Durchsatz und die Antwortzeiten der betriebenen Anwendungen haben.
  Es ist zu prüfen, ob die Anforderungen an die Verfügbarkeit und den Durchsatz der Applikationen mit der eingesetzten Virtualisierungslösung erfüllt werden können. Dies kann dadurch geschehen, dass vor der Überführung in den Wirkbetrieb getestet wird, ob das virtuelle IT-System akzeptable Antwortzeiten und Verarbeitungsgeschwindigkeiten erreicht.
- Weiterhin sollten die Leistungseigenschaften virtueller Server überwacht werden, damit bei Engpässen zeitnah Anpassungen der Konfiguration vorgenommen werden können. Die Überwachung kann auf der Ebene der virtuellen IT-Systeme oder auf der Ebene des jeweiligen Virtualisierungsservers erfolgen. Hierbei ist zu beachten, dass Leistungswerte, die durch die virtuellen IT-Systeme selbst ermittelt werden, nicht immer der Realität entsprechen. Bei einigen Virtualisierungsprodukten wird einem virtuellen IT-System beispielsweise ein gewisser Anteil an der Gesamt-Prozessorzeit zugeteilt. Meldet das virtuelle System nun eine Auslastung seines (virtuellen) Prozessors, entspricht dies nicht in jedem Fall der tatsächlichen Auslastung des physischen Prozessors, sondern nur einer Auslastung der zugeteilten Prozessorzeit.

Prüffragen:

- Werden die Zugriffsrechte der Administratoren auf die virtuellen IT-Systeme auf das notwendige Maß beschränkt und nur die tatsächlich erforderlichen Zugriffsmöglichkeiten erlaubt?
- Stehen die für die virtuellen IT-Systeme notwendigen Netzverbindungen zur Verfügung?
- Sind die Administratoren der Virtualisierungsumgebung, der virtuellen IT-Systeme und der darauf betriebenen Anwendungen mit den Auswirkungen der Virtualisierung vertraut?
- Sind die Anforderungen an die Isolation und Kapselung der virtuellen IT-Systeme sowie der darauf betriebenen Anwendungen hinreichend erfüllt?
- Sind die Anforderungen an die Verfügbarkeit und den Durchsatz der virtuellen IT-Systeme ermittelt worden?
- Wird die Performance der virtuellen IT-Systeme im laufenden Betrieb überwacht?

# M 2.448 Überwachung der Funktion und Konfiguration virtueller Infrastrukturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Konfigurationsdateien von Virtualisierungsservern enthalten die für den Betrieb einer virtuellen Maschine notwendigen Informationen der virtuellen Infrastruktur. Hierzu gehören die Ressourcenzuteilung für jedes virtuelle IT-System und die Definition der Netze für die virtuellen IT-Systeme.

**Überwachung der Konfiguration virtueller IT-Systeme**

Die Konfiguration der virtuellen IT-Systeme für Server- und Betriebssystemvirtualisierung in einer virtuellen Infrastruktur bestimmt die Eigenschaften des virtuellen IT-Systems. Es wird festgelegt,

- welche Prozessorressourcen,
- wie viel Hauptspeicher und
- wie viel Festplattenplatz

einem virtuellen IT-System vom Virtualisierungsserver zur Verfügung gestellt werden.

Darüber hinaus werden bei einer Servervirtualisierung, bei der die Hardware vollständig virtualisiert wird, zusätzlich in der Konfiguration noch Eigenschaften der Hardwareemulation festgelegt. Hierzu gehören z. B.:

- Art eines Massenspeichergeräts und der Netzwerkkarten,
- Zugriff auf Laufwerke (Floppy, CD/DVD etc.) und andere, dem virtuellen IT-System zur Verfügung zu stellende Hardware sowie
- Verbindung der virtuellen IT-Systeme mit physischen Netzen.

Werden Konfigurationen der virtuellen IT-Systeme verändert, können diese unter Umständen nicht auf dringend benötigte Ressourcen zugreifen. Es ist auch möglich, dass ein virtuelles IT-System unbeabsichtigt Zugriff auf Ressourcen erhält, auf die es nicht zugreifen dürfen sollte. Ein Beispiel hierfür wäre die entstehende Zugriffsmöglichkeit auf sämtliche Lohndaten eines Unternehmens für die Mitarbeiter der Entwicklungsabteilung.

Somit sind die Konfigurationsdateien der virtuellen IT-Systeme besonders hinsichtlich ihrer Integrität oft besonders schutzbedürftig. Es sollte festgelegt werden, wie eine Prüfung dieser Konfigurationsdateien auf unautorisierte Änderungen erfolgen soll. In Abhängigkeit vom Schutzbedarf der auf dem Virtualisierungsserver laufenden virtuellen IT-Systeme sind

- automatisierte Prüfungen (z. B. mittels Prüfsummenverfahren) oder
- regelmäßige Prüfungen durch die Administratoren der Virtualisierungsserver

zu erwägen.

**Überwachung der Funktion der virtuellen Infrastruktur**

Auf einem Virtualisierungsserver werden in der Regel virtuelle Netze definiert, mittels derer die virtuellen IT-Systeme mit den physischen Netzen verbunden werden. Diese Netzfunktionen der Virtualisierungsserver können durch eine fehlerhafte Konfiguration oder falsche Verkabelung unbeabsichtigt Kommunikationswege öffnen, die sonst nicht nutzbar sein sollen. Ein Beispiel hierfür

wäre die fälschliche Anbindung eines hoch schutzbedürftigen ERP-Systems an eine DMZ, die für die Einwahl von Kunden vorgesehen ist. Daher ist regelmäßig zu überprüfen, dass die Netzkonfiguration bezüglich der Verkabelung und der logischen Einrichtung der Virtualisierungsserver den Planungen entspricht. Dies betrifft die Netzinfrastruktur und die Einbindung der Virtualisierungsserver in Speichernetze.

Bei einigen Virtualisierungsprodukten werden Ressourcen, wie z. B. Netzverbindungen, nur anhand eines nahezu frei zu vergebenen Namens unterschieden. Diese Ressourcen werden nun den virtuellen IT-Systemen über diesen Namen zugewiesen. Diese Zuordnung bleibt häufig erhalten, wenn ein virtuelles IT-System von einem Virtualisierungsserver auf einen Anderen migriert wird. Sind physisch oder logisch unterschiedliche Netzverbindungen mit dem gleichen Namen versehen, wird ein virtuelles IT-System möglicherweise mit einem falschen Netz verbunden. Dies kann gegebenenfalls fatale Folgen haben, wenn wegen eines Fehlers in der Konfiguration beispielsweise *Internet* und *Intranet* verwechselt worden sind.

Aus diesem Grund ist eine eindeutige und aussagekräftige Benennung der Netze zu wählen und regelmäßig zu prüfen, ob solche Netzzuordnungen korrekt sind. Dies kann durch eine Funktionsprüfung wie z. B. einem Erreichbarkeitstest des virtuellen Systems im zugewiesenen Netz geschehen.

Prüffragen:

- Ist sichergestellt, dass die Konfigurationsdateien der virtuellen Infrastruktur regelmäßig auf unautorisierte Änderungen überprüft werden?
- Wird überwacht, ob Netzzuordnungen dem dokumentierten Zustand entsprechen?
- Wurden eindeutige und aussagekräftige Identifikatoren für die Netze gewählt?

# M 2.449 Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zahlreiche gängige Lösungen zur Virtualisierung von IT-Systemen bieten die Möglichkeit, sich entweder lokal am Virtualisierungsserver oder über ein Netz von einer entfernten Arbeitsstation aus mit Hilfe einer Clientsoftware an der Virtualisierungssoftware anzumelden (z. B. *Citrix XenCenter* oder *VMware Console*). Diese Clientsoftware dient dazu, die Virtualisierungssoftware auf dem Virtualisierungsserver einzurichten, sowie sie zu warten und zu überwachen. Bei Produkten zur Servervirtualisierung muss sie aber auch genutzt werden, um auf die Konsolen der virtuellen Maschinen zu zugreifen. Dies ist bei diesen Produkten in der Regel auf Grund der Architektur der virtuellen IT-Systeme auch nicht anders realisierbar, da ein virtuelles IT-System keine physische Konsole besitzt. Auf diese Weise kann z. B. der Betriebszustand einer virtuellen Maschine auch während des Bootprozesses überwacht werden.

Virtuelle IT-Systeme bestehen bei einer Servervirtualisierung ausschließlich aus virtuellen Hardwarekomponenten. Diese Geräte, wie Netzwerkkarten, Massenspeichergeräte und Grafikkarten, müssen durch die Virtualisierungssoftware nachgebildet (emuliert) werden. Bei der Emulation von Netzwerkkarten und Massenspeichergeräten können die Befehle der virtuellen IT-Systeme in der Regel einfach an die jeweiligen physischen Geräte übermittelt werden. Sie müssen daher nicht vollständig emuliert werden. Grafikkarten müssen jedoch in der Regel vollständig durch die Virtualisierungssoftware emuliert werden. Daher wird dem virtuellen IT-System aus Performancegründen die ständige Existenz der Grafikkarte nur vorgespiegelt. Erst beim Zugriff auf die Konsolenschnittstelle eines virtuellen IT-Systems wird die tatsächliche Emulation in Software gestartet. Dies bindet in der Regel erhebliche Prozessor- und Speicherressourcen auf dem Virtualisierungsserver.

Da Konsolenzugriffe auf die virtuellen IT-Systeme starken Einfluss auf die Leistungsfähigkeit der Verwaltungssoftware eines Virtualisierungsservers haben, sind sie auf ein Mindestmaß zu beschränken.

Virtuelle IT-Systeme sollten somit möglichst nicht über direkte Konsolenzugriffe, sondern bevorzugt über das Netz, z. B. via RDP oder X-Window mittels SSH-Tunneling, gesteuert werden.

Prüffragen:

- Sind die Konsolenzugriffe auf die virtuellen IT-Systeme auf ein Mindestmaß beschränkt, damit sie keinen Einfluss auf die Leistungsfähigkeit des Virtualisierungsservers haben?
- Werden die virtuellen IT-Systeme über das Netz, z. B. via RDP oder X-Window mittels SSH-Tunneling gesteuert?

# M 2.450 Einführung in DNS-Grundbegriffe

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Der Domain Name System (DNS) ist ein Netzdienst, um Hostnamen von IT-Systemen in Computernetzen aufzulösen. Vorwärtsauflösung ist, wenn die IP-Adresse zu einem Hostnamen ermittelt wird. Wird dagegen der Hostname zu einer IP-Adresse ermittelt, wird dies als Rückwärtsauflösung bezeichnet.

**Domain-Namensraum**

DNS ist eine verteilte Datenbank die den baumförmigen Domain-Namensraum verwaltet. Der Baum besteht aus Knoten und Blättern, die als Label bezeichnet werden. Die Verkettung der durch Punkte getrennten Labels ergibt einen Domain-Namen. Der Domain-Namensraum ist in verschiedene Domains unterteilt. Die oberste Ebene, die Wurzel, wird als Punkt dargestellt und als "*root*" bezeichnet. Darunter folgen die Top-Level-Domains wie beispielsweise *com.*, *edu.*, *de.*, *at.*, danach die Second-Level-Domains wie *bund.,* usw.

Im Domain-Namensraum werden Informationen über die Zuordnung von IP-Adressen zu Domain-Namen gespeichert. DNS kann als eine Art Telefonbuch in Computernetzen bezeichnet werden, dessen Hauptaufgabe es ist, Namen aufzulösen. Es genügt beispielsweise den Domainnamen *www.bsi.bund.de.* im Browser einzugeben, DNS findet im Domain-Namensraum die zugehörige IP-Adresse und der Browser kann sich mit dem Ergebnis der Suche zum entsprechenden Webserver verbinden.

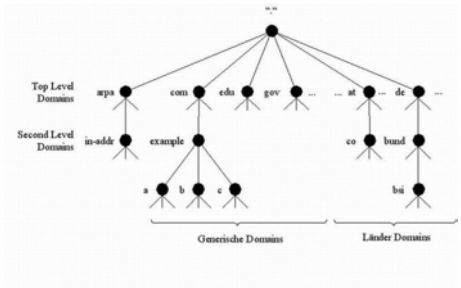



Abbildung: Domain-Namensraum

Grundsätzlich muss zwischen Domains und Zonen unterschieden werden. Eine Zone, wie in der Abbildung Domain vs. Zone dargestellt, ist eine Verwaltungseinheit, die ein DNS-Server über ein Master File einliest. Ein Master File enthält alle Domain-Informationen einer Zone, und wird von den zuständigen Administratoren verwaltet. Beispiele für Zonen sind *arpa*, *com*, *example, a, b* und *c,* wobei *com*, *example, a, b* und *c* jeweils eine eigene Zone darstellen. Unter einer Domain hingegen versteht man beispielsweise eine Domain wie *com* und alle darunter liegenden Subdomains, in diesem Fall *example*, *a*, *b*, *c*.

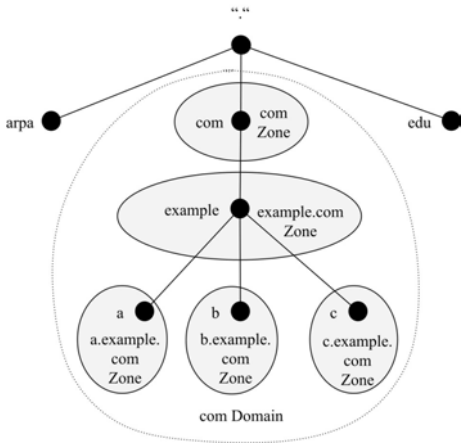



Abbildung: Domain vs. Zone

Für jede Zone sind mindestens zwei DNS-Server autoritativ, dies bedeutet, dass diese DNS-Server die Domain-Informationen dieser Zone verwalten. Zusätzlich kennt jeder DNS-Server die autoritativen DNS-Server für seine Subdomains. Das bedeutet, dass beispielsweise der DNS-Server für *com* den DNS-Server für *example* kennt, und somit bei einer Namensauflösung an diesen verweisen kann.

**Resolver**

Clientanwendungen benötigen einen Resolver, um an DNS teilzunehmen. Dieser ist oft Teil des Betriebssystems. Wenn eine Clientanwendung eine Namensauflösung benötigt, stellt sie eine Anfrage an den Resolver. Dieser packt die Anfrage in ein DNS konformes Paket, sendet dieses an einen DNS-Server, interpretiert die Antwort und übermittelt die Daten an die entsprechende Anwendung zurück. Um die Leistungsfähigkeit von DNS zu steigern, speichert der Resolver die Antwortdaten für eine bestimmte Zeit im Cache. Solange sich die Daten im Cache befinden, wird bei einer wiederholten Auflösung der DNS-Server nicht erneut befragt.

**DNS-Server**

DNS-Server sind Anwendungen, die Informationen über einen bestimmten Bereich des Domain-Namensraums verwalten. Die Informationen sind in sogenannten Zonendateien gespeichert. Verwaltet ein DNS-Server mehrere Domains, beispielsweise *bund.de* und die zugehörige Subdomain *bsi.bund.de*, werden diese in jeweils eigenen Zonen gespeichert. Die Informationen über eine Zone liest ein DNS-Server aus den Master Files ein.

DNS-Server werden nach ihren Aufgaben unterschieden, es gibt grundsätzlich zwei verschiedenen Typen:

- Advertising DNS-Server
- Resolving DNS-Server

Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen bezüglich eigener Domains aus dem Internet zu verarbeiten. Haben sie die gewünschten Domain-Informationen gespeichert, liefern sie die entsprechende Antwort. Andernfalls verweisen sie an einen anderen DNS-Server. Die Hauptaufgabe eines Advertising DNS-Servers ist es, seine gespeicherten Domain-Informationen zur Verfügung zu stellen.

Resolving DNS-Server hingegen verarbeiten üblicherweise Anfragen aus dem institutionsinternen Netz. Haben sie die gewünschten Domain-Informationen

gespeichert, liefern sie, ebenso wie Advertising DNS-Server, die entsprechende Antwort. Andernfalls verweisen Resolving DNS-Server jedoch nicht an einen anderen DNS-Server, sondern übernehmen die Namensauflösung selbst. Die Namensgebung "Resolving" deutet schon an, dass die Hauptaufgabe eines solchen DNS-Servers die Resolver-Funktionalität ist.

In allen Gefährdungen und Maßnahmen des Bausteins wird zwischen diesen beiden Funktionalitäten unterschieden. Der Begriff "DNS-Server" wird bei allgemeinen Erklärungen und Beschreibungen verwendet, die sowohl für Advertising als auch für Resolving DNS-Server gültig sind.

DNS-Server, die Anfragen mithilfe der eigenen Zoneninformationen beantworten können, werden als autoritativ bezeichnet. Erhält ein DNS-Server eine Anfrage, die nicht seine eigene(n) Zone(n) betreffen und zu denen er auch keine Informationen im Cache hat, kann ein DNS-Server auf drei Arten reagieren:

- Delegierung
  Delegierung bedeutet, dass ein Teil der Informationen über den Domain-Namensraum in eine Subdomain ausgelagert wurde. Wenn der DNS-Server beispielsweise eine Anfrage für *bund.de* erhält, wird der DNS-Server die Anfrage an den zuständigen DNS-Server weiterleiten. Da ein DNS-Server alle für die delegierten Zonen zuständigen DNS-Server kennen muss, kann er die Anfrage direkt an die zuständigen DNS-Server weiterleiten.
- Auflösung über Root-Nameserver
  Es gibt insgesamt 13 Root-DNS-Server. Diese Root-DNS-Server haben gespeichert, welche DNS-Server für die Top-Level-Domains autoritativ sind. Befinden sich die gewünschten Daten außerhalb der verwalteten Domain und sind auch keine Daten im Cache vorhanden, muss eine rekursive Auflösung, beginnend bei den Root-Nameservern, gestartet werden. Diese Verhaltensweise entspricht einem Resolving DNS-Server.
- Weiterleitung (Forwarding)
  Kann ein DNS-Server die gewünschten Informationen nicht liefern, leitet er die Anfrage an einen vorher konfigurierten DNS-Server weiter.

**Kommunikation**

Wie bereits beschrieben, kommunizieren Anwendungen über die Resolver-Schnittstelle mit DNS-Servern, unabhängig ob es sich dabei um einen Advertising oder Resolving DNS-Server handelt. Resolver senden stellvertretend für Anwendungen, die Namensauflösungen benötigen, Anfragen an DNS-Server und interpretieren die erhaltenen Antworten, um diese an die Anwendung zurück zu liefern. Grundsätzlich wird zwischen zwei Arten von Anfragen unterschieden:

- iterative Anfragen:
  Iterativ bedeutet, dass der befragte DNS-Server, sofern er die benötigten Daten nicht gespeichert hat, an den nächsten zuständigen DNS-Server verweist. Der befragte DNS-Server ist also ein Advertising DNS-Server. Der anfragende Resolver muss selbst die gesamte Namensauflösung durchführen. Eine Namensauflösung zu *www.bsi.bund.de* über die Root-DNS-Server (Root-DNS-Server beantworten nur iterative Anfragen und sind somit Advertising DNS-Server) würde wie folgt aussehen. Im ersten Schritt fragt der Resolver bei den Root-DNS-Servern nach dem Advertising DNS-Server, der für *de.* zuständig ist. Im zweiten Schritt wird durch den Resolver vom für *de.* zuständigen Advertising DNS-Server der DNS-Server ermittelt, der für *bund.de.* zuständig ist. Danach wird von diesem der Advertising DNS-Server für *bsi.bund.de.* erfragt. Schließ-

lich kann der Advertising DNS-Server für *bsi.bund.de.* die IP-Adresse zu *www.bsi.bund.de* an den Resolver liefern.

- rekursive Anfragen:
  Bei der rekursiven Anfrage funktioniert die Auflösung sehr ähnlich. Jedoch übernimmt der für den Resolver zuständige DNS-Server die komplette Namensauflösung, wie oben beschrieben. Es handelt sich also um einen Resolving DNS-Server. Der Resolver des Clients muss nur eine Anfrage stellen.

Ein Advertising DNS-Server akzeptiert nur iterative Anfragen, ein Resolving DNS-Server hingegen akzeptiert sowohl iterative als auch rekursive Anfragen. Rekursive Anfragen bedeuten im Vergleich zu iterativen Anfragen eine höhere Belastung für den DNS-Server.

**Zonentransfers**

Da DNS von sehr vielen Netzanwendungen benötigt wird, müssen laut Spezifikation (RFC 1034) mindestens zwei autoritative DNS-Server für jede Zone betrieben werden. Da es zu aufwendig ist, für jeden DNS-Server eigene Master Files zu verwalten, die konsistent sein müssen, wird eine Synchronisation über Zonentransfer durchgeführt. Der DNS-Server, der die Domain-Informationen direkt aus den Master Files bezieht, wird als Primary oder Master DNS-Server bezeichnet. Jeder weitere DNS-Server wird als Secondary oder Slave DNS-Server bezeichnet und bezieht die Daten über einen Zonentransfer vom Primary DNS-Server. Ein Secondary DNS-Server kontrolliert in regelmäßigen Abständen, ob sich die Domain-Informationen seiner Zone(n) geändert haben oder er wird von seinem Primary DNS-Server über Änderungen informiert. Ist dies der Fall, wird vom Secondary DNS-Server ein Zonentransfer initiiert, um seine Domain-Informationen auf den neusten Stand zu bringen.

**Caching-Only DNS-Server**

Der Caching-Only DNS-Server ist ein Spezialfall eines Resolving DNS-Servers. In der Regel ist ein DNS-Server, unabhängig davon ob es sich um einen Advertising oder Resolving DNS-Server handelt, für eine oder mehrere Zonen autoritativ. Das bedeutet, er hat die Domain-Informationen über diese Zonen aus den Master Files ausgelesen beziehungsweise von seinem Master DNS-Server über einen Zonentransfer erhalten. Caching-Only DNS-Server sind hingegen für keine Zone autoritativ, sie haben selbst keine Zonen gespeichert. Sie dienen in der Regel dazu, Anfragen entgegen zu nehmen und die Namensauflösung durchzuführen. Caching-Only DNS-Server werden oft als Forwarder für institutionsinterne Resolving DNS-Server eingesetzt, wenn diese Domain-Informationen aus dem Internet auflösen müssen.

**Sicherheitsaspekte**

Bezüglich DNS sind vor allem Integrität und Verfügbarkeit von großer Bedeutung. Jedoch wird auch der Vertraulichkeit eine immer wichtigere Rolle zugewiesen, wie in M 2.451 *Planung des DNS-Einsatzes* dargestellt. Angriffe auf DNS haben meist das Ziel Dienste zu manipulieren, die Namensauflösungen benötigen.

# M 2.451 Planung des DNS-Einsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Eine grundlegende Voraussetzung für den sicheren Einsatz von DNS-Servern ist eine angemessene Planung im Vorfeld. Hierzu muss zunächst ein Konzept erstellt werden, das unter anderem enthalten sollte, wie DNS aufgebaut werden soll und welche Domain-Informationen schützenswert sind. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können. Hinweise zum Aufbau und zur prinzipiellen Struktur von DNS bietet die Maßnahme M 2.450 *Einführung in DNS-Grundbegriffe*.

**Auswahl der Hardware**

Die Hardware, auf der ein DNS-Server betrieben werden soll, hat einen entscheidenden Einfluss auf die Gesamtleistung des entstehenden Systems. Dabei spielt es eine Rolle, wie viele Anfragen ein DNS-Server durchschnittlich bedienen muss, ob es sich um einen Resolving DNS-Server handelt, der rekursive Anfragen akzeptiert oder ob es sich um einen Advertising DNS-Server handelt, der nur iterative Anfragen akzeptiert und ob der Einsatz von DNSSEC (DNS Security Extensions) geplant ist.

Für DNS-Server ist ein ausreichender Hauptspeicherausbau wichtig, dadurch wird verhindert, dass der Server Speicherinhalte auf die Festplatte auslagern muss und somit die Antwortzeiten steigen. Wird DNSSEC eingesetzt, ist es wichtig darauf zu achten, dass die Prozessorgeschwindigkeit entsprechend erhöht wird, um einen angemessenen Durchsatz bei kryptografischen Operationen aufrecht zu erhalten. Die in der Planung ausgewählten Kapazitäten für Hauptspeicher und Prozessorgeschwindigkeit müssen im Betrieb überprüft werden, da die tatsächlich benötigten Kapazitäten erst im laufenden Betrieb genau ermittelt werden können.

**Sichtbarkeit der Domain-Informationen**

Ein DNS-Server verwaltet die Informationen für seine autoritativen Zonen. Einige davon sind für die Öffentlichkeit bestimmt, wie die IP-Adresse eines Webservers oder Mailservers. Ein Teil der Domain-Informationen betrifft aber die interne Struktur des Netzes der Institution. Diese Informationen können oft etwas über die Funktion oder den Standort der entsprechenden Netzkomponenten aussagen. Daher sollte die Sichtbarkeit dieser Domain-Informationen mithilfe der Unterscheidung zwischen Advertising und Resolving DNS-Servern eingeschränkt werden, wie nachfolgend im Abschnitt "separate DNS-Server beschrieben.

Der Namensraum eines Informationsverbundes sollte in einen öffentlichen und einen institutionsinternen Bereich aufgeteilt werden. Im öffentlichen Teil sollten nur solche Domain-Informationen (in der Regel IP-Adresse und Hostname) enthalten sein, damit Dienste, die von extern erreichbar sein sollen, reibungslos funktionieren. Dies sind üblicherweise:

- Webserver
- Mailserver
- DNS-Server
- VPN Verbindungspunkte

Innerhalb der Institution muss die Sichtbarkeit der Informationen meist nicht eingeschränkt werden. Welche Domain-Informationen nach außen hin sichtbar sind und welche nicht, muss bei der Planung des DNS-Einsatzes berücksichtigt werden.

**Separate DNS-Server**

DNS-Server können nach ihren Aufgaben unterschieden werden, dabei gibt es grundsätzlich zwei verschiedenen Typen:

- Advertising DNS-Server
- Resolving DNS-Server

Advertising DNS-Server sind üblicherweise dafür zuständig, Anfragen aus dem Internet zu verarbeiten. Resolving DNS-Server hingegen verarbeiten Anfragen aus dem internen Netz. Da dies zwei unterschiedliche Aufgaben sind, sollten diese auch unbedingt getrennt werden. Es empfiehlt sich daher für Advertising und für Resolving DNS-Server jeweils eigene physische Server einzusetzen. Der Advertising DNS-Server verwaltet die von Außen verfügbaren Domain-Informationen und unterstützt nur iterative Anfragen, der Resolving DNS-Server verwaltet die nach Innen sichtbaren Informationen und unterstützt sowohl iterative als auch rekursive Anfragen.

Ist der Aufwand für die Trennung in Advertising und Resolving DNS-Server zu groß, oder können aus technischen Gründen keine getrennten Server eingerichtet werden, so kann gegebenenfalls auf eine einfachere Konfiguration zurückgegriffen werden. Ein BIND-DNS-Server bietet beispielsweise die Möglichkeit, verschiedene Sichten ("Views") auf die Domain-Informationen zu definieren. In diesem Fall kann ein DNS-Server eine View für Anfragen aus dem internen Netz verwalten, in der alle Domain-Informationen des Informationsverbundes bereitgestellt werden. Dies ist der Resolving DNS-Server. Die zweite View für Anfragen mit Ursprung aus dem Internet enthält nur den Teil der Domain-Informationen, die bei der Klassifizierung als öffentlich eingestuft wurden. Dies ist der Advertising DNS-Server. Dieses Design bietet ein geringeres Sicherheitsniveau, als zwei getrennte DNS-Server, es muss im Einzelfall genau abgewogen werden, ob das höhere Risiko akzeptabel ist.

**Platzierung der DNS-Server im Netz**

Die Platzierung der DNS-Server ist abhängig von der Netzinfrastruktur der jeweiligen Organisation. Es gibt jedoch einige Grundregeln, die einzuhalten sind:

- Primary und Secondary DNS-Server sind in verschiedenen IP-Subnetzen zu platzieren. Des Weiteren dürfen sie nicht an dasselbe Netzkoppelelement angeschlossen werden. Somit wird durch Ausfall eines IP-Subnetzes oder eines Netzkoppelelements die Verfügbarkeit der Namensauflösung nicht beeinträchtigt, siehe auch G 1.2 *Ausfall von IT-Systemen*.
- Advertising DNS-Server sollten in der Demilitarisierten Zone (DMZ) platziert werden. Weitere Hinweise hierzu finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)*.
- Resolving DNS-Server sind für Anfragen von institutionsinternen IT-Systemen zuständig. Sie sollten daher innerhalb des vertrauenswürdigen Netzes der Institution so nahe wie möglich bei den anfragenden IT-Systemen platziert werden, um lange Antwortzeiten und unnötige Netzbelastung zu vermeiden. Darüber hinaus dürfen Resolving DNS-Server nicht von externen IT-Systemen erreichbar sein.

- Wird die Sichtbarkeit der Informationen eingeschränkt, sollte der öffentliche Teil der Domain-Informationen vom Advertising DNS-Server in der DMZ verwaltet werden.
- Wird für die internen Nameserver ein Forwarder für die Auflösung des Internet-Domainnamensraums verwendet, so sollte dieser nicht im internen Netz platziert werden.
- Werden Caching-Only DNS-Server im firmeninternen Netz eingesetzt, sollten die Resolver auf den Clients keine Domain-Informationen zwischenspeichern. Das Zwischenspeichern übernimmt der Caching-Only DNS-Server. Durch den zentralen Speicher wird die Anzahl der Anfragen minimiert. Des Weiteren kann im Falle eines erfolgreichen Cache-Poisoning Angriffs der zentrale Cache des Caching-Only DNS-Servers einfach gelöscht werden, um die gefälschten Daten zu entfernen.
- In Informationsverbünden werden heute standardmäßig Sicherheitsgateways eingesetzt. Um DNS-Netzverkehr zu akzeptieren, müssen auf den Sicherheitsgateways und Paketfiltern entsprechende Regeln eingerichtet werden, dargestellt in M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* oder in M 5.118 *Integration eines DNS-Servers in ein Sicherheitsgateway* . Bei der Planung sollte darauf geachtet werden, dass möglichst wenige Routen und Ports geöffnet werden müssen.

Eine beispielhafte Verteilung der DNS-Server im Zusammenspiel mit Sicherheitsgateways und Paketfiltern wird in M 5.118 *Integration eines DNS-Servers in ein Sicherheitsgateway* dargestellt.

**Resolver**

Resolver sind standardmäßig in den gängigen Betriebssystemen integriert und müssen daher nicht explizit ausgewählt und beschafft werden. Es sollte jedoch sicher gestellt werden, dass die Resolver der internen IT-Systeme die internen Resolving DNS-Server zur Namensauflösung verwenden. Sie sollten auf keinen Fall standardmäßig externe DNS-Server befragen. Zusätzlich sollten im Zuge dessen auch die DNS-Suffixe, die von den Resolvern verwendet werden, festgelegt werden, beispielsweise "bsi.bund.de". Dadurch wird bei der Namensauflösung von "hostx" automatisch der Rest des Domainnamens zum Fully Qualified Domain Name (FQDN) "hostx.bsi.bund.de." ergänzt.

**Verwaltung der Domainnamen**

Im Zuge der Planung muss festgelegt werden, wer für die Verwaltung der Internet-Domainnamen verantwortlich ist. Die verantwortliche Person muss für die Einhaltung der Maßnahmen sorgen, wie in M 2.298 *Verwaltung von Internet-Domainnamen* dargestellt.

Prüffragen:

- Werden für die Anfragen von institutionsinternen und institutionsexternen IT-Systemen separate DNS-Server verwendet?
- Wurde die Sichtbarkeit von Domain-Informationen eingeschränkt?
- Gibt es einen Plan für die Integration der DNS-Server in das Netz des Informationsverbundes?
- Verwenden die Resolver der internen Hosts die internen Resolving DNS-Server zur Namensauflösung?
- Gibt es einen Zuständigen für die Verwaltung der Internet-Domainnamen?
- Wurde für die nötigen Kapazitäten bezüglich der Hardware der DNS-Server gesorgt?

# M 2.452 Auswahl eines geeigneten DNS-Server-Produktes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bei der Beschaffung neuer DNS-Server-Produkte besteht die Möglichkeit, diese so auszuwählen, dass im späteren Betrieb nur geringe personelle, technische und organisatorische Aufwände nötig sind, um ein hohes Maß an Sicherheit zu erreichen. Zusätzlich bieten verschiedene DNS-Server-Produkte unterschiedliche Leistungsumfänge und unterschiedlichen Bedienkomfort. Bei der Beschaffung sollte auf folgende Aspekte geachtet werden.

- Das DNS-Server-Produkt sollte sich in der Praxis bereits bewährt haben.
- Falls für ein bestimmtes Produkt genügend geschultes Personal vorhanden ist und alle Anforderungen bezüglich der Funktionalität erfüllt sind, sollte dieses DNS-Server-Produkt verwendet werden.
- Es gibt DNS-Server-Produkte deren Implementierung von den Standards zu DNS (RFC 1034, 1035 etc.) abweicht. Ist insbesondere die Verwendung verschiedener DNS-Server-Produkte geplant, um Softwaremonokulturen zu vermeiden, sollte dies nur nach einer Kompatibilitätsprüfung gemacht werden.
- Für den Fall das DNSSEC eingesetzt wird, muss darauf geachtet werden, dass diese Technik vom DNS-Server-Produkt unterstützt wird.

**Syntaxprüfung der Zoneninformationen**

DNS-Server-Produkte unterstützen den Administrator unterschiedlich stark bei der Erstellung syntaktisch korrekter Zonendateien. Bei der Beschaffung des DNS-Server-Produktes sollte festgelegt werden, wie die Prüfung der Master Files durchzuführen ist. Werden die Master Files händisch editiert, kann eine toolgestützte Prüfung der Syntax der Zoneninformationen hilfreich sein. Dazu kann beispielsweise im Falle eines BIND DNS-Servers das Tool *named-checkzone* verwendet werden. Wird ein grafisches Frontend zum Editieren der Zoneninformationen benutzt, muss beispielsweise durch ein 4-Augen-Prinzip sicher gestellt werden, dass die eingegebenen Informationen in syntaktisch korrekte Zoneninformationen umgesetzt werden.

Prüffragen:

- Ist für das ausgewählte DNS-Server-Produkt genügend geschultes Personal vorhanden?
- Inwieweit unterstützt das DNS-Server-Produkt den Administrator bei der Erstellung syntaktisch korrekter Master Files?

# M 2.453 Aussonderung von DNS-Servern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wird entschieden, einen DNS-Server nicht weiter zu betreiben, weil beispielsweise die Domain aufgelöst wird, sind bei dessen Außerdienststellung einige Punkte zu beachten. Der Aussonderungsplan soll unter anderem verhindern, dass Verweise auf nicht mehr existierenden DNS-Server im Domain-Namensraum verbleiben.

### Löschen/Entsorgen der Speichermedien

Die Speichermedien aller betroffenen Rechner sind vor der Wiederverwendung sicher zu löschen (siehe M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*). Wird die Hardware entsorgt, so muss dies ebenfalls auf sichere Weise geschehen (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*).

### Löschen des DNS-Servers aus dem Domain-Namensraum

Wurde der DNS-Server nicht bei der übergeordneten Domain registriert, müssen keine weiteren Schritte unternommen werden. Ist der DNS-Server jedoch bei der übergeordneten Domain registriert, muss die Aussonderung den Administratoren der übergeordneten Domain bekannt gegeben werden, damit diese in der übergeordneten Domain alle Zoneneinträge der ausgesonderten DNS-Server löschen.

### System aus dem Netzverbund löschen

Alle Referenzen auf Netz- und Betriebssystemebene sind zu löschen. Ist der ausgesonderte Server als Standard DNS-Server bei internen Systemen der Institution eingetragen, müssen diese Einträge gelöscht werden. Zonentransfers, die zwischen dem ausgesonderten DNS-Server und noch existierenden DNS-Server konfiguriert sind, müssen ebenfalls gelöscht werden.

Prüffragen:

- Wurden die Festplatten des DNS-Servers sicher gelöscht?
- Wurde die Hardware des DNS-Servers ordnungsgemäß entsorgt?
- Wurde im Falle eines registrierten DNS-Servers die Registrierung gelöscht?
- Wurden sämtliche Konfigurationen auf den Clients, die auf den ausgesonderten DNS-Server verweisen, gelöscht?

# M 2.454 Planung des sicheren Einsatzes von Groupware-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bevor ein Groupware-System eingeführt wird, muss entschieden werden, für welche Einsatzzwecke das System genutzt werden soll und für welche Art von Informationen es vorgesehen ist. Von der Nutzungsart hängt ab, welche Hard- und Software beschafft werden muss, und sie bestimmt Art und den Umfang der notwendigen Planungen. Insbesondere hängen auch die festzulegenden Sicherheitsrichtlinien stark vom geplanten Einsatzszenario ab.

Generell kann grob zwischen den folgenden Einsatzvarianten von Groupware-Systemen unterschieden werden:

- Einsatz als Intranet-Server und Zugriff über Groupware-Clients: In diesem Szenario liegt das Hauptaugenmerk auf dem Einsatz als internem System zur Bürokommunikation (E-Mail, Terminvereinbarung, Koordination von Gruppenarbeit).
- Einsatz als Intranet-Server und Zugriff über Web-Clients: In diesem Szenario wird auf einen Groupware-Server über Browser zugegriffen. Da an der Web-Schnittstelle eines Groupware-Servers gänzlich andere Sicherheitsmechanismen genutzt werden, wird die sichere Konfiguration der Web-Schnittstelle als eigenes Szenario betrachtet.
- Einsatz in der DMZ (Demilitarisierte Zone) oder Perimeter-Netz: Ein Groupware-Server kann auch als öffentlich zugänglicher Informationsserver in einer DMZ eingesetzt werden. Diese Nutzungsart erfordert aufgrund der exponierten Stellung des Servers besondere Aufmerksamkeit bei der Systemkonfiguration.
- Nutzung von Groupware-Applikationen externer Dienstleister (z. B. Cloud Computing): Hierbei wird auf Groupware-Applikationen zugegriffen, die externe Dienstleister im Internet bereitstellen. Aus Sicherheitssicht ist hierbei besonders auf die Vertraulichkeit der Daten, die bei Dritten gespeichert werden, und auf die Verfügbarkeit der Dienstleistung zu achten.

Innerhalb dieser Einzelszenarien kann weiter dahingehend unterschieden werden, welche Funktionen von der eingesetzten Groupware genutzt werden sollen. Grundsätzlich gilt, dass für die Nutzung jeder Funktionalität eine eigene Planung erforderlich ist, bei der auch Sicherheitsaspekte zu berücksichtigen sind.

Abhängig davon, wofür Groupware-Systeme eingesetzt werden sollen, unterscheiden sich auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten.

Grundsätzlich müssen bei der Einsatzplanung von Groupware folgende Aspekte berücksichtigt werden:

- Es ist zu klären, welche Arten von Informationen über welche Wege über das Groupware-System kommuniziert werden soll und welchen Schutzbedarf diese Informationen und die damit zusammenhängenden Geschäftsprozesse haben.
- Es ist festzulegen, welche Groupware-Komponenten und -Dienste genutzt werden sollen, und welche Benutzer(-Rollen) mit welchen Berechtigungen diese benutzen sollen.
- Bei der Konzeption der Groupware-Nutzung muss auch festgelegt werden, welche kryptographischen Sicherungsmechanismen eingesetzt wer-

den sollen, vor allem für E-Mails (siehe dazu auch M 5.108 *Kryptographische Absicherung von Groupware bzw. E-Mail*).
- Um die Kommunikation in fremde Netze zu ermöglichen, muss der Einsatz exponierter Server geplant werden. Diese sollten in einer entmilitarisierten Zone oder zumindest hinter einem Sicherheitsgateway (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) platziert werden.

Bei der Planung sollte auch festgelegt werden, wie durch organisatorische Regelungen oder durch die technische Umsetzung ein ordnungsgemäßer Dateitransfer gewährleistet wird. Dazu gehören z. B. die folgenden Punkte:

- Die Groupware-Clients müssen durch die Administratoren so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Weitere Details zur Absicherung der E-Mail-Clients finden sich in M 5.57 *Sichere Konfiguration der Groupware-/Mail-Clients*.
- Die Übermittlung von Daten darf erst nach erfolgreicher Identifizierung und Authentisierung des Senders beim Übertragungssystem möglich sein.
- Die Benutzer müssen vor erstmaliger Nutzung von Groupware-Systemen in die relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zu Datenaustausch müssen ihnen bekannt sein.

Grundsätzlich sollten Nachrichten, die an interne Adressen verschickt wurden, nicht über externe Strecken oder an externe Adressen weitergeleitet werden. Sollen hiervon Ausnahmen gemacht werden, sind alle Mitarbeiter darüber zu informieren. Beispielsweise kann für Außendienstmitarbeiter oder andere Mitarbeiter, die viel unterwegs sind, die E-Mail an externe Zugriffspunkte weitergeleitet werden. Die Nutzung von Groupware-Anwendungen und vor allem die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Institution sollte über sichere Kanäle, z. B. ein VPN oder eigene Standleitungen, erfolgen.

Bei der Konzeption der sicheren Groupware-Nutzung sind außerdem folgende Punkte zu berücksichtigen:

- Die Behandlung aktiver Inhalte bei der Groupware-Kommunikation muss konsistent geplant werden. Dabei muss eine organisationsweit einheitliche Vorgehensweise festgelegt werden, nachdem die jeweiligen Vor- und Nachteile gegeneinander abgewogen wurden.
- Es muss entschieden werden, ob Abwesenheitsbenachrichtigungen ("Out-of-Office"-Nachrichten) verwendet werden dürfen, da bei der Verwendung dieser Funktionalität interne, personenbezogene Informationen nach außen gelangen können.
- Die Verwendung von E-Mail-Filtermechanismen zur Abwehr von Spam-Mail (unerwünschte Werbe-E-Mail) muss geplant werden.
- Für die Benutzung der Kalenderfunktion und der Aufgabenliste muss festgelegt werden, wer mit welchen Berechtigungen auf diese Funktionen zugreifen darf. Dies ist vor allem bei der Zusammenarbeit mit anderen Organisationseinheiten oder Externen wichtig.
- In der Planung ist zu berücksichtigen, wenn Benutzer gemeinsame Rechner verwenden. Entsprechend sind Profile auf diesen Rechnern anzulegen und abzusichern.
- Sollen Chat-, Instant Messaging-, Audio- oder Videokonferenz-Dienste in der Institution genutzt werden, so muss deren Einsatz konzipiert werden.

Wenn für den Groupware-Einsatz externe Dienstleister genutzt werden sollen, z. B. Mailprovider, sind hierfür die im Baustein B 1.11 *Outsourcing* beschriebenen Sicherheitsempfehlungen umzusetzen. Vor allem ist zu klären, welche

Sicherheitsmaßnahmen durch den Dienstleister ergriffen werden (siehe auch M 2.123 *Auswahl eines Groupware- oder Mailproviders*).

Es wird immer wieder diskutiert, ob und inwieweit dienstliche Groupware-Anwendungen, vor allem E-Mail, für private Zwecke benutzt werden dürfen. Solange die private Nutzung sich in Grenzen hält, wird dies sogar von vielen Institutionen unterstützt, da sich dies positiv auf die Mitarbeiter-Motivation auswirkt. Generell empfiehlt es sich aber, hierzu in der Groupware-Richtlinie zu vereinbaren, welche Spielregeln bei der Groupware-Nutzung allgemein und auch hinsichtlich privater Nutzung von E-Mail und anderen Groupware-Diensten einzuhalten sind.

Bei der Nutzung von Groupware-Systemen in Institutionen sollte auch festgelegt werden, welche Groupware-Anwendungen die Benutzer einsetzen dürfen. Neben den verschiedenen Diensten, die die im Haus eingesetzten Groupware-Systeme bieten, kann auch auf andere, über die Arbeitsplatzrechner nutzbare Groupware-Anwendungen zugegriffen werden, wie z. B. Webmail oder Internet-Terminalkalender. Es muss klar geregelt sein, welche internen oder externen Groupware-Anwendungen die Mitarbeiter nutzen dürfen. Wie dies aussehen kann, ist im Folgenden am Beispiel Webmail beschrieben. Grundsätzlich gilt immer, dass Mitarbeiter nur von ihrer Institution freigegebene Programme und externe Dienstleistungen benutzen dürfen.

Als Webmail werden Angebote bezeichnet, bei denen über einen Browser auf webbasierte E-Mail-Dienste zugegriffen wird. Verschiedene Mailprovider bieten entsprechende Erweiterungen entweder direkt in ihr Produkt integriert oder als Zusatzmodule an. Webmail hat den Vorteil, dass hierbei von jedem Rechner mit Internet-Anschluss weltweit auf die E-Mail-Postfächer zugegriffen werden kann, ohne dass hierfür in aufwendige Infrastruktur investiert werden muss. Es ist allerdings schwieriger als beim Transport über die internen E-Mail-Server, die organisationsweit gültigen Sicherheitsrichtlinien durchzusetzen, beispielsweise im Hinblick auf Virenschutz oder Verschlüsselung. Außerdem ist die Gefahr, dass vertrauliche E-Mails mitgelesen oder Passwörter abgehört werden, beim externen Zugriff auf Webmailzugänge wesentlich höher.

Bei der Nutzung von Webmail aus einem Behörden- bzw. Unternehmensnetz heraus muss unbedingt der Schutz vor Schadsoftware beachtet werden. Bei aktuellen Virenwarnungen kann es einige Zeit in Anspruch nehmen, die neuen Virenschutz-Updates auf alle Clients aufzuspielen. In einer solchen Situation kann es sinnvoll sein, den Zugriff auf Webmail zumindest solange zu verhindern, bis die Verantwortlichen sicher sind, dass ein ausreichender Schutz besteht.

Der Umgang mit Webmail in der Behörde bzw. dem Unternehmen sollte geregelt sein. Hierbei gibt es mehrere Varianten:

- Institutionen können beschließen, die Nutzung von Webmail generell zu verbieten. Dies muss dann natürlich den Mitarbeitern bekannt gegeben werden. Das Verbot kann außerdem technisch durch Filterung bezüglich der bekannten Anbieter unterstützt werden, wobei man sich hier darüber klar sein sollte, dass Benutzer immer neue Wege finden können, um auf solche Dienste zuzugreifen.
- Es kann die Empfehlung ausgesprochen werden, Webmail für private E-Mails, die aus dem internen LAN verschickt werden sollen, zu nutzen. Damit kann vermieden werden, dass Mitarbeiter trotz entsprechender Verbote dienstliche E-Mail-Zugänge für private Zwecke nutzen - beispielsweise, weil es dringend oder einfach praktisch ist.

- Es gibt auch Institutionen, in denen Webmail offiziell für dienstliche E-Mails freigegeben ist. Die Gründe hierfür sind unterschiedlich. So gibt es z. B. eine Reihe kleinerer Institutionen, die keinen eigenen E-Mail-Server haben und Webmail für Kommunikation nach außen einsetzen. Webmail kann auch für Mitarbeiter praktisch sein, die auf Dienstreisen auf ihre E-Mail zugreifen müssen, für die aber kein Zugang über Remote Access eingerichtet ist. Ein weiterer Grund für die Nutzung von Webmail kann darin bestehen, dass die jeweilige Institution bei bestimmten E-Mails nicht nach außen in Erscheinung treten will oder dass Webmail-Adressen dort angegeben werden, wo Spam erwartet wird, also bei bestimmten Downloads, Newsgruppen etc.

Wenn Webmail eingesetzt wird, sollten die Empfehlungen in M 5.96 *Sichere Nutzung von Webmail* beachtet werden.

Prüffragen:

- Liegen Eckpunkte für den sicheren Einsatz von Groupware-Systemen vor?
- Wurde festgelegt, welche Arten von Informationen im Hinblick auf den Schutzbedarf unter welchen Rahmenbedingungen über Groupware-Dienste übertragen werden dürfen?
- Ist die private Nutzung von Groupware-Diensten geregelt?
- Ist der Umgang mit Webmail geregelt?

# M 2.455 Festlegung einer Sicherheitsrichtlinie für Groupware

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Wie für jedes in einer Behörde oder einem Unternehmen eingesetzte Client-Server-System muss auch für den Einsatz von Groupware-Servern und -Clients eine geeignete Sicherheitsrichtlinie festgelegt werden, in der die Regelungen beschrieben sind, die von den Groupware-Administratoren und den Groupware-Benutzern zu beachten sind.

- Die Sicherheitsrichtlinie für Groupware-Systeme muss konform zu den geltenden generellen Sicherheitsrichtlinien des Unternehmens bzw. der Behörde sein.
- Es muss festgelegt werden, wann eine Kommunikationsabsicherung, z. B. für Netz- oder E-Mail-Kommunikation, vorgenommen werden muss (z. B. beim Zugriff über das Internet). Dabei ist auch festzulegen, welche Mechanismen dafür genutzt werden sollen.
- Die Sicherheitsrichtlinie muss an alle mittel- und unmittelbar betroffenen Personen der Institution verteilt werden. Am Besten sollte sie im Rahmen einer internen Schulung vorgestellt werden. Die Sicherheitsrichtlinie muss regelmäßig aktualisiert werden. Änderungen müssen in geeigneter Weise den betroffenen Personen mitgeteilt werden.

Es ist sinnvoll, die Groupware-Sicherheitsrichtlinie in einen Teil für Benutzer und einen Teil für Administratoren zu trennen, um sie verständlicher gestalten zu können. In der Sicherheitsrichtlinie für Groupware für Benutzer ist beispielsweise festzulegen,

- welche Benutzer auf welche Groupware-Server zugreifen dürfen und welche Benutzer auf welche Groupware-Server nicht zugreifen sollen (Ausschlussliste),
- welche Benutzer mit welchen Rechten auf welche Groupware-Datenbanken zugreifen dürfen,
- welche Informationen an welche Kommunikationspartner weitergegeben werden dürfen,
- wie die übermittelten Informationen (in Abhängigkeit von ihrem Schutzbedarf) abzusichern sind, vor allem sollte geregelt sein, wann übertragene Dateien verschlüsselt bzw. digital signiert werden müssen.

Die Groupware-Sicherheitsrichtlinie für Administratoren sollte unter anderem umfassen,

- wie die Groupware-Komponenten durch die Administratoren zu konfigurieren sind, um angemessene Sicherheit zu ermöglichen,
- welche anderen Server auf einen Groupware-Server zugreifen dürfen und
- von wo aus auf einen Groupware-Server zugegriffen werden darf.

In der Groupware-Sicherheitsrichtlinie wäre beispielsweise beim Einsatz von Microsoft Exchange festzulegen, welche Benutzer mit welchen Rechten auf welche Exchange-Objekte zugreifen dürfen. Da sich Microsoft Exchange-Systeme sehr stark in die Windows-Umgebung integrieren, speziell in das Active Directory, muss die Windows-Sicherheitsrichtlinie berücksichtigt werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie zu Groupware-Systemen?

- Werden alle Benutzer über neue oder veränderte Sicherheitsvorgaben zu Groupware-Systemen informiert?

# M 2.456 Sichere Administration von Groupware-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Administration von Groupware-Systemen erfordert eine sorgfältige Planung. Dabei sollte auf eine ausreichende Trennung der administrativen Aufgaben und der zugehörigen Administratorkonten geachtet werden. Die im Folgenden beschriebenen sicherheitsrelevanten Aspekte sollten bei der Administration von Groupware-Systemen berücksichtigt werden.

**Ernennung von Administratoren**

Zum reibungslosen Ablauf eines Groupware-Systems müssen Administratoren ernannt und geschult werden. Administratoren für E-Maildienstes werden auch Postmaster genannt. Zu ihren Aufgaben gehören:

- Bereitstellen der Groupware-Dienste auf lokaler Ebene,
- Absicherung der Groupware-Systeme vor missbräuchlicher Nutzung,
- Überprüfung, ob die externen Kommunikationsverbindungen funktionieren,
- Anlaufstelle bei Groupware-Problemen für Endbenutzer sowie für die Betreiber von Gateway- und Relaydiensten.

Für die Wahrnehmung dieser Aufgaben sind die Postfächer *postmaster@<domain>* und *abuse@<domain>* einzurichten. Diese Postfächer müssen auch für alle am E-Mail-Verkehr teilnehmenden Subdomains eingerichtet werden.

Alle Fehlermeldungen können an die Administratoren über die Adresse *postmaster@<domain>* weitergeleitet werden, die versuchen sollten, die Fehlerquellen zu beheben. Die Administratoren sollten auch proaktiv in den Protokollen der betreuten IT-Komponenten prüfen, ob Fehler auftauchen und diese beseitigen.

Missbrauch von E-Mail-Diensten wird den Administratoren typischerweise über das Postfach *abuse@<domain>* mitgeteilt. Laufen in diesem Postfach Beschwerden von externen Mailteilnehmern ein, z. B. Beschwerden über Spamversand aus dem eigenen Netz, müssen die Administratoren zeitnah diese Beschwerden prüfen und die Gründe dafür beseitigen. Andernfalls riskiert sie, dass der E-Mail-Dienst in der Funktionalität einschränkt wird, beispielsweise weil er auf Blacklists gesetzt wird.

Daneben müssen je nach Organisationsstruktur und -größe ein oder mehrere Verantwortliche für die Pflege der angebotenen Kommunikationsdienste benannt werden. Neben dem Serverbetrieb müssen auch die von den Benutzer eingesetzten Kommunikationsclients betreut werden. Alle Betreuer bzw. deren Vertreter sollten jederzeit von den Benutzern telefonisch und per E-Mail erreicht werden können.

**Berechtigungen**

Bei der Rechtevergabe sollten folgende Grundsätze beachtet werden (siehe auch M 4.355 *Berechtigungsverwaltung für Groupware-Systeme*):

- Es sollte klare Berechtigungsstrukturen geben. Alle administrativen Aufgabenbereiche und Berechtigungen sollten ausreichend dokumentiert werden.

- Der administrative Zugang zu Groupware-Systemen sollte aufgrund der weitreichenden Berechtigungen besonders geschützt werden. Es sollten nur die unbedingt notwendigen Rechte vergeben werden, die zur Ausübung der administrativen Tätigkeiten erforderlich sind.
- Die administrativen Aufgaben sollten sorgfältig aufgeteilt und nachvollziehbar den zuständigen Personen zugewiesen werden. Es sollte überprüft werden, ob die Aufgabenteilung durch die Ausnutzung vorhandener Administratorrollen im Groupware-System unterstützt werden kann.
- Standardmäßig ist im Allgemeinen bei der Erstinstallation eines Groupware-Systems ein übergreifender Administrator angelegt, der auf alle Groupware-Komponenten und alle Datenbank-Objekte volle Zugriffsrechte besitzt. Dies sollte bei der Erstinstallation geändert werden. Die Verteilung der Zugriffsrechte sollte gemäß dem zuvor festzulegenden administrativen Modell erfolgen.

**Ausreichende Dimensionierung eines Groupware-Systems**

Groupware-Servern muss ausreichend Speicherplatz und -leistung zur Verfügung gestellt werden. Drei der wichtigsten zu berücksichtigenden Faktoren sind die Wahl des Prozessors, die Größe des Arbeitsspeichers und die Auswahl der Speicherlösung. Es sollte regelmäßig überprüft werden, ob das Groupware-System noch ausreichend dimensioniert ist.

**Nutzung der Groupware-Dokumentation**

Softwarehersteller stellen in der Regel eine Vielzahl von Dokumenten und Informationen zur Verfügung, vieles davon als Online-Dokumentation. Die sicherheitsrelevante Dokumentation muss insbesondere Administratoren bekannt und zugänglich sein. Es sollte, vor allem bei Online-Dokumentation, regelmäßig geprüft werden, ob es neue Versionen und neue Sicherheitshinweise gibt.

**Sichere Konfiguration von Groupware-Servern**

Nach der Installation der eingesetzten Groupware-Lösung muss die Software sowohl der Server- als auch der Client-Komponenten sicher konfiguriert werden. Bevor ein Administrator nach der erfolgreichen Installation der Groupware mit der Konfiguration fortfährt, sollten allgemeine Empfehlungen zur Administration umgesetzt werden. Bei der eigentlichen Konfiguration der Groupware ist dann vor allem auf folgendes zu achten:

- Einschränkung der Zugriffsberechtigungen auf das notwendige Maß,
- sichere Konfiguration der Groupware-Schnittstellen und anderer Komponenten,
- sichere Konfiguration der Kommunikationsprotokolle und Einrichtung einer angemessenen Protokollierung.

**Sichere Konfiguration von Groupware-Clients**

Nach der Installation bzw. Verteilung von Groupware-Clients innerhalb einer Institution muss die Client-Software entsprechend konfiguriert werden, um einen sicheren Betrieb der Groupware-Umgebung zu gewährleisten. Als Grundlage ist hier die Maßnahme M 5.57 *Sichere Konfiguration der Groupware-/Mail-Clients* umzusetzen.

**Sichere Konfiguration der Datenbank in Groupware-Systemen**

Groupware-Systeme nutzen typischerweise eine Datenbank, um alle wesentlichen Informationen persistent zu speichern. Die Kommunikation zwischen Groupware-System und Datenbank erfolgt über Anfragen, die über das lokale

Netz übertragen werden, sofern Datenbank und die Groupware-Systemkomponenten nicht auf demselben Rechner installiert werden. Daher muss der Zugriff auf die Datenbank möglichst gut geschützt werden. Diese Datenbank ist eine kritische Komponente, die vor unberechtigtem Zugriff unbedingt geschützt werden muss. Sie muss sicher installiert und betrieben werden, dafür sind die spezifischen Empfehlungen aus Baustein B 5.7 *Datenbanken* umzusetzen.

Prüffragen:

- Sind die Administrationsaufgaben und die vergebenen Berechtigungen ausreichend dokumentiert?
- Wurden die Groupware-Komponenten nach der Installation sicher konfiguriert?

# M 2.457 Konzeption für die sichere Internet-Nutzung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Nahezu jede Institution nutzt heute das Internet. Neben den vielen Vorteilen des Internet gibt es permanent neue Meldungen über Risiken, denen Anwender bei der Internet-Nutzung ausgesetzt sind. Um diese zu minimieren, sollte jede neue Variante der Internet-Nutzung sorgfältig geplant werden sowie alle IT-Komponenten und ihre Vernetzung sicher installiert und konfiguriert werden.

In einer Konzeption für die sichere Internet-Nutzung muss zunächst geklärt werden, wer welche Internet-Dienste nutzen darf, welche Regelungen dabei zu beachten sind und wie die internen IT-Systeme zu schützen sind. Die Konzeption muss in die allgemeine Sicherheitsstrategie der jeweiligen Institution eingebettet sein und daher mit dem Informationssicherheitsmanagement abgestimmt werden.

**Planung**

Es muss festgelegt werden, welche Arten von Internet-Kommunikation zugelassen werden (siehe auch M 2.459 *Überblick über Internet-Dienste*). Dazu muss geklärt werden, welche Ziele mit der Internet-Nutzung erreicht werden sollen. Es muss eine geeignete und den Bedürfnissen der Institution entsprechende Auswahl von Internet-Diensten getroffen werden. Dies kann von dem Extrem, dass nur ausgewählte Mitarbeiter Internet-Zugang haben und dieser restriktiv gehandhabt wird, bis zu dem anderen Extrem, dass von jedem Arbeitsplatz aus Internet-Anwendungen aller Art genutzt werden können, reichen. Der Aspekt der Sicherheit muss bereits sehr früh in der Planungsphase berücksichtigt werden, um die entstehende Architektur entsprechend sicher auslegen zu können.

Wird für bestimmte Bereiche keine oder nur eine eingeschränkte Internet-Nutzung zugelassen, so kann es sinnvoll sein, für den Internet-Zugang in diesen Bereichen eigenständige Internet-PCs bereitzustellen (siehe Baustein B 3.208 *Internet-PC*).

In der Sicherheitskonzeption für die Internet-Nutzung sollten die folgenden Fragen beantwortet werden:

- Wer erhält Internet-Zugang?
- Unter welchen Bedingungen bzw. zu welchen Zwecken darf auf das Internet zugegriffen werden?
- Welche Dienste dürfen im Internet benutzt werden?
- Welche Informationen dürfen oder dürfen nicht im Internet weitergegeben werden?
- Sind Benutzerschulungen erforderlich und falls ja, wie werden sie durchgeführt?
- Wie wird technische Hilfestellung für die Benutzer gewährleistet?

Die Nutzung der einzelnen Internet-Dienste sollte geregelt und für jede Gruppe von Benutzern und/oder IT-Systeme geklärt werden, welche Sicherheitsbedingungen zu beachten sind. Dabei sollten nur die Dienste zugelassen werden, die zur Erfüllung der Aufgaben unbedingt notwendig sind. Dienste, für die noch keine expliziten Regeln festgelegt wurden, dürfen nicht eingesetzt

werden, ehe entweder neue Regeln festgelegt oder bestehende Regelungen angepasst wurden. Dazu gehören beispielsweise das Sicherheitskonzept und auch die Benutzerrichtlinien. Weiterhin muss die private Internet-Nutzung geklärt werden.

Die Entscheidungen, die zur Nutzung der verschiedenen Internet-Dienste getroffen wurden, sollten, ebenso wie die Gründe für diese Entscheidungen, nachvollziehbar dokumentiert werden.

**Aktualität**

Die Konzeption für die Internet-Nutzung muss regelmäßig aktualisiert werden, mindestens einmal jährlich, da sich dieser Bereich sehr dynamisch entwickelt. Auch sollte die Entwicklung und Aktualisierung der Konzeption zur Internet-Nutzung Hand in Hand mit der Konzeption der Internet-Anbindung erfolgen, um eine sichere Anbindung an das Internet und damit auch eine sichere Nutzung des Internets zu gewährleisten.

Bei Änderungen in den Zielen, der Strategien oder der Gefährdungslage der Institution muss geprüft werden, welche Auswirkungen diese auf die Internet-Nutzung haben.

Prüffragen:

- Ist eine aktuelle Konzeption für die Internet-Nutzung vorhanden?
- Wird die Konzeption regelmäßig überprüft und falls erforderlich angepasst?

# M 2.458 Richtlinie für die Internet-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Für die Internet-Nutzung in Behörden oder Unternehmen muss eine verbindliche Richtlinie festgelegt werden. Die Rechte und Pflichten aller Mitarbeiter bei der Internet-Nutzung müssen darin klar geregelt sein. Unter Umständen gibt es weitere Richtlinien für bestimmte Internet-Dienste (z. B. E-Mail), die natürlich auch zu beachten sind. Jedem Mitarbeiter müssen diese Richtlinien bekannt gegeben und auch regelmäßig in Erinnerung gerufen werden.

Dazu ist es sinnvoll, die Richtlinie für die Internet-Nutzung, wie auch andere Richtlinien, im Intranet abrufbar zu halten. Ein Beispiel für eine Sicherheitsrichtlinie für die Internet-Nutzung findet sich auf den BSI-Webseiten unter den Hilfsmittel zum IT-Grundschutz. In einer Richtlinie für die Internet-Nutzung sollten mindestens folgende Aspekte berücksichtigt werden:

- Die Benutzer sollen in kurzer, verständlicher Form über die Risiken informiert werden, die mit der Internet-Nutzung verbunden sind.
- Die Benutzer müssen die erforderlichen Kenntnisse zur verantwortungsbewussten Internet-Nutzung haben. Sie sollten wissen, wie Browser und typische Internet-Dienste korrekt zu nutzen sind, um Fehlbedienungen und unsicheres Verhalten zu vermeiden. Sie sollten natürlich auch die organisationsinternen Richtlinien kennen. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden (siehe dazu auch M 3.77 *Sensibilisierung zur sicheren Internet-Nutzung*).
- In der Richtlinie sollte festgelegt werden, unter welchen Rahmenbedingungen Internet-Dienste benutzt werden dürfen. Als Beispiel könnte darin also geregelt sein, dass ein Übersetzungsdienst im Internet für öffentlich zugängliche Dokumente genutzt werden darf, nicht aber für vertrauliche Informationen. In diesem Zusammenhang ist auch festzulegen, ob Internet-Dienste ausschließlich dienstlich oder ebenfalls privat genutzt werden dürfen, z. B. in der Mittagspause.
- Zusätzlich ist festzulegen, welche Anwendungen für den Zugriff auf Internet-Dienste genutzt werden dürfen. Es sollte geregelt sein, dass Benutzer für die Nutzung von Internet-Diensten keine nicht freigegebene Software installieren dürfen. Dazu gehören auch Browser-Erweiterungen ("Plug-Ins"). Die Browser der Benutzer müssen durch die Administratoren so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann (siehe auch M 5.45 *Sichere Nutzung von Browsern* ).

Informationen, die vertraulich sind oder die Institution in einem falschen Licht erscheinen lassen können, dürfen nicht über ungeschützte Internet-Dienste weitergegeben werden. Sie dürfen also weder auf Webserver eingestellt werden, noch über Mailinglisten verbreitet werden. Umgekehrt sind Benutzer auch darauf hinzuweisen, dass sie solche Informationen nicht unberechtigt herunterladen dürfen oder sich anderweitig aktiv besorgen dürfen. Beispielsweise dürfen also keine Dateien, deren Inhalt Anstoß erregen könnte, auf Webservern nachgefragt werden. Es muss festgelegt werden, welche Inhalte als anstößig gelten. In der Richtlinie muss auch vorgegeben werden, wie mit aus dem Internet beschafften Informationen zu verfahren ist. Mitarbeiter müssen darauf hingewiesen, dass bei der Weiterverwendung fremder Informationen

Urheberrechte und Nutzungsbedingungen zu beachten sind. Nicht alle Quellen sind außerdem vertrauenswürdig. Abgesehen davon, dass Daten aus nicht vertrauenswürdigen Quellen Schadsoftware enthalten könnten, können auch Falschinformationen bei ungeprüfter Verwendung Schaden anrichten. Auch gut aufbereitete Webseiten können Falschinformationen enthalten. In diesem Zusammenhang muss ebenfalls geregelt werden, unter welchen Bedingungen Daten aus dem Hausnetz über das Internet transportiert werden dürfen.

Es sind daher Kriterien zu formulieren, die es Mitarbeitern erleichtern, abzuleiten welche Informationen im Internet weitergegeben werden dürfen und welche nicht. Dazu gehören auch Regelungen, ob und wie die Daten bei der Übertragung und bei der Verarbeitung geschützt werden müssen.

Alle Mitarbeiter sollten wissen, welche Internet-Angebote und -Dienste sie benutzen dürfen, wie sie diese sicher und vertrauenswürdig benutzen können und welche Verhaltensweisen dabei empfehlenswert sind (siehe auch M 3.78 *Korrektes Auftreten im Internet*).

Für die Nutzung von Internet-Angeboten ist oftmals eine Anmeldung notwendig, bei der Benutzername, E-Mail-Adresse und teilweise auch weitere Informationen, die einen Rückschluss auf die Person und die Institution geben könnten, angegeben werden müssen. Es ist zu klären, ob Verweise auf die Institution unerwünscht sind und daher z. B. keine dienstlichen E-Mail-Adressen für die Nutzung von Internet-Diensten verwendet werden dürfen. Insgesamt ist zu regeln, welche persönlichen Daten und welche Informationen über die Institution weitergegeben werden dürfen, um beispielsweise keine Werbeaktionen auszulösen oder Informationen für ein erfolgreiches Social Engineering herauszugeben (siehe auch M 2.313 *Sichere Anmeldung bei Internet-Diensten*).

Weiterhin müssen die Benutzer darauf hingewiesen werden,

- welche Daten protokolliert werden,
- wer die Ansprechpartner bei Sicherheitsproblemen sind und
- dass die Konfiguration der Browser und anderer Programme nicht eigenmächtig geändert werden darf.

Je nach Anwendungsfall und Einsatzumgebung müssen unter Umständen weitere Aspekte geregelt werden.

In der Internet-Sicherheitsrichtlinie sollten die zur Verfügung stehenden Kommunikationsdienste kurz erläutert und alle relevanten Regelungen aufgeführt werden. Gesetzliche Vorgaben, insbesondere zum Datenschutz, müssen dabei selbstverständlich beachtet werden. Der Datenschutzbeauftragte und die Personalvertretung sollten frühzeitig beteiligt werden.

Es kann unter Umständen sinnvoll sein, die Benutzer durch Unterschrift bestätigen zu lassen, dass die Regelungen für die Internet-Nutzung zur Kenntnis genommen wurden und bei Benutzung der Kommunikationsdienste beachtet werden.

Prüffragen:

- Existiert eine Sicherheitsrichtlinie für die Internet-Nutzung?
- Ist die Richtlinie für die sichere Internet-Nutzung allen Mitarbeitern bekannt gemacht worden?

# M 2.459 Überblick über Internet-Dienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT

Das Internet ist ein weltumspannendes Computernetz, das eine Infrastruktur zur Verfügung stellt, mit der verschiedene Dienste angeboten und genutzt werden können. Zwei der wichtigsten und ältesten Dienste sind das World Wide Web und E-Mail. Daneben gibt es viele weitere Dienste. Zu den wichtigsten und bekanntesten Internetdiensten gehören:

**World Wide Web (WWW)**

Das WWW wurde als Hypertext-System entwickelt, in dem verteilte Informationen miteinander vernetzt sind. Für den Zugriff auf die Informationen können Webbrowser genutzt werden. Mit Hilfe von Links ist es möglich, sich von Begriff zu Begriff oder von Dokument zu Dokument zu bewegen. Das WWW bietet weltweit Informationen unterschiedlicher Art wie beispielsweise Texte, Bilder, Grafiken, Applikationen, Spiele, Klänge und Videos an. Neben der zeitsparenden Informationsgewinnung können sich Privatnutzer und Institutionen im WWW darstellen, eigene Publikationen veröffentlichen sowie Dienstleistungen anbieten. Doch muss immer damit gerechnet werden, dass sich unter den Informationen auch Falschmeldungen befinden. Zusätzlich besteht die Gefahr, dass über die Webseiten Schadprogramme verteilt werden, die beispielsweise sensible Daten abfangen oder fälschen.

**E-Mail**

Per E-Mail können elektronische Nachrichten weltweit von einem Sender an eine Vielzahl von Empfängern übermittelt werden. Unverschlüsselte und unsignierte E-Mails müssen dabei mit einer Postkarte verglichen werden, da ihr Inhalt offen und relativ einfach änderbar versendet wird. E-Mail ist einer der viel genutzten Wege, um Schadsoftware zu verbreiten.

**Diskussionsforum / Internetforum**

Ein Internetforum beschäftigt sich zumeist mit einem bestimmten Themenbereich, zu dem Diskussionsbeiträge hinterlassen werden können, die dann von anderen Interessierten gelesen, beantwortet oder kommentiert werden. Viele Internetforen lassen eine Teilnahme erst nach einer vorherigen Anmeldung bzw. Registrierung zu. Das Verhalten in einem Forum wird durch die Forumsnetiquette, den von den Forumsbetreibern festgelegten Verhaltensregeln, bestimmt. Benutzer, die sich nicht an die Forumsregeln halten, können von den Administratoren des Forums ausgeschlossen werden. Die Beiträge in Internetforen können meistens noch lange Zeit nachgelesen werden. Diskussionsforen können unter anderem dadurch missbraucht werden, indem dort bewusste Falschmeldungen oder schmähende Beiträge veröffentlicht werden. Die Möglichkeit, in den Beiträgen auch Links zu hinterlegen, um z. B. auf zusätzliche Informationen hinzuweisen, wird oft auch genutzt, um auf Webseiten mit Schadsoftware zu verweisen.

**Newsserver / Netnews**

Über Newsserver können Nachrichten, die sogenannten Netnews, ausgetauscht und abgerufen werden. In Newsgruppen können Gleichgesinnte weltweit miteinander kommunizieren. Je nach Intention werden Informationen zu bestimmten Themen oder Hilfe zur Problemlösung gesucht. Mit Hilfe der

Newsgruppen werden die Themen gegliedert und erhalten eine systematische Struktur mit Anfrage und Antworten.

News werden üblicherweise abonniert, die Abonnenten jedoch von keiner Stelle verifiziert oder zugelassen, so dass jeder, auch anonym oder mit falscher Identität teilnehmen kann. News können zum Lesen lokal gespeichert oder von einem Newsserver abgerufen werden. Die lokale Speicherung benötigt je nach Themenbereich und aufgefundenen News sehr viel Speicherplatz, lässt aber auch schnelleres Arbeiten und vor allem eine Volltextsuche zu.

**Chat**

Als Chatten wird der synchrone Austausch von zwei bis mehreren Kommunikationspartnern in Echtzeit über das Internet bezeichnet. Verbreitete Internet-Varianten sind Internet Relay Chat (IRC), Webchat und Instant Messaging. Chats werden häufig in öffentlichen, sogenannten Chaträumen (Chatrooms) eines Chatbetreibers durchgeführt. Für viele Chats ist eine vorherige Registrierung notwendig, es können jedoch von den Benutzern meistens frei gewählte Identitäten angenommen werden. Aus diesem Grund gibt es Chats, in denen nur ein bestimmter Teilnehmerkreis zugelassen ist, ohne vorherige Registrierung oder Freischaltung durch einen Administrator ist die Teilnahme nicht möglich. Zusätzlich ist es möglich die Chat-URL nur einem bestimmten Benutzerkreis bekannt zugeben oder Privaträume in einem Chat einzurichten, um den Missbrauch durch Unbefugte einzuschränken. Zusätzlich kann ein Administrator die Beiträge überwachen, Benutzer verwarnen und vom Chat ausschließen. Die Beiträge können in der Gesamtheit als Protokoll gesichert werden.

**Blog/Weblog**

Ein Blog ist ein auf einer Webseite geführtes Tagebuch, dass einer beschränkten Leserschaft oder öffentlich zugänglich ist. Der Begriff Weblog oder kurz Blog leitet sich ab aus den Begriffen World Wide Web und Log für Logbuch. Privatpersonen oder Personen mit institutionellem Auftrag berichten darin über ihr Erlebnisse in ihrem Leben oder Aspekte eines speziellen Themas. Je nach den vom Blogverantwortlichen gewählten Einstellungen kann jeder einzelne Eintrag von Lesern kommentiert und diskutiert werden.

Blog-Einträge können unter Umständen stark verbreitet werden und lange archiviert werden. Da sie Meinungen widerspiegeln, sollte rechtzeitig bedacht werden, ob diese auch für die Öffentlichkeit gedacht sind. Sollen Blogs für eine Institution eingesetzt werden, sollte ein Verantwortlicher abgestimmte Inhalte einstellen und regelmäßig pflegen. Da Kommentare und Mitteilungen nicht nur positiver Natur sein können, die Löschung negativer Bemerkungen aber als Manipulation gesehen werden kann, ist zu überlegen, wie mit der Kommentierungsfunktion umgegangen werden soll.

**Twitter**

Twitter ist ein Mikro-Blogging-Dienst, über den kurze Nachrichten mit maximal 140 Zeichen veröffentlicht werden können. Über Twitter werden Informationen in Echtzeit ausgetauscht. Viele Benutzer nutzen Twitter über Mobiltelefon (überall, jederzeit). Benutzer müssen sich registrieren, die gewählte Identität wird aber in der Regel nicht kontrolliert. Registrierte Benutzer können die Beiträge kommentieren und darauf antworten. Nicht registrierten Benutzern können Beiträge nur lesen. Neben Privatpersonen verbreiten auch Institutionen Informationen über Twitter.

Jeder Beitrag (Tweed) kann mit einem Keyword, dem sogenannten Hashtag gekennzeichnet werden, um bei einer Schlagwortsuche schneller gefunden zu werden. Auch kann damit analysiert werden, welche Themen bei Twitter besonders beliebt sind. Sicherheitsempfehlungen zu Twitter finden sich in M 5.156 *Sichere Nutzung von Twitter*.

**Online-Banking**

Mittels Online-Banking lassen sich Bankgeschäfte über das Internet abwickeln. Alle Transaktionen werden in elektronischer Form mit Zugriff auf den entsprechenden Bankrechner durchgeführt. Dabei erfolgt der Zugriff entweder browserbasiert über die Webseite der Bank oder aber unter Verwendung einer entsprechenden Applikation für Online-Banking. Ein Vorteil für die Benutzer liegt darin, dass viele Bankgeschäfte unabhängig vom Ort und Banken-Öffnungszeiten getätigt werden können.

Beim Online-Banking ist das bedeutendste Risiko, dass Angreifer auf Kundenkonten zugreifen können. Typischerweise versuchen Angreifer hierfür an Authentisierungsinformationen zu gelangen, z. B. über Phishing, oder die Kunden auf manipulierte Webseiten zu lenken, z. B. über Trojanische Pferde.

**Instant Messaging**

Instant Messaging ist eine Chat-Variante. Hierbei kommunizieren zwei oder mehr Teilnehmer über einen Instant Messaging Dienst. Instant Messaging kann als kostengünstige und schnelle Alternative zu Telefon, SMS oder E-Mail genutzt werden. Viele Dienste bieten neben der reinen Textübermittlung zusätzliche Funktionen wie beispielsweise die Übermittlung von Dateien oder spezielle Chat-Kanäle an. Nachrichten müssen in einer Instant-Messaging-Sitzung nicht unbedingt sofort gelesen und beantwortet werden, aber ein zeitnaher Kontakt ist möglich.

Um Instant Messaging zu nutzen, ist eine Registrierung notwendig, wobei die Angaben allerdings normalerweise nicht geprüft werden. Die Messanger-Kennung, die aus Benutzername, Messanger-Nummer oder Messanger-ID bestehen kann, muss zunächst möglichen Kommunikationspartnern mitgeteilt werden. Es folgt die Aufnahme der Kommunikationspartner in eine Kontaktliste. Oft kann auch der Status des Benutzers übermittelt werden, beispielsweise ob er abwesend, beschäftigt oder besonders interessiert an einer Kommunikation ist. Bei vielen Instant Messaging-Diensten kann die öffentliche Statusanzeige abgeschaltet werden. Gesendeten Links sollte nur gefolgt werden, wenn sichergestellt ist, dass der bekannte Kommunikationspartner diesen gesendet hat und der Link nicht zu Schadsoftware führt. Ebenso sollte keine unverlangt gesandte Datei geöffnet werden.

Ein wesentlicher Nachteil bei der Nutzung von Instant Messangern ist, dass es unterschiedliche Anbieter gibt, die verschiedene Protokolle verwenden. Potentielle Kommunikationspartner müssen also darauf achten, dass sie das gleiche System nutzen, damit sie miteinander kommunizieren können.

**Internet-Telefonie**

Als Internet-Telefonie oder IP-Telefonie wird die Sprachübertragung über öffentliche IP-Netze, vor allem das Internet, bezeichnet. Für die Sprachübertragung über IP-Netze gibt es unterschiedliche Anwendungsszenarien und entsprechend unterschiedliche Sicherheitsanforderungen (siehe dazu B 4.7 *VoIP*). Internet-Telefonie ist eine Variante von Voice over IP (VoIP).

Zur Internet-Telefonie können Softphones eingesetzt werden, die meist, ähnlich zu Messaging-Diensten, über zentrale Verzeichnisse registriert sind. Zunehmende Verbreitung finden kompakte und kostengünstige VoIP-Gateways, die es ermöglichen, mit herkömmlichen Telefonen Internet-Telefonie-Dienste zu nutzen. Außerdem gibt es auch spezielle Endgeräte für die Internet-Telefonie (Hardphones). Bei der Internet-Telefonie muss das als Gateway benutzte IT-System zum Telefonieren eingeschaltet und ans Internet angeschlossen sein. Zusätzlich können Instant Messaging Systeme sowie mobile Geräte eingebunden werden.

**Skype**

Skype ist eine Software zur Internet-Telefonie mit Instant Messaging Funktionen. Über Skype kann beispielsweise telefoniert, Daten übertragen oder Videokonferenzen abgehalten werden.

Sobald die Kommunikationspartner mit ihrem Rechner online gehen, sind sie unter ihrer Skype-Nummer erreichbar. Für eine permanente Erreichbarkeit müsste also der Rechner immer laufen. Fällt der Skype-Anbieter aus, ist Skype jedoch komplett nicht mehr zu benutzen.

**Soziale Netzwerke**

Soziale Netzwerke sind im Web zur Verfügung gestellte Plattformen, die zur Kommunikation und zum Austausch von Daten der Benutzer untereinander genutzt werden. Je nach Ausrichtung der Plattform können dort neben persönlichen Daten auch Fotos eingestellt und verschiedene Anwendungen genutzt werden. Die inhaltliche Ausgestaltung übernehmen die Nutzer selbst.

Die in einem sozialen Netzwerk verwendete Identität kann fiktiv sein, fälschlicherweise verwendet oder von einem Unbefugten ohne Wissen des eigentlichen Besitzers angelegt worden sein. Die Vernetzung der Benutzer untereinander erfolgt aufgrund von sozialen Interaktionen zwischen den Benutzern und wird mithilfe spezieller Plattformfunktionen im Datenbestand der Software gespeichert.

Sicherheitsempfehlungen zur Nutzung sozialer Netzwerke finden sich in M 5.157 *Sichere Nutzung von sozialen Netzwerken*.

**Internetfernsehen/WebTV**

Internetfernsehen bezeichnet die Übertragung von Fernsehprogrammen und Filmen als breitbandige Anwendungen über das Internet. Beim Internetfernsehen wird keine Übertragungsqualität gewährleistet. Diese liegt allein im Verantwortungsbereich des Internetzugangs des Benutzers und dem entsprechenden Endgerät.

Zusätzlich gibt es auch Dienste im Internet, die es ermöglichen, Fernsehsendungen aufzunehmen. Die aufgenommene Fernsehsendung kann entweder als Videodatei heruntergeladen oder direkt im Browser-Fenster angesehen werden.

**Internetradio/Webradio**

Das internetbasierte Angebot der Hörfunksendungen wird auch als Internet- oder Webradio bezeichnet. Die Übertragung erfolgt meistens als Streaming Audio, für deren Nutzung entsprechende Software benötigt wird. Viele Sender nutzen diese Art der alternativen Übertragung, um Hörer, die weder via

Satellit noch terrestrisch das entsprechende Programm empfangen können, zu erreichen.

Der Empfang von Webradio-Angeboten ist nicht auf am Internet angeschlossene PCs beschränkt. Es können dazu auch eigene Webradio-Empfänger, die über einen Router an das Internet angeschlossen sind, wie auch unzählige weitere Geräte (Mobiltelefone, Spielkonsolen) genutzt werden.

**Web-Speicherplatz**

Web-Speicherplatz (auch Online-Festplatte genannt) kann genutzt werden, um Informationen im Internet abzuspeichern. Auf die abgespeicherten Informationen kann von verschiedenen IT-Systemen aus zugegriffen werden. So kann beispielsweise ein Benutzer von verschiedenen IT-Systemen aus auf die Informationen zugreifen oder die Informationen mit anderen Benutzern teilen. Um Web-Speicherplatz zu nutzen, müssen sich die Benutzer in der Regel registrieren. Je nach eingesetztem Dienst kann es notwendig sein, eine Applikation auf dem IT-System des Benutzers zu installieren, damit der Web-Speicherplatz wie ein lokales Laufwerk genutzt werden kann (daher den Name Online-Festplatte). Einige Dienste unterstützen offene Standards wie WebDAV (Web-based Distributed Authoring and Versioning), die von vielen Betriebssystemen unterstützt werden, ohne dass zusätzliche Applikationen installiert werden müssen. In der Regel kann auch über Webanwendungen auf die Informationen zugegriffen werden. Ordner müssen explizit für andere Benutzer freigegeben werden oder sind hierfür reserviert ("Public-Folder").

Kennen Dritte das Passwort, dass in der Regel zur Authentisierung benötigt wird, können sie auf alle abgelegten Informationen zugreifen.

**Webshops**

Über Webshops können Produkte bezogen werden. Oft sind Webshops über das World Wide Web erreichbar, mit Hilfe eines Browsers können Waren ausgewählt, in einen virtuellen Einkaufswagen gelegt und dann bestellt werden.

Insbesondere bei mobilen Endgeräten können oft zusätzliche Applikationen direkt über eine separate Anwendung ausgewählt und auf dem Endgerät installiert werden. Gelingt es einem Angreifer, eine Software mit Schadsoftware den Anwendern in Webshop anzubieten oder während der Übertragung zu verändern, kann er das IT-System des Benutzers kompromittieren.

**Sicherheitsaspekte**

Einige typische Sicherheitsaspekte im Zusammenhang mit Internet-Diensten sind im Folgenden exemplarisch aufgeführt:

- Benutzerkennungen können bei vielen Internet-Diensten bei der Anmeldung frei ausgewählt werden. Dadurch ist die Nutzung falscher Identitäten möglich.
- Im Allgemeinen werden auch schwache Passwörter zur Anmeldung akzeptiert, damit ist Identitätsdiebstahl möglich.
- Durch die schnelle und breit gestreute Informationsweitergabe werden Informationen häufig zu früh oder unautorisiert weitergegeben, aber auch ungeprüft geglaubt.
- Die Geschäftsbedingungen vieler Internet-Dienste erlauben eine Nutzung der angegebenen Benutzerinformationen für Werbezwecke.

# M 2.460 Geregelte Nutzung von externen Dienstleistungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Mitarbeiter

Über das Internet werden eine Vielzahl attraktiver Dienstleistungen angeboten, die nicht nur privat, sondern auch in der Arbeitswelt die Zusammenarbeit in Teams erleichtern oder Arbeitserleichterungen bringen. Hierzu gehören beispielsweise Webmail-Dienste, Gruppen-Terminkalender, Fernhilfesoftware, Internet-Textverarbeitungssysteme, Online-Officeprogramme, Adressbuch-Verwaltung, Datenspeicherung und vieles mehr. Viele dieser Dienste sind ohne großen Aufwand direkt nutzbar und können bei einer Vielzahl verschiedener Abläufe in einer Institution helfen.

Grundsätzlich sollte allen Mitarbeitern klar sein, dass sie nur von ihrer Institution freigegebene externe Dienstleistungen benutzen dürfen. Für die eigenmächtige Nutzung von externen Dienstleistungen gilt ebenso wie für die Installation nicht-freigegebener Software, dass hierdurch eine Vielzahl von Sicherheits- und Datenschutz-Problemen entstehen können (siehe G 3.105 *Ungenehmigte Nutzung von externen Dienstleistungen*).

Die Mitarbeiter müssen über die Problematik und die Sicherheitsrisiken aufgeklärt werden, die die ungenehmigte Nutzung solcher Dienstleistungen mit sich bringen kann. Dies kann beispielsweise im Rahmen von geeigneten internen Veranstaltungen angesprochen werden, oder durch Hinweise im Intranet mit konkreten Beispielen aufgegriffen werden. In den Hilfsmitteln zum IT-Grundschutz findet sich ein Muster einer Mitarbeiterinformation über die unberechtigte Nutzung externer IT-Dienstleistungen, das als sinnvolle Grundlage für eine entsprechende Veröffentlichung dienen kann.

Generell sollte aber auch innerhalb der Institution nach Ursachen und Lösungen gesucht werden, wenn Mitarbeiter externe Dienstleistungen zur Arbeitsunterstützung nutzen wollen. Beispielsweise könnte überlegt werden, ob die interne IT-Abteilung eine vergleichbare Dienstleistungsqualität zur Verfügung stellen kann oder ein Nutzungsvertrag mit einem vertrauenswürdigen Anbieter geschlossen werden kann.

Prüffragen:

- Ist die Nutzung von externen Dienstleistungen für alle Mitarbeiter transparent geregelt?
- Ist allen Mitarbeitern bekannt, was bei der Nutzung von externen Dienstleistungen, z. B. Web-Mail-Diensten, zu beachten ist?

# M 2.461 Planung des sicheren Bluetooth-Einsatzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Bluetooth kann anhand der vielen verfügbaren Anwendungsprofile in unterschiedlichen Szenarien zum Einsatz kommen. Daher sind im Vorfeld einige Planungen in der Institution notwendig, um Bluetooth sicher betreiben zu können. Generell ist festzulegen, welche Strategie die Institution im Hinblick auf Bluetooth einnimmt und in welchem Umfang die einzelnen Funktionen und Anwendungsprofile verwendet werden sollen.

Generell müssen zwei Arten von Bluetooth-Geräten unterschieden werden:

- Endgeräte mit Bluetooth-Funktionalitäten (kurz: Bluetooth-Endgeräte), beispielsweise Mobiltelefone, Smartphones, Laptops usw..
- Peripheriegeräte mit Bluetooth-Funktionalitäten (kurz: Bluetooth-Peripheriegeräte), beispielsweise Maus, Tastatur, Headset usw.

Bluetooth-Endgeräte verfügen in der Regel über alle Funktionen der Bluetooth-Spezifikationen und die implementierten Sicherheitsfunktionen können frei verwendet werden. Bluetooth-Peripheriegeräte erweitern Bluetooth-Endgeräte durch ihre speziellen Funktionen. Sie können in der Regel die vorhandenen Sicherheitsfunktionen allerdings nur eingeschränkt nutzen. Bluetooth-Peripheriegeräte verwenden dafür meist einzelne Anwendungsprofile der Bluetooth-Endgeräte.

Der Einsatzzweck der Bluetooth-Peripheriegeräte ist meist durch die Bauart festgelegt. So kann ein Bluetooth-Headset ausschließlich zur Sprachübermittlung und eine Bluetooth-Tastatur nur als Eingabegerät verwendet werden. Die Endgeräte haben im Gegenzug eine Vielzahl von Einsatzmöglichkeiten. So kann beispielsweise ein Mobiltelefon über Bluetooth einem Laptop Modem-Funktionalitäten anbieten oder es können Daten zwischen zwei Bluetooth-Endgeräten ausgetauscht werden.

Zunächst muss also überlegt werden, für welche Zwecke innerhalb und außerhalb der Institution Bluetooth-Geräte eingesetzt werden sollen. Im nächsten Schritt ist zu definieren, in welchen Bereichen und unter welchen Rahmenbedingungen Bluetooth eingesetzt werden darf und in welchen nicht. So sollte beispielsweise in Institutionsbereichen, in denen geschäftskritische Informationen verarbeitet werden, keine Bluetooth-Eingabegeräte verwendet werden, da bei diesen über Keylogging-Angriffe Tastatureingaben mitgeschnitten werden könnten. Daher muss klar geregelt sein, welche Bluetooth-Funktionen in welchen Bereichen der Institution eingesetzt werden darf. Auch wenn die Bluetooth-Nutzung innerhalb bestimmter räumlicher Grenzen untersagt wird, können sich trotzdem Geräte mit Bluetooth-Schnittstellen innerhalb dieser Bereiche befinden. Um zu verhindern, dass diese von außen angesprochen werden, sind entweder die Bluetooth-Schnittstellen dieser Geräte zu deaktivieren oder die Mitnahme von Geräten mit Bluetooth-Schnittstellen wie z. B. Mobiltelefonen oder PDAs in diese Bereiche zu verbieten.

Darüber hinaus muss entschieden werden, welche Sicherheitsfunktionen grundlegend eingesetzt werden sollen, um die Bluetooth-Geräte und die Kommunikation zwischen zwei Bluetooth-Geräten abzusichern (siehe M 3.79 *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*). Diese Entscheidung ist die Grundlage für die sichere Konfiguration und den sicheren

Betrieb der Bluetooth-Geräte (siehe M 4.362 *Sichere Konfiguration von Bluetooth* und M 4.363 *Sicherer Betrieb von Bluetooth-Geräten*). Ebenso müssen Regelungen für die Benutzer existieren, die beschreiben, was bei der Nutzung von Bluetooth-Geräten und deren Sicherheitsfunktionen beachtet muss.

Die Rahmenbedingungen für die Bluetooth-Nutzung müssen in der Sicherheitsrichtlinie der Institution verankert sein.

Um Bluetooth und die damit verbundenen Geräte sicher betreiben zu können, sind die folgenden Punkte wesentlich:

- Die Arbeitsweise und Technik der eingesetzten drahtlosen Kommunikationssysteme müssen von den für den Betrieb Verantwortlichen vollständig verstanden werden.
- Die Sicherheit der eingesetzten Technik sollte regelmäßig evaluiert werden. Ebenso sollten regelmäßig die Sicherheitseinstellungen der benutzten Endgeräte (z. B. Mobiltelefone, Laptops, PDAs) untersucht werden. Sicherheitsrelevante Patches und Updates müssen schnellstmöglich aufgespielt werden.
- Die Rahmenbedingungen für die Bluetooth-Nutzung müssen in der Sicherheitsrichtlinie der Institution verankert sein.
- Es ist festzulegen, ob die Bluetooth-Nutzung genehmigt oder unterbunden werden soll. Beispielsweise kann es aus Sicherheitsgründen sinnvoll sein, die Bluetooth-Nutzung bei dienstlichen IT-Geräten generell oder in bestimmten Bereichen zu untersagen.
- Um die übertragenen Daten zu schützen, müssen Vorgaben ausgearbeitet werden, die sich unter anderem mit der Auswahl adäquater Verschlüsselungs- und Authentikationsverfahren, deren Konfiguration und Schlüsselmanagement beschäftigen.

**Sicherheitshinweise für die Bluetooth-Nutzung**

Den Benutzern sollten einfache und klare Sicherheitshinweise für die Bluetooth-Nutzung zur Verfügung gestellt werden. In diesen muss unter anderem erklärt werden, welche Verantwortung die Benutzer bei Bluetooth-Nutzung übernehmen, welche Einstellungen an den Bluetooth-Geräten sicherheitsrelevant sind,sowie welche Einstellungen von den Benutzern vorgenommen werden dürfen bzw. müssen und welche von den Administratoren durchgeführt werden. Darüber hinaus ist darin zu definieren welche Arten von Daten über Bluetooth übertragen werden dürfen.

Viele von Endbenutzern verwendete Geräte wie Mobiltelefone oder PDAs besitzen Bluetooth-Schnittstellen, die bei der Auslieferung meistens nicht deaktiviert sind. Es muss klar geregelt sein, ob diese Bluetooth-Schnittstellen genutzt werden dürfen, und wenn ja, unter welchen Rahmenbedingungen.

Um Benutzer nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene Bluetooth-Benutzerrichtlinie zu erstellen. In einer solchen Nutzungsrichtlinie sollten dann kurz die Besonderheiten bei der Bluetooth-Nutzung beschrieben werden, wie z. B.

- unter welchen Rahmenbedingungen Bluetooth-Komponenten genutzt werden dürfen,
- wie Bluetooth-Endgeräte korrekt zu installieren und zu verwenden sind,
- welche Schritte bei (vermuteter) Kompromittierung von Bluetooth-Komponenten zu unternehmen sind, vor allem, wer zu benachrichtigen ist.

Die Sicherheit von Bluetooth basiert stark auf der Güte der verwendeten Bluetooth-Passwörter. Diese müssen daher sehr sorgfältig ausgewählt werden, Benutzer und Administratoren sind über deren herausgehobene Bedeutung

zu informieren (siehe auch M 3.80 *Sensibilisierung für die Nutzung von Bluetooth*).

Wichtig ist auch, dass klar beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass keine sicherheitsrelevanten Konfigurationen verändert werden dürfen.

Außerdem sollte die Nutzungsrichtlinie ein klares Verbot enthalten, ungenehmigt Bluetooth-Komponenten anzuschließen. Des Weiteren sollte die Richtlinie insbesondere im Hinblick auf die Nutzung von klassifizierten Informationen, beispielsweise Verschlusssachen, Angaben dazu enthalten, welche Informationen über Bluetooth übertragen werden dürfen und welche nicht. Benutzer sollten für Bluetooth-Gefährdungen sowie für Inhalte und Auswirkungen der Bluetooth-Richtlinie sensibilisiert werden.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Bluetooth-Nutzung?
- Existieren dokumentierte Rahmenbedingungen für die sichere Bluetooth-Nutzung?

# M 2.462 Auswahlkriterien für die Beschaffung von Bluetooth-Geräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Einzelne Bluetooth-Geräte unterscheiden sich darin, welche Bluetooth-Spezifikationen verwendet wurden, den verfügbaren Anwendungsprofilen und der Art und Weise, wie Bluetooth von den Herstellern implementiert wurde. Daher sind einzelne Kriterien zu definieren, die bei der Auswahl von Bluetooth-Geräten zu berücksichtigen sind.

Zunächst sollten alle Geräte ausgeschlossen werden, bei denen bekannt ist, dass diese durch Bluetooth-Schwachstellen gefährdet sind. Im Internet gibt es einschlägige Listen zu den einzelnen Schwachstellen, in denen die betroffenen Geräte aufgeführt sind.

Darüber hinaus ist festzulegen, welche Anwendungsprofile für die jeweiligen Einsatzzwecke der Bluetooth-Geräte notwendig sind und welche nicht enthalten sein dürfen bzw. deaktiviert werden müssen. Hierbei sind in den Bluetooth-Geräten die Anwendungsprofile enthalten, die für die jeweiligen Funktionen notwendig sind. So ist in einer Bluetooth-Maus oder -Tastatur stets das HID-Profile implementiert, das für die Funktionen von Zeigegeräten erforderlich ist (siehe M 3.79 *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*). Jedoch kann es einen sicherheitsrelevanten Vorteil haben, wenn beispielsweise ein Mobiltelefon kein SIM Access Profile hat, da dieses den Zugriff auf die SIM-Karte des Mobiltelefons ermöglicht und so einen potentiellen Angriffspunkt darstellt.

Auf jeden Fall sollte bei der Auswahl der Endgeräte darauf geachtet werden, dass diese mindestens der Bluetooth-Spezifikationsversion 2.1 entsprechen, da ab dieser wesentliche Sicherheitsfunktionen wie beispielsweise das Secure Simple Pairing enthalten sind. Es sollte auch gewährleistet sein, dass keine Geräte verwendet werden, die auf einer Bluetooth-Spezifikation älter als Version 2.1 basieren, da dann auf schwächere Sicherheitsmechanismen zurückgegriffen wird (siehe M 4.362 *Sichere Konfiguration von Bluetooth*).

Die wichtigsten sicherheitsrelevanten Kriterien zur Auswahl von Bluetooth-Komponenten sind hier zusammengestellt:

- Die Bluetooth Special Interest Group (SIG) entwickelt nicht nur die Bluetooth-Spezifikationen weiter, sondern überprüft und zertifiziert auch die Interoperabilität von Bluetooth-Geräten. Allerdings gibt es eine große Anzahl nicht nach den Qualitätsanforderungen der Bluetooth-SIG zertifizierter Produkte auf dem Markt. Diese Produkte weisen womöglich nicht das gewünschte Maß an Kompatibilität auf. Bei der Beschaffung sollte daher darauf geachtet werden, nur solche Produkte zu kaufen, die das offizielle Bluetooth-Label tragen.
- Nicht bei jedem Bluetooth-Gerät kann die Bluetooth-Schnittstelle deaktiviert werden, dies sollte bereits bei der Auswahl beachtet werden.
- Die Bluetooth-Spezifikation sieht drei Leistungsklassen vor, durch deren jeweilige maximale Sendeleistung die Reichweite der Geräte bestimmt ist. Bei der Entscheidung für Geräte der Leistungsklassen 1 bis 3 sollte auch berücksichtigt werden, dass mit höherer Reichweite auch der potentielle Kreis der Angreifer zunimmt.

- Bei Bluetooth-Peripheriegeräten, z. B. einem Headset, ist die Bluetooth-PIN typischerweise voreingestellt oder sogar fest vorgegeben. Da dies eine massive Sicherheitseinschränkung bedeutet, sollte bei der Beschaffung darauf geachtet werden, dass die PIN möglichst frei wählbar ist.
- Bei dem Bluetooth-Gerät sollten die Spezifikationen von Version 2.1 + EDR implementiert sein. Hierdurch wird gewährleistet, dass der Sicherheitsmodus 4 in Kombination mit den Secure Simple Pairing Funktionalitäten vorhanden ist.

Vor der Beschaffung muss überprüft werden, ob die Bluetooth-Komponenten alle benötigten Profile unterstützen. Wird ein Profil wie das Advanced Audio Distribution Profile (A2DP) nicht unterstützt, ist es beispielsweise nicht möglich, hochwertige Audiodaten über Bluetooth zu übertragen.

Prüffragen:

- Wurden Kriterien für die Bescahffung von Bluetooth-Geräten definiert?
- Wurde festgelegt, welche Anwendungsprofile für die jeweiligen Einsatzzwecke der Bluetoothgeräte notwendig sind?
- Unterstützen die ausgewählten Endgeräte die Bluetooth-Spezifikationsversion 2.1?

# M 2.463 Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Einige Endgeräte haben in der Standardkonfiguration kein Bluetooth-Modul oder deren Bluetooth-Module entsprechen nicht einer aktuellen Bluetooth-Spezifikation. Um solche Endgeräte kurzfristig mit einer aktuellen Bluetooth-Technologie auszustatten, kann es hilfreich sein, einen zentralen Pool mit Bluetooth-Peripheriegeräten aufzubauen. In diesem Pool können unterschiedliche Bluetooth-Geräte verwaltet werden. Angefangen von Bluetooth-Mäusen und -Tastaturen über GPS-Empfänger, die mittels Bluetooth mit einem Bluetooth-Endgerät kommunizieren können, bis hin zu Bluetooth-Adaptern (als USB-Stick oder als Einsteckkarte für Laptops), die einem Endgerät die Möglichkeit bieten, Bluetooth einzusetzen.

Vor allem bei Bluetooth-Tastaturen und -Mäusen ist zu beachten, dass hierzu stets ein Bluetooth-Adapter gehört, um diese Funktechnik nutzen zu können. Mit diesem Bluetooth-Adapter ist ein Endgerät auch generell als Bluetooth-Gerät erkennbar und muss entsprechend sicher konfiguriert werden. Ansonsten sind die Empfehlungen der Maßnahme M 4.254 *Sicherer Einsatz von drahtlosen Tastaturen und Mäusen* bei der Verwendung von Bluetooth-Tastaturen und -Mäusen zu beachten.

Auf dem Markt sind eine Vielzahl von Produkten erhältlich, die über Bluetooth kommunizieren. Bei korrekter Implementierung und Konfiguration der Bluetooth-Sicherheitsmerkmale bieten diese im Allgemeinen einen höheren Schutz als Funksysteme mit proprietärer Technik. Vor allem bei Tastaturen ist aber darauf zu achten, dass ein ausreichend langer Schlüssel für die Bluetooth-Verbindung verwendet wird. Darüber hinaus sollten die Eingabegeräte der Bluetooth-Spezifikation 2.1 + EDR entsprechen, da mit dieser Spezifikation das sogenannte Simple Secure Pairing möglich ist (siehe M 4.362 *Sichere Konfiguration von Bluetooth*) was für eine höhere Sicherheit für die Bluetooth-Verbindung darstellt und Keylogging-Angriffe erschweren.

Alle in dem Pool enthaltenen Bluetooth-Geräte sollten den Kriterien entsprechen, die durch die Empfehlungen der Maßnahme M 2.462 *Auswahlkriterien für die Beschaffung von Bluetooth-Geräten* für die Institution definiert wurden.

Bei der Ausgabe der Bluetooth-Geräte sind die jeweiligen Benutzer über die korrekte Verwendung des Bluetooth-Gerätes und die damit verbundenen Sicherheitsfunktionen zu informieren. Hierzu ist ein Übersichtsblatt zu Sicherheitshinweisen für die Bluetooth-Nutzung zu erstellen, die auch Installations- und Verwendungshinweise für das Bluetooth-Endgerät enthalten sollte. Darüber hinaus ist zu dokumentieren, wer wann welches Bluetooth-Gerät ausgeliehen hat und für welchen Einsatzzweck das Gerät verwendet werden soll. Den Empfang des Bluetooth-Gerätes muss der Benutzer durch seine Unterschrift bestätigen. Mit seiner Unterschrift bestätigt der Benutzer darüber hinaus, dass er die die Sicherheitshinweise für die Bluetooth-Nutzung kennt und diese einhält. Auch die Rückgabe des Bluetooth-Gerätes wird auf dem Formular vermerkt.

Eventuell ist es von Vorteil, den zentralen Pool für Bluetooth-Geräte und einen eventuell vorhandenen Pool für Mobiltelefone zusammenzulegen und die Bluetooth-Geräte dort mit aufzunehmen (siehe M 2.190 *Einrichtung ei-*

*nes Mobiltelefon-Pools*). Viele Mobiltelefone haben heutzutage standardmäßig Bluetooth, was dazu führt, dass dort auch dieselben Sicherheitseinstellungen wie bei anderen Bluetooth-Geräten vorgenommen werden müssen.

Prüffragen:

- Werden Bluetooth-Geräte aus zentralen Pools nach Rückgabe wieder auf die Standardeinstellungen zurückgesetzt?

# M 2.464 Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei dem Einsatz von Terminalserver-Systemen sind geeignete Sicherheitsrichtlinien aufzustellen. Die hierin schriftlich festgehaltenen Maßgaben sowie Zielsetzungen müssen die individuellen Bedingungen und Anforderungen einer sicheren Terminalserver-Umgebung widerspiegeln. Das allgemeine Sicherheitskonzept, die Sicherheitsleitlinie sowie die hiervon abgeleiteten Sicherheitsrichtlinien stellen dabei den Rahmen dar, in dem sich die Terminalserver-spezifischen Erweiterungen widerspruchsfrei integrieren sollen. Die Richtlinien müssen regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Die auf Terminalserver bezogenen Vorgaben können in den vorhandenen Richtlinien ergänzt oder in einem eigenen Dokument zusammengefasst werden.

Die Richtlinien sollten unter anderem folgende Punkte regeln:

- Die Mindestanforderungen, die Clients erfüllen müssen, um für den Zugang zum Terminalserver benutzt werden zu dürfen.
- Das Umfeld, in dem diesen Clients der Zugriff erlaubt ist. Insbesondere sollten kritische Zugangsmöglichkeiten, etwa am Telearbeitsplatz, aus einem Internetcafé heraus oder mittels Notebook über ein unsicheres WLAN (siehe auch M 2.389 *Sichere Nutzung von Hotspots*) geregelt sein.
- Zusätzliche Geräte, die an Clients angeschlossen werden dürfen (Drucker, USB-Sticks, andere Endgeräte).
- Die internen bzw.externen Netze, an die die Terminalserver-Umgebung gekoppelt werden darf.
- Die Informationen oder nachgelagerten Dienste, auf die über Terminalserver-Systeme zugegriffen werden darf und wem dies erlaubt ist.
- Sicherheitsmaßnahmen und eine Standard-Konfiguration sollten für alle Terminalserver-Komponenten festgelegt werden.
- Bei einem Verdacht auf Sicherheitsprobleme, muss der IT-Sicherheitsbeauftragte hierüber informiert werden, damit dieser weitere Schritte einleiten kann (siehe auch B 1.8 *Behandlung von Sicherheitsvorfällen*).
- Administratoren, aber auch Benutzer von Terminalservern, sollten über die Gefährdungen bei der Verwendung der Terminalserver-Architektur und die zu beachtenden Sicherheitsmaßnahmen informiert bzw. geschult werden.
- Die korrekte Umsetzung, der in den Richtlinien beschriebenen Maßnahmen, sollte überdies regelmäßig kontrolliert werden.

**Benutzerrichtlinie für Terminalserver-Umgebungen**

Um Benutzer nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene Benutzerrichtlinie für Terminalserver-Umgebungen zu erstellen. In ihr sollten dann kurz die Besonderheiten der Terminalserver-Nutzung beschrieben werden, wie z. B.:

- Von welchen internen bzw. externen Netzen darf der Zugang zum Terminalserver-System erfolgen?
- Unter welchen Rahmenbedingungen dürfen sich Benutzer bei der Umgebung anmelden?
- Dürfen organisationsfremde Clients genutzt werden und wenn ja wie?

- Welche Schritte sind bei einer (vermuteten) Kompromittierung des Terminalservers oder des Clients zu unternehmen? Wer ist zu benachrichtigen?

Wichtig ist auch, dass klar beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass

- keine sicherheitsrelevanten Konfigurationen verändert oder an Dritte versandt werden und,
- nur ausdrücklich freigegebene Softwarestände der Terminalsoftware verwendet werden dürfen,

Beim Zugriff auf Terminalserver über ein entferntes Netz ist klarzustellen, dass

- stets ein Virenscanner aktiviert ist,
- eine vorhandene Personal Firewall nicht abgeschaltet werden darf (siehe auch M 5.91 *Einsatz von Personal Firewalls für Clients* ) und
- einer Überprüfung der Client-Authentizität durch ein Sicherheitsgateway vom Benutzer zugestimmt werden muss, da sonst kein normaler oder nur ein eingeschränkter Zugang gewährt wird.

Terminalserver-Sitzungen können während der Benutzung willentlich oder durch einen Verbindungsabbruch getrennt werden. Bereits gestartete Anwendungen laufen dabei in der Regel weiter und die Sitzung kann zu einem späteren Zeitpunkt fortgesetzt werden. Um Wartungsarbeiten an den Servern nicht zu behindern und Datenverluste durch regelmäßige Neustartzyklen zu vermeiden, sind daher Verhaltensweisen zum sicheren Umgang in den Benutzerrichtlinien festzuhalten.

- Sitzungen, die durch Verbindungsstörungen unterbrochen wurden, sollten sobald wie möglich wieder aufgenommen werden.
- Benutzer sollten auf die maximale Dauer ihrer Terminalserver-Sitzung hingewiesen werden.
- Spätestens am Ende der Nutzungszeit sind die entfernt ausgeführten Programme durch den Anwender zu beenden und Terminalserver-Sitzungen regulär vom Benutzer abzumelden.

Außerdem sollte die Richtlinie insbesondere im Hinblick auf die Nutzung von klassifizierten Informationen, beispielsweise Verschlusssachen, Angaben dazu enthalten, welche Daten über Terminalserver-Systeme genutzt und auf den Client übertragen werden dürfen. Benutzer sollten für Terminalserver-Gefährdungen sowie für Inhalte und Auswirkungen der Terminalserver-Richtlinie sensibilisiert werden.

**Richtlinien für Administratoren**

Daneben sollte eine Terminalserver-spezifische Richtlinie für Administratoren erstellt werden, die auch als Grundlage für die Schulung der Administratoren dienen kann. Darin sollte festgelegt sein, wer für die Administration der unterschiedlichen Terminalserver-Komponenten zuständig ist, welche Schnittstellen es zwischen den beteiligten Administratoren gibt und wann welche Informationen zwischen den Zuständigen ausgetauscht werden müssen. So ist es durchaus üblich, dass für den Betrieb einer Terminalserver-Farm eine andere Organisationseinheit zuständig ist, als für die Betreuung der Clients oder für das Identitäts- und Berechtigungsmanagement oder für den Perimeterschutz.

Die Terminalserver-Richtlinie für Administratoren sollte des Weiteren die wesentlichen Kernaspekte zum Betrieb einer Terminalserver-Infrastruktur umfassen, wie z. B. :

- Festlegung einer sicheren Terminalserver-Konfiguration und Definition von sicheren Standardkonfigurationen für Clientsysteme.

- Konfiguration von gegebenenfalls vorhandenen Verwaltungsservern für Terminalserver.
- Verfahren zur administrativen Durchsetzung individueller Berechtigungen von Benutzern, für den Zugriff auf Dateien und Anwendungen.
- Verfahren zur administrativen Durchsetzung individueller Berechtigungen von Benutzern, für den Zugang zu nachgelagerten Diensten (Backends) und Netzen.
- Auswahl und Einrichtung von Verschlüsselungsverfahren beim Aufbau von Terminalserver-Sitzungen über unsichere Netze.
- Umgang mit Sitzungsunterbrechungen.
- Regelungen von Neustartzyklen zur Vorbeugung von Speicherlecks, Prozessproblemen und zur Durchführung von Wartungsfenstern.
- Regelmäßige Auswertung von Protokolldateien.
- Durchführung von Tests und Überwachung der Netz- und Systemauslastung.
- Inbetriebnahme von Ersatzsystemen.
- Maßnahmen bei Kompromittierung von Terminalservern.

Administratoren haben beim Einsatz von Terminalservern oft die Möglichkeit, Sitzungen zu spiegeln (shadowing). Hierbei sind datenschutzrechtliche Anforderungen zu berücksichtigen. So greift eine Überwachung von Sitzungen ohne die ausdrückliche Zustimmung in die Persönlichkeitsrechte des Anwenders ein. Die Verwendung dieser Funktion ist daher innerhalb der Administratorenrichtlinien zu regulieren.

Alle Terminalserver-Anwender, egal ob Benutzer oder Administratoren, sollten mit ihrer Unterschrift bestätigen, dass sie den Inhalt der Sicherheitsrichtlinie gelesen haben und die darin definierten Anweisungen auch einhalten. Ohne diese schriftliche Bestätigung sollte niemand diese Systeme nutzen dürfen. Die unterschriebenen Erklärungen sind an einem geeigneten Ort, beispielsweise in der Personalakte, aufzubewahren.

Prüffragen:

- Wurden Sicherheitsrichtlinien für die Terminalserver-Administratoren und -Benutzer erstellt?
- Werden die Richtlinien zur Nutzung von Terminalservern regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst?
- Müssen alle Benutzer und Administratoren bestätigen, dass sie die Sicherheitsrichtlinie zu Terminalservern gelesen und die dort definierten Anweisungen auch erhalten haben?

# M 2.465 Analyse der erforderlichen Systemressourcen von Terminalservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Verfügbarkeit von Terminalservern gewährleisten zu können, ist die Dimensionierung der Systemressourcen von entscheidender Bedeutung. Prozessorleistung, Datendurchsatz zu Speichersystemen und deren Größe, sind Merkmale, die die Geschwindigkeit eines Terminalservers beschreiben, aber ebenso im hohen Maße die Stabilität eines derartigen Mehrbenutzersystems beeinflussen.

Im Gegenzug ist die Leistungsfähigkeit der Terminalserver-Clients weniger wichtig, da diese selbst nur die Anzeige- und Eingabeverwaltung übernehmen.

Je mehr Benutzer einen einzelnen Terminalserver nutzen, desto mehr Prozesse werden auf ihm gestartet und müssen zeitnah und parallel ablaufen können. Sind bestimmte Grenzen erreicht, kann der Terminalserver den Zugang weiterer Benutzer behindern, für die bereits angemeldeten Benutzer zu langsam reagieren oder sogar vollständig ausfallen.

**Skalierbarkeit**

Gerade Terminalserver-Systeme können die verwendete Technik schnell an ihre Leistungsgrenzen stoßen lassen. Hierbei ist zu beachten, dass kein einzelnes IT-System beliebig ausbaufähig ist und daher, individuell abhängig vom jeweiligen Anwendungsfall, ab einer bestimmten Lastgrenze Engpässe entstehen. Diese Engpässe können unter Umständen beseitigt werden, offenbaren aber, dass bei einer weiteren Steigerung der Serverlast, möglicherweise Limitierungen an einer anderen Stelle auftreten können.

Begrenzende Faktoren können sein:

- Die Anzahl der installierbaren Prozessoren
- Die Adressierbarkeit von Hauptspeicher durch die Systemarchitektur
- Die Verwaltbarkeit des Speichers durch das Betriebssystem
- Die Geschwindigkeit der Massenspeichersysteme
- Die Bandbreite der internen Bussysteme

Beispielsweise adressiert der Microsoft Windows Server 2003 als Basis für den Terminalserver-Dienst auf einem 32-Bit-System maximal 4 GB Hauptspeicher. Das Betriebssystem unterteilt diesen in der Standardkonfiguration in zwei Bereiche zu jeweils 2 GB für Anwendungen und die Systemorganisation.

Daher sollte bei der Planung einer Terminalserver-Umgebung im Vorfeld eine Strategie entwickelt werden, um wachsenden Benutzerzahlen, höheren Datenmengen und damit größeren Lasten, gerecht zu werden.

In der Praxis haben sich dafür Konzepte wie Server-Verbünde (Terminalserver-Farmen) bewährt, deren sichere Umsetzung in M 6.142 *Einsatz von redundanten Terminalservern* behandelt wird. Die Entscheidungen, die gemäß dieser Maßnahme getroffen werden, haben jedoch auch wechselseitig Einfluss auf die erforderliche Dimensionierung der Systemressourcen. So kann die Bereitstellung der notwendigen Leistung und die damit verbundene Aus-

fallsicherheit, entweder durch die Redundanz der Server, oder die Redundanz der Komponenten in den Servern selbst erfolgen.

**Erstellen eines Anforderungsprofils**

Für die Ermittlung der tatsächlich benötigten Ressourcen bietet sich eine eingehende Analyse der Zielumgebung an. Hierbei kann nicht aus dem Speicherverbrauch einer einzelnen Applikation, die von einem Benutzer ausgeführt wird, auf den des Systems mit der angestrebten Benutzerzahl, geschlossen werden. Zudem sollten im Hintergrund laufende Prozesse, wie Virenscanner, Dateiindizierungsmechanismen und Bildschirmeffekte mit berücksichtigt werden.

Zuerst muss daher überprüft werden, welche Programme zum Einsatz kommen, welche Aufgaben damit auf welche Art und Weise erledigt werden und wie schnell die Anwendungen für die Erledigung der Tätigkeiten der Benutzer reagieren müssen. Gegebenenfalls können automatisierte Tests oder Tests mit Benutzergruppen die vorhandenen Erfahrungswerte absichern.

Prüffragen:

- Wurde geprüft, welche Anwendungen auf dem Terminalserver eingesetzt und welche Aufgaben hiermit gelöst werden sollen?
- Wurde geprüft, welche Leistungsanforderungen die Anwendungen bei der geplanten Anzahl von Benutzern an die Terminalserver-Umgebung stellt?
- Wurde eine Strategie zur Nutzung von Terminalservern entwickelt, um wachsenden Benutzerzahlen, höheren Datenmengen und damit größeren Lasten zu bewältigen?

# M 2.466 Migration auf eine Terminalserver-Architektur

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Migration einer bestehenden Client-Server-Architektur auf eine Terminalserver-gestützte Umgebung muss vor der Umsetzung eingehend überprüft werden, ob die zu migrierenden Anwendungen dafür geeignet sind.

Treten bei der Überprüfung Datei- oder Zugriffskonflikte auf dem Zielsystem auf, so ist dies meist auf eine mangelnde oder fehlende Trennung der Benutzersitzungen durch die betroffene Anwendung zurückzuführen. Windows-basierte Server-Betriebssysteme bieten an dieser Stelle die Möglichkeit, innerhalb eines besonderen Installationsmodus die notwendige Kapselung, stellvertretend für die Anwendungen durchzuführen. Die Registrierungsdatenbank (Windows-Registry) und Dateien in wichtigen Systemverzeichnissen werden so für jede Sitzung individuell separiert. Auch Applikationen, die laut den Herstellern für Terminalserver geeignet sind, z. B. unter Windows Terminalserver und den Terminalserver-Lösungen der Firma Citrix, sind zumeist darauf ausgelegt, in dieser Form installiert zu werden. Ist die beschriebene Kapselungstechnik bei der geplanten Terminalserver-Lösung verfügbar, sollte diese verwendet werden. Wurde die Installation der Anwendung erfolgreich durchgeführt ist der Installationsmodus wieder zu verlassen.

**Analyse der Anforderungen**

Anwendungen mit stark unterschiedlichem Anforderungen an den Schutzbedarf sollten nicht ohne Weiteres auf einem Terminalserver betrieben werden. Ob sie gemeinsam auf einem Terminalserver betrieben werden können, hängt vom verwendeten Produkt und von den individuellen Gefährdungen und Anforderungen der Organisation bzw. der Anwendungen ab. Daher ist zu bewerten, inwieweit die in Frage kommende Terminalserver-Lösung dafür geeignet ist, Anwendungen unterschiedlichen Schutzbedarfs gemeinsam auf einem Terminalserver zu betreiben.

Zusätzlich sind angemessene Maßnahmen zu ergreifen, um ein ausreichendes Schutzniveau für alle Anwendungen zu gewährleisten. Die Applikation mit dem höchsten Schutzbedarf im Bereich Verfügbarkeit, Vertraulichkeit und Integrität ist daher maßgeblich für das jeweilige Schutzniveau aller auf dem Terminalserver betriebenen Anwendungen. Kann das notwendige Schutzniveau nicht für alle Anwendungen erreicht werden, sollte auf separate IT-Systeme ausgewichen werden.

Werden sehr viele unterschiedliche Anwendungen benötigt, können diese gegebenenfalls entsprechend den Anforderungen ihrer Benutzer gruppiert werden. Denn soll eine große Zahl unterschiedlichster Bedürfnisse durch eine einzelne oder einige wenige IT-Systeme erfüllt werden, wächst die Komplexität des Informationsverbundes und die Wahrscheinlichkeit, dass Applikationen sich gegenseitig stören. Hier empfiehlt es sich daher, die zuvor aufgestellten Benutzergruppen und Anwendungen passend auf verschiedene Systeme zu verteilen.

Überdies sind die in M 2.465 *Analyse der erforderlichen Systemressourcen von Terminalservern* und M 5.162 *Planung der Leitungskapazitäten beim Einsatz von Terminalservern* ermittelten Richtwerte mit den Leistungsmerkmalen

der bestehenden Netzinfrastruktur zu vergleichen und eventuell unüberwindbare Engpässe bereits im Vorfeld zu berücksichtigen.

Prüffragen:

- Sind die Anwendungen für den Einsatz auf einem Terminalserver geeignet?
- Ist sichergestellt, dass Anwendungen auf Terminalservern nicht in unerlaubter Weise auf kritische Systempfade und Registrierungsdatenbanken zugreifen, z. B. mittels eines besonderen Installationsmodus?
- Ist berücksichtigt, dass Anwendungen mit unterschiedlichen Anforderungen an den Schutzbedarf ohne angemessene Maßnahmen nicht auf Terminalservern betrieben werden dürfen?

# M 2.467 Planung von regelmäßigen Neustartzyklen von Terminalservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um den reibungsfreien Betrieb von Terminalservern zu gewährleisten, sollten regelmäßige Neustartzyklen eingeplant werden. Während des geregelten Herunter- und erneuten Hochfahrens können skriptgesteuert Wartungsarbeiten durchgeführt werden. Darüber hinaus werden durch diesen Vorgang die Auswirkungen etwaiger Speicherlecks, die die Leistungsfähigkeit der Terminalserver im Laufe der Zeit reduzieren können, begrenzt.

In großen Terminalserver-Verbünden sollten Neustartzyklen nicht für alle Terminalserver zu einem gemeinsamen Zeitpunkt erfolgen, um Lasten an den Verwaltungsservern beim Wiederanlauf über einen größeren Zeitraum zu verteilen. Zudem sollten Terminalserver, auf denen aktive Benutzersitzungen ablaufen, vom Neustart ausgenommen werden.

Dafür ist ein Anlaufplan auf der Grundlage des aktuellen Ausbaus der Terminalserver-Umgebung zu erstellen.

Prüffragen:

- Wurde ein Plan zum geregelten Neustart von Terminalservern erarbeitet?

# M 2.468 Lizenzierung von Software in Terminalserver-Umgebungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sollen Anwendungen, die bislang in einer Client-Server basierten Netzarchitektur genutzt werden, auf einem Terminalserver zentral bereitgestellt werden, sind lizenzrechtlich relevante Verträge im Vorfeld der Migration zu prüfen. So können Schutzmechanismen vor fehlerhafter Lizenzierung der Software möglicherweise nicht greifen, da diese unter Umständen die Anzahl der Installationen als Grundlage zur Bemessung der Benutzerzahl heranzieht.

Auf einem Terminalserver muss die Applikation jedoch zumeist nur ein einziges Mal installiert werden. In Abhängigkeit von den zur Verfügung stehenden Ressourcen des Applikationsservers ist diese dann durch beliebig viele Personen gleichzeitig ausführbar. Auch der Schutz eines sogenannten Hardwaredongles wird so möglicherweise unterlaufen.

Die unrechtmäßige Verwendung von nicht lizenzierter Software kann zivilrechtlich und eventuell sogar strafrechtlich belangt werden. Daher sollte die Nutzung der bereitgestellten Programme auf dem Terminalserver im Einklang mit den erworbenen Lizenzen reglementiert und angemessen protokolliert werden.

Einige Terminalserver-Systeme wie beispielsweise der Microsoft Windows Server 2003 erlauben mittels Lizenzserver die Steuerung der konkurrierend angemeldeten Benutzer. Zudem kann unter anderem abweichend hiervon eine Anzahl von registrierten Endgeräten lizenzrechtlich überwacht werden.

Die Installation und Aktivierung eines Lizenzservers zur Nutzung des Terminalserver-Dienstes ist bei dieser Softwarelösung sogar obligatorisch. Ein Terminalserver unter Microsoft Windows 2003 versagt nach 120 Tagen ohne Verbindung zu einem Lizenzserver seinen Dienst und lässt keine Anmeldungen von Benutzern zu. Die ordnungsgemäße Funktionalität des Lizenzservers wird damit von erheblicher Bedeutung für die Verfügbarkeit des Terminalservers.

Das korrekte Arbeiten des Lizenzservers sollte daher regelmäßig überwacht und dessen Ersatz im Falle dessen Versagens geplant und vorbereitet werden. In großen Installationen ist der Terminalserver vorsorglich redundant auszulegen.

Prüffragen:

- Wird die Nutzung der bereitgestellten Applikationen auf dem Terminalserver im Einklang mit den erworbenen Lizenzen reglementiert und angemessen protokolliert?

# M 2.469 Geregelte Außerbetriebnahme von Komponenten einer Terminalserver-Umgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sollen Terminalserver, an Terminalserver angeschlossene Clients oder Infrastrukturkomponenten einer Terminalserver-Umgebung außer Betrieb genommen werden, ist eine sorgfältige Planung der notwendigen Schritte unerlässlich.

Analog zu der Maßnahme M 2.320 *Geregelte Außerbetriebnahme eines Servers* ist daher sicherzustellen, dass

- keine wichtigen Daten innerhalb der Terminalserver-Umgebung verloren gehen,
- keine Anwendungen, Clients oder nachgelagerte Dienste beeinträchtigt werden, die mit den Applikationsservern verbunden sind und
- keine sensitiven Daten auf den Datenträgern der Terminalserver- und Client-Infrastruktur zurückbleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf dem System gespeichert sind und von wo aus darauf zugegriffen wird. Im Folgenden werden daher an dieser Stelle die zu berücksichtigen Punkte aus M 2.320 *Geregelte Außerbetriebnahme eines Servers* in Bezug auf Terminalserver-Umgebungen konkretisiert.

- Umfang der Datensicherung:
  Folgende Informationen sollten regelmäßig gesichert werden:
  - Benutzerprofile
  - Auf dem Lizenzserver hinterlegte Informationen
  - Authentisierungsinformationen
  - die Konfiguration der Sitzungsdatenbank (Session Directory) falls vorhanden
  - die Konfiguration des Independent Management Architecture (IMA) Datenspeichers bei Citrix Systemen
  - eingesetzte Verwaltungswerkzeuge
  - eventuell vorhandene vorher definierte, geprüfte und funktionstüchtige Systemzustände des Terminalservers
  - eventuell vorhandene vorher definierte, geprüfte und funktionstüchtige Systemzustände des Clients
- Ersatzsystem
  Für die Wartung und Aussonderung von Terminalservern in einer Terminalserver-Farm ist die Definition einer Standardarchitektur sinnvoll. Dies bedeutet, das innerhalb einer Terminalserver-Farm nur gleichartige Server-Hardware mit einem identischen Softwarestand eingesetzt werden. IT-Systeme, die auf einer Standardarchitektur basieren, haben den Vorteil, dass handelsübliche Ersatzsysteme und Ersatzteile beschafft oder auf Vorrat gekauft werden können. Im Falle eines Defekts kann das defekte Gerät kostengünstig und zeitnah ausgetauscht werden.
- Information der Benutzer
  Die Benutzer sollten darüber informiert werden, wie und wann der Terminalserver außer Betrieb genommen werden soll. Haben die Benutzer noch Sitzungen auf dem Terminalserver geöffnet, müssen sie aufgefordert werden, diese vorher zu beenden.

- Entfernen von Verweisen auf das System
  Damit der Terminalserver abgeschaltet werden kann, muss vorher verhindert werden, dass die Benutzer sich an dem System anmelden können, damit keine Sitzung abrupt beim Ausschalten beendet wird. Werden, um die Last gleichmäßig auf verschiedene Terminalserver zu verteilen, Loadbalancer oder andere interne Lastverteilungssysteme eingesetzt, sollte im Vorfeld der abzuschaltende Terminalserver aus den vorhandenen Lastverteilungsplänen ausgetragen werden.
- Löschen der Daten auf dem abzuschaltenden System
  Um zu vermeiden, dass sensible Information von unberechtigten Personen eingesehen werden können, sollten folgende Informationen von dem Terminalserver gelöscht werden:
  - Benutzerprofile
  - Authentisierungsinformationen
  - Zertifikate
- Wenn nicht nur einzelne Terminalserver, sondern die gesamte Terminalserver-Umgebung entfernt werden soll, sind folgende Informationen zu löschen:
  - Sensible Daten in der Sitzungsdatenbank,
  - Independent Management Architecture (IMA) Datenspeicher bei Citrix Systemen,
  - Zone Data Collector (ZDC) bei Citrix Systemen,
  - jegliche temporäre Dateien wie Bitmaps auf den Clients und jegliche Caches.
- Löschen von Datensicherungsmedien
  Es wird empfohlen, nach der Außerbetriebnahme alle Datensicherungsmedien zu löschen. Eine Ausnahme bilden Datensicherungen von Terminalservern, die redundant eingesetzt werden oder die anderen Terminalservern gleichen. In diesem Fall kann es unter Umständen zu einem späteren Zeitpunkt nötig sein, die gesicherten Informationen auf den verbleibenden Terminalservern zurückzuspielen.
- Entfernen sonstiger Information
  Bevor ein Terminalserver entsorgt wird, sollten Komponenten, wie USB-Sticks und Speicher-Karten entfernt und Informationen, die nicht auf den Festplatten gespeichert sind, gelöscht werden. Hierzu gehören z. B. Preboot eXecution Environment (PXE)-Informationen und BIOS-Einträge. Auch Fernwartungskarten und Beschriftungen sollten entfernt werden.

Prüffragen:

- Gibt es Regelungen für die Außerbetriebnahme des Terminalservers?
- Wurden die Benutzer vor der Außerbetriebnahme der Terminalserver informiert, ihre Sitzungen zu beenden?
- Falls sich auf den Terminalservern Daten der Benutzer befinden, wurden diese zuvor gesichert?
- Wurden die Terminalserver, die ausgesondert werden sollen, aus den Lastverteilungsplänen entfernt?
- Wurden alle vertraulichen Daten auf den Datenträgern vor einer eventuellen Aussonderung der Terminalserver vernichtet?

# M 2.470 Durchführung einer Anforderungsanalyse für TK-Anlagen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bevor eine TK-Anlage beschafft oder eine bestehende Anlage erweitert wird, ist es sinnvoll eine Anforderungsanalyse durchzuführen. In deren Rahmen muss zunächst die grundsätzliche Frage geklärt werden, welche Funktionen die TK-Anlage neben der reinen Telefonie bieten muss. Darüber hinaus ist das Einsatzszenario der TK-Anlage zu klären. Denkbar ist die Installation einer TK-Anlage beispielsweise für reinen Kundenkontakt, für die bürointerne Kommunikation oder für die Nutzung in einem Call Center. Einsatzszenarien können klären, welche Kommunikationsdienste sinnvollerweise benötigt werden. Für die Auswahl einer TK-Anlage spielt weiterhin die Anzahl der Endgeräte und die Anzahl der gleichzeitig nutzbaren Verbindungen eine Rolle. Das Ergebnis soll die Planung und damit die Auswahl einer für die Institution passenden und sicheren TK-Anlage ermöglichen.

Die Ergebnisse der Anforderungsanalyse müssen dokumentiert und mit den entsprechenden IT-Verantwortlichen abgestimmt werden.

Im Rahmen der Anforderungsanalyse müssen unter anderem folgende Punkte geklärt werden:

- In welcher Ausprägung soll die TK-Anlage genutzt werden: als klassische TK-Anlage, als VoIP-System oder als Hybrid-Anlage? Oder ist ein IP-Anlagenanschluss eine mögliche Alternative?
- Wie viele interne und wie viele externe Anschlüsse soll die TK-Anlage verwalten können? Lässt sich diese Anzahl nach dem Kauf noch erhöhen?
- Wie wird die Anbindung ans öffentliche Telefonnetz (PSTN) erfolgen? Ist die Zahl der gleichzeitig zu führenden Gespräche festgelegt (ISDN bzw. S2m-Leitungen) oder soll diese variabel nach Bedarf gestaltet werden können (IP-Anlagenanschluss)?
- Wie viele interne Kommunikationsverbindungen sollen gleichzeitig möglich sein?
- Welche Aufgaben soll die zu planende TK-Anlage erfüllen? Welche Funktionen sollen bereitgestellt werden? Gibt es Funktionen, die in jedem Fall bereit gestellt werden müssen?
- Können vorhandene Endgeräte alle geforderten Funktionen im Zusammenspiel mit der TK-Anlage am Arbeitsplatz zur Verfügung stellen oder müssen neue Endgeräte beschafft werden?
- Genügt eine eventuell bereits vorhandene Verkabelung den Anforderungen der TK-Anlage oder muss die Verkabelung erneuert werden?
- Soll eine TK-Anlage neu beschafft oder kann eine bestehende TK-Anlage erweitert werden?
- Gibt es besondere Anforderungen an die Verfügbarkeit der TK-Anlage oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Bietet die TK-Anlage die Möglichkeit, nachträglich weitere Funktionen zu implementieren (Hard-, Soft- und/oder Firmware)?
- Ist eine Kommunikation zwischen mehreren TK-Anlagen geplant, um verschiedene Standorte oder Niederlassungen der Institution miteinander zu verbinden? Sind diese vorhandenen TK-Anlagen mit der neu zu planen-

den kompatibel, so dass alle geforderten Funktionen unternehmensweit zur Verfügung stehen?
- Wie wird die Sicherheit der TK-Anlage (Zutritt und Zugriff), des Telefonnetzes und der Endgeräte gewährleistet?
- Ist ein Service- oder Wartungsvertrag für die TK-Anlage notwendig? Sind eine zeitnahe Reparatur und Störungsbehebung möglich?

Auf Grundlage der Ergebnisse sind die Anforderungen an die TK-Anlage zu definieren und festzulegen. Zusätzliche Marktanalysen und eventuell die Beratung externer Fachfirmen helfen, aus den Anforderungen eine konkrete Planung auszuarbeiten und die für die Institution passende TK-Anlage zu beschaffen. Vertiefende Informationen sind in den Maßnahmen M 2.471 *Planung des Einsatzes von TK-Anlagen* und M 2.105 *Beschaffung von TK-Anlagen* zu finden.

Prüffragen:

- Wurden die Anforderungen bei dem Einsatz der TK-Anlage berücksichtigt?
- Wurden die Anforderungen der TK-Anlagen mit den IT-Verantwortlichen abgestimmt?

# M 2.471 Planung des Einsatzes von TK-Anlagen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Vor der Planung des Einsatzes einer TK-Anlage ist eine umfangreiche Analyse durchzuführen, in der die wichtigsten Anforderungen an eine TK-Anlage festgelegt werden (siehe M 2.470 *Durchführung einer Anforderungsanalyse für TK-Anlagen*).

Eine grundlegende Voraussetzung für den sicheren Einsatz von TK-Anlagen ist eine angemessene Planung im Vorfeld. Der Einsatz von TK-Anlagen kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs geplant werden: Ausgehend vom Gesamtsystem werden konkrete Planungen für Teilkomponenten durchgeführt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

Es ist daher sinnvoll, das eventuell vorhandene Telekommunikationssystem der Institution mit seinen Funktionen detailliert zu erfassen. Zusätzlich ist es notwendig, einen Überblick über die am Telekommunikationssystem angeschlossenen Komponenten zu erhalten.

Von grundlegender Bedeutung ist auch die, in der Anforderungsanalyse bestimmte Betriebsart der TK-Anlage als klassische TK-Anlage, VoIP-Anlage, hybride TK-Anlage oder IP-Anlagenanschluss.

Die nachfolgenden Aspekte sollten bei der Planung des Einsatzes von TK-Anlagen berücksichtigt werden:

### Richtlinien für die Nutzung

Um TK-Anlagen sicher und effektiv einsetzen zu können, müssen Sicherheitsvorgaben erstellt werden, die auf den vorhandenen Sicherheitszielen basieren. Außerdem sollen Anforderungen aus den geplanten Einsatzszenarien mit einbezogen werden. Diese spezifischen Sicherheitsvorgaben müssen mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein (siehe dazu auch M 2.472 *Erstellung einer Sicherheitsrichtlinie für TK-Anlagen*).

### Ausstattungsmerkmale/Endgeräte

Je nach Nutzung der TK-Anlage muss festgelegt werden, welche Endgeräte benötigt werden. Neben der klassischen Funktion der Sprachtelefonie bieten schon einfache TK-Anlagen eine Reihe von komfortablen Ausstattungsmerkmalen. Dabei wird sowohl bei klassischen als auch bei hybriden TK-Anlagen zwischen analogen und digitalen Geräten und den Gerätetypen wie Modem, Fax sowie schnurlosen und schnurgebundenen Telefonen unterschieden. Die Auswahl sollte auch Bedieneigenschaften, Bedienkomfort und Geräteeigenschaften berücksichtigen. So können bei den Telefonen beispielsweise je nach konkretem Einsatzbereich auch Headsets oder ganz einfache Geräte ausgewählt werden.

### Leistungsmerkmale

TK-Anlagen bieten eine Vielzahl von Leistungsmerkmalen. Diese können sicherheitsrelevante Aspekte beinhalten, die beachtet werden müssen. So ge-

hören zu den sicherheitskritischen Leistungsmerkmalen beispielsweise das Aufschalten, bei dem weitere Gesprächsteilnehmer zu einem bestehenden Telefongespräch hinzugefügt werden können, die Konferenzschaltung, bei der mehrere Teilnehmer gleichzeitig miteinander über die Anlage miteinander telefonieren, und das Heranholen eines ankommenden Telefongespräches von einem fremden auf das eigene Telefon. Während der Planung des Einsatzes ist zu entscheiden, welche der von der TK-Anlage bereitgestellten Leistungsmerkmale verwendet werden sollen.

**Zuständigkeiten**

Da bei der Nutzung von TK-Anlagen eine Vielzahl von Komponenten benötigt werden, ist zu klären, welche Organisationseinheiten für welche Aufgaben zuständig sind, also beispielsweise, wer sich um Beschaffung und Einrichtung von Hardware, Softwareupdates, Benutzerkennungen oder Benutzerbetreuung kümmert. Es ist auch zu klären, ob eventuell eine Betreuung durch einen externen Support erfolgen soll.

**Berechtigungskonzept**

Aufgrund der ausgewählten Leistungsmerkmale sollten in einem Rollenkonzept die Berechtigungen zur Nutzung festgelegt werden wie beispielsweise:

- Wer darf welche Funktionen und Kommunikationsdienste nutzen?
- Wer entscheidet darüber, wie der in der TK-Anlage integrierte Anrufbeantworter besprochen wird und wer darf wann welche Aufnahmen löschen?
- Wer kümmert sich um eine musikalische Ansage in der Warteschleife oder um die automatische Weiterleitung?
- Werden die Endgeräte zentral durch einen Administrator konfiguriert oder erhält jeder Benutzer eigene Berechtigungen?

**Administration und Konfiguration**

Die mit dem Berechtigungskonzept gestarteten Überlegungen zur Konfiguration und Administration der TK-Anlage müssen verfeinert werden. Es muss überlegt werden, wie das System administriert werden soll und welche Einstellungen über ein zentrales Administrations- und Konfigurationsmanagement und welche lokal an den Endgeräten vorgenommen werden. Zentrale Aufgaben wären beispielsweise das Anbinden zusätzlicher Gerätetypen, die Einrichtung von Notruf- und Sondernummern sowie die Adressbuchverwaltung beziehungsweise die Anbindung von Verzeichnisdiensten wie LDAP. An den Endgeräten könnten lokal Klingeltöne, Tastensperren, die Belegung von Funktionstasten oder private Telefonbücher eingestellt werden.

Zu klären ist weiterhin, wer für die Administration der TK-Anlage und ihrer Komponenten verantwortlich ist. Dazu gehören auch Aufgaben wie beispielsweise das Aufspielen von Patches oder Updates auf ein Teilsystem, die Einführung neuer Benutzergruppen, Änderungen der Rechte und in der Zusammensetzung von Benutzergruppen, die Aktivierung neuer Funktionen der TK-Anlage und Konfigurationsänderungen, die über eine einfache Benutzerverwaltung hinausgehen. Die TK-Anlage ist in das Patch- und Änderungsmanagement der Institution einzugliedern (siehe B 1.14 *Patch- und Änderungsmanagement*).

Änderungen an der Konfiguration der TK-Anlage sollten protokolliert werden, so das sie zu einem späteren Zeitpunkt nachvollziehbar sind (siehe auch M 4.5 *Protokollierung bei TK-Anlagen*).

**Protokollierung**

In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal in der Anlage oder auf einem zentralen Server im Netz gespeichert werden sollen. Auch bei einem IP-Anlagenanschluss muss eine Protokollierung möglich sein. Sinnvollerweise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Daten ausgewertet werden. Hierbei ist zu prüfen, inwieweit das Datenschutzgesetz zu beachten ist und welche Konsequenzen daraus zu ziehen sind.

Eine TK-Anlage liefert im Allgemeinen Protokolldaten zu Zeiten und Rufnummern abgehender und ankommender Telefonate. Mit diesen Daten können beispielsweise Telefonate an Kostenstellen verrechnet werden. Die Daten können mithilfe entsprechender Software gesichert werden.

**Datensicherung**

Die Konfigurationen, die aktuellen Versionen der verwendeten Programme und die Protokolldaten der TK-Anlage und deren Komponenten sollten regelmäßig gesichert werden, um bei Ausfällen in kurzer Zeit ein Ersatzsystem bereitstellen zu können. Sicherungszeitpunkte und -formen sollten festgelegt werden, um den Anforderungen an den maximal tolerablen Datenverlust gerecht zu werden. Die entsprechenden Festlegungen sind in einen Gesamt-Datensicherungsplan des zentralen IT-Bereichs aufzunehmen, siehe dazu auch Maßnahme M 6.26 *Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten*.

**Notfallvorsorge**

Um schnell und effektiv auf Probleme zu reagieren, müssen die organisatorischen Rahmenbedingungen geschaffen werden, um in Notfällen schnell auf alternative Kommunikationskanäle umschalten oder Notrufe absetzen zu können. Dabei ist auch auf die Schulung aller Mitarbeiter zu achten. Sie müssen für mögliche Gefährdungen der TK-Anlage sensibilisiert, auf mögliche Warnanzeigen, -symbole und -töne hingewiesen und in die Bedienung der entsprechenden Kommunikationsdienste eingewiesen werden. Nicht nur für die Geschäftsprozesse ist die Verfügbarkeit der Telekommunikation eine wichtige Voraussetzung. Daher müssen entsprechende Vorkehrungen getroffen werden. Weitere Informationen hierzu sind in der Maßnahme M 6.145 *Notfallvorsorge für TK-Anlagen* zu finden.

Die Planung muss der Leitungsebene zur Entscheidung vorgelegt und alle Entscheidungen nachvollziehbar dokumentiert werden.

Prüffragen:

- Sind alle Planungen bezüglich der TK-Anlage nachvollziehbar dokumentiert worden?

# M 2.472 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die Sicherheitsvorgaben für die TK-Anlage der Institution ergeben sich aus der organisationsweiten Sicherheitsrichtlinie. Ausgehend von dieser allgemeinen Richtlinie müssen die Anforderungen konkretisiert und in einer Sicherheitsrichtlinie für die TK-Anlage zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben wie beispielsweise zur Nutzung von VoIP (Voice-over-IP) zu berücksichtigen sind.

Die Sicherheitsrichtlinie sollte grundlegende Aussagen zur Verfügbarkeit der TK-Anlage sowie zur Vertraulichkeit und Integrität der gespeicherten oder verarbeiteten Daten treffen. Dabei ist zu beachten, dass für Kommunikationsdienste grundsätzlich hohe Erwartungen an die Verfügbarkeit und auch in die Vertraulichkeit gesetzt werden. Bei der Speicherung von personenbezogenen Daten müssen auch Aspekte wie Datenschutz und Aufbewahrungspflichten für Daten berücksichtigt werden. Letztere dienen als Basis für Sicherheitsanalysen im Verdachts- oder Revisionsfall.

Die Sicherheitsrichtlinie für TK-Anlagen muss allen Personen und Gruppen, die an der Beschaffung, dem Aufbau, der Umsetzung und dem Betrieb der TK-Anlage beteiligt sind, bekannt sein und die Grundlage für deren Arbeit darstellen. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Im Rahmen der Sicherheitsrichtlinie für TK-Anlagen sollten die Benutzer in kurzer, verständlicher Form über die Gefährdungen informiert werden, die mit der Nutzung einer TK-Anlage und ihrer Kommunikationsdienste verbunden sind (siehe auch M 3.82 *Schulung zur sicheren Nutzung von TK-Anlagen*). Dabei sollten auch immer aktuelle Entwicklungen im Bereich der Technik und neu bekannt gewordenen Gefahren berücksichtigt werden. Diese Informationen sollen die Benutzer sensibilisieren und motivieren, diese Richtlinie auch einzuhalten.

Neben den Leistungsmerkmalen einer klassischen TK-Anlage wie beispielsweise Makeln, Rückfrage, Rückruf bei Besetzt, Anklopfen und auch Aufschalten auf ein bestehendes Gespräch, Konferenzschaltung und Heranholen eines Gespräches, verfügen Hybrid-Anlagen und VoIP-Anlagen durch die Kopplung von Eigenschaften der klassischen TK-Anlage und von IT-Systemen zusätzlich über eine Vielzahl von weiteren IT-basierten Funktionen. Beispielsweise können Sprachnachrichten und Faxe über E-Mail übertragen, Anrufe per Mausklick von einer Anwendung am PC initiiert und vermittelt und die aktuelle Verfügbarkeit eines Teilnehmers angezeigt werden. In der Richtlinie sollte daher festgelegt werden, welche Funktionen und Leistungsmerkmale der TK-Anlage genutzt werden sollen. Zusätzlich muss festgelegt werden, wer für welche Zwecke welche Dienste benutzen darf. In diesem Zusammenhang ist ebenfalls der Umfang der privaten Nutzung festzulegen.

Weiterhin müssen Sicherheitsmaßnahmen beachtet werden, welche die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der TK-Anlage und ihrer Endgeräte regeln. Bei Nutzung einer Hybrid-Anlage oder eines VoIP-Systems sind dies zusätzlich die für diese Systeme geltenden Richtlinien. In einigen Fällen kann es zweckmäßig sein, dass Benutzer bestimmte Konfigurationseinstellungen, wie beispielsweise das Sperren des Telefonendgeräts bei Abwesenheit, direkt am Endgerät selbst vornehmen dürfen. Dies sollte in den Richtlinien vermerkt, anderenfalls untersagt werden.

Sinnvoll ist es weiterhin, beispielsweise folgende Punkte in die Richtlinien mit aufzunehmen:

- Regelungen zur physikalischen Zugriffskontrolle:
  Eine TK-Anlage sollte grundsätzlich in einem separaten Sicherheitsbereich, wie zum Beispiel in einem abschließbaren Rechnerraum aufgestellt werden. Dabei ist zu regeln, wer Zutritt zu dem Raum beziehungsweise Zugriff auf die Anlage selbst erhalten soll. Der Zugang zur Administration, der in der Regel über eine Administrations-SW aber auch über separate Endgeräte erfolgen kann, sollte auf das TK-Betriebspersonal beschränkt sein (siehe auch M 2.27 *Wartung einer TK-Anlage* ).
- Regelungen für die Arbeit der Administratoren:
  Festzulegen ist, nach welchem Schema die Administrationsrechte vergeben werden. Es ist dabei zu überlegen, ob die Aufgabenbereiche des Administrators für die IT-Systeme von denen des Verantwortlichen für die TK-Anlage getrennt werden. Es ist darzulegen, welcher Administrator welche Rechte ausüben darf und wie er diese Rechte erlangt. In einem weiteren Schritt müssen die Zugangswege bestimmt werden, über die die Administratoren auf die Systeme zugreifen. Denkbar ist der lokale Zugriff an der TK-Anlage selbst, über ein eigenes Administrationsnetz oder über die Fernwartungsschnittstelle (siehe auch M 5.14 *Absicherung interner Remote-Zugänge von TK-Anlagen* und M 5.15 *Absicherung externer Remote-Zugänge von TK-Anlagen*).

Zusätzlich muss geregelt werden, welche Vorgänge dokumentiert werden müssen und in welcher Form die Dokumentation erstellt und gepflegt wird. Dazu gehören die folgenden Vorgaben für die Installation und Konfiguration:

- Vorgehen bei der Installation der gesamten TK-Anlage und der Endgeräte,
- Überprüfung und gegebenenfalls Änderung der Default-Einstellungen hinsichtlich ihrer Sicherheitsgefährdungen sowie die Änderung der Standard-Passwörter,
- Verwendung und Konfiguration der TK-Anlage und Endgeräte,
- Dokumentation und Sicherung der Konfiguration.

Es sollten Vorgaben für den sicheren Betrieb gemacht werden, wie beispielsweise:

- Absicherung der Administration (Technische Beschränkung des Zugangs zur Administration auf das TK-Betriebspersonal),
- Logging aller Anmeldeversuche an der TK-Anlage, Protokollierung und regelmäßige Kontrolle von Fernwartungszugriffen,
- erlaubte Werkzeuge für Betrieb und Wartung,
- Abschaltung sonstiger, nicht zur Verwendung vorgesehener Zugriffsmöglichkeiten,
- Vergabe von Berechtigungen,
- Vorgehensweisen bei Software-Updates und Konfigurationsänderungen,
- Datensicherung und Wiederherstellung,

- Regelungen für die Reaktion auf Betriebsstörungen, technische Fehler (lokaler Support, Fernwartung) und Sicherheitsvorfälle.

Auch auf die sichere Entsorgung der Komponenten der TK-Anlage sollte in der Sicherheitsrichtlinie hingewiesen werden. So werden zum Teil Verbindungsdaten und andere personenbezogene Daten auf Datenträgern in der TK-Anlage gespeichert. Endgeräte sind häufig von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Die einzelnen Komponenten müssen so vernichtet werden, dass eine Rekonstruktion der Daten nicht möglich ist.

Die Verantwortung für die Umsetzung der Sicherheitsrichtlinie für TK-Anlagen liegt beim IT-Betrieb, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsbeauftragten erfolgen.

Prüffragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für TK-Anlagen?
- Ist die Sicherheitsrichtlinie für TK-Anlagen allen Mitarbeitern bekannt gemacht worden?

# M 2.473 Auswahl von TK-Diensteanbietern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** TK-Anlagen-Verantwortlicher, Administrator, Leiter IT

Fast immer ist es nötig, dass die Anwender mit anderen Personen telefonieren können, deren TK-Endgeräte nicht an der eigenen TK-Anlage angeschlossen. Beispiele hierfür sind

Um mit Personen telefonieren zu können, die nicht an der institutionseigenen TK-Anlage angeschlossen sind (beispielsweise Endgeräte in anderen Standorten der Institution, Mobiltelefone und externe Gesprächspartner), muss die TK-Anlage über eine Teilnehmeranschlussleitung (TAL, auch "letzte Meile") an das PSTN (Public Switched Telephone Network) angeschlossen werden. Hierfür muss ein TK-Diensteanbieter ("Service Provider") beauftragt werden.

Der TK-Diensteanbieter stellt die physische Verbindung zwischen der TK-Anlage der Institution und dem PSTN bereit, und regelt auch den Anschluss an das PSTN. Eine Ausnahme bilden IP-Anlagenanschlüsse, bei denen ausschließlich Internetverbindungen genutzt werden und der Anschluss an das PSTN komplett beim TK-Diensteanbieter liegt. Da die externen TK-Verbindungen über den TK-Diensteanbieter übermittelt werden, ist die Auswahl des Anbieters, der bereitgestellten Dienste und die Anzahl der gleichzeitig nutzbaren Verbindungen wichtig.

Für die Auswahl können folgende Anforderungen berücksichtigt werden:

- Anschlussart
  Soll die TK-Anlage mit einem oder mehreren ISDN-Basisanschlüssen oder S2m-Primärmultiplexanschlüssen an das PSTN angeschlossen werden? Ist ein IP-Anlagenanschluss möglich?
- Standortvernetzung
  Wie werden die TK-Anlagen unterschiedlicher Standorte verbunden?
- Referenzinstallationen bzw. -kunden
  Hat der TK-Diensteanbieter Erfahrungen mit Institutionen, deren Anforderungen sich mit den eigenen Anforderungen decken?
- Größe und Qualität des Serviceteams
  Wie schnell können die Techniker vor Ort sein? Welche Reaktionszeit garantiert der Anbieter?
- Hardware
  Wird zusätzliche Hardware beim Kunden benötigt? Kann diese gekauft oder gemietet werden? Welche Outsourcing- und Service-Verträge gibt es?
- Kapazität
  Kann der Anbieter nachweislich die geforderte Anzahl an ausgehenden Leitungen bereitstellen?
- Redundante Leitungen
  Kann die TK-Anlage für einen hohen Schutzbedarf bezüglich der Verfügbarkeit redundant über mehrere physisch unabhängige Leitungen und Trassen an das PSTN angebunden werden?

Neben den Sicherheitsaspekten, sollten auch vertragliche und finanzielle Aspekte berücksichtigt werden:

- Vertragliche Bindung an den Anbieter

Wie lange ist der Kunde an den Anbieter gebunden? Wie lange sind die Kündigungsfristen? Kann zu einem späteren Zeitpunkt problemlos zu einem anderen Anbieter gewechselt werden?

- Flexibilität und Bereitschaft
  Hat der TK-Diensteanbieter in der Vergangenheit regelmäßig neue Produkte, Serviceideen und Tarife eingeführt? Wird dem Kunden ermöglicht, einzelne Produkte oder Dienste nacheinander einzuführen?
- Tarifmodelle
  Gibt es Tarifmodelle die dem Nutzungsverhalten der Institution entgegenkommen, wie beispielsweise Festpreise ("Flatrate") oder gestaffelte Preise? Gibt es spezielle Tarifoptionen für günstige Auslandsgespräche, wenn oft mit Gesprächspartnern im Ausland telefoniert werden soll? Mit welcher Taktung werden die Gespräche abgerechnet (sekunden- oder minutengenau)?

Alle vereinbarten Leistungen müssen genau und eindeutig schriftlich festgehalten werden.

Prüffragen:

- Sind alle Vereinbarungen mit TK-Dienstleistern schriftlich fixiert?

# M 2.474 Sichere Außerbetriebnahme von TK-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auf einigen Komponenten von TK-Anlagen werden während des Betriebs vertrauliche Informationen gespeichert, zu denen personenbezogene Daten, wie beispielsweise Telefonbücher, Kontaktdaten sowie Verbindungsdaten zählen.

Bei WLAN-Komponenten gehören dazu insbesondere die Authentifizierungsinformationen für den Zugang zum WLAN (vergleiche M 2.390 *Außerbetriebnahme von WLAN-Komponenten*). Auf VoIP-Komponenten können je nach Einsatzzweck eine Vielzahl verschiedener sensibler Informationen gespeichert sein. Dazu gehören beispielsweise IP-Adressen und weitere Informationen, die auf den Netzaufbau schließen lassen sowie organisationsweite Telefonverzeichnisse mit allen Mitarbeitern (M 2.377 *Sichere Außerbetriebnahme von VoIP-Komponenten*).

Lokal auf den verschiedenen Komponenten gespeicherten Daten, die noch benötigt werden, sollten entweder extern gesichert oder archiviert (beispielsweise auf Magnetbändern, CD- oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.

Sollen Komponenten außer Betrieb genommen oder ersetzt werden, ist darauf zu achten, dass Datenträger wie Festplatten, auf denen personenbezogenen Daten gespeichert werden, sicher entsorgt werden. Dies gilt besonders dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben (beispielsweise verkauft) werden. Auch wenn ein Gerät im Rahmen eines Garantieaustausches oder einer Reparatur an den Hersteller oder eine Service-Firma übergeben wird, müssen die vertraulichen Daten vorher unlesbar gemacht werden.

Hierfür sollten die Datenträger entweder physisch zerstört oder die Daten auf dem Datenträger so gelöscht werden, dass eine Rekonstruktion nicht möglich ist (siehe dazu auch den Baustein B 1.15 *Löschen und Vernichten von Daten*).

Oft sind die Komponenten zusätzlich von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Zusätzlich muss darauf geachtet werden, dass den auszusondernden Komponenten die Berechtigungen entzogen werden, um eine unbefugte Verwendungen zu verhindern.

Auf die sichere Entsorgung der Komponenten des Telekommunikationssystems sollte auch in der Sicherheitsrichtlinie hingewiesen werden.

Prüffragen:

- Werden die Daten auf den entsprechenden Komponenten der TK-Anlage vor der Entsorgung sicher gelöscht?
- Ist die sichere Entsorgung von Komponenten der TK-Anlage in der entsprechenden Sicherheitsrichtlinie berücksichtigt?

# M 2.475 Vertragsgestaltung bei Bestellung eines externen IT-Sicherheitsbeauftragten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung

Falls ein externer IT-Sicherheitsbeauftragter bestellt wird, sind die folgenden Hinweise zu beachten.

Insbesondere in kleinen Unternehmen oder Behörden kann es unter Umständen zweckmäßig sein, die Rolle des IT-Sicherheitsbeauftragten nicht durch einen eigenen Mitarbeiter zu besetzen, sondern auf die Dienstleistung eines externen IT-Sicherheitsbeauftragten zurückzugreifen. Hierzu muss zunächst ein geeigneter, qualifizierter Experte für Informationssicherheit ausgewählt werden. Hinweise zu den notwendigen Qualifikationen, zur Funktion und zu den Aufgaben eines IT-Sicherheitsbeauftragten finden sich im BSI-Standard 100-2 sowie in der Maßnahme M 2.193 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit*.

Bevor ein externer IT-Sicherheitsbeauftragter bestellt wird, ist zwischen dem Dienstleister und der eigenen Institution ein Vertrag zu schließen, in dem die Aufgaben des externen IT-Sicherheitsbeauftragten sowie die gegenseitigen Rechte und Pflichten möglichst präzise geregelt werden müssen. Die Beauftragung eines externen IT-Sicherheitsbeauftragten ist somit eine besondere Form des Outsourcings.

Folgende Aspekte sollten in dem Vertrag mindestens geregelt werden:

- Anforderungen an die Qualifikation des externen IT-Sicherheitsbeauftragten
- Vertretungsregelungen und Mindest-Ressourcen
- Aufgaben, die der externe IT-Sicherheitsbeauftragte übernehmen muss
- Melde-, Berichts- und Eskalationswege, Ansprechpartner (Rollen)
- Einbindung in Kommunikationskanäle der beauftragenden Institution
- Arbeitsorte, Räumlichkeiten und Anwesenheits- bzw. Erreichbarkeitszeiten
- Zutritts-, Zugangs- und Zugriffsrechte
- Vortragsrechte und Berichtspflichten gegenüber der Leitungsebene der beauftragenden Institution
- Mitwirkungspflichten des Auftraggebers
- Vertraulichkeitsvereinbarung
- Interessenskonflikte
- Folgen bei Vertragsverstößen
- Regelungen zur Beendigung des Vertragsverhältnisses, z. B. Übergabe von Aufgaben und Unterlagen
- Kosten

Durch den Vertrag muss der externe IT-Sicherheitsbeauftragte in die Pflicht und in die Lage versetzt werden, seine Aufgaben mindestens so gut wie ein interner IT-Sicherheitsbeauftragter zu erfüllen.

Falls auf die Dienstleistung eines externen IT-Sicherheitsbeauftragten zurückgegriffen wird, ist auch der Baustein B 1.11 *Outsourcing* anzuwenden. Zu beachten ist insbesondere die Maßnahme M 2.226 *Regelungen für den Einsatz von Fremdpersonal*.

Prüffragen:

- Falls ein externer IT-Sicherheitsbeauftragter bestellt wurde: Umfasst der hierzu geschlossene Dienstleistungsvertrag alle Aufgaben des IT-Sicherheitsbeauftragten sowie die damit verbundenen Rechte und Pflichten?
- Falls ein externer IT-Sicherheitsbeauftragter bestellt wurde: Verfügt der IT-Sicherheitsbeauftragte über die notwendigen Qualifikationen?
- Falls ein externer IT-Sicherheitsbeauftragter bestellt wurde: Ermöglicht der hierzu geschlossene Dienstleistungsvertrag eine kontrollierte Beendigung des Vertragsverhältnisses einschließlich Übergabe der Aufgaben an den Auftraggeber?
- Falls ein externer IT-Sicherheitsbeauftragter bestellt wurde: Umfasst der hierzu geschlossene Dienstleistungsvertrag eine geeignete Vertraulichkeitsvereinbarung?

# M 2.476 Konzeption für die sichere Internet-Anbindung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

In den verschiedenen Arten von Institutionen finden sich verschiedenste Varianten der internen und externen Vernetzung. Nahezu überall gehört dazu auch die Anbindung der internen IT-Systeme und Netze ans Internet. Jeder Anschluss an offene externe Netze birgt aber auch Gefahren, da dieser ein potentielles Einfallstor für Schadsoftware, Angriffsversuche aller Art und Datenabflüsse sein kann. Die Art der Internet-Anbindung und deren zuverlässige Absicherung muss daher sorgfältig konzeptioniert werden. Ebenso sollte jede neue Variante der Internet-Nutzung sorgfältig geplant sowie alle IT-Komponenten und ihre Vernetzung sicher installiert und konfiguriert werden.

In einer Konzeption für die sichere Internet-Anbindung muss zunächst geklärt werden, wie die internen IT-Systeme zu schützen sind. Die Rahmenbedingungen zur Internet-Nutzung, also beispielsweise wer welche Internet-Dienste nutzen darf und welche Regelungen dabei zu beachten sind, sind ebenso zu klären (siehe M 2.457 *Konzeption für die sichere Internet-Nutzung*). Dabei muss auch abgestimmt werden, welche Arten von Internet-Kommunikation und welche Internet-Dienste generell zugelassen werden (siehe auch M 2.459 *Überblick über Internet-Dienste*). Je nach den Zielen, die die Institution mit der Internet-Nutzung verbindet, ändern sich auch die Anforderungen an die Internet-Anbindung, z. B. erfordert der Betrieb eines Webservers eine höhere Bandbreite und Verfügbarkeit der Internet-Anbindung als sporadische Informationssuche über Webdienste.

Die Konzeption muss in die allgemeine Sicherheitsstrategie der jeweiligen Institution eingebettet sein und daher mit dem Informationssicherheitsmanagement abgestimmt werden.

### Organisation

Bei der Internet-Nutzung wird eine Vielzahl von IT-Komponenten benötigt. Daher ist zu klären, welche Organisationseinheiten für welche Aufgaben in diesem Zusammenhang zuständig sind, also z. B. Einrichtung von Benutzerkennungen, Benutzerbetreuung oder Redaktion für das Webangebot. Um schnell und effektiv auf Probleme reagieren zu können, ist die Festlegung der organisatorischen Rahmenbedingungen ebenfalls erforderlich, z. B. um einen Internetdienst in Notfällen schnell abschalten zu können.

Um einen geeigneten Internet Service Provider (ISP) und eine zweckmäßige Anschlusstechnik auswählen zu können, sollten weiterhin die benötigten Bandbreiten und Antwortzeiten für die einzelnen Internet-Dienste dokumentiert werden (siehe M 2.176 *Geeignete Auswahl eines Internet Service Providers*).

Im Rahmen der Anpassung der Netzstruktur muss geklärt werden, welche anderen Systeme und welche Netzverbindungen durch die Internet-Nutzung beeinträchtigt werden könnten. Weiterhin sollte festgelegt werden, wie mit Daten aus dem Internet, z. B. heruntergeladenen Dateien, umgegangen wird, ob diese z. B. auf anderen Systemen weiterverarbeitet werden dürfen oder archiviert werden müssen.

Hinsichtlich der Sicherheitsanforderungen sollte im Konzept festgelegt werden, ob die Informationen, die aus dem Internet abgerufen oder an andere Computer im Internet gesendet werden, gegen unbefugtes Mitlesen oder unerlaubte Veränderung geschützt werden müssen.

**Sichere Internet-Anbindung**

Sobald in einem lokalen Netz (LAN) auch Dienste wie das World Wide Web (WWW), E-Mail oder andere Internet-Dienste genutzt werden, muss das LAN an ein nicht vertrauenswürdiges Netz wie z. B. das Internet angeschlossen werden. Damit setzt eine Institution ihr bislang geschlossenes Netz erheblichen Gefährdungen aus, noch bevor die erste Anwendung installiert und genutzt wird. Angreifer aus dem Internet könnten versuchen, Schwachstellen der grundlegenden Internet-Protokolle, -Dienste und -Komponenten auszunutzen und den Datenverkehr abzuhören (Sniffing), Absenderangaben zu fälschen (Spoofing) oder in das interne Netz einzudringen.

Durch eine robuste Netzanbindung, eine geeignete Geräteauswahl, sichere Konfigurationseinstellungen und einen kontrollierten Betrieb kann diesen Gefährdungen begegnet werden. Um das LAN mit einem nicht vertrauenswürdigen Netz zu koppeln, kann eine Architektur gewählt werden, die aus vier Zonen besteht:

- Die erste Zone umfasst das interne Netz. Sie enthält alle Client-Systeme sowie alle Infrastruktur- und Anwendungsserver, die für den autonomen, lokalen LAN-Betrieb benötigt werden.
- In der zweiten Zone befindet sich das Sicherheitsgateway (siehe B 3.301 *Sicherheitsgateway (Firewall)*), das das LAN vor Angriffen aus dem Internet schützt. Des Weiteren sind hier die erforderlichen Server zum Anbieten von Diensten im Internet untergebracht, die wiederum durch Paketfilter abgesichert werden, sich also in sogenannten Demilitarisierten Zonen befinden.
  Mittels einer Demilitarisierten Zone (DMZ), einem Zwischennetz, das an Netzübergängen gebildet wird, können die internen Netzstrukturen geschützt werden. Es können nur kontrollierte Zugriffe auf die daran angeschlossenen Server erfolgen. Dienste können so sowohl dem WAN als auch dem LAN zur Verfügung gestellt werden. Mit Hilfe von Proxy-Servern können die beiden Netze miteinander verbunden werden.
- Die dritte Zone umfasst die Komponenten zur Internet-Anbindung. Sie enthält im einfachsten Fall einen einzelnen Router, der mit dem Netz eines Internet-Diensteanbieters verbunden ist. Bei höheren Anforderungen an die Verfügbarkeit muss die Anbindung redundant ausgelegt werden.
- In der Management-Zone könnten alle Management-Daten zentral gesammelt und verarbeitet werden. Hier könnte auch ein Zeitserver untergebracht werden, mit dem sämtliche Systemuhren im Netz synchronisiert werden.

Alle weiteren Aspekte sollten bereits mit dem Verhalten des Sicherheitsgateways festgelegt worden sein, siehe dazu M 2.71 *Festlegung einer Policy für ein Sicherheitsgateway*.

**Aktualität**

Die Konzeption für die Internet-Anbindung muss regelmäßig aktualisiert werden, mindestens einmal jährlich, da sich dieser Bereich sehr dynamisch entwickelt. Auch sollte die Entwicklung und Aktualisierung der Konzeption zur Internet-Anbindung Hand in Hand mit der Entwicklung des Konzepts für Sicher-

heitsgateways erfolgen (siehe M 2.70 *Entwicklung eines Konzepts für Sicherheitsgateways*), um eine sichere Anbindung an das Internet zu gewährleisten.

Bei Änderungen in den Zielen, der Strategien oder der Gefährdungslage der Institution muss geprüft werden, welche Auswirkungen diese auf die Internet-Anbindung haben.

Prüffragen:

- Ist eine aktuelle Konzeption für die Internet-Anbindung vorhanden?
- Wird das Konzept für die Internet-Anbindung regelmäßig überprüft und falls erforderlich angepasst?

# M 2.477 Planung einer virtuellen Infrastruktur

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Aufgrund der hohen Komplexität ist eine detaillierte Planung beim Aufbau einer virtuellen Infrastruktur unerlässlich. Daher sollte schon bei einer konzeptionellen Betrachtung und im Vorfeld einer Projektierung eine genaue Analyse der notwendigen Rahmenbedingungen durchgeführt werden.

**Festlegung der Virtualisierungstechnik**

In einem ersten Planungsschritt ist daher unter Berücksichtigung der für eine Virtualisierung infrage kommenden IT-Systeme festzulegen, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) die virtuelle Infrastruktur basieren soll. Hierbei sind im Wesentlichen folgende Kriterien heranzuziehen:

- Die Servervirtualisierung, bei der ein vollständiger Server mit all seinen Hardwarekomponenten virtuell dargestellt wird, eignet sich besonders gut für den Betrieb von sehr unterschiedlichen virtuellen IT-Systemen mit stark variierenden Aufgaben. Bei Systemen auf der Basis einer Servervirtualisierung ist es möglich, unterschiedliche Betriebssysteme (Windows, Linux, Solaris) in den virtuellen IT-Systemen gleichzeitig auf einem Virtualisierungsserver zu betreiben, da jedes virtuelle System seinen eigenen Betriebssystemkern nutzen kann. Mit Hilfe der Servervirtualisierung kann eine sehr starke Kapselung der virtuellen IT-Systeme erreicht werden. Dies bedeutet, dass das virtuelle IT-System beispielsweise keine Betriebssystemkomponenten oder Softwarebibliotheken des Virtualisierungsservers oder anderer virtueller IT-Systeme nutzt. Weiterhin sind bei der Servervirtualisierung die virtuellen Systeme stärker voneinander isoliert als bei der Betriebssystemvirtualisierung, d. h. eine wechselseitige funktionale Beeinflussung ist weitgehend ausgeschlossen.
- Mittels der Betriebssystemvirtualisierung können auf einfache Weise große Mengen gleichartiger Server auf einem Virtualisierungsserver betrieben werden. Mit der Betriebssystemvirtualisierung können daher hohe Verdichtungsgrade (Verhältnis von virtualisierten IT-Systemen zu Virtualisierungsservern) erreicht werden. Es ist allerdings mit der Betriebssystemvirtualisierung in der Regel nicht möglich, unterschiedliche Betriebssysteme auf einem Server als virtuelle Systeme zu betreiben, da die virtuellen IT-Systeme meist den Betriebssystemkern und die Softwarebibliotheken des Virtualisierungsservers nutzen. In Grenzen ist dies bei einigen Produkten innerhalb einer Betriebssystemfamilie möglich. Beispielsweise ermöglicht *Parallels Virtuozzo* die Nutzung unterschiedlicher Editionen des Betriebssystems *Microsoft Windows Server 2003*. Die virtuellen IT-Systeme sind untereinander nicht so stark isoliert wie bei der Servervirtualisierung. Beispielsweise werden Softwarebibliotheken gemeinsam genutzt und die virtuellen IT-Systeme nutzen den selben Betriebssystemkern. Die Kapselung der virtuellen IT-Systeme ist meist gar nicht vorhanden oder nur sehr schwach ausgeprägt, da sie Soft- und Hardwarekomponenten des Virtualisierungsservers mit nutzen.

Diese schwache Kapselung der virtuellen IT-Systeme bei der Betriebssystemvirtualisierung führt dazu, dass virtuelle IT-Systeme mit stark unterschiedlichen Anforderungen an den Schutzbedarf nicht ohne Weiteres gemeinsam auf einem Virtualisierungsserver betrieben werden können. Dies ist bei Virtua-

lisierungslösungen auf Basis einer Servervirtualisierung in der Regel anders, da die Kapselung der virtuellen Systeme stärker ausgeprägt ist. Ob allerdings virtuelle IT-Systeme mit unterschiedlichem Schutzbedarfs auf einem Virtualisierungsserver zusammen betrieben werden können, hängt neben dem verwendeten Produkt auch von den individuellen Gefährdungen und Anforderungen der Organisation bzw. der virtuellen IT-Systeme ab. Daher ist bei der Planung zu bewerten, inwieweit die in Frage kommende Virtualisierungstechnik dafür geeignet ist, virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver gemeinsam zu betreiben.

**Auswahl eines Virtualisierungsproduktes**

Ist die Virtualisierungstechnik ausgewählt, müssen konkrete Virtualisierungsprodukte geprüft werden, ob sie für den konkreten Anwendungsfall geeignet sind. Die hierbei zu berücksichtigenden Anforderungen leiten sich dabei aus den innerhalb der virtuellen Umgebung benötigten Prozessorarten sowie deren Funktionen und der Verfügbarkeit von erforderlichen Geräteemulationen oder Schnittstellen ab.

In einer möglichst frühen Planungsphase muss geprüft und entschieden werden, mit welcher Technik virtuelle IT-Systeme mit dem Netz des Rechenzentrums verbunden werden sollen: Entweder durch eine direkte Zuordnung von physischen Netzkarten des Servers zu den virtuellen IT-Systemen oder die Verbindung der virtuellen Systeme über einen so genannten virtuellen Switch. Auf dieser Basis kann festgelegt werden, wie Regelungen und Richtlinien umgesetzt werden können, die auf der Basis der Maßnahmen M 2.141 *Entwicklung eines Netzkonzeptes*, M 5.61 *Geeignete physische Segmentierung* sowie M 5.62 *Geeignete logische Segmentierung* entwickelt worden sind. Hierdurch ergeben sich schon frühzeitig Vorgaben für den Aufbau der Virtualisierungsserver und der dazugehörigen Infrastruktur.

Sind die Anforderungen an die Zielumgebung geklärt, können eine passende Virtualisierungslösung und hierzu kompatible physische IT-Systeme ausgewählt werden.

**Rechenzentrumsübergreifende Planung**

Auf Virtualisierungsservern können eine Vielzahl von virtuellen IT-Systemen betrieben werden. Auf diesen virtuellen IT-Systemen, in der Regel Serversysteme mit unterschiedlichen Betriebssystemen, können weiterhin eine große Anzahl von verschiedenen Applikationen ausgeführt werden. Diese Applikationen wiederum benötigen in der Regel grundlegende Dienste wie DNS, Verzeichnisdienste zur Authentisierung oder Datenbanken. Daher müssen die Virtualisierungsserver auf alle Ressourcen zugreifen können, die für den Betrieb der Virtualisierungsserver selbst sowie der virtuellen IT-Systeme nötig sind. Die folgenden Anforderungen müssen bei der Planung eines Virtualisierungsprojektes beachtet werden. Die Virtualisierungsserver benötigen

- physische Verbindungen in alle Netze, in denen virtuelle IT-Systeme betrieben werden sollen.
- Verbindungen in Speichernetze zum Zugriff auf Massenspeicherkomponenten.
- Zugriff auf Infrastruktursysteme wie DNS-, DHCP- und Verzeichnisdienstserver.

Daher sollten alle Administratorengruppen, die mit der Bereitstellung dieser Dienste beauftragt sind, bei der Einführung der Virtualisierung angemessen beteiligt werden, damit diese ihre Kenntnisse einbringen und ihrerseits Anforderungen an das Virtualisierungsprojekt formulieren können.

**Planung der Rollen und Verantwortlichkeiten**

Da die Virtualisierungsserver häufig den Zugriff der virtuellen IT-Systeme und der darauf betriebenen Applikationen auf grundlegende Dienste des Rechenzentrums, sowie Netze und Speichernetze bereitstellen, sind sie aus der Sicht der virtuellen IT-Systeme selbst Bestandteil der Rechenzentrumsinfrastruktur. Daher wird empfohlen, für den Zugriff auf Netze und Speichernetze existierende Regelungen und Richtlinien an die Erfordernisse der virtuellen Infrastruktur anzupassen. Werden zum Beispiel gemäß M 5.130 *Absicherung des SANs durch Segmentierung* Vorgaben zur Segmentierung des Speichernetzes und zur Zugriffsregelung auf Speicherressourcen gemacht, muss sichergestellt sein, dass diese auch innerhalb der virtuellen Infrastruktur umgesetzt werden können. Der Zugriff auf Speicherressourcen muss für die Virtualisierungsserver möglicherweise weiter gefasst werden, da diese auf die Speicherressourcen vieler virtueller IT-Systeme zugreifen können müssen, damit sie wiederum selbst den virtuellen IT-Systemen Ressourcen zur Verfügung stellen können. Trotzdem sind die Anforderungen der angegebenen Maßnahme im Rahmen des Bausteins B 3.303 *Speicherlösungen / Cloud Storage* umzusetzen. Die Umsetzung muss hier jedoch mit den Mitteln der verwendeten Virtualisierungslösung möglich sein. Dies zeigt, dass durch die Administratoren der Virtualisierungsserver möglicherweise Aufgaben wahrgenommen werden müssen, die vorher durch die Administratoren des Speichernetzes bzw. der Speicherkomponenten darin ausgeführt wurden.

Gleiches gilt für die Aufgaben der Netzadministration. Die Verbindung von virtuellen IT-Systemen zu den unterschiedlichen Netzen des Informationsverbunds wird auf einem Virtualisierungsserver durch dessen Administratoren festgelegt, da sie die virtuellen IT-Systeme den physischen Netzverbindungen des Virtualisierungsservers zuordnen. Dies ist traditionell eine Aufgabe der Netzadministratoren. Sollen auf einem Virtualisierungsserver virtuelle IT-Systeme in unterschiedlichen Netzen betrieben werden, muss die Verantwortung für die richtige Netzzuordnung und die Überwachung dieser Zuordnung durch die Administratoren der Virtualisierungsserver übernommen werden. Zusätzlich muss berücksichtigt werden, dass das mit der Segmentierung des Netzes verfolgte Ziel, die Sicherheit durch Aufteilung der IT-Systeme auf verschiedene Bereiche des Rechenzentrums zu steigern, durch eine fehlende Kapselung und Isolation der virtuellen IT-Systeme auf dem Virtualisierungsserver nicht unterlaufen werden kann.

Es muss daher bei der Planung einer virtuellen Infrastruktur entschieden werden, wie die Aufgaben der Netz- und Speichernetzadministratoren, falls bei der gewählten Virtualisierungslösung notwendig, von den Administratoren der Virtualisierungsserver wahrgenommen werden sollen. Weiterhin ist zu prüfen, ob die Aufgaben der Verwaltung von Netz- und Speichernetzverbindungen durch die Administratoren der Virtualisierungsserver an die Netz- und Speichernetzadministratoren delegiert werden können. Die Betriebsverantwortung für die Umsetzung von bestehenden Regelungen und Richtlinien muss eindeutig und klar festgelegt werden.

**Anpassung der Infrastruktur an die Virtualisierung**

In klassischen Informationsverbünden sind IT-Systeme wie Server meist mit nur einem, seltener mit mehreren Netzen verbunden. Ein Virtualisierungsserver muss jedoch mit mehreren Netzen verbunden sein, wenn auf diesem Server virtuelle IT-Systeme in unterschiedlichen Netzen betrieben werden sollen.

Daher wird empfohlen, die Umsetzung der folgenden Maßnahmen aus dem Baustein B 4.1 *Lokale Netze* und B 3.302 *Router und Switches*

- M 2.141 *Entwicklung eines Netzkonzeptes*,
- M 2.142 *Entwicklung eines Netz-Realisierungsplans*,
- M 5.61 *Geeignete physische Segmentierung*,
- M 5.62 *Geeignete logische Segmentierung*,
- M 5.77 *Bildung von Teilnetzen*,
- M 4.81 *Audit und Protokollierung der Aktivitäten im Netz*und
- M 4.206 *Sicherung von Switch-Ports*

an die Besonderheiten und Erfordernisse der Virtualisierungsserver anzupassen. Es muss darauf geachtet werden, dass die Virtualisierungsserver in einer virtuellen Infrastruktur alle Verbindungsanforderungen der virtuellen IT-Systeme erfüllen können.

Werden beispielsweise MAC-Filter auf Switch-Ports (siehe auch M 4.206 *Sicherung von Switch-Ports*) eingesetzt, muss die Konfiguration dieser Filter an die Erfordernisse der virtuellen Infrastruktur angepasst werden. Wenn das nicht der Fall ist, können virtuelle IT-Systeme, die bei einigen Virtualisierungslösungen eine eigene MAC-Adresse besitzen, nicht von einem Virtualisierungsserver auf einen anderen verschoben werden. Da diese Funktion möglicherweise für die Verteilung von virtuellen IT-Systemen auf Virtualisierungsserver benötigt wird, um auf Performance-Engpässe zu reagieren, ist ohne geeignete Anpassungen der Filterregeln die Verfügbarkeit von virtuellen IT-Systemen gefährdet.

Auch bei der Umsetzung der folgenden Maßnahmen aus dem Baustein B 3.303 *Speichersysteme und Speichernetze* müssen gegebenenfalls Anforderungen, die sich aus der Nutzung von Virtualisierungstechniken ergeben, berücksichtigt werden:

- M 2.525 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen*
- M 5.130 *Absicherung des SANs durch Segmentierung*
- M 4.275 *Sicherer Betrieb einer Speicherlösung*

**Einsatzplanung für Virtualisierungsserver**

Bei der Einsatzplanung müssen neben der Umsetzung der Maßnahme M 2.315 *Planung des Servereinsatzes* einige Besonderheiten beachtet werden. Diese Besonderheiten ergeben sich daraus, dass auf einem Virtualisierungsserver in der Regel mehrere virtuelle IT-Systeme betrieben werden sollen. Es muss daher ermittelt werden, wie viel Prozessorleistung, Hauptspeicher und Festplattenplatz für den Betrieb der virtuellen IT-Systeme benötigt wird. Weiterhin muss festgelegt werden, welche Netzverbindungen für die Virtualisierungsserver und die virtuellen IT-Systeme benötigt werden (siehe auch M 5.135 *Sicherer Medientransport mit SRTP*).

Für die Auswahl geeigneter Virtualisierungsserver sind die Gesamtanforderungen bezüglich Performance und Ressourcenverbrauch für die geplanten virtuellen IT-Systeme zu ermitteln. Hierdurch erst kann die Anzahl und die benötigte Leistungsfähigkeit der Virtualisierungsserver festgelegt werden.

Bei einer Migration bereits produktiv betriebener physischer IT-Systeme in virtuelle Umgebungen sollte zudem der tatsächliche Ressourcenbedarf nicht einfach durch Addition der Ressourcen der zu virtualisierenden IT-Systeme ermittelt werden. Stattdessen empfiehlt es sich, die Performance der zu virtualisierenden Systeme zu messen und die Anforderungen an die Virtualisierungsserver auf Basis der erforderlichen Performancewerte der gemessenen physischen Server festzulegen.

Neben ausreichenden Ressourcen für die individuellen virtuellen Maschinen müssen darüber hinaus weitere Kapazitäten in der virtuellen Infrastruktur vorgehalten werden, die durch die Virtualisierungssoftware selbst benötigt werden. So entsteht ein zusätzlicher Bedarf an Massenspeicherkapazität etwa für die Speicherung von Snapshots, Ereignisprotokollen und Auslagerungsdateien des Virtualisierungsservers. Weiterhin benötigt der Hypervisor eines Virtualisierungsservers ebenfalls Prozessorkapazität und Hauptspeicherplatz.

In Test- und Entwicklungsumgebungen kann von den obigen Vorgaben abgewichen werden. Es ist bei der Planung solcher Umgebungen darauf zu achten, dass sich keine unerwünschten Wechselwirkungen mit Produktivsystemen ergeben. Daher sind Test- und Entwicklungsumgebungen hinreichend von Produktivumgebungen abzuschotten.

**Verfügbarkeit der virtuellen Infrastruktur**

Es wird empfohlen, in der Planungsphase schon zu berücksichtigen, dass für die Virtualisierungsserver möglicherweise höhere Anforderungen an die Verfügbarkeit bestehen, da auf Virtualisierungsservern eine große Zahl an IT-Systemen betrieben wird. Fällt ein Virtualisierungsserver aus, sind auch alle darauf laufenden virtuellen IT-Systeme nicht mehr lauffähig. Dadurch übertragen sich alle Verfügbarkeitsanforderungen der einzelnen virtualisierten IT-Systeme auf den Virtualisierungsserver (*Kumulationsprinzip*). Es ist ratsam, zu prüfen, ob für Virtualisierungsserver eine hochverfügbare oder fehlertolerante Architektur gewählt werden sollte, oder ob in einer aus mehreren Virtualisierungsservern aufgebauten virtuellen Infrastruktur Mechanismen existieren, die den Ausfall eines oder mehrerer Virtualisierungsserver kompensieren.

Prüffragen:

- Steht die Vorgehensweise zur Nutzung von Virtualisierungsservern und virtuellen IT-Systemen in Einklang mit den Regelungen und Richtlinien für den Betrieb von IT-Systemen, Applikationen, Netzen und Speichernetzen?
- Sind die Aufgaben der einzelnen Administratorengruppen (Anwendungs-, Server-, Netz- und Speichernetzadministratoren) klar voneinander abgegrenzt?
- Ist die Betriebsverantwortung für die einzelnen Komponenten einer virtuellen Infrastruktur (Virtualisierungsserver, virtuelle IT-Systeme, Speichernetz, Netz) klar geregelt und können die jeweiligen Verantwortlichen ihre Aufgabe auch technisch wahrnehmen?
- Enthält die virtuelle Infrastruktur ausreichend Redundanzen, um den Verfügbarkeitsanforderungen Rechnung zu tragen?

# M 2.478 Planung des sicheren Einsatzes von Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die geregelte und sichere Einführung von Mac OS X setzt eine umfangreiche Planung voraus. In dieser Maßnahme wird auf softwaretechnische Aspekte eingegangen, um eine reibungslose Projektumsetzung zu ermöglichen. Die verwendeten Hardwarekomponenten in einem Mac-System sind von Apple vorgegeben und daher überschaubar. Beim Prozessor besteht jedoch ein gravierender Unterschied zwischen den früheren und den aktuell verwendeten Mac-Systemen. Mac OS X unterstützt ab der Version Snow Leopard (10.6) keine PowerPC-Prozessoren mehr. Eine Installation von Mac OS X 10.6 auf älteren Apple-Computern ohne Intel-CPU ist nicht möglich. Wird von PowerPC-basierten Apple Computern zu Apple Computern mit Intel-Prozessor gewechselt, muss im Vorfeld geprüft werden, ob es sich um "Universal"-Anwendungen handelt, also Anwendungen, die sowohl auf PowerPC-Prozessoren als auch auf Intel-Prozessoren ausführbar sind.

Bei einem Plattformwechsel von einem anderen Betriebssystem zu Mac OS X muss ebenfalls im Vorfeld geprüft werden, ob gleiche oder gleichwertige Anwendungen für Mac OS X zur Verfügung stehen und ob diese zu bestehenden Systemen (wie einem Lotus Domino-Server oder Microsoft Exchange-Server) kompatibel sind. Dies betrifft nicht nur die Anwendungen, die direkt auf dem Client betrieben werden, sondern auch serverbasierte Anwendungen, mit bestimmten Voraussetzungen. Zum Beispiel benötigen bestimmte webbasierte Anwendungen ActiveX. ActiveX steht unter Mac OS X nicht zur Verfügung. Vorhandene Software, die nicht kompatibel zu Mac OS X ist, kann mithilfe einer Software-Virtualisierungslösung betrieben werden. Jedoch ist dies nur als Notlösung anzusehen, da zum einen höhere Ansprüche an die Hardware gestellt werden und es um ein Vielfaches komplexer ist, eine Anwendung in einer virtualisierten Umgebung zu betreiben.

Generell sollte geprüft werden, ob bestehende Software-Lizenzverträge auch Mac OS X Systeme abdecken. Falls nicht, sollte in zukünftigen Lizenzverträgen nach Möglichkeit darauf geachtet werden, dass Software gewählt wird, die auf verschiedenen Plattformen betrieben werden kann bzw. deren Lizenzverträge den Einsatz auf anderen Plattformen gestatten.

Bei der Einführung von Mac OS X Systemen muss ebenfalls geprüft werden, ob bestehende externe Hardware, wie zum Beispiel Drucker, Plotter, Kartenlesegeräte oder sonstige benötigte Geräte kompatibel zu Mac OS X sind und entsprechende Gerätetreiber zur Verfügung stehen. Ebenfalls muss geprüft werden, ob die eingesetzten Netzprotokolle von Mac OS X unterstützt werden, um eine Verbindung zwischen unterschiedlichen IT-Systemen herstellen zu können. Wird zum Beispiel das "Andrew File System"-Protokoll (AFS) als verteiltes Netz-Dateisystem verwendet, muss im Vorfeld ein geeigneter Client für Mac OS X gewählt werden.

**Benutzerkonzept**

Ein Benutzerkonzept legt fest, mit welchen Rechten die Benutzer bestimmte Arbeiten verrichten können. Bei der Planung des Benutzerkonzepts ist zwischen lokalen und domänenweiten Benutzerkonten zu unterscheiden. Sowohl bei lokalen als auch bei domänenweiten Benutzerkonten ist darauf zu achten, dass die Benutzerrechte möglichst restriktiv gewählt werden. So wird das mög-

liche Schadensmaß bei einer absichtlichen oder versehentlichen missbräuchlichen Nutzung des Benutzerkontos begrenzt. Unter Mac OS X ist für jeden Benutzer ein Konto mit Standardbenutzer-Rechten einzurichten, dass zum täglichen Arbeiten verwendet werden sollte.

Wenn die Clients unter Mac OS X in einen Verzeichnisdienst integriert werden, sollte B 5.15 *Allgemeiner Verzeichnisdienst* beachtet werden. Falls es sich um ein heterogenes Netz mit einem Windows-Server als Basis des Verzeichnisdienstes handelt, ist auch B 5.16 *Active Directory* zu beachten.

**Administrationskonzept**

Im Vorfeld der Einführung von Mac OS X ist ein Administrationskonzept zu erstellen, falls es noch nicht vorhanden ist. Es sind grundsätzlich zwei verschiedene Konten für die Administration vorzusehen.

Mac OS X unterscheidet zwischen Benutzer- und Administratorenkonten. Ein Benutzer, der unter einem Benutzerkonto angemeldet ist, kann keine Systemeinstellungen verändern, Applikationen in allgemein zugängliche Verzeichnisse installieren oder andere Benutzerkonten verwalten. Administratoren haben hingegen diese genannten Möglichkeiten. Soweit möglich, sollten die Administratoren für ihre Arbeit ein Konto mit den Privilegien eines Standardbenutzers verwenden. Nur wenn diese Privilegien nicht mehr ausreichend sind, sollte ein Konto mit administrativen Privilegien genutzt werden. Bei Mac OS X sind Aufgaben, die die erweiterten Rechte eines Administrators erfordern, durch das Symbol eines kleinen Vorhängeschlosses gekennzeichnet. Bei Klick auf das Schloss werden die Zugangsdaten des Administrators abgefragt, danach sind Änderungen mit administrativen Privilegien möglich. Nach der Erfüllung der Aufgaben sollte sich der Administrator durch einen weiteren Klick auf das Symbol wieder vom Konto mit administrativen Privilegien abmelden und mit dem Standardbenutzerkonto weiterarbeiten.

Als Besonderheit existiert bei Mac OS X zudem ein root-Konto, dass in der Standardeinstellung deaktiviert ist. Administratoren- und root-Konto unterscheiden sich dahingehend, dass ein Administratorkonto keine Berechtigung besitzt, um Informationen aus wichtigen Systemordnern zu löschen. Somit kann ein Administrator zwar viele Änderungen am System vornehmen, aber nicht das gesamte Betriebssystem komplett unbrauchbar machen.

Es ist jedoch möglich, mit einem Administratorenkonto das root-Konto zu aktivieren und zu nutzen. Die Deaktivierung des root-Kontos stellt also nur einen unvollständigen Schutz gegen das unbeabsichtigte Löschen von Systemdateien dar.

**Protokollierungskonzept**

Um Angriffe oder Unregelmäßigkeiten erkennen zu können, sollten die Protokollierungsmöglichkeiten des einzelnen Systems aktiviert und benutzt werden. Die Maßnahmen M 4.106 *Aktivieren der Systemprotokollierung* und M 4.25 *Einsatz der Protokollierung im Unix-System* sind ebenfalls für Mac OS X zutreffend, da es auf Unix basiert. Um sinnvoll zu protokollieren, sollte im Vorfeld überlegt werden, welche Programme auf dem Client unter Mac OS X eine bedeutende Rolle einnehmen. Allen geschäftskritischen Anwendungen sollte ein möglichst hohes Log-Level zugeordnet werden, dadurch können insbesondere alle (Warn-)Meldungen protokolliert werden. In einem Störfall stehen dann genug Informationen zur Fehlerbeseitigung zur Verfügung. Wird ein Client zum Beispiel hauptsächlich zum Versenden von E-Mail-Nachrichten

verwendet, sollten jegliche Hinweise bezüglich des E-Mail-Programms an eine zentrale Stelle weitergeleitet und ausgewertet werden.

**Datenablage, Datensicherung und Verschlüsselung**

Es ist festzulegen, wo die Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). Werden alle relevanten Daten auf Servern gespeichert, so kann auf Verschlüsselung der lokalen Festplatten des Client-Rechners verzichtet werden. Dadurch ist es auch möglich, Datensicherungen zentral durchzuführen, so dass auch auf lokale Datensicherungen verzichtet werden kann. Werden alle relevanten Daten auf Servern gespeichert, so kann auf Verschlüsselung der lokalen Festplatten des Client-Rechners verzichtet werden. Dadurch ist es außerdem auch möglich, Datensicherungen zentral durchzuführen, so dass auch auf lokale Datensicherungen verzichtet werden kann. Dieses Vorgehen ist jedoch stark von den lokalen Gegebenheiten abhängig. Wird zum Beispiel auf einem Client spezielle Software eingesetzt, die nach einem Defekt nur mit hohem Arbeitsaufwand wieder in Betrieb genommen werden kann, sollte eine Datensicherung des Clients in regelmäßigen Zyklen erfolgen. Weitere Informationen zum Thema Datensicherung finden sich in den Maßnahmen M 6.146 *Datensicherung und Wiederherstellung von Mac OS X Clients* und M 6.32 *Regelmäßige Datensicherung* sowie dem Baustein B 1.4 *Datensicherungskonzept*.

Werden mobile Computer eingesetzt, so ist zumindest eine temporäre lokale Datenhaltung erforderlich. Somit sollte die clientseitige Datenablage und ihr (kryptographischer) Schutz geplant werden (siehe M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme*). Ist eine Verschlüsselung des Benutzerverzeichnisses ausreichend, kann FileVault (siehe M 4.372 *Einsatz von FileVault unter Mac OS X*) verwendet werden. Werden sicherheitsrelevante Daten außerhalb des Benutzerlaufwerks abgelegt, sollten diese ebenfalls verschlüsselt werden. Weitere Informationen, wie Daten sicher abzulegen oder zu transportieren sind, sind in M 4.379 *Sichere Datenhaltung und sicherer Transport unter Mac OS X* zu finden. Bei höherem Schutzbedarf ist der hierdurch erreichte Schutz im Allgemeinen nicht ausreichend, so dass hier zusätzliche Sicherheitsapplikationen eingesetzt werden müssen, beispielsweise ein Verschlüsselungsprogramm, das die gesamte Festplatte des Clients verschlüsseln kann.

Prüffragen:

- Ist sichergestellt, dass Administratoren für alle nicht-administrativen Arbeiten ein Konto mit unprivilegierten Rechten benutzen?
- Gibt es ein Benutzer- und Administrationskonzept unter Mac OS X?
- Gibt es ein Protokollierungskonzept für Mac OS X genutzt?

# M 2.479 Planung der Sicherheitsrichtlinien von Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Eine der wichtigsten organisatorischen Aufgaben bei der Einführung von Mac OS X ist es, eine entsprechende Sicherheitsrichtlinie für Mac OS X zu planen und zu definieren. Diese Richtlinie sollte auf M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz* und legt die später umzusetzenden Sicherheitsbestimmungen für Mac OS X Clients fest.

Die Sicherheitsrichtlinie muss allen Anwendern und anderen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die in der Mac OS X Sicherheitsrichtlinie definierten Anforderungen werden durch die entsprechenden Sicherheitseinstellungen auf Betriebssystemebene umgesetzt. In Fällen, in denen technische Maßnahmen nicht ausreichen, müssen sie durch zusätzliche organisatorische Maßnahmen begleitet und unterstützt werden. Nach Möglichkeit sollte eine technische Lösung gegenüber einer organisatorischen den Vorzug bekommen.

Die zu erstellende Sicherheitsrichtlinie hat sich an den bisher geltenden Sicherheitsrichtlinien der jeweiligen Institution zu orientieren und darf diesen nicht widersprechen. In der Regel werden die existierenden Regelungen für Mac OS X angepasst oder sinngemäß erweitert. Dabei sind insbesondere spezifische Technologien von Mac OS X wie beispielsweise FileVault und Time Machine zu berücksichtigen. Generell gilt, dass sich die Planung der Mac OS X Infrastruktur an der jeweiligen übergreifenden Sicherheitsrichtlinie orientiert. Die Infrastruktur besitzt jedoch über einen Feedback-Prozess Einfluss auf diese übergreifende Sicherheitsrichtlinie. Nicht zuletzt ist beim Erstellen der Sicherheitsrichtlinie darauf zu achten, dass geltende rechtliche Bestimmungen berücksichtigt werden. Die Sicherheitsrichtlinie für Mac OS X ist zu dokumentieren und den Benutzern des Client-Server-Netzes im erforderlichen Umfang mitzuteilen. Alle Administratoren sollten die Sicherheitsrichtlinie kennen und umsetzen.

Die folgenden Themenbereiche geben einen Überblick über die abzudeckenden Bereiche einer solchen Richtlinie. Je nach Institution und umzusetzenden Einsatzszenarien müssen weitere Aspekte in Betracht gezogen werden.

**Konfigurations- und Administrationsstrategie**

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen wesentlich von dieser Festlegung abhängen.

Für Clients mit normalem Schutzbedarf kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Aber auch in diesen Fällen ist es empfehlenswert, die Strategie nur so liberal wie nötig auszulegen.

Bei Clients mit hohem Schutzbedarf wird grundsätzlich eine restriktive Strategie empfohlen. Für Clients mit besonderem Schutzbedarf bezüglich einem der drei Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

**Physische Sicherheit**

Die physische Sicherheit muss bei der Planung der Mac OS X Sicherheitsrichtlinie berücksichtigt werden, da diese Betriebssysteme auch auf mobilen Rechnern zum Einsatz kommen können. Es müssen die generellen Empfehlungen zu physischen Sicherheit aus den Baustein B 3.201 *Allgemeiner Client* umgesetzt werden.

**Verantwortlichkeiten**

Die Verantwortlichkeiten für den Betrieb der Mac OS X Systemen müssen durch die Mac OS X Sicherheitsrichtlinie geregelt werden.

Es ist festzulegen, welche Verantwortung die einzelnen Administratoren übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein, um:

- Sicherheitsparameter zu ändern,
- Protokolldaten auszuwerten,
- Zugriffsrechte und Systemberechtigungen zu vergeben,
- Passwörtern zu wechseln und zu hinterlegen sowie
- Datensicherungen und Datenwiederherstellungen durchzuführen.

Auch die Endbenutzer müssen in einem Client-Server-Netz Verantwortlichkeiten übernehmen, sofern sie administrative Tätigkeiten ausführen sollen. In der Regel beschränken sich diese Verantwortlichkeiten auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von den Voreinstellungen des übergeordneten Verzeichnisses übernommen werden. Die Endbenutzer müssen in der Anwendung der administrativen Tätigkeiten im Rahmen ihrer Verantwortlichkeit geschult werden.

Die Administration der Systeme sollte durch geschulte Netzadministratoren erfolgen, wobei im Rahmen der Notfallvorsorge für eine geeignete Stellvertreterregelung zu sorgen ist.

**Kommunikationssicherheit**

Auch Anforderungen an die Sicherheit bei der Datenübertragung müssen ein Bestandteil der Sicherheitsrichtlinie sein. Es ist empfehlenswert, Grundanforderungen an die Übertragungssicherheit in der Sicherheitsrichtlinie zu formulieren (Sollzustand) und anschließend Ausnahmen zu erfassen, die aufgrund lokaler Gegebenheiten notwendig sind. Dabei sind vor allem die Fragen der erforderlichen Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit zu berücksichtigen.

Es muss entschieden werden, welche Netzdienste des Mac OS X Systems für andere IT-Systeme bereitgestellt werden sollen. Jeder aktivierte Netzdienst kann ein Angriffsziel darstellen, daher sollte die Auswahl auf notwendige Netzdienste beschränkt werden. In M 5.165 *Deaktivieren nicht benötigter Mac OS X-Netzdienste* sind Empfehlungen zu finden, wie die nicht benötigten Netzdienste ausgeschaltet werden können.

Bei der Umsetzung der Anforderungen ist auch der mögliche Einsatz der Mac OS X-eigenen Desktop Firewall zu berücksichtigen (siehe M 5.166 *Konfiguration der Mac OS X Personal Firewall*).

**Verschlüsselung**

Es muss entschieden werden, ob und welche Informationen wie verschlüsselt werden sollen. Insbesondere auf mobilen IT-Systemen wird empfohlen, die Informationen zu verschlüsseln. Bestandteil von Mac OS X ist die Software FileVault, mit der Benutzerverzeichnisse durch Verschlüsselung geschützt werden können. Vertiefende Informationen zu FileVault sind in M 4.372 *Einsatz von FileVault unter Mac OS X* zu finden. Alternativ könnte die Festplatte durch Software von Drittanbietern vollständig verschlüsselt werden.

Beim Einsatz verschlüsselter Dateisysteme sollte ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden. Im Fall von Problemen wie dem Verlust des Schlüssels oder der Passphrase zum Schlüssel, inkorrekter Konfiguration oder Ähnlichem, könnten die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein.

**Datensicherung**

Um Datenverlusten entgegenzuwirken, müssen regelmäßig alle relevanten Informationen des Mac OS X Clients gesichert werden. Dazu sind Ort und Häufigkeit der Sicherung festzulegen. Diese Entscheidungen müssen in das organisationsweite Datensicherungskonzept eingebunden werden, beziehungsweise dürfen diesem nicht widersprechen. Die erstellten Datensicherungen müssen regelmäßig auf Fehler überprüft werden. Vertiefende Informationen zur Datensicherung unter Mac OS X sind unter M 6.146 *Datensicherung und Wiederherstellung von Mac OS X Clients* zu finden.

**Protokollierung**

Wie viele Unix-Systeme stellt Mac OS X sehr ausführliche Möglichkeiten zur Protokollierung sicherheitsrelevanter Ereignisse (erfolgreiche und/oder fehlgeschlagene Versuche) zur Verfügung. Im Vorfeld müssen folgende Fragen entschieden werden:

- Welche Ereignisse werden protokolliert?
- Wo werden die Protokolldateien gespeichert?
- Wie und in welchen Abständen werden die Protokolle ausgewertet?

Bei der Definition der Protokolleinstellungen ist das Gesamtkonzept der Systemüberwachung zu berücksichtigen. Vertiefende Informationen zur Protokollierung unter Unix-Systemen sind in M 4.106 *Aktivieren der Systemprotokollierung* und M 4.25 *Einsatz der Protokollierung im Unix-System* zu finden.

Prüffragen:

- Existiert eine Sicherheitsrichtlinie für Mac OS X?
- Orientiert sich die Sicherheitsrichtlinie für Mac OS X an den bisher geltenden Sicherheitsrichtlinien des jeweiligen Unternehmens bzw. der jeweiligen Behörde?
- Wurde die Sicherheitsrichtlinie im erforderlichen Umfang Mac OS X Benutzern bekannt gegeben?
- Sind alle relevanten Bereiche durch die Mac OS X Sicherheitsrichtlinie abgedeckt?

# M 2.480 Nutzung der Exchange- und Outlook-Dokumentation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Microsoft stellt eine Vielzahl von kostenlosen Informationen zentral über den Microsoft TechNet Service (http://technet.microsoft.com) zur Verfügung. Hier sind Dokumentationen, Online-Hilfen, Bedienungsanleitungen etc. zu Microsoft-Produkten erhältlich.

Das Microsoft TechNet verweist außerdem auf weitere Informationsquellen. Im Folgenden werden einige Beispiele genannt:

- Über das Microsoft TechNet werden Hinweise oder zusätzliche Software angeboten. Beachtet werden sollten vor allem die sicherheitsrelevanten Informationen, die hinter den Menüeinträgen zu "Security" zu finden sind. Wichtig sind außerdem die Microsoft Produkt-Sicherheitsleitfäden, die über das Downloadcenter angeboten werden. Im vorliegenden Kontext sind insbesondere die Sicherheitsleitfäden für "Messaging" und "Collaboration" relevant.
- Das Microsoft Developer Network (http://msdn.microsoft.com) ist als Informationsquelle für Entwickler gedacht. Hier ist eine kostenfreie Registrierung notwendig.

Für die Produkte der Exchange Server-Familie ist die aktuelle Online-Dokumentation versionsspezifisch im Microsoft TechNet abgelegt. Im Exchange Server TechCenter sind alle notwendigen Informationen abrufbar. Gleiches gilt für die Dokumentation zu Microsoft Outlook, welche im Office TechCenter zu finden ist.

Für die sicherheitsrelevanten Dokumente und Anleitungen sei auf das "Security Compliance Management Toolkit" verwiesen, welches die aktuellen Sicherheitsleitfäden, Hinweise zur sicheren Installation und Überwachung sowie weitere Dokumente und Hilfen anbietet.

Für Microsoft Exchange/Outlook 2010 bedeutet dies beispielhaft:

- Für die Version Microsoft Exchange Server 2010 sind relevante Dokumentationen, Downloads und Anleitungen im Exchange TechCenter (Stichwort Microsoft Exchange Server) zu finden.
- Besonders das Sicherheitshandbuch für Exchange 2010 (noch nicht veröffentlicht) ist für die sichere Installation und den Betrieb einer Exchange -Installation wichtig. Dieses Handbuch wurde für IT-Administratoren geschrieben, die für die Absicherung der Exchange 2010-Bereitstellung verantwortlich sind. Es ist dazu bestimmt, den IT-Administrator beim Verständnis und der Verwaltung der gesamten Sicherheitsumgebung zu unterstützen, in der Exchange installiert ist.
- Die aktuellste Version der Exchange Server 2010-Dokumentation wird unter "Exchange Server 2010 Home Page" zur Verfügung gestellt.
- Für die Version Microsoft Outlook 2010 sind relevante Dokumentationen, Downloads und Anleitungen im Outlook 2010 Ressource Kit ("Office 2010 Beta Resource Kit") zu finden. Aspekte zur Informationssicherheit werden unter "Security and protection for Office 2010 Beta" behandelt.

Prüffragen:

- Ist die aktuelle Online-Dokumentation zu Microsoft Exchange und Microsoft Outlook den Administratoren bekannt?

# M 2.481 Planung des Einsatzes von Exchange für Outlook Anywhere

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Outlook Anywhere ermöglicht Benutzern den Zugriff auf Exchange über das Internet. Es handelt sich dabei um einen serverseitigen Bereitstellungsdienst und nicht um eine Client-Software. Da der Datenverkehr im Internet anfälliger gegenüber Angriffen ist als der Datenverkehr in einem Intranet wird empfohlen, dass eine Sicherheitsstrategie gewählt wird, die so viele Sicherheitsoptionen wie möglich einbezieht.

### Verwenden von SSL für Outlook Anywhere

Wenn Outlook Anywhere für den Zugriff auf Exchange-Informationen aus dem Internet verwendet werden soll, dann muss ein gültiges SSL-Zertifikat (Secure Sockets Layer) installiert werden, das von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt wurde, die für das Betriebssystem des Clientcomputers vertrauenswürdig ist.

### Verwenden der SSL-Verschiebung für Outlook Anywhere

Bei dem Einsatz eines SSL-Proxies, der die SSL-Verschlüsselung des an den Clientzugriffsserver gerichteten Datenverkehrs übernimmt, muss die sogenannte SSL-Verschiebung für Outlook Anywhere korrekt konfiguriert werden. Dabei wird der SSL-Verbindungsaufbau komplett über den SSL-Proxy abgewickelt und wertvolle Bandbreite sowie Ressourcen eingespart.

### Konfigurieren der Authentisierung für Outlook Anywhere

Die zu verwendete Authentisierungsmethode für Outlook Anywhere muss ausgewählt werden. Es sollten nicht Standardauthentisierung und integrierte Windows-Authentisierung gleichzeitig konfiguriert sein, wobei letztere sicherer ist.

Die konkrete Umsetzung dieser Anforderungen sieht beispielsweise für die Version 2010 wie folgt aus:

- Für den sicheren Einsatz von Outlook Anywhere sind die Ausführungen auf den Microsoft Technet-Webseiten unter "Understanding Security for Outlook Anywhere: Exchange 2010 Help" zu berücksichtigen. Die Konfigurationseinstellungen sind unter "Managing Outlook Anywhere: Exchange 2010 Help" dokumentiert: Vorwiegend sind hier Aktivierung, Deaktivierung, Authentikation, SSL-Verschlüsselung und Zertifikatsmanagement im Fokus.

Prüffragen:

- Wird ein gültiges SSL-Zertifikat bei der Verwendung von Outlook Anywhere genutzt?
- Ist die SSL-Verschiebung bei Outlook Anywhere richtig konfiguriert?
- Wurde genau eine Authentisierungsmethode für Outlook Anywhere ausgewählt und konfiguriert?

# M 2.482 Regelmäßige Sicherheitsprüfungen für Exchange-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Revisor

Die Sicherheit eines Microsoft Exchange-Systems kann nur dann auf Dauer gewährleistet werden, wenn dieses regelmäßig auf Fehlkonfigurationen und Schwachstellen geprüft wird.

Sicherheitsprüfungen sollten in regelmäßigen Abständen durch unter-schiedliche Personen erfolgen. So sollten beispielsweise Administratoren in relativ kurzen Abständen (etwa monatlich) Kurzprüfungen durchführen. Es empfiehlt sich dabei, eine Prüfliste aufzubauen, damit ein definierter Prüfumfang gewährleistet ist. Festgestellte kleinere Probleme können meist sofort durch die Administratoren korrigiert werden, größere Probleme sind entsprechend der Prozessvorgaben weiter zumelden. In mittleren Zeitabständen (mehrere Monate) sollten Sicherheitsprüfungen durch andere, interne Rollen (z. B. Informationssicherheit, IT-Revision) erfolgen. In längeren Zeitabständen können dann auch Prüfungen durch externe Prüfer sinnvoll sein.

Folgende Aspekte sind bei Prüfungen zu berücksichtigen:

**Regelmäßige Recherche von sicherheitsrelevanten Informationen**

Generell müssen sich Administratoren und für die Informationssicherheit verantwortliche Personen regelmäßig über Neuerungen und Änderungen informieren, die die verantworteten Systeme betreffen. Dazu sind insbesondere die Microsoft-Informationsquellen regelmäßig zu sichten (siehe dazu auch M 2.480 *Nutzung der Exchange- und Outlook-Dokumentation*).

**Berechtigungen für Revisionsbenutzer**

Für das Benutzerkonto, das zur Prüfung der Systemkonfiguration durch externe Personen genutzt wird, sollten nur lesende Berechtigungen vergeben sein. Veränderungen dürfen durch den Revisionsbenutzer nicht durchgeführt werden. Können die Berechtigungen des Revisionsbenutzers nicht auf den lesenden Zugriff beschränkt werden, so darf der Zugriff nur im Vier-Augen-Prinzip erfolgen.

**Regelmäßige Prüfung der Berechtigungen**

Das vollständige Prüfen von Berechtigungen ist in der Regel aufgrund des Mengengerüstes eines Exchange-Systems nicht manuell möglich. Daher ist ein gutes Berechtigungskonzept unbedingt notwendig. Aber auch dann müssen die Berechtigungen regelmäßig auf Konsistenz mit dem Berechtigungskonzept geprüft werden. Hier können Stichproben für wichtige Benutzergruppen durchgeführt werden. Das Berechtigungskonzept muss sicherstellen, dass Prozesse aufgesetzt sind, die verhindern, dass Berechtigungen angesammelt werden.

Benutzerberechtigungen sollten regelmäßig geprüft werden. Folgende Informationen sind dabei sicherheitsrelevant:

- Benutzer mit kritischen Berechtigungen

Es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen.
- Änderungsbelege für Benutzer, Rollenzuordnungen, Rollen, Profile und Berechtigungen
- Hierbei ist insbesondere auf Änderungen an administrativen Objekten zu prüfen.

**Aktualität der Updates prüfen**

Für das Microsoft Exchange-System ist die Aktualität der installierten Updates zu prüfen. Der aktuelle Patch-Stand des Systems muss dann mit den verfügbaren Patches verglichen werden. Dies erfordert, dass dem Prüfer die von Microsoft verfügbaren Patches bekannt sind. Die Prüfung muss auch auf Fehler oder Warnungen bei Updates erfolgen.

**Sicherheit der Kommunikationsschnittstellen prüfen**

Die Sicherheit der unterschiedlichen Kommunikationsschnittstellen (siehe auch M 5.100 *Absicherung der Kommunikation von und zu Exchange-Systemen*) sollte geprüft werden. Hier ist insbesondere zu prüfen, wer administrative Berechtigungen besitzt und welche Dienste und Funktionen verfügbar sind.

Bei der Microsoft Exchange Version 2010 wird beispielsweise die Überwachung und Protokollierung eines Exchange Servers über das Microsoft Operations Framework (siehe Microsoft Technet "Monitoring and Operations Management: Exchange 2007 Help") analog Microsoft Exchange 2007 realisiert.

Prüffragen:

- Wird jedes Microsoft Exchange-System regelmäßig einer Sicherheitsprüfung unterzogen?
- Werden die Exchange-Berechtigungen regelmäßig mindestens stichprobenartig geprüft?
- Ist das Microsoft Exchange-System auf einem aktuellen Patch-Stand?

# M 2.483 Sicherheit beim Customizing von Exchange-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Im Rahmen des Customizings wird ein Groupware-System so konfiguriert und angepasst, dass es die spezifischen Anforderungen der Institution erfüllen kann. Diese Aufgabe ist in der Regel zeitaufwendig. Folgendes ist dabei aus Sicherheitssicht zu bedenken:

- Für das Customizing ist ein entsprechendes Konzept zu erstellen, das den gewünschten Soll-Zustand des Groupware-Systems möglichst genau beschreibt. In dem Konzept sind auch die Prozesse definiert, nach denen das Customizing durchgeführt wird. Das Konzept ist mit dem Informationssicherheitsmanagement abzustimmen.
- Das Customizing darf nur von sachkundigen und vertrauenswürdigen Personen durchgeführt werden.
- Anpassungen der Konfiguration des Groupware-Systems sollten nicht direkt im Produktiv-System erfolgen, sondern in einer Testumgebung.
- Im Rahmen des Customizing-Prozesses sind Rückmelde-Prozesse vorzusehen, die Anpassungen des Konzeptes während der Umsetzung (siehe auch M 4.162 *Sichere Konfiguration von Exchange-Servern*) erlauben

Wie die konkrete Umsetzung der Anforderungen aus dieser Maßnahme aussehen kann, ist beispielsweise für die Version 2010 im Microsoft Technet beschrieben. Eine angepasste Installation des Exchange Servers 2010 wird unter ""Perform a Custom Exchange 2010 Installation: Exchange 2010 Help" beschrieben. Nachträgliche Veränderungen werden unter "Modify or Remove Exchange 2010: Exchange 2010 Help" behandelt.

Prüffragen:

- Ist ein Customizing-Konzept für Microsoft Exchange erstellt worden?
- Wird das Customizing des Microsoft-Exchange-Systems durch geschultes Personal durchgeführt?
- Ist sichergestellt, dass beim Customizing Anpassungen und Änderungen nicht direkt im Produktivsystem vorgenommen werden?

# M 2.484 Planung von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Der Einsatz von OpenLDAP in einer Institution muss sorgfältig geplant werden. Der Planung des konkreten Einsatzes von OpenLDAP geht immer die Maßnahme M 2.403 *Planung des Einsatzes von Verzeichnisdiensten* voraus. Aus den im Rahmen dieser Maßnahme getroffenen Entscheidungen, insbesondere wie OpenLDAP genutzt werden soll, ergeben sich Anforderungen an OpenLDAP. Die konkrete Planung hängt auch von der verwendeten Infrastruktur ab. Wenn OpenLDAP geplant wird, sind mindestens die folgenden Punkte zu berücksichtigen:

- **Einbindung in andere Anwendungen**
  OpenLDAP besitzt zahlreiche Möglichkeiten, zur Unterstützung in Betriebssysteme und andere Anwendungen eingebunden zu werden, zum Beispiel:

  - zur Benutzerverwaltung in Unix- und Linux-Systemen über das Pluggable Authentication Module (PAM) und den Name Service Switch (NSS),
  - als zentraler Verzeichnisdienst in heterogenen Netzen oder zusammen mit Active Directory mittels Samba (siehe B 5.17 *Samba*) oder
  - als Adressbuch und Zertifikatsverzeichnis für E-Mail-Programme wie Microsoft Outlook oder Mozilla Thunderbird (siehe B 5.3 *Groupware*).

  Soll OpenLDAP gemeinsam mit anderen Anwendungen verwendet werden, so müssen die Planung, Konfiguration und Installation von Anwendungen und OpenLDAP unbedingt aufeinander abgestimmt werden. Im Rahmen der IT-Grundschutz-Systematik sind korrespondierende Maßnahmen parallel umzusetzen. Die "OpenLDAP Frequently Asked Questions" (http://www.openldap.org/faq) halten Informationen zur Anbindung an andere Anwendungen in einem eigenen Abschnitt unter *Faq-O-Matic* | *OpenLDAP Software FAQ* | *Integration* bereit.
- **Auflösung von Abhängigkeiten**
  Um alle Funktionen eines Verzeichnisdienstes gemäß des LDAPv3-Standards zu erfüllen, ist OpenLDAP darauf angewiesen, Funktionen weiterer Anwendungen zu nutzen. Dies gilt insbesondere für die zur Datenhaltung verwendete BerkeleyDB, für die OpenLDAP optimiert wurde. Nur mit dieser hierarchischen Datenbank verfügt OpenLDAP über seinen vollen Funktionsumfang. Dabei ist zu beachten, dass es sich bei BerkeleyDB und OpenLDAP um zwei unabhängig voneinander entwickelte Software-Anwendungen handelt. OpenLDAP benötigt eine unterstützte Version der BerkeleyDB.
  Einen Überblick über die unterstützten oder notwendigen Versionen der BerkeleyDB gibt der Anhang "Recommended Versions" des OpenLDAP Administrator's Guide (http://www.openldap.org/doc). Der Anhang gibt auch Auskunft über weitere Softwarepakete, von denen die Funktion von OpenLDAP abhängt. Deren Anforderungen sind zu beachten, besonders die Installation einer Transport Layer Security-Variante wie "OpenSSL" oder "GnuTLS" und die Installation des Simple Authentication and Security Layers "Cyrus-SASL". Die denkbare Alternative "GnuSASL" wird in der Version 2.4 noch nicht von OpenLDAP unterstützt. Ohne diese beiden unterstützenden Anwendungen kann OpenLDAP den LDAPv3-Standard nicht vollständig umsetzen. Soll die Authentisierung mit Kerberos abge-

sichert werden, ist eine Installation der Dienste "Heimdal Kerberos" oder "MIT Kerberos" nötig. Auf die im Anhang der Administrators Guide aufgeführte Software "TCP Wrappers" zur Absicherung der Kommunikation mit dem Verzeichnisdienst sollte zugunsten eines anderen IP-Filter-Mechanismus verzichtet werden (siehe M 4.238 *Einsatz eines lokalen Paketfilters*).

- **Auswahl der Konfigurationsmethode**
  OpenLDAP unterstützt seit der Version 2.3 zwei verschiedene Konfigurationsmethoden. Die klassische Konfiguration wird statisch in einer Konfigurationsdatei (slapd.conf) vorgenommen, die der Serverprozess "slapd" beim Start einliest. Die aktuellere Konfiguration wird auch als Online-Konfiguration bezeichnet und speichert Konfigurationseinstellungen in einem speziellen Bereich des Verzeichnisbaumes ("slapd-config"). Die Online-Konfiguration bietet mehrere Vorteile:

  - Änderungen der Online-Konfiguration erfolgen durch LDAP-Operationen und sind über eine Netzverbindung möglich, ohne Zugriff auf das Dateisystem des IT-Systems, auf dem OpenLDAP betrieben wird.
  - Die Administration ist mit einfach zu bedienenden grafischen LDAP-Clients durchführbar.
  - Einstellungen in der Online-Konfiguration können zur Laufzeit des Servers geändert werden und werden sofort wirksam, ohne dass ein Neustart des Server-Prozesses "slapd" erforderlich ist.
  - Die Konfiguration kann als Teil des Verzeichnisses auf andere Server repliziert werden, wodurch die Administration von verteilten Verzeichnisdiensten erleichtert wird. Zum Beispiel werden Änderungen von Zugriffsrechten schneller auf allen beteiligten Servern wirksam.

  Andererseits unterstützen nicht alle Backends und Overlays die Online-Konfiguration. Zudem schützt die statische Konfiguration vor unüberlegten Änderungen der Konfiguration und begrenzt die Auswirkungen von Sicherheitsvorfällen.
  Bei der Planung von OpenLDAP ist ein Konfigurationsweg auszuwählen und dann durchgehend beizubehalten. Die Online-Konfiguration ist umso sinnvoller,

  - desto umfangreicher der Verzeichnisdienst ist,
  - desto höher seine Verfügbarkeitsanforderungen sind und
  - desto mehr Server an einem verteilten Aufbau beteiligt sind.

- **Auswahl der zu verwendenden Backends**
  Aus den geplanten Nutzungsmöglichkeiten des Verzeichnisdienstes folgt, welche Backends für die spätere Installation und Konfiguration vorzusehen sind. Details zur Auswahl von Backends enthält die Maßnahme M 2.485 *Auswahl von Backends für OpenLDAP*.
- **Auswahl der zu verwendenden Overlays**
  Ebenso wie für Backends ist auch eine Liste der zu verwendenden Overlays zu erstellen. Um über den Einsatz von Overlays zu entscheiden, sollte das entsprechende Kapitel des OpenLDAP Administrator's Guide durchgearbeitet werden. Für jedes Overlay ist zu prüfen, ob dieses einen experimentellen Status hat oder nicht mehr weiter gepflegt wird. In beiden Fällen sollte der Einsatz in einer Produktionsumgebung vermieden werden. Weiter ist für jedes Overlay über die zugehörige Dokumentation, wie der Manpage, zu prüfen, ob die Online-Konfiguration unterstützt wird. Bei der Auswahl von Overlays ist zu berücksichtigen, dass die Reihenfolge ihres Aufrufs ("stapeln") Auswirkungen auf ihre Funktionsfähigkeit haben kann, Dies ist beispielsweise der Fall, wenn ein Overlay Daten umformt, die von einem anderen Overlay in der ursprünglichen Form erwartet werden.

- **Umsetzung der festgelegten Baumstruktur**
  Während der Planung des Verzeichnisdienstes wurde dessen Struktur festgelegt, die nun der Planung von OpenLDAP zugrunde zu legen ist:

  - Es muss ein geeignetes Namensmodell ausgewählt werden, sofern dies noch nicht im Rahmen der allgemeinen Planung erfolgt ist. Das klassische Namensmodell des X.500 Standards ist auf eine Abbildung von Organisationsstrukturen ausgerichtet und kennt Bezeichner wie "OrganizationalUnit" (OU), "Organization" (O) und "Country" (C) (z. B. OU=bsi, O=bund, C=de). Demgegenüber erlangt das Namensmodell im Internet-Stil eine immer größere Verbreitung. Dieses Namensmodell verwendet auf den oberen Ebenen der Baumstruktur lediglich "DomainComponents" (DC), ohne die einzelnen Bestandteile unterschiedlich zu bezeichnen (z. B. DC=bsi, DC=bund, DC=de).
  - Geeignete Schemas, die zum Namensmodell und zur gewünschten Struktur passen, sind auszuwählen. Schemas legen fest, welche Daten in der Datenbank in welcher Form gespeichert werden können und welche Beziehungen zwischen den Daten bestehen. OpenLDAP bringt alle in RFCs spezifizierten Schemas bereits mit, weitere sind im Internet verfügbar. In der Regel sind die vorhandenen Schemas für normale Einsatzzwecke ausreichend. Sind dennoch eigene Schema-Erweiterungen notwendig, müssen diese mit äußerster Sorgfalt vorgenommen werden, denn von ihnen hängt die Funktionsfähigkeit des Verzeichnisdienstes ab.
  - OpenLDAP bietet durch Overlays zudem die Möglichkeit, Attribute von Objekten im Betrieb einzuschränken. Ein entsprechend konfigurierter slapd-Server wird dann nach den Schemas zulässige Belegungen von Objekten nicht durchführen. Detailinformationen sind in der Maßnahme M 4.386 *Einschränkung von Attributen bei OpenLDAP* zu finden.
  - Schemas können auch unabhängig von der festgelegten Baumstruktur notwendig sein, damit Backends und Overlays fehlerfrei funktionieren, die ihre Daten via LDAP oder im Format LDIF ablegen. Beispielsweise benötigt das Backend "back-monitor" das Schema "core.schema". Derartige Abhängigkeiten sind über die Dokumentation der Komponenten zu prüfen und zu berücksichtigen.
  - Um die Baumstruktur in OpenLDAP festzulegen, ist auch zu entscheiden, ob dynamische Objekte durch das Overlay "dds" (Dynamic Directory Services) zugelassen werden. Solche Objekte werden nach einer festgelegten Zeitspanne oder beim Ausbleiben bestimmter Ereignisse automatisch aus dem Verzeichnisdienst entfernt. Über das Overlay "dynlist" (Dynamic Lists) können zudem dynamische Gruppen gebildet werden. Dynamische Gruppen werden nicht manuell befüllt, sondern enthalten automatisch alle Objekte, die einem definierten Suchkriterium entsprechen. Dadurch können beispielsweise ohne weiteren Wartungsaufwand Gruppen und Listen eingerichtet werden, die alle Mitarbeiter auf einem Stockwerk enthalten. Dynamische Listen können auch für die Zugriffskontrolle (siehe M 4.387 *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*) verwendet werden. Dabei ist jedoch Vorsicht geboten, da der verringerte Administrationsaufwand zu unübersichtlichen Zugriffsberechtigungen führen kann.

- **Planung der Benutzerzugriffe**
  Der Zugriff durch anonyme Benutzer sollte vermieden werden. Wenn ein anonymer Zugriff dennoch notwendig ist, so sollte der Verzeichnisdienst nur Daten mit geringem Schutzbedarf enthalten. Soll auf einen Teilbereich

mit geringem Schutzbedarf zugegriffen werden, während der Verzeichnisdienst auch Daten mit höherem Schutzbedarf enthält, so wird empfohlen, zwei verschiedene slapd-Serverdienste einzurichten, von denen einer anonymen Zugriff erlaubt und nur die Daten mit geringem Schutzbedarf enthält. Dies kann unter anderem durch Replikation gelöst werden (siehe M 4.389 *Partitionierung und Replikation bei OpenLDAP*). Dazu wird beispielsweise aus einem Verzeichnisdienst mit Mitarbeiter-Daten nur der Name und die Durchwahl für ein öffentliches Telefonbuch repliziert.
Zur Planung der Benutzerzugriffe gehört auch, Verantwortlichkeiten von Administratoren festzulegen. So können verschiedene Administratoren für verschiedene Datenbanken im Verzeichnisdienst zuständig sein (siehe auch M 2.407 *Planung der Administration von Verzeichnisdiensten*).

- **Planung des Client-Einsatzes**
  Die Planung von OpenLDAP darf nicht auf den slapd-Server beschränkt bleiben, auch die Auswahl und Unterstützung durch die Clients muss berücksichtigt werden. OpenLDAP stellt geeignete Anwendungen in Form der ldap*-Werkzeuge bereit. Diese Werkzeuge werden jedoch vollständig über die Kommandozeile gesteuert. Sie erfordern einen hohen Schulungsaufwand und haben nur eine geringe Benutzerakzeptanz. In der Praxis werden meist grafische Werkzeuge eingesetzt oder der Client ist Bestandteil einer Anwendung. Werden beim Anwender bereits Verzeichnisdienste über LDAP gesteuert, sind gegebenenfalls schon Client-Anwendungen im Einsatz, deren Fähigkeiten bei der Planung von OpenLDAP zu berücksichtigen sind. Es kann auch sinnvoll sein, durch den slapd-Server Funktionen zu übernehmen, die nach der LDAP-Spezifikation nicht vorgesehen sind, wenn den Clients entsprechende Funktionen fehlen. Overlays für OpenLDAP stellen solche Funktionen bereit:

  - Durch das Overlay "chain" (Chaining) wird ein Server in die Lage versetzt, selbstständig Referrals (dies sind Verweise auf übergeordnete Server, Repliken etc.) zu verfolgen, statt dem Client die Adresse mitzuteilen, unter der dieser selbst suchen könnte.
  - Durch das Overlay "valsort" (Value Sorting) übergibt der Server Suchergebnisse an einen Client bereits in einer sortierten Reihenfolge.
- **Performance Tuning**
  Zuletzt ist bei der Planung auch die benötigte Leistung zu berücksichtigen, die die Verfügbarkeit stark beeinflussen kann. Insbesondere sind häufig gesuchte Attribute zu indizieren.

Prüffragen:

- Wird die verwendete Version der BerkeleyDB von OpenLDAP unterstützt?
- Werden Abhängigkeiten von OpenLDAP zu anderen Anwendungen geprüft und erfüllt?
- Werden Backends und Overlays für OpenLDAP passend zu den Anforderungen ausgewählt?
- Werden die OpenLDAP-Overlays in der korrekten Reihenfolge eingesetzt?
- Wird die Auswahl und Unterstützung von Client-Anwendungen für OpenLDAP bei der Planung berücksichtigt?

# M 2.485 Auswahl von Backends für OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Aus den geplanten Nutzungsmöglichkeiten des Verzeichnisdienstes folgt, welche Backends für die spätere Installation und Konfiguration vorzusehen sind:

- Verwaltet OpenLDAP eine oder mehrere Datenbanken direkt, so ist ein Backend auszuwählen, das für eine entsprechende Datenhaltung geeignet ist. Für die Verwaltung von Daten ist OpenLDAP darauf optimiert, das Datenbankmanagementsystem (DBMS) BerkeleyDB zu verwenden. Für BerkeleyDB stehen zwei verschiedene Backends zur Verfügung: "back-bdb" und die Weiterentwicklung "back-hdb". Das Backend "back-hdb" erzeugt zwar eine höhere Last im IT-System und hat höhere Anforderungen an den für das Zwischenspeichern von Daten benötigten Datenspeicher, besitzt jedoch einen größeren Funktionsumfang und unterstützt das Umbenennen ganzer Teilbäume in der Verzeichnisstruktur (subtree renaming). Die mittelfristige Planung des OpenLDAP-Teams sieht vor, "back-bdb" aufzugeben. Für Neuinstallationen von OpenLDAP wird deshalb empfohlen, "back-hdb" zu verwenden.
  OpenLDAP kann mit dem Backend "back-ldif" Daten auch in Dateien im LDAP Data Interchange Format (LDIF) speichern. Im Format LDIF wird die gesamte Datenbank im Klartextformat in Textdateien abgelegt. Diese Art der Datenhaltung ist ineffizient für größere Datenmengen und für eine große Zahl von Benutzern ungeeignet. Wird die Online-Konfiguration verwendet, so ist dennoch "back-ldif" notwendig, da das Suffix "CN=config" immer im Format LDIF abgelegt wird.
- OpenLDAP kann ganz oder teilweise als Proxy für andere LDAP-Server eingesetzt werden. In diesem Fall wird das Backend "back-ldap" oder die Weiterentwicklung "back-meta" benötigt. Im Gegensatz zu "back-ldap" ist "back-meta" in der Lage, gleichzeitig verschiedene Server anzusprechen. Das Backend hat einen größeren Funktionsumfang als "back-ldap", ist dafür allerdings auch sehr aufwändig zu konfigurieren. Für die meisten Anwendungsfälle ist "back-ldap" ausreichend.
  Das Backend "back-ldap" wird auch immer dann benötigt, wenn der slapd-Server selbst ldap-Operationen auslöst. Dies ist beispielsweise der Fall, wenn der slapd-Server Verweise eigenständig auflöst oder eine Replikation im push-Modus durchgeführt wird.
- Es ist darüber hinaus möglich, dass OpenLDAP auf Daten einer relationalen Datenbank zugreift. Hierfür wird das Backend "back-sql" verwendet. Es wird darauf hingewiesen, dass eine relationale Datenbank ungeeignet ist, um die Daten eines Verzeichnisdienstes vollständig zu speichern. Es kann lediglich sinnvoll sein, OpenLDAP an eine relationale Datenbank anzubinden, um einzelne Zusatzinformationen aus einer solchen Datenquelle auszulesen, wie eine Telefonnummer aus einer Telefonliste in einen Verzeichnisdienst, der alle Benutzer einer Institution verwaltet.
- Gegebenenfalls muss OpenLDAP Daten aus selbst entwickelten Anwendungen beziehen oder wird eingesetzt, um solche Anwendungen zu steuern. Geschieht die Kommunikation nicht über den LDAP-Standard, so ist in Abhängigkeit von der selbst erstellten Schnittstelle eines der Backends "back-perl", "back-shell" oder "back-sock" notwendig.
- Wird entschieden, dass der Betrieb von OpenLDAP überwacht werden soll (Monitoring), so stellt das Backend "back-monitor" die dafür nötigen Funk-

tionen bereit (siehe M 4.407 *Protokollierung beim Einsatz von OpenLDAP*).

Andere Backends als die hier genannten sollten nicht in der Planung für Produktionsumgebungen berücksichtigt werden. Sie sind entweder veraltet (back-ldbm, back-tcl), nur für Testzwecke gedacht (back-passwd, back-null) oder haben in der OpenLDAP-Version 2.4 noch einen experimentellen Status (back-dnssrv, back-ndb, back-relay).

Prüffragen:

- Werden in einer Produktionsumgebung nur die benötigten OpenLDAP-Backends verwendet?

# M 2.486 Dokumentation der Architektur von Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter Entwicklung
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Das Verständnis der Software-Architektur einer Webanwendung beziehungsweise eines Web-Service ist notwendig, um diese effizient und fehlerfrei zu warten, zu entwickeln und zu erweitern. Neben der systemspezifischen Dokumentation (siehe zum Beispiel M 2.25 *Dokumentation der Systemkonfiguration*, M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*) sind bei der Dokumentation von Webanwendungen und Web-Services einige Besonderheiten zu berücksichtigen.

Die Dokumentation muss alle Bestandteile berücksichtigen. Dabei sollten mindestens folgende Punkte durch die spezifische Dokumentation abgedeckt werden:

- Alle Abhängigkeiten (zum Beispiel zu Frameworks, Bibliotheken, Betriebssystemen, Hardware) und Schnittstellen (zum Beispiel zu Hintergrundsystemen) sollten dokumentiert werden. Bei Web-Services muss auch die Interaktion mit anderen Web-Services dokumentiert werden.
- Für den Betrieb notwendige Komponenten, die nicht Bestandteil der Webanwendung oder des Web-Service sind, müssen als solche gekennzeichnet werden (zum Beispiel Hintergrundsysteme wie eine Datenbank).
- Aus der Dokumentation muss hervorgehen, welche Komponenten Sicherheitsmechanismen umsetzen. Im Folgenden sind die Sicherheitsfunktionen von Webanwendungen und Web-Services aufgeführt, die mindestens berücksichtigt werden sollten:
  - Benutzermanagement,
  - Rollen- und Berechtigungskonzept,
  - Authentisierung,
  - Autorisierung,
  - Session-Management,
  - Protokollierung und
  - Transportsicherheit.
- Die Integration in eine gegebenenfalls bestehende Netzinfrastruktur muss in der Dokumentation behandelt werden. Hierbei ist die Maßnahme M 5.169 *Systemarchitektur einer Webanwendung* zu beachten.
- Die eingesetzten kryptographischen Funktionen und Verfahren müssen dokumentiert sein, siehe Baustein B 1.7 *Kryptokonzept*.

Die Dokumentation sollte während des Projektverlaufs aktualisiert und angepasst werden, sodass sie schon während der Entwicklungstätigkeit genutzt werden kann und Entscheidungsfindungen dokumentiert sind.

Prüffragen:

- Ist die Software-Architektur der Webanwendung beziehungsweise des Web-Service mit allen Bestandteilen und Abhängigkeiten dokumentiert?
- Werden für den Betrieb notwendige Komponenten, die nicht Bestandteil der Webanwendung beziehungsweise des Web-Service sind, als solche gekennzeichnet?

- Ist eine Zuordnung umgesetzter Sicherheitsmechanismen zu den Komponenten der Webanwendung beziehungsweise des Web-Service dokumentiert?
- Berücksichtigt die Dokumentation eine Integration der Webanwendung beziehungsweise des Web-Service in bestehende Netzinfrastruktur?
- Sind die eingesetzten kryptographischen Funktionen und Verfahren dokumentiert?
- Erfolgt die Dokumentation der Architektur einer Webanwendung beziehungsweise eines Web-Service bereits während der Entwicklungstätigkeit?

# M 2.487 Entwicklung und Erweiterung von Anwendungen

**Verantwortlich für Initiierung:** Fachverantwortliche, Verantwortliche der einzelnen Anwendungen
**Verantwortlich für Umsetzung:** Entwickler, Beschaffer, Leiter Entwicklung, Tester

Für die effiziente Entwicklung von Anwendungen (auch Webanwendungen) sollten Regeln festgelegt und eingehalten werden. Das Ziel dabei ist, sowohl Konzeptions- als auch Programmierfehler bereits in der frühen Phase des Entwicklungs- und Erweiterungsprozesses zu vermeiden oder zumindest frühzeitig zu erkennen.

Die folgenden Punkte sollten daher bei der Entwicklung und Erweiterung von Anwendungen beachtet werden.

### Entwicklung nach einem Vorgehensmodell

Es sollte nach einem geeigneten Vorgehensmodell (bzw. V-Modell XT, Wasserfallmodell, Spiralmodell) entwickelt werden. Dabei hat eine Anwendung vor der Inbetriebnahme alle Entwicklungsphasen des Vorgehensmodells zu durchlaufen.

Das verwendete Vorgehensmodell sollte mindestens die folgenden oder vergleichbare Phasen abdecken.

### Anforderungsanalyse

Unternehmenssicherheitsrichtlinien und unternehmensspezifische Vorgaben sollten bei der Erhebung der Anforderungen an die Anwendung berücksichtigt und den Entwicklungsteams zur Verfügung gestellt werden (z. B. Erfüllung von Industrie-Standards wie PCI DSS oder Vorgaben zur Barrierefreiheit). Hierzu zählen z. B. auch Vorgaben und Anforderungen an die Verwendung kryptographischer Algorithmen und sicherer Programmierrichtlinien (siehe auch Abschnitt *Umsetzung von Programmierrichtlinien*).

In dieser Phase sollten alle von der Anwendung zu verarbeitenden Daten identifiziert und nach dem Schutzbedarf klassifiziert werden. Es müssen adäquate Schutzmechanismen der Anwendung festgelegt werden, welche die Daten gemäß ihrem Schutzbedarf schützen.

### Konzeption und Design

Bei der Konzeption sollten die Architektur und der Aufbau der Anwendung festgelegt und dokumentiert werden. Hierbei sollte die Auswahl von Entwicklungstechniken (z. B. Programmiersprachen, Frameworks) miteinbezogen werden. Auch das Wissen und der Erfahrungsschatz der Entwickler sollten aus Kosten- und Sicherheitsgründen berücksichtigt werden.

Die Architektur sollte vorsehen, dass Komponenten (z. B. zur Autorisierung, Authentisierung) vorzugsweise in Modulen umgesetzt werden, die wiederverwendet werden können. Durch die zentrale Verfügbarkeit und Nutzung von Modulen können Redundanzen vermieden und die Pflege erleichtert werden.

Bei Client-/Server-Architekturen (z. B. Webanwendung) sollten die zentralen Sicherheitsmechanismen nach Möglichkeit mindestens serverseitig umgesetzt werden.

Es sollte darauf geachtet werden, dass Sicherheitsanforderungen vollständig durch Sicherheitsmechanismen erfüllt und zur Erstellung von Testfällen festgehalten werden.

Getroffene Entscheidungen sollten dokumentiert werden, sodass später eine effiziente Weiterentwicklung der Anwendung durch ausreichende Dokumentation gewährleistet ist.

**Entwicklung**

Bei der Umsetzung der Anwendung sollten Programmierrichtlinien (siehe auch Abschnitt *Umsetzung von Programmierrichtlinien*) für die sichere Entwicklung der Komponenten eingehalten werden.

Es sollte darauf geachtet werden, dass die Dokumentation während der Entwicklungstätigkeit fortgeführt wird (z. B. durch Kommentare im Quelltext und Werkzeuge zur Generierung der Dokumentation). Somit ist der Quelltext zu einem späteren Zeitpunkt auch für Dritte nachvollziehbar.

Zum Schutz vor dem Verlust bereits entwickelter und verworfener Lösungen sowie zu Dokumentationszwecken sollte die Historie der Änderungen festgehalten werden (z. B. durch ein Revisionssystem).

**Tests**

Testfälle sollten nicht nur die Geschäftsfunktionen, sondern ebenfalls die Sicherheitsfunktionalität berücksichtigen. Dazu zählen z. B. Sicherheitskomponenten wie Autorisierungs-, Authentisierungs- und Filterkomponenten. Nach Möglichkeit sollten Penetrationstests und (für hohen Schutzbedarf) auch Source-Code-Analysen durchgeführt werden, um die umgesetzten Sicherheitsmechanismen zu kontrollieren (M 5.150 *Durchführung von Penetrationstests*).

Vor der Inbetriebnahme einer Anwendung sollte nicht nur die Funktionstüchtigkeit, sondern auch ein möglicher Missbrauch der angebotenen Funktionalität geprüft werden. Dies kann durch Penetrationstests erreicht werden. Damit ein Vier-Augen-Prinzip beim Testen umgesetzt wird, sollten die Tests nicht von den Personen durchgeführt werden, die zuvor an der Konzeption oder der Entwicklung der Anwendung beteiligt waren.

Bei den Tests ist darauf zu achten, dass diese nur mit Testdaten und nicht mit Live-Daten bzw. Kundendaten durchgeführt werden.

Bei Webanwendungen sollten die Webseiten auf Konformität zu dem verwendeten Standard (z. B. HTML-Standard) getestet werden. Dadurch können unvorgesehene Seiteneffekte aufgrund einer Fehlinterpretation seitens der Browser vermieden werden. Eine Überprüfung mit verschiedenen Browsern kann hier sehr hilfreich sein.

Bei der Planung und Durchführung der Tests sollte die Maßnahme M 2.62 *Software-Abnahme- und Freigabe-Verfahren* berücksichtigt werden.

**Integration und Softwareverteilung (Deployment)**

Vor der produktiven Inbetriebnahme sind die Anwendungen und gegebenenfalls notwendige Hintergrundsysteme sicher zu konfigurieren. Hierbei sollte

die Anbindung möglicher Hintergrundsysteme (z. B. Identitätsspeicher, Datenbanken) an die Anwendung berücksichtigt werden. Vor der Inbetriebnahme der Anwendung ist ebenfalls sicherzustellen, dass der Transportkanal geschützt ist.

Sensible Daten der Anwendung sind häufig in Hintergrundsystemen hinterlegt. Daher sollte das Sicherheitsniveau der Anwendung und möglicher Hintergrundsysteme einheitlich sein. Der Zugriff auf die Hintergrundsysteme sollte Benutzern lediglich über die definierten Schnittstellen der Anwendung möglich sein.

Darüber hinaus sollte sichergestellt werden, dass die Daten bei der Verteilung der Anwendung nicht durch Dritte manipuliert werden können.

**Wartung**

Es muss ein Prozess zur Pflege der Anwendung definiert werden, der auch die regelmäßige Prüfung der Sicherheit der Anwendung auf Schwachstellen bzw. verfügbare Patches berücksichtigt.

Wird die Anwendung angepasst oder erweitert, muss darauf geachtet werden, dass die Wirksamkeit der Sicherheitsmechanismen nicht beeinträchtigt wird. Zusätzlich sollte durch Tests in einer gesonderten Testumgebung die Wirksamkeit der Sicherheitsmechanismen erneut überprüft werden.

**Umsetzung von Programmierrichtlinien**

Eine Programmierrichtlinie hilft, einen einheitlichen Programmierstil zu definieren und ein einheitliches Sicherheitsniveau zu etablieren (z. B. durch die Verwendung von Sicherheitsbibliotheken). Die Qualität und Verständlichkeit des Quelltexts kann hierdurch verbessert und nachvollziehbarer werden. In der Folge können Fehler und Schwachstellen einfacher gefunden und eine spätere Erweiterung der Anwendung kosteneffektiv umgesetzt werden.

Programmierrichtlinien sollten nicht nur bei der Entwicklung im eigenen Haus, sondern auch beim Outsourcing der Entwicklungstätigkeit umgesetzt werden.

**Zukunftssichere Entwicklung von Sicherheitsmechanismen**

Wenn Sicherheitsmechanismen entworfen und entwickelt werden, sollten hierbei auch zukünftige Entwicklungen von Angriffstechniken als auch Standards (z. B. neuer HTML-Standard) berücksichtigt werden. So sollte beispielsweise eine Filterkomponente, die als schadhaft klassifizierte <script>-Tags filtert, ebenso unbekannte Tags filtern. Unbekannte Tags können gegebenenfalls zukünftig verwendet werden (z. B. mit der Einführung eines neuen HTML-Standards), um Sicherheitsmechanismen der Webanwendung zu umgehen.

**Produktspezifische Sicherheitsfunktionalität**

Falls eine Webanwendung ausschließlich mit einem spezifischen Browser (u. U. nur eines Herstellers) genutzt wird, so sollte der Einsatz von produktspezifischen Sicherheitsfunktionen des Browsers berücksichtigt werden.

**Outsourcing der Anwendungsentwicklung**

Im Fall von Outsourcing muss sichergestellt werden, dass das beauftragte Dritt-Unternehmen die nötigen Sicherheitsanforderungen bei der Umsetzung der Anwendung erfüllt. Dies kann beispielsweise durch die Vorgabe eines Vorgehensmodells oder durch Programmierrichtlinien erreicht werden.

Wird für die Entwicklung einer Anwendung mit hohem Schutzbedarf ein Dienstleister beauftragt, sollte der Quelltext (z. B. das Projektarchiv) unter der administrativen Kontrolle des Auftraggebers stehen. Dabei sollte der Auftraggeber jederzeit auf den Quelltext der Anwendung zugreifen und Änderungen am Quelltext nachvollziehen können.

**Festlegung der Entwicklungsumgebung**

Die Produktiv-, Test- und Entwicklungsumgebungen sind auf getrennten Systemen zu betreiben. In den Umgebungen sollten unterschiedliche Zugangsdaten gewählt werden. Testkonten sollten hierbei, soweit möglich, keine privilegierten Rechte erhalten. Grundsätzlich dürfen erfolgreiche Angriffe auf die Entwicklungs- oder Testumgebung keine Auswirkungen auf die Produktivumgebung haben.

Prüffragen:

- Wird die Anwendung nach einem geeigneten Vorgehensmodell entwickelt?
- Werden alle Phasen bei der Entwicklung von Anwendungen durch das Vorgehensmodell abgedeckt und vor der Inbetriebnahme vollständig durchlaufen?
- Werden Programmierrichtlinien für die Entwicklung von Anwendungen vorgegeben?
- Werden bei dem Entwurf und der Entwicklung von Sicherheitsmechanismen bei Anwendungen auch zukünftige Standards und Angriffstechniken berücksichtigt?
- Werden bei der Anwendungsentwicklung die Entwicklungs-, Test- und Produktivsysteme voneinander getrennt?
- Werden für die Anwendung Penetrationstests durchgeführt, bei denen die Anwendungslogik geprüft wird?
- Werden die Penetrationstests bei Anwendungen nach einem Vier-Augen-Prinzip durchgeführt?

# M 2.488 Web-Tracking

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Web-Tracking bezeichnet die Auswertung von Nutzerdaten z. B. zur Verfolgung der Aktivitäten von Benutzern eines Webauftritts. Auf Grundlage dieser Auswertungen kann beispielsweise auf den Benutzer zugeschnittene Werbung eingeblendet oder die Popularität von Beiträgen anhand von Statistiken gemessen und daraufhin der Webauftritt optimiert werden. Hierfür können personenbezogene Informationen wie der Standort des Benutzers, der Status einer Transaktion (z. B. Geschäftsabschluss bei einer Einkaufsplattform) und eine Abrufstatistik über Webseiten protokolliert und herangezogen werden.

Werden externe Dienstleister beauftragt diese Nutzerdaten auszuwerten, ist zu beachten, dass diese Dienstleister möglicherweise die Nutzerdaten mit den Daten anderer Kunden und Webanwendungen korrelieren können. Auf dieser Basis können anwendungsübergreifend detaillierte Benutzerprofile erstellt werden.

Mögliche Techniken zur Sammlung von Nutzerdaten sind z. B.

- (persistente) Cookies,
- Web-Bugs (Ein-Pixel große Bildelemente z. B. in einer E-Mail zur Führung einer Abrufstatistik),
- Browser-Fingerabdrücke (z. B. durch Attribute wie installierte Zusatzprogramme, Bildschirm-Auflösung, Zeitzone, User-Agent, HTTP-Header),
- Protokollierung der IP-Adresse.

Die Techniken können darüber hinaus kombiniert werden, um Benutzer zuverlässiger zu identifizieren.

Falls eine Auswertung von Nutzerdaten, insbesondere personenbeziehbare Daten, vorgesehen ist oder ein Anbieter diesen Dienst übernehmen soll, müssen die rechtlichen Grundlagen geprüft werden.

# M 2.489 Planung der Systemüberwachung unter Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Revisor

### Neuerungen von Windows Server 2008

Bei Windows-Servern müssen die Grundsätze der Überwachung und Protokollierung angewendet werden, siehe M 5.9 *Protokollierung am Server*. Mit Einführung von Windows Vista und Windows Server 2008 wurde das Ereignisprotokollmodul von Grund auf neu entwickelt. Neben der Erhöhung der Protokolldateigröße auf nunmehr maximal 1 Petabyte wurde auch der Schreibdurchsatz bei der Erstellung der Protokolle erhöht. Grundsätzlich ist das Ereignisprotokollmodul nun in der Lage, Zehntausende von Ereignissen pro Sekunde zu verarbeiten und zu speichern. Gleichzeitig wurde das Format der Einträge von*.evt* nun in das XML-Format *.evtx* geändert.

Neben diesen Veränderungen und der Einführung neuer Ereignisse gibt es zwei wesentliche zu beachtende Neuerungen:

- Sammeln von Ereignissen auf einem zentralen Windows-System
  Seit der Version Windows Server 2008 ist es möglich, Kopien von Ereignissen auf einem zentralen Computer zu sammeln (siehe Abschnitt Planung).
- Neue Nummerierung der Ereignis-IDs
  In der Regel wurden die Identifikationsnummern (ID) der Sicherheitsereignisse durch Verschiebung um den numerischen Wert 4096 verändert, somit hat das ehemalige Ereignis *528 Erfolgreiche Anwendung* nun die neue ID *4634* bekommen. Dies sollte bei schon vorhandenen Auswertungen von Ereignis-IDs, zum Beispiel durch eigene Skripten, berücksichtigt werden.

### Planung

Grundsätzlich sollten während der Planungsphase die folgenden Maßnahmen mitberücksichtigt werden, da sie die Basis der für Windows Server 2008 relevanten Konfigurationen darstellen:

- M 5.9 *Protokollierung am Server*
- M 2.64 *Kontrolle der Protokolldateien*
- M 2.110 *Datenschutzaspekte bei der Protokollierung*
- M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*

Seit Windows Server 2008 ist es möglich, Kopien zuvor definierter Ereignisse auf einem zentralen Windows-System zu sammeln und zu konsolidieren. Vor der notwendigen Konfiguration sowohl der weiterleitenden als auch der sammelnden Computer sollten grundsätzliche Aspekte betrachtet werden.

Um die notwendigen Schritte zur Konfiguration der Überwachung einzuleiten, müssen auf Quellcomputer und Sammlungscomputer die notwendigen Dienste aktiviert werden. Es muss festgelegt, welche Ereignisse von Windows-Servern auf das zentrale System weitergeleitet werden. Erst danach können sogenannte Abonnements erstellt werden. Durch Abonnements sind die zu überwachenden Quellcomputer, der Ereignistyp oder auch Abfragefilter festzulegen. Auch erweiterte Abonnementeinstellungen, wie zum Beispiel Bandbreitenoptimierung, sind danach möglich. Es muss geklärt werden, ob der Abon-

nententyp Sammlungs- oder Quellcomputer initiiert ist. Unter Umständen müssen vor diesem Hintergrund Firewallregeln angepasst werden.

Für die Betriebsphase nach erfolgter Planung sollte die Maßnahme M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008* berücksichtigt werden.

Prüffragen:

- Wurde festgelegt, welche Ereignisse von Windows-Servern auf das zentrale System weitergeleitet werden?

# M 2.490 Planung des Einsatzes von Virtualisierung mit Hyper-V

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Leiter IT

Microsoft stellt mit Hyper-V eine eigene hypervisorbasierte Virtualisierungslösung zur Verfügung. Beim Einsatz von Hyper-V muss grundsätzlich B 3.304 *Virtualisierung* auf den Server angewendet werden. Je nach Ausgestaltung der virtuellen Infrastruktur können dabei recht umfangreiche Abhängigkeiten in der Modellierung entstehen. Neben den virtualisierten Servern (den Gästen) werden auch eine virtuelle Netzinfrastruktur sowie möglicherweise virtuelle aktive Netzkomponenten aufgebaut.

Zusätzlich zu den im Baustein Virtualisierung behandelten Rahmenbedingungen müssen bei der Planung einer Hyper-V-basierten Virtualisierung systemspezifische Entscheidungen getroffen werden.

Hyper-V wird als Rolle unter Windows Server 2008 installiert. Nach der Installation läuft das Betriebssystem selbst unter dem Hypervisor als virtuelle Maschine. Es "degradiert" sich dabei zu einer reinen Management-Konsole und agiert als Ressourcenverwaltung für die anderen virtuellen Maschinen.

Besondere Beachtung bei der Planung für Hyper-V sollte der Schutzbedarf der Gastsysteme finden. Der Schutzbedarf für das Host-System und die Management-Instanz von Windows Server 2008 bestimmen sich nach dem Maximum- und Kumulationsprinzip aus dem Schutzbedarf der Gäste. Nach einer Erweiterung um weitere Gast-Systeme kann es erforderlich sein, den Schutzbedarf eines Host-Systems nachträglich anzupassen. Sind zukünftige Erweiterungen in der Planungsphase bereits absehbar, sollten diese daher entsprechend berücksichtigt werden.

Bestimmte Merkmale lassen sich nachträglich nicht oder nur mit großem Aufwand ändern und müssen bereits bei der Planung berücksichtigt werden. Dazu zählt insbesondere die Installation als Server Core (siehe M 4.416 *Einsatz von Windows Server Core*), die sich bei erhöhtem Schutzbedarf zur Reduzierung der Angriffsfläche anbietet.

Auf die Installation als Server Core sollte nur dann verzichtet werden, wenn absehbar keine erhöhten Schutzanforderungen an die Gastsysteme gestellt werden. Der Nachteile der fehlenden Bedienoberfläche werden durch die Vorteile wie geringerer Ressourcenverbrauch, weniger Bedarf für Patches, geringere Angriffsfläche und die Remoteverwaltungstools für Hyper-V oft aufgewogen.

Als Alternative zur Installation als Server Core ist auch die Installation des Hyper-V Server 2008 R2 möglich. Diese Option ist eine eingeschränkte Version von Server Core, die nur die Hyper-V-Rolle unterstützt und ein verändertes Lizenzmodell ohne eingebaute Gastlizenzen aufweist

Da ein Hyper-V-Server eine ganze Infrastruktur inklusive Netz abbilden kann, sollten für die Administration differenzierte Rollen definiert werden, damit einzelne Administratoren nicht übermäßig viele Rechte erhalten. M 5.153 *Planung des Netzes für virtuelle Infrastrukturen* beschreibt beispielsweise die Trennung von Netzsegmenten auf virtualisierten Systemen. Ein Administrator eines Gastsystems, der die Verbindung der virtuellen Netzwerkkarten ändern

kann, ist in der Lage, Mechanismen zur Netztrennung außer Kraft zu setzen (siehe G 3.99 *Fehlerhafte Netzanbindungen eines Virtualisierungsservers*). Dies kann durch eine geeignete Planung der Administrationsrollen vermieden werden, bei der Hyper-V-Rollen die existierenden Berechtigungen auf die physischen Ressourcen (SAN, Netz-Anbindungen) widerspiegeln.

Für die Umsetzung der Administrationsrollen unter Hyper-V bietet Microsoft den ab Windows Server 2003 eingeführten Autorisierungs-Manager ("Authorization Manager" bzw. "*azman.msc*") an. Mit diesem Werkzeug können Rollen über die Kombination von Vorgängen (z. B. Zuordnung externer Ethernet-Ports) und Bereichen (z. B. Gruppen von Gastsystemen) definiert werden. Die Rollen sollten bereits in der Planungsphase festgelegt werden.

Für die virtuelle Infrastruktur muss ein integriertes Backup-Konzept erarbeitet werden, das die systemspezifischen Aspekte von Hyper-V berücksichtigt. Hyper-V stellt mit dem Hyper-V VSS Writer ("Volume Shadow Copy Service") einen eigenen Backup-Mechanismus zur Verfügung, der auch Metadaten der Gastsysteme sichert. Die Nutzung setzt aber eine Kompatibilität mit der verwendeten Backup-Software voraus.

Prüffragen:

- Ist der zukünftig zu erwartende Schutzbedarf in die Planung für die Virtualisierungsumgebung Hyper-V mit einbezogen worden?
- Sind die Berechtigungsstrukturen der physischen Ressourcen (SAN, Netz-Anbindungen) in den Rollen für die Virtualisierungsumgebung Hyper-V abgebildet?
- Ist ein integriertes Backup-Konzept für Server und Gastsysteme der Virtualisierungsumgebung Hyper-V vorhanden?

# M 2.491 Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

### Neuerungen von Windows Server 2008

Für die Nutzung von Rollen und Sicherheitsvorlagen ergeben sich ab Windows Server 2008 einige Neuerungen. Neben der Umstellung des Formats der administrativen Vorlagendateien (siehe M 2.368 *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*) wurden weitere Veränderungen oder Ergänzungen insbesondere im Bereich Gruppenrichtlinienobjekte und Verwaltungstools vorgenommen. Generell sind Kriterien zu definieren, wie die Vorlagen auf die jeweiligen Systeme anzuwenden sind.

### Server-Manager

Die Basis-Konfiguration von Rollen und Funktionalitäten erfolgt über das zentrale Werkzeug des *Server-Managers*. Er wurde im Vergleich zu den Vorgängerversionen deutlich aufgewertet. Vorlagen in Form von INF-Dateien oder sonstigen Vorlagen (*Templates*) können über den *Server-Manager* jedoch nicht bearbeitet werden.

### Security Configuration Wizard

Mit Einführung von Windows Server 2008 wurde der *Security Configuration Wizard* (SCW) integraler Bestandteil des Systems (siehe M 4.416 *Einsatz von Windows Server Core*). Allerdings geht die Bedeutung dieses Werkzeugs durch die Einführung des *Server-Managers*, der einen zentralen Zugang zu fast allen Konfigurationseinstellungen des Servers bietet, zurück. Darüber hinaus bietet der SCW keine oder nur eingeschränkte Möglichkeiten, Vorlagen zu erstellen oder zu verwalten. Grundsätzlich können die mit dem SCW erstellten XML-Dateien in Gruppenrichtlinienobjekte migriert werden, allerdings ist dieser Prozess aufwendig. Damit eignet sich der SCW eher für die Verwaltung von sogenannten Stand-Alone-Systemen.

### Starter-Gruppenrichtlinienobjekte

Starter-Gruppenrichtlinienobjekte stellen eine Basis für weitere Konfigurationsvorlagen dar. Sie sind unter Windows Server 2008 integraler Bestandteil der Gruppenrichtlinienstruktur innerhalb der Gruppenrichtlinienverwaltung. Es ist zu beachten, dass ursprünglich keine Starterobjekte in Windows Server 2008 R2 und Windows 7 vorhanden sind. Diese wurden durch Microsoft erst später nachgeliefert.

Eine direkte Bearbeitung eines Starter-Gruppenrichtlinienobjektes ist nicht möglich. Für eine veränderbare Version der Vorlage muss die Option *Neues Gruppenrichtlinienobjekt aus Starter-Gruppenrichtlinienobjekt...* gewählt werden. Diese Option kopiert das gewünschte Objekt innerhalb des Active Directory in den Ordner *Gruppenrichtlinienobjekte*.

Das aus einem Starter-Gruppenrichtlinienobjekt erstellte neue Gruppenrichtlinienobjekt erhält alle zuvor vorhandenen Richtlinieneinstellungen für administrative Vorlagen sowie für die definierten Werte.

Alle in einer Domäne vorhandenen Starter-Gruppenrichtlinienobjekte werden im Verzeichnis StarterGPOs im Sysvol-Verzeichnis der Domäne gespeichert.

**Security Compliance Manager**

Zentrales Werkzeug zur Verwaltung von Vorlagen ist der *Microsoft Security Compliance Manager* (SCM). Er ist Bestandteil der frei verfügbaren Security Solution Accelerators, die von Microsoft bereitgestellt werden.

Der SCM konsolidiert die vormals vorhandenen Werkzeuge wie das *Security Compliance Management Toolkit* und den *GPOAccelerator*. Diese Werkzeuge werden nicht mehr weiterentwickelt und sind nicht mehr verfügbar.

Über eine Webschnittstelle werden aktualisierte Vorlagen des Herstellers Microsoft bereitgestellt. Darüber hinaus können Vorlagen weiterer Hersteller zugeführt werden.

Der SCM setzt auf Starter-Gruppenrichtlinienobjekte auf. Dabei handelt es sich um Vorlagen mit Standardeinstellungen für unterschiedliche Anwendungsszenarien, die sich in zwei Gruppen teilen:

- **Enterprise Client (EC)**

Diese Vorlagen sind für Standard-Systeme im betrieblichen Anwendungsumfeld gedacht, die Mitglied in einer Domäne sind. *WS08R2-EC-Member-Server* ist die entsprechende Vorlage zur Konfiguration eines Mitgliedservers.

- **Specialized Security - Limited Functionality (SSLF)**

Diese Vorlagen sind für Systeme mit höheren Sicherheitsanforderungen gedacht, bei denen Einschränkungen in der Funktionalität zugunsten einer erhöhten Sicherheit vorgenommen werden. *WS08R2-SSLF-Member-Server* ist die entsprechende Vorlage für Server-Systeme mit höheren Sicherheitsanforderungen.

Hauptaufgaben des SCM sind:

- zentrale Speicherung von Sicherheitseinstellungen in sogenannten Baselines
- zentrale Verwaltung von Sicherheitseinstellungen für die Domäne
- Nutzung von Baselines von Dritt-Herstellern
- Exportmöglichkeit der Baselines

Die folgenden Formate können durch den Security Compliance Manager erstellt und exportiert werden:

- Desired Configuration Management (DCM) Packs
- Security Content Automation Protocol (SCAP)
- XLS (setzt Excel 2007 voraus)
- Group Policy Objects (GPOs)

Es ist zu beachten, dass nur Kopien der Vorlagen bearbeitet werden sollten. Ebenso sind alle Sicherheitsvorlagen für den Windows Server 2008 an zentraler Stelle zu verwalten und zu bearbeiten. Die gewählten Sicherheitseinstellungen müssen dokumentiert werden.

Mit Einführung des SCM wurden die bisher fehlenden Baselines für Windows 7, Windows Server 2008 R2 oder Microsoft Office 2010 bereitgestellt. Für alle Systeme oder Produkte gilt weiterhin die Unterscheidung zwischen den beiden Vorlagen EC und SSLF.

Neben der Installation des Security Compliance Manager wird zusätzlich ein Werkzeug namens *LocalGPO* bereitgestellt Dieses dient der Transformation der lokalen Richtlinien in ein GPO-Backup. Das Backup kann für andere Systeme als Basiskonfiguration genutzt werden. Umgekehrt wandelt das Werkzeug GPO-Backups in eine lokale Richtlinie um. Das Tool *LocalGPO* muss bei Bedarf über ein bereitgestelltes MSI-Paket nachinstalliert werden.

Prüffragen:

- Werden alle Sicherheitsvorlagen für Windows Server 2008 an zentraler Stelle verwaltet und bearbeitet?
- Wurden Kriterien definiert, wie die Vorlagen auf die jeweiligen Systeme anzuwenden sind?
- Existiert eine Dokumentation zu den gewählten Sicherheitseinstellungen des Windows Server 2008?

# M 2.492 Integration der Lotus Notes/Domino-Umgebung in die vorhandene Sicherheitsinfrastruktur

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Lotus Notes/Domino besitzt eigene Sicherheitsmechanismen und kann durch zusätzliche Sicherheitskomponenten (wie z. B. speziell für Lotus Notes/Domino angepasste Virenschutzprogramme oder Spam-Filter) ergänzt werden. Eine Institution, die den Lotus Notes/Domino-Einsatz erstmalig plant (oder die Aktualisierung der Lotus Notes/Domino-Plattform plant), ist gefordert, die Sicherheitsmechanismen von Lotus Notes/Domino in die bestehende Sicherheitsarchitektur zu integrieren, um "Sicherheitsinseln" zu vermeiden.

Vor allem die an den für die Lotus Notes/Domino-Umgebung relevanten Netzübergängen eingesetzten Sicherheitskomponenten wie Sicherheitsgateways, Content Scanner bzw. Filter und Virenschutzprogramme müssen an die besonderen Anforderungen der Lotus Domino-Protokolle und -Dienste angepasst werden.

Umgekehrt können die Lotus Notes/Domino-Sicherheitsmechanismen dazu benutzt werden, andere Sicherheitskomponenten anzupassen und Schwachstellen der Perimetersicherheit zu schließen. Das Zusammenspiel der Lotus Notes/Domino-eigenen Sicherheitsmechanismen mit den vorhandenen Sicherheitskomponenten muss daher vor Einführung oder Aktualisierung der Plattform geplant werden.

**Zusammenspiel von Lotus Notes/Domino mit Sicherheitsgateways**

Lotus Domino Server können in einer DMZ platziert werden und durch Sicherheitsgateways entsprechend geschützt werden. Die konkrete Positionierung der einzelnen Lotus Notes/Domino-Serverkomponenten ist Teil der Sicherheitsarchitektur für die Lotus Notes/Domino-Umgebung.

Insbesondere bei bereits vorhandenen Sicherheitskomponenten, die für die Lotus Notes/Domino-Umgebung mit genutzt werden, ist es erforderlich, das Zusammenspiel dieser Komponenten mit Lotus Notes/Domino konzeptionell zu regeln. Dabei sind die fachlichen Anforderungen an die Lotus Notes/Domino-Dienste und die technischen Besonderheiten der von Lotus Notes/Domino genutzten Protokolle (z. B. die vorhandene oder nicht vorhandene Möglichkeit, das Protokoll für die Nutzung über eine sichere Verbindung zu konfigurieren) zu berücksichtigen.

**Zusammenspiel von Lotus Notes/Domino mit Lösungen gegen Spam, Content Scannern/Filtern und Virenschutzprogrammen**

Es sollten bevorzugt Sicherheitskomponenten für die Absicherung des Lotus Domino Web Gateways und den Schadprogrammschutz von Lotus Notes/Domino zum Einsatz kommen, die speziell die Lotus Notes/Domino-Plattform unterstützen. Die eingesetzten Lösungen gegen Spam, Content Scanner, Content Filter und Schadprogrammschutz sind an die Anforderungen der Lotus Domino-Dienste und die genutzten Protokolle anzupassen.

**Zusammenspiel von Lotus Notes/Domino mit Sicherheitskomponenten zur zentralen Protokollierung und automatischen Protokollauswertung**

Protokollierung und Protokollauswertung auf zentralen Systemen bieten unter anderem Schutz gegen Manipulation der Lotus Notes/Domino-eigenen Sicherheitsprotokollierung durch Benutzer mit hohen Berechtigungen, Administratoren oder erfolgreiche Angreifer. Ein fortlaufendes Wegschreiben der Sicherheitsprotokollierung in eine gegen Manipulation geschützte zentrale Umgebung (z. B. einen zentralen Protokollierungsserver) ist daher eine wichtige Maßnahme gegen eine Reihe von Bedrohungen, insbesondere auch durch Innentäter mit administrativen Privilegien.

Werden zentrale Protokollierungs- und Auswertungssysteme (auch Security Information and Event Monitoring oder kurz SIEM-Lösungen genannt) genutzt, so ist zu regeln, welcher Teil der Lotus Notes/Domino-Protokollierung über diese Systeme läuft und welches die Lotus Notes/Domino-spezifischen Auswertungskriterien sind.

Prüffragen:

- Wurden die an den für die Lotus Notes/Domino-Umgebung relevanten Netzübergängen eingesetzten Sicherheitskomponenten wie Sicherheitsgateways, Content Scanner bzw. Filter und Virenschutzprogramme an die besonderen Anforderungen der Lotus Domino-Protokolle und -Dienste angepasst?

# M 2.493 Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/ Domino

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Beschaffer, Fachverantwortliche

Mit der wachsenden Komplexität der Lotus Notes/Domino-Plattform und der gängigen Lizenzpolitik aller großen Softwarehersteller wird das Thema Lizenzierung zunehmend schwieriger zu beherrschen. Dabei spielen auch für Lotus Notes/Domino Lizenzierungsaspekte eine immer wichtigere Rolle. Zum einen kann durch passende Lizenzierung erheblich gespart werden, zum anderen ist es technisch und organisatorisch immer aufwendiger sicherzustellen, dass die Lizenzierung vertraglich und in der Umsetzung angemessen ist und keine oder geringe Risiken beinhaltet.

Es ist insbesondere zu berücksichtigen, dass bei archivierungspflichtigen Vorgängen die Notwendigkeit bestehen kann, Programmkomponenten für die gesamte Archivierungsdauer vorzuhalten, da ein Zugriff auf archivierte Daten ohne diese Komponenten eventuell nicht möglich oder extrem aufwendig sein kann. Übliche Lizenzen mit fester Laufzeit enthalten eine Klausel, die die Vernichtung aller Programmkopien nach Ende der Laufzeit der Lizenz vorsieht. Archivierungspflicht kann im Fall von Lotus Notes/Domino für E-Mails bestehen, für Workflows, aber auch andere Komponenten, wie z. B. eigenentwickelte Anwendungen, die auf der Lotus Notes/Domino-Plattform laufen.

### Prozess für Lizenzierung und Lizenzmanagement

Seitens der IT-Leitung ist sicherzustellen, dass ein angemessener Prozess für Lizenzierung und Lizenzmanagement existiert, der zur Abbildung der Lizenzierung von Lotus Notes/Domino geeignet ist.

Eine passende Lizenzierung bedarf der Zusammenarbeit des Anwendungsverantwortlichen für die Lotus Notes/Domino-Plattform, der Projektleiter für laufende Projekte auf der Lotus Notes/Domino-Plattform (speziell auch wegen Serverlizenzen für Entwicklungs- und Testsysteme) und des für die Beschaffung verantwortlichen Bereichs.

Eine Anpassung des Prozesses für Lizenzierung und Lizenzmanagement in definierten Intervallen und bei wesentlichen Änderungen der Lizenzmodelle des Herstellers ist sicherzustellen. Das Lizenzmanagement muss nicht nur in der Lage sein, jederzeit einen Überblick über den aktuellen Status der Lizenzierung liefern zu können, sondern auch strategische und proaktive Lizenzplanung betreiben, unter Berücksichtigung von Upgradeschutz und benötigtem Herstellersupport.

### Besonderheiten bei der Lizenzierung für Lotus Notes/Domino auf virtuellen Maschinen (z. B. unter VMware)

Werden Lotus Notes/Domino-Lizenzen unter Verwendung von Virtualisierungstechniken genutzt (wie z. B. in einer virtuellen Maschine, die nur einen Teil der Ressourcen einer physischen Hardware nutzt) kann eine Lizenzierung über die *Passport Virtualisation Capacity*-Lizenzierungsvereinbarung (ehe-

mals *Sub-Capacity Licensing*) sinnvoll sein. Das Lizenzmanagement muss diese Möglichkeiten berücksichtigen.

Eine technische Unterstützung des Lizenzmanagements für Lotus Notes/Domino ist ab einer gewissen Anzahl von Lizenzen erforderlich. Dieses kann entweder mit bereits in der Institution vorhandenen Prozessen und Hilfsmitteln zum Asset Management und Lizenzmanagement abgebildet werden oder ist für die Lotus Notes/Domino-Plattform gesondert aufzusetzen. Dabei können (oder müssen, abhängig von den vertraglichen Vereinbarungen mit dem Hersteller) die seitens des Herstellers angebotenen Hilfsmittel, wie das *IBM License Management Tool* (ILMT), genutzt werden.

**Lizenzierungsberichte und Lizenzierungs-Audits**

Es ist sicherzustellen, dass die vertraglichen Vereinbarungen der Lizenzierung bekannt und angemessen umgesetzt sind.

Bestimmte Lizenzmodelle des Herstellers erfordern seitens des Kunden beispielsweise die Erstellung und Ablage (Archivierung) von Lizenzierungsberichten, schriftlichen Aufzeichnungen und Ausgaben von Systemtools. Da dies Vertragsbestandteil ist, muss diese Aufgabe mit entsprechender Sorgfalt wahrgenommen werden. Eine periodische Prüfung der Umsetzung ist erforderlich.

Lizenzierungsverträge sehen in der Regel die Durchführung von Lizenzierungs-Audits unter Beteiligung externer Auditoren des Herstellers oder von ihm beauftragter unabhängiger Prüfer vor.

Seitens der Institution ist sicherzustellen, dass ein Prozess "Lizenzierungs-Audit" existiert, der eine kompetente Vorbereitung und Begleitung von Lizenzierungs-Audits gewährleistet.

Die mit dem Hersteller getroffenen Vereinbarungen für Lizenzierungs-Audits von Lotus Notes/Domino sind in der konkreten Ausgestaltung dieses Prozesses für Lotus Notes/Domino zu berücksichtigen.

Prüffragen:

- Existiert ein angemessener Prozess für Lizenzierung und Lizenzmanagement, der zur Abbildung der Lizenzierung von Lotus Notes/Domino geeignet ist?
- Existiert ein Prozess "Lizensierungs-Audit", der eine kompetente Vorbereitung und Begleitung von Lizensierungs-Audits gewährleistet?

# M 2.494 Geeignete Auswahl von Komponenten für die Infrastruktur einer Lotus Notes/ Domino-Umgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Insbesondere der neue, auf Eclipse-Technologie basierende Notes Client (*Standard Client*, auch *Full Client* genannt), aber auch die Serverkomponenten benötigen deutlich umfangreichere Systemressourcen als die Komponenten der Lotus Notes/Domino-Plattform vor Version 8. Dies ist bei einem Upgrade auf die Versionen ab 8.0 zu berücksichtigen. Die bestehenden herstellerseitigen Vorgaben zur Beschaffung von Hardware für Server und Clients, auf denen Domino- bzw. Notes-Komponenten eingesetzt werden sollen, sind daher im Hinblick auf die neuen Anforderungen zu überprüfen und als Konsequenz ist eventuell die vorhandene IT-Ausstattung entsprechend anzupassen.

Die Entscheidung, für Endanwender weiterhin den proprietären Notes Client (*Basic Client*) zu nutzen, kann dazu beitragen, Performanz- und Sicherheitsprobleme (bzw. größere Änderungen an der Client-Infrastruktur) zu vermeiden. Neue Dienste des Domino-Servers, wie Presence und Instant Messaging, werfen auch neue Sicherheitsanforderungen auf, die Auswirkungen auf die Konfiguration vorhandener Komponenten der Sicherheitsinfrastruktur wie Firewalls und IDS/IPS haben können oder aber die Beschaffung neuer Komponenten der Sicherheitsinfrastruktur, die zur Absicherung dieser Dienste geeignet sind, anstoßen. Eine Abstimmung mit den Betreibern der operativen Sicherheitsinfrastruktur und eine entsprechende Anpassung der Vorgaben für die Beschaffung und den Betrieb von Sicherheitskomponenten im Lotus Notes/Domino-Umfeld ist daher im Vorfeld erforderlich. Zu den Komponenten der Sicherheitsinfrastruktur, die dabei zu berücksichtigen sind, zählen:

- Sicherheitsgateways,
- netzbasierte Systeme zur Angriffserkennung- und Vermeidung (NIDS/ NIPS),
- serverseitige Systeme zur Angriffserkennung- und Vermeidung (HIDS/ HIPS),
- serverseitige Komponenten zum Malwareschutz,
- clientseitige Personal Firewalls,
- clientseitige Komponenten zum Malwareschutz und clientseitige HIDS (oft als clientseitige *Security Suite* gebündelt),
- Content Security-Lösungen (auch Appliances),
- Lösungen zur Vermeidung von Abflüssen sensitiver Daten (Data Loss Prevention- oder DLP-Lösungen).

Vor jeder Releaseänderung der Lotus Domino-Umgebung und vor allen wesentlichen Änderungen in der Nutzung der Domino-Dienste (z. B. Freischaltung neuer Dienste) sollte diese mit den für Lotus Notes/Domino relevanten Komponenten der Sicherheitsinfrastruktur abgestimmt werden.

Prüffragen:

- Existiert ein Prozess, der sicherstellt, dass die Hardware den aktuellen Anforderungen der Lotus Notes/Domino-Komponenten genügt?
- Wird vor jeder Releaseänderung der Lotus Domino-Umgebung und vor allen wesentlichen Änderungen in der Nutzung der Domino-Dienste

(z. B. Freischaltung neuer Dienste) eine Abstimmung mit den für Lotus Notes/Domino relevanten Komponenten der Sicherheitsinfrastruktur vorgenommen?

# M 2.495 Aussonderung von Lotus Notes/ Domino-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Im Lebenszyklus der Lotus Notes/Domino-Umgebung ist auch die Phase der Aussonderung zu berücksichtigen. In der Regel findet keine ersatzlose Aussonderung statt, da die durch Lotus Notes/Domino unterstützten Geschäftsprozesse sich nicht soweit ändern, dass Dienste wie E-Mail, Web-Dienste, etc. ersatzlos wegfallen. Somit wird eine Aussonderung nur beim Einsatz eines neuen Produktes stattfinden, so dass meistens auf eine neue Groupware- bzw. Collaboration-Lösung migriert wird.

Die Aussonderung ohne Aspekte der Migration betrifft daher in der Regel einzelne Komponenten der Lotus Notes/Domino-Umgebung (oder Infrastrukturkomponenten und die auf diesen befindlichen Lotus Notes/Domino-Komponenten).

Bei der Aussonderung einer Komponente sind alle Referenzen auf die ausgesonderte Komponente (z. B. Cross-Zertifikate) in der verbleibenden Umgebung zu löschen und die Inventurlisten bzw. -datenbanken entsprechend anzupassen. Eine "Wiederverwendung" einer solchen Referenz durch einen Angreifer, z. B. durch die Einbringung einer Komponente bzw. eines Systems mit der Identität der ausgesonderten Komponente, wird dadurch verhindert. Die Lizenzierung und das Lizenzmanagement sind zu überprüfen und bei Bedarf anzupassen.

Analog zu den Referenzen der ausgesonderten Komponente in der verbleibenden Lotus Notes/Domino-Umgebung ist mit den Daten und Referenzen der Komponente auf Betriebssystemebene, im Netzverbund, auf Überwachungs- und Sicherheitskomponenten (Sicherheitsgateways, IDS, Content Security Appliances, SIEM-Plattformen, Komponenten zum Schutz vor Schadsoftware, Komponenten zur Netzüberwachung) zu verfahren. Dies erübrigt sich, wenn die ausgesonderte Komponente durch eine neue Komponente mit gleicher Identität im Lotus Notes/Domino-Verbund ersetzt wird, wie z. B. bei einer 1:1-Übertragung eines Domino-Servers auf eine leistungsstärkere Hardware.

Nach erfolgreicher Migration ist vor der physischen Entsorgung der ausgesonderten Lotus Notes/Domino-Infrastruktur der Baustein B 1.15 *Löschen und Vernichten von Daten* anzuwenden. Gleiches gilt für Infrastruktur, die für andere Zwecke wiederverwendet wird (z. B. als Entwicklungsserver).

Es ist zu berücksichtigen, dass die archivierten Daten auch nach der Aussonderung der Lotus Notes/Domino-Umgebung weiterhin vorgehalten werden müssen und der Zugriff auf diese Daten mit angemessenem Aufwand und bei Einhaltung angemessener Fristen (diese sind dem Archivierungskonzept zu entnehmen) möglich ist. Es sind daher entsprechende Ressourcen (Hardware, Software, Lizenzen) vorzuhalten.

Prüffragen:

- Ist das Verfahren zur Aussonderung von Lotus Notes/Domino-Komponenten dokumentiert (z. B. in der Dokumentation der Betriebsverfahren oder dem Betriebshandbuch)?

# M 2.496 Geregelte Außerbetriebnahme eines Protokollierungsservers

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Auf einem Protokollierungsserver werden Protokolldaten gesammelt, verarbeitet, gespeichert und archiviert. Diese Daten können unter anderem IP-Adressen, Benutzernamen und Namen von IT-Systemen enthalten. Daher muss sichergestellt werden, dass auf Festplatten und anderen Speichermedien keine schützenswerten Informationen mehr enthalten sind, wenn der Protokollierungsserver außer Dienst gestellt wird. Alle Datenträger müssen sicher gelöscht sein, unabhängig davon, ob sie weitergegeben, repariert oder ausgesondert werden.

Im Fall einer Reparatur reicht es nicht aus, die Festplatten nur zu formatieren oder Löschfunktionen des Betriebssystems zu nutzen. Sie müssen mit geeigneten Löschprogrammen so überschrieben werden, dass die Daten nicht mit Hilfe von speziellen Methoden wiederhergestellt werden können. Weitere Informationen, wie Datenträger sicher gelöscht und vernichtet werden können, sind unter M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* zu finden.

Wird ein Protokollierungsserver ausgesondert, ist es empfehlenswert, die Speichermedien zusätzlich zur Löschung mechanisch zu vernichten ("schreddern"). Können die Speichermedien nicht zeitnah vernichtet werden, sind sie bis zur Zerstörung vor unberechtigtem Zugriff zu schützen. Magnetische Speichermedien lassen sich auch mittels eines Degaussers elektromagnetisch löschen.

Wenn die Datenträger durch Dritte gelöscht werden, muss der Auftrag unter anderem nach datenschutzrechtlichen Anforderungen vergeben und ein Auftragsdatenverarbeitungsvertrag geschlossen werden.

Prüffragen:

- Ist sichergestellt, dass sich nach der Außerbetriebnahme eines Protokollierungsservers keine schützenswerten Daten mehr auf den Datenträgern befinden?

# M 2.497 Erstellung eines Sicherheitskonzepts für die Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Damit die Protokollierung in einem sicheren Rahmen erfolgen kann, muss ein Sicherheitskonzept erstellt werden. Darin werden alle Aspekte festgeschrieben, die den sicheren Einsatz der Protokollierung betreffen, zum Beispiel welche Daten erfasst und wie lange diese gespeichert werden sollen, wie die Auswertung erfolgen muss und wie die Protokolldaten bei einer zentralen Protokollierung über das Netz verschickt werden.

Die folgende Aufzählung nennt einige wichtige Bereiche, die im Konzept geregelt werden sollten. Sie ist aber nicht vollständig und muss den Einsatzszenarien in der Institution entsprechend angepasst, ausgestaltet und erweitert werden. Detailinformationen zu den angesprochenen Aspekten finden sich in den einzelnen Maßnahmen von B 1.0 *Sicherheitsmanagement*.

In einem Sicherheitskonzept wird geregelt, wie, wo und was bei welchem Schutzbedarf protokolliert werden soll. Darunter fällt auch die Entscheidung, ob lokal oder zentral protokolliert werden soll, siehe auch M 3.90 *Allgemeine Grundlagen für die zentrale Protokollierung*. Es ist in der Regel einfacher, einen Überblick über die sicherheitsrelevanten Vorkommnisse im Informationsverbund zu gewinnen, wenn ein zentraler Protokollierungsserver eingesetzt wird, der die unterschiedlichen Protokolldaten zusammenführt, diese analysiert und überwacht. Dabei sind unter anderem die folgenden Aspekte relevant:

- Ist eine zentrale Protokollierung notwendig oder können die Protokolldaten lokal gespeichert und ausgewertet werden?
- Wie sollen bei einer zentralen Protokollierung die Server abgesichert werden?
- Wo sollte ein zentraler Protokollierungsserver im Netz platziert werden?
- Welche synchronisierte und exakte Zeitbasis wird von den Protokollmeldungen genutzt?
- Wie werden Protokollierungsserver sicher außer Betrieb genommen?

Es muss entschieden werden, welche IT-Systeme, Netze und Anwendungen im Sicherheitskonzept für die Protokollierung berücksichtigt werden sollen. Generell sollten alle sicherheitsrelevanten Ereignisse von IT-Systemen wie Servern, Clients, Netzkoppelelementen und Sicherheitsgateways protokolliert und ausgewertet werden, wie in M 4.430 *Analyse von Protokolldaten* beschrieben ist. Dazu können folgende Fragen sinnvoll sein:

- Welche Ereignisse sollen von der Protokollierung erfasst werden?
- Welche Dienste, Anwendungen und welche Hosts werden protokolliert?
- In welchem Format sollen die Informationen erfasst und verarbeitet werden?

Damit alle Funktionen und Sicherheitsmerkmale der Protokollierung optimal genutzt werden können, ist es wichtig, die Administratoren entsprechend zu schulen, siehe auch M 3.89 *Schulung zur Administration der Protokollierung*. In den Schulungen sollten Informationen über Einrichtung und Betrieb der Komponenten eines Protokollierungsservers sowie Kenntnisse über die Ad-

ministration vermittelt werden. Wichtig sind unter anderem die aufgelisteten Punkte:

- Wer darf zu welchem Zweck auf die Protokollierungsdaten zugreifen?
- Welche Administrationsaufgaben dürfen bzw. sollen delegiert werden?
- Welche Schulungen sollen Administratoren in Bezug auf die Protokollierung erhalten?
- Wie werden die Tätigkeiten der Administratoren überwacht?

Die gesammelten Protokollinformationen können lokal oder an einem zentralen Protokollierungsserver ausgewertet werden. Das wird in M 4.431 *Auswahl und Verarbeitung relevanter Informationen für die Protokollierung* näher beschrieben. Im Fall der zentralen Analyse müssen die Protokollinformationen über das Netz an einen zentralen Server übertragen werden. Hierbei ist die Kommunikation zwischen den beteiligten IT-Systemen ausreichend abzusichern, siehe M 5.171 *Sichere Kommunikation zu einem zentralen Protokollierungsserver*. Dazu sollten die folgenden Aspekte beachtet werden:

- Mit welchen Mechanismen werden Verfügbarkeit, Vertraulichkeit und Integrität der Protokolldaten während der Übertragung geschützt?
- Können die Protokollierungsdaten über das Datennetz übertragen (In-Band) oder muss dafür ein eigenes Protokollierungs- und Administrationsnetz eingerichtet werden? (Out-of-Band)
- Gibt es eine ausreichend genaue Zeitbasis, mit der alle Protokollquellen synchronisiert sind?

Treten bestimmte Ereignisse ein oder werden Schwellwerte überschritten, sollte ein Alarm beispielsweise per E-Mail oder SMS ausgelöst werden. Um eine sinnvolle Alarmierung durchführen zu können, ist es beispielsweise wichtig, die Anzahl der Fehlalarme zu reduzieren und die relevanten Personen schnell zu informieren. Nähere Informationen sind in M 6.151 *Alarmierungskonzept für die Protokollierung* zu finden. Dazu können die folgenden Fragen hilfreich sein:

- Welche Filtereinstellungen sind notwendig, um die relevanten Informationen in den Protokolldaten zu finden?
- Wie und wie lange werden Protokolldaten archiviert und entspricht das den Datenschutzbestimmungen?
- Wie müssen die Schwellwerte eingestellt werden, damit False-Positives (Fehlalarm) und False-Negatives (Vorfall wurde nicht erkannt) vermieden werden?
- Wie soll auf Alarme reagiert werden?
- Wie werden die verantwortlichen Personen über Alarme informiert?

Bei der Protokollierung spielt der Datenschutz eine wichtige Rolle, da er zum einen Vorgaben macht, was zu protokollieren ist und zum anderen, was nicht protokolliert werden darf und wie mit den protokollierten Daten umzugehen ist (siehe M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Das Sicherheitskonzept zur Protokollierung muss mit dem übergreifenden Sicherheitskonzept der Institution abgestimmt sein. Außerdem ist es regelmäßig zu aktualisieren und an Änderungen der Technik genauso anzupassen wie an Änderungen innerhalb der Institution.

Prüffragen:

- Wurde das Sicherheitskonzept für die Protokollierung mit dem Sicherheitskonzept der gesamten Institution abgestimmt?
- Wird das Sicherheitskonzept für die Protokollierung regelmäßig aktualisiert?

# M 2.498 Behandlung von Warn- und Fehlermeldungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für die Behandlung von Warn- und Fehlermeldungen müssen strukturierte und nachvollziehbare Prozesse eingeführt und die umgesetzten Maßnahmen dokumentiert werden.

In diesen Prozessen sollte beschrieben sein, wer für die Bearbeitung der Meldung zuständig ist (Rollen oder Personen) und auf welche Weise die Information über die Meldung übermittelt wird (z. B. E-Mail, SMS, Generierung eines Trouble-Tickets).

Verfügt die Institution bereits über ein Alarmierungskonzept, so sind die Warn- und Fehlermeldungen des Netzmanagements hierin einzubetten.

Im Folgenden sind mögliche Ereignisse, Ursachen und Reaktionen für Warn- und Fehlermeldungen aufgeführt.

**Warnmeldungen**

Eine Warnmeldung kann durch unterschiedliche Ereignisse ausgelöst werden, beispielsweise:

- Die im Netzkonzept definierten und im Netzmanagementsystem hinterlegten Schwellwerte werden über- oder unterschritten.
- Angebotene Dienste werden nicht mit der erforderlichen Güte bereitgestellt.
- Es kommt zu Anomalien im Netzverkehr, die vom Netzmanagementsystem erkannt werden.

Als mögliche Ursachen können infrage kommen:

- Neu eingeführte Geschäftsprozesse benötigen eine unerwartet hohe Bandbreite.
- Im Internet gibt es ein interessantes Angebot, das von vielen Mitarbeitern genutzt wird, zum Beispiel der Live-Stream eines Spiels einer Fußball-WM.
- Ein Computer im internen Netz ist mit Malware infiziert, die versucht, über nicht erlaubte Ports zu kommunizieren.
- Die Institution wird von außen angegriffen.
- Peer-to-Peer (P2P) Dienste werden in unerlaubter Weise genutzt und führen zu einer Überlastung der Internetverbindung.
- Es wurde ein Versuch unternommen, ungenehmigt ein IT-System mit dem internen Netz zu verbinden.
- Nicht erlaubte Protokolle werden genutzt (z. B. Remote-Desktop-Verbindung zu einem Computer außerhalb des internen Netzes).
- Jemand probiert verschiedene Passwörter aus, um sich unbefugt bei einer aktiven Netzkomponente anzumelden.

Je nach Ursache der Warnmeldung müssen die Verantwortlichen entsprechende Maßnahmen einleiten:

- Erfolgt die Warnmeldung, weil ein Schwellwert über- oder unterschritten wurde, beispielsweise wegen eines intensiv genutzten Internetangebots, können entweder technische und/oder organisatorische Maßnahmen zur Abhilfe ergriffen werden. Ist abzusehen, dass sich der Vorfall in dieser Form nicht wiederholen wird, muss nicht reagiert werden.

- Bei Verdacht auf eine Vireninfektion sollte eine Überprüfung auf Schadsoftware gestartet werden.
- Wenn anzunehmen ist, dass das Problem wieder auftreten wird, ist zu klären, ob eine geänderte Konfiguration aktiver Netzkomponenten Abhilfe schafft, beispielsweise indem Dienste aktiviert oder deaktiviert werden. Sollte es sich um ein bereits bekanntes Problem handeln, können vom Hersteller zur Verfügung gestellte Updates oder Patches eingespielt werden (siehe B 1.14 *Patch- und Änderungsmanagement*).
- Werden Schwellwerte dauerhaft verletzt, muss überlegt werden, ob der Beeinträchtigung von Diensten im Netz durch zusätzliche oder leistungsfähigere Hardware entgegengewirkt werden kann. Eine solche Maßnahme könnte die Migration in bestimmten Netzabschnitten von Fast-Ethernet auf eine Anbindung mit höheren Übertragungsraten sein. Sind die Maßnahmen abgeschlossen, muss der Netzplan auf den neuesten Stand gebracht werden.
- Lässt sich die Warnung nicht durch einzelne Maßnahmen abstellen, muss unter Umständen auch über eine Änderung der Topologie nachgedacht und ein Netzdesignprozess (siehe B 4.1 *Lokale Netze*) angestoßen werden. So könnten Dienste beispielsweise redundant ausgelegt werden oder es kann eine erweiterte Netztopologie notwendig sein.

**Fehlermeldungen:**

Fehlermeldungen weisen immer auf den Ausfall einer aktiven Netzkomponente oder eines Dienstes hin, der durch das Netzmanagement überwacht wird. Generell kann ein Ausfall mit oder ohne Fremdeinwirkung verursacht worden sein.

- Ausfall von IT-Systemen, die Dienste im Netz anbieten (z. B. E-Mail-Server).
- Ausfall von aktiven Netzkomponenten (z. B. ein Port am Switch ist defekt).
- Ausfall von passiven Netzkomponenten (z. B. Kabel wurde versehentlich bei Umbauarbeiten beschädigt).

Die Ursachen für den Fehler können vielfältig sein, darunter sind:

- Umweltfaktoren wie Hitze und Wasser lösen einen Hardwaredefekt aus oder es liegt ein Fehler in der technischen Infrastruktur vor, zum Beispiel ein Stromausfall.
- Eine Softwareschwachstelle führt zum Absturz eines IT-Systems oder einer aktiven Netzkomponente.
- Ein IT-System wurde erfolgreich von innen oder von außen angegriffen und fällt aus.
- Bei einem Test von Sicherheitsvorrichtungen wurden produktive Systeme gestört. Beispielsweise startet die Notstromversorgung bei einem Test nicht.

Die Ursachenforschung ist sehr wichtig. Es muss das Ziel sein, solche Fehler in Zukunft zu verhindern oder zumindest möglichst schnell zu beheben, wenn sie trotzdem wieder auftreten. Wenn mehrere ungünstige Umstände zusammenspielen, ist es schwer, die Ursachen und deren Zusammenwirken zu entdecken. Zum Abstellen des Fehlers können beispielsweise folgende Maßnahmen erfolgreich sein:

- Eine defekte Hardwarekomponente wird ausgetauscht oder eine abgestürzte Software wird neu installiert.
- Unter Umständen kann auch die Reparatur einer defekten Hardwarekomponente möglich und wünschenswert sein.

- Steht für ein ausgefallenes IT-System ein Standby-System zur Verfügung (Cold- oder Hot-Standby), so wird dieses anstelle des defekten IT-Systems verwendet.

Es muss das primäre Ziel sein, auftretende Fehler zu beheben. Trotzdem ist es auch wichtig zu lernen, wie solche Fehler künftig vermieden werden können. Die Analyse des Fehlers und die eingeleiteten Maßnahmen sollten dokumentiert werden.

Prüffragen:

- Wurden für die Behandlung von Warn- und Fehlermeldungen nachvollziehbare Prozesse eingeführt und die umgesetzten Maßnahmen dokumentiert?
- Wurden die Warn- und Fehlermeldungen des Netzmanagements in ein bereits vorhandenes Alarmierungskonzept integriert?

# M 2.499 Planung der Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Auf vielen IT-Systemen innerhalb eines Informationsverbundes werden sicherheitsrelevante Ereignisse protokolliert und dadurch größere Mengen Protokolldaten erzeugt. Diese enthalten wichtige Informationen, die dabei helfen können, Hard- und Softwareprobleme sowie Ressourcenengpässe festzustellen und zu lokalisieren. Des Weiteren werden Protokolldaten auch verwendet, um Sicherheitsprobleme und Angriffe frühzeitig erkennen zu können und dadurch das Niveau der Informationssicherheit zu erhöhen. Um sicher protokollieren zu können, ist ein angemessenes Maß an Planung im Vorfeld notwendig. So sollte ein Protokollierungskonzept erstellt und geklärt werden, ob lokal oder zentral protokolliert werden soll. Darüber hinaus müssen Administration, Einsatz, Frühwarnung und Beweissicherung geregelt werden.

### Protokollierungskonzept

In einem Protokollierungskonzept wird geregelt, wie, wo und was bei welchem Schutzbedarf protokolliert werden soll. Darunter fällt auch die Entscheidung, ob lokal oder zentral protokolliert werden und was mit den protokollierten Ereignissen geschehen soll. Das Protokollierungskonzept wird ausführlich in M 2.500 *Protokollierung von IT-Systemen* beschrieben.

### Platzierung im Netz bei zentralem Protokollierungsserver

Die Platzierung des zentralen Protokollierungsservers muss genau durchdacht werden, denn er muss einerseits von sämtlichen IT-Systemen aus erreichbar sein, darf aber keinen unberechtigten Zugriff aus nicht-vertrauenswürdigen Netzen ermöglichen. Ein Beispiel hierfür ist ein Perimeterrouter vor dem Sicherheitsgateway (Firewall), der direkt mit dem Internet verbunden ist und dessen Protokolldaten auch zentral verwaltet werden sollten.

Wichtig für die Platzierung ist, dass keine zusätzlichen Schwachstellen entstehen, wie die Möglichkeit zur Umgehung von Sicherheitskomponenten. Besonders bei erhöhtem Schutzbedarf der Protokolldaten sollten Protokollierungsserver in einem eigenen Protokollierungs- und Administrationsnetz platziert werden. Hierfür benötigt jedes zu protokollierende IT-System einen separaten Anschluss für das Protokollierungs- und Administrationsnetz, beispielsweise eine Netzkarte. Die Protokolldaten sollten in diesem Fall nur über das hierfür bereitgestellte Netz übertragen werden (Netztrennung, Out-of-Band).

### Sichere Übertragung bei Einsatz eines zentralen Protokollierungsservers

Wenn Protokolldaten von den einzelnen IT-Systemen an den zentralen Protokollierungsserver übertragen werden, sind besonders die Integrität und die Vertraulichkeit sicherzustellen (siehe dazu auch M 5.171 *Sichere Kommunikation zu einem zentralen Protokollierungsserver*). Protokolldaten sollten vor unberechtigtem Zugriff (einsehen, verändern, löschen) zum Beispiel durch Verschlüsselung geschützt werden.

Denkbar sind auch Mechanismen, die die Integrität der Informationen während der Übertragung erhöhen. Ein Beispiel ist die Übermittlung in einem separaten LAN (Netztrennung, Out-of-Band), über das keine weiteren Informationen

übermittelt werden und das nicht von unsicheren Netzen aus erreicht werden kann.

**Administration**

Protokolldaten werden nicht nur für die Fehlersuche und Überwachung, sondern auch für Kontrollen, wie beispielsweise im Rahmen eines Audits, einer Revision oder einer computerforensischen Analyse verwendet. Um die Beweiskraft der Protokollinformationen zu erhalten, müssen sie davor geschützt werden, fahrlässig oder vorsätzlich geändert werden zu können. Darum sollten nur berechtigte Personen auf diese Informationen Zugriff haben.

Für die Systemverwaltung ist ein vertrauenswürdiger Administrator (siehe M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters*) zu wählen. Dies ist besonders bei einem hohen Schutzbedarf der Protokolldaten relevant, da sie personenbezogene Daten enthalten können.

Es ist empfehlenswert auch die Tätigkeiten der Administratoren zu überwachen, insbesondere bei erhöhtem Schutzbedarf. Da in den meisten Fällen bei der Protokollierung auf personenbezogene Daten zugegriffen wird, sollte sichergestellt werden, dass die Sammlung lokaler und zentraler Protokolldaten den Anforderungen des Datenschutzes genügt. So dürfen die Daten nur zur Datenschutzkontrolle, zur Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebes nach datenschutzrechtlichen Regelungen (siehe M 2.110 *Datenschutzaspekte bei der Protokollierung*) erhoben werden. Das Verfahren der Protokollierung und die Kriterien für deren Auswertung sind in einem Verfahrensverzeichnis zu dokumentieren.

**Einsatz**

Bereits bei der Planung muss entschieden werden, wozu die Protokolldaten in einem Informationsverbund verwendet werden sollen. In die Erfassung müssen alle Datenquellen einfließen, die für den definierten Einsatzzweck benötigt werden. Zum Beispiel spielen bei der Überwachung eines Informationsverbundes unter anderem die Protokolldaten der folgenden IT-Systeme eine Rolle:

- Aktive Netzkomponenten (wie z. B. Router, Switche),
- Betriebssysteme,
- Applikationen und Dienste (wie Webserver, Mailserver, Fileserver),
- Sicherheitskomponenten im Netz (wie Firewall, Proxy, IDS),
- Sicherheitskomponenten auf Hosts (wie Sicherheitsgateways, Virus-Scanner),
- Physikalische Zutrittssysteme.

Für die umfassende Überwachung des Informationsverbunds können die Protokolldaten dieser Systeme an zentraler Stelle gesammelt werden.

**Frühwarnung**

Zentral gesammelte Protokolldaten eignen sich hervorragend zur Ergänzung eines Frühwarnsystems. Es ist wichtig, die Daten laufend und möglichst in Echtzeit zuzuführen und regelmäßig auszuwerten. Dazu müssen die Protokolldaten aggregiert und korreliert werden.

Unter Aggregation wird das Zusammenfassen von Protokollmeldungen mit redundantem Inhalt verstanden, doppelte Informationen werden zu einem Eintrag zusammengefasst. Bei der Korrelation werden verschiedene Protokolldaten miteinander verknüpft. Angriffe auf einen Informationsverbund lassen sich oft erst durch die Kombination unterschiedlicher Protokolldaten erkennen. So

versuchen Angreifer häufig, ihre Spuren zu verwischen. Werden Protokolldaten aus verschiedenen Quellen miteinander abgeglichen, steigt die Chance, dass der Angreifer nicht alle Einträge, die ihn entlarven könnten, entfernen konnte. Die Daten können nur an zentraler Stelle, wo die verschiedenen Informationen zusammenlaufen, verknüpft und zusammengefasst werden.

Um eine sinnvolle Analyse und darauf aufbauende Frühwarnung zu ermöglichen, muss durch Aggregation und Korrelation erkannt werden, wann die Integrität der Protokolldaten nicht mehr gewährleistet ist. Zusätzlich sollte in dem Frühwarnsystem eine Anomaliekomponente integriert sein, die einen Alarm auslöst, wenn der überwachte Informationsverbund vom Normalzustand abweicht (siehe dazu M 6.151 *Alarmierungskonzept für die Protokollierung*).

**Beweissicherung**

Protokolldaten können in einem Informationsverbund für die Untersuchung von Sicherheitsvorfällen (Computerforensik) verwendet werden. Hierbei werden die Protokollinformationen für die Beweissicherung herangezogen. Bei diesen Untersuchungen wird versucht, anhand der Protokolldateien einen bereits aufgetretenen Sicherheitsvorfall zu rekonstruieren, um den entstandenen Schaden zu ermitteln.

Prüffragen:

- Wird ein Protokollierungskonzept erstellt?
- Ist die Integration des Protokollierungsservers in das Netz des Informationsverbundes sorgfältig geplant worden?
- Ist bei zentraler Protokollierung sichergestellt, dass der Protokollierungsserver von sämtlichen zu protokollierenden IT-Systemen aus erreichbar ist und keine unberechtigten Zugriffsmöglichkeiten bietet?
- Werden die Protokolldaten von den einzelnen Systemen unter Wahrung der Integrität und Vertraulichkeit an den zentralen Protokollierungsserver übertragen?
- Werden bei den gesammelten Protokolldaten die Anforderungen des Datenschutzes erfüllt?
- Werden das Verfahren der Protokollierung und die Kriterien für die Auswertung dokumentiert?
- Werden die Protokolldaten möglichst in Echtzeit überwacht und regelmäßig ausgewertet?

# M 2.500 Protokollierung von IT-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sicherheitsrelevante Aktivitäten an informationsverarbeitenden Systemen sollten aus vielen Gründen protokolliert werden. Zum einen hilft eine aktivierte Protokollierung, potenzielle Schwachstellen frühzeitig erkennen und damit beseitigen zu können. Zum anderen kann Protokollierung dabei helfen, Verstöße gegen Sicherheitsvorgaben zu erkennen oder Nachforschungen über einen Sicherheitsvorfall anzustellen. Hierfür werden Ereignisse aufgezeichnet, die auf den zu betrachtenden IT-Systemen auftreten.

Jede Institution sollte generelle Regeln aufstellen, wie bei der Protokollierung von IT-Systemen, Netzen oder Anwendungen vorzugehen ist. Diese sind dann entsprechend auf die spezifischen Systeme anzupassen und umzusetzen. In verschiedenen Bausteinen der IT-Grundschutz-Kataloge zu IT-Systemen, Netzen oder Anwendungen sind vertiefende Informationen darüber zu finden, was bei der Protokollierung auf den jeweiligen IT-Systemen zu beachten ist, beispielsweise in M 4.302 *Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten*. Umfassend wird das Thema Protokollierung im Baustein B 5.22 *Protokollierung* beschrieben. Der Baustein betrachtet alle spezifischen Gefährdungen und Maßnahmen, die unabhängig vom eingesetzten Betriebssystem für die Protokollierung und Überwachung relevant sind.

Der Aufwand zur Erstellung und Umsetzung eines solchen Prozesses ist nicht gering. Daher sollte dieser Baustein vor allem bei größeren Informationsverbünden umgesetzt werden und wenn in einem Informationsverbund zentral protokolliert werden soll. Bei kleineren und wenig komplexen Informationsverbünden reicht im Allgemeinen die Umsetzung dieser Maßnahme.

Zunächst sollte ein Protokollierungskonzept für die Institution erstellt werden. Darin wird geregelt, wie, wo und was bei welchem Schutzbedarf protokolliert werden soll. Generell sollte jede Anmeldung unter administrativen Rechten immer zu einem Eintrag im Protokoll führen. Was mit den protokollierten Ereignissen geschehen soll, muss ebenfalls Bestandteil des Konzepts sein und wird in M 4.431 *Auswahl und Verarbeitung relevanter Informationen für die Protokollierung* beschrieben. Im Folgendem werden Aspekte vorgestellt, die bei der Konzeption berücksichtigt werden sollten.

**Zentrale oder lokale Protokollierung**

Ziel der Protokollierung ist es, wesentliche Veränderungen an IT-Systemen, Netzen oder Anwendungen nachvollziehen zu können, um deren Sicherheit aufrechterhalten zu können. Hierbei kann zwischen lokaler und zentraler Protokollierung unterschieden werden.

Bei der zentralen Protokollierung werden Protokollinformationen, die von verschiedenen IT-Systemen generiert werden, auf ein dediziertes IT-System übertragen und dort ausgewertet. So lassen sich die zu protokollierenden Ereignisse an einer Stelle auswählen, filtern und auswerten. Dies bietet unter anderem den Vorteil, dass Sicherheitsprobleme und Angriffe auf verschiedene IT-Systeme in Zusammenhang gebracht und so besser erkannt werden können. Die dabei relevanten Aspekte werden in M 3.90 *Allgemeine Grundlagen für die zentrale Protokollierung* detailliert beschrieben.

Bei einer lokalen Protokollierung verbleiben die zu betrachtenden Ereignisse auf den IT-Systemen, die sie erzeugt haben. Dort werden sie ausgewählt, gefiltert und ausgewertet. Die Alarmierung, wenn ein bestimmtes Ereignis eintritt, erfolgt ebenfalls dezentral von den jeweiligen IT-Systemen aus.

Bei der Planung der Protokollierung ist für die verschiedenen IT-Komponenten zu entscheiden, ob auftretende Ereignisse lokal oder zentral protokolliert werden sollen. Generell wird der Einsatz einer zentralen Protokollierung empfohlen. Aber nicht alle IT-Systeme lassen eine zentrale Protokollierung zu.

**Planung der Protokollierung**

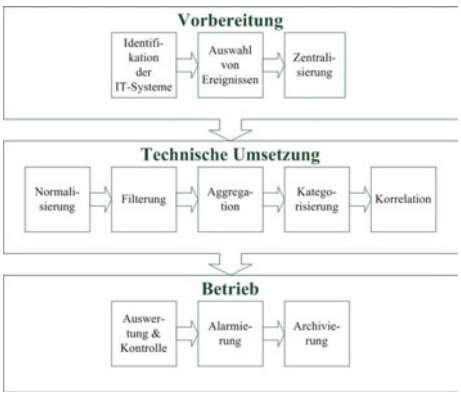



Abbildung: Schritte bei der Protokollierung

Je nachdem, ob lokal oder zentral protokolliert wird, können verschiedene Schritte erforderlich sein. Diese müssen im Protokollierungskonzept berücksichtigt werden und umfassen:

- Identifikation der IT-Systeme
  Es muss entschieden werden, welche IT-Systeme, Netze oder Anwendungen im Protokollierungskonzept berücksichtigt werden sollen. Generell sollten die sicherheitsrelevanten Ereignisse von allen IT-Systemen protokolliert und ausgewertet werden. Hierzu gehören unter anderem:
- Clients, inklusive mobiler IT-Geräte
- Server
- Netzkoppelelemente (Router und Switches)
- Datenbanken für wichtige Geschäftsprozesse
- TK-Anlagen und
- Sicherheitsgateways
  Soll zentral protokolliert werden, müssen die zu protokollierenden IT-Systeme dies unterstützen. Hierfür muss in der Regel ein Agent oder eine andere Applikation auf dem zu protokollierenden IT-System installiert werden. Diese Applikation nimmt die Ereignisse auf den jeweiligen IT-Systemen entgegen und sendet die Daten direkt an den zentralen Protokollierungsserver.
- Auswahl von sicherheitsrelevanten Ereignissen
  Grundsätzlich sollten alle sicherheitsrelevanten Vorkommnisse innerhalb eines Informationsverbundes protokolliert werden. Auf folgende Ereignisse ist beispielsweise besonders zu achten:
- abgewiesene Zugriffsversuche auf Benutzer-Kennungen, z. B. wegen falscher Passworteingaben,
- Sperrung von Benutzer-Kennungen,
- Anmeldungen von Benutzern oder Administratoren zu ungewöhnlichen Tageszeiten,
- Ausfall oder Störungen der Hardware,

- Fehlfunktionen oder Überlastungen der Applikationen, wie z. B. durch fehlenden Speicherplatz oder abgebrochene wichtige Prozesse,
- Daten zur Netzauslastung und -überlastung,
- Informations- oder Warnmeldungen von Intrusion Detection Systemen, sowie
- Zugriffe auf aktive Netzkomponenten (wer hat sich wann angemeldet?).

Welche Ereignisse insgesamt protokolliert werden sollten, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab und muss daher in der Institution vorab abgestimmt und festgelegt werden.

- Zentralisierung
  Es wird empfohlen, alle protokollierten Daten an einer Stelle zusammenzufassen. Dies können bei einer lokalen Protokollierung einzelne Verzeichnisse sein, damit die Protokolldateien übersichtlich an einer Stelle abgelegt werden und schnell wiedergefunden werden können. Bei einer zentralen Protokollierung sollten die aufgetretenen Ereignisse über einen sicheren Kanal an einen zentralen Server übertragen und anschließend in einer Datenbank gespeichert werden.
- Normalisierung
  Die zusammengefassten, unterschiedlichen Meldungen können für die spätere Auswertung normalisiert werden, da es keinen einheitlichen Standard für Format und Übertragungsprotokoll gibt. Durch die Normalisierung lassen sich die unterschiedlichen Protokoll-Formate, wie beispielsweise Syslog, MS Eventlog, SNMP, Netflow oder IPFIX aneinander anpassen. Die unterschiedlichen Datenformate werden somit in ein einheitliches Format umgewandelt und können anschließend ausgewertet werden.
- Filterung
  Durch eine geeignete Filterung der Protokolldaten können je nach Einsatzzweck irrelevante Daten möglichst frühzeitig ausgesondert und somit vom weiteren Verarbeitungsprozess ausgeschlossen werden. Es werden die informativen Inhalte von den sicherheitsrelevanten Meldungen getrennt, danach erfolgen weitere Schritte.
- Aggregation
  Bei der Aggregation können die protokollierten Ereignisse mit redundantem Inhalt zu einem Datensatz zusammengefasst werden. Oft werden identische Protokollmeldungen mehrmals hintereinander von dem gleichen IT-System erzeugt, daher ist es oft ausreichend, nur das erste Ereignis zu verarbeiten. Treten redundante Ereignisse auf, sollte die Anzahl der aufgetretenen Ereignisse abgespeichert werden, um nachträglich feststellen zu können, wie häufig die identischen Protokollmeldungen auftraten.
- Kategorisierung und Priorisierung
  Insbesondere bei einer zentralen Protokollierung können die protokollierten Ereignisse kategorisiert und priorisiert werden. Dadurch lässt sich der Informationsgehalt der Meldung noch stärker verfeinern.
- Korrelation
  Innerhalb eines Informationsverbundes haben die unterschiedlichen IT-Systeme, wie Sicherheitsgateways, Server und Clients, nur eine beschränkte Sicht auf ihre jeweilige Funktion. Um dieses Problem zu beseitigen, können die entsprechenden Protokolldaten korreliert werden. Beispielsweise lassen sich Sicherheitsgateway-Protokolldaten und Router-Protokolleinträge verbinden.
- Auswertung und Kontrolle
  Nur wenn die protokollierten Ereignisse regelmäßig ausgewertet und kontrolliert werden, können eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkannt werden. Eine Analyse zeigt neben Sicherheitsereignissen und Fehlern auch Informationen über die aktuelle Auslastung an.

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten in regelmäßigen Abständen durch einen Revisor ausgewertet werden, also von einer Person, die die jeweiligen Systeme nicht administriert. Ist es personell oder technisch nicht möglich, die Rolle eines unabhängigen Revisors für Protokolldateien zu besetzen, kann ihre Auswertung auch durch einen Administrator erfolgen. Möglichst sollte dies aber nicht der für den Betrieb der jeweiligen Systeme zuständige Administrator sein, da sonst die administrativen Tätigkeiten nur schwer kontrolliert werden können.
Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, Werkzeuge zur Auswertung, wie beispielsweise grafische Benutzeroberflächen oder Berichtsgeneratoren, zu benutzen. Diese Werkzeuge sollten wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfache fehlerhafte Anmeldeversuche) hervorheben.
Vertiefende Informationen zur Auswertung sind in M 2.64 *Kontrolle der Protokolldateien* zu finden.

- Alarmierung
  Treten bestimmte, vorher als kritisch festgelegte Ereignisse ein oder werden Schwellwerte überschritten, sollte ein Alarm beispielsweise per E-Mail oder SMS ausgelöst werden. Um eine sinnvolle Alarmierung durchführen zu können, ist es wichtig, die Anzahl der Fehlalarme zu reduzieren. Dazu müssen Schwellwerte realistisch eingestellt und an die Gegebenheiten des Informationsverbundes angepasst werden.
- Archivierung
  Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokolldateien gelten. Um die Nachvollziehbarkeit von Aktionen zu gewährleisten, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch Löschungspflichten geben (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*). Wenn Protokolldaten archiviert werden, sind die Empfehlungen von B 1.12 *Archivierung* zu berücksichtigen.

**Vertraulichkeit und Integrität der protokollierten Ereignisse**

Einige Datenquellen generieren Protokollmeldungen, die eine konkrete Zuordnung zu einer Person ermöglichen. Daher sollte gewährleistet werden, dass nur berechtigte Personen die protokollierten Ereignisse einsehen können. Es sollte ebenfalls nicht möglich sein, dass protokollierte Ereignisse von Unbefugten gelöscht oder nachträglich geändert werden können. Dies darf nur Personen vorbehalten sein, die unter einer Rolle wie Revisor angemeldet sind. Wenn technisch möglich, sollte es auch unter Administrator-Rollen nicht möglich sein, die Daten zu löschen oder zu ändern.

Daher muss durch entsprechende Dateisystemrechte der Zugriff durch Unberechtigte verhindert werden. Auch während der Übertragung von Protokolldaten bei einer zentralen Protokollierung sollten die Ereignisse geschützt werden, beispielsweise durch Verschlüsselung oder indem sie über ein eigenes Administrationsnetz (Out-of-Band-Management) übertragen werden. Auf diese Weise wird auch der Schutz der Integrität und Vertraulichkeit der Protokollmeldungen während der Übertragung erhöht.

Bei einem höheren Schutzbedarf ist zu prüfen, ob die protokollierten Ereignisse auf ein WORM-Medium ("Write Once Read Many") geschrieben werden. Diese Datenträger lassen sich nur einmalig beschreiben, eine nachträgliche Änderung der beschriebenen Datenträger ist nicht möglich.

**Zeitsynchronisation**

Um Angriffe auf IT-Systeme, Netze und Anwendungen oder deren Fehlfunktionen erkennen zu können, sollte auf allen IT-Systemen und virtuellen Instanzen die gleiche Uhrzeit eingestellt sein. Um auch in einem großen Informationsverbund sicherzustellen, dass alle Systeme zeitsynchron sind, ist ein zentraler Zeitserver zu verwenden. Dieser stellt den zentralen Zeittakt zum Beispiel über das Network Time Protokoll (NTP) zur Verfügung (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*). Alle weiteren Systeme im Informationsverbund können sich über diesen Zeittakt synchronisieren.

Prüffragen:

- Gibt es eine Konzeption zur Protokollierung?
- Sind die protokollierten Ereignisse vor dem Zugriff von Unbefugten geschützt?

# M 2.501 Datenschutzmanagement

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter

Mit Datenschutzmanagement werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen. Datenschutzmanagement ist die übergeordnete Umsetzung des Datenschutzes in einer Organisation oder bei Großverfahren. Nachfolgend wird ein Musterprozess für das Datenschutzmanagement beschrieben, der als Beispielprozess und Vorschlag zu sehen ist. Der Prozess orientiert sich an den BSI-Standards 100-1 und 100-2 und ist als integrativer Bestandteil des Sicherheitsprozesses nach IT-Grundschutz anzusehen, kann aber auch als eigenständiger Prozess behandelt werden, wenn vorrangig der Datenschutzaspekt behandelt werden soll. Sinnvollerweise wird dieser Prozess nicht für einzelne Verfahren eingerichtet und betrieben, sondern für die gesamte Organisation und alle Verfahren, in denen personenbezogene Daten verarbeitet werden.

### Der Datenschutzprozess

Herzstück des Datenschutzmanagements ist der Datenschutzprozess. Er ist wie der Sicherheitsprozess als zyklischer Prozess ausgelegt, um bei geändertem Umfeld die Einhaltung geltenden Datenschutzrechtes kontinuierlich sicherstellen zu können. Er deckt die Aufgaben in einer Organisation ab, die sich auf strategischer, taktischer oder operativer Ebene ergeben. Der Prozess bedient sich dabei einzelner Maßnahmen, die im Folgenden beschrieben sind. Er ist so ausgelegt, dass er die Errichtung eines Datenschutzmanagements auch in Organisationen ermöglicht, die noch über keine Strukturen zur Umsetzung des Datenschutzes verfügen. Die folgende Abbildung stellt den Prozess dar:

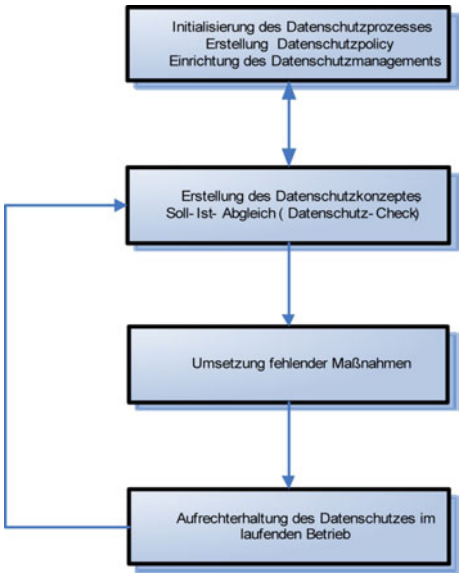



Abbildung 1: Datenschutzprozess

Im Folgenden werden die nun die einzelnen Prozessschritte bzw. Teilprozesse erläutert.

**Initialisierung des Datenschutzprozesses**

In diesem Prozessschritt sind die Maßnahmen angesiedelt, die eine strategische Zielstellung (Geltungsdauer bis zu fünf Jahren) haben. Sie beinhalten:

Erarbeitung einer Datenschutz-Richtlinie, in der Regel im Rahmen einer behörden- oder unternehmensweiten Sicherheitsrichtlinie: Diese kann als Zielstellungen unter anderem formulieren:

- Regelkonformität ("Compliance") mit minimalen Aufwand oder
- Datenschutz als Wettbewerbsvorteil ("USP": Unique Selling Proposition)

Einrichtung eines Datenschutzmanagements, in der Regel innerhalb des Sicherheitsmanagements. Wichtige Teilaspekte sind die Regelung der Zuständigkeiten (Rolle und Funktion des Datenschutzbeauftragten in Abgrenzung zu und Zusammenarbeit mit den Datensicherheitsbeauftragten), Prozessdefinitionen und Bereitstellung von Ressourcen (Personalkapazitäten).

**Erstellung eines Datenschutzkonzepts**

Das Datenschutzkonzept ist das Pendant zum Sicherheitskonzept (Geltungsdauer ein bis drei Jahre). Für den Inhalt wird auf Maßnahme M 2.503 *Aspekte eines Datenschutzkonzeptes* verwiesen.

**Umsetzung der erforderlichen Maßnahmen**

Dieser Prozessschritt beinhaltet die Umsetzung der im Datenschutzkonzept festgelegten, bislang noch nicht umgesetzten Maßnahmen. Die Umsetzung erfolgt im Rahmen eines klassischen Projektmanagements mit einem Projekt- und Arbeitsplan.

**Aufrechterhaltung des Datenschutzes im laufenden Betrieb**

Die Aufgabe dieses Teilprozesses ist es, auf Änderungen und Störungen im laufenden Betrieb der Verfahren zu reagieren, in denen personenbezogener Daten verarbeitet werden. Dies sind vor allem:

- Änderungen im Datenschutzrecht
- Änderungen in den (IT-)Verfahren
- Störungen in den operativen Betriebsabläufen, die als Sicherheitsvorfall zu klassifizieren sind
- Technischer Fortschritt und reduzierter Aufwand für bisher nicht realisierte Maßnahmen.

Zu diesem Zweck wird begleitend zum Sicherheitsprozess eine Reihe von Sub-Prozessen benötigt, die Änderungen und Störungen aus Datenschutzsicht eigenständig bearbeiten bzw. lösen. Die Ergebnisse können gegebenenfalls auch Strukturänderung im Datenschutzmanagement oder Aktualisierungen des Datenschutzkonzeptes (Aktualisierung) zur Folge haben.

Die folgende Abbildung stellt die Sub-Prozesse in einer Übersicht dar:

Abbildung 2: Teilprozesse der

Aufrechterhaltung des Datenschutzes im laufenden Betrieb

**Management von Sicherheitsvorfällen**

Das Management von Sicherheitsvorfällen bei IT-Verfahren im laufenden Betrieb muss auch gegebenenfalls die Vorfälle und ihre Folgen unter dem Gesichtspunkt des geltenden Datenschutzrechtes behandeln. Dies geschieht zweckmäßigerweise in Zusammenarbeit mit dem IT-Sicherheitsbeauftragten, der das Sicherheitsvorfall-Team leitet. Aufgaben des begleitenden Datenschutzmanagements können hier sein:

- Priorisierung von technischen und organisatorischen Maßnahmen zur Problemanalyse und Problemlösung bzw. Beweissicherung unter Datenschutzgesichtspunkten
- Behandlung juristischer Aspekte unter dem Gesichtspunkt des Datenschutzrechtes.

Unter dem Gesichtspunkt der Prozessintegration ist es sinnvoll, dass der Sicherheitsprozess das entsprechende Datenschutzmanagement auslöst bzw. den entsprechenden Sub-Prozess aufruft. In der Praxis kann dies beispielsweise bedeuten, dass bei Sicherheitsvorfällen, die Verfahren betreffen, in denen personenbezogene Daten verarbeitet werden, der Datenschutzbeauftragte automatisch Mitglied des Sicherheitsvorfall-Teams wird. Er kann so in die Informationen und Prozessabläufe optimal eingebunden werden. Unter diesem Management ist auch eine Beschreibung zu verstehen, wo bzw. von wem im Unternehmen oder der Behörde Datenschutzvorfälle gemanagt werden.

**Management der Lebenszyklen von IT-Verfahren unter Datenschutzgesichtspunkten**

Beim Management der Lebenszyklen von IT-Produkten und -Verfahren kommt ein Lebenszyklusmodell zur Anwendung, das sich am allgemeinen Lebenszyklusmodell der BSI-Standards und der IT-Grundschutz-Kataloge orientiert.

Innerhalb der jeweiligen Phasen ist eine Reihe von Maßnahmen aus dem Baustein B 1.5 *Datenschutz* zu berücksichtigen. Dies umfasst:

- In der Planung und Konzeption die Maßnahmen: M 2.501 *Datenschutzmanagement* bis M 2.505 *Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten*
- Bei der Umsetzung der Planung und Konzeption bis hin zum laufenden Betrieb die Maßnahmen: M 2.506 *Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten* bis M 2.512 *Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten*
- Im laufenden Betrieb die Maßnahmen: M 2.513 *Dokumentation der datenschutzrechtlichen Zulässigkeit* bis M 2.515 *Datenschutzgerechte Löschung/Vernichtung*
- Nach Einstellung bis zur endgültigen Löschung des Verfahrens und aller zugehörigen Daten die Maßnahmen: M 2.508 *Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten*, M 2.110 *Datenschutzaspekte bei der Protokollierung* und M 2.515 *Datenschutzgerechte Löschung/Vernichtung*

Darüber hinaus sollte bei der Planung und Konzeption von neuen IT-Verfahren geprüft werden, ob Privacy Enhancing Technologies (PETs) eingesetzt werden können. PETs unterstützen technisch die Umsetzung von Datenschutzgrundsätzen wie Datensparsamkeit, Zweckbindung oder das Transparenzge-

bot. Beispiele für PETs sind Protokolle wie P3P (Platform for Privacy Preferences) und Verfahren zur Anonymisierung und Pseudonymisierung von Daten beim Netzwerktransfer, der Datenhaltung in Datenbanken oder dem Data-Mining (Privacy Preserving Data Mining, PPDM). Aber auch Wiedervorlagefunktionen in Programmen, die die Einhaltung von Löschfristen bei der Speicherung von personenbezogenen Daten unterstützen, zählen dazu.

**Management von Änderungen im Datenschutzrecht**

Änderungen im Datenschutzrecht sind zu verfolgen und hinsichtlich ihrer Auswirkungen auf die Verfahren, in denen personenbezogene Daten verarbeitet werden, zu beurteilen. Dieser Sub-Prozess lässt sich auch in das behörder- oder unternehmensweite Monitoring von Änderungen in relevanter Gesetzgebung integrieren.

**Technologie-Monitoring**

Das Technologie-Monitoring verfolgt gemeinsam mit dem Sicherheits-Management den "Stand der Technik" bezogen auf Informationssicherheit und Datenschutz. Unter Maßgabe der einschlägigen Datenschutzgesetzgebung und deren Anwendung gibt dieser Sub-Prozess Impulse für die Weiterentwicklung von Datenschutz- und Sicherheitskonzept.

**Monitoring und Management von Änderungen in den IT-Grundschutz-Katalogen**

Beim allgemeinen Monitoring sind auch Aktualisierungen der BSI-Standards und der IT-Grundschutz-Kataloge, insbesondere des Datenschutzbausteins zu berücksichtigen. Neben Impulsen für die Weiterentwicklung von Datenschutz- und Sicherheitskonzept sind auch die Schnittstellen zu Sicherheitsmanagement zu überprüfen und gegebenenfalls anzupassen.

**Zusammenfassung**

Das vorgeschlagene Prozessmodell bietet vielfältige Anknüpfungspunkte und dadurch Synergien zu den entsprechenden Sicherheitsprozessen der BSI-Standards. Diese Synergien können von einer Kooperation der Prozesse, der Integration von Dokumenten (z. B. Datenschutz- und Sicherheitskonzept) und Dokumentation bis hin zur vollständigen Integration der Prozesse reichen. Dies kann sich auch auf Funktionsträger erstrecken: ein IT-Sicherheitsbeauftragter kann die Rolle des Datenschutzbeauftragten in Personalunion wahrnehmen, wenn er die geeignete Sachkunde mitbringt und im Bereich der IT nicht gleichzeitig konzeptionelle und operative Aufgaben wahrnimmt (Vermeidung einer Interessenkollision). Dies ist insbesondere in kleinen Organisationen von Bedeutung.

Die folgende Abbildung 3 stellt dies schematisch dar.

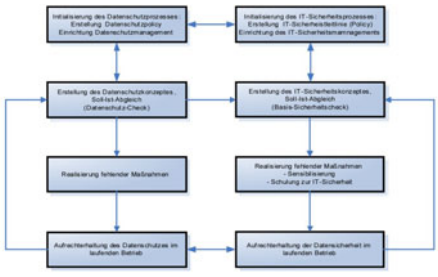


Abbildung 3: Schematische Darstellung von

Wechselwirkungen und Synergien zwischen Datenschutz- und Datensicherheitsprozess

Prüffragen:

- Liegt eine aktuelle Datenschutz-Richtlinie vor?
- Sind Datenschutz- und Sicherheitsmanagement aufeinander abgestimmt?
- Werden Änderungen im Datenschutzrecht und von anderen Rahmenbedingungen verfolgt und in den Datenschutzprozess integriert?

# M 2.502 Regelung der Verantwortlichkeiten im Bereich Datenschutz

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung

Datenschutz ist für alle IT-Systeme und -Verfahren, mit deren Hilfe personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Die Aspekte des Datenschutzes sind daher von Beginn der Planungen zur Einführung eines IT-Verfahrens im Rahmen des Sicherheitsmanagements zu integrieren. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtlich anfallende Aufgaben effizient und effektiv erledigt werden.

Eine detaillierte Auflistung zu bearbeitender Aufgaben und zu treffender Regelungen, die unter datenschutzrechtlichen Aspekten zu betrachten sind, sind zu finden in M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen*.

Die Bestellung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) und seine Integration in das Sicherheitsmanagement ist eine Maßnahme, die sich dazu in besonderem Maße eignet. Es besteht auch die Möglichkeit, einen externen bDSB zu bestellen.

Der bDSB kontrolliert eigenständig die Einhaltung des Datenschutzes, bildet aber auch gewissermaßen das Bindeglied zwischen der eigenverantwortlichen Gesetzesanwendung durch die datenverarbeitende Stelle auf der einen und der staatlichen Kontrolle auf der anderen Seite.

Die Bestellung ist, von wenigen Ausnahmen abgesehen, gesetzlich vorgeschrieben:

- Für öffentliche Stellen des Bundes und nicht-öffentliche Stellen im BDSG (§§ 4 f, g) und für die Sozialversicherungsträger im Sozialgesetzbuch (§ 35 SGB I, § 81 Abs. 1 SGB X i. V. m. §§ 4 f, g BDSG).
- Für öffentliche Stellen der Länder ist die Pflicht zur Bestellung in einigen Landesdatenschutzgesetzen ebenfalls vorgeschrieben.

Auch in den Bereichen, in denen eine Bestellung eines Datenschutzbeauftragten nicht erfolgt, muss die Einhaltung der datenschutzrechtlichen Anforderungen sichergestellt sein. Dies kann auch durch das Sicherheitsmanagement erfolgen. Hierzu sollte zumindest eine interne IT-Revision und Datenschutzkontrolle eingerichtet werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

### Bestellung eines Datenschutzbeauftragten

Zum Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

Zur Aufgabenerfüllung gehören technische, organisatorische und rechtliche Kenntnisse. Der bDSB muss die gesetzlichen Regelungen, wie z. B. das Recht auf informationelle Selbstbestimmung, die Grundrechte mit Datenschutzbezug, das Bundesdatenschutzgesetz, bereichsspezifische datenschutzrechtliche Regelungen und die einschlägigen Spezialvorschriften des Fachbereichs, kennen und sicher anwenden können. Er sollte ferner gute Kenntnisse der Organisation und vertiefte Kenntnisse der Informationstechnik besitzen.

Soweit ihm die fachliche Qualifikation in Teilbereichen noch fehlt, ist ihm Gelegenheit zu geben, diese zu erwerben. Mit den Aufgaben und der Arbeitsweise seiner Behörde bzw. seines Unternehmens sollte der bDSB möglichst aus eigener Erfahrung gut vertraut sein, um seinen Kontroll- und Beratungsaufgaben nachkommen zu können.

Der bDSB muss nicht ausschließlich mit den Funktionen eines Datenschutzbeauftragten betraut sein. Je nach Art und Umfang der personenbezogenen Datenverarbeitung und der damit verbundenen Datenschutzprobleme kann es angebracht sein, ihm daneben weitere Aufgaben zu übertragen. Dies wird besonders bei kleineren Behörden bzw. Unternehmen in Betracht kommen, wenn die Einarbeitungszeit oder die Aufbauperiode abgeschlossen ist.

Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die seine Aufgabenerfüllung gefährden. Interessenkonflikte können insbesondere dann auftreten, wenn der bDSB gleichzeitig Aufgaben in den Bereichen Personal, Informationstechnik oder in Organisationseinheiten mit besonders umfangreicher oder sensitiver Verarbeitung von personenbezogenen Daten wahrnimmt oder Geheimschutzbeauftragter ist. Möglich ist dagegen die Zusammenlegung der Funktionen des bDSB mit denen des IT-Sicherheitsbeauftragten. Ist der IT-Sicherheitsbeauftragte organisatorisch unabhängig von der für die IT verantwortlichen Organisationseinheit eingerichtet, ist die Zusammenfassung in einer Hand empfehlenswert. Auch der Leiter oder ein Mitarbeiter der Bereiche Justitiariat/Recht oder Organisation bietet sich für die Aufgabe an.

Im Interesse einer späteren vertrauensvollen Zusammenarbeit sollte der Personal- bzw. Betriebsrat im Verfahren der Bestellung des bDSB frühzeitig beteiligt werden.

Wenn die Bestellung gesetzlich vorgeschrieben ist, gelten meist bestimmte Formvorschriften. In jedem Fall ist die Bestellung zum bDSB allen Mitarbeitern bekannt zu machen. Dabei ist darauf hinzuweisen, dass jeder Mitarbeiter sich in eigenen und dienstlichen Angelegenheiten unmittelbar an den bDSB wenden kann.

Die unabhängige und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des bDSB von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben nicht den Weisungen der Organisationseinheiten unterliegen, die er zu kontrollieren hat. In seiner Funktion als bDSB sollte er der Leitung des Hauses zugeordnet sein, entweder durch unmittelbare Unterstellung oder im Sinne einer Stabsfunktion. Dies ist im Organigramm für alle Mitarbeiter erkennbar darzustellen.

Der bDSB muss das direkte und jederzeitige Vortragsrecht bei der Behörden- bzw. Unternehmensleitung haben und über das Geschehen in der Behörde bzw. dem Unternehmen, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet werden. Er ist an datenschutzrelevanten Vorgängen zu beteiligen, und Planungen, die den Umgang mit personenbezogenen Daten betreffen, sind ihm bekannt zu geben.

Der bDSB muss von der Behörden- bzw. Unternehmensleitung und von allen Mitarbeitern unterstützt werden. Soweit erforderlich, sind ihm Hilfspersonal sowie Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Für den Fall, dass er vertiefte rechtliche oder technische Beratung benötigt, müssen ihm geeignete Ansprechpartner der betreffenden Fachabteilungen benannt werden, auf die er bei Bedarf zurückgreifen kann.

Der bDSB soll dazu beitragen, dass seine Behörde bzw. sein Unternehmen den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Er hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen. Er nimmt seine Aufgaben im Wesentlichen durch Beratung und Kontrollen wahr. Seine vorrangige Aufgabe ist die Beratung. Für die Mitarbeiter sollte der bDSB Ansprechpartner in allen Fragen des Datenschutzes sein, an den sie sich jederzeit vertrauensvoll wenden können.

Bei Schwachstellen und Versäumnissen sollte er zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen. Wichtig ist dabei, den Mitarbeitern bewusst zu machen, dass Datenschutz positiv und nützlich ist. Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren. Wenn nämlich eine Behörde bzw. ein Unternehmen zu viele personenbezogene Daten sammelt, personenbezogene Daten zu spät löscht oder unberechtigt übermittelt, verstößt sie nicht nur gegen Datenschutzrecht, sondern verursacht auch erhöhten Verwaltungsaufwand und Mehrkosten. Vor allem ist der Datenschutz ein wichtiges Element eines bürger- und kundenfreundlichen Verhaltens, weil er die Verfahrensabläufe transparent macht.

Der bDSB hat das Recht, jederzeit unangekündigte Kontrollen durchzuführen. Zu diesem Zweck hat er Zutritt zu allen Räumen und kann alle Unterlagen einsehen, die personenbezogene Daten enthalten oder den Umgang mit diesen betreffen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Allerdings ist die Einsicht in Personalakten, ärztliche Unterlagen, Beihilfeakten und Sicherheitsvorgänge nur mit Einwilligung des Betroffenen zulässig.

Bei Kontrolle und Beratung im Bereich einer Personalvertretung ist deren unabhängige Stellung zu beachten. Dies schließt die Durchführung von Kontrollen allerdings nicht aus.

Der bDSB hilft der Behörden- bzw. Unternehmensleitung, ihre Verantwortung für die Wahrung des Persönlichkeitsschutzes wahrzunehmen und Zwischenfälle zu vermeiden, die dem Ansehen der Behörde bzw. des Unternehmens abträglich wären. Er sollte auch Kontakt zum Personal- bzw. Betriebsrat halten. Eine gute Zusammenarbeit ist nicht nur wegen der Sensibilität der Personaldatenverarbeitung wünschenswert.

Zur sachgemäßen Durchführung seiner Aufgaben hat sich der bDSB weiterzubilden. Sehr nützlich ist auch der Erfahrungsaustausch im Kreis mit anderen bDSB des Geschäftsbereichs oder aus Behörden bzw. Unternehmen mit ähnlichen Fachaufgaben.

Der spezielle Zuschnitt der Aufgaben des bDSB richtet sich im Einzelfall nach den zu erfüllenden Aufgaben, aber auch nach Größe, dem Aufbau und der Gliederung der jeweiligen Behörde bzw. des Unternehmens.

Der folgende Katalog gibt einen Überblick über die Aufgaben, die dem bDSB in jeder Behörde bzw. jedem Unternehmen übertragen werden können:

**Grundlegende Aufgaben:**
- Beratung der Hausleitung und der übrigen Mitarbeiter in datenschutz-relevanten Fragen
- Durchführung angekündigter oder unangekündigter Kontrollen

**Übersichten und Register:**
- Führung oder Überwachung der Führung des Verzeichnisses der eingesetzten Datenverarbeitungs-anlagen

- Führung der Übersicht über alle Dateien und Verfahren, in denen personenbezogene Daten gespeichert sind oder verarbeitet werden
- Wahrnehmung der gesetzlichen Meldepflichten

**Automatisierte Abrufverfahren und Auftragsdatenverarbeitung:**
- Unterrichtung der zuständigen Datenschutzkontrollinstanz über automatisierte Abrufverfahren
- Kontrolle der Einhaltung der Weisungen des Auftraggebers bei Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

**Mitwirkung:**
- Erarbeitung oder Mitwirkung bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen und weiteren allgemeinen Verlautbarungen, die den Umgang mit personenbezogenen Daten betreffen
- Bearbeitung oder Mitwirkung bei Auskunfts-, Berichtigungs-, Sperrungs- oder Löschungsverlangen, bei der Erstellung von Bürgerinformationen sowie bei allgemeinen Bürgereingaben und Anfragen zum Datenschutz
- Beteiligung bei der Auswertung von Protokolldateien
- Beteiligung bei der Einführung von Verfahren zur Verarbeitung personenbezogener Daten durch die Fachabteilung
- Beteiligung bei Regelungen zur Informationssicherheit

**Schulung und Zusammenarbeit:**
- Schulung der Mitarbeiter in datenschutzrechtlichen Aspekten sowie zur Umsetzung datenschutzrechtlicher Bestimmungen
- Regelmäßige oder gelegentliche Berichte an die Hausleitung über den Stand des Datenschutzes innerhalb der Behörde bzw. des Unternehmens
- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten
- Ansprechpartner der externen Datenschutz-Kontrollinstanzen, z. B. des Bundesbeauftragten für den Datenschutz und gegebenenfalls der Datenschutzbeauftragten der vorgesetzten Behörde bzw. des Unternehmens, anderer Behörden bzw. Unternehmen des Geschäftsbereichs und öffentlicher Stellen mit verwandten Aufgaben

Prüffragen:

- Wurde ein Datenschutzbeauftragter bestellt?
- Ist der Datenschutzbeauftragte ausreichend qualifiziert?
- Stehen dem Datenschutzbeauftragten ausreichend Ressourcen zur Verfügung?
- Sind die Aufgaben und Kompetenzen des Datenschutzbeauftragten klar definiert?

# M 2.503 Aspekte eines Datenschutzkonzeptes

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter

Für ein Unternehmen bzw. eine Behörde ist festzulegen und zu dokumentieren, welche Anforderungen des Datenschutzes bei der Verarbeitung personenbezogener Daten eingehalten werden müssen und wie diese Anforderungen umgesetzt worden sind. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines individuellen Datenschutzkonzeptes für einzelne Verfahren zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig und auch für neue IT-Systeme anwendbar ist, für die noch kein Datenschutzkonzept erarbeitet wurde.

Vorrangig sind natürlich die jeweils geltenden gesetzlichen Bestimmungen zu beachten. In diesem Umfeld gibt es allerdings allgemein gültige Aspekte, die bei der Verarbeitung personenbezogener Daten in der Regel zu berücksichtigen sind. Die genannten Aspekte sollen auch als Orientierungshilfe für individuelle Datenschutzkonzepte dienen.

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen und kann auch als Grundlage für datenschutzrechtliche Prüfungen genutzt werden.

**Zu berücksichtigende Aspekte**

- Verzeichnis aller Verfahren
- Umfang und Verwendung der zu verarbeitenden personenbezogenen Daten. Ist ein direkter Bezug (z. B. Adresse, Steuerdaten) oder ein indirekter Bezug vorhanden (z. B. Kfz-Kennzeichen, Flurstück)?
- Rechtsgrundlage der Verarbeitung
- Zweckbindung
- Berücksichtigung besonderer Datenarten
- Einhaltung von Datensparsamkeit, Datenvermeidung
- Schutzbedarf der Daten: Schutzbedarfsfeststellung nach Schutzstufenkonzept und unter Berücksichtigung des Verwendungszusammenhangs (normal, hoch, sehr hoch) nach datenschutzrechtlichen Gesichtspunkten, Kategorienbetrachtung siehe BSI-Standard 100-2, Kapitel 4.2 oder auch Schutzstufenkonzepte in verschiedenen Bundesländern
- Besonderheiten bei "Automatisierten Abrufverfahren"
- Verbot automatisierter Bewertungen
- Recht auf Auskunft, Berichtigung, Sperrung, Widerspruch, Schadensersatz
- Vermeidung von Rechtsverletzungen und ihrer Folgen
- Löschung von Daten
- Protokollierung
- Vorabkontrolle (dazu gibt es Checklisten in verschiedenen Bundesländern)
- Regelung der Verantwortlichkeiten im Datenschutz (siehe M 2.502 *Regelung der Verantwortlichkeiten im Bereich Datenschutz*)
- Dokumentation und Verfahrensweise der Beteiligung des betrieblichen bzw. behördlichen Datenschutzbeauftragten

- Dokumentation und Verfahrensweise der Beteiligung des Bundes- oder Landesbeauftragten für Datenschutz oder Beteiligung der Aufsichtsbehörde
- Vertragliche Regelungen einer Auftragsdatenverarbeitung
- Besonderheiten einer Datenverarbeitung in Drittländern (unter Anderem Safe-Harbor-Regeln)
- Technische und organisatorische Maßnahmen nach der Anlage zu § 9 BDSG bzw. entsprechenden Regelungen in den Landesdatenschutzgesetzen oder/und nach den spezialgesetzlichen Bestimmungen, Zuordnung der Maßnahmen der IT-Grundschutz-Kataloge nach Zielvorgaben der Gesetze (Basis-Sicherheitscheck-Tabellen des BSI, eine Tabelle zu Baustein B 1.5 *Datenschutz* ist auf den BSI-Webseiten unter den Hilfsmitteln zum IT-Grundschutz zu finden), Soll-Ist-Abgleich bei der Umsetzung und späteren Revision und datenschutzrechtlichen Kontrolle
- Verpflichtung auf den Datenschutz bzw. entsprechende Unterrichtung (siehe Formblatt des BfDI im Internetangebot unter www.bfdi.de oder entsprechende Merkblätter der Datenschutzbeauftragten und Aufsichtsbehörden)
- Freigabe der Verfahren
- Verfahrensbeschreibung für jedes Verfahren
- Meldungen an Registerstellen (siehe auch M 2.510 *Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten*)
- Bestellung und Aufgaben eines Datenschutzbeauftragten (siehe Maßnahme M 2.502 *Regelung der Verantwortlichkeiten im Bereich Datenschutz*)
- Berücksichtigung der unterschiedlichen datenschutzrechtlichen Zuständigkeiten (Bundesbeauftragter für Datenschutz, Landesbeauftragte für Datenschutz, Aufsichtsbehörden)

Prüffragen:

- Liegt ein Datenschutzkonzept vor, das alle Bereiche der Institution abdeckt?
- Wird das Datenschutzkonzept regelmäßig aktualisiert?
- Werden sämtliche Mitarbeiter, auch neu eingestellte, auf das Datenschutzkonzept verpflichtet bzw. unterrichtet?
- Sind ausreichende Betriebsmittel für die Umsetzung des Datenschutzkonzepts vorhanden?

# M 2.504 Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Fachverantwortliche, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche, IT-Sicherheitsbeauftragter

Im Rahmen der Prüfung der rechtlichen Rahmenbedingungen als Voraussetzung der Datenverarbeitung müssen folgende Aspekte betrachtet werden:

- Prüfung, ob personenbezogene Daten verarbeitet werden
- Zulässigkeit der Datenverarbeitung
- Erforderlichkeit der Datenverarbeitung
- Verwendung der Daten hinsichtlich der Zweckbindung
- Verwendung der Daten hinsichtlich der besonderen Zweckbindung
- Durchführung einer Vorabkontrolle

Bei der Betrachtung dieser Aspekte sollte wegen eventuell schwieriger Rechtsmaterie, insbesondere zu Datenschutzfragen, auf juristische Unterstützung zurückgegriffen werden.

**Zulässigkeit der Datenverarbeitung**

Für die Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt (z. B. § 4 Abs. 1 BDSG).

Die Prüfung der Zulässigkeit der Datenverarbeitung sollte im Regelfall in Zusammenarbeit mit den fachlich zuständigen Stellen erfolgen.

Vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist zu prüfen, ob

- dies durch die Datenschutzgesetze oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist oder
- der Betroffene gemäß § 4 BDSG oder entsprechender landes- oder spezialgesetzlicher Regelungen eingewilligt hat.

Bei der Speicherung, Veränderung und Übermittlung personenbezogener Daten durch nicht-öffentliche Stellen ist zu prüfen, ob dies

- im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen erfolgt oder
- zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (im Sinne von §§ 28 ff. BDSG).

**Prüfung der Erforderlichkeit**

Für öffentliche Stellen gilt der Grundsatz, dass personenbezogene Daten nur erhoben werden dürfen, wenn sie für die Aufgabenerfüllung erforderlich sind.

Das ist der Fall, wenn ohne ihre Kenntnis die Durchführung der betreffenden Aufgaben unmöglich oder wesentlich erschwert wäre. Dies ist im Einzelfall zu überprüfen.

Die einzelnen Nutzer dürfen nur auf diejenigen Daten zugreifen, die für die Erfüllung ihrer Aufgaben erforderlich sind.

Schwierigkeiten bereitet dies hinsichtlich der Systemverwalter. Sie haben in den marktüblichen Systemen beliebigen Zugriff auf alle Daten. Auch sie müssen in bestimmtem Umfang im Zugriff beschränkt werden, insbesondere dann, wenn es sich um Daten handelt, die einem besonderen Amtsgeheimnis unterliegen, wie etwa Personalaktendaten. Geeignete Maßnahmen hierfür sind Verschlüsselung der Daten, Zugriffsbeschränkungen, abgestufte Berechtigungskonzepte, Menüführung, Aufteilung der Systemadministratorfunktionen auf verschiedene Rollen sowie die sichere Protokollierung der Aktivitäten des Systemverwalters.

Bei der Gestaltung von Technik sind solche Verfahren zu wählen, bei denen möglichst wenig personenbezogene Daten verarbeitet werden. Es gilt das Gebot der Datenvermeidung bzw. Datensparsamkeit. Soweit möglich, sind Verfahren anonym zu gestalten oder Pseudonyme zu verwenden. Bei Dienstleistungsangeboten sollte den Kunden zumindest die Möglichkeit gegeben werden, ein anonymes Verfahren zu wählen.

**Prüfung der Verwendung von Daten hinsichtlich der Zweckbindung**

Vor der Speicherung, Veränderung und Nutzung personenbezogener Daten ist zu prüfen, ob dies für die Zwecke erfolgt, für die die Daten erhoben worden sind bzw., falls keine Erhebung voranging, es für die Zwecke erfolgt, für die sie gespeichert worden sind.

Von diesem Zweckbindungsgrundsatz gibt es eine Reihe, zum Teil weit reichender gesetzlicher Ausnahmen (siehe z. B. § 14 BDSG).

**Prüfung der Verwendung der Daten hinsichtlich der besonderen Zweckbindung**

Es ist zu prüfen, ob personenbezogene Daten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, auch ausschließlich für diese Zwecke verwendet werden (siehe z. B. § 14 Abs. 4, § 31 BDSG).

**Vorabkontrolle**

Im Rahmen der Vorabkontrolle ist vor dem erstmaligen Einsatz automatisierter Verfahren zur Bearbeitung personenbezogener Daten zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können.

Weist eine Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen auf wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle durchzuführen (§ 4d Abs. 5 BDSG). Eine Vorabkontrolle ist nicht durchzuführen, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die

Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. In manchen Landesdatenschutzgesetzen ist eine Vorabkontrolle generell bei allen Verfahren vorgeschrieben, mit denen personenbezogene Daten durch öffentliche Stellen verarbeitet werden. Die Voraussetzungen hierfür können von den beim Bund geltenden Regelungen abweichen.

Automatisierte Verfahren dürfen nur dann eingesetzt werden, wenn sichergestellt ist, dass keine Gefahren für das informationelle Selbstbestimmungsrecht bestehen.

Folgende Aspekte sind hierbei zu überprüfen:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobene Daten

Die zu ergreifenden Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Gefahren und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Werden personenbezogene Daten nicht automatisiert verarbeitet, sind Maßnahmen zu treffen, die den Zugriff Unbefugter bei der Verarbeitung, der Aufbewahrung, dem Transport und der Vernichtung verhindern.

Die Anforderungen weichen in den Formulierungen und Konsequenzen der einzelnen Landesdatenschutzgesetze voneinander ab. Eine Entscheidung über die Durchführung der Vorabkontrolle ist daher im Einzelfall zu treffen.

Prüffragen:

- Wird vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geprüft, ob dies erforderlich und rechtlich zulässig ist?
- Wird bei allen Geschäftsprozessen und Verfahren darauf geachtet, dass personenbezogene Daten angemessen geschützt sind?

# M 2.505 Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche, IT-Sicherheitsbeauftragter

Ein sehr wichtiger Bereich des Datenschutzes sind die technischen und organisatorischen Maßnahmen, die getroffen werden müssen, damit das Recht auf informationelle Selbstbestimmung gewährleistet ist und die personenbezogenen Daten vor Missbrauch, Fehlern und Unglücksfällen möglichst sicher sind.

Welche Maßnahmen notwendig sind, hängt nicht nur von der Art der Daten und der Aufgabe ab, für die sie verwendet werden sollen, sondern ebenso von den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen.

Die Gesetze verzichten deshalb darauf, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, sondern verlangen nur allgemein, "die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Gesetze zu gewährleisten".

Welche Wirkung diese Maßnahmen im Bereich der automatisierten Verarbeitung haben müssen, legen die Datenschutzgesetze katalogmäßig fest. Nach §9 BDSG müssen die Maßnahmen geeignet sein,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Diese Anforderungen weichen in den Formulierungen und Konsequenzen der einzelnen Landesdatenschutzgesetze voneinander ab.

Entscheidend bei Planung und Durchführung der technischen und organisatorischen Maßnahmen ist, dass sie als ein zusammenwirkendes Schutzsystem verstanden werden. Ein solches Schutzsystem sichert neben dem rechtlich erforderlichen Datenschutz auch die ordnungsgemäße Aufgabenerfüllung und einen ordentlichen Betriebsablauf. Deshalb ist es wichtig, das Datenschutzkonzept jeweils in Abstimmung mit den Fachkonzepten der betreffenden Organisationseinheiten und den sonstigen Sicherheitskonzepten, z. B. dem Informationssicherheitskonzept, zu entwickeln und anzuwenden.

Der Aufwand für die notwendigen Maßnahmen sollte in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen (zu den Schutzstufen siehe BSI-Standard 100-2 bzw. landesspezifische Regelungen zum Datenschutz). Je schwerer die den Betroffenen drohende Rechtsverletzung und je größer das Risiko eines Schadenseintritts ist, umso höher ist der angemessene Aufwand. Ein Ermessen besteht zwar bei der Auswahl der einzelnen Maßnahmen, nicht aber bei der Festlegung des Schutzniveaus. Als notwendig erkannte Maßnahmen sind auch dann zu treffen, wenn sie die Entwicklung und den Einsatz einer IT-Anwendung erschweren. Ist dies mit den vorgesehenen Maßnahmen nicht zu gewährleisten, muss entweder ein höherer Aufwand in Kauf genommen werden oder eine andere, mit weniger Aufwand verbundene Verfahrensgestaltung in Betracht gezogen werden. Diese Maßnahmen sind entsprechend dem aktuellen Stand der Technik fortzuschreiben.

Ebenso ist sicherzustellen, dass die gesetzlichen Datenschutzvorschriften durch Informationssicherheits- und Datenschutz-Regelungen umgesetzt werden.

Soweit ein behördlicher bzw. betrieblicher Datenschutzbeauftragter (bDSB) institutionalisiert ist (in einigen Datenschutzgesetzen bestehen hierzu gesetzliche Vorgaben), sollten Richtlinien, Rundschreiben o. ä., die die Hausleitung als Querschnittsregelung zum Umgang mit personenbezogenen Daten in der gesamten Dienststelle erlässt, mit seiner Beteiligung erarbeitet werden.

Er sollte stets bei der Behandlung von Dienst- bzw. Betriebsvereinbarungen zwischen Dienststelle bzw. Betrieb und Personal- bzw. Betriebsrat über den Umgang mit personenbezogenen Daten hinzugezogen werden. Die Einhaltung der Regelungen sollte kontrolliert werden.

Beispiele für technisch-organisatorische Maßnahmen sind

- das physikalische Löschen von Daten (siehe z. B. M 4.32 *Physikalisches Löschen der Datenträger vor und nach Verwendung*),
- die kryptographische Verschlüsselung (siehe z. B. M 5.36 *Verschlüsselung unter Unix und Windows NT*),
- interne IT- und Datenschutz-Regelungen (siehe z. B. M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen*) sowie

- Protokollierung und Dokumentation von Verfahren, um die Nachvollziehbarkeit zu gewährleisten (siehe z. B. M 4.25 *Einsatz der Protokollierung im Unix-System*).

Eine Übersicht der Maßnahmen der IT-Grundschutz-Kataloge, die zur Erreichung der oben genannten Anforderungen geeignet sind, wird in der Tabelle zu Baustein B 1.5 *Datenschutz* unter den Hilfsmitteln zum IT-Grundschutz dargestellt.

Prüffragen:

- Sind alle technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um ausreichenden Datenschutz zu gewährleisten?
- Existieren geeignete Vorgaben zum Umgang mit personenbezogenen Daten in der gesamten Institution?

# M 2.506 Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Personalabteilung, Vorgesetzte

Die bei der Datenverarbeitung beschäftigten Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung ihrer Tätigkeit fort. Die Verpflichtung/ Unterrichtung muss in geeigneter Weise durchgeführt werden, die Durchführung ist zu dokumentieren und sollte bei Bedarf wiederholt werden.

Einzelne Landesdatenschutzgesetze haben die Verpflichtung durch eine Unterrichtung ersetzt.

**Hinweis:**

Auch wenn eine Verpflichtung bzw. Unterrichtung der Mitarbeiter zur Wahrung des Datengeheimnisses bereits aus anderen Gründen besteht, sollte sie wiederholt werden, um die Mitarbeiter für die Belange des Datenschutzes zu sensibilisieren. Sowohl für den behördlichen als auch den betrieblichen Datenschutzbeauftragten gibt es als Hilfsmittel entsprechende Muster-Verpflichtungserklärungen des Bundesbeauftragten für Datenschutz unter www.bfdi.de. Für die Unterrichtung gibt es geeignete Merkblätter bei den Landesbeauftragten für Datenschutz.

Prüffragen:

- Werden alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet bzw. darüber unterrichtet?
- Werden die Mitarbeiter regelmäßig für die Belange des Datenschutzes sensibilisiert?

# M 2.507 Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Fachverantwortliche
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche

Es sind technisch-organisatorische Verfahren zu entwickeln, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in Dateien- bzw. Verfahrensverzeichnisse (soweit solche Verzeichnisse vorgeschrieben sind) sicherzustellen.

Diese Verfahren sollen so beschaffen sein, dass die Rechte der Betroffenen schnell und zweckmäßig umgesetzt werden können.

**Beispiele:**
- Ein Verfahren zur Verarbeitung personenbezogener Daten enthält ein Auswerteprogramm oder einen Menüpunkt, mit dessen Hilfe ein vollständiger Ausdruck der gespeicherten Daten des Betroffenen erzeugt wird.
- Ein Verfahrensverzeichnis wird mit Hilfe einer Datenbank so automatisiert, dass über bestimmte Stichworte ein sehr einfacher Zugriff auf den umfangreichen Datenbestand möglich ist und damit alle Querbezüge erkannt werden können.

Prüffragen:

- Existieren technisch-organisatorische Verfahren, um die Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten zu wahren?

# M 2.508 Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche

Neben den zentralen Datenverarbeitungsanlagen sind bei dezentraler Datenverarbeitung alle eingesetzten IT-Systeme zu erfassen (siehe auch BSI-Standard 100-2, Erfassung der IT-Systeme und Erfassung der IT-Anwendungen und der zugehörigen Informationen).

Es muss jederzeit auf ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten zugegriffen werden können. In einigen Datenschutzvorschriften gibt es konkrete Vorgaben für die Ausgestaltung dieser Verzeichnisse.

Verfahren automatisierter Verarbeitungen zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind von der verantwortlichen Stelle in einer Übersicht (Verfahrensverzeichnis) zu führen. Die Übersicht enthält grundsätzlich die Angaben nach §§ 4d und 4e BDSG und wird nach § 4g Absatz 2 BDSG in den meisten Fällen vom bDSB geführt. Ähnliche Regelungen enthalten auch die Datenschutzgesetze der Länder, sofern die Bestellung eines bDSB vorgesehen ist.

Unter bestimmten Voraussetzungen sind nicht-öffentliche Stellen verpflichtet, Registermeldungen, die mit den Angaben des Verfahrensverzeichnisses weitgehend übereinstimmen, gegenüber der zuständigen Aufsichtsbehörde abzugeben. Von der Meldepflicht sind nach § 4d Abs. 4 BDSG im Prinzip nur Stellen erfasst, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung verarbeiten.

Während für öffentliche Stellen des Bundes gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit keine Meldepflicht besteht, sind öffentliche Stellen in den Ländern nach Landesrecht teilweise dazu verpflichtet, solche Meldungen gegenüber den jeweiligen Landesbeauftragten für den Datenschutz abzugeben, insbesondere auf Grund von Regelungen in den Bereichen der Strafverfolgung und der Gefahrenabwehr.

Damit der bDSB seiner Aufgabe zur Führung des Verfahrensverzeichnisses nachkommen kann, müssen die dafür erforderlichen Angaben nach § 4e BDSG vollständig und aktuell sein. Dabei ist besonders darauf zu achten, dass die Rechtsgrundlage für die Datenverarbeitung und die Zweckbindung hinreichend präzisiert sind, damit eine spätere Zweckänderung ausschließlich im Rahmen der gesetzlichen Anforderungen erfolgen kann.

Prüffragen:

- Existiert ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten?

# M 2.509 Datenschutzrechtliche Freigabe

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Datenschutzbeauftragter
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung

Software und IT-Verfahren sind mit systematisch entwickelten Fall-Konstellationen (Testdaten, keine personenbezogenen Echtdaten) nach einem Testplan, aus dem das gewünschte Ergebnis hervorgeht, zu überprüfen (siehe auch M 2.83 *Testen von Standardsoftware*). Massentests können, wenn erforderlich, nach Zustimmung und Vorgaben der fachlich dafür zuständigen Stelle mit anonymisierten Originaldaten durchgeführt werden. Die Zustimmung der fachlich zuständigen Stelle zur Anonymisierung von Originaldaten und alle Testergebnisse sind revisionssicher zu dokumentieren.

Tests mit einer Kopie der erforderlichen, nicht-anonymisierten Originaldaten (personenbezogene Echtdaten) sind nur zulässig, wenn

- eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder
- sich im Ausnahmefall trotz Nachbildung im Testbereich ein Fehler aus dem Produktionsbetrieb nicht ermitteln, sondern nur mit Originaldaten aufklären lässt, oder die Verfahrenssicherheit nicht anders gewährleistet werden kann,
- eine bereichsspezifische Rechtsvorschrift dies nicht ausdrücklich untersagt,
- eine Anonymisierung der Originaldaten für die vorgesehene Test-Konstellation nur mit einem unvertretbar hohem Aufwand verbunden wäre,
- die fachliche verantwortliche Stelle dem Vorgehen schriftlich zugestimmt hat,
- bei der Durchführung oder Auswertung des Tests die schutzwürdigen Belange der Betroffenen und die Informationssicherheit angemessen berücksichtigt werden,
- sichergestellt ist, dass nur die für die Fehlerbehebung und Durchführung des Tests erforderlichen Personen die Daten nutzen können und
- Zugang zu diesen Daten nur Personen erhalten, die den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften unterliegen.

Der/die behördliche bzw. betriebliche Datenschutzbeauftragte bzw. eine sonstige dafür zuständige Stelle ist rechtzeitig vor den geplanten Tests mit Originaldaten zu informieren.

Der Kopierzugriff auf die Originaldaten ist zu protokollieren. Nach Beendigung des Tests ist die benutzte Kopie der Originaldaten unverzüglich aus dem Testbereich zu löschen bzw. im Testbereich zu anonymisieren. Die Verwendung von Originaldatenkopien ist mit Anlass, Begründung, Umfang und Dauer, die getroffenen Sicherheitsmaßnahmen sowie die vorangehenden Tests mit Testdaten revisionssicher zu dokumentieren.

Es muss geregelt sein, wie IT-Verfahren abgenommen, freigegeben, eingespielt bzw. benutzt werden dürfen. Auf die Maßnahmen M 2.62 *Software-Abnahme- und Freigabe-Verfahren* bzw. Baustein B 1.10 *Standardsoftware* wird verwiesen.

Die Freigabe von IT-Verfahren mit der Verarbeitung personenbezogener Daten setzt eine Prüfung auch aus datenschutzrechtlicher Sicht voraus. Die vorherige Beteiligung des Landesbeauftragten für den Datenschutz wird in einigen Landesdatenschutzgesetzen vorgeschrieben.

Prüffragen:

- Wird der Datenschutzbeauftragte vor den Software-Tests mit Daten, die Personbezug haben könnten, informiert?
- Wird vor der Freigabe von IT-Verfahren, die personenbezogene Daten verarbeiten, eine datenschutzrechtliche Prüfung durchgeführt?

# M 2.510 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche

Den automatisierten Abrufverfahren kommt unter dem Aspekt des Datenschutzes und der Datensicherung besondere Bedeutung zu, weil die abrufende Stelle je nach Einrichtung eines solchen Anschlusses ohne Einzelentscheidung der zuständigen Stelle über den gesamten Bestand oder wesentliche Teile der von der übermittelnden Stelle bereitgehaltenen personenbezogenen Daten verfügen kann. Deshalb sehen die entsprechenden gesetzlichen Regelungen (z. B. § 10 BDSG) den technischen und organisatorischen Datenschutz zwingend bereits als Teil der Planung von Abrufverfahren vor.

Automatisierte Abrufverfahren werden in den Datenschutzgesetzen als eine Phase der Datenverarbeitung definiert, bei der gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten an einen Dritten in der Weise bekannt gegeben werden, dass die Daten durch die datenverarbeitende Stelle zum Abruf bereitgestellt werden und der Abruf durchgeführt wird.

Ein Beispiel für ein automatisiertes Abrufverfahren ist das Elektronische Grundbuch, das zugelassenen Teilnehmern nach Maßgabe der gesetzlichen Bestimmungen die unmittelbare Online-Einsicht auf Grundbuchdaten von ihren Arbeitsplatz-Rechnern ermöglicht. Dieser Dienst kann insbesondere von Notaren, Rechtsanwälten, Banken, Sparkassen und Versicherungen, aber auch Landes- und Kommunalbehörden genutzt werden, die zur Ausübung ihrer Tätigkeiten häufig auf die Grundbucheinsicht angewiesen sind.

Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger.

Für die Einrichtung eines automatisierten Abrufverfahrens sind die besonderen Zulässigkeitsvoraussetzungen in den einschlägigen Gesetzen dargestellt. Zur Kontrollierbarkeit der Zulässigkeit sind die wesentlichen Details des Abrufverfahrens schriftlich festzulegen.

Zu beachten ist, dass die Unterrichtung des Bundes- bzw. Landesbeauftragten für den Datenschutz über die Einrichtung eines Abrufverfahrens in einigen Datenschutzgesetzen gefordert ist.

Allgemeine Aspekte:

- Anlass und Zweck sowie beteiligte Stellen am Abrufverfahren sind festzulegen.
- Abrufberechtigungen sind festzulegen und zu kontrollieren.
- Art und Umfang der bereitgehaltenen Daten sind festzulegen.
- Sperr- und Löschfristen für Daten sind zu definieren.
- Es ist festzulegen, in welchen Fällen die speichernde Stelle von der abrufenden Stelle zu informieren ist.

Maßnahmen gegen unbefugten Abruf:

- Der Abruf von Daten durch nicht Abrufberechtigte ist durch geeignete Vorkehrungen zu verhindern:
- Nach einer festgelegten Anzahl von Fehlversuchen ist die Berechtigung zu sperren.
- Passwörter müssen in regelmäßigen Abständen gewechselt werden. Soweit möglich, ist dies durch die entsprechenden Programme zu erzwingen.
- Der Abruf besonderer Arten personenbezogener Daten muss durch ein höheres Schutzniveau gesichert werden (Besitz und Wissen).
- Zur Überprüfung der Protokolldateien sollten programmgesteuerte Prüfungsverfahren eingesetzt werden.
- Art und Umfang der Protokollierung müssen festgelegt werden.
- Es sollten zufallsgesteuerte Stichprobenkontrollen oder eine Dauerprotokollierung durchgeführt werden.
- Es ist festzulegen, an welcher Stelle die Protokollierungen durchgeführt werden, ob bei der abrufenden Stelle, bei der speichernden Stelle, oder an beiden Stellen.
- Die Protokollierung muss so konzipiert sein, dass nachträglich festgestellt werden kann, aufgrund wessen Abrufberechtigung Daten abgerufen wurden.
- Die Gründe des Abrufs müssen protokolliert werden.
- Beim Abruf von Daten sollte protokolliert werden, über welchen Anschluss und welche Endgeräte die Übertragung stattfindet.

Netzanbindung:

Bei der Vernetzung von IT-Systemen ist zu überprüfen, wie der Netzanschluss der Endsysteme realisiert ist. Bei Wählanschlüssen ist beispielsweise zu überprüfen, welche Sicherheitsmaßnahmen vorgesehen sind, bei virtuellen Festverbindungen, ob geschlossene Benutzergruppen eingerichtet worden sind. In lokalen Netzen sollten geschlossene Benutzergruppen so eingerichtet werden, dass sie jeweils nur geschlossene Organisationseinheiten umfassen.

Prüffragen:

- Wird bei der Einrichtung von Abrufverfahren geprüft, dass alle datenschutzrechtlichen Rahmenbedingungen eingehalten sind?

# M 2.511 Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche

Werden personenbezogene Daten im Auftrag verarbeitet, bleibt der Auftraggeber für die Einhaltung der Gesetze und Vorschriften über den Datenschutz verantwortlich. Er hat den Auftragnehmer sorgfältig auszuwählen.

Der Auftrag ist im Rahmen der gesetzlichen Vorgaben schriftlich zu erteilen und etwaige Unterauftragsverhältnisse sind festzulegen (§ 11 BDSG). In einigen Bereichen sind zusätzliche gesetzliche Regelungen zu beachten, z. B. Krankenhausgesetze der Länder.

Je nachdem, wie schutzbedürftig die personenbezogenen Daten sind, die im Auftrag verarbeitet werden sollen, sind die Anforderungen an den Vertrag mit dem Auftragnehmer zu stellen: Je schutzbedürftiger, umso enger und präziser der Auftrag. Bei besonders sensiblen Verarbeitungen kann sich eine Vergabe an Außenstehende verbieten (z. B. Fahndungsdaten).

Auftragnehmer müssen sicherstellen, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Unterauftragsverhältnisse unterliegen der Zustimmung des Auftraggebers.

Wenn der Auftragnehmer keine öffentliche Stelle ist, sind die mit der Verarbeitung personenbezogener Daten beschäftigten Personen bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Bei Sozialdaten sind die Regelungen des Sozialgesetzbuches (SGB) zu beachten. Die Verarbeitung personenbezogener Daten im Auftrag durch nichtöffentliche Stellen ist nur zulässig, wenn anders Störungen im Betriebsablauf auftreten können oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfass (§ 80 Abs. 5 SGB X). Bei den Aufsichtsbehörden haben die erforderlichen Anzeigen zu erfolgen.

Der Auftraggeber und gegebenenfalls der zuständige Datenschutzbeauftragte haben ein jederzeitiges Kontrollrecht.

Prüffragen:

- Wurden bei der Vertragsgestaltung zur Auftragsdatenverarbeitung, bei der personenbezogene Daten verarbeitet werden, alle relevanten Datenschutz-Aspekte berücksichtigt?
- Ist sichergestellt, dass externe Dienstleister die Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden?
- Wurden auch beim Auftragnehmer alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet?

# M 2.512 Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Fachverantwortliche

In den typischen IT-Anwendungen wird der Benutzer am Bildschirm vom Rechner mittels "Masken" durch ein "Menü" geführt. Diese erleichtern ihm die Benutzung des Programms durch vorformulierte "Fragebögen", in denen er seine Abfragen z. B. "ankreuzen" kann. Sie erlauben nur solche Abfragen und Auswertungen, die vom Anwendungsprogramm vorgegeben, unter Datenschutzaspekten geprüft und genehmigt sind. Andere Abfragen werden abgewiesen. Anders ist dies bei Datenbanksprachen ("freien Abfragesprachen") und moderner Office-Software: Sie ermöglichen dem Anwender, selbst Abfragen über den Datenbestand zu formulieren, ohne an die Restriktionen einer strikten Menüführung gebunden zu sein. Damit könnten auch Auswertungen gemacht werden, die nicht erforderlich und damit nicht zulässig sind.

Da die technische Entwicklung inzwischen Möglichkeiten bietet, die mit einer "freien Abfragesprache" verbundenen datenschutzrechtlichen Risiken abzubauen, kann in begründeten Einzelfällen der eingeschränkte Einsatz "freier Abfragesprachen" vertretbar sein. Eine Beeinträchtigung des Persönlichkeitsrechts der Betroffenen muss aber ausgeschlossen sein. Auch die Zustimmung der Personal- bzw. Betriebsräte ist einzuholen. Die Möglichkeit zum Einsatz "freier Abfragesprachen" bzw. der Funktionalität von Office-Software ist weitestgehend zu beschränken. Datenauswertungen, die voraussehbar regelmäßig zur Aufgabenerfüllung benötigt werden, sind über Menüsteuerung bzw. Bildschirmmasken zur Verfügung zu stellen. Der Einsatz "freier Abfragesprachen" sollte auf Ausnahmefälle beschränkt bleiben.

Bevor die sogenannten freien Abfragesprachen im Zusammenhang mit personenbezogener Datenverarbeitung zugelassen werden, muss geprüft werden, ob dies mit der Schutzwürdigkeit der Daten vereinbar ist. Wenn es grundsätzlich vereinbar ist, sollten folgende Anforderungen beachtet werden: Das System muss eine technische Begrenzung aufweisen, ähnlich einem Filter, der sicherstellt, dass die "freie Abfragesprache" nur im vereinbarten Umfang eingesetzt werden kann. Der Umfang kann beispielsweise durch eine Zugriffsbeschränkung auf bestimmte, weniger sensitive Datenfelder festgelegt sein. Ein Umgehen des Filters ist insbesondere programmtechnisch zu verhindern.

Die Daten, auf die mit einer solchen Abfragesprache zugegriffen werden soll, und die zu eröffnenden Abfragearten müssen vorab geprüft werden. Kriterien sind hierbei insbesondere

- die Erforderlichkeit für die Aufgabenerfüllung,
- der Nachweis, dass eine anonymisierte Auswertung für den jeweils verfolgten Zweck nicht genügt,
- die Sensibilität der einzelnen Daten in der vorgesehenen Verknüpfung und Systemumgebung sowie
- der jeweilige Zweck und Kontext der Datennutzung.

Keine datenschutzrechtlichen Bedenken bestehen gegen den Einsatz einer "freien Abfragesprache" dann, wenn die Auswertung nur zu anonymisierten

Ergebnissen führt, d. h. Rückschlüsse auf einzelne Personen nicht möglich sind.

Prüffragen:

- Ist die Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten geregelt?
- Wird vor Verarbeitung personenbezogener Daten die datenschutzrechtliche Unbedenklichkeit geprüft?

# M 2.513 Dokumentation der datenschutzrechtlichen Zulässigkeit

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche

Bevor Software oder Hardware für die Verarbeitung von personenbezogenen Daten eingesetzt werden, sollten sie, bezogen auf den vorgesehenen Einsatz, auf die datenschutzrechtliche Zulässigkeit geprüft werden. Hier wird es je nach IT-System (z. B. nicht vernetzter PC oder zentrales Rechenzentrum) sehr unterschiedliche Anforderungen geben. Das Prüfungsergebnis sollte dokumentiert werden. Für Datenschutzkontrollen sind derartige Dokumentationen besonders wichtig.

Der betriebliche bzw. behördliche Beauftragte für den Datenschutz (bDSB) ist nach § 4g Abs. 1 BDSG über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten. Er hat die ordnungsgemäße Anwendung (vorhandener und neuer) Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet sollen, zu überwachen. Aus diesem Grunde empfiehlt es sich, den bDSB von Anfang an, d.h. im Rahmen der ersten Planungen, mit einzubeziehen. Nur so können bereits in der Planungsphase datenschutzrechtliche Fehler vermieden werden, deren Behebung zu einem späteren Zeitpunkt unter Umständen zeit- und kostenintensiv sein könnten.

Prüffragen:

- Wird Hard- und Software, die für die Verarbeitung von personenbezogenen Daten eingesetzt wird, auf die datenschutzrechtliche Zulässigkeit geprüft?
- Werden die Prüfungsergebnisse dokumentiert?

# M 2.514 Aufrechterhaltung des Datenschutzes im laufenden Betrieb

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter

Abgesehen von der Bestellung eines betrieblichen bzw. behördlichen Datenschutzbeauftragten (bDSB) ist die Einrichtung einer internen IT-Revision und Datenschutzkontrolle eine wichtige Maßnahme im Rahmen der durch die Datenschutzgesetze vorgeschriebenen Organisationskontrolle. Sie hilft dabei, vor Ort und zeitnah die Sicherheit der Datenverarbeitung und die Einhaltung der datenschutzrechtlichen Anforderungen zu gewährleisten.

Die IT-Revision überprüft die Ordnungsmäßigkeit der Datenverarbeitung durch Kontrolle der Umsetzung des IT-Sicherheitskonzeptes. Dazu gehören insbesondere eine Kontrolle der Dokumentation der Verfahren, der vorgeschriebenen Verfahrensanwendung und der gesamten Sicherheitsmaßnahmen.

Die interne Datenschutzkontrolle, die meist dem Datenschutzbeauftragten obliegt (vergleiche M 2.502 *Regelung der Verantwortlichkeiten im Bereich Datenschutz*), überprüft hingegen die Einhaltung der aus den Datenschutzgesetzen herrührenden Anforderungen. Dazu gehören:

- die Kontrolle der Verfahren auf Einhaltung der Rechtsgrundlage und der Zweckbestimmung,
- die Sicherstellung der Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung und Schadensersatz,
- die Unterrichtung über bzw. die Verpflichtung der Mitarbeiter auf den Datenschutz,
- das Führen von Datei- bzw. Verfahrensübersichten und Geräteverzeichnissen und
- die Kontrolle der aus den gesetzlichen Vorschriften abgeleiteten technisch-organisatorischen Maßnahmen zur Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und "getrennte Verarbeitung gemäß der Zweckbestimmung".

IT-Revision und Datenschutzkontrolle arbeiten sinnvollerweise zusammen und ergänzen sich. Durch zeitnahe Überprüfung der Protokolldaten helfen sie z. B. mit, einen möglichen Missbrauch schnell aufzudecken und die Aufbewahrungszeit und den Umfang der Protokolldaten so gering wie möglich zu halten. Sie können die Leitung der datenverarbeitenden Stelle bei der Neukonzeption und der Fortentwicklung von Verfahren beraten und dienen als kompetente Ansprechpartner bei Kontrollbesuchen der Aufsichtsbehörden oder des Bundes- und der Landesbeauftragten für Datenschutz. Beide Funktionen können Mitarbeitern auch im Nebenamt übertragen und bei kleinen Stellen auch in einer Hand zusammengelegt werden. Grundsätzlich ist aber darauf zu achten, dass keine Interessenkollision mit sonst wahrgenommenen Aufgaben eintritt (siehe auch M 2.502 *Regelung der Verantwortlichkeiten im Bereich Datenschutz*).

Prüffragen:

- Wird die Einhaltung der datenschutzrechtlichen Anforderungen regelmäßig überprüft?
- Sind die Zuständigkeiten und Kompetenzen von IT-Revision und Datenschutzkontrolle abgestimmt?

# M 2.515 Datenschutzgerechte Löschung/ Vernichtung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter

**Sicheres Löschen magnetischer Datenträger**

Sowohl aus der Sicht des Datenschutzes als auch der Informationssicherheit ist beim Löschen von sensiblen oder vertraulichen Daten auf magnetischen Datenträgern zu gewährleisten, dass die Daten sicher, d. h. vollständig und unumkehrbar gelöscht werden. Einfache Löschbefehle des jeweiligen Betriebssystems oder auch das Formatieren des Datenträgers reichen hierzu in der Regel nicht aus, da eine Rekonstruktion der Daten mit frei verfügbaren Softwarewerkzeugen leicht möglich ist. Daten, die sicher gelöscht werden sollen, müssen durch physikalische Maßnahmen (mechanische oder thermische Zerstörung, magnetische Durchflutung des Datenträgers) oder durch mehrmaliges Überschreiben unkenntlich gemacht werden. Beim Löschen durch Überschreiben sind die spezifischen Besonderheiten der Verwaltung und Speicherung von Daten zu berücksichtigen, wie z. B. die Existenz von Sicherheitskopien, von automatisch durch das System oder einzelne Anwendungen angelegten temporären und Auslagerungsdateien oder von Journalen bei bestimmten Dateisystemen.

Aus Datenschutzsicht gibt es in diesem Zusammenhang die folgenden Empfehlungen:

- Der Problemkreis des sicheren Löschens von Daten erfordert die Sensibilisierung der verantwortlichen Entscheidungsträger, Administratoren, Sicherheits- und Datenschutzbeauftragten sowie jedes einzelnen Nutzers. Dies ist durch geeignete Information und Schulung zu erreichen.
- Im jeweiligen Verantwortungsbereich sind technisch-organisatorische Maßnahmen festzulegen, die eine sichere Löschung von Daten gewährleisten. Sie sind in das übergreifende Datenschutz- bzw. Sicherheitskonzept zu integrieren. Insbesondere sind Maßnahmen vor der Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern zu bestimmen.
- Die Maßnahmen sind durch konkrete Handlungsanweisungen für das sichere Löschen zu untersetzen. Diese Anweisungen müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.
- Schutzwürdige Daten sind (soweit möglich) bereits in verschlüsselter Form auf dem Datenträger zu speichern. Hierzu sollten verschlüsselte Dateisysteme verwendet werden. Auch für temporäre und Auslagerungsdateien sowie für Sicherheitskopien sollten verschlüsselte Dateisysteme verwendet werden, da diese ebenfalls schutzwürdige Daten enthalten können.
- Daten auf intakten Datenträgern sind durch das ein- oder mehrmalige, komplette Überschreiben mit Zufallszahlen zu löschen. Hierbei können spezielle Softwarewerkzeuge zum Einsatz kommen. Die Verwendung gleichförmiger Überschreibmuster beim Löschen ist nicht zu empfehlen, da so kein Schutz gegen ausführliche Laboranalysen besteht.
- Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Die Überschreibprozedur sollte aus mindestens zwei, besser drei Durchläufen bestehen. Beim zweiten Durchlauf sollte das zum ersten Durchlauf komplementäre Muster (Bit-

folge) verwendet werden. Für den dritten Durchlauf werden Zufallsdaten empfohlen. Dadurch wird eine verbesserte Schutzwirkung erzielt.
- Soll ein noch intakter Datenträger verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger mehrmals komplett mit Zufallszahlen zu überschreiben. Diese Form der Wiederaufbereitung gestattet anschließend die weitere Nutzung des Datenträgers (z. B. die Neuinstallation eines Betriebssystems).
- Das selektive Löschen einzelner Dateien durch Überschreiben ist meist problematisch. Es eignet sich nur dann, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien enthaltenen Daten an anderen Orten abgelegt wurden (z. B. in temporären Dateien, Auslagerungsdateien oder Sicherungskopien) oder diese Orte eindeutig bestimmt und auch die Kopien sicher gelöscht werden können. Weiter ist zu gewährleisten, dass die Metadaten der gelöschten Dateien überschrieben werden, falls sie sensible Informationen enthalten.
- Bei der Festlegung von technisch-organisatorischen Maßnahmen sowie von Handlungsanweisungen für das Löschen durch Überschreiben sind geeignete Softwarewerkzeuge anhand eines Kriterienkatalogs auszuwählen, zu bewerten und für die betreffenden Nutzer bereitzustellen. Die Anwendung der Werkzeuge ist stichprobenartig zu kontrollieren.
- Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen. Um die Zuverlässigkeit der Verfahren zu sichern, ist eine korrekte Anwendung zu gewährleisten.
- Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z. B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen und eventuell mit Schadensersatzansprüchen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Gegebenenfalls ist auf Garantieansprüche zu verzichten.

**Vernichten von Unterlagen**

Da die Aussonderung und Vernichtung von Unterlagen im Allgemeinen in mehreren Schritten erfolgt, sind von der Zwischenlagerung in Papierkörben oder Sammelbehältern oder dem Sammeln der Unterlagen am Arbeitsplatz über den Transport und die zentrale Deponierung bis hin zum eigentlichen Vernichtungsverfahren alle Sicherheitsaspekte zu betrachten.

**Allgemeine Anforderungen**

Soweit keine bereichsspezifischen Vernichtungsregelungen einschlägig sind, unterliegt die Vernichtung von Unterlagen mit personenbezogenen Daten in den öffentlichen Stellen des Bundes und im nicht-öffentlichen Bereich dem Bundesdatenschutzgesetz, ansonsten den jeweiligen Landesdatenschutzgesetzen.

Dabei sind die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten sicherzustellen; dies gilt auch für den Verarbeitungsschritt "Vernichtung". Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Un-

befugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Grundsätzlich gilt, dass eine Stelle für die Sicherheit der Daten in Unterlagen, die vernichtet werden sollen, solange verantwortlich ist, bis die in den Unterlagen enthaltenen personenbezogenen Daten als gelöscht im Sinne der Datenschutzgesetze gelten können, die Vernichtung also abgeschlossen ist. Die betroffene Stelle muss daher über alle Unterlagen mit personenbezogenen Daten bis zu deren Vernichtung die uneingeschränkte Verfügungsgewalt besitzen. Insbesondere dürfen zu vernichtende Unterlagen mit personenbezogenen Daten vor Abschluss der Vernichtung nicht in das Eigentum Dritter übergehen.

Der Zustand, in dem die Unterlagen als vernichtet gelten können, ist festzulegen. Als Orientierung kann hierzu die Norm DIN 66399 (Vernichten von Datenträgern) herangezogen werden. Hiernach ist eine Informationsträgervernichtung dann ausreichend, wenn die Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand an Personen, Hilfsmitteln oder Zeit möglich ist (Sicherheitsstufe 3).

Auch für die Vernichtung von Unterlagen gilt, dass sich die betroffene Stelle regelmäßig durch Kontrollen von der ordnungsgemäßen Durchführung der Vernichtung zu überzeugen hat. Daraus folgt, dass insbesondere dann, wenn die Vernichtung als Auftrag nach außerhalb vergeben wurde, die betroffene Stelle den gesamten technischen Vorgang oder das Verfahren kennen muss. Mit der Kontrolle der Vernichtung von Unterlagen sollte eine Person oder Organisationseinheit schriftlich beauftragt werden.

**Vernichtung von Unterlagen in Eigenregie**

Oberstes Prinzip sollte sein, dass Unterlagen möglichst umgehend von den Stellen vernichtet werden, die die Einstufung zur Aussonderung vornehmen. Zwischenlagerungen und Weiterreichungen über viele Hände sind fehleranfällig und erfordern genaue Regelungen und Kontrollen. Insofern ist eine unmittelbare Unterlagenvernichtung durch die zuständige Sachbearbeitung ein wirksamer Datenschutz. In jedem Fall sollte schriftlich geregelt sein, wie Mitarbeiterinnen und Mitarbeiter die Vernichtung ihrer Unterlagen durchzuführen haben. Daneben sind sie zu verpflichten, die Unterlagen bis zu deren Vernichtung sicher zu verwahren.

Werden Unterlagen zentral vernichtet, ist der gesamte Ablauf schriftlich zu regeln. Dies gilt beispielsweise für zentrale, besonders zu sichernde Sammelstellen, wie auch für den Transport zur Sammelstelle. Die Sicherheit der zu vernichtenden Unterlagen ist ebenfalls bis zu deren Ablieferung bei der Sammelstelle zu gewährleisten. Falls die Unterlagen durch einen zentralen Dienst eingesammelt werden, ist auch diese Phase unter Sicherheitsaspekten zu betrachten. Die Vernichtung der Unterlagen ist in geeigneter Weise zu protokollieren.

**Vernichtung von Unterlagen durch externe Stellen**

Werden Unterlagen durch externe Dritte als "**Datenverarbeitung im Auftrag**" vernichtet, ist die gesamte Handhabung und Sicherung der Unterlagen zwischen der Übergabe und dem Abschluss der Vernichtung vertraglich festzulegen. Es müssen der Transport, eine eventuell erforderliche Zwischenlagerung, der Vernichtungsort und der höchstzulässige Zeitraum zwischen der Übergabe der Unterlagen sowie dem Abschluss der Vernichtung geregelt sein. Weiter

ist schriftlich festzulegen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet gelten zu können. Durch den Auftragnehmer ist zu gewährleisten, das Unbefugte keine Kenntnis der in den Unterlagen gespeicherten Daten erhalten können. Die Übergabe von Unterlagen an das Auftragsunternehmen sollte quittiert werden und die Durchführung jeder Vernichtungsaktion sollte schriftlich bestätigt werden. Generell gilt, dass die Erteilung von Unterauftragsverhältnissen möglichst ausgeschlossen werden sollte.

Die betroffene Stelle muss über ihre Unterlagen bis zum Abschluss der Vernichtung uneingeschränkt verfügen können. Die Unterlagen müssen deshalb bis zum Abschluss der Vernichtung in ihrem Eigentum bleiben. Dies beinhaltet, dass sie vor ihrer Vernichtung nicht mit fremden Unterlagen vermischt werden dürfen. Es ist deshalb auch mit dem Auftragsnehmer zu vereinbaren, dass der Auftraggeber und der zuständige Datenschutzbeauftragte bis zum Abschluss der Vernichtung zu Kontrollen berechtigt ist.

Bezüglich der Regelungen zur Auftragsdatenverarbeitung wird auf Maßnahme M 2.511 *Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten* verwiesen.

Prüffragen:

- Werden Datenträger, die personenbezogene Daten enthalten, sicher gelöscht bzw. vernichtet?
- Kontrolliert der Datenschutzbeauftragte regelmäßig, dass Datenträger mit personenbezogenen Daten datenschutzgerecht gelöscht bzw. vernichtet werden?

# M 2.516 Bereitstellung von Sicherheitsrichtlinien für Cloud-Anwender

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche

Beim Cloud Computing sind sowohl Anbieter als auch Anwender für die Sicherheit der Cloud Computing Plattformen verantwortlich.

Beim Cloud Computing muss der Cloud-Anwender bei der Umsetzung von Sicherheitsmaßnahmen mitwirken. Je nach Servicemodell (IaaS, PaaS oder SaaS, siehe nachfolgende Zwischenüberschriften) kann der Umfang dieser Mitwirkung variieren. Abhängig von der Art des Cloud-Dienstes und den vertraglichen Regelungen sollte der Cloud-Diensteanbieter daher den Cloud-Anwender auf diese Verantwortung hinweisen und ihm Sicherheitsempfehlungen in Form einer Richtlinie zur Verfügung stellen.

Die Richtlinie sollte eine Beschreibung der durch den Cloud-Diensteanbieter umgesetzten Sicherheitsmaßnahmen enthalten. Dies kann das Vertrauensverhältnis stärken und die Transparenz der Cloud-Infrastruktur für den Cloud-Anwender steigern.

**Software as a Service (SaaS)**

Wird vom Cloud-Diensteanbieter Software as a Service betrieben, so muss sich der Cloud-Anwender weder mit Betriebssystemsicherheit noch mit der Sicherheit der Cloud-Anwendung selbst auseinandersetzen, da hierfür der Cloud-Diensteanbieter verantwortlich ist. Dennoch sind Mitwirkungen bei bestimmten Sicherheitsmaßnahmen durch den Cloud-Anwender notwendig. Daher sollte der Cloud-Diensteanbieter in den Sicherheitsrichtlinien ein ausreichend umfangreiches Beantragungs- und Genehmigungsverfahren aufstellen, welches das für die Cloud-Anwendung zu etablierende Rollen- und Berechtigungskonzept steuert. Grundsätzlich sollte der Cloud-Diensteanbieter hierbei Standardrollen mit entsprechenden Berechtigungen vorgeben. Sollten Cloud-Anwender hierüber hinaus weitere Rollen und Berechtigungen benötigen, besteht die Möglichkeit, die Erstellung dieser Rollen durch den Cloud-Anwender vornehmen zu lassen. Die Genehmigung, ob ein Benutzer bestimmte Rollen oder Berechtigungen erhalten darf, muss in der Hoheit des Cloud-Anwenders liegen. Aufgabe des Cloud-Diensteanbieters ist es hingegen die Sicherheitsgrundsätze zum Benutzer- und Berechtigungskonzept dem Cloud-Anwender in der Richtlinie zu erläutern. Hierzu gehört insbesondere das Prinzip der geringsten Berechtigungen (oft englisch *Least Privilege*). Für den Cloud-Diensteanbieter ist es empfehlenswert, dass er eine Anbindung an ein externes Identitäts- und Rechtemanagement für seine SaaS-Angebote zulässt und unterstützt.

In den Richtlinien für Cloud-Anwender sollte der Cloud-Diensteanbieter die Möglichkeit wahrnehmen, den Kunden zusätzliche Sicherheitsmaßnahmen für höheren Schutzbedarf zu erläutern. So kann ein Cloud-Diensteanbieter beispielsweise mögliche Mittel und Wege zur Verschlüsselung von Cloud-Daten beschreiben. Hier kann er entweder weiterführende Cloud-Dienste anbieten oder z. B. auf Verschlüsselungsmittel für Cloud-Anwender verweisen.

**Platform as a Service (PaaS)**

Beim Cloud-Bereitstellungsmodell Platform as a Service kommen den Cloud-Anwendern deutlich mehr Einflussmöglichkeiten zur Umsetzung von Sicherheitsmaßnahmen für Cloud-Dienste zu. Hier sollte der Cloud-Diensteanbieter Sicherheitsempfehlungen zur Absicherung von Cloud-Anwendungen geben. Da es sich üblicherweise um Webanwendungen handelt, sollten sich die Empfehlungen an anerkannten Sicherheitsstandards wie OWASP (Open Web Application Security Project) oder dem Baustein B 5.21 *Webanwendungen* ausrichten. Insbesondere sind zentrale Maßnahmen zur sicheren Programmierung und zur sicheren Konfiguration von Webanwendungen (M 4.398 *Sichere Konfiguration von Webanwendungen*) vorzugeben.

Ebenso sind bei PaaS eine sichere Zugriffskontrolle und eine abgesicherte, verschlüsselte Authentisierung gegenüber den vom Cloud-Diensteanbieter bereitgestellten Infrastruktur-Diensten (sofern der Cloud-Anwender diese nicht selbst stellt) notwendig. Auch die Zugriffsverwaltung muss für PaaS vom Cloud-Anwender mitgestaltet oder verantwortlich umgesetzt werden. Dazu kann man sich an bestehenden IT-Grundschutzmaßnahmen wie M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle* orientieren. Es wird empfohlen, den Cloud-Anwendern die eingerichteten Maßnahmen zum Schutz von PaaS-Angeboten (z. B. Standards zur Härtung einer Datenbank) in Form von Dokumentationen und Umsetzungsbeispielen zur Verfügung zu stellen.

Je nach Cloud-Dienst und vereinbarten Verantwortungsbereichen sollte auch eine Sicherheitsempfehlung zum Patch- und Änderungsmanagement gegeben werden, welche durch den Cloud-Anwender eingehalten werden sollte. Wichtig ist hierbei, dass dem Cloud-Anwender auf den Weg gegeben wird, dass er (sofern es sich in seiner Verantwortung befindet) nach aktuellen Patches und Updates sucht und sich regelmäßig über mögliche Schwachstellen der Anwendungen und Plattformen informiert. Ebenso sollten die Sicherheitsrichtlinien eine Sicherheitsempfehlung zum Testen von Patches und Änderungen vor deren Inbetriebnahme enthalten.

**Infrastructure as a Service (IaaS)**

Bei IaaS werden den Cloud-Anwendern virtuelle Maschinen zur Verfügung gestellt, auf die z. B. über eine Webschnittstelle zugegriffen werden kann. Zur Absicherung der virtuellen Maschinen ist es hilfreich, wenn der IaaS-Anbieter seinen Kunden Richtlinien zur Härtung der virtuellen Maschinen an die Hand gibt.

Bei IaaS liegt die Hauptverantwortung für die Umsetzung von Sicherheitsmaßnahmen für Server und für die sichere Anbindung von Zugriffen und an Verzeichnisdienste beim Cloud-Anwender. Wichtige Maßnahmen zur Erreichung eines Basis-Sicherheitsniveaus zur Absicherung eines Servers sollten dennoch vom Cloud-Diensteanbieter empfohlen werden. Hier sollten die Cloud-Anwender vom Cloud-Diensteanbieter z. B. auf Maßnahmen aus den passenden Server-Bausteinen der Schicht IT-Systeme des IT-Grundschutzes hingewiesen werden.

Der Cloud-Diensteanbieter sollte die Anbindung an die von ihm angebotenen Virenschutz-Services erläutern und einen durch den Cloud-Anwender zu installierenden Virenschutz als notwendige Basis für den Betrieb eines Cloud-Dienstes empfehlen. Gegebenenfalls kann der Cloud-Diensteanbieter auch die Anbindung an Virenschutz-Hersteller als Dienst in der Cloud-Umgebung anbieten. Darüber hinaus sind grundlegende Härtungsmaßnahmen, wie die

Deaktivierung von nicht benötigten Diensten, an den Cloud-Anwender weiterzugeben.

Dem Cloud-Anwender sollten Standardmaßnahmen zum Schutz von IT-Systemen, wie etwa Host Firewalls, Host-based Intrusion Detection Systems etc. durch den Cloud-Diensteanbieter näher gebracht werden. Auch regelmäßige Integritätsprüfungen wichtiger Systemdateien können als Empfehlung an den Cloud-Anwender weitergegeben werden.

Genauso sollten neben konzeptionellen Sicherheitsempfehlungen für Cloud-Anwender auch technische Hilfsmittel für die sichere Konfiguration an die Hand gegeben werden. Hier können z. B. vorkonfigurierte Profile für virtuelle Maschinen angeboten werden. Solche Vorlagen und Profile standardisieren und vereinfachen die Konfiguration. Es können Vorlagen für eine bekannte, validierte Konfiguration (mit Einstellungen für Netz, Speicher und Sicherheit) erstellt und diese auf mehreren Hosts zur Verfügung gestellt werden, um die Einrichtung zu vereinfachen. Hostprofil-Richtlinien können auch zur Compliance-Überwachung dienen.

Hierbei sollte der Cloud-Diensteanbieter die Profile oder virtuellen Images testen und freigeben. Die Veröffentlichung bzw. Bereitstellung der Profile und Images sollte eine Integritätsprüfung für die Cloud-Anwender bieten, z. B. über eine Prüfsummenbildung der angebotenen Datei.

**Informationssicherheitsvorfallmanagement (für SaaS, PaaS und IaaS)**

Die Sicherheitsrichtlinien für Cloud-Anwender müssen die notwendigen Schnittstellen zum Informationssicherheitsvorfallmanagement beschreiben. Meldewege und Ansprechpartner aufseiten des Cloud-Diensteanbieters müssen benannt werden. Zudem sollte dem Cloud-Anwender eine Auflistung von Kriterien und Beispielen für sicherheitsrelevante Ereignisse in seinen Cloud-Nutzungsrichtlinien mitgegeben werden. Hierzu gehören:

- Name des Meldenden,
- Zeitpunkt der Meldung,
- betroffener Cloud-Dienst,
- Ausprägung des Ereignisses,
- Beschreibung der Auswirkungen, insbesondere welche Daten und Informationen vom Ereignis betroffen sind,
- *optional*: Wurden Schwachstellen identifiziert?
- *optional*: Hinweise des Cloud-Anwenders für die Behebung

Auf diesem Wege werden die Cloud-Anwender dafür sensibilisiert, effektiv das Meldewesen des Informationssicherheitsvorfallmanagements des Cloud-Diensteanbieters zu unterstützen.

Prüffragen:

- Wurde eine Sicherheitsrichtlinie für Cloud-Anwender erstellt und wird diese den Cloud-Anwendern zur Verfügung gestellt?
- Enthält die Richtlinie die Sicherheitsmaßnahmen, für die der Cloud-Anwender verantwortlich ist oder an deren Umsetzung er mitwirken muss?
- Sind in der Richtlinie Ansprechpartner und Meldestellen für Informationssicherheitsthemen benannt?
- Sind in der Richtlinie meldepflichtige, sicherheitsrelevante Ereignisse benannt?

# M 2.517 Vertragsgestaltung mit Dritt-Dienstleistern

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Leiter Beschaffung

Der Cloud-Diensteanbieter arbeitet bei der Bereitstellung von Cloud Services oft mit Softwareherstellern oder weiteren Cloud-Diensteanbietern zusammen. Hierbei müssen Sicherheitsmaßnahmen des Cloud-Diensteanbieters an diese Dienstleister weitergegeben werden (vgl. Baustein B 1.11 *Outsourcing*).

Es sollte darauf geachtet werden, folgende Aspekte vertraglich zu regeln.

**Sicher programmieren**

Die Softwarehersteller müssen verpflichtet werden, Standards für das sichere Programmieren umzusetzen. Um sichere Programmierung zu gewährleisten, sollte ein Software Development Lifecycle definiert und umgesetzt werden (siehe auch M 2.487 *Entwicklung und Erweiterung von Anwendungen*). Der Baustein B 5.21 *Webanwendungen* enthält zudem viele Maßnahmen zum sicheren Entwickeln von webbasierten Anwendungen. Diese sollten vom Softwarehersteller bei der Softwareentwicklung eingehalten werden.

**Sicherheitsfunktionen einbauen**

Der Cloud-Diensteanbieter ist für die Sicherheitsfunktionen in den Cloud-Anwendungen verantwortlich. Er muss dementsprechend die sicherheitsspezifischen Anforderungen an die Softwarehersteller weitergeben. Dieses umfasst z. B. kryptografische Maßnahmen (verschlüsselte Übertragung oder Ablage von Daten), sichere Authentisierungsverfahren oder Datensicherungsmethoden. Außerdem müssen Performance-Anforderungen als erforderliche Leistungen hinsichtlich Durchsatz und Laufzeitverhalten festgelegt an den Drittdienstleister weitergegeben werden.

Für die standardisierten SaaS-Lösungen ist ein entsprechender Anforderungskatalog gemäß Maßnahme M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* zu erstellen und der Softwarehersteller zu dessen Einhaltung zu verpflichten.

Die Anforderungen umfassen auch

- eindeutig definierte Schnittstellen,
- Zusagen zur Virtualisierbarkeit der Anwendung (z. B. muss eine Standardanwendung in der Cloud einfach und automatisiert reproduzierbar sein können),
- Verträglichkeit mit vorgegebenen Versionsständen von Schnittstellen, Software oder Diensten.

Diese Zusicherungen sollten eindeutig und belastbar (wenn möglich schriftlich) von den Drittherstellern oder Cloud-Diensteanbietern abgefragt werden.

**Mandanten trennen**

Eine Mandantentrennung kann z. B. über die Virtualisierung der Anwendungsinfrastruktur erfolgen (d. h. x-fache virtuelle Kopie der Anwendungslandschaft des Drittherstellers für die Cloud-Anwender). Hierbei kann es sein, dass Cloud-Diensteprofile vollständig von Drittherstellern oder anderen Cloud-Diensteanbietern bereitgestellt werden. Es muss vom auftraggebenden Cloud-Diensteanbieter geprüft werden, ob die Konfiguration automatisierbar

und für zusätzliche Mandanten (Cloud-Anwender) erweiterbar ist und dabei eine Umsetzung einer Mandantentrennung auf allen Schichten der Cloud-IT-Infrastruktur (Anwendung, Plattform, Betriebssystem, virtueller Server, Storage, Netze) korrekt erfolgt.

**Patch- und Änderungsmanagement bei verteilter Cloud**

Nutzt ein Cloud-Diensteanbieter (z. B. für ein SaaS-Angebot) das PaaS- oder IaaS-Angebot eines externen Cloud-Diensteanbieters, dann muss mit dem zuliefernden Cloud-Diensteanbieter abgestimmt werden, welche virtuellen Ressourcen mit welchem Patch-Stand und welcher Konfiguration benötigt werden. Hier ist es essenziell für den Cloud-Diensteanbieter, einen geregelten Prozess für das Patch- und Änderungsmanagement mit klaren Verantwortlichkeiten zu vereinbaren. Es wird empfohlen, mit standardisierten Schnittstellen (API) zu arbeiten, sodass lediglich Änderungen an den Schnittstellen im Änderungsmanagement-Prozess betrachtet werden müssen. Für detaillierte Maßnahmen ist der Baustein B 1.14 *Patch- und Änderungsmanagement* heranzuziehen.

**Orte der Datenverarbeitung bei verteilter Cloud**

In vielen Fällen ist es sinnvoll oder sogar unerlässlich festzulegen, wo Daten durch einen Cloud-Dienst verarbeitet werden. In solchen Fällen müssen die Orte der Datenverarbeitung in den vertraglichen Vereinbarungen angegeben werden. Ebenso muss dann vertraglich geregelt werden, wie vorzugehen ist, wenn Orte der Datenverarbeitung im Zeitverlauf geändert werden sollen.

**Schwachstellenmanagement bei Drittdienstleistern**

Im Vertrag mit dem Drittdienstleister müssen für beide Seiten Ansprechpartner für Informationssicherheit benannt werden. Ferner müssen die Verantwortungsbereiche und die Schnittstellen für das Informationssicherheitsvorfallmanagement definiert werden. Damit wird erreicht, dass eine geregelte Kommunikation stattfinden kann und geregelte Prozesse greifen können, wenn bei Cloud-Diensten, die auf den Leistungen des Drittdienstleisters aufsetzen, oder bei der eingesetzten Software neue Schwachstellen auftreten oder bekannt werden.

**Haftung**

Ebenfalls muss die Haftung für Schäden, die durch Softwarefehler des Herstellers entstehen, im Vertrag geregelt werden.

**Urheberrecht und Nutzungsrechte**

Neben den Sicherheitsanforderungen muss der Vertrag mit dem Drittdienstleister Regelungen zu Nutzungsrechten von Software und zum Urheberrecht definieren, insbesondere Nutzungsdauer, Weiterverwendung und Eigentümerschaft.

**Regelungen zur Beendigung von Diensten**

Genauso muss schriftlich vereinbart werden, wie mit den in der Anwendung verarbeiteten Daten umgegangen wird, wenn der Cloud-Dienst für einen Cloud-Anwender eingestellt wird.

**Auftragsdatenverarbeitung**

Für den Fall, dass personenbezogene Daten durch die Drittdienstleister verarbeitet werden, muss geprüft werden, ob es sich um Auftragsdatenverarbeitung im Sinne des Bundesdatenschutzgesetzes handelt. Dann sind die entspre-

chenden rechtlichen Vorschriften zu beachten (siehe Maßnahme M 2.511 *Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten*).

Prüffragen:

- Ist mit allen Dritt-Dienstleistern ein schriftlicher Vertrag abgeschlossen worden?
- Sind alle notwendigen sicherheitsrelevanten Regelungen im Vertrag enthalten?

# M 2.518 Einsatz einer hochverfügbaren Firewall-Lösung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Ausfallsicherheit der Cloud-Infrastruktur muss gewährleistet werden. Wenn an die Verfügbarkeit von Sicherheitsgateways hohe oder sehr hohe Anforderungen gestellt werden, sollten Redundanzen bei physischen Ressourcen und bei der Netzanbindung bzw. Vernetzung von Cloud-Infrastrukturkomponenten eingerichtet werden.

Ein Sicherheitsgateway sollte immer die einzige Schnittstelle zwischen dem externen und dem zu schützenden Netz darstellen. Damit stellt das Sicherheitsgateway einerseits einen potenziellen Flaschenhals bezogen auf den Datendurchsatz und andererseits eine mögliche Sicherheitsschwachstelle für den gesamten Netzverkehr einer Organisation dar. Grundsätzlich können die Sicherheitsgateways zur Cloud-Infrastruktur ebenso wie klassische Absicherungen von Unternehmensnetzen konzipiert werden, also mittels separater physischer und zu einem Cluster verbundener Hardware. Alternativ können Cloud-Diensteanbieter auch ihre virtuelle IT-Infrastruktur nutzen und das Sicherheitsgateway als netztechnisch gekapselte virtuelle Maschine betreiben (z. B. per VLAN getrennt), wobei hierfür eine Risikoanalyse durchzuführen ist.

Die wichtigsten Komponenten eines Sicherheitsgateways sollten redundant ausgelegt werden. Dies sind vor allem diejenigen Komponenten, die zum Übertragen von Informationen genutzt werden. In diese Kategorie fallen in der Regel Router, Paketfilter, Application-Level-Gateway und eventuell VPN-Komponenten. Bei anderen Komponenten (z. B. Virenscanner oder Intrusion Detection Systeme) muss die Bedeutung für die Sicherheit des zu schützenden Netzes im Einzelfall betrachtet werden.

Es gibt verschiedene Möglichkeiten, die Verfügbarkeit von Komponenten eines Sicherheitsgateways zu steigern. Hot-Standby-Systeme oder Lösungen mit zu Clustern verbundenen Systemen können einen dynamischen Parallelbetrieb von Firewalls ermöglichen. Dies kann z. B. über eine Hochverfügbarkeits-Lösung (oft HA-Lösung, *High Availability*) erreicht werden. Hier wird die Verfügbarkeit von Komponenten des Sicherheitsgateways überwacht und bei einem Ausfall übernehmen die Ersatzsysteme automatisch den Betrieb. Eine ständige Überwachung der HA-Komponenten ist dabei ebenso wichtig wie ein funktionierendes Failover im Bedarfsfall. Zudem muss für eine ausreichende Lastverteilung (englisch *Load Balancing*) gesorgt werden, die verhindert, dass einzelne Systeme oder Zuleitungen mit dem Übertragen von Datenpaketen überlastet werden.

Weitere Anforderungen an Hochverfügbarkeits-Lösungen und hochverfügbare Sichergateways gibt die Maßnahme M 2.302 *Sicherheitsgateways und Hochverfügbarkeit*, welche heranzuziehen und umzusetzen ist.

Prüffragen:

- Sind die Firewall-Systeme für die Cloud-Dienste redundant ausgelegt?
- Werden die Failover-Funktionen regelmäßig getestet?

# M 2.519 Geregelte Benutzer- und Berechtigungsverwaltung im Cloud Computing

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Sowohl für die Benutzer des Cloud-Diensteanbieters als auch für diejenigen des Cloud-Anwenders (Cloud-Mandanten) sollten ein zentrales Identitäts- und ein rollenbasiertes Berechtigungsmanagement benutzt werden.

Generell sollten immer nur so viele Zugriffsrechte auf Daten und Informationen vergeben werden, wie es für die Aufgabenwahrnehmung in der Anwendung notwendig ist (Prinzipien *Need to know* und *Least privilege*).

Neben den Prozessen für die Einrichtung von Benutzern und Berechtigungen müssen auch geregelte Prozesse eingerichtet werden, wie Benutzer und Berechtigungen entfernt (de-provisioniert) werden. Dies kann durch Sperrung oder Löschung geschehen. Der Cloud-Diensteanbieter muss gewährleisten, dass die zu sperrenden oder zu löschenden Konten ("Identitäten") und Berechtigungen von Cloud-Benutzern auf allen betroffenen Ebenen der Cloud-IT-Infrastruktur entfernt werden. Mit einem zentralen System für die Berechtigungsverwaltung können Rechte zuverlässig aus allen betroffenen Bereichen entfernt werden, z. B. Betriebssystemkonten, Speicherbereiche (Cloud Storage), Konten im Self-Service-Portal, Datenbanken.

Benutzerkonten und Berechtigungen sollten regelmäßig (z. B. zwei Mal im Jahr) verifiziert werden. Dabei sollte geprüft werden, ob der angelegte Benutzer noch als aktiver Benutzer registriert ist (andernfalls muss er gesperrt oder gelöscht werden) und ob die Rollen und Berechtigungen, die ihm zugewiesen sind, noch korrekt sind. Hierbei sind auch Vertretungsregelungen zu beachten.

**Benutzer des Cloud-Diensteanbieters und des Cloud-Anwenders**

Die Benutzerverwaltung (Management der Identitäten) beim Cloud-Diensteanbieter ist prinzipiell in zwei Bereiche aufzuteilen. Zum einen sind dies die Mitarbeiter des Cloud-Diensteanbieters selbst und auf der anderen Seite die Cloud-Benutzer des Cloud-Anwenders (Cloud-Mandanten). Hier ist noch zu unterscheiden, ob die Verwaltung der Cloud-Benutzer in der Hand des Cloud-Diensteanbieters liegt oder ob dieser (wie bei IaaS) nur die technischen Mittel bereitstellt und die Verwaltung der Cloud-Benutzer beim Cloud-Anwender liegt.

Bei der Benutzerverwaltung kann ein über Organisationsgrenzen hinweg arbeitendes Identitätsmanagement (englisch *Federated Identity Management, FIDM*) einbezogen oder angebunden werden, sofern gängige Standards (z. B. *Security Assertion Markup Language SAML*) und sichere Authentisierungsverfahren eingesetzt werden.

Die Berechtigungsverwaltung (Management der Berechtigungen) ist ähnlich aufgeteilt wie die Benutzerverwaltung: Man kann die Berechtigungen einerseits der Mitarbeiter des Cloud-Diensteanbieters und andererseits der Cloud-Benutzer des Cloud-Anwenders unterscheiden. Der Cloud-Anwender kann den Cloud-Benutzern dabei nur in dem Maß Rechte zur Verfügung stellen, wie es ihm der Cloud-Diensteanbieter im genutzten Cloud-Servicemodell ermöglicht.

**Benutzer, Rollen und Rechte beim Cloud-Diensteanbieter**

Der Cloud-Diensteanbieter sollte die Rechtevergabe rollenbasiert organisieren, wobei jede Rolle bestimmte Berechtigungen erhält. Den Benutzern werden dann über die Zuordnung zu Rollen die entsprechenden Rechte gewährt.

Hierbei sind z. B. Rollen für folgende Bereiche hilfreich, die Personen oder Systemen zugeordnet werden können:

- Cloud-Diensteprofile
- Virtualisierungs-Hosts (Starten, Stoppen und Migrieren der virtuellen IT-Systeme, Zuweisung von physischen Ressourcen)
- Netz
- Storage-System
- Self-Service-Portal
- Rechnungsstellung (englisch *Billing*)
- Berichtswesen (englisch *Reporting*)
- Middleware (Datenbanken, Webserver)

Eine Person oder ein System kann bzw. muss je nach Aufgabe mehrere Rollen nutzen können, um die zur Erfüllung der Aufgabe notwendigen Rechte zu erhalten. So muss der automatisiert ablaufende Prozess zum Provisionieren eines neuen Cloud-Mandanten mehrere Rollen haben, da er über weitreichende Rechte verfügen muss. Super-User, die alle Rechte in allen Bereichen haben, sind zu vermeiden.

**Benutzer, Rollen und Rechte beim Cloud-Anwender**

Die Rollen zur Nutzung von SaaS- und PaaS-Angeboten werden vom Cloud-Diensteanbieter definiert und dem Cloud-Anwender zur Verfügung gestellt. Sie sind an die verschiedenen Angebote des Cloud-Diensteanbieters angepasst, auf die die Cloud-Benutzer des Cloud-Anwenders Zugriff haben. Bei IaaS-Angeboten hat der Cloud-Anwender auf der virtuellen Maschine alle Freiheiten und kann/muss seine eigene Benutzer-, Rollen- und Berechtigungsverwaltung aufbauen.

In der Regel gibt es mindestens zwei verschiedene Arten von Rollen: privilegierter und normaler Benutzer.

- Der privilegierte Benutzer verwaltet die Nutzung des Cloud-Dienstes durch die Mitarbeiter (Cloud-Benutzer) des Cloud-Mandanten. Er kann in der Regel neue Benutzer hinzufügen oder löschen, Rollen zuweisen oder entziehen. Stellt der Cloud-Diensteanbieter dem Cloud-Anwender verschiedene Optionen der Cloud-Dienste oder unterschiedliche Cloud-Dienste zur Verfügung, so kann der privilegierte Benutzer den normalen Benutzern die Dienste oder Optionen freischalten. Hierzu stellt der Cloud-Diensteanbieter eine Schnittstelle (als Webservice oder als Webanwendung im Self-Service-Portal) zur Verfügung. Die Benutzerinformationen werden auf diesem Weg an das Cloud-Management beim Cloud-Diensteanbieter weitergegeben, durch das die entsprechenden Berechtigungen gesetzt werden. Ob und welche Rechte ein Cloud-Benutzer erhält, liegt in der Hand des Cloud-Anwenders. Der Cloud-Anwender muss diese Rechte verwalten und dafür bei sich intern die entsprechenden Prozesse aufsetzen. Der Cloud-Diensteanbieter muss dafür die Rahmenbedingungen setzen und hinterlegen, wie viele Benutzer angelegt und wie viele Ressourcen vergeben werden dürfen, damit Missbrauch verhindert werden kann.
- Der normale Benutzer ist der eigentliche Anwender des Cloud-Dienstes. Er hat in der Regel keine oder nur sehr geringe Möglichkeiten zur Verwaltung von Identitäten oder Rechten von Cloud-Diensten. Insbesondere darf

ein normaler Benutzer seine eigenen Rechte (und damit seine Zugriffsmöglichkeiten) nicht selbst ändern können. Im Fall eines Privatanwenders, der hier nicht betrachtet wird, sind die beiden Rollen privilegierter und normaler Benutzer in einer Person vereint, was aber bei Business-Anwendungen möglichst zu vermeiden ist, da die Cloud-Dienste sonst unkontrolliert sind und somit nicht mehr gesteuert genutzt werden können.

Übernimmt der Cloud-Diensteanbieter die Benutzer- und Berechtigungsverwaltung für einen Cloud-Anwender, so sind geeignete Prozesse zwischen den beiden Parteien zu etablieren. Diese Prozesse müssen gewährleisten, dass der Cloud-Diensteanbieter nachweislich im Sinne des Cloud-Mandanten handelt.

**Trennung unterschiedlicher Cloud-Mandanten**

In manchen Fällen und bei sehr großen Kunden kann der Cloud-Diensteanbieter mit der Forderung konfrontiert werden, dass nur bestimmte Administratoren den angebotenen Cloud-Dienst verwalten. Dann muss das Rollen- und Rechtemanagement (Berechtigungsverwaltung) des Cloud-Diensteanbieters zusätzlich noch mandantenfähig sein, um zu verhindern, dass unberechtigte Personen die Dienste eines Mandanten verwalten.

**Zugriff von Cloud-Administratoren auf Kundendaten**

Die Administratoren des Cloud-Diensteanbieters sollen möglichst keinen Einblick in die Daten und Anwendungen des Cloud-Mandanten erhalten und nicht in die Berechtigungsverwaltung einer SaaS- bzw. PaaS-Anwendung eingreifen, sofern diese von privilegierten Cloud-Benutzern verwaltet wird.

Zur Problemlösung kann es aber erforderlich sein, dass Administratoren des Cloud-Diensteanbieters auf Daten von Cloud-Mandanten Zugriff haben müssen. Hierzu sind technische Maßnahmen zu etablieren, die den Zugriff möglichst auf die zur Problemlösung relevanten Bereiche beschränken. Ferner sollte die Ausübung dieser Berechtigung nur für eine fest definierte Zeit möglich sein.

**Dokumentation**

Die folgenden Informationen zum Benutzer- und Berechtigungsmanagement müssen nachvollziehbar (Historie) dokumentiert werden:

- welche Funktion unter Beachtung der Funktionstrennung mit welchen Zugriffsrechten ausgestattet wird,
- welche Gruppen und/oder Profile eingerichtet werden,
- welche Person welche Funktion wahrnimmt,
- welche Zugriffsrechte eine Person im Rahmen welcher Rolle erhält.

Prüffragen:

- Ist ein rollenbasiertes Berechtigungskonzept für die Administratoren des Cloud-Diensteanbieters und für die Cloud-Benutzer des Cloud-Anwenders umgesetzt?
- Wurden Super-User vermieden?
- Sind alle angelegten Benutzer und deren Berechtigungen inklusive der Änderungshistorie dokumentiert?
- Ist ein Prozess vorhanden, in dem regelmäßig die vorhandenen Benutzerkonten geprüft werden?

# M 2.520 Sicheres und vollständiges Löschen von Cloud-Anwenderdaten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Im Rahmen des Cloud-Managements kann es aus unterschiedlichen Gründen dazu kommen, dass Teile von Datenbeständen oder alle Daten eines Cloud-Anwenders sicher gelöscht werden müssen. Zum Beispiel können Aufbewahrungspflichten ablaufen, außerordentliche Anforderungen zum Löschen von Daten von Dritten an den Cloud-Anwender herangetragen werden, oder der Vertrag über die Cloud-Dienste beendet werden.

Innerhalb welcher Fristen die Löschung geschehen muss sowie die Art und Weise, wie der Cloud-Diensteanbieter hierzu aufgefordert wird, sind in der Regel Bestandteile der vertraglichen Regelungen zwischen Cloud-Diensteanbieter und Cloud-Anwender. Dies sollte im Rahmen der Vertragsgestaltung berücksichtigt werden (siehe Maßnahme M 2.517 *Vertragsgestaltung mit Dritt-Dienstleistern*).

Das Löschen von Daten der Cloud-Anwender bezieht sich allerdings nicht nur auf Daten, die innerhalb der Cloud-Dienste verwaltet werden, sondern auch auf Daten für Cloud-Management-Prozesse, wie z. B. Daten zur Rechnungslegung, Daten zur Rollen- und Berechtigungsvergabe, Protokollierung und Cloud-Vertragsdaten (z. B. im Cloud Repository) sofern nicht rechtliche Anforderungen eine Aufbewahrungspflicht für den Cloud-Diensteanbieter vorschreiben.

Der Cloud-Diensteanbieter muss in der Lage sein, die Daten von allen virtuellen und physischen Speichermedien entsprechend den vertraglichen Vereinbarungen zu löschen.

Um die Vollständigkeit der Löschung zu gewährleisten, muss für den Cloud-Diensteanbieter der Speicherort aller Daten feststellbar sein, d. h. er muss wissen, welche Daten auf welchen Speichersystemen und -medien aufbewahrt werden. Zur Löschung der Daten aus dem Cloud Storage ist die Maßnahme M 2.527 *Sicheres Löschen in SAN-Umgebungen* umzusetzen.

Zur sicheren Löschung oder Vernichtung müssen zum einen geeignete Verfahren und zum anderen geeignete Geräte, Anwendungen oder Dienstleistungen zur Verfügung stehen. Hierfür muss der Cloud-Diensteanbieter einen Prozess zum sicheren Löschen (gemäß den geschlossenen vertraglichen Vereinbarungen) schriftlich definieren und mit Verantwortlichkeiten zur Umsetzung belegen. Für entsprechende Vorgaben und Prozesse sind die Vorgaben des Bausteins B 1.15 *Löschen und Vernichten von Daten*, soweit auf Cloud Computing übertragbar - zu berücksichtigen.

Prüffragen:

- Sind Prozesse und Verantwortlichkeiten vorhanden, wie einzelne Informationen oder der gesamte Datenbestand von Cloud-Anwendern gemäß vertraglichen Vereinbarungen gelöscht werden können?
- Stehen Geräte, Anwendungen und Dienstleistungen für ein vertragsgemäßes sicheres Löschen zur Verfügung?

- Können sowohl Nutzdaten als auch administrative Daten bei Bedarf gelöscht werden?

# M 2.521 Geregelte Provisionierung und De-Provisionierung von Cloud-Diensten

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Die Elastizität im Cloud Computing ermöglicht eine zeitnahe Bereitstellung von Cloud-Ressourcen für die Cloud-Anwender. Hierzu ist eine geregelte Provisionierung und De-Provisionierung von Cloud-Diensten notwendig.

Als Provisionierung wird die Zuweisung eines Cloud-Dienstes an einen Cloud-Anwender und die damit verbundene Bereitstellung der hierfür notwendigen Cloud-Ressourcen sowie deren Konfiguration bezeichnet. *Cloud-Ressourcen* sind CPU, Arbeitsspeicher, Datenspeicher (Storage), virtuelle Netze usw. Die Provisionierung erfolgt über Vorlagen mit den hinterlegten Informationen zu Cloud-Ressourcen und Konfigurationen. Die Vorlagen werden Cloud-Dienste-profile genannt.

Als De-Provisionierung, dem Gegenstück zur Provisionierung, wird die Rücknahme der Zuweisung von Cloud-Ressourcen eines bestimmten Cloud-Dienstes zu einem bestimmten Mandanten (Cloud-Anwender) bezeichnet. Provisionierung steht am Anfang der Nutzung eines Cloud-Dienstes durch einen Cloud-Anwender, De-Provisionierung am Ende.

Es müssen für alle Phasen der Verwaltung eines Cloud-Dienstes definierte Prozesse und Arbeitsabläufe etabliert und gepflegt werden. Für eine geregelte Provisionierung und De-Provisionierung von Cloud-Diensten muss ein Prozess mit Verantwortlichen hinterlegt und dokumentiert werden, der den kompletten Lebenszyklus eines Cloud-Dienstes berücksichtigen muss.

Der Prozess für Provisionierung und De-Provisionierung von Cloud-Diensten richtet sich nach den folgenden Phasen aus:

### Vorbereitung: Planung von Cloud-Diensten

Die Cloud-Dienste müssen geplant und die vom Cloud-Diensteanbieter ermittelten Anforderungen aufgenommen werden. Hierzu ist die Maßnahme M 4.437 *Planung von Cloud-Diensteprofilen* umzusetzen. Ergebnis dieser Planung ist die Referenzarchitektur (oft engl. *Blueprint*) eines Cloud-Dienstes. Hierzu gehören die benötigten Cloud-Ressourcen (CPU, Arbeitsspeicher, Netzanbindung und Netztrennung, Netz-Speicher) und deren Mengengerüste je Cloud-Benutzer.

### Planung und Umsetzung der Provisionierung

Der Cloud-Diensteanbieter muss die Bereitstellung der Cloud-Dienste gemäß der aktuellen Nachfrage steuern können. Die Arbeitsschritte für die Provisionierung müssen vorbereitet werden. Der Satz an Informationen von Eigenschaften und Ausprägungen des Cloud-Dienstes und die damit verbundenen Angaben zur Dienstgüte werden in einem Cloud-Dienste-Katalog des Cloud-Diensteanbieters hinterlegt. Der Dienste-Katalog enthält darüber hinaus die Information, welche Cloud-Anwender zu welchen Konditionen ausgewählte Cloud-Dienste nutzen dürfen.

Wird der Cloud-Dienst über ein Portal (ein sogenanntes Self-Service-Portal) angeboten, muss für die Provisionierung berücksichtigt werden, dass, je nach

Cloud-Dienst, der Cloud-Anwender direkten Einfluss auf die einzurichtende Konfiguration erhält. Entsprechend müssen für das Portal und für die Cloud-Diensteprofile logische Grenzen für die Ressourcenzuordnungen gesetzt werden. In solchen Fällen wäre die Anfrage eines Cloud-Anwenders über das Portal Initiator für den Provisionierungsprozess. Der Cloud-Diensteanbieter muss automatische oder manuelle Prüf- und Genehmigungsschritte vor der automatisierten Bereitstellung von Cloud-Diensten einrichten.

Die Provisionierung und De-Provisionierung mit Cloud-Diensteprofilen ermöglicht Administratoren, die Entwicklung komplexer Automatisierungsaufgaben in Prozessabläufen abzubilden. Anschließend können die Prozessabläufe schnell direkt über die Verwaltungssoftware der Cloud oder über verschiedene Auslösemechanismen aufgerufen und gestartet werden. Die manuellen Arbeitsschritte für die Cloud-Administratoren müssen in Form von Arbeitsanweisungen definiert und dokumentiert sein und Verantwortliche für die Arbeitsschritte festgelegt und bekannt gegeben werden.

Die korrekte Umsetzung der Konfigurationen auf Basis der Cloud-Diensteprofile muss für die automatisiert bereitgestellten Cloud-Dienste getestet werden. Zudem muss auf Basis von Stichproben die Konfiguration überprüft oder mittels der Cloud-Verwaltungslösung nachvollzogen werden, dass die Cloud-Dienste korrekt und anforderungsgemäß bereitgestellt werden.

Auch die Umsetzung der Konfigurationen und Sicherheitsmaßnahmen muss auf allen betroffenen Schichten der Cloud-Infrastruktur sichergestellt werden. Daher sind die Konfigurationseinstellungen in den Cloud-Diensteprofilen und in den provisionierten Cloud-Diensten zu kontrollieren. Insbesondere muss der Cloud-Diensteanbieter darauf achten, dass die Kommunikation zwischen Cloud-Verwaltungssoftware und den Cloud-Elementen oder deren Verwaltungssystemen (Element Manager) störungsfrei und korrekt verläuft.

**Beendigung von Cloud-Diensten: De-Provisionierung**

Kündigt der Cloud-Anwender den genutzten Cloud-Dienst oder läuft der Vertrag aus, muss eine geregelte Beendigung der Cloud-Dienste gewährleistet sein.

Mit der De-Provisionierung im Rahmen der Außerbetriebnahme von Cloud-Diensten muss die Konfiguration aus dem Provisionierungsprozess rückgängig gemacht werden. Der Cloud-Diensteanbieter muss sicherstellen, dass die Cloud-Ressourcen wieder freigegeben werden und die Cloud-Dienste mitsamt der Konten und Berechtigungen der Cloud-Benutzer nicht mehr aktiv sind. Die Administratoren des Cloud-Diensteanbieters müssen über die Cloud-Verwaltungssoftware nachvollziehen und überprüfen, dass die Cloud-Ressourcen (Speicher, VLANs, virtuelle Maschinen) freigegeben worden sind. Je nach Cloud-Infrastruktur muss die Freigabe der Cloud-Ressourcen auch an den Verwaltungskomponenten (Element Managern) kontrolliert werden.

Prüffragen:

- Wurden Verantwortliche für die Provisionierung und De-Provisionierung von Cloud-Diensten festgelegt und hinreichend kommuniziert?
- Sind die manuellen Arbeitsschritte der Cloud-Administratoren für die Provisionierung von Cloud-Diensten dokumentiert?
- Richtet sich die Planung der Cloud-Dienste nach den Anforderungen der Cloud-Anwender?

- Werden automatisch provisionierte Cloud-Dienste in der korrekten Umsetzung geprüft und die anforderungsgemäße Konfiguration der Cloud-Dienste nachvollzogen?
- Wie wird sichergestellt, dass nach Beendigung eines Cloud-Dienstes die zugehörigen Ressourcen und Berechtigungen entzogen werden?
- Führt die Planung zu Referenzarchitekturen für die Cloud-Dienste, die die Anforderungen widerspiegeln?

# M 2.522 Berichtswesen und Kommunikation zu den Cloud-Anwendern

**Verantwortlich für Initiierung:** Fachverantwortliche, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche

Es gibt zwei wesentliche Formen der Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwendern:

- Berichtswesen des Cloud-Diensteanbieters an die Cloud-Anwender
- Meldungen der Cloud-Anwender an den Cloud-Diensteanbieter

Nachstehend werden zunächst das Berichts- und dann das Meldewesen angesprochen.

**Berichtswesen**

In der Vereinbarung über die Dienstgüte (Dienstgüte-Vereinbarung, *Service Level Agreement, SLA*) oder im Cloud-Dienstekatalog ist der Cloud-Dienst beschrieben. Hier sind die konkreten Vereinbarungen zu den Eigenschaften des Cloud-Dienstes hinterlegt. Auch Mindestanforderungen an Kommunikations- bzw. Reaktionszeiten müssen vereinbart werden, um dem Cloud-Diensteanbieter und dem Cloud-Anwender ein Management der Dienstgüte zu ermöglichen.

Ein regelmäßiges Berichtswesen sollte eingeführt sein, damit der Cloud-Diensteanbieter gegenüber den Cloud-Anwendern die Dienstgüte (z. B. Verfügbarkeit) nachweisen kann: Berichte mit Angaben zu Dienstgüte, Nutzungsumfang durch den Cloud-Anwender (z. B. Verbrauch des gebuchten Speicherplatzes) und Kosten sollten regelmäßig an die Cloud-Anwender verteilt werden.

In der Dienstgüte-Vereinbarung oder im Cloud-Dienstekatalog muss definiert werden, welche Berichte und Messwerte den Cloud-Anwendern in welchen Zeitzyklen zur Verfügung gestellt werden. Hierbei müssen die Kennzahlen zur Messung der Dienstgüte und die Berichtsform sowie die Form der Bereitstellung festgelegt werden (z. B. über ein Web Dashboard eines Self Service Portals für Cloud-Anwender). Auf Basis der Messungen und der Kennzahlen im SLA sollte der Cloud-Anwender transparent nachvollziehen können, inwieweit der Cloud-Diensteanbieter die im SLA festgelegten Kennzahlen erreicht hat. Grundlage für die Messungen bildet die Protokollierung des Cloud-Dienstes.

**Meldewesen**

Etwaige Störungen oder Ausfälle von Ressourcen (wie z. B. Virtualisierungsserver, virtuelle Maschine, Load Balancer) müssen zeitnah erkannt werden, sodass rasch Gegenmaßnahmen eingeleitet werden können. Dementsprechend müssen Schnittstellen zum technischen Betrieb bei Sicherheitsproblemen (Benachrichtigung der Administratoren) definiert werden.

Hier muss der Cloud-Diensteanbieter eine Schnittstelle zu seinem bestehenden Informationssicherheitsvorfallmanagement schaffen und entsprechende Ansprechpartner definieren (siehe auch M 3.46 *Ansprechpartner zu Sicherheitsfragen* sowie M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

Allen Cloud-Anwendern müssen sowohl die Ansprechpartner zu Sicherheitsfragen als auch die Meldewege für Sicherheitsvorfälle bekannt gemacht wer-

den. Störungen, die von Cloud-Anwendern gemeldet werden, müssen sodann zum betrieblichen Störungsmanagement des Cloud-Diensteanbieters gelangen und dort bearbeitet werden.

Prüffragen:

- Wird der Cloud-Anwender regelmäßig und transparent über die vom Cloud-Diensteanbieter erbrachten Leistungen informiert?
- Sind den Cloud-Anwendern Kontaktmöglichkeiten zur Meldung von Störungen bekannt gemacht worden?

# M 2.523 Sichere Automatisierung der Cloud-Regelprozesse

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Cloud Computing sieht vor, dass ein geteilter Pool von konfigurierbaren Cloud-Ressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) mit minimalem Verwaltungsaufwand oder geringer Interaktion des Cloud-Diensteanbieters zur Verfügung gestellt wird. Hierfür müssen die Anfragen von Cloud-Diensten und deren Provisionierung automatisiert erfolgen. Die Herausforderung für Cloud-Diensteanbieter besteht darin, die Ressourcen in kürzester Zeit bereitzustellen und dabei dennoch die Informationssicherheit zu gewährleisten. Zugleich streben Cloud-Diensteanbieter aus betriebswirtschaftlichen Gründen an, die Serverauslastung der Cloud-Infrastruktur hochzuhalten und die laufenden Kosten zu minimieren.

Automatisierung der Cloud-Regelprozesse besteht derzeit meist in der skriptgesteuerten Abfolge von Konfigurationen über die Cloud-Verwaltungssoftware. Eine sichere Automatisierung der Cloud-Regelprozesse liegt vor, wenn die skriptbasierten Konfigurationen korrekt umgesetzt werden.

**Regelprozesse im Cloud Management**

Das Cloud Management umfasst mehrere Regelprozesse, um Cloud-Dienste in der vereinbarten Güte bereitzustellen, zu betreiben und abzurechnen. Zu den Regelprozessen gehören:

- Provisionierung und De-Provisionierung (auch: Orchestrierung)
- Registrierung von Cloud-Diensten im Dienste-Katalog
- Überwachung (Monitoring) der Cloud-Ressourcen und der Cloud-Dienstenutzung
- Zugangs- und Zugriffsmanagement für Cloud-Dienste
- Aufrechterhaltung von Cloud-Diensten

Die Cloud-Regelprozesse können durch Automatisierung für eine Verwaltung von einer großen Anzahl von Cloud-Diensten vereinfacht werden.

**Sichere Automatisierung bei der Provisionierung und De-Provisionierung von Cloud-Diensten**

Für eine sichere Automatisierung in der Provisionierung sind Grenzwerte für die Cloud-Ressourcen festzulegen. Wenn die Grenzwerte überschritten werden, besteht die Gefahr, dass nicht genügend Cloud-Ressourcen für alle Cloud-Dienste zur Verfügung stehen.

Dieses ist auch bei Portalen zur direkten Anfrage von Cloud-Diensten durch den Cloud-Anwender zu berücksichtigen. In den sogenannten Self-Service-Portalen sind die Anfragen von Cloud-Anwendern gegen Grenzwerte abzugleichen. Grenzwerte sind für die genutzte Bandbreite zur Bereitstellung von Cloud-Diensten, für die Rechenkapazitäten (CPU und Arbeitsspeicher) und für den Speicherplatz (*Storage*) zu definieren. Bei SaaS-Angeboten können die Grenzwerte auch die Anzahl der Cloud-Benutzer eines Cloud-Anwenders, Anzahl von Transaktionen etc. sein.

Über das Ressourcenmanagement des Cloud-Verwaltungsservers müssen Prozessor- und Arbeitsspeicherressourcen, die auf demselben physischen Server ausgeführt werden, den virtuellen Maschinen für die Cloud-Dienste

automatisiert zugewiesen werden. Für die automatisierte Bereitstellung von Cloud-Diensten muss der Cloud-Diensteanbieter die minimalen, maximalen und anteiligen Ressourcenanteile für CPU, Arbeitsspeicher, Festplatte sowie Netzwerkbandbreite festlegen.

Die Voreinstellungen für automatisierte Konfigurationsänderungen durch die Cloud-Verwaltungssoftware müssen geplant und die Prozessschritte definiert werden. Diese Prozessschritte umfassen automatisierte Schritte zur Lastverteilung und Priorisierung von Cloud-Diensten (u. a. unter Berücksichtigung von unterschiedlichen Service Levels von Cloud-Mandanten). Der Cloud-Diensteanbieter muss für die Cloud-Anwender Priorisierungen vornehmen, um im Fall von Ressourcenengpässen zu regulieren, welche Cloud-Dienste höheren Anspruch auf Cloud-Ressourcen erhalten.

Falls es regelmäßige Änderungen an Cloud-Diensten gibt, wie z. B. Lastspitzen oder "Wellen" in der Nutzungsverteilung von Cloud-Diensten, muss eine zeitliche Planung für die automatisierte Konfiguration (oft engl. *Scheduling*) erfolgen.

Die automatisierte Provisionierung und De-Provisionierung erfordert, dass die Cloud-Ressourcen korrekt miteinander interagieren. Dies ist nur möglich, wenn die unterschiedlichen Produkte und Cloud-Elemente über definierte Schnittstellen und Protokolle miteinander kommunizieren. Insbesondere die Interaktionen zwischen den Verwaltungskomponenten (Element Manager) der physischen und virtuellen Cloud-Ressourcen und der orchestrierenden Verwaltungssoftware müssen integer und korrekt ablaufen.

Um integre und korrekte Abläufe bei der Automatisierung von Cloud-Regelprozessen sicherzustellen, sind organisatorische *und* technische Maßnahmen nötig. Diese werden in den nachfolgenden Absätzen behandelt.

Organisatorisch: Die Cloud-Diensteprofile müssen kontrolliert werden. Dieses muss bei neuen oder geänderten Cloud-Diensteprofilen geschehen. Dabei werden die Konfigurationen der Cloud-Ressourcen gegen die Soll-Konfiguration aus den Anforderungen der Cloud-Dienste abgeglichen. Um die Kompatibilität der Cloud-Komponenten untereinander zu prüfen, sollten die Hersteller der Cloud-Komponenten zur Verträglichkeit und Anbindung der eingesetzten Produkte befragt werden.

Technisch: Die Kommunikation zwischen Cloud-Komponenten muss abgesichert werden. Dazu muss eine sichere und integre bidirektionale Kommunikation zwischen den Cloud-Komponenten eingerichtet werden. Dieses muss über die eingesetzten Protokolle für die Übertragung der automatisierten Konfigurationsänderungen erfolgen. Entweder werden Management-Protokolle eingesetzt, welche eigene integritätssichernde Mechanismen bereits enthalten oder die Kommunikation muss verschlüsselt werden. So kann zum Beispiel SNMP Version 3 eingesetzt werden, um Verschlüsselung und ausreichende Authentisierung zu erreichen. Für die detaillierte Umsetzung ist die Maßnahme M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll* heranzuziehen.

**Sichere Automatisierung der Registrierung von Cloud-Diensten**

Die in der Provisionierung zugewiesenen Cloud-Ressourcen und die bereitgestellten Dienstgüten (z. B. Speicherplatz) müssen in einem Verzeichnis in der Cloud-Verwaltung abgelegt werden, dem sogenannten Cloud-Dienstekatalog. Die Cloud-Verwaltungssoftware muss gewährleisten, dass eine aktuelle Übersicht über die aktiven Cloud-Dienste zeitnah bereitgestellt werden kann.

Der Cloud-Dienstekatalog muss die automatisiert bereitgestellten Cloud-Dienste und die Zuordnung zu den Cloud-Anwendern korrekt enthalten. Die Korrektheit der Angaben im Cloud-Dienstekatalog muss sichergestellt sein und durch integre Angaben in der Cloud-Verwaltungssoftware erfolgen. Der Cloud-Diensteanbieter muss deshalb die Angaben des Cloud-Dienstekatalogs mit den tatsächlich angebotenen Cloud-Diensten und deren Dienstgüte, sowie deren Zuordnung zu Cloud-Anwendern überprüfen. Der Cloud-Dienstekatalog (oft engl. *Cloud Repository*) muss aufgrund der Integritätsanforderungen zugriffsbeschränkt werden und es müssen sämtliche Änderungen protokolliert werden.

**Überwachung (Monitoring) der Cloud-Ressourcen und der Cloud-Dienstenutzung**

Die Überwachung der Cloud-Ressourcen und der Cloud-Dienstenutzung erfolgt über die Protokollierung von Ereignissen an Komponenten der Cloud-Infrastruktur. Die Auswertung der Protokollierung muss (teil-) automatisiert erfolgen und hier eine Verdichtung (über eine Korrelation von Ereignissen) der wesentlichen Informationen zur Überwachung der Cloud vorgenommen werden. Die Grenzwerte (Minima/Maxima) für die Auslastung der Cloud-Ressourcen müssen definiert und die Protokollierungsinformationen hinsichtlich dieser Schwellwerte ausgewertet werden. Auf Basis der Ressourcen-Überwachung muss entweder direkt die Cloud-Verwaltungssoftware Cloud-Ressourcen umorganisieren (z. B. können priorisierte Cloud-Dienste vorrangig versorgt werden) oder eine Alarmierung an die Cloud-Administration erfolgen.

**Automatisierung des Zugangs- und Zugriffsmanagements für Cloud-Dienste**

Bei der Bereitstellung von Cloud-Diensten muss der Zugriff auf diese Dienste gesteuert werden. Hierbei muss ein Zugriffsschutz eingerichtet werden, der bereits in den Cloud-Diensteprofilen berücksichtigt werden muss. Insbesondere bei der automatisierten Provisionierung von Cloud-Diensten muss eine Authentisierung der Cloud-Benutzer mit Zugriffsschutz vorhanden sein. Alternativ kann ein Zugriffsschutz mit Authentisierung der berechtigten Cloud-Benutzer vorgelagert erfolgen. Dies kann z. B. über ein über Organisationsgrenzen hinweg arbeitendes Identitätsmanagement geschehen, oft englisch *Federated Identity Management (FIDM)*.

**Automatisierung bei der Aufrechterhaltung von Cloud-Diensten**

Bei der Aufrechterhaltung des Betriebs von Cloud-Diensten müssen automatisierte Mechanismen für den Schutz der Verfügbarkeit eingesetzt werden. Diese Automatisierung wird durch netzbasierte Komponenten des Load Balancing erreicht, durch Serverbetrieb im Cluster und durch automatisierte Funktionen in der Virtualisierung (z. B. automatische Zuordnung von virtuellen Ressourcen).

Prüffragen:

- Sind Grenzwerte (Minima und Maxima) für die Cloud-Ressourcen und Reaktionen bei Verletzung dieser Grenzwerte festgelegt?
- Sind die Cloud-Dienste und Zuweisungen der Cloud-Ressourcen priorisiert?
- Wird die Korrektheit der automatischen Konfigurationen im Rahmen der Provisionierung und De-Provisionierung überprüft?

- Wird sichergestellt, dass die automatisiert angesteuerten Cloud-Komponenten zueinander kompatibel sind und korrekt miteinander kommunizieren?
- Werden integritätsgesicherte Managementprotokolle für die automatisierte Konfiguration verwendet?
- Werden die Angaben des Cloud-Dienstekatalogs mit den tatsächlich angebotenen Cloud-Diensten und deren Dienstgüte abgeglichen?
- Werden Protokollierungsinformationen an Cloud-Komponenten (teil-) automatisch ausgewertet?
- Enthalten die automatisiert bereitgestellten Cloud-Dienste Zugriffsschutzmechanismen und erfordern eine Authentisierung?

# M 2.524 Modellierung von Cloud Management

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

In dieser Maßnahme wird erläutert, wie Cloud Management korrekt nach der IT-Grundschutz-Vorgehensweise modelliert wird. Es werden die notwendigen Bausteine des IT-Grundschutzes benannt und es wird beschrieben, wie die verschiedenen Servicemodelle (SaaS, PaaS, IaaS) des Cloud Computing in einer Sicherheitskonzeption abgebildet werden können. Zur Definition von Begriffen für Cloud Computing, z. B. zu den Servicemodellen (siehe Maßnahme M 4.446 *Einführung in das Cloud Management*).

Der Baustein B 5.23 *Cloud Management* richtet sich an Cloud-Diensteanbieter.

Um eine angemessene Gesamtsicherheit für den IT-Betrieb von Cloud-Diensten zu erreichen, müssen alle Cloud-Dienste (mit ihren zugeordneten virtuellen IT-Systemen, Netzen und weiteren Cloud-Komponenten) systematisch in der Sicherheitskonzeption berücksichtigt werden. Alle über Cloud-Dienste bereitgestellten IT-Systeme, Netze und Anwendungen, die sich einerseits in der Betriebsverantwortung und andererseits im Geltungsbereich des Informationssicherheits-Managementsystems des Cloud-Diensteanbieters befinden, müssen in der Strukturanalyse und in der Modellierung gemäß der IT-Grundschutz-Vorgehensweise berücksichtigt werden.

Als Modellierung wird in der IT-Grundschutz-Vorgehensweise die Zuordnung von Bausteinen zu den vorhandenen Zielobjekten (IT-Systeme, Anwendungen, Räume etc.) bezeichnet. Die Modellierung erfolgt für virtuelle IT-Systeme, Netze und Anwendungen der Cloud nach den selben Regeln wie für physische IT-Systeme, die nicht über Cloud Computing bereitgestellt werden, und die Hinweise in Abschnitt 4.4 *Auswahl und Anpassung von Maßnahmen* des BSI-Standards 100-2 *IT-Grundschutz-Vorgehensweise* sind zu beachten.

Bei der Modellierung eines Informationsverbunds mit einem Cloud Management, das die verwaltenden Tätigkeiten des Cloud-Diensteanbieters umfasst, wird der Baustein B 5.23 *Cloud Management* auf den Cloud-Verwaltungsserver angewendet. Er wird somit nicht für jede Anwendung, jedes Netz oder jedes IT-System der Cloud-Infrastruktur modelliert. Am Cloud-Verwaltungsserver werden die zentralen Maßnahmen des Cloud Managements umgesetzt, wie z. B. Zugriffschutz, Überwachung von Cloud-Ressourcen und Orchestrierung (Provisionierung und De-Provisionierung) der Cloud-Ressourcen. Dementsprechend ist es bei allen Servicemodellen notwendig, den Baustein B 5.23 *Cloud Management* in die Modellierung aufzunehmen.

Der Umfang des Informationsverbundes unterscheidet sich dabei je nach dem Servicemodell.

Der Geltungsbereich des Informationsverbundes kann gleichzeitig als Grenze der Verantwortlichkeit verstanden werden: An der Grenze des Informationsverbundes endet die Verantwortung des Cloud-Diensteanbieters und beginnt die Verantwortung des Cloud-Anwenders.

**Modellierung von IaaS-Angeboten**

Bei IaaS ist der Umfang der Cloud-Dienste im Vergleich zu PaaS und SaaS am geringsten (vergleiche Abbildung Größe des Informationsverbunds für Cloud Management in Abhängigkeit vom Servicemodell):

Bei IaaS verantwortet der Cloud-Diensteanbieter den Verwaltungsserver für die Cloud und den Virtualisierungsserver.

Deshalb kommen bei IaaS aus der Schicht 5 *Anwendungen* nur die Verwaltungs- und die Virtualisierungssoftware als Zielobjekte vor. Für diese müssen somit die zugehörigen Bausteine ausgewählt werden. Nach der IT-Grundschutz-Vorgehensweise sind dies Bausteine für IT-Systeme als Server. Für den Cloud-Verwaltungsserver werden die Bausteine B 3.304 *Virtualisierung* und B 5.23 *Cloud Management* zugeordnet.

Für IaaS stellt der Cloud-Diensteanbieter nicht mehr als eine virtuelle "Hülle" über ein virtuelles Netz bereit. Die Absicherung des Netzes nach IT-Grundschutz verantwortet bei IaaS der Cloud-Diensteanbieter, wohingegen die Cloud-Anwender die IT-Systeme des Cloud-Angebotes verantworten. Für das Netz sind die passenden Bausteine aus der Schicht 4 zu modellieren (z. B. B 4.1 *Lokale Netze*, B 4.2 *Netz- und Systemmanagement*). In der Regel wird dem virtuellen Server ein Speicherkontingent aus einem Speichernetz zugeordnet und hierfür ist der Baustein B 3.303 *Speicherlösungen / Cloud Storage* ebenfalls vom Cloud-Diensteanbieter umzusetzen.

Ein virtueller Server aus der Cloud, der per IaaS angeboten wird, wird durch den Cloud-Anwender konfiguriert. Die Umsetzungsverantwortung für seine Sicherheitsmaßnahmen liegt somit ebenfalls beim Cloud-Anwender. Im Hinblick auf die Abgrenzung des Informationsverbundes des Cloud-Diensteanbieters befindet sich also dieser virtuelle Server außerhalb des Informationsverbundes des Cloud-Diensteanbieters.

Die Schnittstelle zur Bereitstellung von IaaS-Cloud-Diensten (Self-Service-Portal) ist durch Trenneinrichtungen (Netze, virtuelle Firewalls, Routing) vom Cloud-Diensteanbieter abzusichern und gegebenenfalls der Baustein B 5.21 *Webanwendungen* umzusetzen.

Eine Modellierung der IaaS-Server als IT-Systeme im Sicherheitskonzept des Cloud-Diensteanbieters ist möglich, allerdings nicht notwendig, da die Cloud-Anwender diese IT-Systeme verwalten.

**Modellierung von PaaS-Angeboten**

Bei PaaS verantwortet der Cloud-Diensteanbieter zusätzlich zu IaaS die sichere Bereitstellung eines virtuellen Servers und einer angebotenen Plattform (z. B. einer Datenbank oder eines Webservers).

Dementsprechend muss der Cloud-Diensteanbieter im Servicemodell PaaS zunächst, wie bei IaaS, den Cloud-Verwaltungsserver und dessen Verwaltungssoftware modellieren. Dort erfolgt zentral die Zuordnung des Bausteins B 5.23 *Cloud Management*.

Darüber hinaus muss der Cloud-Diensteanbieter sodann ein IT-System mit Betriebssystem modellieren. Zu diesem IT-System ist je nach Cloud-Dienst auf Anwendungsschicht eine Datenbank oder ein Webserver zu modellieren.

Das PaaS-IT-System mit den verbundenen Cloud-Anwendungen muss für jeden Cloud-Mandanten modelliert werden, wobei Mandanten mit gleichen Plattformen, gleichen Anwendungen und gleichem Schutzbedarf gemäß den Vorgaben des BSI-Standards 100-2 Abschnitt 4.2.1 in einer Gruppe zusammengefasst werden können.

In der Praxis werden Cloud-Dienste des Servicemodells PaaS über virtuelle Profile bereitgestellt, die für mehrere Cloud-Anwender bzw. Mandanten eingesetzt werden können. Es bietet sich daher in der IT-Grundschutzmodellierung an, diese Kombinationen in Form von Musterservern zu modellieren und pro Mandant zu verknüpfen bzw. zu vervielfachen.

**Modellierung von SaaS-Angeboten**

Bei SaaS müssen zunächst für die unterliegende Cloud-Infrastruktur die Zielobjekte wie bei IaaS und PaaS betrachtet und diesen Bausteinen zugeordnet werden, wie in den vorangehenden Abschnitten beschrieben.

Im Vergleich zu PaaS werden bei SaaS weitere Anwendungen auf den Cloud-IT-Systemen modelliert (z. B. ein Webservice, eine Webanwendung oder ein SAP-System). Die Anwendungen werden vom Cloud-Diensteanbieter verantwortet und die Umsetzung der Sicherheitsmaßnahmen erfolgt durch den Cloud-Diensteanbieter weitestgehend selbst (Ausnahmen, wie Umsetzung durch Dritt-Hersteller, müssen in der Beschreibung zur Maßnahmenumsetzung erläutert werden).

Die SaaS-Anwendungen müssen somit im Informationsverbund des Cloud-Diensteanbieters modelliert werden. Dabei können sowohl mehrfache Ausprägungen der gleichen SaaS-Anwendung als auch Gruppen von SaaS-Anwendungen gemäß den Vorgaben des BSI-Standards 100-2 Abschnitt 4.2.1 *Komplexitätsreduktion durch Gruppenbildung* zusammengefasst werden, wenn die dort angegebenen Voraussetzungen erfüllt sind.

**Informationsverbund für Cloud-Management**

Die nachstehende Abbildung stellt die beschriebenen Servicemodelle und deren zu modellierende Bereiche dar.

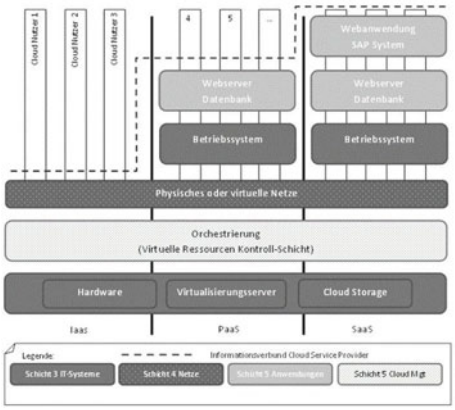



Abbildung: Größe des Informations-

verbunds für Cloud Management
in Abhängigkeit vom Servicemodell

**Fallbeispiel: Modellierung eines Cloud-Dienstes für das Servicemodell PaaS**

Um die Modellierung von Cloud Management zu verdeutlichen, wird im Folgenden ein Beispiel aus der Praxis beschrieben.

Um das Beispiel übersichtlich zu halten, werden Bausteine der Schicht 2 *Infrastruktur* nicht im Beispiel betrachtet.

**Szenario:**

Ein Cloud-Diensteanbieter stellt über Cloud Computing eine Plattform, in Form eines Apache-Webservers und einer Oracle-Datenbank, für webbasierte Anwendungen bereit, die von den Cloud-Benutzern entwickelt werden können.

Das Szenario wird durch die Abbildung *Beispiel zur Modellierung eines PaaS-Cloud-Dienstes* illustriert. Auf der linken Seite sind die Komponenten des PaaS-Cloud-Dienstes zu sehen: vom *Blade Server* für die Cloud-Verwaltung als Grundlage bis zu den Anwendungen *Oracle DB* und *Apache*. Rechts im Bild sind diesen Komponenten die jeweils anwendbaren Bausteine der verschiedenen Schichten des IT-Grundschutzes zugeordnet.

In diesem Beispiel muss ein Virtualisierungsserver als Zielobjekt modelliert werden. Dabei sind die IT-Grundschutz-Bausteine B 3.101 *Allgemeiner Server* und B 3.304 *Virtualisierung* zuzuordnen. Baustein B 3.101 *Allgemeiner Server* behandelt dabei die Sicherheitsaspekte, die unabhängig vom eingesetzten Betriebssystem für Server relevant sind. Dieser Baustein ist deshalb stets zuzuordnen, unabhängig davon, ob die Virtualisierungssoftware mit oder ohne unterliegendes Betriebssystem läuft.

Auf dem Virtualisierungsserver (Beispiel: Blade Server als Hardware) werden eine Cloud-Verwaltungssoftware und eine Virtualisierungssoftware betrieben.

Bei Virtualisierungssoftware und Cloud-Verwaltungssoftware gibt es Produkte, die ein unterliegendes Betriebssystem benötigen, und andere, die selbstständig laufen, ohne unterliegendes Betriebssystem. Wenn der Virtualisierungssoftware oder der Cloud-Verwaltungssoftware ein Betriebssystem unterliegt, muss der dazu passende Baustein ebenfalls zugeordnet werden, z. B. B 3.102 *Server unter Unix*.

Mit dem Virtualisierungsserver als zentralem IT-System wird in der Modellierung der Baustein B 5.23 *Cloud Management* auf Schicht 5 als Anwendungsbaustein verknüpft.

Zudem kann dieser Server zur Cloud-Verwaltung weitere Anwendungen wie einen Webdienst bereitstellen, um auf die Cloud-Verwaltungssoftware zuzugreifen. In diesem Fall sind die Bausteine B 5.4 *Webserver* und B 5.21 *Webanwendungen* zu modellieren.

Mithilfe der Cloud-Verwaltungssoftware wird jedem Cloud-Anwender des PaaS ein virtuelles LAN (VLAN) für den Zugriff auf seine Cloud-Dienste bereitgestellt. Zur Modellierung muss zunächst ein virtuelles IT-System (im Beispiel mit Windows 2003 Server) als Server modelliert werden. Für den virtuellen Server werden die Bausteine B 3.101 *Allgemeiner Server* und B 3.108 *Windows Server 2003* angewendet. Sodann müssen die anwendbaren Netzbausteine B 4.2 *Netz- und Systemmanagement* und B 4.1 *Lokale Netze* an einem

Netz *VLAN-XY* modelliert werden. Das *VLAN-XY* wird mit dem virtuellen IT-System verknüpft.

Auf der Schicht 5 *Anwendungen* wird eine Oracle-Datenbank mit dem Baustein B 5.7 *Datenbanken* modelliert und dem virtuellen IT-System zugeordnet. Ferner wird ein Apache-Webserver mit dem Baustein B 5.4 *Webserver* modelliert und ebenfalls dem virtuellen IT-System zugeordnet.

Der modellierte Server mit den Anwendungen und dem zugehörigen VLAN kann nun als Profil für die Nutzung des PaaS durch verschiedene Cloud-Anwender als Mandanten verwendet werden. (Hierbei können sinnvolle Gruppen gebildet werden, wobei die Hinweise zur korrekten Gruppierung gemäß BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise* Abschnitt 4.2.1 zu beachten sind.) Wie oft der PaaS-Cloud-Dienst bereitgestellt wird (also wie viele "Kopien" dieses "Profils" aktiv sind), muss der Cloud-Diensteanbieter über die Cloud-Verwaltungssoftware nachvollziehen können.

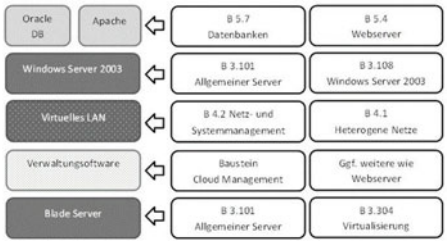



Abbildung: Beispiel zur Modellierung eines PaaS-Cloud-Dienstes

# M 2.525 Erstellung einer Sicherheitsrichtlinie für Speicherlösungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Speicherlösungen als zentrale Instanz zur Datenspeicherung einzusetzen, ist für viele Abläufe und Geschäftsprozesse einer Institution essenziell. Der sichere und ordnungsgemäße Betrieb kann nur sichergestellt werden, wenn Planung, Stationierung, Administration und Betrieb von Speicherlösungen in die bestehenden sicherheitstechnischen Vorgaben integriert sind.

Die zentralen sicherheitstechnischen Anforderungen und das zu erreichende Sicherheitsniveau ergeben sich aus der organisationsweiten Sicherheitsleitlinie. Die Anforderungen sollten in einer spezifischen Sicherheitsrichtlinie für Speicherlösungen formuliert werden, um die übergeordnete und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

Grundlage für eine angemessene Definition von Forderungen, die in der Sicherheitsrichtlinie Ausdruck finden, ist die Dokumentation der Schutzbedarfsfeststellung aller Daten, die in einer ausgewählten Speicherlösung (M 2.362 *Auswahl einer geeigneten Speicherlösung*) gespeichert werden sollen. Nur hieraus lässt sich ableiten, welche Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der Daten gestellt werden und entsprechend, welcher technische und organisatorische Aufwand angemessen ist.

Werden in einer Institution unterschiedliche Speicherlösungen (z. B. SAN, NAS, Objekt-Storage, Cloud Storage) eingesetzt, kann es sinnvoll für die Verantwortlichen sein, für die einzelnen Anwendungsfälle separate Sicherheitsrichtlinien zu erstellen und sich dabei an der vorliegenden Maßnahme zu orientieren.

Da SAN-Lösungen ein dediziertes Netz enthalten, ist für die Erstellung einer Sicherheitsrichtlinie für SAN-Lösungen zusätzlich die Maßnahme M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches* zu beachten. Dort werden die allgemeinen Sicherheitsvorkehrungen für IT-Komponenten, die in einem internen Netz den Zugang zu Informationen oder anderen Systemen ermöglichen, vorgestellt. Für die Erstellung einer Sicherheitsrichtlinie für NAS-Lösungen ist zusätzlich die Maßnahme M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server* zu beachten. Dort werden die allgemeinen Sicherheitsvorkehrungen für IT-Systeme mit einer Serverfunktion vorgestellt. Sofern Cloud-Storage-Lösungen zum Einsatz kommen, sind zusätzlich die Vorgaben aus M 2.535 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* aus dem Baustein B 1.17 *Cloud-Nutzung* zu betrachten.

Weitere Aspekte, die in der Sicherheitsrichtlinie für Speicherlösungen behandelt werden müssen, sind:

**Vorgaben für die Planung von Speichersystemen**

- Es sind Vorgaben für die technische Infrastruktur zu entwickeln, in der Speicherkomponenten aufgestellt werden. Die Infrastruktur der Räume, in denen Komponenten der Speicherlösung stationiert werden, muss geeignet sein, um die Verfügbarkeitsanforderungen der Speicherlösung durch

entsprechende Strom-, Netz- und Klimaversorgung zu erfüllen. Ebenso soll der Zutritt zu diesen Räumen angemessen geschützt werden.
- Es sind Vorgaben zu machen, die den Zugriff Externer (beispielsweise zu Wartungszwecken) regeln. Da Überwachungs- und Wartungsverträge von Lieferanten der Speicherkomponenten oftmals direkte Anbindung der Speicherlösung an Überwachungssysteme des Herstellers oder Lieferanten fordern, ist festzulegen, wie solche Zugriffe kontrolliert und protokolliert werden.
- Wenn in Bezug auf die Verfügbarkeit ein sehr hoher Schutzbedarf festgestellt wird, sollte der Einsatz einer desastertoleranten SAN-Lösung eingefordert werden. Zu diesem Zweck sollte die Speicherlösung hinsichtlich SPoFs (Single Points of Failure), die bei einem Ausfall den Komplettausfall des Systems nach sich ziehen, analysiert werden. Ist eine sehr hohe Verfügbarkeit der Speicherlösung gefordert, ist die Analyse von SpoFs in jedem Fall vorzunehmen. Sollen neue Komponenten in eine hochverfügbare SAN-Lösung eingebracht werden, ist deren reibungslose Integration zunächst innerhalb spezieller Testsysteme zu überprüfen.

**Vorgaben für die Arbeit von Administratoren**
- Es ist zu dokumentieren, nach welchem Schema Administrationsrechte für einzelne Komponenten der Speicherlösung oder das Gesamtsystem vergeben werden. Es ist empfehlenswert, ein entsprechendes Rollenkonzept zu entwickeln.
- Es sollten Administrator-Rollen definiert werden, denen aufgabenbezogen die notwendigen Rechte eingeräumt werden. Insbesondere sollte die routinemäßige Systemverwaltung (zum Beispiel Backup) nur mit den unbedingt notwendigen Rechten durchgeführt werden können. Die Administrator-Kennungen werden in der Folge den Rollen zugeordnet. Um die Auswirkungen von Fehlern zu reduzieren, darf unter einer Administrator-Kennung nur gearbeitet werden, wenn es zwingend notwendig ist.
- Der administrative Zugriff ist mindestens durch Einsatz starker Passwörter, gegebenenfalls auch durch besondere Maßnahmen zur Benutzerauthentisierung abzusichern.
- Die Verwaltung und Kontrolle von Speicherressourcen durch die Administratoren und der Zugriff für Revisoren auf die Systeme ist entweder nur lokal über eine direkt angeschlossene Konsole, ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen zulässig. Der Zugriff auf Speicherressourcen ist auf definierte Systeme zu beschränken und z. B. durch Sicherheitsgateways zu kontrollieren.
- IT-Systeme, die als Managementkonsole oder zur Revision eingesetzt werden, sind auf bestmögliche Weise vor Schadprogrammen zu schützen.
- Durch die vorgegebene Aufgabenteilung, durch Vorgaben und Regelungen und eine stets aktuelle Dokumentation der Einstellungen aller Speicherkomponenten ist sicherzustellen, dass Administratoren keine Aktionen ausführen oder Einstellungen an der Speicherlösung vornehmen, die zu Inkonsistenzen, Ausfällen oder Datenverlust führen können. Relevante Änderungen müssen dokumentiert werden. Es ist dazu empfehlenswert, ein Änderungsmanagement-Verfahren, z. B. in Anlehnung an ITIL (IT Infrastructure Library) zu betreiben.
- Es ist festzulegen, ob für bestimmte Änderungen das Vieraugenprinzip anzuwenden ist.

**Vorgaben für die Installation und Konfiguration der Speicherlösung**
- Das Vorgehen bei der Erstinstallation ist zu dokumentieren. Da diese in den meisten Fällen vom Hersteller oder Lieferanten vorgenommen wird, ist die entsprechende Dokumentation einzufordern.

- Nach der Installation sind die Default-Einstellungen in Bezug auf Sicherheitsgefährdungen zu überprüfen, unsichere Dienste auf Netzkomponenten und Speichergeräten zu deaktivieren und die Standardkennungen und -passwörter zu ändern.
- Zugriffe von Systemkonsolen auf Speicherkomponenten über das LAN sollten ausschließlich über verschlüsselte Verbindungen ermöglicht werden. Der Kreis der zugriffsberechtigten Anwender auf die Geräte ist möglichst klein zu halten. Regeln zur Verwendung und Konfiguration der Konsole und Restriktion der Zugriffsarten sind zu dokumentieren.
- Es ist zu regeln, wie Dokumentationen zu erstellen und zu pflegen sind und in welcher Form die Dokumentationen (z. B. Verfahrensanweisungen für die Einrichtung administrativer Kennungen, Betriebshandbücher für Abläufe und Kontrollen im Normalbetrieb) vorliegen sollen.
- Innerhalb des SANs sollten spezifische Methoden der Segmentierung (siehe M 5.130 *Absicherung des SANs durch Segmentierung*) genutzt werden. Damit wird im SAN ein besserer Schutz von Teilbereichen sowohl bezüglich der Vertraulichkeit und Verfügbarkeit als auch bezüglich der Integrität der Konfiguration und der Verfügbarkeit des SANs erreicht.

**Vorgaben für den sicheren Betrieb**

- Die Administration der Speicherlösung ist abzusichern, indem Zugriffe nur über besondere Verbindungen (ein separates Administrationsnetz, gegebenenfalls auch das Speichernetz selbst) zugelassen werden.
- Es sind gegebenenfalls Werkzeuge auszuwählen, mit denen die Speicherkomponenten in einem bestehenden Netzmanagement betrieben, gewartet und integriert werden können. Vorgaben für eine sichere Konfiguration dieser Werkzeuge müssen definiert werden. Wenn möglich, sollten nur verschlüsselte Verbindungen genutzt und nicht benötigte Schnittstellen und Dienste deaktiviert bzw. gesperrt werden.
- Falls eine Fernwartung oder Überwachung durch den Hersteller genutzt werden soll, müssen Vorgaben für die Absicherung der Zugänge definiert werden. Beispielsweise ist die Anbindung per VPN oder exklusiv genutzte Verbindungen zu realisieren und eine für die Institution nachvollziehbare Protokollierung dieser Aktivitäten einzufordern. Weitere Informationen sind in der Maßnahme M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration* enthalten.
- Es ist eindeutig festzulegen, wer berechtigt ist, Software-Updates zu initiieren oder Konfigurationen zu ändern. Die Vorgehensweise ist zu dokumentieren. Sobald sehr hohe Anforderungen an die Verfügbarkeit bestehen, ist zu fordern, dass Änderungen und Updates stets vor dem Wirkbetrieb an baugleichen Testsystemen zu erproben und zu bewerten sind.
- Während des Betriebes einer Speicherlösung sind alle administrativen Tätigkeiten zu protokollieren. Darüber hinaus muss ein Konzept für die Verwaltung und Überwachung der Speichersysteme erstellt werden. Informationen zu diesem Thema finden sich in M 2.359 *Überwachung und Verwaltung von Speicherlösungen*.
- In Abhängigkeit vom Schutzbedarf (z. B. hoch oder sehr hoch), vom Betreibermodell (z. B. bei Fremdbetrieb), von der Lokation (z. B. Unterbringung einzelner Komponenten oder der kompletten Speicherlösung bei einem Dienstleister) oder in Abhängigkeit von der Mandantenfähigkeit besteht die Notwendigkeit zum Einsatz von Verschlüsselung. Hinweise hierzu finden sich in M 4.448 *Einsatz von Verschlüsselung für Speicherlösungen*.
- Die Regelungen für die Datensicherung der Speicherlösung sind mit dem übergreifenden Datensicherungskonzept der Institution (siehe dazu Baustein B 1.4 *Datensicherungskonzept*) und mit den Schutzbedarfsanforderungen der Speicherlösung abzustimmen. Bei besonderen Anforderungen

an die Vertraulichkeit ist hier die Rechteverwaltung auf Backups vorzugeben.
- Aufgrund der zentralen Bedeutung einer Speicherlösung sind deren Notfallvorsorge und die Pläne für den Notfall (siehe auch M 6.98 *Notfallvorsorge und Notfallreaktion für Speicherlösungen*) in das organisationsweite Notfallmanagement einzubinden.
- Verantwortlichkeiten und Vorgehen für Revision und Audit sind zu beschreiben. Die Revision von Speicherlösungen ist in ein übergreifendes Revisionskonzept zu integrieren.

Prüffragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb von Speicherlösungen erstellt?
- Wurde ein Sicherheitsniveau in der Sicherheitsrichtlinie definiert?
- Wurden in der Sicherheitsrichtlinie Vorgaben zur Planung, Administration, Installation und Konfiguration sowie zum Betrieb von Speicherlösungen beschrieben?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde die Sicherheitsrichtlinie für Speichersysteme in das organisationsweite System für Revision und Audits aufgenommen und Schnittstellen zum Notfallmanagement geschaffen?

# M 2.526 Planung des Betriebs der Speicherlösung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Der dauerhafte sichere Betrieb einer Speicherlösung erfordert eine sorgfältige Planung. Neben der Festlegung des Betreiberkonzeptes und des Aufstellungsortes der Speicherlösung muss der Betrieb der Speicherlösung organisatorisch geregelt und dokumentiert werden. Zur Unterstützung des Betriebes sollte ein Betriebshandbuch erstellt und regelmäßig aktualisiert werden.

Die wesentlichen Themen für die Planung des Betriebs der Speicherlösung sind im Folgenden ausführlich beschrieben.

### Auswahl eines Betreiberkonzeptes

Die Entscheidung für ein Betreiberkonzept ist in der Regel bereits im Rahmen der Planung der Speicherlösung gefallen. Für den Betrieb der Speicherlösung werden hierzu nähere Angaben, beispielsweise hinsichtlich der verantwortlichen Ansprechpartner, benötigt. Daher ist durch die Institution zu dokumentieren, ob der Betrieb der Speicherlösung durch eigenes Personal oder durch einen Dienstleister mit oder ohne Übergabe der Betriebsverantwortung erfolgen wird.

Angaben zum ausgewählten Dienstleister, zu den verantwortlichen Ansprechpartnern und möglichen Besonderheiten beispielsweise bei der Entscheidung für die Nutzung von Storage as a Service (SaaS) sind ebenfalls zu dokumentieren.

### Aufstellung der Speicherlösung

Die notwendigen Maßnahmen hinsichtlich der Aufstellung der Speicherlösung sollten ebenfalls bereits im Rahmen der Planung einer Speicherlösung betrachtet werden. In der Regel stehen sie in engem Zusammenhang mit dem gewählten Betreiberkonzept. Die Entscheidung hinsichtlich der Unterbringung in eigenen Räumen oder bei einem Dienstleister ist schriftlich festzuhalten.

In M 2.351 *Planung von Speicherlösungen* wird eine Reihe wichtiger Aspekte bezüglich der erforderlichen Infrastruktur für die einzusetzende Speicherlösung dargestellt. Für die Planung des Betriebs der Speicherlösung ist die Einhaltung dieser Vorgaben zu prüfen, und die Informationen hinsichtlich des gewählten Aufstellungsortes der Speicherlösung und möglicher Besonderheiten sind gegebenenfalls zu ergänzen.

Es ist sicherzustellen, dass die dokumentierten Maßnahmen zur Aufstellung der Speicherlösung nicht im Widerspruch zu M 1.59 *Geeignete Aufstellung von Speicher- und Archivsystemen* stehen.

### Erstellung und Pflege eines Betriebshandbuchs

Es ist ein Betriebshandbuch zu erstellen und zu pflegen, das alle relevanten Informationen im Zusammenhang mit dem Betrieb der Speicherlösung beinhaltet. Neben einem Überblick hinsichtlich Architektur und Schnittstellen der Speicherlösung sollte das Betriebshandbuch Aufschluss über die notwendigen administrativen Schritte zur Installation und zur Aufnahme des tatsächlichen Betriebs enthalten. Darüber hinaus ist die Betriebsdokumentation im

Rahmen dieser Maßnahme auf Vollständigkeit der Vorgaben zum laufenden Betrieb, zur Unterbrechung des Betriebs, zur Überwachung der Speicherlösung und hinsichtlich der Archivierung und Löschung von Daten zu prüfen. Fehlende oder fehlerhafte Angaben sind zu ergänzen bzw. zu korrigieren.

Es ist festzuschreiben, dass die Administratoren zur Einhaltung der Vorgaben des Betriebshandbuchs verpflichtet sind und Abweichungen gesonderter Regelungen bedürfen. Das Betriebshandbuch ist regelmäßig, mindestens einmal im Jahr zu aktualisieren,

In den Hilfsmitteln des IT-Grundschutzes findet sich ein Dokument, in dem eine Mustergliederung zur Erstellung eines Betriebshandbuchs für eine Speicherlösung dargestellt ist.

**Abgrenzung bzw. Definition der Verantwortungsbereiche**

In Abhängigkeit vom gewählten Betreiberkonzept sind weitergehende Angaben zu erfolgten Abgrenzungen hinsichtlich des Leistungs- bzw. Funktionsumfangs der Speicherlösung schriftlich festzuhalten.

Darüber hinaus sind alle benötigten Verantwortungsbereiche zu definieren. So sind beispielsweise Aussagen darüber zu treffen, wer im Fall einer Störung des Betriebs verantwortlich ist, wie die Alarmierungskette aussieht und welche Reaktionszeiten in einem solchen Fall festgelegt sind. Die Kontaktdaten der Ansprechpartner müssen den zuständigen Administratoren bekannt und zugänglich gemacht werden. Sie sollten in einem deutlich kürzeren Intervall als einmal im Jahr aktualisiert werden.

Weitere Angaben hierzu finden sich auch in M 2.356 *Vertragsgestaltung mit Dienstleistern für Speicherlösungen* sowie in M 6.98 *Notfallvorsorge und Notfallreaktion für Speicherlösungen*. Es ist sicherzustellen, dass die dokumentierten Abgrenzungen und definierten Verantwortungsbereiche nicht widersprüchlich sind.

**Umsetzung der Mandantenfähigkeit des Betriebs**

Maßnahme M 2.528 *Planung der sicheren Trennung von Mandanten in Speicherlösungen* beschreibt die vorhandenen Möglichkeiten zur Umsetzung der Mandantenfähigkeit in Speicherlösungen.

Es ist sicherzustellen, dass im Rahmen der Planung des Betriebs der Speicherlösung dokumentiert wird, welche konkreten organisatorischen oder technischen Maßnahmen die Institution zur Trennung unterschiedlicher Mandanten ergreift. Dabei ist darzustellen, ob die Mandantentrennung allein auf Netzebene oder zusätzlich durch den Einsatz produktspezifischer Funktionen wie beispielsweise mittels virtueller Fileserver (auch unter diversen Herstellerbezeichnungen wie vFiler, virtuelle Datamover etc. bekannt) umgesetzt wird.

Darüber hinaus wird eine Übersicht aller erfassten Rollen und der zugehörigen Rechte benötigt. Diese Übersicht sollte regelmäßig auf ihre Aktualität überprüft werden.

**Integration der Speicherlösung in die vorhandene Umgebung**

Es ist zu dokumentieren, wie die geplante Speicherlösung für den Betrieb in die vorhandene Umgebung integriert werden soll. Dazu sollte die Institution zunächst alle benötigten Schnittstellen erfassen und entsprechend darstellen. Daneben sind Vorgaben zur notwendigen Erweiterung bzw. zum Austausch bestehender Komponenten und zur Anpassung bestehender Prozesse darzu-

stellen. Während der Planung des Betriebs der Speicherlösung sind veränderte Anforderungen und Aufgaben für die Mitarbeiter zu identifizieren und den Verantwortlichen frühzeitig mitzuteilen. Im Rahmen der erforderlichen Maßnahmen sind insbesondere die Vorgaben aus M 3.54 *Schulung der Administratoren des Speichersystems* zu beachten.

**Umgang mit Tests und Freigabe der Teile der Speicherlösung**

Es sind Vorgaben zur Durchführung von Tests sowie zur Freigabe von Komponenten der Speicherlösung und Steuerungssoftware zu machen und schriftlich festzuhalten.

Dabei sind Regelungen hinsichtlich benötigter Wartungsfenster und bestehender vertraglicher Vereinbarungen zu beachten. Es ist festzulegen, unter welchen Bedingungen der Einsatz einer Testumgebung verpflichtend ist und welche Voraussetzungen für die Freigabe eines Systems erfüllt sein müssen.

Wird die Speicherlösung durch einen externen Dienstleister betrieben, sind daneben die Vorgaben aus M 2.356 *Vertragsgestaltung mit Dienstleistern für Speicherlösungen* zu beachten.

**Einsatz von Verschlüsselung**

Für den Betrieb ist zu regeln, welche Aufgaben die Administratoren der Speicherlösung beim Einsatz von Verschlüsselung haben. Hierzu gehören z. B. die Verwaltung der Schlüssel, die Durchführung von Datensicherungen und insbesondere auch die Wiederherstellung verschlüsselter Daten.

Bei Verschlüsselung der Informationen sind der Baustein B 1.7 *Kryptokonzept* sowie die Maßnahme M 4.448 *Einsatz von Verschlüsselung für Speicherlösungen* zu beachten.

Prüffragen:

- Sind alle erforderlichen Regelungen, Anforderungen und Einstellungen zum Betrieb der Speicherlösung dokumentiert?
- Wann wurde die Betriebsdokumentation für die Speicherlösung das letzte Mal aktualisiert?
- Sind die Auswahl und Festlegung des Betreibermodells sowie die zugehörigen Entscheidungskriterien nachvollziehbar dokumentiert?

# M 2.527 Sicheres Löschen in SAN-Umgebungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Werden die in einer Speicherlösung erfassten Daten nicht länger benötigt, müssen diese gelöscht werden. Institutionen finden im Baustein B 1.15 *Löschen und Vernichten von Daten* bereits eine Vielzahl relevanter Maßnahmen zum sicheren Löschen von Daten. Insbesondere M 2.431 *Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen* geht auf die Problematik der selektiven Datenlöschung ein, die auch in modernen Speicherlösungen von Bedeutung ist.

Das sichere Löschen von Daten in SAN-Umgebungen stellt insbesondere bei der Nutzung durch unterschiedliche Mandanten, wie sie beispielsweise bei Cloud-Storage anzutreffen ist, eine besondere Herausforderung dar. Daher ist hier die Umsetzung zusätzlicher Maßnahmen zu empfehlen.

Verfahren zum sicheren Löschen in SAN-Umgebungen müssen bei der Planung von Notfalltests und -übungen von Speicherlösungen (siehe auch Maßnahme M 6.98 *Notfallvorsorge und Notfallreaktion für Speicherlösungen*) beachtet werden. Bei solchen Tests und Übungen werden in kurzer Zeit große Datenmengen in vielen LUNs mit gegebenenfalls unterschiedlichem Schutzbedarf erzeugt, die nach Abschluss des Tests wieder gelöscht werden müssen. Vergleichbares gilt, wenn bei einem Desaster-Fall LUNs kopiert wurden und nach der Bewältigung des Desasters mehrfach vorliegen.

Grundsätzlich bestehen folgende Möglichkeiten zur Löschung von Daten in SAN-Umgebungen:

- Löschen einer logischen Festplatte in einem Speichersystem (LUN):
  Beim Löschen einer LUN werden die logischen Strukturen auf den zugehörigen Festplatten, RAID-Gruppen oder Festplattenpools aufgebrochen, somit wird die Kapazität der gelöschten LUN wieder freigegeben. Es werden keine physischen Blöcke "genullt", also mit "Pattern" überschrieben. Der Zugriff auf die Daten einer LUN aus Anwendungssicht ist in der Folge nicht mehr möglich, da eine gelöschte LUN mit den Bordmitteln eines Speichersystems nicht wiederhergestellt werden kann. Nach dem Löschen der LUN ist nicht mehr nachvollziehbar, welche Sektoren einer Speichereinheit bzw. Festplatte der LUN in welcher Form zugeordnet waren, sodass Angreifer lediglich Zugriff auf Bit- oder Byteebene erhalten können, nicht aber auf zusammenhängende Datensätze. Das Wiederherstellen der Daten einer LUN ist extrem aufwendig und benötigt physischen Zugang zu den Speichermedien. Unter Umständen können Angreifer hierfür spezielle forensische Werkzeuge einsetzen, mit deren Hilfe die logische Struktur durchbrochen werden kann.
- Mehrfaches Überschreiben der Daten einer LUN:
  Ausgehend vom zugeordneten Server werden die Daten einer LUN (mehrfach) mit festgelegten Daten oder "random Pattern" überschrieben. Je nach Anforderung zur Datenlöschung einer Institution ist ein zertifiziertes Löschen nach US-Standard DoD 5220-22.M möglich. Institutionen können sich hierzu am Markt erhältlicher Software bedienen. Daneben kann die Durchführung einer zertifizierten Löschung häufig in Form eines Services durch den Hersteller der Speicherlösung beauftragt werden. Die auf diese Weise überschriebenen Daten lassen sich im Anschluss nicht mehr wie-

derherstellen. Es gilt jedoch zu beachten, dass die zertifizierte Datenlöschung auf LUN-Basis nur serverseitig sichergestellt werden kann, da die Speichersysteme an sich diese Möglichkeit nicht bieten. Beim Löschen von Daten auf diese Weise entsteht eine erhöhte Schreibaktivität in einem Teil der Speicherlösung, die auch von anderen Mandanten genutzt werden kann. Es ist beim Löschen darauf zu achten, dass dadurch keine Daten anderer Mandanten beeinträchtigt werden und die vorgesehene Dienstgüte den anderen Mandanten weiterhin zur Verfügung steht. Ferner sollte beachtet werden, dass in SAN-Umgebungen dieses Verfahren nicht unbedingt funktioniert, wenn beispielsweise verschiedene Platten für unterschiedliche Aktivitätsmodi bereitstehen. Liegt eine LUN beispielsweise in dem Bereich, der für wenig Schreibaktivitäten vorgesehen ist, und wird dann durch mehrfaches Überschreiben eine hohe Aktivität erzeugt, kopieren solche SANs diese LUN in den Bereich für hohe Schreibaktivität. Dann wird nur diese neue LUN überschrieben, aber die Daten in dem Bereich für geringere Schreibaktivität bleiben unüberschrieben.

- Löschen von Daten eines Speichersystems:
  Sollen die gesamten Daten eines Speichersystems mithilfe eines zertifizierten Verfahrens durch Überschreiben gelöscht werden, bieten Hersteller von Speicherlösungen dies häufig als Service an.
- Disk Retention:
  Wird im Wartungsvertrag mit dem Hersteller "Disk-Retention" vereinbart, verbleiben defekte Festplatten im Fehlerfall in der Institution und werden nicht an den Hersteller übergeben. Die Verantwortung für die sichere Löschung der Inhalte der Festplatten obliegt in der Folge der Institution. In der Regel werden die defekten Festplatten durch die Institution physisch zerstört. Disk Retention ist oft mit höheren Kosten verbunden, sollte aber auch schon bei normalem Schutzbedarf bezüglich Vertraulichkeit geprüft werden.

Die dargestellten Verfahren zum Löschen von Daten in einem Speichersystem sind vielschichtig und komplex. Den Verantwortlichen einer Institution sollte daher bewusst sein, dass dem sicheren Löschen von Daten ein besonderes Augenmerk gewidmet werden muss.

Aufgrund der Funktionsweise moderner SAN-Umgebungen ist die Wiederherstellung von Daten jedoch mit einem extrem hohen Aufwand verbunden, sodass derzeit bei normalem Schutzbedarf das Löschen einer LUN als ausreichend sicher angesehen wird.

Das Überschreiben einer LUN unter Einbeziehung aller möglichen zugehörigen Speichersegmente sollte bei einem erhöhten Schutzbedarf hinsichtlich der Vertraulichkeit geprüft werden.

Wird eine Speicherlösung außer Betrieb genommen, so sind die Inhalte der Maßnahme M 2.361 *Außerbetriebnahme von Speicherlösungen* umzusetzen.

Prüffragen:

- Ist für das Speichersystem festgelegt, welche Informationen mit welchen Verfahren zu löschen sind?
- Ist in mandantenfähigen Speicherlösungen die Löschung der LUNs sichergestellt, die einem bestimmten Mandanten zugeordnet sind?
- Werden bei der Löschung von Daten mit hohem Schutzbedarf die zugehörigen Speichersegmente einer LUN mehrfach überschrieben?

# M 2.528 Planung der sicheren Trennung von Mandanten in Speicherlösungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Für viele Institutionen ist Mandantenfähigkeit eine wesentliche funktionale Eigenschaft von Speicherlösungen. Sofern die Anforderung zur Trennung von Mandanten in Speicherlösungen vorhanden ist, sollten Institutionen daher Maßnahmen ergreifen, um diese sicher zu gestalten.

Im Hinblick auf die Planung eines Speichersystems ist grundsätzlich zu hinterfragen, in welcher Form und in welchem Umfang die Mandantenfähigkeit (multi-tenancy) bei Einsatz dieser Lösung bereits durch den Hersteller umgesetzt ist. Viele Anbieter von Speicherlösungen werben damit, dass die von ihnen angebotenen Produkte mandantenfähig sind. Nicht immer versteht ein Anbieter dabei allerdings unter Mandantenfähigkeit jene Funktionalität, die den Anforderungen der Institution entspricht.

Die Realisierung von Speicherlösungen, wie sie in typischen Serviceprovider-Umgebungen anzutreffen sind, bedingt beispielsweise, dass die Daten unterschiedlicher Anwender über die Applikationsisolation hinaus sicher voneinander getrennt sind.

Es ist daher darauf zu achten, dass die Hersteller bei der technischen Realisierung der von ihnen angebotenen Mandantenfähigkeit zumindest eine der nachfolgend beschriebenen Varianten zur Verfügung stellen.

- Im **Block-Storage-Umfeld** muss die Trennung von Mandanten mithilfe des LUN Maskings sichergestellt werden können. Die Managementkomponente der Speicherlösung sollte entsprechende Konfigurationsmöglichkeiten zur Verfügung stellen.
- In **Fileservice-Umgebungen** sollte die Möglichkeit bestehen, mit virtuellen Fileservern (auch unter diversen Herstellerbezeichnungen wie vFiler, virtuelle Datamover etc. bekannt) zu agieren. Diese bieten die Möglichkeit, jedem Mandanten einen eigenen Fileservice zuzuordnen. Virtuelle Fileserver bieten die Möglichkeit, als gekapselte Umgebung administriert zu werden. Für den Einsatz in hochverfügbaren Umgebungen können virtuelle Fileserver in dieser Form mit all ihren Eigenschaften von einem Rechenzentrum ins andere gespiegelt werden. So kann die sichere Trennung von Mandanten auch nach dem Ausfall einer Speicherlösung oder einzelner Komponenten aufrechterhalten werden.
- **Bei höherem Schutzbedarf** sollte die Möglichkeit bestehen, Mandanten, also internen oder externen Anwendern, Speicherressourcen aus unterschiedlichen sogenannten Speicher-Pools zur Verfügung zu stellen. Dazu werden verschiedene, physisch voneinander getrennte, Speichermedien zu einem Speicher-Pool zusammengefasst. Ein Speichermedium darf dabei immer nur einem einzigen Pool zugewiesen werden. Die logischen Festplatten (LUNs), die aus einem solchen Pool generiert werden, dürfen in der Folge nur einem einzigen Mandanten zugeordnet werden. Der Zugriff eines Mandanten auf die Speichermedien eines anderen Mandanten ist damit nicht möglich.

Neben der Umsetzung der Mandantentrennung über Funktionen, die direkt durch die Speicherlösung zur Verfügung gestellt werden, besteht auch die Möglichkeit, die sichere Trennung von Mandanten über Maßnahmen auf Net-

zebene vorzunehmen. Beim Einsatz von IP, iSCSI und FC-SAN kann die technische Trennung von Mandanten über eine Segmentierung im Netz vorgenommen werden.

- Im IP- und iSCSI-Umfeld kann dies durch physisch getrennte Netze oder auch durch die Einführung von VLANs sichergestellt werden. Weitere Informationen hierzu finden sich in M 5.77 *Bildung von Teilnetzen* und M 5.62 *Geeignete logische Segmentierung*.
- Im FC-Umfeld kommt meist nur ein zentrales redundantes Netz zum Einsatz. Nur in Ausnahmefällen wird hier eine physische Trennung der Netze realisiert. Die Separierung wird in Regel unter Zuhilfenahme von VSANs und Soft Zoning sichergestellt. Hard Zoning kommt üblicherweise heute eher selten zum Einsatz, da die höhere Sicherheit, durch die feste Zuordnung von Speichermedien an ein bestimmtes Netz, die in SAN-Umgebungen benötigte Flexibilität einschränkt. Weitere Informationen hierzu können M 5.130 *Absicherung des SANs durch Segmentierung* und M 4.447 *Sicherstellung der Integrität der SAN-Fabric* entnommen werden.
- Zusätzliche Maßnahmen bei hohem Schutzbedarf:
  Besteht hoher Schutzbedarf, insbesondere hinsichtlich der Vertraulichkeit, ist zu empfehlen, die Einführung von Verschlüsselung und ein entsprechendes Schlüsselmanagement zu prüfen. Verschlüsselung kann dabei auf unterschiedlichen Ebenen eingeführt werden. Nähere Angaben hierzu finden sich unter anderem in M 4.448 *Einsatz von Verschlüsselung für Speicherlösungen*.

Prüffragen:

- Sind die Anforderungen an die Mandantentrennung nachvollziehbar dokumentiert?
- Erfüllen die eingesetzten Methoden zur Mandantentrennung die dokumentierten Anforderungen?
- Wird im Block-Storage-Umfeld LUN Masking zur Mandantentrennung eingesetzt?
- Wird beim Einsatz von virtuellen Fileservern jedem Mandanten ein eigener Fileservice zugeordnet?
- Wird beim Einsatz von IP, iSCSI und FC-SAN eine Trennung der Mandanten über eine Segmentierung im Netz vorgenommen?

# M 2.529 Modellierung von Speicherlösungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Um eine angemessene Gesamtsicherheit für den IT-Betrieb zu erreichen, muss die gesamte Speicherlösung mit allen Speichersystemen systematisch im Sicherheitskonzept der Institution berücksichtigt werden. In Bezug auf die IT-Grundschutz-Vorgehensweise bedeutet dies insbesondere, dass alle Speicherlösungen in die Strukturanalyse und in die Modellierung einbezogen werden müssen.

Als Modellierung wird in der IT-Grundschutz-Vorgehensweise die Zuordnung von Bausteinen zu den vorhandenen Zielobjekten (IT-Systeme, Anwendungen, Räume etc.) bezeichnet. Grundsätzlich sind zur Modellierung von Speicherlösungen die Hinweise in Kapitel 2.2 der IT-Grundschutz-Kataloge zu beachten. Die Zuordnung der IT-Grundschutz-Bausteine richtet sich in erster Linie nach der Funktion des IT-Systems (Server, Client etc.), nach dem verwendeten Betriebssystem (Unix, Windows etc.) und nach den darauf betriebenen Applikationen (Datenbank, Webserver etc.).

Aufgrund der teils hohen Komplexität moderner Speicherlösungen finden sich in der Folge einige zusätzliche Modellierungshinweise, die auf konkrete Umsetzungsvarianten eingehen.

**Modellierung eines Network Attached Storage (NAS)**

Network-Attached-Storage-Systeme ermöglichen über die Protokolle NFS (Network File System) oder CIFS (Common Internet File System) Zugriffe auf die Speichersysteme. Der Hauptanwendungsfall eines NASs besteht darin, Fileserverdienste zur Verfügung zu stellen. Viele Anbieter verwenden deshalb den Begriff "Filer" für solche Systeme.

Für NAS-Lösungen ist daher auch zusätzlich der Baustein B 3.101 *Allgemeiner Server* anzuwenden.

**Modellierung eines Storage Area Network (SAN)**

Storage Area Networks (SAN) werden in der Regel durch ein dediziertes Speichernetz zwischen Speichersystemen und angeschlossenen Servern oder Endgeräten geschaffen. SANs wurden für die serielle, sehr schnelle und kontinuierliche Übertragung großer Datenmengen konzipiert. Sie basieren heute für hochverfügbare, hochperformante Installationen auf der Implementierung des Fibre-Channel- oder IP-Protokolls (iSCSI).

Für SAN-Lösungen ist daher auch der Baustein B 4.1 *Lokale Netze* anzuwenden. Auf die Netzkomponenten des SANs (z. B. Fibre-Channel-Switches) ist zusätzlich der Baustein B 3.302 *Router und Switches* anzuwenden.

**Modellierung von Hybrid-Storage- oder Unified-Storage-Lösungen**

Eine Speicherlösung, die eine Mischform zwischen NAS und SAN darstellt, wird oftmals als Hybrid-Storage oder kombinierte Speicherlösung (Unified Storage) bezeichnet. Nach außen können sie jedoch sowohl als NAS als auch als SAN betrieben werden. Dieser Mischbetrieb wird durch den Einsatz entsprechender Systemkomponenten und eine entsprechende Konfiguration ermöglicht. So kann sich ein Speichersystem sowohl für einige Anwendungen per

Ethernet-Anschluss als "Filer" präsentieren und somit Fileservices über CIFS und NFS zur Verfügung stellen als auch für andere Server per Fibre Channel oder iSCSI Speicherkapazität zugänglich machen.

Für die Mischform zwischen NAS und SAN sind daher die Bausteine B 3.101 *Allgemeiner Server* und B 4.1 *Lokale Netze* anzuwenden. Auf die Netzkomponenten des SAN (z. B. Fibre-Channel-Switches) ist zusätzlich der Baustein B 3.302 *Router und Switches* anzuwenden.

**Modellierung von Speichervirtualisierung**

Mit dem Einsatz von Speichervirtualisierung wird dem Speichernetz eine neue virtuelle Schicht hinzugefügt, die die Speicherbereitstellung von den physischen Gegebenheiten abkoppelt. Die Grundlage einer Speichervirtualisierung stellt die Virtualisierungs-Appliance dar. Sie ermöglicht die zentrale Verwaltung aller Speicherbereiche.

Auf die Komponenten der Speichervirtualisierungslösung sind zusätzlich die Bausteine B 3.101 *Allgemeiner Server* und B 3.304 *Virtualisierung* anzuwenden.

**Modellierung von Objekt-Storage**

Objekt-Storage (oftmals auch als "Object-based Storage" bezeichnet) ermöglicht gegenüber den traditionellen blockbasierten und filebasierten Zugriffsmethoden einen objektbasierten Zugriff.

Objektbasierende Speicherlösungen speichern Daten in Verbindung mit den zugehörigen Metadaten auf einem Speichersystem in Form von Objekten und nicht in Form von Dateien. Mittels der Vergabe einer eindeutigen Objekt-ID (Hash-Wert), die in den Metadaten des Objekts festgehalten wird, kann das Objekt eindeutig identifiziert werden. Der Zugriff auf einen objektbasierten Speicher erfolgt über eine führende Anwendung. Die Anwendung greift hierbei über eine spezielle API und deren mögliche Kommandos oder direkt per IP auf den Objekt-Storage zu. Im Falle eines Zugriffs per API muss die führende Applikation die herstellerspezifische API des Objekt-Storage unterstützen. Objekt-Storage wird typischerweise vor allem im Bereich Archivierung, Dokumentenmanagement und beim Ablegen von Objekten in einer Cloud eingesetzt.

Für objektbasierte Speicherlösungen sind daher auch zusätzlich die Bausteine B 3.101 *Allgemeiner Server* und B 5.24 *Web-Services* anzuwenden.

**Modellierung von Cloud-Storage**

Im Zusammenhang mit Weiterentwicklungen im Speicherumfeld etabliert sich zunehmend auch der Begriff des Cloud Storage. Hierunter wird Speicher für die Cloud-Nutzung verstanden. Die Speicherlösung an sich bleibt dabei weitgehend unverändert, jedoch liegt eine von den klassischen SAN- oder NAS-Architekturen abweichende Art des Zugriffs auf die gespeicherten Daten vor. Dieser wird in der Regel mittels Web-Services realisiert.

Eine besondere Herausforderung im Zusammenhang mit Cloud-Storage ist die Mandantenfähigkeit der Gesamtlösung.

Aus Anwendersicht sind daher zusätzlich die Bausteine B 1.17 *Cloud-Nutzung* und B 5.24 *Web-Services* (gegebenenfalls zusammen mit B 5.21 *Webanwendungen*) zu betrachten.

Aus Betreibersicht ist zusätzlich der Baustein B 5.23 *Cloud Management* relevant. Während die Funktionsweise und die relevanten Sicherheitsaspekte des Storage-Element-Managers im Baustein B 3.303 *Speicherlösungen / Cloud Storage* betrachtet werden, behandelt der Baustein B 5.23 *Cloud Management* die Gesamt-Orchestrierung der Cloud. Da die reibungslose Kommunikation mit dem "Cloud Orchestrator" durch den Storage-Element-Manager sichergestellt wird, entsteht hier die Schnittstelle zum Baustein B 5.23 *Cloud Management*.

**Weitere Hinweise zur Modellierung von Speicherlösungen**

Neben den bereits erwähnten Bausteinen sind in Abhängigkeit von der Ausgestaltung der Speicherlösung zusätzlich folgende Hinweise zu beachten:

**Datensicherung**

Für Datensicherungsgeräte, die an das Speichersystem angeschlossen sind, ist der Baustein B 1.12 *Archivierung* zu betrachten. Konzeptionelle Aspekte der Datensicherung werden im Baustein B 1.4 *Datensicherungskonzept* erläutert.

**Management von Speicherlösungen**

Die Element-Manager von Speicherlösungen oder deren Komponenten stellen in der Regel das zentrale Verwaltungswerkzeug dar, das mithilfe unterschiedlicher Protokolle das Management der Speicherlösung bzw. der zugehörigen Komponenten steuert. Die Funktion und der Aufbau von Element-Managern unterscheidet sich nicht wesentlich von anderen Managementsystemen. Diese lassen sich daher mit den vorhandenen Bausteinen aus den IT-Grundschutz-Katalogen abbilden. Hierzu gehört insbesondere der Baustein B 4.2 *Netz- und Systemmanagement* sowie systemspezifische Bausteine wie z. B. B 3.101 *Allgemeiner Server*, B 3.102 *Server unter Unix*, B 3.108 *Windows Server 2003*, B 5.7 *Datenbanken* und B 5.21 *Webanwendungen*.

**Cloud Storage Gateways**

"Cloud Storage Gateways" sind spezielle Applikationsserver, die eine Umsetzung von Cloud-Protokollen (Simple Object Access Protocol, SOAP und Representational State Transfer, REST) auf Storage basierende Protokolle (block- oder filebasierend) gewährleisten.

Sofern ein Cloud Storage Gateway eingesetzt wird, sollten die Bausteine B 3.301 *Sicherheitsgateway (Firewall)* und B 5.24 *Web-Services* zur Anwendung kommen. Darüber hinaus sind die protokollspezifischen Gefährdungen beim Übergang in SOAP/REST zu berücksichtigen.

Bei der Beschaffung und Implementierung von Cloud Storage Gateways ist darauf zu achten, dass diese nicht auf proprietären Standards basieren, sondern mit gängigen Storageprotokollen umgehen können und sich somit einfach in die bestehende Anwendungsinfrastruktur einbinden lassen. Grundsätzlich sind hier zwei mögliche Ausprägungen zu betrachten:

- Der Betreiber einer Speicherlösung möchte seinen Anwendern den Zugriff mittels SOAP bzw. REST ermöglichen, wobei die Schnittstelle der Speicherlösung diese Zugriffsmöglichkeit zur Verfügung stellt.
- Der Anwender möchte eine Cloud-Storage-Lösung verwenden, die lediglich SOAP bzw. REST als Zugriffsprotokoll verwendet. Da die Systeme des Anwenders jedoch NFS, FC oder iSCSI erwarten, kommt ein Cloud

Storage Gateway zum Einsatz, mit dessen Hilfe die Protokollumsetzung erfolgt.

Sofern Cloud Storage Gateways über Zusatzfunktionen wie Backup-Lösungen oder Verschlüsselung verfügen, sind weiterhin die erforderlichen Bausteine anzuwenden.

# M 2.530 Planung und Vorbereitung von Migrationen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Migrationen von IT-Infrastrukturen sind in der Regel sehr komplexe Vorhaben mit einer großen Anzahl von Einflussfaktoren und möglichen Fehlerquellen. Migrationen verlaufen in aller Regel nur dann erfolgreich, wenn sie im Vorfeld sorgfältig geplant und vorbereitet werden.

Um nicht an der Komplexität des Themas zu scheitern, empfiehlt sich die Wahl eines bewährten Vorgehensmodells. In der Praxis haben sich weder reine Top-Down-Ansätze mit einmaliger Komplettumstellung noch ein reines punktuell aus den Fachabteilungen getriebenes Bottom-Up-Vorgehen bewährt. Zielführend ist der Mittelweg einer iterativen, priorisierten wechselseitigen Abstimmung der Geschäftsprozesse und IT-Modelle aus den Fachabteilungen und aus den Geschäftsanforderungen heraus. Reifegradmodelle können helfen, den jeweils nächsten Entwicklungsschritt einer Iteration zu planen.

Nachdem die im nächsten Migrationsschritt zu erreichenden Ziele festgelegt und die zu migrierenden Dienste identifiziert sind, werden im Planungsschritt die Anforderungen an die IT aus den Geschäftszielen (einschließlich der Sicherheitsanforderungen) abgeleitet. Die Phase der Migration umfasst die technische Umsetzung dieser Anforderungen in Form von Anwendungen und Systemen, die anschließend in den Betrieb überführt werden. Dieser Zyklus wird wiederholt, bis der gewünschte Reifegrad erreicht ist. In jeder Iteration ist dabei zu prüfen, welche Anpassungen an (Alt-)Anwendungen und Schnittstellen vorgenommen werden müssen.

Stehen der zeitliche Rahmen und Umfang der Migration fest, ist die notwendige technische Infrastruktur zu planen. Hier sind insbesondere Fragen der Dimensionierung wichtig, denn Web-Service-Umgebungen unterscheiden sich hinsichtlich der benötigten Ressourcenparameter im Allgemeinen deutlich von den bestehenden Umgebungen. Sinnvollerweise werden Lasttests durchgeführt, mindestens aber Fachverstand in Bezug auf die Ressourcenausstattung herangezogen.

Die Migrationsplanung hat zu berücksichtigen, welche Systeme und Anwendungen wann migriert werden, ob Ausfallzeiten nötig und vertretbar sind. Für unerwartete Komplikationen müssen Abbruchkriterien und Rückfallszenarien definiert werden, mit denen sich die Umgebung in einen betriebsfähigen Zustand zurücksetzen lässt.

Besonders zu Berücksichtigen bei der Planung sind die dadurch entstehenden Abhängigkeiten von Anbietern und Standards. Letztere sind sorgfältig auszuwählen und sollten in ihrer Weiterentwicklung und auch auf möglicherweise bekannt werdende Sicherheitslücken in den Standards selbst beobachtet werden.

Wenn besondere Systeme zum Einsatz kommen sollen, die bisher nicht benötigt wurden - etwa eine XML-Firewall als Application Level Gateway -, so sind diese vorher ausführlich im Hinblick auf die erforderliche Funktionalität zu testen und in das Sicherheitskonzept mit aufzunehmen.

In dem Maße, wie eine Migration die Chance bietet, zukünftig zentrale Dienste wie Identitätsmanagement oder eine PKI standardisiert nutzbar zu machen,

müssen auch diese Dienste betrachtet und zusätzlich abgesichert werden. Insbesondere wenn ein Single Sign-On geplant wird, sind die Implikationen auf die Sicherheit genauestens zu prüfen, siehe auch M 4.456 *Authentisierung bei Web-Services*, M 4.455 *Autorisierung bei Web-Services* und M 4.453 *Einsatz eines Security Token Service (STS)*.

Die spezifischen Risiken, die sich durch eine Migration ergeben, beziehen sich zum einen auf die damit verbundenen Änderungen der Architektur. Die für die Zielarchitektur erforderlichen Sicherheitsmaßnahmen sind daher (anhand der einschlägigen Bausteine oder einer ergänzenden Sicherheitsanalyse und gegebenenfalls zusätzlichen Risikoanalyse) vorab zu identifizieren und zu berücksichtigen. Beachtet werden muss auch, dass durch die Migration Abhängigkeiten entstehen können, die die Anforderungen an die Verfügbarkeit deutlich erhöhen können. Zum anderen birgt auch die Migration selbst Risiken, da diese sowohl mit hohen Kosten als auch mit einer langen Projektlaufzeit einhergehen kann. Beide Klassen von Risiken sind im Zuge der Migrationsplanung zu analysieren und dokumentieren.

Für eine umfangreiche Migration oder eine tief greifende Umstellung der Architektur ist es zudem dringend anzuraten, ein eigenes Sicherheitskonzept zu erarbeiten und das Ergebnis der Migration im vorhandenen Sicherheitskonzept zu behandeln.

Dies trifft insbesondere dann zu, wenn eine Migration auf einen zentralen Servicebus (meist *ESB, Enterprise Service Bus*) vollzogen wird. Dieser stellt einen möglichen zentralen Ausfallpunkt dar und sollte daher angemessen in der Notfallplanung berücksichtigt sein, falls es Anforderungen in Bezug auf die Verfügbarkeit der SOA gibt.

Nicht zu vernachlässigen ist auch die Frage des Wissenstransfers: Durch die tief greifende Umstellung der Architektur wird von den Administratoren, letztlich aber auch von den Fachverantwortlichen ein Umdenken verlangt, das bereits in der Planungsphase mit entsprechenden Zeitaufwänden und Schulungen zu berücksichtigen ist.

Eine Migration stellt immer ein langfristiges und strategisches Programm dar, das, um Erfolg zu haben, von der Leitungsebene getragen und gesteuert werden und von den Beteiligten über die komplette Laufzeit mit Leben gefüllt werden muss.

Prüffragen:

- Wurde ein geeignetes Vorgehensmodell für die Migration gewählt?
- Wurden die zu migrierenden Dienste identifiziert und deren Anforderungen, einschließlich der Sicherheitsanforderungen, erhoben und dokumentiert?
- Wurde die notwendige Auslegung der Infrastruktur und der Systeme durch Expertise oder realistische Lasttests bestimmt?
- Wurden notwendige Ausfallzeiten ermittelt, geplant und abgestimmt?
- Ist ein Rückfall-Szenario vorbereitet, und sind Abbruchkriterien für die Migration definiert?
- Sind die spezifischen Risiken der Migration analysiert und dokumentiert?
- Ist ein Wissenstransfer an das Betriebspersonal und die Fachverantwortlichen gesichert?
- Wird die Migrationsstrategie von der Leitungsebene getragen und die Migration von ihr gesteuert?

# M 2.531 Erarbeitung einer Sicherheitsrichtlinie für Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Um ein angemessenes Sicherheitsniveau für einen Web-Service zu gewährleisten, muss entschieden werden, wie die erforderlichen Sicherheitsfunktionen konkret realisiert werden, und wer dafür verantwortlich ist. Um die Revisionsfähigkeit zu gewährleisten, müssen solche Entscheidungen nachvollziehbar dokumentiert sein. Diese Dokumentation erfolgt am besten in einer Sicherheitsrichtlinie, die sich in das Sicherheitsregelwerk der Institution einfügt (siehe auch M 2.338 *Erstellung von zielgruppengerechten Sicherheitsrichtlinien*).

Die Sicherheitsrichtlinie sollte Regelungen zu den folgenden Themen umfassen. Sofern Themenbereiche bereits in anderen Dokumenten verbindlich vorgegeben sind, genügt ein entsprechender Verweis.

**Architektur und Plattformen**

**Übergreifende Aussagen zur Rolle von Web-Services im Rahmen der IT-Strategie**

**Festlegung der eingesetzten (service-orientierten) Architektur**

**Beschreibung der Komponenten der Architektur:**
- Beteiligte Systeme
- Beteiligte Softwarekomponenten
- Einsatz von Verzeichnissen (Registries und Repositories)
- Einsatz eines Enterprise Service Bus
- Einsatz von Sicherheitskomponenten (XML-Firewalls, Protokollserver und ähnliches), Einbeziehung von Sicherheits-Diensten Dritter
- Einsatz von Identitäts-Diensten und Authentisierungs- oder Autorisierungsdiensten

**Festlegung der eingesetzten**
- Produkte,
- Programmiersprachen und Ablaufumgebungen,
- XML-Schemata,
- Standards und
- Protokolle.

**Sicherheitsanforderungen an Web-Services**

**Einsatzzweck von Web-Services in der Institution**
- resultierende Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität
- gegebenenfalls Definition von verschiedenen Sicherheitsklassen je nach Schutzbedarf
- Berücksichtigung der Sicherheitsanforderungen Dritter (zum Beispiel externer Consumer des Web-Service, siehe M 2.532 *Anbieten von Web-Services für Dritte*)

**Ableitung von konkreten Anforderungen und Ausarbeitung von Vorgaben für**

- die Authentisierung (Authentisierungsverfahren, Einbindung Dritter, Föderation),
- die Autorisierung,
- die Datenhaltung und -integrität,
- die Realisierung von Schnittstellen (Anbindung von Backend-Systemen, Einsatz eines Enterprise Service Bus, eingesetzte Protokolle)
- die Verschlüsselung der Kommunikation/der XML-Nachrichten und der Datenhaltung
- die Integritätssicherung der Kommunikation/der XML-Nachrichten und der Daten,
- das Schlüssel- und Zertifikatsmanagement (Anbindung an PKI, Nutzung von Zertifikaten Dritter, Sicherung der kryptographischen Schlüssel)
- die Orchestrierung und Choreographie der Web-Services zur Erfüllung übergreifender Geschäftsfunktionen,
- die Datensicherung,
- die Skalierbarkeit,
- die Ausfallsicherheit,
- die Protokollierung und
- die Dokumentation.

**Management von Web-Services**

- Entwicklungsvorgaben,
- Test- und Freigabeverfahren,
- Lebenszyklus-Management,
- Klare Festlegung von Verantwortlichen für jeden Web-Service und jedes beteiligte System, klare Abgrenzung bei einer Verteilung der Verantwortung auf mehrere Bereiche oder Personen (zum Beispiel Entwicklung und Betrieb, Plattform und Web-Service),
- Umsetzung des Benutzer- und Rechtemanagements (Abläufe, Zuständigkeiten, Dokumentation)
- Schulung und Weiterbildung des eingesetzten Personals (Entwickler, Administratoren) einschließlich Sensibilisierungsmaßnahmen für die Sicherheit
- Auswertung sicherheitsrelevanter Ereignisse
- Durchführung von regelmäßigen Audits
- Notfallplanung für Web-Services (siehe auch M 6.154 *Notfallmanagement für Web-Services*).

Die Sicherheitsrichtlinie muss mit den beteiligten Stellen in der Institution abgestimmt und von einer dazu autorisierten Stelle offiziell in Kraft gesetzt sein. Die gültige Richtlinie muss allen betroffenen Personen bekannt und leicht zugänglich sein. Durch geeignete Prozesse und Verantwortlichkeiten muss sichergestellt werden, dass die Richtlinie bedarfsgerecht fortgeschrieben und aktualisiert wird.

Die Einhaltung der Vorgaben aus der Richtlinie muss, zum Beispiel im Rahmen von Revisionsprüfungen, regelmäßig überwacht werden.

Prüffragen:

- Sind die in dieser Maßnahme aufgeführten Themenbereiche in einem geeigneten Dokument geregelt?
- Sind die Vorgaben in der Institution verbindlich (Freigabe der Regelungen)?

- Ist die Aktualisierung und Pflege der Regelungen in einem angemessenen Zyklus sichergestellt?
- Wird die Einhaltung der Vorgaben regelmäßig in angemessener Form überprüft?

# M 2.532 Anbieten von Web-Services für Dritte

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Vertrieb, Vertragsmanagement

Web-Services können auf verschiedene Weise bereitgestellt werden. Sie können entweder als fertige Lösung verkauft (Betrieb durch den Consumer selbst) oder als Dienstleistung bereitgestellt werden (Betrieb durch den Anbieter). Beim Betrieb durch einen Anbieter müssen alle relevanten Modalitäten der Zusammenarbeit mit dem Web-Service-Consumer vertraglich geregelt und geeignete Service Level Agreements (SLAs) vereinbart werden, zum Beispiel Ansprechpartner, Reaktionszeiten, Kontrolle über die Daten, Leistungen, Ausgestaltung der Sicherheitsvorkehrungen (siehe hierzu M 2.533 *Vertragliche Aspekte bei der Bereitstellung von Web-Services* ).

Folgende Aspekte sind zu berücksichtigen, wenn Web-Services für Dritte betrieben werden:

**Umgebung**

Die Bereitstellung von Web-Services durch einen Anbieter kann auf einer eigenen IT-Infrastruktur des Anbieters, auf der des Kunden oder sogar eines Dritten erfolgen. Entsprechend ergeben sich unterschiedliche Zuständigkeiten für die Sicherheit der eingesetzten Umgebung, aber auch zum Beispiel für die Durchführung von Datensicherungen und Notfallübungen. Die Verantwortlichkeiten für die Betriebsumgebung, ihre einzelnen Bestandteile und Betriebsprozesse muss zwischen den beteiligten Parteien festgelegt und nachvollziehbar dokumentiert werden.

**Ansprechpartner**

Alle Parteien (Web-Service-Anbieter und -Consumer) müssen Ansprechpartner benennen, mindestens für

- vertragliche Fragen
- inhaltliche/fachliche Fragen
- die Meldung und Behebung von Störungen sowie die Alarmierung im Notfall
- die Kommunikation und Behandlung von Sicherheitsvorfällen
- die Übermittlung beziehungsweise den Empfang der vereinbarten Berichte zu Leistungskennzahlen, sicherheitsrelevanten Ereignissen sowie Änderungen an den Systemen und Diensten.

Für eine mögliche Nichtverfügbarkeit der Ansprechpartner ist eine Vertretung einzuplanen und zu benennen.

**Benutzer- und Rechteverwaltung**

Je nachdem, wer die für die Web-Services erforderlichen Benutzer- und Rechteprofile pflegt, müssen dafür entsprechende Verfahren, Kommunikationsschnittstellen und Dokumentationswege eingerichtet werden. Sowohl die Einrichtung von Benutzern als auch die Pflege von Berechtigungen kann jeweils durch den Anbieter oder durch den Consumer selbst möglich sein. Denkbar sind auch mehrstufige Modelle, in denen der Anbieter Administrationskonten für die Consumer einrichtet, mit denen diese eigenständig die Benutzer innerhalb der eigenen Institution verwalten. In komplexeren Umgebungen können auch Dritte entsprechende Dienste zur Identifizierung, Authentisierung und

Autorisierung von Benutzern anbieten, die zum Beispiel auch wiederum als Web-Service realisiert sein können.

**Wartung und Pflege**

Maßnahmen zur Wartung und Pflege der Systeme, insbesondere zum Einspielen von Patches und Updates für die Web-Services oder zugrunde liegende Komponenten, können Auswirkungen auf die Consumer haben. Dies umfasst beispielsweise Änderungen in der Funktionalität oder kurzfristige Einschränkungen der Verfügbarkeit. Daher müssen Verfahren eingerichtet sein, um solche Wartungsmaßnahmen vorab mit den betroffenen Consumern abzustimmen und zu koordinieren, zum Beispiel durch die Vereinbarung von Wartungsfenstern.

**Berichts- und Meldepflichten**

Der Web-Service-Anbieter muss Abläufe einrichten, um die mit den Consumern vereinbarten Berichts- und Meldepflichten zu erfüllen. Dazu gehören auch Berichtsformate und Übermittlungswege.

**Sicherheitsvorfallsbehandlung**

Der Prozess zur Sicherheitsvorfallsbehandlung muss berücksichtigen, dass zur Aufklärung und Behandlung von Vorfällen auch eine übergreifende Zusammenarbeit zwischen Web-Service-Anbieter und den Web-Service-Consumern erforderlich sein kann. Entsprechend müssen hierfür Schnittstellen, Ansprechpartner, Alarmierungswege und Dokumentationsverfahren eingerichtet werden.

**Notfallplanung**

Auch im Bereich der Notfallplanung ist eine Koordination der Aktivitäten von Web-Service-Anbieter und Web-Service-Consumer erforderlich. So muss sich insbesondere die Notfallplanung des Web-Service-Anbieters an den Anforderungen der Consumer orientieren. Aber auch bei der Umsetzung der Notfallvorsorgemaßnahmen ist eine Abstimmung und Koordination erforderlich, zum Beispiel bei der gemeinsamen Durchführung von Notfallübungen.

Prüffragen:

- Sind die Verantwortlichkeiten für die genutzte Betriebsumgebung geklärt und dokumentiert?
- Sind bei allen Partnern die relevanten Ansprechpartner festgelegt und bekannt?
- Sind Verfahren für die Benutzer- und Rechteverwaltung vorhanden?
- Sind Verfahren für die Wartung, Pflege und Weiterentwicklung der Web-Services und der Betriebsumgebung eingerichtet und mit allen Beteiligten abgestimmt?
- Sind geeignete Abläufe, Formate und Kommunikationswege für das Berichts- und Meldewesen vorhanden?
- Ist das Zusammenwirken von Anbieter und Consumer in den jeweiligen Prozessen zur Sicherheitsvorfallsbehandlung berücksichtigt?
- Sind die Anforderungen der Consumer im Notfallmanagement des Web-Service-Anbieters berücksichtigt, und werden entsprechende Notfallvorsorgemaßnahmen untereinander abgestimmt?

# M 2.533 Vertragliche Aspekte bei der Bereitstellung von Web-Services

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Vertrieb, Vertragsmanagement

Wenn Web-Services für Dritte bereitgestellt werden, sind zwischen Web-Service-Anbieter und Web-Service-Consumer schriftliche Regelungen zu treffen, die die Sicherheit der Dienstnutzung, aber auch die Nachvollziehbarkeit und Ordnungsmäßigkeit der Leistungserbringung gewährleisten.

Die konkrete Ausgestaltung muss sich am Schutzbedarf der Anwendungen und Geschäftsprozesse orientieren, die durch den Web-Service abgebildet werden. Dabei kommt insbesondere der Verfügbarkeit häufig ein besonderer Fokus zu, da der Ausfall eines Web-Service unter Umständen weitere, abhängige Web-Services und Anwendungen betrifft und dadurch einen oder sogar mehrere Geschäftsprozesse beeinträchtigen kann.

Die folgende Liste umfasst Aspekte, die bei der Vertragsgestaltung mit dem Web-Service-Consumer geprüft und gemäß dem jeweiligen Schutzbedarf berücksichtigt werden sollten.

**Generelle vertragliche Gestaltung**

Fachliche Regelungen

- Art und Umfang der Nutzung der Web-Services durch den Consumer, Einsatzzweck
- Fachliche Beratung und Unterstützung der Web-Service-Consumer durch den Web-Service-Anbieter
- Schulungen und Dokumentation
- Kundeninformationen/gesetzliche Änderungen

Technische Leistungsparameter

- Verfügbarkeit (mittlere Verfügbarkeit, Wartungsfenster, maximale Ausfallzeiten)
- Leistungskennzahlen (Transaktionsgeschwindigkeit, Anzahl gleichzeitiger Zugriffe, Bandbreite der Anbindung)
- Datenhaltung (Speicherorte, Verschlüsselung, Datensicherung)

Organisatorische Regelungen

- Festlegung von Kommunikationswegen und Ansprechpartnern
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
- Verfahren zur Behebung von Problemen, Benennung von Ansprechpartnern mit den nötigen Befugnissen
- regelmäßige Abstimmungsrunden
- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses)
- Erfordernis und Ausgestaltung von Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Benutzers zu den Räumlichkeiten und IT-Systemen des Web-Service-Anbieters
- Abrechnungsmodell und Abrechnungsgrundlagen für die Nutzung

**Personal**

- Festlegung und Abstimmung von Vertretungsregelungen

**Notfallvorsorge und Notfallreaktion**
- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit
- Erforderliche Handlungen beim Eintreten eines Störfalls
- Kontakte für die Alarmierung einschließlich Kontaktwegen und Vertretern
- Reaktionszeiten und Eskalationsstufen
- Mitwirkungspflicht des Nutzers bei der Behebung von Notfällen
- Art und zeitliche Abfolge von regelmäßigen und adäquaten Notfallübungen
- Art und Umfang der Datensicherung
- Vereinbarung, ob und welche Systeme redundant ausgelegt sein müssen
- Regelungen bei Schäden durch höhere Gewalt
- Regelungen zur Vertragsbeendigung im Falle einer Insolvenz oder Aufgabe der Geschäftstätigkeit von Web-Service-Anbieter oder -Consumers, inklusive Regelungen zum Umgang mit beim Anbieter gespeicherten Daten.

**Sicherheitskonzept**

Ein Sicherheitskonzept inklusive eines Notfallvorsorgekonzepts ist nachzuweisen und Sicherheitsmaßnahmen zum Schutz der Informationen sind umzusetzen und zu dokumentieren. Der Web-Service-Anbieter muss hierüber dem Consumer einen geeigneten Nachweis führen, insbesondere zur Umsetzung der technisch-organisatorischen Maßnahmen bei Auftragsdatenverarbeitung. Der Web-Service-Anbieter sollte sich auf die Einhaltung aller relevanten Gesetze und Vorgaben, vor allem aber des Datenschutzes nach dem Bundesdatenschutzgesetz (BDSG) verpflichten.

**Entwicklung und Erweiterung von Web-Services**

Für die effiziente Entwicklung von Web-Services sollten Regeln festgelegt werden, die von allen Partnern eingehalten werden. Das Ziel dabei ist es, sowohl Konzeptions- als auch Programmierfehler frühzeitig zu erkennen, um diese rechtzeitig zu vermeiden. Es sollte nach einem geeigneten Vorgehensmodell (zum Beispiel V-Modell XT) entwickelt werden.

**Änderungs- und Patchmanagement**
- Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Web-Service Consumer in der Lage ist, sich neuen Anforderungen anzupassen. Es ist festzulegen, wie geänderte Anforderungen des Consumers behandelt werden.
- Der Zeitrahmen für die Behebung von Fehlern ist festzulegen.
- Testverfahren für neue Soft- und Hardware sind zu vereinbaren. Dabei sind folgende Punkte einzubeziehen:
  - Informationspflicht und
  - Absprache vor wichtigen Eingriffen ins System

**Kontrolle**
- Es ist zu vereinbaren, inwieweit dem Consumer Auditrechte für die Systeme und Abläufe des Web-Service-Anbieters eingeräumt werden. Wenn der Web-Service-Anbieter im Rahmen von Sicherheitszertifizierungen auditiert wird, ist zu klären, dass dem Consumer die Auditberichte zur Verfügung gestellt werden (mindestens als Auszug der für ihn relevanten Passagen).
- Anforderungen an die Protokollierung und Auswertung von Protokolldateien müssen festgelegt werden.
- Es ist zu vereinbaren, inwieweit der Web-Service-Consumer Protokolldaten anfordern oder einsehen darf, und welche weiteren Informationen oder Zugriffe ihm zur Aufklärung von Sicherheitsvorfällen zugänglich sind.

Die zu diesen Punkten getroffenen Regelungen müssen zwischen den beteiligten Parteien wirksam vereinbart werden, also einen Bestandteil der Vertragsbeziehung für die Erbringung beziehungsweise Nutzung der Dienste ausmachen.

Prüffragen:

- Sind alle Vereinbarungen schriftlich fixiert?
- Enthält der Vertrag alle hier aufgeführten Punkte, die für die konkrete Anbieter-Nutzer-Beziehung relevant sind?
- Sind die entsprechenden Regelungen rechtswirksam zwischen Web-Service-Anbieter und -Nutzer vereinbart worden?

# M 2.534 Erstellung einer Cloud-Nutzungs-Strategie

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Fachverantwortliche

Die Entscheidung einer Institution zur Nutzung von Cloud Services hat immer eine strategische Komponente, auch wenn der Umfang des Cloud Services gering ist. Letzteres kann dazu verleiten, die Konsequenzen dieses Outsourcings zu verkleinern oder zu verleugnen, zumal es in vielen Fällen der erste Fall von Outsourcing von IT-Dienstleistungen in der Institution ist. Oft unterscheidet sich IT-Outsourcing von Cloud-Nutzung im Umfang, in der Vertragsdauer sowie in der Art und Weise, wie die Dienste erbracht werden. Trotz allem ist die Nutzung von Cloud-Diensten immer ein Outsourcing (zumindest, wenn ein externer Dienstleister beauftragt wird) und somit strategischer Natur. Dies bedingt die ausführliche Betrachtung der wirtschaftlichen, technischen und organisatorischen Randbedingungen sowie der sicherheitsrelevanten Aspekte.

Die vorliegende Maßnahme wird dann umgesetzt, wenn sich eine Institution bereits grundsätzlich für die Nutzung von Cloud-Diensten entschieden hat. Darüber hinaus hat die Institution bereits konkrete Vorstellungen, welche Cloud-Dienste (zum Beispiel Online-Speicherdienst) genutzt werden sollen. Die abschließende Auswahl beziehungsweise Definition eines konkreten Cloud-Dienstes ist nicht Bestandteil dieser Maßnahme. Sie erfolgt erst im Anschluss an die Erarbeitung einer grundlegenden Cloud-Nutzungs-Strategie.

Die nachfolgend beschriebenen Gesichtspunkte sollten bei der Erstellung einer Cloud-Nutzungs-Strategie betrachtet und dokumentiert werden.

### Einbindung in die Unternehmensstrategie

Es ist zu klären, wie die Institution strategisch mit dem Thema Cloud-Nutzung umgeht. Ausgehend von der grundsätzlichen Entscheidung für den Einsatz von Cloud-Diensten ist dabei festzuhalten, welcher Grad an Service-Orientierung angestrebt wird, also in welchem Umfang klassische IT durch Cloud Services abgelöst werden soll. Es ist zu erarbeiten, welche Services für eine Cloud-Nutzung grundsätzlich infrage kommen.

Es sollte unter anderem die Frage nach den Treibern für den Einsatz von Cloud Services beantwortet werden. Darüber hinaus sind die Ziele zu definieren, die die Institution mit der Cloud-Nutzung verbindet. Dies können beispielsweise Kosteneinsparungen, die Möglichkeit zu einer flexibleren Service-Erbringung, die Ablösung beziehungsweise der Ersatz bisheriger Services oder die Nutzung neuer Services sein.

Diese Ergebnisse sollten möglichst auch in die Unternehmensstrategie eingebunden werden.

### Machbarkeitsstudie mit Zusammenstellung aller Rahmenbedingungen

Es gibt unterschiedliche äußere Faktoren, die Einfluss auf die Entscheidung zur Cloud-Nutzung nehmen können oder diese bedingen. Dies sind sowohl rechtliche Rahmenbedingungen (beispielsweise Vorgaben des Datenschutzes oder von Aufsichtsbehörden), organisatorische Rahmenbedingungen (beispielsweise Reife der Institution hinsichtlich Organisation und IT) als auch technische Anforderungen, die sich aus der Nutzung von Cloud Ser-

vices ergeben (beispielsweise Vorgaben bezüglich des benötigten Datennetzes, Leistungsfähigkeit der Internetanbindung, Verfügbarkeit der Netze und der IT-Systeme).

Die Ergebnisse dieser Untersuchung sind in einer Machbarkeitsstudie zu dokumentieren, die aussagt, ob der untersuchte Cloud-Dienst überhaupt zu verwenden ist.

**Betriebswirtschaftliche Aspekte mit erster Kosten-Nutzen-Abschätzung**

Da beim Cloud Computing oft finanzielle Einsparungen ein starker Treiber sind, stehen Kosten und Nutzen besonders im Fokus. Die Kosten-Nutzen-Abschätzung ergibt eine erste Indikation, ob durch die Nutzung eines Cloud-Dienstes wirtschaftliche Vorteile gezogen werden können.

Hier sind auf der Kostenseite nicht nur die reinen Betriebskosten des Cloud-Dienstes zu berücksichtigen, sondern auch die Kosten für die Migration, die Schulung der Mitarbeiter und Administratoren, gegebenenfalls neuer Hardware und Ausbau der Netzkapazitäten.

Da die Kosten-Nutzen-Abschätzung im Rahmen der Erstellung der Strategie angesetzt ist, soll die Institution auch den strategischen Wert der Ressourcen Know-how, Mitarbeiter, IT-Systeme und Anwendungen berücksichtigen. Denn diese Ressourcen können durch die Nutzung von Cloud Computing teilweise verloren gehen und nicht schnell wieder zurückgeholt werden. Auf der Nutzenseite stehen zum Beispiel obsolet gewordene Hardware mitsamt Lizenzen und Administration, bessere und schnellere Anpassung der IT an den tatsächlichen Bedarf, und gegebenenfalls können auch Sicherheitsgewinne auf der Nutzenseite verbucht werden.

Sobald der Cloud Service genauer definiert ist und erste konkrete Angebote einzelner Cloud-Diensteanbieter vorliegen, erfolgt eine detaillierte Kosten-Nutzen-Analyse (siehe M 2.540 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*).

**Auswahl der Services und des Bereitstellungsmodells**

Nach diesen strategischen Überlegungen sollte festgehalten werden, welche konkreten Dienste zukünftig von einem Cloud-Diensteanbieter bezogen werden könnten. Daneben ist auf der Basis der erhobenen Anforderungen zu entscheiden, welches Bereitstellungsmodell (zum Beispiel Private, Public, Hybrid Cloud) geeignet erscheint. Sowohl in der Literatur als auch im Zusammenhang mit der praktischen Umsetzung wird dieser Schritt häufig auch als Sourcing bezeichnet.

**Berücksichtigung von Sicherheitsaspekten von Anfang an**

Die Institution muss sicherstellen, dass grundlegende technische und organisatorische Sicherheitsaspekte bereits zu Beginn der Planungsmaßnahmen zur Cloud-Nutzung ausreichend berücksichtigt werden. Insbesondere ist auch zu klären, ob und inwieweit die Nutzung von Cloud Computing in der Sicherheitsleitlinie abgedeckt ist. Dabei sollten sich die Verantwortlichen innerhalb einer Institution insbesondere folgender Cloud-Spezifika bewusst sein:

- Der Cloud-Diensteanbieter erhält je nach Cloud-Nutzungs-Modell Zugriff auf die Daten der beauftragenden Institution. Von diesem Zugriff können auch Daten mit hohem Schutzbedarf betroffen sein.
- Die technische Umsetzung des Cloud-Nutzung-Vorhabens bedingt die Übertragung von Daten zwischen beauftragender Institution und dem

Cloud-Diensteanbieter. Das sich daraus ergebende erhöhte Gefahrenpotenzial ist durch die Institution zu ermitteln und entsprechend zu bewerten.
- Die Einführung von Cloud Services setzt den Entwurf, die Einführung und Umsetzung neuer Prozesse und Arbeitsabläufe voraus. Die Folgen der sich ergebenden notwendigen Umstellungen sind zu ermitteln und abzuschätzen.

Im Rahmen der Nutzung von Cloud Services sollten Vor- und Nachteile, die einen Bezug zur Informationssicherheit aufweisen, durch die Institution betrachtet, bewertet und dokumentiert werden.

**Erstellen einer Sicherheitsanalyse**

Zur Festlegung der Cloud-Strategie sollte eine individuelle Sicherheitsanalyse für den geplanten Cloud Service durchgeführt werden, die bei wesentlichen Veränderungen der technischen und organisatorischen Rahmenbedingungen zu wiederholen ist.

Nur so kann festgestellt werden, wie bestehende Geschäftsprozesse oder Informationsverbünde abgegrenzt und getrennt werden können, damit Teile davon als Cloud Service genutzt werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten. Die Sicherheitsanalyse sollte nach der in der IT-Grundschutz-Vorgehensweise beschriebenen Methodik durchgeführt werden.

Wenn der Schutzbedarf wichtiger Systeme oder Anwendungen hoch ist oder die Modellierung des Informationsverbunds nach IT-Grundschutz nicht möglich ist, muss eine ergänzende Sicherheitsanalyse (zum Beispiel Risikoanalyse) durchgeführt werden. Sind die sicherheitsrelevanten Gefährdungen analysiert worden, kann festgelegt werden, ob und wie diesen begegnet werden soll.

Zusätzlich weist sie bestehende Restrisiken im Zusammenhang mit der Cloud-Nutzung auf. Die Ergebnisse der Sicherheitsanalyse fließen in der Regel unmittelbar in die Kosten-Nutzen-Abschätzung ein, die nach der Sicherheitsanalyse gegebenenfalls wieder angepasst werden muss.

**Erstellung einer Roadmap**

Nachdem die strategischen und sicherheitsrelevanten Aspekte untersucht wurden, sollten erste Überlegungen hinsichtlich einer geeigneten technischen Realisierung erfolgen. Sofern die Einführung mehrerer Cloud Services durch die Institution geplant ist, hat es sich in der Praxis als hilfreich erwiesen, eine sogenannte Cloud Roadmap zu erstellen. Diese stellt einen Fahrplan zur Nutzung der Cloud Services dar und beschreibt deren Ausrollen mithilfe eines Phasenmodells. So kann die Akzeptanz der Cloud Services durch den Benutzer erhöht werden, während gleichzeitig das Risiko technischer Probleme bei der späteren Umsetzung gemindert wird.

Prüffragen:

- Wurde eine Strategie für die Nutzung von Cloud Computing erstellt?
- Wurden die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen, die sich aus der Nutzung von Cloud Services ergeben, untersucht?
- Sind grundlegende technische und organisatorische Sicherheitsaspekte der Cloud-Nutzung betrachtet worden?

- Ist eine individuelle Sicherheitsanalyse für geplante Cloud Services vorgesehen?
- Ist festgehalten, welche Dienste in welchem Bereitstellungsmodell zukünftig durch einen Cloud-Diensteanbieter bezogen werden sollen?
- Existiert eine Cloud Roadmap?

# M 2.535 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Aus der Strategie zur Cloud-Nutzung (siehe M 2.534 *Erstellung einer Cloud-Nutzungs-Strategie*) ergeben sich, je nach Detaillierungsgrad, bereits Sicherheitsvorgaben für die Nutzung von Cloud-Diensten. Diese müssen in der Sicherheitsrichtlinie weiter verfeinert werden, sodass darauf ein gewünschter Cloud Service umfassend definiert (siehe hierzu Maßnahme M 2.536 *Service-Definition für Cloud-Dienste durch den Anwender*) und ein geeigneter Cloud-Diensteanbieter ausgewählt werden kann (siehe Maßnahme M 2.540 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*).

Grundsätzlich müssen in diesem Zusammenhang möglichst alle Sicherheitsanforderungen betrachtet werden, die sich aus den ermittelten Schnittstellen sowie den organisatorischen, technischen und rechtlichen Rahmenbedingungen ergeben. Neben den Sicherheitsanforderungen an die eingesetzte Technik, einschließlich der benötigten Kommunikationswege und -dienste, ist daher zum Beispiel auch notwendig Datenschutzaspekte sowie Aspekte zur Informationsklassifizierung für alle ausgelagerten Daten zu berücksichtigen. Auch organisatorische Auswirkungen wie beispielsweise notwendige Schulungsmaßnahmen für Administratoren und Benutzer sollten bereits in der Sicherheitsrichtlinie berücksichtigt werden.

Weiterhin sollten insbesondere die nachfolgend beschriebenen Aspekte Eingang in die Sicherheitsrichtlinie für die Cloud-Nutzung finden:

- **Sicherheitsanforderungen an den Cloud-Diensteanbieter** sollten die benötigte technische Verfügbarkeit des angebotenen Services sowie Vorgaben zum Standort der Leistungserbringung des Cloud-Diensteanbieters berücksichtigen, sofern dieser ein eigenes Rechenzentrum betreibt. Zudem sollten Anforderungen hinsichtlich bestehender organisatorischer Regelungen und gelebter Prozesse beim Cloud-Diensteanbieter (beispielsweise die Einhaltung des Vier-Augen-Prinzips bei der Administration) festgelegt sein. Auch Regelungen für den Einsatz von Fremdpersonal fallen unter mögliche Sicherheitsanforderungen an den Cloud-Diensteanbieter (siehe hier Maßnahme M 2.226 *Regelungen für den Einsatz von Fremdpersonal*). Weitere Beispiele für Sicherheitsanforderungen an den Cloud-Diensteanbieter sind konkrete Vorgaben zur Datenablage, Datenverarbeitung und Datenlöschung. Auch geforderte Zertifizierungen des Dienstleisters (vorzugsweise nach IT-Grundschutz) sollten bereits in der Sicherheitsrichtlinie dokumentiert werden.
- **Sicherheitsanforderungen in Abhängigkeit vom Bereitstellungsmodell.** Setzt eine Institution Cloud Services ein, die mithilfe einer Hybrid Cloud oder einer Private Cloud On-Premise, die von einem Dienstleister betrieben wird, erbracht werden, ist unter anderem festzulegen, welche Nutzungsrechte (zum Beispiel Zutrittsrechte, Zugangsrechte, Zugriffsrechte auf Daten und Systeme) dem Cloud-Diensteanbieter vom Auftraggeber eingeräumt werden.
- **Sicherheitsanforderungen aus relevanten Gesetzen und Vorschriften.** Ein besonderes Augenmerk sollte hierbei auf länderübergreifende oder international agierende Cloud-Diensteanbieter gelegt werden, die

unter Umständen unterschiedlichen gesetzlichen Anforderungen und Bestimmungen unterliegen.

Die **Sicherheitsanforderungen an die eigene Institution** sind in einem Sicherheitskonzept für die Cloud-Nutzung festzulegen, wie in der Maßnahme M 2.539 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* beschrieben ist. Der Institution bietet sich hierbei die Möglichkeit, ein eigenes Konzept für jeden spezifischen Nutzungsfall zu erstellen oder sich für ein Gesamtkonzept zu entscheiden, mit dessen Hilfe alle beziehungsweise mehrere Nutzungsfälle abgedeckt werden.

Prüffragen:

- Beinhaltet die Sicherheitsrichtlinie konkrete und ausreichend detaillierte Sicherheitsvorgaben für die Umsetzung innerhalb der Institution?
- Sind spezifische Sicherheitsanforderungen an den Cloud-Diensteanbieter dokumentiert?
- Ist der festgelegte Schutzbedarf für den Einsatz von Cloud Services hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert?
- Sind länderspezifische Anforderungen beziehungsweise gesetzliche Bestimmungen bei Nutzung von Cloud Services internationaler Cloud-Diensteanbieter bekannt?

# M 2.536 Service-Definition für Cloud-Dienste durch den Anwender

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Entscheidet sich eine Institution für die Nutzung von Cloud-Diensten, muss eine entsprechende Service-Definition erarbeitet werden. Die IT Infrastructure Library (ITIL) definiert einen Service als die Möglichkeit, einen Mehrwert für einen Auftraggeber zu generieren. Dazu soll die Erreichung der vom Auftraggeber angestrebten Ergebnisse erleichtert oder gefördert werden. Der Auftraggeber selbst hat dabei keine Verantwortung für bestimmte Kosten oder Risiken zu tragen.

Angewandt auf die Cloud-Nutzung bedeutet dies, dass ein Mehrwert durch einen beauftragten Diensteanbieter nur generiert werden kann, sofern die angestrebten Ergebnisse innerhalb der Institution auch tatsächlich bekannt und dokumentiert sind. Grundlage für die sorgfältige Definition der zu verwendenden Cloud Services sind die Anforderungen aus der Institution heraus, wie sie im Rahmen der Maßnahmen M 2.534 *Erstellung einer Cloud-Nutzungs-Strategie* und M 2.535 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* zu ermitteln und zu dokumentieren sind. Es empfiehlt sich, eine einheitlich gestaltete Auflistung vorzunehmen, in der alle für die Verwendung vorgesehenen Cloud Services übersichtlich dargestellt sind. Hierfür bietet sich beispielsweise die Erstellung sogenannter Service Templates nach ITIL an. Mögliche Inhalte in diesem Zusammenhang sind:

- Servicekürzel und Servicename
- Kurzbeschreibung
- Kategorie
- Sub- beziehungsweise Sekundärservices
- Varianten
- Technische Parameter
- Service-Parameter/SLA
- SLA-Messung
- Gültigkeit des Services (Zeitraum)
- Service-Übergabe
- Methoden der Kostenermittlung
- Preis/Verrechnung
- Ansprechpartner für den Service
- Berechtigte und Anforderer
- Voraussetzungen

Im Rahmen der Service-Definition für Cloud-Dienste sollten durch die Institution zumindest die nachfolgenden, näher beschriebenen Aspekte thematisiert werden.

**Schnittstellen und Verantwortlichkeiten**

Die nutzende Institution sollte alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifizieren und dokumentieren.

Eine wesentliche Anwendungskomponente und wichtige Schnittstelle des Cloud-Dienstes stellt die Client-Software (zum Beispiel zur Integration eines zusätzlichen Laufwerks bei Nutzung eines Online-Speicherdienstes) dar. Daher ist insbesondere deren Auswahl für die Cloud-Nutzung ausreichende Bedeutung beizumessen. Hierbei sind eine Reihe von Aspekten zu berücksich-

tigen, und die Beantwortung der nachfolgenden Fragen kann der Institution wichtige Aufschlüsse zur Wahl einer geeigneten Lösung liefern.

- Existiert eine definierte Rückfallebene beim Ausfall der Client-Software?
- Sind eventuelle Abhängigkeiten oder Inkompatibilitäten im Zusammenhang mit der vorhandenen IT-Infrastruktur zu erwarten?
- Kann die Client-Software ohne Weiteres in die bestehenden Prozesse des Änderungsmanagements integriert werden oder sind Anpassungen notwendig? Nähere Hinweise hierzu finden sich auch in M 2.221 *Änderungsmanagement* beziehungsweise B 1.14 *Patch- und Änderungsmanagement*.
- Erfüllt die Client-Software die Anforderungen der Institution hinsichtlich bestehender Test- und Freigabeprozesse?

**Auswahl sicherer Authentisierungsmethoden**

Plant eine Institution die Nutzung von Cloud-Diensten, sollte dabei auf die Auswahl und den Einsatz sicherer Authentisierungsmethoden geachtet werden. Dabei sind starke Authentisierungsmechanismen (zum Beispiel 2-Faktor-Authentisierung) zumindest für die Administration der Cloud Services einzusetzen. Wurde für den Cloud Service ein hoher Schutzbedarf identifiziert, sollten auch für Benutzer außerhalb der Administration starke Authentisierungsmechanismen zum Einsatz kommen. Gleiches gilt bei Nutzung von Cloud Services über das Internet, falls kein VPN eingesetzt wird. Bei der Nutzung von Cloud Services mit normalem Schutzbedarf und beim Einsatz von VPN ist hingegen in der Regel eine 1-Faktor-Authentisierung ausreichend, wobei das dabei verwendete Passwort den Regeln für sichere Passwörter der Institution unterliegt.

**Berücksichtigung weiterer Sicherheitsaspekte**

Neben den genannten Aspekten sind im Rahmen der Service-Definition für Cloud-Dienste auch Vorgaben zur Verschlüsselung von Informationen zu erstellen. Sofern weitere Sicherheitsvorgaben als notwendig angesehen werden, wie beispielsweise die Durchführung eigener Datensicherungen, sollten diese ebenfalls in die Service-Definition einfließen.

**Definition von OLA und SLA**

Es sind gezielt konkrete interne Anforderungen an die zu verwendenden Cloud Services auszuarbeiten, und der Service-Level für die Anwender innerhalb der eigenen Institution zu definieren. Diese internen Regelungen, die auch als OLA (Operational Level Agreement) bezeichnet werden, dienen in der Folge als Basis für die Erarbeitung entsprechender SLA (Service Level Agreements) mit einem externen Cloud-Diensteanbieter.

Nach abschließend erfolgter Service-Definition für den Cloud-Dienst ist dessen Einbindung in die Institution, wie in Maßnahme M 2.538 *Planung der sicheren Einbindung von Cloud Services* beschrieben, sicherzustellen.

Ist der Cloud Service definiert, muss ein geeigneter Cloud-Diensteanbieter für dessen Erbringung gefunden werden (siehe hierzu M 2.540 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*). Basis für die tatsächliche Erbringung des definierten Cloud Services ist anschließend ein entsprechender Vertrag zwischen Auftraggeber und Cloud-Diensteanbieter (siehe hierzu M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*).

Prüffragen:

- Gibt es eine Service-Definition des zu nutzenden Cloud-Dienstes?

- Existiert eine Auflistung, die alle geplanten und verwendeten Cloud Services zusammenfasst?
- Sind alle relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Nutzung identifiziert und dokumentiert?
- Wurden Vorgaben zur Auswahl und zum Einsatz sicherer Authentisierungsmethoden definiert?
- Wurden konkrete interne Anforderungen an die zu verwendenden Cloud Services ausgearbeitet?
- Wurden Vorgaben zur Verschlüsselung von Informationen für den Cloud-Dienst gemacht?

# M 2.537 Planung der sicheren Migration zu einem Cloud Service

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Entscheidet sich eine Institution zur Nutzung von Cloud Services, sind in der Folge umfangreiche Planungsmaßnahmen durchzuführen, um deren sicheren Betrieb auch fortlaufend gewährleisten zu können. Ein besonderes Augenmerk ist hierbei auf die Planung der sicheren Migration und Einbindung von Cloud Services zu richten. Der Begriff Migration bezeichnet dabei immer entweder den technischen Wechsel von einem System auf ein anderes oder den Wechsel des Cloud-Diensteanbieters.

Die Planung der sicheren Einbindung von Cloud Services (siehe Maßnahme M 2.538 *Planung der sicheren Einbindung von Cloud Services*) konzentriert sich dabei auf unterschiedliche Aspekte, die über die Überlegungen der Migrationsplanung hinaus betrachtet werden sollten.

Im Rahmen der Planung der sicheren Migration zu einem Cloud Service muss die Institution ein Migrationskonzept erstellen, welches als Teil des Sicherheitskonzeptes für die Cloud-Nutzung auszulegen ist (siehe Maßnahme M 2.539 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*). Dabei sind verschiedene Cloud-spezifische Besonderheiten und Voraussetzungen zu beachten und entsprechend im Migrationskonzept darzustellen.

**Planung der Einführung eines Cloud Services in die Institution**

Die Einführung eines Cloud Services erfolgt in der Regel stufenweise und unterscheidet sich hierbei von der Umsetzung eines klassischen Outsourcing-Vorhabens. In der Regel ist keine "echte" Transition erforderlich. Unter Transition ist hier der Übergang von einem Betriebsmodell in ein anderes zu verstehen, also etwa der Übergang aus dem Eigenbetrieb in eine Outsourcing-Situation.

Zu Beginn der Planung sollten zunächst organisatorische Regelungen wie hierarchische Strukturen, Rollen und Verantwortlichkeiten sowie die Aufgabenverteilung festgelegt werden.

Zusätzlich sollten geeignete Test- und Übergabeverfahren geplant werden, um sowohl eine reibungslose Migration als auch fortlaufend einen sicheren Betrieb gewährleisten zu können.

Im weiteren Verlauf der Migrationsplanungen sind festgelegte Anforderungen hinsichtlich des zu gewährleistenden Sicherheitsniveaus und Service Levels auf Einhaltung zu überprüfen und eventuell notwendige Anpassungen vorzunehmen, sofern Abweichungen vom definierten Soll-Zustand auftreten.

Zudem empfiehlt es sich, weitere vertragliche Regelungen zwischen Institution, Cloud-Diensteanbieter und gegebenenfalls externen Migrations-Dienstleistern zu definieren. Dies dient unter anderem der Beantwortung der Frage, wann eine Migration als abgeschlossen zu betrachten und wann die Übergabe in die Produktion erfolgt ist. Auch der Zeitpunkt, ab dem eine Institution die Einhaltung vereinbarter Service Level Agreements einfordern kann, gilt als genau zu definieren. Es ist hilfreich, nach der Abnahme der Migrationen ein Review über die gesamte Migration vorzunehmen. Wichtig sind in diesem Zu-

sammenhang auch Nachweise, was der Migrations-Dienstleister an Konvertierungen von Daten und Systemen vorgenommen hat.

**Berücksichtigung der eigenen IT**

Um einen reibungslosen Einsatz von Cloud Services zu gewährleisten, ist eine enge Einbindung in die IT der Institution erforderlich. Die bestehende IT-Umgebung ist daher in besonderem Maße bei den Migrationsplanungen zu berücksichtigen. Hierbei sollten bereits vorhandene sowie zusätzlich benötigte Schnittstellen im Vorfeld identifiziert und gegebenenfalls an veränderte Anforderungen angepasst werden.

**Auswirkung auf Betriebsprozesse**

In der Praxis hat der Einsatz von Cloud Services häufig Veränderungen von Prozessen beim Auftraggeber zur Folge. Im Rahmen der Cloud-Nutzung empfiehlt es sich daher, bestehende Betriebsprozesse zu überprüfen und an neue Gegebenheiten anzupassen. Dabei sind auch etwaige Auswirkungen auf Mitarbeiter zu berücksichtigen. Gegebenenfalls müssen hier die neuen Aufgaben und damit einhergehenden Verantwortungsbereiche eindeutig definiert und zusätzlicher Schulungsbedarf identifiziert werden.

Prüffragen:

- Ist das Migrationskonzept für den definierten Cloud Service als Teil des Sicherheitskonzeptes für die Cloud-Nutzung ausgelegt?
- Sind organisatorische Regelungen hinsichtlich der Migration definiert?
- Wurden bestehende Betriebsprozesse hinsichtlich der Cloud-Nutzung identifiziert und angepasst?
- Ist die eigene IT ausreichend im Migrationsprozess berücksichtigt worden?
- Wurde ein entsprechender Schulungsbedarf für Mitarbeiter ermittelt?

# M 2.538 Planung der sicheren Einbindung von Cloud Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Entscheidet sich eine Institution zur Nutzung von Cloud Services, sind in der Folge umfangreiche Planungsmaßnahmen durchzuführen, um deren sicheren Betrieb zu gewährleisten. Insbesondere sind hierbei die Planung der sicheren Migration und die Planung der sicheren Einbindung in die vorhandene IT-Landschaft zu nennen.

In M 2.537 *Planung der sicheren Migration zu einem Cloud Service* finden sich beispielsweise Hinweise auf die stufenweise Einführung von Cloud Services sowie die generelle Notwendigkeit, Cloud Services eng in die IT der eigenen Institution einzubinden. Bei der tatsächlichen Planung der sicheren Einbindung von Cloud Services in die eigene Institution sind darüber hinaus allerdings weitere Aspekte zu betrachten, die über die ersten Überlegungen der Migrationsplanung hinausgehen.

Basierend auf den ermittelten Anforderungen für die Cloud-Nutzung (siehe M 2.534 *Erstellung einer Cloud-Nutzungs-Strategie*) sind notwendige Anpassungen mindestens in den nachfolgend beschriebenen Bereichen der Institution zu prüfen und zu planen. Die Ergebnisse der Prüfung sind dabei zu dokumentieren und für den Fall sich verändernder Anforderungen entsprechend anzupassen. Sofern sich aus den ermittelten Ergebnissen Handlungsbedarf ergibt, ist dies ebenfalls zu dokumentieren und als Grundlage für die Umsetzung weiterer Maßnahmen im Rahmen der Umsetzung oder für die Durchführung von Kosten-Nutzen-Analysen anzusehen.

**Anpassung der Schnittstellensysteme**

Als Schnittstellensysteme sollten auf jeden Fall betrachtet werden: Loadbalancer, Proxys, Router, Sicherheitsgateways, Federation-Systeme.

Um den Anpassungsbedarf an bestehenden Schnittstellensystemen sowie den Bedarf an potenziellen Neuanschaffungen in diesem Bereich zu ermitteln, empfiehlt sich die Beantwortung folgender Fragestellungen:

- Besteht ein Bedarf an der Bereitstellung neuer Schnittstellensysteme?
- Ist die Interoperabilität aller benötigten Schnittstellensysteme mit dem betrachteten Cloud-Dienst gegeben?
- Können die vorhandenen Schnittstellensysteme auf allen Ebenen mit den zu nutzenden Services umgehen? Kann beispielsweise der vorhandene Proxy den Applikationsverkehr angemessen inspizieren?
- Welche Performance beziehungsweise welchen Datendurchsatz müssen geeignete Schnittstellensysteme zur Verfügung stellen können?
- Müssen Schnittstellensysteme redundant ausgelegt sein und wenn ja, wie wird dies umgesetzt?

Sofern eine Schnittstelle (API - Application Programming Interface) zur Einbindung eines Cloud Services genutzt wird, sind zusätzlich die entsprechenden Maßnahmen des Bausteins B 5.24 *Web-Services* anzuwenden.

**Anpassung der Netzanbindung**

Um zu ermitteln, ob die vorhandene Netzanbindung angepasst werden muss, sollten folgende Punkte geklärt werden:

- Ist die bestehende Bandbreite der Netzanbindung ausreichend oder muss sie für die Cloud-Nutzung angepasst werden?
- Stellen die zu nutzenden Cloud Services spezielle Anforderungen an die Latenz der Netzanbindung?
- Besteht Bedarf an einer redundanten Anbindung von Cloud Services? Wie kann in diesem Fall die Umsetzung der redundanten Anbindung sichergestellt werden?
- Besteht Bedarf an der Priorisierung unterschiedlichen Netzverkehrs (Quality of Service - QoS), um beispielsweise Videoinformationen oder Sprache qualitativ hochwertig übertragen zu können?
- Welche Vorkehrungen wurden hinsichtlich der Ausfallsicherheit der Netzanbindung getroffen? Ist in diesem Zusammenhang die Umsetzung weiterer Maßnahmen notwendig?

**Anpassung des Administrationsmodells**

Um notwendige Anpassungen des Administrationsmodells zu identifizieren, sollten nachfolgende Fragen beantwortet werden:

- Liegen sorgfältige Planungen für die Administration von Cloud Services vor?
- Existiert ein Rollen- und Berechtigungskonzept, welches eine Trennung von Administratoren (Customer Cloud Service Administrator, oft auch lediglich als Service Administrator bezeichnet) und Benutzern für die Cloud-Nutzung vorsieht?

**Anpassung des Datenmanagementmodells**

Je nach gewähltem Bereitstellungsmodell befinden sich gegebenenfalls eigene Daten nicht mehr ausschließlich in der administrativen Hoheit der eigenen Institution. Es ist daher zu planen, ob und in welcher Form sich die Datensicherungs- und Datenaufbewahrungs-Strategien durch die Nutzung von Cloud Services verändern.

Prüffragen:

- Werden die Ergebnisse der Prüfung hinsichtlich potenziell notwendiger Anpassungen der Institution an die Nutzung von Cloud Services dokumentiert?
- Wurde der Bedarf an der Bereitstellung neuer Schnittstellensysteme untersucht?
- Existiert ein Administrationsmodell (inkl. Rollen- und Berechtigungskonzept) für die Cloud-Nutzung?
- Wurden mögliche Veränderungen an Datensicherungs- und Datenaufbewahrungs-Strategien untersucht?

# M 2.539 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Entscheidet sich eine Institution zur Nutzung von Cloud Services, ist hierfür ein Sicherheitskonzept zu erstellen.

IT-Sicherheitskonzepte für Cloud-Nutzungs-Vorhaben unterscheiden sich dabei in der Regel nur wenig von Sicherheitskonzepten für IT-Systeme, die durch die Institution selbst betrieben werden. Das Sicherheitskonzept sollte möglichst auf der Basis der IT-Grundschutz-Vorgehensweise erstellt werden.

Eine der wenigen Besonderheiten im Zusammenhang mit der Nutzung von Cloud Services stellt die Beteiligung mehrerer Parteien dar. Dies ist auch bei der Erstellung des Sicherheitskonzeptes zu berücksichtigen. In der Regel sind mindestens die nachfolgenden drei Parteien an einem Cloud-Nutzungs-Vorhaben beteiligt:

- Auftraggeber der Cloud Services (nutzende Institution)
- Anbieter von Cloud Services (Cloud-Diensteanbieter)
- ein (oder mehrere) Netzprovider

Grundsätzlich ist die Erstellung eines Sicherheitskonzeptes durch jeden der genannten Beteiligten vorzunehmen. Sofern der Bedarf nach einen Sicherheitskonzept des Netzproviders besteht, sind hierzu in der Regel vorab entsprechende Vereinbarungen mit ihm zu treffen. Die nutzende Institution muss sich das Recht einräumen lassen, das Sicherheitskonzept des Cloud-Diensteanbieters mithilfe eines Audits überprüfen zu können, das ggf. auch durch einen unabhängigen, qualifizierten Dritten erfolgen kann.

Die Erstellung des Sicherheitskonzeptes dient der Dokumentation der notwendigen Sicherheitsmaßnahmen im Zusammenhang mit der Nutzung von Cloud Services. Die Grundlage für diese Dokumentation bilden dabei jene Anforderungen, die sich aus der Erstellung der Sicherheitsrichtlinie zur Cloud-Nutzung (siehe M 2.535 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) für einen konkreten Anwendungsfall beziehungsweise einen konkreten Cloud Service ableiten lassen.

Das Sicherheitskonzept für einen Cloud Service sollte sich an den Sicherheitsanforderungen und Sicherheitsmaßnahmen für einen klassischen IT-Service orientieren. Die sich hieraus ergebenen Maßnahmen sollten die Basis für die Betrachtung des Cloud Service darstellen.

Im Sicherheitskonzept für die Cloud-Nutzung sollte zusätzlich die besondere Gefährdungslage durch die Erbringung als Cloud Service beschrieben werden. Hierbei sollten insbesondere folgende Punkte betrachtet werden:

- Vorzeitige oder zwangsweise Vertragsbeendigung
- Fehlende Portabilität von Daten (insbesondere bei Software as a Service), Anwendungen (insbesondere bei Platform as a Service) und Systemen (insbesondere bei Infrastructure as a Service) für den Fall, dass der gewählte Cloud-Dienst von etablierten Standards abweicht
- Abhängigkeit von einem Cloud-Diensteanbieter durch fehlende Möglichkeit, den Anbieter zu wechseln (Vendor-Lock-in)

- Nutzung proprietärer Datenformate kann die Integrität der Informationen gefährden und den Wechsel des Anbieters erschweren
- Gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Institutionen (multi-tenancy)
- Fehlende Kenntnis über den Speicherort von Informationen
- In der Regel hohe Mobilität der Informationen
- Unbefugter Zugriff auf Informationen, zum Beispiel durch Administratoren des Cloud-Diensteanbieters oder Dritte

Abgeleitet aus diesen spezifischen Gefährdungen für den konkreten Cloud Service müssen konkrete Sicherheitsmaßnahmen festgelegt werden. Diese sollten in jedem Fall im Rahmen der Vertragsgestaltung mit dem Cloud-Diensteanbieter verbindlich vereinbart werden. Hierbei sollten insbesondere folgende Punkte betrachtet werden:

- Vorgaben zur sicheren Administration des Cloud Services (zum Beispiel 4-Augen-Prinzip für bestimmte, besonders kritische administrative Tätigkeiten wie das Kopieren einzelner Datenbestände oder Systeme)
- Vorgaben zu Betriebsprozessen und Prozessen im Sicherheitsmanagement (Schnittstellen zum Beispiel für das Change-, Incident-, Sicherheitsvorfalls- und Risikomanagement)
- Regelungen zur Überwachung der Service-Erbringung und zum Berichtswesen
- Verschlüsselung der Informationen
- Vergabe und Entzug von Berechtigungen
- Durchführung von Datensicherungen, sowohl durch den Cloud-Diensteanbieter als auch durch die Institution

Prüffragen:

- Existiert ein Sicherheitskonzept für die Cloud-Nutzung basierend auf den identifizierten Sicherheitsanforderungen?
- Wurden Regelungen für die Erstellung eines Sicherheitskonzeptes durch den Netzprovider getroffen?
- Werden Existenz und Umsetzung des Sicherheitskonzeptes aufseiten des Cloud-Diensteanbieters durch den Auftraggeber oder unabhängige Dritte überprüft?

# M 2.540 Sorgfältige Auswahl eines Cloud-Diensteanbieters

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT

Nach Abschluss der Planungs- und Konzeptionsphase ist durch die Institution ein geeigneter Dienstleister für die Erbringung des definierten Cloud Services auszuwählen.

Die Voraussetzung für die sorgfältige Auswahl eines geeigneten Cloud-Diensteanbieters bildet die Erstellung eines möglichst detaillierten Anforderungsprofils. Neben der Definition des einzusetzenden Cloud Services finden sich in Maßnahme M 2.536 *Service-Definition für Cloud-Dienste durch den Anwender* weitere Aspekte, die für das Anforderungsprofil für den Cloud-Diensteanbieter relevant sind. Weitere Sicherheitsanforderungen sind aus den Maßnahmen M 2.535 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* und M 2.539 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* einzubeziehen. Daneben sollte eine Anforderungsanalyse durchgeführt werden, die den dokumentierten Vorgaben eine Gewichtung beziehungsweise Bewertung zuordnet.

Aus der Gesamtheit der ermittelten Anforderungen ist ein Leistungskatalog beziehungsweise Lastenheft zu generieren. Auf dieser Basis kann die Institution individuelle Angebote einholen beziehungsweise verfügbare (Standard-) Angebote der Cloud-Diensteanbieter vergleichen.

**Beschaffung und Auswertung weitergehender Informationen**

Neben den oben aufgeführten Anforderungen sind bei der Auswahl eines geeigneten Cloud-Diensteanbieters weitere Aspekte zu betrachten. Als Bewertungsmethode hat sich in der Praxis die Verwendung einer Punkte-Matrix (zum Beispiel Balanced Scorecard) bewährt.

Nachfolgend beschriebene Aspekte sollten für die Auswahl eines geeigneten Cloud-Diensteanbieters herangezogen werden.

- **Reputation des Anbieters.** Sofern Informationen hierüber zur Verfügung stehen, sollte eine Institution auch die Reputation eines Cloud-Diensteanbieters in ihre Entscheidung einbeziehen. Dabei ist zusätzlich zu klären, ob innerhalb der eigenen Institution bereits Erfahrungen mit einem Cloud-Diensteanbieter verfügbar sind oder ob auf Erfahrungen anderer Kunden mit ähnlichen Anforderungen zugegriffen werden kann. Eventuell sind Informationen hinsichtlich der vertragstreuen Service-Erbringung gegenüber anderen Kunden verfügbar.
- **Kerngeschäft des Anbieters.** Es sollte kritisch hinterfragt werden, ob das Anbieten von Cloud Services als Kerngeschäft des Dienstleisters angesehen werden kann. Daneben sollte geprüft werden, inwieweit der Cloud-Diensteanbieter bereits eine gewisse Historie aufzuweisen hat, die auch auf eine möglichst hohe Zukunftssicherheit schließen lässt. Die Auswahl eines Cloud-Diensteanbieters, der erst seit kurzer Zeit am Markt in Erscheinung tritt und für den die Erbringung von Cloud-Diensten nicht das Kerngeschäft darstellt, birgt unter Umständen ein erhöhtes Risikopotenzial. Die Gefahr, dass ein solcher Anbieter die Erbringung von Dienstleistungen kurzfristig einstellt, sich stark verändert oder komplett vom Markt ver-

schwindet, ist größer einzuschätzen als bei ausgewiesenen Cloud-Dienstleistern, die ihr Service-Angebot bereits über einen längeren Zeitraum aufrechterhalten und immer weiter ausbauen.

- **Öffentlich verfügbare Rankings oder Bewertungsmatrizen.** Auch öffentlich verfügbare Rankings oder Bewertungsmatrizen, die von (unabhängigen) Dritten erstellt wurden, können zur Auswahl eines geeigneten Cloud-Diensteanbieters beitragen. Dabei ist darauf zu achten, dass die Bewertung möglichst objektiv und neutral erfolgt. Hier empfehlen sich Marktanalysen, die beschreiben, welcher Cloud-Diensteanbieter für welche Kundensituation am geeignetsten erscheint. In diesem Zusammenhang werden häufig Bewertungen hinsichtlich Sicherheitsaspekten, Kosten oder der Leistungserbringung vorgenommen.
- **Due-Diligence-Prüfung.** Bei entsprechendem Bedarf und sofern möglich, ist die Durchführung einer Due-Diligence-Prüfung (due diligence - "gebotene Sorgfalt") ratsam. Hierbei sollten alle relevanten Parameter im Zusammenhang mit der Nutzung von Cloud Services (zum Beispiel Sicherheitsaspekte, eingesetzte Technik, Schnittstellen, Prozesse usw.) geprüft werden. Ziel der Prüfung ist, die Leistungsfähigkeit des Diensteanbieters zu ermitteln und zu klären, ob der Cloud-Diensteanbieter die Voraussetzungen für die gewünschte Service-Erbringung erfüllt.
- **Zugriffe durch den Diensteanbieter oder Dritte.** Ein weiteres Auswahlkriterium für einen geeigneten Cloud-Diensteanbieter kann dessen Möglichkeit zum Zugriff auf Daten oder Verfahren der Institution darstellen. Unter Umständen räumt der Diensteanbieter ein solches Zugriffsrecht für sich oder Dritte ein, was in der Regel aber den Anforderungen an den Cloud Service widerspricht. Darüber hinaus ist zu beobachten, dass Diensteanbieter Subunternehmer beauftragen, die in der Folge Zugriff auf Kundendaten erhalten können.
- **Installation bestimmter Softwarelösungen.** In einigen Fällen setzt die Nutzung des Cloud Services die vorherige Installation einer bestimmten Software-Lösung auf den Systemen der Institution voraus. Hier empfiehlt sich zu hinterfragen, welche potenziellen Sicherheitsrisiken beziehungsweise -erfordernisse mit einer solchen Installation einhergehen. Möglicherweise ergeben sich Kompatibilitätsprobleme, oder es entstehen zusätzliche Kosten, die nicht auf den ersten Blick ersichtlich sind. Zudem entsteht eine weitere Abhängigkeit vom Cloud-Diensteanbieter.
- **Standorte des Cloud-Diensteanbieters.** Auch der Sitz des Cloud-Diensteanbieters (und die damit einhergehende Jurisdiktion), die Standorte der von ihm betriebenen oder genutzten Rechenzentren sowie die Sitze und Standorte der zur Service-Erbringung beauftragen Subunternehmen können für eine Institution von entscheidender Bedeutung sein. Der mögliche Ort der Leistungserbringung kann durch Compliance-Vorgaben eingeschränkt sein. Abhängig von der Standortwahl des Diensteanbieters unterliegt dieser gegebenenfalls staatlichen Eingriffs- und Einsichtsrechten. Denkbar sind hier ebenfalls existierende Prüfpflichten zu gespeicherten Daten, denen der Diensteanbieter nachkommen muss, oder auch gerichtlich einklagbare Einsichtsrechte Dritter.
- **Subunternehmen zur Service-Erbringung.** Häufig sind viele Subunternehmen an der Erbringung eines Cloud Services beteiligt. Unstimmigkeiten zwischen den Vertragspartnern oder unzuverlässige Subunternehmer können sich nachteilig auf die Leistungsfähigkeit des Cloud-Diensteanbieters auswirken. In der Regel ist die Beteiligung von Subunternehmen wesentlich stärker ausgeprägt, als dies beispielsweise beim Outsourcing der Fall ist. Bei der Auswahl eines Cloud-Diensteanbieters sollten daher auch die Subunternehmen betrachtet werden.
- **Berücksichtigung vertraglicher Regelungen.** Bereits bei der Auswahl eines Cloud-Diensteanbieters sollten dessen vertragliche Regelungen be-

rücksichtigt werden. Besteht ein Cloud-Diensteanbieter beispielsweise auf Vertragsbestandteilen, die durch die nutzende Institution nicht zu akzeptieren sind, sollte der entsprechende Cloud-Diensteanbieter als potenzieller Vertragspartner ausscheiden. Weitere Informationen zu vertraglichen Regelungen sind in der Maßnahme M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter* beschrieben.

**Durchführung einer Kosten-Nutzen-Analyse**

Die vorliegenden konkreten Angebote einiger Cloud-Diensteanbieter ermöglichen in der Folge die Durchführung einer Kosten-Nutzen-Analyse, die für jeden definierten Cloud Service durchzuführen ist. Der Fokus sollte dabei auf der Ermittlung der realistischen Kosten liegen. In der Praxis ist zu beobachten, dass im Verlauf der Service-Definition die gestellten Anforderungen an den zu nutzenden Cloud-Dienst, beispielsweise in Form konkreter SLAs, stetig wachsen. Häufig wird dabei jedoch der Einfluss solcher Leistungsmerkmale auf die Kosten eines Services unterschätzt oder gänzlich aus den Augen verloren.

Die Kosten-Nutzen-Analyse liefert einer Institution in diesem Fall Aufschlüsse über ein sinnvolles Verhältnis zwischen dem potenziellen Mehrwert konkreter Anforderungsanpassungen und den sich daraus ergebenden Kosten. Weist die Kosten-Nutzen-Betrachtung des definierten Cloud Services höhere Kosten als Nutzen auf, sollte in der Folge die Service-Definition überdacht und gegebenenfalls angepasst oder auf die Nutzung des Cloud Services verzichtet werden.

Bei der Betrachtung der Kosten ist zwischen Investitionskosten (Capex - capital expenditure) und Kosten für den operativen Geschäftsbetrieb (Opex - operational expenditure) zu unterscheiden. Bei der Nutzung von Cloud Services entstehen zunächst zusätzliche Kosten, da ein Umstieg auf die Cloud nicht sofort vorhandene Services und die dafür benötigte Infrastruktur ablöst. So übernehmen beispielsweise die Mitarbeiter einer Institution neue Aufgaben, für die sie zusätzlich geschult werden müssen, auch sind weitere organisatorische Anpassungen innerhalb der nutzenden Institution notwendig. Diese Kosten müssen ebenso in die Analyse des Kosten-Nutzen-Verhältnisses einbezogen werden, wie die in der Regel verbrauchsorientierten Nutzungskosten für die Inanspruchnahme eines Cloud-Dienstes.

Auf diesem Weg soll sichergestellt werden, dass die potenzielle Ersparnis durch die Einführung von Cloud Services realistisch betrachtet wird. In der Praxis hat sich gezeigt, dass sich der tatsächliche Vorteil bei der Cloud-Nutzung häufig aus Einsparungen durch frei werdende Rechenzentrumsfläche ergibt.

**Mögliche Fallstricke bei der Auswahl eines Cloud-Diensteanbieters**

In der Praxis zeigt sich oft, dass Anwender zwar über ein grundsätzliches Verständnis von Maßnahmen zur geeigneten Auswahl eines Cloud-Diensteanbieters verfügen, sie aber dennoch an häufig wiederkehrenden Fallstricken scheitern. Auf die nachfolgend beschriebenen Aspekte sollte daher, in Abhängigkeit von den Anforderungen der Institution, ein besonderes Augenmerk gelegt werden. Die Ausführungen sind dabei als unterstützende Hinweise für den Anwender zu sehen, eine vollständige Umsetzung wird nicht als notwendig erachtet.

**Prüfung der vertraglichen Grundlagen**

Die Nutzungsbedingungen, Geschäftsbedingungen oder sonstige vertragliche Grundlagen des Cloud-Diensteanbieters, die bereits vor dem eigentlichen Vertragsabschluss zur Einsicht vorliegen, sollten umfassend geprüft werden. Häu-

fig verbergen sich hier hinter unverständlichen, unübersichtlichen, auffallend umfangreichen oder intransparenten Unterlagen nachteilige Regelungen für den Anwender.

**Service-Beschreibungen**

Die verfügbaren Service-Beschreibungen des Cloud-Diensteanbieters sollten sorgfältig geprüft und hinterfragt werden. Es ist zu klären, wie die darin enthaltenden Angaben zu verstehen sind. Bei Unklarheiten oder Unsicherheiten sollte der entsprechende Cloud-Diensteanbieter direkt kontaktiert werden. Häufig ist in der Praxis zu beobachten, dass insbesondere im Zusammenhang mit Cloud Services Leistungen durch den Anwender als inklusiver Bestandteil der Service-Beschreibung vorausgesetzt werden, die in dieser Form vom Cloud-Diensteanbieter nicht oder lediglich als kostenpflichtige Zusatzleistung erbracht werden.

Beispiel:

- Der Anwender beauftragt einen Online-Speicher, den er für Daten einsetzen möchte, die häufigen Änderungen unterliegen. In der zugehörigen Service-Beschreibung des Cloud-Diensteanbieters wird das Backup der Daten als Inklusiv-Leistung beschrieben. Da der Anwender in seiner eigenen Institution täglich ein Backup der Daten vornimmt, setzt er diesen Backup-Zyklus auch beim beauftragten Diensteanbieter als Standard voraus. Der Cloud-Diensteanbieter bietet tatsächlich aber nur ein wöchentliches Backup an. Für die Verkürzung des Backup-Zyklus fallen zusätzliche Kosten an.

**Erwartete und tatsächliche Leistungserbringung**

Ein Cloud-Diensteanbieter muss aus Gewinnerzielungsabsicht heraus seine Services möglichst kostengünstig erbringen, was unter Umständen den Erwartungen des Auftraggebers (hohe Dienstleistungsqualität, Flexibilität, Kundenfreundlichkeit, Sicherheitsniveau etc.) widerspricht.

Insbesondere bei Cloud-Nutzung ist in der Praxis jedoch häufig zu beobachten, dass IT-Verantwortliche die Werbeaussagen des Dienstleisters in der Erwartung der Senkung von IT-Kosten nicht hinterfragen. Missverständnisse hinsichtlich erwarteter und tatsächlich erbrachter Leistungen, die häufig nur mit zusätzlichen Kosten zu beheben sind, stellen sich daher oft erst im laufenden Betrieb heraus.

Aus diesem Grund sollten die Verantwortlichen innerhalb einer Institution bereits vorab eine Vergleichsrechnung durchführen, die Aufschluss darüber gibt, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit sowohl Auftraggeber als auch Auftragnehmer von einem Vertragsverhältnis profitieren. Das Ergebnis der Berechnung zeigt unter Umständen, dass eine seriöse Leistungserbringung zu den angebotenen günstigen Konditionen nicht als realistisch angesehen werden kann.

**Standardisierte SLA-Beschreibungen**

Standardisierte SLA-Beschreibungen des Cloud-Diensteanbieters, die nicht individuell vereinbart werden, sollten bereits im Rahmen der Auswahl eines Cloud-Diensteanbieters sorgfältig hinsichtlich ihres Inhaltes und ihrer Aussagekraft untersucht werden. Häufig sind in der Praxis unklare Beschreibungen innerhalb von SLAs vorzufinden. Dies kann im laufenden Betrieb zu Unstimmigkeiten und Störungen führen. Sofern keine SLA-Beschreibungen vorlie-

gen, sollten Institutionen die verfügbaren AGBs auf ähnliche Weise prüfen und ggf. mit konkreten Fragen an den Cloud-Diensteanbieter herantreten.

**Beispiel:**

- Ein Cloud-Diensteanbieter garantiert innerhalb des SLAs eine Serviceverfügbarkeit von 99,5 %, spezifiziert diese Zahl aber nicht genauer. Für den Anwender ist nicht transparent, was sie bedeutet. Der Service dürfte nach diesem SLA zwei Tage am Stück ausfallen, was einer für den Anwender maximal tolerierbaren Ausfallzeit von vier Stunden entgegenstehen würde.

**Außendarstellung zur Leistungsfähigkeit des Cloud-Diensteanbieters**

Die Außendarstellung zur Leistungsfähigkeit eines Cloud-Diensteanbieters ist kritisch zu betrachten und im Zweifelsfall durch individuelle Kontrollen zu überprüfen. Cloud-Nutzung wird nach wie vor als Trend-Thema angesehen. Verantwortliche in Institutionen sehen sich daher aus unterschiedlichen Gründen unter Umständen dazu verleitet, die Werbeversprechen von Cloud-Diensteanbietern nicht in ausreichendem Maße kritisch zu hinterfragen. Anwender gewinnen so gegebenenfalls einen falschen Eindruck davon, wer sich tatsächlich hinter dem Cloud-Diensteanbieter verbirgt und hinterfragen dessen getroffene Aussagen zur eigenen Leistungsfähigkeit in der Folge nicht ausreichend. In einem solchen Fall hätte beispielsweise die Besichtigung eines Rechenzentrums vor Ort zum Aufdecken der falschen Versprechungen beigetragen.

Legt eine Institution bei der Auswahl ihres Cloud-Diensteanbieters besonderen Wert darauf, dass Zertifizierungen vorhanden sind, sollten auch diese näher hinterfragt werden. Häufig sind Zertifizierungen (zum Beispiel nach ISO/IEC 27001, ISO 9001 etc.) zwar grundsätzlich vorhanden, werden aber nicht regelmäßig aktualisiert und sind daher nicht mehr gültig oder der Scope deckt den betroffenen Service nicht ab. Auch sind der Inhalt und Umfang zu hinterfragen und gegebenenfalls weitere Informationen vom Cloud-Diensteanbieter zu fordern. Als zuverlässig sind in diesem Zusammenhang Zertifizierungen nach IT-Grundschutz auf Basis von ISO 27001 anzusehen.

**Kundenfreundlichkeit**

Verwendet der Cloud-Diensteanbieter in seiner Leistungsbeschreibung unklare Definitionen und ist nicht willens oder in der Lage, diese verständlich zu erläutern, sollte der Anwender prüfen, ob dies ein geeigneter Vertragspartner für den geplanten Cloud Service ist.

Prüffragen:

- Wurde auf der Basis der Service-Definition für den Cloud-Dienst ein detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellt?
- Existiert eine Leistungsbeschreibung oder ein Lastenheft zum Abgleich und zur Bewertung vorliegender Angebote unterschiedlicher Cloud-Diensteanbieter?
- Fanden ergänzende Informationsquellen (zum Beispiel Marktanalysen, vertragliche Regelungen oder Standortwahl) Eingang in die Bewertung eines Cloud-Diensteanbieters?
- Wurden die verfügbaren Service-Beschreibungen (SLAs oder AGBs) des Cloud-Diensteanbieters sorgfältig geprüft und hinterfragt?

# M 2.541 Vertragsgestaltung mit dem Cloud-Diensteanbieter

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT

Hat die Institution einen geeigneten Cloud-Diensteanbieter ausgewählt, sollten alle relevanten Aspekte der geplanten Cloud-Nutzung vertraglich in sogenannten Service Level Agreements, kurz SLA, festgehalten und geregelt werden. Dabei sollten Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen dem Schutzbedarf der Daten und Anwendungen angepasst werden, die im Zusammenhang mit der Cloud-Nutzung stehen.

Bei der Vertragsgestaltung mit dem Cloud-Diensteanbieter ist eine Vielzahl unterschiedlicher Themen zu betrachten. Es ist darauf zu achten, dass alle zuvor definierten Anforderungen auch im Vertrag mit dem Cloud-Diensteanbieter berücksichtigt werden. Grundsätzlich sollten sich die vertraglichen Regelungen zumindest an den nachfolgend beschriebenen Punkten orientieren.

### Ort der Leistungserbringung durch den Cloud-Diensteanbieter

Es ist festzuhalten, an welchen Standorten ein Cloud-Diensteanbieter die beauftragten Cloud Services erbringt (zum Beispiel national, innerhalb der Europäischen Union etc.). Wenn notwendig, können auch explizit bestimmte Rechenzentren festgelegt werden.

### An der Erbringung des Services beteiligte Subunternehmer oder andere Dritte

Sofern Subunternehmer an der Service-Erbringung beteiligt sind beziehungsweise der Cloud-Dienst auf anderen Cloud-Diensten basiert, ist dies unter Angabe der beteiligten Dritten vertraglich festzuhalten. Änderungen müssen dem Cloud-Anwender mitgeteilt werden, und bei kritischen Diensten muss auch ein außerordentliches Kündigungsrecht eingeräumt werden.

### Regelungen hinsichtlich der Infrastruktur des Cloud-Diensteanbieters

In diesem Zusammenhang sind unter anderem Vorgaben zur Absicherung der vorhandenen Infrastruktur und umzusetzende Maßnahmen zur Ausfallsicherheit beim Cloud-Diensteanbieter festzuhalten. Auch Vorgaben zur Ausgestaltung der Umsetzung einer mandantenfähigen Infrastruktur durch den Cloud-Diensteanbieter sollten vertraglich geregelt werden. Gegebenenfalls kann in diesem Zusammenhang ein Nachweis mithilfe von Zertifizierungen erfolgen.

### Regelungen hinsichtlich des Personals beim Cloud-Diensteanbieter

Sofern die nutzende Institution besondere Anforderungen an Skill-Level, Qualifikationen und Zertifizierungen des Personals beim Cloud-Diensteanbieter stellt, sind diese vertraglich festzulegen. Dabei sind unter anderem folgende Aspekte denkbar:

- Regelungen zum Vorgehen des Cloud-Diensteanbieters bei der Einstellung von IT-Administratoren oder anderen Mitarbeitern mit Zugriffsrechten auf Kundendaten. Bei Vertragspartnern mit Standorten in mehreren Ländern sollte sichergestellt sein, dass unabhängig vom Einsatzort des Mitar-

beiters die gleichen Kriterien (zum Beispiel hinsichtlich Aus- und Weiterbildung, benötigten Zertifikaten, Sprachvermögen) angesetzt werden.

Weiterhin sind folgende Themen hinsichtlich des Personals zu regeln:

- Vorgaben zu notwendigen Schulungen zu Informationssicherheit durch den Cloud-Diensteanbieter
- Sofern dies als erforderlich angesehen wird, kann ein Nachweis der Sicherheitsüberprüfung von Mitarbeitern eingefordert werden.
- Vorgaben zur regelmäßigen Beurteilung des Personals, um das erforderliche Qualitätsniveau dauerhaft gewährleisten zu können.

**Regelungen zu Kommunikationswegen und Ansprechpartnern**

Es sind klare Verantwortlichkeiten, Eskalationsstufen und Kommunikationswege zwischen der beauftragenden Institution und dem Cloud-Diensteanbieter zu definieren. Die Kommunikationssprache ist festzulegen. Es ist insbesondere darauf zu achten, dass Regelungen zu Ansprechpartnern im Notfall, zum Sicherheitsvorfall-Management und zur Behebung von Fehlern getroffen werden. Je nach Anforderungen des Auftraggebers sind hier explizit Telefonnummern, Kontaktpersonen sowie Erreichbarkeitszeiten anzugeben.

**Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten**

Folgende Themen sollten vertraglich vereinbart werden:

- Vorgaben zur Durchführung regelmäßiger Security-Monitoring-Aktivitäten
- Vorgaben zum Incident Handling
- Vorgaben zur Durchführung regelmäßiger Abstimmungsrunden
- Vorgaben zum Änderungsmanagement beim Cloud-Diensteanbieter
- Vorgaben zu den Fernzugangsrichtlinien des Cloud-Diensteanbieters
- Umzusetzende Maßnahmen zum Schutz gegen Schadprogramme
- Detaillierte Dokumentation des Backup- und Recovery-Prozesses
- Einräumung des Rechts zur eigenen Datensicherung durch die nutzende Institution (soweit dies beim angebotenen Dienst möglich ist)
- Bereitstellung von verschlüsselten Transportwegen
- Mitwirkungspflichten des Cloud-Anwenders

**Regelungen zur Beendigung des Vertragsverhältnisses**

Es sind unter anderem Regelungen zur Rückgabe der Daten zu treffen. Weiterführende Informationen zu umzusetzenden Maßnahmen, für den Fall, dass das Vertragsverhältnisses beendet wird, sind der Maßnahme M 2.307 *Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses* zu entnehmen.

**Sicherstellung der Datenlöschung beim Cloud-Diensteanbieter**

Es sind Vereinbarungen darüber zu treffen, was unter der Löschung von Daten zu verstehen ist und was die vollständige Löschung der Daten beinhaltet. Hierbei kann beispielsweise zwischen dem Entfernen von Tags und dem (mehrfachen) Überschreiben von Daten unterschieden werden.

Weiterhin sind Vereinbarungen darüber zu treffen, welches Sicherheitsniveau bei der Datenlöschung durch den Cloud-Diensteanbieter zu erzielen ist und ob eine Unterscheidung hinsichtlich der Datenlöschung im regulären Betrieb oder bei Vertragsbeendigung erfolgen soll. Hierfür bietet es sich an, den notwendigen Aufwand zur Wiederherstellung der Daten als Maßstab heranzuziehen. In den meisten Fällen sollte ein Sicherheitsniveau angestrebt werden, bei dem die Wiederherstellung der Daten mithilfe professioneller Recovery-Tools nicht möglich ist. Sofern höhere Anforderungen an das Sicherheitsniveau der Da-

tenlöschung, beispielsweise die Zerstörung der Datenträger nach DIN-Norm 66399, existieren, ist bereits im Vorfeld zu klären, ob diese durch den Cloud-Diensteanbieter tatsächlich erfüllt werden können (siehe hierzu auch Maßnahme M 2.540 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*).

Die Problematik des sicheren Löschens in modernen Speicherlösungen ist in der Maßnahme M 2.527 *Sicheres Löschen in SAN-Umgebungen* des Bausteins B 3.303 *Speicherlösungen / Cloud Storage* betrachtet worden. Hier können sowohl Anwender als auch Cloud-Diensteanbieter Hilfestellung hinsichtlich des zu erzielenden Sicherheitsniveaus finden.

**Regelungen zu Zutritts- und Zugriffsberechtigungen**

Sofern sich eine solche Anforderung aus den vorangegangenen Betrachtungen der Institution ergibt, ist hier beispielsweise die Beschränkung von Zugriffsberechtigungen ausschließlich auf zertifiziertes Personal denkbar. Weiterhin sind Vorgaben zu umzusetzenden Sicherheitsmaßnahmen in den Rechenzentren des Cloud-Diensteanbieters festzuhalten.

**Regelungen zur Notfallvorsorge**

Es sollte vertraglich geregelt werden, dass der Cloud-Diensteanbieter Notfallpläne vorhält und diese für den Cloud-Anwender zur Einsichtnahme zur Verfügung stehen.

Abhängig von den Verfügbarkeitsanforderungen der Anwender sind Dringlichkeitsstufen festzulegen, garantierte Reaktionszeiten im Notfall zu vereinbaren sowie die Durchführung von Notfallübungen beim Cloud-Diensteanbieter zu fordern.

**Regelungen zu rechtlichen Rahmenbedingungen**

Folgende Themen sind zu betrachten:

- Verpflichtung des Cloud-Diensteanbieters zur Einhaltung geltender Normen und Gesetze in Abhängigkeit des Standortes und der relevanten Branche.
- Regelungen zur Einbindung Dritter. Der Cloud-Diensteanbieter sollte zur Schaffung von Transparenz verpflichtet werden. Services, welche die Service Delivery Supply Chain betreffen, die Sicherheit (zum Beispiel die Verfügbarkeit) gefährden und durch Subunternehmer erbracht werden, sind offenzulegen. Darüber hinaus ist festzuhalten, dass SLAs, die Subunternehmer dem Cloud-Diensteanbieter bieten, nicht geringer sein sollten als jene, die der Cloud-Diensteanbieter seinen Kunden bietet. Der Cloud-Diensteanbieter sollte über Methoden verfügen, die ihn befähigen, den tatsächlichen Service-Level seiner Subunternehmer zu überprüfen. Zudem ist vertraglich zu regeln, dass Sicherheitsrichtlinien und Kontrollen auch von Dritten angewendet werden.
- Vorgaben zur Beendigung der Cloud-Nutzung, zum Beispiel Kündigungsregelungen
- Vertraulichkeitsvereinbarungen
- Vereinbarung von Vertragsstrafen
- Festlegung von Haftungsfragen
- Gerichtsstand und anwendbares Recht auch hinsichtlich geltender Datenschutzbestimmungen

**Festlegungen zum Änderungsmanagement und zu Testverfahren**

In Bezug auf das Änderungsmanagement und die Umsetzung von Testverfahren ist festzulegen, inwiefern flexible Anpassungsmöglichkeiten gegeben

sind. Dies ist insbesondere bei der Konfrontation mit gesetzlichen Änderungen oder gestiegenen Anforderungen relevant.

**Regelungen zur Durchführung von Kontrollen**

Die nutzende Institution sollte sich das Recht zur Durchführung eigener Audits beim Cloud-Diensteanbieter vertraglich einräumen lassen. Ebenso sollte die Akzeptanz von Audits durch Dritte sowie die Durchführung von Penetrationstests schriftlich bestätigt werden. In diesem Zusammenhang sind Regelungen dazu zu treffen, wer die Kosten für die Durchführung von Audits trägt. Darüber hinaus ist festzulegen, wie mit den Audit-Logs des Cloud-Diensteanbieters umzugehen ist. Folgende Themen sollten betrachtet werden:

- Vorgaben zur Aufbewahrungsfrist für Log-Daten
- Wirksame Kontrollen zum Schutz von Logs vor nicht autorisiertem Zugriff
- Methoden zur Überprüfung und Sicherung der Integrität von Audit-Logs
- Durchführung von Audit-Log-Reviews
- Vorgaben zur Zeitquelle, die genutzt wird, um Systeme zu synchronisieren und einen exakten Zeitstempel für Audit-Logs anzubieten

Weiterhin sollte vertraglich geregelt werden, welche Messungen auf die Einhaltung von SLAs vorgenommen werden. Auch das regelmäßige Reporting zu anstehenden Änderungen beim Cloud-Diensteanbieter (zum Beispiel bezüglich Funktionsumfang, Subunternehmern und sämtlichen für SLA relevanten Ereignissen) ist sicherzustellen.

**Berücksichtigung besonderer Anforderungen**

Unter Umständen können Institutionen besondere Anforderungen an einen Cloud Service stellen. Diese sollten ebenfalls als vertragliche Regelung festgehalten werden. Denkbar sind beispielsweise folgende Anforderungen:

- Zusicherung der Nutzung ausschließlich bestimmter, vorab definierter Rechenzentren
- Regelungen zum Import beziehungsweise Export von Daten sowie zu benötigten Schnittstellen zu anderen Services und Systemen
- Festlegung der konkreten Konfigurationsparameter bezüglich definierter Interoperabilitätsanforderungen
- Einräumen des Rechts zur Durchführung eigener Datensicherungen und Erfassung notwendiger Schnittstellen und Parameter.

Prüffragen:

- Sind die vertraglichen Regelungen in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Daten und Anwendungen angepasst, die im Zusammenhang mit der Cloud-Nutzung stehen?
- Wurde geregelt, an welchem Standort der Cloud-Diensteanbieter seine Leistungen erbringt?
- Wurden klare Verantwortlichkeiten, Eskalationsstufen und Kommunikationswege zwischen der beauftragenden Institution und dem Cloud-Diensteanbieter definiert?
- Existieren Vereinbarungen über die sichere Löschung von Daten durch den Cloud-Diensteanbieter?
- Wurden Kündigungsregelungen schriftlich fixiert?

# M 2.542 Sichere Migration zu einem Cloud Service

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT

Hat die Institution einen Cloud-Diensteanbieter für ihr Cloud-Nutzungs-Vorhaben ausgewählt, müssen bei der Umsetzung der Migration verschiedene Sicherheitsaspekte betrachtet werden. Die Vorgaben zur sicheren Migration sollten auch angewendet werden, wenn ein Cloud Service wieder zurück in die eigene Institution geholt oder er an einen anderen Anbieter übertragen wird.

Grundlegende Aspekte der Planung einer sicheren Migration zu einem Cloud Service werden ausführlich in der Maßnahme M 2.537 *Planung der sicheren Migration zu einem Cloud Service* beschrieben. Dabei ist zu beachten, dass die Zielinfrastruktur für einen Cloud Service in der Regel durch den Cloud-Diensteanbieter bereitgestellt wird. Sie ist daher nicht Gegenstand der Betrachtungen im Rahmen der Migrationsumsetzung.

**Durchführung der Migration**

Die Migration erfolgt auf Basis des Migrationskonzeptes, das bereits in der Planungsphase erstellt wurde und technische sowie organisatorische Voraussetzungen für eine Migration enthält. Darüber hinaus sind hier bestimmte Vorgaben zum Ablauf der Migration wie die Ausgestaltung einer Testphase oder Pilotphase beschrieben.

Im Rahmen der Migration sind die Vorgaben des Migrationskonzeptes mit den tatsächlichen Gegebenheiten der Institution abzugleichen. Im Falle von Abweichungen müssen diese erfasst und dokumentiert werden. In diesem Fall sind Maßnahmen zu ergreifen, um den im Migrationskonzept definierten Zustand herzustellen.

Auch das Sicherheitskonzept, das in der Planungsphase erstellt wurde (siehe hierzu Maßnahme M 2.539 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*), ist während der Umsetzung der Migration auf notwendige Anpassungen zu prüfen und gegebenenfalls zu aktualisieren. Um während der Einführungsphase das notwendige IT-Sicherheitsniveau kontinuierlich zu gewährleisten, ist ein besonderes Augenmerk auf die Abstimmung folgender sicherheitsrelevanter Aspekte zu richten:

- Um die Übertragung von Daten der Institution zu einem Cloud-Diensteanbieter vornehmen zu können, sind gegebenenfalls privilegierte Zugriffsrechte notwendig. Um das angestrebte Sicherheitsniveau gewährleisten zu können, ist entsprechend sicherzustellen, dass die Vergabe der zugriffsrechte ausschließlich gemäß den Vorgaben der Planung erfolgt und diese wieder entzogen werden, nachdem die MIgration abgeschlossen ist.
- Wird die Migration durch einen externen Dritten geplant und durchgeführt und bei der Migrationsplanung besondere Regelungen aufgestellt, so ist deren Einhaltung zu prüfen.
- Im Falle einer fehlgeschlagenen oder abgebrochenen Migration ist sicherzustellen, dass die notwendigen Maßnahmen um die bereits übermittelten Daten zu löschen durch den Cloud-Diensteanbieter realisiert werden.

Bevor die ersten Daten einer Institution an den Cloud-Diensteanbieter übermittelt werden, sind zusätzlich alle Maßnahmen zur Notfallvorsorge auf Vollständigkeit und Aktualität zu prüfen. Gegebenenfalls müssen daraufhin Fall-

back-Szenarien angepasst werden, um im Notfall die Daten wieder aus der Cloud zurückholen zu können. Regelungen, wie die Institution mit einem Abbruch einer Datenübertragung umzugehen hat, sind auf deren Anwendbarkeit und Einhaltung hin zu überprüfen. Auch wenn bereits ein Teil der Daten migriert wurde und alle notwendigen Voraussetzungen zur Nutzung von Cloud Services geschaffen sind, besteht die Notwendigkeit zur kontinuierlichen Sicherung des Datenbestandes durch den Anwender. Die ordnungsgemäße Durchführung der Datensicherung ist daher während der Migration regelmäßig zu kontrollieren.

**Durchführung der Migration im Rahmen eines Testbetriebs**

Um einen möglichst reibungslosen Übergang zur Cloud-Nutzung ohne Beeinträchtigung des laufenden Betriebs zu gewährleisten, empfiehlt es sich, die Migration zunächst in einem Testbetrieb auf ihre Umsetzbarkeit hin zu überprüfen.

Dabei wird der Cloud Service zunächst mithilfe einiger Testdaten betrieben. Dies hat den Vorteil, dass die Vorgaben des Migrations- und des SIicherheitskonzeptes auf deren grundsätzliche Realisierbarkeit hin überprüft werden können. Gegebenenfalls kann bereits zu diesem Zeitpunkt zusätzlicher Nachbesserungs- oder Entwicklungsbedarf identifiziert werden. Im Rahmen des Testbetriebs sollten, sofern möglich und sinnvoll, Leistungsmessungen vorgenommen werden, um diese mit den geforderten Leistungswerten zu vergleichen. So kann festgestellt werden, ob sich der geplante Migrationsweg grundsätzlich als umsetzbar erweist. Zudem erhält man Erkenntnisse, ob die geplante Bandbreite ausreichend ist und ob sich der zeitgleiche Umzug der festgelegten Anzahl an Datensätzen wie geplant realisieren lässt.

**Durchführung der Migration innerhalb einer Pilotphase**

Abhängig vom Umfang des Cloud-Nutzung-Vorhabens wird nach erfolgreich abgeschlossenem Testbetrieb der Übergang in eine Pilotphase empfohlen.

Ziel der Pilotphase ist es, einen Abgleich der Produktion gegenüber den zuvor definierten Anforderungen der Institution an den Cloud Service zu erhalten. Hierbei ist noch einmal zu prüfen, ob alle Zusagen und Vereinbarungen mit dem Cloud-Diensteanbieter auch eingehalten werden.

Die Durchführung der Pilotphase dient in der Regel weiterhin dazu, dass sich Service-Administratoren auf der Anwenderseite zunehmend mit dem neuen Service vertraut machen können. Im Rahmen der Migration in einer Pilotphase sollten Service-Administratoren ihre Erfahrungen entsprechend dokumentieren, um erlerntes Wissen zu dokumentieren und daraus gegebenenfalls zusätzliche Schulungsinhalte für zukünftiges Personal ableiten zu können.

**Übergang in den Produktionsbetrieb**

Sind der Testbetrieb und der Übergang in die Pilotphase positiv verlaufen, erfolgt die anschließende Durchführung der Migration und damit die Überführung des Cloud Services in den Produktionsbetrieb. In diesem Zusammenhang sind die zwischen Anwender, Cloud-Diensteanbieter und gegebenenfalls externem Migrations-Dienstleister getroffenen Regelungen gemäß den Übergabeprozessen zu berücksichtigen.

Prüffragen:

- Ist das Sicherheitskonzept im Rahmen der Umsetzung der Migration und der damit verbundenen Regelungen auf etwaige Anpassungen und Anforderungen überprüft und gegebenenfalls angepasst worden?
- Wurden im Rahmen der Umsetzung der Migration alle Maßnahmen hinsichtlich der Notfallvorsorge auf Vollständigkeit und Aktualität überprüft?
- Wurde die Funktionalität der Cloud-Nutzung zuvor in einem Testbetrieb überprüft?
- Erfolgte ein Abgleich der Produktion gegenüber den definierten Anforderungen der Institution an den Cloud Service?

# M 2.543 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Nach der erfolgreich abgeschlossenen Migration zu einem Cloud Service muss die Aufrechterhaltung der Informationssicherheit im laufenden Betrieb gewährleistet werden. Hierzu sind eine Reihe von Maßnahmen zu ergreifen, die im Folgenden näher beschrieben sind.

Die regelmäßige Aktualisierung von Dokumentationen und Richtlinien innerhalb der Institution ist sicherzustellen. Dies gilt beispielsweise für Betriebshandbücher, Nutzungsanweisungen oder Anleitungen.

Weiterhin ist sicherzustellen, dass regelmäßige Kontrollen durchgeführt werden, die sich über möglichst viele Bereiche der Cloud-Nutzung erstrecken. Es sind zumindest folgende Aspekte zu betrachten und in regelmäßige Kontrollen einzubeziehen:

- **Sicherstellung der ordnungsgemäßen Administration von Cloud Services.**
  Im Rahmen der Maßnahme M 3.11 *Schulung des Wartungs- und Administrationspersonals* werden grundlegende Vorgaben zu den Anforderungen an Administratoren beschrieben. Es ist sicherzustellen, dass alle Administratoren von Cloud Services diese Anforderungen kennen und dazu befähigt werden, diese zu erfüllen. Regelmäßige Reviews der vergebenen Berechtigungen können ebenfalls zur Sicherstellung der ordnungsgemäßen Administration von Cloud Services beitragen. Sofern dies im Rahmen der Planungsmaßnahmen als notwendig angesehen und dokumentiert wurde, ist an dieser Stelle auch auf die Einhaltung des 4-Augen-Prinzips zu achten.
- **Regelmäßige Kontrolle der Service-Erbringung.**
  In diesem Bereich sind die für die Service-Erbringung unabdingbaren Parameter zu überprüfen, neben den im Vertrag (SLA) mit dem Cloud-Diensteanbieter vereinbarten Kennzahlen (zum Beispiel Verfügbarkeit, maximale Anzahl gleichzeitiger Benutzer, Schnelligkeit der Einrichtung neuer Benutzer oder neuer Ressourcen, um nur einige zu nennen). Hinzu kommen weitere Parameter, die Leistungen der eigenen Institution oder von Dritten beschreiben, wie beispielsweise die Performance der Netzanbindung und -verbindungen.
- **Regelmäßige Service-Reviews zwischen Cloud-Diensteanbieter und Anwender**.
  Ein wichtiger Aspekt der Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb ist die regelmäßige Durchführung von Service-Reviews zwischen dem beauftragten Cloud-Diensteanbieter und der Institution. Dabei sollten die vereinbarten und die tatsächlich erreichten Service-Level gegenübergestellt werden. Die Behandlung von Ausnahmesituationen, wie beispielsweise eines groß angelegten Angriffs oder eines globalen Netzausfalls, sollte ebenfalls Inhalt der Reviews sein. Die Forderung nach regelmäßigen Service-Reviews unter Beteiligung von Auftraggeber und Auftragnehmer ist in der Praxis nicht für jeden Cloud-Dienst

umsetzbar. Das Service-Review kann daher auch zunächst vom Auftraggeber allein vorgenommen werden. Nur bei ermittelten Problemen oder bei hohem Schutzbedarf sollte eine entsprechende Abstimmung mit dem Cloud-Diensteanbieter erfolgen.

- **Sicherstellung der Interoperabilität von Cloud Services.**
  Um bei Nutzung mehrerer Cloud Services deren Interoperabilität sicherstellen zu können, empfiehlt sich die Durchführung von Interoperabilitätstests.
- **Erbringung von Sicherheitsnachweisen durch den Cloud-Diensteanbieter**.
  Die Institution sollte regelmäßig die vorhandene Dokumentation aufseiten des Cloud-Diensteanbieters zur Einsicht einfordern. Ebenso sollte der Cloud-Diensteanbieter in der Lage sein, Nachweise über die Zertifizierung von internen Kontrollsystemen für seine Prozesse und Services zu erbringen, sofern dies vertraglich vereinbart ist.
- **Die ordnungsgemäße Durchführung von Datensicherungen.**
- **Die Sicherstellung der Einhaltung vorgesehener und vereinbarter Prozesse.**
- **Die Kontrolle der technischen Maßnahmen zur Verhinderung der Nutzung nicht "erlaubter" Services, beispielsweise mithilfe des Einsatzes von Proxys.**
- **Die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests oder Schwachstellenanalysen.**

Neben den bereits beschriebenen Maßnahmen bietet die Durchführung regelmäßiger Abstimmungsrunden zwischen Cloud-Diensteanbieter und nutzender Institution weitere Möglichkeiten zur Gewährleistung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb. In diesem Zusammenhang können Abstimmungen zu unterschiedlichen Themen von Interesse sein. Aktuelle Informationen bezüglich des Änderungsmanagements bieten sich beispielsweise ebenso an wie Änderungen hinsichtlich der Personalsituation aufseiten des Cloud-Diensteanbieters. Auch eine Diskussion über die Kundenzufriedenheit und mögliche Verbesserungspotenziale könnten Inhalt einer solchen Abstimmungsrunde sein.

Die Planung und Durchführung von Übungen und Tests leistet einen wichtigen Beitrag, um die Informationssicherheit aufrecht zu erhalten. Dabei ist, mit Schwerpunkt auf der Kommunikation zwischen Institution und Cloud-Diensteanbieter, vor allem die Reaktion auf Systemausfälle (Teilausfall und Totalausfall) zu planen und zu überprüfen. Weiterhin müssen Planungen hinsichtlich des Wiedereinspielens von Datensicherungen vorgenommen und dokumentiert werden. Generell sind Vorgaben zum Sicherheitsvorfallsmanagement bei Cloud-Nutzung festzuhalten.

Prüffragen:

- Werden Dokumentationen und Richtlinien (zum Beispiel Betriebshandbücher und Nutzungsanweisungen) regelmäßig aktualisiert?
- Wird die Service-Erbringung regelmäßig kontrolliert?
- Wurden Sicherheitsnachweise durch den Cloud-Diensteanbieter erbracht?
- Werden regelmäßige Abstimmungsrunden zwischen Cloud-Diensteanbieter und nutzender Institution durchgeführt?
- Werden Übungen und Tests zur Reaktion auf Systemausfälle geplant und durchgeführt?

# M 2.544 Auditierung bei Cloud-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Durchführung von Audits wird im Zusammenhang mit der Nutzung von Cloud Services als eine notwendige Maßnahme angesehen. Erfahrungen aus der Praxis haben gezeigt, dass die nutzende Institution Abweichungen zu vertraglichen Vereinbarungen, wie beispielsweise die Nichteinhaltung bestimmter Service-Level oder die Missachtung von Sicherheitsvorgaben häufig nur im Rahmen von Audits transparent machen kann.

Da der Auditierung im Cloud-Nutzungs-Umfeld eine solch große Bedeutung zukommt, sollten Audits in verschiedenen Phasen der Cloud-Nutzung thematisiert werden:

- Bei der Auswahl des Providers im Hinblick auf die generelle Einräumung eines Audit-Rechts.
- Bei der Vertragsgestaltung mit dem Cloud-Diensteanbieter hinsichtlich der Ausgestaltung des Audit-Rechts.
- Bei der Festlegung von Maßnahmen zur regelmäßigen Durchführung von Audits im Cloud-Nutzungs-Betrieb.

Die nutzende Institution sollte die Umsetzung der mit dem Cloud-Diensteanbieter vereinbarten Sicherheitsmaßnahmen regelmäßig überprüfen. Zu diesem Zweck bieten sich zur Durchführung der Audits aber auch speziell ausgearbeitete Fragebögen an.

**Durchführung von Audits beim Cloud-Diensteanbieter**

Bei der Durchführung von Audits beim Cloud-Diensteanbieter können grundsätzlich drei Ausprägungen unterschieden werden, die von der Art der Service-Erbringung abhängig sind. Bei der Nutzung eines Services, der in Form einer Private Cloud On-Premise erbracht wird, erfolgt die Überprüfung als internes Audit. Werden andere Service-Erbringungs-Modelle genutzt, wird der Cloud-Diensteanbieter einem externen Audit unterzogen. Eine Sonderform stellen sogenannte Fremd-Audits dar. Diese werden häufig mit dem Ziel einer anschließenden Zertifizierung (zum Beispiel ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz) durchgeführt.

Die unterschiedlichen Service-Modelle bei Cloud-Nutzung bedingen verschiedene Audit-Ebenen. Die Existenz solch unterschiedlicher Ebenen stellt eine Besonderheit bei der Nutzung von Cloud-Diensten dar. Diese Besonderheit ist sowohl während der Planung als auch im Verlauf der Durchführung von Audits zu berücksichtigen. Dem Auditor muss klar sein, welche Art von Service er zu bewerten hat, da sich der Aufwand für ein Audit in Abhängigkeit der Ebene ändert.

Bei der Modellierung des IT-Verbundes nach IT-Grundschutz muss, in Abhängigkeit vom Service-Modell, die Bausteinauswahl anders getroffen werden. Während bei der Nutzung von Cloud-Diensten als Infrastructure as a Service (IaaS) hauptsächlich das Rechenzentrum und die zugehörige Infrastruktur zu betrachten sind, wird dies bei Nutzung von Cloud-Diensten als Platform as a Service (PaaS) bereits um die Betrachtung von Betriebssystemen und Middleware (zum Beispiel Webserver, Datenbanken, sonstige Anwendungen mit zugehörigen Schnittstellen) ergänzt. Bei Nutzung von Software as a Service (SaaS) ist zusätzlich die Anwendungsebene einzubeziehen.

Der Auditor muss daneben auch immer den Schutzbedarf der Informationen sowie die Abhängigkeiten zu anderen Bereichen wie Infrastruktur, Systemen, Anwendungen oder Diensten, die den Service bilden, berücksichtigen.

Prüffragen:

- Hat sich die Institution das Recht zur Durchführung von Audits vertraglich zusichern lassen?
- Wird die Umsetzung der mit dem Cloud-Diensteanbieter vereinbarten Sicherheitsmaßnahmen regelmäßig in Form von Audits oder durch die Beantwortung von Fragebögen überprüft?
- Werden bei der Planung und der Durchführung von Audits die Besonderheiten der Service-Modelle IaaS, PaaS und SaaS berücksichtigt?

# M 2.545 Modellierung der Cloud-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

**Allgemeine Hinweise zur Anwendung des Bausteins**

Der Baustein B 1.17 *Cloud-Nutzung* richtet sich an alle Institutionen, die bereits Cloud Services in Anspruch nehmen oder deren zukünftigen Einsatz planen. Die Gefährdungen und Maßnahmen des Bausteins gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell.

Sofern in Abhängigkeit eines spezifischen Service- oder Bereitstellungsmodells Besonderheiten auftreten sollten, sind diese in der entsprechenden Gefährdung beziehungsweise Maßnahme gesondert vermerkt. Nähere Informationen zu den genannten Service-Begriffen sowie weitere grundlegende Definitionen und Erläuterungen finden sich in Maßnahme M 4.462 *Einführung in die Cloud-Nutzung*.

Der Baustein B 1.17 *Cloud-Nutzung* ist immer auf einen konkreten Cloud Service anzuwenden. Nutzt eine Institution einen Verbund von Cloud Services, so sind alle Services einzeln zu modellieren. Die Schnittstelle zwischen den Services ist ebenfalls Gegenstand des Bausteins und muss für alle Services betrachtet werden.

Cloud-Nutzung umfasst alle Themengebiete, die zur Nutzung einer Cloud-Umgebung erforderlich sind. Insbesondere sind damit die folgenden Punkte durch die Inhalte des Bausteins abgedeckt:

- Anwendung des Cloud Services durch Mitarbeiter der nutzenden Institution
- Administration des Cloud Services durch Mitarbeiter der nutzenden Institution

**Schnittstellen zu anderen Bausteinen**

Der Baustein Cloud-Nutzung ist eng verwandt mit dem Baustein B 1.11 *Outsourcing*. In nahezu allen Bereitstellungsmodellen, abgesehen von der Nutzung einer Private Cloud On-Premise, stellt die Nutzung von Cloud Services eine Sonderform des Outsourcings dar.

Um die Lesbarkeit und Anwendbarkeit des Bausteins zu verbessern, wurden relevante bestehende Gefährdungen aus dem Bereich des Outsourcings auch in den Baustein Cloud-Nutzung aufgenommen. Ergänzend findet sich eine Reihe spezifischer Gefährdungen, die gezielt Besonderheiten bei der Nutzung von Cloud Services betrachten.

Eine Reihe der neu konzipierten Maßnahmen des Bausteins Cloud-Nutzung weist Redundanzen zu bereits bestehenden Maßnahmen des Bausteins Outsourcing auf. Die komplette Neuerstellung wurde dabei der bloßen Ergänzung bestehender Maßnahmen um Cloud-spezifische Aspekte bewusst vorgezogen. Durch die gewählte Gestaltung der Bausteininhalte kann der Baustein Cloud-Nutzung eigenständig betrachtet werden, was auch dem starken Interesse an der Thematik Cloud-Nutzung Rechnung trägt.

Neben den genannten Schnittstellen zum Outsourcing weisen weitere Bausteine Berührungspunkte mit dem Baustein Cloud-Nutzung auf. Einige Gefährdungen und Maßnahmen aus dem Bereich des Cloud Managements (sie-

he Baustein B 5.23 *Cloud Management*) sprechen ähnliche Aspekte an, wie sie auch bei der Cloud-Nutzung relevant sind. Ein Beispiel hierfür stellt die Gefährdung G 2.176 *Mangelnde Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Anwender* dar, die in beiden Bausteinen Anwendung findet. Übernimmt die eigene IT die Rolle des Cloud-Diensteanbieters, beispielsweise in Verbindung mit dem Einsatz einer Private Cloud On-Premise, ist neben dem Baustein Cloud-Nutzung auch der Baustein Cloud Management anzuwenden.

Erfolgt die Administration des Cloud-Dienstes durch den Cloud Service Administrator aufseiten der nutzenden Institution über eine Management-Software, die Webservices verwendet, ist zusätzlich der Baustein B 5.24 *Web-Services* anzuwenden.

**Abgrenzungen zu anderen Bausteinen**

Alle Aspekte, die im Zuständigkeitsbereich des Cloud-Diensteanbieters liegen, sind durch den Baustein B 5.23 *Cloud Management* abgedeckt.

Eine Besonderheit stellen Cloud Services dar, die über die Bereitstellung einer entsprechenden API (Application Programming Interface) durch den Cloud-Diensteanbieter angebunden werden. Zur Betrachtung aller relevanten Gefährdungen und Maßnahmen im Zusammenhang mit der entstehenden Schnittstelle ist der Baustein B 5.24 *Web-Services* anzuwenden.

Bestehende Bausteine der IT-Grundschutz-Kataloge, die auch im Rahmen der Cloud-Nutzung relevant sind, werden im Baustein nicht neu betrachtet. Hierzu zählen insbesondere die Themen Netze (LAN, Internet, VPN) sowie Gebäude beziehungsweise Infrastrukturen. Diese sind auf Basis der IT-Grundschutzvorgehensweise und anhand der Hinweise aus Kapitel 2 Schichtenmodell und Modellierung der IT-Grundschutz-Kataloge anzuwenden.

Sofern sich für diese Themengebiete besondere Aspekte aus der Cloud-Nutzung ergeben, werden diese im Rahmen des Bausteins Cloud-Nutzung betrachtet. Ein Beispiel für eine solche gesonderte Betrachtung ist die steigende Wichtigkeit der Internetanbindung, wenn kritische Unternehmensprozesse in Cloud Services abgebildet werden.

# M 2.546 Analyse der Anforderungen an neue Anwendungen

**Verantwortlich für Initiierung:** Fachverantwortliche
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter Organisation

Bevor eine neue Anwendung geplant und projektiert wird, sollten die Rahmenbedingungen für den Einsatz geklärt werden, also beispielsweise

- welche Geschäftsprozesse sie wie unterstützen soll,
- welche Informationen mit welchem Schutzbedarf mit ihr verarbeitet werden sollen,
- wer auf welche Teile der Anwendung zugreifen darf und soll,
- welche rechtlichen Rahmenbedingungen einzuhalten sind (siehe M 2.547 *Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen*),
- wie der Informationsverbund aussieht, in dem sie eingesetzt werden soll, also beispielsweise, wie die Netzstrukturen aussehen, und
- welche IT-Komponenten für den Betrieb der Anwendung benötigt werden, also beispielsweise Hardware-Plattform, Betriebssysteme, Datenbanken).

Es empfiehlt sich, bereits bei der initialen Planung über Bedrohungen und Risiken zu diskutieren, die beim Betrieb der Anwendung relevant sein können. Hierzu sollte eine erste Analyse durchgeführt werden, um potenzielle Angriffe und andere Risiken für Vertraulichkeit, Integrität und Verfügbarkeit der Anwendung frühzeitig zu identifizieren. Die dokumentierten Ergebnisse zu den Sicherheitsrisiken fließen dann in die detaillierte Risikoanalyse ein, die im Zuge der Erstellung des Lastenhefts durchgeführt wird (siehe M 2.548 *Erstellung eines Lastenheftes*). Auch im späteren Projektverlauf sollten mögliche Bedrohungen regelmäßig betrachtet werden, sowohl seitens der Fachverantwortlichen als auch der Entwickler, damit alle sicherheitsrelevanten Anforderungen berücksichtigt werden. Darauf aufbauend können passende Sicherheitsmaßnahmen und Testanforderungen abgeleitet werden, die in die Sicherheitsarchitektur mit einfließen.

Wenn sich während des Betriebes einer Anwendung die Rahmenbedingungen wesentlich ändern, also beispielsweise neue Serverplattformen installiert werden, müssen die Sicherheitsmaßnahmen neu bewertet werden.

Daher müssen innerhalb des Sicherheitsmanagements Prozesse aufgebaut werden, um Anwendungen sicher zu entwickeln, zu installieren, zu betreiben, zu überwachen und zu warten sowie die Administratoren und Benutzer in deren sicherer Handhabung zu trainieren.

Im Rahmen dieser Prozesse müssen die Rollen, Verantwortlichkeiten und Aufgaben für Konzeption, Aufbau und Betrieb der jeweiligen Anwendungen festgelegt werden. Darauf aufbauend können die Berechtigungen in den verschiedenen Lebenszyklusphasen einer Anwendung geeignet festgelegt werden. Außerdem sollte im Rahmen des Rollenkonzepts festgehalten werden, welche Qualifikationen erforderlich sind, um die Rollen wahrnehmen zu können. So kann auch etwaiger Schulungsbedarf identifiziert und die jeweiligen Rolleninhaber gezielt zu ihrer Sicherheitsverantwortung sensibilisiert werden.

Prüffragen:

- Wurden die Rahmenbedingungen für den Einsatz der betrachteten Anwendungen geklärt?

# M 2.547 Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Organisation
**Verantwortlich für Umsetzung:** Fachverantwortliche

Um sicherstellen zu können, dass Geschäftsprozesse oder Verwaltungsverfahren, die die Anwendungen unterstützen sollen, rechtskonform betrieben werden, wird zu Planungs- (und später auch zu Audit-/Prüfungszwecken) eine vollständige Übersicht über einschlägige Rechtsgrundlagen benötigt (siehe B 1.16 *Anforderungsmanagement*). Diese Übersicht ist auch hilfreich für die Erstellung eines Verfahrensverzeichnisses nach Bundesdatenschutzgesetz (BDSG). Wenn in der Institution ein Justiziariat vorhanden ist, kann es bei der Erstellung dieser Zusammenstellung unterstützen. Die Rechtsgrundlagen sollten in einer Übersicht zusammengefasst werden, die als Anlage für das Lastenheft, das Datenschutzkonzept und das Sicherheitskonzept verwendet werden kann.

Aus den für die jeweiligen Institutionen geltenden Rechtsgrundlagen können sich konkrete Vorgaben für die Informationssicherheit ergeben, zum Beispiel:

- Zum Schutzbedarf (zum Beispiel Verarbeitung besonderer Arten personenbezogener Daten nach § 3 Absatz 9 BDSG, bereichsspezifische Amtsgeheimnisse wie das Steuer- oder Sozialgeheimnis etc.)
- Vorgaben zur inhaltlichen Ausrichtung und Ausgestaltung von Sicherheitsmaßnahmen. Insbesondere bei der Verarbeitung personenbezogener Daten sind rechtliche Vorgaben wie die Einhaltung der Zweckbindung (wirkt sich zum Beispiel auf die Anforderungen zur Gestaltung und Absicherung von externen Schnittstellen und Berichten aus) oder der Datenminimierung und Datensparsamkeit (wirkt sich zum Beispiel auf die Anforderung an die Gestaltung von Löschfristen aus) zu beachten.
- Vorgaben zu konkreten Sicherheitsmaßnahmen, wie zum Beispiel der Einsatz von Spiegeldatenbanken, der Qualifizierten Elektronischen Signatur (QES), zur Pseudonymisierung oder Anonymisierung der zu verarbeitenden Daten oder zur Gestaltung der Protokollierung
- Vorgaben zu Speicher- oder Archivierungsfristen

Prüffragen:

- Besteht eine Übersicht über die Rechtsgrundlagen zur Verarbeitung von Daten mit den Anwendungen?

# M 2.548 Erstellung eines Lastenheftes

**Verantwortlich für Initiierung:** Fachverantwortliche
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT

Ein Lastenheft beschreibt die Anforderungen, die eine Anwendung im Rahmen des betrachteten Geschäftsprozesses oder Verwaltungsverfahrens erfüllen soll. Dabei sind nicht nur die fachlichen (funktionalen) Anforderungen an die Anwendung zu betrachten, sondern auch nicht-funktionale Anforderungen.

Neben den fachlichen und IT-betrieblichen Anforderungen sind dabei auch Sicherheitsanforderungen zu betrachten. Auch bei diesen sind funktionale und nicht-funktionale Sicherheitsanforderungen zu unterscheiden. Funktionale Sicherheitsanforderungen decken konkrete Funktionen der Anwendung ab wie beispielsweise:

- Identitäts- und Berechtigungsmanagement
- Passwort-Management
- Kryptographische Absicherung der Daten

Die Art und Ausprägung von funktionalen Sicherheitsanforderungen wie beispielsweise zu der Integration einer Zwei-Faktor-Authentisierung, dem Aufbau einer PKI, die Nutzung von SAML oder WS-Security sind stark von dem jeweiligen Schutzbedarf der Anwendung abhängig.

Über nicht-funktionale Sicherheitsanforderungen wird beschrieben, welche Qualitätseigenschaften die Anwendung haben soll. Hierzu gehören Aspekte wie Softwarequalität, Zuverlässigkeit, Fehlertoleranz, Wartbarkeit und natürlich die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit. Ein Beispiel einer nicht-funktionalen Anforderung ist es, die Anwendung resistent gegenüber bestimmten Angriffen zu machen.

Bei einem Lastenheft handelt es sich um das Grobkonzept aus Sicht des Auftraggebers, das die Art der Umsetzung in weiten Teilen noch offen lassen kann. Das Lastenheft ist die wesentliche Grundlage, um ein Entwicklungsprojekt zu starten, in ähnlicher Weise wie dies der Anforderungskatalog im Fall von Standardsoftware ist (siehe M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*).

Bei der Erstellung des Lastenheftes müssen die folgenden Aspekte Berücksichtigung finden:

- Schutzbedarf der im Geschäftsprozess oder Verwaltungsverfahren verarbeiteten Informationen (Daten)
- Rechtsgrundlagen, die beim Betrieb und somit auch bereits bei der Konzeption der Anwendung zu beachten sind (siehe M 2.547 *Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen*)
- Vorgaben, Standards und Kriterienwerke, die zu berücksichtigen sind. Je nach Anwendungsgebiet können hierzu Sicherheitskriteriensysteme, technische Richtlinien oder Architekturempfehlungen gehören und auch Anforderungen hinsichtlich Barrierefreiheit

Beispiele für solche Vorgaben und Kriterienwerke sind:

- Common Criteria for Information Technology Security Evaluation (ISO 15408), insbesondere Teil 2 "Security functional requirements"
- Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik
- Standards und Architekturen für eGovernment (SAGA)

- Mindestanforderungen der Rechnungshöfe zum Einsatz der Informations- und Kommunikationstechnik
- Best Practices wie "Die zehn goldenen Regeln der IT-Sicherheit" aus dem Secologic-Projekt des deutschen Bundesministeriums für Wirtschaft, die Guides des Open Web Application Security Projects (OWASP), der Leitfaden "Sicheres Programmieren, Einführung in die sichere Anwendungsentwicklung" der Sicherheitsinitiative Deutschland sicher im Netz und weitere Dokumente von Unternehmen (siehe Hilfsmittel)

Zur Vorbereitung des Lastenheftes, insbesondere um die benötigten Sicherheitsfunktionen herzuleiten und auszugestalten, hat es sich als zweckmäßig erwiesen, bei Bedarf (d. h. insbesondere bei hohem oder sehr hohem Schutzbedarf) bereits eine erste Risikoanalyse, beispielsweise auf Grundlage der im BSI-Standard 100-3 beschriebenen Methode, durchzuführen. Diese erste Fassung der Risikoanalyse muss dann im Zuge der Erstellung des Pflichtenheftes (siehe M 2.552 *Erstellung eines Pflichtenheftes*), bei der Fertigstellung der Anwendung und der Vorbereitung der Freigabe fortgeschrieben werden. In dieser ersten Runde der Risikoanalyse kann natürlich nur untersucht werden, gegen welche Gefährdungen die Anwendung widerstehen können soll und erste Sicherheitsziele gesetzt werden. Konkrete Sicherheitsmaßnahmen können erst im Pflichtenheft festgelegt werden.

Das Lastenheft sollte so detailliert, wie in dieser Phase möglich, über die funktionalen (fachlichen) Anforderungen hinaus Aussagen zu folgenden nichtfunktionalen Aspekten enthalten:

- Qualitätsanforderungen (zum Beispiel Benutzerfreundlichkeit, Zuverlässigkeit, Performance),
- Vorgaben hinsichtlich der Architektur und IT-Infrastruktur, für die die Anwendung ausgelegt wird (siehe M 2.214 *Konzeption des IT-Betriebs*). Jede Institution sollte eine klar umrissene Vorgabe haben, wie IT in der Institution eingesetzt wird und zusammenspielt. Dies kann z. B. in einem IT-Rahmenplan und einem Architekturkonzept festgelegt sein. Bei der Planung neuer IT-Komponenten und Anwendungen ist sicherzustellen, dass diese in die Infrastruktur und die generellen Planungen passen.
- Weitere technische Anforderungen (zum Beispiel Anwendungsarchitektur, Programmiersprache, Betriebssystem, Erweiterbarkeit),
- Anforderungen an die Dokumentation (zum Beispiel Modellierung in UML),
- Vorgaben zur geplanten Einführung. Hier ist zu unterscheiden, ob es sich um eine Migration, bei der Daten und Bearbeitungsabläufe aus einer vorhandenen Anwendung übernommen werden oder um eine komplette Neuentwicklung handelt. Wichtig kann auch sein, ob die Einführung der neuen Anwendung mit einer Stichtagsumstellung oder durch schrittweise Einführung geplant ist. Wertvolle Hinweise zur Planung des Vorgehens bei der Migration von Anwendungen gibt in einem Phasenmodell der Migrationsleitfaden der Beauftragten der Bundesregierung für Informationstechnik.
- Anforderungen an die Abnahme (Grundsätzliches zu Abnahmetests und Pilotbetrieb).
- Vorgaben zu den benötigten Sicherheitsfunktionen

Diese Sicherheitsfunktionen können unter anderem beinhalten:

- Vorgaben für die Verfügbarkeit des Verfahrens (tolerable Ausfallzeiten, Wiederherstellungszeiten etc.)
- Anforderungen an die Mandantentrennung (siehe M 2.549 *Erstellung eines Mandantenkonzeptes*)
- Anforderungen an die Datensicherung (siehe M 6.33 *Entwicklung eines Datensicherungskonzepts*) und, falls erforderlich, zur Archivierung
- Anforderungen an externe Schnittstellen und deren Absicherung

- Anforderung an die Verschlüsselung der Datenhaltung und des Datentransports (siehe M 2.161 *Entwicklung eines Kryptokonzepts*)
- Anforderungen an Authentisierung und Autorisierung
- Anforderungen an die Datenhaltung und -strukturierung
- Anforderungen zur effizienten und effektiven Löschung von Daten

Das Lastenheft sollte die Anforderungen an die Anwendung so ausreichend beschreiben, dass hierauf aufbauend die Anwendung so erstellt werden kann, dass sich mit ihr die erforderlichen Sicherheitsmaßnahmen umsetzen lassen und sich eine dem Schutzbedarf angemessene Gesamtsicherheit erreichen lässt.

Prüffragen:

- Wurden bei der Erstellung des Lastenheftes fachliche Anforderungen, Vorgaben hinsichtlich der Architektur und IT-Infrastruktur, Vorgaben zur Einführung der Anwendungen und benötigte Sicherheitsfunktionen ausreichend berücksichtigt?

# M 2.549 Erstellung eines Mandantenkonzeptes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT

Häufig werden von mehreren Institutionen zentrale IT-Infrastrukturen oder Dienste eines Dienstleisters gemeinsam genutzt. Hierbei können auch Anwendungen gemeinsam betrieben und genutzt werden, wobei Datenhaltung und Datenverarbeitung z. B. infolge rechtlicher Anforderungen oder aufgrund von Betriebs- und Geschäftsgeheimnissen getrennt erfolgen müssen. In diesen Fällen wird häufig von mandantenfähigen Anwendungen gesprochen, wobei jeder nutzenden Institution ein Mandantenbereich, kurz Mandant, zugeordnet wird.

Ein Beispiel hierfür sind in der öffentlichen Verwaltung Registeranwendungen wie das ePersonenstandsregister, in denen mehrere Kommunen als eigenständige datenverarbeitende Stellen ihre Personenstandsdaten ablegen und verwalten. Cloud-basierende Anwendungen (auch als "Software as a Service", SaaS bezeichnet) sind ein weiteres Beispiel.

In jedem dieser Fälle ist durch ein geeignetes Mandantenkonzept sicherzustellen, dass die Anwendungen mandantenfähig betrieben werden. Dazu gehört, dass jede datenverarbeitende Stelle innerhalb ihres Bereichs, also ihres Mandantensystems, die fachlichen Vorgaben (z. B. bezogen auf Protokollierungsumfang und Speicherfristen) umsetzen sowie ihren Kontrollpflichten nachkommen kann. Das Mandantenkonzept ist durch den Betreiber der mandantenfähigen Anwendung zu erstellen und den nutzenden Institutionen zur Verfügung zu stellen. Diese müssen sich überzeugen, dass das Mandantenkonzept für ihren Schutzbedarf eine angemessene Sicherheit bietet, bevor sie solche Systeme oder Dienste gemeinsam mit weiteren Anwendern nutzen. Das Mandantenkonzept ist somit Bestandteil des Sicherheitskonzeptes, das für ein Outsourcingvorhaben zu stellen ist (siehe B 1.11 *Outsourcing*, insbesondere M 2.254 *Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben*).

Auch unter datenschutzrechtlichen Gesichtspunkten sind Anforderungen an die Trennung von Mandanten zu beachten. Hinweise dazu gibt die "Orientierungshilfe Mandantenfähigkeit" des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder.

Wenn eine Anwendung neu beschafft, erstellt oder wesentlich geändert wird, muss außerdem zunächst grundsätzlich sichergestellt sein, dass diese Anwendung Mandanten sauber trennen kann (siehe M 2.552 *Erstellung eines Pflichtenheftes*).

Ein Mandantenkonzept sollte mindestens folgende Punkte berücksichtigen:

- Geeignete Rechtsgrundlagen: Rechtliche Vorgaben dürfen einem gemeinsamen, mandantenfähigen Verfahrensbetrieb nicht entgegenstehen. Ferner muss sichergestellt werden, dass die technische Ausgestaltung der Mandantentrennung dem Schutzbedarf der Daten in den jeweiligen Mandanten entspricht.
- Die Abgeschlossenheit von Transaktionen: Datenverarbeitungsschritte, die in einem Mandanten durchgeführt werden, dürfen nicht dazu führen, dass die Daten in anderen Mandanten verändert werden oder lesend auf sie zugegriffen werden kann.

- Konfigurative Unabhängigkeit der Mandanten untereinander: Es sollten mindestens zwei administrative Ebenen vorhanden sein. Die erste Ebene dient der Mandantenadministration: Hier werden Mandantensysteme eingerichtet und gelöscht, mandantenübergreifende konfigurative Einstellungen durchgeführt, die Rollen der Mandantenadministratoren zugewiesen, die mandantenübergreifende Protokollierung angestoßen und deren Revision durchgeführt. Die zweite Ebene dient der Administration eines Mandantensystems: Hier werden die Berechtigungen im Mandantensystem vergeben, mandanteninterne Konfigurationen durchgeführt, die mandanteninterne Protokollierung konfiguriert und die Protokollrevision durchgeführt.
- Trennung von Berechtigungskontexten: Jeder Mandant hat seinen eigenen, abgeschlossenen Berechtigungskontext. Die Berechtigungen in einem Mandantensystem dürfen sich nicht in anderen Mandantensystemen auswirken. Die Vergabe oder Veränderung von Berechtigungen durch die Administratoren der jeweiligen Mandanten darf sich nicht auf Berechtigungen in anderen Mandanten auswirken.
- Es muss eine administrative Ebene zur Mandantenadministration seitens des Betreibers geben, die aber keine Berechtigung zur Verarbeitung von Daten innerhalb eines Mandanten besitzen sollte.
- Trennung von Protokollierungskontexten: Protokollrevisoren eines Mandatensystems dürfen keinen Zugriff auf Protokolldaten anderer Mandantensysteme haben. Beispielsweise können Mandanten eigene Log-Dateien haben. Eine andere Lösung könnte sein, dass eine Institution über vom Dienstleister entsprechend eingerichtete Filter oder Report-Generatoren auf die Protokolldaten ihres Mandanten zugreifen kann.
- Beschränkung der mandantenübergreifenden Datenverarbeitung: Die Ebene der Mandantenadministration sollte grundsätzlich keine Verarbeitung von Daten innerhalb eines Mandanten außerhalb der Mandantenadministration zulassen. Der Datenaustausch zwischen Mandanten sollte über definierte und geeignet abgesicherte Schnittstellen erfolgen (siehe Schnittstellenkonzept).

Die Umsetzung dieser Anforderungen kann auf vielfältige Weise erfolgen. Eine herausragende Rolle spielt dabei ein geeignetes Rollen- und Berechtigungskonzept innerhalb von Anwendungen. Darüber hinaus können auf der Infrastruktur- und Diensteebene hierzu z. B. Virtualisierungstechniken eingesetzt werden wie:

- Einsatz verschiedener Datenbanken (auch Instanzen genannt) in einem gemeinsamen Datenbankmanagementsystem (DBMS)
- VPD (Virtual Private Database) auf der Diensteebene bei Datenbanken
- Speicherung von mit einem Mandantenattribut versehenen Datensätzen in einer gemeinsamen Datenbank und gemeinsamen Tabellen, sodass die Mandantentrennung durch die Anwendung erfolgt.
- Virtuelle Maschinen auf der Systemebene
- VLAN (Virtual LAN), VRF (Virtual Routing and Forwarding), VPN (Virtual Private Network) in der Netzinfrastruktur (siehe auch M 5.62 *Geeignete logische Segmentierung*)

Der Auftraggeber sollte prüfen, ob die vom Dienstleister gewählte Lösung zur Mandantentrennung effektiv ist.

Prüffragen:

- Wurde konzeptionell berücksichtigt, dass Anwendungs- und Datenkontexte unterschiedlicher nutzender Institutionen sauber getrennt sind?

- Sind die benötigten Mechanismen zur Mandantentrennung beim Dienstleister ausreichend umgesetzt?
- Liegt ein geeignetes Sicherheitskonzept für das Outsourcing-Vorhaben vor?

# M 2.550 Geeignete Steuerung der Anwendungsentwicklung

**Verantwortlich für Initiierung:** Leiter Organisation
**Verantwortlich für Umsetzung:** Verantwortliche der einzelnen Anwendungen

Kann für einen bestimmten Einsatzzweck keine Standardsoftware beschafft werden, wird die Entwicklung von Individualsoftware erforderlich. Dies kann in der Institution selbst oder mithilfe externer Auftragnehmer erfolgen.

Neben wirtschaftlichen Aspekten ist eine geeignete Steuerung der Softwareentwicklung auch aus Sicherheitsgesichtspunkten wichtig, weil sie hilft, Fehler in Anwendungen und Sicherheitslücken zu vermeiden. Je früher Fehler und Sicherheitsrisiken identifiziert werden, desto einfacher ist es, diese zu beheben.

Für die Steuerung der Entwicklung und das Projektmanagement sollte ein geeignetes Steuerungs- und Projektmanagementmodell festgelegt werden, das den besonderen Gegebenheiten der Institution und den dort eingesetzten Methoden von Softwareentwicklungsprojekten Rechnung trägt. Dieses sollte die folgenden Aspekte berücksichtigen:

- Das für die Entwicklung vorgesehene Personal sollte über die notwendige Qualifizierung verfügen.
- Für die Steuerung der Erstellung und Pflege der Anwendungen sollte ein Gesamtprozess eingeführt werden, der alle Phasen des Lebenszyklus (Application Lifecycle Management, ALM) abdeckt. Dabei sollten geeignete Phasen der Softwareentwicklung berücksichtigt werden, um die notwendigen Aktivitäten entsprechend aufteilen und bearbeiten zu können (Geschäftsprozessmodellierung, Anforderungsanalyse, Softwaredesign, Implementierung, Test, Auslieferung etc.). Für die erfolgreiche Einführung des Gesamtprozesses hat sich die sorgfältige Beschreibung und Abgrenzung der benötigten Rollen und Funktionsträger als besonders wichtig erwiesen.
- Zur geordneten Durchführung des Anwendungsprojektes sollten die benötigten Voraussetzungen geschaffen werden. Diese beinhalten die Bestellung eines Projektleiters, die Besetzung der Rollen im beschriebenen Gesamtprozess und die Auswahl eines Vorgehensmodells für die Entwicklung, das für die jeweilige Institution sowie die Art und Größe des Softwareprojektes geeignet ist. Dies kann beispielsweise sequenzielles Durchlaufen der Phasen (Wasserfallmodell) oder iteratives Durchlaufen (Spiralmodell) vorsehen.
- Die Risiken bei der Softwareentwicklung sind zu bewerten und zu behandeln. Hierbei sind spezifische Sicherheitsrisiken zu berücksichtigen, die üblicherweise durch Einsatz von Sicherheitsfunktionen reduziert werden, und Risiken im Entwicklungsvorhaben selbst, wie unzureichende Dokumentation, unzureichende Qualitätssicherungsmaßnahmen, Überschreiten des Zeitplans etc.. Auch die Risiken im Entwicklungsvorhaben können sich mittelbar auf die Sicherheit der Anwendung auswirken, etwa wenn aus Zeitdruck Sicherheitsfunktionen nicht oder nur unzureichend implementiert werden.
- Es müssen die Qualitätsaspekte des Entwicklungsprozesses ausreichend berücksichtigt werden, die auch für die Gesamtsicherheit wichtig sind. So lässt sich beispielsweise gut dokumentierter und strukturierter Code

nicht nur einfacher warten, auch sicherheitsrelevante Probleme lassen sich schneller identifizieren.

Für die Entwicklung von Software haben sich eine Reihe von Vorgehensmodellen und Best Practices bewährt. Diese lassen sich grob in zwei Kategorien unterscheiden:

- Schwergewichtige Vorgehensmodelle: Diese haben einen formalen Charakter, verfolgen eher einen vorab festgelegten Plan und legen ein starkes Gewicht auf Verträge und Dokumentation. Sie eignen sich vor allem für große Projektteams oder bei einer sehr formalen Beziehung zwischen Auftraggeber und Auftragnehmer und setzen eine umfassende Anforderungsklärung zum Projektbeginn voraus. Bekannte Vertreter sind das V-Modell XT und der Rational Unified Process (RUP).
- Leichtgewichtige, agile Vorgehensmodelle: Sie setzen stärker auf die persönliche Interaktion der Projektbeteiligten und weniger auf die formale Durchführung und eignen sich für kleinere Projekte oder Projekte mit intensiver Beteiligung des Auftraggebers. Sie bieten die Möglichkeit, vage Anforderungen während des Projektverlaufs zu präzisieren oder auf Änderungen der Anforderungen flexibel zu reagieren. Beispiele für agile Vorgehensmodelle sind Scrum, Kanban, Crystal Clear.

Vorgehensmodelle lassen sich kombinieren: So können beispielsweise Arbeitsmethoden aus eXtreme Programming (Pair Programming) bei Scrum angewendet werden. Innerhalb eines V-Modell XT-Projektes können kleine Entwicklungszyklen als Scrum-Sprints angelegt werden.

Die für Softwareentwicklung relevanten Teilgebiete und Prozesse werden unter anderem beschrieben in:

- IEEE Software Body of Knowledge (SWEBOK) und
- ISO/IEC 12207 "Systems and software engineering - Software life cycle processes"

Auch für die Qualitätssicherung im Softwareentwicklungsprozess existieren verschiedene Vorgehensmodelle und -methoden. Dazu gehören unter anderem CMMI (Capability Maturity Model Integration) und SPICE (Software Process Improvement and Capability Determination) bzw. ISO/IEC 15504 "Information technology - Process assessment".

Ebenfalls relevant in diesem Bereich ist die Normenreihe ISO 250xx. Die Norm ISO/IEC 25000 "Software-Engineering - Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE) - Leitfaden für SquaRE" gibt einen Überblick über die Grundbegriffe und Prinzipien dieser Reihe.

Es muss festgelegt werden, welche Qualitätssicherungsmethode und welches konkrete Verfahren in der Institution oder für das jeweilige Projekt genutzt wird. Aus wirtschaftlichen Gründen sind in der Regel nicht alle Arten von Prüfungen in allen möglichen Tiefen möglich. Daher muss entschieden werden, welche davon zu welchem Zeitpunkt und für welche Teile der Anwendung sinnvoll sind. Dabei ist sicherzustellen, dass die Sicherheitsanforderungen ausreichend abgedeckt sind.

Prüffragen:

- Wurde für Entwicklungsvorhaben ein geeignetes Modell zur Steuerung festgelegt?
- Wurde für das Entwicklungsvorhaben ein Qualitätssicherungsverfahren genutzt, bei dem auch Sicherheitsaspekte ausreichend berücksichtigt werden?

# M 2.551 Durchführung eines geeigneten und rechtskonformen Vergabeverfahrens

**Verantwortlich für Initiierung:** Leiter Organisation
**Verantwortlich für Umsetzung:** Fachverantwortliche

Für ein Vergabeverfahren zur Beschaffung einer Standard- oder Individualsoftware kann es eine Reihe von Vorgaben geben, die zu beachten sind. Während dies im Bereich von Unternehmen meistens eigene Vorgaben oder Konzernrichtlinien sind, sind für die öffentliche Hand in Deutschland die folgenden Vorgaben zu berücksichtigen:

- Vergabeordnung der Länder und des Bundes (insbesondere die Vergabeordnung für Leistungen (VOL) und die Vergabeordnung für freiberufliche Leistungen (VOF)). Diese regeln detailliert, wie (zum Beispiel als Freihandvergaben, öffentliche Ausschreibungen etc.) und in welchen Schritten Vergabeverfahren durchzuführen sind.
- Mindestanforderungen der Rechnungshöfe zum Einsatz der Informations- und Kommunikationstechnik. Diese beschreiben die Vorgaben der Rechnungshöfe für Anwendungen, mit denen Mittel der öffentlichen Hand verwaltet werden.

Jede Institution sollte im Vorfeld von Beschaffungen geklärt haben, welche rechtlichen oder sonstigen Rahmenbedingungen dabei zugrunde zu legen sind. Für Beschaffungen und Auftragsvergaben sollte es definierte Prozesse und festgelegte Ansprechpartner in der Institution geben (siehe M 2.547 *Ermittlung und Dokumentation der Rechtsgrundlagen für Anwendungen*).

In jedem Falle ist es sinnvoll, frühzeitig zu klären, welche Rolle Zertifikate bei der Vergabeentscheidung spielen sollen. Dazu gehören Zertifikate, die die Sicherheit von Produkten bewerten wie die Common Criteria, solche, die die Managementsysteme bewerten, wie das Zertifikat "ISO 27001 auf Basis IT-Grundschutz", und auch Personenzertifikate (siehe M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*).

Prüffragen:

- Entsprechen Planung und Durchführung des Vergabeverfahrens den bestehenden Vorgaben?

# M 2.552 Erstellung eines Pflichtenheftes

**Verantwortlich für Initiierung:** Fachverantwortliche, Leiter Organisation
**Verantwortlich für Umsetzung:** Fachverantwortliche

Ein Pflichtenheft beschreibt, wie das Lastenheft technisch umgesetzt werden soll. In der Regel gibt der Auftraggeber, also z. B. die verantwortliche Fachabteilung, das Lastenheft vor. Darauf aufbauend erarbeitet die (interne oder externe) Entwicklungsabteilung, die die Anwendung erstellen soll, das Pflichtenheft, in dem die technische Umsetzung der Anforderungen des Lastenhefts ausformuliert wird. Das Pflichtenheft muss vom Auftraggeber daraufhin überprüft werden, ob alle Anforderungen aus dem Lastenheft so abgebildet werden, dass die angestrebten Entwicklungsziele erreicht werden können. Es ist sinnvoll, dabei das Sicherheitsmanagement mit einzubinden, um zu gewährleisten, dass die auch die formulierten Sicherheitsziele erreicht werden.

Dabei sind mindestens die folgenden Aspekte zu berücksichtigen:

**Beschreibung der fachlichen Anforderungen**

Es ist detailliert zu beschreiben, wie die fachlichen Anforderungen umgesetzt werden sollen (z. B. Workflows, Dialoge, Bearbeitungsmasken, Datenstrukturen).

**Einbettung in den Informationsverbund**

Es sollte im Pflichtenheft ausgearbeitet werden, wie sich die Anwendung in den Informationsverbund einpassen wird bzw. welche Anpassungen durchzuführen sind. Dazu ist beispielsweise zu klären, welche und wie viele Betriebsumgebungen (Entwicklung, Test, Qualitätssicherung, Produktion etc.) benötigt werden und wie sie infrastrukturell umgesetzt werden sollen (z. B. unter Nutzung virtueller Maschinen (VM) oder Terminalserver-Dienste).

**Planung der Einführung einer Anwendung**

Die Einführung der neuen Anwendung ist zu planen. Hierfür sind im Pflichtenheft unter anderem folgende Punkte zu berücksichtigen:

- Bevor eine Anwendung in den Echtbetrieb übernommen werden darf, muss sie getestet und freigegeben werden. Im Pflichtenheft sind mindestens die geplanten Abläufe und Kriterien für die Tests und Freigaben zu nennen. Es hat sich als zweckmäßig erwiesen, im Pflichtenheft zumindest die für eine erfolgreiche Freigabe kritischen Testszenarien zu beschreiben (siehe Test und Freigabe, M 2.83 *Testen von Standardsoftware* und M 2.62 *Software-Abnahme- und Freigabe-Verfahren*).
- Migration: Wenn durch die neue Anwendung eine bestehende Anwendung abgelöst wird, müssen Geschäftsprozesse und die IT-Umgebung angepasst und Datenbestände in die neue Anwendung migriert werden. Die Migrationsphase ist erfahrungsgemäß immer besonders sicherheitskritisch und muss sorgfältig vorbereitet und durchgeführt werden. Gegen Ende der Migrationsphase müssen auch die zugehörigen Daten in die neue Anwendung und die dort verwendeten Datenformate übertragen werden. Weitere Hinweise finden sich auch in M 2.319 *Migration eines Servers*. Wertvolle Hinweise zur Planung des Vorgehens bei der Migration von Anwendungen gibt der Migrationsleitfaden der Beauftragten der Bundesregierung für Informationstechnik.

**Sicherheitsfunktionen in der Anwendung:**

Es muss festgelegt werden, welche Sicherheitsfunktionen die Anwendung enthalten soll und wie diese realisiert werden sollen (siehe auch M 4.42 *Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung*). Diese können beinhalten:

- Verfügbarkeitskonzeption bzw. Redundanzkonzept (siehe M 6.157 *Entwicklung eines Redundanzkonzeptes für Anwendungen*)
- Mandantentrennung:
  Im Pflichtenheft muss ausformuliert werden, wie durch die Anwendung gewährleistet werden kann, dass die Mandanten sauber getrennt werden (siehe M 2.549 *Erstellung eines Mandantenkonzeptes*)
- Planung und Dokumentation des Einsatzes von Verschlüsselung, Checksummen und anderen kryptografischen Verfahren. Kryptografie kann bei geeigneter Einsatzkonzeption genutzt werden, um die Daten während des Transports innerhalb des der Anwendung, beim Transport über externe Schnittstellen und innerhalb der Anwendung gegen unbefugten Zugriff abzusichern.
  Die Planung und Umsetzung angemessener kryptographischer Verfahren ist eine komplexe Aufgabe, daher empfiehlt es sich, die Anforderungen und Überlegungen hierzu in einem Kryptokonzept zusammenzufassen, siehe M 2.161 *Entwicklung eines Kryptokonzepts*.
- Datensicherungskonzept (siehe M 6.33 *Entwicklung eines Datensicherungskonzepts*)
- Archivierungskonzept (siehe M 2.243 *Entwicklung des Archivierungskonzepts*):
  Bei der Archivierung ist darauf zu achten, dass alle Komponenten der Anwendung archiviert werden, die für eine eventuelle Wiederaufnahme des Betriebs erforderlich sind, also beispielsweise Software, Konfigurationsdaten und Inhaltsdaten. Unter Umständen kann es aber auch sinnvoll sein, Hardware-Komponenten zu archivieren, wie beispielsweise Authentisierungstoken. Das Archivierungskonzept sollte ein Rollenkonzept (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*), ein Authentisierungskonzept (siehe M 2.555 *Entwicklung eines Authentisierungskonzeptes für Anwendungen*), eine Konzeption der Softwarepflege (siehe M 2.553 *Entwicklung eines Pflegekonzeptes für Anwendungen*) und eine Konzeption der Nutzung und Absicherung der externen Schnittstellen beinhalten.

Des Weiteren sind die Anforderungen an Form, Sprache, Tiefe und ggf. auch die Auslieferungszeitpunkte der Quellcodedokumentation sowie an Aufbau, Inhalt und Format (Papier, PDF-Dokument, Online-Hilfe) der Handbücher zu formulieren.

Dabei ist zu beschreiben, welche der an der Einführung der neuen Anwendung beteiligten Institutionen (Auftraggeber, Dienstleister etc.) welche der beschriebenen Aufgaben wahrnimmt.

Außerdem sollte ein Protokollierungskonzept erstellt werden, in dem festgelegt wird, welche Ereignisse in der Anwendung auf welche Art protokolliert werden sollen und wie mit den Protokolldaten umgegangen wird (siehe M 2.500 *Protokollierung von IT-Systemen*). Dabei sind unter anderem die folgenden Aspekte zu berücksichtigen:

- Welche Ereignisse sollen wie protokolliert werden?
- Wie wird die Löschung nicht mehr benötigter Protokolldaten umgesetzt?
- Wie soll der Zugriff auf die Protokolldaten abgesichert werden? Ist eine revisionssichere Speicherung erforderlich?

- Sollen zur Unterstützung der Auswertung standardisierte Reports eingesetzt werden?
- Sollen bei bestimmten, protokollierten Ereignissen in der Anwendung weitere Ereignisse ausgelöst werden (Einsatz von Security Incident und Event Monitoring, SIEM)?

Da bei der Protokollierung immer auch personenbezogene Daten anfallen, müssen hierbei auch die Vorgaben des Datenschutzes berücksichtigt werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Prüffragen:

- Wurden bei der Erstellung des Pflichtenheftes fachliche Anforderungen sowie Vorgaben hinsichtlich der Architektur und IT-Infrastruktur, Vorgaben zur Einführung der Anwendungen und benötigte Sicherheitsfunktionen ausreichend berücksichtigt?

# M 2.553 Entwicklung eines Pflegekonzeptes für Anwendungen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Leiter IT

Soll eine individuell entwickelte Anwendung eingesetzt werden, wird für den Betrieb ein Pflegekonzept benötigt, um die Funktionsfähigkeit und Sicherheit der Anwendung im laufenden Betrieb sicherzustellen (siehe auch M 4.107 *Nutzung von Hersteller- und Entwickler-Ressourcen*). Dies sollte folgende Aspekte berücksichtigen, die in das Änderungsmanagement der Institution (siehe B 1.14 *Patch- und Änderungsmanagement*) eingebunden sein müssen:

- Neue oder geänderte fachliche Anforderungen müssen zeitnah in der Anwendung umgesetzt werden können.
- Im laufenden Anwendungsbetrieb auftretende funktionale Fehler (z. B. falsche Berechnungen bei unerwarteten Fallkonstellationen) müssen zeitnah bereinigt werden können.
- Die Kompatibilität zu Patchs und Updates der eingesetzten Betriebsumgebung, wie z. B. Betriebssysteme und Middlewarekomponenten wie Programmbibliotheken, Frameworks (z. B. .NET) und Runtime Environments (z. B. Java Runtime Environment, JRE) ist sicherzustellen. Idealerweise lassen sich Patchs bei diesen Komponenten unabhängig von der Anwendungssoftware separat einspielen. Ist das Patchen dieser Komponenten nur zusammen mit der Anwendung möglich, ist sicherzustellen, dass der Hersteller der Anwendungssoftware entsprechende Patchs für alle betroffenen Komponenten zeitnah bereitstellt. Es ist darauf zu achten, dass alle im Rahmen der Anwendung eingesetzten Softwarekomponenten Patchsupport durch die jeweiligen Hersteller haben. Komponenten, die vom jeweiligen Hersteller abgekündigt werden oder sind, sind zeitnah auszutauschen.
- Das zeitnahe Beseitigen von Sicherheitslücken in der Software selber ist vorzusehen.
- Es ist festzulegen, wie mit Prozessen für die Fehleranalyse oder zur Optimierung umzugehen ist. Hierzu können besondere Schnittstellen verwendet werden bzw. Zugriffe auf geschützte Daten erlaubt werden.

Zur geeigneten Vorbereitung von Tests (siehe M 2.83 *Testen von Standardsoftware*) und dem Einspielen von Änderungen in Anwendungen hat es sich als zweckmäßig erwiesen, zwischen Sicherheitspatchs und funktionalen Änderungen (sonstige Patchs und Updates) zu unterscheiden. Sicherheitspatchs dienen nur dem Schließen von Sicherheitslücken und sind in der Regel nicht mit funktionalen Änderungen in der Anwendung verbunden (vergleiche auch M 3.66 *Grundbegriffe des Patch- und Änderungsmanagements*). Daher können für Sicherheitspatchs Tests und Freigaben in vereinfachtem Verfahren durchgeführt werden (z. B. im Rahmen eines gestuften Roll-Outs im ersten Schritt an Pilotnutzer und durch generell erteilte Freigaben unter Datenschutz- und Sicherheitsgesichtspunkten).

Bei der Erstellung des Pflegekonzeptes sollte auch geklärt werden, über welche Wege Informationen über Sicherheitslücken, Updates und Patchs zur Verfügung stehen, z. B. Mailinglisten der Hersteller, Computer Emergency Response Teams (CERTs) (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*) und wie sie im eigenen Patch- und Änderungs-

prozess (siehe Baustein B 1.14 *Patch- und Änderungsmanagement*) bearbeitet werden.

Prüffragen:

- Ist die Pflege der Anwendung geeignet geregelt bzw. vertraglich vereinbart?
- Wurden neben funktionalen Änderungen auch Sicherheitspatchs in der Anwendung und den eingesetzten Middlewarekomponenten geeignet berücksichtigt?

# M 2.554 Geeignete Vertragsgestaltung bei Beschaffung, Entwicklung und Betriebsunterstützung für Anwendungen

**Verantwortlich für Initiierung:** Leiter Organisation
**Verantwortlich für Umsetzung:** Fachverantwortliche

Bei Beschaffung, Entwicklung oder Betrieb einer Anwendung kann sich eine Institution auf einen oder mehrere Dienstleister abstützen. Dies können interne oder externe Dienstleister sein. Typischerweise sind mindestens drei Parteien zu unterscheiden: die späteren Nutzer, Entwickler und Betreiber der Anwendung. Wird die Anwendung von Externen entwickelt oder betrieben, müssen geeignete vertragliche Rahmenbedingungen geschaffen werden.

Die Umsetzung der im Lasten- und Pflichtenheft sowie in den Teilkonzepten vorgegebenen, auch sicherheitstechnischen Eigenschaften einer Anwendung ist vertraglich mit den beteiligten Institutionen und Dienstleistern zu vereinbaren.

Hierbei sind unter Sicherheitsgesichtspunkten insbesondere die folgenden Aspekte zu berücksichtigen:

- Der Liefer- bzw. Leistungsumfang (Funktionsumfang einschließlich Sicherheitsfunktionen, Bereitstellungsformat, Lizenztyp, Dokumentation, Handbücher etc.) muss geeignet beschrieben werden.
- Es müssen Vereinbarungen über die Softwarepflege getroffen werden (siehe M 2.553 *Entwicklung eines Pflegekonzeptes für Anwendungen*). Bei Entwicklungen im Auftrag müssen geeignete Nutzungsrechte für den erzeugten Quellcode und Zugriff auf diesen vereinbart werden (siehe auch M 6.137 *Treuhänderische Hinterlegung (Escrow)*).

Beim Betrieb einer Anwendung durch einen Dienstleister sind die Maßnahmen aus dem Baustein B 1.11 *Outsourcing* zu berücksichtigen.

In der öffentlichen Verwaltung in Deutschland sind die "Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik" (EVB-IT) rechtlich vorgegeben (siehe auch § 9 Abs. 1 Satz 2 und § 11 EG Abs. 1 Satz 2 VOL/A und § 55 BHO). Diese enthalten sowohl Vertragsvorlagen für die Entwicklung als auch den Betrieb einer Anwendung durch einen Dienstleister.

Prüffragen:

- Werden bei der Gestaltung von Verträgen mit externen Dienstleistern zur Beschaffung, Entwicklung und Betriebsunterstützung von Anwendungen alle wichtigen Aspekte aufgelistet, bewertet und vertraglich berücksichtigt?

# M 2.555 Entwicklung eines Authentisierungskonzeptes für Anwendungen

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT

Im Zuge der Konzeption des Einsatzes einer neuen Anwendung sollte geklärt werden, wie sich Benutzer vor dem Zugriff auf die mit der Anwendung verarbeiteten Daten authentisieren. Im Authentisierungskonzept ist zu klären, ob die Anwendung überhaupt über Authentisierungsmechanismen verfügen soll (bei Bürokommunikationssoftware ist dies z. B. unüblich, da die Berechtigung auf Ebene der verarbeiteten Dokumente geregelt wird). Ist dies vorgesehen, ist zu klären, ob die Anwendung über eine eigenständige Benutzerverwaltung verfügt oder ob die Authentisierung über einen zentralen Verzeichnisdienst (siehe Baustein B 5.15 *Allgemeiner Verzeichnisdienst*) erfolgen soll. Kann ein Verzeichnisdienst genutzt werden, sollte geklärt werden, ob ein Single-Sign-On (SSO) vorgesehen ist.

Grundsätzlich sollte die Anbindung einer selbst entwickelten Authentisierung an einen Verzeichnisdienst oder SSO-Dienst vorgezogen werden. Ist dies nicht möglich, sollte in jedem Fall sichergestellt werden, dass Authentisierungsinformationen (Credentials, Kennwörter etc.) verdeckt eingegeben werden können und nicht ungesichert (d. h. unverschlüsselt) auf Datenträgern wie Festplatten gespeichert oder über Kommunikationsnetze übertragen werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Weitere, im Konzept behandelte Aspekte können sein:

- Vorgaben für ein Login-Banner: Beispielsweise ist es sinnvoll, bei einer Anmeldung den letzten Anmeldezeitpunkt und Nutzungshinweise anzuzeigen. Andererseits sollten Login-Banner nicht zu viele Informationen enthalten, vor allem keine, die Angreifern Ansatzpunkte liefern könnten, wie z. B. Netzadressen oder Art und Version der eingesetzten Software.
- Behandlung paralleler Sitzungen eines Benutzers in der Anwendung (wenn ja, wie viele sind erlaubt)
- Absicherung der Authentisierungsinformationen: Es ist festzulegen, wie die Speicherung und Übermittlung der Authentisierungsinformationen kryptographisch abgesichert wird.
- Zeitgesteuerte Zwangstrennung bei Untätigkeit des Benutzers sowie eine geeignete Information (Hinweisfenster) bei vollzogener automatischer Trennung und Abmeldung

Außerdem sollte die vorgesehene Art und Stärke der Authentisierungsmechanismen beschrieben werden. Hierbei sind insbesondere die in M 4.133 *Geeignete Auswahl von Authentikationsmechanismen* genannten Kriterien zu berücksichtigen:

- Art und Kombination der eingesetzten Techniken bzw. Faktoren zur Authentisierung (Wissen, Besitz, biometrische Merkmale)
- Stärke der eingesetzten Faktoren (beim Faktor Wissen siehe auch M 2.11 *Regelung des Passwortgebrauchs*)

Prüffragen:

- Wurden die Anforderungen an Funktion und Sicherheit der Authentisierung geeignet umgesetzt?
- Ist die Speicherung und Übermittlung von Authentisierungsinformationen kryptographisch ausreichend abgesichert?

# M 2.556 Planung und Umsetzung von Test und Freigabe von Anwendungen

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche

Für einen geordneten Betriebsübergang einer Anwendung und bei wesentlichen Änderungen ist ein geeignetes Vorgehen bei Test und Freigabe erforderlich. Für die Planung und Umsetzung von Tests sowie der darauf basierenden Freigabe sind üblicherweise vier Ebenen zu berücksichtigen, bei denen jeweils andere Funktionsträger mit ihrer fachlichen Perspektive einzubeziehen sind:

- die fachliche Ebene (Vertreten durch Fachverantwortliche)
- die Ebene des IT-Betriebs (Vertreten durch den IT-Leiter)
- die Ebene der Informationssicherheit (Vertreten durch den IT-Sicherheitsbeauftragten)
- die Ebene des Datenschutzes (Vertreten durch den Datenschutzbeauftragten)

Je nach Art und Komplexität einer Anwendung können noch weitere Funktionsträger benötigt werden, z. B. die Personalvertretung.

Für alle genannten Ebenen sind Test- und Überprüfungsszenarien sowie Kriterien für die Freigabe zu entwickeln. Hierbei sollte Berücksichtigung finden:

- Auf der fachlichen Ebene sollten die Maßnahmen M 2.62 *Software-Abnahme- und Freigabe-Verfahren* und M 2.83 *Testen von Standardsoftware* (diese Maßnahme ist auch auf Individualsoftware anwendbar) angewendet werden, die ein Vorgehen für Tests, Abnahme und Freigabe beschreiben.
- Der IT-Betrieb sollte sicherstellen, dass die Anwendung in die IT-Infrastruktur und die IT-Betriebsabläufe integriert werden kann.
- Die Anwendungskonzeption und der Anwendungsbetrieb müssen konform mit dem Regelwerk (Leitlinien, Richtlinien), den Konzepten (z. B. Kryptokonzept) und den Best Practices (z. B. OWASP) zur Informationssicherheit sein. Es ist insbesondere darauf zu achten, dass die benötigten Sicherheitsfunktionen umgesetzt wurden und einwandfrei funktionieren.
- Es muss geplant werden, dass, sofern notwendig, eine datenschutzrechtliche Freigabe eingeholt wird (siehe M 2.509 *Datenschutzrechtliche Freigabe*).

Die Ergebnisse der Tests bzw. Prüfungen sind zu dokumentieren und zu bewerten. Beispielsweise können Abweichungen und Fehler in drei Kategorien hinsichtlich ihrer Kritikalität (z. B. niedrig, mittel, hoch) bewertet werden. Auf Grundlage dieser Bewertung entscheidet der Freigabeverantwortliche über die Freigabe. Der Freigabeverantwortliche ist üblicherweise die Institutionsleitung oder ein von ihr beauftragter Funktionsträger. Die Freigabe ist geeignet zu dokumentieren, insbesondere sind rechtliche Vorgaben, z. B. zur Schriftform, zu berücksichtigen (siehe auch M 2.85 *Freigabe von Standardsoftware*).

Prüffragen:

- Sind die zur Freigabe von Anwendungen durchgeführten Tests dokumentiert und die Ergebnisse bewertet?

# M 2.557 Konzeption eines Schulungsprogramms zur Informationssicherheit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Damit ein Sicherheitskonzept in einer Institution etabliert werden kann, müssen die Mitarbeiter es akzeptieren, beachten und dauerhaft umsetzen. Wesentliche Erfolgsfaktoren hierfür sind auf die Institution zugeschnittene und sichtbar vom Management unterstützte Programme zur Sensibilisierung und Schulung zur Informationssicherheit.

Bei der Sensibilisierung zur Informationssicherheit geht es vor allem darum, ein Bewusstsein aller Mitarbeiter für Gefährdungen in ihrem Arbeitsumfeld zu schaffen bzw. es zu schärfen und daraus Verhaltensweisen abzuleiten, um Schäden vorzubeugen oder bestmöglich zu begrenzen (siehe M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit*). In Schulungen werden den Mitarbeitern ergänzend alle notwendigen Kenntnisse und Fähigkeiten vermittelt, um die angesprochenen Verhaltensweisen richtig durchzuführen. Der Begriff Schulung umfasst alle möglichen Formen der geplanten und überprüften Wissensvermittlung, z. B. Präsenzschulungen, Online-Lernprogramme, Einweisung durch verantwortliche Mitarbeiter oder Kenntnisnahme relevanter Regelungen und Verpflichtungen.

Sensibilisierung und Schulung ergänzen sich und sollten daher aufeinander abgestimmt entwickelt werden.

Es sollte ein Schulungsprogramm geben, das jeden Mitarbeiter in der Institution einbezieht, zielgruppenorientiert ist und auch die Mitarbeiterlaufbahn berücksichtigt (z. B. Funktions-, Abteilungs- oder Standortwechsel). Das Schulungsprogramm muss zwingend vom Management unterstützt werden, damit seine besondere Bedeutung erkennbar ist und die benötigten Ressourcen für Planung, Umsetzung und Aufrechterhaltung vorhanden sind (siehe M 3.96 *Unterstützung des Managements für Sensibilisierung und Schulung*).

Im Folgenden werden die wichtigen Schritte beschrieben, um ein Schulungsprogramm zur Informationssicherheit zu konzeptionieren.

**1. Definition von Schulungszielen**

Das Schulungsprogramm soll die Ziele der Informationssicherheit und die daraus resultierenden Maßnahmen bei allen Mitarbeitern der Institution verankern. Daher müssen die Schulungsziele aus den Informationssicherheitszielen abgeleitet werden.

Typische Ziele solcher Schulungsmaßnahmen können sein:

- Aufmerksamkeit und Interesse für Informationssicherheit gewinnen,
- Grundwissen zur Informationssicherheit vermitteln,
- spezielle Informationssicherheitskenntnisse vermitteln, die für Fachaufgaben der Mitarbeiter benötigt werden,
- Praxiswissen vermitteln, sodass Mitarbeiter in sicherheitskritischen Situationen richtig reagieren und

- dauerhafte Verhaltensänderungen erzielen, damit Mitarbeiter erkennen und akzeptieren, dass Richtlinien und Maßnahmen zur Informationssicherheit notwendig sind und sie diese in ihren Arbeitsalltag integrieren.

Außerdem sollten Erfolgskriterien für die Schulungsprogramme definiert werden, um deren Wirkung beurteilen zu können.

**2. Analyse von Zielgruppen**

Mitarbeiter mit vergleichbaren Anforderungen und Aufgaben in Bezug auf die Informationssicherheit sollten durch eine Zielgruppenanalyse identifiziert werden, um Schulungsmaßnahmen möglichst bedarfsgerecht, wirksam und konfektioniert gestalten zu können. Für genauere Empfehlungen zur Zielgruppenanalyse siehe Maßnahme M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*.

**3. Definition des Schulungsbedarfs für Zielgruppen**

Für zielgerechte Schulungsinhalte muss vorab der Schulungsbedarf pro Zielgruppe analysiert werden. Es ist festzulegen, wer in welcher Situation welche Kenntnisse haben sollte. Um den aktuellen Wissensstand von Zielgruppen zu evaluieren, können beispielsweise Fragebögen zur Selbsteinschätzung verwendet werden. Folgende Bereiche sollten auf jeden Fall berücksichtigt werden:

- Grundlagenwissen für alle Mitarbeiter,
- Managementebene zur Wahrnehmung der Vorbildfunktion für Informationssicherheit,
- Einarbeitung neuer Mitarbeiter,
- Spezialkenntnisse für bestimmte Gruppen wie z. B. Administratoren und Telearbeiter,
- Zusatzkenntnisse bei Wechseln zwischen den Zielgruppen.

**4. Ableitung von Schulungsinhalten**

Alle Mitarbeiter sollten die internen Regelungen, Konzepte und Verfahren zur Informationssicherheit kennen, die für ihren Arbeitsplatz relevant sind, und wissen, wo sie diese finden. Es ist wichtig, dass die Dokumentation zur Informationssicherheit einfach, überschaubar und allgemein verständlich gehalten ist.

- Die weitere inhaltliche Ausgestaltung der Schulungsmaßnahmen wird beschrieben in Maßnahme M 3.45 *Planung von Schulungsinhalten zur Informationssicherheit*.
- Inhalte zu Grundlagen der Informationssicherheit sind in den Maßnahmen M 3.26 *Einweisung des Personals in den sicheren Umgang mit IT* und M 3.5 *Schulung zu Sicherheitsmaßnahmen* spezifiziert.
- Für Inhalte zu Spezialthemen können die Maßnahmen M 3.45 *Planung von Schulungsinhalten zur Informationssicherheit* und M 3.49 *Schulung zur Vorgehensweise nach IT-Grundschutz* herangezogen werden. Wenn für die Trainingsmaßnahmen auf externe Veranstalter zurückgegriffen wird, können diese auch als Checkliste genutzt werden, um zu prüfen, ob vorkonfektionierte Seminare die benötigten Inhalte bieten.

Zur Vermittlung von Fähigkeiten gehören auch praktische Übungen, wie bestimmte Sicherheitsvorgaben im Arbeitsalltag eingehalten werden können. Ziel ist, dass sie sich mehr und mehr zur Selbstverständlichkeit entwickeln, statt ständig als unangenehmer Mehraufwand empfunden zu werden.

Die Schulungsmaßnahmen zur Informationssicherheit sind eng mit den sonstigen Schulungsmaßnahmen der Institution abzustimmen. Wo immer mög-

lich, sollten Informationssicherheitsthemen in bestehende Schulungen integriert werden, um auch dadurch zu fördern, dass Mitarbeiter das Thema als selbstverständlich wahrnehmen. Wenn nötig, müssen hierfür die bisherigen Dozenten zusätzlich qualifiziert werden. Des Weiteren muss Informationssicherheitsaspekten ausreichend Zeit innerhalb der Schulung eingeräumt werden.

**5. Entwicklung von Schulungsmodulen**

Ziel dieses Schrittes ist es, die Schulungsinhalte, inklusive geeigneter Medien und Methodik, bestmöglich zu konfektionieren. Dazu müssen anhand der entwickelten Schulungsinhalte entsprechende Module festgelegt werden. Außerdem ist zu definieren, wie die Module realisiert werden (siehe auch M 3.48 *Auswahl von Trainern oder externen Schulungsanbietern*), zum Beispiel durch:

- von eigenen Mitarbeitern durchgeführte Schulungen,
- von externen Lehrkräften durchgeführte Schulungen, die entweder speziell auf die Institution zugeschnitten (in der Regel innerhalb der Institution) sind oder im Rahmen des Angebots von Seminaranbietern (gegebenenfalls innerhalb der Institution) stattfinden,
- Einbettung in bereits vorhandene Schulungen oder
- die Erstellung von Schulungsunterlagen zum selbstständigen Lernen.

Als mögliche Medien und Methoden kommen infrage:

- klassische Präsenzschulung,
- Informationsbörse, Blog oder News zur Informationssicherheit im Intranet,
- Mitarbeiterzeitung,
- Zeitschriften mit sicherheitsrelevanten Themen,
- interne Informationsveranstaltungen,
- externe Seminare, Messen und Konferenzen,
- Videos, die Spezialthemen zur Informationssicherheit aufzeigen,
- E-Learning-Programme, Computer Based Training, Infotainment, Webinare und
- Planspiele zur Informationssicherheit (siehe M 3.47 *Durchführung von Planspielen zur Informationssicherheit*).

Alle bereits in der Institution vorhandenen Schulungsprogramme und -materialien sollten darauf untersucht werden, ob sie sich als erfolgreich erwiesen haben und als Vorbild übernommen werden können und ob Sicherheitsthemen in andere Programme integriert werden können.

Bei der Auswahl von E-Learning-Programmen sollte auch berücksichtigt werden, dass diese sich nicht negativ auf die Informationssicherheit in der eingesetzten IT-Umgebung auswirken. Wenn E-Learning-Angebote nicht nur im Intranet, sondern auch über das Internet präsentiert werden sollen, ist beispielsweise auf aktive Inhalte (Java, Javascript, ActiveX, etc.) zu verzichten. Grundsätzlich sollten E-Learning-Anwendungen wie jede andere Anwendung auch vor ihrem Einsatz getestet und nur freigegeben werden, wenn keine Sicherheitsbedenken bestehen (siehe B 5.25 *Allgemeine Anwendungen*).

**6. Festlegung von Schulungsplänen**

Für die verschiedenen Zielgruppen sollten Schulungspläne und dazu außerdem Zyklen bzw. definierte Zeitpunkte innerhalb der Mitarbeiterlaufbahn festgelegt werden, in denen bestimmte Module durchlaufen werden sollten. Die Schulungsmodule sollten um eine entsprechende Zeit- und Ressourcenplanung ergänzt und als Veranstaltung etabliert werden. Damit können die ver-

antwortlichen Führungskräfte Informationssicherheitsschulungen für ihre Mitarbeiter planen.

**7. Lernerfolgskontrolle**

Bei Schulungsmaßnahmen zur Informationssicherheit muss sichergestellt werden, dass die geplanten Schulungsziele bei den Teilnehmern auch erreicht werden. Andernfalls sind entsprechende Korrekturmaßnahmen vorzusehen.

Eine Lernerfolgskontrolle sollte sowohl während der Schulung nach wichtigen Schulungsabschnitten (z. B. durch gemeinsames Zusammenfassen und Fragen der Dozenten) als auch am Ende der Schulung und noch einmal nach einigen Wochen stattfinden (siehe dazu auch M 3.94 *Messung und Auswertung des Lernerfolgs*).

Die Institution sollte einen aktuellen und vollständigen Überblick über die Sicherheitskenntnisse ihrer Mitarbeiter haben, beispielsweise über Schulungsnachweise oder Personenzertifikate.

**8. Lernstoffsicherung und -aktualisierung**

Einmal erworbenes Wissen sollte kontinuierlich aufgefrischt werden. Wie schnell und intensiv das geschehen muss, ist abhängig von der Dynamik des Themas und dem Grad der praktischen Umsetzung des erworbenen Wissens. So machen es neue Techniken, aber auch neue Bedrohungen, Schwachstellen und mögliche Abwehrmaßnahmen erforderlich, Informationssicherheitswissen ständig aufzufrischen und zu erweitern. Das Schulungsprogramm muss diese Tatsache durch regelmäßige Auffrischungs- und Ergänzungsveranstaltungen für Mitarbeiter berücksichtigen. Weiterhin ist es wichtig, das gesamte Programm regelmäßig zu aktualisieren und es nötigenfalls an neue Gegebenheiten anzupassen (siehe hierzu auch M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit* sowie M 3.95 *Lernstoffsicherung*).

Prüffragen:

- Ist eine Zielgruppen- und Schulungsbedarfsanalyse für die Schulungsmaßnahmen zur Informationssicherheit durchgeführt worden?
- Werden bei den Schulungsprogrammen zur Informationssicherheit alle Mitarbeiter der Institution entsprechend ihren Aufgaben und Kenntnisse berücksichtigt?
- Werden die Inhalte der Schulungsmaßnahmen zur Informationssicherheit mit den sonstigen Schulungsmaßnahmen der Institution abgestimmt?
- Werden die Schulungsprogramme zur Informationssicherheit regelmäßig aktualisiert?

# M 2.558 Sensibilisierung der Mitarbeiter zur Informationssicherheit bei Mobiltelefonen, Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Zusätzlich zur allgemeinen Schulung und Sensibilisierung zur Informationssicherheit (siehe M 3.5 *Schulung zu Sicherheitsmaßnahmen* und M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*) müssen Mitarbeiter, die Mobiltelefone, Smartphones, Tablets und PDAs einsetzen, für die besonderen Aspekte der Informationssicherheit bei diesen Geräten sensibilisiert werden. Für die Schulungs- und Sensibilisierungsplanung sind daher die Mitarbeiter, die diese Geräte nutzen, gesondert zu erfassen und entsprechend diesem Plan zu schulen und zu sensibilisieren.

Mobiltelefone, Smartphones, Tablets und PDAs sind durch ihre geringe Größe und den vergleichsweise hohen Preis besonders gefährdet, verloren oder gestohlen zu werden. Eine Erhebung der Pointsec aus dem Jahre 2005 in einem großen Chicagoer Taxiunternehmen mit 900 Taxen ergab, dass in einem Zeitraum von sechs Monaten 85619 Mobiltelefone und 21460 PDAs in den Fahrzeugen liegen gelassen worden sind. Mitarbeiter sind daher besonders darauf hinzuweisen, diese Geräte nicht aus den Augen zu lassen und bei einem Verlust umgehend angemessene Maßnahmen wie Ortung, Löschung und Sperrung der Geräte selbst bzw. durch den IT-Betrieb zu veranlassen.

Mit dem Verlust des Gerätes sind, wenn weitere Sicherheitsmaßnahmen fehlen, auch die Daten auf dem Gerät verloren. Heutige Endgeräte können Datenmengen im zweistelligen Gigabyte-Bereich speichern, was ausreichend Platz für vertrauliche Geschäftsdaten, Preiskalkulationen, Adressbücher und E-Mails bietet. Deswegen müssen Sicherheitsmaßnahmen ergriffen werden, wie z. B. die vollständige Verschlüsselung aller Daten auf dem Endgerät und die Sperrung des Gerätes durch ein Passwort, nachdem es mehrere Minuten nicht benutzt wurde. Erfahrungsgemäß werden solche notwendigen Maßnahmen von den Mitarbeitern kritisch gesehen, da der Aufwand bei der Nutzung der Endgeräte steigt. Daher müssen die Mitarbeiter für die hier genannte Gefährdung der Informationssicherheit sensibilisiert und in der zusätzlichen Sicherheitsmaßnahme geschult werden.

Mobiltelefone, Smartphones und Tablets können in der Regel auf das Internet und auf E-Mails zugreifen. Mitarbeiter müssen die damit verbundenen Gefahren kennen: Das Gerät kann mit Schadsoftware infiziert werden. Schützenswerte Daten können vom Gerät gestohlen bzw. das Gerät kann zum Abhören von Raumgesprächen (siehe G 5.95 *Abhören von Raumgesprächen über Mobiltelefone*) und Telefonaten genutzt werden. Daher müssen die Geräte vor Schadsoftware geschützt werden, beispielsweise durch die Installation geeigneter Schutzsoftware. Zudem sollte überlegt werden, den gesamten Datenverkehr der Mobiltelefone, Smartphones oder Tablets über VPN durch einen Server der Institution zu leiten, um dort bereits Schadsoftware und Angriffe abzuwehren. Auch für diese Gefährdungen und die dadurch entstehenden Einschränkungen müssen die Mitarbeiter entsprechend sensibilisiert werden.

Da oft leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, sollten Institutionen prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die Abhörgefahren zu informieren und damit auch zu sensibilisieren.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen nicht ohne Weiteres telefonisch weitergeben sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*). Bei der Benutzung von Mobiltelefonen sollten sie außerdem darauf achten, dass vertrauliche Mitteilungen nicht in der Öffentlichkeit besprochen werden. Dies gilt insbesondere auch bei Kurzmitteilungen, die von einer vermeintlich bekannten Nummer abgesendet wurden (siehe G 5.192 *Vortäuschen falscher Anrufer-Telefonnummern oder SMS-Absender* (Spoofing)). Werden über Kurzmitteilungen oder Chats vertrauliche Informationen angefragt, sollte immer durch einen Rückruf überprüft werden, ob die Anfrage wirklich vom vorgegebenen Kommunikationspartner stammt. Eine solche Überprüfung sollte auch stattfinden, wenn unerwartet von einer bekannten Nummer ein Dateianhang oder ein Link geschickt wurde.

Immer wieder kursieren spektakuläre, aber falsche Warnmeldungen (siehe G 5.80 *Hoax*). Damit nicht wertvolle Arbeitszeit auf die Prüfung des Wahrheitsgehaltes solcher Nachrichten verschwendet wird, sollten alle Mitarbeiter schnellstmöglich über das Auftreten eines neuen Hoax informiert werden. Es gibt verschiedene Informationsdienste, die entsprechende Warnungen weitergeben.

Diese Sicherheitsmaßnahmen schränken den Komfort der Endgeräte in der Regel ein. So führt die vollständige Verschlüsselung zu einer längeren Wartezeit beim Einschalten des Gerätes, ein angemessenes Passwort laufend einzugeben, wird als störend empfunden und den kompletten Datenverkehr durch VPN durch einen Server der Institution zu leiten, führt zu längerer Wartezeit beim Surfen im Internet. Zudem erhöht jedes zusätzliche Sicherungsprogramm den Stromverbrauch und verkürzt damit die Akkulaufzeit. Diese Einschränkungen können daher dazu führen, dass die Mitarbeiter Sicherheitsmaßnahmen zu umgehen versuchen, weshalb im Rahmen der Sensibilisierung der Mitarbeiter besonders auf die Gefährdung der Informationssicherheit durch mobile Endgeräte wie Mobiltelefon, Smartphone oder Tablet eingegangen werden muss, damit die Maßnahmen auch dauerhaft wirksam sein können.

Prüffragen:

- Werden die Mitarbeiter für die besonderen Gefährdungen der Informationssicherheit durch Mobiltelefone, Smartphones, Tablets und PDAs sensibilisiert?
- Ist in der Sensibilisierungsplanung die Gruppe der Mitarbeiter mit Mobiltelefonen, Smartphones, Tablets und PDAs besonders berücksichtigt?

# M 2.559 Beschaffung von Windows 8

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Beschaffungsstelle

Aufgrund der gegenüber früheren Windows-Versionen gestiegenen Anforderungen oder Empfehlungen an die einzusetzende Hardware von Windows-8-Systemen, z. B. UEFI (Unified Extensible Firmware Interface) oder Secure Boot, ist es notwendig, vor der Beschaffung sowohl der Hard- als auch der Software den Einsatzzweck und die Einsatzvariante exakt zu planen.

Die offiziellen Windows Hardware Certification Requirements, früher als Windows Logo Requirements bekannt, spezifizieren die Anforderungen an Computer oder Komponenten, die das offizielle Windows-Logo tragen wollen. Im Rahmen dieser Anforderungen wird zwischen den Plattformen ARM und x86 unterschieden.

Während für ARM-Plattformen die Nutzung von UEFI und Secure Boot verbindlich umzusetzen ist, müssen Hersteller von x86-basierter Hardware die Deaktivierung des Secure Boot ermöglichen. Die Umsetzung dieser Vorgabe durch Microsoft ist bei der Auswahl geeigneter Hardware zu berücksichtigen.

Darüber hinaus sollte bei der Auswahl der Hard- und Software der Grad der Umsetzung der Empfehlungen des Eckpunktepapiers der Bundesregierung zu "Trusted Computing" und "Secure Boot" durch den jeweiligen Hard- oder Software-Hersteller berücksichtigt werden (siehe auch M 4.471 *Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8*).

Wenn die 64-Bit-Version der jeweiligen Edition genutzt werden soll, so sind die einzusetzende Hardware und die zu installierenden Applikationen auf 64-Bit-Kompatibilität zu überprüfen.

Grundsätzlich sind vier Editionen von Windows 8 verfügbar. Die beiden im Organisationsumfeld am häufigsten eingesetzten Editionen sind Pro und Enterprise.

| **Editionen von Windows 8** | **Zusammenfassung** |
|---|---|
| Windows RT 8.1 | Die RT-Version von Windows 8 wird zurzeit nur für ARM-Prozessoren angeboten. Sie ist auf Tablet-PCs vorinstalliert und wird nicht frei verkauft. |
| Windows 8.1 | Standardversion von Windows 8 für sogenannte Heimanwender. |
| Windows 8.1 Pro | Neben den Funktionen der Standardversion enthält diese Edition u. a. Funktionen wie Beitritt zu einer Domäne, BitLocker-Verschlüsselung oder Virtualisierung über die integrierte Hyper-V-Funktion |
| Windows 8.1 Enterprise | Zusätzlich zu den Funktionen der Pro-Edition sind in dieser Edition Funktionen wie Applocker, DirectAccess und Windows to Go integriert. |

| Editionen von Windows 8 | Zusammenfassung |
|---|---|
| | Enterprise-Versionen sind ausschließlich über Volumenlizenzen verfügbar. |

Weitere Details zu den Unterschieden der Editionen Pro und Enterprise finden sich in M 4.470 *Grundlagenwissen zu Windows 8*.

Von Windows RT abgesehen sind alle Editionen für 32- und 64-Bit-Prozessoren verfügbar.

Darüber hinaus können Anwender oder Institutionen aus dem europäischen Wirtschaftsraum und der Schweiz eine sogenannte N-Edition erwerben. Diese Edition ermöglicht es, die Anwendungen zur Wiedergabe und zur Verwaltung von z. B. DVDs oder digitalen Mediendateien frei auszuwählen. Sie entspricht ansonsten dem Funktionsumfang der jeweiligen zugrunde liegenden Versionen.

Bei der Beschaffung aus einem Volumenlizenzvertrag ist auch die notwendige Infrastruktur für die Aktivierung der Systeme entsprechend zu berücksichtigen. Dies gilt vor allem für die neu hinzugekommene Aktivierungsvariante ADBA (Active Directory Based Activation) zur Volumenaktivierung von Windows-8-Systemen.

Es gilt zu berücksichtigen, dass ältere Systeme wie Windows 7 oder Windows Server 2008 R2 nach wie vor auf den KMS-Dienst angewiesen sind. Der ausschließliche Betrieb einer ADBA-Aktivierung ist dadurch nur in einer reinen Windows-8- und Windows-Server-2012-Umgebung möglich (siehe M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

Prüffragen:

- Wurde vor der Beschaffung des Windows 8 Systems geprüft welche Editionen für den Einsatzzweck notwendig sind?
- Wurde geprüft, ob die Anwednungen die unter einer 64-Bit-Variante von Windows laufen sollen, 64-Bit fähig sind?
- Erfüllen die zum Einsatz kommenden Hardware-Plattformen die Anforderungen der Windows Hardware Certification Requirements?
- Stehen angemessene Verfahren für die Lizensierung, Aktivierung oder Re-Aktivierung der Systeme zur Verfügung?

# M 2.560 Integration eines SOA-basierten Need-to-share-Konzepts in das Sicherheitsmanagement

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Organisation

Führt eine Institution ein Need-to-share-Prinzip auf der Basis einer serviceorientierten Architektur (SOA) ein, ist eine Sicherheitskultur zu etablieren, die geprägt ist durch ein hohes Sicherheitsbewusstsein für die neue Technik bzw. Denkweise. Das Need-to-share-Prinzip bedingt, dass grundsätzlich mehr Informationen für alle Teilnehmer einer Kommunikation bereitgestellt werden.

Die Mitarbeiter müssen sich ihrer Verantwortung bewusst sein und ausreichend Kenntnisse über die möglichen Risiken haben, beispielsweise über unberechtigten Informationsabfluss. Hierzu muss ein geeignetes Sicherheitsbewusstsein erzeugt und vermittelt werden.

Dasselbe gilt, wenn ein bestehendes Need-to-know-Prinzip als Need-to-share-Prinzip auf alle Teilnehmer einer Informationsdomäne ausgeweitet wird. Bei allen Beteiligten muss auch hier das Sicherheitsbewusstsein etabliert sein, damit sie sich sachgerecht verhalten und Risiken vermeiden. Außerdem darf das Need-to-share-Prinzip nicht unmittelbar auf alle Need-to-know-Dokumente ausgeweitet werden.

Prüffragen:

- Unterstützen die Sicherheitsmechanismen in einem IT-System ein Need-to-share-Konzept?
- Sind Prozesse implementiert, die das für die Einführung des Need-to-share-Prinzips bzw. die Ausweitung des Need-to-know-Prinzips notwendige Sicherheitsbewusstsein fördern?

# M 2.561 Erstellen spezifikationskonformer SOA-Implementierungen und Konfigurationen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Implementierungen und Konfigurationen in serviceorientierten Architekturen (SOA) müssen spezifikationskonform zu Standards (z. B. WS-Security) sein. Dies ist mit geeigneten technischen Hilfsmitteln und organisatorischen Prozessen (z. B. Vier-Augen-Prinzip) sicherzustellen. Zudem sollten unerprobte oder wenig verbreitete Standards und Frameworks gemieden werden.

Da insbesondere auf dem Gebiet der serviceorientierten Architekturen die Technik schnell fortschreitet, ist eine kontinuierliche Weiterbildung hinsichtlich aktueller Standards, Protokolle, Architekturansätze und Techniken zwingend erforderlich.

Institutionen sollten möglichst standardisierte Netzprotokolle einsetzen, die auch für den entsprechenden Anwendungszweck entwickelt wurden und über integrierte Sicherheitsmechanismen verfügen.

Werden in einer Architektur Protokolle genutzt, die keine angemessenen Schutzmechanismen bereitstellen, sollten zusätzliche Techniken bzw. alternative Protokolle verwendet werden, um ein angemessenes Sicherheitsniveau zu gewährleisten. Insbesondere ältere Netzprotokolle sind häufig nicht genügend gegen Angriffe abgesichert. So verfügt zum Beispiel FTP (File Transfer Protocol) über keine Schutzmechanismen hinsichtlich der Authentizität, Integrität oder Vertraulichkeit von Nachrichten. Diese Funktionen müssen auf andere Weise bereitgestellt werden.

Es ist auch darauf zu achten, dass nur Schlüssellängen und kryptographische Verfahren eingesetzt werden, die ein ausreichendes Maß an Sicherheit bieten, z. B. SOAP mit SHA-512 und AES-256 (siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*).

# M 2.562 Regelung des Einsatzes von eingebetteten Systemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von eingebetteten Systemen gestellt werden. Diese Systeme müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden. Dafür müssen die folgenden organisatorischen Regelungen getroffen werden.

Es sind geeignete personelle Maßnahmen hinsichtlich Schulung, Benutzer-Support, Vertretungsregelungen, Verpflichtungen, Rollenzuteilungen festzulegen bzw. umzusetzen. Die Benutzer sollten im Umgang mit den von ihnen zu bedienenden eingebetteten Systemen bzw. Geräten mit eingebetteten Systemen regelmäßig geschult werden. Handbücher müssen im erforderlichen Umfang und in aktueller Version vorhanden sein.

Es müssen Verantwortliche für Firmware-Aktualisierungen, Wartungs- und Reparaturarbeiten, Protokollauswertung und für die Reaktion auf Sicherheitsverstöße und Fehlfunktionen benannt werden. Bei Ausfällen, Fehlfunktionen und bei Sicherheitsvorfällen muss klar definiert sein, was zu unternehmen ist. Alle Benutzer müssen über die entsprechenden Verhaltensregeln und Meldewege informiert sein.

Es sind Regelungen festzulegen, um die Integrität und Funktionsfähigkeit zu testen. Dabei sind Angaben z. B. zu den Intervallen, zur Vereinbarkeit mit dem Betrieb und zu den Verantwortlichen zu machen. Die Anforderungen an die physikalische Einsatzumgebung, wie z. B. der Luftfeuchtigkeits- und Temperaturbereich und die Energieversorgung, müssen festgelegt sein. Falls erforderlich sind dafür ergänzende Maßnahmen bei der Infrastruktur zu etablieren.

Für die Benutzer müssen die eingebetteten Systeme durch den Hersteller oder den Administrator so vorkonfiguriert sein, dass eine angemessene Sicherheit und Funktionalität erreicht werden kann. Die Konfiguration eingebetteter Systeme muss dokumentiert sein, damit sie nach einem Austausch, einer Aktualisierung oder um ein System wieder herzustellen entsprechend den Verfügbarkeitsanforderungen wieder eingerichtet werden kann.

Bei eingebetteten Systemen mit kryptografischen Anteilen sind weitergehende Regelungen in einem Kryptokonzept festzulegen.

Prüffragen:

- Sind Verantwortliche für den Betrieb des eingebetteten Systems festgelegt?
- Sind Benutzer und Administratoren ausreichend geschult im Umgang mit dem eingebetteten System bzw. dem Gerät, das ein eingebettetes System enthält?
- Sind alle Benutzer und Administratoren über Verhaltensregeln und Meldewege bei Ausfällen, Fehlfunktionen oder bei Verdacht auf einen Sicherheitsvorfall informiert?
- Sind Regelungen zum Test der Integrität und Funktionsfähigkeit festgelegt?
- Sind Anforderungen an die physikalische Einsatzumgebung festgelegt?

- Ist das eingebettete System sicher vorkonfiguriert und ist dies dokumentiert?

# M 2.563 Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Beschaffer

Schaltungen und Chips werden häufig von unterschiedlichen Institutionen funktional beschrieben und physisch produziert. Sowohl viele bekannte Chiphersteller als auch hochspezialisierte Kleinunternehmen sind sogenannte "fabless companies". Sie entwickeln Schaltungen und Chips, produzieren diese aber nicht selbst. Die Fertigung erfolgt durch darauf spezialisierte Firmen, sogenannte "silicon foundries", in der ganzen Welt, zumeist außerhalb von Europa. Die gefertigten Chips werden von dort direkt an die Kunden oder den Großhändler ausgeliefert. Auch die bekannten Distributoren sind weltweit verstreut.

Der Systemhersteller muss deshalb sicherstellen, dass die hergestellten Bauteile absolut genau der Spezifikation entsprechen, keine verdeckten Zusatzfunktionen enthalten und alle Qualitätsanforderungen einhalten. Bei der Lagerung, beim Zwischenhandel und während des Transports darf es nicht möglich sein, die programmierbaren Logikbausteine zu manipulieren oder Komponenten zu tauschen. In der Logistikkette sind dahingehend wirksame Kontrollen durchzuführen. Die Hersteller und Logistikunternehmen sollten nach anerkannten Standards zertifiziert sein.

Bei erhöhtem Schutzbedarf sind Hersteller und deren Subunternehmer zu qualifizieren, ob sie vertrauenswürdig sind Hard- und Software herzustellen. Der Nachweis ist zu dokumentieren. Eine Hersteller-Qualifizierung muss regelmäßig erneuert werden.

Bei allen mit der Entwicklung und Instandsetzung betrauten Fremdfirmen dürfen keine zu schützenden Informationen über das eingebettete System und die sich darauf befindlichen Daten nach außen gelangen. Hierzu ist ein IT-Sicherheitskonzept zu planen und umzusetzen. Die Mitarbeiter sind geeignet zu schulen und zu sensibilisieren. Es sind Regelungen zur Weitergabe von Informationen zu treffen. Vorfälle sind zu melden und zu kategorisieren. Nach einem Vorfall sind die Regelungen zu überprüfen und im Falle von Lücken oder zu weichen Forderungen entsprechend anzupassen. Seitens des Auftraggebers ist sicherzustellen, dass Fremdfirmen die Anforderungen des Sicherheitskonzeptes umsetzen.

Prüffragen:

- Ist sichergestellt, dass das eingebettete System keine manipulierten, gefälschten oder getauschten Komponenten enthält?
- Ist sichergestellt, dass das eingebettete System der Spezifikation entspricht und keine verdeckten Funktionen bei der Herstellung implementiert wurden?
- Ist sichergestellt, dass Unbefugte nicht an vertrauliche Informationen über das eingebettete System gelangen?
- Sind die beteiligten Unternehmen nachweisbar qualifiziert?

# M 2.564 Beschaffungskriterien für eingebettete Systeme

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Beschaffer

Eingebettete Systeme werden im Zuge der Entwicklung übergeordneter Systeme beschafft oder sie sind Teil von zu beschaffenden übergeordneten Systemen. Zusammen mit der reinen Hardware und Firmware können auch noch zusätzliche Komponenten und Leistungen beschafft werden.

Werden bei der Beschaffung eines eingebetteten Systems Fehler gemacht, so kann dies negative Folgen auf den sicheren Betrieb des übergeordneten Systems bzw. die sichere Durchführung einer Anwendung oder Fachaufgabe haben. Bevor ein eingebettetes System beschafft wird, muss daher eine Anforderungsliste erstellt werden, anhand derer die in Frage kommenden Systeme oder Komponenten bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das eingebettete System im praktischen Betrieb den Sicherheitsanforderungen genügt. Die Anforderungsliste sollte im Wesentlichen die im Folgenden dargestellten sicherheitsrelevanten Bereiche und Kriterien umfassen.

### Organisatorische Randbedingungen

Die folgenden Aspekte sollten bei der Beschaffung berücksichtigt werden:

- Kann ein effektiver Prozess zur Versorgung mit sicherheitsrelevanten Firmwareupdates etabliert werden?
- Informiert der Hersteller die betroffenen Stellen, wenn Sicherheitslücken bekannt werden?
- Bietet der Hersteller einen technischen Kundendienst an, der in der Lage ist, in einer vertretbaren Zeit Auskunft zu geben bzw. Fehlfunktionen zu beheben?
- Bietet der Hersteller Schulungen oder Handbücher zur Sicherheit des eingebetteten Systems an?

### Vorgaben aus dem Anwendungsgebiet

Das eingebettete System muss im jeweiligen Anwendungsgebiet geltenden Standards und Normen entsprechen, sowie, falls zutreffend, die Kriterien für eine produktspezifische Zulassung erfüllen. Derartige Zulassungen sind z. B. in den Bereichen Luftverkehr, Straßenverkehr und Medizintechnik üblich.

### Materielle Sicherheit

Wird das eingebettete System bei rauen Umweltbedingungen wie Feuchtigkeit, extremen Temperaturen, mechanischen Belastungen und Staub eingesetzt, muss es physikalisch robust sein. Es sollten keine oder nur wenige zuverlässige Steckverbindungen vorhanden sein. Empfindliche Komponenten sollten speziell gekapselt und mit Dämpfungsvorrichtungen versehen sein. Auf Bauteile mit beweglichen Komponenten sollte soweit wie möglich verzichtet werden.

### Ausfall- und Betriebssicherheit

Abhängig von der geforderten Verfügbarkeit sind an das eingebettete System Anforderungen zur Ausfallsicherheit, zur elektromagnetischen Verträglichkeit,

zu internen Überwachungs- und Selbsttestmechanismen und zum Wiederanlauf zu stellen.

**Prozessorarchitektur**

Die Bandbreite für Prozessorarchitekturen ist sehr groß. Neben Neuentwicklungen kommen, anders als im PC- oder Serverbereich, auch oftmals ältere Architekturen zum Einsatz. Gründe dafür sind die niedrigeren Kosten für den Prozessor selbst und die Möglichkeit das Anwendungsdesign, Programmcode und Entwicklungswerkzeuge sowie Debugtools wiederverwenden zu können. Es ist darauf zu achten, dass die gewählte Prozessorarchitektur geeignet ist, die notwendigen Sicherheitsfunktionen zu realisieren.

**Firmware-Speicher**

Die Firmware kann sich auf einem ROM, EPROM, EEPROM oder einem Flash-Speicher befinden. Beim Flash-Speicher kann ein Firmware-Update erfolgen, ohne dass der Chip ausgewechselt werden muss. Bei einem ROM muss meistens der gesamte Chip ausgewechselt werden, manchmal auch die gesamte Schaltung. Der Firmware-Speicher soll so realisiert sein, dass zusammen mit dem geplanten Wartungsprozess ein sicheres Update möglich ist.

**Betriebssystem und Anwendungssoftware**

Wird das eingebettete System zusammen mit einem Betriebssystemen und/ oder Anwendungssoftware beschafft, muss festgelegt werden, welche sicherheitsrelevanten Merkmale diese aufweisen sollen, z. B. hinsichtlich

- Sicherem Bootprozess
- Nutzung sicherer Kommunikationsprotokolle
- Sicherer Installation und Aktualisierung
- Absicherung von Zugang und Zugriff
- Benutzer- und Rechteverwaltung
- Protokollierung
- Alarmierung
- Integritätsschutz

**Entwicklungsumgebung**

Falls mit dem eingebetteten System auch eine Entwicklungsumgebung mit beschafft wird, ist darauf zu achten, dass diese neben der erforderlichen Funktionalität auch die nötigen Sicherheitseigenschaften aufweist. Beispielsweise dürfen bei den Schritten zur Codeerzeugung keine ungewollten Funktionen oder Hintertüren entstehen und die Entwicklungsumgebung sollte über Mechanismen verfügen, um selbst gegen Manipulationen geschützt werden zu können. Wenn möglich sollten zertifizierte Werkzeuge beschafft werden.

**Kriterien ohne direkten Sicherheitsbezug**

Kriterien wie z. B.

- Stromverbrauch,
- Grad der Integration,
- Signallaufzeiten,
- Erfüllung von Echtzeitanforderungen,
- Platzbedarf und
- Kosten

haben keine direkte Auswirkung auf die Informationssicherheit. Allerdings muss beachtet werden, dass die sicherheitsrelevanten Kriterien unter Umstän-

den anders bewertet werden, wenn die oben genannten Kriterien optimiert werden.

**Prüfsiegel und Zertifizierungen**

Für eingebettete Systeme bzw. generell für elektronische Komponenten existieren zahlreiche Prüfsiegel und Zertifizierungen. Wenn Anforderungen hierzu in die Beschaffungskriterien mit einfließen, muss beachtet werden, dass es auch gefälschte, qualitativ minderwertige und irreführende Ausprägungen davon gibt.

Prüffragen:

- Werden bei der Beschaffung eines eingebetteten Systems Aspekte der materiellen Sicherheit ausreichend berücksichtigt?
- Werden bei der Beschaffung eines eingebetteten Systems Anforderungen an die Sicherheitseigenschaften der Hardware ausreichend berücksichtigt?
- Werden bei der Beschaffung eines eingebetteten Systems Anforderungen an die Sicherheitseigenschaften der Software ausreichend berücksichtigt?
- Werden bei der Beschaffung eines eingebetteten Systems Sicherheitsaspekte der Entwicklungsumgebung ausreichend berücksichtigt?
- Werden bei der Beschaffung eines eingebetteten Systems organisatorische Sicherheitsaspekte ausreichend berücksichtigt?

# M 2.565 Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Grundsätzlich sind sicherheitsrelevante Ereignisse im Betrieb des eingebetteten Systems zu dokumentieren. Die technischen Möglichkeiten dazu können bei unterschiedlichen Arten eingebetteter Systeme und deren Umgebung stark variieren. Mögliche Ausprägungen, Funktionalitäten und Parameter sind:

- Protokollierung in einen nicht flüchtigen Speicher, kumulativ durch unterschiedliche Prozesse,
- Datenaufzeichnung in einfachen, formatierten Textdateien, z. B. CSV oder XML,
- Aufzeichnung von Prozessdaten über Datenlogger, im Zeittakt, ereignisgesteuert oder bei Änderungen,
- Strukturierte Speicherung der Ereignisse in einem Datenbanksystem,
- Echtzeitüberwachung mit Information eines Anwenders und der Möglichkeit einer Interaktion zur Laufzeit,
- Protokollierung aller oder konfigurierbarer Zustands- und Transitionsänderungen,
- Variablenablaufverfolgung, z. B. Audit Trails,
- Statistische Auswertung in Berichtsform oder als grafische Darstellung und
- Korrelation, Bewertung.

Soweit möglich, sollten bei eingebetteten Systemen zumindest Sicherheitsverstöße protokolliert werden, wie versuchter und durchgeführter unautorisierter Zugang und Zugriff. Insbesondere sind die Aktivitäten von privilegierten Benutzern zu überwachen, wie z. B. Technikern und Administratoren. Dadurch kann zwar der Missbrauch von Rechten nicht verhindert werden, es ist aber die Voraussetzung, um gezielt Schwachstellen zu schließen. Daneben wirkt sich die Protokollierung, zumindest hinsichtlich des Risikos entdeckt zu werden, abschreckend auf potentielle Täter aus.

Ist eine elektronische Protokollierung wegen konzeptioneller Einschränkungen durch die begrenzten Ressourcen nicht oder nur sehr begrenzt realisierbar, sollten organisatorische Regelungen geschaffen werden. Zum einen sollten alle Arbeiten an einem eingebetteten System mit Angaben zu Ort, Zeit, Ausführendem sowie Art und Grund der Tätigkeit in einem Logbuch festgehalten werden. Zum anderen sollten alle Ausfälle, offensichtliche Zugangs- und Zugriffsverletzungen und sonstige Auffälligkeiten im Logbuch dokumentiert werden. Die Einträge sollten regelmäßig und anlassbezogen ausgewertet werden.

Sowohl automatisch erzeugte Protokolle als auch Aufzeichnungen durch das Personal sind gegen unerlaubte nachträgliche Veränderung zu schützen. Nur dezidiert Berechtigte dürfen auf die Protokolle zugreifen können. Soweit technisch möglich, sind Vorkehrungen zu treffen, dass die Protokolldaten auch nicht von privilegierten Nutzern gelöscht oder geändert werden können, z. B. durch Speicherung auf nicht wiederbeschreibbaren Datenträgern oder mittels elektronischer Signatur. Datenträger mit Protokolldaten sind sicher zu verwahren und die beteiligten Personen sind über den korrekten Umgang zu belehren.

Prüffragen:

- Werden sicherheitsrelevante Ereignisse automatisch protokolliert?
- Enthalten die Protokolle die benötigten Informationen in geeigneter auswertbarer Darstellung?
- Können die Protokolle in einem sinnvollem Maße (manuell) ausgewertet werden, sofern die Notwendigkeit besteht?
- Existieren organisatorische Regelungen zur Protokollierung?
- Werden die Protokolle in sinnvollem Umfang ausgewertet?
- Sind die Protokolle gegen unerlaubten Zugriff und Manipulation geschützt?

# M 2.566 Sichere Aussonderung eines eingebetteten Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bevor ein eingebettetes System ausgesondert wird, sind alle auf Datenträgern vorhandenen bzw. permanent gespeicherten Daten so zu löschen, dass sie nachträglich auch nicht durch spezielle Software lesbar wiederhergestellt und missbräuchlich verwendet werden können. Ist es nicht möglich, die Daten sicher zu löschen, sind die betreffenden Datenträger sicher zu vernichten. Grundsätzlich gelten die Empfehlungen in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* aus B 1.9 *Hard- und Software-Management* und B 1.15 *Löschen und Vernichten von Daten*:

- Bei magnetischen Festplatten ist der gesamte Datenträger mit einem Zufallszahlenmuster zu beschreiben und der Vorgang zu verifizieren.
- Bei flüchtigen Halbleiterspeichern, z. B. SRAM oder DRAM, ist zum Löschen die Stromversorgung auszuschalteten und, wenn vorhanden, vorher die Pufferbatterie zu entfernen.
- Bei flüchtigen Halbleiterspeichern, z. B. SRAM oder DRAM, mit sehr hohem Schutzbedarf ist der Speicher mit beliebigen Daten einmal zu überschreiben, bevor die Stromversorgung ausgeschaltet wird.
- Bei nichtflüchtigen Halbleiterspeichern, z. B. EPROM, EEPROM oder Flash, ist bei hohem Schutzbedarf der gesamte Speicherbereich mit geeigneter Software dreimal zu überschreiben.

Abhängig von der Art des eingebetteten Systems und des Schutzbedarfs der gespeicherten Daten sind weitergehende Aktionen nötig:

- Festplatten sind mit einem für den Schutzbedarf zugelassenen Verfahren zu löschen bzw. physisch zu zerstören.
- Festplatten mit Halbleiterspeicher, SSD oder Hybridformen, sind physisch zu zerstören.
- Wenn bereits die Architektur bzw. eine teilweise in Hardware realisierte Programmierung eine schützenswerte Information darstellt, sind diese Komponenten physisch zu zerstören.
- Chipkarten sind physisch zu vernichten. Dazu können sie z. B. zerkleinert oder eingeschmolzen werden. Nähere Anforderungen an Einrichtungen zur Vernichtung von Informationsträgern enthält die DIN 66399 "Büro- und Datentechnik Vernichtung von Datenträgern". Diese Norm unterscheidet sieben Sicherheitsstufen bei der Vernichtung und berücksichtigt bei der Festlegung den Grad der Schutzwürdigkeit von Informationen, die physikalischen Eigenschaften von Informationsträgern und die zur Anwendung kommenden technischen Verfahren.

Eingebettete Systeme, auf denen sensible Informationen abgespeichert sind, sollten bei hohem Schutzbedarf über eine Notlöschfähigkeit verfügen. Wenn diese Funktion initiiert wird, müssen alle eingestuften Informationen zuverlässig entfernt werden. Falls das System dazu physisch zerstört werden muss, kann, wie in M 4.487 *Tamper-Schutz (Erkennung, Verhinderung, Abwehr) bei eingebetteten Systemen* beschrieben, eine Thermitreaktion vorgesehen werden.

Sofern eine zentral ausgelöste, automatische Notlöschprozedur des umgebenden Systems, z. B. Central Clear, Crash Clear, besteht, muss die Notlöschfunktion des eingebetteten Systems integrierbar sein. Hierfür sind entsprechende Schnittstellen vorzusehen.

Falls erforderlich, kann auch eine automatische Notlöschung, die aktiv alle sensitiven Daten löscht oder vernichtet implementiert werden.

Wenn Datenträger bei ausgesonderten eingebetteten Systemen gelöscht oder vernichtet werden und wenn Hardware vernichtet wird, ist dies zu dokumentieren.

Prüffragen:

- Werden sämtliche Daten auf dem eingebetteten System vor der Aussonderung sicher gelöscht?
- Wird die Hardware des eingebetteten Systems vor der Aussonderung sicher zerstört?
- Verfügt das System über eine angemessene Notlöschfähigkeit?
- Werden die Löschung oder Vernichtung dokumentiert?

# M 2.567 Auswahl vertrauenswürdiger Entwicklungswerkzeuge

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Beschaffer, Entwickler

Wenn Hardware oder Software für Systeme entwickelt werden, wird für gewöhnlich eine Reihe von Werkzeugen eingesetzt. Dabei handelt es sich oft um mächtige, grafikbasierte Entwicklungstools. Diese sind hochintegriert und verbinden Anforderungsmanagement, graphischen Entwurf und Codeerzeugung. Des Weiteren wird ihre Datenbasis als Grundlage automatisierter Tests verwendet. Durch die hohe Automatisierung der Prozessschritte von der Idee zum Code wird dem Werkzeug bzw. den Werkzeugen potenziell ein hoher Grad an Autonomie überlassen. Entwicklungswerkzeuge müssen daher fehlerfrei sein und dürfen nicht unerkannt manipuliert werden können, da sonst auch die Hardware und Software des Zielsystems gefährdet sind. Die Entwicklungswerkzeuge dürfen nicht dazu missbraucht werden können, verdeckte Hintertüren oder Schwachstellen einzubauen. Entwicklungswerkzeuge der Systemhersteller müssen entsprechend dem Schutzbedarf der zu entwickelnden Funktion bzw. der damit verarbeiteten Informationen qualifiziert werden. Hierzu hat der Hersteller dem Auftraggeber eine Tool-Richtlinie vorzulegen, welche die wesentlichen Sicherheitsanforderungen an das Werkzeug, die vorgesehene Tool-Landschaft, Einkaufsrichtlinien und die Qualifizierungsmaßnahmen enthält. Diese Tool-Richtlinie ist bei beschafften Werkzeugen von Seiten des Auftraggebers separat zu überprüfen.

Compiler übersetzten Codes, sie wandeln den Code einer Hochsprache in einen Zwischencode oder Maschinencode um. Ein Assembler ist auch als ein Compiler anzusehen, wobei er eine hardwarenahe Sprache in Maschinencode übersetzt. Cross-Compiler werden normalerweise verwendet, weil die Computerarchitektur des übersetzenden Systems nicht die gleiche ist, wie die des eingebetteten Systems. Dabei läuft der Compiler nicht auf dem Zielsystem, sondern beispielsweise auf einem Standard-PC und erzeugt dort den Code, der auf das Zielsystem geladen wird.

Die Programmiersprache Java spielt derzeit (Stand 2015) eine zunehmende Rolle bei der Softwareentwicklung. In Java geschriebene Programme werden zunächst in maschinenunabhängigen Bytecode übersetzt. Diesen interpretiert dann ein Interpreter auf der jeweiligen Hardware. Moderne Interpreter sind auf eine hohe Ausführungsgeschwindigkeit hin optimiert. Bei der modellbasierten Entwicklung werden Eigenschaften und Verhalten eines Systems mittels Modellierungssprachen oder graphischer Modelle spezifiziert. Aus diesen wird anschließend der Code in einer Hochsprache generiert. Mit Debuggern bzw. Cross-Debuggern werden Fehler in der Hardware und Software gefunden, wobei zum Debugging auch zusätzliche Hardware und Software eingesetzt werden kann. Einige Hersteller bieten für ihre Mikrocontroller komplette Pakete zur Systementwicklung an, sogenannte System Design Kits. Diese bestehen meist aus einer prototypischen Hardware mit Platine, Mikrocontroller, Schnittstellen und Peripherie sowie einem Software Development Kit, mit dem sich Software für diesen Mikrocontroller erstellen lässt. Das Software Development Kit läuft typischerweise auf einem handelsüblichen PC, der über eine Debug-Schnittstelle z. B. gemäß IEEE-Standard 1149.1 mit der Prototypenplatine verbunden wird.

Prüffragen:

- Werden zur Entwicklung des Systems nur Werkzeuge mit nachgewiesenen Sicherheitseigenschaften verwendet?
- Ist sichergestellt, dass die Werkzeuge nicht manipuliert werden können?
- Werden an den Hersteller von Hardware oder Software hinreichende Anforderungen zur Sicherheit seiner Werkzeuge gestellt?

# M 2.568 Testverfahren für Software

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter IT
**Verantwortlich für Umsetzung:** Tester

Um die Qualität von Software zu sichern, existieren statische Verfahren, bei denen das Programm nicht ausgeführt wird, und dynamische Verfahren während der Laufzeit.

### Statische Verfahren

Bei statischen Verfahren wird der Programmcode verifiziert. Bedeutende statische Verfahren sind Code Reviews und die automatische statische Code Analyse.

### Code Reviews

Bei der Entwicklung von Systemen sollten Code Reviews stattfinden, da es hardwareabhängige Fehler gibt, die nur so mit vertretbarem Aufwand gefunden werden können. Der Aufwand dafür sollte sich am Schutzbedarf und am Kosten-Nutzen-Verhältnis orientieren. Eine einfache, wenig formale Variante ist ein sogenannter Walkthrough, in dem der Autor schrittweise sein Gewerk präsentiert und die Teilnehmer Rückmeldungen geben. Bei höheren Sicherheitsanforderungen sollte eine formale Code-Inspektion durchgeführt werden. Beide Arten können auch als Peer Reviews durchgeführt werden. Dabei ist neben dem Autor nur ein weiterer, hierarchisch gleichgestellter Mitarbeiter beteiligt. Peer Reviews senken die Kosten und bringen oft nur einen vertretbaren Sicherheitsverlust mit sich. Reviews sollten sich an einer Checkliste orientieren, die z. B. folgende Fragen enthalten kann:

- Können Feld-Indizes überlaufen?
- Sind alle Variablen im richtigen Kontext definiert?
- Ist die Bit-Breite der Variablen ausreichend?
- Werden arithmetische Überläufe erkannt und behandelt?
- Werden bekannte fehlerträchtige Konstrukte vermieden?

### Automatische statische Code Analyse

Zur automatischen statischen Code Analyse sind Werkzeuge mit einer großen Preisspanne am Markt. Es gibt sowohl kostengünstige als auch hochpreisige Werkzeuge. Kostengünstige Werkzeuge können bereits eine Vielzahl an Analysemethoden aufweisen und z. B. den Kontroll- und den Datenfluss analysieren, nach nicht initialisierten Variablen suchen und Zahlenwerte verfolgen. Neben den zusätzlichen Analysemöglichkeiten liegen die Vorteile der hochpreisigen Systeme darin, dass sie besser bedienbar sind und deutlich weniger false positives erzeugen. Einen Hinweis auf die Qualität von Code können auch Code Metriken geben, wie z. B. die Verschachtelungstiefe, die Anzahl dynamisch erzeugter Objekte oder die Kommentardichte.

### Dynamische Verfahren

Beim dynamischen Verfahren wird das fertige Programm oder Teile davon validiert. Dabei wird die zu testende Software mit systematisch festgelegten Testdaten ausgeführt. Testdaten bestehen aus Vor- und Nachbedingungen und bilden mit der zu testenden Funktion einen Testfall. Beim Testen sollen vor allem Programmfehler erkannt werden, die in Abhängigkeit von dynami-

schen Laufzeitparametern auftreten, wie z. B. Sensordaten oder Nutzer-Interaktionen. Allgemein sind die Phasen beim Testen wie folgt gegliedert:

- Herstellung der Vorbedingungen des Testfalls
- Ausführung des Programms oder der Teilfunktion des Testfalls
- Vergleich des erwarteten Werts mit dem tatsächlich gelieferten Wert und Überprüfung der Nachbedingungen
- Abbau des Testfalls

Dabei kann bereits während der Entwicklung des Software-Designs parallel mit dem Test-Design begonnen werden. So kann die Testphase verkürzt werden und es können Testfälle identifiziert werden, für die spezielle Test-Hardware benötigt wird. Dynamische Tests können beginnen, wenn die ersten Module der Software fertig gestellt sind. Anstatt Testfälle erst zum Schluss festzulegen, können Testfälle auch vor der Implementierung angelegt werden und steuern auf diese Weise die Entwicklung maßgeblich. Dieses Vorgehen wird testgetriebene Entwicklung (englisch: Test-Driven-Development, TDD) genannt.

Tests können auf unterschiedlichen Arten hergeleitet werden. Grundlegende Kategorien sind

- spezifikationsorientierte Verfahren, sogenannte Black-Box-Tests, und
- strukturorientierte Verfahren, sogenannte White-Box-Tests.

Tests haben verschiedene Ebenen der Granularität und Ausführungsreihenfolge. Die übliche Reihenfolge, in der Software getestet wird, ist:

- Komponententest
- Integrationstest
- Systemtest

Dabei hat der Komponententest die niedrigste Granularität und der Systemtest die höchste. Es sollten auch alle Komponententests abgeschlossen sein, auf die ein Integrationstest aufbaut. Das Gleiche gilt für Systemtests. Ein weiterer wichtiger Aspekt ist, wie Tests ausgeführt werden.

**Black-Box-Test**

Bei einem Black-Box-Test wird der Testgegenstand gegen seinen im Design spezifizierten Zweck getestet. Neben der erwarteten Funktionalität ist das Verhalten bei ungewöhnlichen Eingaben zu testen. Da fast nie alle möglichen Eingaben und Ausgaben getestet werden können, sind Äquivalenzklassen zu bilden. Diese sollten so eingeteilt werden, dass der Tester davon ausgeht, dass sich die jeweiligen Eingaben aus einer Äquivalenzklasse gleich verhalten. Tests sind verstärkt mit den Grenzwerten einer Äquivalenzklasse durchzuführen, also z. B. den betragsgrößten und -kleinsten negativen und positiven Werten. Auch der Wert Null und Werte in seiner Umgebung sollten getestet werden.

**White-Box-Test**

Bei White-Box-Tests werden die Testfälle aufgrund des Softwarequellcodes bestimmt. Sie können grob unterteilt werden in komplexe, in der Praxis nicht weit verbreitete datenflussorientierte Methoden und kontrollflussorientierte Methoden. Bei letzteren hängt die Aussagekraft von der Testabdeckung ab. Diese ist definiert als der prozentuale Anteil von Einheiten wie z. B. Anweisungen und Zweige einer Software, der durch Tests bereits ausgeführt wurde. Unterschiedliche Grade der Testabdeckung werden mit Überdeckungstests erreicht, die auf Grund der geringeren Größe der Testobjekte besonders für

Komponententests geeignet sind. Die gebräuchlichsten Metriken dafür sind, sortiert nach zunehmender Strenge:

- Anweisungsüberdeckung (statement coverage): Die einfachste Metrik zur Testabdeckung prüft welcher Anteil der Programm-Statements ausgeführt wurde. 100% Anweisungsüberdeckung gilt als relativ schwacher Nachweis und genügt höchstens bei Systemen mit geringem Schutzbedarf.
- Zweigüberdeckung (branch coverage): Es wird geprüft, ob bei jeder Verzweigung jede Option mindestens einmal durchlaufen wurde.
- Verzweigungs- und Bedingungsabdeckung (decision and condition coverage): Zusätzlich zur Zweigüberdeckung wird eine Änderung jeder Teilbedingung eines Booleschen Ausdrucks gefordert.
- Modifizierter Bedingungs-/Entscheidungsüberdeckungstest (modified decision and condition coverage): Jede der Teilbedingungen, die auf eine Verzweigung Einfluss haben kann, muss zeigen, dass sie unabhängig von den anderen den Programmfluss bestimmen kann.

**Komponententest**

Komponententests beziehen sich auf die kleinsten sinnvoll isoliert testbaren Einheiten. Sie können als Black-Box- und/oder White-Box-Tests durchgeführt werden. Komponententests sollten auf dem Zielsystem ablaufen, da es nur dadurch möglich ist, Compilerfehler zu finden und mögliche Interpretationsfreiheiten zu erkennen, die zu unterschiedlichen Ergebnissen auf einem Host- und einem Zielsystem führen könnten. So ist z. B. bei C-Compilern das Ergebnis eines Rechts-Shifts eines negativen Integer-Wertes nicht exakt definiert oder Datenbreite und Endianess können an Host- und Zielsystem unterschiedlich sein.

**Integrationstests**

Mittels Integrationstests wird geprüft, ob Softwarekomponenten miteinander und mit Hardwarekomponenten korrekt zusammenwirken. Dabei werden die Testfälle als Black-Box-Tests ausgeführt. Typische Methoden für Software/Software-Integrationstests sind Bottom-Up-Komponententests, strukturierte Integrationstests und die Messung der Testabdeckung der Aufrufe von Unterprogrammen. Jede Methode hat Stärken und Schwächen. Bottom-Up-Komponententests können für kleine Projekte sinnvoll sein, wenn keine zyklischen Abhängigkeiten der Komponenten vorliegen. Strukturierte Integrationstests und die Messung der Testabdeckung der Aufrufe von Unterprogrammen sind problematisch, wenn globale Variablen verwendet werden. Ein Nachteil der letztgenannten Strategie ist auch, dass Fehler bei der Integration erst relativ spät erkannt werden.

Ziel des Hardware/Software-Integrationstests ist es, das Zusammenwirken von Hard- und Software zu überprüfen. Ist die Zielumgebung von Anfang an verfügbar, können Bottom-Up-Komponententests stets darauf laufen. Beim Regressionsverfahren werden die Zugriffe auf die Hardware durch eine Abstraktionsschicht gekapselt. Hat das System einen hohen Schutzbedarf, sind bei den Analysen auch alle denkbaren Fehlerzustände der Hardware zu betrachten und die Ergebnisse genau zu dokumentieren, idealerweise gibt es zu jedem funktionalen Merkmal und jedem Fehlverhalten einer Schnittstelle einen nachgewiesenen Test.

Wegen der möglicherweise beschränkten Ressourcen ist es bei einigen Systemen auch wichtig Ressourcentests durchzuführen. In diesen ist zu prüfen, ob die CPU und der vorhandene Speicher für die vorgesehene Software ausreichend leistungsfähig bzw. dimensioniert sind.

**Systemtests**

Mittels Black-Box-Tests wird überprüft, ob das System insgesamt die spezifizierten Anforderungen erfüllt. Begleitend sollte mittels Traceability-Tabellen verfolgt werden, welche Anforderung in welchem Test geprüft wird. Die Testdaten werden durch Äquivalenzklassenbildung über gültige und ungültige Eingangsdaten gebildet. Pro Testfall darf nur ein einziger Wert aus einer Äquivalenzklasse mit ungültigen Werten genommen werden.

**Ausführungsarten von Tests**

Tests können manuell, halbautomatisch oder automatisch ablaufen. Eine hohe Testautomatisierung bietet den Vorteil, sich wiederholende Tests schnell und unkompliziert durchführen zu können. Sie ist z. B. besonders für Regressionstests geeignet, also Tests die nach einer Fehlerbehebung durchgeführt werden um sicher zu gehen, dass dadurch nicht Fehler an anderer Stelle erzeugt wurden. Sie macht es auch möglich, manuell nur schwer zu realisierende Tests wie z. B. Lasttests wirtschaftlich durchzuführen. Beim Test sind gegebenenfalls notwendige manuelle Eingriffe zu berücksichtigen, beispielsweise beim Testen von eingebetteten Systemen.

Prüffragen:

- Werden Code Reviews und eine automatische statische Codeanalyse durchgeführt?
- Werden bei den Komponententests sinnvolle Äquivalenzklassen gebildet und alle kritischen Grenzwerte getestet?
- Ist die zur Testabdeckung gewählte Metrik dem Schutzbedarf angemessen und werden Komponententests auf dem Zielsystem durchgeführt?
- Werden dem Schutzbedarf angemessene Integrationstests und Systemtests durchgeführt?
- Wird getestet, ob die CPU und der vorhandene Speicher für die vorgesehene Software ausreichend leistungsfähig bzw. dimensioniert sind?

# M 2.569 Definition von Rollen und Verantwortlichkeiten bei der Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Entwicklung, Leiter Organisation
**Verantwortlich für Umsetzung:** Leiter Entwicklung, Leiter Organisation

Die Rollen und Verantwortlichkeiten bei der Software-Entwicklung müssen eindeutig zugewiesen sein, insbesondere dürfen keine relevanten Funktionen vernachlässigt werden. Jedem Mitarbeiter eines Projektes muss klar sein, welche Aufgaben in seinem Zuständigkeitsbereich liegen und wer der Ansprechpartner für Aufgaben außerhalb seines Zuständigkeitsbereichs ist.

Es ist ein Gesamtverantwortlicher für die Sicherheit im Software-Entwicklungs-Prozess zu benennen, der alle Sicherheitsmaßnahmen festlegt, überwacht und Ansprechpartner für Fragen hinsichtlich der Maßnahmen ist. Der Gesamtverantwortliche muss

- über ein klares Verständnis seiner Rolle,
- ausreichende Fähigkeiten,
- genügend Zeit,
- geeignete Werkzeuge und Befugnisse,
- Zugang zu interner und externer Informationssicherheits-Expertise,
- dokumentierte Methoden für Routine-Sicherheitsmaßnahmen und
- aktuelle Informationen über Informationssicherheit

verfügen. In regelmäßigen Abständen ist der Status der Informationssicherheit in jedem Projekt zusammen mit dem Entwicklungsverantwortlichen und den zuständigen Fachabteilungen zu überprüfen. Zusätzlich ist für jede der folgenden Schlüsselaktivitäten ein Verantwortlicher zu benennen:

- Einhaltung von Entwicklungsrichtlinien
- Anforderungsanalyse
- Risikoanalyse
- Design und Realisierung
- Test und Roll-out

Wenn die Teamgröße es zulässt, sollten alle Rollen von unterschiedlichen Personen besetzt werden. Entwicklung, Test- und Produktiv-Betrieb sollten von unterschiedlichen Personen durchgeführt werden.

Prüffragen:

- Wurde ein Gesamtverantwortlicher für den Software-Entwicklungs-Prozess benannt?
- Wurden die Rollen und Verantwortlichkeiten für jede Schlüsselaktivität festgelegt?

# M 2.570 Auswahl eines Vorgehensmodells zur Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Leiter Entwicklung

Für einen geregelten Ablauf des gesamten Entwicklungsprozesses ist es von elementarer Bedeutung, ein geeignetes Vorgehensmodell zur Software-Entwicklung auszuwählen. Alle am Prozess beteiligten Personen können sich besser orientieren und koordinieren, wenn die Methodik stringent angewendet wird.

Je nach Umfang und Anforderungen der zu entwickelnden Software ist ein Vorgehensmodell auszuwählen, das alle Aspekte des Entwicklungsprozesses ausreichend berücksichtigt. Beispielsweise sollte das Spiralmodell gegenüber dem Wasserfallmodell bevorzugt werden, wenn bereits zu Beginn des Prozesses klar ist, dass während der Entwicklung noch häufig funktionelle Anforderungen für die Software geändert werden.

Einige Vorgehensmodelle bieten einen eher starren Rahmen und eignen sich nur für Projekte, deren Anforderungen klar feststehen und sich im Verlauf des Projekts voraussichtlich nicht maßgeblich ändern werden. Andere Vorgehensmodelle unterstützen dynamische und agile Software-Entwicklung und ermöglichen mit mehrfachen Iterationen über alle Entwicklungsphasen die flexible Anpassung des Projektverlaufs an geänderte Anforderungen.

Etablierte Vorgehensmodelle zur Software-Entwicklung sind beispielsweise:

- **Wasserfallmodell**
  Die Entwicklung wird hier in klar definierte Phasen eingeteilt, die aufeinanderfolgend durchlaufen werden. Es beginnt mit der Anforderungsanalyse, auf die das Systemdesign folgt. Danach wird die eigentliche Software programmiert und modular getestet. Schließlich folgt auf den Integrations- und Systemtest die Auslieferung und Wartung der Software für das Produktivsystem.
- **Spiralmodell**
  Dieses generische Vorgehensmodell ist eine Weiterentwicklung des Wasserfallmodells und betrachtet die Software-Entwicklung als iterativen Prozess, dessen Zyklen mehrfach durchlaufen werden. Jeder Zyklus ist in vier Quadranten unterteilt. Zuerst werden die Ziele und Rahmenbedingungen festgelegt. Danach werden Alternativen evaluiert und Risiken bewertet. Daraufhin wird ein festgelegtes Zwischenziel realisiert und überprüft. Schließlich wird der nächste Zyklus für die Fortsetzung geplant.
- **Allgemeines V-Modell**
  Das V-Modell basiert auf dem Wasserfallmodell und definiert den Entwicklungsprozess sowie die Qualitätssicherung der Software phasenweise, indem jeder Entwurfsstufe eine Teststufe gegenübergestellt wird. Anzahl und Bezeichnung der Phasen sind hierbei flexibel.
- **V-Modell XT**
  Basierend auf dem V-Modell hat die öffentliche Verwaltung in der Bundesrepublik Deutschland das V-Modell XT als Entwicklungsstandard definiert. Im V-Modell XT werden Aktivitäten und Ergebnisse festgelegt, deren zeitliche Abfolge flexibel ist. Die Aktivitäten können beispielsweise auch auf das Wasserfallmodell abgebildet werden.
- **Prototyping**

Beim Prototyping liegt der Fokus der Software-Entwicklung darauf, dass schnell Prototypen bereitgestellt werden, deren Funktionalität dann in Zusammenarbeit von Auftragnehmern und Auftraggebern schrittweise genauer definiert und optimiert wird.

- **MDSD (Model-Driven Software Development)**
  Bei der modellgetriebenen Entwicklung wird Software automatisch aus formalen Modellen erzeugt, die mit Modellierungssprachen oder grafischen Modellierungstools erstellt werden. Die Funktionalität des gewünschten Systems kann hierbei auf einer abstrakten Ebene definiert werden.
- **TDD (Test-Driven Development)**
  In diesem Vorgehensmodell wird immer zuerst ein Software-Test erstellt, bevor die eigentliche Software erzeugt wird. Nachdem die Testfälle (sogenannte Grey-Box-Tests) fertiggestellt sind, wird mit möglichst geringem Aufwand der eigentliche Programmcode erstellt und bei Bedarf an die Tests angepasst. Testfälle können hierbei sowohl für einzelne Module (Unit-Tests) als auch für ein Gesamtsystem (Systemtest) erzeugt werden.

Es existieren vielfältige weitere Vorgehensmodelle zur Software-Entwicklung. Außerdem beschäftigen sich die ISO-Standards 12207 und 13407 mit dem Verständnis von Software-Entwicklung sowie der prototypischen benutzerorientierten Produktion von Software.

Die Entscheidung für ein Vorgehensmodell muss dokumentiert und ein entsprechender Ablaufplan für das Projekt erstellt werden, der alle Umsetzungsschritte und die jeweiligen Verantwortlichen enthält. Auf Basis des ausgewählten Vorgehensmodells muss eine interne Richtlinie zur Software-Entwicklung erstellt werden. Außerdem ist festzulegen

- auf welche Weise die institutionsweite Sicherheitsrichtlinie, rechtliche Anforderungen und spezifische Sicherheitsanforderungen während der Systementwicklung zu berücksichtigen sind und
- wie in den spezifischen Entwicklungsphasen Anforderungsanalyse, Design und Implementierung, Test und Roll-out die Sicherheitsbetrachtungen durchzuführen sind.

Das Personal sollte in der Methodik des gewählten Vorgehensmodells geschult werden. Die Richtlinie zur Software-Entwicklung sollte regelmäßig überprüft und auf dem neuesten Stand gehalten werden. Die Einhaltung der Richtlinie ist an allen Schlüsselpunkten der Software-Entwicklung zu prüfen.

Soll die Methodik des einmal gewählten Vorgehensmodells gegen eine andere Vorgehensweise ausgewechselt werden, kann dies einen erhöhten Entwicklungsaufwand in der Umstellungsphase verursachen. Aus diesem Grund muss die Auswahl des Vorgehensmodells möglichst sorgfältig durchgeführt werden.

Prüffragen:

- Wurde ein geeignetes Vorgehensmodell zur Software-Entwicklung festgelegt?
- Wurde anhand des gewählten Vorgehensmodells ein Ablaufplan für die Software-Entwicklung erstellt und die Sicherheitsanforderungen dokumentiert?
- Wurden institutionsweite Sicherheitsrichtlinien, rechtliche Anforderungen und spezifische Sicherheitsanforderungen berücksichtigt?
- Wurde das Personal in der Methodik des gewählten Vorgehensmodells geschult?
- Wird die Richtlinie zur Software-Entwicklung regelmäßig überprüft und gegebenenfalls angepasst?

# M 2.571 Berücksichtigung von Compliance-Anforderungen für die Software-Entwicklung

**Verantwortlich für Initiierung:** Anforderungsmanager
**Verantwortlich für Umsetzung:** Entwickler, Anforderungsmanager

Bei der Entwicklung von Software und beim Einsatz der entwickelten Software muss darauf geachtet werden, dass keine rechtlichen oder normativen Bedingungen verletzt werden. Beispielsweise drohen erhebliche rechtliche und finanzielle Konsequenzen, wenn urheberrechtlich geschützte Programmteile, Bibliotheken oder Grafiken unbedacht verwendet werden.

Sowohl für die eingesetzten Entwicklungswerkzeuge als auch für das entwickelte Softwareprodukt sind mindestens die folgenden Aspekte zu überprüfen:

- Verstoß gegen Gesetze oder Verträge
- Nichteinhaltung von Normen
- Verstoß gegen Lizenzbedingungen verwendeter Software
- Verletzung von Patentrechten
- Nachahmung von Geschmacksmustern
- Persönlichkeitsrechte

Alle Mitarbeiter sollten sensibilisiert sein, um frühzeitig erkennen zu können, wenn gegen Compliance-Anforderungen verstoßen wird. Weiterhin ist sicherzustellen, dass möglichst alle Verstöße bereits in der Entwicklungsphase festgestellt werden können und das Produktivsystem nicht erreichen. Bei Bekanntwerden von Verstößen sind umgehend Maßnahmen einzuleiten und die Entwicklung der Software an die gültigen Bedingungen anzupassen.

Prüffragen:

- Werden alle Compliance-Anforderungen für die Software-Entwicklung berücksichtigt?

# M 2.572 Beschaffung von Werkzeugen zur Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Beschaffung, Leiter Entwicklung
**Verantwortlich für Umsetzung:** Beschaffer

Neben der Entwicklungsumgebung können weitere Werkzeuge zur Software-Entwicklung erforderlich sein, beispielsweise Grafikprogramme oder Management-Tools. Ebenso können zusätzliche Geräte benötigt werden, beispielsweise Chipkartenleser oder Grafiktabletts.

Werkzeuge, die eine aktive Komponente der Software-Entwicklung sind, sollten nach standardisierten, dokumentierten Vorgehensweisen beschafft werden, die unter anderem spezifizieren:

- Richtlinien zur Auswahl von Hard- und Software
- Methoden, um Sicherheitsmängel von beschaffter Hard- und Software zu identifizieren und damit umzugehen
- Anforderungen an akzeptable Software-Lizenzbestimmungen
- Review- und Freigabeverfahren für angeschaffte Hard- und Software

Bei der Beschaffung sollten die Anbieter überprüft und die bestehenden Sicherheitsanforderungen des jeweiligen Anwendungszwecks berücksichtigt werden. Die Verfügbarkeit ist vor allem bei spezieller Hardware ein wichtiges Auswahlkriterium.

Weiterhin muss berücksichtigt werden, ob die beschaffte Hard- und Software für die Software-Entwicklung verwendet werden darf und die Weitergabe von damit erstellten oder bearbeiteten Informationen keinen Konflikt mit den Lizenzbedingungen des Herstellers erzeugt.

Externe Sicherheitsüberprüfungen und -zertifizierungen von Hard- und Software reduzieren die Wahrscheinlichkeit von Sicherheitsmängeln. Die Beschaffungsentscheidung sollte einer Qualitätssicherung durch Mitarbeiter unterzogen werden, die die Sicherheitsanforderungen verstehen und beurteilen können, ob diese erfüllt werden.

Prüffragen:

- Erfolgt die Beschaffung von Werkzeugen für die Software-Entwicklung nach standardisierten und dokumentierten Vorgehensweisen?

# M 2.573 Einhaltung einer sicheren Vorgehensweise bei der Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Leiter Entwicklung

Der Implementierungsprozess bei der Software-Entwicklung muss sicher gestaltet werden, um beispielsweise erkennen und vermeiden zu können, dass die Software versehentlich geändert oder absichtlich manipuliert wird. Insbesondere sicherheitskritische Software-Komponenten, z. B. Authentisierungssysteme, müssen während der Entwicklung von mehreren Entwicklern geprüft und getestet werden, z. B. durch stringente Anwendung des Vier-Augen-Prinzips, um die Informationssicherheit für die zu entwickelnde Software zu gewährleisten.

Es ist eine Versionskontrolle für die entwickelte Software zu gewährleisten. Insbesondere die Dokumentation der Unterschiede zwischen Versionen und die Möglichkeit zur Rückkehr zu vorherigen Versionen sind erforderlich (siehe M 6.32 *Regelmäßige Datensicherung*).

Damit die Integrität der Software nicht kompromittiert werden kann, sind regelmäßige Code-Reviews erforderlich. Diese müssen von unabhängigen Dritten oder zumindest von Entwicklern, die den Code nicht selbst geschrieben haben, durchgeführt werden. Hierbei ist zu prüfen, ob der Programmcode alle gewünschten Funktionen enthält und gleichzeitig keinerlei zusätzliche oder ungewollte Funktionen beinhaltet.

Werden externe Bibliotheken oder Code aus externen Quellen in die Entwicklungsumgebung eingebunden, so sind diese auf Schwachstellen und mögliche Konflikte mit anderen bereits verwendeten Komponenten zu überprüfen. Dies sollte mittels externer Informationsquellen (z. B. Online-Verzeichnisse mit bekannten Fehlermeldungen und Sicherheitslücken) und durch eigene Tests stets in Abstimmung mit dem Entwicklungsverantwortlichen geschehen.

Prüffragen:

- Wird eine Versionskontrolle für die entwickelte Software umgesetzt?
- Werden regelmäßig unabhängige Code-Reviews durchgeführt?

# M 2.574 Ausführliche Dokumentation der Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Fachabteilung
**Verantwortlich für Umsetzung:** Leiter IT, Fachabteilung

Bei der Software-Entwicklung muss nachvollziehbar dokumentiert werden, damit sicherheitsrelevante Aspekte erkennbar sind und die Software wartbar bleibt. Die Dokumentation kann unterschieden werden in Projektdokumentation, Informationen zum Projektmanagement der Software-Entwicklung und der Dokumentation zur Entwicklung des Systems (Systemdokumentation).

Die Projektdokumentation sollte mindestens folgende Informationen ausführlich beinhalten:

- Anforderungen an das zu entwickelnde System: In Form eines Anforderungskatalogs oder Pflichtenheftes
- Entscheidungsgrundlage für Eigenentwicklung oder Beauftragung: Die Entscheidungsgrundlage einschließlich der Risikobetrachtung, die zu einer Auftragsvergabe, Eigenentwicklung oder sonstigen Form einer Entwicklung geführt hat, muss ausreichend dokumentiert werden.
- Dokumentation des Vergabeprozesses: Sowohl für öffentliche als auch für die meisten privaten Institutionen ist die Nachvollziehbarkeit der Auftragsvergabe zumindest vom internen Controlling vorgeschrieben.
- Vertrag: Alle Leistungen, Bedingungen und Abkommen zwischen dem Auftraggeber und Auftragnehmer müssen schriftlich festgehalten werden.
- Dokumentation des Projektverlaufs: Nicht nur während des laufenden Projekts, auch um spätere Fragen klären zu können, ist es wichtig, den Projektverlauf nachvollziehbar zu dokumentieren. Dazu gehört es, Verantwortlichkeiten, Protokolle, Projektentscheidungen, Meilensteine, Abnahmen und Freigaben festzuhalten.

Die Systemdokumentation enthält die Dokumentation des Entwicklungsprozesses einschließlich:

- System-Spezifikation
- Systemarchitektur und Design (Ablaufpläne)
- Schnittstellen Definitionen (inklusive Dokumentation der intern genutzten Bibliotheken, Entwicklungsumgebungen und weiterer Software)
- Codierungsrichtlinien (z. B. Namenskonventionen, Strukturierungsrichtlinien, etc.)
- Code-Kommentierung
- Dokumentation der Konfiguration
- Dokumentation von Änderungen
- Dokumentation der Qualitätssicherung und der Tests (siehe auch M 2.568 *Testverfahren für Software*)
- Dokumentation für die Installation und die Inbetriebnahme, Anleitungen für die Administratoren
- Bedienungsanleitung für die Anwender

Insbesondere wenn eine Zertifizierung eines Systems angestrebt wird (z. B. nach Common Criteria), empfiehlt es sich, rechtzeitig die Dokumentationsanforderungen für die Zertifizierung in Erfahrung zu bringen und einzuhalten. Nachträgliche Dokumentation kann sehr kostspielig werden oder Fehler beinhalten.

Prüffragen:

- Liegen ausreichende Projekt- bzw. Systemdokumentationen vor?

# M 2.575 Regelmäßige Sicherheitsaudits für die Software-Entwicklungsumgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Leiter Entwicklung

Mitarbeiter oder Dienstleister, die nicht dem Entwicklungsteam angehören, sollten regelmäßige Sicherheitsaudits der Entwicklungsumgebung und auch der Testumgebung durchführen. Hierbei sollten die Sicherheitsaktivitäten bezüglich der Entwicklungsprojekte und der Status der sicheren Implementierung in der Entwicklungsumgebung überprüft werden. Dem Sicherheitsaudit müssen definierte und dokumentierte Festlegungen zugrunde liegen und deren Einhaltung muss überprüft werden.

Bei allen Mitarbeitern sollte ein Sicherheitsbewusstsein geschaffen werden, das die Notwendigkeit von Maßnahmen für die Informationssicherheit festigt und erläutert, warum diese umgesetzt werden müssen.

Im Rahmen des Audits wird die Sicherheit der Entwicklungsumgebung getestet und es sollten mindestens die folgenden Aspekte geprüft werden:

- Aktualität der Entwicklungs- und Testumgebung (Versionsstand, Patches, Updates, Virenschutz und bekannte Schwachstellen)
- Funktionalität der Entwicklungs- und Testumgebung (z. B. Konfiguration und Einsatzbedingungen)
- Zugriffsbeschränkungen auf die Entwicklungs- und Testumgebung (berechtigte und unberechtigte Benutzer)
- Zugriffsbeschränkungen auf Entwicklungs- und Testdaten (z. B. Code, extern eingebundene Bibliotheken und kompilierte Softwaremodule)
- Zugriffsbeschränkungen auf weitere Daten im Zusammenhang mit der Entwicklung und dem Test, insbesondere bei erhöhtem Schutzbedarf (z. B. Dokumentationen von Schnittstellen oder geheimen Funktionen)

Prüffragen:

- Finden regelmäßige Sicherheitsaudits der Software-Entwicklungsumgebung statt?
- Finden regelmäßige Sicherheitsaudits der Software-Testumgebung statt?

# M 2.576 Erstellung einer Sicherheitsrichtlinie für den Einsatz von lokalen Netzen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Behörden-/Unternehmensleitung

Eine der wichtigsten organisatorischen Aufgaben bei der Einführung von lokalen Netzen ist es, eine entsprechende Sicherheitsrichtlinie zu planen und zu definieren. Diese Richtlinie legt die später umzusetzenden Sicherheitsbestimmungen für LANs fest.

Der sichere und ordnungsgemäße Betrieb eines LANs kann nur sichergestellt werden, wenn Planung und Konzeption sowie Betrieb in die bestehenden sicherheitstechnischen Vorgaben integriert sind.

Die zentralen sicherheitstechnischen Anforderungen und das zu erreichende Sicherheitsniveau ergeben sich aus der organisationsweiten Sicherheitsleitlinie. Die Anforderungen sollten in einer spezifischen Sicherheitsrichtlinie für LANs formuliert werden, um die übergeordnete und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

Grundlage für eine angemessene Definition von Forderungen, die in der Sicherheitsrichtlinie Ausdruck finden, ist die Dokumentation der Schutzbedarfsfeststellung aller Informationen, die im LAN verarbeitet, übertragen und gespeichert werden sollen. Nur hieraus lässt sich ableiten, welche Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der Informationen gestellt werden und entsprechend, welcher technische und organisatorische Aufwand angemessen ist.

Da ein LAN aus vielfältigen IT-Systemen besteht, sind für Erstellung einer Sicherheitsrichtlinie für LANs weitere Sicherheitsrichtlinien bzw. Regelungen zu beachten und mit der vorliegenden Sicherheitsrichtlinie für lokale Netze abzustimmen. Zu nennen sind beispielsweise:

- Sicherheitsrichtlinie für Router und Switches (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*),
- Sicherheitsrichtlinie für Sicherheitsgateways (siehe M 2.299 *Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway*),
- Sicherheitsrichtlinie zur VPN-Nutzung (M 2.418 *Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung*),
- etc.

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Teilnetze mit normalem Schutzbedarf kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei Teilnetzen mit hohem Schutzbedarf wird grundsätzlich eine restriktive Strategie empfohlen.

Nachfolgend sind einige Punkte aufgeführt, die in der Sicherheitsrichtlinie für LANs berücksichtigt werden sollten. Sofern Aspekte bereits in anderen Dokumenten (z. B. Sicherheitsrichtlinien) verbindlich vorgegeben sind, genügt ein entsprechender Verweis.

**Vorgaben für die Planung von LANs**

Es sind Vorgaben für die Infrastruktur zu entwickeln, in der LAN-Komponenten (z. B. Router und Switches, Sicherheitsgateway, Speicherkomponenten, Server) aufgestellt werden. Die Infrastruktur der Räume, in denen LAN-Komponenten betrieben werden, muss geeignet sein, um die Verfügbarkeitsanforderungen des LANs durch entsprechende Strom-und Klimaversorgung zu erfüllen. Ebenso muss der Zutritt zu diesen Räumen angemessen geschützt werden.

Es sind Vorgaben zu machen, die den Zugriff Externer auf das LAN (beispielsweise zu Wartungszwecken) regeln. Hierbei ist auch festzulegen, wie solche Zugriffe kontrolliert und protokolliert werden.

Ist eine sehr hohe Verfügbarkeit des LANs gefordert, ist die Analyse von Single-Points-of-Failure (SPoFs) in jedem Fall vorzunehmen. Sollen neue Komponenten in ein hochverfügbares LAN eingebracht werden, ist deren reibungslose Integration zunächst innerhalb spezieller Testsysteme zu überprüfen.

**Vorgaben für die Arbeit von Administratoren**

Es ist zu dokumentieren, nach welchem Schema Administrationsrechte für einzelne Komponenten des LANs vergeben werden. Es ist empfehlenswert, ein entsprechendes Rollenkonzept zu entwickeln.

Es sollten Administrator-Rollen definiert werden, denen aufgabenbezogen die notwendigen Rechte eingeräumt werden. Insbesondere sollte die routinemäßige Systemverwaltung (zum Beispiel Backup) nur mit den unbedingt notwendigen Rechten durchgeführt werden können. Die Administrator-Kennungen werden in der Folge den Rollen zugeordnet. Um die Auswirkungen von Fehlern zu reduzieren, darf unter einer Administrator-Kennung nur gearbeitet werden, wenn es zwingend notwendig ist.

Administrative Zugriffe sind mindestens durch Einsatz starker Passwörter (siehe M 2.11 *Regelung des Passwortgebrauchs*), besser durch Mehr-Faktor-Authentisierung abzusichern.

Die Verwaltung und Kontrolle von LAN-Ressourcen durch die Administratoren ist entweder nur lokal über eine direkt angeschlossene Konsole, ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen zulässig. Administrative Zugriffe sollten auf definierte Systeme beschränkt werden und z. B. durch Sicherheitsgateways kontrolliert werden.

IT-Systeme, die als Managementkonsole oder zur Revision eingesetzt werden, sind besonders zu härten (siehe B 3.201 *Allgemeiner Client*).

Durch die vorgegebene Aufgabenteilung, durch Vorgaben und Regelungen und eine stets aktuelle Dokumentation der Einstellungen aller LAN-Komponenten ist sicherzustellen, dass Administratoren keine Aktionen ausführen oder Einstellungen an den einzelnen LAN-Komponenten vornehmen, die zu Inkonsistenzen, Ausfällen oder Datenverlust führen können. Relevante Änderungen müssen dokumentiert werden. Es ist dazu empfehlenswert, ein Änderungsmanagement-Verfahren zu betreiben (siehe B 1.14 *Patch- und Ände-*

*rungsmanagement*). Es ist festzulegen, ob für bestimmte sicherheitskritische Änderungen das Vier-Augen-Prinzip anzuwenden ist.

**Vorgaben für die Installation und Konfiguration von LAN-Komponenten**

Das Vorgehen bei der Erstinstallation von LAN-Komponenten ist zu dokumentieren.

Nach der Installation sind die Default-Einstellungen in Bezug auf Sicherheitsgefährdungen zu überprüfen, unsichere Dienste auf LAN-Komponenten zu deaktivieren und die Standardkennungen und -passwörter zu ändern.

Zugriffe von Systemkonsolen auf einzelne LAN-Komponenten sollten ausschließlich über verschlüsselte Verbindungen ermöglicht werden. Der Kreis der Zugriffsberechtigten auf die Geräte ist möglichst klein zu halten. Regeln zur Verwendung und Konfiguration der Konsole und Restriktion der Zugriffsarten sind zu dokumentieren.

Es ist zu regeln, wie Dokumentationen (z. B. Verfahrensanweisungen für die Einrichtung administrativer Kennungen, Betriebshandbücher für Abläufe und Kontrollen im Normalbetrieb) zu erstellen und zu pflegen sind und in welcher Form die Dokumentationen vorliegen sollten.

LANs sollten geeignet segmentiert werden (siehe M 5.61 *Geeignete physische Segmentierung*, M 5.62 *Geeignete logische Segmentierung* und M 5.77 *Bildung von Teilnetzen*).

**Vorgaben für den sicheren Betrieb**

Die LAN-Administration ist abzusichern, indem Zugriffe nur über besondere Verbindungen (ein separates Administrationsnetz) zugelassen werden.

Es sind gegebenenfalls Werkzeuge auszuwählen, mit denen die LAN-Komponenten in einem bestehenden Netzmanagement betrieben, gewartet und integriert werden können (siehe B 4.2 *Netz- und Systemmanagement*). Vorgaben für eine sichere Konfiguration dieser Werkzeuge müssen definiert werden. Wenn möglich, sollten nur verschlüsselte Verbindungen genutzt und nicht benötigte Schnittstellen und Dienste deaktiviert bzw. gesperrt werden.

Falls eine Fernwartung oder Überwachung durch den Hersteller genutzt werden soll, müssen Vorgaben für die Absicherung der Zugänge definiert werden. Beispielsweise ist die Anbindung per VPN oder exklusiv genutzte Verbindungen zu realisieren. Außerdem müssen Fernzugriffe für die Institution nachvollziehbar protokolliert werden. Weitere Informationen sind in M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration* enthalten.

Es ist eindeutig festzulegen, wer verantwortlich dafür ist, Software-Updates zu initiieren oder Konfigurationen zu ändern. Die Vorgehensweise ist zu dokumentieren. Sobald sehr hohe Anforderungen an die Verfügbarkeit bestehen, sollten Änderungen und Updates stets vor dem Wirkbetrieb an baugleichen Testsystemen erprobt und bewertet werden.

Während des Betriebes eines LANs sind alle administrativen Tätigkeiten zu protokollieren.

Die Daten sind verschlüsselt zu transportieren bzw. zu speichern, wenn dies aufgrund ihres Schutzbedarfs erforderlich ist.

Die Regelungen für die Datensicherung im LAN sind mit dem übergreifenden Datensicherungskonzept der Institution (siehe dazu B 1.4 *Datensicherungskonzept*) abzustimmen. Bei besonderen Anforderungen an die Vertraulichkeit ist hier die Rechteverwaltung auf Backups vorzugeben.

Aufgrund der zentralen Bedeutung eines LANs müssen Pläne für den Notfall erstellt und in das organisationsweite Notfallmanagement eingebunden werden (siehe auch M 6.165 *Erstellen eines Notfallplans für den Ausfall des lokalen Netzes*).

Verantwortlichkeiten und Vorgehen für Revision und Audit sind zu beschreiben. Die Revision von LANs ist in ein übergreifendes Revisionskonzept zu integrieren.

Prüffragen:

- Wurde eine Sicherheitsrichtlinie für den Einsatz von lokalen Netzen erstellt?
- Wurden in der Sicherheitsrichtlinie Vorgaben zu Planung und Konzeption sowie Betrieb von LANs beschrieben?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde die Sicherheitsrichtlinie für den Einsatz von LANs in das organisationsweite System für Revision und Audits aufgenommen und wurden Schnittstellen zum Notfallmanagement geschaffen?

# M 2.577 Auswahl geeigneter Kryptoverfahren für Netze

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Kommunikationsnetze transportieren Daten zwischen IT-Systemen. Dabei werden die Daten selten über eine dedizierte Kommunikationsleitung zwischen den an der Kommunikation beteiligten Partnern übertragen. Vielmehr werden die Daten über viele Zwischenstationen geleitet. Sollen die übertragenen Informationen nicht von unberechtigten Dritten abgehört, von diesen manipuliert oder durch technische Fehler verändert werden, dann sollte ein geeignetes kryptographisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung genutzt werden. Neben dem eigentlichen Schutz der Informationen ist ebenso die Identifikation und Authentisierung von Systemen untereinander, von Systemen gegenüber Benutzern und von Benutzern gegenüber Systemen wichtig.

Der netzbasierte kryptographische Schutz von Informationen kann auf den unterschiedlichen Schichten des OSI-Referenzmodells erfolgen. Auf Layer 2 beispielsweise kann eine ortsbasierte Netzzugangskontrolle für LAN und WLAN realisiert werden. Bevor einem IT-System (Client) Zugang zu einem Netz gewährt wird, muss es sich an einem Authentikator anmelden (z. B. Switch, Router oder WLAN Access Point). Der Authentikator überprüft die übermittelten Authentisierungsdaten mit Hilfe eines Authentisierungsservers und gibt je nach Ausgang dieser Überprüfung den Zugriff auf das Netz frei.

Auf Layer 3 erfolgt der kryptographische Schutz von Informationen typischerweise mit IPSec und IKE. IPSec bietet Funktionen zur Verschlüsselung und Integritätssicherung für IP-Kommunikation. In Kombination mit dem IKE-Verfahren (Internet Key Exchange) kann auch ein automatisierter Schlüsselaustausch sowie eine Authentisierung der Tunnel-Endpunkte erfolgen. Ein manueller Schlüsselaustausch wird durch IPSec ebenfalls unterstützt. Die Authentisierung der Benutzer muss jedoch über andere Verfahren erfolgen.

Auf Layer 5 bis 7 des OSI-Modells erfolgt die kryptographische Absicherung von Informationen häufig mit SSL/TLS, PGP, S/MIME etc.

Unabhängig vom ausgewählten Verfahren ist bei der Absicherung der Informationen darauf zu achten, kryptographische Verfahren für den jeweiligen Einsatzzweck auszuwählen, die dem Stand der Technik entsprechen und keine bekannten Schwachstellen aufweisen (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Weiterhin sind die Anforderungen aus M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation* und M 2.46 *Geeignetes Schlüsselmanagement* zu beachten.

Prüffragen:

- Werden zum Schutz der Informationen kryptographische Verfahren eingesetzt, die dem Stand der Technik entsprechen?

# M 2.578 Installation, Konfiguration und Betreuung eines lokalen Netzes durch Dritte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Wenn ein LAN durch einen externen Auftragnehmer installiert, konfiguriert oder betreut werden soll, so sind bei diesem, neben den Empfehlungen in Baustein B 1.11 *Outsourcing*, die im Folgenden beschriebenen Punkte zu beachten:

- Es ist stets zu prüfen, ob eine LAN-Installation nicht selbst durchgeführt werden kann. Eine Machbarkeits- und eine Kostenprüfung sollte hierfür durchgeführt werden.
- Die LAN-Sicherheitsrichtlinie sollte stets selbst erstellt werden und nicht durch Dritte. Dadurch wird verhindert, dass sich in der Institution niemand mehr ausführlich mit den Sicherheitsaspekten von LANs auseinandersetzt und somit eventuell notwendige Sicherheitsmaßnahmen vergessen werden. Es ist aber sinnvoll, zur Erstellung einer LAN-Sicherheitsrichtlinie Beratungen und Hilfestellungen durch Dritte in Anspruch zu nehmen, wenn keine internen Ressourcen dafür vorhanden sind.
- Bei der Vergabe von Installation, Konfiguration und Betreuung eines lokalen Netzes ist der IT-Sicherheitsbeauftragte mit einzubeziehen. Es ist ein detailliertes Pflichtenheft zu erstellen. Darin sind alle Mindestanforderungen an die LAN-Komponenten zu definieren.
- Dem Auftragnehmer ist die LAN-Sicherheitsrichtlinie vorzulegen. Er muss vertraglich dazu verpflichtet werden, diese einzuhalten und umzusetzen. Dies ist bei der Umsetzung der vertraglich vereinbarten Leistungen regelmäßig zu überprüfen, um frühzeitig eventuelle Probleme zu erkennen. Die Sicherheitsrichtlinie sollte fester Bestandteil des Pflichtenheftes sein.
- Der Auftragnehmer sollte weitreichende und am besten langjährige Erfahrungen im Aufbau und in der Absicherung eines LANs haben. Entsprechende Referenzen sind vorzulegen und zumindest stichprobenweise zu prüfen.
- Der Auftragnehmer muss vertraglich dazu verpflichtet werden, die Konfiguration der LAN-Komponenten, sowie Passwörter, Verbindungsschlüssel und Zugangskennungen und -mechanismen nicht an unbefugte Personen weiterzugeben. Ebenso sollte der Auftragnehmer dazu verpflichtet werden, die durch den Aufbau eines LANs eventuell bekannt gewordenen Informationen und Daten nicht zwischenzuspeichern oder an unbefugte Personen weiterzugeben.
- Vor der Installation eines LANs durch den Auftragnehmer sind entsprechende Teststellungen durchzuführen. Dabei sollten alle geplanten Sicherheitseinstellungen ausführlich getestet werden.
- Während Installation, Konfiguration und Betreuung eines lokalen Netzes durch einen Auftragnehmer sollte darauf geachtet werden, dass keine Hintertüren in das LAN durch den Auftragnehmer eingebaut werden. Alle Einstellungen und Konfigurationen sind durch den Auftragnehmer genau zu dokumentieren und mit Abschluss der Installation an den Auftraggeber vollständig zu übergeben.
- Nach Abschluss einer LAN-Installation sollte anhand des Leistungsverzeichnisses eine Abnahme durchgeführt werden. Darüber hinaus können die im Pflichtenheft nach der Vergabe erstellten Ausführungsunterlagen als Prüfungsgrundlage dienen, da hierin beispielsweise Verfahren für Abnahmemessungen spezifiziert sein können.

- Die Abnahme einer LAN-Installation sollte mit Hilfe eines unabhängigen Experten erfolgen, um auch die technischen Details genau überprüfen zu lassen. Hierbei ist der IT-Sicherheitsbeauftragte auch mit einzubeziehen.
- Als wesentlicher Schwerpunkt sollte bei der Abnahme zudem die Dokumentation auf Vollständigkeit und eventuelle Inkonsistenzen geprüft werden.
- Soll das LAN auch nach der Installation durch einen externen Auftragnehmer betreut werden, so muss der Auftragnehmer auch hier vertraglich verpflichtet werden, alle hierbei bekannt gewordenen Informationen, wie Passwörter, sensible Daten, Konfigurationseinstellungen usw. nicht an unbefugte Personen weiterzugeben. Ebenso sollte ein Notfallvorsorgeplan (siehe auch M 6.165 *Erstellen eines Notfallplans für den Ausfall des lokalen Netzes*) mit dem Auftragnehmer erstellt werden. Hierbei sollte für jedes möglicherweise im LAN auftretende Problem der Schweregrad, die Reaktionszeit, die jeweiligen Arbeitsschritte und wer im Notfall informiert werden muss genau definiert werden.

Prüffragen:

- Sind Auftragnehmer bei Installation, Konfiguration oder Betreuung eines lokalen Netzes auf die LAN-Sicherheitsrichtlinie verpflichtet worden?
- Wurde mit dem Auftragnehmer ein Notfallvorsorgeplan für Probleme im LAN erstellt?

# M 2.579 Regelmäßige Audits des lokalen Netzes

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Behörden-/Unternehmensleitung

Bei allen Komponenten der LAN-Infrastruktur muss regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und ob diese korrekt konfiguriert sind. Dabei sollte allen Beteiligten deutlich gemacht werden, dass Audits immer nur dazu dienen sollen, um Tatsachen festzustellen und nicht für Schuldzuweisungen (siehe auch M 2.199 *Aufrechterhaltung der Informationssicherheit*).

Das Resultat eines Audits kann als eine einfache Soll-Ist-Gegenüberstellung gehalten werden. Der Bericht sollte in gebotener Kürze die Vorgaben z. B. aus der Sicherheitsrichtlinie darstellen und die Feststellungen des Audits zu den einzelnen Vorgaben darstellen. Werden Abweichungen vom Soll-Zustand gefunden und sind Abhilfe-Maßnahmen bekannt, so sollten diese im Report aufgenommen werden.

**Unabhängigkeit der Auditoren**

Die Durchführung der Audits muss durch unabhängige Auditoren erfolgen, d. h. das durchführende Personal darf sich und seine Arbeit nicht selbst auditieren.

Auch wenn die Tätigkeit der Auditoren durch die Administratoren unterstützt wird, benötigen sie tiefere Kenntnisse über das LAN, um ihre Tätigkeit durchführen zu können. Diese Kenntnisse sind durch regelmäßige Schulungen zu erwerben bzw. zu aktualisieren. Auditoren dürfen keine Änderungen im Netz vornehmen, daher benötigen sie höchstens Leserechte.

Wenn keine konkreten Vorgaben der Institution vorliegen, so sollten bei einem Audit mindestens die folgenden Bereiche geprüft werden:

- Es gibt ein Sicherheitskonzept für die technische Ausgestaltung und organisatorische Regelungen des LANs.
- Der Schutzbedarf der Informationen in Bezug auf Verfügbarkeit und Vertraulichkeit wurde nach Vorgaben der Anwender festgelegt und dokumentiert.
- Bei Inbetriebnahme wurden in allen LAN-Komponenten (Server, Router und Switches, Sicherheitsgateways, Speicherlösungen, Administrations-PC etc.) die Standardpasswörter ersetzt.
- Die LAN-Komponenten (Server, Router und Switches, Sicherheitsgateways, Speicherlösungen etc.) sind in zutrittsgeschützten Räumen mit angemessener Infrastruktur (Stromversorgung, Klimatisierung) stationiert.
- Administrative Zugriffe auf die LAN-Komponenten erfolgen ausschließlich verschlüsselt oder über ein separates Administrationsnetz.
- Das Administrationsnetz ist durch Firewall, Anti-Viren-Software und gegebenenfalls ein IDS abgesichert.
- Zur Administration werden nur gesicherte Verbindungen (z. B. über HTTPS, SSH) genutzt.
- Die Daten werden verschlüsselt transportiert bzw. gespeichert, wenn dies aufgrund ihres Schutzbedarfs erforderlich ist.

- Das Logging ist so eingestellt, dass Fehlersituationen und Missbrauchsversuche protokolliert werden. Die Protokolldateien werden regelmäßig kontrolliert.
- Grundkonfiguration und folgende relevante Änderungen der Konfiguration sind schriftlich dokumentiert. Sowohl eine Beschreibung der logischen als auch physischen Topologie des LANs ist vorhanden und aktuel. Diese Dokumentation ist auch im Notfall verfügbar.
- Nach Änderungen werden sicherheitsrelevante Einstellungen entsprechender LAN-Komponenten erneut überprüft.
- Der störungsfreie Ablauf von Datensicherungen und die Brauchbarkeit von Sicherungsmedien werden regelmäßig kontrolliert.

Prüffragen:

- Wird bei allen Komponenten der LAN-Infrastruktur regelmäßig überprüft, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und ob die LAN-Komponenten korrekt konfiguriert sind?

# M 2.580 Außerbetriebnahme von Netzkomponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Sollen Netzkomponenten eines LANs, wie beispielsweise Router oder Switches, außer Betrieb genommen oder ersetzt werden, so müssen Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert oder auf ein Ersatzsystem übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*. Darüber hinaus müssen alle sicherheitsrelevanten Informationen gelöscht werden. Dies gilt besonders dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben (beispielsweise verkauft) werden oder wenn ein Gerät im Rahmen eines Garantieaustausches oder einer Reparatur an den Hersteller oder eine Service-Firma übergeben wird, aber selbst dann, wenn die Geräte intern weiter verwendet oder verschrottet werden.

Je nach Einsatzzweck der Netzkomponenten können beispielsweise folgende Informationen und Daten auf den Geräten gespeichert sein:

- Konfigurationsdateien, aus denen Informationen über die Netzstruktur der Institution entnommen werden können,
- Passwortdateien,
- Protokolldateien, die sicherheitsrelevante Informationen oder personenbezogene Daten enthalten,
- Zertifikate und kryptographische Schlüssel (etwa für den Zugang auf andere IT-Systeme)

Bei "normalen" IT-Systemen sollten die Festplatten mit einem geeigneten Tool so gelöscht werden, dass keine Wiederherstellung der Dateien mehr möglich ist. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Weitere Hinweise finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* sowie in M 2.433 *Überblick über Methoden zur Löschung und Vernichtung von Daten*.

Handelt es sich bei dem IT-System um eine Appliance, dann kann sich das Löschen schwieriger gestalten. Bei Appliances hängt die Vorgehensweise davon ab, wo und wie die Daten gespeichert werden, also beispielsweise auf einer eingebauten Festplatte oder in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Sind auf einer Netzkomponente besonders sicherheitskritische Informationen gespeichert und kann nicht mit hinreichender Sicherheit gewährleistet werden, dass die Daten wirklich gelöscht sind, so kann es erforderlich sein, Festplatten bzw. die Speicherbausteine physisch zu zerstören bzw. unbrauchbar zu machen.

Neben den Informationen, die auf der Netzkomponente selbst gespeichert sind, sollte auch überprüft werden, ob auf den Backup-Medien sensitive Informationen enthalten sind. Falls es nicht aus anderen Gründen (beispielsweise Archivierung, Aufbewahrungspflicht aufgrund gesetzlicher Regelungen) erforderlich ist, die Backup-Medien aufzubewahren, so sollten die Medien nach der Außerbetriebnahme des Gerätes ebenfalls gelöscht werden.

Oft sind die Netzkomponenten von außen mit IP-Adressen, Hostnamen oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden.

Prüffragen:

- Ist sichergestellt, dass vor der Außerbetriebnahme oder dem Austausch von Netzkomponenten die gespeicherten Daten entweder extern gesichert bzw. archiviert oder auf ein Ersatzsystem übertragen werden?
- Ist sichergestellt, dass vor der Außerbetriebnahme oder dem Austausch von Netzkomponenten die gespeicherten Daten sicher gelöscht werden?
- Ist eine vollständige physische Zerstörung der Netzkomponenten gewährleistet, wenn eine sichere Löschung der darauf gespeicherten Daten nicht möglich ist?
- Sofern die Backup-Medien von Netzkomponenten nicht mehr benötigt werden: Werden die sensitiven Informationen auf den Backup-Medien sicher gelöscht?
- Werden eventuell vorhandene Beschriftungen auf den Netzkomponenten vor der Ausmusterung entfernt?

# M 2.581 Aufbau eines Administrationsnetzes für das Netzmanagement

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die Verwaltung und Überwachung von Ressourcen innerhalb eines Netzes, an das hohe Sicherheitsanforderungen gestellt werden, muss angemessen umgesetzt werden. Die Ressourcen innerhalb eines Netzes müssen entsprechend verwaltet und überwacht werden, vor allem die Systeme mit erhöhtem Sicherheitsbedarf wie z. B. aktive Netzkomponenten. Das hierfür eingesetzte Netzmanagement-System muss angemessen geschützt werden.

Der Aufbau eines eigenen LANs für das Netzmanagement, das ausschließlich administrativen Aufgaben dient, ist oft der übersichtlichste, effektivste und wirtschaftlichste Weg, um diesen Anforderungen zu genügen. In diesem Administrationsnetz werden PCs stationiert, die ausschließlich zur Verwaltung kritischer Komponenten dienen.

Grundsätzlich müssen auch innerhalb dieses Netzes sichere Protokolle (SSH statt Telnet, HTTPS statt HTTP) zur Administration genutzt werden. Die zumindest logische, wenn nicht gar physische Trennung dieses Administrationsnetzes von Produktionsnetzen macht jedoch den Einsatz unsicherer Protokolle, insbesondere des in vielen Produktionsumgebungen immer noch fast unvermeidlichen SNMP Version 1, tolerierbar.

**Konzeption/Planung**

- Ein sehr einfacher Aufbau eines Administrationsnetzes kann damit starten, dass ein separater Switch in Betrieb genommen wird.
- Alle Clients der Administratoren werden mit ihrem Netzanschluss an das Administrationsnetz gebunden.
- Alle Server und Systeme mit erhöhtem Sicherheitsbedarf (aktive Netzkomponenten) erhalten einen zusätzlichen Netzanschluss und werden damit an das Administrationsnetz gebunden.
- Auf den Servern wird der Administrationszugang der Betriebs- und Anwendungssoftware, wo immer das möglich ist, exklusiv an die Netzadresse im Administrationsnetz gebunden.

Im Administrationsnetz sollten private Adressen benutzt werden, wie in RFC-Standard 1918 beschrieben. Solche Adressen werden in "offiziellen" Netzen nicht geroutet, so dass ein Anschluss an offizielle Netze, wenn er denn nötig werden sollte, stets NAT (Network Address Translation) und weitere Schutzmaßnahmen, die durch eine Firewall realisiert werden, erfordert.

Im Administrationsnetz sollte auf allen IT-Komponenten durch Nutzung oder Einsatz eines NTP-Servers eine einheitliche Uhrzeit sichergestellt werden (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*). Damit wird die Auswertung von Protokollen erleichtert und die Bewertung von Vorfällen mit Auswirkungen auf mehreren Komponenten ermöglicht.

Die verfügbaren Ressourcen für den gesamten Aufbau des Administrationsnetzes sind zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür notwendigen finanziellen Ressourcen. Die Ergebnisse sind entsprechend zu dokumentieren.

Es ist zudem zu prüfen, ob im Administrationsnetz zusätzliche Überwachungsmaßnahmen etabliert werden sollten. Zum Beispiel kann durch Einsatz von netzbasierten IDS zusätzlich überwacht werden, ob unzulässige Aktivitäten im Netz zu beobachten sind.

Ebenso könnte in einem Administrationsnetz auch eine zentrale Protokollierung etabliert werden, in der eine zentrale Instanz als Protokollserver die Logdaten aller ans Netz angeschlossenen Komponenten verwaltet. Zunächst ist zu untersuchen, wie ein Produktionsnetz und die darin stationierten Server und sonstigen Geräte (z. B. aktive Netzkomponenten, Speichersysteme) um ein Administrationsnetz erweitert werden können.

Für den Aufbau eines Administrationsnetzes sind M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und M 2.140 *Analyse der aktuellen Netzsituation* zu bearbeiten. Anschließend sind die Anforderungen an die Netzkommunikation des neu aufzubauenden Administrationsnetzes zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

**Umsetzung**

Mit Aufnahme des Testbetriebes muss eine Prüfung stattfinden, die die Sicherheitsvorkehrungen testet und zur Grundlage der Betriebsdokumentation dieses Netzes wird. Typische Prüffragen sind:

- Ist eine durchgängige Trennung des Administrationsnetzes vom Produktionsnetz gegeben?
- Werden, wo immer möglich, sichere Dienste (secure shell, https) genutzt? Sind die unsicheren Varianten dieser Dienste (telnet, http) auf den administrierten Geräten deaktiviert?
- Ist überschaubar und dokumentiert, wo auf den Einsatz unsicherer Dienste nicht verzichtet werden kann?
- Sind alle Default-Kennungen und -Passwörter auf allen Systemen wie Servern und aktiven Netzkomponenten geändert?

Anschließend kann der produktive Betrieb gestartet werden.

**Betrieb**

Im laufenden Betrieb des Netzes muss darauf geachtet werden, dass durch Änderungen am Netz, dessen Komponenten oder an den Berechtigungen die Sicherheit des Administrationsnetzes nicht beeinträchtigt wird. Die erfassten Protokolle müssen regelmäßig ausgewertet werden. Darüber hinaus muss auch während des Betriebs regelmäßig die Sicherheit des Administrationsnetzes überprüft werden (siehe M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*).

**Aussonderung**

Wenn Netzkomponenten oder andere Hardware ausgesondert oder auch nur zur Reparatur zeitweise aus dem Administrationsnetz genommen werden, ist sicherzustellen, dass keine internen Informationen (Passwörter, Protokolldateien, Dokumente zu Interna etc.) darauf gespeichert sind.

**Notfallvorsorge**

Es muss eine Notfallplanung geben, so dass der Betrieb des produktiven Netzes sichergestellt wird, wenn das Administrationsnetz ausfällt.

Prüffragen:

- Ist ein abgesichertes Administrationsnetz eingerichtet?
- Ist für alle Komponenten des Administrationsnetzes eine einheitliche Uhrzeit sichergestellt?
- Werden während des Testbetriebs des Administrationsnetzes die Sicherheitsvorkehrungen getestet und der Test sowie die Ergebnisse dokumentiert?
- Gibt es eine Notfallplanung, so dass bei Ausfall des Administrationsnetzes das produktive Netz weiterbetrieben werden kann?

# M 2.582 Möglichkeiten zur Einrichtung eines Managementnetzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Managementnetz stellt die Kommunikationsverbindungen zwischen dem Netz- bzw. Systemmanagement-System und den verwalteten Komponenten zur Verfügung. Hierfür stehen verschieden Varianten zur Auswahl:

- Out-of-Band: Es wird ein separates, physikalisches Managementnetz aufgebaut, dass ausschließlich für das Management der Netz- oder Systemkomponenten verwendet wird. Diese müssen demnach über eine zusätzliche Netzschnittstelle mit dem Managementnetz verbunden werden.
- In-Band: Die Netz- oder Systemkomponenten werden über das bestehende (Daten-)Netz verwaltet.
- Lokal: Die Netz- oder Systemkomponenten werden lokal z. B. über eine Konsole gewartet.
- Gemischtes Managementnetz: Kritische Netz- oder Systemkomponenten sind über ein Out-of-Band-Managementnetz angeschlossen und die anderen Systeme im Netz per In-Band-Management.

Out-of-Band-Management ist die sicherste, aber auch zugleich aufwändigste Variante eines Managementnetzes. Sie empfiehlt sich z. B. bei aktiven Netzkomponenten, deren Verfügbarkeit angegriffen werden kann, wie beispielsweise ein Perimeterrouter. Nur so kann im Falle eines Denial-of-Service-Angriffs mit der Netzkomponente kommuniziert werden.

Für große Netze empfiehlt sich zudem, über eine geeignete Segmentierung des Managementnetzes nachzudenken, um so beispielsweise Netzadministratoren nur Zugriff auf den Bereich des Netzes zu geben, für den sie zuständig sind.

Weit verbreitet ist In-Band-Management, da es kein zusätzliches Netz und keine zusätzlichen Schnittstellen an den Netz- oder Systemkomponenten benötigt. Hierfür sollte die Management-Kommunikation geschützt sein, was durch ein entsprechendes Management-Protokoll gewährleistet werden kann.

Eine ausschließlich lokales Management der Netz- oder Systemkomponenten ist nur in sehr kleinen Netzen möglich, aber auch dann nur in begründeten Ausnahmefällen einzusetzen.

Genauer zu betrachten ist die Verwaltung der IT-Systeme in der DMZ (Demilitarisierte Zone) eines Sicherheits-Gateways bei der Nutzung von SNMP als Netzmanagement-Protokoll. Die für das Sicherheitsgateway definierten Regeln sollen nicht für das Netzmanagement aufgeweicht werden.

Dies ist am einfachsten realisierbar, wenn ein Out-of-Band-Netz zur Kommunikation mit den überwachten Komponenten verwendet wird. Falls die Kommunikation In-Band durch das Sicherheitsgateway abläuft, sollte Folgendes beachtet werden:

Da oftmals keine UDP-Verbindungen aus einer DMZ in das interne Netz zugelassen werden sollen, kommt eine In-Band-Kommunikation über UDP zwischen einem Manager im internen Netz und Komponenten in der DMZ nicht in Frage. Für diesen Fall bieten diverse Hersteller Möglichkeiten an, die Managementinformationen über andere verbindungsorientierte Protokolle auszut-

auschen. Mangels eines einheitlichen Standards sei hier auf die Informationen der Hersteller verwiesen.

# M 2.583 Geeignete Auswahl eines Netzmanagement-Systems

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um ein komplexes Netz und dessen Komponenten zu verwalten, sollte ein geeignetes Netzmanagement-System ausgewählt werden. Dazu muss die aktuelle Netzsituation bestimmt (siehe M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*), ein Netzmanagement-Konzept festgelegt (siehe M 2.143 *Entwicklung eines Netzmanagement-Konzeptes*) und die Anforderungen an das Netzmanagement-System ermittelt werden (siehe M 2.145 *Anforderungen an ein Netzmanagement-Tool*). Je nach Größe des zu verwaltenden Netzes können hier unterschiedliche Realisierungen zweckmäßig sein:

- Für kleine und mittlere Netze kann das Netzmanagement durch eine Sammlung von einzelnen Tools durchgeführt werden oder aber durch ein Netzmanagement-System.
- Für große Netze sollte ein Netzmanagement-System benutzt werden.

Die Wahl des richtigen Netzmanagement-Systems ist deshalb sehr wichtig. Folgende Kriterien sollten bei der Wahl des zu beschaffenden Systems beachtet werden:

- Welchen Funktionsumfang bietet das Produkt an?
- Kosten
  - für die Anschaffung der Software
  - für die Anschaffung zusätzlicher Hardware (bei einigen Systemen müssen ein oder mehrere zentrale Managementserver angeschafft werden.)
  - für Installations- und Betriebsaufwand (u. U. müssen externe Experten beauftragt werden.)
  - für die Schulung der Administratoren
  - andere (z. B. Migrationskosten bei einer existierenden Plattform, Anpassung/Neuentwicklung lokaler Software, bauliche Maßnahmen z. B. gesicherter Serverraum)
- Investitionssicherung
  - Inwieweit ist das Netzmanagement-Produkt skalierbar (z. B. Anzahl der verwaltbaren Komponenten)?
  - Wie sind die Migrationspfade zur betrachteten Lösung?
  - Wie sind die Migrationspfade von dieser Lösung zu einem anderen Produkt?
- Integrationsmöglichkeit mit anderen Produkten
  - Kann ein bestehendes Netzmanagement-System integriert werden?
  - Kann ein bestehendes Datensicherungssystem integriert werden?
  - Welche Applikationen von Drittanbietern gibt es für dieses Produkt?
- Zuverlässigkeit und Ausfallsicherheit
  - Gibt es Aussagen oder sogar Garantien über maximale Ausfallzeiten?
  - Ist ein Hotswap für zentrale Komponenten möglich?
  - Existiert ein systemeigener Backup- und Recovery-Mechanismus? Bei einem Ausfall des Netzmanagement-Systems müssen innerhalb des Managementsystems Mechanismen zum geregelten Wiederanlaufen existieren. Dies umfasst u. U. das Einspielen von Daten

aus einer Datensicherung und die automatische Konsistenzprüfung, idealerweise mit Konfliktauflösung bei der Feststellung von Inkonsistenzen.
  - Werden regelmäßig Updates zur Verfügung gestellt? Sind sie einfach einspielbar?
- Sicherheit: Zugriffsbeschränkungen auf die Managementfunktionen
  - Kann eine Aufteilung der Administrationstätigkeiten vorgenommen werden? Kann also z. B. die Verwaltung von Komponenten auf bestimmte Bereiche eingeschränkt werden?
- Sicherheit: Netzadministration über das Netz
  - Wie sind Fernzugriffe abgesichert?
  - Können Fernzugriffe verschlüsselt erfolgen?
  - Ist sichergestellt, dass eine (starke) Authentisierung vor einer Fernadministration erforderlich ist?
  - Ist es möglich, die Berechtigung für Fernadministration auf bestimmte Personen oder Rollen einzuschränken?
  - Werden Benutzer automatisch über Fernzugriffe informiert?
- Sicherheit: Datensicherheit, Datenschutz
  - Werden die gesammelten Daten sicher abgelegt (Zugriffsbeschränkungen, Verschlüsselung)?
  - Findet die Datenübertragung zwischen den Managementkomponenten gesichert statt (Authentisierung, Verschlüsselung, Integritätssicherung)?
  - Ist die Integration von Virensuchprogrammen möglich?
  - Kann die Art der gesammelten Informationen reguliert werden (Anonymisierung, Rückverfolgung, Beweisbarkeit)?
  - Welche Protokollierungsmöglichkeiten werden angeboten?
- Benutzerfreundlichkeit
  - Gibt es ein graphisches Benutzerinterface?
  - Wie einfach ist die Navigation?
  - Wird die lokale Sprache oder auch mehrere Sprachen (bei globalem Einsatz) unterstützt?
  - Werden Ausnahmen und Alarmierungen geeignet angezeigt?
  - Ist das Monitoring, auch im Detailgrad, einstellbar?
  - Wird die Komplexität von Netzkomponenten geeignet "versteckt" (So dass der Benutzer nicht ein Experte für die jeweilige Komponente, die verwaltet werden soll, sein muss)?
  - Sind Onlinehilfen und Anleitungen vorhanden?
- Ergonomie beim Management komplexer Systeme
  - Werden verschiedene Netzprotokolle, Netzkomponenten und Betriebssysteme (z. B. von Routern) unterstützt?
  - Wie geht die Plattform mit geographisch verteilten Systemen um und wie ist deren Repräsentation?
  - Wie einfach ist es, neue Komponenten zu integrieren oder aus dem System zu entfernen (Autodiscovery, manuell)?
- Konformität zu Standards (je nach Umgebung kann die Konformität zu mindestens einem Standard erforderlich sein)
  - Application Program Interface (API), für den Fall, dass eigene Erweiterungen des Netzmanagement-Systems notwendig sind.

Die hier angeführten Aspekte sind als Anhaltspunkte bei der Bewertung von Managementsystemen zu verstehen. Je nach lokalen Gegebenheiten sollten Anforderungen an das Netzmanagement-System formuliert werden, die als

"K.O.-Kriterien" bei der Entscheidung herangezogen werden können. Die obigen Kriterien sollten immer eine Gewichtung erfahren, die die lokalen Präferenzen wiedergeben.

Die Anforderungen an das Netzmanagement-System und die Leistungen des ausgewählten Netzmanagement-Systems sind in der Regel nicht vollständig in Einklang zu bringen. Dies macht es notwendig, das erstellte Netzmanagement-Konzept nach Auswahl des konkreten Produktes an dessen Funktionsumfang anzupassen.

Prüffragen:

- Erfolgt die Auswahl eines geeigneten Netzmanagement-Systems auf Grundlage der zuvor festgestellten Anforderungen?

# M 2.584 Geregelte Außerbetriebnahme eines Netz- und Systemmanagement-Tools

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

In einem Netz- und Systemmanagement-Tool werden Daten über das Netz und die angeschlossenen Systeme gesammelt, verarbeitet und gespeichert. Diese Daten können unter anderem IP-Adressen, Benutzernamen und Namen von IT-Systemen enthalten. Daher muss sichergestellt werden, dass auf Festplatten und anderen Speichermedien keine schützenswerten Informationen mehr enthalten sind, wenn das Tool außer Dienst gestellt wird. Alle Datenträger müssen sicher gelöscht werden, bevor sie weitergegeben, repariert oder ausgesondert werden.

Im Fall einer Reparatur reicht es nicht aus, die Festplatten nur zu formatieren oder Löschfunktionen des Betriebssystems zu nutzen. Sie müssen mit geeigneten Löschprogrammen so überschrieben werden, dass die Daten nicht wiederhergestellt werden können. Weitere Informationen, wie Datenträger sicher gelöscht und vernichtet werden können, sind unter M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* zu finden. Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z. B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen und eventuell mit Schadensersatzansprüchen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Gegebenenfalls ist auf Garantieansprüche zu verzichten.

Wird ein Netz- und Systemmanagement-Tool ausgesondert, ist es empfehlenswert, die Speichermedien zusätzlich zur Löschung mechanisch zu vernichten ("schreddern"). Können die Speichermedien nicht zeitnah vernichtet werden, sind sie bis zur Zerstörung vor unberechtigtem Zugriff zu schützen. Magnetische Speichermedien lassen sich auch mittels eines Degaussers elektromagnetisch löschen.

Wenn die Datenträger durch Dritte gelöscht werden, muss der Auftrag unter anderem nach datenschutzrechtlichen Anforderungen vergeben und ein Auftragsdatenverarbeitungsvertrag geschlossen werden.

Prüffragen:

- Ist sichergestellt, dass sich nach der Außerbetriebnahme eines Netz- und Systemmanagement-Tools keine schützenswerten Daten mehr auf den Datenträgern befinden?

# M 2.585 Konzeption eines Identitäts- und Berechtigungsmanagements

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Diese Maßnahme beschreibt, welche grundsätzlichen Schritte im Rahmen eines Identitäts- und Berechtigungsmanagements durchgeführt werden müssen.

Um die Geschäftsprozesse, Informationen und IT-Systeme einer Institution angemessen schützen zu können, ist ein zweckmäßiges und passendes Identitäts- und Berechtigungsmanagement erforderlich. Als Grundlage hierfür müssen die rechtlichen, organisatorischen und technischen Rahmenbedingungen in der jeweiligen Institution geklärt werden. Darauf aufbauend muss eine generelle Vorgehensweise für den generellen Umgang mit Identitäten und Berechtigungen in den verschiedenen Bereichen der Institution festgelegt werden.

Immer wieder kommt es zu gravierenden Problemen, weil einzelne Benutzer unnötige Privilegien angehäuft haben oder oder ungenutzte Benutzerkennungen nicht gelöscht wurden, beispielsweise nach dem Weggang von Mitarbeitern. Um dies zu vermeiden, muss es daher oberstes Ziel des Identitäts- und Berechtigungsmanagements sein, allen legitimen Benutzern zu jeder Zeit genau die Rechte zuzuteilen, die für die Erfüllung ihrer jeweiligen Aufgaben notwendig sind (Prinzipien Need-to-Know und Least Privileges). Hierfür sind klar geregelte Verfahren und Sicherheitsvorgaben erforderlich. In einer Behörde oder einem Unternehmen gibt es normalerweise eine Vielzahl zu verwaltender Objekte und Benutzer. Es ist daher sinnvoll, das Identitäts- und Berechtigungsmanagement zentral zu regeln.

Das Berechtigungsmanagement sollte alle Arten und Varianten von Berechtigungen umfassen, die in der Institution relevant sind, also sowohl Zutritts-, Zugangs- und Zugriffsberechtigungen. Die Struktur der Berechtigungen sollte für alle Geschäftsprozesse und auf allen Systemen möglichst einheitlich sein, gleiche Rollen sollten auch mit den gleichen Namen bezeichnet werden. Ebenso muss festgelegt werden, in welcher Form und Struktur Informationen zu Identitäten erfasst werden.

Als einer der wichtigsten Punkte muss festgelegt werden, wer welche Aufgaben und Zuständigkeiten im Rahmen des Identitäts- und Berechtigungsmanagement hat. Häufig kümmert sich die Personalabteilung um die Aufgaben im Rahmen des Identitätsmanagements und der IT-Betrieb um das Berechtigungsmanagement.

Es sollte ein übergreifendes Konzept für das Identitäts- und Berechtigungsmanagement für die gesamte Institution geben, aus dem (wenn notwendig) für einzelne Bereiche oder Systeme angepasste Regelungen abgeleitet werden können. Das Konzept sollte die einzelnen Aufgaben und Prozessschritte für das Identitäts- und Berechtigungsmanagement beschreiben, die dann auf die einzelnen Bereiche angepasst werden müssen. Dazu gehören:

- Erstellung eines Überblicks über Gruppen und Arten von Identitäten und Berechtigungen, die typischerweise in den verschiedenen Bereichen einer Institution verwaltet werden,
- Vorgaben zur Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen,

- Umgang mit den Benutzerkennungen, Berechtigungen und Authentisierungsmitteln durch die Benutzer,
- Vorgaben zum Umgang mit Kennungen von Administratoren, Notfallbenutzern und anderen priviligierten Benutzern sowie Vorgaben der Gewährung von zeitlich eingeschränktem Zugriff auf erweiterte Berechtigungen,
- Festlegung von Berechtigungsstrukturen, Dokumentation und Genehmigungsverfahren für die Vergabe von Berechtigungen,
- Festlegen und Einhalten von Administrationsprozessen,
- Vorgaben zur Erstellung und restriktiven Zuweisung von Berechtigungen auf den Zielsystemen
- regelmäßige Überprüfung der Berechtigungen darauf, ob
- - alle Personen und Prozesse die notwendigen Berechtigungen haben, also weder zuviel noch zu wenig (Need-to-Know und Least Privileges),
  - alle Berechtigungen aktuell sind, es also z. B. keine Benutzerkennungen gibt, die nicht mehr aktiv sind, aber nicht gelöscht wurden,
  - Berechtigungen Benutzern unter Umgehung des Identitäts- und Berechtigungsmanagements direkt auf den Zielsystemen zugewiesen wurden.

Grundsätzlich ist für jeden Bereich zunächst zu klären, welchen Schutzbedarf die zu schützenden Informationen und Geschäftsprozesse haben, welche Gefährdungen relevant sind und welche Sicherheitsmaßnahmen bereits vorhanden sind. Außerdem muss geregelt werden, wer die Informationen und Geschäftsprozesse wie nutzen darf.

**Richtlinien erstellen**

Es sollten Richtlinien für das Identitäts- und Berechtigungsmanagement geben, in denen spezifisch für den betreffenden Bereich und die Zielgruppe (z. B. Administratoren, Benutzer, Fachverantwortliche) die einzelnen Aufgaben und Prozessschritte beschrieben werden. Dazu gehören die folgenden Punkte:

- Wer ist zuständig für die Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen?
- Wer darf Berechtigungen genehmigen?
- Was müssen die Benutzer wissen über den korrekten Umgang mit den Benutzerkennungen, Berechtigungen und Authentisierungsmitteln?

Außerdem sollte es Vorgaben an Art und Ausgestaltung der jeweiligen Authentisierung geben, z. B. über die Art der Authentisierung über Besitz, Wissen oder biometrische Eigenschaften sowie Mindestanforderungen an Passwörter (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle* und M 2.11 *Regelung des Passwortgebrauchs*).

Zu regeln ist auch, welche Personen auf welche Weise Zugriff auf welche Informationen erhalten, also z. B. nur aus dem Intranet oder von unterwegs und welche IT-Systeme dabei für Zugriffe zugelassen sind.

Dabei müssen die spezifischen Rahmenbedingungen berücksichtigt werden, wie z. B. vorhandene Sicherheitsrichtlinien und gesetzliche Vorgaben. Bereits vorhandene Berechtigungskonzepte müssen konsolidiert und in einem übergreifenden Konzept zusammengeführt werden. Dabei dürfen auch verstreute Anwendungen nicht vergessen werden. Daher ist der Einsatz von Werkzeugen zur Benutzer- und Rechte-Verwaltung meistens sinnvoll.

**Funktionen trennen**

Ein Identitäts- und Berechtigungsmanagement muss den Ansatz verfolgen, Aufgaben und Funktionen und somit auch Berechtigungen geeignet zu tren-

nen und entsprechend gesetzlicher oder organisatorischer Vorgaben auf verschiedene Mitarbeiter zu verteilen (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*).

**Rollen trennen**

Personen können verschiedene Rollen wahrnehmen. Dabei müssen diese Rollen aber organisatorisch und technisch klar voneinander getrennt werden, insbesondere bei unterschiedlichen Sicherheitsanforderungen. Die Konzentration mehrerer sicherheitskritischer Rollen auf eine Person sollte verhindert werden (wie Administration und Prüfung, siehe auch M 2.38 *Aufteilung der Administrationstätigkeiten*).

**Berechtigungen anlegen, ändern und löschen**

Im Mittelpunkt des Identitäts- und Berechtigungsmanagement steht, dass Berechtigung angelegt, geändert und gelöscht werden (siehe M 2.586 *Einrichtung, Änderung und Entzug von Berechtigungen* ).

**Mit Passwörtern umgehen**

Es muss geregelt werden, wie Authentikationsmechanismen anzuwenden sind. Außerdem müssen die Benutzer darin eingewiesen worden sein (siehe beispielsweise M 4.1 *Passwortschutz für IT-Systeme*, M 4.7 *Änderung voreingestellter Passwörter* und M 3.63 *Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten*).

In jeder Institution muss es eine geeignete Vorgehensweise für den Umgang mit Identitäten und Berechtigungen geben. Es wird daher empfohlen, die Aufgaben aus den generischen Prozesse der Maßnahme M 2.587 *Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement* in der Institution sinngemäß einzurichten.

Prüffragen:

- Ist festgelegt worden, wer welche Aufgaben und Zuständigkeiten im Rahmen des Identitäts- und Berechtigungsmanagement hat?
- Existiert ein Konzept für das Identitäts- und Berechtigungsmanagement?

# M 2.586 Einrichtung, Änderung und Entzug von Berechtigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

In einer Institution müssen eine Vielzahl verschiedener Berechtigungen pro Benutzer vergeben und verwaltet werden (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*, M 2.7 *Vergabe von Zugangsberechtigungen*, M 2.8 *Vergabe von Zugriffsrechten*).

Für die Zuweisung und Verwaltung von aufgabenspezifischen Berechtigungen ist die Entwicklung eines Rollenmodells für die jeweilige Anwendung bzw. für das jeweilige System empfehlenswert. Dies macht die Verwaltung übersichtlicher und einfacher.

Benutzerkennungen und Berechtigungen unterliegen einem Lebenszyklus, sie werden angelegt, geändert und gelöscht. Berechtigungen sollten zentral verwaltet werden, hilfreich sind dabei angemessene Benutzer- und Rechtemanagement-Werkzeuge, um den Administrations- und Pflegeaufwand zu reduzieren.

**Einrichtung und Änderungen von Berechtigungen**

Bei der Einrichtung von Benutzerkennungen und Berechtigungen sind häufig Vielzahl von Genehmigungsschritten erforderlich, die zusammengetragen und verfolgt werden müssen. Daher ist es empfehlenswert, hierfür ein standardisiertes und möglichst automatisiertes Antrags- und Vergabeverfahren zu nutzen.

Beim Identitäts- und Berechtigungsmanagement können folgende generische Rollen betrachtet werden:

- Benutzer: Dies ist die Einzelperson, die auf die Informationen, Anwendungen oder IT-Systeme unter der Benutzerkennung zugreift. Mit Ausnahme von Gruppenkennungen ist der Benutzer normalerweise identisch mit dem Besitzer.
- Genehmigende: Dies ist die Person, die die Vergabe von Zugangs-, Zugriffs oder Zutrittsrechten genehmigt, typischerweise die Fachverantwortlichen. Ein Genehmigender sollte keine Rechte für sich selbst genehmigen dürfen.
- Fachverantwortliche: Die Fachverantwortlichen sind die "Eigentümer" von Informationen, Anwendungen, Fachverfahren, Geschäftsprozessen oder Systemen. Diese haben das letzte Wort zu allen Fragen im Zusammenhang mit Inhalten und Verwendung sowie Anforderungen der jeweiligen Informationen, Anwendungen oder Systeme.
- IT-Betrieb: Die Mitarbeiter des IT-Betriebs haben die Aufgabe, die genehmigten Berechtigungen technisch einzurichten.

Generell sollten Benutzerkennungen und Berechtigungen immer nur sollten auf der Grundlage eines legitimen Bedarfs zur Erfüllung zugewiesener Tätigkeiten vergeben werden, also so, wie es für die Aufgabenwahrnehmung notwendig ist (Prinzip Need-to-know. Berechtigungen sollten außerdem immer restriktiv vergeben vergeben. Es dürfen immer nur so viele Rechte vergeben werden, wie im aktuellen Kontext zur Durchführung der fachlichen Aufgabe benötigt werden (Prinzip der geringsten Berechtigungen, englisch Least Privileges).

Bevor neue Benutzerkennungen eingerichtet oder Berechtigungen vergeben werden, ist Folgendes zu beachten:·

- Es muss ein Antrag gestellt werden, aus dem die Rolle, Funktionsbreite und auch zeitliche Begrenzungen der Aufgaben des Antragsstellers erkennbar sind. Es empfiehlt sich, die Form der Anträge vorzugeben, damit alle erforderlichen Informationen erfasst werden (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*). Hierfür können Formblätter, Webformulare oder E-Mails verwendet werden. Anträge sollten einfach zu stellen und zu bearbeiten sein, aber auch alle erforderlichen Informationen enthalten.
- Dieser Antrag muss durch die entsprechend der Art der Berechtigung zuständige Rolle genehmigt werden. Privilegierte Benutzerkennungen müssen zusätzlich vom Fachverantwortlichen der jeweiligen Ressource genehmigt werden.
- Alle Vergaben, Änderungen und Löschungen von Berechtigungen müssen dokumentiert aufbewahrt werden.
- Jede Benutzerkennung muss eindeutig einem registrierten Benutzer zugeordnet werden können. Ebenso muss für jede Gruppenkennung eindeutig nachweisbar sein, welche Personen dieser Gruppe zugehören. Für jede Gruppenkennung muss eine einzelne Person bzw. ein Rolleninhaber als für die Nutzung der Kennung verantwortlich benannt sein.
- Bevor einer Person eine Benutzerkennung oder ein Authentisierungsmittel wie ein Passwort zugeteilt wird, muss diese auf die Einhaltung aller Sicherheitsvorgaben und regelungen verpflichtet werden.
- Passwörter für Erst-Anmeldungen müssen bei der ersten Anmeldung des Benutzers geändert werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).
- Es muss sichergestellt sein, dass nur die berechtigten Benutzer die Zurücksetzung eines Passwortes oder Anpassung eines Authentikationsmittels anfordern können.
- Es sollte nach Möglichkeit vermieden werden, Gruppenkennungen einzurichten, wenn dies die Zuordnung zu handelnden Personen erschwert. Dies gilt vor allem für administrative Kennungen und sicherheitsrelevante Bereiche.

Wird ein Zugriff auf Daten benötigt, ohne dass der Besitzer der Kennung zugestimmt hat, muss dieser Zugriff sowohl von einem autorisierten Genehmigenden als auch vom IT-Sicherheitsbeauftragten genehmigt werden. Ein solcher Zugriff ist zu dokumentieren und dem Besitzer mitzuteilen.

**Entzug von Berechtigungen**

Wenn Mitarbeiter die Institution verlassen oder die Position wechseln, müssen die nicht mehr benötigten Benutzerkennungen und Berechtigungen innerhalb einer definierten Zeit gesperrt und nach einer definierten Wartezeit vollständig gelöscht werden. Dabei kann es sinnvoll sein, zwar die Berechtigungen zu löschen, aber in den Unterlagen zu dokumentieren, von wann bis wann die Benutzerkennung welche Berechtigungen hatte, um auch Aktionen nach dem Weggang von Mitarbeitern nachvollziehbar zu halten. Wichtig ist, dass die Berechtigungen durchgängig geändert bzw. entfernt werden.

Zum Entzug bzw. zur Sperrung von Benutzerkennungen und Authentikationsmitteln gehört beispielsweise, dass Benutzerkennungen deaktiviert, Passwörter geändert und Mitarbeiterausweise eingezogen werden. Außerdem muss die Benutzerkennung in Rollenzuweisungen und Gruppen entfernt werden. Voraussetzung dafür ist, dass die für das Berechtigungsmanagement zuständige Stelle zeitnah informiert wird, wenn Mitarbeiter ausscheiden. Gegebe-

nenfalls ist ein entsprechender Punkt in eine einschlägige Checkliste der Personalabteilung aufzunehmen.

Es wird empfohlen, Benutzerkennungen zunächst lediglich zu deaktivieren (beispielsweise für 30 Tage), damit sie im Fehlerfall leicht wieder eingerichtet werden können. Alle Benutzerkennungen und damit verbundene Daten müssen jedoch mittelfristig, z. B. innerhalb von 90 Tagen, nach Weggang des Mitarbeiters von den Produktivsystemen entfernt werden. Um die dort gespeicherten Informationen und die Nachvollziehbarkeit von Tätigkeiten für einen längeren Zeitraum sicherzustellen, sollten die Daten in einen anderen Bereich, also z. B. ein Archivsystem, mit geeignetem Besitzer (z. B. Audit) kopiert werden.

Prüffragen:

- Werden alle Benutzerkennungen und Berechtigungen ausschließlich auf Basis des tatsächlichen Bedarfs vergeben?
- Werden bei personellen Veränderungen die nicht mehr benötigten Benutzerkennungen und Berechtigungen unbrauchbar gemacht?
- Werden die vorgenommenen Berechtigungsänderungen dokumentiert?

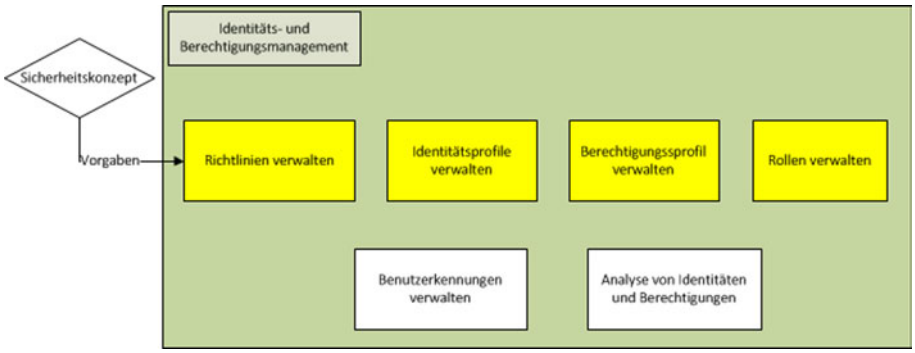
# M 2.587 Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, IT-Sicherheitsbeauftragter

Die Verwaltung von Identitäten und Berechtigungen wird mit steigender Benutzerzahl immer aufwendiger. Je mehr manuelle Aktivitäten erforderlich sind, um so mehr Fehler und Sicherheitsprobleme können entstehen.

Daher ist es zu empfehlen, dass auch kleinere Institutionen ein Identitäts- und Berechtigungsmanagement aufbauen und betreiben. Im Folgenden werden generische Prozesse für das Identitäts- und Berechtigungsmanagement beschrieben, die aufzeigen, wie die erforderlichen Aufgaben und Anforderungen erfüllt werden können.

Ein Identitäts- und Berechtigungsmanagement besteht aus folgenden generischen Prozessen:




Identitäts- und Berechtigungsmanagement

Abgeleitet aus dem Sicherheitskonzept einer Institution sollten die Vorgaben mit Bezug auf das Identitäts- und Berechtigungsmanagement in einer Richtlinie beschrieben werden. Die Richtlinie sollte mindestens die umfassen, wie Identitäten, Benutzerkennungen und Berechtigungen angelegt, verändert, gelöscht und kontrolliert werden.

In jeder Institution muss es eine geeignete Vorgehensweise für den Umgang mit Identitäten und Berechtigungen geben. Es wird daher empfohlen, die Aufgaben aus den generischen Prozesse der folgend beschriebenen Maßnahmen für ein effizientes Identitäts- und Berechtigungsmanagement in der Institution sinngemäß einzurichten.

### Prozess Richtlinien verwalten

Im Rahmen des Prozesses *Richtlinien verwalten* werden Richtlinien für die Beantragung, Veränderung und dem Entzug von Rollen und (Einzel-)Berechtigungen und die Verwaltung von Identitäten und Benutzerkonten innerhalb von IT-Systemen erstellt, überprüft und fortgeschrieben.

In der Richtlinie zum Identitäts- und Berechtigungsmanagement werden die Vorgehensweisen zu den folgenden Teilprozessen beschrieben und wie diese zusammenspielen sollten:

- *Identitätsprofile verwalten*,
- Berechtigungsprofile verwalten,
- Benutzerkennungen verwalten,
- Rollen verwalten,
- *Analyse von Identitäten und Berechtigungen* und
- Konten verwalten.

Vergabe, Änderungen und Löschungen von Berechtigungen müssen protokolliert und für eine zu definierende Zeit (z. B. 10 Jahre) aufbewahrt werden. Die Richtlinien sollen bei wesentlichen Änderungen oder zeitlich gesteuert einem Review unterzogen werden.

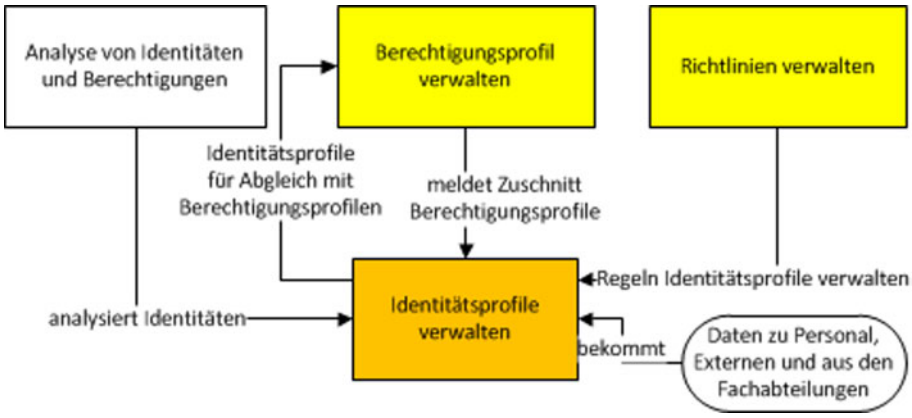
**Prozess Identitätsprofile verwalten**

Der Prozess *Identitätsprofile verwalten* umfasst die Erfassung, Veränderung und das Löschen von Identitätsprofilen. Identitätsprofile sind beispielsweise Stammdaten von Mitarbeitern einer Institution. Typische Eigenschaften, die verarbeitet werden, sind u.a.:

- Name
- Organisationseinheit
- Aufgabenbeschreibung

Die Verarbeitung der Informationen im Prozess *Identitätsprofile verwalten* wird in Form von Anträgen (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*) initiiert. Die Anträge enthalten die wichtigen Informationen zu einem Mitarbeiter (gilt auch für IT-Systeme) als auch die entsprechende Aufgabenbeschreibung. Die Anträge können z. B. aus den Prozessen der Mitarbeitereinstellung oder der Veränderung von Aufgabenbeschreibungen (z. B. Mitarbeiter übernimmt eine andere Aufgabe) ausgelöst werden. Die Änderungen werden in einem Identitätsprofil dokumentiert.

Das Ergebnis aus dem Prozess *Identitätsprofile verwalten* ist die Komplettierung eines Identitätsprofils mit Stammdaten und einer konkreten Aufgabenbeschreibung. Es muss geregelt sein, wer die Berechtigungsvergabe initiiert und der Vorgang als Ganzes muss dokumentiert werden.




Prozess Identitätsprofile verwalten

Im Folgenden werden Stellen einer Institution aufgelistet, wo eine Neueinrichtung bzw. eine Veränderung von Identitätsprofilen erfolgen kann:

- Personalzu- oder -abgänge von Mitarbeitern oder Externen, Aufgabenänderungen (Personalabteilung, Verwaltung, Fachabteilung)
- Externe Mitarbeiter / Zu- und Abgang, Änderung (Einkauf, Beschaffung)
- Berechtigte Dritte, z.B. Kunden / Zu- und Abgang, Änderung (Vertrieb, Support u.a.)

Der Prozess *Analyse von Identitäten und Berechtigungen* untersucht die Identitäten gemäß dem Antrag auf den Bedarf an Sicherheit. Der Prozess *Richtlinie verwalten* regelt die Rahmenbedingung für das Einrichten und Verändern von Identitäten. Mit den Ergebnissen aus den Prozessen *Analyse von Identitäten und Berechtigungen* und *Richtlinie verwalten* können die Informationen gemäß dem Antrag eingerichtet, verändert oder gelöscht werden. Die Informationen der erstellten bzw. überarbeiteten Identitätsprofile werden mittels dem Antrag dem Prozess *Benutzerprofil verwalten* zur weiteren Verarbeitung übertragen.

**Prozess Berechtigungsprofil verwalten**

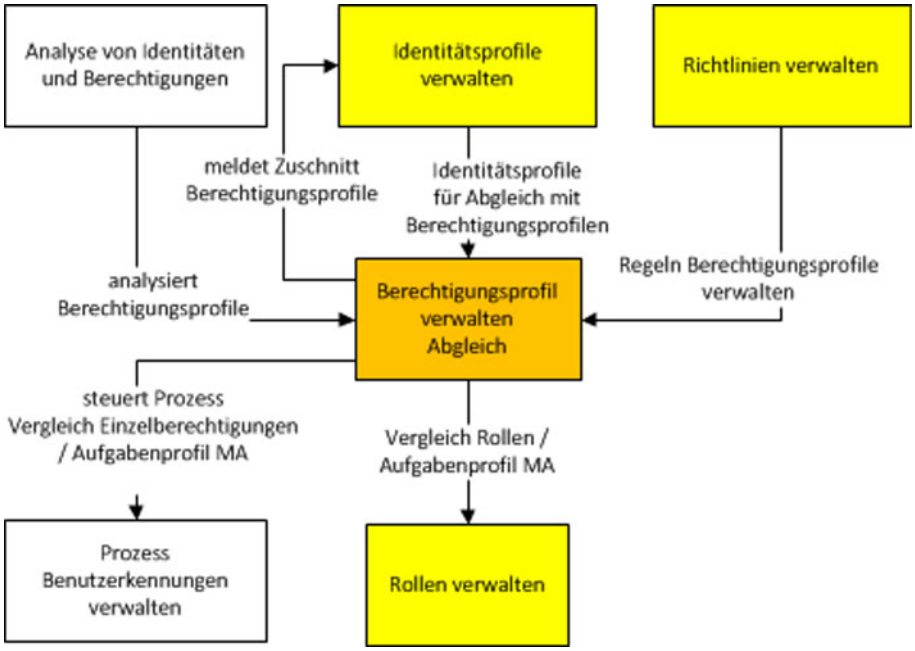
Der Prozess *Berechtigungsprofil verwalten* beschreibt das Verfahren für einen Abgleich zwischen der Aufgabenbeschreibung, welche in dem Prozess *Identitätsprofile verwalten* verfasst wurden, und den dazugehörigen Rollen und Einzelberechtigungen für einen Mitarbeiter.

Für das Verfahren *Abgleich* benötigt der Prozess *Berechtigungsprofil verwalten* diverse Informationen über die Identitätsprofile aus verschiedenen Quellen, z. B. aus der Personalverwaltung Stammdaten der Mitarbeiter oder aus den Fachabteilungen über deren Fachaufgaben. Dazu gehören auch vergleichbare Informationen zu externen Mitarbeitern sowie zu technischen Berechtigungen von IT-Systemen .

In einem Mitarbeiter-Berechtigungsprofil werden alle Rollen und Einzelberechtigungen verwaltet, die diesem zugeordnet sind. Das Verhältnis zwischen rollenbasierten Berechtigungen und Einzelberechtigungen ist qualitativ und damit mittelbar auch für die IT-Sicherheit relevant. Erfahrungen haben gezeigt, dass reine rollenbasierte Berechtigungsvergaben zu starr sind und daher nicht funktionieren. Hingegen erfordert ein zu hoher Anteil von Einzelberechtigungen einen zu großen Wartungsaufwand. Daher wird aus der Praxis ein Richtwert von 80:20 für das Verhältnis zwischen rollenbasierten Berechtigungen und Einzelberechtigungen empfohlen.

Untersucht werden muss, ob Aufgaben und die dazugehörigen Berechtigungen miteinander vereinbar sind (Prozess *Analyse von Identitäten und Berech-*

*tigungen)* oder unter Umständen neu verteilt werden müssen (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*).

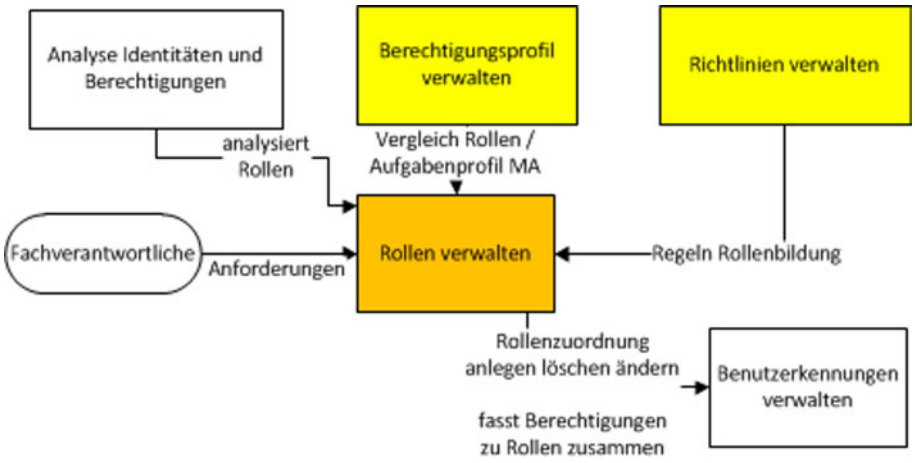



Prozess Berechtigungsprofile verwalten

**Prozess Rollen verwalten**

Im Prozess *Rollen verwalten* werden Berechtigungsprofile für einzelne Rollen angelegt. In Rollen werden Aufgaben, Verantwortlichkeiten und damit zusammenhängende Berechtigungen gebündelt, um die Benutzerverwaltung zu erleichtern. Ein Rollen-Berechtigungsprofil kann als für die gleiche Tätigkeit mehrerer Mitarbeiter verwendet werden. Dazu werden der Rolle die Zugangsberechtigungen zugeordnet, die für die Aufgabenerfüllung notwendig ist. Rollen sollten modular und in sich geschlossen definiert werden, so dass sie beliebig kombinierbar sind. Der Rollenzuschnitt muss auf Ebene der Fachverantwortlichen abgestimmt werden.

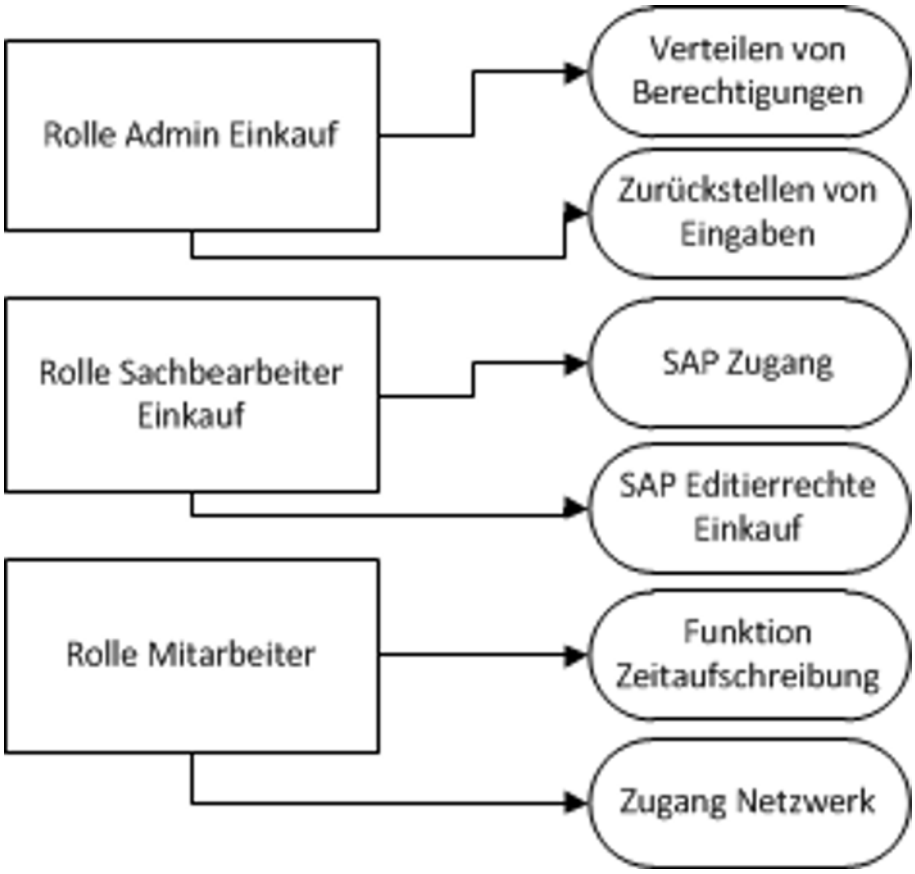
Im Grunde besteht der Prozess *Rollen verwalten* aus zwei Ebenen. Die Ebene der Fachverantwortlichen definiert die Rollen und die administrative Ebene legt Berechtigungsprofile für diese Rollen an, ändert und löscht sie.




Prozess Rollen verwalten

Der Prozess *Richtlinien verwalten* gibt Regeln für die Rollenbildung vor. Zwischen dem Prozess *Identitätsprofile verwalten* und dem Prozess *Rollen verwalten* erfolgt der Vergleich der Aufgabenprofile von Mitarbeitern und den tatsächlich zugeordneten Rollen (Soll-Ist-Abgleich). Im Prozess *Benutzer verwalten* wird die Zuordnung von Rollen zu Mitarbeitern angelegt, gelöscht oder geändert. Im Prozess *Rollen verwalten* werden Einzelberechtigungen zu einem Berechtigungsprofil für ein Benutzerkonto in der Kontenverwaltung zusammengefasst. Der Prozess *Sicherheit der Profile analysieren* untersucht die Rollen und klassifiziert den jeweiligen Bedarf an Sicherheit.

Eine Rolle kann wie folgt aufgebaut sein:




Beispiel für Rollen mit Berechtigungen

***Prozess Benutzerkennungen verwalten***

Der Prozess *Benutzerkennungen verwalten* beschreibt den operativen Anteil der Prozesse innerhalb des Identitäts- und Berechtigungsmanagements und umfasst das Anlegen, das Löschen und das Ändern von Benutzerkennungen, Initialpasswörtern und Berechtigungen. Generische Vorgänge sind z. B.:

- Neue Mitarbeiter,
- Anlage neuer Benutzerkennungen,
- Weggang von Mitarbeitern,
- Veränderung von Aufgaben,
- Kennungen bei längeren Abwesenheiten sperren,
- Löschen der Benutzerkennung.

Im Rahmen des Vorgangs "Neue Mitarbeiter" muss eine Benutzerkennung erstellt werden, ein Initialpasswort vergeben werden, Mitarbeiterstammdaten erfasst, die Zuordnung zur Organisationseinheit erfolgen sowie Rollen und Berechtigungen zugewiesen werden. Eine Neuanlage erfolgt auch zur Schaffung zusätzlicher Benutzerkennungen.

Der Vorgang "Weggang von Mitarbeitern" umfasst das vollständige Löschen aller Rollenzuordnungen und Berechtigungen für den jeweiligen Mitarbeiter sowie, falls erforderlich, die Rückgabe von Authentisierungstoken.

Der Vorgang "Veränderung von Aufgaben" umfasst den Wechsel einer Organisationseinheit, den Ein- und Austritt in Projekten und andere Aufgabenänderungen mit dem jeweiligen Datum. Es kann erforderlich sein, dass einige Berechtigungen vor oder nach der erfolgten Aufgabenänderung zugewiesen werden.

Der Vorgang "Kennungen sperren bei längeren Abwesenheiten" erfolgt bei längerer Abwesenheit von Mitarbeitern, z. B. bei Erziehungsurlaub oder Reha-Maßnahmen. Die Berechtigungen bleiben während des Zeitraums erhalten.

Der Vorgang "Löschen der Benutzerkennung" enthält das vollständige Löschen der Benutzerkennung einschließlich aller Stammdaten und Berechtigungen.

Jede Benutzerkennung muss eindeutig einem Mitarbeiter als Besitzer zugeordnet sein. Bei Gruppen- und Systemkennungen muss mindestens eine Person als verantwortlich benannt werden.

Mitarbeiter können mehrere Benutzerkennungen haben. Es ist zu klären, ob

- die Benutzerkennungen getrennt geführt werden,
- die Benutzerkennungen getrennt geführt, aber verkettet werden, oder
- die Benutzerkennungen zusammengeführt werden sollen.

Auf jeden Fall ist es zweckmäßig, automatisch zu prüfen, ob es Doppeleinträge (Dubletten) gibt. Solche Einträge führen zu Intransparenz im Identitäts- und Berechtigungsmanagement.

Die folgende Abbildung zeigt den Prozess *Benutzerkennungen verwalten* mit den entsprechenden Schnittstellen.


Prozess Benutzerkennung verwalten

Im Prozess *Benutzerprofile verwalten* erfolgt das Mapping zwischen den Aufgaben eines Mitarbeiters und den entsprechenden Rollen und Berechtigungen. Der Prozess *Benutzerkennungen verwalten* führt die logische Zuordnung der Berechtigungen zu einer Aufgabe innerhalb der IT-Systeme durch. Der Prozess *Richtlinien verwalten* gibt die Rahmenbedingungen vor, wie die Zuordnung der Berechtigungen in den IT-Systemen erfolgt. Zum Abschluss des Prozesses *Benutzerkennungen verwalten* liegt eine eingerichtete oder veränderte Benutzerkennung inklusive der entsprechenden Berechtigungen vor.

**Unterstützende Prozesse**

Der Prozess *Benutzerkennungen verwalten* beschreibt die unterstützenden Abläufe zur Durchführung des Prozesses *Benutzerkennungen verwalten*. Damit werden insbesondere die IT-nahen Aktivitäten erfasst.

Der Prozess *Benutzerkennungen verwalten* umfasst die folgende Subprozesse:

- Dokumentation Benutzerkennungen anlegen, ändern, sperren und löschen,
- Passwörter zurücksetzen, Benutzerkennungen entsperren,
- Benutzerkennungen /Protokoll-Dateien auditieren.

**Dokumentation Benutzerkennungen anlegen, ändern, sperren und löschen:**

Einzelberechtigungen und Benutzerkennungen dürfen nur angelegt, gelöscht und geändert werden, wenn es dazu einen legitimierten Antrag gibt. Dies ist zu dokumentieren.

Bei einer manuellen Administration sollen mindestens zwei Verantwortliche die Aufgaben innerhalb des Prozesses durchführen können und sich damit gegenseitig unterstützen und kontrollieren.

**Passwörter zurücksetzen, Benutzerkennungen entsperren:**

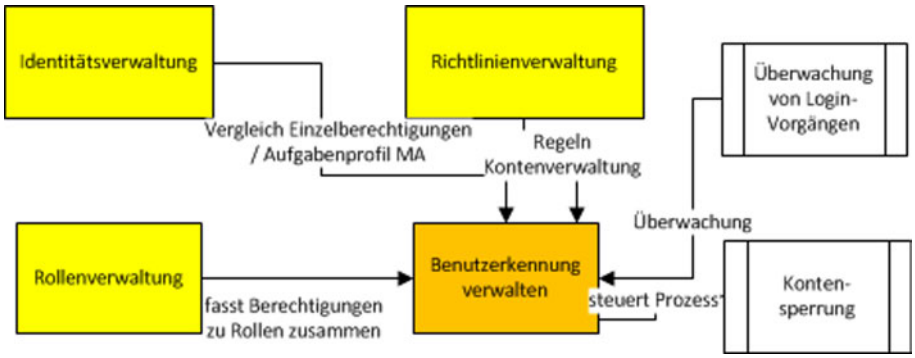
Dieser Subprozess umfasst die Tätigkeiten Passwort zurücksetzen, Benutzerkennungen entsperren sowie die vertrauliche Übermittlung des Benutzernamens und des Passwortes an den Benutzer. Es muss sichergestellt sein, dass nur die berechtigten Benutzer ihre Passwörter zurücksetzen oder die Anpassung eines Authentikationsmittels anfordern können.

**Benutzerkennungen prüfen / Protokolldateien auditieren:**

Die Zulässigkeit von Berechtigungen einzelner Benutzerkennungen sollte regelmäßig überprüft werden, der begleitende Subprozess *Dokumentation Benutzerkennungen anlegen, ändern, sperren und löschen* bietet die notwendigen Informationen.

Es gehört zu einem sicheren Identitäts- und Berechtigungsmanagement, die Zugriffsprotokolle regelmäßig auszuwerten. Es ist zu untersuchen, ob nur zugelassene Kennungen in einem System aktiv sind. Helfen können dabei automatische Vergleiche zwischen den aktiven Benutzerkennungen und den genehmigten Benutzerkennungen. Bei Bedarf können weitere Aspekte analysiert werden. Bei Verdacht auf einen Sicherheitsvorfall ist eine systematische Auswertung erforderlich.

Sofern Mitarbeiter berechtigt sind, Stammdaten und Passwörter eigenständig zu bearbeiten, muss sichergestellt werden, dass sie nur auf die eigenen Daten zugreifen können.




Unterstützende Prozesse Benutzerkennung verwalten

**Prozess Analyse von Identitäten und Berechtigungen**

Für Neueinrichtungen oder Änderungen von Identitäten, Benutzerprofilen und Rollen muss das angestrebte Sicherheitsniveau berücksichtigt werden. Es sollte eine festgelegte Vorgehensweise für Neueinrichtungen, Veränderungen und Rücknahme von Identitäten, Berechtigungsprofilen und Rollen geben, die auf den Sicherheitsbedarf der Informationen ausgerichtet ist. Je größer eine

Institution ist, desto mehr Identitäten, Benutzerprofile und Rollen sind zu verwalten und desto wichtiger ist eine nachvollziehbare, formale Vorgehensweise.

Im Prozess werden folgende Informationsquellen untersucht:

- Rollen aus dem Prozess *Rollen verwalten*
- Berechtigungsprofile aus dem Prozess *Berechtigungsprofile verwalten*
- Identitätsprofile aus dem Prozess *Identitätsprofile verwalten*

Die Ergebnisse werden den Quellprozessen zur Weiterverarbeitung übergeben.

Als Ergebnis des Prozesses *Analyse von Identitäten und Berechtigungen* wird geregelt, wer welche Informationen und IT-Anwendungen in welchem Umfang nutzen darf, z. B. können Berechtigungen auf mehrere Benutzerkennungen verteilt werden (siehe hierzu M 2.5 *Aufgabenverteilung und Funktionstrennung*). Um entscheiden zu können, ob die vorgefundenen oder zu vergebenden Berechtigungen für das angestrebte Sicherheitsniveau angemessen sind, müssen alle Informationen, IT-Systeme und Dienstleistungen entsprechend von den Fachverantwortlichen analysiert werden (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

# M 3 Maßnahmenkatalog Personal

M 3.25 Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer **- entfallen**

M 3.26 Einweisung des Personals in den sicheren Umgang mit IT

M 3.27 Schulung zur Active Directory-Verwaltung

M 3.28 Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen

M 3.29 Schulung zur Administration von Novell eDirectory

M 3.30 Schulung zum Einsatz von Novell eDirectory Clientsoftware

M 3.31 Schulung zur Systemarchitektur und Sicherheit von Exchange-Systemen für Administratoren

M 3.32 Schulung zu Sicherheitsmechanismen von Outlook für Benutzer

M 3.33 Sicherheitsüberprüfung von Mitarbeitern

M 3.34 Einweisung in die Administration des Archivsystems

M 3.35 Einweisung der Benutzer in die Bedienung des Archivsystems

M 3.36 Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS **- entfallen**

M 3.37 Schulung der Administratoren eines Apache-Webservers **- entfallen**

M 3.38 Administratorenschulung für Router und Switches

M 3.39 Einführung in die zSeries-Plattform

M 3.40 Einführung in das z/OS-Betriebssystem

M 3.41 Einführung in Linux und z/VM für zSeries-Systeme

M 3.42 Schulung des z/OS-Bedienungspersonals

M 3.43 Schulung der Administratoren des Sicherheitsgateways

M 3.44 Sensibilisierung des Managements für Informationssicherheit

M 3.45 Planung von Schulungsinhalten zur Informationssicherheit

M 3.46 Ansprechpartner zu Sicherheitsfragen

M 3.47 Durchführung von Planspielen zur Informationssicherheit

M 3.48 Auswahl von Trainern oder externen Schulungsanbietern

M 3.49 Schulung zur Vorgehensweise nach IT-Grundschutz

M 3.50 Auswahl von Personal

M 3.51 Geeignetes Konzept für Personaleinsatz und -qualifizierung

M 3.52 Schulung zu SAP Systemen

M 3.53 Einführung in SAP Systeme

| | |
|---|---|
| M 3.54 | Schulung der Administratoren des Speichersystems |
| M 3.55 | Vertraulichkeitsvereinbarungen |
| M 3.56 | Schulung der Administratoren für die Nutzung von VoIP |
| M 3.57 | Szenarien für den Einsatz von VoIP |
| M 3.58 | Einführung in WLAN-Grundbegriffe |
| M 3.59 | Schulung zum sicheren WLAN-Einsatz |
| M 3.60 | Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten |
| M 3.61 | Einführung in Verzeichnisdienst-Grundlagen |
| M 3.62 | Schulung zur Administration von Verzeichnisdiensten |
| M 3.63 | Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten |
| M 3.64 | Einführung in Active Directory |
| M 3.65 | Einführung in VPN-Grundbegriffe |
| M 3.66 | Grundbegriffe des Patch- und Änderungsmanagements |
| M 3.67 | Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten |
| M 3.68 | Schulung der Administratoren eines Samba-Servers |
| M 3.69 | Einführung in die Bedrohung durch Schadprogramme |
| M 3.70 | Einführung in die Virtualisierung |
| M 3.71 | Schulung der Administratoren virtueller Umgebungen |
| M 3.72 | Grundbegriffe der Virtualisierungstechnik |
| M 3.73 | Schulung der Administratoren eines DNS-Servers |
| M 3.74 | Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren |
| M 3.75 | Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer |
| M 3.76 | Einweisung der Benutzer in den Einsatz von Groupware und E-Mail |
| M 3.77 | Sensibilisierung zur sicheren Internet-Nutzung |
| M 3.78 | Korrektes Auftreten im Internet |
| M 3.79 | Einführung in Grundbegriffe und Funktionsweisen von Bluetooth |
| M 3.80 | Sensibilisierung für die Nutzung von Bluetooth |

M 3.81 Schulung zum sicheren Terminalserver-Einsatz

M 3.82 Schulung zur sicheren Nutzung von TK-Anlagen

M 3.83 Analyse sicherheitsrelevanter personeller Faktoren

M 3.84 Einführung in Exchange-Systeme

M 3.85 Einführung in OpenLDAP

M 3.86 Schulung der Administratoren von OpenLDAP

M 3.87 Einführung in Lotus Notes/Domino

M 3.88 Zielgruppenspezifische Schulungen zu Lotus Notes/Domino

M 3.89 Schulung zur Administration der Protokollierung

M 3.90 Allgemeine Grundlagen für die zentrale Protokollierung

M 3.91 Schulung der Administratoren von Cloud-Infrastrukturen

M 3.92 Grundlegende Begriffe beim Einsatz von Speicherlösungen

M 3.93 Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme

M 3.94 Messung und Auswertung des Lernerfolgs

M 3.95 Lernstoffsicherung

M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung

M 3.97 Schulung des Projektteams für die Software-Entwicklung

M 3.98 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen

# M 3.1 Geregelte Einarbeitung/ Einweisung neuer Mitarbeiter

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Neuen Mitarbeitern müssen nicht nur in ihre neuen Aufgaben eingearbeitet werden, sie müssen auch über interne Regelungen, Gepflogenheiten und Verfahrensweisen informiert werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner zu Fragen der Informationssicherheit nicht, sie wissen nicht, welche Sicherheitsmaßnahmen durchzuführen sind und welche Sicherheitsstrategie die Behörde bzw. das Unternehmen verfolgt. Daraus können Störungen und Schäden für die Institution erwachsen. Daher kommt der geregelten Einarbeitung neuer Mitarbeiter eine entsprechend hohe Bedeutung zu. Die erfahrenen Mitarbeiter sollte entsprechend sensibilisiert werden, damit sie neue Mitarbeitern unterstützen und somit Sicherheitsprobleme bereits im Vorfeld auf ein Minimum reduziert werden können. Neuen Mitarbeitern sollte ein erfahrener Kollege für Fragen zur Seite gestellt werden.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Alle neuen Mitarbeiter sollten in die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und Anwendungen eingewiesen bzw. geschult werden. Außerdem sollten alle neuen Mitarbeiter zu allen relevanten Sicherheitsmaßnahmen sensibilisiert und geschult werden (siehe auch Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit*). Neue Mitarbeiter sollten ausreichend Zeit zur Einarbeitung haben.
- Es sollten alle Ansprechpartner vorgestellt werden, insbesondere die zu Fragen rund um Informationssicherheit und Datenschutz.
- Die Sicherheitsziele der Behörde bzw. des Unternehmens sollten den neuen Mitarbeitern vorgestellt werden. Alle hausinternen Regelungen und Vorschriften zur Informationssicherheit müssen erläutert werden. Für alle Arten von potentiellen Sicherheitsvorfällen sollten die Verhaltensregeln und Meldewege dargelegt werden.

Hilfreich zur Durchführung der Einarbeitung ist ein Laufzettel oder eine Checkliste, aus der die einzelnen Aktivitäten und der erreichte Stand der Einarbeitung ersichtlich sind.

Prüffragen:

- Ist die Einarbeitung von neuem Personal im Bereich der Informationssicherheit geregelt?
- Wird jeder neue Mitarbeiter über die relevanten Regelungen zur Informationssicherheit informiert?

# M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Bei der Einstellung von Mitarbeitern sollen diese verpflichtet werden, einschlägige Gesetze (z. B. zum Datenschutz), Vorschriften und interne Regelungen einzuhalten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen rund um das Thema der Informationssicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und den Empfang quittieren zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur ständigen Einsichtnahme vorzuhalten. Auf neue Gesetze und Regelungen sollte geeignet hingewiesen werden, z. B. über das Intranet.

Alle Mitarbeiter sollten darauf hingewiesen werden, dass alle Arbeitsergebnisse und alle während der Arbeit erhaltenen Informationen ausschließlich zum internen und dienstlichen Gebrauch bestimmt sind. Außerdem sollten die Mitarbeiter dafür sensibilisiert werden, dass sie vor der Weitergabe personenbezogener oder vertraulicher Informationen prüfen, ob diese zulässig ist. Dies gilt ebenso für Daten, die lizenz- oder urheberrechtlich geschützt sind.

Prüffragen:

- Werden die Mitarbeiter verpflichtet, alle bestehenden Gesetze, Vorschriften und Regelungen einzuhalten?
- Ist den Mitarbeitern bekannt, welcher rechtliche Rahmen ihre Tätigkeit bestimmt?

# M 3.3 Vertretungsregelungen

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter Organisation
**Verantwortlich für Umsetzung:** Vorgesetzte

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Für alle wesentlichen Geschäftsprozesse und Aufgaben müssen tragfähige Vertretungsregelungen vorhanden sein. Diese müssen regelmäßig aktualisiert werden.
- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
- Das Benennen eines Vertreters reicht in der Regel nicht aus, es muss überprüft werden, wie der Vertreter zu schulen ist, damit er die Aufgaben inhaltlich übernehmen kann. Stellt sich heraus, dass es Personen gibt, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, einen Vertreter zu schulen.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

Prüffragen:

- Existieren in allen Bereichen Vertretungsregelungen?
- Ist sichergestellt, dass in Vertretungsfällen ausreichend kompetente Vertreter zur Verfügung stehen?

# M 3.4 Schulung vor Programmnutzung

**Verantwortlich für Initiierung:** Vorgesetzte, Leiter Personal
**Verantwortlich für Umsetzung:** Fachverantwortliche, Vorgesetzte

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die Benutzer eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die Benutzer vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden. Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen.

Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.

Stehen leicht verständliche Handbücher oder Hilfetexte zu IT-Anwendungen bereit, so kann anstelle der Schulung auch die Aufforderung stehen, sich selbstständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings, dass die Benutzer ausreichend Zeit zur Einarbeitung bekommen.

Prüffragen:

- Werden Mitarbeiter, die eine Aufgabe neu übernehmen sollen, ausreichend geschult?
- Werden bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt?
- Haben die Mitarbeiter ausreichende Möglichkeiten und Zeit, um sich in neue Aufgaben und Anwendungen einzuarbeiten?

# M 3.5 Schulung zu Sicherheitsmaßnahmen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Wie sich an vielen konkreten Beispielen wie den Schadensstatistiken von Elektronik-Versicherern belegen lässt, resultieren Schäden oft schlicht aus der Unkenntnis elementarer Sicherheitsmaßnahmen. Um dies zu verhindern, ist jeder einzelne Mitarbeiter zum sorgfältigen Umgang mit geschäftsrelevanten Informationen und der IT zu schulen und zu motivieren. Nur durch die Vermittlung der notwendigen Kenntnisse kann ein Verständnis für die erforderlichen Maßnahmen zur Informationssicherheit geweckt werden.

Im Folgenden werden die Kernthemen, die bei einer Schulung zu Sicherheitsmaßnahmen vermittelt werden sollten, vorgestellt. Eine ausführliche und zielgruppengerichtete Beschreibung von Schulungsinhalten findet sich in M 3.45 *Planung von Schulungsinhalten zur Informationssicherheit*.

- **Sensibilisierung für Informationssicherheit**
  Jeder Mitarbeiter ist auf die Bedeutung der Sicherheitsbelange hinzuweisen. Ein geeigneter Einstieg in die Sensibilisierung ist es beispielsweise, die Abhängigkeit der Behörde bzw. des Unternehmens und damit der Arbeitsplätze vom reibungslosen Funktionieren der Geschäftsprozesse aufzuzeigen. Darüber hinaus ist der Wert von Informationen unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit herauszuarbeiten. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen.
- **Mitarbeiterbezogene Informationssicherheitsmaßnahmen**
  Zu diesem Thema sollen die Sicherheitsmaßnahmen vermittelt werden, die in einem Informationssicherheitskonzept erarbeitet wurden und von den einzelnen Mitarbeitern umzusetzen sind. Je nach Geschäftsprozess oder Fachaufgabe kann es andere Werte geben, die zu schützen sind, oder einen anderen Schutzbedarf haben. Den Mitarbeitern sollte vermittelt werden, welche Bedeutung Informationen oder andere Objekte für die Institution haben und was sie beim Umgang mit diesen beachten sollten. Dieser Teil der Schulungsmaßnahmen hat eine große Bedeutung, da viele Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.
- **Produktbezogene Sicherheitsmaßnahmen**
  Zu diesem Thema sollen die Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Produkt wie beispielsweise einem IT-System verbunden sind und häufig bereits im Lieferumfang enthalten sind. Dies können neben Passwörtern zur Anmeldung auch Möglichkeiten zur Verschlüsselung von Dokumenten oder Datenfeldern sein. So können beispielsweise Hinweise und Empfehlungen über die Strukturierung und Organisation von Dateien den Aufwand zur Datensicherung deutlich reduzieren.
- **Verhalten bei Auftreten von Schadsoftware**
  Hier soll den Mitarbeitern vermittelt werden, wie mit Computer-Viren oder anderer Schadsoftware umzugehen ist. Mögliche Inhalte dieser Schulung sind (siehe M 6.23 *Verhaltensregeln bei Auftreten von Schadprogrammen*):

  - Erkennen einer Schadsoftware-Infektion
  - Wirkungsweise und Arten von Schadsoftware
  - Sofortmaßnahmen im Verdachtsfall

  - Maßnahmen zur Eliminierung von Schadsoftware
  - Vorbeugende Maßnahmen
- **Authentikation**
  Mitarbeiter sollten mit den vorhandenen Authentikationsmechanismen und den hierfür genutzten Authentikationsmitteln (z. B. Passwörtern oder Token) korrekt umgehen gehen können. Beispielsweise sollen die Bedeutung von Passwörtern für die Informationssicherheit sowie die Randbedingungen erläutert werden, die einen wirksamen Einsatz eines Passwortes erst ermöglichen (siehe auch M 2.11 *Regelung des Passwortgebrauchs*).
- **Bedeutung der Datensicherung und deren Durchführung**
  Die regelmäßige Datensicherung ist eine der wichtigsten Sicherheitsmaßnahmen in jedem Informationsverbund. Vermittelt werden soll das Datensicherungskonzept (siehe Baustein B 1.4 *Datensicherungskonzept*) der Behörde bzw. des Unternehmens und die von jedem einzelnen durchzuführenden Datensicherungsaufgaben. Besonders wichtig ist dies für solche Bereiche, in denen Benutzer selbst die Datensicherungen durchführen müssen.
- **Umgang mit personenbezogenen Daten**
  An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen. Dies betrifft beispielsweise den Umgang mit Auskunftsersuchen, Änderungs- und Verbesserungswünschen der Betroffenen, gesetzlich vorgeschriebene Fristen zur Datenlöschung, Schutz der Vertraulichkeit und die Übermittlung der Daten.
- **Einweisung in Notfallmaßnahmen**
  Sämtliche Mitarbeiter sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehört die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer oder anderen Notfällen, der Umgang mit Feuerlöschern und das Notfall-Meldesystem (wer als erstes wie zu benachrichtigen ist).
- **Vorbeugung gegen Social Engineering**
  Die Mitarbeiter sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten erläutert werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten Mitarbeiter regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

Bei der Durchführung von Schulungen sollte immer beachtet werden, dass es nicht reicht, einen Mitarbeiter einmal während seines gesamten Arbeitsverhältnisses zu schulen. Für nahezu alle Formen von Schulungen - insbesondere Front-Desk-Schulungen - gilt, dass sehr viele neue Informationen auf die Teilnehmer einstürzen. Diese gelangen nur zu einem kleinen Teil ins Langzeitgedächtnis, 80% des vermittelten Wissens sind meist schon bei Schulungsende wieder vergessen.

Daher sollten Mitarbeiter immer wieder zu Themen rund um die Informationssicherheit geschult bzw. sensibilisiert werden. Dies kann beispielsweise

- in kürzeren Veranstaltungen zu aktuellen Sicherheitsthemen,
- im Rahmen regelmäßiger Veranstaltungen wie Abteilungsbesprechungen, oder
- durch interaktive Schulungsprogramme, die allen Mitarbeitern zur Verfügung stehen, erfolgen.

Prüffragen:

- Werden die Mitarbeiter zu Themen rund um die Informationssicherheitsmaßnahmen geschult?
- Wird den Mitarbeitern vermittelt, welche Bedeutung Informationen oder andere Objekte haben und was sie beim Umgang mit diesen beachten sollten?
- Werden Mitarbeiter, die mit personenbezogenen Daten arbeiten, für die gesetzlich erforderlichen Sicherheitsmaßnahmen geschult?
- Werden die Mitarbeiter regelmäßig zu Themen der Informationssicherheit geschult bzw. sensibilisiert?

# M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Vorgesetzte, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Verlässt ein Mitarbeiter die Institution oder wechselt die Funktion, so ist zu beachten:

- Vor dem Weggang ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen. Dafür ist es wünschenswert, dass sich die Arbeitszeiträume wenigstens kurz überschneiden.
- Von dem Ausscheidenden sind sämtliche Unterlagen (wie auch entliehene institutionseigene Bücher), ausgehändigte Schlüssel, ausgeliehene Geräte (z. B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise sowie sonstige Karten zur Zutrittsberechtigung einzuziehen. Ferner sind bei biometrischen Verfahren (z. B. Irisscanner, Fingerabdrücke und Handrückenerkennung) entsprechende Zutrittsberechtigungen zu löschen bzw. auf die getroffene Vertreterregelung anzupassen.
- Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Weggang einer der Personen die Zugangsberechtigung zu ändern.
- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.
- Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.
- Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen, zu verwehren. Auch bei Funktionsänderungen muss unter Umständen die Zutrittsberechtigung zu bestimmten Räumlichkeiten wie Serverräumen entzogen werden.
- Optional kann sogar für den Zeitraum zwischen Aussprechen einer Kündigung und dem Weggang der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.

Alle notwendigen Aktivitäten, wenn ein Mitarbeiter die Institution verlässt oder die Funktion wechselt, sind klar zu regeln. Als ein praktikables Hilfsmittel haben sich sogenannte Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.

Prüffragen:

- Sind die Aktivitäten, die beim Weggang oder Funktionswechsel von Mitarbeitern durchzuführen sind, klar geregelt?

- Werden die zuständigen Stellen über das Ausscheiden eines Mitarbeiters rechtzeitig unterrichtet?
- Wird sichergestellt, dass sämtliche Zutrittsrechte, Zugangsberechtigungen und Zugriffsrechte einer ausscheidenden Person entzogen und gelöscht werden?
- Wird sichergestellt, dass sämtliche institutionseigenen Werte (z. B. Unterlagen, Schlüssel, Rechner, Speichermedien) von einer ausscheidenden Person zurückgefordert und eingezogen werden?

# M 3.7 Anlaufstelle bei persönlichen Problemen

**Verantwortlich für Initiierung:** Personalrat/Betriebsrat, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Personalrat/ Betriebsrat

Für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme eines Arbeitnehmers ursächlich sein. Als Probleme lassen sich beispielsweise hohe Schulden, Suchtkrankheiten aber auch Schwierigkeiten am Arbeitsplatz (Über-/Unterforderung, Mobbing) aufzählen. Um dem Betroffenen bei der Bewältigung dieser Probleme zu helfen, kann es in vielen Fällen hilfreich sein, wenn eine Vertrauensperson zur Verfügung steht. Dieser Ansprechpartner sollte dabei sowohl die Interessen des Betroffenen im Auge haben und konkrete Hilfestellung anbieten als auch die Interessen des Unternehmens bzw. Behörde wahren und gemeinsam mit dem Betroffenen nach Lösungsmöglichkeiten suchen.

An diese Vertrauensperson müssen sich aber auch Vorgesetzte und Kollegen wenden können, wenn wiederholt Auffälligkeiten Dritter wahrgenommen wurden, die auf eine verminderte Zuverlässigkeit schließen lassen. Die Vertrauensperson muss dann die Möglichkeit haben, sich an den Betroffenen zu wenden und Hilfe anzubieten.

Eine solche Stelle können Personalrat, Betriebsrat, Betriebsärzte einnehmen. Die Einrichtung einer solchen Anlaufstelle ist allen Mitarbeitern bekannt zu geben. Externe Stellen sind zum Beispiel die Beratungsstellen der gesetzlichen Krankenkassen.

Prüffragen:

- Stehen den Mitarbeitern bei persönlichen Problemen vertrauenswürdige Ansprechpartner zur Verfügung?

# M 3.8 Vermeidung von Störungen des Betriebsklimas

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Personalrat/Betriebsrat, Leiter Personal

**Verantwortlich für Umsetzung:** Personalabteilung, Personalrat/ Betriebsrat, Vorgesetzte

Durch ein positives Betriebsklima werden die Mitarbeiter einerseits zur Einhaltung von Sicherheitsmaßnahmen motiviert, andererseits wird die Gefahr von fahrlässigen oder vorsätzlichen Handlungen reduziert, die den Betrieb stören können. Störungen des Betriebsklimas können dabei eine Vielzahl von inner- und außerbetrieblichen Ursachen haben, treten jedoch häufig bei gravierenden innerbetrieblichen Veränderungen auf. Beispiele für solche Veränderungen sind Umstrukturierungen, Sanierungen, Verkauf oder Fusionen von Organisationseinheiten und Outsourcing-Vorhaben. Diese können das Betriebsklima negativ beeinflussen, da sie meistens Ängste unterschiedlicher Art (z. B. Kompetenzverlust, Versagensängste, Arbeitsplatzverlust) hervorrufen. Diese können besser bewältigt werden, wenn das Betriebsklima schon vor den Veränderungen möglichst gut ist.

Auch unter Sicherheitsaspekten sollte daher versucht werden, ein positives Betriebsklima zu erreichen und dauerhaft aufrechtzuerhalten. Die Vielzahl der Möglichkeiten kann hier nicht angeführt werden, deshalb ist hier lediglich eine Auswahl möglicher Maßnahmen genannt, deren Angemessenheit und Realisierbarkeit im Einzelnen zu prüfen wäre:

- Einrichtung eines Sozialraums,
- Vermeidung von Überstunden,
- Vermeidung von großen Resturlaubsansprüchen,
- Einhaltung von Pausenzeiten,
- geregelte Aufgabenverteilung,
- gleichmäßige Arbeitsauslastung,
- leistungsgerechte Bezahlung,
- bestehende Vertreterregelung.

Kommunikationsprobleme in einer Organisation führen fast zwangsläufig auch zu Sicherheitsproblemen. Dies kann im Extremfall zu bewussten Sicherheitsverletzungen führen. Wenn die Benutzer Sicherheitsmaßnahmen nur als "lästig" empfinden, weil sie nicht über deren Zweck informiert worden sind, kann das bereits dazu führen, dass diese umgangen werden.

Auch das Überbringen schlechter Nachrichten muss möglich sein, ohne dass der Bote deswegen Sanktionen befürchten muss. Es sollte ein Betriebsklima vorhanden sein, in dem es für jeden Betroffenen möglich ist, Sicherheitsvorfälle innerhalb des eigenen Unternehmens bzw. der eigenen Behörde zu melden. Nur so können bestehende Sicherheitsdefizite wirkungsvoll und offen angegangen werden.

Mitarbeiter können nicht nur über finanzielle Anreize motiviert werden. Wichtig ist vor allem die Anerkennung ihrer Arbeitsleistung. Mitarbeiter sollten, wo immer möglich, in Entscheidungen mit einbezogen werden.

Zumindest sollten sie über die Gründe für die getroffenen Entscheidungen informiert werden, damit sie aktiv und motiviert an deren Umsetzung mitwirken.

Häufig äußert sich z. B. Protest gegen die Auswahl bestimmter Hard- oder Software darin, dass die Benutzer zu zeigen versuchen, dass die aufgezwungene Hard- oder Software nicht so sicher ist, wie die von ihnen präferierte.

Das Betriebsklima und das Verhalten von Mitarbeitern kann besonders bei großen Veränderungen, wie etwa bei Outsourcing-Vorhaben, von besonderer Bedeutung sein: unzufriedene oder verärgerte Mitarbeiter können ein solches Vorhaben zum Scheitern verurteilen (z. B. Kündigung von Know-how-Trägern in kritischen Phasen der Veränderung oder bewusstes Ignorieren von Sicherheitsanweisungen), was für das Unternehmen in Folge existenzbedrohend sein kann. Bei größeren Umstrukturierungen oder Outsourcing-Vorhaben ist die Beachtung folgender Aspekte empfehlenswert:

- Die Mitarbeiter sollten frühzeitig in Entscheidungsprozesse wie die Auswahl eines Outsourcing-Dienstleisters eingebunden werden. Im weiteren Projektverlauf sollten sie an der Gestaltung von eventuellen Übernahmeverträgen beteiligt werden.
- Die Mitarbeiter sollten umfassend und frühzeitig über Veränderungen informiert werden und einen Ansprechpartner für Probleme und Fragen haben. Indirekte Informationen durch die Medien, z. B. über Zeitungen, statt direkte durch die Firmen- oder Behördenleitung schafft Misstrauen, zerstört die Vertrauensbasis und bereitet Spekulationen und Gerüchten den Boden.
- Bei organisatorischen Veränderungen sollten den betroffenen Mitarbeitern Zukunftsperspektiven aufgezeigt werden. Oftmals sind Outsourcing-Dienstleister darauf angewiesen, dass ein möglichst hoher Anteil der Mitarbeiter des auszulagernden Bereichs zu ihnen wechselt. Nur so kann eine befriedigende Dienstleistungsqualität garantiert werden. Mitarbeiter, die Zukunftsangst haben oder sich unfair behandelt fühlen, lassen in ihrer Arbeitsqualität nach oder verlassen sogar vorzeitig das Unternehmen.
- Anspruchsvolle oder belastende Tätigkeiten, die im Rahmen von Umstrukturierungen nicht zu vermeiden sind, sollten ausreichend gewürdigt und anerkannt werden. Die erforderliche Mehrarbeit sollte honoriert werden.

Prüffragen:

- Wird das Betriebsklima von den Mitarbeitern und Vorgesetzten gleichermaßen als positiv beschrieben?
- Werden Punkte, die das Betriebsklima negativ beeinflussen, zeitnah abgestellt?
- Gibt es bei größeren Umstrukturierungen einen Verantwortlichen, der für die betroffenen Mitarbeiter als Ansprechpartner zur Verfügung steht?
- Werden die Mitarbeiter in Veränderungsprozesse mit einbezogen?

# M 3.9 Ergonomischer Arbeitsplatz

**Verantwortlich für Initiierung:** Personalrat/Betriebsrat, Leiter Haustechnik
**Verantwortlich für Umsetzung:** Benutzer, Personalrat/Betriebsrat, Vorgesetzte

Die Belastungen durch dauerhafte Tätigkeiten an schlecht ausgestatteten Arbeitsplätzen sind nicht zu unterschätzen, da sie bei längerer Dauer zu gesundheitlichen Beschwerden führen können. Durch einen ergonomischen Arbeitsplatz können diese Belastungen jedoch verringert werden. Eine verbesserte Ergonomie bedeutet zudem eine effektivere Arbeitsweise. Das bringt nicht nur gesundheitliche Vorteile für den Arbeitnehmer, sondern hat auch ein wirtschaftlicheres Arbeiten und eine verbesserte Umsetzung von Sicherheitsmaßnahmen zur Folge.

Daher sollte jeder Arbeitsplatz ergonomisch gestaltet werden. Bei Computerarbeitsplätzen müssen beispielsweise Stuhl, Tisch, Bildschirm und Tastatur individuell einstellbar sein, um eine möglichst fehlerfreie Bedienung der IT zu ermöglichen und zu fördern. Das beinhaltet unter anderem, dass Rückenlehne, Sitzhöhe und Sitzfläche des Stuhls verstellbar sein müssen, aber auch, dass die Arbeitsmittel so angeordnet werden können, dass für die jeweilige Arbeitsaufgabe eine möglichst geringe Belastung entsteht.

Ein entsprechend ausgestatteter Arbeitsplatz erleichtert es auch, Sicherheitsmaßnahmen einzuhalten. Gibt es verschließbare Schreibtische oder Schränke, so können Datenträger, Dokumentationen, Unterlagen und Zubehör darin verschlossen werden.

Auch die am Arbeitsplatz eingesetzten IT-Systeme, vor allem der Bildschirm, müssen ergonomisch aufgestellt werden. So sollte beispielsweise der Bildschirm immer im rechten Winkel zum Fenster aufgestellt werden, um die direkte Lichteinstrahlung darauf zu vermeiden. Außerdem sollte an IT-Systemen ein ungestörtes Arbeiten möglich sein. So sollten den Benutzern nicht ständig andere Personen über die Schulter blicken können. Dies ist auch sinnvoll, um unbefugtes Einsehen von Informationen zu vermeiden.

Weitere Hinweise sind den Empfehlungen der Berufsgenossenschaften oder Arbeitsschutzexperten zu entnehmen.

Prüffragen:

- Sind die Arbeitsplätze aller Mitarbeiter ergonomisch gestaltet?
- Ist die Ausrüstung der Computerarbeitsplätze für die möglichst fehlerfreie Bedienung der IT individuell einstellbar?
- Sind die am Arbeitsplatz eingesetzten IT-Systeme, vor allem der Bildschirm, ergonomisch und für ungestörtes Arbeiten aufgestellt?

# M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** Leiter IT, Leiter Personal

Den IT-System- oder TK-Anlagen-Administratoren und deren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals alle Befugnisse. Administratoren und ihre Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, gegebenenfalls zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre.

Administratoren für IT-Systeme und deren Vertreter müssen sorgfältig ausgewählt werden. Sie müssen regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

Da der Administrator hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle inne hat, muss auch bei seinem Ausfall die Weiterführung seiner Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben.

Hat ein Unternehmen oder eine Behörde mehrere Administratoren mit vergleichbaren IT-Systemkenntnissen, so können sich diese auch wechselseitig vertreten, wenn diese dafür noch freie Kapazitäten haben. In allen Bereichen, in denen nur ein Administrator hauptverantwortlich IT-Systeme betreut, sollten zwei Stellvertreter eingearbeitet werden, da bei längerer Abwesenheit des Administrators erfahrungsgemäß auch der Stellvertreter zeitweise nicht für Administrationsaufgaben zur Verfügung steht.

Um die Funktionsfähigkeit des IT-Betriebs zu gewährleisten, muss insbesondere bei bevorstehenden Personalveränderungen oder Veränderungen der Organisationsstruktur geprüft werden, ob die erforderlichen Administrationstätigkeiten auch durch die benannten Administratoren und deren Vertreter bewältigt werden können.

Insbesondere bei bevorstehenden Umzügen kann es durch Administrationsaufgaben an einem weiteren Standort zu einem erheblichen höheren Arbeitsaufkommen des Administrators kommen. Auch in solchen Fällen muss sichergestellt sein, dass der Produktionsbetrieb am bisherigen Standort bis zum Zeitpunkt des Umzugs nicht beeinträchtigt wird.

Prüffragen:

- Werden Administratoren für IT-Systeme und deren Vertreter sorgfältig ausgewählt?
- Haben die Vertreter die notwendigen Kenntnisse für die Administration der IT-Systeme?
- Bei bevorstehenden Veränderungen: Wird geprüft, ob ausreichende Ressourcen für die erforderlichen Administrationstätigkeiten bereitstehen?

# M 3.11 Schulung des Wartungs- und Administrationspersonals

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** Vorgesetzte

Wartungs- und Administrationspersonal benötigt detaillierte Kenntnisse über die eingesetzten IT-Komponenten. Daher sollte es mindestens soweit geschult werden, dass

- alltägliche Administrationsarbeiten selbst durchgeführt,
- einfache Fehler selbst erkannt und behoben,
- Datensicherungen regelmäßig selbsttätig durchgeführt,
- die Eingriffe von externem Wartungspersonal nachvollzogen und
- Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt und rasch behoben

werden können.

Entsprechende Schulungen werden in der Regel von den Herstellern der IT-Systeme bzw. TK-Anlagen angeboten. Administratoren von TK-Anlagen sollten außerdem in der Lage sein,

- das Betriebsverhalten der TK-Anlage mit Hilfe der Kontrollanzeigen an den Geräten zu beurteilen,
- die TK-Anlage selbständig außer- und in Betrieb nehmen zu können.

Prüffragen:

- Wird das Wartungs- und Administrationspersonal für die Durchführung seiner Aufgaben hinreichend geschult?

# M 3.12 Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Personalrat/ Betriebsrat, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Bedeutung der Warnanzeigen, -töne und -symbole der TK-Anlage sollte allen Mitarbeitern bekannt sein. Hierzu zählen insbesondere:

- Aufmerksamkeitston für direktes Ansprechen,
- Aufschalte-Warnton,
- Freisprechanzeige,
- Anzeige für aktiviertes direktes Ansprechen,
- Anzeige für automatischen Rückruf und
- Anzeige/Einblendung bei Dreierkonferenz.

Da die Nutzung bestimmter, eigentlich nicht freigegebener Leistungsmerkmale (Beispiel: Zeugenschaltung) zu Beeinträchtigungen der Sicherheit führen kann, sollten besonders deren Warnanzeigen und -töne bekannt sein.

Prüffragen:

- Sind die Warnanzeigen, Warnsymbole und Warntöne mit ihren Bedeutungen allen Benutzern bekannt?

# M 3.13 Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Personalrat/ Betriebsrat, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Mitarbeiter müssen über die mit dem Benutzen einer digitalen TK-Anlage verbundenen Gefährdungen informiert werden. Dies könnte z. B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein abnormes Verhalten der TK-Anlage gemeldet werden soll. Bei Manipulationen an der TK-Anlage sollte eine unabhängige Kontrollinstanz wie Sicherheitsmanagement oder Datenschutzbeauftragte informiert werden.

Prüffragen:

- Existiert eine Regelung zur nachhaltigen Sensibilisierung der Benutzer für Aspekte der IT-Sicherheit?
- Anzeichen von Sicherheitsvorfällen: Existiert eine Regelung zur Meldung und Überprüfung von potentiellen Sicherheitsvorfällen?

# M 3.14 Einweisung des Personals in den geregelten Ablauf der Informationsweitergabe und des Datenträgeraustausches

**Verantwortlich für Initiierung:** Leiter Organisation
**Verantwortlich für Umsetzung:** Fachverantwortliche

Mitarbeiter müssen ausreichend darüber informiert werden, welche Rahmenbedingungen und Restriktionen bei der Informationsweitergabe einzuhalten sind (siehe M 2.45 *Regelung des Datenträgeraustausches*). Wenn sie hierin nur unzulänglich eingewiesen werden, kann dies zu einer Vielzahl von Sicherheitsproblemen führen. Hierzu gehört beispielsweise, dass Mitarbeiter darüber informiert werden,

- mit welchen Kommunikationspartnern welche Informationen ausgetauscht werden dürfen (siehe M 2.42 *Festlegung der möglichen Kommunikationspartner*),
- welche Arten von Datenträger für Datenträgeraustausch zulässig sind und wie diese abzusichern sind,
- dass die Identität der Kommunikationspartners überprüft werden sollte, bevor vertrauliche Informationen weitergegeben werden.

Außerdem sind die prinzipiellen Schritte für den Ablauf eines Datenträgeraustausches zu fixieren und zu veröffentlichen, z. B. im Intranet. Die Mitarbeiter sind zur Einhaltung der Regelungen zu verpflichten.

Zusätzlich sollten die am Datenträgeraustausch beteiligten Mitarbeiter sensibilisiert werden, welche konkreten Gefährdungen vor, während und nach dem Transport bestehen. Dementsprechend sollten diese Mitarbeiter ausführlich mit den einzuhaltenden Sicherheitsmaßnahmen vertraut gemacht werden.

Bevor digitale Datenträger eingelesen werden, die im Postfach lagen, obwohl sie nicht erwartet wurden, sollte bei den angegebenen Absendern nachgefragt werden, ob sie die Datenträger wirklich geschickt haben (siehe auch M 2.224 *Vorbeugung gegen Schadprogramme*). Bei unbekanntem Absender sollte das Sicherheitsmanagement informiert werden, wenn von der Leitungsebene keine anderen Regelungen für diesen Fall verabschiedet wurden.

Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung oder Checksummen-Verfahren), so sind die dafür zuständigen Mitarbeiter in die Handhabung dieser Verfahren ausreichend einzuarbeiten.

Prüffragen:

- Sind alle Mitarbeiter über die Regelungen für Informationsweitergabe und Datenträgeraustausch informiert?

# M 3.15 Informationen für alle Mitarbeiter über die Faxnutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Alle Mitarbeiter sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen sowie darüber zu informieren, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Bei Verwendung herkömmlicher Faxgeräte sollte eine verständliche Bedienungsanleitung am Faxgerät zur Verfügung stehen. Beim Einsatz eines Faxservers sollten die Benutzer mindestens eine Kurzreferenz zur eingesetzten Faxclient-Software erhalten.

Insbesondere ist, gegebenenfalls in Form einer Dienstanweisung, festzulegen,

- wer der Fax-Verantwortliche ist und damit für die manuelle Verteilung eingehender Faxsendungen und als Ansprechpartner in Fax-Problemfällen zuständig ist,
- wer das Faxgerät bzw. den Faxserver benutzen darf,
- dass ein einheitliches Faxvorblatt benutzt werden soll,
- dass das Versenden von vertraulichen Informationen per Fax vermieden werden sollte. Falls dies nicht möglich ist, sollten sich vor dem Austausch schutzbedürftiger Informationen über Fax Empfänger und Absender hierüber telefonisch verständigen,
- dass Faxgeräte mit Verschlüsselungsoption zum Übertragen von vertraulichen Informationen benutzt werden sollten wenn diese zur Verfügung stehen,
- dass Einzelsendenachweise bzw. Übertragungsprotokolle für die korrekte Übertragung zu kontrollieren und diese den Unterlagen beizufügen und bei Bedarf zu archivieren sind,
- dass beim Einsatz eines Faxservers mit automatischer Eingangs-Fax-Verteilung für die Akten ein Ausdruck von Eingangs-Faxsendungen zu fertigen ist bzw. diese elektronisch zu archivieren sind,
- dass bei Ausgangsfaxen, die über einen Faxserver versendet werden, für die Akten ein Ausdruck zu erstellen ist bzw. diese elektronisch zu archivieren sind,
- dass die Adressbücher und Verteillisten regelmäßig kontrolliert werden, damit die Faxe nicht versehentlich an falsche Empfänger gesendet werden.

Prüffragen:

- Liegt am Faxgerät eine verständliche Bedienungsanleitung aus?
- Einsatz eines Faxservers: Existiert mindestens eine Kurzreferenz zur eingesetzten Faxclient-Software, die für alle Benutzer zugreifbar ist?
- Existiert eine Anweisung zur korrekten Faxnutzung?

# M 3.16 Einweisung in die Bedienung des Anrufbeantworters

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 3.17 Einweisung des Personals in die Modem-Benutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Mitarbeiter sind über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb eines Modems zu unterrichten. Hierbei sind insbesondere die Auswirkungen verschiedener Konfigurationen auf die Betriebssicherheit des Modems zu vermitteln.

Jeder Modem-Benutzer sollte sich mit der Bedienung vertraut machen und so Möglichkeiten und Grenzen des Gerätes kennen lernen.

Prüffragen:

- Sind die Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb eines Modems unterrichtet?

# M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, IT-Sicherheitsbeauftragter, Leiter IT

Wird ein IT-System oder eine IT-Anwendung von mehreren Benutzern verwendet und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet. Ist es einem Dritten möglich, an einem IT-System oder in einer IT-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden. Aus technischen Gründen (z. B. damit alle offenen Dateien geschlossen werden) sollten auch dann Regelungen für die Abmeldung von IT-Systemen und IT-Anwendungen getroffen werden, wenn keine Zugriffskontrolle realisiert ist.

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen (siehe auch M 4.2 *Bildschirmsperre*). Bei längerer Abwesenheit sollte die Bildschirmsperre automatisch aktiviert werden.

Einige IT-Systeme und IT-Anwendungen bieten die Möglichkeit, einen Zeitraum vorzugeben, nach dessen Ablauf ein Benutzer bei Inaktivität automatisch vom System abgemeldet wird. Es sollte überlegt werden, ob dieses Verfahren benutzt wird, da es auch zu Datenverlusten führen kann. Eine automatische Abmeldung kann z. B. bei PC-Pools mit starkem Publikumsverkehr zum Einsatz kommen, da hier ein angemeldeter Benutzer den Arbeitsplatz mit Hilfe der Bildschirmsperre unberechtigterweise blockieren kann.

Je nach Arbeitsplatzumgebung ist abzuwägen, welche Vorkehrungen für kurzfristige Abwesenheiten von Benutzern zu treffen sind. So sollte eine automatische Aktivierung der Bildschirmsperre bei Mehr-Benutzer-Systemen schneller erfolgen als bei solchen für einen Benutzer, also z. B. bereits nach 5 Minuten.

Prüffragen:

- Erfolgt eine Verpflichtung aller Benutzer, sich nach Aufgabenerfüllung entsprechend vom IT-System oder von der Anwendung abzumelden?
- Sind technische Verfahren (z. B.automatisches Aktivieren der Bildschirmsperre) etabliert, um unerwünschte Benutzerwechsel unter ein und derselben Benutzerkennung bei kurzen Unterbrechungen der Arbeit am IT-System zu verhindern?

# M 3.19 Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 3.20 Einweisung in die Bedienung von Schutzschränken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Nach der Beschaffung eines Schutzschrankes sind die Benutzer in die korrekte Bedienung einzuweisen. Dies sollte auch bei der Neuübertragung einer Aufgabe erfolgen, die die Nutzung des Schutzschrankes umfasst. Dabei sind zumindest folgende Punkte zu vermitteln:

- Der korrekte Umgang mit dem Schloss des Schutzschrankes ist vorzuführen. Auf typische Fehler ist hinzuweisen, zum Beispiel das Nichtverwerfen von Codeschlössern. Die Regelungen zur Schlüsselverwaltung, Schlüsselhinterlegung und Vertretungsregelung sind aufzuzeigen. Insbesondere ist einzufordern, dass der Schutzschrank bei Nichtbenutzung, auch kurzfristiger Art, verschlossen wird.
- Die Tastatur eines Servers ist unbedingt im Serverschrank aufzubewahren, damit nicht unberechtigte Konsol-Eingaben erfolgen können.
- Im Falle eines Serverschrankes ist darauf hinzuweisen, dass unnötige brennbare Materialien (Ausdrucke, überzählige Handbücher, Druckerpapier) nicht im Serverschrank aufbewahrt werden sollen.
- Datensicherungsträger des Servers sollten in einem anderen Brandabschnitt gelagert werden. Eine Aufbewahrung im Serverschrank ist daher ungeeignet und nur dann zulässig, wenn ein Doppel der Datensicherungsbestände in einem anderen Brandabschnitt ausgelagert ist.
- Wird ein klimatisierter Serverschrank eingesetzt, sollten die Öffnungszeiten des Serverschrankes minimiert werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

Prüffragen:

- Werden die Benutzer von Schutzschränken in die Bedienung eingewiesen?
- Bei Einsatz des Schutzschrankes als Serverschrank: Werden Datensicherungsträger des Servers in einem anderen Brandabschnitt gelagert?

# M 3.21 Sicherheitstechnische Einweisung der Telearbeiter

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Telearbeiter arbeiten ausschließlich oder zeitweise außerhalb der Gebäude des Arbeit- bzw. Auftraggebers. Das bedeutet, dass für die Telearbeit teilweise andere Sicherheitsmaßnahmen gelten, als für die Arbeit innerhalb der Institution. Deshalb ist es notwendig, dass auf dem übergreifenden Sicherheitskonzept der Institution aufbauend ein Sicherheitskonzept für die Telearbeitsplätze erstellt wird (siehe dazu M 2.117 *Erstellung eines Sicherheitskonzeptes für Telearbeit*). Zusätzlich sollten für die Telearbeiter entsprechende Sicherheitsrichtlinien erstellt und veröffentlicht werden. An Hand der Sicherheitsrichtlinien für Telearbeit müssen die Telearbeiter in die entsprechenden Sicherheitsmaßnahmen eingewiesen und eventuell in ihrem Umgang geschult werden. Insbesondere sind bei der Einweisung des Telearbeiters folgende Punkte zu berücksichtigen:

- Dienstliche Unterlagen müssen am Telearbeitsplatz sicher aufbewahrt werden, also z. B. nach der Bearbeitung in Schränke weggeschlossen werden.
- Fenster und nach außen gehende Türen (Balkone, Terrassen) abzuschließen, wenn der Telearbeitsplatz verlassen wird.
- Strukturelle und sicherheitsrelevante Änderungen an der Telearbeitsplatz-IT dürfen nur durch die Administratoren der Institution vorgenommen werden.
- Der Telearbeitsrechner darf nur über den dafür vorgesehenen Anschluss an öffentliche Kommunikationsnetze angebunden sein. Privat genutzte TK- und Internet-Zugängen müssen von den dienstlichen getrennt bleiben.
- Beim Datenaustausch mittels Datenträgern zwischen IT-Systemen der Institution und dem Arbeitsplatz-PC am Telearbeitsplatz dürfen nur die von der Institution beschafften Datenträger benutzt werden. Datenträger sollten nur verschlüsselt transportiert werden, damit bei einem Verlust keine vertraulichen Daten offengelegt werden. Dienstliche und private IT-Systeme oder Datenträger sollten sorgfältig getrennt bleiben, um z. B. die Verbreitung von Schadsoftware zu unterbinden.
- Der unbefugte Zugriff auf Telearbeits-IT ist durch Zugriffssperren zu verhindern, z. B. Boot- und Bildschirm-Sperren. Passwörter sind generell geheim zu halten, auch die für den Zugang zum Arbeitsplatzrechner und zum Kommunikationsrechner.

Darüber hinaus sind die Telearbeiter soweit im Umgang mit den Telearbeitsrechnern zu schulen, dass sie einfache Fehlerkorrekturen (z. B. Druckerpatrone wechseln) vornehmen bzw. einfache Probleme selbständig beheben können.

Prüffragen:

- Sind die Telearbeiter in die Telearbeit-spezifischen Sicherheitskonzepte und Sicherheitsrichtlinien eingewiesen worden?

# M 3.22 Vertretungsregelung für Telearbeit

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Die Inhalte wurden in M 2.113 *Regelungen für Telearbeit* integriert.

# M 3.23 Einführung in kryptographische Grundbegriffe

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Der Einsatz von Kryptoprodukten kann für die Benutzer zusätzlichen Aufwand bedeuten oder - je nach Komplexität der eingesetzten Produkte - sogar vertiefte Kenntnisse erfordern. Daher sollten alle Mitarbeiter, die kryptographische Verfahren und Produkte einsetzen sollen, für den Nutzen und die Notwendigkeit der kryptographischen Verfahren sensibilisiert werden und eine Einführung in kryptographische Grundbegriffe erhalten. Dies gilt natürlich insbesondere für diejenigen, die ein Kryptokonzept erstellen, Kryptoprodukte auswählen, installieren oder betreuen sollen.

Der folgende Text soll ein elementares Verständnis der grundlegenden kryptographischen Mechanismen vermitteln. Nachfolgend wird an Beispielen erläutert, in welcher Situation welche kryptographische Technik eingesetzt werden kann.

**Elemente der Kryptographie**

Mathematische Methoden und Techniken, die zum Schutz von Information gegen unbefugte Kenntnisnahme und/oder absichtliche Manipulation dienen können, nennt man kryptographisch. Der Schutz der Information durch kryptographische Methoden ist - im Unterschied zu infrastrukturellen und technischen Sicherungsmaßnahmen - *mathematisch-logischer* Natur.

Bei kryptographischen Verfahren wird ein mathematischer Rechenvorgang - ein *Algorithmus* - in konkrete Technik umgesetzt. Ihre Wirksamkeit beruht darauf, dass ein potentieller Angreifer ein gewisses mathematisches Problem nicht zu lösen vermag - und zwar nicht wegen mangelnder Fähigkeiten, sondern wegen fehlenden Wissens um ganz bestimmte "Schlüssel"-Informationen.

Kryptographische Methoden beziehen sich stets auf folgende Situation: Ein Sender A (dieser wird, wie in der Kryptographie üblich, "Alice" genannt) schickt über einen *unsicheren Kanal* eine Nachricht an einen Empfänger B (er wird "Bob" genannt).

Sender und Empfänger dürfen dabei auch identisch sein, unter einem Kanal ist ein beliebiges Transportmedium zu verstehen. Bei der Verschlüsselung lokaler Daten sind Sender und Empfänger natürlich identisch, unter "Kanal" ist hier das Speichermedium zu verstehen.

**Kryptographische Grundziele**

Auf Grund theoretischer und praktischer Erwägungen unterscheidet man vier kryptographische Grundziele:

- Vertraulichkeit/Geheimhaltung: Keine unbefugte dritte Partei E (sie sei "Eve" genannt) soll an den Inhalt der Nachricht bzw. Datei gelangen.
- Integrität: Unbefugte Manipulationen an der Nachricht bzw. Datei (z. B. Einfügen, Weglassen, Ersetzung von Teilen) sollen entdeckt werden können.

- Authentizität:
    - Identitätsnachweis (Authentisierung von Kommunikationspartnern): Eine Kommunikationspartei (z. B. Person, Organisation, IT-System) soll einer anderen ihre Identität zweifelsfrei beweisen können.
    - Herkunftsnachweis (Nachrichtenauthentisierung): A soll B beweisen können, dass eine Nachricht von ihr stammt und nicht verändert wurde.
- Nichtabstreitbarkeit (Verbindlichkeit, non repudiation): Hier liegt der Schwerpunkt verglichen mit der Nachrichtenauthentisierung auf der Nachweisbarkeit gegenüber Dritten.
    - Nichtabstreitbarkeit der Herkunft: Es soll A unmöglich sein, das Absenden einer bestimmten Nachricht an B nachträglich zu bestreiten.
    - Nichtabstreitbarkeit des Erhalts: Es soll B unmöglich sein, den Erhalt einer von A gesendeten Nachricht nachträglich zu bestreiten.

Es ist klar, dass zwischen diesen Zielen Beziehungen bestehen, aber eine wesentliche Einsicht der modernen Kryptographie ist folgende: Die Gewährleistung von Vertraulichkeit bzw. von Authentizität sind unabhängige Grundziele eines kryptographischen Systems: Authentisierung beschränkt den Kreis der möglichen Sender einer Nachricht, Geheimhaltung den der möglichen Empfänger.

Die grundlegende kryptographische Methode zur Wahrung von Vertraulichkeit ist **Verschlüsselung**, die grundlegenden Methoden zur Gewährleistung von Integrität, Authentizität und Nichtabstreitbarkeit sind **Hashfunktionen, Message Authentication Codes (MACs), digitale Signaturen** und **kryptographische Protokolle**. Die einzelnen kryptographischen Konzepte werden im folgenden kurz vorgestellt.

**I. Verschlüsselung**

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt. In allen modernen Verschlüsselungsalgorithmen sind Klartexte, Geheimtexte und Schlüssel jeweils als Folgen von Bits gegeben.

Um praktisch einsetzbar zu sein, müssen Verschlüsselungsalgorithmen folgende Mindestanforderungen erfüllen:

- Sie sollten entzifferungsresistent sein, d. h. ohne Kenntnis des Schlüssels darf das Chiffrat nicht entschlüsselt werden können, insbesondere muss hierfür die Menge der möglichen Schlüssel "ausreichend groß" sein, da sonst ein einfaches Ausprobieren aller Schlüssel möglich wäre,
- sie müssen einfach einzusetzen sein, und
- Ver-/Entschlüsselung müssen "schnell genug" sein.

Die Forderung nach Entzifferungsresistenz ist immer relativ zu den aktuellen technischen und mathematischen Möglichkeiten zu betrachten. Wichtig bei der Bewertung von Verschlüsselungsalgorithmen ist, dass es zum Nutzungszeitpunkt praktisch nicht möglich sein darf, das Chiffrat ohne Kenntnis des Schlüssels zu entschlüsseln, d. h. nicht mit der dann verfügbaren Technik innerhalb eines akzeptablen Zeitrahmens.

Wenn A und B eine vertrauliche Verbindung einrichten wollen, gehen sie wie folgt vor:

1. sie vereinbaren ein Chiffrierverfahren,
2. sie vereinbaren einen Schlüssel bzw. ein Schlüsselpaar,
3. A verschlüsselt eine Nachricht und sendet diese an B,
4. B entschlüsselt das von A gesendete Chiffrat.

Es gibt zwei große Klassen von Chiffrierverfahren:

**Symmetrische** Verschlüsselungsverfahren benutzen denselben Schlüssel sowohl für die Ver- als auch für die Entschlüsselung. Symmetrische Verfahren werden deshalb gelegentlich auch als "ein-Schlüssel"-Verfahren bezeichnet, da die Kenntnis eines Schlüssels ausreicht, um chiffrieren und dechiffrieren zu können.

Bekannte symmetrische Verschlüsselungsverfahren sind z. B. DES, Tripel-DES, IDEA oder RC5.

Bei symmetrischen Verfahren unterscheidet man weiter zwischen Stromchiffren und Blockchiffren.

Bei Stromchiffren wird unter Verwendung des Schlüssels eine möglichst zufällig aussehende Bitfolge (ein Bitstrom) generiert, die auf die Klarbitfolge (modulo 2) aufaddiert wird. Die Klarbitfolge wird also Bit für Bit (durch Addition von Schlüsselstrombits) verschlüsselt. Für die Sicherheit von Stromchiffren ist wesentlich, dass niemals zwei (verschiedene) Nachrichten mit demselben Schlüsselstrom verschlüsselt werden - dafür muss mit speziellen Maßnahmen (Synchronisierinformation in Form eines Spruchschlüssels) gesorgt werden. Beispiele für Stromchiffren sind RC4 und SEAL.

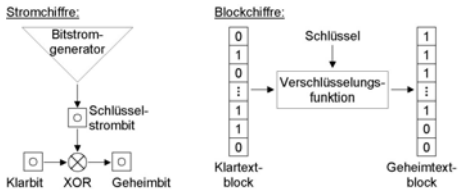



Abbildung: Chiffrierung

Bei Blockchiffren dagegen wird in einem Verschlüsselungstakt jeweils ein ganzer Block von Bits verschlüsselt, heutzutage sind dies in der Regel 64 Bits. Die meisten symmetrischen Verschlüsselungsverfahren sind Blockchiffren, dazu gehören auch DES, IDEA oder RC5. Für Blockchiffren sind eine Reihe von Betriebsarten (Modi) definiert (und standardisiert). Es sind dies

- der ECB (Electronic Code Book)-Modus, bei dem jeder Block für sich - unabhängig von den anderen Blöcken - verschlüsselt wird,
- der CBC (Cipher Block Chaining)-Modus und der CFB (Cipher Feed Back)-Modus, bei diesen Modi wird, nach Wahl eines zusätzlichen Initialisierungsvektors, eine Abhängigkeit der Chiffretextblöcke von allen vorhergehenden Chiffretextblöcken hergestellt, sowie
- der OFB (Output Feedback Modus), dieser Modus kann so aufgefasst werden, dass die verwendete Blockchiffre zur Generierung eines "Blockstroms" verwendet wird, der auf die Klarblöcke bitweise (modulo 2) aufaddiert wird.

Beim Einsatz symmetrischer Verfahren ist generell zu beachten, dass ein Schlüsselaustausch zwischen den Kommunikationspartnern vorausgegangen sein muss. Dieser muss über einen sicheren Kanal (z. B. Kurier, persönliche Übergabe) erfolgen und beide Parteien müssen anschließend den Schlüssel

geheim halten. Es gibt verschiedene Verfahren für einen sicheren Schlüsselaustausch. In geschlossenen Systemen ist der Schlüsselaustausch im allgemeinen unproblematisch zu realisieren, da hier meist "sichere Kanäle" vorhanden sind. In offenen Systemen mit einer Vielzahl von Kommunikationspartnern gestaltet sich dies schwieriger. Generell besteht jedoch das Problem, dass bei einer Vielzahl möglicher Kommunikationspartner entsprechend viele Schlüssel vor der eigentlichen Kommunikation ausgetauscht werden müssen und dass dabei die potentiellen Kommunikationspartner vorab bekannt sein müssen.

**Asymmetrische (Public Key)** -Chiffrierverfahren dagegen benutzen zwei verschiedene (aber mathematisch verwandte) Schlüssel: einen "öffentlichen" Schlüssel (Public Key) für die Verschlüsselung, und einen "privaten" Schlüssel (Private Key) für die Entschlüsselung. Das Schlüsselpaar muss dabei folgende Eigenschaft aufweisen: für alle, die lediglich den "Public Key" kennen, muss es praktisch unmöglich sein, den zugehörigen "Private Key" zu bestimmen oder eine mit dem "Public Key" verschlüsselte Nachricht zu entschlüsseln.

Asymmetrische Verschlüsselung hat also eine "Einbahn"-Eigenschaft: eine Nachricht kann nicht wiederhergestellt werden, wenn der "Private Key" vergessen oder gelöscht wurde.

Die Bezeichnung "Public Key"-Verschlüsselung rührt daher, dass der "Public Key" öffentlich bekannt gemacht werden kann, ohne die Sicherheit des Verfahrens zu kompromittieren. Der "Private Key" hingegen muss **geheim**gehalten werden.

Will nun Alice eine Nachricht verschlüsselt an Bob senden, so holt sich Alice den öffentlichen Schlüssel Bobs aus einer frei zugänglichen Datei und verschlüsselt damit die Nachricht. Nach Erhalt der Nachricht benutzt Bob seinen geheimen Schlüssel, um die von Alice erhaltene Nachricht zu entschlüsseln. Wenn Alice und Bob ein asymmetrisches Verfahren zum Zweck der Vertraulichkeit verwenden, benötigen sie also keinen sicheren Kanal für den Schlüsselaustausch, aber Alice muss sicher sein, dass sie tatsächlich Bobs öffentlichen Schlüssel benutzt und keinen Schlüssel, der ihr als Bobs Schlüssel untergeschoben wurde. Würde Alice eine Nachricht mit einem untergeschobenen Schlüssel verschlüsseln, so könnte der Täter, dem ja der passende geheime Schlüssel bekannt ist, die Nachricht entschlüsseln. Der Sender benötigt in der Regel die Bestätigung einer vertrauenswürdigen dritten Partei, dass der öffentliche Schlüssel des Empfängers wirklich zu diesem gehört. Diese Bestätigung, das "Zertifikat", wird im allgemeinen auch durch ein kryptographisches Verfahren erzeugt und dem öffentlichen Schlüssel beigefügt.

Zwei bekannte asymmetrische Verschlüsselungsverfahren sind das RSA-Verfahren (benannt nach den Erfindern Rivest, Shamir, Adleman) und die Klasse der Elgamal-Verfahren. Zu letzteren gehören auch die auf Elliptischen Kurven basierenden Verschlüsselungsverfahren.

Symmetrische und asymmetrische Chiffrierverfahren haben z. T. sich ergänzende Vor- und Nachteile:

Vorteile (guter) symmetrischer Verfahren:

- Sie sind schnell, d. h. sie haben einen hohen Datendurchsatz.
- Die Sicherheit ist im wesentlichen durch die Schlüssellänge festgelegt, d. h. bei guten symmetrischen Verfahren sollte es keine Attacken geben, die wesentlich besser sind als das Durchprobieren aller Schlüssel (Brute-Force-Attacken).

- Sie bieten hohe Sicherheit bei relativ kurzem Schlüssel.
- Die Schlüsselerzeugung ist einfach, da gewöhnlich als Schlüssel jede Bitfolge einer festen Länge erlaubt ist und als Schlüssel eine Zufallszahl gewählt werden kann.

Nachteile symmetrischer Verfahren:

- Jeder Teilnehmer muss sämtliche Schlüssel seiner Kommunikationspartner geheim halten.
- Zur Schlüsselverteilung sind sie weniger gut geeignet als asymmetrische Verfahren, insbesondere bei einer großen Anzahl von Kommunikationspartnern.
- Für Verbindlichkeitszwecke sind sie weniger praktikabel als asymmetrische Verfahren, da bei der Verwendung symmetrischer Schlüssel nicht ohne weiteres erkannt werden kann, welcher der beiden Kommunikationspartner die Nachricht verschlüsselt hat. Dies lässt sich nur durch eine zwischengeschaltete dritte Partei sicherstellen, die über entsprechende kryptographische Protokolle in den Nachrichtenfluss eingebunden wird.

Vorteile (guter) asymmetrischer Verfahren:

- Jeder Teilnehmer einer vertraulichen Kommunikation muss nur seinen eigenen privaten Schlüssel geheim halten.
- Sie lassen sich einfach für digitale Signaturen benutzen.
- Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, da die öffentlichen Schlüssel bzw. Schlüsselzertifikate frei zugänglich auf zentralen Servern gespeichert werden können, ohne die Sicherheit des Verfahrens zu beeinträchtigen.
- Sie sind gut geeignet für Nicht-Abstreitbarkeitszwecke.

Nachteile asymmetrischer Verfahren:

- Sie sind langsam, d. h. sie haben im allgemeinen einen geringen Datendurchsatz.
- Sicherheit: für alle bekannten Public-Key-Verfahren gilt:
  - Es gibt wesentlich bessere Attacken als das Durchprobieren aller Schlüssel, deshalb werden (im Vergleich zu symmetrischen Verfahren) relativ lange Schlüssel benötigt, um ein gleich hohes Maß an Sicherheit zu erreichen.
  - Die Sicherheit beruht "nur" auf der vermuteten, aber von der Fachwelt anerkannten, algorithmischen Schwierigkeit eines mathematischen Problems (zum Beispiel die Zerlegung einer großen Zahl in die Primfaktoren).
- Die Schlüsselerzeugung ist i. allg. komplex und aufwendig, da die Erzeugung "schwacher" Schlüsselpaare vermieden werden muss.

**Hybride Verfahren** versuchen, die Vorteile beider Arten von Verschlüsselung zu kombinieren: sie benutzen asymmetrische Verschlüsselung, um einen Sitzungsschlüssel ("Sessionkey") für ein symmetrisches Verfahren zu übermitteln, und verschlüsseln die Massendaten mit dem symmetrischen Verfahren. Der Sessionkey wird gewöhnlich nur für eine Sitzung (Übertragung) verwendet und dann vernichtet. Das asymmetrische Schlüsselpaar wird je nach Umständen für einen langen Zeitraum verwendet.

### II. Integritätsschutz

Das Ziel des Integritätsschutzes ist es, dass ein Empfänger einer Nachricht feststellen kann, ob er diese Nachricht unverfälscht erhalten hat. Das Grundprinzip des Integritätsschutzes besteht darin, die Nachricht unverschlüsselt und unverändert zu übersenden, gleichzeitig aber bestimmte Kontrollinforma-

tionen mitzuschicken, die die Kontrolle auf Unverfälschtheit der eigentlichen Nachricht ermöglichen. Voraussetzung dazu ist allerdings, dass der Empfänger die Kontrolldaten unmanipuliert erhält. Für diese Kontrolldaten stellen sich damit folgende Bedingungen:

- Der Umfang der Kontrollinformationen muss möglichst gering sein, um die zusätzlich zu übertragenden Informationen zu minimieren.
- Praktisch jede Manipulation, auch nur eines einzelnen Bits der Nachricht muss anhand der Kontrollinformationen feststellbar sein.
- Die Kontrollinformationen müssen unmanipulierbar übertragen bzw. Manipulationen müssen entdeckt werden können.

Zur Berechnung der Kontrollinformationen werden typischerweise zwei Verfahren verwendet: Hashfunktionen und Message Authentication Codes.

Eine (Einweg-)**Hashfunktion** ist eine Datentransformation mit folgenden Eigenschaften:

- Kompressionseigenschaft: Beliebig lange Bitfolgen werden auf Bitfolgen fester, i. allg. kürzerer Länge abgebildet (typischerweise 128 - 160 Bit).
- "Einweg"-Eigenschaft: Es muss "praktisch unmöglich" sein, zu einem vorgegebenen Hashwert eine Nachricht zu finden, deren Hashwert der vorgegebene Hashwert ist.
- Kollisionswiderstand: Es muss "praktisch unmöglich" sein, zwei Nachrichten zu finden, die zum gleichen Hashwert führen.

Mit Hilfe einer beiden Kommunikationspartnern bekannten Hashfunktion können A und B die Integrität einer Nachricht überprüfen: Alice hasht ihre Nachricht, und übermittelt diese und den Hashwert so an Bob, dass die Unverfälschtheit des Hashwertes gewährleistet ist. Bob hasht die empfangene Nachricht ebenfalls und vergleicht sein Ergebnis mit dem von Alice gelieferten Hashwert. Stimmen beide Werte überein, so kann er davon ausgehen, dass kein Bit der Nachricht verändert wurde.

Ein **Message Authentication Code (MAC)** ist eine kryptographische Checksumme zur Nachrichtensicherung, also eine Datentransformation, bei der zusätzlich ein geheimer Schlüssel in die Berechnung eingeht, mit folgenden Eigenschaften:

- Kompressionseigenschaft: Beliebig lange Bitfolgen werden auf Bitfolgen fester, i. allg. kürzerer Länge abgebildet.
- Fälschungssicherheit: Für jeden, der nicht im Besitz des Schlüssels ist, muss es "praktisch unmöglich" sein, den MAC-Wert einer neuen Nachricht zu berechnen, selbst wenn er in den Besitz einiger alter Nachrichten mit den zugehörigen MAC-Werten gelangt ist.

Besitzen Alice und Bob einen MAC und einen gemeinsamen, geheimen MAC-Schlüssel, so authentisiert Alice ihre Nachricht einfach dadurch, dass sie den MAC-Wert der Nachricht berechnet und zusammen mit der Nachricht an Bob schickt. Bob berechnet seinerseits den MAC-Wert der empfangenen Nachricht mit dem auch ihm bekannten MAC-Schlüssel. Stimmt dieser mit Alices Wert überein, so kann er davon ausgehen, dass die Nachricht authentisch ist (d. h. dass sie nicht verändert wurde und wirklich von Alice stammt). Alice hat also ihre Nachricht durch Verwendung des nur ihr und Bob bekannten Schlüssels gegenüber Bob authentisiert.

MACs werden häufig auf Basis symmetrischer Chiffrierverfahren konstruiert. Die bekannteste Variante ist hierbei die Verschlüsselung einer Nachricht mit DES oder einem anderem Block-Chiffrierverfahren im CBC- oder CFB-Mode. Dabei wird als MAC der letzte verschlüsselte Block an die Nachricht angehängt. Daneben gibt es aber auch MACs, die nicht auf Chiffrierverfahren be-

ruhen. Der MAC-Wert einer Nachricht kann als fälschungssichere, schlüsselabhängige, kryptographische Checksumme dieser Nachricht angesehen werden. Die Anwendung von MACs zum Zweck der Authentisierung

erfordert, dass beide Parteien den geheimen Authentisierungsschlüssel zuverlässig schützen. Als Nebeneffekt des Integritätsschutzes kann mit oben skizzierten Verfahren gleichzeitig vom Empfänger der Nachricht nachgeprüft werden, dass die als unmanipuliert verifizierte Nachricht nur vom tatsächlich bekannten Sender verschickt werden konnte. Dieser Schluss lässt sich ziehen, da nur dieser Sender die notwendigen Schlüssel zur Verschlüsselung bzw. Ermittlung der Kontrollinformationen besitzt.

**III. Authentizitätsnachweise**

Bei der Authentisierung von Benutzern gegenüber Kommunikationspartnern/IT-Systemen bzw. Clients gegenüber Servern sollen

- illegitime Zugriffe erkannt und abgewehrt werden,
- legitime Zugriffe erlaubt werden und
- sensible Daten auch bei Übertragungen über Netze geschützt bleiben.

Dazu sind Verfahren erforderlich, die allen Beteiligten die Feststellung der Identität ihrer Kommunikationspartner unmissverständlich erlauben. Dies schließt einen Zeitaspekt ein: Alice will Bob in "real time" davon überzeugen, dass tatsächlich sie mit ihm kommuniziert. Die Haupttechniken für solche Authentisierungen sind kryptographische Challenge-Response-Protokolle.

Hierbei sendet Bob Daten an Alice und fordert sie auf (Challenge), ihm den Besitz eines Geheimnisses (also einer Schlüsselinformation) nachzuweisen, und Alice demonstriert ihm diesen Besitz ohne das Geheimnis selbst preiszugeben, indem sie eine vom Geheimnis und seiner Challenge abhängige Antwort sendet (Response). Bob wiederum überprüft anhand der Antwort, dass zur Berechnung der Antwort wirklich das korrekte Geheimnis verwendet wurde.

Für eine "starke" Authentisierung dürfen sich die Challenges nicht wiederholen. Bei Challenge-Response-Verfahren können sowohl symmetrische als auch asymmetrische Techniken verwendet werden.

**Beispiel:** Alice und Bob verständigen sich vorab auf ein symmetrisches Verschlüsselungsverfahren und einen gemeinsamen kryptographischen Schlüssel. Zur Authentisierung sendet Bob eine Zufallszahl als Challenge an Alice. Alice wiederum verschlüsselt diese Zufallszahl mit dem gemeinsamen geheimen Schlüssel und sendet das Ergebnis zurück an Bob. Im nächsten Schritt entschlüsselt Bob die Nachricht und vergleicht, ob das Ergebnis seine anfangs gewählte Zufallszahl ist. Bei Gleichheit ist es tatsächlich Alice, da nur sie den geheimen Schlüssel kennt.

**IV. Digitale Signatur**

Das kryptographische Konstrukt einer digitalen Signatur dient dem Ziel, für digitale Dateien und Nachrichten ein Pendant zur handschriftlichen Unterschrift einsetzen zu können. Dazu werden einige der schon erläuterten kryptographischen Verfahren wie Hashfunktionen und asymmetrische Verfahren zusammengeführt. Die wesentliche Voraussetzung für digitale Signaturen ist, dass jeder Teilnehmer ein nur ihm bekanntes Geheimnis besitzt, mit dem er zu beliebigen Dateien eine digitale Signatur bilden kann. Anhand von öffentlichen Informationen muss es dann möglich sein, diese digitale Signatur zu überprüfen.

In diesem Sinne ist eine digitale Signatur ein spezieller Integritätsschutz mit zusätzlichen Besonderheiten. Eine **digitale Signatur** ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

Kann also anhand der öffentlich zugänglichen Informationen die digitale Signatur verifiziert werden, so ist einerseits die Integrität der signierten Datei gegeben und andererseits die Nichtabstreitbarkeit, da nur die Person, der die digitale Signatur eindeutig zugeordnet werden kann, diese Signatur anhand ihrer geheimen Informationen gebildet haben kann. Zu beachten ist, dass unterschiedliche Dateien auch unterschiedliche digitale Signaturen zur Folge haben und das geringste Änderungen an den Dateien zu nicht verifizierbaren Signaturen führen.

**Beispiel:** Ein weit verbreitetes Verfahren für digitale Signaturen ist die umgekehrte Anwendung des RSA-Verfahrens. Dabei besitzt jeder Teilnehmer einen nur ihm bekannten geheimen Signierschlüssel. Öffentlich zugänglich sind Verifizierschlüssel-Zertifikate, in denen der passende öffentliche Schlüssel und die Angaben zum Besitzer des passenden geheimen Signierschlüssels unfälschbar miteinander verknüpft sind. Diese Zertifikate werden von vertrauenswürdigen Stellen herausgegeben, die zuvor die Personalien der Teilnehmer geprüft haben.

Um für eine beliebige Datei eine digitale Signatur zu berechnen und zu prüfen, wird nun wie folgt vorgegangen:

1. Schritt: Alice berechnet den Hashwert der ausgewählten Datei.
2. Schritt: Alice verschlüsselt diesen Hashwert mit dem nur ihr bekannten geheimen Signierschlüssel. Das Ergebnis ist die digitale Signatur von Alice zu dieser Datei.
3. Schritt: Alice überträgt die digitale Signatur gemeinsam mit dem Verifizierschlüssel-Zertifikat und der Datei an Bob.
4. Schritt: Bob verifiziert das Zertifikat (z. B. mit dem öffentlichen Schlüssel einer Zertifizierungsstelle).
5. Schritt: Bob berechnet den Hashwert der erhaltenen Datei.
6. Schritt: Anhand des im Verifizierschlüssel-Zertifikat enthaltenen öffentlichen Verifizierschlüssels entschlüsselt Bob die digitale Signatur.
7. Schritt: Bob vergleicht den in Schritt 4 berechneten Hashwert und die entschlüsselte Signatur. Sind sie identisch, so ist die digitale Signatur verifiziert. Besteht keine Gleichheit, kann Bob keine weiteren Schlüsse ziehen.
8. Schritt: Nach der Verifikation der digitalen Signatur kann Bob als Ergebnisse festhalten:

    - Falls sichergestellt ist, dass tatsächlich nur Alice den geheimen Schlüssel besitzt, kann Bob sicher sein, dass die digitale Signatur von Alice, die im Verifizierschlüssel-Zertifikat aufgeführt ist, erzeugt wurde.
    - Die erhaltene Datei ist identisch mit der Datei, für die Alice die digitale Signatur berechnet hat.

Betont sei, dass digitale Signaturen ausschließlich die Ziele Integrität und Nichtabstreitbarkeit sicherstellen, jedoch in keiner Weise die Vertraulichkeit. Eine digital signierte Nachricht wird im Klartext übertragen, ist sie vertraulich, muss sie **zusätzlich** verschlüsselt werden.

Enthält eine digital signierte Datei eine Willenserklärung des Signierers, kann dann anhand der Signatur diese Willenserklärung unabstreitbar dem Signierer, ggf. auch vor Gericht, zugerechnet werden.

Die verwendeten Verifizierschlüssel-Zertifikate wiederum sind selbst von der vertrauenswürdigen Stelle digital signierte Dateien, die analog überprüft werden können und die Auskunft geben über den Verifizierschlüssel und die Person, die den dazu passenden geheimen Signierschlüssel besitzt.

Man beachte die Unterschiede zwischen MACs und digitalen Signaturen:

- Die digitale Signatur kann durch jeden, der das Verifizierschlüssel-Zertifikat besitzt, verifiziert werden, MACs dagegen nur durch die Parteien, die den geheimen Authentisierungsschlüssel kennen.
- Alices digitale Signatur einer Nachricht kann nur von Alice erstellt werden, der MAC-Wert einer Nachricht dagegen von beiden Parteien, Alice und Bob (und allen anderen, die den geheimen Authentisierungsschlüssel kennen). Es ist deshalb unmöglich, MACs für den Zweck der Verbindlichkeit einzusetzen.

Mit Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes (Bundesgesetzblatt 1879, Teil 1, 1997) ist für die Bundesrepublik Deutschland ein Gesetz zur digitalen Signatur in Kraft getreten. Dieses regelt, welche Sicherheitsanforderungen die technischen Komponenten, die für digitale Signaturen eingesetzt werden, erfüllen müssen und welche Aufgaben Zertifizierungsstellen, die Verifizierschlüssel-Zertifikate ausstellen, haben. Darüber hinaus wird geregelt, wie die erforderliche Sicherheit der Komponenten und Zertifizierungsstellen geprüft wird. Im Ergebnis wird digitalen Signaturen nach dem Signaturgesetz auch vor Gericht eine hohe Sicherheit zugebilligt.

**Schlüsselmanagement**

Bei jedem Einsatz von Verschlüsselung entsteht die Aufgabe, die Schlüssel angemessen zu verwalten. Es stellt sich die Frage, wie man

- Erzeugung/Initialisierung,
- Vereinbarung/Etablierung,
- Verteilung/Transport,
- Wechsel/Update,
- Speicherung,
- Beglaubigung/Zertifizierung,
- Rückruf,
- Wiedergewinnung im Fall von Vernichtung/Verlust,
- Vernichtung/Löschen,
- Archivierung und
- Escrow (treuhänderische Hinterlegung)

während des gesamten Lebenszyklus der Schlüssel durchführt. Das Schlüsselmanagement kann und wird sich gewöhnlich auch kryptographischer Techniken bedienen. Es muss für die Gesamtheit der Kryptomodule eines kryptographisch basierten Sicherungssystems durchgeführt werden. Geheime Schlüssel müssen vor unbefugter Aufdeckung, Modifizierung und Ersetzung geschützt werden. Öffentliche Schlüssel müssen vor unbefugter Modifizierung und Ersetzung geschützt werden. Angemessenes Schlüsselmanagement ist die Voraussetzung dafür, dass Information durch kryptographische Methoden überhaupt geschützt werden kann. Schlüsselmanagement benötigt eigens dieser Aufgabe gewidmete Ressourcen!

**Zertifizierungsstellen**

Trust Center bzw. Zertifizierungsstellen werden immer dann benötigt, wenn man für eine nicht mehr überschaubare Anzahl von Teilnehmern asymmetrische Kryptoverfahren für die digitale Signatur oder für Verschlüsselung einsetzen will. Solche Verfahren benötigen bei der Signaturbildung bzw. der Verschlüsselung einen anderen Schlüssel als bei der Signaturprüfung bzw. der Entschlüsselung. Dazu wird benutzerbezogen ein Schlüsselpaar korrespondierender Schlüssel erzeugt. Ein Schlüssel, der so genannte öffentliche Schlüssel, wird öffentlich bekanntgegeben. Der andere Schlüssel, der so genannte private Schlüssel, ist absolut geheim zu halten. Mit dem privaten Schlüssel - und nur mit diesem - kann eine digitale Signatur erzeugt bzw. ein Text entschlüsselt und mit dem zugehörigen öffentlichen Schlüssel - und nur mit diesem - verifiziert bzw. verschlüsselt werden. Will man nun die Echtheit der öffentlichen Schlüssel und die sichere Zuordnung der Schlüssel zu Personen sicherstellen, bedarf es der bereits erwähnten Trust Center / Zertifizierungsstellen, die die Zuordnung einer Person zu einem öffentlichen Schlüssel durch ein Zertifikat bestätigen.

Innerhalb solcher Zertifizierungsstellen werden typischerweise folgende Aufgaben wahrgenommen:

- Schlüsselgenerierung: Es sind für die Zertifizierungsstelle und ggf. für Teilnehmer Schlüsselpaare zu generieren.
- Schlüsselzertifizierung: Die Teilnehmerdaten, der korrespondierende öffentliche Schlüssel und weitere Daten werden zu einem Zertifikat zusammengefasst und von der Zertifizierungsstelle digital signiert.
- Personalisierung: Das Zertifikat und ggf. öffentlicher und privater Schlüssel werden auf eine Signaturkomponente (i. a. eine Chipkarte) übertragen.
- Identifizierung und Registrierung: Die Teilnehmer werden gegen Vorlage eines Ausweispapieres identifiziert und registriert.
- Verzeichnisdienst: Zertifikate werden in einem öffentlichen Verzeichnis abrufbar gehalten. Darüber hinaus muss der Verzeichnisdienst Auskunft darüber geben, ob ein Zertifikat gesperrt ist oder nicht.
- Zeitstempeldienst: Für bestimmte Daten kann es notwendig sein, diese mit einem vertrauenswürdigen Zeitpunkt zu verknüpfen. Dazu wird der Zeitpunkt an die Daten angehängt und das Ergebnis vom Zeitstempeldienst digital signiert.

Trust Center können außerdem zusätzlich Schlüsselaufbewahrung als Dienstleistung anbieten, wenn die kryptographischen Schlüssel für Verschlüsselung eingesetzt werden sollen. Um bei Schlüsselverlust noch auf die verschlüsselten Daten zugreifen zu können, kann dann der Schlüsselbesitzer (und nur dieser) eine Schlüsseldublette erhalten, die im Trust Center geschützt aufbewahrt wird.

**Schlüsselverteilungszentralen**

Die Sicherheit symmetrischer Verschlüsselungsverfahren hängt davon ab, ob der gemeinsam benutzte geheime Schlüssel nur den zum Zugriff auf die geschützten Informationen berechtigten Benutzern bekannt ist. Im Falle des Schutzes gespeicherter Daten, auf die nur deren Eigentümer Zugriff haben soll, ist dies relativ einfach zu gewährleisten, da dieser Eigentümer lediglich den Schlüssel so schützen muss, dass Unbefugte nicht darauf zugreifen können.

Anders sieht es jedoch aus, wenn Nachrichten, die von einem Sender über ein unsicheres Übertragungsmedium an einen Empfänger zu übermitteln sind, mit

einem symmetrischen Verschlüsselungsverfahren geschützt werden sollen. In diesem Fall muss der geheime Schlüssel sowohl beim Sender als auch beim Empfänger vorliegen, d. h. es muss eine Möglichkeit geschützten Informationsaustauschs zwischen den beiden Partnern verfügbar sein. In der Praxis wird dies oft durch die verschlüsselte Verteilung von Kommunikationsschlüsseln durch so genannte Schlüsselverteilungszentralen (Key Distribution Centers, KDCs) realisiert, wobei ganze Hierarchien voneinander sicherheitstechnisch abhängiger Schlüssel aufgebaut werden. Die hier zum Einsatz kommenden Verfahren sind teilweise sehr komplex und hängen hinsichtlich ihrer Sicherheit von einer Vielzahl von Komponenten ab, insbesondere von der physischen, organisatorischen, personellen und technischen Sicherheit der KDCs und der zur Kommunikation mit den KDCs vereinbarten Schlüssel.

Eine Kompromittierung eines geheimen Schlüssels, d. h. sein Bekanntwerden gegenüber einem unberechtigten Dritten, führt zum Verlust der Vertraulichkeit aller Daten, deren Verschlüsselung mit diesem Schlüssel erfolgte bzw. davon abhängt. Dies ist insbesondere dann kritisch, wenn einer der zentralen Schlüssel einer Schlüsselverteilungshierarchie kompromittiert wurde.

**Einsatz kryptographischer Verfahren**

Bei sachgemäßem Einsatz sind kryptographische Verfahren hervorragend geeignet, folgende Bedrohungen abzuwehren:

- Kenntnisnahme von Informationen durch Unbefugte,
- bewusste Manipulation von Daten durch Unbefugte und
- Manipulationen an der Urheberschaft von Informationen.

Der alleinige Einsatz von Kryptographie reicht allerdings **nicht** aus, um alle Bedrohungen abzuwehren.

- Der Einsatz kryptographischer Methoden trägt nichts dazu bei, um die Verfügbarkeit von Daten zu gewährleisten (bei unsachgemäßem Gebrauch von Verschlüsselung droht sogar Datenverlust!).
- Kryptographische Methoden können gegen Denial-of-Service-Attacken (siehe auch G 5.28 *Verhinderung von Diensten*) nichts ausrichten. Sie können aber zur frühzeitigen Erkennung solcher Attacken beitragen.
- Sie helfen auch nicht gegen zufällige Verfälschungen von Informationen (etwa durch "Rauschen"). Sie können Verfälschungen aber nachträglich erkennbar machen.

# M 3.24 Schulung zur Lotus Notes Systemarchitektur für Administratoren

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 3.88 *Zielgruppenspezifische Schulungen zu Lotus Notes/Domino* integriert.

# M 3.25 Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 3.88 *Zielgruppenspezifische Schulungen zu Lotus Notes/Domino* integriert.

# M 3.26 Einweisung des Personals in den sicheren Umgang mit IT

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Viele Sicherheitsprobleme entstehen durch fehlerhafte Benutzung bzw. Konfiguration der IT. Um solchen Problemen vorzubeugen, sind alle Mitarbeiter und alle externen IT-Benutzer in den sicheren Umgang mit der IT der Institution einzuweisen. Hierzu müssen alle Mitarbeiter entsprechend sensibilisiert und geschult werden (siehe auch M 3.5 *Schulung zu Sicherheitsmaßnahmen* und M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*).

Allen IT-Benutzern muss deutlich gemacht werden, welche Rechte und Pflichten sie bei der IT-Nutzung haben. Ihnen sollten spezifische Richtlinien an die Hand gegeben werden, was sie im Umgang mit der IT beachten müssen. In einer solchen Richtlinie ist zu beschreiben, welche Randbedingungen es beim Einsatz der betrachteten IT-Systeme gibt und welche Sicherheitsmaßnahmen zu ergreifen sind. Dabei sind die Benutzer klar und unmissverständlich darauf hinzuweisen, was sie auf keinen Fall machen dürfen. Diese Richtlinien sollten verbindlich, verständlich, aktuell und verfügbar sein. Um die Verbindlichkeit zu dokumentieren, sollten sie von der Behörden- bzw. Unternehmensleitung oder zumindest vom IT-Verantwortlichen unterzeichnet sein. Es empfiehlt sich auch, sie kurz und verständlich zu formulieren, sodass sie beispielsweise als Poster, Merkzettel, Flyer, Karteikarte oder Ähnliches verteilt werden können. Zusätzlich sollten sie im Intranet abrufbar sein.

Benutzerrichtlinien sollten grundsätzlich nur Regelungen enthalten, die auch umgesetzt werden können, und so positiv wie möglich formuliert werden. Beispielsweise könnte eine Benutzerrichtlinie statt

"Benutzer dürfen keine Software selbständig installieren."

so lauten:

"Alle IT-Systeme werden in einer Standardkonfiguration ausgeliefert, die auf Ihre spezifischen Arbeitsbedingungen angepasst wurde und Ihnen maximale Sicherheit bietet. Bei Problemfällen können wir Ihnen durch eine Neuinstallation der Standardkonfiguration eine schnelle Problemlösung garantieren. Bitte verändern Sie daher die Einstellungen möglichst nicht. Wenn Sie zusätzliche Hard- oder Software benötigen, wenden Sie sich bitte an den Benutzerservice."

Weitere Beispiele für Benutzerrichtlinien finden sich unter den Hilfsmitteln zum IT-Grundschutz.

Eine Benutzerrichtlinie für die allgemeine IT-Nutzung sollte mindestens die folgenden Punkte umfassen:

- Hinweis, dass keine IT-Systeme oder IT-Komponenten ohne ausdrückliche Erlaubnis benutzt werden dürfen
- Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT-Systemen ändern dürfen, die dazu autorisiert sind
- Umgang mit Passwörtern (siehe M 2.11 *Regelung des Passwortgebrauchs*)

- Nutzungsverbot nicht freigegebener Software (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*)
- Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen, beziehungsweise eine präzise Beschreibung möglicher Ausnahmen von dieser Regel, falls es sie gibt,
- Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern
- Schutz vor Computer-Viren und anderer Schadsoftware
- Durchführung von Datensicherungen
- Nutzung von Internet-Diensten

Neben solchen Richtlinien müssen klare Aussagen darüber vorliegen, welche Benutzer auf welche Informationen zugreifen dürfen, an wen diese weitergegeben werden dürfen und welche Maßnahmen bei einem Verstoß gegen diese Richtlinien unternommen werden.

Wenn ein Benutzer seinen Arbeitsplatz verlässt, sollte er sich davon überzeugen, dass jedes Arbeitsmittel (Dokumente, Datenträger, etc.) sicher verwahrt ist (siehe auch M 2.37 *Der aufgeräumte Arbeitsplatz*). Alle IT-Systeme sollten durch Passwörter gegen unbefugten Zugriff geschützt sein. Bei unbeaufsichtigten IT-Systemen ist der Computer mindestens zu sperren.

Die Grundkonfiguration aller IT-Systeme sollte möglichst eingeschränkt sein. In der Standardkonfiguration von Arbeitsplatzrechnern sollten nur die Dienste vorhanden sein, die von allen Benutzern einer Gruppe benötigt werden (siehe auch M 4.109 *Software-Reinstallation bei Arbeitsplatzrechnern*). Weitere Programme oder Funktionen dürfen nur dann aufgespielt bzw. freigeschaltet werden, wenn die Benutzer in deren Handhabung eingewiesen und für eventuelle Sicherheitsprobleme sensibilisiert wurden.

Jede Benutzerordnung sollte in Zusammenarbeit mit Vertretern aller beteiligten Gruppen erstellt werden, insbesondere sind Personalvertretungen und Datenschutz- sowie IT-Sicherheitsbeauftragte rechtzeitig zu beteiligen. Bei jeder Änderung einer Benutzerordnung ist darauf zu achten, dass die Betroffenen wieder im Vorfeld beteiligt werden. Die geänderte Benutzerordnung muss allen Benutzern bekannt gegeben werden.

Die Aufgabenbeschreibung sollte alle für die Informationssicherheit relevanten Aufgaben und Verpflichtungen enthalten. Dazu gehört u. a. die Verpflichtung auf die hausinternen Leitlinien zur Informationssicherheit (siehe auch M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*).

Werden IT-Systeme oder Dienste in einer Weise benutzt, die den Interessen der Behörde bzw. des Unternehmens widersprechen, sollte jeder, der davon Kenntnis erhält, dies seinen Vorgesetzten mitteilen.

Prüffragen:

- Sind alle IT-Benutzer in den sicheren Umgang mit der IT der Institution eingewiesen worden?
- Gibt es eine verbindliche, verständliche, aktuelle und verfügbare Richtlinie zur IT-Nutzung?

# M 3.27 Schulung zur Active Directory-Verwaltung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Das Active Directory ist die zentrale Datenbank der Serverbetriebssysteme Windows Server 2000 und Windows 2003 Server (im Folgenden unter dem Begriff Windows-Server zusammengefasst), in der Benutzerdaten, Gruppenzugehörigkeiten und andere Verwaltungsdaten abgelegt werden. Clients können im Active Directory ab der Version Windows 2000 verwaltet werden.

Für die Administration eines Windows-Netzes werden detaillierte Kenntnisse des Active Directory und seiner grundlegenden Konzepte benötigt. Ansonsten kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitstechnische Auswirkungen haben können. Eine Schulung der Administratoren auf diesem Gebiet und insbesondere zu Active Directory Sicherheitsthemen ist daher unerlässlich.

**Schulungsinhalte**

Je nach Größe und Komplexität des Netzes, wird ein Active Directory nicht von einem einzelnen Administrator, sondern von einer ganzen Reihe von Administratoren mit speziellen Aufgaben und Tätigkeitsbereichen durchgeführt. Insoweit besteht auch nicht für alle Administratoren eines Active Directories der gleiche Schulungsbedarf. Zur Gewährleistung eines sicheren Betriebes muss jedoch jeder Administrator über ein hinreichendes Grundwissen verfügen, um seine eigenen Tätigkeiten in einen Gesamtkontext einordnen zu können.

Schulungsinhalte sollten in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern. Wie tief ein Administrator sich mit den einzelnen Punkten beschäftigen muss, hängt von seinem späteren Tätigkeitsfeld ab.

**Grundlagen**
- Überblick über die Sicherheitsmechanismen von Windows-Server
- Neuerungen in Sicherheitsmechanismen von aktuellen Windows-Client-Betriebssystemen (mit Berücksichtigung der von neuen Betriebssystemversionen oder aktuellen Service Packs hervorgerufenen Änderungen)
- Sicherheitsverwaltung (MMC, Security Editor, GPMC)
- Active Directory und DNS
- Vertrauensbeziehungen zwischen Domänen
- Notwendiger physikalischer Schutz aller Domänen-Controller als Träger der Kerberos Daten

**Active Directory**
- Allgemeines: Planung, Einrichtung, Administration
- Schema-Verwaltung
- Replikation
- Backup
- Rechtevergabe
- Authentisierung
- Gruppenrichtlinien

**PKI (Public Key Infrastruktur)**
- Funktionsweise einer PKI
- Zertifikate und Zertifikatstypen

- Planung einer PKI
- Einrichten einer PKI
- Verwalten einer PKI
- Benutzerinteraktion mit der PKI

**EFS (Encrypting File System)**
- Funktionsweise des EFS
- Konfiguration des EFS (Recovery-Agent, Zertifikate)
- Schlüsselbackup
- Schutz verschlüsselt gespeicherter Dateien bei der Netzkommunikation

**IPSec**
- Funktionsweise des IPSec
- Konfiguration des IPSec
- Umgang mit *ipsecmon.exe* oder einem IPSec-Monitor eines Drittherstellers

**WFP (Windows File Protection)**
- Funktionsweise der WFP
- Konfigurationsmöglichkeiten der WFP

**DFS (Distributed File Service)**
- Funktionsweise des DFS
- Administration des DFS
- Planung der DFS-Struktur
- Schutz der über DFS zugreifbaren Daten

Die einzelnen Active Directory Themen sollten dabei wie folgt detaillierter dargestellt werden:

**Schema-Verwaltung**

Im Normalfall ist eine installationsspezifische Veränderung des Active Directory-Schemas durch einen Administrator nicht notwendig. Die Schulung kann sich insofern auf die Problematik und Auswirkungen von Schema-Veränderungen beschränken.

Sollen individuelle Anpassungen des Schemas vorgenommen werden, sind weitergehende Schulungen zu Interna des Active Directory notwendig.

**Replikation des Active Directory**
- Verwendete Mechanismen zur Replikation des Active Directory (RPC und SMTP)
- Voreingestellte Parameter zur Replikation von Active Directory Inhalten
- Problematik der dezentralen Administration des AD im Zusammenhang mit Replikationskonflikten

**Backup**
- Problematik des Erstellens eines "Backups des Active Directory"
- Wiedereinspielen von Backups eines Domänen-Controllers
- Zu ergreifenden Maßnahmen bei Ausfall von Domänen-Controllern, die FSMO-Rollen innehaben

**Rechtevergabe im Active Directory**
- Vergabe von Zugriffsrechten auf AD-Objekte auf Attributsebene
- Vererbung von Zugriffsrechten und Blockade der Vererbung
- Mögliche Zugriffsrechte
- Delegation von administrativen Aufgaben auf der Ebene einzelner OUs

**Authentisierung**
- Kerberos
- PKI
- Smart Cards

**Gruppenrichtlinien**
- Lokale Gruppenrichtlinien und im Active Directory gespeicherte Gruppenrichtlinien
- Konfigurationsmöglichkeiten mit Hilfe von Gruppenrichtlinien
- Wann werden Gruppenrichtlinien angewandt? Wie lässt sich dies konfigurieren?
- Gruppenrichtlinienobjekte (GPOs) sind Objekte im Active Directory
- Gruppenrichtlinienobjekte können an Standorte / Domänen / OUs gebunden werden
- Reihenfolge, in der Gruppenrichtlinien abgearbeitet werden
- Möglichkeiten, die Anwendung von Gruppenrichtlinien zu kontrollieren
    - Vergabe von Zugriffsrechten auf Gruppenrichtlinien
    - *No Override* Eigenschaft der Bindung eines Gruppenrichtlinienobjektes an ein AD-Objekt
    - *Block Policy Inheritance* Eigenschaft von AD-Objekten
- Möglichkeiten zur selektiven Anwendung der Gruppenrichtlinien unter Windows XP:
    - *Sicherheitsfilter*
    - *WMI Filters*

Prüffragen:

- Sind die Administratoren für die Arbeit mit Active Directory geschult?
- Sind die Administratoren mit allen Sicherheitsmechanismen und -aspekten von Active Directory in ihrem Tätigkeitsbereich vertraut?

# M 3.28 Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, Vorgesetzte

Die Sicherheit der Daten, die auf Windows-Systemen gespeichert sind, hängt zu einem großen Teil vom korrekten Umgang der Benutzer mit den Sicherheitsmechanismen der Windows-Systeme ab. Um diese effektiv nutzen zu können, sollten Benutzer von Windows-Systemen entsprechend geschult werden, dazu ist ein Konzept notwendig.

**Benutzersicht auf Sicherheitsmechanismen**

Beim Umgang mit Windows-Systemen kann dem Benutzer ein großer Teil der sicherheitsrelevanten Einstellungen durch entsprechende Vorarbeiten und Voreinstellungen des Administrators abgenommen werden. Um einheitliche und überprüfbare Systemkonfigurationen zu erhalten, ist ein solches Vorgehen unabdingbar (siehe M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*).

Einige sicherheitsrelevante Einstellungen können allerdings vom Benutzer selbst vorgenommen werden. Dazu gehören die Zugriffsrechte auf die eigenen Dateien und Verzeichnisse. Die Zugriffsrechte können einzelnen Benutzern oder Benutzergruppen eingeräumt oder verweigert werden. Widersprechen sich die für einen Benutzer konfigurierten Zugriffsrechte wird der Zugriff verweigert. Ein Beispiel dafür wäre, wenn der Benutzer Mitglied der beiden Gruppen A und B ist, wobei der Zugriff für Gruppe A zugelassen ist, während er für Gruppe B verweigert wird.. Generell gilt, dass die Zugriffsrechte auf die eigenen Dateien eines Benutzers vom Administrator voreingestellt und automatisch auf neue Dateien und Ordner übertragen werden. Da Benutzer jedoch in der Regel die Möglichkeit besitzen, die Zugriffsrechte zu verändern, ist es notwendig, dass jeder Benutzer entsprechend geschult wird (siehe dazu auch M 4.149 *Datei- und Freigabeberechtigungen unter Windows*). In den Richtlinien der Institution sollte festgelegt werden, welche Benutzer welche Einstellungen vornehmen dürfen oder ob die Änderung der Zugriffsrechte durch den Benutzer generell verboten wird. Empfehlenswert ist hier die Regelung, dass zumindest Benutzer mobiler Clients im Umgang mit der Vergabe der Zugriffsrechte an ihren Daten geschult werden. Für Benutzer mit stationären Clients kann dies als optional vereinbart werden.

Ein weiterer Aspekt, auf den eine Benutzerschulung eingehen muss, ist die Verwendung des verschlüsselnden Dateisystems EFS (Encrypting File System). Neben der Vermeidung von Fallstricken bei der Benutzung des EFS sollte hier vor allem vermittelt werden, in welchem Ausmaß EFS die Vertraulichkeit von Daten in Dateien schützen kann, und wo dieser Schutz aufhört (siehe auch M 4.147 *Sichere Nutzung von EFS unter Windows*). Bei Einsatz von Windows Vista und Windows 7 sollte auf die Möglichkeiten eingegangen werden, die ein gleichzeitiger Einsatz von BitLocker zur Festplattenverschlüsselung und EFS bieten. Die Benutzer sollten auf jeden Fall darin geschult werden, wie sie die Schlüsselinformationen zu verwalten haben, um die Verfügbarkeit der Daten stets zu gewährleisten.

Bei der Verwendung von BitLocker zur Festplattenverschlüsselung (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*) muss das dadurch erreichbare Schutzniveau der Vertraulichkeit in der Benutzerschulung behandelt werden. Des Weiteren sollte den Benutzern das gewählte Verfahren zur Authentisierung des Benutzers gegenüber BitLocker beim Start von Windows Vista und Windows 7 sowie die Bedeutung des Wiederherstellungskennworts und die Grenzen der Schutzwirkung in der Schulung erläutert werden.

Windows Vista und Windows 7 bieten verschiedene Methoden der Datensicherung an (siehe M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*).

Dem Benutzer muss erläutert werden, welche Methoden der Datensicherung von ihm angewandt werden sollten. Weiterhin muss dem Benutzer bekannt sein, wo sich gesicherte Daten befinden, wie er bei Bedarf auf diese zugreifen kann und was er zur Wiederherstellung seiner Daten unternehmen muss.

**Schulungsinhalte**

Die folgenden Stichpunkte fassen notwendige Schulungsinhalte für den sicheren Umgang von Benutzern mit Windows-Systemen zusammen:

**Verwendung von Zugriffsrechten im NTFS Dateisystem**
- Schutz von Dateien durch Zugriffsrechte
- Vererbung von Zugriffsrechten
- Kopieren und Verschieben von Dateien
- Übergabe einer Datei an einen neuen Besitzer
- Sensibilisierung für Beschränkungen des Schutzes von Dateien durch Zugriffsrechte
- Benutzer mit administrativen Rechten können Zugriffsrechte umgehen.
- Bei direktem Zugriff auf die Hardware (z. B. nach Ausbau einer Festplatte) lassen sich Zugriffsrechte umgehen.
- Dateien sind beim Transport über das Netz nicht geschützt.
- Bedeutung, Funktionsweise und Bedienung der Benutzerkontensteuerung (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*) falls Benutzer damit in Berührung kommen.

**Einsatz der integrierten Windows Firewall**
- Funktionsweise und Schutzwirkung

**Benutzung von EFS (siehe auch M 4.147 *Sichere Nutzung von EFS unter Windows*)**
- Nutzen von EFS (EFS bietet einen zusätzlichen Schutz der Vertraulichkeit von Dateien)
- Bedienung von EFS
- Problematik des "nachträglichen Verschlüsselns"
- Geeignete Passwort-Auswahl (Passwortqualität ist wesentlich für die Effektivität von EFS)
- Verwendung eines zusätzlichen Startpasswortes mittels *syskey* (wesentlich bei Verwendung lokaler Benutzerkonten)
- Sensibilisierung für Beschränkungen des Schutzes durch EFS
- Benutzer mit administrativen Rechten können die Verschlüsselung umgehen.
- Verschlüsselt gespeicherte Dateien sind beim Transport über das Netz nicht geschützt es sei denn, EFS wird mit WebDAV verwendet.
- Einsatz von EFS ergänzend zu BitLocker unter Windows Vista und Windows 7, falls eine Verschlüsselung im laufenden System erforderlich ist.

- Einsatz von BitLocker unter Windows Vista und Windows 7
- Verschlüsselte und nicht verschlüsselte Partitionen
- Schutzwirkung durch BitLocker besteht nur im ausgeschalteten Zustand (Offline Verschlüsselung).
- Angemessener Umgang mit den Authentisierungsmitteln (USB-Stick und/ oder PIN)
- Einsatzzweck sowie angemessener Umgang mit dem Wiederherstellungskennwort, wenn dies dem Benutzer zugänglich sein soll
- Reaktion auf BitLocker-Fehlermeldungen, insbesondere in Bezug zu erkannten Integritätsverletzungen

**Sonstige Sicherheitshinweise**

- Sicheres Löschen von Dateien (siehe M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*, die auch auf Windows 2000, Windows XP, Windows Vista und Windows 7 angewendet werden sollten
- Sicherheitshinweise zum automatischen Erkennen von CD-ROMs und zur Autostart-Funktion (siehe M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*)
- Sicherheitshinweise zum sicheren Umgang mit Wechselmedien, wie USB-Speichermedien (siehe M 4.200 *Umgang mit USB-Speichermedien* und speziell beim Einsatz von Windows Vista und Windows 7 M 4.339 *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*).
- Sicherheitshinweise zur sicheren Benutzung von spezifischen Sicherheitstechnologien unter Windows XP, Windows Vista und Windows 7 Sicherheitszentrum / Wartungscenter, Windows Firewall und WPA (WiFi Protected Access)
- Bedeutung, Funktionsweise und Bedienung der Benutzerkontensteuerung (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*) falls Benutzer damit in Berührung kommen.

Prüffragen:

- Existiert ein Konzept für die Benutzerschulung zur Sicherheit von Windows Client-Betriebssystemen?
- Werden die Benutzer in die Vergabe von Zugriffsrechten auf eigene Dateien eingewiesen?
- Werden die Benutzer auf die Sicherheitsmechanismen (z. B. Verschlüsselung mit EFS und BitLocker) der verwendeten Werkzeuge hingewiesen und in deren Nutzung geschult?
- Werden die Benutzer auf die Methoden zur Datensicherung hingewiesen und geschult?
- Werden die Benutzer in der Benutzung der Windows Firewall geschult?

# M 3.29 Schulung zur Administration von Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für die Administration eines eDirectory-Verzeichnisdienstes werden detaillierte Kenntnisse über dieses Produkt und seine grundlegenden Konzepte benötigt. Sind diese Kenntnisse nicht vorhanden, kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitstechnische Auswirkungen haben können. Eine Schulung von Administratoren auf diesem Gebiet ist daher unerlässlich.

Im Folgenden wird kurz zusammengefasst, welche Themen bei der Schulung der Administratoren behandelt werden sollten.

Der eDirectory-Verzeichnisdienst ist baumartig hierarchisch strukturiert. Die einzelnen Knotenpunkte des Verzeichnisbaums bestehen aus den *Container*-Objekten, die wiederum andere Objekte enthalten können, und den so genannten *Leaf*-Objekten, welche die Endpunkte (Blätter) des Verzeichnisbaums darstellen. Jedes Objekt gehört einer eindeutigen Objektklasse an. Die Objektklasse definiert die Werte bzw. Attribute oder auch Eigenschaften, welche einem Objekt dieser Objektklasse zugewiesen werden können. Zudem werden hierarchische Relationen darin definiert, d. h. was potentielle Vater- und Kindobjekte sein können. Es gibt dafür bereits eine Anzahl seitens eDirectory vordefinierter Objektklassen. Die Definitionen der Objektklassen werden im so genannten Schema festgehalten. Werden Veränderungen an der Definition einzelner Objektklassen vorgenommen, z. B. eine Erweiterung des zugehörigen Attributsatzes, so geschieht dies über eine Änderung bzw. Erweiterung des Schemas. Eine Schemaänderung ist gewissermaßen die sensibelste Operation überhaupt, die an einem eDirectory-Verzeichnisbaum vorgenommen werden kann. Diese hat Auswirkungen auf den gesamten Baum, so dass die bisherige Konzeption des Baums neu überdacht werden muss. Die Administration des eDirectory-Schemas verlangt daher eine hohe Kompetenz im Verzeichnisdienst und ein sehr hohes Sicherheitsbewusstsein.

Jedem einzelnen Objekt und jeder Objektklasse können Zugriffsrechte auf die einzelnen Attribute des Objektes erteilt werden. Die explizite Zuweisung erfolgt dabei über die *Trustee*-Beziehungen, d. h. Eintragung von Trustees in die *Access Control List* (ACL). Die Rechte reichen dabei von *Supervisor*, d. h. einem vollständigen Administrationsrecht, bis hin zum *Browsen*, was das Durchlaufen des entsprechenden Verzeichnisbaum-Abschnittes gestattet. Die Zugriffsrechte auf die Objekte vererben sich dabei standardmäßig in der Baumhierarchie von oben nach unten. Es ist jedoch möglich, Einfluss auf den Vererbungsprozess zu nehmen, in dem so genannte *Inherited Rights Filter* (IRF) eingeführt werden. Mit diesen Filtern können automatische Vererbungen explizit ausgeblendet werden. Weiterhin besteht die Möglichkeit, so genannte Sicherheitsäquivalenzen zwischen einzelnen Objekten bzw. Objektklassen X und Y zu definieren. Dabei werden sämtliche Trustees von Objekt X automatisch auch zu Trustees von Objekt Y, d. h. das Objekt Y besitzt zumindest die gleichen Zugriffsmöglichkeiten wie Objekt X.

Schließlich kommen beim eDirectory-Zugriff dann die *effektiven Rechte* zum tragen, welche die Folge der oben genannten Rechtevergabe darstellen und bei jedem einzelnen Zugriff dynamisch berechnet werden.

Im Intranet greifen die Benutzer über geeignete Clientsoftware auf das eDirectory zu. Der Zugriff der Clients auf das eDirectory erfolgt dabei über ein proprietäres Protokoll, bei dem der private Schlüssel des sich anmeldenden Benutzers vom eDirectory verschlüsselt an den Client geschickt wird. Bei dieser Verschlüsselung ist das Benutzerpasswort involviert. Gibt der Benutzer nun sein Passwort ein, so kann der Client den privaten Schlüssel entschlüsseln, und zwischen dem Client und dem eDirectory-Server findet ein Challenge-/Response-Verfahren zur Authentisierung statt. Bei erfolgreicher Authentisierung besitzt der Benutzer nun die für ihn definierten Zugriffsrechte auf das eDirectory.

Netzapplikationen und Internet-Benutzer greifen in der Regel über das LDAP-Protokoll auf den eDirectory-Verzeichnisdienst zu. Hierbei gibt es standardmäßig drei verschiedene Anbindungsarten: den *anonymous bind*, den *proxy user anonymous bind* sowie den *NDS-user bind*. Die Voreinstellung ist, dass der anonyme Login dabei die Rechte des [Public] Objektes hat, welches standardmäßig das uneingeschränkte *Browse*-Recht auf den gesamten Verzeichnisbaum besitzt. Der anonyme Login setzt keine Authentisierung voraus. Für die Passwort-Authentisierung kann konfiguriert werden, ob dabei das Passwort im Klartext übertragen werden darf oder nicht. Für eine gesicherte Anbindung über LDAP steht das SSL-Protokoll zur Verfügung, und zwar wahlweise mit ein- oder zweiseitiger Authentisierung.

Der eDirectory-Zertifikatsserver spielt eine wichtige Rolle für die Rechtevergabe und damit für die Systemsicherheit. Ebenso hängen die Authentisierungen im Netz sowie der Aufbau eines verschlüsselten Kanals (via SSL) vom Zertifikatsmanagement ab. Die sorgfältige Administration des eDirectory-Zertifikatsservers ist daher besonders wichtig.

Der eDirectory-Verzeichnisdienst erlaubt zur Verbesserung der Skalierbarkeit und Performance eine Partitionierung der Verzeichnisdatenbank auf mehrere Server. Für die Partitionierung eines Verzeichnisbaums sind dabei eine Reihe von Regeln zu beachten, siehe dazu M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*.

Wie die Vorgängerprodukte unterstützt der eDirectory-Verzeichnisdienst *Repliken* zur Erhöhung der Fehlertoleranz und des Systemdurchsatzes. Dabei gibt es mehrere Typen von Repliken, nämlich *Master Replica*, *Read/Write Replica*, *Read-Only Replica*, *Filtered Read/Write Replica*, *Filtered Read-Only Replica* sowie *Subordinate Reference Replica*. Detaillierte Hinweise hierzu finden sich in M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*.

eDirectory unterstützt die rollenbasierte Administration sowie die Delegation von Administrationsaufgaben. Entsprechend den bei der Planung getroffenen Entscheidungen (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory* sowie M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*) müssen die verschiedenen Administratoren für ihre jeweilige Aufgabe geschult werden. Dies gilt besonders für die Gruppe der Schemaadministratoren, die in der Lage sind, das gesamte Datenbankdesign des Verzeichnisbaums zu verändern (siehe oben).

Auch die Administration der eDirectory-Clientsoftware und des LDAP-Zugriffs setzt detaillierte Kenntnisse über die Konfigurationsmöglichkeiten des Systems voraus. Dabei spielt auch das zugrunde liegende Betriebssystem eine Rolle für die Definition einer Sicherheitsumgebung, insbesondere der Dateisystemsicherheit.

Weiterhin müssen auch die für das Logging und Monitoring zuständigen Administratoren genauestens in ihre Tätigkeit eingewiesen werden.

**Schulungsinhalte**

Die Administration eines eDirectory-Verzeichnisbaums wird im Allgemeinen, je nach Größe des Netzes, nicht von einem einzelnen Administrator, sondern von einer ganzen Reihe von Administratoren mit speziellen Aufgaben und Tätigkeitsbereichen durchgeführt. Insoweit besteht auch nicht für alle Administratoren eines eDirectory-Verzeichnisses der gleiche Schulungsbedarf. Zur Gewährleistung eines sicheren Betriebes muss jedoch jeder Administrator über ein hinreichendes Grundwissen verfügen, damit er seine eigenen Tätigkeiten in einen Gesamtkontext einordnen kann.

Schulungsinhalte sollten in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern. Wie tief sich ein Administrator mit den einzelnen Aspekten beschäftigen muss, hängt von seinem späteren Tätigkeitsfeld ab.

**Grundlagen**
- Überblick über die Sicherheitsmechanismen von eDirectory
- Sicherheitsverwaltung (ConsoleOne, iMonitor)
- Baumstruktur und Namensauflösung
- Vererbung innerhalb des Verzeichnisbaums
- notwendiger physikalischer Schutz aller eDirectory-Server inklusive Replica

**Verzeichnisdienst**
- Allgemeines: Planung, Einrichtung, Administration
- Schema-Verwaltung
- Partitionierung
- Replikation
- Backup
- Rechtevergabe
- Rechtevererbung und Kalkulation der effektiven Rechte
- Authentisierung

**Public Key Infrastruktur (PKI)**
- Funktionsweise einer PKI
- Zertifikate und Zertifikatstypen
- Planung einer PKI
- Benutzerinteraktion mit der PKI
- eDirectory-Key Management Objects
- Administration des eDirectory-Zertifikatsservers

**Secure Sockets Layer (SSL)**
- Funktionsweise des SSL-Protokolls
- Konfiguration von SSL

**Lightweight Directory Access Protocol (LDAP)**
- LDAP-Zugriff auf das eDirectory
- mögliche Anbindungen der Benutzer

**Novell Client**
- Funktionsweise des Novell Clients
- Authentisierung des Novell Clients

Die einzelnen Themen sollten dabei wie folgt detaillierter dargestellt werden:

**Schema-Verwaltung**

Oftmals ist eine installationsspezifische Veränderung des eDirectory-Schemas durch einen Administrator nicht notwendig. Die Schulung kann sich insofern auf die Problematik und die Auswirkungen von Schema-Veränderungen beschränken. Sollen individuelle Anpassungen des Schemas vorgenommen werden, sind weitergehende Schulungen zu Interna von eDirectory notwendig.

**Replikation**
- Verwendete Mechanismen zur Replikation
- Voreingestellte Parameter zur Replikation von eDirectory-Inhalten
- Problematik der dezentralen Administration des eDirectory im Zusammenhang mit Replikationskonflikten

**Backup**
- Problematik des Erstellens eines "Backups des eDirectory"
- Wiedereinspielen von Backups eines eDirectory-Servers
- zu ergreifende Maßnahmen beim Ausfall von eDirectory-Servern, die die Baumstruktur definieren (d. h. die erste eDirectory-Installation innerhalb eines Verzeichnisbaums)

**Rechtevergabe im eDirectory**
- Vergabe von Zugriffsrechten auf eDirectory-Objekte auf Attributsebene
- Vererbung von Zugriffsrechten und Blockade der Vererbung
- Definition von Sicherheitsäquivalenzen
- effektive Zugriffsrechte
- rollenbasierte Administration
- Delegation von administrativen Aufgaben

Auch wenn eine Rollentrennung zwischen der Administration des eDirectory- Verzeichnisses und des zugrunde liegenden Betriebssystems in Kraft ist, sollte den eDirectory-Administratoren Grundlagenwissen zum Betriebssystem vermittelt werden. Anderenfalls wird eine Zusammenarbeit bei der Problemlösung erschwert.

Prüffragen:

- Sind alle für eDirectory zuständigen Administratoren für die Arbeit mit eDirectory geschult?

# M 3.30 Schulung zum Einsatz von Novell eDirectory Clientsoftware

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, Vorgesetzte

Für den Einsatz im Intranet wird der eDirectory-Verzeichnisdienst auf einem oder in der Regel mehreren Servern installiert. Die im eDirectory eingerichteten Benutzer und Benutzergruppen können dann über geeignete eDirectory-Clientsoftware auf den Verzeichnisdienst zugreifen, entsprechend der ihnen im eDirectory erteilten Rechte.

Je nach Art der eingesetzten Clientsoftware erfolgt der Zugriff auf eDirectory für den Benutzer transparent, so dass eine Schulung zu eDirectory-spezifischen Aspekten der Software für den Benutzer nicht notwendig ist. Sofern der eingesetzte Client jedoch eine Authentisierung des Benutzers gegenüber dem eDirectory erfordert, wie z. B. der Novell Client für Windows, müssen dem Benutzer in einer Schulung zumindest die folgenden Inhalte vermittelt werden:

- Funktionsweise und Anwendung des verwendeten Login-Mechanismus,
- Umgang mit Passwörtern sowie
- Umgang mit SSL-Authentisierung über Benutzer-Zertifikat oder Passwort.

Wird ein LDAP-Client verwendet, der dem Benutzer ein Durchlaufen des hierarchisch angeordneten Verzeichnisbaums oder die Formulierung eigener Suchanfragen auf der Ebene von LDAP-Attributen erlaubt, so ist zusätzlich eine Schulung der Benutzer zu den Themen

- Informationsmodell von eDirectory und
- effiziente Formulierung von Suchanfragen

erforderlich.

Neben den generellen Verzeichnisdienst-Clients (dem *Novell Client für Windows* sowie Libraries für Unix-Betriebssysteme) gibt es noch eine Klasse weiterer Client-Applikationen für eDirectory, die ganz speziell zur Benutzerverwaltung in (auch heterogenen) IT-Landschaften dienen: das *Novell Account Management Modul*. Diese Applikationen sind in den Anmeldevorgang der entsprechenden Betriebssysteme eingebunden und übernehmen so auch die Authentisierung von Benutzern. Daneben stehen die NDS-AS (NDS Authentication Service) für eine ganze Reihe von Plattformen (Linux, FreeBSD, HP-UX, MVS, OS/390, Solaris) zur Verfügung. NDS-AS setzt den Einsatz von Netware voraus (ab Netware 5.0, SP 4A).

Die Authentisierung ist ein wesentlicher Aspekt beim sicheren Betrieb von eDirectory. Aus Sicht des Verzeichnisdienstes sollte dabei sichergestellt sein, dass sich sowohl der Client gegenüber dem System authentisiert, als auch der Benutzer gegenüber dem Client. War die Authentisierung erfolgreich, so bietet eDirectory einen automatisierten Zugriff auf sämtliche für ihn zugängliche Objekte und Services (so genannte *Background Authentication*). Auf diese Weise wird ein *Single Sign On* realisiert.

Die Authentisierung umfasst dabei folgende Schritte: Der Benutzer gibt beim Novell Client seinen Benutzernamen ein, welcher direkt an das eDirectory weitergeleitet wird. eDirectory sucht den zugehörigen privaten Schlüssel aus seinem Verzeichnis und verschlüsselt diesen. Bei dieser Verschlüsselung ist das Benutzerpasswort sowie ein Geheimnis des Clients involviert. Dieser verschlüsselte *private key* wird an den anfragenden Client übertragen. Der Benutzer wird nun nach seinem Passwort gefragt, welches er dem Client mitteilt.

Der Client entschlüsselt daraufhin mit Hilfe dieses Passwortes und dem Client-Credential den privaten Schlüssel und hält ihn im Arbeitsspeicher. Auf Basis dieses *private keys* sowie dem Zertifikatsgegenstück findet nun die eigentliche Authentisierung mit dem eDirectory gemäß einem *Challenge-/Response*-Verfahren statt. Ist dieses erfolgreich, so ist der Benutzer eingeloggt und der private Schlüssel des Benutzers wird aus dem Arbeitsspeicher des Clients gelöscht.

Nach außen erscheint das System somit wie ein Passwort-gestütztes Authentisierungsschema, nach innen werden asymmetrische kryptographische Mechanismen eingesetzt.

Die Sicherheit der auf eDirectory-Servern gespeicherten Daten hängt zu einem großen Teil auch vom korrekten Umgang der Benutzer mit den Sicherheitsmechanismen ab. Um diese effektiv nutzen zu können, sollten Benutzer von eDirectory-Clientsoftware entsprechend geschult werden.

**Benutzersicht auf Sicherheitsmechanismen**

Beim Umgang mit eDirectory-Clientsoftware kann ein großer Teil der sicherheitsrelevanten Einstellungen dem Benutzer durch entsprechende Vorarbeiten und Voreinstellungen des Administrators abgenommen werden. Um einheitliche und überprüfbare Client-Konfigurationen zu erreichen, ist ein solches Vorgehen unabdingbar. Einige sicherheitsrelevante Einstellungen müssen allerdings vom Benutzer selbst vorgenommen werden. Dazu gehören in der Regel auf der Ebene des Betriebssystems die Zugriffsrechte auf die eigenen Dateien und Verzeichnisse eines Benutzers. Eine Verwaltung der Zugriffsrechte auf Dateien mit den Mitteln von eDirectory ist direkt nur für Datei-Server auf Basis des Betriebssystems *Netware* möglich. Indirekt sind Dateizugriffsrechte auf anderen Plattformen über die *Organizational Roles* administrierbar.

**Schulungsinhalte**

Die folgenden Stichpunkte fassen die relevanten Schulungsinhalte zusammen. Anhand des Nutzungsszenarios sollte hieraus eine geeignete Auswahl getroffen werden:

- Funktionsweise und Anwendung des verwendeten Login-Mechanismus,
- Umgang mit Passwörtern,
- Umgang mit SSL-Authentisierung über Benutzer-Zertifikat oder Passwort,
- Informationsmodell von eDirectory,
- effiziente Formulierung von Suchanfragen,
- Grundkenntnisse über die unterliegenden Betriebssysteme und deren Sicherheitskonfiguration sowie
- sicheres Löschen von Dateien (siehe z. B. auch M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*).

Prüffragen:

- Authentisierung des Benutzers gegenüber dem eDirectory erforderlich: Erhalten Benutzer eine Schulung zum eDirectory?
- Wenn Benutzer Zugriffsrechte auf eigene Verzeichnisobjekte vergeben können, werden sie in den notwendigen Konzepten und Mechanismen geschult?

# M 3.31 Schulung zur Systemarchitektur und Sicherheit von Exchange-Systemen für Administratoren

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Microsoft Exchange integriert sich in hohem Maße in das Active Directory einer Microsoft Windows-Systemumgebung. Das Active Directory ist die zentrale Konfigurations-Datenbank von Windows-Netzinfrastrukturen, in der Benutzerdaten, Gruppenzugehörigkeiten und andere Verwaltungsdaten abgelegt werden. Für die Administration von Microsoft Exchange werden daher Kenntnisse über Active Directory und seine grundlegenden Konzepte benötigt, sonst kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitsrelevante Auswirkungen haben können. Eine Schulung der Administratoren auf diesem Gebiet ist daher unerlässlich (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*).

Bei der Installation von Microsoft Exchange auf einem Windows-Server wird eine Schema-Erweiterung auf dem Schema-Master vorgenommen, um spezifische Exchange-Objekte sowie zusätzliche Attribute zu bereits bestehenden Objekten zu erzeugen. Microsoft Exchange verlangt die ständige Verfügbarkeit eines Global Catalog Servers, der in jeder Active Directory-Site angeboten wird. Außerdem müssen die Netzdienste (speziell DNS) eingerichtet und funktionsfähig sein.

Danach müssen die Einstellungen für die externe Anbindung vorgenommen werden. Dabei sind die jeweiligen Protokolle zu aktivieren und es müssen entsprechende Regeln auf den betroffenen Sicherheitsgateways definiert werden. Schließlich müssen dann noch Benutzerkonten und Gruppen konfiguriert werden.

Die beschriebenen Aspekte beziehen sich jedoch nur auf die Server-Komponente des Microsoft Exchange-Systems. Für das Gesamtsystem ist zusätzlich auch die korrekte Administration der Client-Komponenten wichtig.

Entsprechend dem oben skizzierten Vorgehen ergeben sich in der Folge eine Reihe administrativer Aufgaben, die von einem oder mehreren spezialisierten Administratoren bewerkstelligt werden müssen. Eine intensive Schulung der Administratoren und ihrer Stellvertreter auf Microsoft Exchange und Outlook ist deshalb für das reibungslose Funktionieren des Systems besonders wichtig. Die Schulung der Administratoren sollte zumindest folgende Themen umfassen:

**Grundlagen**
- Überblick über die Sicherheitsmechanismen von Windows-Server-Betriebssystemen
- Sicherheitsverwaltung (MMC-Snap-In)
- Active Directory (siehe M 3.27 *Schulung zur Active Directory-Verwaltung*) und DNS
- Vertrauensbeziehungen zwischen Domänen
- Möglichkeiten der Zugriffskontrolle auf Server

**Microsoft Exchange-Server**
- Architektur eines Exchange-Systems
- Grundlegende Konzepte und Routineaufgaben

- Konnektoren-Konzept zur Anbindung zu fremder Kommunikationssysteme
- Outlook Web Access (OWA)
- E-Mail-Filter
- Postfächer und Ordner sowie die Rechtevergabe auf diese Objekte
- Schutz der Client-Server-Kommunikation

**Microsoft Outlook**
- Benutzerprofile
- aktive Inhalte und potentiell gefährliche Dateiformate
- Auto-Reply-Funktion

Im Microsoft Technet finden sich hierzu beispielsweise für Microsoft Exchange Server 2010 die Grundlagen einer Schulung unter "Getting Started With Exchange 2010: Exchange 2010 Help".

Prüffragen:

- Wurden alle Administratoren für die Arbeit mit Microsoft Exchange, Windows Server und Active Directory geschult?
- Sind die Administratoren im Umgang mit allen relevanten Sicherheitsmechanismen von Microsoft Exchange geschult worden?
- Wurden im Rahmen der Schulung die möglichen E-Mail-Clients, insbesondere Microsoft Outlook, behandelt?

# M 3.32 Schulung zu Sicherheitsmechanismen von Outlook für Benutzer

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Outlook Nutzer müssen regelmäßig für bestehende und neue Gefährdungen in Zusammenhang mit der Benutzung von Outlook sensibilisiert werden. Dazu gehören z. B. Phishing und Vishing.

Außerdem empfiehlt es sich, die Benutzer ausreichend zu Microsoft Outlook zu schulen. Eine Schulung für Benutzer von Microsoft Outlook sollte unter anderem folgende Themen behandeln:

- Überblick: Zugriffskontrolle auf einen Microsoft Exchange-Server
- Überblick: Zugriffskontrolle auf Postfächer
- Anerkennen von Zertifikaten (Was bedeuten Cross-Zertifikate?)
- Authentisierung an der Web-Schnittstelle sowie deren Schwächen und Stärken
- Sicherer Umgang mit Internet-Zertifikaten
- Erzwingen der Kommunikationsabsicherung: Port-Verschlüsselung und SSL-Nutzung
- Beschränkungen für die Ausführung aktiver Inhalte in Microsoft Outlook
- E-Mail-Verschlüsselung und E-Mail-Signaturen
- Speicherung von Benutzerprofilen
- Umgang mit Offline-Ordnern
- Sicherheitseinstellungen für persönliche Ordner (Verschlüsselung)
- Gefährdungen bei der Nutzung der Out of Office-Funktionalität
- Umgang mit Verteilerlisten
- Umgang mit Stellvertreterberechtigungen ("Senden als")
- Verhaltensregeln für die Nutzung des Outlook Web Access (sofern diese Funktionalität überhaupt zur Verfügung gestellt wird)
- Umgang mit Outlook-Formularen

Diese Liste stellt nur einen Ausschnitt aus den notwendigen Sicherheitsthemen dar und muss organisationsspezifisch angepasst und erweitert werden. Wichtig ist, dass die Benutzer in den Umgang mit allen relevanten Sicherheitsmechanismen von Microsoft Outlook eingewiesen werden. Daneben müssen die Benutzer jedoch auch die geltenden Sicherheitsvorschriften der Institution kennen, damit diese bei der Nutzung der Sicherheitsmechanismen von Microsoft Outlook auch entsprechend umgesetzt werden können.

Prüffragen:

- Wurden alle Benutzer für die Arbeit mit Microsoft Outlook geschult?
- Werden alle Mitarbeiter auf mögliche Gefährdungen bei der Benutzung von Outlook hingewiesen?
- Sind die Benutzer in den Umgang mit allen relevanten Sicherheitsmechanismen von Microsoft Outlook eingewiesen worden?

# M 3.33 Sicherheitsüberprüfung von Mitarbeitern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder fremdem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme von neuen oder externen Mitarbeitern in Projekte überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Projekten, und
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen an der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Wenn externes Personal intern eingesetzt wird oder im Rahmen von Projekten, Kooperationen oder Outsourcing-Vorhaben auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit externen Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

Prüffragen:

- Wird die Vertrauenswürdigkeit von neuen Mitarbeitern und externem Personal hinreichend durch geeignete Nachweise geprüft?
- Ist mit externen Dienstleistern die Überprüfung des eingesetzten Personals vertraglich vereinbart?

# M 3.34 Einweisung in die Administration des Archivsystems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, Leiter IT

Um ein Archivsystem korrekt und sicher administrieren zu können, müssen sich die Verantwortlichen und hier vor allem die Administratoren und Archivverwalter mit den eingesetzten Systemen auskennen. Hierfür ist eine Schulung der verantwortlichen Archivverwalter und Administratoren notwendig. Dadurch sollen Konfigurationsfehler und Fehlverhalten vermieden werden. Die Schulung sollte mindestens folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems, Handhabung der verwendeten Archivmedien und Kennzeichnung der Archivmedien (siehe auch M 2.3 *Datenträgerverwaltung*),
- Einsatzbedingungen (Klimatisierung, etc.) des Archivsystems und der Archivmedien,
- Dokumentation der Administrationstätigkeiten,
- Protokollierung der Systemereignisse am Archivsystem,
- Vorgehensweise bei der Auffrischung der Datenbestände (siehe M 2.263 *Regelmäßige Aufbereitung von archivierten Datenbeständen* und M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*),
- Grundbegriffe von Verschlüsselung und digitaler Signatur, wenn kryptographische Verfahren verwendet werden,
- Vorgehensweise bei der Vernichtung ausgesonderter Archivmedien,
- Systemüberwachung und Wartung (Operating) des Archivsystems,
- Eskalationsprozeduren, z. B. bei
    - Nichteinhaltung von Reaktionszeiten,
    - Unterschreiten der Rest-Speicherkapazität der Archivmedien,
    - Manipulation oder Sabotage des Archivsystems oder Ereignissen höherer Gewalt sowie
    - unberechtigten Zugriffen auf archivierte Daten.

Die Schulung der Administratoren und Archivverwalter ist zu dokumentieren. Bei Systemänderungen sollten die Administratoren und Archivverwalter entsprechend weitergebildet werden.

Prüffragen:

- Werden die verantwortlichen Archivverwalter und Administratoren für ihren Aufgabenbereich geschult
- Systemänderungen am Archivsystem: Werden Administratoren und Archivverwalter bezüglich der Änderungen geschult?

# M 3.35 Einweisung der Benutzer in die Bedienung des Archivsystems

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Archivverwalter, Leiter IT

Die Archivierung ist eine besonders verantwortungsvolle Aufgabe und stellt hohe Anforderungen an die Bedienung. Die dafür vorgesehenen Mitarbeiter sind auf diese Verantwortung besonders hinzuweisen und vorzubereiten. Hierzu müssen die Benutzer entsprechend geschult werden.

Eine derartige Schulung sollte unter anderem folgende Themen umfassen:

- Vorgehensweise bei der Umwandlung analoger Daten:
  Die korrekte Vorgehensweise bei der Erfassung der Dokumente, der Umwandlung in die elektronische Form sowie der elektronischen Archivierung sind zu erläutern und anhand von praktischen Beispielen zu üben.
- Rechtliche Rahmenbedingungen der Archivierung:
  Bei der Archivierung sind rechtliche Anforderungen einzuhalten (siehe M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung*). Diese Anforderungen und die Folgen bei Nichteinhaltung müssen den Benutzern deutlich gemacht werden.
- Schutz der Vertraulichkeit und Integrität der Dokumente:
  Die korrekte Vorgehensweise bei der Behandlung vertraulicher Dokumente sowie bei der Integritätssicherung und -prüfung archivierter Dokumente ist zu demonstrieren. Auf mögliche Folgen bei fehlerhafter Bedienung ist hinzuweisen.
- Besonderheiten bei der Verwendung von WORM-Medien:
  Auf die Besonderheiten bei der Speicherung auf einmal beschreibbare Medien ist besonders hinzuweisen, das heißt es ist zu beachten, dass einmal gespeicherte Daten nicht mehr gelöscht werden können (allenfalls eine neue Version könnte erneut archiviert werden). Dies kann nicht nur zu Kapazitätsengpässen, sondern auch zu Datenschutz- oder Vertraulichkeitsproblemen führen, da Daten nur als "zu löschen" markiert, aber nicht tatsächlich gelöscht werden.
- Organisationsspezifische Sicherheitsrichtlinien und ihre Anwendung bei der elektronischen Archivierung:
  Bei der Konzeption des Archivsystems sind üblicherweise diverse Sicherheitsmaßnahmen vorgesehen worden, die von den einzelnen Benutzern des Archivsystems umgesetzt werden müssen. Dies kann z. B. die Art der Kennzeichnung der Archivmedien oder auch den Umgang mit als vertraulich oder anderweitig klassifizierten Informationen betreffen. Alle Benutzer müssen auf diese organisationsspezifischen Sicherheitsrichtlinien hingewiesen werden.

Die Schulung der Mitarbeiter ist zu dokumentieren.

Prüffragen:

- Werden Benutzer des Archivsystems bezüglich der Nutzung des Systems geschult?
- Wird die Schulung der Benutzer dokumentiert?

# M 3.36 Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 3.37 Schulung der Administratoren eines Apache-Webservers

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 3.38 Administratorenschulung für Router und Switches

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Für den sicheren Betrieb von Routern und Switches ist es wichtig, dass alle Arbeiten durch Personal durchgeführt werden, das in der Lage ist, alle gebotenen Funktionen und Sicherheitsmerkmale optimal zu nutzen. Daher ist es unerlässlich, dass die Administratoren entsprechend geschult werden.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb von Routern und Switches notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte zum gewählten Produkt. In dieser Maßnahme werden Anforderungen an Schulungen beschrieben, die Administratoren in die Lage versetzen, Router und Switches in einer typischen Umgebung installieren und betreiben zu können.

In den Schulungen sollten die Grundlagen, Konzepte und Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche vermittelt werden. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.

Auch wenn in einer Gruppe von Administratoren die Aufgaben so verteilt sind, dass jeder Administrator nur einen bestimmten Verantwortungsbereich hat, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern hierfür ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein Budget eingeplant werden und ein Schulungsplan für Administratoren erstellt werden. Die Inhalte einer Schulung sollten die folgenden Punkte umfassen:

- Grundlagen
  - ISO/OSI Schichten Modell
  - Netztopographien / -topologien und Übertragungstechniken
  - Verkabelung
  - Aktive Netzkomponenten
  - Grundlagen von IP und der damit zusammenhängenden Protokolle (IP-Adressierung, Subnetting, IP, ICMP, TCP, UDP)
  - Überblick über Hersteller und Produkte
- Switching
  - Funktionsweise eines Switches
  - "Cut Through" und "Store and Forward"
  - Transparent Bridging Funktion (IEEE 802.1d)
  - Spanning Tree Algorithmus (IEEE 802.1d)
  - VLAN (VLAN Typen, Tagging, IEEE 802.1q)

- Routing
  - Funktionsweise eines Routers
  - Statisches und dynamisches Routing
  - Dynamische Routing-Protokolle (RIPv1, RIPv2, OSPFv2, BGPv4, IGRP, EIGRP)
- WAN-Anbindung
  - Grundlagen der WAN-Technologien und Protokolle
  - Vermittlungsarten (Fest-, Wählverbindung)
  - Virtuelle Private Netze (VPN)
  - Weitverkehrsverbindungen (xDSL, ISDN)
  - WAN-Protokolle (PPP, Frame Relay)
- Einrichtung
  - Zusammenbau und Verkabelung
  - Einrichtung und Konfiguration von Routern und Switches (Schwerpunkt: Betriebssystem)
- Betrieb
  - Management der Geräte, Werkzeuge
  - Integration in Netzmanagementsysteme (NMS)
  - Protokollierung (syslog)
  - Sicherung und Verwaltung von Konfigurationsdateien
- Fehlerbehebung
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge
  - Teststrategien zur Fehlersuche
  - Anforderungen an sichere Netzinstallationen
- Informationssicherheit
  - Grundlagen der Informationssicherheit sowie für Router und Switches relevante Sicherheitsaspekte
  - Authentisierung, Autorisierung
  - Kryptoverfahren und Anwendungen
  - Angriffsszenarien (Denial of Service Attacken, ARP-Spoofing, IP-Spoofing)
  - Gefahrenquelle "Default-Einstellungen"
  - Vorsorgemaßnahmen, Reaktion und Analyse
  - Incident Handling

Prüffragen:

- Werden regelmäßige Schulungen der zuständigen Administratoren durchgeführt?
- Werden in den Schulungen die Grundlagen, Konzepte und Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung, Sicherheit und Fehlersuche vermittelt?
- Werden in den Schulungen die herstellerspezifischen Aspekte zu den gewählten Produkten berücksichtigt?
- Verfügen alle Administratoren über ein allgemeines Grundwissen im Bereich Router und Switches?
- Existieren Schulungspläne für die Administratoren?

# M 3.39 Einführung in die zSeries-Plattform

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die zSeries-Architektur ist der Nachfolger der 1964 eingeführten S/360-Architektur und wird bei heutigen Mainframe-Installationen häufig eingesetzt. Die zSeries-Systeme (als Teil von IBMs eServer-Familie) können sowohl für Stapelverarbeitungen und Transaktionen als auch für E-Business-Anwendungen eingesetzt werden.

Zum Betrieb der zSeries-Plattform stehen die Betriebssysteme OS/390 (31 Bit-Architektur) und z/OS (64 Bit-Architektur) zur Verfügung. Da das z/OS-Betriebssystem als Nachfolger von OS/390 gilt, sollte es bei neuen Installationen eingesetzt werden.

Nachfolgende Abschnitte enthalten eine Übersicht über die Komponenten der zSeries-Plattform, sie erheben jedoch keinen Anspruch auf Vollständigkeit. Umfangreiche und detaillierte Informationen sind in der einschlägigen Literatur des Herstellers IBM zu finden (siehe Literaturhinweise am Ende der Maßnahmenbeschreibung).

Das z/OS-Betriebssystem ist in der Maßnahme M 3.40 *Einführung in das z/OS-Betriebssystem* beschrieben, das Betriebssystem Linux für z/OS in der Maßnahme M 3.41 *Einführung in Linux und z/VM für zSeries-Systeme*.

### Historie

Die Basis für die zSeries-Architektur entstand im Jahr 1964, als IBM die S/360-Architektur entwickelte und einführte. Von Anfang an war es Ziel der Architektur, dass Maschinencode auf allen damaligen und zukünftigen Modellen ohne wesentliche Modifikationen lauffähig sein sollte.

Im Laufe der Zeit erweiterte IBM sukzessiv die S/360-Architektur, wobei sich die Bezeichnung mehrfach änderte, erst zu *S/370*, danach zu *S/390* und jetzt zur aktuellen *zSeries*. Die wesentlichen Grundlagen der Architektur (z. B. Maschinencode, Register und Adressierung oder auch die Festlegung der Relation zwischen Bit und Byte) wurden jedoch immer beibehalten und gelten heute noch.

### Mainframe-Architektur

IBMs Dokumentation *z/Architecture Principles of Operations* teilt das zSeries-System in die Bestandteile

- Main Storage,
- einem oder mehreren Central Processing Units (CPUs),
- Operator Facilities,
- einem Channel Subsystem und
- I/O Devices

auf. Die *I/O Devices* hängen an sogenannten *Control Units* (CU), die wiederum am *Channel Subsystem* hängen.

Die S/390-Architektur entspricht - mit Ausnahme der neuen zSeries-Funktionen - im wesentlichen der zSeries-Architektur. Im Folgenden werden einige Aspekte der z/Architektur dargestellt:

*EBCDIC Code*

zSeries-Systeme verwenden beim Abspeichern den sogenannten *EBCDIC*-Code (*Extended binary coded decimal interchange code*) mit einer Länge von acht Bit, im Gegensatz zu dem bei anderen Rechner-Architekturen verwendeten *ASCII*-Code (sieben Bit). Kommunizieren Rechner miteinander, die unterschiedliche Formate einsetzen, sind Konvertierungen der Codes erforderlich.

*Register*

Ein zSeries-Rechner arbeitet mit verschiedenen Registern von 64 Bit Länge (z. B. Kontrollregister oder Mehrzweckregister). Der *Instruction Operation Code* (IOC) bestimmt, welches Register verwendet wird.

Beim S/390-Rechner sind die Register 32 Bit lang.

*Programmverzweigung (Linkage Convention)*

Die zSeries-Architektur verwendet beim Aufruf eines Unterprogramms mehrere Mehrzweckregister. Die Verwendung bestimmter Register ist in der Literatur auch als *Linkage Convention* bekannt.

Alternativ ist die Benutzung eines *Linkage Stacks* möglich, wofür andere Assembler-Instruktionen zur Verfügung stehen.

*Speicherschutz*

Ein zusätzlicher Speicherschutz stellt bei der zSeries-Architektur sicher, dass Fehler beim Speicherzugriff weitgehend vermieden werden. Die Hardware teilt den Hauptspeicher in 4 kB große Blöcke auf und vergibt pro Block einen Speicherschutzschlüssel, der bei der späteren Verarbeitung überprüft wird.

Diese Art des Speicherschutzes stellt eine der Stärken des Betriebssystems dar, da Überschreiben fremden Speichers im normalen Problem-Modus weitgehend ausgeschlossen ist.

*Ein-/Ausgabe*

Der zSeries-Ein-/Ausgabe-Verkehr wird durch ein *Channel Subsystem* gesteuert. Bis zu 65536 Ein-/Ausgabe-Einheiten können über Steuereinheiten (*Control Units*) an das *Channel Subsystem* angeschlossen und mittels *Channel Paths* mit diesem verbunden werden.

Die einzelnen Anschlüsse werden vom *Channel Subsystem* als logische Verbindungen (*Subchannels*) geführt. Sie sind über *Channel Paths* mit dem *Channel Subsystem* verbunden.

*Operator Facilities*

Mit dieser Funktion kann der Systemadministrator, ähnlich der BIOS-Kommunikation beim PC, mit dem zSeries-System in Verbindung treten und Systemanpassungen vornehmen.

Zur Kommunikation dient ein herkömmlicher PC, der an das *Service Element* angeschlossen ist und als *Management Console* bezeichnet wird (siehe auch Abschnitt *Ein-/Ausgabe - zSeries-Mainframe-Konsolen*). Diese Konsole dient ausschließlich der Nutzung durch den Systemadministrator bzw. das Wartungspersonal des Herstellers.

*Betriebssystem-Unterstützung*

Die z/Architektur unterstützt alle drei existierenden Hardware-Adressierungsbereiche, 24 Bit-, 31 Bit- und 64 Bit-Adressierung. Betriebssysteme und Middleware-Produkte wurden für die Möglichkeit der erweiterten Adressierung angepasst. Viele Beschränkungen, z. B. die 2 GB-Grenze bei S/390-Systemen oder jetzt weitgehend unnötige Funktionen, wie z. B. die Verlagerung von Seiten des Hauptspeichers in den erweiterten Speicher (*Expanded Storage*), fallen damit weg. Dadurch kann der Durchsatz des Systems in vielen Fällen erhöht werden. *Expanded Storage* wird jedoch weiterhin bei S/390-(31-Bit)-Anwendungen und z/VM unterstützt.

Anmerkung: Das S/390-System ist zwar in Bezug auf die Hardware ein 32 Bit-System, die Software darauf läuft jedoch mit 31 Bit, da das erste Bit zur Umschaltung zwischen 24 und 31 Bit-Modus benötigt wird.

*Unterschiede der S/390-Architektur zur zSeries-Architektur*

Der Hauptunterschied zwischen S/390- und zSeries-Systemen ist die erweiterte Adressierbarkeit. Während die S/390-Architektur nur die 31 Bit- Adressierung unterstützt, wurden in den Rechnern der zSeriesfast alle Register auf 64 Bit erweitert. Ein Umschalten zwischen den beiden Modi ist jederzeit möglich.

Die neuesten zSeries-Systeme sind noch immer kompatibel zu früher entwickelten 31 Bit-Programmen, es laufen sogar noch 24 Bit-Programme.

**Hardware**

Mainframe-Hardware ist in den verschiedensten Varianten verfügbar. Modelle und Ausstattung lassen sich flexibel zusammenstellen, periphere Einheiten können weitgehend beliebig daran angeschlossen werden. Eine vollständige Darstellung kann an dieser Stelle nicht gegeben werden.

Nachfolgend eine kurze Übersicht über die wichtigsten Merkmale:

*Modelle*

Zur Zeit sind die Typen S/390 (G5, G6 und Multiprise) aus der S/390-Architektur verfügbar, aus der zSeries-Architektur die Typen z800-Server, z900- Server und z990-Server (Stand Ende 2003).

*Prozessoren*

Die Systeme sind auf bis zu 32 Prozessoren aufrüstbar, wobei diese bei der zSeries-Architektur dynamisch (d. h. während des Betriebs) hinzugefügt werden können.

*Hauptspeicher*

Je nach Typ können zwischen 1 GB bis max. 256 GB Hauptspeicher verwendet werden.

*Kanäle*

Verfügbar sind 256 bis max. 512 Kanäle, wobei unterschiedliche Kanaltypen zusammen betrieben werden können (*Escon*, *Ficon*). Je nach Konstellation gibt es Einschränkungen.

*Logical Partitioning*

Ein zSeries-System lässt sich in bis zu 15, bei z990-Servern in bis zu 30, sogenannte logische Partitionen (*Logical Partition, LPAR*) aufteilen. Dies wird durch das interne PR/SM-Feature (teils Hardware, teils Microcode im *Licensed Internal Code*) unterstützt. Jede einzelne Partition verhält sich dabei wie ein separates System. Auf den *LPARs* lassen sich unterschiedliche Betriebssysteme installieren, so dass der Einsatz von Linux (für zSeries) parallel mit dem z/OS-Betriebssystem auf dem gleichen Rechner möglich ist.

*Komponenten*

- Multichip Module (MCM)
  Die wesentlichen Komponenten des Rechners sind in sogenannten *Multichip Modules* zusammengepackt und auf einem Glaskeramikträger aufgebracht. Ein MCM beinhaltet *Processor Unit Chips* (PUs), Chips für den L2-Cache und dessen Ansteuerung sowie die Ein-/Ausgabe-Steuerung. Die Verbindung aller Komponenten auf dem Träger erfolgt über waagerechte und senkrechte Leitungsverbindungen, die über Kontakte mit der Platine verbunden sind.
- Thermo Conduction Module (TCM)
  Die in einem MCM entstehende Wärme leitet ein auf dem MCM sitzender Kühler (TCM) ab.
- SMP
  Das MCM stellt einen in sich symmetrischen Multiprozessor (SMP) dar.
- Logical Channel Subsystem (LCSS)
  Das LCSS ist eine Erweiterung des früher schon verfügbaren *Channel Subsystems* (CSS), das es erlaubt, von allen *Processor Units* aus bis zu 512 Kanäle anzusprechen.
- HiperSockets
  Die schnelle TCP/IP-basierende Verbindung zwischen LPARs und *Virtual Servers* (Linux) stellt eine Art TCP/IP-Netz innerhalb des Servers dar.
- Intelligent Resource Director (IRD)
  Der *Intelligent Resource Director* unterstützt den *Workload Manager* (WLM) und besteht aus den wesentlichen Teilen

  - LPAR CPU Management,
  - Dynamic Channel Path Management (DCM) und
  - Channel Subsystem Priority Queueing (CSSPQ).

  Bei Problemen im System kann der *Workload Manager* dynamisch über den IRD veranlassen, dass LPAR-Gewichtungen verändert, Kanal-Pfade umgehängt oder im *Channel Subsystem* I/O-Prioritäten verändert werden.

*Prozessoren und Einsatz*

Die Prozessoren sitzen auf MCMs und bestehen im wesentlichen aus den folgenden Typen:

- Processor Units (Mikroprozessor-Chips),

  - CPU (CP),
  - Ein-/Ausgabe-Prozessoren,
  - Reserve-PUs,
- Level 2 Cache Chips,
- System-Assist-Prozessoren (*SAPs,* Ausführung des Channel Subsystems),
- Storage Control Chips,
- Memory Bus Adapter Chips und

- Clock Chips.

Die Anzahl der standardmäßig gelieferten CPs und SAPs ist abhängig von dem jeweils bestellten Modell. Die Anzahl der Reserve-PUs ist abhängig davon, wie viele PUs insgesamt vorhanden und noch nicht mit Funktionen belegt sind.

Reserve-PUs lassen sich leicht über den *Licensed Internal Code Configuration Control (LICCC)* via *Host Management Console (HMC)* den folgenden Funktionen zuordnen:

- Central Processor (CP)
- Integrated Facility for Linux (IFL)
- Internal Coupling Facility (ICF)
- System Assist Processor (SAP)

*Kryptographische Komponenten*

Die zSeries bietet verschiedene kryptographische Hardware-Komponenten an, die die Daten-Ver- und -Entschlüsselung unterstützen.

- Cryptographic Coprocessor Facility (CCF)
  Dieser Coprozessor ist auf dem Prozessormodul der 9672- und zSeries-Hardware angeordnet (außer z990). Es sind ein oder zwei CCFs je Modul erhältlich. Im CCF können die Schlüssel *DES Master Key, Key Management Master Key (PKA KMMK*) und *Signature Master Key (PKA SMK)* gespeichert werden.
- Peripheral Component Interconnect Crypto Coprocessor (PCI-CC)
  zSeries-Systeme unterstützen die PCI-CC-Karte, die zusätzlich eingesetzt werden kann, um die Funktionalitäten und Performance des CCF zu unterstützen.
- Peripheral Component Interconnect Crypto Accelerator (PCI-CA)
  Diese neue Krypto-Karte wurde speziell entwickelt, um die SSL-Ver- und -Entschlüsselung auf zSeries-Systemen zu beschleunigen.
- z990 PCIX-CC Enhanced Cryptographic Functionality
  Der PCIX Cryptographic Coprocesser ersetzt die CCF- und PCI-CC- Krypto-Hardware im z990-Server.

**Ein-/Ausgabe**

Die Ein- oder Ausgabe von Daten läuft bei der zSeries-Plattform über ein Netz von Verbindungen, die im folgenden kurz beschrieben werden:

*Channel Subsystem (CSS)*

Das *Channel Subsystem* ist eine Einheit (aus Hard- und Software), die für die Verarbeitung der Daten von und zu den Ein-/Ausgabe-Einheiten zuständig ist und die CPU entlastet. Es besteht aus Kanälen (*Channel Paths*), die wiederum in Unterkanäle (*Subchannels*) unterteilt sind. Die Unterkanäle führen die Kanalprogramme (*Channel programs*) aus. Bei dem zSeries-System z990 wurde das CSS zum *Logical Channel Subsystem* (LCSS) erweitert und unterstützt jetzt mehr als 15 CPUs.

*Escon / MIF*

*Escon*-Kanäle sind serielle Kanäle, die als Folgeentwicklung der alten Parallel-Channel-Entwicklung gelten können. Das *Multiple Image Facility* (EMIF bis z/900 oder MIF ab z/990) unterstützt den parallelen Zugriff von Ressourcen über LPAR-Grenzen hinweg (resource sharing). *Escon*-Kanäle werden über sogenannte *Directors* den Einheiten zugeordnet.

*Ficon*

*Ficon*-Express-Kanäle (Fibre channels) können parallel zu *Escon*-Kanälen betrieben werden. Bei der z990 können bis zu 120 solcher *Ficon*-Kanäle angeschlossen werden. Die Übertragungsrate reicht bis zu 100 MB pro Sekunde. Auch *Ficon*-Kanäle werden über *Directors* den Einheiten zugeordnet.

*Integrated Cluster Bus (ICB)*

ICBs werden unter anderem im Rahmen der Sysplex-Kommunikation als *Coupling Link* für Highspeed-Verbindungen zwischen Systemen benutzt.

*OSA/Express*

*OSA/Express* bietet einen zSeries-Kanalanschluss für Ethernet-Geräte wie z. B. Switches oder Router.

*Channel To Channel (CTC)*

*Channel-To-Channel*-Verbindungen gestatten schnelle Verbindungen zwischen zwei zSeries-Rechnern und werden von diversen Software-Produkten, wie z. B. JES3 und VTAM, unterstützt.

*zSeries-Mainframe-Konsolen*

Die *Host Management Konsole(HMC)* erlaubt die folgenden Aktionen:

- Setzen von Datum und Zeit,
- Konfigurieren von LPARs und Systemen,
- Reset von Subsystemen,
- Boot Manager (Initial Program Load - IPL - einer LPAR),
- Laden des Microprogramms (Initial Microcode Load - IML - eines zSeries Systems),
- Eingriff bei Fehlerbedingungen,
- Ersatz-MVS-Konsole und
- Fehlerkorrekturen seitens des Herstellers (Microcode-Patches).

Es können zwei Konsolen (Primary und Alternate) angeschlossen werden. Sie sind für das komplette System zuständig (alle LPARs) und nicht nur für ein spezielles Betriebssystem. Der Zugriff auf diese Konsolen muss aus Sicherheitsgründen gut geschützt sein.

Die *z/OS-System-Konsolen* (MVS) sind für die Steuerung und Kontrolle eines z/OS-Betriebssystems zuständig und lassen sich für verschiedene Zwecke konfigurieren, z. B. als Konsole für alle Nachrichten aus dem Bandbereich (Tape-Pool). Es sind mehrere MVS-Konsolen pro z/OS möglich, wovon nur eine die Master-Konsole sein kann. Im Fehlerfall schaltet diese Konsole auf die nächste verfügbare um. Der Zugriff auf die MVS-Konsolen (speziell auf die Master-Konsole) muss aus Sicherheitsgründen gut geschützt sein.

*Remote Support Facility (RSF)*

zSeries-Systeme sind meist durch eine Remote-Konsole mit dem Hersteller verbunden. Diese Funktion meldet erkannte Hard- und Software-Probleme automatisch weiter, so dass Fehler oft behoben werden können, bevor der Anwender einen Fehler selbst erkennt. Prinzipiell unterstützt diese Verbindung auch die Installation von Patches durch den Hersteller, dies muss jedoch vorher vereinbart und die Remote-Access-Verbindung entsprechend geschützt werden.

*Parallel-Sysplex-Konzept*

Sind die Anforderungen von einem System (einer LPAR) nicht mehr zu bewältigen, können mehrere LPARs zu einem logischen Verbund, dem *Parallel Sysplex* zusammengefasst werden. Dieser stellt sich nach außen als eine Einheit dar.

Der *Parallel Sysplex* ist eine Zusammenarbeit von bis zu 32 z/OS-Systemen, dies entspricht maximal 512 Prozessoren in einem Rechnerverbund. Innerhalb dieses Verbundes können Lasten auf den Rechnern verteilt werden. Treten an einer Maschine Probleme auf, lässt sich diese aus dem Verbund lösen. Die Last wird von den im *Sysplex* verbleibenden Maschinen übernommen.

- Coupling Facility (CF)
  Die *Coupling Facility* (CF) hat die Aufgabe, die Arbeitslast der Systeme zu steuern und Informationen für alle Systeme zur Verfügung zu stellen. Sie ist für die flexible Lastverteilung und die Skalierung zuständig. Die CF übernimmt Aufgaben des *Locking*, *Caching* und *Queuing*. Sie wird über den CCFC (*Coupling Facility Control Code*) gesteuert.
- Sysplex Timer
  Damit die einzelnen Systeme innerhalb des *Sysplex* zusammenarbeiten können, ist der *Sysplex Timer* nötig. Er übernimmt die Aufgabe, allen im *Sysplex* befindlichen Systemen eine synchrone Tageszeit zu liefern.
- Work Load Manager (WLM)
  Der *Work Load Manager* ist Teil einer jeden Betriebssystem-Instanz und übernimmt in Verbindung mit der *Coupling Facility* einen wichtigen Teil der Steuerung des *Sysplex Clusters*. Ein Teil des WLM ist der *System Resource Manager* (SRM). Dieser übernimmt die Überwachung der angeschlossenen Systeme. Überwacht werden durch den SRM z. B. Prozessorlast, Plattenauslastung, Hauptspeichernutzung und andere Parameter. Die Informationen werden dazu genutzt, die Last auf die im *Sysplex* angeschlossenen Systeme zu verteilen (siehe Abschnitt zum Thema *Intelligent Resource Director*).
- Cloning
  Alle Systeme eines *Sysplex Clusters* werden auf Basis eines Plattensatzes erstellt. Die lokale Anpassung erfolgt im Normalfall über Variablen der Systemkonfiguration.

**Peripherie**

*Platten*

Im Gegensatz zu anderen Betriebssystemen ist der Plattenbereich eines z/OS-Betriebssystems in sogenannte *Volumes* aufgeteilt. Ein *Volume* umfasst bei der Emulation einer Platte vom Typ 3390 Mod. 3 einen Speicherbereich von ca. 2,7 GB und ist in Zylinder und Spuren aufgeteilt.

Die *Volumes* sind an Steuereinheiten angeschlossen. Zur Steigerung der Performance und Betriebssicherheit ist ein paralleler Anschluss an verschiedene Steuereinheiten möglich. Diese werden bestimmten Aufgaben zugeordnet (z. B. JES-Spool-Datei oder System-Residenz) und lassen sich über *Subchannel*-Adressen ansprechen.

*Band*

Das z/OS-Betriebssystem unterstützt verschiedene Bandeinheiten, von einzelnen Stationen bis zu Robotersystemen, in denen die Bänder automatisch verwaltet und zur Verfügung gestellt werden. Darüber hinaus gibt es auch virtuelle Band-Systeme (z. B. *VTS* von IBM oder *VSM* von StorageTek), die Da-

teien zuerst auf integrierten Festplatten zwischenspeichern. Danach werden diese Dateien sehr effektiv auf Bänder in diesen Einheiten geschrieben (Komprimierung und Ausnutzung der gesamten Bandlänge).

VTS oder VSM werden vom z/OS-Betriebssystem als Bandeinheit 3490 verarbeitet, d. h. aus der Sicht des Betriebssystems handelt es sich um ein normales Band.

*Drucker*

Drucker werden von z/OS-Betriebssystemen sowohl direkt am Kanal als auch als Netzwerkdrucker im SNA- oder TCP/IP-Netz unterstützt. Bei entsprechend großen Druckvolumina, z. B. in Druckzentren, erledigen z/OS-Systeme auch reine Druckaufgaben.

*Terminalfamilie 327x*

Klassische 3270-Terminals an den entsprechenden Steuereinheiten sind heute praktisch nicht mehr in Betrieb. 3270-basierte Terminals haben als PC-Terminalemulation jedoch einen hohen Stellenwert und befinden sich noch recht häufig im Einsatz (bekannt als "grüner Schirm"). Sie basieren auf dem TN3270-Protokoll und lassen sich so betreiben, wie die 327x-Terminals aus früheren Jahren (von Modell 2 bis Modell 5 in verschiedenen Bildschirm-Formaten).

*SNA-Komponenten (Systems Network Architecture)*

SNA ist eine hierarchisch aufgebaute Netztechnologie mit vordefinierten Verbindungen. Die Knoten im Netz sind in der Regel als Hardware-Komponenten ausgeführt und werden als *Physical Units* (PUs) bezeichnet. Die Endpunkte im Netz sind entweder Software-Schnittstellen zu einer Applikation (*Application Control Block*, ACB) oder ein Terminal bzw. Terminal-Emulator oder Drucker. Daneben gibt es seit längerer Zeit die APPN-Technologie (*Advanced Peer to Peer Network*), die sich von der hierarchischen Form deutlich unterscheidet.

SNA kommt heute als alleiniges Netzprotokoll nur noch selten zum Einsatz. SNA-Netzinstallationen sind vielfach abgelöst oder durch ein TCP/IP-Netz ergänzt, so dass die Anzahl der im Betrieb befindlichen SNA-Hardware-Komponenten stark rückläufig ist.

*SNA-Topologie*

Das hierarchische SNA-Netz war in der Vergangenheit so aufgebaut, dass unter einem VTAM ein Front-End-Prozessor 3745/46 angeschlossen war. Angeschlossen an diesen waren die *Control Units*, an denen letztlich die Endgeräte (Terminals, Drucker oder Applikationen) betrieben wurden. Diese Konstellation ist heute zwar immer noch im Einsatz, Front-End Prozessoren und auch *Control Units* werden von IBM jedoch nicht mehr vertrieben (aber noch unterstützt). Die Anbindung an TCP/IP Netze erfolgt heute meistens über die Software-Funktion *Enterprise Extender*. SNA in der heutigen Ausprägung wird hauptsächlich noch im Rechenzentrum benutzt, um SNA-basierende Applikationen wie z. B. TSO (*Time Sharing Option*) anzubinden, während das Netzwerk von TCP/IP abgedeckt wird.

- Physical Units (PUs)
  *Physical Units* stellen physische Knoten im SNA-Netz dar. An diesen können weitere Einheiten hängen. Zu den PUs gehören z. B. die oben erwähnten Front-End-Prozessoren 3745/46.

Darüber hinaus existieren Komponenten, die die früher vorhandenen *Control Units* (3174) emulieren und deren Funktion wahrnehmen. VTAM im z/OS-Betriebssystem stellt ebenfalls eine *Physical Unit* dar. Aus historischen Gründen werden selbst neuere Funktionen (wie z. B. APPN) bei VTAM Displays immer noch als *Physical Units* dargestellt, obwohl diese Bezeichnung hierbei eigentlich ohne Bedeutung ist.

- Logical Units (LUs)
  Eine *Logical Unit* stellt sich entweder als Schnittstelle zu einer Applikation, als ein Terminal (oder Terminal-Emulator auf einem PC) oder als ein Drucker dar.

Weitere Informationen zu SNA finden sich in der Maßnahme M 3.40 *Einführung in das z/OS-Betriebssystem* im Abschnitt *Communications Server*.

*Support Elements (SEs)*

Jede zSeries-Hardware besitzt zwei *Support Elements* (S/390-G5 Modelle haben nur ein SE), die eine Konfiguration und Kontrolle des Systems erlauben. SEs sind über ein schnelles internes Ethernet-Netz untereinander und mit den Prozessoren verbunden (ein *Support Element* ist ein IBM Laptop PC). Sie erlauben die Systemkommunikation im Rahmen der *Operator Facilities*.

**Firmware**

*Licensed Internal Code (LIC)*

Zwischen der Hard- und der Software existiert auf einer weiteren Ebene der Microcode (*Licensed Internal Code*). Für den LIC gibt es bei PCs keine direkte Entsprechung, am ehesten ist er mit dem BIOS bei einem PC vergleichbar (siehe Abschnitt zum Thema *IML*).

*Processor Resource/System Manager (PR/SM)*

Der *Processor Resource/System Manager* ist eine LIC-Funktion und erlaubt die logische Aufteilung der physischen zSeries-Hardware in verschiedene Teile, *Logical Partitions (LPARs)* genannt. Jeder logische Rechner beinhaltet sein eigenes Betriebssystem, wobei verschiedene Betriebssysteme parallel eingesetzt werden können (also zum Beispiel z/OS, OS/390, TPF, Linux oder VSE/ESA auf einer Hardware). Die gemeinsame Nutzung aller Ressourcen wird von PR/SM kontrolliert.

*Initial Microcode Load (IML)*

DerIMList ein Vorgang, der den LIC in einen nicht zugreifbaren Speicherbereich lädt. Der IML bezieht sich immer auf die gesamte Maschine, d. h. mit IML werden alle LPARs auf der Maschine neu initialisiert (und damit auch die Betriebssysteme gestoppt). IML ist ein Teil der *Operator Facilities* und kann über die HMC-Konsole aktiviert werden. Der Aufruf des IML muss entsprechend geschützt werden.

*Hardware Configuration Definition (HCD)*

Zur Anpassung der Software-Konfiguration an die Hardware wird eine Datei (*I/O Definition File*, IODF) erstellt, in der die logischen *Subchannels* auf den physischen *Channel Pathid* abgebildet werden.

Dem Bediener stehen dazu verschiedene Tools zur Verfügung. Auf diese Tools sollte nur autorisiertes Personal Zugriff haben.

**Betriebssystem**

Für die S/390- und der zSeries-Architektur sind verschiedene Betriebssysteme verfügbar (Stand Januar 2004):

S/390-Architektur (24 und 31 Bit):

- OS/390 Version 2, Release 10
- Linux on S/390
- z/VM Version 3, Release 1
- z/VM Version 4, Release 2 bis 4
- VSE/ESA Version 2, Release 5, 6, 7
- TPF Version 4, Release 1 (nur ESA-Mode)

z/Series-Architektur (64 Bit):

- OS/390 Version 2, Release 10
- z/OS Version 1, Release 2 bis 5
- Linux on zSeries
- z/VM Version 3, Release 1
- z/VM Version 4, Release 2 bis 4

Weitergehende Informationen über die Betriebssysteme OS/390 und z/OS sind in der Maßnahme M 3.40 *Einführung in das z/OS-Betriebssystem* zu finden.

**Betrieb**

*IML*

Der Start eines zSeries-Systems beginnt mit dem *Initial Microcode Load* (IML). Er wird entweder über die HMC-Konsole manuell initiiert oder mittels entsprechender Definitionen automatisch angestoßen. Der IML-Vorgang lädt den Microcode und stellt die Systeminfrastruktur bereit (alle LPARs verfügbar, kein Betriebssystem geladen). Während des IML-Vorgangs wählt der Bediener die gewünschte I/O-Konfiguration aus.

*IPL*

Das z/OS-Betriebssystem wird durch den *Initial Program Load* (IPL) von der *Host Management Console (HMC)* aus aktiviert. Dabei muss mindestens die IPL-Ladeadresse und der IPL-Parameterstring (Ladeadresse der IOCDS-Datei) angegeben werden. Nach der NIP-Phase (*Nucleus InitializationProcess*) kommuniziert das z/OS-System mit dem Bediener über die MVS-Master-Konsole. Die weiteren Schritte hängen von den Definitionen des Betriebssystems ab. Entweder wird das System manuell aktiviert (Ausnahmefall) oder automatisch.

*Operation*

Zu den Betriebsaufgaben gehört das Starten und Stoppen der Tasks und Jobs, Aktivieren von Ressourcen, Beantworten von Systemanfragen (*Replies*) und Bereitstellen von Bandstationen (wenn nötig).

*Monitoring*

Das System kommuniziert mit dem Operator über Nachrichten und *Replies*, die an der MVS-Konsole ausgegeben bzw. eingegeben werden. Eine laufende Kontrolle der Nachrichten ist daher notwendig. Dies kann entweder manuell

(relativ aufwendig) oder besser über Automatismen erfolgen (separate Programme). Gleiches gilt für die Kontrolle der Stapelverarbeitung.

**Literaturhinweise**

Für das zSeries-System existiert eine Vielzahl an Literatur und Dokumentationen. Die folgende Aufstellung beschränkt sich auf die wichtigsten und für die Sicherheit des zSeries-Systems besonders relevanten Quellen der Firma IBM. Die Aufstellung ist jedoch keineswegs vollständig.

***Redbooks***

| **Formnummer** | **Titel** |
|---|---|
| SG24-5975-nn | IBM @server zSeries 900 Technical Guide |
| SG24-6863-nn | IBM @server zSeries 990 Technical Introduction |
| SG24-6851-nn | z/OS Version 1 Release 3 and 4 Implementation |
| SG24-6540-nn | Putting the latest z/OS Security Features to work |
| SG24-7023-nn | Linux on IBM eServer zSeries and S/390: Best Practices |
| SG24-6981-nn | ABCs of z/OS System Programming Volume 1 (Introduction to z/OS and storage concepts, TSO/E, ISPF, JCL, SDSF, MVS delivery and installation) |
| SG24-6982-nn | ABCs of z/OS System Programming Volume 2 (z/OS implementation and daily maintenance, defining subsystems, JES2 and JES3, LPA, LNKLST, authorized libraries, catalogs) |
| SG24-5653-nn | ABCs of System Programming Volume 3 (Introduction to DFSMS, storage management) |
| SG24-5654-nn | ABCs of System Programming Volume 4 *(Communication Server, TCP/IP, and VTAM )* |
| SG24-5655-nn | ABCs of System Programming Volume 5 (Base and Parallel Sysplex, system logger, global resource serialization, z/OS system operations, automatic restart management, hardware management console, performance) |
| SG24-6989-nn | ABCs of z/OS System Programming Volume 9 *(z/OS UNIX System Services)* |
| SG24-6990-nn | ABCs of z/OS System Programming Volume 10 (Introduction to z/Architecture, zSeries processor design, zSeries connectivity, LPAR concepts, and HCD) |

| Formnummer | Titel |
|---|---|
| TIPS0382 | z/OS V1R3 and V1R5 Technical Guide |
| SG24-7035-nn | Unix System Services z/OS V1R4 Implementation |
| SG24-6968-nn | Implementing PKI Services on z/OS |
| SG24-5637-nn | OS/390 Parallel Sysplex Configuration Volume 1 |
| SG24-5638-nn | OS/390 Parallel Sysplex Configuration Volume 2 |
| SG24-5639-nn | OS/390 Parallel Sysplex Configuration Volume 3 |

***IBM Dokumentation***

| Formnummer | Titel |
|---|---|
| SA22-7832-nn | z/Architecture Principles of Operation |
| SA22-7591-nn | z/OS Initialization and Tuning Guide |
| SA22-7592-nn | z/OS Initialization and Tuning Reference |
| SA22-7683-nn | Security Server RACF Security Administrator's Guide |
| SA22-7681-nn | Security Server RACF System Programmer's Guide |
| SA22-7682-nn | Security Server RACF Macros and Interfaces |
| SA22-7684-nn | Security Server RACF Auditor's Guide |
| SA22-7801-nn | z/OS Unix System Services Users Guide |
| GA22-7800-nn | z/OS Unix System Services Planning |
| SA22-7670-nn | z/OS SDSF Operation and Customization |
| SA22-7532-nn | z/OS JES2 Initialization and Tuning Guide |
| SA22-7533-nn | z/OS JES2 Initialization and Tuning Reference |
| SA22-7549-nn | z/OS JES3 Initialization and Tuning Guide |
| SA22-7550-nn | z/OS JES3 Initialization and Tuning Reference |
| SA22-7783-nn | z/OS TSO/E Customization |
| SA22-7692-nn | z/OS MVS Planning: Workload Management |
| SA22-7597-nn | z/OS MVS JCL Reference |
| SA22-7593-nn | z/OS MVS Installation Exits |
| SC34-4826-nn | HTTP Server Planning, Installing and Using |

| Formnummer | Titel |
|---|---|
| SC31-8775-nn | z/OS CS : IP Configuration Guide |
| SC31-8776-nn | z/OS CS : IP Configuration Reference |
| SA22-7600-nn | z/OS MVS Planning : Global Resource Serialization |
| SA22-7623-nn | z/OS MVS Recovery and Reconfiguration Guide |
| SA22-7625-nn | z/OS MVS Setting up a Sysplex |
| SA22-7630-nn | z/OS MVS System Management Facilities (SMF) |
| SA22-7642-nn | z/OS MVS Using the Subsystem Interface |
| SC26-7402-nn | z/OS DFSMSdfp Storage Administration Reference |
| SC35-0422-nn | z/OS DFSMShsm Storage Administration Reference |
| SC26-7405-nn | z/OS DFSMSrmm Implementation and Cust. Guide |
| SC26-7414-nn | z/OS DFSMSdfp Utilities |
| SC33-7989-nn | z/OS HCM User's Guide |
| GC35-0033-nn | Device Support Facilities User's Guide and Reference |
| SH19-8163-nn | MVS/DITTO V2 User's Guide and Reference |
| SC33-1701-nn | CICS RACF Security Guide |
| SG24-5363-nn | IMS V6 Security Guide |

# M 3.40 Einführung in das z/OS-Betriebssystem

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

In seinen Grundstrukturen unterscheidet sich z/OS kaum von anderen Betriebssystemen. Sein Aufbau ist eingeteilt in Hardware-nahe Funktionen, Betriebssystemprozesse und Benutzerprozesse. Zwischen dem eigentlichen Betriebssystem (*Base Control Program*) und den Benutzerprozessen existieren eine Reihe von Subsystemen, von denen die bekanntesten das *Job Entry Subsystem* für die Behandlung der Stapelverarbeitung, die *Time Sharing Option* für die Unterstützung des interaktiven Betriebs und die *Unix System Services* für den Unix-kompatiblen Betrieb sind.

Die folgende Beschreibung gilt für die Betriebssysteme OS/390 und z/OS. Zur Vereinfachung wird nur noch z/OS aufgeführt, eventuell vorhandene Unterschiede zu OS/390 werden angesprochen, wo sie existieren.

### Base Control Program (BCP)

Dieser Teil des z/OS-Betriebssystems ist mit dem Unix-Kernel vergleichbar. Hierin sind die wesentlichen Funktionen des Betriebssystems vereint, die dementsprechend im Kernel-Modus laufen.

### Subsysteme

Subsysteme erledigen Aufgaben des Betriebssystems, die nicht im Kernel angesiedelt sind, und laufen in einem separaten Adressraum. Wird ein Subsystem vor dem JES-Start vom MVS-Kernel aktiviert, erfolgt seine Interpretation durch das z/OS selbst (dies erledigt dann der *Master Scheduler*), was mit gewissen Einschränkungen verbunden ist. Ansonsten startet das *Job Entry Subsystem* weitere Subsysteme. Eine Definition in der Konfigurations-Datei des z/OS (PARMLIB) legt fest, wie und in welcher Reihenfolge solche Subsysteme gestartet werden.

Subsysteme werden von IBM und von anderen Software-Herstellern geliefert.

### Job Entry Subsystem (JES2/3)

Ein Stapelverarbeitungsauftrag wird im z/OS *Batch-Job* genannt. Dieser besteht aus einer Reihe von prozeduralen Anweisungen, die gemäß der *Job ControlLanguage* (JCL) aufgebaut sind. Ein Batch-Job kann aus einem oder einer größeren Anzahl von Ablaufschritten (Steps) bestehen. Auch *TSO-User* oder *Started Tasks* werden dem System über JCL bekannt gemacht.

Das *Job Entry Subsystem* (JES) dient zur Verwaltung der Job-Verarbeitung (hauptsächlich Batch-Jobs, aber auch *Started Tasks* und *TSO-User*) und deren Ein- bzw. Ausgaben. Aus historischen Gründen gibt es bis heute zwei unterschiedliche Systeme, JES2 und JES3.

Das JES2/3 wird als *Primary Subsystem* in der Subsystem-Tabelle von z/OS geführt und sollte in einem z/OS-System als erste Task gestartet werden, da erst im Anschluss daran Batch-Jobs gestartet werden können.

Die Verarbeitung der Jobs wird über sogenannte *Initiators* kontrolliert. Dabei werden unter anderem Klassen, Prioritäten und Anzahl von Jobs definiert, die parallel im System arbeiten.

Ein- und Ausgaben werden in einer zentralen Datei gespeichert, die *Spool* genannt wird. Mehrere *LogicalPartitions* (LPARs) lassen sich zu einem JES-Verbund zusammenlegen, bei JES3 *Complex*, bei JES2 *Multiple Access Spool* (MAS) genannt.

Beide JES-Subsysteme beinhalten ähnliche Funktionen. JES3 bietet über den Standard hinaus Funktionen wie *Networking* (zur Automation von Batch-Jobs), *Clustering* (LPAR-ähnlicher Verbund mit Global/Local-Funktion, jedoch nur auf JES-Basis) und *Locate* (Job wird nur gestartet, wenn alle Ressourcen verfügbar sind). Viele Funktionen stehen dem Bediener parallel zu den JES-Subsystemen über andere z/OS-Funktionen zur Verfügung (z. B. über GRS, Sysplex, Job Scheduler Programme).

NJE (*Network Job Entry*) erlaubt das Versenden und Empfangen von Dateien, Batch-Jobs und auch deren Ausgaben zwischen den einzelnen Netzknoten eines Verbundes. So ist es damit z. B. möglich, einen Batch-Job vom System A zum System B zu schicken, dort zu verarbeiten und die Ausgabe dann am System C auszugeben.

**Time Sharing Option (TSO)**

Im Online-Betrieb ermöglicht TSO einen Multi-Tasking- und Multi-User-Betrieb.

Der *TSO Terminal Control Address Space* (TCAS), ein eigener Adressraum, verwaltet dabei den Ablauf. Er initiiert und terminiert die einzelnen Benutzeradressräume (einen pro Benutzer) und verwaltet den Nachrichtenfluss zwischen Terminal und Adressraum.

TSO unterstützt über eine einfache Scriptsprache sogenannte *Command Lists* (*Clists*), häufiger ist jedoch die modernere Interpreter-Sprache REXX im Einsatz. Zu Vereinfachung der Kommunikation steht dem Bediener ein weiteres Software-Paket zur Verfügung, das *Interactive System Productivity Facility* (ISPF). Es erlaubt einen Dialog im *Full Screen Modus*. Neben den Standardfunktionen von ISPF kann der Bediener eigene Dialoge für neue Applikationen entwickeln.

**Communications Server (CS)**

Der *Communications Server* für z/OS beinhaltet die Software-Komponenten, die für die Kommunikation von und zu einem Mainframe nötig sind. TCP/IP-Komponenten, wie z. B. FTP-Server und TN-Server, sind in diesem Paket ebenso enthalten wie SNA-Komponenten.

Der *Communications Server* liefert die folgenden Funktionalitäten:

- Bereitstellung der TCP/IP- und SNA-Dienste
- Lastverteilung auf die Netzkomponenten in einem *Sysplex*-Verbund
- Kontrolle und Steuerung der VPN-Kommunikation
- Implementierung der Sicherheitskomponenten für Applikationen
- Telnet-3270- und Secure-Telnet-3270-Unterstützung, Telnet/SSH zu den *Unix System Services* des z/OS
- Unterstützung von IPv6 für das z/OS-Betriebssystem

*Systems Network Architecture (SNA)*

Ein Knoten im SNA-Netz ist durch eine *Network Addressable Unit* (NAU) definiert. Die Wege zwischen den einzelnen Knoten werden in Form von Routen konfiguriert. Die Weiterentwicklung des statischen SNA-Netzes, *Advanced Peer to Peer Networking* (APPN) genannt, erlaubt den Einsatz dynamischer Netzkonfigurationen ähnlich dem TCP/IP-Netz.

Der *Communications Server* bildet eine Gateway-Funktion zwischen der heute üblichen IP-Netzinfrastruktur und den noch vielfach vorhandenen SNA/APPN-basierenden Komponenten, wie z. B. TSO-, IMS- oder CICS- Anwendungen.

SNA-Kommunikationsbeziehungen werden häufig über das IP-Netz mittels *Enterprise Extender* betrieben. Voraussetzung dafür ist APPN/HPR (*High Performance Routing*).

Klassische SNA-Netze gelten als relativ sicher, da die Netzzugänge komplett definiert sein müssen und das Gesamtnetz somit geschlossen ist. Als weiterführende Sicherheitsmaßnahme kann der *Session Management Exit* (SME) von VTAM eingesetzt werden.

*TCP/IP*

TCP/IP ist unter den *Unix System Services* (USS) im z/OS implementiert. Der TCP/IP-Service unter z/OS bietet ähnliche Funktionen wie die IP-Dienste anderer Unix-Versionen. Über den Telnet TN3270 IP-Service ist der Zugriff auf SNA-basierende Anwendungen (TSO, CICS, IMS usw.) möglich. Unter TCP/IP stehen für z/OS eine ganze Reihe von Applikationen zur Verfügung, wie z. B. ein HTTP-Webserver, Unterstützung für File-Transfer via FTP, E-Mail via SMTP, Network File System (NFS), Domain Name Service (DNS) und weitere Services. TCP/IP unterstützt Verschlüsselung über IPSec, SSH und TLS (SSL).

Durch den Einsatz von Dynamic VIPA (*Virtual IP Address*) wird es ermöglicht, dass beim Ausfall eines Systems innerhalb eines *Parallel SysplexClusters* eine IP-Adresse automatisch von einem Backup-System übernommen werden kann. Unterstützt die Anwendung diese Funktionalität auch, trägt dies wesentlich zur Erhöhung der Verfügbarkeit bei.

Durch Einsatz des *Workload Managers* ist es darüber hinaus möglich, eine Lastverteilung der Netzdienste auf mehrere CPUs innerhalb eines *Sysplex-Verbundes* zu erreichen.

TCP/IP gewinnt immer mehr an Bedeutung, wohingegen die Bedeutung des SNA-Netzes abnimmt (speziell bei der Neuentwicklung von Applikationen).

*Kerberos*

z/OS unterstützt das Authentisierungssystem *Kerberos*.

*AnyNet*

Die Bezeichnung *AnyNet* steht für zwei Funktionalitäten, die mit dem *Communications Server* ausgeliefert werden:

- SNA over TCP/IP und
- AnyNet Sockets over SNA.

*SNA over TCP/IP* erlaubt es Applikationen, die nur das SNA-Protokoll unterstützen, mit einem TCP/IP-Netz verbunden zu werden, ohne dass die Applikationen angepasst werden müssen.

*AnyNet Sockets over SNA* erlaubt es Applikationen unter z/OS *Unix System Services* (USS), Verbindungen über ein vorhandenes SNA-Netz aufzubauen.

**System Authorization Facility (SAF)**

Die SAF ist ein Teil des z/OS-Betriebssystems und dient als Sicherheitsschnittstelle zwischen dem System und dem Sicherheitssubsystem (z. B. RACF, TopSecret, ACF2).

*Resource Manager*, z. B. IMS, DFHSM, JES oder CICS, fragen über die SAF-Schnittstelle bei RACF bzw. dem jeweiligen Sicherheitssubsystem an (RACROUTE Macro), ob ein Anwender berechtigt ist, auf eine Ressource zu zugreifen. SAF gibt die Antwort des Sicherheitssubsystems an den *Resource Manager* zurück, woraufhin dieser den Zugriff gewährt (*Return Code* ist gleich Null) oder ablehnt (*Return Code* ist größer Null).

**SecureWay Security Server für z/OS**

Der *Secure Way Security Server* für z/OS bildet eine Sicherheitsplattform für das Mainframe-System. Der *Secure Way Security Server* umfasst folgende Komponenten:

*RACF (Resource Access Control Facility)*

RACF ist eine Zusatz-Software zur Absicherung des z/OS-Betriebssystems. RACF arbeitet mit Kennungen, Gruppen und Ressourcen (Dateien, Klassen), die in der RACF-Datenbank eingetragen sein müssen. Anhand dieser Definitionen regelt RACF nicht nur den Zugang zum System, sondern auch die Zugriffe auf die Ressourcen. Jede Ressource, z. B. Datei, muss über ein entsprechendes RACF-Profil geschützt sein. Durch den Einsatz von Platzhaltern ist es möglich, mit einem generischen Profil eine Gruppe von Ressourcen zu schützen, womit die Verwaltung vereinfacht wird. Zugriffe auf diese so geschützten Ressourcen müssen dann entweder einzelnen Usern oder Usergruppen durch die RACF-Administration vergeben werden.

Im RACF gibt es Attribute, die einem Besitzer höhere Rechte einräumen können:

- *SPECIAL* - berechtigt zur Administration des RACF (Verwalten von Gruppen, Kennungen und Ressourcen).
- *OPERATIONS* - für *Space Manager*, mit diesem Recht können Dateien verwaltet werden.
- *AUDITOR* - für die Überwachung der Tätigkeiten im Sicherheitsbereich in der Funktion eines Audits.

Diese Rechte können zusätzlich auf Gruppenebene vergeben werden *(Group Special, Group Operations, Group Auditor).*

Für die Berechtigung zur Nutzung interaktiver Programme, z. B. TSO oder *Unix System Services*, bietet RACF zusätzliche Segmente an. In diesen Segmenten werden die Rechte zur Nutzung der interaktiven Programme festgelegt. Darüber hinaus können Abrechnungsinformationen (*Accounting*) oder Ressourcenbeschränkungen (dem Anwender zur Verfügung stehender Hauptspeicher, Anzahl zu startender Tasks) in diesen Segmenten festgeschrieben werden.

Jeder Anwender (darunter fallen die Kennungen von *Batch-Jobs*, *TSO-Usern* und *Started Tasks*) wird im laufenden System von RACF über sogenannte ACEEs (*Accessor Environment Element*) verwaltet. Das sind Kontrollblöcke, die bei der Initialisierung des Adressraumes angelegt werden.

*Public Key Infrastructure (PKI)*

RACF bietet den gesicherten Systemzugang mittels digitaler Zertifikate an. Dies ist besonders für den Einsatz im Internet/Intranet sinnvoll. RACF kann Zertifikate erzeugen, signieren, prüfen und verwalten. Die Zertifikate können in der RACF-Datenbank oder in einer speziellen Hardware gespeichert werden. Der Aufbau einer Public Key Infrastructure mit eigenen RACF-Zertifikaten ist hiermit möglich. Auch der Zugang zu geschützten Webserver-Bereichen kann über Zertifikate erfolgen.

*Firewall Technologies*

Die *Firewall Technologies* des *Secure Way Security Server* für z/OS ermöglichen die Trennung interner und externer Netzbereiche. Sie unterstützen folgende Funktionalitäten:

- Packet Filter
- sichere Tunnel mit IPSec-Technik zum Aufbau von VPNs (Virtual Private Networks)
- Socks Server
- FTP Proxy Server
- Network Address Translation (NAT) von einer internen zu einer externen Adresse und zurück

Für den Einsatz von IPSec wird zusätzlich der *Communications Server* für z/OS benötigt.

*LDAP*

Zusammen mit dem *Secure Way Security Server* liefert IBM einen LDAP-Server aus. Dieser unterstützt die gängigen LDAP-Clients und kann somit als Auskunftssystem dienen. Zur Verwaltung großer Datenmengen kann sowohl die RACF-Datenbank als auch eine unabhängige DB2-Datenbank eingesetzt werden.

*Distributed Computing Environment (DCE)*

DCE ist eine Sammlung von Tools und Diensten, welche die Erstellung, Nutzung und Pflege von verteilten Anwendungen unterstützen.

DCE unter z/OS unterstützt das *Distributed File System* (DFS), welches innerhalb der DCE-Umgebung die gemeinsame Nutzung von Daten (*Sharing*) erlaubt, und *Network File System* (NFS), welches unter anderem Unix-Workstations gestattet, auf Daten der z/OS-Rechner zuzugreifen.

**Integrated Cryptographic Service Facility (ICSF)**

Das ICSF ist ein Software-Element, das mit der Krypto-Hardware und dem *Secure Way Security Server* zusammenarbeitet, um die Ver- und Entschlüsselung zu beschleunigen.

**Sysplex Failure Managements (SFM)**

Die *SFM Policy* erkennt, ob Fehler an einem im *Sysplex*-Verbund arbeitenden System aufgetreten sind und leitet gegebenenfalls entsprechende Maßnah-

men ein. Ohne SFM wird, falls eine Maschine im Verbund Probleme hat, eine Nachricht an den Operator gesendet. Der Operator kann daraufhin das fehlerhafte System aus dem Verbund nehmen und Recovery-Maßnahmen einleiten. SFM erlaubt die Installation einer Policy, die bei bestimmten Fehlern automatisch festgelegte Recovery-Aktionen initiiert und so den Betrieb der Maschine aufrechterhalten kann.

**Automatic Restart Manager (ARM)**

Der ARM erlaubt ein schnelles Wiederherstellen von Subsystemen, die aufgrund kritischer Ressourcen (z. B. *Deadlocks*) angehalten wurden. Hierdurch werden die aktiven Systemeingriffe durch das Operating reduziert.

**Global Resource Serialization (GRS)**

GRS stellt in einer Multitasking/Multiprocessing-Umgebung sicher, dass der Zugriff auf Ressourcen, die von mehr als einem Rechner benutzt werden, koordiniert abläuft. Im Rahmen einer *Sysplex*-Konfiguration sollte GRS in jedem Fall eingesetzt werden.

GRS kann einerseits im *RING*-Modus konfiguriert werden. Dabei wird ein *RSA Message Control Block* (Ring System Authority) sequentiell von z/OS-System zu z/OS-System transportiert, in dem jedes System seine Anforderungen einträgt. Jedes System kopiert sich die RSA Message in den eigenen Speicher, d. h. die Information ist nicht aktueller, als bei der zuletzt vorbeigekommenen RSA-Information.

Als weitere, modernere Konfiguration steht der *STAR*-Modus zur Verfügung. Dabei sind alle z/OS-Systeme im Sysplex mit einer *Lock Structure* in der *Coupling Facility* verbunden, wobei jedes z/OS-System nur die eigene Sicht im lokalen Speicher halten muss. Die Abfrage nach Ressourcen durch GRS ist im *STAR*-Modus effektiver als im *RING*-Modus.

**Unix System Services (USS)**

USS ist keine Unix-Portierung, sondern ein POSIX-kompatibles Subsystem von MVS. Früher wurde es als *Open Edition MVS* vertrieben. Die Aufgabe des USS Subsystems liegt im Betrieb POSIX-kompatibler Anwendungen. Hierfür wurde das *Hierarchical File System* (HFS) und eine *Unix Shell* eingeführt.

Parallel zu HFS steht seit geraumer Zeit auch das Filesystem zFS zur Verfügung, das für alle neuen Entwicklungen benutzt wird (siehe auch nachfolgenden Abschnitt *Dateisysteme und Zugriffsarten*).

Unter USS laufen viele Programme, die auch unter POSIX-konformen Unix-Betriebssystemen laufen können. So sind die Funktionen von TCP/IP für z/OS größtenteils unter USS realisiert. Ebenso steht ein HTTP-Webserver zur Verfügung, der als *Daemon* unter USS oder als *Started Task* unter MVS laufen kann.

**System Managed Storage (SMS)**

SMS vereinfacht das Verwalten von Daten auf Festplatten, indem diese Funktion viele Aufgaben, z. B. das Anlegen von Dateien auf bestimmten Festplatten, die Festlegung von Charakteristiken der *Datasets* usw., übernimmt. Hierzu werden sogenannte ACS-Routinen (*Automated Control Storage*) definiert, die nach vorgegebenen Regeln den Plattenspeicher verwalten. *Datasets* werden dabei anhand ihrer Namensgebung in vorher festgelegte Plattenpools gespeichert. Da Mainframe-Systeme nicht selten über eine große Anzahl von

Platten verfügen, vereinfacht SMS die Verwaltung der Dateien außerordentlich. Die Verwaltung von SMS kann über das interaktive Dialog-System ISMF erfolgen (*Interactive Storage Management Facility*).

Im Rahmen des SMS-Konzepts gibt es eine Reihe von Software-Produkten, die die effiziente Verwaltung von Daten in einer Umgebung mit dem z/OS-Betriebssystem ermöglichen (z. B. DFHSM- oder DFxxx-Produkte). Darüber hinaus stehen als *Storage Management* Funktionen eine Reihe von Dienstprogrammen zur Verfügung, die die Verwaltung der Datenbestände unterstützen.

**Hierarchical Storage Manager (HSM)**

HSM ist ein wesentlicher Bestandteil des SMS-Konzeptes von z/OS. Das Programm-Produkt unterstützt die Verwaltung der z/OS-Dateien, die Datensicherung sowie die effektive Nutzung von Speichermedien. Gesteuert über sogenannte *Policies* (Regel-Definitionen) werden von HSM zu vorgegebenen Zeiten Dateien auf andere Medien verschoben (migriert) und dabei komprimiert. Es gibt zwei Migrations-Level:

- Migration-Level 1 auf HSM-eigene Platten
- Migration-Level 2 auf Bänder (in Roboterstationen) oder nach VTS (*Virtual Tape System*)

Migrierte Dateien können erst wieder gelesen werden, wenn sie über den HSM wieder erstellt worden sind. Diese Funktion kann entweder manuell initiiert werden oder erfolgt automatisch, wenn die Datei angesprochen wird (*Recall*-Funktion).

Weiterhin können *logische Dumps* (bestimmte Dateien) oder *Full Volume Dumps* (der Inhalt einer ganzen Festplatte) zu bestimmten Zeiten gestartet werden und somit automatisch Datensicherungen durchgeführt werden.

**System Management Facility (SMF)**

SMF ist die zentrale Protokollierungsfunktion im z/OS-Betriebssystem. Nahezu alle Komponenten und auch viele ISV-Produkte (*Independent Software Vendor*) schreiben SMF-Sätze, in denen die Aktivitäten protokolliert werden. Auch RACF schreibt solche Sätze. Hier ist besonders der Satztyp 80 wichtig für spätere Auswertungen.

**Resource Measurement Facility (RMF)**

RMF protokolliert das Systemverhalten in Bezug auf Kapazität und Performance. Die Protokolldaten werden als SMF-Sätze gesichert und stehen für spätere Auswertungen zur Verfügung. RMF ist optional, alternative Programme (Monitore) sind am Markt verfügbar.

**Generalized Trace Facility (GTF)**

Der Begriff *Trace* stellt die Möglichkeit dar, den Datenfluss zwischen zwei Komponenten im System (z. B. einer Anwendung und einem Endbenutzer) mitzuschreiben und in einer Datei zur späteren Auswertung zur Verfügung zu stellen. GTF ist die zentrale *Trace*-Funktion von z/OS, die *Traces* von vielen z/OS-Komponenten ermöglicht. Darüber hinaus werden auch *Traces* der Netzfunktionen unterstützt. Zum Auswerten der *Traces* stehen verschiedene Programme zur Verfügung, z. B. ACFTAP für Netzanalysen. Für *Online-Traces* bietet sich auch NLDM an (*Network Logical Data Manager*), eine Komponente der *NetView* Software.

**Transaktionsmonitore und Datenbanksysteme**

*IMS TM (Information Management System Transaction Monitor)*

IMS TM wird die Transaktionskomponente des IMS-Systems genannt, mit der die IMS-Transaktionen in einem IMS-System verwaltet und gesteuert werden. (In älteren IMS-Versionen ist diese Funktion auch unter dem Kürzel *DC* bekannt.)

*IMS DB (Information Management System Database)*

IMS DB wird die Datenbankkomponente des IMS-Systems genannt, mit der die IMS-Datenbanken in einem IMS-System verwaltet werden. Bei IMS-Datenbanken handelt es sich um hierarchische Datenbankmodelle.

*CICS TS (Customer Information Control System Transaction Server)*

CICS TS ist ein weiterer Transaktionsmonitor. Mit CICS TS werden die CICS-Transaktionen in einem System verwaltet und gesteuert. Als Datenbank werden häufig VSAM-Files oder DB2-Datenbanken eingesetzt.

*DB2 (Database 2)*

DB2 ist ein Programmpaket, mit dessen Hilfe relationale Datenbanken erstellt und verwaltet werden können. Über IMS TM, CICS TS oder über die Sprache SQL (*Structured Query Language*) können Daten in der Datenbank in Tabellen abgelegt oder aus dieser Datenbank extrahiert werden.

IMS, CICS und DB2 sind nicht im Fokus des Bausteins *S/390- und zSeries-Mainframe* und werden nur am Rande betrachtet.

**File Transfer Protocol (FTP)**

FTP-Programme erlauben den Transport von Daten sowohl zwischen z/OS-Systemen, als auch zu und von anderen Plattformen.

FTP ist nicht im Fokus des Bausteins *S/390- und zSeries-Mainframe* und wird nur am Rande betrachtet.

**Middleware**

MQSeries (Message Queueing System)

MQSeries stellt eine Verbindung zwischen unterschiedlichen Applikationen auf der Basis von Nachrichten (Messages) her, beispielsweise zwischen CICS, IMS oder Batch-Applikationen. Über entsprechende APIs (*Application Programming Interfaces*) werden die Nachrichten an MQSeries weitergegeben und danach an die vorgegebenen Ziele ausgeliefert. Ist die Lieferung nicht möglich, werden die Nachrichten zwischengespeichert (*Queued*) und erst dann weitergeleitet, wenn der Verbindungsaufbau wieder möglich ist.

MQSeries ist nicht Gegenstand des Bausteins *S/390- und zSeries-Mainframe*.

**Dateisysteme und Zugriffsarten**

Dateien werden unter z/OS mit bestimmten Charakteristiken angelegt, z. B. Größe, Art der Speicherung (innere Struktur), auf welcher Platte sich die Datei befindet und unter welchem Dateinamen die Datei gespeichert und normalerweise zu finden ist. Insbesondere in Bezug auf die innere Struktur der Dateien

bestehen teilweise erhebliche Unterschiede zu anderen, häufig eingesetzten Betriebssystemen. Nachfolgend die wichtigsten Dateitypen:

*HFS (Hierarchical File System)*

Das HFS-Filesystem ist mit typischen Unix-Dateisystemen vergleichbar. Es wird in einem MVS *Dataset* abgelegt, das MVS-seitig mit den üblichen Werkzeugen verarbeitet werden kann (z. B. Datensicherung über HSM). Gegenüber USS stellt sich das Filesystem hierarchisch dar. Daten in diesem Filesystem werden im EBCDIC-Zeichensatz gespeichert.

*z/OS File System (zFS)*

Das zFS entspricht konzeptionell dem HFS, jedoch können hier mehrere Filesysteme in einem z/OS *Dataset* gespeichert werden und die Daten lassen sich auch im ASCII-Zeichensatz abspeichern. Laut IBM ist zFS das strategische Filesystem, in dem nur noch neue Funktionen entwickelt werden. zFS kann bis jetzt nicht als Root-Filesystem verwendet werden.

*MVS Physical Sequential (PS) Datasets*

In dieser Art von *Dataset* können Daten nur sequentiell gelesen oder geschrieben werden. *Physical Sequential Datasets* dienen im Systemumfeld oft der Verarbeitung großer Datenmengen.

*MVS Partitioned Organized (PO) Datasets*

*Partitioned Organized Datasets* können mit einer Bibliothek verglichen werden. In einem *PO Dataset* gibt es einen Index (*Directory*) und die einzelnen Bücher (*Member*). Die *Member* enthalten die Informationen.

Bei häufigem Abspeichern von *Membern* muss die Datei zeitweise reorganisiert werden. Dies kann durch die Benutzung einer PDSE-Datei (*Partitioned Dataset Enhanced*) umgangen werden.

*Virtual Storage Access Method (VSAM)*

Im z/OS-Betriebssystem stellt VSAM eine der wichtigsten Zugriffsmethoden auf Dateien dar. Die Datensätze werden über einen Index oder eine relative Byte-Adresse gefunden. Vier VSAM-Dateiarten lassen sich unterscheiden:

- ESDS (Entry Sequenced Data Set)
- KSDS (Key Sequenced Data Set),
- RRDS (Relative Record Data Set) und
- LDS (Linear Data Set).

*Weitere Zugriffsmethoden*

Neben der allgemein bekannten VSAM-Methode gibt es weitere Methoden wie *Sequential Access Method* (SAM) und *Queued Sequential Access Method* (QSAM) sowie diverse andere Methoden, die hier wegen ihrer geringeren Verbreitung nur am Rande erwähnt werden.

**Server- und Client-Konzepte**

Durch die Erweiterung des z/OS-Betriebssystems um den *Unix System Server* (USS) können Rechner mit diesem Betriebssystem zusätzliche Server- und Client-Funktionen wahrnehmen. Beispiele für solche Server-Funktionen sind unter anderem der HTTP-Server, der FTP-Server oder der *Domain Name Server*. Die FTP-Funktion lässt sich z. B. auch als Client einsetzen. Darüber

hinaus wird das z/OS-System in heutigen 2-Schicht- oder 3-Schicht-Architekturen vielfach als Datenbank-Server eingesetzt, wo es mit anderen Plattformen kommuniziert.

**Konfiguration des z/OS (OS/390)**

*I/O-Config*

Die Eingabe-/Ausgabe-Konstellation eines z/OS-Betriebssystems wird im Rahmen des HCD-Dialogs über eine I/O-Konfiguration erstellt und über das *Operator Facility* (via HMC-Konsole) für die jeweilige *LPAR* abgelegt. Zum *IML*-Zeitpunkt ist bereits festgelegt, welche I/O-Profile für die spätere Auswahl zur Verfügung stehen. Ein dynamisches Nachkonfigurieren während des Betriebs ist jederzeit möglich (siehe Maßnahme M 3.39 *Einführung in die zSeries-Plattform*).

*IPL Volume*

Zum Starten eines z/OS-Betriebssystems benötigt das System ein spezielles *IPL-Volume*, eine Platte mit einer speziellen *Bootstrap-Routine*, die die notwendigen Betriebssystemprogramme lädt und zum Starten bringt. Dieser Vorgang entspricht einem Boot-Vorgang bei Unix und nennt sich bei z/OS *Initial Program Load* (IPL).

*Parmlib / Proclibs*

Eine (oder mehrere) Parameter-Datei(en) stehen über den *Parmlib*-Mechanismus zur Verfügung, um alle wesentlichen z/OS-Systemparameter zu definieren. Dazu gehört z. B., welche Subsysteme gestartet werden sollen, welche Sicherheitsmechanismen aktiviert werden und welche Bibliotheken autorisiert sein sollen. Alle wichtigen System-Jobs - auch *Started Tasks* genannt - stehen auf Prozedur-Bibliotheken (*Proclibs*) bereit, um zum Startzeitpunkt aktiviertwerden zu können (siehe Maßnahme M 3.39 *Einführung in die zSeries-Plattform*). Dieser Bereich muss sehr sorgfältig definiert und geschützt werden, da hier wesentliche Sicherheitsmechanismen verankert sind.

*Kataloge*

Dateien werden über Kataloge geführt und dem System bekannt gegeben. Als oberste Instanz existiert der *Master-Katalog*, an den über *Alias*-Definitionen verschiedene Benutzerkataloge angebunden sind.

*Arbeitsdateien*

Zur Minimalkonfiguration eines z/OS-Betriebssystems gehören mehrere Arbeitsdateien, die bei Produktionsbeginn angelegt sein müssen:

- Syslog
- JES2/3 Spool und Checkpoint
- SMF-Dateien
- Log-Writer-Dateien
- Couple Datasets (bei Sysplex)
- Page Datasets zum Auslagern von Hauptspeicher

# M 3.41 Einführung in Linux und z/VM für zSeries-Systeme

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Neben den unter z/OS laufenden *Unix System Services* (USS) steht auch Linux für die zSeries-Hardware zur Verfügung.

Linux für zSeries entspricht dem Linux für andere Plattformen, die Modifikationen im Kernel beziehen sich ausschließlich auf Anpassungen an die zSeries-Hardware (Systemumgebung, CPU-Architektur und Hardware-abhängige Treiber). Da das zSeries-Linux eine Portierung darstellt, arbeitet es mit dem ASCII-Zeichensatz (im Gegensatz zum USS HFS-Dateisystem, das im EBCDIC-Modus läuft). Derzeit sind zwei Linux-Versionen für diese Plattformfamilie erhältlich: eine 31 Bit-Version für S/390-Hardware und eine 64 Bit-Version für die zSeries-Hardware (das S/390-System ist zwar ein 32 Bit-System, die Software darauf läuft jedoch mit 31 Bit, da das erste Bit zur Umschaltung zwischen 24 Bit- und 31 Bit-Modus benötigt wird).

**Betriebsarten von Linux unter zSeries**

Es sind drei unterschiedliche Betriebsarten von Linux unter zSeries möglich:

- Linux Native auf zSeries Hardware
- Linux in einer zSeries LPAR
- Linux unter dem Träger-System z/VM

*Linux Native auf zSeries Hardware*

In dieser Betriebsart wird Linux als Single-System auf der zSeries Hardware eingesetzt. Dies bedeutet, dass die gesamte zSeries Hardware vom Linux-System benutzt wird. Single-Systeme stellen in der Praxis derzeit eher eine Ausnahme dar.

*Linux in einer zSeries LPAR*

Bei dieser Variante erfolgt der Betrieb von Linux in einer *LPAR (Logical Partition)* auf der zSeries-Maschine. Der *LPAR*-Mode der zSeries-Hardware erlaubt den Betrieb von mehreren unabhängigen Betriebssystem-Installationen auf einer zSeries-Maschine. Jede einzelne Partition verhält sich wie eine unabhängige Hardware. Auf diesen *LPARs* können unter anderem *z/OS* oder *Linux* als Betriebssystem installiert werden.

Die Betriebsart *Linux in einer zSeries LPAR* kommt zum Beispiel in Betracht, wenn zusätzlich zu einem schon vorhandenen z/OS-Datenbank-Server Internet-Applikationen, wie z. B. Webserver, betrieben werden sollen.

Die Konsolidierung von Linux und z/OS auf einem physischen zSeries-System an Stelle zweier getrennter Systeme reduziert nicht selten den Aufwand für die Installation und den Betrieb.

*Linux unter dem Träger-System z/VM*

Es können mehrere Linux-Installationen auf einem zSeries-Rechner oder innerhalb einer LPAR unter dem Träger-System z/VM betrieben werden. Das z/VM stellt sogenannte virtuelle Maschinen zur Verfügung, unter denen die ein-

zelnen Linux-Installationen unabhängig von einander betrieben werden können.

Die Betriebsart *Linux unter dem Träger-System z/VM* kommt zum Beispiel in Betracht, wenn die z/Series-Hardware im Rahmen eines Server-Konsolidierungsprojektes eingesetzt wird. Hierbei wird die Installation von Linux durch das System-Cloning erleichtert. Es können viele Linux-Systeme parallel auf einer Maschine betrieben werden. Darüber hinaus erleichtert diese Konstellation eine zentrale Kontrolle und Administration.

**Communications Server for Linux on zSeries**

Linux für zSeries unterstützt ohne zusätzliche Komponenten TCP/IP. Der *Communications Server for Linux on zSeries* als separates Produkt ermöglicht zusätzlich eine Kommunikation über SNA oder TCP/IP mit anderen Systemen in den folgenden Bereichen:

- Advanced Peer to Peer Networking (APPN)
- High Performance Routing (HPR)
- TN3270E Server
- Telnet Redirector
- SSL data encryption scalability
- Client Authentication
- Application Programming Support
- Advanced Program to Program Communication (APPC)
- Common Programming Interface for Communications (CPI-C)

Das Programm bietet den Administratoren und Bedienern Unterstützung bei der Installation, Konfiguration und Problemanalyse.

**HiperSockets**

*HiperSockets* erlauben eine LPAR-übergreifende Kommunikation. Mit dieser Funktion lässt sich innerhalb des Systems ohne eine zusätzliche physische Verbindung ein "systeminternes Netz" über TCP/IP aufbauen.

Ein von Linux abgesetzter TCP/IP-Auftrag wird auf Maschinenebene abgefangen und an die adressierte Partition umgeleitet. Dies ist mit Übertragungsraten von mehreren GByte/s möglich. Gegenüber dem Linux-Betriebssystem verhält sich diese Kommunikationsschnittstelle wie ein herkömmliches TCP/IP-Netz. Auch z/OS-Systeme in einer anderen LPAR lassen sich so mit Linux-Systemen verbinden.

**Integrated Facility for Linux (IFL)**

Diese Hardware-Funktion gestattet den zusätzlichen Einsatz von Linux auf einem System. Die speziellen IFL-Prozessoren bringen zusätzliche Rechenkapazität.

IFL wird von PR/SM wie eine separate LPAR verwaltet, die jedoch nur Linux-Betriebssysteme (oder z/VM mit Linux-Betriebssystemen) unterstützen kann.

**z/VM**

Das Betriebssystem z/VM ermöglicht eine - Software-basierte - Aufteilung des Rechners in mehrere parallele *Virtual Machines*. z/VM verwaltet mit dem *Control Program* (CP) die Hardware der Partition und stellt den Gast-Betriebssystemen die *Virtual Machines* zur Verfügung.

Die Hardware-Zugriffe erfolgen über das CP, das dem aufrufenden Betriebssystem das Ergebnis in seiner gewünschten Form präsentiert.

Darüber hinaus stellt z/VM das *Conversational Monitoring System* (CMS) zur Verfügung, in dem z. B. Scripts ablaufen können, um korrektive Maßnahmen durchzuführen oder neue Systeme zu aktivieren.

**Linux-Sicherheitsaspekte**

*Hardware*

Die Verbindung zwischen den Linux Betriebssystemen oder zwischen Linux und z/OS-Systemen kann über *HiperSockets* erfolgen. Diese sind integraler Bestandteil der Hardware und ermöglichen eine schnelle und - bei korrekter Konfiguration - sichere TCP/IP-Verbindung.

Durch den z/VM-Einsatz wird die Bereitstellung und Absicherung der Hardware zu einem Teil durch eine Software-Lösung ersetzt. Die Ressourcen sind deshalb nicht als reale Hardware verfügbar, sondern werden virtuell in der Software (z/VM) abgebildet. Dem entsprechend müssen die Ressourcen mit Software-Mitteln abgesichert werden.

*RACF/VM*

Die *Resource Access Control Facility for z/VM* (RACF/VM) erweitert die Standard-Security des z/VM um eine Zugriffskontrolle für die Ressourcen des z/VM-System. Daneben überprüft es die Zugriffe auf die Systemressourcen und die *Virtual Machine*.

*DIRMAINT*

Die zentrale Konfigurationsdatei von z/VM ist das *z/VM-System-Directory*. Die Verwaltung dieser Datei wird von *DIRMAINT* unterstützt, wobei die *DIRMAINT*-Funktion die folgenden Aufgabenbereiche abdeckt:

- Distributed Virtual Machine Management
- automatische Minidisk-Administration (Allokieren, Löschen, usw.)
- Unterstützung der Benutzer
- Auditing
- Backup/Recovery des Directory

Auch wenn das Directory mit einem herkömmlichen Editor bearbeitet werden kann, ist *DIRMAINT* für alle Installationen mit größeren User-Anzahlen empfehlenswert, da die dialoggestützte *DIRMAINT*-Funktion die Verwaltung vereinfacht. Dies hilft bei der Vermeidung von Eingabefehlern.

*Access Control*

Die Steuerung der Zugriffskontrolle ist bei Linux im Wesentlichen über drei Mechanismen möglich:

- Permission Bits wie bei anderen Unix-Betriebssystemen
- Mandatory Access Control (MAC)
- Access Control Lists (ACLs)

Während die erste Methode in der Regel für normale Sicherheitsanforderungen ausreicht, sollten MAC und ACLs bei höheren Sicherheitsanforderungen in Betracht gezogen werden. Für MAC und ACLs sind zusätzliche Software-Komponenten erforderlich.

*Pluggable Authentication Module (PAM)*

Zur Zentralisierung der Benutzerverwaltung bietet es sich für Linux auf LPARs an, die Verwaltung der Userids über ein z/OS-RACF abzuwickeln. Dazu muss das Linux-System über ein *Pluggable Authentication Module* (PAM) verfügen und mit dem vorgeschalteten LDAP-Server des z/OS-RACF-Systems über die *HiperSockets* Verbindung aufnehmen.

Ist die Kennung im RACF administriert und sind User-ID und Passwort korrekt, so wird der Zugang zu dem Linux-System freigegeben. Dateizugriffe lassen sich jedoch nach wie vor nur über die Sicherheitsmechanismen von Linux (Permisson Bit) realisieren.

**Transaction Processing Facility (TPF)**

TPF ist ein weiteres Betriebssystem für die zSeries-Plattform und stellt eine Sonderform dar. Es handelt sich dabei um ein transaktionsorientiertes System, das speziell im Bereich Flugzeugbuchung eingesetzt wird, wo es besonders auf hohe Performance ankommt. Transaktionen laufen hierbei direkt im Kernel-Modus.

TPF wird an dieser Stelle aus Gründen der Vollständigkeit erwähnt und ist nicht Gegenstand des Bausteins *S/390- und zSeries-Mainframe*.

# M 3.42 Schulung des z/OS-Bedienungspersonals

**Verantwortlich für Initiierung:** Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** Administrator, Vorgesetzte

Der Betrieb von z/OS-Systemen ist komplex und so gestaltet, dass viele Bereiche daran beteiligt sind. Es ist deshalb darauf zu achten, dass das Bedienungspersonal die für seine Tätigkeit benötigte Ausbildung erhält. Neben den Empfehlungen aus Maßnahme M 3.11 *Schulung des Wartungs- und Administrationspersonals* sind für die Mitarbeiter im z/OS-Bereich zusätzlich die folgenden Hinweise zu beachten:

- Die Administratoren sollten durch regelmäßige Teilnahme an Schulungsmaßnahmen und Anwendertagungen entsprechend ihren Aufgaben ausgebildet werden. Es sollte überlegt werden, die Ausbildung anhand eines Schulungsplanes festzulegen.
- Zusätzlich sollten RACF-Adminstratoren in allen sicherheitsrelevanten Bereichen des z/OS-Systemes ausgebildet werden.
- Die Auditoren sollten entsprechend ihren Aufgaben geschult werden. Die Aufgaben der Auditoren sind in Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS* beschrieben.
- Es sollte überlegt werden, ob eine regelmäßige sicherheitstechnische Schulung für alle Mitarbeiter, die mit z/OS-Systemen arbeiten, durchgeführt werden sollte. Dabei sollte den Mitarbeitern das vorhandene Regelwerk, die Sicherheitsdefinitionen und die Gründe, die zu den Sicherheitsmaßnahmen geführt haben, erläutert werden (*Sensibilisierung für ein Sicherheitsdenken*).

Prüffragen:

- Werden die Administratoren des z/OS-Systems durch regelmäßige Teilnahmen an Schulungsmaßnahmen und Anwendertagungen entsprechend ihrer Aufgaben ausgebildet?
- Werden die RACF-Administratoren in allen sicherheitsrelevanten Bereichen des z/OS-Systems ausgebildet?

# M 3.43 Schulung der Administratoren des Sicherheitsgateways

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Ein Sicherheitsgateway stellt ein zentrales Element bei der Absicherung eines Netzes gegen Gefährdungen von außen dar. Deswegen ist es unerlässlich, dass die Administratoren des Sicherheitsgateways ausreichend geschult sind, damit sie in der Lage sind, alle gebotenen Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der Komponenten des Sicherheitsgateways notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte zu einzelnen Produkten, die als Komponenten des Sicherheitsgateways eingesetzt werden. Für die Anforderungen an die Schulungen für Betriebssysteme von Rechnern, die als Komponenten des Sicherheitsgateways eingesetzt werden sowie für aktive Netzkomponenten (insbesondere Router, die als Paketfilter Teil eines Sicherheitsgateways sind) sollten die Hinweise in den jeweiligen Bausteinen der Betriebssysteme beziehungsweise im Baustein B 3.302 *Router und Switches* berücksichtigt werden.

Allgemein sollten in den entsprechenden Schulungen folgende Elemente enthalten sein:

- Grundlagen und Konzepte der Administration, Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche für jede Komponente des Sicherheitsgateways. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.
- Grundlagen der Informationssicherheit, insbesondere Vorsorgemaßnahmen, Reaktion, Analyse und Incident Handling (siehe beispielsweise auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*)
- Angriffsszenarien (z. B. Denial of Service Angriffe, ARP-Spoofing, IP-Spoofing, DNS-Spoofing, Viren und andere Schadsoftware)
- Grundlagen der Strukturierung von Netzen
- ISO/OSI Schichten Modell
- Grundlagen von IP und der damit zusammenhängenden Protokolle (IP-Adressierung, Subnetting, IP, ICMP, TCP, UDP) und der verschiedenen Möglichkeiten zur Filterung anhand der Header-Daten
- Grundlagen des Routing, statisches und dynamisches Routing, Grundlagen der eingesetzten Routing-Protokolle und ihrer Sicherheitsaspekte
- Grundlagen der wichtigsten eingesetzten Protokolle der Anwendungsschicht (beispielsweise SMTP, HTTP und HTTPS, Secure Shell, SMB/CIFS) und der verschiedenen Möglichkeiten zur Filterung anhand von Protokollbefehlen oder Befehlsparametern
- Grundlagen zum Thema Virtuelle Private Netze (VPN)
- Grundlagen zum Thema Intrusion Detection/Intrusion Prevention (IDS/IPS)
- Grundlagen zum Umgang mit verschlüsselten Daten (Verschlüsselung z. B. mit HTTPS oder IPSec) und Möglichkeiten zur Behandlung verschlüsselter Daten
- Betrieb
    - Management der Geräte, Werkzeuge
    - Protokollierung

  - Sicherung und Verwaltung von Konfigurationsdaten
- Fehlerbehebung
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge, Werkzeuge zur automatischen Überprüfung der einzelnen Komponenten des Sicherheitsgateways auf korrekte Funktion
  - Teststrategien zur Fehlersuche
  - Anforderungen an sichere Netzinstallationen
- Relevante rechtliche Aspekte wie Datenschutz, rechtliche Aspekte der Netzanbindung (in Deutschland beispielsweise Teledienstegesetz) und ähnliche Regelungen

Auch wenn in einer Gruppe von Administratoren die Aufgaben so verteilt sind, dass jeder Administrator nur einen bestimmten Verantwortungsbereich hat, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern hierfür ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein Budget eingeplant werden und ein Schulungsplan für Administratoren erstellt werden.

Prüffragen:

- Finden regelmäßige Schulungen für die Administratoren des Sicherheitsgateways statt?
- Decken die Schulungsinhalte neben den allgemeinen Informationen auch die herstellerspezifischen Besonderheiten ab?

# M 3.44 Sensibilisierung des Managements für Informationssicherheit

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Eine nachdrückliche und aktive Unterstützung durch die Behörden- bzw. Unternehmensleitung ist essentiell, damit Sicherheitskampagnen für die Mitarbeiter erfolgreich sein können. Daher ist es unabdingbar, dass vor dem Beginn von Sensibilisierungsmaßnahmen zur Informationssicherheit für Mitarbeiter das Management für Sicherheitsfragen sensibilisiert wird.

Die wichtigsten Informationen, die dem Management dabei geliefert werden müssen sind:

- **Darstellung der Sicherheitsrisiken und damit verbundenen Kosten**
  Die Aufmerksamkeit der Entscheidungsträger kann z. B. durch Berichte über Sicherheitsvorfälle erreicht werden, die die eigene Institution ebenso betreffen könnten (aus Institutionen derselben Branche oder mit ähnlicher IT). Beispiele konkreter Sicherheitsvorfälle aus der Nachbarschaft oder bei vergleichbaren Institutionen können die Rückendeckung des Managements erleichtern. Solche Beispiele finden sich mittlerweile nicht nur in Fachzeitschriften, sondern auch in Tageszeitungen (z. B. nach Hackerangriffen oder Virenvorfällen) und natürlich in großer Menge im Internet. Tatsächliche Schadensfälle aus der Vergangenheit aus der eigenen Institution können ebenfalls zu diesem Ziel eingesetzt werden.
  Die Darstellung von finanziellen Schäden in konkreten Zahlen ist erfahrungsgemäß schwierig. Statistiken und Auswertungen, wie sie beispielsweise von den Polizeien (BKA, FBI) oder Sicherheitsfachzeitschriften von Zeit zu Zeit veröffentlicht werden, bieten in manchen Fällen geeignete Informationen.
- **Auswirkungen auf die Geschäftsprozesse**
  Des Weiteren ist es wichtig, dass die Auswirkungen von Informationssicherheitsvorfällen auf die geschäftskritischen Prozesse geschildert werden. Mögliche Abhängigkeiten von Anwendungen und IT-Systemen sind der Geschäftsführung nicht immer bekannt.
  Eine Auflistung von möglichen Sicherheitsrisiken reicht jedoch in der Regel nicht aus, um die Unterstützung des Managements zu gewinnen. Eine ausgewogene Argumentation sollte darüber hinaus auch die folgenden Punkte beinhalten.
- **Rechtliche Sicherheitsanforderungen**
  Gesetze und andere juristische Vorgaben können ebenfalls Anforderungen an die Informationssicherheit in einer Institution nach sich ziehen, hierzu gehören beispielsweise Datenschutzgesetze, Sozialgesetzbuch, Handelsgesetzbuch, Bürgerliches Gesetzbuch, Strafgesetzbuch, etc.
  Viele gesetzliche Formulierungen zu Anforderungen der Informationssicherheit sind allgemein gehalten und können unter Umständen unverbindlich erscheinen.
  In der Tat lassen sich hieraus jedoch konkrete Verpflichtungen für die Gewährleistung eines angemessenen Sicherheitsniveaus ableiten. Eine Institution muss untersuchen, welche Regularien und Gesetze im Einzelnen Fall zur Wirkung kommen können.
- **Vorteile einer Zertifizierung**

Eine Zertifizierung der Informationssicherheitsprozesse bestätigt offiziell die hohe Wertschätzung der Informationssicherheit in einer Institution. Das Vertrauen der Geschäftspartner und der Öffentlichkeit in die IT der Institution wird dadurch gestärkt. Eine Zertifizierung kann außerdem bei Ausschreibungen Wettbewerbsvorteile mit sich bringen.

- **Standard-Vorgehensweisen zur Informationssicherheit für die Branche**
  Eine zusätzliche Motivation für den Einsatz von Informationssicherheitsstandards ist das Verhalten anderer ähnlicher Organisationen. Informationen zu Branchen-Standards können aus Fachzeitschriften der Branchen, aus Veranstaltungen oder durch Kontakte zu Kammern und Verbände bezogen werden.

Ein geeigneter Einstieg für die Sensibilisierung der Leitungsebene ist ein kurzer Bericht, gefolgt von einer Präsentation, die mit aktuellen Beispielen (extern und intern) das Thema Informationssicherheit erläutert. Hierbei sollte beispielsweise aufgezeigt werden, dass technische Maßnahmen ohne gleichzeitige personelle und organisatorische Maßnahmen sinnlos sind. Um die Unterstützung des Managements zu bekommen, ist es hilfreich, den Nutzen solcher Maßnahmen aufzuzeigen.

Durch die Präsentation von Sicherheitsrisiken und Lösungsalternativen kann das Management für die Notwendigkeit der Umsetzung von Sicherheitsmaßnahmen überzeugt werden.

Informationssicherheit wird erfahrungsgemäß in einer Institution nur dann erfolgreich umgesetzt, wenn alle Vorgesetzten hier mit gutem Beispiel vorangehen. Sinnvoll ist es daher, alle Führungskräfte explizit darauf zu verpflichten, ihre Mitarbeiter auf die Einhaltung der Sicherheitsvorgaben hinzuweisen und zu sensibilisieren.

Prüffragen:

- Wird das Management für Sicherheitsfragen sensibilisiert?
- Unterstützt die Leitungsebene die Informationssicherheit durch beispielhaftes Verhalten?

# M 3.45 Planung von Schulungsinhalten zur Informationssicherheit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Personalabteilung, Vorgesetzte

Ein Schulungsprogramm zur Informationssicherheit sollte den Mitarbeitern alle Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können (siehe M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit*).

Nachdem die Ziele der Informationssicherheitsschulungen für die Institution festgelegt sowie relevante Zielgruppen und deren spezifischer Schulungsbedarf identifiziert wurden (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*), müssen nun die konkreten Schulungsmodule und -inhalte geplant werden.

Hierzu sollten folgende Aspekte betrachtet werden:

- In welcher Tiefe und mit welcher Methodik soll welche Zielgruppe geschult werden?
- Welche Mitarbeiter gehören in welche Zielgruppe?
- Welche Ressourcen sind für eine Zielgruppe erforderlich, z. B. Trainerkapazität, Räumlichkeiten, benötigte IT-Infrastruktur, Organisation etc.?
- Welche speziellen Arbeitsumgebungen mit ihren Anforderungen an die Informationssicherheit und welche zugeordneten Maßnahmen müssen berücksichtigt werden, z. B. Prozesse, Verfahren, Aufgaben und Rollen inklusive möglicher Veränderungen?

Im Folgenden werden beispielhaft eine Struktur und wichtige Inhalte von Schulungsmodulen vorgestellt, die entsprechend den dargestellten Aspekten noch rollen- und ressourcenbezogen aufbereitet werden müssen.

Die Module unterscheiden sich zunächst nur nach Themen. Jedes Modul kann fast immer in unterschiedlicher inhaltlicher Tiefe durchgeführt werden, abhängig davon, für welche Arbeitsumgebung oder welchen Abschnitt einer Mitarbeiterlaufbahn es bestimmt ist.

Die Schulungsinhalte sollten auf Basis der in Maßnahme M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit* erarbeiteten Analyse festgelegt sowie regelmäßig überprüft und angepasst werden, um eine größtmögliche Wirksamkeit der Schulungsmaßnahmen zu erzielen. Zusätzlich sollten alle für den jeweiligen Informationsverbund relevanten Bausteine der IT-Grundschutz-Kataloge daraufhin überprüft werden, ob die erforderlichen Maßnahmen nicht nur angeordnet, sondern auch geschult wurden.

Ebenfalls exemplarisch wurden hier die Schulungsmodule den Zielgruppen zugeordnet. Dabei wird mit "X" gekennzeichnet, dass das jeweilige Modul für die entsprechende Rolle empfohlen wird. Mit einem "O" werden die optionalen Schulungsmodule gekennzeichnet, bei denen von Fall zu Fall entschieden werden sollte, ob die Inhalte für die entsprechende Rolle benötigt werden.

**Schulungsmodule**

Modul 1: Grundlagen der Informationssicherheit

Modul 2: Informationssicherheit am Arbeitsplatz

Modul 3: Gesetze und Regularien

Modul 4: Sicherheitskonzept der Organisation

Modul 5: Risikomanagement

Modul 6: Informationssicherheitsmanagement

Modul 7: IT-Systeme

Modul 8: Operativer Bereich

Modul 9: Technische Realisierung von Sicherheitsmaßnahmen

Modul 10: Notfallvorsorge/Notfallplanung

Modul 11: Neue Entwicklungen im IT-Bereich

Modul 12: Betriebswirtschaftliche Seite der Informationssicherheit

Modul 13: Infrastruktur-Sicherheit

| **Modul / Funktion** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vorgesetzte | X | X | X | X | | | | | | | O | X | |
| Sicherheitsmanagement | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Datenschutzbeauftragter | X | X | X | X | | | | | | | X | O | |
| Infrastrukturverantwortliche | X | X | X | X | X | O | | | | X | | | X |

| Modul / Funktion | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Benutzer | X | X | | | | | | | | | | | |
| Administratoren | X | X | | X | X | | X | X | X | X | X | | O |

Tabelle: Vorgeschlagene Schulungsmodule je Funktion

In diesem Beispiel dienen die beiden Module 1 und 2 als Basisschulung für alle Mitarbeiter und sind eng mit Sensibilisierungsmaßnahmen abzustimmen (siehe M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*). Alle anderen Module zeigen auf, welche Vertiefungsgebiete je nach Fachaufgabe außerdem vermittelt werden sollten.

Je nach Art der Institution wird es sinnvoll sein, weitere Zielgruppen und die zugehörigen Schulungsziele zu definieren (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*). Wichtig ist, dass auch Mitarbeiter nicht vergessen werden, die in erster Linie nichts mit Informationstechnik zu tun haben, wie z. B. der Sicherheits- und Reinigungsdienst.

**Modul 1: Grundlagen der Informationssicherheit**

Institutionen sind stark von einer ausreichend verfügbaren und gegen Angriffe geschützten IT und Infrastruktur abhängig. Daher ist die wichtigste Aufgabe von Sensibilisierung und Schulung, den Mitarbeitern den Wert von Informationssicherheit für die Institution und entsprechende Grundlageninformationen zu vermitteln.

Unter anderem sollten in diesem Modul folgende Themen behandelt werden:

- Motivation
  - Fallbeispiele aus der Praxis für Gefährdungen und Risiken
  - Auswirkungen von Angriffen, inklusive Social Engineering
- Informationen als Werte einer Institution und ihr Schutzbedarf
- Begriffserläuterungen:
  - Informationssicherheit
  - Vertraulichkeit, Integrität, Verfügbarkeit
  - Security, Safety, Datenschutz und ihre Abgrenzung zur Informationssicherheit
- Informationssicherheit in der eigenen Institution
  - Aufgaben und Ziele der Institution
  - Sicherheitsanforderungen und Risiken in der Institution
  - Informationssicherheitsstrategie und -konzept der Institution im Überblick
  - Aufgaben und Verpflichtungen der einzelnen Mitarbeiter

- Wesentliche Sicherheitsregeln für Mitarbeiter
    - Überblick über interne Sicherheitsregelungen
    - Umgang mit sensiblen Informationen (inklusive Passwörtern)
    - Nutzung von E-Mail und Internet
    - Schutz vor Schadprogrammen und Datensicherung
    - Umgang mit mobilen Endgeräten
    - Arbeiten in fremden oder öffentlichen Umgebungen

**Modul 2: Informationssicherheit am Arbeitsplatz**

Mitarbeiter können oft bereits durch die Beachtung einfacher Vorsichtsmaßregeln dazu beitragen, dass Schäden vermieden werden. Das Modul zur Umsetzung von Informationssicherheit am Arbeitsplatz sollte unter anderem die folgenden Themenschwerpunkte umfassen:

- Sensibilisierung von Mitarbeitern
- Motivation typische Fehler von Anwendern zu vermeiden
    - leichtsinniger Umgang mit Passwörtern
    - Verzicht auf Verschlüsselung
    - mangelnder Schutz von Informationen
    - mangelndes Misstrauen
    - Laptop-Diebstahl
- Vorbeugung gegen Social Engineering
- Organisation und Sicherheit
    - Die Sicherheitsvorgaben der Institution und deren Bedeutung für den Arbeitsalltag
    - Verantwortlichkeiten und Meldewege in der Institution (mit persönlicher Vorstellung der IT-Sicherheitsbeauftragten)
- Zutritts, Zugangs- und Zugriffsschutz
- Bedeutung der Datensicherung und gegebenenfalls deren Durchführung
- E-Mail- und Internet-Sicherheit
- Schutz vor Schadprogrammen
- Sicherheitsaspekte relevanter IT-Systeme und Anwendungen
- Rechtliche Aspekte
- Verhalten bei Sicherheitsvorfällen
    - Erkennung von Sicherheitsvorfällen
    - Meldewege und Ansprechpartner
    - Verhaltensregeln im Verdachtsfall

Die hier angegebenen Themen stellen lediglich eine Auswahl dar. Ein Schulungsmodul "Informationssicherheit am Arbeitsplatz" sollte stets den individuellen Gegebenheiten der Institution angepasst sein.

**Modul 3: Anforderungen, Gesetze und Regularien**

Dieses Schulungsmodul soll den rechtlichen Anforderungsrahmen, in dem Informationssicherheit innerhalb der Institution zu betrachten ist, für die Mitarbeiter umreißen.

Hierzu zählen Sicherheitsanforderungen, die sich ergeben können aus:

- Verträgen (z. B. mit Kunden, Lieferanten, Outsourcing-Partnern, Kreditgebern)
- regulatorischen Anforderungen, einschlägigen Gesetzen, Vorschriften, Informationssicherheitsstandards und -richtlinien, etc.
- sonstigen Anforderungen der Institution (z. B. bewusste Marktdifferenzierung, Produktstrategie, Sicherheitsimage etc.)

Es ist wichtig, Mitarbeiter nicht nur auf die Einhaltung relevanter Anforderungen zu verpflichten, sondern ihnen diese auch nahe zu bringen sowie Hintergründe und Auswirkungen zu erläutern.

Relevante Anforderungen können je nach Branche und Land, in dem eine Institution tätig ist, sehr unterschiedlich sein. Eine wichtige Komponente stellen die Standards und Richtlinien zur Informationssicherheit und ihre konkrete Umsetzung in der Institution dar, da hier erfahrungsgemäß schon eine Reihe der übrigen Anforderungen verarbeitet wurde.

Beispielhafte Themen sind:

- Datenschutz in der Institution
  - Rolle und Aufgabe des Datenschutzbeauftragten
  - Datenschutzgesetze
  - Organisationspflichten
  - Umgang mit personenbezogenen Daten durch Mitarbeiter, z. B. Zusammenhang mit Protokoll-Dateien
- Arbeitsschutz
  - Rolle des Arbeitsschutzbeauftragten
  - Regelungen zu Bildschirmarbeitsplätzen
- Rechtliche oder regulatorische Vorgaben mit Bezug zur Informationssicherheit, soweit sie für die Institution relevant sind, wie z. B. PCI DSS, Basel III, etc.
- Gesetze und Normen zur technischen Infrastruktur
  - Brandschutz, Klimatisierung, Verkabelung, Blitzschutz, etc.
- Juristische Haftungsrisiken und IT-Nutzung
  - Nutzung oder Angebot von TK- oder Internetdiensten
  - Haftung des Unternehmens nach außen (z. B. KonTraG, Schäden durch Schadsoftware)
  - Haftung bei der Privatnutzung von IT-Komponenten
  - Rechtsrahmen bei der Mitarbeiterüberwachung
- Sonstige rechtliche Rahmenbedingungen
  - Ausfuhrbestimmungen für IT-Produkte, z. B. bei Verschlüsselung
  - digitale Signaturen und ihre rechtliche Stellung
  - Lizenz- und Urheberrecht für Software
- Umgang mit Angriffen auf interne IT
  - Strafbarkeit im Bereich Hacking
  - Gesetzlich zulässige Abwehrmaßnahmen
  - Verfolgung von Hacker-Straftaten

**Modul 4: Sicherheitskonzept der Institution**

Dieses Schulungsmodul vertieft die im Modul 2 behandelten Themen. Darüber hinaus soll es die System- und Aufgabenverantwortlichen in die Lage versetzen, an der permanenten Anpassung des Sicherheitskonzeptes aufgrund technischer, organisatorischer oder rechtlicher Änderungen mitzuwirken.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- detaillierte Kenntnis der Anforderungen und Risiken, die als Basis für das Sicherheitskonzept dienen

- spezifische Risiken und Sicherheitsmaßnahmen des Sicherheitskonzeptes aus den Bereichen Management, Organisation, Infrastruktur, IT-Betrieb und Mitarbeiter
- Anpassung dieser Sicherheitsmaßnahmen an neue technische, organisatorische und rechtliche Gegebenheiten
- Revision und Aufrechterhaltung des Sicherheitskonzeptes

**Modul 5: Risikomanagement**

Dieses Schulungsmodul zeigt Verantwortlichen, wie sie Risiken der Informationssicherheit systematisch analysieren, bewerten und behandeln können.

- Definitionen und Beispiele zu den Begriffen: Gefährdung, Bedrohung, Schwachstelle, Risiko, Sicherheitsziel
- Typische Gefährdungen und Bedrohungen:
    - Höhere Gewalt: Feuer, Wasser, Explosion, Sturm, Erdbeben, Blitzschlag, Streik, Demonstration, etc.
    - Organisatorische Mängel: fehlende oder unzureichende Regelungen, ungeeignete Rechtevergabe, unkontrollierter Einsatz von IT-Systemen, Umgang mit sensiblen Informationen / Datenträgern etc.
    - Menschliche Fehlhandlungen: Irrtum, Nachlässigkeit, Neugier, Unwissenheit, etc.
    - Technisches Versagen: Stromausfall, Ausfall der Klimaanlage, Überspannung, Ausfall von Schaltelementen oder Schaltkreisen, Störungen in der Mechanik oder Elektronik, etc.
    - Vorsätzliche Handlungen: Schadprogramme, Diebstahl, Sabotage, Spionage, Manipulation, Vandalismus, Hacking und Cracking inklusive Gegenüberstellung von Angreifertypen und Motivationen, z. B. bei Innentätern oder bei Angreifern von außen
- Risikomanagement
    - Begriffe zum Risikomanagement: Risikoanalyse, -bewertung, -behandlung, -akzeptanz, Restrisiko
    - Erstellung einer Gefährdungsübersicht
    - Ermittlung zusätzlicher Gefährdungen
    - Gefährdungsbewertung
    - Identifizierung und Bewertung der Risiken
    - Risikobehandlung (Reduktion, Vermeidung, Übernahme, Transfer)
    - Umgang mit Restrisiken

**Modul 6: Sicherheitsmanagement**

Dieses Schulungsmodul zeigt wichtige Grundlagen dafür auf, wie Verantwortliche Informationssicherheit in der Institution umsetzen können. Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Sicherheitsmanagement
    - Ziel und Aufgaben
    - Prozess (Informationssicherheitsmanagementsystem, ISMS) und Strategie (Leitlinie)
    - Bereitstellung von Ressourcen
    - Organisation und Verantwortlichkeiten
    - Standards wie ISO/IEC 2700x, IT-Grundschutz, ITIL, CobiT etc.
    - Durchführen von Reviews, Audits, Managementbewertungen
    - Planung und Umsetzung von Verbesserungsmaßnahmen
    - Einbindung der Mitarbeiter
- Sicherheitskonzept
    - Ziele und Inhalte eines Sicherheitskonzeptes

  - Aufbau eines Sicherheitskonzeptes
  - Verpflichtung von Mitarbeitern, System- und Aufgabenverantwortlichen zur Umsetzung des Sicherheitskonzeptes
- System- und anwendungsspezifische Sicherheitsrichtlinien
- Berechtigungsmanagement
  - Berechtigungskonzepte, Gestaltung der Rechtevergabe
  - Zugriffsrechte auf Systemressourcen, Zuweisung und zeitliche Begrenzung
  - Authentisierung (z. B. Stärken und Auswahl von Mechanismen)
  - Remote Zugriff (z. B. bei Telearbeit)
- Sensibilisierung und Training zur Informationssicherheit
  - Ausarbeitung passender Programme entsprechend den Rahmenbedingungen der Institution
- Evaluierung und Zertifizierung im Bereich Informationssicherheit
  - Produkt-/System-Zertifizierung (z. B. nach ITSEC, Common Criteria usw.)
  - Zertifizierung des Sicherheitsmanagements (z. B. nach IT-Grundschutz)
  - Experten-Zertifikate (z. B. TISP, CISA, CISSP, IT-Sicherheitskoordinator, Security+ usw.)
- Spezielle Probleme in der Informationssicherheit
  - Kommunikation mit Management und Fachabteilung
  - Kosten- und Akzeptanzprobleme

**Modul 7: IT-Systeme**

Dieses Schulungsmodul beschreibt die Steuerungsinstrumente, die in den verschiedenen Phasen des Lebenszyklus von IT-Systemen gewährleisten, dass die Sicherheitsnormen eingehalten werden.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Sicherheitsmaßnahmen in den Lebenszyklus-Phasen
  - Planung
  - Beschaffung/Entwicklung
  - Test und Evaluierung
  - Implementierung bzw. Installation
  - produktiver Betrieb
  - Aussonderung
  - Notfallvorsorge
- Sicherheitsplanung für den Systembetrieb
  - Feststellung des Einsatzzweckes und -nutzens eines bestimmten IT-Systems
  - Festlegung der Schutzmaßnahmen für dieses System
  - Bestimmung der für den Systembetrieb Verantwortlichen
  - Installation und Konfiguration der in jeder Phase des Lebenszyklus erforderlichen Sicherheitsmechanismen
- Festlegung von Konfigurations-, Patch- und Änderungsmanagement in Abhängigkeit von den Sicherheitszielen
- Festlegung der Freigabekriterien für den operativen Betrieb
- Tests und Freigabe der Sicherheitsmechanismen

**Modul 8: Operativer Bereich**

Dieses Schulungsmodul beschreibt die Prozeduren und Maßnahmen, die operationelle Systeme und Anwendungen schützen sollen.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Infrastruktur-Maßnahmen
  - Zugangskontrollen, Werkschutz, Alarmanlagen, etc.
  - Haustechnik, Energie- und Wasserversorgung, etc.
  - Brandschutzeinrichtungen
  - Klimaanlagen
- Organisatorische Maßnahmen
  - Dokumentation von Systemen und Konfigurationen, Applikationen, Software, Hardware-Bestand, etc.
  - Regelmäßige Kontrolle von Protokolldateien
  - Regelungen für die Datensicherung
  - Regelungen für den Datenträgeraustausch
  - Lizenzverwaltung und Versionskontrolle von Standardsoftware
- Maßnahmen im Bereich Personal
  - Auswahl, Einarbeitung und Schulung von Mitarbeitern
  - Geregelte Verfahrensweise beim Weggang von Mitarbeitern
  - Funktionen und Verantwortlichkeiten
  - Funktionstrennung und funktionsbezogene Rechtevergabe
  - Vertretungsregelungen
  - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Maßnahmen im Bereich Hardware und Software
  - Grundlagen Betriebssystem-Sicherheit
  - Sichere Konfiguration von Hardware und Software
  - Schutz vor Schadprogrammen
  - Nutzung der in der Hardware bzw. den Anwendungsprogrammen vorhandenen Sicherheitsfunktionen
  - Implementierung zusätzlicher Sicherheitsfunktionen
  - Rechteverwaltung
  - Protokollierung
- Maßnahmen im Bereich Kommunikation
  - Sichere Konfiguration von TK-Anlagen und Netzdiensten
  - E-Mail- und Internet-Sicherheit
  - Absicherung externer Remote-Zugriffe
  - Virtual Private Networks (VPN)
  - Sichere Nutzung mobiler IT-Systeme und drahtloser Kommunikation
  - Information über Sicherheitslücken (z. B. über CERTs) und Umgang mit Sicherheitsvorfällen

**Modul 9: Technische Realisierung von Sicherheitsmaßnahmen**

Dieses Schulungsmodul vermittelt Kenntnisse über die Möglichkeiten der technischen Realisierung der in den Modulen 6 bis 8 abstrakt beschriebenen Steuerungs- und Kontrollinstrumente.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Basiswissen Kryptographie
  - Problemabgrenzung Vertraulichkeit, Integrität, Authentizität

  - Grundbegriffe wie Klartext, Chiffrat, Schlüssel
  - Symmetrische, asymmetrische und hybride Verschlüsselung
  - Public Key Infrastrukturen
  - Digitale Signaturen
  - Aufzählung "guter" und "schlechter" bekannter Algorithmen
- Identifizierung und Authentikation, z. B.
  - Begriffsdefinition (Wissen, Besitz, Eigenschaft)
  - Authentisierung durch Wissen: Passwörter, Einmal-Passwörter, Challenge-Response-Verfahren, digitale Signaturen
  - Authentisierung durch Besitz: Token, Chipkarten, z. B.
  - Biometrische Verfahren: Fingerabdruckerkennung, Handvenenerkennung, Iriserkennung, Gesichtserkennung, z. B.
  - Single Sign-On
  - Berechtigungsmanagement
- Protokollierung und Monitoring, z. B.
  - Technische Möglichkeiten des "Transaction Logging"
  - Intrusion Detection, Response und Prevention Systeme (IDS, IRS, IPS): Unterschiede zwischen aktiven und passiven Systemen
  - Zwangsprotokollierung aller Administratoraktivitäten
  - Datenschutzaspekte
- Überblick über Administrationswerkzeuge
  - Werkzeuge, mit denen Sicherheitsvorgaben realisiert und kontrolliert werden können
  - Zusatzprodukte zur Ergänzung bzw. Verbesserung der Sicherheitsfunktionen von Betriebssystemen ("gehärtete Betriebssysteme")
  - Netzmanagement-Software
  - Remote-Management-Software
- Firewalls (Sicherheitsgateways)
  - Internet-Technik (OSI-Modell, TCP/IP)
  - Realisierungsformen (statische Paketfilter, Stateful Inspection, Application Level Gateways)
  - Content Security
  - Hochverfügbare Firewalls
- Schutz der Vertraulichkeit: Kryptografische Verfahren und Produkte, Zugriffsschutz z. B. durch Festplattenverschlüsselung, Kryptografie auf den verschiedenen Schichten des OSI-Modells
  - Protokolle für Schicht 1 und 2 (ISDN-Verschlüsselung, ECP und CHAP, WLAN, Bluetooth )
  - Protokolle für Schicht 3 IPSec, IKE, SINA)
  - Protokolle für Schicht 4 und höher SSL, TLS, S/MIME)
- Schutz der Verfügbarkeit
  - Organisatorische Maßnahmen zur Erhöhung der Verfügbarkeit SLAs, Change Management, Vermeidung von SPOF)
  - Datensicherung, Datenwiederherstellung
  - Speichertechnologien
  - Netzkonfigurationen zur Erhöhung der Verfügbarkeit
  - Infrastrukturelle Maßnahmen zur Erhöhung der Verfügbarkeit
  - Verfügbarkeit auf der Client, Server und Anwendungsebene (Server-Standby, Failover)
  - Methoden zur Replikation von Daten
  - Wiederanlauf- und Geschäftsfortführungsmaßnahmen

- Technische Möglichkeiten zum Schutz von TK-Anlagen
    - Schutz vor Abhören
    - Schutz der Datenleitungen z. B. durch alarmüberwachte und plombierte Leitungsschächte, gesicherte Verteiler (Knoten), Verschlüsselung der Nachrichten, etc.
    - Sicherung von Wartungs-, Fernwartungs-, und Administratorenzugängen
    - Protokollierung jedes Systemzugangs, Löschungsschutz der Protokolldateien
- Erkennen von Schwachstellen des eigenen Systems mittels Penetrationstests
- Hacker-Methoden, Web-Seiten-Hacking, Schutz vor: Sniffer, Scanner, Password Cracker, etc.

**Modul 10: Notfallmanagement**

Dieses Schulungsmodul soll die Grundlagen zur Etablierung und Aufrechterhaltung eines Notfallmanagements in der Institution vermitteln. Thematisch stellt es einen Aufbaukurs zum Modul 5 "Risikomanagement" dar. Die Schulungsinhalte können gemäß der Struktur des BSI-Standards 100-4 aufgebaut werden.

Folgende Inhalte sollten vorgesehen und entsprechend den Inhalten des BSI-Standards 100-4 weiter detailliert werden:

- Einführung: Ziel, Aufgaben, Begriffe, Abgrenzung von Business Continuity und IT Service Continuity, Standards
- Der Prozess im Überblick
- Initiierung des Prozesses
- Konzeption
- Umsetzung des Notfallvorsorgekonzepts
- Notfallbewältigung und Krisenmanagement
- Tests und Übungen

**Modul 11: Neue Entwicklungen im IT-Bereich**

Dieses Schulungsmodul soll IT-Systembetreiber über Innovationen auf ihrem Gebiet informieren. Um stets auf dem aktuellen Stand zu sein, sollte dieses Seminar in regelmäßigen Abständen von etwa zwei Jahren wieder besucht werden. Alternativ können der angesprochenen Zielgruppe auch die Ressourcen bereitgestellt werden, um sich aus verfügbaren Informationsquellen entsprechend selbstständig zu informieren.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Hardware-Architekturen, Schnittstellen, Bussysteme, Peripherie
- Speicher-/Archivierungstechnologien und -systeme
- Hochverfügbarkeitslösungen
- Client- / Server-Betriebssysteme
- Software-Architekturen
- Terminal Server, N-Tier, Host versus Client/Server
- Datenbanken
- Cloud Computing
- Mobile Computing
- Data Warehouse, SharePoint, etc.
- Netztechnologie
- Informationssicherheit, insbesondere neue Bedrohungen und Schwachstellen zu allen angesprochenen Themen

**Modul 12: Betriebswirtschaftliche Seite der Informationssicherheit**

Dieses Schulungsmodul ist speziell für das Management und Entscheidungsträger gedacht, um Informationssicherheit übergreifend in die Planung der Institution zu integrieren.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Betriebswirtschaftliche Vorteile der Informationssicherheit
  - Risikominimierung
  - Beschleunigung der Bearbeitung
  - Reduzierung des Aufwands
  - Umsatzerhöhung
  - Erschließen neuer Geschäftsfelder
  - sonstiger Nutzen
- Kalkulation der Investitionen für Informationssicherheit
  - Erstellung einer Kostenübersicht
  - Abgrenzung gegenüber Betriebs- und Fortschreibungskosten
  - Verdeckte Kosten
- Investitionsrechnung in der Informationssicherheit
  - Investitionsrechnung
  - Argumentation gegenüber dem Management
- Verzahnung von Sicherheitsmaßnahmen im Unternehmen
  - Berücksichtigung der Geschäftsprozesse und der Geschäftsvorfälle bei den Sicherheitsmaßnahmen
  - Einfluss- und Verantwortungsbereiche, typische Stolpersteine
  - Informationssicherheit bei der IT-Beschaffung und in IT-Projekten
- Erfolgsfaktoren der Informationssicherheit
  - Wie gelingt ein Projekt zur Informationssicherheit?
  - Klärung der Erwartungshaltung
  - Konzeption von Sicherheitslösungen
  - Erstellen eines Konzepts
  - Gliedern in Teilprojekte
  - Umsetzen der Teilprojekte
  - Modul- und Funktionstests
  - Akzeptanz- und Integrationstests
  - Inbetriebnahme
- Häufige Fehler bei der Umsetzung von Informationssicherheit
  - Fehler bei der Projektleitung
  - andere typische Fehler

**Modul 13: Infrastruktursicherheit**

Dieses Modul befasst sich mit dem Schutz der Informationstechnik mit Hilfe von baulichen und technischen Maßnahmen. Wichtige Punkte dabei sind unter anderem:

- Objektschutz
  - Absicherung des Standortes: Umgebung, Umfriedung, Freilandschutz, Nachbarschaftsgefahren, Zonenbildung
  - Bautechnik: Einbruchschutz, Brandschutz, Schutz gegen Wasser, etc.
  - Technische Überwachung
  - Geräteschutz

- Zutrittskontrolle
    - Pförtnerdienst
    - Verschluss von Räumen
    - Technische Zutrittskontrolle
- Stromversorgung
    - Überspannungsschutz
    - Unterbrechungsfreie Stromversorgung
    - Trassen / Verkabelung
- Brandschutz
- Klimatechnik

Prüffragen:

- Ist gewährleistet, dass alle Mitarbeiter entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden?
- Werden die Schulungsinhalte zur Informationssicherheit regelmäßig auf Aktualität überprüft und bei geändertem Schulungsbedarf angepasst?
- Sind die Schulungsinhalte zur Informationssicherheit entsprechend den existierenden Zielgruppen, Aufgaben und Verantwortlichkeiten der Mitarbeiter strukturiert und geplant?

# M 3.46 Ansprechpartner zu Sicherheitsfragen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

In jeder Institution sollte es Ansprechpartner für Sicherheitsfragen geben, sowohl für scheinbar einfache wie auch für technische Fragen. Das können IT-Administratoren, IT-Anwendungsverantwortliche oder IT-Sicherheitsbeauftragte sein (siehe auch M 2.12 *Betreuung und Beratung von IT-Benutzern* und M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

Oft ist die Hemmschwelle, konkrete Sicherheitsvorfälle zu melden, hoch. Wenn der IT-Sicherheitsbeauftragte den Mitarbeitern jedoch bereits als Ansprechpartner zu allgemeinen Fragen der Informationssicherheit bekannt ist, kann dies die Bedenken abbauen, konkrete Sicherheitsprobleme zu melden.

Die Institution sollte den Mitarbeitern zudem glaubhaft kommunizieren, dass die Meldung von Sicherheitsvorfällen sich nicht negativ für sie auswirkt und sie auffordern, jeden Verdacht eines Sicherheitsvorfalls zeitnah und notfalls anonym zu melden.

Da viele Sicherheitsfragen bei der privaten Nutzung von IT-Systemen auftreten, sollten IT-Sicherheitsbeauftragte auch zu vermeintlich nicht dienstlichen Belangen Informationen weitergeben, z. B. zur Problematik von Computer-Viren und Trojanischen Pferden bei der Internet-Nutzung oder zum Schutz von persönlichen Daten beim E-Commerce. Dadurch werden die Mitarbeiter gegenüber Sicherheitsmaßnahmen offener und der IT-Sicherheitsbeauftragte wird mehr akzeptiert. Zudem können viele vermeintlich private Probleme auch im Büro auftreten.

Allen Mitarbeitern sollten die Ansprechpartner zu Sicherheitsfragen ebenso wie die Meldewege für Sicherheitsvorfälle bekannt sein. Hierzu könnte z. B. im internen Telefonverzeichnis oder im Intranet eine Liste mit Namen, Telefonnummern und E-Mail-Adressen der jeweiligen Ansprechpartner veröffentlicht werden.

Prüffragen:

- Gibt es Ansprechpartner zu Sicherheitsfragen innerhalb der Behörde oder des Unternehmens?
- Sind die Ansprechpartner zu Sicherheitsfragen allen Mitarbeitern bekannt?

# M 3.47 Durchführung von Planspielen zur Informationssicherheit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Sicherheitsschulungen empfinden Teilnehmer oft als trocken. Dadurch wird der gewünschte Lerneffekt häufig nicht erreicht. Eine gute Möglichkeit, den Lernstoff aufzulockern, sind Plan- oder Rollenspiele. An solche Spiele erinnern sich die Teilnehmer meist länger und prägnanter als an klassische Folienpräsentationen. Auch tragen sie dazu bei, die Bedrohungen stärker zu verdeutlichen und typische Schwachstellen, aber auch Lösungsmöglichkeiten in der eigenen Arbeitsumgebung aufzuzeigen. Sie ermöglichen es den Teilnehmern, Situationen zu üben, um dann im Ernstfall routinierter zu agieren.

Planspiele können aus praktischen Beispielen, z. B. anhand aktueller Vorfälle aus den Medien, selbst zusammengestellt oder bei Schulungsdienstleistern in Auftrag gegeben werden. Dabei sind die Inhalte der Planspiele möglichst an die eigene Institution anzupassen. Dadurch können sich die Mitarbeiter besser mit den aufgezeigten Lösungen identifizieren. Durch die Simulation z. B. von Sicherheitsvorfällen, die geschäftskritische Prozesse beeinträchtigen können, sind die Mitarbeiter im Ernstfall bestens vorbereitet.

Genau wie bei Schulungen ist die zielgruppengerechte Planung von Inhalten auch hier sehr wichtig. Die Teilnehmer sollen die Relevanz der Rollenspiele erkennen und in ihrem Arbeitsumfeld unmittelbar davon profitieren können.

Bei allen Bemühungen, die Mitarbeiter auf die Bedeutung von Informationssicherheit aufmerksam zu machen, sollte eine positive und konstruktive Grundstimmung bewahrt werden. Ständige Angst vor Sicherheitsvorfällen kann einerseits zur Verdrängung von Sicherheitsproblemen und andererseits zu Panikreaktionen verleiten.

Die folgenden Beispiele zeigen, dass Planspiele von sehr einfach zu realisierenden Übungen, die im Rahmen einer Schulung durchgeführt werden können, bis hin zu komplexen Simulationsübungen reichen können. Die Aufgabe der verantwortlichen Planer ist es nun, entsprechend den Erfordernissen der unterschiedlichen Zielgruppen die geeigneten Szenarien zu entwickeln.

**Tragen von Mitarbeiterausweisen**

Durch kurze Rollenspiele können Mitarbeiter sehr gut üben, wie sie sich verhalten sollen, wenn sie innerhalb der Institution organisationsfremde Personen antreffen. Es kann eingeübt werden, wie die Mitarbeiter optimal auf diese Situation reagieren können, beispielsweise indem sie anbieten, die Externen "zu ihrer besseren Orientierung" zum Gesprächspartner zu begleiten. Auch der Umgang mit Besuchern, die die Hausregeln kennen, aber verweigern, kann trainiert werden, beispielsweise wenn ein Besucher das Tragen eines Ausweises ablehnt, weil er persönlich mit dem Geschäftsführer bekannt sei.

**Social-Engineering-Attacken**

Im Rahmen von Simulationen können Mitarbeiter üben, wie sie sich bei Social-Engineering-Attacken verhalten sollen. Dazu werden die ausgewählten Zielgruppen wie z. B. IT-Betreuer und verschiedene Administratorengruppen in einer gemeinsamen Simulation mit vermeintlich harmlosen Anfragen kon-

frontiert. Erst durch das fachübergreifende Betrachten dieser Anfragen wird deutlich, dass hier ein Angriff vorliegt. Ziel der Simulation ist es, diese Zusammenhänge durch entsprechende Übungen herauszufinden, um im Anschluss in definierter Art und Weise reagieren zu können. Diese Art von Simulation lässt sich in der Praxis sehr gut durch Workshops mit Moderationsmaterialien wie Pinnwand und Moderationskarten durchführen.

**Simulationsübungen**

Besonders wichtig sind Simulationen, in denen die Behandlung von Sicherheitsvorfällen bis hin zu Notfallsituationen geübt wird. Sie sollen Mitarbeiter in die Lage versetzen, zugeordnete Rollen und Verantwortlichkeiten innerhalb eines Szenarios auch unter erschwerten Bedingungen (Anspannung, Häufung von Anweisungen, unklare oder oft wechselnde Sachlage, Ressourcenmangel, Kommunikationsprobleme etc.) möglichst sicher wahrzunehmen. Das Ziel von Simulationen liegt primär im Training persönlicher Fähigkeiten anhand repräsentativer Szenarien, die dann in möglichst vielen Vorfallssituationen genutzt werden können. Daher sollte eine Simulation von einem erfahrenen Trainer geleitet werden, der nach ihrer Durchführung im Rahmen eines Reviews mit den Teilnehmern ihre Erfahrungen diskutiert und vertieft (siehe M 6.117 *Tests und Notfallübungen*).

Prüffragen:

- Werden schwierige Situationen in Planspielen trainiert?
- Sind Sensibilisierungs- und Schulungsinhalte auf die sinnvolle Unterstützung durch Planspiele geprüft worden?

# M 3.48 Auswahl von Trainern oder externen Schulungsanbietern

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Personalabteilung

Die Verantwortlichen für Sensibilisierungs- und Schulungsprogramme müssen klären, ob und in welchem Umfang sie eigene Mitarbeiter oder externe Anbieter als Trainer einsetzen wollen. Außerdem muss die Form der Ausbildung festgelegt werden.

Wenn eigene Mitarbeiter als Trainer eingesetzt werden sollen, müssen diese das benötigte Fachwissen haben und dazu fähig sein, dieses Wissen auch zielgruppengerecht zu vermitteln. Neben den erforderlichen Informationssicherheitskenntnissen müssen die Trainer über ausgeprägte didaktische und kommunikative Fähigkeiten verfügen. Speziell für Sensibilisierungsmaßnahmen sind außerdem ausreichende Kenntnisse über die Institution, deren Sicherheitskultur sowie die Geschäftsprozesse der Zielumgebung erforderlich. Wichtig ist auch, dass Trainer die Sprache ihres jeweiligen Zielpublikums beherrschen, also die zu schulenden Informationssicherheitsaspekte in die jeweiligen Arbeits- und Projektzusammenhänge stellen können. Interne Trainer müssen die erforderliche Zeit bekommen, um Sensibilisierungs- und Schulungsmaßnahmen nicht nur durchführen, sondern auch vorbereiten und auswerten zu können.

Aus Kosten- oder Qualifikationsgründen kann es zumindest zu Beginn vorteilhafter sein, die Schulung durch externe Fachkräfte durchführen zu lassen. Dann ist zu klären, welche finanziellen Ressourcen dafür verfügbar sind. Die externen Trainer sollten sorgfältig anhand der oben genannten Kriterien ausgewählt und auf ihre Aufgabe vorbereitet werden. Insbesondere müssen ihnen die erforderlichen institutionsinternen Hintergründe vermittelt werden.

Auch bei externer Durchführung von Sensibilisierungs- oder Schulungsmaßnahmen sind interne Ressourcen erforderlich. Es muss ein verantwortlicher Schulungskoordinator benannt werden, der

- qualifizierte Schulungsanbieter auswählt,
- Lerninhalte und -methoden vorgibt sowie den Trainern erforderliche Informationen zur Verfügung stellt,
- die interne Schulungsplanung, -vorbereitung und -durchführung koordiniert,
- die Kommunikationsschnittstelle zwischen Trainern und eigenen Mitarbeitern bildet,
- die Teilnehmerbewertungen analysiert und geeignete Verbesserungsmaßnahmen festlegt, gegebenenfalls zusammen mit den Trainern.

Die Schulungskoordination kann der IT-Sicherheitsbeauftragte oder auch ein Mitarbeiter aus der Personalabteilung übernehmen. Der IT-Sicherheitsbeauftragte und die Personalabteilung müssen hierbei auf jeden Fall eng zusammenarbeiten.

Erfahrungsgemäß gibt es eine Reihe von externen Anbietern, die geeignete Sensibilisierungs- oder Schulungsmaßnahmen in einer Form anbieten, die den Bedürfnissen der Institution entsprechen oder die mit vertretbarem Aufwand angepasst werden können.

Bei Sensibilisierungs- oder Schulungsmaßnahmen, die in mehreren Zyklen eine größere Zahl von Mitarbeitern erreichen sollen, bietet es sich an, über ein "Train the Trainer"-Konzept nachzudenken. Hierbei werden die initialen Maßnahmen entweder von geeigneten internen Mitarbeitern oder externen Trainern mit dem Ziel durchgeführt, dass die Teilnehmer dieser Maßnahmen später selbst eine Trainerrolle übernehmen. Dies kann für diese Mitarbeiter einen sehr positiven Effekt auf ihre eigene Sensibilisierung und Motivation für Informationssicherheit haben. Darüber hinaus können sie ihre eigenen Erfahrungen in die Trainingsmaßnahmen einbringen. Gerade bei Trainingsthemen, die Aspekte der Kultur und bestimmter Verhaltensweisen innerhalb der Institution beinhalten, kann ein interner Trainer aufgrund seiner tieferen Kenntnis interner Prozesse und Bekanntheit bei den Teilnehmern die Akzeptanz und den Lernerfolg des Trainings erhöhen. Sofern das "Train the Trainer"-Konzept eingesetzt werden soll, müssen die initialen Maßnahmen neben den vorgesehenen Fachinhalten auch Anleitungen zur methodisch-didaktischen Lernstoffvermittlung beinhalten.

Prüffragen:

- Wurden für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit geeignete Trainer ausgewählt?
- Wurde ein Schulungskoordinator ernannt?
- Sind die Angebote verschiedener Schulungsanbieter daraufhin verglichen worden, welche inhaltlich, qualitativ und preislich am besten geeignet sind?
- Werden die durchgeführten Sensibilisierungs- oder Schulungsmaßnahmen von den Teilnehmern bewertet und diese Erfahrungen regelmäßig intern ausgewertet?

# M 3.49 Schulung zur Vorgehensweise nach IT-Grundschutz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

IT-Sicherheitsverantwortliche müssen die IT-Grundschutz-Methodik gut kennen, um sie erfolgreich anwenden zu können. Es gibt verschiedene Möglichkeiten, um sich in die Vorgehensweise nach IT-Grundschutz einzuarbeiten:

- Selbststudium
- Web-Kurs des BSI zum Einstieg in die IT-Grundschutz-Vorgehensweise
- Durcharbeiten der BSI-Beispielunterlagen des fiktiven Unternehmens RECPLAST
- Externe Schulungsanbieter von IT-Grundschutz-Schulungen (Auf den BSI-Webseiten findet sich eine Liste von Schulungsanbietern zum Thema IT-Grundschutz. Das BSI hat dabei Schulungsqualität und Schulungsinhalte nicht bewertet.)
- Erarbeitung eigener IT-Grundschutz-Schulungen.

Wenn eine neue IT-Grundschutz-Schulung geplant wird oder eine extern angebotene Schulung zu beurteilen ist, sollten die folgenden Themen betrachtet werden:

- Sensibilisierung für Informationssicherheit
- Was ist ein Informationssicherheitsmanagementsystem (ISMS) ?
  Wie wird ein funktionierender Sicherheitsprozess etabliert?
- Überblick über das IT-Grundschutzkonzept (Philosophie, Anwendungsgebiet, Struktur)
- Erstellung einer Leitlinie zur Informationssicherheit
  - Definition von Informationssicherheitszielen
  - Definition des Informationsverbundes
- Informationssicherheitsmanagement
  - Organisationsstrukturen (Darstellung geeigneter Organisationsstrukturen für das Informationssicherheitsmanagement)
  - Rollen (IT-Sicherheitsbeauftragte, Sicherheitsmanagement-Team, etc.)
  - Verantwortlichkeiten
- Sicherheitskonzept: typischer Aufbau und Inhalte
- Strukturanalyse
  - Gruppenbildung
  - Erfassung der Anwendungen und der zugehörigen Informationen
  - Erstellung eines Netzplans
  - Erhebung der IT-Systeme
  - Erfassung der Räume
- Schutzbedarfsfeststellung
  - Vorgehensweise
  - Definition der Schutzbedarfskategorien inklusive individueller Anpassung der Bewertungstabellen
  - Schadensszenarien
  - Schutzbedarfsfeststellung für Anwendungen, IT-Systeme Kommunikationsverbindungen und Räume
- Modellierung nach IT-Grundschutz
  - Überblick über die IT-Grundschutz-Bausteine

    - Schichtenmodell
        - Übergeordnete Aspekte der Informationssicherheit
        - Sicherheit der Infrastruktur
        - Sicherheit der IT-Systeme
        - Sicherheit im Netz
        - Sicherheit der Anwendungen
    - Prüfung auf Vollständigkeit
    - Lebenszyklusmodell der Maßnahmen
- Basissicherheits-Check
    - Darstellung der Vorgehensweise
    - Umsetzungsstatus
- Ergänzende Sicherheitsanalyse: Risikoanalyse basierend auf IT- Grundschutz
- Realisierung der Sicherheitsmaßnahmen
    - Sichtung aller fehlenden Maßnahmen
    - Konsolidierung der Maßnahmen
    - Kosten und Aufwandsabschätzungen (Budgetierung)
    - Realisierung der Maßnahmen (Umsetzungsreihenfolge, Verantwortliche, Realisierungsplan)
- Hilfsmittel zur Arbeit mit den IT-Grundschutz-Katalogen
  Das BSI stellt verschiedene Hilfsmittel zur Verfügung, die die praktische Arbeit mit den IT-Grundschutz-Katalogen erleichtern. Die Folgenden sollten den Anwendern vorgestellt werden:
    - Leitfaden als Motivation für Informationssicherheit
    - Webkurs als Einstieg in die IT-Grundschutz-Vorgehensweise
    - Tabellen und Formblätter als Hilfsmittel bei der Umsetzung
    - Musterrichtlinien und Profile als Beispielanwendungen
    - Tool-Unterstützung bei der Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten auf der Basis von IT-Grundschutz. Diverse Hersteller bieten hierfür geeignete IT-Grundschutz-Tools an.
- Kurzvorstellung der ISO 27001
    - Die Standardfamilie ISO 2700x
    - Aufbau des Standards ISO 27001
    - Zuordnung der Normkapitel von ISO 27001 zu den BSI-Standards sowie der Themen im Anhang A zu den Bausteinen der Schicht 1
- Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz: Überblick Zertifizierungsschema

In einer umfassenden IT-Grundschutz-Schulung sollten die Teilnehmer die dargestellte Vorgehensweise anhand von Beispielen üben.

Zur Gestaltung neuer IT-Grundschutz-Schulungen wird unter den Hilfsmitteln auf den BSI-Webseiten zu IT-Grundschutz ein Foliensatz zur Verfügung gestellt. Dieser kann benutzt werden, um eigene Schulungen hierauf aufzubauen. Alle Lehrinhalte werden in Übersichten und Struktogrammen kurz angeschnitten. Es wird aufgezeigt, welche Inhalte eine Schulung beinhalten sollte, die in die Vorgehensweise IT-Grundschutz und die Anwendung der IT-Grundschutz-Kataloge einführen soll.

Prüffragen:

- Sind die Sicherheitsverantwortlichen mit der IT-Grundschutz-Methodik vertraut?

- Werden bei der Planung einer IT-Grundschutz-Schulung die Themen der Schulung vorher festgelegt?
- Wird in der IT-Grundschutz-Schulung die Vorgehensweise auch anhand von Beispielen geübt?

# M 3.50 Auswahl von Personal

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Bereits bei der Formulierung der Anforderungen sollten die erforderlichen Qualifikationen und Fähigkeiten genau beschrieben sein. Ob diese bei Bewerbern tatsächlich vorhanden sind, sollte zunächst anhand der Unterlagen nachgeprüft, anschließend im Gespräch geklärt werden.

Personen, die sicherheitsrelevante Aufgaben ausüben sollen (beispielsweise Sicherheitsverantwortliche, Datenschutzbeauftragte, Administratoren, Mitarbeiter mit Zugang zu finanzwirksamen oder vertraulichen Informationen), müssen vertrauenswürdig und zuverlässig sein (siehe hierzu auch M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*).

Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die die Aufgabenerfüllung gefährden. Interessenkonflikte können insbesondere dann auftreten, wenn ein Mitarbeiter gleichzeitig verschiedene Rollen inne hat, die ihm zu weitreichende Rechte geben oder sich ausschliessen. Außerdem sollten die Aufgaben von Mitarbeitern auch nicht von Interessenkonflikten außerhalb der Behörde oder des Unternehmens beeinträchtigt werden, beispielsweise durch frühere Stellen oder durch anderweitige Verpflichtungen. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, können Konkurrenzverbote und Karrenzzeiten vereinbart werden.

Soweit die fachlichen Qualifikationen in Teilbereichen noch nicht ausreichend vorhanden sind, müssen Mitarbeiter die Gelegenheit bekommen, diese zu erweitern. Um die erforderlichen Qualifikationen und Fähigkeiten zu erhalten und zu aktualisieren, sollten alle Mitarbeiter regelmäßig geschult werden und auf die Bedeutung von Informationssicherheit hingewiesen werden (siehe auch Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit*).

Auch bei der Auswahl von Mitarbeitern für befristete Stellen oder Dienstleistern sollten diese Punkte berücksichtigt werden.

Prüffragen:

- Sind die Anforderungen an die Qualifikationen und Fähigkeiten des auszuwählenden Personals schriftlich fixiert?
- Werden etwaige Interessenkonflikte bei der Auswahl von Mitarbeitern beachtet?

# M 3.51 Geeignetes Konzept für Personaleinsatz und -qualifizierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Für jeden Mitarbeiter sollten die am Arbeitsplatz wahrzunehmenden Aufgaben dokumentiert sein: "Jeder sollte wissen, was er zu tun hat". Die Aufgaben sind so zu definieren, dass keine Überschneidungen entstehen, damit es keine Probleme mit Zuständigkeiten gibt. Die Mitarbeiter müssen alle für ihr Aufgabengebiet relevanten Ansprechpartner kennen. Dazu gehören insbesondere alle, die ähnliche Aufgaben erledigen oder die sie bei Bedarf unterstützen. Beispielsweise sollten Mitarbeiter wissen, wer für den IT-Support zuständig ist, damit einerseits Probleme unmittelbar nach dem Auftreten abgestellt werden können und andererseits kein Mitarbeiter auf falsche Support-Mitarbeiter hereinfällt (siehe G 5.42 *Social Engineering*). Zusätzlich müssen geeignete Vertreter benannt sind.

Die Rollen, die ein Mitarbeiter wahrnehmen soll, müssen klar definiert sein. Darauf aufbauend sind alle erforderlichen Berechtigungen zu vergeben (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter* und M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Alle Mitarbeiter sind für die Erfüllung ihrer Aufgaben ausreichend zu schulen sowie für mögliche Gefährdungen und richtiges Verhalten zu sensibilisieren. Dies schließt insbesondere den sorgfältigen Umgang mit Informationen und IT-Systemen entsprechend ihrem Schutzbedarf sowie die Kenntnis der relevanten Sicherheitsrichtlinien ein. Hierfür ist ein angemessenes Sensibilisierungs- und Schulungskonzept zu erstellen (siehe Baustein B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit*).

Prüffragen:

- Sind die Aufgabengebiete der Mitarbeiter schriftlich fixiert?
- Ist die Vertreterregelung erfasst?
- Sind den Mitarbeitern die Zuständigkeitsbereiche der Kollegen innerhalb der Institution bekannt?
- Besteht ein Sensibilisierungs- und Schulungskonzept für die Mitarbeiter?

# M 3.52 Schulung zu SAP Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Vorgesetzte

Ein SAP System ist sowohl in der Administration und im Betrieb als auch in der Benutzung komplex. Alle Personen, die mit einem SAP System arbeiten, müssen daher zwingend geschult werden. Dies gilt in besonderem Maße für Administratoren.

**Schulungen**

Schulungen zu allen SAP Themen und Produkten werden von SAP selbst und von Dritten angeboten. Das Spektrum reicht dabei von Schulungen, die für Personen geeignet sind, die SAP Systeme in ihrer normalen Büroarbeit nutzen - also ausführliche, applikationsspezifische Inhalte abdecken - bis hin zu Schulungen, die für die Ausbildung von Administratoren geeignet sind und ausführliche technische Inhalte abdecken. Für große Unternehmen oder Behörden mit vielen Mitarbeiten ist es sinnvoll, eigene Schulungsvarianten zu entwickeln und intern anzubieten.

Die Schulungsinhalte sind dem Nutzungsspektrum der zu schulenden Personen anzupassen. Ein Teil der Schulung sollte immer auch sicherheitsrelevante Themen ansprechen, so dass eine Sensibilisierung für den sicheren Umgang mit SAP Systemen erfolgt.

Es empfiehlt sich, in regelmäßigen Abständen das Bewusstsein für die Sicherheit aufzufrischen (Security-Awareness-Programm) und auf veränderte oder neue Situationen, Mechanismen oder Verfahren hinzuweisen. Generell ist es wichtig, dass das Sicherheitsbewusstsein im Lauf der Zeit von einer rein informellen Einstellung zu einer proaktiven verändert wird.

**Online-Informationen**

SAP stellt online umfangreiche Informationen zu den angebotenen Produkten und Lösungen zur Verfügung. Alle Informationen sind über das Internet verfügbar (siehe M 2.346 *Nutzung der SAP Dokumentation*).

Administratoren sollten diese Informationsquellen regelmäßig nutzen, um sich insbesondere über die Java-basierten Technologien zu informieren. Dabei sollten speziell die sicherheitsrelevanten Themen Beachtung finden.

Prüffragen:

- Sind alle Personen, die mit dem SAP System arbeiten, ausreichend zum sicheren Umgang mit SAP geschult?
- Informieren sich die SAP Administratoren regelmäßig über sicherheitsrelevante Themen im Umgang mit SAP Systemen?

# M 3.53 Einführung in SAP Systeme

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Leiter IT

**Kernkomponenten einer SAP Systeminstallation**

Eine SAP Systeminstallation besteht vereinfacht dargestellt aus folgenden Kernkomponenten:

- SAP NetWeaver ApplicationServer
  Der SAP NetWeaver ApplicationServer führt die SAP Applikationen oder Module aus.
- Datenbank-Instanz
  Die Datenbank-Instanz hält die Datenbank, in der alle Daten des SAP Systems gespeichert werden.
- SAP Clients
  Die SAP Clients bestehen aus dem SAPGui oder einem normalen Browser.

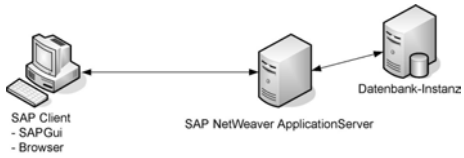



Abbildung: SAP Systemüberblick

Der SAP NetWeaver ApplicationServer besteht generell aus zwei Komponenten: dem ABAP-Stack und dem Java-Stack. Hier werden je nach verwendeter Programmiersprache die eigentlichen Funktionen der Applikationen und Module ausgeführt.

**ABAP-Stack**

Der ABAP-Stack ist die traditionelle Ausführungsumgebung eines SAP Systems. Dies trifft insbesondere auf die Systemversionen zu, die allgemein mit dem Begriff SAP R/3 bezeichnet werden, da die R/3 Komponenten und Module im ABAP-Stack ausgeführt werden.

Der ABAP-Stack besteht aus der so genannten SAP Basis, einer Sammlung aus (ABAP-) Programmen und Funktionen, die die Grundfunktionalitäten (z. B. Benutzerverwaltung) implementieren. Zusätzlich können dann weitere ABAP-Programme installiert werden. Diese sind in anwendungsspezifischen Modulen (z. B. HCM, FI) zusammengefasst. Die Programme des ABAP-Stack werden über so genannte Transaktionen gestartet. Dabei ist nicht jedem ABAP-Programm eine Transaktion zugeordnet. Vielmehr existieren Transaktionen, die Programme aufrufen, die den Start von anderen Programmen erlauben (z. B. Transaktion SE38, Start von Programmen).

**Java-Stack**

Der Java-Stack besteht aus einzelnen so genannten System-Diensten, die die System-Funktionen des Java-Stacks implementieren. Zusätzlich können weitere Dienste und Applikationen installiert werden, um den Funktionsumfang zu erweitern. Applikationen können dabei auf die Funktionen der unterschiedlichen Dienste zugreifen. Auf die Dienste, Funktionen und Applikationen des Java-Stack wird in der Regel über Internet-basierte Protokolle (z. B. HTTP) zugegriffen.

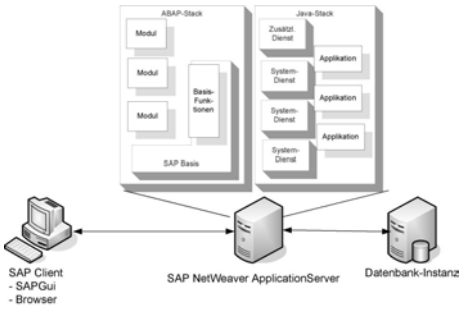



Abbildung: ABAP und Java Stack eines SAP Systems

**Instanzen**

Damit SAP Systeme auch mit großen Benutzerzahlen umgehen können, besteht die Möglichkeit, ein SAP System aus mehreren einzelnen so genannten Instanzen von NetWeaver ApplicationServern (insgesamt dann Cluster genannt) aufzubauen. Diese tragen die Benutzerlast dann gemeinsam und bilden aus Client-Sicht ein einziges SAP System. Die Arbeitsverteilung zwischen den einzelnen Servern erfolgt durch systeminterne Mechanismen. Eine der Instanzen ist die Hauptinstanz und wird auch Zentral-Instanz genannt. Die Zentral-Instanz kann durch weitere Installationen von SAP NetWeaver ApplicationServern um weitere Instanzen erweitert werden. Die einzelnen Instanzen kommunizieren miteinander, damit der Cluster von den Clients als ein SAP System wahrgenommen wird.

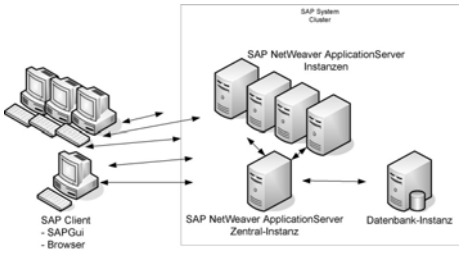



Abbildung: SAP Instanzen

**Mandanten und DDIC**

Der ABAP-Stack ist verwaltungstechnisch in so genannte Mandanten gegliedert. Zusätzlich existiert das so genannte Data Dictionary (DDIC), in dem alle Objekte des ABAP-Stacks gehalten werden. Die wichtigsten sind die Tabellen, die ABAP-Programme sowie sonstige in ABAP-Programmen verwendete Objekte. Mandanten stellen eine in sich geschlossene Menge von Benutzern, Funktionen und Tabellen dar. Zugriffe zwischen Mandanten sind in der Regel nicht möglich. Eine Ausnahme bilden hier die so genannten mandanten-unabhängigen Objekte (z. B. Tabellen), die von jedem Mandanten aus zugegriffen werden können. Änderungen an solchen Objekten wirken sich dann auf alle anderen Mandanten aus.

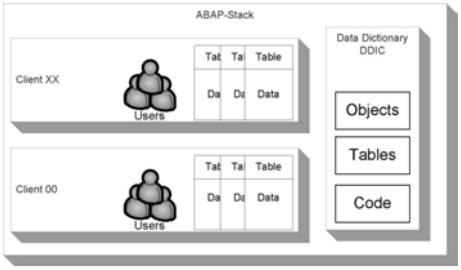



Abbildung: Mandanten eines SAP Systems

**Benutzer**

In Bezug auf Benutzer unterscheidet der ABAP-Stack zwischen unterschiedlichen Benutzerarten: solche mit eigenem Benutzerstammsatz und solche ohne eigenen Benutzerstammsatz. Da Benutzer mit eigenem Benutzerstammsatz über die Transaktion SU01 verwaltet werden, werden diese Benutzer oft auch SU01-Benutzer genannt. Im Gegensatz dazu ist so genannten Internet-Benutzern kein eigener Benutzerstammsatz zugeordnet. Internet-Benutzer wurden bisher über die Transaktion SU05 verwaltet. Dieses Vorgehen ist von SAP mittlerweile nicht mehr empfohlen. Vielmehr ist empfohlen, auch Internetbenutzer über die Transaktion SU01 anzulegen und einen Verweis auf einen so genannten Referenzbenutzer einzutragen, der auch von unterschiedlichen Internet-Benutzern referenziert werden kann. Für SU01-Benutzer können in Abhängigkeit von der Verwendung folgende Typen spezifiziert werden, die mit unterschiedlichen Einschränkungen verbunden sind:

- Dialog-Benutzer: Der Benutzer darf sich interaktiv am SAP System anmelden (Dialoganmeldung).
- System-Benutzer: Eine Dialoganmeldung am SAP System ist nicht möglich. Der Benutzer kann für die Hintergrundverarbeitung (Batch-Jobs) verwendet werden.
- Kommunikations-Benutzer: Der Benutzer kann die technischen Kommunikationsarten (z. B. Remote Function Call, RFC) nutzen. Eine Dialoganmeldung am SAP System ist nicht möglich.
- Service-Benutzer: Der Benutzer wird als technischer Benutzer eingesetzt. Eine Dialoganmeldung ist möglich.
- Referenz-Benutzer: Der Benutzer dient als Referenz für Internet-Benutzer. Eine Anmeldung am System ist nicht möglich.

**SAP Informationsquellen**

SAP Systeme sind komplex und bestehen aus vielen Komponenten. Um Betreiber von SAP Systemen mit Hinweisen und Empfehlungen zu den SAP Produkten zu unterstützen, nutzt SAP die so genannten SAP Hinweise (SAP Notes). Diese werden über eindeutige Nummern identifiziert und können über den SAP Service Marketplace (siehe M 2.346 *Nutzung der SAP Dokumentation*) abgerufen werden.

# M 3.54 Schulung der Administratoren des Speichersystems

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Ein Speichersystem ist die Instanz, die viele oder gar alle immateriellen Werte der Institution trägt. Zudem wird die Administration von Speichersystemen mit steigender Funktionalität immer komplexer und erfordert stets aktuelle Kenntnisse. Deswegen ist es unerlässlich, dass die Administratoren des Speichersystems ausreichend geschult sind, damit sie in der Lage sind, Probleme aus eigenem Handeln heraus zu vermeiden, technische Probleme rechtzeitig zu erkennen und die Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der Komponenten des Speichersystems notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Über Kenntnisse der grundlegenden IT-Technik hinaus gilt dies auch für herstellerspezifische Aspekte zu einzelnen Produkten, die als Komponenten des Speichersystems eingesetzt werden. Das bedeutet, dass beim Einsatz von neuen Produkten die Administratoren speziell zu diesen Produkten nachgeschult werden müssen.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein ausreichendes Budget eingeplant werden und ein Schulungsplan für Administratoren erstellt werden. Die Inhalte einer Schulung sollten die folgenden Punkte umfassen:

- Grundlagen zu Speichersystemen und Speichernetzen
  - Überblick über Netze und Protokolle
  - Aufbau von Massenspeichersystemen
  - Funktionsweise eines Storage Area Network (im Fall eines SAN-Einsatzes)
  - SAN-Switching (im Fall eines SAN-Einsatzes)
  - Datensicherung von Massenspeichern
- Einrichtung von Speichersystemen und Speichernetzen
  - Zusammenbau und Verkabelung
  - Einrichtung und Konfiguration von Speichereinheiten, SAN- Switches und Backup-Geräten
- Betrieb von Speichersystemen und Speichernetzen
  - Management der Geräte, Software-Werkzeuge
  - Integration in Netzmanagementsysteme (NMS)
  - Protokollierung
  - Einstellung, Verwaltung und Sicherung der Konfiguration.
- Fehlerbehebung bei Speichersystemen und Speichernetzen
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge
  - Teststrategien zur Fehlersuche
- Informationssicherheit bei Speichersystemen und Speichernetzen
  - Grundlagen der Informationssicherheit sowie relevante Sicherheitsaspekte
  - Virenschutz
  - Authentisierung, Autorisierung

- Kryptoverfahren und Anwendungen
- Gefahrenquelle "Default-Einstellungen"
- Vorsorgemaßnahmen, Reaktion und Analyse
- Incident Handling
- Disaster Recovery Maßnahmen

Auch wenn in einer Gruppe von Administratoren die Aufgaben so verteilt sind, dass jeder Administrator nur einen bestimmten Verantwortungsbereich hat, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern hierfür ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Prüffragen:

- Wurden die Administratoren für Planung und Betrieb von Speichernetzen geschult?

# M 3.55 Vertraulichkeitsvereinbarungen

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Externe Mitarbeiter erhalten häufig für die Erfüllung ihrer Aufgaben Zugang zu vertraulichen Informationen oder erzielen Ergebnisse, die vertraulich behandelt werden müssen. In diesen Fällen müssen sie verpflichtet werden, diese entsprechend zu behandeln. Hierüber sollten Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) abgeschlossen werden, die vom externen Mitarbeiter unterzeichnet wird.

In einer Vertraulichkeitsvereinbarung sollte beschrieben sein,

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z. B. Vernichtung oder Rückgabe von Datenträgern,
- wie die Eigentumsrechte an Informationen geregelt sind,
- welche Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner gelten, falls dies notwendig ist,
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten.

In der Vertraulichkeitsvereinbarung kann auch auf die relevanten Sicherheitsrichtlinien und weitere Richtlinien der Organisation hingewiesen werden. In dem Fall, dass externe Mitarbeiter Zugang zu organisationsinternen IT-Infrastruktur haben, sollten diese neben der Vertraulichkeitsvereinbarung auch die Sicherheitsrichtlinien für die Nutzung der jeweiligen IT-Systeme unterzeichnen.

Eine Vertraulichkeitsvereinbarung bietet die rechtliche Grundlage für die Verpflichtung externer Mitarbeiter zur vertraulichen Behandlung von Informationen. Aus diesem Grund muss sie alle relevanten Gesetze und Bestimmungen für die Organisation in dem speziellen Einsatzbereich berücksichtigen, klar formuliert sein und aktuell gehalten werden.

Es kann sinnvoll sein, verschiedene Vertraulichkeitsvereinbarungen je nach Einsatzzweck zu verwenden. In diesem Fall muss klar definiert werden, welche Vereinbarung für welche Fälle notwendig ist.

Prüffragen:

- Werden mit Externen Vertraulichkeitsvereinbarungen getroffen, bevor sie Zugang und Zugriff auf vertraulichen Informationen erhalten?
- Werden durch die verwendeten Vertraulichkeitsvereinbarungen alle wichtigen Aspekte zum Schutz von organisationsinternen Informationen berücksichtigt?

# M 3.56 Schulung der Administratoren für die Nutzung von VoIP

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Telefonie stellt unabhängig von der TK-Anlage zugrunde liegenden Technologie die Kommunikationsbasis der Organisation dar. Deswegen ist es unerlässlich, dass die Administratoren ausreichend geschult sind, damit sie in der Lage sind, die benötigten Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der VoIP-Komponenten notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte einzelner Produkte, die als VoIP-Komponenten eingesetzt werden.

Für den effizienten Einsatz von VoIP werden ausführliche Kenntnisse über Netze benötigt. Diese müssen ebenfalls in der Schulung vermittelt werden. Oft werden die VoIP-Komponenten auf Standard-IT-Systemen mit eigenständigem Betriebssystem eingesetzt. Hinweise zu diesem Schulungsbestandteil sind in den jeweiligen IT-Grundschutz-Bausteinen zu den Betriebssystemen zu finden.

Im Allgemeinen sollten in den entsprechenden Schulungen mindestens folgende Elemente enthalten sein:

- Grundlagen zu VoIP - Kompression und Übertragung von Sprachnachrichten mit möglichen Auswirkungen wie Jitter, Delay und Echo
- Grundlagen der eingesetzten Protokolle der Anwendungsschicht (beispielsweise RTP, SIP und H 3.23)
- Administration
    - Sicherheitsrelevante Grundlagen und Konzepte der Administration, Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche für jede VoIP-Komponente. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.
    - Kenntnisse über die Administration der IT-Systeme, auf denen die VoIP-Komponenten betrieben werden sollen.
    - Überblick über relevante rechtliche Aspekte beim VoIP-Betrieb wie z. B. Datenschutz
    - Management der Geräte, Werkzeuge
    - Protokollierung
    - Sicherung und Verwaltung von Konfigurationsdaten
    - Angriffsszenarien (z. B. Denial of Service Angriffe, ARP-Spoofing, IP-Spoofing, DNS-Spoofing, Viren und andere Schadsoftware)
    - Grundlagen zum Thema Virtuelle Private Netze (VPN)
    - Grundlagen zum Umgang mit verschlüsselten Daten (Verschlüsselung z. B. mit SRTP oder IPSec) und Möglichkeiten zur Behandlung verschlüsselter Daten
- Netztechnik
    - Grundlagen der Strukturierung von Netzen und Dienstgüte
    - Grundlagen von IP und der darauf aufbauender Protokolle (IP-Adressierung, ICMP, TCP, UDP)

  - Virtuelle Netzsegmentierung (VLAN)
- Fehlerbehebung
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge, Werkzeuge zur automatischen Überprüfung der einzelnen Komponenten des Sicherheitsgateways auf korrekte Funktion
  - Teststrategien zur Fehlersuche

Auch wenn in einer Gruppe von Administratoren die Aufgaben verteilt sind, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein ausreichendes Budget eingeplant und ein Schulungsplan für alle Administratoren erstellt werden.

Prüffragen:

- Verfügen die verantwortlichen Administratoren über ausreichendes Fachwissen im Bereich VoIP?

# M 3.57 Szenarien für den Einsatz von VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für VoIP, also die Sprachübertragung über IP-Netze, gibt es unterschiedliche Anwendungsszenarien. Das Bedrohungspotenzial und die Sicherheitsanforderungen sind dementsprechend ebenfalls unterschiedlich. Im Folgenden werden derzeit typische Anwendungsfälle dargestellt.

**Einsatz von VoIP im Endgeräteanschlussbereich**

Das erste Anwendungsszenario besteht darin, VoIP für die interne Sprachkommunikation in Firmen- und Behördennetzen zu verwenden.

Dies umfasst, vollständig oder auch nur komponentenweise, den Einsatz von IP-Telefonen, eines LAN-basierten Telekommunikationssystems, das die Vermittlungs- und Mehrwertfunktionen übernimmt sowie die Verbindung in die Außenwelt sicherstellt, und eines IP-Netzes für die Verbindung von Endgeräten und TK-Anlage. Die Verbindung in das digitale Fernsprechnetz kann dabei über lokale Gateways oder über einen VoIP-Provider erfolgen. Bei so genannten "hybriden Anlagen" werden in herkömmliche TK-Anlagen VoIP-Baugruppen integriert, die den Anschluss von IP-Telefonen, meist proprietären Systemtelefonen, ermöglichen.

Ziel dabei ist die Integration der Daten- und Telefonienetze. Den möglichen Einsparungen an Leitungen, Netzkomponenten, Management, Administration und Wartung stehen allerdings zusätzliche Bedrohungen gegenüber wie z. B. das mit geringen Kenntnissen durchführbare Abhören der Datenverbindung, denen Rechnung zu tragen ist. Die erforderlichen Sicherheitsmaßnahmen relativieren einen Teil der Einsparpotenziale, insbesondere bei der Anpassung eines vorhandenen Datennetzes für den VoIP-Einsatz, sind jedoch zwingende Voraussetzung für den sicheren und verlässlichen Einsatz dieser Technologie.

**Einsatz von VoIP zur TK-Anlagen-Kopplung**

Traditionell werden TK-Anlagen überwiegend über separate Wähl- oder Standleitungen miteinander verbunden.

Eine zunehmend realisierte Anwendung von VoIP ist die Kopplung von lokalen Telekommunikationsanlagen (Trunking) über IP-Verbindungen. Dabei werden traditionelle TK-Anlagen an verschiedenen Standorten unter Nutzung eines WAN-Datennetzes gekoppelt. Die Zusammenführung von Telefonie- und Datennetz in der Standortvernetzung bietet dabei erhebliche Flexibilität, eine effizientere Bandbreitennutzung und damit auch ein Einsparpotenzial.

**Einsatz von VoIP zur Internet-Telefonie**

Ein weiteres Szenario ist die Sprachübertragung über öffentliche IP-Netze, vor allem über das Internet. Die zunehmend größeren Bandbreiten im Backbone- und Endanschlussbereich, die zu einer mittlerweile akzeptablen Sprachqualität führen, beschleunigen den Trend zur Internet-Telefonie im privaten Bereich.

Dabei können Softphones eingesetzt werden, die meist, ähnlich zu Messaging-Diensten, über zentrale Verzeichnisse registriert sind. Zunehmende Verbreitung finden kompakte und kostengünstige VoIP-Gateways, die es er-

möglichen, mit herkömmlichen Telefonen (analog oder ISDN) Internet-Telefonie-Dienste zu nutzen. Es werden aber auch kostengünstige Hardphones für eine private Nutzung von den Herstellern angeboten.

Unternehmen und Behörden nutzen die Sprachübertragung über öffentliche IP-Netze dagegen derzeit kaum. Der Hauptgrund ist, dass hier keine Mechanismen zur Verfügung stehen, um eine bestimmte Sprach- oder Übertragungsqualität zu garantieren.

# M 3.58 Einführung in WLAN-Grundbegriffe

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

WLANs können in zwei verschiedenen Architekturen betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte, die mit einer WLAN-Karte ausgestattet sind (Clients), direkt miteinander.

In den meisten Fällen wird ein WLAN im Infrastruktur-Modus betrieben, d. h. die Kommunikation der Clients erfolgt über eine zentrale Funkbrücke, den sogenannten Access Point. Über den Access Point erfolgt auch die Verbindung in kabelgebundene LAN-Segmente.

Der Infrastruktur-Modus lässt mehrere Einsatzvarianten zu:

- Mittels mehrerer Access Points können überlappende Funkzellen installiert werden, sodass beim Übergang eines Clients in die nächste Funkzelle die Funkverbindung aufrecht erhalten werden kann ("Roaming"). Auf diese Weise können große Bereiche flächendeckend versorgt werden. Die Reichweite einer Funkzelle ist extrem abhängig von den Umgebungsbedingungen und liegt im Bereich von ca. 10 bis 150 Meter.
- Zwei Access Points können auch als Brücke (Bridge) zwischen zwei leitungsgebunden LANs eingesetzt werden. Ebenso ist der Einsatz eines Access Points als Relaisstation (Repeater) zur Erhöhung der Reichweite möglich.
- Bei der Verwendung entsprechender Komponenten (Richtantennen) an den Access Points kann ein WLAN auch zur Vernetzung von Liegenschaften eingesetzt werden. Hier können laut Herstellerangaben Reichweiten im Kilometerbereich erreicht werden. Die Access Points können dabei als Relaisstation oder Brücke betrieben werden.

Im Standard IEEE 802.11 werden die Bezeichnungen Independent Basic Service Set (IBSS) für Funk-Netze im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur-Modus mit einem Access Point verwendet. Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netz wird Distribution System (DS) genannt.

Die in Deutschland und in fast allen Staaten Europas zugelassenen WLAN-Systeme nach IEEE 802.11, 802.11b und 802.11g nutzen das ISM-Frequenzband (Industrial-Scientific-Medical) zwischen 2,4 und 2,48 GHz, das gebührenfrei und ohne zusätzliche Genehmigung verwendet werden kann. Die Sendeleistung ist auf maximal 100 mW EIRP (Effective Isotropic Radiated Power) begrenzt.

Systeme des Standards IEEE 802.11 übertragen die Daten mit einer Rate von 1 bzw. 2 Mbit/s mittels Bandspreizverfahren, entweder mittels Frequenzsprung- (FHSS) oder Direct-Sequence- (DSSS) Verfahren. Der Vollständigkeit halber sei erwähnt, dass 802.11 auch eine Infrarot-Übertragung definiert, die bisher aber in der Praxis bedeutungslos geblieben ist.

Die Systeme nach IEEE 802.11b verwenden nur das DSSS-Verfahren. Die zu übertragenen Daten werden mit einem festen Code gespreizt, um die Übertragung unempfindlicher gegen Störung zu machen. Der Zugriff auf den Funkkanal erfolgt, wie bei allen Systemen der 802.11 Standards, nach einem zufallsgesteuerten Verfahren, genannt Carrier Sense Multiple Access with Col-

lision Avoidance (CSMA/CA). Die Brutto-Datenübertragungsrate beträgt bei IEEE 802.11b maximal 11 Mbit/s. Die Übertragungsraten können, wie bei allen Systemen der 802.11 Standards, nicht garantiert werden, sie hängen ab von der Anzahl der Clients und der Qualität der Funkübertragungsstrecke.

Systeme des Standards IEEE 802.11g verwenden die Übertragungstechnik Orthogonal Frequency Division Multiplexing (OFDM) nach IEEE 802.11a und erlauben daher auch Datenraten von bis zu 54 Mbit/s.

Im 2,4 GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung nach 802.11b zur Verfügung. Bei einer Kanalbandbreite von ca. 22 MHz können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden, beispielsweise die Kanäle 2, 7 und 12.

Systeme der Standards IEEE 802.11a und 802.11h nutzen den 5 GHz-Bereich. Im Frequenzbereich von 5,15 bis 5,35 GHz und bei 5,47 bis 5,725 GHz sind in Deutschland insgesamt 19 Kanäle in einem Abstand von 20 MHz unter Auflagen freigegeben worden. Bei einer Kanalbandbreite von 20 MHz werden direkt benachbarte Kanäle hier nicht gestört. Im 5 GHz Frequenzbereich arbeiten auch militärische und zivile Radar- und Navigationsanwendungen und es dürfen hier nur Systeme eingesetzt werden, die eine dynamische Frequenzwahl und eine Anpassung der Sendeleistung unterstützen.

**Überblick über Sicherheitsmechanismen**

Die Sicherheitsmechanismen aller 802.11 kompatiblen Systeme sind im Standard IEEE 802.11 definiert. Die Erweiterungen a, b, g und h des Standards bieten keine zusätzlichen Sicherheitsmechanismen, nur die Erweiterung i definiert neue Sicherheitsmechanismen. Die in IEEE 802.11 definierten Mechanismen dienen ausschließlich zur Sicherung der Funkstrecke zwischen den Clients und Access Points. Darüber hinaus lässt der Standard aber auch Freiraum für proprietäre Erweiterungen.

Sämtliche Sicherheitsmechanismen des Standards IEEE 802.11, die im Folgenden dargestellt werden, sind überwindbar und bieten keinen verlässlichen Schutz für sensible Informationen.

- Der Standard bietet die Möglichkeit einen Netznamen (ESSID bzw. SSID: (Extended) Service Set Identity) zu vergeben. Dabei gibt es zwei Betriebsarten. Wird durch den Nutzer die Kennung "Any" angegeben, akzeptiert die WLAN-Komponente beliebige SSIDs. Im anderen Fall wird der eingetragene Name überprüft und nur Teilnehmer mit der gleichen SSID können am Netz teilnehmen. Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID dazu, den nächsten Access Point zu finden. Da die SSID im Klartext über das Netz gesendet wird, kann ein Angreifer sie mit einfachen Mitteln in Erfahrung bringen. Einige Access Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden. Das Unterdrücken der SSID auf diese Weise ist jedoch nicht standardkonform.
- Jede Netzkarte verfügt über eine eindeutige Hardwareadresse, die sogenannte MAC-Adresse (Media Access Control-Adresse). Prinzipiell ist es möglich, in einem WLAN MAC-Adressen zu definieren, denen es erlaubt ist, mit einem Access Point zu kommunizieren. Die Adresslisten müssen hierfür allerdings "von Hand" gepflegt werden, was sehr aufwendig ist. In vielen Einsatzszenarien ist dies nicht möglich. Das Filtern der MAC-Adressen ist nicht im Standard enthalten. Andererseits ist die Filterung von MAC-

Adressen standardkonform, da die Filterung keine Auswirkungen auf die Kompatibilität der Clients hat.

- Vertraulichkeit, Integrität und Authentizität im WLAN sollen durch das "Wired Equivalent Privacy"-Protokoll (WEP) gesichert werden. Das WEP-Protokoll basiert auf der Stromchiffre RC4, mit der Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffratdaten umgewandelt werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder optional 104 Bit und muss den am WLAN beteiligten Clients sowie dem Access Point vorab zur Verfügung gestellt werden. Dabei wird für das gesamte WLAN ein gemeinsamer Schlüssel verwendet. Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Der IV wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und über das WLAN übertragen.
  WEP verschlüsselt nur die übertragenen Nutzdaten und die Integritätschecksumme. Management- und Steuersignale (Management- und Control-Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

Während der Entwicklung des Standards IEEE 802.11i wurde von der Wi-Fi Alliance, basierend auf dem Draft 3.0 von IEEE 802.11i, Wi-Fi Protected Access (WPA) veröffentlicht. WPA enthält bereits einige Verbesserungen der Sicherheitsmechanismen und beschreibt zum einen den Einsatz des im Wesentlichen auf dem Wired Equivalent Protocol (WEP) basierenden Temporary Key Integrity Protocol (TKIP) in Kombination mit dem Integritätsprüfungsverfahren MICHAEL zur Verschlüsselung der Datenpakete. Durch MICHAEL ist in WPA das Problem der mangelhaften Integritätsprüfung in WEP gelöst worden. TKIP und MICHAEL sind als temporäre Lösung zu verstehen, da TKIP nur optional verwendet werden kann und laut WPA-Spezifkationen nicht zwingend ist.

Im Standard IEEE 802.11i, welches bis auf einige Freiheitsgrade bei der Auswahl der EAP-Methoden dem WPA2 der Wi-Fi Alliance entspricht, wird ein anderes Verschlüsselungsverfahren fest vorgeschrieben, das CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code, CCMP). Dieses Verfahren setzt, im Gegensatz zu RC4 in WEP und WPA, den Advanced Encryption Standard (AES) zur Verschlüsselung der Authentisierungs- und Nutzdaten ein. Bei der Authentisierung wird hierbei nicht direkt der Klartext mit AES verschlüsselt, sondern ein aus dem symmetrischen Schlüssel gebildeter Zähler. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartexts mit dem AES-verschlüsselten Zähler. Außerdem wird die Methode Cipher Block Chaining (CBC) zur Integritätssicherung der Daten verwendet. Zur Schlüsselverwaltung und -verteilung wird IEEE 802.1X vorausgesetzt.

Die in IEEE 802.11i verwendete Schlüssellänge des AES-Schlüssels beträgt 128 Bit. Dieses Verfahren ist langfristig tragbar, erfordert aber - im Gegensatz zu der TKIP-Variante - neue Hardware.

Als zusätzlicher Schutz der Authentisierung kann das Extensible Authentication Protocol (EAP) gemäß Standard IEEE 802.1X verwendet werden. EAP wird im RFC 3748 genau beschrieben. Der Benutzer meldet sich hier bei einer Authentisierungsinstanz, z. B. an einem RADIUS-Server, an und dieser prüft die Zugangsberechtigung, bevor der Sitzungsschlüssel ausgetauscht wurde. EAP unterstützt eine Reihe von Authentisierungsmethoden, so dass auch Zertifikate und Zwei-Faktor-Authentisierungen genutzt werden können.

Prüffragen:

- Erfolgt in Sicherheitszonen mit hohem Schutzbedarf, die LAN benötigen, die Identifizierung und Authentisierung mittels der MAC-Adresse?

- Wird beim Einsatz von WEP, bei der Übertragung der Datenpakete, jeweils ein unterschiedlicher Initialisierungsvektor gewählt?
- Wird zur Absicherung des WLANs langfristig der Sicherheitsstandard WPA2 eingesetzt?
- Wird als zusätzlicher Schutz der Authentisierung das Extensible Authentication Protocol (EAP) eingesetzt?

# M 3.59 Schulung zum sicheren WLAN-Einsatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Beim Betrieb von WLAN-Komponenten sind eine Vielzahl von Kenntnissen sowohl über die grundlegende Funktionsweise als auch über spezielle technische Ausprägungen, aber auch über eine Vielzahl von Sicherheitsaspekten erforderlich. Daher ist es unabdingbar, dass sowohl die IT-Verantwortlichen als auch das Sicherheitsmanagement über WLAN-Grundlagen informiert sind.

**Schulung von Administratoren**

Die Administratoren für den Betrieb von WLAN-Komponenten sollten außerdem neben theoretischen auch praktische Kenntnisse besitzen. WLAN-Schulungen für Administratoren sollten unter anderem folgende Themen behandeln:

- Überblick über Sicherheitsaspekte bei WLANs
  - Typische Gefährdungen
  - SSID, Betriebsmodi, Verbindungsaufbau, Adressfilterung, Verhinderung von Spoofing, MAC-Adress-Filterung
- Auswahl geeigneter Sicherheitsmechanismen, Authentikation und Absicherung der Kommunikation
  - WEP, WPA, WPA2, IEEE 802.11i, IEEE 802.1X
  - Schlüsselmanagement in TKIP, CCMP usw.
  - Authentisierungsmechanismen im WLAN, wie z. B. EAP, RADIUS
  - Aufspüren von WLANs
- Sicherheitsmaßnahmen für den WLAN-Betrieb
  - sicherheitsrelevante WLAN-Konfigurationsparameter
  - Systemmanagement
  - Netz-Analyse-Programme und Wireless Intrusion Detection Systeme
  - VPNs für WLANs, IPSec, DHCP
  - Zusammenspiel WLANs mit Sicherheitsgateways
  - Absicherung von WLAN-Komponenten gegen unbefugten Zugriff

**Schulung von Benutzern**

Aber auch die Benutzer von WLAN-Komponenten, vornehmlich von WLAN-Clients, sind zu schulen. Dabei sollten die Benutzer die Funktionsweise und die sichere Bedienung der WLAN-Komponenten kennen lernen. Benutzern muss genau erläutert werden, was die Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem müssen sie auf die Gefahren hingewiesen werden, wenn diese Sicherheitseinstellungen aus Bequemlichkeit bzw. zur Reduktion von störenden Warnmeldungen umgangen oder deaktiviert werden. Durch eine gezielte Sensibilisierung der Benutzer kann eine ordnungsgemäße Bedienung der WLAN-Komponenten und deren Sicherheitseinstellungen erreicht werden.

**Schulung von Werkschutz und Pförtner**

Vor dem Hintergrund von Wardriving-Attacken sollte außerdem eine Sensibilisierung des Werkschutzes und der Pförtner erfolgen. So sollte der Werkschutz

darauf achten, ob sich über einen längeren Zeitraum unbekannte Personen mit Notebook und eventuell sogar WLAN-Antennen vor dem Betriebsgelände aufhalten. Bei Verdachtsfällen sollte das Sicherheitsmanagement informiert werden.

Die Schulungsinhalte müssen immer entsprechend der jeweiligen Einsatzszenarien angepasst werden. Auch Schulungen mit Hilfe von webbasierten interaktiven Programmen im Intranet sind hier denkbar. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen müssen die Mitarbeiter jedoch auch die WLAN-Sicherheitsrichtlinie ihrer Organisation vorgestellt bekommen.

Prüffragen:

- Sind Mitarbeiter als auch Werkschutz/Pförter sensibilisiert für Wardriving-Angriffe?

# M 3.60 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

In zunehmendem Umfang werden die verschiedensten Arten von mobilen Datenträgern in Behörden und Unternehmen eingesetzt. Ebenso nimmt die Zahl von Geräten zu, die neben ihrer offensichtlichen Funktion zusätzlich als mobile Datenträger eingesetzt werden können. Damit steigt sowohl die Zahl möglicher Verbreitungswege für Informationen als auch die Zahl möglicher Sicherheitslücken. Einige dieser Sicherheitsrisiken können zwar technisch minimiert werden, aber ohne eine Einbeziehung der Mitarbeiter in den sicheren und sachgerechten Umgang mit mobilen Datenträgern werden Behörden oder Unternehmen immer wieder von technischen Neuerungen überrollt werden.

Alle Mitarbeiter sollten über die Arten und Einsatzmöglichkeiten von mobilen Datenträgern und Geräten aufgeklärt werden. Dazu gehört auch, dass sie über die verschiedenen Bauformen und Varianten informiert werden, also dass beispielsweise auch ein MP3-Player ein mobiler Datenträger ist. Außerdem sollten die Mitarbeiter über potentielle Risiken und Probleme bei der Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen informiert werden. Die Mitarbeiter sollten regelmäßig über neue Gefahren und Aspekte von mobilen Datenträgern und Geräten aufgeklärt werden, z. B. über entsprechende Artikel im Intranet oder in der Mitarbeiterzeitschrift.

Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen Datenträgern und Geräten umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten. Dabei sollten beispielsweise Fragen zur Aufbewahrung außerhalb von Büro- oder Wohnräumen sowie zur Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen behandelt werden. Beschädigungen oder Verluste sollten zeitnah gemeldet werden (siehe M 2.306 *Verlustmeldung*).

Weitere Aspekte, auf die die Benutzer hingewiesen werden sollten, sind:

- welche Daten auf mobilen Datenträgern gespeichert werden dürfen und welche nicht (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*),
- wie die auf diesen mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- wie Daten auf mobilen Datenträgern sicher gelöscht werden können und wie Datenträger zu entsorgen sind.

Prüffragen:

- Werden die Mitarbeiter auf den sicheren und sachgerechten Umgang mit mobilen Datenträgern und Geräten hingewiesen?
- Existieren Vorgaben zur sicheren und sachgerechten Aufbewahrung von mobilen Datenträgern und mobilen IT-Komponenten?

# M 3.61 Einführung in Verzeichnisdienst-Grundlagen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Immer mehr Institutionen nutzen dezentrale, länderübergreifende oder gar weltweite Computer-Netze, um im Rahmen ihres Geschäftsbetriebs, ihrer Fachaufgaben oder Verfahren die benötigten Informationen auszutauschen und verteilte Anwendungen zu realisieren. Dabei müssen die Daten, aber auch die externen und internen Anwendungen vor Missbrauch geschützt werden.

Für den Datenaustausch innerhalb solcher Netze ist es von großer Bedeutung, dass eine Vielzahl von Informationen über die verschiedenen Kommunikationspartner, Benutzer und Ressourcen im Netz den Nutzern und Anwendungen, die diese benötigen, bereitgestellt werden. Dabei muss sichergestellt werden, dass nur autorisierte Nutzer und Anwendungen auf diese Informationen, wie beispielsweise Zertifikate, Eigenschaften usw., zugreifen können. Außerdem muss gewährleistet werden, dass die Informationen nicht manipuliert oder kompromittiert werden können. Nur dann ist sichergestellt, dass nur mit vertrauenswürdigen Partner Kommunikationsverbindungen aufgebaut und Daten hinreichend abgesichert ausgetauscht werden.

Vor allem, wenn viele gleichartige Informationen für verschiedene Verfahren zur Verfügung stehen sollen, sollten diese Daten effektiv und effizient verwaltet werden. Wenn diese Daten häufig abgerufen, aber selten geändert werden, sollte ein Verzeichnisdienst in das Netz integriert werden, um die Informationen in einer einheitlichen Art und Weise zu organisieren und gleichzeitig standardisierte Schnittstellen zu ihrer Nutzung anzubieten.

Darüber hinaus unterstützen Verzeichnisdienste "Single Sign-On", also Verfahren, die es ermöglichen, dass Benutzer nach nur einer Authentisierung ohne weitere Anmeldung auf weitere Ressourcen im Netz zugreifen können.

Heutige Verzeichnisdienste haben ihren Ursprung im X.500-Standard der International Telecommunication Union (ITU) zu Verzeichnisdiensten. X.500 wurde auch als ISO 9594 verabschiedet. Von diesem Standard haben aktuelle Verzeichnisdienste im Wesentlichen dessen internen Aufbau hinsichtlich Namens- und Datenstrukturen übernommen.

Ein Nachteil des X.500-Standards ist jedoch das komplexe Zugangsprotokoll des Verzeichnisdienstes, das Directory Access Protocol (DAP), welches zudem auf einem vollständigen ISO/OSI-Protokollstapel beruht. Als praktikable Alternative wurde das Lightweight Directory Access Protocol (LDAP) entwickelt, welches den Zugang zu Verzeichnisdiensten vereinfacht hat und so auch zu deren Popularität beigetragen hat. LDAP implementiert gegenüber DAP lediglich einen reduzierten Umfang an Funktionen und Datentypen und setzt auf einem TCP/IP-Stack auf.

LDAP hat sich inzwischen in der Version LDAPv3 als Industriestandard durchgesetzt und ist als Internetstandard im RFC 4511 (ehemals RFC 2251) spezifiziert. Praktisch alle Verzeichnisdienste bieten heute eine LDAP-Schnittstelle an, wenngleich daneben auch proprietäre Protokolle bzw. Schnittstellen zum Einsatz kommen.

Aufgrund des Protokolls werden Verzeichnisdienst-Server im administrativen Sprachgebrauch gelegentlich auch als LDAP-Server bezeichnet.

Verzeichnisdienste sind wie eine hierarchische Datenbank organisiert. Die hierarchische Gliederung der Objekte erfolgt in Form eines Baumes, wobei die einzelnen Knotenpunkte des Verzeichnisbaums aus den Container-Objekten bestehen, welche wiederum andere Objekte enthalten können. Die so genannten Leaf-Objekte (Blätter) stellen die Endpunkte des Verzeichnisbaums dar. Die Objekte (Einträge, Entries) bilden den "Directory Information Tree" (DIT). Jedes Objekt besitzt dabei einen eindeutigen Namen, den sogenannten Distinguished Name (DN).

Beispiel: "cn=Max Mustermann, l=Bonn, ou=BSI, o=Bund, c=DE"

Innerhalb einer Ebene können die Objekte durch den Relative Distinguished Name (RDN), z. B. "cn=Max Mustermann", unterschieden werden.

Die Objekte enthalten ihrerseits Eigenschaften (Attribute). Den Attributen werden schließlich Werte zugewiesen, zum Beispiel: "mail: max.mustermann@bsi.bund.de".

Jedem Eintrag im Directory Information Tree (DIT) ist mindestens eine Objektklasse (ObjectClass) zugeordnet, wie z. B. "objectClass inetOrgPerson". Es gibt Objektklassen, die als "Container" für weitere Einträge dienen können, und solche, die sich als "Blattobjekte" an den Enden der Äste in der Baumstruktur des DIT befinden. Der Directory Information Tree stellt innerhalb der Verzeichnisdienst-Struktur eine Grenze des Einflusses von Administratoren und somit auf den Verzeichnisdienst an sich dar.

In den Objektklassen sind Attribute definiert, die für entsprechende Einträge zur Verfügung stehen. Durch die Zuordnung der Attribute zu Objektklassen wird gesteuert, welche Attribute für die Einträge zur Verfügung stehen. Es gibt Attribute, die einen Wert erhalten müssen, und andere, die leer bleiben können. Beispielsweise kann das Attribut "mail", das in der Objektklasse "inetOrgPerson" deklariert wird, leer bleiben.

Es gibt Abhängigkeiten zwischen Objektklassen. Damit etwa die weit verbreitete Objektklasse "inetOrgPerson" verwendet werden kann, muss zunächst die Objektklasse "organizationalPerson" deklariert werden, diese wiederum braucht die Objektklasse "person" und diese die Objektklasse "top". Die im RFC 2798 definierte Objektklasse "inetOrgPerson" ist eine der meist genutzten Klassen, um in LDAP Personen in ihrem organisatorischen Umfeld darzustellen.

Die Definitionen der Objektklassen werden in einem so genannten Schema festgehalten. Ein Schema definiert jeweils Objektklassen mit ihren verbindlichen oder optionalen Attributen. Schemata werden in so genannten Schemadateien gespeichert. So ist beispielsweise die Objektklasse "inetOrgPerson" mit ihren Attributen in der Datei "inetorgperson.schema" beschrieben. Verzeichnisdienste liefern mit ihren Installationspaketen bereits eine Menge an Schemadateien mit. Nichtsdestotrotz besteht die Möglichkeit, bei Bedarf Schemata zu erweitern oder ein eigenes Schema zu entwickeln.

Sollen Veränderungen an der Definition einzelner Objektklassen vorgenommen werden, z. B. durch Erweiterung des zugehörigen Attributsatzes, so geschieht dies über eine Änderung bzw. Erweiterung des Schemas. Somit ist eine Schema Änderung gewissermaßen die sensibelste Operation überhaupt, welche an einem Verzeichnisbaum vorgenommen werden kann. Eine solche

Änderung hat Auswirkungen auf den gesamten Baum, so dass die bisherige Konzeption des Baums neu überdacht werden muss. Die Administration des Verzeichnisdienst-Schemas verlangt daher eine hohe Kompetenz im Verzeichnisdienst sowie ein sehr hohes Sicherheitsbewusstsein.

Auch wenn die Daten eines Verzeichnisdienstes in einer Datenbank gespeichert sind, besitzen Verzeichnisse einige Eigenschaften, die sie von anderen, insbesondere relationalen Datenbanken (siehe B 5.7 *Datenbanken*) unterscheiden:

- Verzeichnisdienste sind in hierarchischer Art und Weise organisiert, in denen die Objekte mit ihren Attributen als Einträge abgelegt sind. Die Objekte eines Verzeichnisdienstes bilden die realen Objekte (z. B. Benutzer oder Rechner) eines Netzes nach. Die Beziehungen der Objekte untereinander werden durch die Baumstruktur ihrer Einträge widergespiegelt.
- Verzeichnisdienste verwenden eine bestimmte genormte Struktur, die gegebenenfalls erweitert werden kann. Die Struktur wird durch das verwendete Schema definiert. Ein Schema definiert jeweils Objektklassen mit ihren verbindlichen oder optionalen Attributen. Diese Attribute können mehrwertig sein, also auch mehrere Werte annehmen.
- Verzeichnisdienste bieten einen einfachen und schnellen Weg für einfach strukturierte suchende und lesende Anfragen. Um mit einem Verzeichnisdienst in Kontakt zu treten, werden Netzprotokolle verwendet. Die meisten Verzeichnisdienste unterstützen hierzu das Lightweight Directory Access Protocol (LDAP), genutzt werden häufig aber auch proprietäre Protokolle und Software-Schnittstellen.
- Verzeichnisdienste stellen ein fein-granulares Sicherheitsmodell bereit. Zugriffsrechte können beispielsweise für einen Eintrag definiert werden und dann für alle darunter liegenden Einträge im Verzeichnisbaum übernommen werden.
- Verzeichnisdienste sind zwar Datenbanken, unterstützen aber keine verteilten Transaktionen oder Rollback-Operationen (Zurücksetzen). Zugunsten einer höheren Verfügbarkeit in einer verteilten Umgebung können weder Objekte noch ihre Attribute für eine Änderung gesperrt werden. Zumindest zeitliche Inkonsistenzen zwischen Datenbank-Repliken werden dafür in Kauf genommen.

Gegenüber hierarchischen Datenbanken, wie sie typischerweise für Verzeichnisdienste Verwendung finden, bieten relationale Datenbanken u. a. folgende Merkmale:

- Mit der Abfragesprache SQL sind komplexere Möglichkeiten von Operationen, wie z. B. "Aggregation" zur Zählung und "Join" zur Verknüpfung gegeben.
- Die Daten liegen in einer Normalform vor, es gibt keine mehrwertigen Attribute.
- Relationale Datenbanken sind für zusammengesetzte und konkurrierende Schreiboperationen aufgrund von Locking-Mechanismen und Transaktionen geeignet.

Verzeichnisdienste sind für kurze Verbindungen und einfache Abfragen beispielsweise zur Existenz von Ressourcen, Werten von Attributen oder Lesen von ganzen Objekten prädestiniert.

Aus dieser Gegenüberstellung folgt daher, dass Verzeichnisdienste beispielsweise nicht für eine Personalverwaltung eingesetzt werden sollten, auch wenn viele Attribute von Personen innerhalb einer Institution von dem Verzeichnisdienst zur Verfügung gestellt werden. Dazu gehören z. B. die Zuordnung von Benutzern zu Telefonnummer, E-Mail-Adresse, Abteilung, aber auch zu

Login-Namen, Passwörtern oder Zertifikaten. Andere Eigenschaften wie Gehaltsstufe, Kontonummer, Urlaubstage oder Arbeitszeitvereinbarungen sind hingegen Daten der Personalverwaltung, die nicht Bestandteil eines Verzeichnisdienstes sein sollten.

Somit können einzelne, für den Verzeichnisdienst relevante Daten auch über andere relationale Datenbanken einer Institution, wie im obigen Beispiel die Datenbank für die Verwaltung der Personaldaten, gepflegt werden. Dadurch können Abhängigkeiten zwischen der Datenbank des Verzeichnisdienstes und anderer Datenbanken entstehen. Im Rahmen der Datensicherung und auch bei der Notfallvorsorge ist daher darauf zu achten, von welchen anderen Datenbanken der Verzeichnisdienst seine Einträge erhält.

**Zugriffsrechte und Vererbung**

Jedem einzelnen Objekt und jeder Objektklasse eines Verzeichnisdienstes können Zugriffsrechte auf die einzelnen Attribute des Objektes erteilt werden. Die explizite Zuweisung erfolgt dabei durch Eintragung von Rechteinhabern in die Access Control List (ACL). Mögliche Rechte reichen dabei von Supervisor, d. h. einem vollständigen Administrationsrecht, bis hin zum Browsen, was das Durchlaufen des entsprechenden Verzeichnisbaum-Abschnittes gestattet. Die Zugriffsrechte auf die Objekte vererben sich dabei standardmäßig in der Baumhierarchie von oben nach unten. Einfluss auf den Vererbungsprozess kann durch das Einführen von Filtern genommen werden, die auch die automatische Vererbungen explizit unterbinden können.

**Effektive Rechte**

Letztendlich kommen beim Verzeichnisdienst-Zugriff die effektiven Rechte eines Benutzers bzw. einer Benutzergruppe zum tragen. Die effektiven Rechte werden dabei dynamisch bei jedem einzelnen Zugriff berechnet und basieren auf den dem Benutzer bzw. der Benutzergruppe zugewiesenen Rechten.

**Authentisierung**

Die Benutzer greifen über geeignete Client-Software auf den Verzeichnisdienst zu. Der Zugriff der Clients auf den Verzeichnisdienst erfolgt dabei über proprietäre Protokolle, dabei wird der private Schlüssel des sich anmeldenden Benutzers vom Verzeichnisdienst verschlüsselt an den Client geschickt. In den Verschlüsselungsvorgang wird das Benutzerpasswort einbezogen. Gibt der Benutzer sein Passwort ein, kann der Client den privaten Schlüssel entschlüsseln. Zwischen dem Client und dem Verzeichnisdienst-Server findet ein so genanntes Challenge-Response-Verfahren zur Authentisierung statt. Nach erfolgreicher Authentisierung besitzt der Benutzer die für ihn definierten Zugriffsrechte auf den Verzeichnisdienst.

**LDAP-Zugriff**

Netzapplikationen und Internet-Benutzer greifen in der Regel über das LDAP-Protokoll (Lightweight Directory Access Protocol) auf den Verzeichnisdienst zu. Hierbei gibt es verschiedene Anbindungsarten, wie beispielsweise den "anonymous bind" oder den "proxy user anonymous bind". In der Voreinstellung hat der anonyme Login dabei die Rechte des anonymen Benutzers. Standardmäßig besitzt dieser uneingeschränkte Lese-Rechte auf den gesamten Verzeichnisbaum. Eine Authentisierung ist für die anonyme Anmeldung nicht erforderlich, dies sollte bei weiteren Sicherheitsbetrachtungen berücksichtigt werden.

Die Passwort-Authentisierung kann so konfiguriert werden, dass das Passwort entweder im Klartext übertragen werden darf oder nicht. Passwörter sollten nie im Klartext übertragen werden. Für eine gesicherte Anbindung mittels Lightweight Directory Access Protocol steht das Secure Sockets Layer Protokoll (SSL-Protokoll) wahlweise mit ein- oder zweiseitiger Authentisierung zur Verfügung.

**Zertifikatsserver**

Ein Zertifikatsserver spielt eine wichtige Rolle für die Rechtevergabe und damit für die Systemsicherheit. Ebenso hängen die Authentisierungen im Netz sowie der Aufbau eines verschlüsselten Kanals (via Secure Sockets Layer, SSL) vom Zertifikatsmanagement ab. Daher erfordert der Zertifikatsserver eine besonders sorgfältige Administration.

**Partitionierung**

Zur Verbesserung der Skalierbarkeit und Leistungsfähigkeit des Verzeichnisdienstes empfiehlt sich eine Partitionierung der Verzeichnisdatenbank auf mehrere Server. Für die Partitionierung sind eine Reihe von Regeln zu beachten, wie beispielsweise bereits innerhalb M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst* beschrieben.

**Replikation**

Verzeichnisdienste unterstützen verschiedene Arten von Replikationen zur Erhöhung der Fehlertoleranz und des Systemdurchsatzes. Aspekte der Replikation sind auch in M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst* beschrieben.

# M 3.62 Schulung zur Administration von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für die Administration eines Verzeichnisdienstes werden detaillierte Kenntnisse über die Technologie, über grundlegende Konzepte sowie über das eingesetzte Produkt benötigt. Sind solche Kenntnisse nicht vorhanden, kann dies leicht zu Fehlkonfigurationen mit erheblichen sicherheitstechnischen Auswirkungen für die Institution führen. Daher sind ausreichende Schulungen der entsprechenden Administratoren auf diesem Gebiet obligatorisch.

**Schulungsinhalte**

Die Administration eines Verzeichnisbaums wird im Allgemeinen, je nach Größe des Netzes, nicht von einem einzelnen Administrator, sondern von einer ganzen Reihe von Administratoren mit speziellen Aufgaben und Tätigkeitsbereichen durchgeführt. Insoweit besteht auch nicht für alle Administratoren eines Verzeichnisses der gleiche Schulungsbedarf. Zur Gewährleistung eines sicheren Betriebes muss jedoch jeder Administrator über ein hinreichendes Grundwissen auch der zugrunde liegenden Betriebssysteme verfügen, damit er seine eigenen Tätigkeiten in einen Gesamtkontext einordnen kann.

Schulungsinhalte sollten in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern. Wie tief sich ein Administrator mit den einzelnen Aspekten beschäftigen muss, hängt von seinem späteren Tätigkeitsfeld und dessen Qualifikation ab.

1. **Grundwissen über Authentisierung**

   - Überblick über Grundbegriffe der Informationssicherheit, die bei Verzeichnisdiensten benötigt werden wie Vertraulichkeit, Integrität und Verfügbarkeit
   - Verfahren zur Identifizierung und Authentisierung, Erläuterungen von Begriffsdefinition wie Wissen, Besitz, Eigenschaft
   - Aufzeigen allgemeiner Möglichkeiten zur Authentisierung mittels Wissen wie Passwörter, Einmal-Passwörter, Challenge-Response-Verfahren, digitale Signaturen etc. und Sensibilisierung zum Umgang mit Authentisierungsmerkmalen
   - Aufzeigen allgemeiner Möglichkeiten zur Authentisierung mittels Besitz wie Token, Chipkarten, Magnetstreifenkarten etc.
   - Aufzeigen von möglichen biometrischen Verfahren zur Authentisierung wie Fingerabdruckerkennung, Iriserkennung, Gesichtserkennung etc.
   - Vor- und Nachteile von Single-Sign-On-Produkten (SSO-Produkt)
   - Anforderungen an die Einsatzumgebung eines SSO-Produktes, wie beispielsweise der Arbeitsplatz des Administrators
   - Übersicht über Sicherheitsfunktionalitäten des eingesetzten SSO-Produktes
   - Allgemeine datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten, z. B. Problemdarstellung Datenschutz, Veröffentlichung von Klarnamen, Rechtliche Einordnung von Verzeichnisdiensten, Beschäftigtendaten in Verzeichnisdiensten
   - Allgemeine Aspekte und Hinweise zum Berechtigungsmanagement

2. **Allgemeine Grundlagen von Verzeichnisdiensten**

- Funktionsweisen eines Verzeichnisdienstes
- Überblick über die Sicherheitsmechanismen allgemeiner Verzeichnisdienste, Sicherheitsverwaltung
- Baumstruktur und Namensauflösung
- Vererbung innerhalb des Verzeichnisbaums
- Authentisierungsmethoden innerhalb eines Verzeichnisdienstes
- notwendiger physikalischer Schutz aller Verzeichnisdienst-Server inklusive Replikationen

3. **Verzeichnisdienst**

- Allgemeines: Was ist bei der Planung, Einrichtung, Administration zu berücksichtigen?
- Schema-Verwaltung
- Partitionierung
- Replikation, z. B. verwendete Mechanismen zur Replikation, voreingestellte Parameter zur Replikation von Verzeichnisdienst-Inhalten, Problematik der dezentralen Administration des Verzeichnisdienstes im Zusammenhang mit Replikationskonflikten
- Backup, z. B. Problematik des Erstellens eines Backups von Verzeichnisdiensten, Wiedereinspielen von Backups eines Verzeichnisdienst-Servers, zu ergreifende Maßnahmen beim Ausfall von Verzeichnisdienst-Servern, die die Baumstruktur definieren
- Rechtevergabe, z. B. Vergabe von Zugriffsrechten auf Verzeichnisdienst-Objekte auf Attributsebene, Vererbung von Zugriffsrechten und Blockade der Vererbung, effektive Zugriffsrechte, rollenbasierte Administration, Delegation von administrativen Aufgaben
- Rechtevererbung und Kalkulation der effektiven Rechte

4. **Grundlagen produktspezifischer / spezieller Verzeichnisdienste**

- produktspezifische Funktionsweise des Verzeichnisdienstes
- produktspezifische Authentisierungsmethoden des Verzeichnisdienstes

5. **Public Key Infrastruktur (PKI)**

- Funktionsweise einer PKI
- Zertifikate und Zertifikatstypen
- Was ist bei der Planung einer PKI zu berücksichtigen?
- Interaktion mittels PKI
- Administration des Zertifikatsservers

6. **Secure Sockets Layer (SSL)**

- Grundlegende Funktionsweise des SSL-Protokolls
- Konfiguration von SSL

7. **Lightweight Directory Access Protocol (LDAP)**

- LDAP-Zugriff auf den Verzeichnisdienst
- mögliche Anbindungen der Benutzer

8. **Administrations- und Clientsoftware**

- Übersicht zu Administratorverantwortlichkeiten, die für den sicheren Betrieb eines SSO-Produktes erforderlich sind
- Übersicht möglicher Fehlermeldungen, welche für den Administrator von Bedeutung sind
- Übersicht möglicher Administratorprivilegien
- Funktionsweise der Administrations- und Clientsoftware
- Authentisierung der Administrations- und Clientsoftware

Wenn bei der Planung von Verzeichnisdiensten Entscheidungen über rollenbasierte Administration sowie die Delegation von Administrationsaufgaben getroffen wurden, müssen die Administratoren auch entsprechend für ihre jeweilige Aufgabe geschult werden. Besonderer Augenmerk liegt dabei auf der Gruppe der Schema-Administratoren, da diese in der Lage sind, das gesamte Datenbankdesign des Verzeichnisbaums zu verändern.

Die Administration der Verzeichnisdienst-Clientsoftware und des LDAP-Zugriffs setzt detaillierte Kenntnisse über die Konfigurationsmöglichkeiten des Systems voraus. Dabei spielt auch das zugrunde liegende Betriebssystem eine Rolle für die Definition einer Sicherheitsumgebung, insbesondere der Dateisystemsicherheit.

Prüffragen:

- Wurden alle Administratoren in Hinblick auf die vom Verzeichnisdienst verwendeten Sicherheitsfunktionalitäten des zugrunde liegenden Betriebssystems geschult?
- Wurden alle Administratoren im Umgang mit den relevanten client- und serverseitigen Sicherheitsmechanismen bezüglich des Verzeichnisdienstes geschult?
- Wurden alle Administratoren im Rahmen der Rollen-basierten Administration und Delegation zusätzlich speziell für ihre Aufgaben geschult?

# M 3.63 Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, Vorgesetzte

Die Authentisierung ist ein wesentlicher Aspekt beim sicheren Betrieb von Verzeichnisdiensten. Dabei sollte sich sowohl der Client gegenüber dem Verzeichnisdienst-System authentisieren, als auch der Benutzer gegenüber dem Client. In manchen Einsatzszenarien für Verzeichnisdienste sollten sich auch der Client gegenüber dem Benutzer und der Server gegenüber dem Client authentisieren, um eine gemeinsame Vertrauensstellung zu gewährleisten. War die Authentisierung erfolgreich, so erhält der Benutzer einen automatisierten Zugriff auf sämtliche für ihn zugängliche Objekte und Services (so genannte Background Authentication). Auf diese Weise wird beispielsweise ein Single Sign-On realisiert.

Da Single-Sign-On (SSO) auf Basis eines Verzeichnisdienstes überwiegend in Verbindung mit Token, Chipkarten, Magnetstreifenkarten oder Systemen zur Fingerabdruck-, Iris- oder Gesichtserkennung realisiert werden, sollen nachfolgende Stichpunkte einen Überblick über notwendige Schulungsinhalte aufzeigen.

Nachfolgende Stichpunkte fassen notwendige Schulungsinhalte für Benutzer zusammen, welche in Hinblick auf einer sicheren Authentisierung mit Hilfe von Verzeichnisdiensten adressiert werden sollten:

- Einführung in die Sicherheitsthematik "Identifizierung und Authentisierung ", Erläuterungen von Begriffsdefinition wie Wissen, Besitz und Eigenschaft
- Sensibilisierung der Benutzer zum Umgang mit Authentisierungsmerkmalen, z. B. Passwörtern und PINs
- Korrekter Einsatz eventuell anderer vorhandener Möglichkeiten zur Authentisierung wie Token, Chipkarten, Magnetstreifenkarten oder biometrischer Verfahren zur Authentisierung wie Fingerabdruckerkennung, Iriserkennung, Gesichtserkennung, etc.
- Umgang mit den Lese- oder Erkennungsgeräten, z. B. Erkennen von sicherheitstechnischen Veränderungen an einem Chipkarten-Lesegerät
- Allgemeine Aspekte und Hinweise zum Berechtigungsmanagement
- Übersicht möglicher Endanwender-Privilegien
- Allgemeine datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten (z. B. Problemdarstellung Datenschutz, Veröffentlichung von Klarnamen, Rechtliche Einordnung von Verzeichnisdiensten, Beschäftigtendaten in Verzeichnisdiensten)
- Anforderungen an die Einsatzumgebung des eingesetzten Verzeichnisdienst-Produktes, wie beispielsweise die Benutzer- Arbeitsplätze
- Übersicht der Sicherheitsfunktionalitäten des eingesetzten Verzeichnisdienst-Produktes
- Übersicht zu Benutzerverantwortlichkeiten, welche für den sicheren Betrieb eines Verzeichnisdienst-Produktes erforderlich sind
- Übersicht möglicher Fehlermeldungen, welche für den Endanwender von Bedeutung sind

Dabei sollten auch die Ansprechpartner zu Fragen rund um Verzeichnisdienste in der Institution vorgestellt werden. Die Benutzer sollten außerdem über

die Möglichkeiten zur Einsichtnahme und Korrektur eines Verzeichnisdiensteintrages informiert werden.

Prüffragen:

- Wurde eine Benutzerschulung zum Verzeichnisdienst durchgeführt?

# M 3.64 Einführung in Active Directory

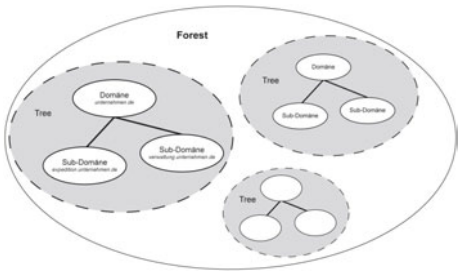
**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Active Directory ist der zentrale Datenspeicher für sämtliche Verwaltungsdaten einer Domäne auf Basis der Serverbetriebssysteme Windows Server 2000 und Windows 2003 Server. Die Serverbetriebssysteme werden im Folgenden unter dem Begriff "Windows-Server" zusammengefasst. Abstrakt gesehen, bildet das Active Directory eine hierarchisch und baumartig organisierte, Objekt-basierte Datenbank. Es ist an den Verzeichnisdienst-Standard X.500 angelehnt, von dem es die interne Struktur und den internen Aufbau entliehen hat. Es ist jedoch kein X.500 kompatibler Verzeichnisdienst.

Das Windows-Server Domänenkonzept gleicht auf Domänenebene prinzipiell dem Windows NT Domänenkonzept: in einer Domäne werden Rechner und Benutzer zusammengefasst und können durch den Domänenadministrator verwaltet werden. Eine Domänengrenze bildet grundsätzlich eine administrative Grenze und begrenzt auch den Wirkungsbereich von Berechtigungen. Zusätzlich zu diesem Konzept bieten Windows-Server an, Domänen baumartig miteinander in Beziehung zu setzen, so dass Vater-Kind-Beziehungen zwischen Domänen bestehen können. Eine Kind-Domäne wird dabei auch als Sub-Domäne bezeichnet, da sich der Name der Kind-Domäne aus dem Namen der übergeordneten Domäne ableitet, indem diesem Namen der Name der Domäne durch einen Punkt getrennt angehängt wird.

**Beispiel:**
Name der Vater-Domäne: unternehmen.de
Name der Sub-Domäne: verwaltung.unternehmen.de

Der so aufgespannte Namensraum ist mit dem zugehörigen DNS Namensraum identisch und kann auch nicht verschieden von diesem gebildet werden. Domänen, die einen gemeinsamen Namensstamm besitzen, bilden einen Baum (englisch *Tree*).




Domänen, die in mehreren Bäumen angesiedelt sind - also unterschiedliche Namensräume aufspannen - können dennoch gemeinsam verwaltet werden.

Derart zusammengeschlossene Domänenbäume bilden einen Wald (englisch *Forest*). Insbesondere bildet eine einzige alleinstehende Domäne auch einen Baum und gleichzeitig auch einen Wald.

In einem Wald gibt es immer eine ausgezeichnete Domäne, die eine gewisse Sonderstellung besitzt. Es ist die als erstes erzeugte Domäne, die auch als *Forest-Root-Domäne* (FRD, Wurzel-Domäne des Waldes) bezeichnet wird. Die Sonderstellung besteht darin, dass Administratoren der Forest-Root-Domäne im gesamten Forest weitreichende Berechtigungen besitzen. Für die Mitglieder der Gruppe Organisations-Admins stellen die Domänengrenzen keine ad-

ministrativen Grenzen dar, da sie in allen Domänen Zugriffsrechte besitzen. Beim Aufbau eines Windows Domänenverbundes ist zu bedenken, dass die zuerst erzeugte Domäne immer die Forest-Root-Domäne ist. Insbesondere kann die "Rolle" der Forest-Root-Domäne nachträglich nicht auf eine andere Domäne "übertragen" werden, so dass die Domänenstruktur ggf. vollständig in der gewünschten Form neu erzeugt werden muss.

Das Active Directory besteht aus verschiedenen Objekten, den Active Directory Objekten (ADOs). Jedes Objekt besitzt einen ausgezeichneten Typ, wie z. B. Benutzerobjekt oder Rechnerobjekt, und ist gemäß dieses Typs aus verschiedenen Attributen zusammengesetzt. Die verschiedenen Objektattribute können verschiedene Werte aufnehmen, wie z. B. Telefonnummer oder IP-Adresse. Das Active Directory kennt verschiedene vordefinierte Objekttypen:

- Domänen-Objekt: Dieses Objekt ist die Wurzel aller Active Directory-Objekte einer Domäne und enthält Informationen über die Domäne, wie z. B. den Namen. Unterhalb eines Domänen-Objektes können andere Objekte angeordnet sein.
- Gruppierungs-Objekte: Diese Objekte dienen dazu, andere Objekte zu gruppieren. Standardmäßig steht das Objekt Organisations-Einheit (Organizational Unit, OU) zur Verfügung. Unterhalb eines OU-Objektes können weitere OU-Objekte enthalten sein, sowie Rechner-, Benutzer- und Benutzer-Gruppen-Objekte.
- Rechner-Objekt: Durch dieses Objekt werden Windows Client Rechner repräsentiert. Unterhalb eines Rechner-Objektes können keine weiteren Objekte mehr angeordnet sein. Das Active Directory ist nur auf die Verwaltung von Windows Rechnern ausgelegt, so dass Rechner-Objekte ausschließlich Windows Rechner repräsentieren können, die mit dem Active Directory zusammenarbeiten. Dies sind standardmäßig Rechner mit den Betriebssystemen ab Windows NT. Für andere Versionen von Windows, wie z. B. Windows 98, stehen Active Directory Anmeldekomponenten zur Verfügung.
- Benutzer-Objekt: Durch dieses Objekt werden Domänenbenutzer repräsentiert. Unterhalb eines Benutzer-Objektes können keine weiteren Objekte mehr angeordnet sein.
- Benutzer-Gruppen-Objekte: Durch diese so genannten Sicherheitgruppen werden Windows Gruppen repräsentiert. Es gibt verschiedene Gruppentypen, die sich im Geltungsbereich (domänen-, forestweit) und in den möglichen Gruppenmitgliedern (Domänen-, Forest-Objekte) unter-scheiden. Es wird unterschieden zwischen lokalen, domänen-lokalen, globalen und universalen Gruppen. Sicherheits-Gruppen werden dazu benutzt, Berechtigungen zu vergeben. Im Vergleich zu Windows NT ist in einem Windows-Server mit einer deutlich höheren Anzahl von Gruppen zu rechnen (mehrere zehntausend für größere Unternehmen), so dass u. U. über eine werkzeuggestützte Verwaltung nachgedacht werden muss. Diese kann sowohl über selbst geschriebene Skripte, als auch über Produkte von Drittherstellern erfolgen. Ob und welche Werkzeuge hier sinnvoll sind, muss jedoch im Einzelfall entschieden werden.

Der generelle Active Directory-Aufbau lässt sich wie folgt darstellen:

- Das Domänen-Objekt ist die Wurzel des Active Directory-Baumes einer Domäne.
- Unter dem Domänen-Objekt werden OU-Objekte erzeugt, um Rechner-, Benutzer- und Benutzer-Gruppen-Objekte strukturiert zusammenzufassen. Da OU-Objekte geschachtelt werden können, ergibt sich eine organisationsspezifische Baumstruktur.

Nach einer Standardinstallation existiert eine einfache und flache Active Directory-Struktur, die von einem Windows-Server angelegt wird und dann entsprechend der Active Directory-Planung verändert werden muss. Da das Active Directory primär der Verwaltung eines Windows Systems dient, sollte beim Aufbau der Active Directory-Struktur darauf geachtet werden, dass die Struktur vornehmlich auf administrative Gegebenheiten abgestimmt wird. Wenn stattdessen zwanghaft die organisatorische Struktur einer Institution bis ins Kleinste nachgebildet wird, kann dies zu Problemen in der Administration führen.

Die möglichen Anordnungen von Active Directory-Objekten, d. h. die Festlegung welches Objekt welche anderen Objekte enthalten darf, welche Attribute existieren und aus welchen Attributen Objekte zusammengesetzt werden, wird durch das so genannte Active Directory-Schema definiert. Das von Microsoft vorgegebene Active Directory-Schema kann auch verändert werden. Dies stellt jedoch einen gravierenden Eingriff in das Active Directory dar, der nur nach sorgfältiger Planung durchgeführt werden darf. Eine Schema-Änderung wirkt sich in allen gemeinsam verwalteten Domänen, d. h. im Wald bzw. Forest, aus. Da die Schemaänderung eine kritische Operation ist, kann diese nur an genau einem Rechner, dem so genannten Schema-Master, durch Mitglieder der Gruppe *Schema-Admins* durchgeführt werden. Schemaänderungen können zudem u. U. nicht mehr rückgängig gemacht werden. Die Mitgliedschaft in dieser Gruppe ist daher unbedingt restriktiv zu vergeben und streng zu kontrollieren.

Die Mitglieder der Gruppe "Organisations-Admins", zu der in der Voreinstellung der Administrator der Forest Root Domäne gehört, haben besondere Befugnisse in allen Domänen des Netzes.

Sie können z. B. neue Domänen in den Forest aufnehmen und haben Administratorrechte auf allen Domänen Controllern des Active Directory.

Innerhalb einer einzelnen Domäne erfolgt die Administration durch Mitglieder der jeweiligen (domänen-spezifischen) Gruppe "Domänen-Admins". Diese Gruppe verfügt innerhalb einer Domäne über unbeschränkte administrative Berechtigungen. Es ist jedoch möglich, einzelne administrative Aufgaben auch für andere Benutzerkonten zu ermöglichen und so administrative Aufgaben zu delegieren (siehe auch M 2.230 *Planung der Active Directory-Administration*).

Eine Delegation administrativer Aufgaben innerhalb einer Domäne kann auch so erfolgen, dass lediglich die Administration eines Teils der Benutzerkonten und Computer einer Domäne delegiert wird. Dies ist innerhalb der Grenzen der OUs möglich, die zur Gruppierung von Benutzer- bzw. Computerkonten innerhalb der Domäne dienen.

Eine Vielzahl von Windows-Client-Konfigurationsparametern ist in den "Gruppenrichtlinien" zusammengefasst. Neben den lokalen Gruppenricht-linien auf jedem einzelnen Windows-Client-Rechner gibt es auch Gruppen-richtlinien, die im Active Directory gespeichert sind. Dies gestattet es, Rechner oder Benutzerkonten zentral zu konfigurieren. Wirkungsbereich einer solchen, im AD-gespeicherten Gruppenrichtlinie, können unter anderem ganze Domänen oder OUs sein. Hier dienen OUs zur Gruppierung gleichartig konfigurierter Rechner oder Benutzerkonten. Da sich OUs schachteln lassen und mit einer einzelnen OU mehrere Gruppenrichtlinien verbunden sein können, wirken auf einen einzelnen Rechner unter Umständen viele verschiedene Gruppenrichtlinien ein (siehe auch M 2.231 *Planung der Gruppenrichtlinien unter Windows* und M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*).

Zur Speicherung der Daten wird eine relationale, transaktionsorientierte Datenbank verwendet. Diese Datenbank wird auf speziellen Servern, den "Domänen-Controllern", verteilt. Der Domänen-Controller nutzt dabei das Active Directory, um eine zentrale Authentisierung und Autorisierung von Benutzern und Computern in einer Domäne zur Verfügung zu stellen. Folgende Protokolle werden dazu verwendet:

- LDAP (Lightweight Directory Access Protocol) zur Abfrage von Objekten und Attributen des Active Directory
- Kerberos zur Authentisierung von Benutzern und Computern
- CIFS (Common Internet File System) zum Transfer von Dateien im Rechnernetz
- DNS (Domain Name System) zur Namensauflösung der Computersysteme im Netz

Mit einigen Ausnahmen enthält jeder Domänen-Controller dabei nur die Daten seiner eigenen Domäne. Diese Ausnahmen sind:

- Jeder Domänen-Controller enthält die Schema- und Konfigurationsdaten des gesamten Forests.
- Mindestens ein Domänen-Controller jeder Domäne enthält zusätzlich noch den "Global Catalog".

Das Active Directory wird auf Domänen Controllern gehalten und innerhalb einer Domäne zwischen diesen durch Replikation synchronisiert. Das Active Directory einer Domäne enthält nur domänenbezogene Informationen. Um in einem Forest schnell auf Informationen aus dem gesamten Forest zugreifen zu können, wird der so genannte *Global Catalog* (GC) aufgebaut. Er besteht aus Teilinformationen von Active Directory-Objekten und wird im gesamten Forest repliziert, so dass über den Global Catalog in einer Domäne auch direkt auf Informationen aus anderen Domänen zugegriffen werden kann.

Neben der beschriebenen baumartigen und hierarchischen Struktur baut Windows-Server automatisch eine zusätzliche und orthogonale Struktur auf. Räumlich nahe Rechner - dies bestimmt Windows-Server über Netzlaufzeiten - werden zu so genannten Standorten (englisch *Sites*) zusammengefasst. Über Sites wird u. a. auch die Replikationsstruktur von Domänen Controllern gesteuert. Pro Site muss mindestens ein Rechner existieren, der eine Kopie des Global Catalogs hält. Der Global Catalog muss im Rahmen des Anmeldeprozesses eines Benutzers angefragt werden, so dass bei der Anmeldung immer ein Global Catalog-Server zugreifbar sein muss. Die von Windows-Server automatisch aufgebaute Standortstruktur sollte an die behörden- oder unternehmensinternen Gegebenheiten, wie z. B. Standorte in verschiedenen Städten oder Ländern, individuell angepasst werden. Da dies Einfluss auf die Active Directory-Replikationsbeziehungen hat, ist dazu jedoch ein Konzept zu erstellen.

Diese Rollen werden in der Windows-Server Terminologie auch als FSMO-Rollen (FSMO = Flexible Single Master Operations) bezeichnet. Bestimmte Änderungen können daher nur an dem Rechner vorgenommen werden, dem die jeweilige Rolle zugeordnet ist.

Der Abgleich der Daten zwischen den einzelnen Domänen-Controllern kann über zwei verschiedene Replikationsmechanismen erfolgen. Welcher Mechanismus verwendet wird, lässt sich ebenso konfigurieren wie die Zeitabstände, in denen die Replikation erfolgt.

Durch das Konzept der verteilten Datenbanken kann eine gewisse Ausfallsicherheit des Active Directory erreicht werden, problematisch sind dabei jedoch die Inhaber der FSMO-Rollen.

Ab Windows 2000 Server werden die Daten des Active Directory mittels Multi-Master-Replikation zwischen den Domänen-Controllern einer Organisation repliziert. Auf jedem Domänen-Controller existiert somit ein Replikat des Active Directory, das geändert und als Grundlage für zukünftige Replizierungen dienen kann. Bei der Verwendung mehrerer Domänen-Controller in einer Institution werden so redundante Kopien des Active Directory erzeugt und die Wahrscheinlichkeit eines Totalausfalls minimiert.

# M 3.65 Einführung in VPN-Grundbegriffe

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Ein Virtuelles Privates Netz (VPN) bietet einen durch Zugriffskontrolle und Verschlüsselung abgeschotteten sicheren Kommunikationskanal zwischen IT-Systemen. Durch die Auswahl und Einbindung geeigneter kryptographischer Verfahren kann die Integrität und Vertraulichkeit der übertragenen Daten geschützt werden. Ebenso können bei geeigneter Konfiguration die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Ein VPN kann dabei über nahezu beliebige Medien aufgebaut werden. VPNs können sich in der Implementierung, den Funktionen und auch der genutzten Schicht des ISO/OSI-Schichtenmodells unterscheiden. Bereits bei der Planung eines VPNs sollte entschieden werden, wie das VPN später betrieben werden soll und ob ein externer Dienstleister mit dessen Aufbau oder Betrieb beauftragt werden sollte.

**Typische VPN-Nutzungsszenarien:**

Nachfolgend werden einige Einsatzszenarien, in denen VPNs üblicherweise eingesetzt werden, beschrieben.

- Mobile Mitarbeiter:
  Mobile Mitarbeiter arbeiten an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen und benötigen dabei unter Umständen einen Fernzugriff auf Daten im LAN innerhalb der Institution. Neben der Absicherung solcher Verbindungen muss auch die Sicherheit des Endgeräts sowie dessen Einsatzumgebung beachtet werden. Je nach Aufgabengebiet kann es sein, dass sich die Mitarbeiter von beliebigen Arbeitsorten, z. B. einem Hotel oder Flughafen, ins interne Netz einwählen möchten. Um hier eine angemessene, mit einem Büroraum vergleichbare Sicherheitssituation zu erreichen, sind zusätzlich die Empfehlungen in B 2.10 *Mobiler Arbeitsplatz* zu beachten. Die Endgeräte der Mitarbeiter sind typischerweise Laptops oder PDAs. Auch hierfür müssen die entsprechenden IT-Grundschutz-Bausteine angewandt werden, also B 3.203 *Laptop*, B 3.405 *Smartphones, Tablets und PDAs*, etc.
- Telearbeitsplatz:
  Bei der Anbindung eines Telearbeitsplatzes greift ein Client-System von einem festen Arbeitsort außerhalb der Büroumgebung auf das interne Netz einer Institution zu.
  Die Kommunikation zwischen Telearbeitsrechner und LAN erfolgt normalerweise über unsichere, öffentliche Netze. Die IT-Systeme des Telearbeitsplatzes sollten zentral administriert werden. Wie die Anbindung der Telearbeitsrechner abgesichert werden kann, ist in B 5.8 *Telearbeit* beschrieben.
- Standortvernetzung:
  Bei der Standortvernetzung werden Teilnetze an unterschiedlichen Standorten einer Institution miteinander verbunden. Hierbei werden die vertrauenswürdigen LANs, die unter eigener Kontrolle stehen, häufig über ein unsicheres öffentliches Transportnetz verbunden. In diesem Szenario ist besonders der Transportkanal abzusichern. Zusätzlich müssen die Netze

und die Client-Systeme der Standorte mittels Sicherheitsgateways gegen Angriffe aus dem Internet gesichert werden.

- Kunden- und Partner-Anbindung:
  Häufig sollen Kunden oder Partner an das interne Netz einer Institution angebunden werden. Folgende Szenarien sind typisch

  - Es sollen bestimmte interne Informationen bereitgestellt werden, so dass diese aus einem nur eingeschränkt vertrauenswürdigen Netz, d. h. von "außen", abgerufen werden können.
  - Aus dem vertrauenswürdigen Netz heraus, d. h. von "innen", sollen externe Datenbanken abgefragt werden, z. B. um Waren aussuchen und bestellen zu können.
  - Auf internen Systemen soll durch externe Firmen Software entwickelt werden.

  Da die IT-Systeme der Kunden oder der Partner nicht unter der Kontrolle der Institution stehen, muss gewährleistet werden, dass nur auf die freigegebenen Ressourcen zugegriffen werden kann. Beispielsweise könnten alle IT-Systeme, auf die Kunden oder Partner zugreifen können, in einem separaten Netz betrieben werden, dass mit einem Sicherheitsgateway (siehe B 3.301 *Sicherheitsgateway (Firewall)*) vom LAN der Institution getrennt ist.
- Fernwartung:
  Bei der Durchführung von Fernwartungstätigkeiten sind privilegierte Administratorzugänge auf interne Systeme erforderlich. Die Fernwartung (Wartung, Support und Betrieb) interner Systeme kann durch eigene oder fremde Mitarbeiter durchgeführt werden. In beiden Fällen bestehen hohe Anforderungen an die Authentisierung des entfernten Benutzers, die Datenflusskontrolle und die Verfügbarkeit der Anbindung. Werden fremde Mitarbeiter beauftragt, die IT-Systeme zu warten, müssen die Empfehlungen des Bausteins B 1.11 *Outsourcing* berücksichtigt werden.

VPNs werden häufig auch verwendet, um die Kommunikation einzelner Protokolle und Anwendungen zu schützen. Unterstützen beispielsweise die vorhandenen WLAN-Komponenten selbst keine sichere Verschlüsselung, könnte die gesamte WLAN-Kommunikation mit einem VPN, das unabhängig vom WLAN ist, verschlüsselt übertragen werden. Die Signalisierung und der Medientransport einer VoIP-Verbindung könnten ebenfalls in einem VPN-Tunnel gebündelt und verschlüsselt werden.

**VPN-Endpunkte**

Bei den VPN-Endpunkten wird grundsätzlich zwischen VPN-Server und VPN-Client unterschieden. Derjenige Endpunkt, zu dem die Verbindung aufgebaut wird, fungiert als VPN-Server. Der initiierende Endpunkt wird als VPN-Client bezeichnet. VPN-Endpunkte lassen sich entweder per Software oder per Hardware realisieren. Bei Mitarbeitern im Außendienst besteht der VPN-Client in der Regel aus einer Software-Applikation auf einem mobilen IT-System. Ein derartiger VPN-Client greift oft sehr stark in das installierte Betriebssystem ein. Die parallele Installation mehrerer unterschiedlicher VPN-Clients auf einem Endgerät sollte daher vermieden werden. Die Vernetzung der einzelnen VPN-Endpunkte untereinander muss anhand der Ergebnisse der Anforderungsanalyse (M 2.415 *Durchführung einer VPN-Anforderungsanalyse*) durchgeführt werden. Bei den VPN-Endpunkten muss, wie in M 4.321 *Sicherer Betrieb eines VPNs* beschrieben, für eine sichere Authentisierung gesorgt werden, damit nur Berechtigte sich über das VPN einwählen können. Hierbei ist, je nach Anwendungsgebiet, auch der Einsatz eines Authentisierungsservers, beispielsweise eines RADIUS-Servers, denkbar.

**Auswahl der Kommunikationsbeziehungen zwischen den Standorten**

Ist geplant, mehrere Standorte zu einem LAN zusammenzufassen, spielt es eine wichtige Rolle, zwischen welchen Standorten eine VPN-Verbindung aufgebaut wird. Folgende Topologien, oder Kombinationen hieraus, eignen sich für die Vernetzung mehrerer Standorte:

- Sternnetz
  Beim Sternnetz wird eine zentrale Stelle (z. B. in der Unternehmenszentrale) ausgewählt, zu der jeder weitere dezentrale Standort eine eigene VPN-Verbindung aufbaut. Um Informationen von einem dezentralen Standort zu einem anderen zu übermitteln, müssen die Informationen immer über den zentralen Standort weitergeleitet werden. Der Ausfall der Zentrale führt daher zum Ausfall des gesamten Netzverbundes. Nachteilig können sich die längeren Übertragungszeiten auswirken, besonders wenn geographisch nahe Standorte miteinander kommunizieren, aber alle Informationen über die Zentrale übermittelt werden.
- Ringnetz
  Bei einem Ringnetz ist jeder Standort mit jeweils zwei anderen Standorten verbunden. Informationen, die zu einem nicht direkt verbundenen Standort versendet werden sollen, werden von den dazwischen liegenden Standorten an den Empfänger weitergeleitet. Fällt nur ein Standort aus, können bei einem Ringnetz die Informationen über die verbleibenden Standorte übermittelt werden. Fallen mehr als zwei Standorte aus, ist die Verfügbarkeit des gesamten VPN-Verbunds bedroht.
- Baumnetz
  Die verschiedenen VPN-Endpunkte in den Standorten werden hierarchisch angeordnet. Es wird ein zentraler Standort als "Wurzel" festgelegt. An diesem sind wiederum einer oder mehrere weitere Standorte mit einer VPN-Anbindung angeschlossen, die wiederum mit weiteren Standorten verbunden sind. Zusätzliche Standorte können bei einem Baumnetz einfach hinzufügt werden. Fällt aber ein zentrales System aus, können die VPN-Segmente, die an dem System angeschlossen sind, nicht mehr im VPN-Verbund kommunizieren.
- Vollvermaschtes Netz
  Jeder Standort ist mit jedem anderen Standort über eine eigene Anbindung verbunden. Fällt eine Leitung aus, kann die Kommunikation über eine der anderen noch zur Verfügung stehenden Leitungen durchgeführt werden. Durch die direkte Verbindung kann die Übertragungszeit verkürzt werden. Diesen Vorteilen stehen die hohen Kosten dieser Topologie gegenüber.

Aus diesen Topologien oder Kombinationen hieraus muss eine geeignete ausgewählt werden. Um einen Kompromiss zwischen Ausfallsicherheit und Kosten zu erzielen, hat es sich in der Praxis durchgesetzt, eine Topologie mit mehreren zentralen Netzzugängen, an denen die einzelnen Standorte angeschlossen sind, einzusetzen.

**VPN-Typen**

VPNs können eingesetzt werden, um entfernte physische Netze zu einem logischen zusammenzufassen oder um einzelne Endgeräte, die sich in unsicheren Netzen befinden, über einen geschützten Kanal an ein zentrales LAN anzubinden. Je nachdem, welche Systeme den Endpunkt der VPN-Verbindung darstellen, wird zwischen Site-to-Site-, End-to-End- und End-to-Site-VPNs unterschieden.

- Site-to-Site-VPN
  Mit Site-to-Site-VPNs werden Netze gekoppelt, um gemeinsame Anwendungen betreiben bzw. nutzen zu können. Es werden netzübergreifende

Zugriffe benötigt. Der Transportkanal wird durch VPN-Gateways in den angeschlossenen Netzen gesichert.
Eine typische Verwendung für Verbindungen zwischen LANs ist die Anbindung von Außenstellen oder Filialen an das institutionsinterne Netz.

- End-to-End-VPN
  End-to-End-VPNs werden meist für die Nutzung einzelner Anwendungen verwendet. Die Verbindungen lassen sich auf spezielle Systeme und Dienste beschränken.
  Typische Verwendungen für End-to-End-VPNs sind:
  - Fernwartung dedizierter Systeme, bei der Zugriffe auf Administratorebene erforderlich sind.
  - Zugriffe auf einzelne Anwendungen oder Datenbanken. Hierbei sind Berechtigungen auf Administrator- bzw. Systemebene häufig nicht erforderlich.
  - Zugriffe über Terminalserver. Durch Fernzugriff auf ein entferntes System können viele dort installierte Anwendungen genutzt werden. Berechtigungen auf Administrator- bzw. Systemebene auf dem Terminalserver sind dafür normalerweise nicht erforderlich.
  - Integration von Geschäftspartnern oder Kunden in Teilbereiche des zentralen Datennetzes einer Institution.
- End-to-Site-VPN (Remote-Access-VPN)
  End-to-Site-VPNs werden auch als Remote-Access-VPN (RAS-VPN) bezeichnet. Solche VPNs werden für Zugriffe eines Clients auf mehrere Anwendungen verwendet, die auf unterschiedlichen IT-Systemen im LAN einer Institution liegen. Dadurch wird Zugriff auf das gesamte Netz benötigt, so dass meist VPN-Software auf dem Client-System und ein VPN-Gateway im LAN den Transportkanal sichern. Telearbeiter und mobile Benutzer werden in der Regel mit End-to-Site-VPNs in das LAN integriert.

**VPN-Varianten**

Der Begriff VPN wird oft als Synonym für verschlüsselte Verbindungen verwendet. VPN-Varianten werden häufig auch nach dem eingesetzten VPN-Protokoll benannt, wie beispielsweise TLS/SSL-VPN oder IPSec-VPN. Zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, wie beispielsweise spezielle Funktionen des genutzten Transportprotokolls. Zusätzlich werden zwei grundlegende VPN-Varianten unterschieden: Trusted-VPN und Secure-VPN.

VPNs werden als Trusted-VPN bezeichnet, wenn die VPN-Verbindung zwischen verschiedenen Standorte durch vertrauenswürdige externe VPN-Dienstleister gewährleistet wird. Dabei werden die Daten aus dem vertrauenswürdigen Netz in der Regel unverschlüsselt über einen dedizierten Kommunikationskanal zu einem Gateway-Router des Anbieters geleitet. Die Bildung des VPNs erfolgt durch logische Abschottung des VPN-Datenverkehrs vom übrigen Datenverkehr (z. B. mittels Multiprotocol Label Switching, MPLS). Für mobile Nutzer stellen Dienstleister zudem VPNs über Gateway-Router bereit, die nur über spezielle Einwahl-Knoten erreicht werden können, die vor unberechtigtem Zugriff geschützt sind.

Wird ein externer Dienstleister beauftragt, ein Trusted-VPN zur Verfügung zu stellen, sollte zusätzlich der Baustein B 1.11 *Outsourcing* berücksichtigt werden.

Für vertrauliche Daten sind Trusted-VPNs ohne zusätzliche Verschlüsselung auf der Anwendungsschicht nicht geeignet, da die Sicherheit solcher Verbindungen ausschließlich in Händen des VPN-Dienstleisters liegt. So bietet ein

Trusted-VPN zum Beispiel keinen Schutz gegen Innentäter des Anbieters. Für die vertrauliche Datenkommunikation empfiehlt sich daher ein Secure-VPN.

Die Abhängigkeit von Dritten in Bezug auf Vertraulichkeit kann vermieden werden, wenn die Kommunikation an den Endpunkten der Verbindung durch Verschlüsselung geschützt wird, die im eigenen Verantwortungsbereich des VPN-Nutzers liegt. Diese Lösung wird auch als Secure-VPN bezeichnet.

Werden für die Realisierung des VPNs dedizierte Carrier-Leitungen eingesetzt, handelt es sich um eine Sonderform eines Trusted-VPNs. Auch in diesem Fall müssen vertrauliche Daten vor der Übertragung durch Verschlüsselung geschützt werden, die im eigenen Verantwortungsbereich des VPN-Nutzers liegt. Die Verschlüsselung kann an den VPN-Endpunkten auf Transportebene (Secure-VPN) oder auf Anwendungsebene erfolgen.

**VPN-Geräte**

Grundsätzlich muss eine Entscheidung darüber getroffen werden, ob das gewählte VPN-Produkt ein dediziertes VPN-Gerät, ein Kombi-Gerät oder eine software-basierte VPN-Lösung auf Standard-IT-Systemen (z. B. Linux mit IPSec) sein soll:

- Dedizierte VPN-Gateways (Appliances):
  Diese VPN-Produkte dienen ausschließlich der Realisierung von VPN-Verbindungen und bieten keine darüber hinausgehenden Funktionalitäten, wie beispielsweise Inhaltsfilterung auf Anwendungsebene. VPN-Appliances haben den Vorteil, dass sie für den VPN-Einsatz optimiert sind und die sichere Konfiguration vereinfacht wird, da beispielsweise das Betriebssystem bereits gehärtet ist.
- Kombi-Geräte:
  Integrierte VPN-Geräte können beispielsweise Router und andere Komponenten von Sicherheitsgateways (z. B. Application Level Gateways, ALGs) darstellen, die über eine VPN-Funktionalität verfügen oder entsprechend erweitert werden können. Kombi-Geräte haben neben den finanziellen Aspekten oft den Vorteil, dass die unterschiedlichen Funktionalitäten gemeinsam an einer Stelle administriert werden können.
  Die Kombination verschiedener Funktionalitäten auf einem Gerät kann jedoch zu Lasten der Performance gehen. Bei einer intensiven VPN-Nutzung ist daher zu prüfen, ob aus Gründen der Verfügbarkeit oder des Durchsatzes eigenständige VPN-Komponenten vorzuziehen sind. Manche Kombi-Geräte bieten die Möglichkeit, nachträglich spezielle Hardware-Verschlüsselungsmodule zur Steigerung der Performance einzubauen.
- VPNs auf Basis von Standard-IT-Systemen:
  VPN-Geräte können mit frei verfügbaren oder kommerziellen Software-Komponenten selbst zusammengestellt werden. Diese Komponenten können oft auf handelsüblicher Hardware mit Standardbetriebssystemen installiert werden. Zusammengestellte VPN-Geräte bieten eine hohe Flexibilität und sind für viele Anwendungsfälle gut geeignet.
  Die Installation und Integration der benötigten Komponenten kann jedoch fehlerträchtig sein. Daraus können sich Sicherheitsrisiken beim Einsatz eines zusammengestellten VPN-Gerätes ergeben. Ein weiterer Nachteil ist, dass bei Support-Anfragen meist unterschiedliche Ansprechpartner für die einzelnen Komponenten des VPN-Gerätes (z. B. Hardware, Betriebssystem, VPN-Software) kontaktiert werden müssen.

Zusammenfassend werden in der nachfolgenden Tabelle die Vor- und Nachteile der unterschiedlichen Aufbauformen tabellarisch gegenübergestellt. Ein

(x) kennzeichnet hierbei die positive Erfüllung, ein (-) steht für das Nicht-Erfüllen eines Kriteriums.

| **Eigenschaft** | **Dedizierte VPN-Gateways** | **Kombi-Geräte** | **VPNs auf Basis von Standard IT-Systemen** |
|---|---|---|---|
| (Selbst-) Schutz der VPN-Komponente | - | x | - |
| hohe Performance | x | - | x |
| günstige Anschaffungskosten | - | - | x |
| geringer Aufwand bis zur Inbetriebnahme | x | x | - |
| einfache Administration | x | x | - |
| leichte Erweiterbarkeit | - | - | x |
| Know-How-Verteilung | x | x | - |
| Support aus einer Hand | x | x | - |

Tabelle 1: Vergleich der VPN-Aufbauformen

Die Tabelleneinträge sind als Erfahrungswerte aus der Praxis zu verstehen und müssen im Einzelfall anhand der tatsächlichen Produkt-Eigenschaften verifiziert werden.

# M 3.66 Grundbegriffe des Patch- und Änderungsmanagements

**Verantwortlich für Initiierung:** Änderungsmanager, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Änderungsmanager

Beim Patch- und Änderungsmanagementprozess werden verschiedenste Aktualisierungen und Verbesserungen in der Produktionsumgebung bereit gestellt, gesteuert und verwaltet. In diesem Bereich haben sich eine Vielzahl von Begriffen etabliert. Diese müssen den Personen, die sich mit der Durchführung des Prozesses beschäftigen, bekannt sein.

Bei **Versionsbezeichnungen** sind sehr unterschiedliche Benennungen gebräuchlich. Das ist darauf zurück zu führen, dass für die Begriffsdefinition kein einheitlicher, verbindlicher, übergreifender Standard existiert. Bei der durchlaufen die zu erstellenden Produkte wie z. B. Hard- oder Software verschiedene **Entwicklungsstadien.** Aufgrund der nicht exakt definierten Begriffe empfiehlt es sich, innerhalb der Institution ein Glossar zu benutzen, um ein einheitliches Verständnis aller Fachausdrücke sicher zu stellen.

Die erste lauffähige Version eines Produkts wird oft **Alpha-Version** genannt. Die Alpha-Version dient oft der internen Verwendung, z. B. um zu demonstrieren, dass ein Softwareprojekt durchführbar ist. Sie enthält deshalb in der Regel bereits die wichtigsten Grundfunktionen.

Eine **Beta-Version** ist eine noch unfertige Produkt-Version, welche vom Entwickler oft zu Test- und Vorverkaufszwecken veröffentlicht wird. Es sind die wesentlichen Funktionen des Produktes bereits vorhanden, jedoch nicht in aller Tiefe getestet. Beta-Versionen werden an sogenannte Beta-Tester verteilt, welche die Funktionalität und Nutzbarkeit des Produktes überprüfen und ggf. Fehler an die Entwickler melden. Bei Software werden so typischerweise eine Vielzahl von Programmierfehler gefunden.

Bei der Software-Entwicklung bezeichnet **Release Candidate** (**RC**) oder **Freigabekandidat** eine abschließende Testversion. In dieser Version sind alle Funktionen, welche die Endversion der Software enthalten soll, verfügbar. Diese Versionsart dient einem abschließenden System- oder Produkttest. Es werden nur dann weitere RCs veröffentlicht, wenn gravierende Qualitätsprobleme dabei ermittelt werden.

Die fertige und veröffentlichte Version einer Software wird als **Release** oder **Stable** bezeichnet und in der Regel zusätzlich mit einer Versionsnummer versehen. Da zu diesem Zeitpunkt auch die Herstellung der Medien (CDs oder DVDs) begonnen wird, wird oft auch der Begriff **Ready to Manufacturing (RTM)** benutzt.

Viele Softwareentwickler, haben Mechanismen für den Umgang mit Softwarekorrekturen veröffentlicht. Dabei werden die nachfolgenden Begriffe nicht immer konsequent einheitlich verwendet. Sie geben jedoch insgesamt den notwenigen Überblick über die Begriffswelt in diesem Themengebiet.

Softwarekorrekturen werden veröffentlicht, um Fehler in bereits veröffentlichter Software zu beheben. Ein **Patch** ist ein generelles **Softwareupdate**, welches Fehlfunktionen in einer Software behebt. Zunächst ist ein solches **Update** nicht kritisch und nicht sicherheitsrelevant. Ist das Update relevant für die Sicherheit der Software, wird also eine Sicherheitslücke geschlossen, wird es oft

**Sicherheitspatch** genannt. Für einen Sicherheitspatch wird oft ein **Schweregrad** angegeben. Dieser bezieht sich in der Regel darauf, für wie schwerwiegend der Hersteller die Sicherheitslücke hält, die der Sicherheitspatch behebt. Wird mit dem Update eine wesentliche Funktionalität der Software korrigiert, die aber nicht unbedingt sicherheitsrelevant ist, beispielsweise eine falsche Berechnung, so wird es oft als **kritisches Update** bezeichnet.

Eine andere Veröffentlichung der Hersteller, die sich jedoch nur auf spezielle Kundensituationen bezieht und oft nur bei gültigem Supportvertrag zur Verfügung gestellt oder erst auf Grund von Supportanfragen erstellt wird, hat die Bezeichnung **Hotfix**. Bei einem Hotfix kann es sich um ein einzelnes Paket aus einer oder mehreren Dateien handeln, um ein Problem in einem Produkt zu beheben.

Bei einem **Servicepack** dagegen handelt es sich um eine kumulative Sammlung von Hotfixes, Sicherheitspatches, kritischen Updates und Updates, die seit der Markteinführung des Produktes veröffentlicht wurden und der Allgemeinheit zur Verfügung gestellt werden.

Der Zeitraum bis zur Veröffentlichung von Servicepacks ist oft sehr lang ist. Für die Bereitstellung der Menge der zwischendurch verfügbaren Softwarekorrekturen kann außerdem eine Zusammenfassung sinnvoll sein. Daher veröffentlichen einige Hersteller zwischendurch sogenannte **Update Roll-Ups**. Die Update Roll-Ups sind eine Sammlung von Sicherheitspatches, kritischen Updates, Updates und Hotfixes, die kumulativ oder für eine einzelne Produktkomponente, wie beispielsweise einen Webserver, angeboten werden.

Nach der Veröffentlichung von Servicepacks werden die dann verfügbaren Produktserien oft im Dezimalkommastellenbereich um eine Nummer erhöht. Dies soll dokumentieren, dass die Softwareprodukte bereits alle bis zu diesem Zeitpunkt verfügbaren Korrekturen enthalten. Einige Hersteller bezeichnen dies auch als **Integriertes Service Pack**.

Auf Grund der verschiedenen Anforderungen von Kunden, welche an den Hersteller gerichtet werden, sieht dieser sich oft gezwungen, neue Optionen (Features) in das Produkt zu integrieren, mit denen die Funktionalität eines Produktes erweitert werden. Diese Funktionalitätserweiterungen werden in der Regel allen Kunden mit gültigen Vertragsbeziehungen zum Hersteller (Supportvertrag, Updatevertrag, Softwarepflegevertrag oder ähnliches) als **Featurepack** angeboten. Die neuen Features fließen gewöhnlich in die nächste Produktversion mit ein.

Zwei Arten der **Änderung** an IT-Komponenten sind in der betrieblichen Praxis üblich. **Standardisierte Änderungen** und **Änderungen**, welche den Patch- und Änderungsmanagementprozess durchlaufen müssen.

Standard-Änderungen sind Änderungen an Anwendungen und IT-Systemen, für die genaue Verfahrensanweisungen existieren und die vorab vom **Änderungsmanager** genehmigt wurden.

Die geschriebene Verfahrensanweisung muss gewährleisten, dass das mit der Änderung zusammenhängende Risiko vernachlässigt werden kann. Die Änderung kann ohne nochmalige Kontaktierung eines Änderungsmanagers ausgeführt werden. Dadurch wird die Arbeitsmenge der mit dem Prozess beauftragten Personen wesentlich reduziert.

Einer der Beweggründe für Hard- oder Software-Änderungen sind Störungen. Eine **Störung** (**Incident**) ist eine Abweichung vom standardmäßigen Be-

trieb einer IT-Dienstleistung (**Service**), die tatsächlich oder potenziell die Service-Qualität mindert oder sogar den Service unterbricht.

Ist die Ursache für eine Störung nicht erkennbar, so liegt ein näher zu untersuchendes Problem vor. Mit dem Begriff **Problem** wird in ITIL eine oder mehrere gleichartige Störungen mit unbekannter Ursache bezeichnet. Wird die zugrunde liegende Ursache ermittelt und eine Möglichkeit gefunden, das Problem zu beheben oder zu umgehen, wird aus einem Problem ein bekannter Fehler (Known Error). Der Lösungsweg wird in einer Änderungsanforderung (Request for Change, RfC) dokumentiert und unter der Kontrolle des Änderungsmanagements (Change Managements) umgesetzt.

Zusätzlich zu der speziellen Begriffswelt des Patch- und Änderungsmanagements (beispielsweise aus ITIL), sollten die mit dem Patch- und Änderungsmanagement betrauten Personen mit der Begriffswelt der Informationssicherheit vertraut sein.

# M 3.67 Einweisung aller Mitarbeiter über Methoden zur Löschung oder Vernichtung von Daten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Mitarbeiter müssen darüber informiert werden, mit welchen Verfahren und Geräten die unterschiedlichen, in der Institution vorkommenden Datenträger gelöscht oder vernichtet werden dürfen und was dabei zu beachten ist. Hierzu sollten z. B. neben einer Richtlinie regelmäßig Hinweise im Intranet veröffentlicht werden. Auch entsprechende Aushänge neben Druckern, Kopieren und Aktenvernichtern unterstützen dies. Sensibilisierende Maßnahmen sollten institutionsweit durchgeführt und regelmäßig wiederholt werden (siehe auch M 2.432 *Richtlinie für die Löschung und Vernichtung von Informationen*). Vor allem wenn sich Verfahren zur Löschung oder Vernichtung von Datenträgern ändern, müssen die Mitarbeiter darüber in Kenntnis gesetzt werden. Wichtig ist es auch, über typische Fehlerquellen aufzuklären. Dazu gehören beispielsweise folgende Fehleinschätzungen:

**Papierkorb im Büro**

Dokumente werden häufig nicht entsprechend ihres Schutzbedarfs entsorgt, sondern landen im normalen Papierkorb. Bei der anschließenden Entsorgung über das Altpapier können Unbefugte auf einfachste Weise Zugang zu vertraulichen Informationen erhalten (siehe auch G 2.48 *Ungeeignete Entsorgung der Datenträger und Dokumente*). Ursache dieses Problems ist, dass die Mitarbeiter die internen Regeln zur Entsorgung nicht kennen oder nicht beachten.

**Papierkorb des Betriebssystems**

Heutige Betriebssysteme bieten Benutzern einen sogenannten "Papierkorb" an, um zu löschende Dateien dort abzulegen. Dieser ist nicht nur vom Namen, sondern auch in der grafischen Aufbereitung und der Nutzung an einen klassischen Papierkorb angelehnt: Dateien können einfach in diesen Papierkorb verschoben werden. Wie bei einem klassischen Papierkorb sind diese Dateien jedoch noch nicht vernichtet, sondern werden dort zunächst nur abgelegt. Sind sie versehentlich in den Papierkorb gelegt worden, können sie auf einfache Weise vollständig wiederhergestellt werden, da sie lediglich von ihrem Originalspeicherort in dieses Papierkorb-Verzeichnis verschoben wurden (siehe auch M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*).

Beim Leeren des Papierkorbes werden nicht etwa die Daten gelöscht, sondern nur der Verweis auf die Informationen im "Inhaltsverzeichnis" des Betriebssystems. Damit könnten diese Daten immer noch wiederhergestellt werden, solange sie nicht von nachfolgenden Schreibvorgängen überschrieben werden. Um sicherzustellen, dass die Informationen nicht wiederhergestellt werden können, müssen sie gezielt überschrieben werden (siehe M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*).

**"Schwärzen" von Textstellen**

Dokumente, die an Dritte weitergegeben werden sollen, können an vereinzelten Stellen Informationen enthalten, die nicht verbreitet werden sollen. Diese Informationen müssen also entfernt werden, bevor die Dokumente weitergegeben werden.

Das Grundproblem liegt darin, alle sensiblen Informationen zu identifizieren, um sie dann sorgfältig entfernen zu können. Hierbei werden einerseits vertrauliche Informationen leicht übersehen und andererseits ungeeignete Methoden verwendet.

Bei Papierdokumenten werden sensible Informationen häufig geschwärzt, um sie unkenntlich zu machen. Dies ist allerdings kein verlässliches Verfahren, da selbst bei Kopien des ursprünglichen Textes die übermalten Stellen oft noch lesbar sein können. Auch bei elektronischen Dokumenten werden immer wieder Textpassagen "geschwärzt". Diese Methode ist allerdings noch unzuverlässiger als bei Papierdokumenten und ist daher unbedingt zu unterlassen (siehe auch G 3.13 *Weitergabe falscher oder interner Informationen*).

Grundsätzlich sollten auf diese Art veränderte Dokumente nicht weitergegeben werden. Ist dies unumgänglich, müssen die Dokumente nach dem Entfernen der kritischen Informationen neu klassifiziert und in eine niedrigere Sicherheitsstufe eingestuft werden. Anschließend müssen sie erneut den Freigabeprozess durchlaufen.

Um den erneuten Durchlauf zu vermeiden, sollten Dokumente so strukturiert sein, dass nicht-öffentliche Inhalte einfach abgetrennt werden können, beispielsweise indem diese Informationen in den Anhang kommen.

**Besucherbereiche**

In Bereichen innerhalb einer Institution, die auch durch Externe benutzt werden können, muss sämtliches Material entfernt werden, das sensitive Informationen enthalten könnte. Zu beachten ist dies vor allem in Besucherbereichen und Besprechungsräumen, aber auch in allgemein zugänglichen Drucker- oder Kopiererräumen. In Besprechungsräumen sollte nach Ende einer Veranstaltung benutztes Flipchart-Papier mitgenommen und Tafeln gesäubert werden. Papierkörbe in solchen Räumen dürfen nicht für vertrauliches Material benutzt werden. Mitarbeiter sollten darauf hingewiesen werden, dass dies zu den Aufgaben aller Mitarbeiter gehört und nicht auf Reinigungspersonal oder Hausarbeiter gewartet werden sollte.

Prüffragen:

- Sind die Mitarbeiter über die zu verwendenden Verfahren und Geräte zur Löschung oder Vernichtung von Daten informiert?
- Sind typische Fehlerquellen erkannt und Lösungsansätze kommuniziert worden?

# M 3.68 Schulung der Administratoren eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um den Samba-Dienst korrekt und sicher administrieren zu können, ist eine Schulung der verantwortlichen Administratoren unumgänglich. Schon kleine Konfigurationsfehler können zu Sicherheitslücken führen. In Hinblick auf die Unterschiede der Unix- und Windows-Dateisysteme erfordert besonders die korrekte Konfiguration und Administration von Zugangsbeschränkungen gute Kenntnisse der vorhandenen Möglichkeiten und ihrer Limitierungen. Aufgrund der starken Interaktion zwischen den Sicherheitsmechanismen von Samba und des zugrunde liegenden Betriebssystems, müssen den Administratoren des Samba-Servers die Sicherheitsmechanismen des Betriebssystems bekannt sein. Dies gilt auch dann, wenn die Administratoren des Samba-Servers nicht gleichzeitig für die Administration des Betriebssystems zuständig sind.

Neben der allgemeinen Betriebssystemsicherheit sollten folgende Aspekte Gegenstand der Schulung sein:

- Methoden der Installation des Samba-Dienstes (Installation über die Paketverwaltung der eingesetzten Distribution, Kompilieren aus dem Quellcode).
- Konfigurationsmöglichkeiten des Samba-Dienstes, Syntax der Konfigurationsdateien.
- Mechanismen der Benutzerauthentisierung beim Samba-Dienst, Einsatzgebiete, Vor- und Nachteile der einzelnen Mechanismen.
- Funktionsweise der Protokolle, die in einer Windows NT4-Domäne und einer Active Directory Domäne zum Einsatz kommen.
- Potentielle Schwachstellen der Protokolle, die in einer NT4-Domäne und einer Active Directory Domäne zum Einsatz kommen. Beispielsweise muss den Administratoren vermittelt werden, dass die Datenübertragung über das Server Message Block (SMB)-Protokoll immer unverschlüsselt erfolgt.
- Unterschiede der Dateisysteme, die unter Windows und Unix eingesetzt werden und wie Samba diese Unterschiede behandelt.
- Zusammenspiel von Zugangsbeschränkungen in der Samba-Konfiguration mit Zugriffsberechtigungen auf Dateisystemebene.
- Maßnahmen zur Sicherstellung der Verfügbarkeit eines Samba-Servers.

Prüffragen:

- Kennen die Administratoren die entsprechenden sicherheitsrelevanten Aspekte eines Samba-Server, wie z. B. dass das SMB-Protokoll keine Verschlüsselung der übertragenen Daten unterstützt?
- Sind die Administratoren im Umgang mit dem genutzten Betriebssystem und seinen sicherheitsrelevanten Aspekten geschult?
- Kennen die Administratoren die verschiedenen Möglichkeiten, Samba zu installieren und konfigurieren?
- Kennen die Administratoren die Mechanismen zur Benutzerauthentisierung bei Samba-Servern?
- Beherrschen die Administratoren die Protokolle, die in einer Windows NT 4.0 Domäne und in einer Active Directory Domäne zum Einsatz kommen, und kennen sie deren Schwachstellen?

- Kennen die Administratoren die Unterschiede der Dateisysteme, die unter Windows und Unix zum Einsatz kommen, und wissen sie, wie Samba diese Unterschiede behandelt?
- Verstehen die Administratoren das Zusammenspiel von Zugriffsberechtigungen in der Samba-Konfiguration mit der Konfiguration der Zugriffsberechtigungen auf Dateisystemebene?
- Sind die Administratoren mit Maßnahmen zur Sicherstellung der Verfügbarkeit eines Samba-Servers vertraut?

# M 3.69 Einführung in die Bedrohung durch Schadprogramme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Schadprogramme sind Programme, die ohne Einwilligung und Wissen des Benutzers auf dessen Rechner schädliche Funktionen ausführen. Meist sind Schadprogramme dabei getarnt und werden heimlich auf einem Rechner ausgeführt. Schadprogramme werden für unterschiedlichste Ziele eingesetzt. Unter anderem werden sie zur Fernsteuerung von Systemen, zum Ausforschen von Passwörtern, zum Sammeln von Daten, aber auch zum Aufzeichnen von Tastatureingaben verwendet.

Im folgenden wird der Begriff Viren-Schutzprogramm verwendet, gemeint ist jedoch ein Programm zum Auffinden jeglicher Schadsoftware. Die nachfolgende Verwendung des Begriffs Schadprogramm schließt die Computer-Viren mit ein.

Schadprogramme können eine Vielzahl unterschiedlicher Schadfunktionen enthalten, die bei einem Angriff auch kombiniert werden können. Anhand der folgenden Merkmale lassen sich Schadprogramme klassifizieren:

**Viren**

Ein Virus (auch Computer-Virus) ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewusst gesteuert auftreten. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen von größter Tragweite.

Die Eigenschaft der Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung "Virus". Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig ist das Überschreiben von Daten oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems. Computer-Viren können im Prinzip bei allen Betriebssystemen auftreten. Aufgrund der starken Verbreitung liegt die größte Bedrohung jedoch im Bereich der Personalcomputer (PC) mit x86-Architektur.

Es werden mehrere Grundtypen von Computer-Viren unterschieden, wobei diese auch in Misch- und Sonderformen auftreten können:

**Boot-Viren**

Boot-Viren befinden sich im Bereich des Boot-Sektors oder Master Boot Records eines Speichermediums, beispielsweise einer Festplatte. Beim Bootvorgang werden unter anderem Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst nicht zugänglichen und im Inhaltsverzeichnis des Speichermediums nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben diese mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert. Ein Boot-Virus wird aktiv, noch bevor das Betriebssystem komplett geladen ist.

**Datei-Viren**

Die meisten Datei-Viren (auch File-Viren genannt) lagern sich an Programmdateien an. Datei-Viren werden beim Aufruf einer infizierten Datei gestartet und verbreiten sich dadurch. Anschließend wird das Originalprogramm gestartet, so das es für den Benutzer so aussieht, als würde das Programm wie gewohnt starten. Es sind jedoch auch primitivere, überschreibende Viren bekannt, die sich an den Anfang des Wirtsprogramms setzen, so dass dieses nicht mehr fehlerfrei läuft.

Datei-Viren können unterschiedlichste Schadfunktionen beinhalten, unter anderem können sie z. B. Dateien löschen oder die Festplatte formatieren. Statt sich an vorhandene Dateien anzulagern, kopieren sich mittlerweile viele Datei-Viren als eigene Datei in das Betriebssystem. Durch Manipulation an den Einstellungen des Betriebssystems (z. B. über Autostart-Einträge) stellen solche Datei-Viren sicher, dass sie zukünftig ausgeführt werden.

**Makro-Viren**

Auch Makro-Viren sind in Dateien enthalten. Makro-Viren infizieren jedoch nicht die Anwendungsprogramme selbst, sondern die damit erzeugten Dateien. Betroffen sind alle Anwendungsprogramme, bei denen in die erzeugten Dateien nicht nur einzelne Steuerzeichen, sondern auch Programme eingebettet werden können (z. B. Microsoft Office, StarOffice/OpenOffice). Einige Datenformate können auch Objekte enthalten, die ihrerseits Programme enthalten können. Durch solche geschachtelten Einbettungen können ebenfalls Viren in Dateien gelangen.

Makros sind Programme, mit deren Hilfe das Anwenderprogramm um zusätzliche Funktionen erweitert werden kann, die auf den Anwendungsfall zugeschnitten sind (z. B. Erzeugen einer Reinschrift aus dem Entwurf eines Textes). Makro-Viren werden beim Arbeiten mit den Dateien gestartet. Häufig verbreiten sich Dateien mit Makro-Viren über E-Mail, das Internet, aber auch über CDs oder USB-Sticks.

**Skript-Viren**

Ein Skript ist ein Programm, das von einem Interpreter ausgeführt wird. Häufig werden solche Skripte auf Web-Servern oder eingebettet in Web-Seiten (z. B. JavaScript) verwendet. Diese Skripte werden meist unbemerkt ausgeführt und können unter Umständen von Angreifern missbraucht werden, um Schadsoftware auf das IT-System zu laden.

**Bot-Viren**

Bei einem Bot-Virus handelt es sich um ein Programm, das meist heimlich, zum Beispiel beim Besuch einer infizierten Web-Seite, installiert wird. Ein Bot-Virus kann beispielsweise heimlich E-Mails versenden, Daten ausspionieren oder aber mit anderen Bots im Netz kommunizieren, um DDoS-Angriffe (Distributed Denial-of-Service) durchzuführen. Viele Bots verhalten sich zunächst ziemlich unauffällig, so dass die Benutzer nichts Ungewöhnliches bemerken. Doch Angreifer können gezielt Bots "aktivieren", indem sie Kommandos an den jeweils befallenen PC versenden. Der Name "Bot" leitet sich vom Begriff "Robot" ab.

**Stealth-Viren**

Stealth-Viren werden auch als Tarnkappen-Viren bezeichnet. Stealth-Viren versuchen, sich vor einer möglichen Entdeckung zu schützen, indem sie z.

B. Viren-Schutzprogramme erkennen und beim Scannen der infizierten Datei ihren Code aus der Datei entfernen, um diesen erst nach dem Scan wieder hinzuzufügen.

**Polymorphe Viren**

Polymorphe Viren gehören zu den gefährlichsten Arten von Viren. Sie ändern bei jeder neuen Infektion ihr Erscheinungsbild durch Verschlüsselung oder Permutation und sind dadurch für Virenscanner schwer zu erkennen. Üblicherweise verschlüsseln Polymorphe Viren ihren Schadenscode bei jeder Infektion neu. Auch der Kodierungsschlüssel wird meist bei jeder Infektion neu erstellt, wobei die Routine, die die Schlüssel neu erstellt, auch selbst im verschlüsselten Code des Virus abgelegt ist.

**Retro-Viren**

Um sich selbst vor einer Erkennung durch Viren-Schutzprogramme oder Firewalls zu schützen, versuchen Retro-Viren, diese zu deaktivieren oder zu manipulieren. Durch die Deaktivierung können z. B. andere Schadprogramme unbemerkt nachgeladen werden.

**Würmer**

Würmer sind selbstständige und selbstreproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten. Würmer benötigen im Gegensatz zu Viren keinen Wirt. In der Regel stehlen Würmer Rechenzeit oder Übertragungskapazität. Dadurch können sie innerhalb kürzester Zeit viele Computer beeinträchtigen und einen großen wirtschaftlichen bzw. finanziellen Schaden verursachen.

**Trojanische Pferde**

Ein Trojanisches Pferd (oft auch verkürzt als "Trojaner" bezeichnet) ist ein Programm mit einer Schadfunktion, das in ein anderes Programm verdeckt eingebettet ist. Trojanische Pferde werden verbreitet, indem sie in möglichst "attraktive" Wirtsprogramme integriert werden, die dann beispielsweise zum Download angeboten oder als Anhang per E-Mail verschickt werden. Trojanische Pferde können nicht nur unmittelbare Schäden verursachen, sondern auch Informationen über einzelne Rechner oder über das lokale Netz ausspähen.

**Rootkits**

Unter Unix bezeichnet man mit "root" den Administrator, der weitgehende Zugangs- und Zugriffsrechte hat. Ein Rootkit ist eine Sammlung von Werkzeugen, die dazu verwendet werden, ohne Wissen des Benutzers möglichst uneingeschränkten Zugriff auf das System zu erhalten. Auch wenn der Begriff "Rootkit" in der Unix-Welt entstanden ist, gibt es heutzutage eine Vielzahl von Windows-Rootkits. Sie verändern zum Beispiel Systemdateien oder ermöglichen es einem Angreifer, die Kontrolle über das infizierte System zu erlangen. Anschließend kann der Angreifer beispielsweise versuchen, weitere Schadprogramme über das infizierte System zu versenden.

**Backdoor**

Eine Backdoor ist eine "Hintertür", die es einem Angreifer ermöglicht, Zugang zu einem Computer oder zu Funktionen von Programmen zu erhalten. Backdoors können unter anderem im Betriebssystem oder in Anwendungsprogrammen installiert werden. Meist wird eine Backdoor dazu verwendet, um weitere

Schadprogramme, wie zum Beispiel ein Trojanisches Pferd, auf einem Computer zu hinterlassen.

**Spyware**

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an Unberechtigte weiterleiten. Spyware gilt häufig als lästig, aber nicht als so gefährlich wie Viren, Würmer oder Trojanische Pferde. Durch Spyware können aber durchaus Sicherheitsprobleme entstehen, was sich beispielsweise in der unbemerkten Weitergabe von persönlichen Daten, aber auch durch die damit verbundenen unerlaubten Eingriffe in das IT-System zeigt. Unter anderem kann die Systemkonfiguration, z. B. in der Windows Registry, geändert werden, oder es kann ausführbarer Code eingespielt werden, beispielsweise DLLs, ActiveX- oder Java-Objekte. Spyware gelangt in vielen Fällen durch unberechtigtes Herunterladen von Software, Updates oder sonstigen Dateien (Musik oder Dokumente aus zweifelhaften Quellen) aus dem Internet auf das IT-System.

In Spyware können auch Programme zum Mitschneiden von Tastatureingaben, sogenannte Keylogger, integriert sein. Hierbei werden alle Tastatureingaben aufgezeichnet und möglichst unbemerkt an den Angreifer übermittelt. Dieser entnimmt dann aus den mitgeschnittenen Informationen die für ihn wichtigen Daten, wie z. B. Anmelde-Informationen oder Kreditkartennummern.

**Dialer**

Kostenpflichtige Internet-Angebote wurden in der Vergangenheit häufig über die Telefonrechnung abgerechnet, indem die Benutzer über spezielle Einwahl-Programme auf kostenpflichtige Telefonnummern umgelenkt wurden. In Deutschland waren dies beispielsweise Nummern mit der Vorwahl 0190 oder 0900.

Die dafür benutzten Dialer sind Programme, die auf dem Rechner einen neuen Internetzugang einrichten. Nach dem Download und der Installation auf dem PC wählt sich der Dialer ins Internet ein. Eine zu dieser Zeit bereits bestehende Internetverbindung wird in der Regel zuvor getrennt. (Dies funktioniert allerdings nur über Wählzugänge, nicht jedoch über DSL oder ähnliche Techniken.) Die kostenpflichtigen Inhalte können dann über die neue Verbindung abgerufen werden. Dabei ist die vom Dialer benutzte Einwahlnummer maßgeblich für die Höhe der anfallenden Kosten. Sowohl pro Einwahl als auch pro Zeiteinheit können hohe Gebühren anfallen.

Durch die Verbreitung von DSL haben Dialer stark an Bedeutung verloren.

**Scareware**

Scareware setzt sich aus den englischen Wörtern "Scare" (deutsch: Schrecken) und "Software" zusammen. Scareware dient in erster Linie dazu, Benutzer zu verunsichern oder ihnen Angst zu machen. Dem Benutzer wird zum Beispiel beim Besuch einer Web-Seite eine Warnmeldung angezeigt, dass sein PC von einem Virus befallen ist. Gleichzeitig wird ihm zur Virusbeseitigung ein kostenloses Viren-Schutzprogramm angeboten. Dieses Programm beinhaltet dann das eigentliche Schadprogramm. Oder aber es werden dem Benutzer kostenpflichtige, meist funktionslose Programme zur Beseitigung des angeblich gefundenen Schadprogrammes angeboten.

Es ist zu beachten, dass die oben aufgeführten Merkmale von Schadprogrammen lediglich Beispiele sind, die in der Praxis häufig auftreten. Im konkreten

Einzelfall kann ein Schadprogramm durchaus andere oder zusätzliche Funktionen enthalten.

In den letzten Jahren sind durch die komplexer werdenden Verbreitungsmechanismen aktueller Schadsoftware die Unterscheidungen zwischen Viren, Würmern und Trojanischen Pferden unscharf geworden. Bei einem Angriff kommen in der Regel verschiedene, modular aufgebaute Programme nacheinander oder zeitgleich zum Einsatz. Die Hersteller von Viren-Schutzprogrammen benutzen deshalb häufig den Sammelbegriff "Malware" (Malicious Software) oder ganz allgemein Schadsoftware oder Schadprogramme.

# M 3.70 Einführung in die Virtualisierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Mit der so genannten Virtualisierung von IT-Systemen steht eine Technik zur Verfügung, mit der ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben werden können. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Diese Technik wird bereits seit den 1970er Jahren bei den Mainframes (z. B. IBM zSeries) eingesetzt. Sie hat aber erst Ende der 1990er Jahre im Bereich der Midrange Server weitere Verbreitung gefunden. Beispiele für Software-Produkte zur Virtualisierung von IT-Systemen mit x86-Architektur sind Microsoft Virtual PC/Server, Parallels Virtuozzo, Sun VirtualBox, VMware Workstation/Server/ESX und Xen. Ein weiteres Beispiel ist SUN Solaris Zones, das für die SPARC- und INTEL-Plattformen von Solaris verfügbar ist. Für die Enterprise Serie der SUN Server ist des Weiteren eine hardwaregestützte Virtualisierung (hier Partitionierung genannt) über die Verwendung so genannter Domains möglich. Im Bereich der zSeries-Großrechner kann eine Virtualisierung beispielsweise über die Nutzung von Logical Partitions (LPARs, hardwaregestützte Virtualisierung) oder über das Produkt z/VM (softwaregestützt) erfolgen (siehe auch B 3.107 *S/390- und zSeries-Mainframe*).

Die Virtualisierungstechnik hat sich sehr schnell als strategisches Mittel zur besseren Auslastung und Konsolidierung von Serversystemen durchgesetzt, da sie es ermöglicht, viele Dienste auf einem physischen Serversystem zu konzentrieren, ohne dass die Aufteilung der Dienste auf einzelne IT-Systeme aufgegeben werden muss. Dadurch werden die Ressourcen der physischen Server besser ausgenutzt und es können vielfach Einsparungen im Serverbetrieb erreicht werden. Diese Einsparungen beziehen nicht nur auf die Anzahl der einzusetzenden physischen IT-Systeme sondern auch auf die Stromkosten, den Platz in Serverräumen und Rechenzentren sowie die Klimatisierung. Weiterhin ist es möglich, durch die Virtualisierung Prozesse zur Bereitstellung neuer Server zu beschleunigen, da beispielsweise nicht für jedes neue Serversystem eine Bestellung durchgeführt werden muss. Bei einigen Virtualisierungslösungen können virtuelle IT-Systeme kopiert werden, wodurch Installationsprozesse vereinfacht werden können, oder es können so genannte Snapshots von virtuellen IT-Systemen angelegt werden, die es ermöglichen, nach einer fehlerhaften Konfigurationsänderung schnell den ursprünglichen Zustand wiederherzustellen.

Mehrere Virtualisierungsserver können des Weiteren zu einer so genannten virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur werden mehrere Virtualisierungsserver gemeinsam mit den darauf laufenden virtuellen IT-Systemen verwaltet. Damit sind weitere Funktionen möglich. Beispielsweise können virtuelle IT-Systeme von einem Virtualisierungsserver auf einen anderen verschoben werden. Dies kann teilweise auch dann durchgeführt werden, während das virtuelle IT-System in Betrieb ist (*Live Migration*). Weiterhin gibt es Möglichkeiten, die Verfügbarkeit der virtuellen IT-Systeme zu steigern. So können mittels der *Live Migration* virtuelle Systeme immer auf den Virtualisierungsserver verschoben werden, der gerade die beste Performance für den Betrieb des virtuellen Systems zur Verfügung stellen kann. Eine weitere Möglichkeit besteht darin, virtuelle IT-Systeme automatisch auf einem anderen Virtualisierungsserver neu zu starten, wenn der ursprüngliche Virtualisierungsserver beispielsweise wegen eines Hardwaredefekts ausgefallen ist.

Die reichhaltigen Möglichkeiten zu Manipulation der virtuellen IT-Systeme durch die Virtualisierungssoftware lassen Virtualisierungsserver besonders für den Aufbau von Test- und Entwicklungsumgebungen geeignet erscheinen. Es ist mittels der Virtualisierung möglich, für Test- und Entwicklung schnell IT-Systeme bereitzustellen und komplexe Umgebungen schnell und effizient aufzubauen. Weiterhin können produktive virtuelle IT-Systeme für eine Test- und Entwicklungsumgebung kopiert werden, damit Aktualisierungen und Anpassungen ohne Störungen des Produktivbetriebes getestet werden können.

**Voraussetzungen für den Betrieb virtueller IT-Systeme auf einem Virtualisierungsserver**

Um verschiedene virtuelle IT-Systeme auf einem Virtualisierungsserver sicher nebeneinander betreiben zu können, muss die Virtualisierungssoftware bestimmte Voraussetzungen erfüllen. Die Virtualisierungssoftware muss dafür sorgen, dass

- sich jedes virtuelle IT-System für die darin ablaufende Software nahezu wie ein eigenständiger physischer Computer darstellt (Kapselung),
- die einzelnen virtuellen IT-Systeme voneinander isoliert werden und nur über festgelegte Wege miteinander kommunizieren können (Isolation),
- die einzelnen virtuellen IT-Systeme in geordneter Weise auf die Ressourcen der Hardware zugreifen können.

Abhängig davon, wie die Virtualisierung der Ressourcen realisiert ist, werden diese Funktionen der Virtualisierungsschicht möglicherweise nur eingeschränkt erfüllt. So gibt es beispielsweise Lösungen, bei denen die Betriebssystem-Software leicht angepasst werden muss, bevor sie in einem virtuellen IT-System laufen kann. Ein anderes Beispiel für Einschränkungen bei der Virtualisierung sind Lösungen, bei denen alle virtuellen IT-Systeme auf einem Virtualisierungsserver verschiedene Instanzen des gleichen Betriebssystems verwenden müssen.

Die Virtualisierungsschicht muss nicht notwendigerweise eine reine Software-Komponente sein. Bei einigen Plattformen unterstützt auch die Hard- oder Firmware die Virtualisierung der Ressourcen. Die Virtualisierungsschicht stellt den virtuellen IT-Systemen in der Regel konfigurierbare Zugriffsmöglichkeiten auf lokale Laufwerke und Netzverbindungen zur Verfügung. Dies erlaubt es den virtuellen IT-Systemen, miteinander und mit fremden IT-Systemen zu kommunizieren.

In der Praxis werden zwei Arten von Virtualisierungssoftware unterschieden, die Servervirtualisierung und die Betriebssystemvirtualisierung.

**Servervirtualisierung**

Die Servervirtualisierung bildet die Basis für virtuelle IT-Systeme, die meist eine vom Virtualisierungsserver abstrahierte, virtualisierte und vollständige Hardwareumgebung besitzen. In dieser virtuellen Hardwareumgebung wird ein vollständiges Betriebssystem installiert, auf dem dann im Folgenden Anwendungen auf gewohnte Weise betrieben werden können.

In der Regel ist das Betriebssystem, das auf dem virtuellen IT-System installiert werden kann, völlig unabhängig von dem Betriebssystem, unter dem die Virtualisierungssoftware betrieben wird. Der Zugriff des virtuellen IT-Systems auf die Ressourcen (Prozessor, Arbeitsspeicher, Massenspeicher, Netz) des Virtualisierungsservers wird durch die Virtualisierungssoftware gesteuert. Dazu erhält jedes virtuelle IT-System virtuelle Geräte, die den Zugriff auf diese Ressourcen erlauben. Diese Geräte werden entweder vollständig emuliert,

oder es werden die physischen Geräte durch die Virtualisierungssoftware an das virtuelle IT-System weiter gereicht. Im jedem Fall sorgt die Virtualisierungssoftware dafür, dass die physischen Geräte auf geordnete Weise durch die virtuellen IT-Systeme genutzt werden können, so dass sich diese gegenseitig möglichst wenig beeinflussen können. Die Treiber, mit denen die virtuellen IT-Systeme auf die Hardwarekomponenten des Virtualisierungsservers zugreifen, müssen in der Regel nach der Betriebssysteminstallation innerhalb der virtuellen IT-Systeme nachinstalliert werden.

Bei der Servervirtualisierung wird zwischen so genannten hypervisorbasierten (Typ 1-) und hostbasierten (Typ 2-) Virtualisierungsprodukten unterschieden. Bei den hypervisorbasierten Virtualisierungsprodukten wird auf der physischen Hardware nur ein auf die Virtualisierung spezialisiertes Rumpf-Betriebssystem, der so genannte Hypervisor, installiert. Dieser erzeugt die für den Betrieb der virtuellen IT-Systeme notwendige virtuelle Hardware-Umgebung und steuert den Zugriff der virtuellen IT-Systeme auf die physischen Ressourcen. Bei den hostbasierten Virtualisierungsprodukten wird der Hypervisor als Dienst in einem voll ausgestatteten und nicht auf den Verwendungszweck optimierten Betriebssystem installiert.

**Betriebssystemvirtualisierung**

Die Betriebssystemvirtualisierung unterscheidet sich von der Servervirtualisierung sehr stark in der Art, wie die virtuellen IT-Systeme erzeugt werden. Die Servervirtualisierung stellt den virtuellen IT-Systemen eine vollständige Hardwareumgebung zur Verfügung. Die Betriebssystemvirtualisierung hingegen stellt eine Lösung dar, in der den virtuellen IT-Systemen isolierte Instanzen des Betriebssystems zur Verfügung gestellt werden, auf dem das Virtualisierungsprodukt installiert wurde. Daher sind beispielsweise für den Zugriff auf die Hardwarekomponenten des physischen Systems in der Regel keine speziellen Treiber notwendig, da die Hardwarekomponenten unverändert an das virtuelle IT-System "durchgereicht" werden. Die Virtualisierungssoftware steuert hier nur den Zugriff, so dass sich die virtuellen IT-Systeme nicht gegenseitig beeinflussen.

Durch diese Art der Virtualisierung ergeben sich einige Einschränkungen für die virtuellen IT-Systeme, die mittels einer Betriebssystemvirtualisierungslösung betrieben werden. Es ist in der Regel nicht möglich, unterschiedliche Betriebssysteme in den auf einem Virtualisierungsserver laufenden IT-Systemen zu nutzen, da das Betriebssystem vom Virtualisierungsserver übernommen werden muss. Bei einigen Produkten können allerdings unterschiedliche Kernelversionen des gleichen Betriebssystems auf einem Virtualisierungsserver genutzt werden.

Bei beiden Virtualisierungstechniken steht für die Administration des Virtualisierungsservers, des Hypervisors und der virtuellen IT-Systemen eine Verwaltungssoftware zur Verfügung. Dies kann eine webbasierte Verwaltungsoberfläche, eine spezielle Verwaltungssoftware oder auch eine kommandozeilen-basierte Benutzerschnittstelle sein. Bei einigen Typ 1-Servervirtualisierungsprodukten wird diese Verwaltungsschnittstelle als virtuelles IT-System unter der vollständigen Kontrolle des Hypervisors ausgeführt.

**Vergleich von Server- und Betriebssystemvirtualisierung**

Der große Vorteil der Betriebssystemvirtualisierung ist es, dass auf dem Virtualisierungsserver so gut wie keine Ressourcen für die Emulation einer virtuellen Hardware benötigt werden, so wie es bei der Servervirtualisierung der Fall ist. Dadurch können mit der Betriebssystemvirtualisierung deutlich mehr

virtuelle IT-Systeme auf einem physischen System betrieben werden als bei der Servervirtualisierung. Dies ermöglicht einen höheren Verdichtungsgrad, also ein höheres Verhältnis von virtuellen zu physischen IT-Systemen.

Wesentliche Nachteile der Betriebssystemvirtualisierung sind allerdings die geringere Flexibilität bei der Verwendung unterschiedlicher Betriebssysteme sowie die schwächere Kapselung der virtuellen IT-Systeme. Für den Einsatz unterschiedlicher Anwendungen innerhalb der virtuellen IT-Systeme können daher ebenfalls Einschränkungen bestehen. Dies hängt im Wesentlichen damit zusammen, dass die Verzahnung von virtuellen IT-Systemen und Virtualisierungsserver stärker ist als bei der Servervirtualisierung. Bei der Betriebssystemvirtualisierung werden häufig viele Teile des Betriebssystems des Virtualisierungsservers gemeinsam mit den virtuellen IT-Systemen genutzt. So werden meist die gleichen Software-Bibliotheken und Betriebssystemkomponenten genutzt, bei einigen Virtualisierungsprodukten werden z. B. Software-Bibliotheken nur einmal im Arbeitsspeicher des physischen Systems gehalten und von allen virtuellen IT-Systemen genutzt.

Die Kapselung der virtuellen IT-Systeme ist daher bei der Betriebssystemvirtualisierung im Vergleich mit der Servervirtualisierung geringer ausgeprägt. In der Folge kann auch die Isolation der virtuellen IT-Systeme untereinander und im Verhältnis zum Virtualisierungsserver weniger stark sein.

Bei der Servervirtualisierung ist der Ressourcenverbrauch pro virtuellem IT-System auf dem Virtualisierungsserver in der Regel höher als bei der Betriebssystemvirtualisierung. Der Aufwand zur Wartung und Pflege (Beispiel: Einspielen von Softwareaktualisierungen) der virtuellen IT-Systeme ist ebenfalls höher, da diese auf Grund der starken Kapselung häufig für jedes virtuelle IT-System einzeln erfolgen muss. Bei der Betriebssystemvirtualisierung können solche Softwareaktualisierungen teilweise durch Installation des Patches auf dem Virtualisierungsserver in allen virtuellen IT-Systemen mit installiert werden.

Weiterhin wird die größere Flexibilität der Servervirtualisierungslösungen mit einem höheren Komplexitätsgrad erkauft. Diese höhere Komplexität ergibt sich durch den etwas höheren Aufwand, mit dem Virtualisierungsserver für eine Servervirtualisierung in die Infrastruktur des Informationsverbundes integriert werden müssen. Die Verfahrensweisen für die Integration dieser Systeme in Netze und Speichernetze sind in der Regel komplexer. Des Weiteren müssen bestehende Prozesse zum Ausrollen neuer IT-Systeme möglicherweise angepasst werden.

Daher eignet sich die Betriebssystemvirtualisierung dann besonders gut, wenn eine große Menge gleichartiger virtueller IT-Systeme benötigt wird, beispielsweise viele gleich oder ähnlich konfigurierte Webserver. Die Servervirtualisierung kann ihre Vorteile dann ausspielen, wenn viele verschiedene virtuelle IT-Systeme betrieben werden müssen. Sollen heterogene Serverlandschaften virtualisiert werden, existiert häufig keine Alternative zur Servervirtualisierung.

**Netzwerkintegration der Virtualisierungsserver und virtuellen IT-Systeme**

Bei den verschiedenen Virtualisierungslösungen bestehen viele unterschiedliche Methoden, den virtuellen IT-Systemen Zugriff auf die Netze des Informationsverbundes zu ermöglichen. Im Wesentlichen können zwei Prinzipien unterschieden werden, wie diese Netzverbindungen realisiert werden.

- Den virtuellen IT-Systemen werden direkt physische Netzschnittstellen des Virtualisierungsservers zugeordnet. Hierbei sind die virtuellen IT-Sy-

steme direkt mit dem Netz verbunden, mit dem der Virtualisierungsserver selbst verbunden ist.
- Die physischen Netzschnittstellen werden indirekt mit den virtuellen IT-Systemen verbunden. Dabei wird ein virtueller Switch durch den Hypervisor erzeugt, mit dem die virtuellen Netzschnittstellen der virtuellen IT-Systeme verbunden sind. Dieser virtuelle Switch wiederum kann mittels einer physischen Netzschnittstelle des Virtualisierungsserver mit dem physischen Netz verbunden werden. Es ist mit dieser Technik auch möglich, virtuelle Switche und Netze zu definieren, die keine Verbindung in das physische Netz des Informationsverbundes haben.

Diese zwei unterschiedlichen Netzintegrationstechniken haben unterschiedliche Auswirkungen darauf, wie die Integration der virtuellen IT-Systeme und der Virtualisierungsserver in das Netz des Informationsverbundes vorgenommen werden muss. Besonders mit der zweiten Variante ist es möglich, flexibel auf unterschiedliche Schutzbedarfsanforderungen der virtuellen IT-Systeme zu reagieren.

**Gastwerkzeuge**

Viele Hersteller stellen für die virtuellen IT-Systeme so genannte Gastwerkzeuge zur Verfügung, mit denen die virtuellen IT-Systeme auf einfache Weise durch die Virtualisierungssoftware gesteuert werden können. Diese Werkzeuge ermöglichen es beispielsweise, virtuelle IT-Systeme über die Virtualisierungssoftware herunterzufahren, ohne dass mit dem virtuellen System direkt interagiert werden muss. Weitere Funktionen sind z. B. der Austausch der Zwischenablage zwischen virtuellem IT-System und dem Rechner des Benutzers des virtuellen IT-Systems oder der vereinfachte Zugriff auf Datenträger wie CD- oder DVD-ROMs, die in die entsprechenden Laufwerke des Virtualisierungsservers oder des Rechners des Benutzers des virtuellen IT-Systems eingelegt werden. Die Treiber für den Zugriff auf die virtualisierte Hardware und die Werkzeuge zur Steuerung der virtuellen IT-Systeme werden häufig als ein integriertes Installationspaket bereitgestellt.

# M 3.71 Schulung der Administratoren virtueller Umgebungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Virtuelle Infrastrukturen stellen ein wichtiges Infrastrukturelement in einem Rechenzentrum dar. Sie bieten ein deutliches Einsparpotenzial gegenüber herkömmlichen Serverstrukturen und finden eine hohe Verbreitung in Rechenzentren. Daher sollte sichergestellt werden, dass alle mit der Administration der Virtualisierungskomponenten betrauten Personen ausreichende Kenntnisse über die der virtuellen Infrastruktur zugrunde liegenden Produkte besitzen.

Virtualisierungsserver haben einen hohen Komplexitätsgrad. Neben virtuellen IT-Systemen enthalten sie auch einen Hypervisor sowie Netzkomponenten wie beispielsweise virtuelle Switches und eigene Dienste. Da Fehlkonfigurationen auf Virtualisierungsservern häufig gravierende Folgen für die darauf betriebenen virtuellen IT-Systeme haben, erhöhen sich die Anforderungen an die Administratoren der Virtualisierungsumgebung. Daher ist es wichtig, dass diese Administratoren ausreichend geschult sind, damit sie Probleme aus eigenem Handeln heraus vermeiden, technische Probleme rechtzeitig erkennen und beseitigen sowie die Funktionen und Sicherheitsmerkmale der Virtualisierungswerkzeuge optimal nutzen. Sie werden dadurch in die Lage versetzt, die Funktionen des jeweiligen Virtualisierungsproduktes zu beherrschen und die Folgen von Konfigurationsänderungen abzuschätzen.

Die Schulungen sollen ausreichende Kenntnisse für die Planung, den Aufbau und den Betrieb der für den Einsatz ausgewählten Virtualisierungsumgebung vermitteln.

Auch bei einer Aufteilung von Administratorenrollen (siehe M 2.446 *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*) müssen alle Administratoren die Grundlagen der ausgewählten Virtualisierungstechnik beherrschen, da die bislang vorherrschende Trennung von Fachbereichen wie Server-, Netz- und Speicherbetrieb aufgelöst wird.

Bereits bei der Planung einer Virtualisierungsumgebung sollte ein ausreichendes Budget für Schulungsmaßnahmen einkalkuliert werden. Ebenfalls sollten Zeiträume für die Schulungen rechtzeitig eingeplant werden, um personelle Ressourcenengpässe zu vermeiden.

Schulungen zur Virtualisierung von IT-Systemen sollten mindestens folgende Elemente enthalten:

- Grundlagen und Konzepte des jeweiligen Virtualisierungssystems
- Erstellung und Umsetzung von internen Richtlinien und Regelungen zum Rechenzentrumsbetrieb
- Kenntnisse der Kommandos oder der Benutzeroberfläche der jeweiligen Komponenten.
- Planung einer Virtualisierungsumgebung in Bezug auf die Netzdimensionierung und -absicherung sowie die Dimensionierung der Hardware für CPU-, RAM-, Netz- und Speichernetzressourcen
- Vorbereiten des Betriebssystems des Virtualisierungsservers
- Installation und Konfiguration des Virtualisierungssystems
- Installation der Betriebssysteme in dem virtuellen IT-System
- Netzkonfiguration des virtuellen IT-Systems

- Betrieb
- Überwachung, Verwaltung
- Protokollierung
- Sicherung und Verwaltung von Konfigurationen
- Sicherung virtueller Maschinen
- Automatisierungsprozesse
- Analyse und Fehlerbehandlung

Es sollte darauf geachtet werden, dass die Schulung neben der Theorie ausreichende praktische Anteile enthält.

Prüffragen:

- Werden Schulungen für die Administratoren virtueller Umgebungen mit den empfohlenen Mindestinhalten durchgeführt?
- Sind die Administratoren der Virtualisierungsumgebung ausreichend geschult, sodass sie Probleme aus eigenem Handeln heraus vermeiden, technische Probleme rechtzeitig erkennen und die Funktionen und Sicherheitsmerkmale der Virtualisierungswerkzeuge optimal nutzen können?

# M 3.72 Grundbegriffe der Virtualisierungstechnik

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Der Begriff "Virtualität" und das dazugehörige Adjektiv "virtuell" werden in der Computertechnologie schon sehr lange in sehr unterschiedlichen Anwendungsfällen verwendet. In den meisten Szenarien wird ein Objekt mit der Eigenschaft "virtuell" versehen, wenn es zwar physisch nicht vorhanden, seiner Wirkung nach jedoch existent erscheint. Somit kann ein virtuelles Objekt durchaus reale Auswirkungen haben, also die Realität verändern oder mit der Realität interagieren. Daher sind die Begriffe "Virtualität" und "Realität" nicht als Gegensätze zu begreifen. Als "Virtualisierung" wird auch der Prozess verstanden, bei dem ein Objekt von einem realen in ein virtuelles transformiert wird oder von vornherein in virtueller Form bereitgestellt wird.

Speziell in der Informationstechnik wird die Virtualisierung von Objekten als technische Substitution dieser Objekte (Ersetzung durch etwas Gleichwertiges oder Gleichwirkendes) verwendet. Wird beispielsweise realer Arbeitsspeicher eines IT-Systems durch virtuellen Arbeitsspeicher substituiert (gleichwertig ersetzt), kann dieser wie der reale verwendet werden, obwohl er beispielsweise auf der Festplatte des Systems als Datei repräsentiert wird. Diese Datei ist tatsächlich kein realer Arbeitsspeicher, ist aber in ihrer Wirkung dem Arbeitsspeicher gleich. Diese Technik wird angewendet, um mehr Arbeitsspeicher verwenden zu können, als tatsächlich vorhanden ist. Durch die Nutzung virtuellen Arbeitsspeichers können allerdings Performancenachteile entstehen. Es existieren noch viele weitere Beispiele für virtualisierte Ressourcen wie VLANs, VPNs oder auch virtuelle Prozessoren (*Intel Hyperthreading*).

In der Vergangenheit ist, wie aus den Beispiel im vorigen Absatz deutlich wird, die Virtualisierung hauptsächlich verwendet worden, um knappe und teure Ressourcen durch solche zu substituieren, die im Übermaß vorhanden oder preiswerter zu beschaffen waren. Mittlerweile hat sich allerdings die Computertechnik und insbesondere die Performance der Rechner soweit entwickelt, dass das Konzept der Virtualisierung auch auf weitere Anwendungsfälle ausgedehnt wird. Der Computer kann mit Hilfe einer entsprechenden Virtualisierungssoftware als universelles Werkzeug eingesetzt werden, um sehr viele Objekte zu virtualisieren, insbesondere den Computer selbst.

### Kapselung und Isolation

Isolation und Kapselung sind zwei wichtige Sicherheitsanforderungen an eine Virtualisierungslösung. Isolation bedeutet in diesem Zusammenhang, dass zwei virtuelle IT-Systeme, die auf dem gleichen Virtualisierungsserver ablaufen, nur über die hierzu vorgesehenen Mechanismen miteinander kommunizieren können. Isolation trägt unter anderem dazu bei, dass von einem virtuellen IT-System nicht unberechtigt auf die Daten eines anderen virtuellen IT-Systems zugegriffen werden kann.

Kapselung bedeutet im Kontext von Virtualisierung, dass jedes virtuelle IT-System nur mit den Ressourcen kommunizieren kann, die hierfür jeweils freigeschaltet sind. Ressourcen können dabei beispielsweise Hardware-Komponenten, Netzverbindungen oder Prozesse, die direkt auf dem Virtualisierungsserver laufen, sein. Die Kapselung trägt somit nicht nur zum Schutz virtueller IT-Systeme vor unberechtigten Zugriffen bei, sondern umgekehrt auch zum

Schutz der Ressourcen vor unberechtigten Zugriffen seitens der virtuellen IT-Systeme. Darüber hinaus dient die Kapselung auch der Portierbarkeit von virtuellen IT-Systemen.

Isolation und Kapselung sind eng verwandte Sicherheitsanforderungen, die auf technischer Ebene mit ähnlichen Mechanismen erreicht werden. In der Praxis wird zwischen den beiden Aspekten häufig nicht unterschieden.

**Systemvirtualisierung**

Durch das Überangebot an Leistung in modernen Rechneranlagen, die durch traditionelle Betriebssysteme und Anwendungen nicht mehr ausgelastet werden, entsteht der Wunsch, diese Leistungsreserven effizienter zu nutzen. Dies könnte beispielsweise durch die Kumulation von Anwendungen auf einem wenig ausgelasteten Rechnersystem geschehen. Aus guten Gründen (siehe auch M 4.97 *Ein Dienst pro Server*) ist eine solche Strategie zur Effizienzsteigerung abzulehnen: Solche Systeme würden nahezu unbeherrschbar, da Applikationen sich möglicherweise auf unvorhersehbare Weise gegenseitig beeinflussen, wenn sie auf einem Rechnersystem installiert sind. Werden sie getrennt betrieben, entstehen solche Beeinflussungen erst gar nicht. Veränderungen an den Betriebssystemen (z. B. Aktualisierungen oder Patches) müssen nicht mit einer Vielzahl von Anwendungen geprüft werden, sondern nur mit einer. Es ist weiterhin weitgehend ausgeschlossen, dass die Aktualisierung einer Anwendung Einfluss auf die Funktionsfähigkeit einer anderen Anwendung hat. Wird nun durch eine geeignete Technik dafür gesorgt, dass

- die auf einem einzelnen Rechnersystem naturgemäß gegebene gemeinsame **Kapselung** von Betriebssystem und Anwendung sowie
- die auf mehreren Rechnersystemen entstehende **Isolation** von Betriebssystem und Anwendungen auf diesen Rechnern voneinander

erhalten bleibt, wenn diese Rechnersysteme als virtuelle Instanzen auf einem Rechnersystem betrieben werden, verbleiben die Vorteile der Aufteilung auf einzelne Rechnersysteme. Die Ausnutzung der Rechnerressourcen wird hingegen verbessert. Durch die Virtualisierung von Rechnersystemen können daher die Leistungsreserven besser ausgenutzt werden, ohne die übersichtliche Aufteilung einzelner Anwendungen und Dienste auf einzelne Serversysteme aufzugeben.

Dieses Konzept der Aufteilung eines Rechnersystems in mehrere virtuelle Instanzen wurde zuerst in der Großrechnerwelt eingeführt. Hier wurde der Großrechner mittels einer so genannten Partitionierungstechnik in viele einzelne Rechner (logische Partitionen z. B. *IBM LPAR*s bei der *z-Series*) mit jeweils eigenem Betriebssystem und eigenen Anwendungen aufgeteilt. Diese Technik wurde später auch auf Server der mittleren Leistungsklasse und auf Serversysteme auf der Basis der x86- bzw. x64-Architektur übertragen, als diese leistungsfähig genug waren, um mehrere Rechnerinstanzen auf einer Hardwareplattform betreiben zu können.

Im Folgenden wird nun beschrieben, wie sich die Virtualisierungstechnik auf Serversystemen auf Basis der x86- bzw. x64-Architektur entwickelt hat und welche Basistechniken und Hardwarevoraussetzungen dafür geschaffen wurden. Weiterhin werden einige Anwendungen der Virtualisierungstechnik vorgestellt.

**Vollständige Systememulation**

Die Virtualisierungstechnik ist zuerst als reine Softwarelösung implementiert worden. Dies bedeutet, dass durch die Virtualisierungssoftware einem virtuel-

len System eine emulierte Hardwareumgebung präsentiert wurde. Die Rechnerkomponenten des virtuellen IT-Systems wie Prozessor, Arbeitsspeicher und Massenspeicher sowie Netzschnittstellen wurden aufwändig emuliert und vollständig in Software nachgebildet. Hierdurch ist die Performance eines solchen virtuellen Systems sehr begrenzt. Sie ermöglicht aber, vor allem auf Grund der Prozessoremulation, sehr flexible Möglichkeiten, da hier auch plattformübergreifende Virtualisierungen von IT-Systemen möglich sind. Es ist mittels solcher vollständiger Rechnervirtualisierungssoftware beispielsweise (hier: Microsoft Virtual PC für Mac 7) möglich, ein Betriebssystem wie Microsoft Windows XP, dass ausschließlich für die x86-Plattform entwickelt wurde und nur dort lauffähig ist, auf einem PowerPC-basierenden Rechner mit Mac OS X 10.4 auszuführen, indem der x86-Prozessor vollständig in Software nachgebildet wurde. Eine solche vollständige Rechnervirtualisierung ist allerdings hochgradig ineffizient, da die vollständige Emulation von Prozessor-Architektur und sonstiger Hardwarebestandteile sehr viele Ressourcen benötigt und das virtuelle IT-System damit nur einen Bruchteil der physisch verfügbaren Performance nutzen kann.

**Servervirtualisierung**

Wesentlich effizienter als die vollständige und plattformübergreifende Virtualisierung eines Rechnersystems ist daher eine plattformspezifische Virtualisierungstechnik. Hier muss keine vollständige Rechnerumgebung (Prozessor, Arbeitsspeicher, Festplattenspeicher usw.) in Software nachgebildet werden. Die Virtualisierungssoftware muss nur so gestaltet sein, dass innerhalb der gegebenen Hardwarearchitektur die Kapselung und Isolation (s. o.) der jeweiligen virtuellen Instanzen ähnlich der von physischen Systemen ist. Eine aufwändige vollständige Emulation von Hardwarekomponenten ist dann nicht mehr notwendig. Die Software, die die Steuerung der virtuellen Systeme und deren Hardwareumgebung simuliert, wird als *Hypervisor* bezeichnet.

Die Virtualisierungssoftware (bzw. der Hypervisor) hat im Wesentlichen nur die folgenden Aufgaben:

- Bereitstellung einer gekapselten und isolierten Laufzeitumgebung für die einzelnen virtuellen Instanzen und
- Steuerung der Zugriffe des virtuellen Systems auf Hardwarekomponenten des physischen Systems.

Diese hier beschriebene plattformspezifische Virtualisierungstechnik wird als Servervirtualisierung bezeichnet. Bei Lösungen auf der Basis einer Servervirtualisierung wird weiterhin noch zwischen hypervisorbasierten (Typ 1) und hostbasierten Lösungen (Typ 2) unterschieden.

Bei den hostbasierten Virtualisierungslösungen wird die Virtualisierungssoftware auf einem Standard-Betriebssystem wie Unix oder *Microsoft Windows Server* installiert, während bei Virtualisierungslösungen vom Typ 1 (Hypervisorbasiert) auf der physischen Hardware nur der Hypervisor installiert wird. Dieser Hypervisor stellt dann ein auf die Virtualisierung spezialisiertes Minimal-Betriebssystem dar. Eine Typ 1-Virtualisierungssoftware wird gelegentlich auch als *Bare Metal Virtualization* bezeichnet.

Produkte, die die Servervirtualisierungstechnik verwenden, sind beispielsweise

- Microsoft Hyper-V (Typ 1), Microsoft VirtualPC (Typ 2) oder Microsoft VirtualServer (Typ 2)
- QEMU (Typ 2, Anmerkung: QEMU kann auch zur vollständigen Systememulation verwendet werden)

- Sun VirtualBox (Typ 2)
- VMware Server (Typ 2) und VMware Workstation (Typ 2)
- VMware vSphere bzw. VMware ESX(i) (Typ 1),
- auf Xen basierende Produkte wie Citrix XenServer, Sun OpenVM (Typ 1)

Bei der Servervirtualisierung wird durch die Virtualisierungssoftware in der Regel ein virtueller Rechner erzeugt, der aus virtualisierten Hardwarekomponenten besteht. Diese Hardwarekomponenten werden dem Betriebssystem des virtuellen Systems präsentiert. Die Virtualisierungssoftware kann nun die Zugriffs- und Steuerungsbefehle, die vom Betriebssystem des virtuellen IT-Systems an dessen virtuelle Hardware gesandt werden, direkt in solche für die physische Hardware umsetzen. Diese Umsetzung ist deutlich effizienter als die oben beschriebene vollständige Emulation der Hardwarekomponenten.

Diese Technik wird als so genannte *Vollvirtualisierung* bezeichnet. Eine weitere Steigerung der Performance kann mittels der so genannten *Paravirtualisierung* erreicht werden. Hierbei wird unter der Kontrolle des Hypervisors ein speziell angepasstes Betriebssystem in dem virtuellen IT-System ausgeführt. Dieses ist so modifiziert, dass keine hardwarenahen Systembefehle mehr im Kernel des Betriebssystems des virtuellen IT-Systems enthalten sind. Diese Systembefehle werden häufig auch als "Ring 0-Befehle" oder "Dom0-Befehle" bezeichnet. Das virtuelle IT-System wird dann im "Ring 1" bzw. in der "DomU" ausgeführt. Unterstützt der Prozessor des Virtualisierungsservers die Paravirtualisierung (z. B. AMD-V und Intel VT), so kann auf ein angepasstes Betriebssystem verzichtet werden. Diese Möglichkeit nutzt beispielsweise XEN 3.0.

**Betriebssystemvirtualisierung**

Die Effizienz der Virtualisierungssoftware kann jedoch noch weiter gesteigert werden, in dem nicht nur die Hardwareplattform allen virtuellen Systemen gemein ist, sondern auch das Betriebssystem für alle virtuellen Instanzen festgelegt wird. Solche Virtualisierungstechniken werden Betriebssystemvirtualisierung genannt. Die Steuerung der Hardwarezugriffe der virtuellen IT-Systeme kann extrem vereinfacht werden, da hier keine virtuellen Hardwarekomponenten notwendig sind. Das virtuelle System hat das gleiche Betriebssystem wie das physische, auf dem es ausgeführt wird, und kann daher die gleichen Hardware-Treiber verwenden. Der Umsetzungsaufwand zwischen virtueller und physischer Hardware fällt somit vollständig weg. Die Kapselung der virtuellen IT-Systeme ist hier allerdings zumindest für das Betriebssystem nicht mehr sehr stark ausgeprägt, da alle virtuellen Instanzen das gleiche (nicht das selbe!) Betriebssystem nutzen. Die Virtualisierungssoftware stellt also nur noch die Isolation der einzelnen virtuellen Instanzen sicher.

Beispiele für solche Betriebssystemvirtualisierungslösungen sind:

- Sun Solaris Containers
- BSD jails
- Parallels Virtuozzo
- User Mode Linux

Der Vorteil der auf einer Betriebssystemvirtualisierung beruhenden Produkte liegt in der hohen Performance der virtuellen Instanzen und ihrem geringen relativen Ressourcenverbrauch auf dem Virtualisierungsserver im Vergleich zur Servervirtualisierung. Hierdurch ist ein sehr großer Verdichtungsgrad (Verhältnis der Anzahl von Virtualisierungsservern zu virtuellen Systemen) erreichbar. Mit einigen Betriebssystemvirtualisierungslösungen können bis zu 200 virtuelle IT-Systeme auf einem Virtualisierungsserver mittlerer Leistungsklasse betrieben werden. Auf einem gleich ausgestatteten Server, der eine Servervirtualisierungslösung nutzt, sind meist nur 10 bis 15 virtuelle Systeme möglich.

Der Nachteil der Betriebssystemvirtualisierungslösungen liegt allerdings in der schwachen Kapselung von Betriebssystem und Anwendungen auf dem Virtualisierungsserver. Diese schwache Kapselung führt dazu, dass virtuelle IT-Systeme mit stark unterschiedlichen Schutzbedarfsanforderungen nicht ohne Weiteres gemeinsam auf einem Virtualisierungsserver betrieben werden können. Dies ist bei Virtualisierungslösungen auf Basis einer Servervirtualisierung in der Regel anders, da die Kapselung der virtuellen Systeme stärker ausgeprägt ist. Ob allerdings virtuelle IT-Systeme unterschiedlicher Schutzbedarfsanforderungen auf einem Virtualisierungsserver zusammen betrieben werden können, hängt neben dem verwendeten Produkt auch von der Schutzbedarfsfestellung und den individuellen Gefährdungen der Organisation bzw. der virtuellen IT-Systeme ab.

**Anwendungen der Virtualisierungstechnik**

Mit Mitteln der Virtualisierungstechnik können einige Anwendungen entwickelt werden, die für physische Systeme in der Regel nur mit unverhältnismäßig hohem Aufwand realisiert werden könnten. Diese Anwendungen basieren in der Regel darauf, dass die Virtualisierungssoftware direkte Kontrolle über den Prozessor, den Arbeitsspeicher und die Massenspeicher des virtuellen IT-Systems hat. Sie kann direkt beeinflussen, wie diese Ressourcen durch das virtuelle System genutzt werden. Die Virtualisierungssoftware kann damit beispielsweise jederzeit den Zustand des Prozessors oder des Arbeitsspeicher des virtuellen IT-Systems auslesen. Diese Möglichkeiten können genutzt werden, um das virtuelle IT-System für unbestimmte Zeit einzufrieren. Weiterhin ist es möglich, in den Prozessor oder den Arbeitsspeicher zuvor gespeicherte Inhalte hinein zu laden. Der zuvor auf die Festplatte des Virtualisierungsservers gespeicherte Zustand von Prozessor und Arbeitsspeicher wird nach der Betriebsunterbrechung wieder geladen und die Ausführung der virtuellen Instanz wird genau an der Stelle fortgesetzt, an der das System eingefroren wurde. Dieses Verfahren ist nicht mit anderen Verfahren wie dem "Ruhezustand", der von *Microsoft Windows XP* oder *Windows Vista* bekannt ist, zu verwechseln. Im Gegensatz zum Ruhezustand geschieht diese Betriebsunterbrechung für das virtuelle IT-System völlig transparent. Die Möglichkeiten, ein virtuelles IT-System einzufrieren, werden genutzt, um so genannte Snapshots im laufenden Betrieb zu erzeugen.

**Snapshots**

Die meisten Virtualisierungslösungen ermöglichen das Konservieren des Zustands eines virtuellen IT-Systems zu einem beliebigen Zeitpunkt, ohne dass die Ausführung des virtuellen IT-Systems hierdurch beeinträchtigt wird. Beim Anlegen eines Snapshots wird die virtuelle Festplatte eingefroren und nachfolgende Schreibzugriffe werden in eine separate Datei umgeleitet. Der aktuelle Zustand ergibt sich bei Maschinen mit aktiven Snapshots aus der Überlagerung aller Snapshot-Dateien mit der Basis-Datei.

Snapshots können mit oder ohne Inhalt des Arbeitsspeichers des virtuellen IT-Systems angelegt werden. Snapshots ohne Arbeitsspeicherinhalt spiegeln meist den Zustand des virtuellen IT-Systems wieder, das nicht heruntergefahren, sondern im laufenden Betrieb ausgeschaltet wurde. Snapshots mit Arbeitsspeicherinhalt erlauben es, das IT-System exakt in den Zustand zu versetzen, wie er zum Zeitpunkt des Snapshots vorlag, d. h., es ist eine Rückkehr in ein laufendes Betriebssystem mit geöffneten Anwendungen möglich. So lange der Snapshot nicht gelöscht wird, befindet sich der Speicherinhalt vom Zeitpunkt des Snapshots meist in Form einer Datei im Verzeichnis des virtuellen IT-Systemes.

***Live Migration* von virtuellen IT-Systemen**

Techniken wie Live Migration für XEN, Citrix XenMotion und Microsoft HyperV Server 2008 R2 oder auch VMotion für VMware erlauben die Übertragung (Migration) von virtuellen IT-Systemen auf andere physische Virtualisierungsserver im laufenden Betrieb.

Aus Benutzersicht, aber auch aus Sicht des virtuellen IT-Systems, geschieht dies unterbrechungsfrei. Hierdurch wird es z. B. möglich, Hardware eines Virtualisierungsserver zu erweitern oder auszutauschen, die Auslastung der Virtualisierungsserver gezielt neu zu verteilen sowie einen bestimmten Dienst oder eine Anwendung auf einen anderen Virtualisierungsserver zu verlagern.

Sowohl vor, während, als auch nach dem Migrationsvorgang muss der Zugang des virtuellen IT-Systems zum eigenen Dateisystem gewährleistet sein. Hierfür kommen Speichernetze (SAN-Storage-Systeme) mittels Fibre Channel oder iSCSI und Netzdateisysteme wie NFS in Frage.

Diese Technik funktioniert im Wesentlichen so, dass zuerst ein Snapshot eines virtuellen IT-Systems vom Quell-Virtualisierungsserver auf den Ziel-Virtualisierungsserver übertragen wird. Der Zielserver lädt nun den Arbeitsspeicher des zu übertragenden virtuellen IT-Systems in seinen Speicher. Da das System auf dem Quellserver weiterläuft, hat sich der Speicher des virtuellen Systems in der Zwischenzeit verändert. Diese Änderungen werden nun fortlaufend übertragen und in Folge dessen wird das Zielsystem mit dem Quellsystem synchronisiert. Ist die Synchronizität hergestellt, wird das virtuelle IT-System auf dem Quellserver gestoppt, der Prozessorzustand auf den Zielserver übertragen und das virtuelle IT-System mit dem übertragenen Prozessorzustand auf dem Zielserver fortgesetzt. Dieser Vorgang erfolgt für das virtuelle IT-System vollständig transparent.

Die *Live Migration* kann genutzt werden, um Performanceengpässen vorzubeugen. Dieser Prozess kann automatisiert werden, so dass jedem virtuellen IT-System immer die maximal mögliche Performance zur Verfügung gestellt werden kann.

**Überbuchung von Arbeitsspeicher**

Bei einigen Virtualisierungslösungen kann den virtuellen IT-Systemen in Summe mehr Arbeitsspeicher zugewiesen werden, als auf dem Virtualisierungsserver insgesamt vorhanden ist. Einem einzelnen virtuellen IT-System kann allerdings nicht mehr Speicher zugewiesen werden, als dem Hypervisor zur Verfügung steht. Ein Virtualisierungsserver verfügt beispielsweise über insgesamt zwei Gigabyte Hauptspeicher. Auf ihm werden drei virtuelle Server betrieben, die jeweils ein Gigabyte, also zusammen drei Gigabyte Hauptspeicher besitzen sollen. Um diese Überbuchung zu ermöglichen, wird den virtuellen IT-Systemen der entsprechende Hauptspeicher nicht zur Gänze zugeteilt. Stattdessen wird dem einzelnen virtuellen IT-System nur dann eine Speicherseite physisch zugewiesen, wenn sie von diesem virtuellen System tatsächlich gebraucht wird. Einmal durch ein virtuelles IT-System angeforderter Speicher kann grundsätzlich nicht durch den Hypervisor wieder zurückgefordert werden. So wächst der physische Speicherbedarf eines virtuellen IT-Systems sukzessive bis zur Konfigurationsgrenze an. Da allerdings davon ausgegangen werden kann, dass das Betriebssystem des virtuellen IT-Systems den ihm zur Verfügung stehenden Speicher mit der Zeit komplett nutzen wird, muss eine Möglichkeit bestehen, wie mit einer Ressourcensättigung auf dem

Virtualisierungsserver umgegangen werden soll. Eine solche Möglichkeit wird in den folgenden Absätzen an einem Beispiel verdeutlicht.

Das Produkt *ESX Server* des Herstellers *VMware* beispielsweise ermöglicht die Überbuchung von Hauptspeicher auf drei verschiedene, miteinander kombinierte Vorgehensweisen:

- *Transparent Memory Sharing*
  Der Hypervisor überwacht alle Speicherseiten aller virtuellen IT-Systeme. Kann der Hypervisor zwei identische Speicherseiten identifizieren, werden diese nur einmal im physischen Arbeitsspeicher des Virtualisierungsservers vorgehalten. Ändert eines der virtuellen IT-Systeme eine dieser Seiten, wird sie für dieses System kopiert, und die anderen virtuellen IT-Systeme nutzen weiter die nicht modifizierte Seite. Diese Technik hat ein hohes Potenzial zur Speichereinsparung, da z. B. bei vielen virtuellen IT-Systemen die gleichen Betriebssystemkerne oder Softwarebibliotheken verwendet werden. Das Speicherabbild dieser Kerne oder Bibliotheken muss nur einmal physisch im Speicher des Virtualisierungsservers gehalten werden.
- *Ballooning*
  In Abhängigkeit vom Hauptspeicherverbrauch des Gesamtsystems kann die Zuordnung von virtuellem Arbeitsspeicher zu den einzelnen virtuellen Systemen dynamisch angepasst werden. Möglich wird dies durch einen Treiber in dem virtuellen System, der gezielt Speicher belegt (Ballooning) und so das Betriebssystem des virtuellen IT-Systems zwingt, Hauptspeicherinhalte auf seine virtuelle Festplatte auszulagern. Der durch den Ballooning-Treiber belegte Speicher wird vom ESX Server erkannt und kann an andere virtuelle IT-Systeme vergeben werden. Mittels dieses Verfahrens können Speicherengpässe kurzzeitig ausgeglichen werden. Da das Betriebssystem des virtuellen IT-Systems kontrolliert, welche Prozesse ausgelagert werden, ist der negative Performanceeinfluss meist kurzzeitig hinnehmbar.
- *Paging*
  Kann der benötigte Speicher für ein virtuelles IT-System weder über *Transparent Memory Sharing* des Virtualisierungsservers noch über *Ballooning* im virtuellen IT-System freigegeben werden, wird der Speicher anderer, gerade nicht aktiver virtueller IT-Systeme durch den Hypervisor auf die Festplatten des ESX-Servers ausgelagert. Wenn dies geschieht, wird die Performance der virtuellen IT-Systeme sehr stark herabgesetzt, da der Hypervisor hier keine Rücksicht auf laufende Prozesse des Betriebssystems der ausgelagerten virtuellen IT-Systeme nimmt.

Der Festplattenplatz des Virtualisierungsservers kann ebenfalls überbucht werden. Hierbei wird den virtuellen IT-Systemen mehr Festplattenplatz zur Verfügung gestellt, als tatsächlich vorhanden ist. Dabei wird der verfügbare Festplattenplatz so zugewiesen, dass die virtuelle Maschine ein Laufwerk mit beispielsweise einer Größe von zehn Gigabyte erkennt und ein Dateisystem von diesen Dimensionen anlegen kann. Auf der Festplatte des Virtualisierungsservers belegt das virtuelle IT-System jedoch nur den tatsächlich genutzten Platz in einer Containerdatei, die dynamisch mit der aktuell benötigten Speichergröße mitwächst. Sobald das virtuelle IT-System weiteren Platz nutzt, wird dieser auch auf der physischen Festplatte des Virtualisierungsservers belegt. Vom virtuellen IT-System freigegebener Speicher wird allerdings in der Regel nicht automatisch wieder physisch freigegeben. Es muss weiterhin beachtet werden, dass die virtuellen IT-Systeme in eine Fehlersituation geraten, wenn der physische Speicher nicht mehr ausreicht, um weitere Speicheranforderungen zu erfüllen: Die virtuellen IT-Systeme "wissen" nichts von der Überbuchung des Speichers und versuchen weiter auf ihre virtuellen Fest-

platten zu schreiben. Es kommt zu Schreibfehlern in den virtuellen IT-Systemen und in der Folge zu Inkonsistenzen im Dateisystem.

**Fehlertoleranz für Hardware-Komponenten**

Virtuelle IT-Systeme können bei einigen Virtualisierungsprodukten von Toleranzmechanismen bei Hardwarefehlern profitieren. Da die Virtualisierungssoftware die Zuordnung beispielsweise einer virtuellen Netzschnittstelle zu einer physischen steuert, kann die Kommunikation des virtuellen IT-Systems auf eine andere Netzschnittstelle umgeleitet werden, wenn die ursprüngliche Schnittstelle von einem Fehler betroffen ist. Stehen also in einem Virtualisierungsserver mehrere redundante Komponenten zur Verfügung, kann die Virtualisierungssoftware beim Ausfall einer Komponente für die Nutzung der noch funktionsfähigen Komponenten sorgen.

**Fehlertoleranz bei virtuellen IT-Systemen**

Die Virtualisierungsprodukte *Citrix XenServer (Marathon EverRun)* und *VMware vSphere (Fault Tolerance)* beispielsweise verfügen über Mechanismen, um für den Fall des Ausfalls eines Virtualisierungsservers fehlertolerante virtuelle IT-Systeme zu erzeugen. Um diese Fehlertoleranz eines virtuellen IT-Systems zu erreichen, wird auf einem anderen Virtualisierungsserver eine Kopie des virtuellen IT-Systems erzeugt. Diese Kopie wird fortlaufend mit dem Original synchronisiert und bleibt solange nicht mit dem Netz verbunden, wie das Original weiterhin funktioniert. Fällt der Virtualisierungsserver aus, auf dem das Original läuft, kann die Kopie mit dem Netz verbunden werden und sofort alle Funktionen des Originals übernehmen. Danach wird auf einem weiteren Virtualisierungsserver sofort wieder eine neue Kopie des virtuellen IT-Systems erzeugt.

# M 3.73 Schulung der Administratoren eines DNS-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um einen DNS-Server korrekt und sicher administrieren zu können, ist eine Schulung der verantwortlichen Administratoren unumgänglich. Bereits kleine Konfigurationsfehler können dazu führen, dass sicherheitskritische Lücken entstehen. Besonders die sorgfältige Planung des Einsatzes eines DNS-Servers und die Einschränkung der Kommunikation auf legitime Teilnehmer erfordert ein solides Fachwissen.

Neben den Aspekten der allgemeinen Betriebssystemsicherheit, wie beispielsweise in den Bausteinen B 3.102 *Server unter Unix* oder B 3.108 *Windows Server 2003* beschrieben, sind folgende Punkte von Bedeutung:

- Installation des DNS-Servers
- Möglichkeiten zur Einbindung des DNS-Server in den Startprozess des Betriebssystems
- Einführung in mögliche Gefährdung, um ein Grundverständnis bezüglich Angriffsweisen zu schaffen
- Entwicklung eines Rechtekonzepts, sowohl für die Konfigurationsrechte durch Administratoren als auch für die Rechte des DNS-Server-Prozesses
- Unterschied zwischen Advertising und Resolving DNS-Server
- Konfigurationsmöglichkeiten des DNS-Servers
- Mechanismen zur Absicherung von Anfragen
- Mechanismen zur Absicherung von Zonentransfers
- Mechanismen zur Absicherung von dynamischen Updates (sofern verwendet)
- Einsatzmöglichkeiten und Konfiguration von DNSSEC
- Mechanismen zur Sicherstellung der Verfügbarkeit von DNS-Servern
- Mechanismen zur Sicherung der Zoneninformationen
- Ist das nötige Budget für die Schulungsmaßnahmen vorhanden?

Prüffragen:

- Sind die Administratoren im Umgang mit DNS-Servern entsprechend geschult und somit mit den sicherheitsrelevanten Aspekten vertraut?

# M 3.74 Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Um ein Groupware-System korrekt und sicher administrieren zu können, ist die Schulung der verantwortlichen Administratoren unumgänglich. Schon kleine Konfigurationsfehler können dazu führen, dass die Systemsicherheit beeinträchtigt wird. Aus diesem Grund müssen Administratoren über die Systemarchitektur und besonders über die spezifischen Sicherheitsmechanismen der eingesetzten Groupware ausreichend geschult werden.

Der Betrieb von Groupware-Systemen ist komplex und es sind viele Bereiche daran beteiligt. Es ist deshalb darauf zu achten, dass das Bedienungspersonal die für seine Tätigkeit benötigte Ausbildung erhält. Dafür sind die Empfehlungen aus M 3.11 *Schulung des Wartungs- und Administrationspersonals* zu beachten.

Außerdem sollten die Administratoren durch Teilnahme an Schulungsmaßnahmen wie Seminare oder Anwendertagungen entsprechend ihren Aufgaben ausgebildet werden. Es sollte überlegt werden, die Ausbildung anhand eines Schulungsplanes festzulegen.

Die Administratoren sollten in allen sicherheitsrelevanten Bereichen des Groupware-Systems ausgebildet werden. Dazu gehören neben einem Überblick über die Sicherheitsfunktionen der eingesetzten Groupware-Komponenten Aspekte wie

- Aktuelle Gefährdungen von Groupware-Systemen z. B. Denial-of-Service-Angriffe, Schadsoftware, Gefahrenquelle "Default-Einstellungen" etc.
- Überblick über SMTP-Sicherheit
- Abwehr von Schadsoftware und Spam (Aufbau und Integration von Antispam- und Antiviruslösungen)
- Überblick über relevante rechtliche Aspekte bei der Groupware-Administration wie z. B. Datenschutz
- Umgang mit allen relevanten Sicherheitsmechanismen der eingesetzten Groupware-Komponenten
- Einrichten von Berechtigungen und Integration von Berechtigungen in die Betriebssystem-Berechtigungen, Authentisierungsmechanismen
- Überblick über die verschiedenen Lösungen für die Nachrichtensicherheit, z. B. Verschlüsselung, Digitale Signatur, VPNs
- Protokollierung
- Sicherung und Verwaltung von Konfigurationsdaten
- Datensicherung
- Incident Handling und Disaster Recovery Maßnahmen

Die Administration der Groupware-Komponenten setzt außerdem Kenntnisse über die Konfigurationsmöglichkeiten der eingesetzten Server-, Client- und Datenbank-Plattformen voraus. Es ist unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden.

Prüffragen:

- Wurden alle Administratoren für die Arbeit mit dem Groupware-System ausreichend geschult?

# M 3.75 Schulung zu Sicherheitsmechanismen von Groupware-Clients für Benutzer

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Groupware-Systeme sind im Allgemeinen derartig komplex, dass es bei fehlerhafter Nutzung oder Konfiguration unbeabsichtigt zu Sicherheitslücken kommen kann. Dies gilt besonders dann, wenn die Benutzer nicht hinreichend im Umgang mit dem eingesetzten Groupware-System geschult sind. Zwar wird die Systemkonfiguration in der Regel so eingestellt, dass diese nur in Grenzen durch die Benutzer verändert werden kann. Unkenntnis über die einem Benutzer zur Verfügung stehenden Sicherheitsmechanismen und -einstellungen können jedoch dazu führen, dass das System unsicher genutzt wird.

Daher müssen alle Benutzer im Umgang mit dem Groupware-Client geschult werden. Neben der reinen Nutzung der Client-Software ist es jedoch auch notwendig, den Benutzern die grundlegende Funktionsweise des Groupware-Systems zu erläutern. Den Benutzern muss insbesondere vermittelt werden, welche Sicherheitsmechanismen ihnen zur Verfügung stehen, so dass sie in der Lage sind, diese korrekt und sinnvoll einzusetzen.

Die Mitarbeiter müssen über die mit dem Benutzen von Groupware- und E-Mail-Clients verbundenen Gefährdungen informiert werden. Dies könnte z. B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein ungewöhnliches Verhalten der Kommunikationssoftware gemeldet werden soll.

Den Benutzern muss insbesondere vermittelt werden, welche Sicherheitsmechanismen ihnen zur Verfügung stehen, so dass sie in der Lage sind, diese korrekt und sinnvoll einzusetzen.

Prüffragen:

- Wurden alle Benutzer für die Arbeit mit dem Groupware-Client geschult?
- Ist den Benutzern der Umgang mit allen relevanten Sicherheitsmechanismen der eingesetzten Groupware dargestellt worden?

# M 3.76 Einweisung der Benutzer in den Einsatz von Groupware und E-Mail

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Die Benutzer müssen vor dem Einsatz von Kommunikationsdiensten und Groupware-Applikationen wie E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen, z. B. beim Versenden bzw. Empfangen von E-Mails, sensibilisiert werden. Es ist darauf hinzuweisen, dass ein abnormes Verhalten der Kommunikationssoftware gemeldet werden sollte.

Benutzer müssen darüber informiert werden, dass Dateien, deren Inhalt Anstoß erregen könnte, weder verschickt noch auf Informationsservern eingestellt werden noch nachgefragt werden sollten. Außerdem sollten Benutzer darauf verpflichtet werden, dass bei der Nutzung von Kommunikationsdiensten

- die fahrlässige oder gar vorsätzliche Unterbrechung des laufenden Betriebes unter allen Umständen vermieden werden muss. Zu unterlassen sind insbesondere Versuche, ohne Autorisierung Zugang zu Netzdiensten, welcher Art auch immer, zu erhalten, Informationen, die über die Netze verfügbar sind, zu verändern, in die individuelle Arbeitsumgebung eines Netzbenutzers einzugreifen oder unabsichtlich erhaltene Angaben über Rechner und Personen weiterzugeben.
- die Verbreitung von für die Allgemeinheit irrelevanten Informationen unterlassen werden muss. Die Belastung der Netze durch ungezielte und übermäßige Verbreitung von Informationen sollte vermieden werden.
- die Verbreitung von redundanten Informationen vermieden werden sollte.

Außerdem sollten Benutzer über folgende Punkte informiert werden:

- Wenn eine E-Mail an mehrere Empfänger geschickt wird, werden diese oft ins "To"- oder "CC"-Feld eingetragen. Dies hat unter Anderem den Vorteil, dass eine E-Mail nur einmal versendet werden muss und jeder Empfänger sofort sehen kann, wer über den Inhalt informiert wurde. Oft ist es aber nicht sinnvoll, dass jeder Empfänger die komplette Empfängerliste sehen kann. Dies ist nämlich nicht nur für die Empfänger lästig, sondern kann auch aus Datenschutzgründen unerwünscht sein und es könnte dadurch auch Spam verursacht werden.
  Bei größeren Empfängerlisten sollte die E-Mail-Adressen statt unter "CC" unter "BCC" eingetragen oder Verteilerlisten benutzt werden. BCC steht für Blind Carbon Copy, hier eingetragene weitere Empfänger werden den anderen Empfänger nicht angezeigt.
- Verteilerlisten müssen regelmäßig auf Korrektheit und Aktualität überprüft werden, damit keine E-Mails aufgrund fehlerhafter oder nicht aktueller Verteilerlisten an falsche Empfänger übertragen werden.
- Die Benutzer sollten alle Regelungen der Institution rund um Kommunikation, Groupware und E-Mail kennen. Dazu gehört beispielsweise, wann und in welcher Form Signatures (Absenderangaben) einer E-Mail angefügt werden sollten.
- Über E-Mail wird viel Schadsoftware transportiert. Benutzer sollten über die Gefahren von Schadsoftware und Verbreitungswege informiert sein. Sie sollten auch wissen, dass es trotz aller Sicherheitsmaßnahmen in ei-

ner Institution passieren kann, dass eingehende E-Mails bzw. deren Anhänge Schadsoftware enthalten können. Benutzer sollten daher keine E-Mails oder Anhänge öffnen, die ihnen in irgendeiner Form zweifelhaft erscheinen, also z. B. keine unerwarteten Anhänge.
- Zur Vermeidung von Überlastung durch E-Mail sind die Mitarbeiter über potentielles Fehlverhalten zu belehren. Sie sollten dabei ebenso vor der Teilnahme an E-Mail-Kettenbriefen wie vor der Abonnierung umfangreicher Mailinglisten gewarnt werden.

Bei den meisten Groupware-Systemen werden die Informationen unverschlüsselt über offene Leitungen transportiert und können auf diversen Zwischenrechnern gespeichert werden, bis sie schließlich ihren Empfänger erreichen. Auf diesem Weg können Informationen leicht manipuliert werden. Aber auch der Versender einer E-Mail hat meistens die Möglichkeit, seine Absenderadresse (From) beliebig einzutragen, so dass man sich nur nach Rückfrage oder bei Benutzung von Digitalen Signaturen der Authentizität des Absenders sicher sein kann. In Zweifelsfällen sollte daher die Echtheit des Absenders durch Rückfrage oder - besser noch - durch den Einsatz von Verschlüsselung und/oder Digitalen Signaturen überprüft werden. Grundsätzlich sollten sich Benutzer bei E-Mail nicht auf die Echtheit der Absenderangabe verlassen.

Bei E-Mail werden schnelle Reaktionszeiten erwartet. Daher sollte mehrfach täglich der Posteingang überprüft werden. Bei längerer Abwesenheit sollte eine Vertretungsregelung getroffen werden, beispielsweise können eingehende E-Mails an einen Vertreter weitergeleitet werden (siehe auch M 2.274 *Vertretungsregelungen bei E-Mail-Nutzung*).

Da in vielen Fällen nicht vorhergesagt werden kann, welchen E-Mail-Client ein E-Mail-Empfänger benutzt und welche Software und Betriebssysteme auf dem Transportweg eingesetzt werden, sollten die Benutzer wissen, dass sowohl bei der Übertragung als auch bei der Darstellung von Nachrichten und Anhängen beim Empfänger Probleme auftreten können. Dies tritt kann insbesondere bei der Verwendung ungewöhnlicher Zeichensätze oder Dateiformate, oder auch beim Einsatz veralteter E-Mail-Software auftreten.

Benutzer sollten auch wissen, dass E-Mails aus den verschiedensten Gründen nicht beim Empfänger ankommen. Vor allem bei zeitkritischen oder wichtigen E-Mails sollten sich die Absender nicht auf eine automatische Empfangsbestätigung verlassen. Besser sollte eine unabhängige Rückmeldung erfolgen, z. B. eine kurze E-Mail mit selbst formulierter Bestätigung.

**Löschen von E-Mails**

Benutzer müssen darüber informiert sein, dass eine E-Mail, die sie selber über ihre Mailanwendung gelöscht haben, dadurch meistens nicht unwiederbringlich gelöscht ist. Viele Mailprogramme löschen E-Mails nicht sofort, sondern transferieren sie in spezielle Ordner. Benutzer müssen darauf hingewiesen werden, wie sie E-Mails auf ihren Clients vollständig löschen können.

Daneben können E-Mails nach dem Löschen auf den Clients trotzdem noch auf Mailservern vorhanden sein. Viele Internet-Provider und Administratoren archivieren die ein- und ausgehenden E-Mails. Viele Mailanwendungen löschen E-Mails nicht, sondern verschieben sie in einen "Papierkorb"-Bereich, der dann ebenfalls gelöscht werden muss.

Die Benutzer müssen wissen, dass die Vertraulichkeit einer E-Mail nur durch Verschlüsselung gewährleistet werden kann, und dass sie sich nicht auf "schnelles Löschen" nach dem Empfang verlassen können. Dasselbe gilt ge-

nauso für andere Groupware-Anwendungen wie z. B. Terminkalender-Einträge.

**Veröffentlichung der Regelungen**

Alle Regelungen und Bedienungshinweise zum Einsatz von Groupware sollten den Mitarbeitern jederzeit zur Verfügung stehen, z. B. im Intranet.

Prüffragen:

- Sind die Benutzer über Gefährdungen und einzuhaltende Sicherheitsmaßnahmen bei der Groupware-Nutzung sensibilisiert worden?

# M 3.77 Sensibilisierung zur sicheren Internet-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Personalabteilung

Das Internet kann in Unternehmen oder Behörden für eine Vielzahl von Zwecken und über verschiedenste Dienste benutzt werden. Hierzu gehören beispielsweise die Kommunikation mit Kunden über E-Mail, Instant Messaging, Diskussionsforen oder Blogs, die Darstellung der Institution über eigene Webseiten oder die Informationssuche. Um das Internet aus Sicht einer Institution sicher nutzen können, kann die Nutzung bestimmter Dienste oder Angebote untersagt oder eingeschränkt werden. Da die Nutzung aller unerwünschten Dienste nicht technisch unterbunden werden kann, unter anderem weil ständig neue Angebote und Dienste hinzukommen, ist es sinnvoller, die Mitarbeiter darin zu schulen, wie sie das Internet sicher und zweckmäßig nutzen können. Dazu gehört auch, die Mitarbeiter darüber zu informieren, wie sie durch richtiges Verhalten und optimale Konfiguration der Internet-Anwendungen, beispielsweise der Browser, vermeiden können, bei der Internet-Nutzung unerwünschten Datenspuren zu hinterlassen.

Die Mitarbeiter müssen über mögliche Gefährdungen und einzuhaltende Sicherheitsmaßnahmen bei der Internet-Nutzung sensibilisiert werden. Sie sollten insbesondere aufgeklärt sein über

- die bestehenden Regelungen der Institution zur Internet-Nutzung (eventuell gibt es neben einer Richtlinie zur Internet-Nutzung separate Richtlinien zum Umgang mit E-Mails, Blogs, etc.),
- den Umgang mit heruntergeladenen Dateien und die Regelungen zur Installation von Software und PlugIns aus dem Internet,
- mögliche Gefährdungen bei der Internet-Nutzung und wie die ergriffenen Sicherheitsmaßnahmen gegen diese wirken,
- aktive Inhalte, wie Java-Applets, ActiveX-Controls und JavaScript, und die Entscheidung der Institution, wie mit aktiven Inhalten umzugehen ist,
- die Informationspolitik der Institution, d. h. welche Informationen nicht im Internet weitergegeben werden dürfen, beispielsweise weil die Inhalte vertraulich oder nicht zur Veröffentlichung geeignet sind,
- das korrekte Verhalten bei der Nutzung von Internet-Diensten, da sie als Mitarbeiter im Namen der Behörde bzw. des Unternehmens agieren,
- Strategien zur Spam-Vermeidung,
- rechtliche Vorgaben (Urheberrecht, z. B. bezüglich der Nutzung von Material aus dem Internet, illegale, verfassungsfeindliche oder extremistische Inhalte, pornografische Inhalte, etc.),
- Basiswissen zu Verschlüsselung und digitale Signaturen, um SSL und Verschlüsselungsprogramme korrekt nutzen zu können,
- die Tatsache, dass Informationen und Angebote im Internet, wie bei vielen anderen Medien auch, aus unterschiedlich vertrauenswürdigen Quellen stammen und bei der weiteren Verwendung kritisch hinterfragt oder überprüft werden müssen.

Die Mitarbeiter sollten nicht nur einmal in die sichere Internet-Nutzung eingewiesen werden, sondern immer wieder über die aktuellsten Entwicklungen informiert werden. Dazu sind neben klassischen Schulungen auch webbasierte interaktive Programme und Hinweise im Intranet denkbar. Aktuelle Entwicklungen können auch mit Hilfe von Newslettern oder Rundbriefen und im Rah-

men regelmäßiger Veranstaltungen wie Abteilungsbesprechungen kommuniziert werden.

Prüffragen:

- Sind die Mitarbeiter über aktuelle Gefahren und Sicherheitsmaßnahmen bei der Internet-Nutzung informiert?

# M 3.78 Korrektes Auftreten im Internet

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Bei der dienstlichen Nutzung von Internet-Diensten werden dort getätigte Aussagen von Mitarbeitern einer Institution typischerweise als Aussage der Institution wahrgenommen und nicht als Aussage einer Privatperson. Daher müssen die Mitarbeiter darüber informiert werden, wie sie sich bei der Internet-Nutzung korrekt verhalten und welches Verhalten explizit zu vermeiden ist.

Informationen sollten im Internet nur nach genauer Überlegung veröffentlicht werden, egal ob über Internet-Portale, eigene Webseiten, Mailinglisten oder Blogs. Auch eigentlich kurzlebige Informationen wie Diskussionsbeiträge in einem Forum, die ursprünglich nur an einen kleinen Leserkreis adressiert waren, bleiben unter Umständen sehr lange zugreifbar. Mit Recherchen, beispielsweise über Suchmaschinen oder soziale Netzwerke, können zusätzlich Informationen aus verschiedensten Lebensbereichen zusammengeführt werden. Um zu verhindern, dass die gezielte Auswertungen von Informationen über eine Person oder bestimmte Bereiche einer Institution zu unangenehmen Überraschungen führt, sollten sich Internet-Nutzer an folgende Grundregeln halten:

- Datensparsamkeit: Vor jeder Weitergabe oder Veröffentlichung von Informationen im Internet sollten sich die Benutzer fragen, wie diese Informationen auf ihre Person oder ihre Institution zurückfallen könnten und ob sie wirklich weitergegeben werden sollten. Persönliche oder geschäftsrelevante Informationen sollten nur sparsam weitergegeben werden. Als Grundsatz sollte gelten, dass nichts veröffentlicht werden sollte, was nicht auch unter dem eigenen Namen in einer Zeitschrift erscheinen könnte.
- Need-to-Know: Informationen sollten nur denen zugänglich gemacht werden, die sie wirklich kennen sollten. Es sollten also beispielsweise zur Datenweitergabe geschlossene Foren bzw. geschützte Bereiche benutzt werden.
- Blogs, Foren, Mailinglisten und ähnliche Anwendungen sollten so genutzt werden, dass private Aussagen nicht mit dienstlichen vermischt oder missverstanden werden können.
- Aus Meta-Daten von Dateien sollten alle unnötigen Zusatzinformationen entfernt werden (siehe M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*). Foto-Dateien können z. B. mehr Bildinformationen enthalten, als auf dem veröffentlichten Foto zu sehen sind.

Jeder Benutzer sollte sich im Internet angemessen verhalten, also die Netiquette beachten. Als Netiquette (die Netz-Etiquette) werden Höflichkeitsregeln und Verhaltensvorschläge bezeichnet, die sich mit der Zeit bei der Nutzung des Internet eingebürgert haben und deren Einhaltung gewährleisten soll, dass jeder das Internet effizient und zu aller Zufriedenheit benutzen kann. Dazu gehören beispielsweise folgende Aspekte:

- Wie auch im echten Leben sollte auch im Internet der Tonfall und die Inhalte immer der Zielgruppe angemessen sein. Hierbei ist für Mitarbeiter von Institutionen immer zu beachten, dass sie sich nur so äußern sollten, dass dies nicht für sie oder die Institution nachteilig ausgelegt werden kann. Der Umgangston sollte immer sachlich bleiben. Äußerungen sollten immer daraufhin abgewogen werden, ob sie in dieser Form auch gedruckt werden könnten. Sie sollten nie arrogant, diskriminierend oder beleidigend sein oder so wirken.

- Je nach Internet-Anwendung gibt es andere Gepflogenheiten für die Gestaltung von Nachrichten. Grundsätzlich sollten Informationen immer so weitergegeben werden, dass sie sich im gewählten Medium möglichst einfach lesen und bearbeiten lassen. Dazu gehören korrekter Satzbau und Rechtschreibung, Groß- und Kleinschreibung und die üblichen Höflichkeitsformeln. Die Nachrichten sollten auf das unbedingt erforderliche Maß gekürzt werden.
- Bei der Weitergabe von Informationen sind immer die jeweiligen gesetzlichen Regelungen zu beachten. Bevor Daten von oder über Dritte weitergegeben werden (Texte, Fotos, etc.), ist z. B. das Urheberrecht, das allgemeine Persönlichkeitsrecht (Recht am eigenen Bild) bzw. ähnliche Gesetze zum Schutz von persönlichen und geschäftlichen Daten zu berücksichtigen.

Die Verhaltensempfehlungen für die Nutzung von Internet-Diensten sollten im Intranet oder anderer geeigneter Form veröffentlicht werden.

Prüffragen:

- Sind die Mitarbeiter darüber informiert, wie sie im Internet auftreten sollten und welches Verhalten explizit zu vermeiden ist?

# M 3.79 Einführung in Grundbegriffe und Funktionsweisen von Bluetooth

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Bluetooth ist eine Funk-Technologie, die vor allem im Nahbereich eingesetzt wird. Diese Maßnahmen gibt einen Überblick über technische Grundlagen für verwendete Datenübertragung, sowie Erläuterungen zu Begriffen und Funktionalitäten, die für den Einsatz von Bluetooth notwendig sind.

**Technische Grundlagen der Datenübertragung**

Bluetooth arbeitet im 2,4-GHz-ISM-Frequenzband auf 79 Kanälen im Frequenzbereich von 2400 bis 2483,5 MHz. Der Kanalabstand beträgt 1 MHz, an den Bandgrenzen wurden 2 bzw. 3,5 MHz freigelassen, damit keine Störungen benachbarter Systeme auftreten.

Die Übertragung der Datenpakete erfolgt zeitschlitzgesteuert (TDD, Time Division Duplex) in Verbindung mit einem Frequenzsprungverfahren (FHSS, Frequency Hopping Spread Spectrum). Dies dient zur Reduzierung der Empfindlichkeit gegenüber Störungen. Im Allgemeinen findet ein Frequenzsprung nach jedem versendeten Paket statt. Die Sprungsequenz deckt alle 79 Kanäle gleichmäßig in kurzen Zeitabständen ab und wiederholt sich erst nach Ablauf mehrerer Stunden. Geräte ab der Bluetooth-Spezifikation 1.2 verwenden ein adaptives Frequenzsprungverfahren (AFH, Adaptive Frequency Hopping), das die von der Sprungsequenz abgedeckten Kanäle auf freie, d. h. ungestörte Frequenzen beschränkt. Hierdurch soll ein störungsfreier Parallelbetrieb mit anderen Funkdiensten, die im selben Frequenzbereich operieren, insbesondere WLAN, erreicht werden.

Als Modulationsverfahren wird eine Frequenz- bzw. Phasenmodulation angewandt. Dabei findet der Frequenzsprung grundsätzlich einmal pro Mikrosekunde statt, was als Symbolrate von 1 Megasymbole pro Sekunde bezeichnet wird. Die resultierende Datenrate ergibt sich aus dem angewendeten Modulationsverfahren, das die Zahl der pro Symbol übertragenen Bits bestimmt. Bluetooth kennt drei verschiedene Verfahren:

- Das erste Verfahren ist eine binäre Frequenzmodulation, das als "Basic Rate" bezeichnet wird, bei der ein Bit pro Symbol übertragen wird. Damit wird eine Datenrate von 1 MBit/s erreicht. Dieses Verfahren ist seit Version 1.1 Bestandteil der Bluetooth-Spezifikation. Alle Bluetooth-Lösungen müssen dieses Verfahren unterstützen.
- Das zweite Verfahren ist eine vierwertige Phasenmodulation, bei der zwei Bits pro Symbol übertragen werden. Dieses Verfahren erreicht eine Datenrate von 2 MBit/s, was als "Enhanced Data Rate" (EDR) bezeichnet wird. Definiert wird das Verfahren in der Bluetooth-Version 2.0 + EDR.
- Das dritte Verfahren ist eine achtwertige Phasenmodulation, bei der drei Bits pro Symbol übertragen werden. Die Datenrate, die ebenfalls als "Enhanced Data Rate" bezeichnet wird, erreicht hierbei 3 MBit/s. Dieses Verfahren ist ebenfalls in der Bluetooth-Version 2.0 + EDR definiert.

Eine Kompatibilität von Geräten mit unterschiedlichen Bluetooth-Spezifikationen wird dadurch erreicht, dass die Protokollinformation am Beginn eines jeden Pakets grundsätzlich mit der "Basic Rate" ausgesendet wird. Erst zur Übertragung der Nutzdaten wird auf eine Variante von EDR umgeschaltet, sofern die Gegenstation dies unterstützt. Ob ein Endgerät die "Enhanced Da-

ta Rate" unterstützt, kann an der Abkürzung "EDR" bei der Angabe der Versionsnummer der Bluetooth-Spezifikation erkannt werden, die das Endgerät unterstützt.

Grundsätzlich verwendet Bluetooth zwei verschiedene Modi bei der Datenübertragung:

- Asynchrone verbindungslose Übertragung (ACL, Asynchronous Connectionless Link)
- Synchrone verbindungsorientierte Übertragung (SCO, Synchronous Connection Oriented)

Während die asynchrone verbindungslose Übertragung vornehmlich für die reine Datenübertragung verwendet wird, kommt die synchrone verbindungsorientierte Übertragung für die Sprachkommunikation zum Einsatz. Hierbei ist die asynchrone Übertragung mit der Übertragung bei WLANs gleichzusetzen, die synchrone Übertragung entspricht der leitungsvermittelnden Übertragung in einem Telefonnetz. Bei der asynchronen Übermittlung können Datenraten von maximal 723 kBit/s bzw. 58 kBit/s (asymmetrisch) bzw. 434 kBit/s (symmetrisch) erreicht werden. Mit EDR kann dieser Wert mit der achtwertigen Phasenmodulation maximal verdreifacht werden.

**Bluetooth-Klassifizierung nach Sendeleistung**

Bluetooth-Stationen werden bezüglich ihrer Sendeleistung klassifiziert. Die Sendeleistung steht dabei in einem direkten Zusammenhang mit der Reichweite der Bluetooth-Funkwellen. Unterschieden werden hierbei folgende drei Klassen:

| **Bluetooth-Klasse** | **max. Sendeleistung** | **max. Reichweite** |
|---|---|---|
| Klasse 1 | 100 Milliwatt | ca. 100 Meter |
| Klasse 2 | 2,5 Milliwatt | ca. 10 Meter |
| Klasse 3 | 1 Milliwatt | ca. 1 Meter |

Tabelle: Bluetooth-Klassen nach Sendeleistung

Die Reichweite ist von vielen Umgebungsbedingungen abhängig, die angegebenen Zahlen stellen Idealwerte dar. Die Reichweite kann durch äußere Störungen, wie zum Beispiel Gebäudekonstruktionen oder andere Funktechnologien wie WLAN kleiner ausfallen. Zur Senkung des Stromverbrauchs sind verschiedene Sparmodi (Sniff-, Park- und Hold-Mode) und eine Sendeleistungsregelung (Power Control) spezifiziert.

**Anwendungsprofile**

Um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sein müssen, hat die Bluetooth SIG sogenannte Anwendungsprofile definiert. Im Folgenden werden einige häufig verwandte Profile aufgeführt:

- Generic Access Profile (GAP): GAP ist das grundlegende Profil zur herstellerübergreifenden Kommunikation von Bluetooth-Geräten. Das GAP beschreibt die für das Erkennen und den Verbindungsaufbau von Bluetooth-Geräten erforderlichen Prozeduren aus Anwendungssicht. Die Anwendungsprofile setzen die im GAP beschriebenen Prozeduren voraus.
- Serial Port Profile: Serielle Kabelverbindungen (RS-232) zwischen zwei Geräten werden oft durch Bluetooth ersetzt. Die Kommunikation erfolgt in diesem Fall über das Protokoll RFCOMM (Radio Frequency Communication). Durch das Serial Port Profil werden Anwendungsprogrammen eine

virtuelle serielle Schnittstelle bereitgestellt. Der im Vergleich mit anderen Funktechniken kostengünstige Ersatz serieller Leitungen durch Bluetooth spielt z. B. im produzierenden Gewerbe eine Rolle, wo Leitungen häufig erhöhten Belastungen ausgesetzt sind (ständige Bewegung, Schmutz, usw.).

- Headset Profile und Handsfree Profile: Diese beiden Profile beschreiben Funktionen, die ein Mobiltelefon im Zusammenspiel mit einer Freisprecheinrichtung benötigt. Neben der reinen Übertragung von Sprache in beiden Richtungen spielt beim Handsfree Profile auch die Fernbedienung des Mobiltelefons eine Rolle.
- Advanced Audio Distribution Profile (A2DP): Dieses Profil beschreibt Funktionen zur Übertragung von digitalen Audiodaten in hoher Qualität. Es wird beispielsweise dazu genutzt, hochwertige Stereo-Kopfhörer drahtlos an Abspielgeräte anzubinden.
- Human Interface Device Profile (HID Profile): Dieses Profil beschreibt die Protokolle und Funktionen, die zur drahtlosen Anbindung von Tastaturen, Mäuse und sonstigen Zeigegeräten an Rechner benötigt werden. Das HID-Profil ersetzt die entsprechenden Funktionen des kabelbasierten Universal System Bus (USB).
- Dialup Network Profile (DUN Profile) und Fax Profile: Diese Profile beschreiben Protokolle und Funktionen zur drahtlosen Anbindung von Modems oder Mobiltelefonen an Rechner mit dem Ziel, darüber Wählverbindungen zur Daten- oder Faxübertragung aufzubauen.
- File Transfer, Object Push und Synchronization Profile: Diese Profile werden zum Austausch von Dateien über Bluetooth genutzt. Wichtigste Anwendung ist die Synchronisierung von Kontakten, Terminen, Aufgaben und E-Mails zwischen tragbaren Geräten (Personal Information Manager, PIM) und Servern. Die Profile basieren auf dem Protokoll OBEX (OBject EXchange).
- Audio/Video Remote Control Profile (AVRCP): Dieses Profil beschreibt Protokolle und Funktionen zur Anbindung von Fernbedienungen an Abspielgeräte.
- SIM Access Profile (SAP): Dieses Profil unterstützt den SIM-Kartenzugriff. Dadurch kann ein Bluetooth-Gerät auf Daten zugreifen, die in der SIM-Karte eines anderen Geräts, typischerweise einem Mobiltelefon, gespeichert sind. Ein typischer Anwendungsfall besteht in einem fest im Fahrzeug eingebauten Autotelefon, das keine eigene SIM-Karte enthält. Stattdessen nimmt es Kontakt zu dem Mobiltelefon des Fahrers auf und meldet sich mit dessen Daten (und auf dessen Kosten) am Mobilfunknetz an.

**Verbindungsaufbau und Netztopologien**

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse, die sogenannte Bluetooth Device Address.

Basis für den Verbindungsaufbau sind die beiden Prozeduren Inquiry und Paging. Durch das Inquiry kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte innerhalb des Empfangsbereichs befinden, vorausgesetzt diese Geräte sind als erkennbar konfiguriert (discoverable). Ab der Bluetooth-Spezifikation 2.1 + EDR unterstützen die Geräte ein erweitertes Inquiry, bei dem neben der Geräteadresse auch der Gerätename und die unterstützten Anwendungsprofile bekannt gemacht werden. Mittels Paging kann nun eine Verbindung zwischen zwei Bluetooth-Geräten aufgebaut werden. Hierbei wird das Gerät, das die Verbindung aufbaut, als Master bezeichnet, das andere als Slave. Auf das Paging erfolgen in der Regel weitere Schritte als Voraussetzung für eine erfolgreiche Kommunikation. Viele Anwendungsprofile stellen beispielsweise durch den Austausch eines sogenannten Verbindungsschlüssel (Link Key) ei-

ne paarweise Geräteverbindung her. Dieser Vorgang wird im Generic Access Profile (GAP) auch als Bonding bezeichnet.

Neben der Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten sieht die Bluetooth-Spezifikation auch eine Punkt-zu-Mehrpunkt-Verbindung vor. Hier können bis zu 255 Bluetooth-Geräte in einem sogenannten Piconet als Slaves mit einem Master vernetzt werden. Innerhalb eines Piconet können bis zu 7 Slaves gleichzeitig aktiv mit einem Master kommunizieren. Alle Geräte in einem Piconet folgen der gleichen Channel Hopping Sequence und dem Zeittakt des Masters. Bluetooth sieht sogar die Möglichkeit vor, dass ein Gerät Mitglied mehrerer Piconets ist. Hierdurch entsteht ein sogenanntes Scatternet. Zur Bildung von Scatternets und zum anschließenden Datenaustausch in einem solchen Netz werden jedoch zusätzliche Protokolle benötigt, für die es derzeit nur Ideen, jedoch keine praktischen Implementierungen gibt.

**Sicherheitsmechanismen von Bluetooth**

Im Folgenden werden einige der wesentlichen Sicherheitsmechanismen von Bluetooth kurz erläutert.

**Kryptographische Sicherheitsmechanismen**

Da Bluetooth ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass unberechtigte Bluetooth-fähige Geräte die Bluetooth-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Die in den Bluetooth-Spezifikationen vorgesehenen kryptographischen Sicherheitsmechanismen haben die Ausschaltung dieser beiden Bedrohungen zum Ziel. Diese Funktionen sind bereits auf Chipebene implementiert und stehen auf der Link-Schicht einheitlich zur Verfügung.

Basis aller eingesetzten kryptographischen Verfahren sind Verbindungsschlüssel (Link Keys), die während der sogenannten Paarung zwischen jeweils zwei Bluetooth-Geräten vereinbart werden.

**Paarung (Pairing) und Verbindungsschlüssel**

In der Regel wird beim Pairing zweier Bluetooth-Geräte ein nur für die Verbindung dieser beiden Geräte genutzter, 128 Bit langer Kombinationsschlüssel (Combination Key) erzeugt und in beiden Geräten zur zukünftigen Nutzung als Verbindungsschlüssel (Link Key, LK) gespeichert.

Bei der Erzeugung des Kombinationsschlüssels gehen von beiden Geräten die Geräteadressen und je eine Zufallszahl ein. Für die gesicherte Übertragung dieser Zufallszahlen wird ein Initialisierungsschlüssel verwendet, der sich aus einer weiteren (öffentlichen) Zufallszahl, einer Geräteadresse und einer im Allgemeinen konfigurierbaren PIN berechnet. Dazu muss in beide Geräte die gleiche PIN eingegeben werden. Die PIN ist entweder durch die Benutzer konfigurierbar oder fest voreingestellt. Verfügt eines der Geräte über eine feste PIN, so muss diese in das andere Gerät eingegeben werden. Zwei Geräte mit fest voreingestellter PIN können nicht gepaart werden. Fest voreingestellt sind typischerweise nur die PINs von Headsets und ähnlichen einfachen Geräten.

Die Eingabe einer langen PIN an zwei Geräten durch den Nutzer ist fehleranfällig und kann zudem mit Zeitschranken für den Paarungsablauf in Konflikt kommen. Zur Vermeidung dieses Problems hat bereits die Bluetooth-Spezifikation 2.0 + EDR alternativ einen automatisierten Austausch zwischen den beiden Bluetooth-Geräten vorgeschlagen, z. B. auf Basis des Diffie-Hell-

mann-Verfahrens. Erst die Spezifikation 2.1 + EDR führt ein derartiges Verfahren ein, das Secure Simple Pairing.

Neben den Kombinationsschlüsseln erlaubt der Standard weitere Möglichkeiten für Link Keys:

- Geräteschlüssel (Unit Keys) können als Link Key genutzt werden. Der Geräteschlüssel wird bei der erstmaligen Verwendung eines Bluetooth-Geräts erzeugt und normalerweise nicht mehr geändert. Die Verwendung von Geräteschlüsseln wird von der Bluetooth-Spezifikation nicht mehr empfohlen, da diese ein Sicherheitsrisiko darstellen.
- Master-Schlüssel (Master Keys) können für die Dauer einer Bluetooth-Sitzung zwischen mehreren Geräten (temporär) vereinbart werden, wenn ein Master mehrere Geräte unter Verwendung desselben Verschlüsselungsschlüssels erreichen will. Master-Schlüssel werden nur bei Punkt-zu-Mehrpunkt-Verbindungen eingesetzt und über die aktuellen Link Keys gesichert vom Master an die Slaves übertragen.

Die Bluetooth-Spezifikation unterscheidet temporäre und semipermanente Verbindungsschlüssel. Temporäre Verbindungsschlüssel sind eine Art Einmal-Schlüssel, d. h. für jede neue Verbindung wird ein neuer Verbindungsschlüssel erzeugt (ein Paarungsvorgang je Verbindung). Semipermanente Verbindungsschlüssel werden dagegen von den beteiligten Bluetooth-Geräten nach Paarungs- und Authentisierungsvorgang in einem nichtflüchtigen Speicher festgehalten. Der Einsatz semipermanenter Verbindungsschlüssel ermöglicht die erneute Verbindung zweier Geräte ohne eine erneute Authentisierung. Der Benutzer braucht dann beim Verbindungsaufbau nicht erneut eine PIN einzugeben. Damit sinkt das Risiko, dass der Verbindungsaufbau abgehört und dabei möglicherweise eine "schwache" PIN erraten werden kann.

**Secure Simple Pairing (SSP)**

Das Verfahren Secure Simple Pairing (SSP) wurde mit der Bluetooth-Spezifikation 2.1 + EDR eingeführt. SSP etabliert im Rahmen des Verbindungsaufbaus einen sicheren Kanal, über den der Verbindungsschlüssel zwischen den Geräten ausgetauscht wird. Zu diesem Zweck erfolgt ein Schlüsselaustausch nach einem Diffie-Hellman-Verfahren mit elliptischen Kurven, das für seine geringen Anforderungen an Rechenleistung bekannt ist.

Zur Vermeidung der beim Diffie-Hellman-Schlüsselaustausch prinzipiell bestehenden Gefahr eines Man-in-the-Middle-Angriffs erfolgt eine gegenseitige Authentisierung der Bluetooth-Geräte. Zur Authentisierung bietet SSP vier verschiedene Assoziationsmodelle an:

- "Numeric Comparison"
  Bei diesem Modell müssen beide Geräte über eine Anzeigeeinheit, auf der sich mindestens eine sechsstellige Zahl anzeigen lässt, sowie über die Möglichkeit, den Anwender "ja" oder "nein" eingeben zu lassen, verfügen. Ein Beispiel wäre die Verbindung zwischen einem Mobiltelefon und einem Laptop. Auf beiden Geräten wird im Rahmen zur Authentisierung dieselbe sechsstellige Zahl angezeigt. Der Anwender bestätigt die Übereinstimmung der Zahlen durch Eingabe von "ja" auf beiden Geräten.
- "Just Works"
  Dieses Modell ist für Geräte gedacht, die weder Zahlen anzeigen können noch über eine Eingabemöglichkeit verfügen, wie dies z. B. bei einfachen Kopfhörern der Fall ist. "Just Works" bietet keinen Schutz gegen Man-in-the-Middle-Angriffe auf die Authentisierung, gleichwohl schützt es ebenso gut vor einem passiven Abhören des Verbindungsvorgangs wie alle anderen Modelle des SSP.

- "Out of Band (OOB)"
  Dieses Modell basiert darauf, dass vor der eigentlichen Bluetooth-Kopplung über ein anderes Medium ein Kanal zwischen den zu verbindenden Geräten etabliert wird. Über diesen "Out-of-Band-Kanal" können sich die Geräte erkennen, ohne dass über Bluetooth Inquiry nach ihnen gesucht werden müsste. Auf jeden Fall wird der Kanal dazu genutzt, die für die Authentisierung erforderliche Information auszutauschen. Aus der Sicht des Anwenders ähnelt "Out of Band" dem "Just Works", da keine Benutzer-Interaktion notwendig ist. Allerdings ermöglicht der zweite, von Bluetooth unabhängige Kanal Man-in-the-Middle-Angriffe auf den Schlüsselaustausch zu erkennen. Eine Voraussetzung dafür ist, dass die für den Kanal verwendete Technik immun gegen solche Angriffe ist. Als "Out-of-Band-Kanal" könnte z. B. die Nahfunktechnik NFC (Near Field Communication) genutzt werden. Voraussetzung für eine erfolgreiche Kopplung unter Zuhilfenahme von NFC ist, dass die beiden zu koppelnden Geräte bis auf wenige Zentimeter angenähert werden.
- "Passkey Entry"
  Hier verfügt nur ein Gerät über eine Anzeigeeinheit, das andere Gerät besitzt darüber hinaus eine Eingabemöglichkeit für Zahlen oder Zeichen. Dieses Modell ist beispielsweise dazu geeignet, eine Bluetooth-Tastatur mit einem Rechner zu verbinden. Vom Gerät mit Anzeigeeinheit muss zur Authentisierung eine sechsstellige Zahl abgelesen und in das andere Gerät eingegeben werden. Denkbar ist auch, dass ein sechsstelliger Passkey in beide Geräte eingegeben wird.

Sofern beim Verbindungsaufbau kein "Out-of-Band-Kanal" zur Verfügung steht, erfolgen Inquiry und Paging auf herkömmliche Weise. Dann kann die Authentisierung nur mittels der drei Methoden "Numeric Comparison", "Just Works" oder "Passkey Entry" erfolgen. Steht der "Out-of-Band-Kanal" zur Verfügung, wird er zunächst dazu genutzt, den Kommunikationspartner zu erkennen, was das Inquiry ersetzt. Anschließend kann die Authentisierung mit jedem der vier Assoziationsmodelle erfolgen.

Das eigentliche Secure Simple Pairing umfasst insgesamt die folgenden fünf Phasen:

- Phase 1: Austausch öffentlicher Schlüssel
  Jedes Bluetooth-Gerät erzeugt ein Schlüsselpaar aus öffentlichem und privatem Schlüssel und beide übertragen ihren öffentlichen Schlüssel zum Kommunikationspartner. Dafür nutzen sie normalerweise den im Rahmen des Pairing etablierten Bluetooth-Kanal. Dieser Vorgang braucht grundsätzlich bei jedem Gerät nur einmal zu erfolgen. Die Bluetooth-Spezifikation lässt dem Hersteller die Freiheit, jederzeit ein neues Schlüsselpaar generieren zu lassen.
- Phase 2: Authentisierung 1. Stufe
  In Phase 2 wird überprüft, dass die Geräte authentische öffentliche Schlüssel von ihrem Kommunikationspartner erhalten haben. Man-in-the-Middle-Angriffe werden in dieser Phase erkannt. Zu diesem Zweck werden für "Numeric Comparison", "Passkey Entry" und "Out of Band" jeweils unterschiedliche Protokolle verwendet. "Just Works" verwendet hingegen dasselbe Protokoll wie "Numeric Comparison".
- Phase 3: Authentisierung 2. Stufe
  Diese Stufe dient einer Bestätigung, dass die Authentisierung und damit das Pairing erfolgreich waren. Diese Phase erfüllt einen wichtigen Zweck im Zusammenhang mit dem "Out of Band"-Assoziationsmodell. Wenn eines der Geräte nur über einen passiven Chip zur Nahfeldkommunikation über NFC (Near Field Communication) verfügt, kann es im "Out-of-Band-Kanal" zwar Daten senden, aber keine empfangen. Ein solches Gerät er-

fährt somit nichts über eine eventuell fehlgeschlagene Authentisierung. Für diesen Fall wird die Überprüfung, ob Authentisierung und Pairing erfolgreich waren, auf einem Bluetooth-Kanal erneut durchgeführt.
- Phase 4: Berechnung des Link Key
  Aus den zwischen beiden Geräten ausgetauschten Daten und dem aus dem Diffie-Hellman-Verfahren gewonnenen symmetrischen Schlüssel wird über eine kryptographische Funktion der Link Key ermittelt. In die Funktion fließt ein weiteres, nur für diesen Zweck erzeugtes Paar von Zufallszahlen ein, das sicherstellt, dass immer ein anderer Link Key entsteht, ohne das Diffie-Hellman-Schlüsselpaar bei jedem Verbindungsaufbau neu erzeugen zu müssen. Außerdem fließen die Geräteadressen und eine konstante Zeichenkette in die Berechnung des Link Key ein.
- Phase 5: Etablieren der Verschlüsselung
  Schließlich ermitteln beide Geräte mit Hilfe des symmetrischen Link Key einen Verschlüsselungsschlüssel, der die Basis für die Verschlüsselung des Datenstroms ist.

Die Phase 2 wird für jedes der vier möglichen Assoziationsmodelle auf eine spezifische Weise durchgeführt. Alle anderen Phasen sind unabhängig vom Modell.

**Sicherheitsbetriebsarten**

Das Generic Access Profile (GAP) von Bluetooth kennt vier Sicherheitsmodi für Geräte. Der Sicherheitsmodus 4 wird erst bei Geräten ab der Bluetooth-Spezifikation 2.1 + EDR mit Einführung des Secure Simple Pairing unterstützt.

- **Sicherheitsmodus 1 (non-secure)**: Das Bluetooth-Gerät initiiert selbst keine speziellen Sicherheitsmechanismen, reagiert aber auf Authentisierungsanfragen anderer Geräte.
- **Sicherheitsmodus 2 (service level enforced security)**: Die Auswahl und Nutzung von Sicherheitsmechanismen werden abhängig vom Bluetooth-Gerät (trusted oder non-trusted) und vom Dienst auf Anwendungsebene, d. h. abhängig vom Bluetooth-Profil, festgelegt. Das Gerät leitet erst dann Sicherheitsprozeduren ein, wenn es eine Aufforderung zum Verbindungsaufbau erhalten hat.
- **Sicherheitsmodus 3 (link level enforced security)**: Es ist generell eine Authentisierung beim Verbindungsaufbau erforderlich. Die Verschlüsselung der zu übertragenden Daten ist optional.
- **Sicherheitsmodus 4 (service level enforced security)**: Dieser Modus entspricht im Prinzip dem Sicherheitsmodus 2. Der Dienst auf Anwendungsebene bestimmt, in welcher Art der Link Key mittels Secure Simple Pairing auszutauschen ist. Im Sicherheitsmodus 4 werden drei Attribute unterschieden:

  - "Authenticated" meint, dass der Benutzer aktiv Eingaben während der Kopplung von zwei Geräten vornehmen muss. Alternativ besteht die Möglichkeit, dass die Endgeräte auf einem zweiten Kanal kommunizieren, der nicht für den normalen Datenaustausch verwendet wird ("Numeric Comparison", "Out-of-Band" oder "Passkey Entry").
  - "Unauthenticated" stellt eine Kopplung zwischen zwei Endgeräten ohne Benutzeraktionen durch ("Just Works").
  - "No Security required" fordert keine Sicherheitsmechanismen.

Die Bluetooth-Spezifikation 2.1 + EDR fordert die Verwendung des Sicherheitsmodus 4. Aus Gründen der Abwärtskompatibilität zu älteren Bluetooth-Geräten kann darüber hinaus der Sicherheitsmodus 2 eingesetzt werden.

Der jeweils genutzte Sicherheitsmodus wird durch die Anwendung ausgewählt. Beispiel: Die Spezifikation des SIM Access Profile, also das Bluetooth-Profil mit den höchsten Sicherheitsanforderungen, fordert grundsätzlich eine Authentisierung und Verschlüsselung. Zu diesem Zweck müssen die Geräte den Sicherheitsmodus 2 oder 3 einsetzen, wenn sie der Bluetooth-Spezifikation 2.0 + EDR oder 1.x entsprechen. Geräte der Spezifikation 2.1 + EDR und 3.0 + HS müssen den Sicherheitsmodus 4 verwenden.

Über diese Sicherheitsmodi hinaus beschreibt das GAP, wie sich das Verhalten von Bluetooth-Geräten beim Verbindungsaufbau steuern lässt:

- **Erkennbarkeit**: Über diesen Modus wird gesteuert, ob das Gerät auf Inquiry antwortet. Neben dem "non-discoverable mode" (Gerät antwortet nicht auf Inquiry) und dem "general discoverable mode" (Gerät antwortet immer auf Inquiry) ist auch der "limited discoverable mode" vorgesehen, bei dem das Gerät nur für eine bestimmte Zeitspanne oder infolge bestimmter Gerätezustände erkennbar wird.
- **Möglichkeit des Verbindungsaufbaus**: Dieser Modus steuert die Fähigkeit von Bluetooth-Geräten, auf Verbindungsanfragen mittels Paging zu antworten. Ein Gerät ist entweder im "connectable mode" oder im "non-connectable mode".
- **Möglichkeit einer paarweisen Geräteverbindung**: Hierunter wird die Fähigkeit der Geräte verstanden, sich im Rahmen des Pairing gegenseitig zu authentisieren und einen paarweisen Schlüssel (Link Key) auszutauschen ("bondable mode"). Ist ein Gerät dagegen im "non-bondable mode", lässt sich eine paarweise Verbindung als Basis einer verschlüsselten Kommunikation nicht herstellen. In älteren Bluetooth-Spezifikationen wurden diese Modi noch mit dem Begriff "pairable" belegt.

**Authentisierung**

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet. Es wird grundsätzlich eine einseitige Authentisierung genutzt, d. h. ein Gerät (Claimant) authentisiert sich gegenüber einem anderen Gerät (Verifier). Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt.

**Verschlüsselung**

Die Verschlüsselung kann optional verwendet werden, wenn sich mindestens eines der beiden kommunizierenden Geräte gegenüber dem anderen authentisiert hat. Dabei kann die Verschlüsselung sowohl vom Master, als auch vom Slave beantragt werden. Die Verschlüsselung selbst wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat. Dazu einigen sich die beiden Geräte zunächst auf die Länge des zu verwendenden Schlüssels. Anschließend startet der Master die Verschlüsselung, indem er eine Zufallszahl an den Slave sendet.

Es stehen für die Verschlüsselung zwei Betriebsarten zur Verfügung: Punkt-zu-Punkt-Verschlüsselung und Punkt-zu-Mehrpunkt-Verschlüsselung. Bei der Punkt-zu-Punkt-Verschlüsselung wird der Authenticated Cipher Offset des Authentisierungsprotokolls als Cipher Offset verwendet. Bei der Punkt-zu-Mehrpunkt-Verschlüsselung wird dagegen die Geräteadresse des Master als Cipher Offset genutzt. Außerdem muss der Verbindungsschlüssel durch einen Master-Schlüssel ersetzt werden, bevor die Verschlüsselung gestartet wird. Eine Punkt-zu-Mehrpunkt-Verschlüsselung wird z. B. in einem Piconet benötigt, wenn der Master eine Nachricht an mehrere Slaves sendet (Multicast).

**Bluetooth über IEEE 802.11 WLAN**

In der Spezifikation Bluetooth 3.0 + HS findet sich die Beschreibung einer alternativen Funktechnik, die als "Alternate MAC/PHY" (AMP) bezeichnet wird. Bluetooth kann unter Nutzung der physikalischen Schnittstelle eines WLANs gemäß IEEE 802.11 höhere Datenraten bereitstellen als bisher. Das "Logical Link Control and Adaption Layer Protocol" (L2CAP) wurde zu diesem Zweck um Funktionen erweitert, die eine Wahl der Funktechnik und des entsprechenden Controllers zulassen. Es gibt sogar Funktionen, die den Wechsel der Funktechnik während einer bestehenden Verbindung erlauben.

Die technologieunabhängige Wahl des Begriffs AMP impliziert, dass es zukünftig weitere Funksysteme für Bluetooth geben kann.

Kernstück der Spezifikation ist der sogenannte "802.11 Protocol Adaption Layer" (802.11 PAL). Es stellt das Bindeglied zwischen der Host-Controller-Schnittstelle (HCI) von Bluetooth und der MAC-Schnittstelle von WLAN her. Der 802.11 PAL leistet unter anderem:

- Aufbau physikalischer Verbindungen nach Anforderung durch das HCI.
- Datenübertragung mit Hilfe von WLAN-Paketen.
- Vermeiden von Interferenzen zwischen WLAN und Bluetooth im 2.4-GHz-Band. Das PAL sorgt dafür, dass verbindungsorientierter Datenverkehr (SCO), der immer über den Bluetooth Controller abgewickelt wird, nicht gleichzeitig mit verbindungslosen Datenpaketen (ACL) auf dem WLAN Controller gesendet wird.

Weitere Hintergrundinformationen und technische Beschreibungen zu den Bluetooth-Spezifikationen finden sich auch in der BSI-Broschüre "Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte", die auf der BSI-Webseite zum Download zur Verfügung steht.

# M 3.80 Sensibilisierung für die Nutzung von Bluetooth

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Beim Betrieb von Geräten mit Bluetooth-Schnittstellen sollten sich die IP-Verantwortlichen und das Sicherheitsmanagement über Bluetooth-Grundlagen informieren. Einen Überblick über die Grundbegriffe bei Bluetooth liefert die Maßnahme M 3.79 *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*.

**Schulung von Administratoren**

Die Administratoren für Geräte mit Bluetooth-Schnittstellen sollten neben theoretischen auch praktische Kenntnisse besitzen. Sie sollten unter anderem in folgenden Themen geschult sein:

- Überblick über Sicherheitsaspekte von Bluetooth
- Typische Gefährdungen bei Bluetooth-Geräten
- Betriebsmodi, Verbindungsaufbau, Authentikation und Absicherung der Bluetooth-Kommunikation
- Auswahl geeigneter Sicherheitsmechanismen für den Bluetooth-Betrieb
- Konfiguration und Test von Bluetooth-Komponenten
- sicherheitsrelevante Bluetooth-Konfigurationsparameter

**Sensibilisierung von Benutzern**

Auch die Benutzer von Geräten mit Bluetooth-Schnittstellen sollten die Funktionsweise und die sichere Bedienung der Bluetooth-Komponenten kennenlernen. Benutzern muss genau erläutert werden, was die Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem müssen sie auf die Gefahren hingewiesen werden, wenn diese Sicherheitseinstellungen aus Bequemlichkeit bzw. zur Reduktion von störenden Warnmeldungen umgangen oder deaktiviert werden. Durch eine gezielte Sensibilisierung der Benutzer kann eine ordnungsgemäße Bedienung der Bluetooth-Komponenten und deren Sicherheitseinstellungen erreicht werden.

Die Verwendung von PINs als Basis für Authentisierung und Verschlüsselung ist ein Problem beim praktischen Einsatz von Bluetooth. Typische Gewohnheiten der Nutzer bei der Vergabe von PINs waren in der Vergangenheit häufig Ziele von Angriffen. Hier bietet Secure Simple Pairing Abhilfe. Insbesondere die Methode der Numeric Comparison bietet eine Chance für den sicheren Einsatz von Bluetooth, da hierbei keine von den Benutzern ausgewählten starken Kennwörter verlangt werden.

Die Absicherung der Kommunikation über Bluetooth lässt sich technisch nicht erzwingen, sie bleibt auch in Anbetracht der aktuellen Verfahren eine Aufgabe für die Benutzer. Dabei stehen sichere Konfiguration und umsichtiger Umgang mit der Technik im Vordergrund.

Die Schulungsinhalte müssen immer entsprechend der jeweiligen Einsatzszenarien angepasst werden. Auch Schulungen mit Hilfe von webbasierten interaktiven Programmen im Intranet sind hier denkbar. Neben der reinen Schulung zu Bluetooth-Sicherheitsmechanismen müssen die Mitarbeiter jedoch auch die entsprechende Sicherheitsrichtlinie ihrer Institution vorgestellt bekommen.

Prüffragen:

- Sind die Administratoren auf den Umgang mit Bluetooth-Komponenten vorbereitet und insbesondere in sicherheitsrelevanten Aspekten geschult?
- Sind die Benutzer mit den Bluetooth-Sicherheitsmechanismen vertraut?

# M 3.81 Schulung zum sicheren Terminalserver-Einsatz

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter Fachabteilung, Leiter IT

Die Verwaltung der Terminalserver-Infrastruktur ist für Administratoren komplex, für Benutzer ohne Vorerfahrung in einigen Punkten erklärungsbedürftig. Alle Personen, die mit einem Terminalserver-System arbeiten, sollten daher geschult werden. Dies gilt im besonderen Maße für Administratoren.

**Schulungsinhalte Administratoren**

Für die Administration werden detaillierte Kenntnisse der verwendeten Applikationsservertechnik und die dahinter stehenden Verwaltungswerkzeuge und Dienste benötigt. Zudem sind Erfahrungen im Umgang mit dem Betriebssystem notwendig, das die Basis der jeweilig eingesetzten Lösung bildet.

Die Terminalserver-Architektur trennt die Eingabe, Ausgabe und Programmausführung voneinander. Durch diese Abstraktion ist es möglich, dass den Terminals ein völlig anderes Betriebssystem zu Grunde liegt, als dem Server. In dem Fall ist zusätzliches Fachwissen der zuständigen Personen über die Client-Systeme erforderlich. Ansonsten kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitstechnische Auswirkungen haben können. Eine Schulung der Administratoren auf diesem Gebiet und insbesondere zu Schutzmechanismen im Terminalserver-Umfeld ist daher unerlässlich.

Die Schulungsinhalte sind dem Nutzungsspektrum der zu schulenden Personen anzupassen. Ein Teil der Schulung sollte immer auch sicherheitsrelevante Themen ansprechen, so dass eine Sensibilisierung für den sicheren Umgang mit Terminalservern erfolgt.

Es empfiehlt sich in regelmässigen Abständen das Bewusstsein für die Sicherheit aufzufrischen (Security-Awareness-Programm) und auf veränderte oder neue Situationen, Mechanismen oder Verfahren hinzuweisen. In diesem Rahmen sollten die in der Institution gültigen Sicherheitsrichtlinien angesprochen und die Terminalserver-spezifischen Themen aufgegriffen sowie etwaige Unklarheiten ausgeräumt werden.

- Grundlagen:
  - Überblick über die eingesetzte Terminalserver-Umgebung
  - Überblick über die zugrundeliegende Netzarchitektur
  - Sicherheitsverwaltung und Werkzeuge
- Anwendungsumgebung:
  - Softwareinstallation
  - Erstellen einer sicheren Benutzerumgebung
  - Serverdimensionierung und Lasterverteilung
  - Druckszenarien
- Anbindung von Benutzern an Terminalserver:
  - Zugangs- und Zugriffsmethoden
  - Perimeterschutz
  - Endgerätesicherheit
  - Verschlüsselung
  - Verteilung der Client-Software
  - Gegebenenfalls Bereitstellung über ein Webportal

- Terminalserver-Umgebung:
  - Anbindung von Verwaltungsservern und nachgelagerten Diensten
  - Migrations- und Integrationsstrategie
  - Lizenzierung
- Betrieb:
  - Rechtevergabe und Härtung der Terminalserver-Umgebung
  - Softwareaktualisierung
  - Neustartzyklen
  - Sicherheits- und Datenschutzaspekte bei der Sitzungsspiegelung
  - Überwachung und Protokollierung
- Notfallvorsorge:
  - Redundanzmechanismen
  - Sicherungsrelevante Daten der Terminalserver-Umgebung
- Aussonderung:
  - Löschen kritischer Daten

**Schulungsinhalte Anwender**

An Schulungen für Anwender sind hiervon abweichende Anforderungen zu stellen. Für Benutzer ist vorrangig das Wissen über die Besonderheiten und Sicherheitsaspekte von entfernten Benutzersitzungen von Bedeutung. Vor allem wenn zuvor noch keine Erfahrungen im Umgang mit der Terminalserver-Technologie bestanden, können leicht Fehler bei der Bedienung entstehen.

So können bei Clients mit eigenständigen Betriebssystem, beispielsweise Dateipfade und Druckernamen anders lauten als auf dem Terminalserver-Client. Zudem kann leicht Verwirrung über das vom Client abweichende Verhalten der entfernten Benutzeroberfläche entstehen.

Personen die Terminalserver nutzen, sind daher mindestens über die folgenden Themengebiete zu unterrichten:

- Aufklärung über die eingesetzten Sicherheitsmaßnahmen, mit dem ausdrücklichen Verbot diese zu deaktivieren oder zu versuchen diese zu umgehen
- Erlaubte Zugangswege und Endgeräte
- Pfade und Laufwerksverknüpfungen zur Dateiablage und zum Drucken
- Zugriff auf nachgelagerte Dienste
- Zugelassene Austauschmöglichkeiten von Informationen zwischen dem Betriebssystem des Clients und dem Terminalserver
- Verhalten bei Verbindungsabbrüchen
- Anweisung zum Abmelden am Ende der Nutzungszeit
- Anweisung zum Sperren des Clients bei Verlassen des Raumes
- Erlaubte Terminalserver, zu denen Benutzer sich mit der Terminalsoftware verbinden dürfen
- Verbot des Versendens von Konfigurationsdaten (z. B. .RDP oder .ICA Dateien)
- Handlungsanweisungen bei verdächtigem Verhalten (wie etwa ein sich selbstständig bewegender Mauszeiger)

Steht leicht verständliches schriftliches Schulungsmaterial zu Terminalservern bereit, so kann anstelle der Schulung auch die Aufforderung stehen, sich selbstständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings die Bereitstellung ausreichender Einarbeitungszeit.

Prüffragen:

- Wurden alle Anwender, insbesondere die zuständigen Administratoren für die Arbeit mit Terminalservern geschult und wurde die Schulungsinhalte an die zu schulenden Personen angepasst?
- Ist der Umgang mit allen Sicherheitsmechanismen der Terminalserver dargestellt worden?
- Wurden die Benutzer über den sicheren Umgang mit entfernt ablaufenden Anwendungen auf Terminalservern geschult?

# M 3.82 Schulung zur sicheren Nutzung von TK-Anlagen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Personal
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Für die korrekte und ihrer Bestimmung entsprechende Verwendung von Diensten und Geräten im Umfeld einer TK-Anlage ist eine Unterweisung der Benutzer notwendig. Zusätzlich sollten den Benutzern der TK-Anlage alle notwendigen Unterlagen zur Bedienung der entsprechenden Endgeräte wie die Bedienungsanleitung für das Telefon zur Verfügung gestellt werden. Mangelnde Sicherheit bei der Bedienung kann die Vertraulichkeit und die Integrität gefährden, aber auch dazu führen, dass nicht alle gegebenen Möglichkeiten bekannt sind und die Anlage nicht wie geplant genutzt wird. In diesem Zusammenhang ist es vorteilhaft, auch Ansprechpartner und Verantwortliche zu nennen. Generell ist auf die Einhaltung der Richtlinien und Regelungen zur Nutzung von TK-Anlagen hinzuweisen.

Zusätzlich ist es für alle Benutzer einer (klassischen) TK-Anlage wichtig, die Bedeutung der üblichen Warnanzeigen, -töne und -symbole der TK-Anlage zu kennen. Zu diesen zählen insbesondere:

- Aufmerksamkeitston für direktes Ansprechen,
- Aufschalte-Warnton,
- Freisprechanzeige,
- Anzeige für aktiviertes direktes Ansprechen,
- Anzeige für automatischen Rückruf und
- Anzeige/Einblendung bei Dreierkonferenz.

Die Warnanzeigen sollen eindeutige Hinweise geben, sobald auf unsichere Merkmale der TK-Anlage zurückgegriffen wird. Die Nutzung bestimmter, eigentlich nicht freigegebener Leistungsmerkmale (Beispiel: Zeugenschaltung) kann zu Beeinträchtigungen der Informationssicherheit führen. Daher sollten besonders deren Warnanzeigen und -töne bekannt sein. Ein wichtiges Beispiel ist ein Warnsignal in dem Fall, dass gerade eine Aufschaltung durch einen Dritten auf ein zurzeit geführtes Telefonat erfolgt.

Jedes auffällige Verhalten der TK-Anlage sollte den entsprechenden Verantwortlichen gemeldet werden und wenn möglich bis zur Klärung alternative Kommunikationskanäle verwendet werden. Bei Manipulationen an der TK-Anlage ist der IT-Sicherheitsbeauftrage oder der Datenschutzbeauftragte zu informieren.

Wichtig ist es, zusätzlich auf den Schutz der Endgeräte durch Passwörter oder PINs hinzuweisen, um zu verhindern, dass Unberechtigte auf vertrauliche, in den Endgeräten gespeicherte Informationen zugreifen können. Viele Endgeräte verfügen bereits über werksseitig eingestellte Standard-Passwörter, die bei der erstmaligen Inbetriebnahme durch den Benutzer geändert werden sollten.

Die Mitarbeiter sollten je nach Benutzergruppen unterschiedlich unterrichtet werden. Administratoren sollten Schulungen mit anderen Inhalten als die Benutzer erhalten. Bei allen kann die sichere Anwendung der geschulten Inhalte gezielt unterstützt werden. Dafür eignen sich unter anderem Einträge im Intranet, Informationsveranstaltungen, Handzettel zur Telefonnutzung für Anwender, Arbeitsanweisungen für das Wachpersonal oder Checklisten für Admini-

stratoren. Derartige Hilfsmittel sollten bereits zum Schulungszeitpunkt erstellt sein und gezielt mit einbezogen werden.

Neben klassischen Schulungen sind auch Schulungen mit Hilfe von webbasierten interaktiven Programmen im Intranet denkbar. Aktuelle Entwicklungen können auch mithilfe von Newslettern oder Rundbriefen und im Rahmen regelmäßiger Veranstaltungen wie Abteilungsbesprechungen kommuniziert werden.

Prüffragen:

- Sind die Endgeräte der TK-Anlage so konfiguriert, dass eindeutige Hinweise gegeben werden, sobald unsichere Leistungsmerkmale verwendet werden?
- Sind die Warnanzeigen, -töne und -symbole der TK-Anlage allen Mitarbeitern bekannt?
- Werden die Mitarbeiter über die mit dem Benutzen einer TK-Anlage verbundenen Gefährdungen informiert?
- Liegen an allen TK-Endgeräten die richtigen Bedienungsanleitungen vor?

# M 3.83 Analyse sicherheitsrelevanter personeller Faktoren

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Zu den wichtigsten Grundpfeilern der Informationssicherheit in einer Institution gehören deren Mitarbeiter. Wie die Erfahrung zeigt, sind selbst die aufwendigsten technischen Sicherheitsvorkehrungen ohne das richtige Verhalten der Mitarbeiter wertlos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Informationen der Institution sind dafür wesentlich.

Die für die Institution ausgewählten Sicherheitsmaßnahmen sollten sich daher immer an den Mitarbeitern orientieren. Dabei sollte deren Wissen und Umgang mit Informationen und IT einbezogen werden. Daher ist es sinnvoll, die verschiedenen Faktoren zu analysieren, die dazu beitragen, wie sich Mitarbeiter aus Sicherheitssicht verhalten. Darauf aufbauend kann dann untersucht werden, wo die personelle und organisatorische Sicherheit noch verbessert werden kann, beispielsweise durch Sensibilisierung und Schulung zur Informationssicherheit.

Folgende Aspekte sollten durchleuchtet werden:

**Sicherheitskultur**

Der Begriff Sicherheitskultur umfasst die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen einer Institution und aller ihrer Mitarbeiter. Zur Sicherheitskultur gehört auch, wie offen der Umgang mit Fragen zur Informationssicherheit in der Institution gelebt wird. So ist für die effektive und effiziente Behandlung von Sicherheitsvorfällen eine vertrauensvolle und offene Kommunikationskultur wichtig, damit Sicherheitsvorfälle auch umgehend weitergemeldet und lösungsorientiert angegangen werden.

- Wie ist der Umgang in der Behörde oder dem Unternehmen mit geschäftsrelevanten Informationen und mit Risiken generell? Ist die Institution eher risiko-orientiert oder eher risiko-vermeidend? Werden Informationen eher freizügig oder nur restriktiv weitergegeben?
- Wie sind die Anforderungen an Genauigkeit und Präzision? Sind kleinere Fehler beispielsweise in Texten tragbar, weil diese ohnehin noch mehrere Abstimmprozesse durchlaufen müssen? Kann ein Eingabefehler bereits zu folgenschweren Schäden führen?
- Wie sind die Ansprüche an Verfügbarkeit? Gibt es eine Vielzahl enger Termine? Können Bearbeitungszeiten für Anfragen und Geschäftsprozesse flexibel festgelegt werden? Sind kleinere Terminüberschreitungen oder -änderungen im Allgemeinen tragbar oder führen sie zu harten Konsequenzen?

Stark beeinflusst wird die Sicherheitskultur einer Institution davon, in welcher Branche sie tätig ist. In Hochsicherheitsbereichen wird naturgemäß weniger offen mit Informationen umgegangen als in Forschungseinrichtungen.

**Wissen und Können**

- Wie gut kennen sich die Mitarbeiter mit IT aus? Ist IT- und Internet-Nutzung eher eine Notwendigkeit, um Geschäftsprozesse effektiver gestalten zu

können, oder sind Leben und Arbeiten ohne IT und Internet nicht mehr vorstellbar?
- Welche Erfahrungen und Kenntnisse haben die Mitarbeiter über Informationssicherheit und Datenschutz? Wie sind deren Fähigkeiten zu IT-basierten Sicherheitsmaßnahmen wie Verschlüsselung? Wie ist das Wissen in den verschiedenen Bereichen der Institution verteilt?
- Wie ist der gelebte Umgang der Mitarbeiter mit Fragen der Informationssicherheit und des Datenschutzes? Wie sehen die Mitarbeiter den Bedarf, Informationen vor Veränderungen oder unbefugter Weitergabe zu schützen?
- Können Mitarbeiter aktiv ihre Ideen und Vorstellungen zur Informationssicherheit in den Sicherheitsprozess einbringen?

**Sicherheitsrichtlinien**
- Passen die Sicherheitsrichtlinien der Institution zu den Geschäftsprozessen und der internen Sicherheitskultur? Sind sie einfach umzusetzen? Sind sie praxisnah und den aktuellen Umgebungsbedingungen angepasst? Behindern sie Arbeitsläufe? Unterstützen sie erwünschte Verhaltensweisen?

**Anwendungen und IT**
- Ermöglichen die vorhandenen IT-Komponenten einen Umgang mit den geschäftsrelevanten Informationen, der sowohl deren Schutzbedarf als auch den festgelegten Sicherheitsvorgaben entspricht?

**Leitungsebene**
- Wie steht die Leitungsebene zur Informationssicherheit? Nehmen Vorgesetzte ihre Vorbildfunktion war? Gibt es Wünsche der Leitungsebene zur Verbesserung der Sicherheitsprozesse?

**Kulturelle Hintergründe**
- Auch die kulturellen Hintergründe können den Umgang mit zu schützenden Informationen und mit Sicherheitsvorgaben generell beeinflussen. Daher sollte untersucht werden, ob es regionale und nationale Unterschiede im Umgang mit Informationssicherheit gibt. Vor allem sollte auch ergründet werden, welche unterschiedlichen Herangehensweisen an Informationssicherheit es in den verschiedenen Bereichen der Institution gibt. Auch einzelne Abteilungen können bereits eigene Regeln und Verhaltensweisen im Umgang mit geschäftsrelevanten Informationen entwickeln.

**Veränderungen**
- Alle Arten von weitreichenden Veränderungen für die Beschäftigten können deren Umgang mit Informationen, Geschäftsprozessen und IT ändern. Dazu gehören beispielsweise Umstrukturierungen, Entlassungen, Wechsel von Aufgaben oder Vorgesetzten.

Sollte sich bei der Analyse herausstellen, dass sich Mitarbeiter anders verhalten als es aus Sicherheitssicht sinnvoll ist, gibt es verschiedene Wege, um hiermit umzugehen. Es kann z. B. versucht werden, das Verhalten zu ändern (siehe B 1.13 *Sensibilisierung und Schulung zur Informationssicherheit*). Andererseits kann es in vielen Fällen einfacher sein, die Sicherheitsvorgaben oder Arbeitsabläufe umzugestalten, da Änderungen von Verhaltensweisen nur langfristig zu erreichen sind.

Prüffragen:

- Wurden in die Sicherheitskonzeption personelle Einflussfaktoren wie die vorhandene Sicherheitskultur einbezogen?

# M 3.84 Einführung in Exchange-Systeme

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, Leiter IT

Im Fokus von Groupware liegt die Unterstützung von Gruppen bei der Zusammenarbeit, bei der Terminabstimmung, Koordination sowie bei der täglichen Kommunikation. Die Groupware-Lösung der Firma Microsoft setzt sich aus dem Microsoft Exchange-Server und Microsoft Outlook zusammen. Der Exchange-Server ist ein Managementsystem für Nachrichten, das überdies Funktionen im Bereich der Workflow-Unterstützung bietet: Es ist unter anderem dazu gedacht, in mittleren bis großen Behörden bzw. Unternehmen den internen und externen Austausch von Nachrichten, wie z. B. E-Mails, zu ermöglichen. Es können Nachrichten mit Exchange verwaltet, zugestellt, gefiltert und versendet werden. Ebenso werden typische Kommunikationsanwendungen wie Newsgroups, Kalender und Aufgabenlisten sowie Unified Messaging angeboten und von Exchange verwaltet.

Microsoft Outlook ist ein Groupware-Client, der Bestandteil des Office Paketes von Microsoft ist. Neben der reinen E-Mail-Funktionen bietet er eine Reihe von Zusatzfunktionen, die Geschäftsprozessabwicklungen, wie z. B. Kommunikation und Messaging, in Unternehmen und Behörden erleichtern sollen.

Als Microsoft Exchange-Systeme werden im Weiteren die Kombination von einem Exchange-Server und angeschlossenen Outlook-Clients bezeichnet. Die Darstellung beschränkt sich im Folgenden auf typische und in der Praxis häufig anzutreffende Installationen.

**Exchange-Architektur**

Der strukturelle und topologische Aufbau eines typischen Microsoft Exchange-Systems ist insbesondere vom Einsatzszenario abhängig: Die Bandbreite von Topologien kann sich von kleinen Unternehmen und Behörden, die über einen einzigen Server verfügen, auf dem alle Funktionen ausgeführt werden, bis hin zu großen Unternehmen und Behörden, die normalerweise getrennte Server für einzelne Funktionen und Liegenschaften haben, erstrecken. Dieser unterschiedliche Aufbau spiegelt sich ebenfalls in der Active-Directory-Standort-Topologie wieder: Das Microsoft Exchange-System integriert den Microsoft Verzeichnisdienst Active Directory (siehe Baustein B 5.16 *Active Directory*). Der Integrationsgrad steigt mit jeder Version von Microsoft Exchange. Der Verzeichnisdienst kann auf mehrere (globale) Katalogserver verteilt sein.

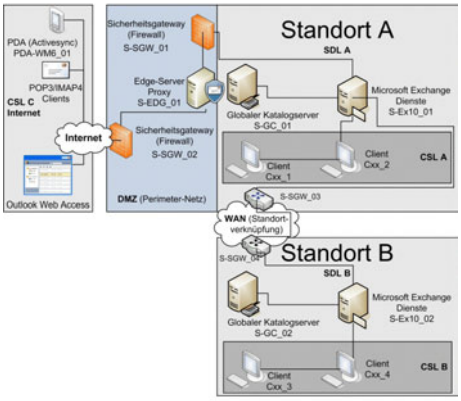



Abbildung 1: Typisches Exchange System

Bei einem Microsoft Exchange-System unterscheidet sich der Bereitstellungsort des Dienstes und der Ort der Inanspruchnahme des Dienstes: Ein Dienst-Bereitstellungsort (Service Delivery Location, SDL) bezieht sich auf einen physikalischen Ort, an dem sich Microsoft Exchange und andere Server befinden. Ein SDL muss alle abhängigen Dienste bieten, die von Microsoft Exchange benötigt werden. Neben einer lokalen Netz-Infrastruktur (Local Area Network, LAN) gehören die Namensauflösung mit DNS (Domain Name System) und Verzeichnisdienste von Active Directory-Domänencontrollern bzw. globalen Katalogservern zu den unverzichtbaren Standortfaktoren. In Abbildung 1 wird der DNS-Dienst, die Funktionen der Domänencontroller und Verzeichnisdienste von den Globalen Katalogservern S-GC_01 und S-GC_02 bereitgestellt. Optional enthalten SDLs auch öffentliche, externe Netzverbindungen und entmilitarisierte Zonen (Demilitarized Zones, DMZ) bzw. Perimeter-Netze. Ein SDL kann aus einem oder mehreren Subnetzen bestehen und einen oder mehrere Active Directory-Standorte enthalten. SDLs entsprechen einem einzelnen Gebäude oder einer dedizierten Umgebung mit einem allgemeinen Backbone-Netz. SDLs sind immer durch eine WAN-Verbindung (Wide Area Network) voneinander getrennt. In Abbildung 1 ist diese Verbindung durch die Standortverknüpfung charakterisiert: In der Darstellung werden die Standorte A und B (wobei es sich jeweils um eine eigenständige Exchange-Organisation handelt) über ein weiteres Perimeter-Netz voneinander getrennt.

Auf einen SDL kann eine Gruppe von Clients von einem Ort zugreifen (Client Service Location, CSL). Ein CSL kann sich am selben Ort wie ein SDL oder an einem vom SDL getrennten Ort befinden. Ein CSL umfasst dabei auch Geräte, die ein gängiges Client-Zugriffsprotokoll (POP3, SMTP, IMAP) über ein öffentliches Netz verwenden.

### Microsoft Exchange Server

Zu dem typischen Funktionsumfang eines Microsoft-Exchange-Systems an einem SDL gehören neben der Bereitstellung von E-Mails, der Verwaltung von Terminen in Kalendern, dem Verwalten von Aufgaben, Kontakten und Adressen auch die Ablage von Dokumenten und Notizen. Ein Client kann von einem CSL über Microsoft Outlook oder Outlook-Web-Access diesen Funktionsumfang nutzen. Mit Outlook-Web-Access kann nicht der volle Funktionsumfang genutzt werden. Gängige E-Mail-Clients sind auf die reinen E-Mail-Funktionen des Exchange-Servers beschränkt. Für eine detaillierte Beschreibung der E-Mail-Protokolle sei auf die RFC-Dokumente der IETF (Internet Engineering Task Force) verwiesen.

Das Microsoft Exchange-System bietet mit dem Activesync-Protokoll ein verbreitetes proprietäres Synchronisierungsprotokoll für mobile Geräte. Sicherheitsfunktionen hinsichtlich Vertraulichkeit und Integrität bietet Exchange über die zertifikatsbasierte Authentisierung und Verschlüsselung über eine PKI mit der Unterstützung für S/MIME, die Unterstützung für das Sender-ID-E-Mail-Authentisierungsprotokoll und die Leitungsverschlüsselung zwischen Client und Server. Neben einem Anti-Spam-Filter werden auch Annahme- und Verweigerungslisten (White-/Blacklists) verwaltet. Über so genannte Konnektoren für einige Drittherstellerprodukte und andere Transportprotokolle kann die Interoperabilität mit Microsoft Exchange gesichert werden.

Neben der geografischen Einordnung von Microsoft Exchange-Systemen werden ebenfalls die physikalischen Topologien betrachtet. Die Beschreibung eines Netzes über die Verteilung von Serverdiensten und Rollen auf physikalische Elemente reicht von SDLs mit einem Server, mit mehreren Servern bis hin zu mehreren Standorten. Dabei können die Serverdienste zentralisiert oder verteilt sein.

**Microsoft Outlook**

Microsoft Outlook ist eine Anwendung, die als E-Mail-Client, Kollaborationswerkzeug und zum Verwalten von persönlichen Informationen (Personal Information Manager, PIM) eingesetzt wird. Unter Mac OS von Apple bietet Microsoft mit Entourage eine vom Funktionsumfang ähnliche Anwendung an. In Verbindung mit dem Microsoft Exchange Server kann Outlook den vollen Funktionsumfang nutzen: Terminverwaltung, die Abstimmung von Besprechungen und die Verwaltung von mehreren Teilnehmern, Ressourcen und Räumen. Microsoft Outlook bietet Kontakt-Datenbanken sowie eine Notizen- und Aufgaben-Verwaltung unter einer Oberfläche an. Allerdings kann Outlook auch ohne Microsoft Exchange Server verwendet werden, da die verbreiteten Internet-Protokolle POP3, IMAPv4 und SMTP für die E-Mail-Funktion unterstützt werden.

**Standard- und Enterprise-Edition**

Microsoft Exchange-Systeme unterscheiden sich zum Teil erheblich in den Ausprägungen und Versionen.

Microsoft Exchange Server wird jeweils als Standard- oder Enterprise-Edition ausgeliefert. Mit den Editionen werden funktionale Einschränkungen über entsprechende Lizenzen realisiert: Unterschiede ergeben sich meist durch die Anzahl der Speichergruppen, die Möglichkeit, mehrere Datenbanken zu verwalten, die maximale Größe von Datenbanken und die Hochverfügbarkeitsoptionen, wie z. B. Clustering. Als Architektur- und Weiterentwicklungs-Konsequenz werden Microsoft Exchange Server und Microsoft Office als 64-Bit Version ausgeliefert, die auf 64-Bit Microsoft-Betriebssystemen ausgeführt werden können. Es ist allerdings nicht möglich, ein Update von einer 32-Bit-Version auf eine 64-Bit-Version durchzuführen.

Die konkreten Ausführungen sind im Folgenden beispielhaft für die Version 2010 aufgeführt:

- Microsoft Exchange 2010 wurde optimiert für die Deployment-Szenarien, in denen die Exchange-Dienste innerhalb einer Institution betrieben werden, so genannte "On Premise"-Installationen, als auch solche, in denen die Exchange-Dienste "on-demand" als externe Dienstleistung "Exchange Online" bereitgestellt werden. Microsoft selbst betreibt Rechenzentren, in denen Exchange Online betrieben und angeboten wird. Die Optimierung

geht allerdings auch soweit, als dass On Premise-Installationen nahtlos zusammen mit Exchange Online betrieben werden können; damit ist die Integration von getrennten Exchange-Organisationen und die Skalierbarkeit durch Zukauf von Exchange Online-Diensten äußerst flexibel. Ein weiteres Highlight ist die integrierte Archivierungsfunktion für E-Mails: Damit ist ein einheitlicher Schutz von Informationen und die Einhaltung von Richtlinien im E-Mail-Archiv realisiert; die neue Funktion erleichtert die Speicherung und das Wiederauffinden von E-Mails im gesamten Unternehmen bzw. der gesamten Behörde mit Hilfe der intuitiven Exchange-Oberfläche.

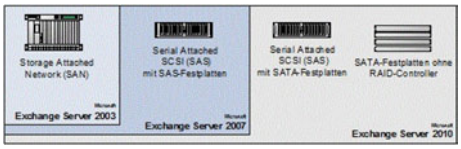



Abbildung 2: Weiterentwicklung der Informationsspeicher bei Microsoft Exchange Server

Die Datenbanken zum Verwalten der Informationsspeicher von Microsoft Exchange Server 2010 wurden in ihrem Zugriffsverhalten umgestellt: Die Input-Output-Vorgänge auf den Festplattenspeichern waren vor der Version 2010 durch den kostspieligen Random-Access-Zugriff gekennzeichnet. Für diese Zugriffsart waren hochverfügbare und zuverlässige Festplattenverbünde notwendig. Durch die Umstellung auf Microsoft Exchange 2010 können nunmehr auch günstige SATA-Festplattenspeicher für den Einsatz als Informationsspeicher für die Datenbanken eingesetzt werden, da Microsoft Exchange 2010 sequentiellen Zugriff für die Verwaltung der Daten verwendet. Die Sicherstellung der Integrität und Verfügbarkeit wird über die Architektur des Microsoft Exchange Kerns realisiert: Wiederherstellungsfunktionen nach Katastrophen und Hochverfügbarkeitsoptionen sind aus den Erfahrungen mit CCR und SCR in eine einzige Lösung kombiniert worden. Neben dieser Lösung sind die Möglichkeiten LCR, SCC und das Clustern der Mailboxserver obsolet. Der Paradigmenwechsel der Serverrollenaufteilung zieht sich nun konsequenterweise bis hin zu den Datenbanken: Einzelne Postfachserver können zu Datenbank-Verfügbarkeitsgruppen (englisch: Data Availability Groups, kurz DAG) verbunden werden. Diese bieten nun automatische Wiederherstellung auf logischer Postfachebene anstatt auf physikalischer Serverebene. Damit entfallen konzeptuell auch die "Speichergruppen", da die Postfachdatenbanken nun nicht mehr mit dem Microsoft Windows Server-System verbunden sind, sondern unabhängig verwaltet werden. Die Neuerungen treffen nicht auf die Informationsspeicher von "Öffentlichen Ordnern" zu.

Wichtige Neuerungen ergeben sich durch die Transport- und Routing- Funktionen in Microsoft Exchange Server 2010: Nunmehr sind Workflow-Genehmigungsprozesse innerhalb der E-Mail-Anwendung umsetzbar. Das Konzept der "Shadow Redundanz" im Nachrichtentransport verhindert einen Nachrichtenverlust innerhalb des Routings, indem der Absender-Server eine Kopie der versendeten Nachrichten zurückhält, bis der nächste Kommunikationspartner die Auslieferung bestätigt. Die Routing-Funktionen ermöglichen die Verknüpfung von mehreren Exchange On-Premise-Installationen ("Cross-Premises") und Exchange-Online Diensten. Routingoptionen, wie z. B. das Verhindern einer Weiterleitung oder das Verschlüsseln von Inhalten, wird über Regeln (englisch: Rights Management Services, kurz RMS) implementiert. Diese können auch über die Exchange-Organisation bzw. SDL hinaus über entsprechende Vertrauensstellungen realisiert werden.

Mit Microsoft Exchange Server 2010 wurde die Web-Unterstützung in Form von Outlook Web Access stark ausgebaut: die native Unterstützung von Brow-

sern wie Safari und Firefox konnte durch die konsequente Vermeidung von Microsoft-spezifischen aktiven Inhalten und Erweiterungen umgesetzt werden. Weiterhin können die Administrationstätigkeiten (englisch: Exchange Control Panel, kurz ECP) nun über die gleiche bekannte Web-Oberfläche von Outlook Web Access durchgeführt werden. Granulare Rollen und Aufgabenzuordnungen für unterschiedliche Administrator-Rollen und Administration durch Benutzer, wie z. B. die Anlage eines neuen Mitarbeiters oder die Verwaltung von Verteilerlisten, können über das Konzept der rollenbasierten Zugriffskontrolle (englisch Role Based Access Control, kurz RBAC) verwaltet werden. Insgesamt orientiert sich der Funktionsumfang der Outlook Web Access-Oberfläche nun deutlich stärker an der des Outlook-Software Clients.

Die Unterschiede der Standard- und Enterprise-Editionen verhalten sich analog zu denen des Microsoft Exchange Servers 2007.

Als Architektur- und Weiterentwicklungs-Konsequenz existiert in Microsoft Exchange Server 2010 ausschließlich die 64-Bit Version, die auf einem 64-Bit Microsoft-Betriebssystem, wie z. B. die x64-Version von Microsoft Windows Server 2003 oder die 64-Bit-Versionen des Microsoft Windows Servers 2008, ausgeführt werden muss.

Mit Microsoft Outlook 2010 wurden die Konzepte und Strategien zur Benutzerfreundlichkeit und Integration der Kommunikationsmöglichkeiten weiter ausgebaut: Voicemails werden in der Vorschau des Posteingangs direkt von natürlicher Sprache in lesbaren Text umgewandelt und angezeigt. Auch die in Microsoft Office 2007 eingeführte Ribbon-Oberfläche für die anderen Office-Anwendungen wird nun in Outlook integriert.

Die neue Funktion "MailTips" verhindert das Versenden von unnötigen E-Mails oder warnt vor eventuellen Missverständnissen beim Versenden an große Verteilergruppen oder externe Empfänger.

Mit den Funktionen "Clean Up" und "Ignore" können im Posteingang nunmehr Thread-basierte Zusammenfassungen der E-Mail-Nachrichten im Posteingang zur Verfügung gestellt werden und unerwünschte Nachrichtendiskussionen ignoriert werden.

# M 3.85 Einführung in OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

OpenLDAP ist ein Verzeichnisdienst, der auf dem LDAP-Projekt der University of Michigan basiert. Das ursprüngliche Projekt hatte zum Ziel, ein Äquivalent für das Directory Access Protocol (DAP) aus dem Verzeichnisdienst-Standard X.500 zu entwickeln. DAP war auf den OSI-Stack zugeschnitten, während LDAP als Lightweight DAP, also "schlankeres" DAP den TCP/IP-Stack nutzt. Das Adjektiv "schlank" deutet dabei an, dass LDAP nicht den kompletten Funktionsumfang von X.500 DAP umsetzt. Die University of Michigan entwickelte auch einen Server, der mit dem Protokoll besonders gut umgehen kann. In diesem Zusammenhang wird von einem LDAP-Server gesprochen, obwohl LDAP eigentlich nur ein Protokoll bezeichnet. Solche Server sind als hierarchische Datenbanken darauf ausgelegt, das Protokoll LDAP besonders gut zu unterstützen und die mit dem Protokoll ausgetauschten Daten effizient zu speichern.

### Open Source Software

OpenLDAP ist Open Source Software. Die Entwickler von OpenLDAP haben auf der Basis des ursprünglichen Projektes der University of Michigan den Server weiterentwickelt und stellen ihre Arbeit inklusive des Quelltextes im Internet kostenlos der Allgemeinheit zur Verfügung. OpenLDAP ist auf Unix- und Linux-Betriebssystemen am weitesten verbreitet, die Software kann jedoch ebenso unter Microsoft Windows oder auf anderen Plattformen wie z/OS eingesetzt werden. Die Entwickler von OpenLDAP legen großen Wert darauf, dass die Software den LDAP-Standard einhält. Im Gegensatz zu abweichenden Implementierungen wie bei Active Directory, oder ausdrücklich abgewandelten Formen des Protokolls LDAP, wie beim Novell eDirectory, hält OpenLDAP den LDAP-Standard in der aktuellen Version 3 (LDAPv3) strikt ein. Dies zeigt sich unter anderem daran, dass OpenLDAP für Konfigurationsdateien und den Import und Export von Daten das LDAP Data Interchange Format (LDIF) verwendet. Daher wird OpenLDAP auch als Referenz-Implementation von LDAPv3 bezeichnet.

OpenLDAP unterstützt neben LDAPv3 auch den LDAP-Standard in der Version 2 (LDAPv2), garantiert dafür jedoch keine strikte Einhaltung des Standards. Zum ursprünglichen X.500 DAP bestehen keine Schnittstellen mehr. Es ist zwar grundsätzlich möglich, Daten zwischen LDAP-Servern und X.500 DAP Directory System Agents auszutauschen, OpenLDAP enthält jedoch keine entsprechende Funktion. OpenLDAP unterstützt nativ IPv4 ebenso wie IPv6, außerdem die Unix Interprozess Kommunikation (IPC).

### Funktionsweise

Wie jeder LDAP-Server speichert OpenLDAP Daten in einer definierten hierarchischen Baumstruktur, dem Directory Information Tree (DIT). M 3.61 *Einführung in Verzeichnisdienst-Grundlagen* beschreibt die übliche Struktur und die verwendeten Begriffe. Seine Daten stellt OpenLDAP über eine Client-Server-Infrastruktur sitzungsorientiert zur Verfügung, d. h. jeder Benutzer des Verzeichnisdienstes nutzt Client-Anwendungen, um sich mit dem Server zu verbinden. Über den Client initiiert der Benutzer Operationen, wie die Suche nach einem Telefonbucheintrag oder die Änderung des eigenen Passworts. Der Server beantwortet diese Benutzeraktionen, beispielsweise indem er den gesuchten Eintrag übermittelt oder die erfolgreiche Passwortänderung bestä-

tigt. Werden dabei Werte von Attributen gelesen oder verändert, so ist zu unterscheiden, ob es sich um normale Attribute handelt oder um so genannte operationelle Attribute, die OpenLDAP zur internen Verwaltung einsetzt. Zu Letzteren gehört zum Beispiel der Dinstinguished Name (DN) oder die Zeitstempel, die im Rahmen der Replikation von Bedeutung sind. Nachdem der Benutzer alle Operationen durchgeführt hat, wird die Verbindung zum Server beendet ("unbind" zum Ende einer Sitzung).

**Architektur von OpenLDAP**

Der LDAP-Server von OpenLDAP ist der slapd-Server (stand-alone LDAP daemon). Er ist neben den LDAP-Bibliotheken, die ein IT-System benötigt, um LDAP-Funktionen zu nutzen, der wichtigste Bestandteil der OpenLDAP-Software. Der slapd-Server speichert Daten des Verzeichnisdienstes nicht selbst, sondern nutzt dafür ein Datenbankmanagementsystem (DBMS), das nicht zur OpenLDAP-Software gehört.

**Backends und Datenbanken**

Als **Backend** wird eine Teilkomponente von OpenLDAP bezeichnet. Der slapd-Server kommuniziert nicht direkt mit einem DBMS, sondern bedient sich dafür der Funktionen eines Backends. Backends werden in der Form "back-*" benannt. Grob wird unterschieden zwischen

- Backends, die tatsächlich Daten speichern (z. B. "back-hdb" zum Zugriff auf die BerkeleyDB),
- Backends, die einen Proxy-Zugriff auf andere Datenspeicher gewähren (z. B. "back-ldap" zum Zugriff auf andere Verzeichnisdienste) und
- Backends, die Daten dynamisch generieren (z. B. "back-monitor" zur Anzeige des aktuellen Zustands von OpenLDAP).

Diese grundsätzliche Unterscheidung sollte bei der Planung der Komponenten bekannt sein, sie ist für die spätere Konfiguration und im Betrieb allerdings nicht mehr wichtig.

Unter einer **Datenbank** wird bei OpenLDAP eine Instanz eines Backends verstanden, zum Beispiel die Datenbank, in der das Teilverzeichnis "OU=BSI, O=Bund, C=DE" gespeichert ist. In der Regel können mehrere Instanzen des gleichen Backends benutzt werden, so kann es eine Datenbank für das Teilverzeichnis "l=Bonn, OU=BSI, O=Bund, C=DE" und eine für das Teilverzeichnis "l=Berlin, OU=BSI, O=Bund, C=DE" geben. Bei manchen Backends ist auch nur eine Instanz möglich, es gibt zum Beispiel nur eine "back-monitor"-Instanz zur Laufzeit. In der Praxis und auch in der Literatur über OpenLDAP werden die Begriffe Backend und Datenbank oft synonym verwendet. Es ist jedoch stets darauf zu achten, Datenbanken als logischen (Teil-)Datenbestand eines Backends nicht mit dem DBMS als eigene Softwarekomponente zu verwechseln.

**Overlays**

Overlays sind dafür da, das Verhalten eines bestehenden Backends zu beeinflussen, ohne das Backend selbst anpassen oder neu schreiben zu müssen. Dazu wird das Overlay dem slapd-Server vorgeschaltet, so das Nachrichten den Server gefiltert erreichen beziehungsweise verändert verlassen. Die meisten Overlays sind auf Datenbankebene anzuwenden, allerdings oft nicht auf einen Backend-Typ beschränkt.

Einen Überblick über die Architektur von OpenLDAP gibt die folgende Grafik:

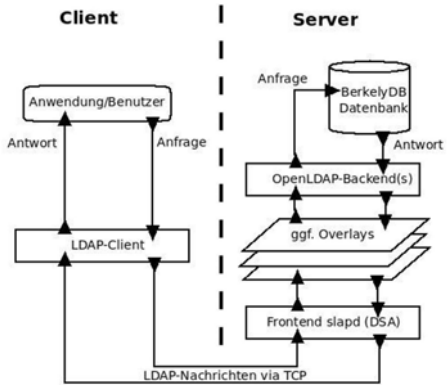


Abbildung: Architektur von OpenLDAP

Um Backends beziehungsweise Datenbanken und Overlays zu benutzen, sind zwei Schritte notwendig: Zum einen muss der Quelltext von Backends und Overlays bei der Übersetzung von OpenLDAP mit übersetzt werden (siehe M 4.383 *Sichere Installation von OpenLDAP*), zum anderen müssen Backends und Overlays in der Konfiguration aufgerufen werden (siehe M 4.384 *Sichere Konfiguration von OpenLDAP*). Backends und Overlays können auch als dynamische Module übersetzt werden.

**Werkzeuge**

Neben Bibliotheken und dem slapd-Server umfasst OpenLDAP auch eine Sammlung von Werkzeugen (Tools). Diese Werkzeuge werden in die ldap*-Werkzeuge und die slap*-Werkzeuge unterteilt.

Zu den ldap*-Werkzeugen gehören:

- ldapadd, um Einträge zu einem Verzeichnisdienst hinzuzufügen
- ldapauth, um sich an einem Verzeichnisdienst zu authentisieren
- ldapdelete, um Einträge aus einem Verzeichnisdienst zu entfernen
- ldapmodify, um bestehende Einträge in einem Verzeichnisdienst zu verändern
- ldapmodrdn, um den Distinguished Name (DN) eines Eintrags zu verändern
- ldappasswd, um das Passwort eines Personen-Objektes im Verzeichnisdienst zu verändern
- ldapsearch, um nach Einträgen im Verzeichnis zu suchen
- ldapwhoami, um die eigene Identität im Rahmen einer Sitzung auszugeben

Die ldap*-Werkzeuge nutzen das Protokoll LDAP selbst und richten Operationen als Clients immer an einen laufenden Verzeichnisdienst. Sie sind dabei vom Typ des slapd-Servers unabhängig, das heißt, sie können mit anderen LDAP-Servern kommunizieren und ihre Funktionen können wiederum durch andere Werkzeuge als die von OpenLDAP umgesetzt werden. Insbesondere werden in der Praxis grafische Werkzeuge eingesetzt.

Die slap*-Werkzeuge umfassen:

- slapacl, um die Wirksamkeit von Zugriffsrechten zu prüfen
- slapadd, um Einträge zu einem Verzeichnisdienst hinzuzufügen
- slapauth, um eine SASL-Identität gegen einen Verzeichnisdienst zu prüfen
- slapcat, um die Objekte aus einem Verzeichnisdienst zu exportieren
- slapdn, um einen Distinguished Name (DN) auf Zulässigkeit im bestehenden Verzeichnisdienst zu prüfen
- slapindex, um die Attribute (erneut) zu indizieren

- slappasswd, um zu einem Passwort den Hashwert zu generieren
- slaptest, um zu prüfen, ob eine Konfiguration syntaktisch korrekt ist

Die slap*-Werkzeuge nutzen **nicht** das Protokoll LDAP. Diese Werkzeuge arbeiten autark vom slapd-Server beziehungsweise umgehen ihn und greifen unter anderem direkt auf die Konfigurationsdateien oder die Dateien einer Datenbank zu. Die slap*-Werkzeuge sind auf den slapd-Server sowie die BerkeleyDB abgestimmt. Als Faustregel gilt, dass der slapd-Server **immer** laufen muss, wenn ldap*-Werkzeuge verwendet werden und **niemals** laufen sollte, wenn slap*-Werkzeuge eingesetzt werden.

**Anpassung von OpenLDAP**

OpenLDAP ist detailliert dokumentiert. Interne Zusammenhänge und Verarbeitungsschritte sind durch die Verfügbarkeit des Quelltextes bekannt. Es ist deshalb einfach möglich, Hilfsmittel für Administrationszwecke wie Skripte zu erstellen und einzusetzen. Es ist auch möglich, den Quelltext zu ändern und selbst zu übersetzen. Darüber hinaus existiert eine generische Programmschnittstelle (Application Programming Interface, API), durch die ohne Änderungen an OpenLDAP selbst eigene Backends und Overlays erstellt und genutzt werden können.

**Weitere Informationen**

Die IT-Grundschutz-Kataloge können nur eine allgemeine Einführung in OpenLDAP leisten und berücksichtigen insbesondere Sicherheitsaspekte. Andere Aspekte, wie Einstellungen zur Verbesserung der Leistung werden nicht betrachtet, obwohl sie bei Planung und Installation eine große Rolle spielen können. Neben der vorhandenen Fachliteratur zu OpenLDAP ist die von den Entwicklern von OpenLDAP kostenlos bereitgestellte Dokumentation eine sehr gute Informationsquelle. Als Hauptdokument ist der zur eingesetzten Version gehörende OpenLDAP Administrator's Guide (http://www.openldap.org/doc) zu nennen. Häufige Fragen (Frequently Asked Questions, FAQ) und Antworten werden unter http://www.openldap.org/faq gesammelt. In den FAQ finden sich allerdings auch Fragen und Antworten, die für eine frühere Version von OpenLDAP geschrieben wurden und aktuell nicht mehr gültig sind.

Für die umfangreichen Einstellungsmöglichkeiten und Parameter wird insbesondere auf die so genannten Manpages hingewiesen. Die Manpages von OpenLDAP werden in der Regel mit OpenLDAP zusammen installiert, sind aber auch im Internet verfügbar (http://www.openldap.org/software/man.cgi). Allerdings existieren zu Teilen der Software, insbesondere zu neu entwickelten Backends und Overlays, noch keine Manpages in hinreichender Qualität.

Für detailliertere Informationen oder im Problemfall empfiehlt sich ein Blick in die offiziellen Mailinglisten des Projekts unter http://www.openldap.org/lists. Die Listen können abonniert werden, ältere Nachrichten stehen unter der angegebenen Adresse auch in Archiven bereit.

# M 3.86 Schulung der Administratoren von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Um OpenLDAP sicher einzurichten und zu betreiben, werden detaillierte Kenntnisse über OpenLDAP und seine grundlegenden Konzepte benötigt. Eine Schulung der Administratoren zu OpenLDAP und den zugehörigen Sicherheitsthemen ist daher unerlässlich.

**Schulungsinhalte**

Wie tief sich ein Administrator mit den einzelnen Punkten beschäftigen muss, hängt von seinem Tätigkeitsfeld ab. Allgemeine Inhalte zu Verzeichnisdiensten werden in M 3.62 *Schulung zur Administration von Verzeichnisdiensten* aufgeführt. Schulungsinhalte sollten für OpenLDAP in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern.

**Grundlagen**
- Überblick über den Aufbau von OpenLDAP, Verständnis von Backends und Overlays
- Planung, Einrichtung, Konfiguration ("slapd.conf" und "slapd-config")
- Grundlegende Kenntnisse, die zur Installation der Anwendung aus dem Quelltext befähigen
- Verständnis im Umgang mit Informationsquellen zu Open Source Software
- Kenntnis des LDAP Data Interchange Formats (LDIF)
- Objektklassen und operationelle Attribute
- Kenntnis der Werkzeuge von OpenLDAP und des systematischen Unterschieds zwischen ldap*- und slap*-Werkzeugen

**Schema-Verwaltung**
- Problematik und Auswirkungen von Schema-Veränderungen
- Attributseinschränkungen durch Overlays innerhalb der Schemata
- Unterscheidung von normalen und operationellen Attributen

**Replikation**
- Verwendete Mechanismen zur Replikation bei OpenLDAP ("refreshOnly" und "refreshAndPersist")
- Suchfilter und operationelle Attribute
- Ausblick auf die Delta-Replikation
- Ausblick auf Multi-Master- und Mirror-Mode-Betrieb im Zusammenhang mit Replikationskonflikten

**Datensicherung**
- Problematik des Erstellens einer Datensicherung von OpenLDAP
- Sicherung der Konfiguration für beide Konfigurationsmodi
- Wiedereinspielen von Datensicherungen mittels "slapadd"

**Vergabe von Zugriffsrechten**
- Vergabe von Zugriffsrechten auf Verzeichnisdienstobjekte
- Zusammenwirken von globalen und datenbankspezifischen ACLs
- Mögliche Zugriffsrechte

**Authentisierung**
- Hash-Algorithmen
- Kerberos

- SASL
- SSL/TLS-Zertifikate

Prüffragen:

- Wurden alle Administratoren zu OpenLDAP und den zugehörigen Sicherheitsthemen geschult?

# M 3.87 Einführung in Lotus Notes/ Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

**Grundbegriffe und historische Entwicklung der Lotus Notes/Domino-Plattform**

Lotus Notes/Domino ist eine Produktfamilie des Bereichs Lotus Software des Herstellers IBM. Ursprünglich von Iris Associates entwickelt, wurde die Lotus Notes Groupware-Plattform das erfolgreichste Produkt der Lotus Software Corporation und über Jahrzehnte die am Markt dominierende Plattform für Kommunikation und Zusammenarbeit (*Communication Platform*). Seit der Verfügbarkeit von Microsoft Exchange und Outlook ist eine kommerzielle Alternative zu Lotus Notes/Domino vorhanden, die ebenfalls signifikante Marktanteile besitzt. Daneben gibt es eine Reihe von Open Source Produkten, mit denen sich die Funktionalität dieser beiden Plattformen abbilden lässt, von denen jedoch nur einzelne Komponenten (wie der Apache Webserver) hohe Marktanteile besitzen.

Mit Aufgabe des IBM Workplace Konzeptes (einer Parallelentwicklung zu Lotus Notes mit Groupware- und Office-Funktionalität auf der technologischen Basis von Open Office und WebSphere Plattform) wurde die Lotus-Produktpalette beim Hersteller strategisch und technisch aufgewertet, bis hin zur strategischen Positionierung des Lotus Notes Full Clients als universellem Client. Das Konzept des universellen Clients sieht die Nutzung eines einzigen Clients für den Zugriff auf unterschiedliche Anwendungen vor und schreibt praktisch die Nutzung eines einzigen Browsers als Client für eine Vielzahl von Web-Anwendungen in die Welt der Fat bzw. Full Clients fort. Hersteller mit umfangreichem Anwendungsportfolio können durch die Bereitstellung eines standardisierten (Full)-Clients für alle angebotenen Anwendungen, die umfangreichere Client-Funktionalitäten als über einen Browser möglich sind, Synergien nutzen.

Offene Standards ergänzen oder ersetzen zunehmend die proprietäre Lotus Notes/Domino-Welt. Lotus Notes/Domino unterstreicht damit zunehmend den Status einer Plattform. Dazu gehört eine breite Reihe von Basis-Diensten, wie E-Mail, Kalender/Terminplaner, Web-Zugriff, Presence und Instant Messaging sowie eine umfangreiche Unterstützung von Anwendungsentwicklung für diese Plattform. Mit eigenentwickelten Anwendungen können die Basis-Dienste um unternehmensspezifische Elemente ergänzt werden, wie z. B. Terminplanung mit Berücksichtigung unternehmensspezifischer Ressourcendatenbanken. Es können aber auch weitgehend unabhängige Anwendungen entwickelt werden, wie z. B. Anwendungen zur Abbildung von Vorgehensmodellen im Projektgeschäft. Hinzu kommen vielfältige Integrationsmöglichkeiten für andere Plattformen, offene Standards und ein Angebot von zusätzlichen Produkten des Herstellers und Dritter für die Lotus Notes/Domino-Plattform.

Im Folgenden wird der Begriff *Lotus Notes/Domino-Plattform* für die Summe der verfügbaren bzw. in der Institution eingesetzten Lotus Notes/Domino-Komponenten eines definierten Releasestandes verwendet, während der Begriff *Lotus Notes/Domino-Umgebung* für eine konkrete Instanz (Installation) mit definierter Funktionalität steht, beispielsweise das über Lotus Domino Dienste und Notes-Clients aufgebaute Intranet der Institution. Innerhalb einer Institu-

tion können mehrere Lotus/Domino-Umgebungen, aber auch mehrere Plattformen (durch den Paralleleinsatz unterschiedlicher Releases von Lotus Notes/Domino) im Einsatz sein.

Die Lotus Notes/Domino-Plattform beinhaltet server- und clientseitige Komponenten, die die anfallende Kommunikation, Datenhaltung und Datenverarbeitung abwickeln.

Lotus Domino ist die Bezeichnung für die serverseitig zu installierende Basiskomponente, während Lotus Notes die clientseitige Basiskomponente bezeichnet. Es ist grundsätzlich möglich, nur serverseitige oder nur clientseitige Komponenten zu nutzen. In der Regel enthält jedoch eine Lotus Notes/Domino-Umgebung sowohl serverseitige wie auch clientseitige Lotus-Komponenten.

Ursprünglich als klassische Client-Server-Anwendung in proprietärer Technologie mit einem Fat Client konzipiert, hat Lotus Notes/Domino grundlegende Änderungen erfahren. Als Clients können mittlerweile auch browserbasierte Clients (iNotes) oder Clients für mobile Endgeräte wie PDAs, Smartphones etc. genutzt werden. Daneben steht der "klassische" Client in einer proprietären (Basic Client) und einer auf dem Standard der Eclipse-Plattform basierenden Variante (*Standard bzw. Full Client*) zur Verfügung. Die Nutzung fremder E-Mail-Clients über POP3 und IMAP-Standards ist gleichfalls möglich.

Serverseitig wurde die Menge der verfügbaren Dienste des Domino-Servers erhöht und eine bessere Anbindung an die unter Web 2.0 zusammengefassten neuen Internet-Standards geschaffen.

Heutige Notes/Domino-Einsatzszenarien können sehr unterschiedlich ausfallen. Von dem einfachen Einsatz als zentrales E-Mail-System mit zusätzlichen Workgroup-Funktionen bis hin zu einer Vielzahl an vernetzten Diensten auf unterschiedlich ausgeprägten Domino-Servern, die im Unternehmens-Intranet, diversen Extranets und an der Schnittstelle zum Internet betrieben werden. Diese Dienste können über unterschiedlich ausgeprägte Clients genutzt werden, wobei Notes/Domino sowohl server- wie auch clientseitig als Integrationsplattform genutzt werden kann, z. B. für den Zugriff auf SAP-Systeme. Aus diesem Grund weder Intranet-Architektur noch Internet-Architektur für den Einsatz von Notes/Domino betrachtet, sondern die Absicherung der von der Notes/Domino-Umgebung bereitgestellten Dienste, abhängig vom Einsatzszenario.

**Sicherheitsrelevante Entwicklungen der Lotus Notes/Domino-Plattform**

Die Lotus Notes/Domino-Plattform hat sich mit den aktuellen Releases 8.0.x und 8.5.x sowohl bezüglich ihrer Funktionalität als auch der eingesetzten Technologie stark weiterentwickelt. Dies betrifft die Anzahl und Funktionalität der bereitgestellten Domino-Dienste, die Anzahl und Funktionalität der möglichen Domino-Clients sowie die Einsatzszenarien der Plattform.

Aus Sicherheitssicht sind insbesondere folgende Entwicklungen wichtig, um eine Absicherung der Notes/Domino-Plattform vornehmen zu können:

- Die Bedeutung elektronischer Kommunikation und Zusammenarbeit nimmt immer weiter zu. Durch die Einbindung in fast alle Geschäftsprozesse steigt auch Schutzbedarf der über Lotus Notes implementierten Dienste, wie z. B. E-Mail und Intranet-/Extranet-Zugang. Dies führt in Summe zu einem ansteigenden Schutzbedarf der Lotus Notes/Domino-Plattform.
- Zu neueren Internet-Diensten, wie Presence und Instant Messaging, sind bislang wenig Betrachtungen zu potentiellen Gefährdungen vorhanden

und damit auch ein nicht besonders ausgeprägtes Bewusstsein zu den damit verknüpften IT-Risiken.
- Die Architektur der Plattform befindet sich im Wandel: Von einer reinen Client-Server-Architektur mit Fat Client ausgehend ist die Lotus Notes/Domino-Plattform heute eine dienstbasierte Plattform. Diese beinhaltet unterschiedlich konfigurierbare Serverkomponenten und Dienste, eine komplexe Entwicklungsumgebung und mehrere Clients, die entweder für den gesamten Funktionsumfang der Plattform genutzt werden können oder selektiv für definierte Dienste (wie z. B. POP3 und IMAP-Clients für E-Mail).
- Die stark gestiegene Komplexität der Software durch Anbindung an etablierte Plattformen des Herstellers und Standards (DB2 als DBMS, Eclipse, Websphere-Technologie, W3C-Standards) vergrößert erheblich die Anzahl potentieller Schwachstellen und erschwert den Überblick: Architektur, Schnittstellen und kritische Komponenten sind aus Sicherheitsgesichtspunkten zunehmend schwerer zu bewerten.
- Die durch Einbindung neuer Technologieplattformen entstehende Heterogenität der Codebasis (clientseitig Eclipse, serverseitig Websphere-Technologie, Web 2.0-Standards) verlangt ein breiteres technologisches Know-How bei der Absicherung der Lotus Notes/Domino-Plattform.
- Die umfangreichen Integrationsmöglichkeiten der Notes-Plattform, speziell die Alloy-Komponente zur SAP-Integration, aber auch die anderen Möglichkeiten server- und clientseitiger Integration können bei entsprechender Nutzung den Schutzbedarf einzelner Lotus Notes/Domino-Komponenten (z. B. des Clients bei Umsetzung einer Universal Client Strategie) wesentlich erhöhen.

**Universeller Client**

Obwohl sich vielfach Web-Browser als Anwendungsfrontends durchgesetzt haben, ist für komplexe Anwendungen oftmals noch ein "klassischer" Client vorhanden, der deutlich mehr Funktionalität bieten kann als der "einfache" Web-Browser. Mittels Browser-Plugins oder des Ajax-Frameworks kann zwar die Funktionalität des Browser-basierten Clients erweitert werden, die Absicherung und Wartung der Komponenten wird jedoch erschwert.

Große Anbieter von Software versprechen sich durch das Konzept eines "universellen" Clients zum einen die Vereinfachung bei der Entwicklung klassischer Clients für die angebotenen Anwendungen, zum anderen aber auch die Reduzierung des beim Kunden anfallenden Installations- und Administrationsaufwands.

IBM besitzt mit dem bisherigen, proprietären Notes Client einen breit akzeptierten Client, der die umfangreiche Funktionalität der Lotus Notes/Domino-Plattform erschließt und bei vielen Kunden auch als Client für Eigenentwicklungen unter Lotus Notes/Domino genutzt wird.

Das Eclipse-Framework ist für die Lotus Notes/Domino-Plattform sowohl Entwicklungs-Framework wie auch Runtime-Framework für den Full Client. Das Framework wird von IBM unterstützt und hat als freie Plattform für Java breite Akzeptanz.

Mit der Umstellung des Notes Clients auf die Eclipse-Plattform unter Notes 8 (Standard bzw. Full Client) und der Freigabe der Eclipse-basierten Lotus Notes/Domino-Entwicklungsumgebung Domino Designer hat IBM alle Voraussetzungen geschaffen, um den Notes Client als universellen Client nicht nur für die eigene Produktfamilie, sondern allgemein für Java-basierte Anwendungen zu etablieren.

Die Auswirkungen eines universellen Clients auf die Informationssicherheit können erheblich sein und sind daher im Vorfeld einer Einführung konzeptionell zu betrachten. Folgende Aspekte sind besonders zu berücksichtigen:

- Die Sicherheitsbetrachtung unterschiedlicher Anwendungen vereinfacht sich bei Verwendung eines universellen Clients, da die Sicherheitsmechanismen des Clients nur einmalig bewertet werden müssen.
- Der Schutzbedarf des Clients steigt durch das anzuwendende Maximum- und Kumulationsprinzip für die unterschiedlichen, den Client nutzenden Anwendungen sowohl bei der Verfügbarkeit, Vertraulichkeit wie auch bei der Integrität.
- Die Absicherung kann sich durch die höhere Komplexität des Lotus Notes Clients schwieriger gestalten. Dazu trägt auch bei, dass es sich bei dem Full Client um einen aus einem Entwicklungsrahmenwerk erzeugten Client handelt, der viel offener (und damit angreifbarer) ist als ein reiner, proprietärer Anwendungsclient wie der Basic Client.

**Anwendungsintegration mit Lotus Notes/Domino**

Die Lotus Notes/Domino-Plattform wird seitens des Herstellers zunehmend auch als Plattform für Anwendungsintegration positioniert. Technisch wird dies durch offene Standards für Schnittstellen und die Ergänzung der proprietären Lotus-Technologie durch bewährte Technologie der WebSphere-Plattform und des Eclipse-Rahmenwerks abgebildet.

**Anwendungsintegration über Lotus Notes Clients**

Die erweiterten Möglichkeiten der clientseitigen Anwendungsintegration (z. B. über Web Services) sind ein weiteres Plus für den Full Client und stärken die strategische Position des Lotus Notes Clients als universeller Client. Clientseitige Anwendungsintegration ist oftmals einfacher und schneller zu realisieren als serverseitige Anwendungsintegration, da keine oder geringe Eingriffe in die Betriebsabläufe der zu integrierenden Anwendungen erforderlich sind.

**Anwendungsintegration über den Lotus Domino Server**

Die vorhandenen Möglichkeiten der serverseitigen Integration, z. B. durch die Anbindung von DB2-Datenbanken, über den Domino Application Server oder unter Nutzung des Lotus Enterprise Integrator for Domino (zusätzlich lizenzierbares Produkt der *Lotus Extended Products*), positionieren die Lotus Notes/Domino-Plattform als Alternative zu proprietären Produkten zur Anwendungsintegration.

In Zusammenarbeit mit SAP entwickelte Produkte wie z. B. Alloy ermöglichen den Zugriff auf SAP-Systeme aus dem Lotus Notes Client und stärken damit die Position des Clients als universeller Client, wobei der Domino-Server und der SAP Application Server über entsprechende Plugins kommunizieren.

Analog zum universellen Client steigt auch bei der Nutzung von Lotus Notes/Domino als Plattform zur Anwendungsintegration den Schutzbedarf sowohl der clientseitigen Notes-Komponenten wie auch der entsprechend für Integration genutzten serverseitigen Domino-Komponenten. Die umzusetzenden Sicherheitsmaßnahmen können daher deutlich aufwendiger ausfallen als bei alleiniger Nutzung der Lotus Notes/Domino-Funktionalität und der für die Lotus Notes/Domino-Plattform bereitgestellten Eigenentwicklungen.

# M 3.88 Zielgruppenspezifische Schulungen zu Lotus Notes/ Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Lotus Notes/Domino stellt eine hoch komplexe Plattform dar. Diese stellt, abhängig von der Größe/Komplexität der im Unternehmen bzw. der Behörde vorhandenen Lotus Notes/Domino-Umgebung(en) und dem Umfang der eingesetzten Funktionen/Dienste, entsprechend hohe Anforderungen an die Lotus Notes/Domino-bezogenen Kenntnisse der Verantwortlichen und Benutzer.

Über angemessene zielgruppenspezifische Schulungen ist daher sicherzustellen, dass die Kompetenz zur Architektur und Sicherheitsarchitektur der Plattform, zur angemessenen Konfiguration und zu plattformspezifischen Betriebsthemen wie auch, falls benötigt, zur Anwendungsentwicklung für die Lotus Notes/Domino-Plattform und zur Anwendungsintegration mittels der Lotus Notes/Domino-Plattform vorhanden ist.

Die Zielgruppen für Lotus Notes/Domino-Schulungen mit unterschiedlichen Schwerpunkten sind:

- Führungskräfte (Schulungsinhalt: Überblicksschulung)
- Informationssicherheitsmanagement (Schulungsinhalte: Lotus Notes/Domino-spezifische Sicherheitsarchitektur und Sicherheitsmechanismen)
- Administratoren (Schulungsinhalte: Grundlagen der Lotus Notes/Domino-Architektur, Betrieb, Parametrisierung, Backup/Recovery)
- System- und Softwarearchitekten, Systemintegratoren (Schulungsinhalte: Architekturen im Lotus Notes/Domino-Umfeld und Lotus Notes/Domino-Schnittstellen)
- Entwicklungsleiter, Softwareentwickler (Schulungsinhalte: Lotus Notes/Domino-spezifische Entwicklungswerkzeuge (Designer) und erprobte Anwendungsentwicklungsverfahren im Lotus Notes/Domino-Umfeld sowohl für die proprietäre Notes-Welt wie auch die Eclipse-basierte Weiterentwicklung)
- Lotus Notes/Domino-Benutzer allgemein (Schulungsinhalte: Änderungen in den neuen Lotus Notes Versionen, produktivitätssteigernde Schulungen, Vermittlung von nutzerbezogenen Sicherheitsaspekten)

Prüffragen:

- Wurden Zielgruppen für Lotus Notes/Domino-spezifische Schulungen definiert und entsprechende Schulungen geplant und durchgeführt?

# M 3.89 Schulung zur Administration der Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Damit alle Funktionen und Sicherheitsmerkmale der Protokollierung optimal genutzt werden können, ist es wichtig, die Administratoren entsprechend zu schulen. In den Schulungen sollten Informationen über Einrichtung und Betrieb der Komponenten eines Protokollierungsservers sowie Kenntnisse über die Administration vermittelt werden. Darunter fallen auch herstellerspezifische Aspekte zu einzelnen Produkten, die im Unternehmen für die Protokollierung verwendet werden.

Neben den Aspekten der allgemeinen Betriebssystemsicherheit, wie beispielsweise in B 3.102 *Server unter Unix* oder B 3.108 *Windows Server 2003* beschrieben, sind folgende Punkte von Bedeutung:

- Konfiguration und Installation des Protokollierungsservers
- Grundlagen und Konzepte der Administration
- Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche
- datenschutzrechtliche Aspekte (siehe dazu M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Es können auch Kenntnisse über mögliche Angriffsszenarien vermittelt werden, um eine sorgfältige Analyse der Protokolldateien zu ermöglichen. Zusätzlich bietet es sich an, Grundlagen zum Thema Intrusion Detection/Intrusion Prevention Systeme (IDS/IPS) zu vermitteln. Darüber hinaus sollten in dieser Schulung auch Themen wie die eines zentralen Protokollierungsservers und datenschutzrechtliche Aspekte angesprochen werden (siehe dazu M 2.110 *Datenschutzaspekte bei der Protokollierung*). Für Schulungsmaßnahmen ist bereits bei der Beschaffung von IT-Komponenten ein Budget einzuplanen und ein Schulungskonzept für Administratoren zu erstellen.

Prüffragen:

- Wurde ein Schulungskonzept für die zentrale Protokollierung erstellt?
- Werden die Administratoren ausreichend über Einrichtung und Betrieb der Komponenten eines Protokollierungsservers, auch beim Einsatz eines zentralen Protokollierungsservers, geschult?

# M 3.90 Allgemeine Grundlagen für die zentrale Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die meisten IT-Systeme innerhalb eines Informationsverbundes können so konfiguriert werden, dass sie Protokolldaten über verschiedene Ereignisse wie Dateizugriffe erzeugen. Diese enthalten wichtige Informationen, die dabei helfen können, Hard- und Softwareprobleme sowie Ressourcenengpässe festzustellen und zu lokalisieren. Des Weiteren werden Protokolldaten auch für die Erkennung von Sicherheitsproblemen und Angriffen verwendet. Um einen Gesamtüberblick über einen Informationsverbund zu erhalten, kann ein zentraler Protokollierungsserver eingesetzt werden, der die unterschiedlichen Protokolldaten zusammenführt, diese analysiert und überwacht.

### Aufbau Protokolldateien

Jede Protokolldatei enthält grundsätzlich neben den erfassten Ereignissen immer Datum und Uhrzeit als zentrale Informationen. Je nach protokollerzeugendem System können diese unterschiedlich angeordnet sein. Uhrzeit und Datum sind für eine zentrale Protokollierung besonders wichtig (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*).

### Zentralisierung

Um die Übersicht zu erhöhen und die gesammelten Daten leichter weiter verarbeiten zu können, werden die Protokolldaten aller involvierten Komponenten häufig über einen sicheren Kanal an einen zentralen Server übertragen. Wenn ein zentraler Protokollierungsserver eingesetzt wird, muss er über ausreichend Speicherkapazität verfügen, um die Protokollmeldungen des Informationsverbunds ablegen zu können.

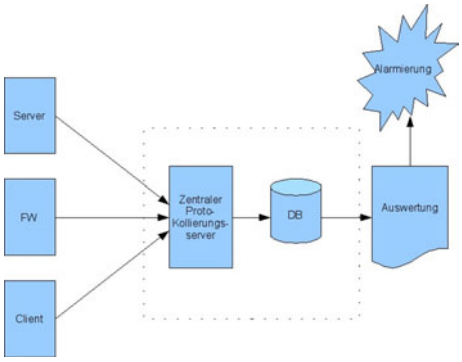



Abbildung: Prinzipieller Aufbau einer zentralen Protokollierung

Zur Übertragung von Status-, Fehler-, Alarm- und sonstigen Meldungen von Servern und Netzkomponenten an den Protokollierungsserver kann beispielsweise syslog verwendet werden. Mit syslog wird einerseits das Protokoll und andererseits auch das Programm bezeichnet, um Ereignismeldungen zu generieren, entgegenzunehmen, weiterzuleiten oder zu speichern. Prinzipiell erfolgt die Übertragung von syslog-Meldungen im Klartext. Erst durch das Tunneling über SSL oder SSH werden die Protokollmeldungen im Netz verschlüsselt übertragen.

Nicht jede einzelne mögliche Protokollierungsmeldung soll gesammelt und später auch ausgewertet werden. Häufig enthalten unterschiedliche Protokolldateien identische Informationen und liefern somit denselben Zusammenhang, der auf ein bestimmtes Ereignis schließen lässt. Deshalb werden redundante Daten zu einem Datensatz zusammengefasst, um die große Menge an Protokollinformationen zu verringern (Aggregation). Die Herausforderung hierbei liegt in der vorher notwendigen Normalisierung der unterschiedlichen Formate, in denen die Protokolldaten zur Verfügung stehen.

**Normalisierung**

Die zusammengefassten, unterschiedlichen Meldungen müssen für die spätere Auswertung in ein einheitliches Format umgewandelt (normalisiert) werden, da es keinen einheitlichen Standard für Format und Übertragungsprotokoll gibt. Durch die Normalisierung können die unterschiedlichen Protokoll-Formate, wie syslog, Microsoft Eventlog, SNMP, Netflow oder IPFIX aneinander angepasst und anschließend ausgewertet werden. Eine Normalisierung lässt sich mithilfe eines einfachen Skripts oder mit komplexen Applikationen durchführen.

**Aggregation**

Der nächste Schritt zur Vorverarbeitung ist die Aggregation. Hier werden Protokollmeldungen mit identischem Inhalt zu einem Datensatz zusammengefasst. Oft werden vom gleichen System mehrmals hintereinander identische Protokollmeldungen erzeugt, was einen geringeren Informationswert für die nachfolgenden Meldungen bedeutet. Aus diesem Grund wird nur die erste Protokolldatei weiterverarbeitet. Allerdings ist es wichtig, die erste Protokollmeldung um die Anzahl der aufgetretenen redundanten Ereignisse zu ergänzen, um die Häufigkeit der identischen Protokollmeldungen feststellen zu können.

**Filterung**

Neben Normalisierung und Aggregation wird für eine sinnvolle zentrale Protokollierung auch eine Filter-Funktion benötigt. Durch eine Filterung können je nach Einsatzzweck irrelevante Daten möglichst frühzeitig ausgesondert und somit vom weiteren Verarbeitungsprozess ausgeschlossen werden. In erster Linie sind die Protokolldaten der sicherheitsrelevanten IT-Systeme interessant. Die Anwendungsprotokolldaten, die dazu dienen, eine ordnungsgemäße Benutzung der jeweiligen Anwendungen zu überwachen, werden erst danach betrachtet. Aus Sicht der Verfügbarkeit sind hingegen regelmäßig abgefragte Monitoring-Informationen über den Betrieb der Systeme relevant. Dazu gehören die Erreichbarkeit der Systeme über das Netz oder Fehlermeldungen aus den Betriebssystemen, die auf Probleme hindeuten.

**Auswertung**

Das Ziel der Protokolldatenauswertung ist es, Probleme beim IT-Betrieb und Angriffe auf ein IT-System möglichst schnell erkennen zu können. Dafür müssen die Komponenten in Echtzeit überwacht werden. Die Analyse zeigt neben Sicherheitsereignissen und Fehlern auch Informationen über die aktuelle Auslastung auf. Bei der Auswertung von Protokolldaten ist auf eine aussagekräftige Darstellung der Ergebnisse in einer leistungsfähigen Benutzeroberfläche und auf die Unterstützung bei der Erstellung von Berichten zu achten. Ereignisse werden bei den meisten Systemen automatisiert aufgefunden, allerdings sollte eine Aussage darüber, ob ein realer Angriff vorliegt, durch einen Administrator bestätigt werden. Für diese Aufgabe müssen die Administratoren aus-

reichend geschult sein und durch sinnvolle Analysesysteme unterstützt werden.

**Alarmierung**

Gesammelte Protokolldaten können ein IT-Frühwarnsystem bei der Aufgabe unterstützen, bestehende Arbeitsabläufe und Datenflüsse zu überwachen und eine Schnittstelle für die Alarmierung bereitzuhalten. Die Alarmierung von wichtigen Ereignissen sollte über verschiedene Arten der Benachrichtigung wie E-Mail oder SMS erfolgen können. Um eine sinnvolle Alarmierung durchführen zu können, ist es wichtig, die Anzahl der Fehlalarme zu reduzieren. Ein wichtiger Aspekt hierbei ist, dass die Schwellwerte realistisch eingestellt und an die Gegebenheiten des Informationsverbundes angepasst werden.

**Archivierung**

Wenn Protokolldaten dauerhaft gespeichert werden sollen, muss geprüft werden, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen dafür gelten. Um die Nachvollziehbarkeit von Aktionen zu gewährleisten, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch eine Löschungspflicht geben (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

# M 3.91 Schulung der Administratoren von Cloud-Infrastrukturen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Cloud-Administratoren müssen für ihre Aufgaben geschult werden. Dies muss vor der Aufnahme ihrer Tätigkeit geschehen, und wegen der kurzen Innovations- und Updatezyklen beim Cloud Computing regelmäßig wiederholt werden.

In den Schulungen muss vermittelt werden, wie die Cloud-Administratoren ihre Aufgaben erfüllen können. Hier ist eine mögliche Spezialisierung zu berücksichtigen, wenn die Administration fachlich auf verschiedene Rollen verteilt wird und der Administrator nur für Teilbereiche der Cloud zuständig ist.

Die wesentliche Aufgabe der Cloud-Administratoren ist es, mithilfe der Cloud-Verwaltungslösung die unterschiedlichen Komponenten der Cloud-Infrastruktur zu verwalten. Das heißt, dass ein Cloud-Administrator im Produktivbetrieb die automatisierte Zuteilung virtueller Ressourcen einrichtet, überwacht und gegebenenfalls zusätzliche physische Ressourcen in die Cloud einbindet. Schulungen müssen somit vermitteln, wie die Cloud-Infrastruktur effektiv und effizient verwaltet werden kann. Dies lässt sich mit herstellerspezifischen Schulungen am besten erreichen. Neben der reinen Kenntnis der eingesetzten Cloud-Verwaltungslösungen müssen die Cloud-Administratoren auch in den Prozessen und Abläufen des Cloud-Diensteanbieters geschult werden.

In den Schulungen müssen folgende zentrale Aspekte der Cloud-Administration abgedeckt werden:

- Kenntnis der relevanten eingesetzten Techniken, Komponenten und Funktionen.
- Die verschiedenen technischen Ebenen (Anwendungen, IT-Systeme, Netze und Speichersysteme) der Cloud-Infrastruktur.
- Der Umgang mit verschiedenen Cloud-Mandanten - gemeinsame Konfigurationseinstellungen einerseits und erforderliche Trennung andererseits.
- Provisionierung und De-Provisionierung von Cloud-Ressourcen.

In den Schulungen sollten weitere Aspekte der Cloud-Administration abgedeckt werden:

- Automatisierung von Vorgängen oder Abläufen, insbesondere der Provisionierung und De-Provisionierung.
- Erstellung, Verwaltung und Vervielfältigung von Cloud-Diensteprofilen.
- Schnittstellen zu Virtualisierung, Netzwerkmanagement und Speichersystemen.
- Erkennung der Auswirkungen von Konfigurationsänderungen, Vorbeugung von Fehlern.
- Fehlerbehebung in der Cloud-Infrastruktur.
- Optimale Nutzung von Sicherheitsmerkmalen und technischen Funktionen.

Prüffragen:

- Wie wird sichergestellt, dass die Cloud-Administratoren die Bedienung der Cloud-Verwaltungswerkzeuge umfassend beherrschen?
- Werden die Cloud-Administratoren hinsichtlich der definierten Prozessabläufe zur Administration der Cloud-Infrastruktur geschult?

# M 3.92 Grundlegende Begriffe beim Einsatz von Speicherlösungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die Geschäftsprozesse in Institutionen sind heutzutage größtenteils von Informationstechnik durchdrungen. Wichtige Informationen wie beispielsweise Kommunikationsdaten, Verträge, Werbematerialien oder Konstruktionspläne liegen in vielen Fällen ausschließlich in digitaler Form vor. Für Unternehmen und Behörden sind diese Daten von großer Bedeutung. Entsprechend sind die Anforderungen, die Institutionen an ihre Speicherlösung stellen, in der Vergangenheit stetig gestiegen. Gleichzeitig erweitern neue Entwicklungen im Speicherumfeld die möglichen Einsatzszenarien, bringen aber gleichzeitig neue Gefährdungen mit sich. Der sorgfältigen Planung kommt daher im Zusammenhang mit dem Einsatz von Speicherlösungen eine wachsende Bedeutung zu.

Voraussetzung für eine erfolgreiche Planung ist unter anderem das gemeinsame Verständnis aller Verantwortlichen über grundlegende Begriffe, wie sie beim Einsatz von Speicherlösungen benötigt werden. Nachfolgend finden sich daher Ausführungen zu Begriffen aus dem Speicherumfeld, die alle relevanten Aspekte abdecken.

### Speicherlösung

Eine Speicherlösung besteht aus einem oder mehreren Speichernetzen sowie einem oder mehreren Speichersystemen. Der Begriff Speicherlösung beschreibt somit die Gesamtheit aller Komponenten, die zum Speichern von Daten und deren Bereitstellung für die zugreifenden Systeme erforderlich sind.

### Speichersystem

Die zentrale Instanz, die für andere Systeme Speicherplatz zur Verfügung stellt, wird als Speichersystem bezeichnet. Der Einsatz eines Speichersystems erlaubt den zeitgleichen Zugriff mehrerer Systeme (z. B. virtuelle und physische Server, Clients, Appliances) auf den vorhandenen Speicherplatz. Ein Speichersystem besteht aus mehreren Komponenten, die in der Folge näher beschrieben sind.

### Speichermedien

Ein Speichersystem beinhaltet ein oder mehrere Speichermedien, die das Speichern und spätere Abrufen von Daten ermöglichen. Speichermedien können dabei beispielsweise in elektronische Speichermedien (z. B. Flash-Speicher), magnetische Speichermedien (z. B. Festplatten oder Magnetbänder) oder optische Speichermedien (z. B. optische Bänder) unterteilt werden.

### Speichergehäuse

Im Regelfall sind Speichermedien in einem separaten Speichergehäuse untergebracht. Bei kleineren Speichersystemen können die Speichermedien allerdings auch zusammen mit den Speicher-Controllern oder NAS-Controllern in einem gemeinsamen Gehäuse verbaut sein.

**Speicher-Controller**

Ein Speichersystem kann mit einem oder mehreren redundant ausgelegten Speicher-Controllern ausgestattet sein. Ein Speicher-Controller besteht dabei in der Regel aus folgenden Komponenten:

- Frontend-Ports (Fibre Channel + Ethernet)
- Speicherprozessor(en) und dazugehöriger RAM
- Speicher-Cache
- Backend-Ports zu den Speichergehäusen (SAS, FC)

Der Speicher-Controller ermöglicht die Konfiguration des Speichersystems und stellt somit eine zentrale Komponente innerhalb des Speichersystems dar. Aufgabe des Speicher-Controllers ist darüber hinaus die Bereitstellung der konfigurierten Speichermedien für das Speichernetz.

**NAS-Controller**

Ein Speichersystem kann mit einem oder mehreren redundant ausgelegten NAS-Controllern ausgestattet sein. Der NAS-Controller ermöglicht unter Verwendung von NFS (Network File System) oder CIFS (Common Internet File System) Zugriff auf die Speichersysteme. Der Hauptanwendungsfall besteht darin, Fileserverdienste zur Verfügung zu stellen. Der NAS-Controller kann einerseits am Speicher-Controller angeschlossen sein, andererseits aber auch zusammen mit dem Speicher-Controller in einem Gehäuse untergebracht sein.

**Mögliche Zugriffsmethoden auf Speichersysteme**

Speichersysteme lassen sich hinsichtlich ihrer Zugriffsmethoden unterscheiden. Nachfolgend sind gängige Varianten von Speichersystemen dargestellt.

- Blockbasierende Speichersysteme: Der Zugriff auf das Speichersystem erfolgt ausschließlich blockbasiert. Es wird kein NAS-Controller eingesetzt.
- Filebasierende Speichersysteme: Der Zugriff auf das Speichersystem erfolgt ausschließlich filebasiert. Es wird ein NAS-Controller eingesetzt.
- Unified Speichersysteme (file- und blockbasierend): Der Zugriff auf das Speichersystem erfolgt sowohl block- als auch filebasiert.

**Speichernetz**

Speichernetze ermöglichen einerseits den Zugriff auf die Speichersysteme, anderseits die Replikation von Daten zwischen Speichersystemen. Innerhalb eines Speichernetzes kommen unterschiedliche Protokolle zum Einsatz. Darüber hinaus existieren, insbesondere bei blockbasiertem Zugriff, spezielle Netzkomponenten, die ein Speichernetz um spezifische Funktionen erweitern.

**Protokolle**

Der Zugriff auf Speichersysteme erfolgt mithilfe von Speichernetzen. Grundsätzlich ist hierbei, wie bereits bei den Speichersystemen, zwischen IP-basiertem Filezugriff (z. B. CIFS), IP-basiertem Blockzugriff (z. B. iSCSI) und rein blockbasiertem Zugriff (z. B. FC) zu unterscheiden. In Abhängigkeit der Zugriffsform kommen jeweils unterschiedliche Protokolle zum Einsatz.

Bei einem IP-basierten Zugriff stehen folgende Protokolle zur Verfügung:

- NFS (Network File System)
- CIFS (Common Internet File System), eine Erweiterung von SMB (Server Message Block)

- HTTP (Hypertext Transfer Protocol)
- WebDav (Web-based Distributed Authoring and Versioning)
- REST (Representational State Transfer), ist eng mit HTTP verknüpft
- SOAP (Simple Object Access Protocol)

Bei einem blockbasierten Zugriff stehen folgende Protokolle zur Verfügung:

- FC (Fibre Channel)
- FCoE (Fibre Channel over Ethernet)
- iSCSI (internet Small Computer System Interface)

Kommt iSCSI zum Einsatz, sollte hierfür ein separates Netz zur Verfügung gestellt werden. Damit liegt in der Folge eine Trennung hinsichtlich des Administrationsnetzes, des Produktionsnetzes für Anwendungen und Anwender sowie des iSCSI-Netzes vor. Dieses Vorgehen hat sich in der Praxis als Best Practice bewährt. Im Fehlerfall kann bei separaten Netzen die Ursache schneller und einfacher gefunden bzw. behoben werden, zudem wirken sich Störungen lediglich auf ein Netz aus und nicht gleichzeitig auf alle Anwendungen.

Beim Ablegen von Objekten in einer Cloud wird häufig Objekt-Storage (oftmals auch als "Object-based Storage" bezeichnet) eingesetzt. Objekt-Storage ermöglicht gegenüber den traditionellen blockbasierten und IP-basierten Zugriffsmethoden einen objektbasierten Zugriff. Dieser erfolgt direkt per IP oder per API und deren Kommandos über eine führende Anwendung.

**FC-SAN-Switches**

FC-SAN-Switches stellen bei einem FC-blockbasierten Zugriff für die zugreifenden Server die Verbindungsstelle ins Speichernetz dar. Sie ermöglichen in der Folge den gleichzeitigen Zugriff mehrerer Server auf die Speichersysteme.

Derzeit existieren folgende relevante Switch-Technologien:

- FC-SAN-Switches, die FC als einziges Protokoll nutzen
- Unified-Fabric-Switches, die, je nach Konfiguration und Bestückung, gleichzeitig als LAN-, FC- und FCoE-Switch dienen

**Replikation**

Unter Replikation ist die mehrfache Speicherung der Daten eines Speichersystems und die Synchronisation dieser Datenquellen zu verstehen. Eine Replikation kann dabei innerhalb eines Brandabschnitts, über Brandabschnitte hinweg und sogar bis über die Grenzen von Rechenzentren oder Ländern hinaus erfolgen. In der Praxis sind zwei Replikationsarten zu unterscheiden.

Die **synchrone Replikation** ermöglicht eine voll redundante Datenhaltung, bei der die Daten eines Speichersystems in Echtzeit auf ein entferntes System gespiegelt werden. Dabei wird sichergestellt, dass die Daten an den Standorten stets synchron gehalten werden. Von synchroner Replikation ist die Rede, wenn eine Änderungsoperation an einem Datenobjekt nur dann erfolgreich abgeschlossen werden kann, wenn sie auch auf den Replikaten durchgeführt wurde (Quittierung).

Der Vorteil einer synchronen Replikation ist, dass die beiden Datenblöcke jederzeit vollständig synchronisiert sind. Ein zuverlässiges Netz und vor allem niedrige Latenzzeiten sind die Voraussetzung für eine synchrone Replikation. Dies bedeutet, dass die Übertragungsreichweite beim Einsatz dieser Technologie begrenzt ist. Die Begrenzung ergibt sich hierbei entweder durch Spezifikationen der Hersteller oder basiert auf einer maximalen herstellerspezifischen Latenzzeit.

Bis zu einer Entfernung von 10 km stellt eine synchrone Datenspiegelung ohne Einsatz zusätzlicher Maßnahmen in der Regel kein Problem dar. Bei Entfernungen, die 10 km überschreiten, ist ein besonderes Augenmerk auf die Qualität der Datenverbindung zu legen. Bei Glasfaserverbindungen über 10 km sind in den Fibre-Channel-Switchen anstelle der Short-Wave-Port-Module Long-Wave-Port-Module zu verwenden. Bei der Kopplung von Rechenzentren mit Entfernungen über 10 km werden auch Technologien wie DWDM (Dense Wavelength Division Multiplexing) oder CWDM (Coarse Wavelength Division Multiplexing) eingesetzt. Hier ist die absolute Latenz der Verbindungsstrecke ausschlaggebend dafür, ob eine synchrone Spiegelung realisiert werden kann.

Im Gegensatz zur synchronen Replikation werden die Daten bei einer **asynchronen Replikation** nicht in Echtzeit, sondern zeitlich versetzt repliziert. Asynchrone Replikationen werden häufig bei IP-Anbindungen zwischen den Standorten eingesetzt. Die Übertragungsreichweite kann sich in diesem Fall auch über Kontinente hinweg erstrecken.

**Speichervirtualisierung**

Mit dem Einsatz von Speichervirtualisierung wird dem Speichernetz eine neue virtuelle Schicht hinzugefügt, welche die Speicherbereitstellung von den physischen Gegebenheiten abkoppelt. Der Einsatz von Speichervirtualisierung bietet einer Institution eine Reihe von Mehrwerten:

- Erhöhte Flexibilität bei Aufbau, Planung und Erweiterung einer Speicherlösung
- Vereinheitlichung des Speichermanagements
- Unabhängigkeit bei der Auswahl der Speichersysteme

In der Praxis häufig anzutreffende Ausprägungen von Speicherlösungen

**Network Attached Storage (NAS)**

Network-Attached-Storage-Systeme bestehen in der Regel aus mindestens einem NAS-Controller und einem oder mehreren Speichergehäusen. Der Hauptanwendungsfall eines NAS besteht darin, den angeschlossenen Servern über ein IP-Netz Fileserverdienste zur Verfügung zu stellen. Viele Anbieter verwenden deshalb den Begriff "Filer" für solche Systeme.

**Storage Area Network (SAN)**

Storage Area Networks werden in der Regel durch ein dediziertes Speichernetz zwischen Speichersystemen und angeschlossenen Servern oder Endgeräten geschaffen. SANs wurden für die serielle, sehr schnelle und kontinuierliche Übertragung großer Datenmengen konzipiert. Sie basieren heute für hochverfügbare, hochperformante Installationen auf der Implementierung des Fibre-Channel- oder IP-Protokolls.

**Hybrid-Storage oder Unified Storage**

Eine Speicherlösung, die eine Mischform zwischen NAS und SAN darstellt, wird oftmals unter der Bezeichnung "Hybrid-Storage" oder kombinierte Speicherlösung (Unified Storage) geführt. Nach außen können sie jedoch sowohl als NAS als auch als SAN betrieben werden. Dieser Mischbetrieb wird durch den Einsatz entsprechender Systemkomponenten und eine entsprechende Konfiguration ermöglicht.

So kann sich ein Speichersystem sowohl für einige Anwendungen per Ethernet-Anschluss als "Filer" präsentieren und somit Fileservices über CIFS und

NFS zur Verfügung stellen als auch für andere Server Speicherkapazität per Fibre Channel oder iSCSI zugänglich machen.

**Objekt-Storage**

Objekt-Storage (oftmals auch als "Object-based Storage" bezeichnet) ermöglicht gegenüber den traditionellen blockbasierten und filebasierten Zugriffsmethoden einen objektbasierten Zugriff.

Objektbasierte Speicherlösungen speichern Daten in Verbindung mit den zugehörigen Metadaten auf einem Datenträger in Form von Objekten und nicht in Form von Dateien. Mittels der Vergabe einer eindeutigen Objekt-ID (Hash-Wert), die in den Metadaten des Objekts festgehalten wird, kann das Objekt eindeutig identifiziert werden. Der Zugriff auf einen objektbasierten Speicher erfolgt über eine führende Anwendung. Die Anwendung greift hierbei über eine spezielle API (IP) und deren mögliche Kommandos oder direkt per IP auf den Objekt-Storage zu. Im Falle eines Zugriffs per API muss die führende Applikation die herstellerspezifische API des Objekt-Storage unterstützen. Objekt-Storage wird vor allem im Bereich Archivierung, Dokumentenmanagement und beim Ablegen von Objekten in einer Cloud eingesetzt.

**Cloud Storage**

Im Zusammenhang mit Weiterentwicklungen im Speicherumfeld etabliert sich zunehmend auch der Begriff des Cloud Storage. Hierunter ist Speicher für die Cloud-Nutzung zu verstehen. Die Speicherlösung an sich bleibt dabei weitgehend unverändert, jedoch liegt eine von den klassischen SAN- oder NAS-Architekturen abweichende Art des Zugriffs auf die gespeicherten Daten vor. Dieser wird in der Regel mittels Web-Service-Schnittstelle (via REST und SOAP) realisiert.

Eine besondere Herausforderung im Zusammenhang mit Cloud-Storage ist die Mandantenfähigkeit der Gesamtlösung.

# M 3.93 Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Wird für eine Institution ein Sensibilisierungs- und Schulungsprogramm erstellt, sind im Konzept die jeweiligen Zielgruppen zu definieren (siehe auch M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit*). Dazu sollte eine detaillierte Zielgruppenanalyse durchgeführt werden, sodass Maßnahmen auf spezielle Anforderungen und unterschiedliche Hintergründe fokussiert werden können.

Es können beispielsweise Mitarbeiter mit vergleichbaren fachlichen Hintergründen, Kenntnissen oder Aufgaben zu einer Zielgruppe zusammengeführt werden. Ein praktikabler Ansatz ist auch die Zielgruppen aus den organisatorischen Einheiten abzuleiten. In der Regel kann hier davon ausgegangen werden, dass Mitarbeiter mit vergleichbarer Technik und ähnlichen Vorgaben arbeiten.

Ein weiteres Kriterium sind Ereignisse, die innerhalb einer Mitarbeiterlaufbahn eintreten. Hierzu zählen z. B. Neueinstellung, Aufgaben- oder Abteilungswechsel, Standortwechsel, Technikwechsel, Änderungen in der bestehenden Organisation oder der Weggang aus der Institution.

Beispiele möglicher Zielgruppen und deren Merkmale:

**Managementebene**

Die Mitglieder der Managementebene haben eine Vorbildfunktion für die Mitarbeiter. Allerdings haben sie auch oft wenig Zeit, sodass die Sensibilisierung- und Schulungsmaßnahmen strukturiert und prägnant sein müssen.

**Mitarbeiter**

Das Verhalten dieser Zielgruppe im Arbeitsalltag hat die stärksten direkten Auswirkungen auf die Informationssicherheit innerhalb der Institution. Hier ist zu berücksichtigen, dass der Wissensstand innerhalb der Zielgruppe sehr unterschiedlich sein kann. Beispielsweise haben Software-Entwickler eine andere IT-Ausstattung und andere Aufgaben und Kenntnisse als Mitarbeiter der Personalverwaltung. Die beiden Gruppen benötigen daher unterschiedliche Schulungsinhalte zum Thema Informationssicherheit.

**Administratoren**

Administratoren und Support-Mitarbeiter müssen tief gehende Fachkenntnisse der von ihnen betreuten IT-Systeme und Anwendungen haben, sodass sie auch in der Lage sind, Sicherheitsprobleme zu erkennen und zu beheben sowie diesen vorzubeugen.

**Personalabteilung**

Mitarbeiter dieser Abteilung haben einen hohen Informationsbedarf über Datenschutzanforderungen.

**Externe Projektmitarbeiter**

In vielen Fällen haben auch Externe, die eng mit oder sogar in der Institution tätig sind, Zugriff auf interne Informationen, Anwendungen oder Systeme. Diese Zielgruppe muss die Informationssicherheitsziele und -regeln der Institution ebenso unterstützen und darauf verpflichtet werden wie interne Mitarbeiter. Dies erfordert entsprechende Schulungsmaßnahmen, z. B. in Form von Einweisungen mit dokumentierter Kenntnisnahme. Diese Maßnahmen sollte die externe Institution entsprechend den mit der eigenen Institution vereinbarten Anforderungen durchführen.

**Neueinstellungen**

Diese Zielgruppe hatte bisher keine Berührung mit der organisationsinternen Informationssicherheit.

Prüffragen:

- Ist der Bedarf an Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zielgruppenorientiert bestimmt?

# M 3.94 Messung und Auswertung des Lernerfolgs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Personalabteilung
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Die Lernerfolge im Bereich Informationssicherheit sollten zielgruppenbezogen gemessen und ausgewertet werden, um festzustellen, inwieweit die in den Sensibilisierungs- und Schulungsprogrammen beschriebenen Ziele erreicht sind (siehe M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit* und M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit*). Dadurch ist es möglich, ein detailliertes Gesamtbild zu erhalten und so punktuelle Korrekturmaßnahmen durchzuführen, wenn einzelne Ziele nicht erreicht wurden.

Die Personalabteilung verfügt oft über gute Erfahrungen in der Auswertung von Schulungsmaßnahmen. Daher ist es empfehlenswert, sich an dieser Vorgehensweise zu orientieren und sich dafür mit der Personalabteilung abzustimmen.

Um den Lernerfolg zu testen, können die folgenden Möglichkeiten genutzt werden:

**Dokumentation durchgeführter Sensibilisierungs- oder Schulungsmaßnahmen**

Die Dokumentation aller Maßnahmen inklusive einer Kurzbeschreibung der Inhalte und der Durchführungszyklen geben einen ersten Überblick über den Umfang und die betroffenen Zielgruppen der durchgeführten Aktivitäten.

**Dokumentation der Teilnehmerzahlen an Sensibilisierungs- oder Schulungsmaßnahmen**

Die Dokumentation der Teilnehmerzahlen von Schulungen oder die Anzahl der von Sensibilisierungsmaßnahmen erreichten Mitarbeiter pro Abteilung, Bereich, Standort, etc. liefern einen Hinweis auf die erzielte Durchdringung der Maßnahmen in der Institution.

**Anzahl der Anfragen an Ansprechpartner in Sicherheitsfragen** (siehe M 3.46 *Ansprechpartner zu Sicherheitsfragen*)

Wenn nach Schulungs- oder Sensibilisierungsmaßnahmen die Anzahl der Kontakte zu den Ansprechpartnern in Sicherheitsfragen steigt, kann das als Indiz für eine stärkere Sensibilität der Mitarbeiter gewertet werden, aber auch als Folge des gestiegenen Bekanntheitsgrades der Einrichtung.

**Schulungsbewertungen**

Einen ersten qualitativen Überblick über die Schulungserfolge geben standardisierte Schulungsbewertungsbögen, wie sie üblicherweise am Ende einer Veranstaltung durch die Teilnehmer ausgefüllt werden. Neben Fragen zum Ablauf, der Veranstaltungsorganisation oder der Vorgehensweise des Referenten können hier Fragen zur Nutzenbewertung durch die Teilnehmer eingearbeitet werden.

**Test zum Schulungsabschluss**

Während oder nach einer Schulungsveranstaltung durchgeführte Wissenstests sind in der Praxis erprobte Methoden zur Lernerfolgskontrolle. Angepasst auf die jeweiligen Veranstaltungsinhalte können dabei Fragen nach erlerntem Wissen, aber auch Fragen zur Einschätzung beschriebener Situationen die Grundlage bilden.

**Wissenstest in zeitlichem Abstand**

Um den Verlauf von Lernkurven nach Schulungsveranstaltungen zu ermitteln, können nach dem Ende einer Schulung zu festgelegten Zeitpunkten weitere Tests durchgeführt werden. Da hier ein direkter Bezug zur Veranstaltung fehlt, kann es schwierig sein, die Teilnehmer dazu zu motivieren, Wissensfragen zu beantworten. Um dem entgegenzuwirken, kann dieser Test auch in Quiz-Form durchgeführt werden, z. B. mit Preisen für die Teilnehmer.

**Mitarbeiterbefragungen**

Durch Mitarbeiterinterviews mit standardisierten Fragebögen können Informationen darüber gesammelt werden, ob auch nicht-schulische Sensibilisierungsmaßnahmen wirksam sind.

**Anzahl von Regelverstößen**

Eine weitere Variante zu bewerten, ob eine Maßnahme erfolgreich war, ist, die Anzahl von Regelverstößen vor und nach den Sensibilisierungsmaßnahmen zu zählen. Dazu können Verantwortliche auch bewusst und kontrolliert Sicherheitslücken platzieren und dann beobachten, wie Mitarbeiter damit umgehen. Hierzu eignen sich beispielsweise:

- Fremdpersonen ohne Mitarbeiterausweis, die unbegleitet in der Institution herumlaufen,
- DVDs, CDs oder USB-Sticks, die an verschiedenen Stellen in der Institution ausliegen,
- E-Mails, die mit Anhang oder Links auf unbekannte Webseiten, aber mit vertraut klingenden Absenderadressen an die Mitarbeiter versendet werden oder
- Türschließfunktionen, die blockiert werden.

Wichtig ist hierbei, die Ergebnisse nie als Fehlverhalten einzelner Mitarbeiter zu deuten, sondern als Ergebnisse von Gruppen.

**Social-Penetration-Tests / Social-Engineering-Audits**

Um einen Lernerfolg im Rahmen der Social-Engineering-Vorbeugung zu prüfen, empfiehlt es sich, Social-Penetration-Tests bzw. Social-Engineering-Audits durchzuführen. Hierbei wird in der Rolle eines externen Angreifers versucht, Fehlverhalten von Mitarbeitern auszunutzen und Informationen zu erlangen, mit deren Hilfe der Tester zu den vorgesehenen Angriffszielen kommt.

Diese Art von Audits sind jedoch immer umstritten, da Mitarbeiter, die ohne ihr Wissen als Angriffsziel ausgewählt wurden, die Auswertung nach einem erfolgreichen Angriff als Vertrauensbruch oder Bloßstellung ansehen könnten. Auf der anderen Seite liefern solche Audits gute Einblicke, inwieweit Informationssicherheit wirklich gelebt wird. Daher ist der Einsatz dieser Methode im Einzelfall zu prüfen und gemeinsam mit der Personalvertretung und dem Management abzuwägen.

**Praktische Übungen**

Als Alternative zu den beschriebenen Social-Penetration-Tests können auch praktische Übungen eingesetzt werden. Hier sind unterschiedliche Varianten möglich, die einen Überblick über das Sensibilisierungs- und Schulungsniveau geben. Im Nachgang zu Schulungen können Übungssequenzen aufgebaut werden, in denen Situationen spielerisch dargestellt sind, zum Beispiel ein Social-Engineering-Angriff. Die Aufgabe für freiwillige Teilnehmer aus der Gruppe würde darin bestehen, auf diesen Angriff zu reagieren. Eine anonyme Bewertung der Übung durch den Seminarleiter gibt Aufschluss über den Lernerfolg vorangegangener Maßnahmen.

**Tools und Spiele**

Lernspiele oder -tools jeglicher Art bieten in den meisten Fällen ebenfalls die Möglichkeit, Spielergebnisse oder Ergebnisentwicklungen auszuwerten.

Prüffragen:

- Wird der Lernerfolg von Sensibilisierungs- und Schulungsprogrammen quantitativ und qualitativ überprüft?

# M 3.95 Lernstoffsicherung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Vorgesetzte

Bei der Konzeption von Sensibilisierungs- und Schulungsprogrammen zur Informationssicherheit ist die Lernstoffsicherung besonders wichtig, da nur dauerhaft präsentes Wissen auch zu den gewünschten Verhaltensänderungen führt. Nach Sensibilisierungs- und Schulungsaktivitäten sind die Teilnehmer in der Regel mit viel neuem Wissen und neuen Fertigkeiten ausgestattet. Wenn sie dieses Wissen im Anschluss an die Veranstaltungen nicht abrufen oder anwenden, besteht die Gefahr, dass sie es wieder ganz oder teilweise vergessen. Damit sich das Bewusstsein für Informationssicherheit bei den Mitarbeitern dauerhaft verbessert, sollten die Inhalte von Sensibilisierungs- und Schulungsmaßnahmen regelmäßig wiederholt bzw. angewendet werden. Dies wird durch die Lernstoffsicherung unterstützt, die sowohl während der Schulung, am Ende einer Schulung als auch im Zeitraum danach durchzuführen ist.

Die Auswahl von Maßnahmen zur Lernstoffsicherung ist auf die jeweilige Organisationskultur und -größe abzustimmen.

Beispiele für Maßnahmen zur Lernstoffsicherung sind:

- schriftliche oder mündliche Tests während der Schulung oder/und zum Abschluss,
- Quizfragebögen mit Gewinnmöglichkeiten zu Schulungsinhalten,
- Intranet-basierte Befragungen zu den Inhalten der durchgeführten Schulungen,
- Nutzung von Teambesprechungen etc. für die Diskussion aktueller Aspekte der Informationssicherheit,
- Durchführung von Plan- oder Rollenspielen (siehe M 3.47 *Durchführung von Planspielen zur Informationssicherheit*),
- regelmäßige Wiederholung von Seminaren,
- kurze Hinweise im Intranet,
- ergänzende Kurzvorträge, z. B. im Rahmen anderer interner Veranstaltungen.

Prüffragen:

- Werden Maßnahmen zur Lernstoffsicherung in der Institution durchgeführt?

# M 3.96 Unterstützung des Managements für Sensibilisierung und Schulung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um Informationssicherheit erfolgreich in einer Institution zu etablieren, sind sensibilisierte und geschulte Mitarbeiter unabdingbar. Ein auf den Bedarf der Institution zugeschnittenes und angemessen ausgestattetes Sensibilisierungs- und Schulungsprogramm ist daher ein wesentlicher Erfolgsfaktor, um die Leitlinien und Maßnahmen zur Informationssicherheit nachhaltig in der Institution zu etablieren und ihre Wirksamkeit zu gewährleisten. Um es umzusetzen, muss das Management selbst sensibilisiert sein (siehe M 3.44 *Sensibilisierung des Managements für Informationssicherheit*) und das Programm im gesamten Lebenszyklus durch geeignete Maßnahmen aktiv unterstützen:

**Initiierung**

Bevor ein Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erarbeitet wird, ist ein expliziter Auftrag des Managements sinnvoll. Dieser ist innerhalb der Institution zu kommunizieren. Dadurch werden die Verantwortlichen für ihre Aufgabe legitimiert und sichtbar unterstützt. Zusätzlich nehmen so die Mitarbeiter das Thema und seine Bedeutung wahr.

**Planung**

Das Ergebnis der Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit sollte dem Management vorgelegt und von diesem verabschiedet werden. Durch einen konkreten Auftrag zur Umsetzung des Programms kann das Management seine weitere Unterstützung signalisieren und die erforderlichen Ressourcen bereitstellen.

**Umsetzung und Etablierung**

Während die konzipierten Programme in der Institution eingeführt und etabliert werden, muss sich das Management sichtbar engagieren, da hierdurch die gewünschte positive Aufnahme durch die Mitarbeiter stark beeinflusst wird. Führungskräfte sollten sich aktiv an Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit beteiligen, z. B. durch

- eigene Beiträge in Medien der Institution,
- Moderation von speziellen Veranstaltungen,
- vorbildliche Verhaltensweisen,
- Bereitstellung ausreichender Ressourcen für ihre Mitarbeiter.

So unterstreichen sie, wie wichtig die Maßnahmen für ihren eigenen Bereich sind. Zudem wird das Thema für die Mitarbeiter nachvollziehbar und glaubwürdig. Sie erkennen und akzeptieren, dass eine angemessene Informationssicherheit mehr und mehr zum notwendigen und selbstverständlichen Teil ihres Arbeitsalltages wird.

**Erfolgskontrolle und Aktualisierung**

Es sollte regelmäßig überprüft werden, ob die etablierten Sensibilisierungs- und Schulungsmaßnahmen noch wirksam sind. Je nach Ergebnis sind die

Maßnahmen entsprechend anzupassen. Das muss auch geschehen, wenn sich die Rahmenbedingungen in der Institution verändert haben (siehe dazu auch M 3.83 *Analyse sicherheitsrelevanter personeller Faktoren*, M 3.94 *Messung und Auswertung des Lernerfolgs* und M 3.95 *Lernstoffsicherung*).

Hierzu kann das Management wertvolle Beiträge leisten, z. B.:

- Es kann die oft schwierigen Abstimmungen eines Verfahrens zur Messung und Auswertung des Lernerfolgs zwischen verschiedenen Interessengruppen moderieren.
- Es kann dafür sorgen, dass über Informationssicherheit offen und vertrauensvoll kommuniziert wird. So akzeptieren die Mitarbeiter diese mehr und sie sind eher bereit, bestehende Schwachstellen zu beheben.
- Wenn Sensibilisierungs- oder Schulungsmaßnahmen angepasst oder neu ausgerichtet werden müssen, sollte das Management zeitnah reagieren und zum Beispiel die erforderlichen Ressourcen bewilligen.

Prüffragen:

- Unterstützt die Leitungsebene die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit in ausreichendem Maße?

# M 3.97 Schulung des Projektteams für die Software-Entwicklung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Entwicklung
**Verantwortlich für Umsetzung:** Leiter Entwicklung, IT-Sicherheitsbeauftragter

Ein geschärftes Sicherheitsbewusstsein des Entwicklungsteams spielt eine entscheidende Rolle bei der Erstellung von sicheren IT-Systemen. Dabei muss dieses Sicherheitsbewusstsein nicht nur bei der Implementierungsphase sondern beim gesamten Lebenszyklus der Software-Entwicklung vorhanden sein.

**Allgemeine Inhalte für die Schulung des Projekt-Teams zur sicheren Software-Entwicklung**

Anforderungsanalyse:
Die Anforderungsanalyse und -Spezifikation ist ein sehr entscheidender Schritt für den Erfolg einer Software-Entwicklung. Dabei muss sichergestellt werden, dass die Anforderungen des Kunden bzw. der Fachabteilung vollständig, eindeutig, konsistent und verständlich definiert und dokumentiert werden. Die Anforderungsanalyse bildet die Basis für die spätere Abnahme des Systems, daher müssen die Anforderungen nachprüfbar sein.

Projektmanagement allgemein sowie speziell bei der Systementwicklung:
Das Projektmanagement bestimmt den Erfolg oder Misserfolg eines Entwicklungsprojektes. Der Projektmanager muss deswegen die notwendige Kenntnisse und Fertigkeiten besitzen, um z. B. Projektmitarbeiter zu motivieren, die Zusammenarbeit im Team zu fördern und Planung und Kontrolle richtig einzusetzen.

Risikomanagement in der Software-Entwicklung:
Relevante Themen aus diesem Gebiet sind Grundlagen zum Risikomanagement von Software-Entwicklungsprojekten, Risiken in der Software-Entwicklung, Methoden zur Risiko-Identifizierung, -Analyse, -Bewertung und Behandlung. Insbesondere ist es hier wichtig, die typischen Risiken in der Software-Entwicklung und ihre möglichen Auswirkungen sowie Maßnahmen zur Behandlung und Überwachung von Risiken in der Software-Entwicklung zu kennen.

Qualitätsmanagement:
Zu den relevanten Themen gehören Methoden und Normen zum Qualitätsmanagement (u. A. die ISO Normen aus der Familie 9000ff) und praxisnahe Erkenntnisse für die Anwendung von Qualitätsplanung, -Sicherung und -Steuerung.

Qualitätssicherung:
Aufgrund ihrer Bedeutung bei der Systementwicklung und der großen Auswahl an Methoden sollte dieser Punkt zumindest für das Test-Team vertieft werden. Zu den möglichen Inhalten hier gehören allgemeine Verfahren zur Qualitätssicherung, Planung und Bewertung, Methoden zur integrierten Software- und Testentwicklung und Methoden zur Aufwandschätzung beim Testen. Das Test-Team sollte mit folgenden Qualitätssicherungs-Verfahren vertraut sein:

- Statische Prüfverfahren (z. B. Code Review)
- Dynamische Prüfverfahren (z. B. Blackbox-Testverfahren wie Äquivalenzklassenbildung, Grenzwertanalyse, Zustandsbezogener Test und White-

box-Testverfahren, z. B. Anweisungs-, Zweig-, Pfadüberdeckung, Test von Bedingungen)

Modelle und Methoden für die Software-Entwicklung:
Das Entwicklungsteam sollte mit den bekannten Methoden, Normen und dem aktuellen Stand der Technik bzw. "Best Practices" für die Software-Entwicklung vertraut sein.

Änderungsmanagement:
Sowohl der Projektleiter der Software-Entwicklung als auch die Mitglieder des Entwicklungsteams müssen Bedeutung des Änderungsmanagements verstehen und die Basiskonzepte und Werkzeuge des Änderungsmanagements kennen und verwenden können. Die Schnittstellen von Änderungsmanagement zu anderen Aktivitäten der Software-Entwicklung müssen richtig definiert werden (z. B. zur Qualitätssicherung und zum Konfigurationsmanagement), gegebenenfalls müssen hier Anforderungen verschiedener Standards an das Änderungsmanagement berücksichtigt werden.

Informationssicherheit:
Ein Sicherheitsbewusstsein ist für die Entwicklung sicherer Produkte unabdingbar. So sollte das Projekt-Team zu allgemeinen Sicherheitsthemen sensibilisiert werden, wie z. B.

- Typische Sicherheitsgefährdungen für ähnliche Systeme (Typische Angriffsszenarien, typische Schwachstellen, typische Systemversagen und damit verbundene Schäden),
- Standard-Sicherheitsmaßnahmen zur sicheren Software-Entwicklung,
- Allgemeine Kenntnisse zur Informationssicherheit.

Sicherheitsvorgaben in der Institution:
Die Sicherheitsleitlinie und weitere Sicherheitsrichtlinien der Institution sollten bei der Software-Entwicklung mit berücksichtigt werden. Dies setzt natürlich voraus, dass das Projekt-Team alle hierfür relevante Vorgaben kennt.

Sicherheitsaspekte in speziellen Bereichen:
Je nach dem Anwendungsbereich der zu entwickelnden Software sollten die Entwickler zu spefischen Aspekten geschult werden. Dazu gehören beispielsweise Netz- und Kommunikationsprotokolle und -Dienste, Authentisierung und Zugriffskontrolle, Datenbanken, kryptographischen Verfahren, Verwaltung von kryptographischen Schlüsseln und Zertifikaten usw.

**Inhalte für die Schulung der Entwickler zur sicheren Programmierung**

Als erstes ist es wichtig, dass das Entwicklungsteam die verwendeten Methoden, Programmiersprachen, Entwicklungsumgebung, Konfigurationsmanagement-Tools und aller weitere Werkzeuge, die in der Software-Entwicklung eingesetzt werden gut kennt. Darüber hinaus sollte auch auf folgende weitere Bereiche eingegangen werden.

Vermeidung von Schwachstellen im System:
Ein Großteil aller Sicherheitslücken in Programmen werden durch dieselben Fehlerarten verursacht. Bei den akuten Sicherheitsproblemen, die bei den CERTs gemeldet werden, steht beispielsweise als Ursache immer wieder Buffer Overflow. Durch eine systematische Fehlerbehandlung (Exception handling) im Code können viele Schwachstellen vermieden werden indem die Korrektheit der verwendeten Daten (Datenbereich, Datenstruktur) vom System überprüft wird und falsche Daten abgefangen werden.

Durch die Verwendung von Code-Konventionen und von Programmiertechniken kann die Qualität des Programmcodes erheblich verbessert werden. Co-

de-Konventionen sind Vorschriften, die eine einheitliche und übersichtliche Gestaltung des Programmcodes ermöglichen, z.B. durch Regeln für den Dateiaufbau und Verzeichnisaufbau, die Code-Kommentierung, die Namensgebung, usw. und somit die Analyse, Wartbarkeit und Wiederverwendung von Programmcode erleichtern.

Ebenfalls wichtig ist hierfür der Einsatz von Programmierrichtlinien, wie beispielsweise die Behandlung von Ausnahmefällen, die Definition von Vorschriften für die Verwendung von Konstanten und für die Referenzierung usw. In der Regel existieren für alle gängige Programmiersprachen Software-Werkzeuge, die die Kontrolle der Einhaltung von Code-Konventionen und Programmierrichtlinien weitgehend unterstützen.

Die Gültigkeitsüberprüfung der Eingabe (Eingabevalidierung) ist unabdingbar um viele Arten von Angriffen abzufangen. Dies muss in allen relevanten Schnittstellen des Systems geschehen. In einer Client-Server Umgebung beispielsweise sollte die Eingabe nicht nur auf der Client-Seite des Systems überprüft werden, sondern auch auf der Server-Seite. Anderenfalls ist das System gegenüber "Man-in-the-middle"-Angriffen anfällig: Wenn ein Angreifer den Datenstrom vom Client zum Server abfängt und verändert, ist keine Abwehr mehr möglich. Daher ist eine Prüfung der Eingaben hinsichtlich Länge, Wertebereich und Format unbedingt erforderlich.

Standard-Einstellungen sollten die möglichst maximale Sicherheit für das System bieten. Auch im Hinblick auf die angebotenen Schnittstellen, Dienste oder die offenen Ports sollte darauf geachtet werden, dass das System eine möglichst geringe Angriffsfläche bietet.

Das Prinzip der minimalen Rechtevergabe muss sowohl für die Entwickler als auch für die Administratoren und Benutzer des Systems beachtet werden. Ein Authentisierungs- und Berechtigungskonzept ist dafür erforderlich, und muss schon in der Design-Phase erstellt werden. Es empfiehlt sich, Rollen für die verschiedenen Zugriffe zu definieren und die Zugriffe auf Systemebene so weit wie möglich einzuschränken. Wichtig dabei ist auch, angemessene Authentisierungs- und Berechtigungsverfahren zu verwenden. Vorgehensweisen, die in Betracht gezogen werden können, sind Zwei-Faktoren-Authentisierung, Sperrfunktionen für Benutzerkonten, Erzwingung von starken Passwörtern, Ablauffristen für Passwörter usw.

Systemabstürze, Ausfälle und Fehler können nicht immer verhindert werden. Daher muss darauf geachtet werden, dass

- jeder Ausfall zu einem sicheren Zustand des Systems führt,
- die Konsistenz des Systems und der Daten nach einem Ausfall oder Fehler erhalten bleibt,
- die Fehlermeldungen beziehungsweise das Verhalten des Systems in solchen Fällen keine sensiblen Informationen verraten oder Angriffsmöglichkeiten bieten,
- die notwendigen Informationen zur Nachverfolgung der Fehlerursachen protokolliert werden.

Die Ausgabe von programminternen Informationen auf der Benutzeroberfläche sollte immer vermieden werden. Dazu gehört beispielsweise, dass Fehlermeldungen an den Benutzer keine internen Informationen über das Programm, das System oder das Netz verraten dürfen,

Insbesondere bei Web-Anwendungen muss darauf geachtet werden, dass keine sensitiven Informationen über die Internetadresse (URL) preisgegeben werden können und dass URL-Manipulationen nicht stattfinden können.

Vertrauliche Informationen müssen bei einer Übertragung und bei der Speicherung ausreichend geschützt werden. Dazu sind bewährte und angemessene Kryptographie-Verfahren einzusetzen. Beispielsweise sollten Passwörter nicht im Klartext übertragen werden und geschützt gespeichert werden.

Um Sicherheitslücken bei neuen Produkten möglichst zu vermeiden, sollten daher alle Entwickler zur Vorbeugung mit den Grundlagen von Informationssicherheit und sicherer Entwicklung vertraut sein. Insbesondere sollten die Entwickler zu Vorgehensweisen zur Vermeidung von typischen Fehlern und Schwachstellen für die verwendete Programmiersprache und das zu entwickelnde System geschult werden (beispielsweise zur Vermeidung von Buffer Overflows).

Allen Entwicklern sollte ihre Verantwortung für die Sicherheit neuer Systeme bewusst gemacht werden.

Prüffragen:

- Sind die Entwickler zu Sicherheitsaspekten geschult?

# M 3.98 Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter Personal
**Verantwortlich für Umsetzung:** Personalabteilung, Vorgesetzte

Alle Mitarbeiter sind in den sicheren Umgang mit den in der Institution eingesetzten Authentisierungsverfahren und -mechanismen einzuweisen. Außerdem müssen alle Mitarbeiter über die Richtlinien und Anweisungen zum Umgang mit Authentisierungsverfahren und -mechanismen informiert werden (siehe beispielsweise M 2.11 *Regelung des Passwortgebrauchs*). Besonders wichtig ist dabei, die Mitarbeiter darüber zu unterrichten, warum die Richtlinien notwendig und angemessen sind. So sind sie besser motiviert, die Vorgaben auch einzuhalten. Die Richtlinien müssen für die Mitarbeiter verständlich sein und dürfen nur Regelungen enthalten, die auch umgesetzt werden können. Sie sollten zudem so positiv wie möglich formuliert werden.

Die Einweisung sollte mindestens folgende Punkte umfassen:

- Wozu dient Authentisierung?
- Grundlagen Identifizierung und Authentisierung, Erläuterungen von Begriffsdefinition wie Wissen, Besitz, Eigenschaft
- Hinweise zur Handhabung der eingesetzten Authentisierungsverfahren und -mechanismen (z. B. Aufbewahrung von Authentikationstoken)
- Vorgaben zum Auswahl und Nutzung von Passwörtern (z. B. Passwörter nicht aufschreiben und nicht weitergeben, Passwörter sollten nicht zu trivial sein, eine bestimmte Länge und Komplexität haben, siehe M 2.11 *Regelung des Passwortgebrauchs*)
- Umgang mit Berechtigungen: Überblick über Berechtigungskonzept der Institution, Gestaltung der Rechtevergabe
- Übersicht über Sicherheitsfunktionalitäten des eingesetzten Produktes zum Identitäts- und Berechtigungsmanagement
- Beschreibung, wie der Prozess (Wieder-)Freigabe bei Sperrung von Benutzerkennungen funktioniert
- Überblick über die verschiedenen Aufgaben und Rollen bei der Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen, Benennung von Ansprechpartnern

Prüffragen:

- Sind alle Mitarbeiter in den korrekten Umgang mit den Authentisierungsverfahren eingewiesen worden?
- Gibt es verständliche Richtlinien für den Umgang mit Authentisierungsverfahren?
- Sind alle Mitarbeiter über die relevanten Regelungen zur Authentisierung informiert?

# M 4 Maßnahmenkatalog Hard- und Software

M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems

M 4.27 Zugriffsschutz am Laptop

M 4.28 Software-Reinstallation bei Benutzerwechsel eines Laptops

M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme

M 4.30 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

M 4.31 Sicherstellung der Energieversorgung im mobilen Einsatz

M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung

M 4.33 Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung

M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

M 4.35 Verifizieren der zu übertragenden Daten vor Versand

M 4.36 Sperren bestimmter Faxempfänger-Rufnummern

M 4.37 Sperren bestimmter Absender-Faxnummern

M 4.38 Abschalten nicht benötigter Leistungsmerkmale **- entfallen**

M 4.39 Abschalten des Anrufbeantworters bei Anwesenheit **- entfallen**

M 4.40 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras

M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme

M 4.42 Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

M 4.43 Faxgerät mit automatischer Eingangskuvertierung

M 4.44 Prüfung eingehender Dateien auf Makro-Viren **- entfallen**

M 4.45 Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW **- entfallen**

M 4.46 Nutzung des Anmeldepasswortes unter WfW und Windows 95 **- entfallen**

M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten

M 4.48 Passwortschutz unter Windows-Systemen

M 4.49 Absicherung des Boot-Vorgangs für ein Windows-System

M 4.50 Strukturierte Systemverwaltung unter Windows NT **- entfallen**

M 4.51 Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT **- entfallen**

M 4.52 Geräteschutz unter NT-basierten Windows-Systemen

M 4.53 Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT **- entfallen**

M 4.54 Protokollierung unter Windows NT **- entfallen**

M 4.55 Sichere Installation von Windows NT **- entfallen**

M 4.56 Sicheres Löschen unter Windows-Betriebssystemen

M 4.57 Deaktivieren der automatischen CD-ROM-Erkennung

M 4.58 Freigabe von Verzeichnissen unter Windows 95 **- entfallen**

M 4.59 Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten

M 4.60 Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten

M 4.61 Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten

M 4.62 Einsatz eines D-Kanal-Filters

M 4.63 Sicherheitstechnische Anforderungen an den Telearbeitsrechner

M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen

M 4.65 Test neuer Hard- und Software

M 4.66 Novell Netware - Sicherer Übergang ins Jahr 2000 **- entfallen**

M 4.67 Sperren und Löschen nicht benötigter Datenbank-Accounts

M 4.68 Sicherstellung einer konsistenten Datenbankverwaltung

M 4.69 Regelmäßiger Sicherheitscheck der Datenbank

M 4.70 Durchführung einer Datenbanküberwachung

M 4.71 Restriktive Handhabung von Datenbank-Links

M 4.72 Datenbank-Verschlüsselung

M 4.73 Festlegung von Obergrenzen für selektierbare Datensätze

M 4.74 Vernetzte Windows 95 Rechner **- entfallen**

M 4.75 Schutz der Registry unter Windows-Systemen

M 4.76 Sichere Systemversion von Windows NT **- entfallen**

M 4.77 Schutz der Administratorkonten unter Windows NT **- entfallen**

M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen

M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration

M 4.111 Sichere Konfiguration des RAS-Systems **- entfallen**

M 4.112 Sicherer Betrieb des RAS-Systems **- entfallen**

M 4.113 Nutzung eines Authentisierungsservers bei Remote-Access-VPNs

M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen

M 4.115 Sicherstellung der Energieversorgung von Mobiltelefonen

M 4.116 Sichere Installation von Lotus Notes/Domino

M 4.117 Sichere Konfiguration eines Lotus Notes Servers **- entfallen**

M 4.118 Konfiguration als Lotus Notes Server **- entfallen**

M 4.119 Einrichten von Zugangsbeschränkungen auf Lotus Notes Server **- entfallen**

M 4.120 Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken **- entfallen**

M 4.121 Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes **- entfallen**

M 4.122 Konfiguration für den Browser-Zugriff auf Lotus Notes **- entfallen**

M 4.123 Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes **- entfallen**

M 4.124 Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes **- entfallen**

M 4.125 Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken **- entfallen**

M 4.126 Sichere Konfiguration eines Lotus Notes Clients **- entfallen**

M 4.127 Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes **- entfallen**

M 4.128 Sicherer Betrieb der Lotus Notes/Domino-Umgebung

M 4.129 Sicherer Umgang mit Notes-ID-Dateien **- entfallen**

M 4.130 Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken **- entfallen**

M 4.131 Verschlüsselung von Lotus Notes Datenbanken **- entfallen**

M 4.132 Überwachung der Lotus Notes/Domino-Umgebung

M 4.133 Geeignete Auswahl von Authentikationsmechanismen

M 4.134 Wahl geeigneter Datenformate

M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien

M 4.136 Sichere Installation von Windows 2000 **- entfallen**

M 4.137 Sichere Konfiguration von Windows 2000 **- entfallen**

M 4.138 Konfiguration von Windows Server als Domänen-Controller

M 4.139 Konfiguration von Windows 2000 als Server **- entfallen**

M 4.140 Sichere Konfiguration wichtiger Windows 2000 Dienste **- entfallen**

M 4.141 Sichere Konfiguration des DDNS unter Windows 2000 **- entfallen**

M 4.142 Sichere Konfiguration des WINS unter Windows 2000 **- entfallen**

M 4.143 Sichere Konfiguration des DHCP unter Windows 2000 **- entfallen**

M 4.144 Nutzung der Windows 2000 CA **- entfallen**

M 4.145 Sichere Konfiguration von RRAS unter Windows 2000 **- entfallen**

M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen

M 4.147 Sichere Nutzung von EFS unter Windows

M 4.148 Überwachung eines Windows 2000/XP Systems

M 4.149 Datei- und Freigabeberechtigungen unter Windows

M 4.150 Konfiguration von Windows 2000 als Workstation **- entfallen**

M 4.151 Sichere Installation von Internet-PCs

M 4.152 Sicherer Betrieb von Internet-PCs

M 4.153 Sichere Installation von Novell eDirectory

M 4.154 Sichere Installation der Novell eDirectory Clientsoftware

M 4.155 Sichere Konfiguration von Novell eDirectory

M 4.156 Sichere Konfiguration der Novell eDirectory Clientsoftware

M 4.157 Einrichten von Zugriffsberechtigungen auf Novell eDirectory

M 4.158 Einrichten des LDAP-Zugriffs auf Novell eDirectory

M 4.159 Sicherer Betrieb von Novell eDirectory

M 4.160 Überwachen von Novell eDirectory

M 4.161 Sichere Installation von Exchange-Systemen

M 4.162 Sichere Konfiguration von Exchange-Servern

M 4.163 Zugriffsrechte auf Exchange-Objekte

M 4.164 Browser-Zugriff auf Exchange 2000 **- entfallen**

M 4.165 Sichere Konfiguration von Outlook

M 4.166 Sicherer Betrieb von Exchange-Systemen

M 4.167 Überwachung und Protokollierung von Exchange 2000 Systemen **- entfallen**

M 4.168 Auswahl eines geeigneten Archivsystems

M 4.169 Verwendung geeigneter Archivmedien

M 4.170 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten

M 4.171 Schutz der Integrität der Index-Datenbank von Archivsystemen

M 4.172 Protokollierung der Archivzugriffe

M 4.173 Regelmäßige Funktions- und Recoverytests bei der Archivierung

M 4.174 Vorbereitung der Installation von Windows NT/2000 für den IIS **- entfallen**

M 4.175 Sichere Konfiguration von Windows NT/2000 für den IIS **- entfallen**

M 4.176 Auswahl einer Authentisierungsmethode für Webangebote

M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen

M 4.178 Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz **- entfallen**

M 4.179 Schutz von sicherheitskritischen Dateien beim IIS-Einsatz **- entfallen**

M 4.180 Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS **- entfallen**

M 4.181 Ausführen des IIS in einem separaten Prozess **- entfallen**

M 4.182 Überwachen des IIS-Systems **- entfallen**

M 4.183 Sicherstellen der Verfügbarkeit und Performance des IIS **- entfallen**

M 4.184 Deaktivieren nicht benötigter Dienste beim IIS-Einsatz **- entfallen**

M 4.185 Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz **- entfallen**

M 4.186 Entfernen von Beispieldateien und Administrations-Scripts des IIS **- entfallen**

M 4.187 Entfernen der FrontPage Server-Erweiterung des IIS **- entfallen**

M 4.188 Prüfen der Benutzereingaben beim IIS-Einsatz **- entfallen**

M 4.189 Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz **- entfallen**

M 4.190 Entfernen der RDS-Unterstützung des IIS **- entfallen**

M 4.191 Überprüfung der Integrität und Authentizität der Apache-Pakete **- entfallen**

M 4.192 Konfiguration des Betriebssystems für einen Apache-Webserver **- entfallen**

M 4.193 Sichere Installation eines Apache-Webservers **- entfallen**

M 4.194 Sichere Grundkonfiguration eines Apache-Webservers **- entfallen**

M 4.195 Konfiguration der Zugriffssteuerung beim Apache-Webserver **- entfallen**

M 4.196 Sicherer Betrieb eines Apache-Webservers **- entfallen**

M 4.197 Servererweiterungen für dynamische Webseiten beim Apache-Webserver **- entfallen**

M 4.198 Installation einer Applikation in einem chroot Käfig

M 4.199 Vermeidung problematischer Dateiformate

M 4.200 Umgang mit USB-Speichermedien

M 4.201 Sichere lokale Grundkonfiguration von Routern und Switches

M 4.202 Sichere Netz-Grundkonfiguration von Routern und Switches

M 4.203 Konfigurations-Checkliste für Router und Switches

M 4.204 Sichere Administration von Routern und Switches

M 4.205 Protokollierung bei Routern und Switches

M 4.206 Sicherung von Switch-Ports

M 4.207 Einsatz und Sicherung systemnaher z/OS-Terminals

M 4.208 Absichern des Start-Vorgangs von z/OS-Systemen

M 4.209 Sichere Grundkonfiguration von z/OS-Systemen

M 4.210 Sicherer Betrieb des z/OS-Betriebssystems

M 4.211 Einsatz des z/OS-Sicherheitssystems RACF

M 4.212 Absicherung von Linux für zSeries

M 4.326 Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver

M 4.327 Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen

M 4.328 Sichere Grundkonfiguration eines Samba-Servers

M 4.329 Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers

M 4.330 Sichere Installation eines Samba-Servers

M 4.331 Sichere Konfiguration des Betriebssystems für einen Samba-Server

M 4.332 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server

M 4.333 Sichere Konfiguration von Winbind unter Samba

M 4.334 SMB Message Signing und Samba

M 4.335 Sicherer Betrieb eines Samba-Servers

M 4.336 Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag

M 4.337 Einsatz von BitLocker Drive Encryption

M 4.338 Einsatz von File und Registry Virtualization bei Clients ab Windows Vista

M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista

M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista

M 4.341 Integritätsschutz ab Windows Vista

M 4.342 Aktivierung des Last Access Zeitstempels ab Windows Vista

M 4.343 Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag

M 4.344 Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008

M 4.345 Schutz vor unerwünschten Informationsabflüssen

M 4.346 Sichere Konfiguration virtueller IT-Systeme

M 4.347 Deaktivierung von Snapshots virtueller IT-Systeme

M 4.348 Zeitsynchronisation in virtuellen IT-Systemen

M 4.407 Protokollierung beim Einsatz von OpenLDAP

M 4.408 Übersicht über neue, sicherheitsrelevante Funktionen in Windows Server 2008

M 4.409 Beschaffung von Windows Server 2008

M 4.410 Einsatz von Netzwerkzugriffsschutz unter Windows

M 4.411 Sichere Nutzung von DirectAccess unter Windows

M 4.412 Sichere Migration von Windows Server 2003 auf Server 2008

M 4.413 Sicherer Einsatz von Virtualisierung mit Hyper-V

M 4.414 Überblick über Neuerungen für Active Directory ab Windows Server 2008

M 4.415 Sicherer Betrieb der biometrischen Authentisierung unter Windows

M 4.416 Einsatz von Windows Server Core

M 4.417 Patch-Management mit WSUS ab Windows Server 2008

M 4.418 Planung des Einsatzes von Windows Server 2008

M 4.419 Anwendungssteuerung ab Windows 7 mit AppLocker

M 4.420 Sicherer Einsatz des Wartungscenters unter Windows 7

M 4.421 Absicherung der Windows PowerShell

M 4.422 Nutzung von BitLocker To Go ab Windows 7

M 4.423 Verwendung der Heimnetzgruppen-Funktion ab Windows 7

M 4.424 Sicherer Einsatz älterer Software ab Windows 7

M 4.425 Verwendung der Tresor- und Cardspace-Funktion auf Clients ab Windows

M 4.426 Archivierung für die Lotus Notes/Domino-Umgebung

M 4.427 Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino

M 4.428 Audit der Lotus Notes/Domino-Umgebung

M 4.429 Sichere Konfiguration von Lotus Notes/Domino

M 4.430 Analyse von Protokolldaten

M 4.431 Auswahl und Verarbeitung relevanter Informationen für die Protokollierung

M 4.432 Sichere Konfiguration von Serverdiensten

M 4.433 Einsatz von Datenträgerverschlüsselung

M 4.434 Sicherer Einsatz von Appliances

M 4.465 Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs

M 4.466 Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs

M 4.467 Auswahl von Applikationen für Smartphones, Tablets und PDAs

M 4.468 Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs

M 4.469 Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion

M 4.470 Grundlagenwissen zu Windows 8

M 4.471 Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8

M 4.472 Datensparsamkeit bei Windows 8

M 4.473 Schutz vor Abhören von XML-Transportcontainern in einer SOA

M 4.474 Schutz vor Schwachstellen in Backend-Anwendungen einer SOA

M 4.475 Schutz vor Spoofing-Angriffen auf Identitätsdienste

M 4.476 Schutz einer WS-Notification-Subscription im Broker

M 4.477 Schutz einer WS-Notification

M 4.478 Schlüsselmittelverwaltung bei SOA

M 4.479 Schutz von Richtlinien in einer SOA

M 4.480 Schutz von WS-Resource in SOA-Umgebungen

M 4.481 Sichere Nutzung verbindungsloser SOAP-Kommunikation

M 4.482 Hardware-Realisierung von Funktionen eingebetteter Systeme

M 4.483 Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen

M 4.484 Speicherschutz bei eingebetteten Systemen

M 4.485 Sicheres Betriebssystem für eingebettete Systeme

M 4.486 Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe

M 4.487 Tamper-Schutz (Erkennung, Verhinderung, Abwehr) bei eingebetteten Systemen

M 4.488 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen

# M 4.1 Passwortschutz für IT-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Der Passwortschutz eines IT-Systems soll gewährleisten, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen. Unmittelbar nach dem Einschalten des IT-Systems muss der Berechtigungsnachweis erfolgen. Kann der Benutzer die erforderliche Berechtigung nicht nachweisen, so verhindert der Passwortschutz den Zugriff auf das IT-System.

Realisiert werden kann der Passwortschutz an einem IT-System auf verschiedene Weise:

- Die meisten BIOS-Varianten bieten die Installation eines Boot-Passwortes an. Bei Fehleingaben wird der Boot-Vorgang nicht fortgesetzt. Ein BIOS-Passwort ist nicht schwer zu überwinden, schützt aber vor Zufallstätern, sollte also zumindest überall da eingesetzt werden, wo keine besseren Zugriffsschutzmechanismen vorhanden sind (siehe auch: M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*).
- Gute Betriebssysteme enthalten bereits Zugriffsschutzmechanismen. In den meisten Fällen müssen diese aber noch aktiviert werden, beispielsweise durch die Vergabe von Passwörtern für alle Benutzer. Näheres hierzu findet sich in den betriebssystem-spezifischen Bausteinen.
- Es wird Zusatzhardware oder -software installiert, die vor dem eigentlichen Start des Rechners ein Passwort abfragt und bei falscher Passworteingabe die weitere Nutzung des IT-Systems verhindert.

Für den Umgang mit Passwörtern sind die Hinweise in M 2.11 *Regelung des Passwortgebrauchs* zu beachten, insbesondere ist das Passwort regelmäßig zu ändern.

Prüffragen:

- Ist sichergestellt, dass nur berechtige Personen auf Anwendungen und IT-Systeme zugreifen können?

# M 4.2 Bildschirmsperre

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Unter einer Bildschirmsperre versteht man die Möglichkeit, die auf dem Bildschirm aktuell vorhandenen Informationen zu verbergen. Eine Bildschirmsperre sollte nur durch eine erfolgreiche Benutzerauthentikation, also z. B. eine Passwortabfrage, deaktiviert werden können, damit bei einer kürzeren Abwesenheit des IT-Benutzers ein Zugriffsschutz für das IT-System gewährleistet wird.

Die Bildschirmsperre sollte sich sowohl manuell vom Benutzer aktivieren lassen, als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet werden. Alle Benutzer sollten dafür sensibilisiert sein, dass sie die Bildschirmsperre aktivieren, wenn sie den Arbeitsplatz für eine kurze Zeit verlassen. Bei längeren Abwesenheiten sollten Benutzer sich abmelden.

Der Zeitraum, nach dem sich eine Bildschirmsperre wegen fehlender Benutzereingaben aktiviert, sollte gewisse Grenzen weder unter- noch überschreiten. Der Zeitraum sollte nicht zu knapp gewählt werden, damit die Bildschirmsperre nicht bereits nach kurzen Denkpausen anspringt. Dieser Zeitraum darf aber auf keinen Fall zu lang sein, damit die Abwesenheit des Benutzers nicht von Dritten ausgenutzt werden kann. Eine sinnvolle Vorgabe ist eine Zeitspanne von 15 Minuten. Das IT-Sicherheitsmanagement-Team sollte Vorgaben für die Einstellung der Wartezeit machen, die die Sicherheitsanforderungen der jeweiligen IT-Systeme und deren Einsatzumgebung berücksichtigen.

Die meisten Betriebssysteme enthalten bereits Bildschirmsperren. Bei deren Nutzung muss darauf geachtet werden, die Passwortabfrage zu aktivieren.

Prüffragen:

- Existiert eine PC-Richtlinie, die neben Sicherheitsmaßnahmen auch Geltungsbereich, Rechtsvorschriften und interne Regelungen, Verantwortlichkeiten, Rollen und Ansprechpartner abdeckt?
- Ist die manuelle Bildschirmsperre allen Mitarbeitern bekannt und wird diese auch eingesetzt?
- Ist ein Zeitraum für die automatische Bildschirmsperre definiert, der sowohl Nutzer- als auch Sicherheitsbelange berücksichtigt?
- Bei fehlender Unterstützung durch das Betriebssystem: Wird eine fehlende Bildschirmsperre durch andere Maßnahmen realisiert?

# M 4.3 Einsatz von Viren-Schutzprogrammen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Zum Schutz vor Schadprogrammen können unterschiedliche Wirkprinzipien genutzt werden. Programme, die IT-Systeme nach sämtlichen bekannten Schadprogrammen durchsuchen, haben sich in der Vergangenheit als wirksames Mittel in der Schadprogramm-Prävention erwiesen. Entsprechend der in M 2.157 *Auswahl eines geeigneten Viren-Schutzprogramms* beschriebenen Anforderungen sollten daher Viren-Schutzprogramme eingesetzt werden.

Bei mobilen Endgeräten, wie Smartphones, Tablets oder PDAs, ist zusätzlich Maßnahme M 4.466 *Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs* umzusetzen.

**Schutz von Internet-Diensten**

Am zentralen E-Mail-Gateway muss ein Viren-Schutzprogramm eingesetzt werden, das ein- und ausgehende E-Mails prüft.

Alle weiteren Internet-Dienste (HTTP, FTP, etc.) sollten ebenfalls mit spezialisierter Schutzsoftware abgesichert werden. Wenn dies beispielsweise aufgrund von Performance-Problemen nicht möglich ist, muss zumindest die Ausführung aktiver Inhalte von nicht vertrauenswürdigen Seiten technisch unterbunden werden.

**Regelmäßige Untersuchung des gesamten Datenbestands**

Auch wenn das Viren-Schutzprogramm bei jedem Dateizugriff eine Prüfung auf Schadprogramme durchführt, ist eine regelmäßige Untersuchung aller Dateien auf Clients und Datei-Servern sinnvoll. So können auch Schadprogramme gefunden werden, für die es noch keine Erkennungssignatur gab, als sie gespeichert wurden. In derartigen Fällen muss beispielsweise untersucht werden, ob das Schadprogramm vor seiner Entdeckung bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Aus Performance-Gründen sollte eine vollständige Prüfung des Datenbestands in Zeiten durchgeführt werden, in denen die IT-Ressourcen nicht stark beansprucht werden. Ideal ist es, wenn die Software die Auslastung des Rechners überwacht und dessen "Arbeitspausen" automatisch für die Überprüfung nutzt. Auf den Arbeitsplatz-Rechnern könnte das Viren-Schutzprogramm z. B. auch mit dem Start des Bildschirmschoners gekoppelt werden.

**Datenaustausch und Datenübertragung**

Daten, die versendet werden sollen, müssen unmittelbar vor dem Versand auf Schadprogramme geprüft werden. Analog müssen empfangene Daten unmittelbar nach dem Empfang auf Schadprogramme geprüft werden. Diese Überprüfungen sind sowohl beim Zugriff auf Datenträger als auch bei der Datenübertragung über Kommunikationsverbindungen erforderlich. Die Überprüfungen sollten so weit wie möglich automatisiert werden.

Als zusätzliche Maßnahme können Prüfstellen für von außen kommende Programme, Dateien und Datenträger eingerichtet werden. Die Prüfstellen sind separate IT-Systeme, die nicht in das lokale Netz integriert sind. Mittels eines

Viren-Schutzprogramms werden auf den Prüfstellen alle von außen kommenden Programme und Dateien zentral getestet und freigegeben.

Dieses Vorgehen kann beispielsweise notwendig sein, wenn besonders hohe Sicherheitsanforderungen vorliegen oder wenn ein besonders gefährliches Schadprogramm im Umlauf ist.

**Wechselwirkungen mit Verschlüsselungstechniken**

Beim Einsatz von Verschlüsselungstechniken müssen die potentiellen Auswirkungen auf den Schutz vor Schadprogrammen bedacht werden. Werden Daten verschlüsselt, so können Systemkomponenten bzw. Anwendungen auf diese Daten nicht zugreifen, solange sie nicht über die entsprechenden Schlüssel verfügen. Dies impliziert, dass ein Viren-Schutzprogramm entweder im Kontext des Benutzers laufen oder mit den entsprechenden kryptografischen Schlüsseln ausgestattet werden muss, um eine verschlüsselte Datei auf Schadprogramme überprüfen zu können. Wird jedoch die Benutzer-Kennung, unter der das Viren-Schutzprogramm ausgeführt wird, mit den entsprechenden kryptografischen Schlüsseln ausgestattet, entstehen neue Sicherheitsrisiken, die es zu vermeiden gilt. Daher wird der Einsatz eines residenten Viren-Schutzprogramms empfohlen, welches die Prüfung auf Schadprogramme im Benutzer-Kontext bei jedem Zugriff auf eine Datei durchführt.

**Schutz vor unerlaubter Deaktivierung oder Änderung**

Die Viren-Schutzprogramme auf den Clients und Endgeräten müssen so konfiguriert sein, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Viren-Schutzprogramme vornehmen können. Insbesondere muss sichergestellt sein, dass die Benutzer die Viren-Schutzprogramme nicht deaktivieren können.

Prüffragen:

- Sind Viren-Schutzprogramme auf allen IT-Systemen installiert, auf denen dies laut Sicherheitskonzept vorgesehen ist?
- Wird sichergestellt, das sowohl Scanprogramm als auch Signaturen stets auf dem aktuellsten Stand sind?
- Sind die Nutzer mit dem Scanprogramm vertraut, insbesondere mit der Möglichkeit des "On-Demand-Scans"?
- Wird das zentrale E-Mail-Gateway durch ein Viren-Schutzprogramm gesichert?
- Ist für die genutzten Internet-Dienste ein ausreichender Schutz vor Schadprogrammen gewährleistet?
- Wird eine regelmäßige Untersuchung des gesamten Datenbestandes auf Schadprogramme durchgeführt?
- Bei Auffinden eines Schadprogrammes: Wird untersucht, ob das gefundene Schadprogramm vor seiner Entdeckung bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat?
- Wird bei Datenaustausch und Datenübertragung eine Suche nach Schadprogrammen durchgeführt?
- Ist auch für verschlüsselte Daten ein ausreichender Schutz vor Schadprogrammen gewährleistet?
- Ist sichergestellt, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Viren-Schutzprogramme vornehmen können?

# M 4.4 Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Handelsübliche PCs sind heute in der Regel mit einem CD-/DVD-ROM-Laufwerk bzw. CD-/DVD-Brenner ausgestattet. Zusätzlich besteht die Möglichkeit, über Schnittstellen externe Speichermedien anzuschließen, die von vielen Betriebssystemen automatisch erkannt und eingebunden werden. Beispiele sind USB-Speicher, die an die USB-Schnittstelle angeschlossen werden, und Firewire-Festplatten. Außerdem sind in vielen IT-Systemen Kartenleser für Speicherkarten eingebaut. Durch solche Laufwerke für Wechselmedien und externe Datenspeicher ergeben sich folgende potentielle Sicherheitsprobleme:

- Das IT-System könnte von solchen Laufwerken unkontrolliert gebootet werden.
- Es könnte unkontrolliert Software von solchen Laufwerken eingespielt werden.
- Daten könnten unberechtigt auf Wechselmedien kopiert werden.

Beim Booten von Wechselmedien oder beim Installieren von Fremdsoftware können nicht nur Sicherheitseinstellungen außer Kraft gesetzt werden, sondern das IT-System kann auch mit Computer-Viren und anderen Schadprogrammen infiziert werden.

Diesen Gefahren muss durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden. Hierfür bieten sich verschiedene Vorgehensweisen an, deren spezifische Vor- und Nachteile im Folgenden kurz dargestellt werden:

- Ausbau von Laufwerken
  Der Ausbau der Laufwerke für Wechselmedien (bzw. der Verzicht bei der Beschaffung) bietet zwar den sichersten Schutz vor den oben genannten Gefährdungen, ist aber meist mit erheblichem Aufwand verbunden. Oft ist ein Ausbau überhaupt nicht möglich, z. B. bei Speicherkartenlesern bei Notebooks. Weiterhin ist zu berücksichtigen, dass der Ausbau unter Umständen die Administration und Wartung des IT-Systems behindert. Diese Lösung sollte in Betracht gezogen werden, wenn besondere Sicherheitsanforderungen bestehen.
- Verschluss von Laufwerken
  Für einige Laufwerksarten gibt es abschließbare Einschubvorrichtungen, mit denen die unkontrollierte Nutzung verhindert werden kann. Bei der Beschaffung sollte sichergestellt werden, dass die Laufwerksschlösser für die vorhandenen Laufwerke geeignet sind und diese nicht beschädigen können. Es muss beachtet werden, dass nicht für alle Laufwerksarten, wie für eingebaute Speicherkartenleser, Schlösser angeboten werden. Außerdem sollte darauf geachtet werden, dass die Schlösser herstellerseitig mit hinreichend vielen unterschiedlichen Schlüsseln angeboten werden. Nachteilig sind die Beschaffungskosten für die Laufwerksschlösser und der Aufwand für die erforderliche Schlüsselverwaltung. Daher ist diese Lösung nur bei höherem Schutzbedarf oder besonderen Sicherheitsanforderungen sinnvoll.
- Deaktivierung im BIOS bzw. Betriebssystem
  Im BIOS bieten die meisten PCs Einstellmöglichkeiten dafür, von welchen Laufwerken gebootet werden kann. In Verbindung mit einem Passwort-

Schutz der BIOS-Einstellungen (siehe auch M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*) kann dadurch das unkontrollierte Booten von Wechselmedien und mobilen Datenträgern unterbunden werden. Weiterhin können die vorhandenen Laufwerke und Schnittstellen bei modernen Betriebssystemen einzeln deaktiviert werden.
Dies erschwert die unberechtigte Nutzung, z. B. die Installation von Fremdsoftware oder das Kopieren auf Wechselmedien. Die Deaktivierung der Laufwerke im BIOS bzw. Betriebssystem hat den Vorteil, dass keine Hardware-Änderungen erforderlich sind. Die entsprechenden Einstellungen im Betriebssystem können gegebenenfalls sogar zentral vorgenommen werden. Damit diese Vorgehensweise wirksam ist, muss sichergestellt sein, dass die Benutzer nicht über die Berechtigungen im Betriebssystem verfügen, um die Deaktivierung der Laufwerke rückgängig zu machen.

- Kontrolle der Schnittstellennutzung
  Der Betrieb von externen Speichermedien wie USB-Speichermedien lässt sich nur sehr schwer verhindern, wenn die verwendete Schnittstelle auch für andere (erlaubte) Zusatzgeräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Dadurch ist es in der Regel nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren.
  Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Bei einigen Zusatzprogrammen zur Absicherung der USB- oder Firewire-Schnittstellen kann zusätzlich festgelegt werden, ob von externen Datenträgern nur gelesen werden kann. Alternativ kann das Hinzufügen von Geräten überwacht werden.
  Beim Anschluss von Datenträgern an externen Schnittstellen werden oft vom Betriebssystem Treiber bzw. Kernelmodule geladen oder Einträge in Konfigurationsdateien (wie der Windows-Registry) erzeugt, die detektiert werden können. Einzelheiten sind produkt- und betriebssystemspezifisch und werden in einer separaten Maßnahme beschrieben (siehe auch M 4.200 *Umgang mit USB-Speichermedien*).
- Verschlüsselung
  Es gibt Produkte, die dafür sorgen, dass ausschließlich Zugriffe auf dafür zugelassene mobile Datenträger möglich sind. Eine Lösung ist beispielsweise, dass nur noch mobile Datenträger gelesen und beschrieben werden können, die mit bestimmten kryptographischen Schlüsseln verschlüsselt worden sind. Dies schützt nicht nur vor unbefugtem Zugriff über manipulierte mobile Datenträger, sondern schützt auch die Daten auf den mobilen Datenträgern bei Verlust oder Diebstahl.
- Richtlinien für die Nutzung
  In vielen Fällen dürfen die Benutzer die eingebauten Laufwerke für Wechselmedien oder Speichermedien an externen Schnittstellen durchaus verwenden, die Nutzung ist jedoch durch entsprechende Richtlinien reglementiert. Auf technischer Ebene sollte dann lediglich das Booten von Wechselmedien im BIOS deaktiviert werden. Ausbau, Verschluss oder Deaktivierung der Laufwerke im Betriebssystem kommen nicht in Frage.
  In diesem Fall sollten die Richtlinien für die Nutzung der Laufwerke und Speichermedien so explizit wie möglich definiert werden. Beispielsweise kann ein generelles Verbot ausgesprochen werden, nur das Kopieren öffentlicher Text-Dokumente wird erlaubt. Die Richtlinien müssen allen Benutzern bekannt gemacht und die Einhaltung kontrolliert werden. Die Installation und das Starten von Programmen, die von Wechselmedien eingespielt wurden, sollte untersagt und soweit wie möglich auch technisch unterbunden werden (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Diese rein organisatorische Lösung sollte nur dann gewählt werden, wenn die Benutzer hin und wieder oder regelmäßig auf die Laufwerke zugreifen müssen. Anderenfalls sollte der Zugriff, wie oben beschrieben, durch technische Maßnahmen unterbunden werden.

Bei der Auswahl einer geeigneten Vorgehensweise müssen immer *alle* Laufwerke für Wechselmedien berücksichtigt werden, aber ebenso auch alle Möglichkeiten, über Vernetzung Daten auszutauschen, also insbesondere auch E-Mail und Internet-Anbindungen. Wenn das IT-System über eine Verbindung zum Internet verfügt, ist es nicht allein ausreichend, alle Laufwerke für Wechselmedien zu deaktivieren oder auszubauen. Besonderes Augenmerk ist auf den Schutz vor Schadprogrammen, z. B. Computer-Viren oder Trojanische Pferde, zu richten (siehe auch M 4.3 *Einsatz von Viren-Schutzprogrammen*).

Unabhängig von der Auswahl einer geeigneten Vorgehensweise sollte verhindert werden, dass Inhalte von Wechseldatenträgern automatisch ausgeführt werden, wenn die Datenträger angeschlossen werden. Hierzu sind die entsprechenden *Autorun*- und *Autoplay*-Funktionen des Betriebssystems zu deaktivieren. Vertiefende Informationen hierzu sind in M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung* zu finden.

Damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden, müssen die Benutzer über die Gefährdung durch Laufwerke für Wechselmedien informiert und sensibilisiert werden.

Prüffragen:

- Wird verhindert, dass Inhalte von eingelegten Wechseldatenträgern automatisch ausgeführt werden?
- Werden technische Maßnahmen ergriffen, um das Booten von anderen als den vorgesehenen Quellen zu verhindern?
- Werden technische Maßnahmen ergriffen, um den unautorisierten Anschluß von externen Geräten und Datenträgern zu verhindern?
- Existiert eine Richtlinie, die den Umgang mit Wechselmedien und externen Datenspeichern regelt?
- Sind die Nutzer über alle Regelungen zum Umgang mit Laufwerken für Wechselmedien und externe Datenspeicher informiert?
- Werden technische Maßnahmen ergriffen, um den Missbrauch von Wechselmedien zu verhindern?

# M 4.5 Protokollierung bei TK-Anlagen

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

TK-Anlagen bieten in der Regel Möglichkeiten zur Protokollierung. Beispielsweise kann protokolliert werden, wer Dienste wie Telefon, Fax oder Datenübertragung nutzt und mit wem kommuniziert wird. Diese Informationen können erfasst, verarbeitet und gespeichert werden. Oft werden die Daten zu Abrechnungs- und Nachweiszwecken benutzt. Die protokollierten Informationen enthalten unter Anderem Einträge über:

- Zeit und Datum eines Gespräches oder einer Verbindung,
- Quell- und Zielrufnummer sowie die
- Gesprächsdauer.

Die Daten können mit der integrierten Verbindungsdatenerfassung intern ausgewertet oder auf entsprechende externe Systeme übertragen werden.

Da es sich um vertrauliche Daten handelt, müssen die Informationen auf allen Systemen und zusätzlich bei der Übermittlung geschützt werden. Es müssen entsprechende Vorkehrungen zum Schutz der Vertraulichkeit und Integrität getroffen werden. Beispielsweise könnten die Informationen über eine dedizierte Netzverbindung oder verschlüsselt über das LAN übertragen werden. Zusätzlich ist sicherzustellen, dass nur Berechtigte auf die gesicherten Daten zugreifen können. Es ist zu dokumentieren, welche Personen in welchen Rollen Zugriff auf die Verbindungsdaten haben.

Protokolliert werden sollten zusätzlich alle systemtechnischen Eingriffe, die Programmveränderungen beinhalten sowie Auswertungsläufe, Datenübermittlungen und Datenzugriffe.

**Administrationsarbeiten**

Alle Administrationsarbeiten an der TK-Anlage sollten protokolliert werden, um nachvollziehbar zu machen, von wem und auf welche Weise Einstellungen verändert wurden. Dazu ist es sinnvoll, dass bei der Authentisierung die Benutzer-Kennung, das Datum und die Uhrzeit sowie die erfolgte Anmeldung protokolliert werden. Bei einem erfolgten Zugriff sollten neben den schon bei der Authentisierung protokollierten Daten zusätzlich die Art des Zugriffs (lesend, schreibend) sowie durchgeführte Administrationstätigkeiten aufgezeichnet werden. Die Protokollierung muss übersichtlich, vollständig und korrekt sein.

Die Protokollierungsfunktion darf von Unbefugten nicht deaktiviert und nachträglich verändert werden können. Auch sollte ausgeschlossen sein, dass die Protokolldaten verändert werden können.

Die protokollierten Informationen sind regelmäßig zu kontrollieren. Gehäufte fehlerhafte Anmeldeversuche sollten gezielt untersucht werden. Bestehen auch bei erfolgreichen Anmeldungen Zweifel, sollten diese mit der Dokumentation durchgeführter Konfigurations- und Wartungsmaßnahmen verglichen werden. Bei Auffälligkeiten muss sofort entsprechend den für die IT bestehenden Regelungen für einen vermuteten Sicherheitsvorfall verfahren werden, bis ein Angriffsverdacht schlüssig widerlegt ist.

Da die Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (siehe M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Organisation abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

Prüffragen:

- Existiert eine Regelung für die Administration und Wartung der IT-Systeme?

# M 4.6 Revision der TK-Anlagenkonfiguration

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Revisor

Um die Sicherheit der TK-Anlagen zu gewährleisten, sind Revisionen der TK-Anlagenkonfiguration in regelmäßigen Abständen durchzuführen. Zur Revisionstätigkeit gehört speziell die Kontrolle der Tätigkeit der Systemverwaltung, des Wartungspersonals, des Ist-Zustands der TK-Anlage und der Einhaltung der datenschutzrechtlichen Vorschriften.

Jede Konfigurationsänderung, wie die Erteilung von Berechtigungen für einen Benutzer, sollte in eine Ist-Bestandsliste eingetragen werden. Diese Liste kann per Hand oder automatisiert geführt werden. In regelmäßigen Abständen, beispielsweise alle 6 Monate, sollte diese Ist-Bestandsliste zumindest stichprobenartig mit der Realität verglichen werden. Durch eine kontinuierliche Revision der Bestandsliste kann das angestrebte Sicherheits- und Datenschutzniveau sichergestellt werden. Werden Unstimmigkeiten festgestellt, sind diese mit Hilfe der Protokolle der TK-Anlage aufzuklären.

Es sollte beispielsweise kontrolliert werden, ob

- alle nicht vergebenen Rufnummern auch wirklich nicht eingerichtet sind,
- Rufnummern und Teilnehmer vollständig zugeordnet sind,
- verbotene Berechtigungen nirgendwo vergeben sind,
- deaktivierte Leistungsmerkmale und Kommunikationsschnittstellen sowie
- deaktivierte Dial-In-Funktionen auch wirklich inaktiv sind.

Ist es nicht gewünscht oder nicht möglich, die Rolle eines unabhängigen Revisors einzurichten, kann die Auswertung der Protokolldateien auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten des Administrators selbst nur schwer möglich ist. Zudem kann der Administrator möglicherweise Einblick in geschützte Daten (Anrufprotokolle) erhalten (siehe M 2.110 *Datenschutzaspekte bei der Protokollierung*). Das Ergebnis der Auswertung sollte daher zumindest dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen, besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Prüffragen:

- Werden Änderungen in der Konfiguration und den Leistungsmerkmalen der TK-Systeme nachvollziehbar dokumentiert?
- Existiert eine Regelung zur kontinuierlichen Überprüfung der TK-Systeme?
- Existiert eine Regelung zur Festlegung von Inhalten und Umfang der kontinuierlichen Überprüfungen?

# M 4.7 Änderung voreingestellter Passwörter

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Viele IT-Systeme, TK-Anlagen und Netzkoppelelemente (beispielsweise ISDN-Router, Sprach-Daten-Multiplexer etc.) besitzen nach der Auslieferung durch den Hersteller noch voreingestellte Standardpasswörter. Von Herstellern oder Administratoren voreingestellte Passwörter sind direkt nach der Installation, spätestens bei erstmaliger Inbetriebnahme von Hard- oder Software zu ändern. Hierbei sind die einschlägigen Regeln für Passwörter zu beachten (siehe M 2.11 *Regelung des Passwortgebrauchs*).

**Achtung**: Bei einigen TK-Anlagen werden vorgenommene Änderungen der Konfiguration nur im RAM abgelegt. Dies gilt auch für Passwortänderungen. Daher ist nach einer solchen Operation stets eine Datensicherung vorzunehmen und eine neue Sicherungskopie zu erstellen. Unterbleibt dies, so ist nach einem "Restart" der Anlage wieder das Standardpasswort gültig. Weiterhin sollte überprüft werden, ob nach Einrichten eines neuen Passworts das Standardpasswort tatsächlich seine Gültigkeit verloren hat und nicht weiterhin für den Systemzugang genutzt werden kann.

Prüffragen:

- Werden Standardpasswörter durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert, bevor IT-Systeme in Betrieb genommen werden?
- Wird überprüft, ob tatsächlich kein Systemzugang mit Standardpasswörtern oder schwachen Passwörtern möglich ist?

# M 4.8 Schutz des TK-Bedienplatzes

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.9 Einsatz der Sicherheitsmechanismen von X-Window

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Release 5 der X-Window-Software bietet nur wenige Maßnahmen, um die Sicherheit bei der Übertragung von Daten zwischen dem X-Server und dem X-Client zu erhöhen, so dass der Einsatz von X-Window-Software nur in einer sicheren Umgebung empfohlen werden kann.

- **Rechnerspezifische Zugriffskontrolle:** Auf jedem X-Server gibt es eine Liste zugelassener Rechner, die mit dem Befehl *xhost* verändert werden kann. Sie muss auf jeden Fall auf die Rechner beschränkt bleiben, die einen Zugriff auf den X-Server benötigen. Es sollte auf keinen Fall ein globaler Zugriff mit *xhost +* ermöglicht werden. Dies kann erreicht werden, indem explizit Rechner in der *xhost*-Tabelle eingetragen werden. Darüber hinaus ist zu beachten, dass jeder Benutzer auf einem der zugelassenen Rechner uneingeschränkten Zugriff auf den X-Server hat. Diese Art der Zugriffskontrolle kann deshalb nur dann empfohlen werden, wenn aus zwingenden Gründen keiner der folgenden Mechanismen eingesetzt werden kann.
- **Benutzerspezifische Zugriffskontrolle:** Der X-Server Prozess lässt sich so konfigurieren, dass bei einem Login (z. B. mit Hilfe von *xdm*) ein Schlüssel generiert wird, der zur Authentisierung bei einer Übertragung zwischen Client und Server benutzt wird. Dieser Schlüssel (*MAGIC COOKIE*) wird im Heimatverzeichnis des Benutzers in der Datei *.Xauthority* abgelegt und kann mit Hilfe des Befehls *xauth* an den X-Client übertragen werden. Während allerdings der *MIT-MAGIC-COOKIE*-Mechanismus nur als eine Art Passwort angesehen werden muss, das bei seiner Übertragung abgehört werden kann, bietet ein in Verbindung mit *NIS* angebotener und mit einer DES-Verschlüsselung arbeitender Mechanismus mehr Sicherheit und sollte deshalb bevorzugt werden.
- **Zugriffskontrolle über Secure Shell:** Die Kommunikation zwischen X-Client und X-Server kann auch über einen abgesicherten Kanal einer *ssh*-Verbindung erfolgen (siehe auch M 5.64 *Secure Shell*). Hierbei erfolgt sowohl eine rechnerbasierte als auch eine benutzerbasierte Zugriffskontrolle. Die Authentisierungs- und Nutzdaten werden verschlüsselt. Für einen sicheren Betrieb von X-Window wird die Nutzung von Secure Shell daher empfohlen.

Mit einem Zusatzprogramm können unter X-Window die Tastendrücke eines entfernten Rechners in Klarschrift übersetzt und eingesehen werden. Bei der Benutzung des Programms *xterm* kann das Weiterleiten von Tastendrücken verhindert werden, indem verhindert wird, dass *KeyPress*-Events, welche es bekommt, noch an andere Applikationen weitergeleitet werden. Dafür muss die *secure keyboard*-Option über das *xterm*-Menü eingeschaltet werden, so dass das entsprechende Fenster exklusiven Zugriff auf die Tastatur hat.

Prüffragen:

- Existiert eine Regelung zum sicheren Einsatz von X-Window?
- Existiert eine sichere Zugriffskontrolle auf den X-Server?
- Wird das Abhören von Tastatureingaben unter X-Window verhindert?

# M 4.10 Schutz der TK-Endgeräte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Benutzer, IT-Sicherheitsbeauftragter

TK-Anlagen bieten eine Vielzahl von Leistungsmerkmalen und Schnittstellen zu den Endgeräten. Je nach TK-Anlage können diese Merkmale oder Schnittstellen in unterschiedlicher Ausprägung oder unter anderer Bezeichnung vorkommen. Bestimmte Leistungsmerkmale müssen in der TK-Anlage selbst freigeschaltet werden, andere werden an den entsprechenden Endgeräten eingestellt.

Neben den TK-Anlagen können auch die Endgeräte zusätzlich zu der Anschlussmöglichkeit an die Telefonie-Verkabelung weitere Schnittstellen aufweisen. Dazu gehört unter anderem Bluetooth, um drahtlose Headsets zu verwenden, oder WLAN, mit dem ein drahtloses VoIP-Telefon an das LAN und mittelbar an die TK-Anlage angebunden wird. Ungenutzte Schnittstellen und nicht genutzte Leistungsmerkmale sind zu deaktivieren. Werden die Schnittstellen verwendet, so sind sie gegen unbefugten Zugriff mittels vorgeschalteter Authentisierung zu sichern.

Der Umfang der verfügbaren Leistungsmerkmale sollte auf das notwendige Minimum beschränkt und grundsätzlich nur die benötigten Leistungsmerkmale freigeschalten werden. Auf diese Weise wird verhindert, dass die Anlage über ihre Leistungsmerkmale unnötig möglichen Angriffen ausgesetzt wird. Bestimmte Leistungsmerkmale können zu gezielten Angriffen, insbesondere auf Vertraulichkeit oder Verfügbarkeit, missbraucht werden. Auch können im Zuge eines derartigen Missbrauchs vom Anlagenbesitzer ungewollte Gebühren entstehen.

Merkmale mit Missbrauchspotenzial an Endgeräten sind beispielsweise:

- das direkte Ansprechen bzw. die automatische Rufannahme, da mit dieser Funktion die Freisprechfunktionalität des Telefons zum Abhören des Raums missbraucht werden kann,
- der Amtszugang bei leicht zugänglichen Apparaten, da Unbefugte damit die Möglichkeit haben, Gespräche auf Kosten der Institution zu führen,
- die Rufumleitung, da beispielsweise durch versehentliche oder böswillige Fehlnutzung der Nutzer eines Telefonanschlusses nicht erreichbar ist,
- das Aufschalten, durch das ein Anrufer ein bestehendes Gespräch mithören kann,
- die Dial-In-Konferenzschaltung, da sich die Teilnehmer selbst in die Telefonkonferenz einwählen können, ohne das es weitere Teilnehmer mitbekommen und so Unbefugte mithören können und
- verschiedene, für den Export bestimmte Merkmale (z. B. "Zeugenschaltung" oder "Abhören"), da sie zu Angriffen auf die Vertraulichkeit nutzbar sind.

Die Endgeräte sollten im Rahmen ihrer vorgegebenen Möglichkeiten so konfiguriert werden, dass eine Warnung erfolgt, sobald sicherheitskritische Merkmale genutzt werden. Die nicht benötigten oder wegen ihres Missbrauchspotenzials als kritisch eingestuften Leistungsmerkmale müssen so weit wie möglich an der zentralen Anlage abgeschaltet werden. Bietet diese dafür nur eingeschränkte oder nicht ausreichend differenzierte Möglichkeiten, so können die zentralen Einstellungen mit entsprechenden Sperreinstellungen auf den Endgeräten kombiniert werden.

Zusätzliche Schutzmaßnahmen sollten für die auf den Endgeräten gespeicherten und abrufbaren vertraulichen Daten wie die Kontaktinformationen oder institutionsweite Telefonbücher, ergriffen werden. Dies gilt insbesondere für Endgeräte in ungeschützten Bereichen wie Besprechungsräumen oder Tiefgaragen. Teilweise ist es jedoch auch möglich, über die TK-Anlage selbst Berechtigungen für die entsprechenden Endgeräteanschlüsse zu vergeben.

Um zu verhindern, dass beispielsweise an frei zugänglichen Endgeräten unberechtigterweise Konfigurationsänderungen vorgenommen werden, sollten diese mit Passwörtern oder PINs geschützt werden.

Werksmäßig sind viele Endgeräte bereits mit Standard-Passwörtern oder PINs ausgestattet. Diese Standard-Passwörter sollten unbedingt bei der erstmaligen Inbetriebnahme geändert werden. Generell sollten Leistungsmerkmale, wie Rufumleitung, Heranholen von Anrufen oder ähnliches erst nach Eingabe der Authentisierungsinformationen am Gerät genutzt werden können. Um einen Missbrauch der Funktionen der Endgeräte zu verhindern, kann von der Möglichkeit des Passwortschutzes Gebrauch gemacht werden.

Da für diese Konfiguration der Endgeräte die Benutzer selbst verantwortlich sind, ist es wichtig, sie zu sensibilisieren und zu schulen (siehe M 3.82 *Schulung zur sicheren Nutzung von TK-Anlagen*).

Prüffragen:

- Wird der Zugang zu TK-Endgeräten mittels Passwort geschützt?

# M 4.11 Absicherung der TK-Anlagen-Schnittstellen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Die Schnittstellen einer TK-Anlage, über die Administrationstätigkeiten ausgeführt werden können, stellen schützenswerte Punkte dar. Sie sollten daher besonders abgesichert werden. Über unbenutzte oder ungesicherte Schnittstellen können von Unbefugten, etwa unter Zuhilfenahme eines Laptops, Manipulationen am System durchgeführt werden. Der Passwortschutz auf einen TK-Bedienplatz oder PC-Gateway wäre in einem solchen Fall wirkungslos. Ziel ist es also, dies zu verhindern, zumindest aber den Versuch erkennbar zu machen. Aus diesem Grund sollten die benutzten Schnittstellen gut verschraubt und ggf. zusätzlich verplombt werden. Unbenutzte Schnittstellen können durch verschraubte und verplombte Abschlusskappen gesichert werden.

Prüffragen:

- Werden nicht benötigte TK-Schnittstellen mit physischen Mechanismen geschützt?

# M 4.12 Sperren nicht benötigter TK-Leistungsmerkmale

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.13 Sorgfältige Vergabe von IDs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In Unix-Systemen werden anhand von Benutzer- und Gruppenkennungen von Prozessen und Dateien unter anderem Verursacher von Aktionen festgestellt und Rechte vergeben. Daher ist eine sorgfältige Vergabe dieser Kennungen erforderlich.

Jeder Login-Name, jede Benutzer-ID (UID) und jede Gruppen-ID (GID) darf nur einmal vorkommen. Auch nach dem Löschen eines Benutzers bzw. einer Gruppe sollen Login-Name und UID bzw. GID für eine bestimmte Zeit nicht neu vergeben werden. Bei vernetzten Systemen muss auch systemübergreifend darauf geachtet werden, dass Benutzernamen und IDs nicht mehrfach vergeben werden. Dies ist insbesondere bei der Verwendung von NFS wegen der Umsetzung der UIDs wichtig, damit keine Daten unberechtigt gelesen werden können.

Jeder Benutzer muss Mitglied mindestens einer Gruppe sein. Jede in der Datei */etc/passwd* vorkommende GID muss in der Datei */etc/group* definiert sein.

Jede Gruppe sollte nur die Benutzer enthalten, die unbedingt notwendig sind. Dieses ist insbesondere für die Systemgruppen (wie *root*, *sys*, *bin*, *adm*, *news*, *uucp*, *nuucp* oder *daemon*) wichtig.

Logins mit UID 0 (*Super-User*) dürfen außer für den Systemadministrator *root* nur für administrative Logins nach vorher festgelegten Regeln vergeben werden (siehe M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix*).

Es ist sinnvoll, für Login-Namen und UIDs bzw. GIDs Namenskonventionen festzulegen. Weiterhin sollte regelmäßig überprüft werden, ob alle UIDs plausibel sind. Sie sollten also z. B. nur aus Ziffern stehen bzw. keine ungültigen Kombinationen wie 00 oder 000 enthalten.

Die Dateien */etc/passwd* und */etc/group* sollten nicht mit Editoren bearbeitet werden, da Fehler die Systemsicherheit stark beeinträchtigen können. Es sollten ausschließlich die entsprechenden Administrationstools benutzt werden, die allerdings sehr systemspezifisch sind.

Prüffragen:

- Ist sichergestellt, dass unter Unix die Benutzer- und Gruppenkennungen sorgfältig vergeben werden?
- Ist unter Unix jeder Benutzer Mitglied einer Gruppe?
- Ist unter Unix jede in der Datei /etc/passwd vorkommende GID in der Datei /etc/group definiert?
- Enthalten unter Unix alle Gruppen nur die notwendigen Benutzer?

# M 4.14 Obligatorischer Passwortschutz unter Unix

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Passwortschutz für jeden Account auf einem Unix-Rechner stellt sicher, dass nur ein berechtigter Benutzer sich unter seinem Login-Namen einloggen kann, indem nach Eingabe des Login-Namens eine Authentisierung durch Eingabe des Passworts erfolgt.

Bei der Verwendung von Passwörtern für Benutzer und Gruppen sind die unter M 2.11 *Regelung des Passwortgebrauchs* beschriebenen Regeln zu beachten. Es muss beachtet werden, dass bei einigen Systemen nur eine begrenzte Zeichenanzahl bei der Passwort-Prüfung berücksichtigt wird. Zur Realisierung dieser Maßnahmen sollten nur Programmversionen von *passwd*, die die Einhaltung dieser Regeln sicherstellen, oder administrative Maßnahmen, z. B. Shellskripts und entsprechende *cron*-Einträge, benutzt werden.

Als weitere Möglichkeit kann auch das Unix-Standard-Kommando *passwd* durch andere Passwort-Programme mit erweiterter Funktionalität ersetzt werden. Dazu gehören auch die Public-Domain-Programme *anlpasswd*, *npasswd* und *passwd+*, die bereits beim Ändern des Passwortes durch den Benutzer das neu gewählte Passwort auf seine Güte testen und zurückweisen, wenn dieses zu schwach ist. Sie sind z. B. über den FTP-Server *ftp://ftp.cert.dfn.de/pub/tools/password/* erhältlich.

Die Passwörter sollen nicht in der allgemein lesbaren Datei */etc/passwd*, sondern in einer für die Benutzer nicht lesbaren *shadow*-Passwortdatei gespeichert sein. In jedem neueren Unix-System ist diese *shadow*-Möglichkeit enthalten, aber leider nach einer Erstinstallation nicht immer aktiviert (so muss z. B. unter RedHat Linux nach der Standardinstallation die Verwendung der *shadow*-Passwortdatei mit dem Befehl *pwconv* aktiviert werden).

Die Datei */etc/passwd* ist regelmäßig auf Benutzer-Kennungen ohne Passwort zu untersuchen. Wird eine solche gefunden, ist der Benutzer zu sperren. Ist für Gruppen Passwortzwang vereinbart worden, so ist entsprechend die Datei */etc/group* zu prüfen. Es empfiehlt sich jedoch, für Gruppen keine Passwörter zu vergeben und für jede Gruppe nur so wenig Benutzer wie möglich einzutragen. Das Wechseln zwischen Gruppen, in denen der Benutzer eingetragen ist, wird dadurch erleichtert, und unberechtigtes Wechseln durch systematisches Ausprobieren von Passwörtern mit Hilfe entsprechender Programme ist nicht möglich.

Alle Logins, insbesondere diejenigen mit UID 0, sollten regelmäßig auf das Vorhandensein und die Güte von Passwörtern getestet werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs* und M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*). Neben den in M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems* beschriebenen Programmen können diese Logins auch z. B. mit

```
awk -F: '{if ($3=="0") print $1}' /etc/passwd
awk -F: '{if ($2=="") print $1}' /etc/passwd
```

ermittelt werden.

Prüffragen:

- Ist sichergestellt, dass alle akzeptierten Zeichen bei der Passwort-Prüfung berücksichtigt werden?
- Werden schwache Passwörter vom IT-System zurückgewiesen?
- Sind die Passwörter in einer für die Benutzer nicht lesbaren shadow-Passwortdatei hinterlegt?
- Wird die Datei /etc/passwd regelmäßig auf Benutzerkennungen ohne Passwort geprüft?

# M 4.15 Gesichertes Login

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es sollte ein Login-Programm verwendet bzw. Optionen aktiviert werden, so dass die folgenden Maßnahmen durchgeführt werden können:

- Jeder Benutzer muss eine eigene Kennung und ein eigenes Passwort erhalten. Es darf kein Zugang ohne Kennung oder Passwort möglich sein. Als Passwort-Ersatz kann die Authentisierung des Benutzers auch über elektronische Signaturen, Pass-Tickets oder Ähnliches erfolgen.
- Die Anzahl erfolgloser Login-Versuche wird beschränkt. Nach jedem erfolglosen Login-Versuch vergrößert sich die Wartezeit bis zur nächsten Login-Aufforderung. Nach einer bestimmten Anzahl von Fehlversuchen wird die betroffene Benutzer-Kennung und / oder das Terminal gesperrt. Dabei ist zu bedenken, dass dadurch nicht der Administrator ausgesperrt werden darf, es muss ihm an der Konsole eine Zugangsmöglichkeit offen bleiben.
- Der Zeitpunkt des letzten erfolgreichen Logins wird dem Benutzer beim Login gemeldet.
- Erfolglose Login-Versuche werden dem Benutzer beim Login gemeldet. Eventuell sollte diese Meldung bei mehreren darauf folgenden Anmeldungen wiederholt werden.
- Der Zeitpunkt des letzten Logouts wird dem Benutzer beim Login gemeldet. Hierbei wird zwischen Logouts zu einem interaktiven Login und solchen zu einem nicht-interaktiven Login (Logout von Hintergrundprozessen) unterschieden.
- Für das Login über Netze, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die zusätzliche Verwendung von Einmalpasswörtern (siehe auch M 5.34 *Einsatz von Einmalpasswörtern*).

Spezielle Hinweise zur Absicherung des Login-Vorgangs unter z/OS finden sich in der Maßnahme M 4.213 *Absichern des Login-Vorgangs unter z/OS*.

Prüffragen:

- Gibt es Regelungen zum Schutz des Zugangs zu IT-Systemen?
- Werden alle erforderlichen Maßnahmen umgesetzt, die den Zugang zu IT-Systemen absichern?

# M 4.16 Zugangsbeschränkungen für Benutzer-Kennungen und / oder Terminals

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Werden stationäre IT-Systeme, die sich in Räumen befinden, die außerhalb von festgelegten Arbeitszeiten nicht zugänglich sind, nachts oder am Wochenende genutzt, kann dies ein Indiz für eine unberechtigte Benutzung sein. Um dies zu vermeiden, sollte überlegt werden, diese IT-Systeme und / oder die zugehörigen Benutzer-Kennungen außerhalb der offiziellen Arbeits- oder Nutzungszeiten zu sperren. Soweit das nicht mit vertretbarem Aufwand möglich ist (zum Beispiel bei sehr unregelmäßigen oder häufig wechselnden Arbeitszeiten), sollte die Sperrung zumindest zu den Zeiten erfolgen, die grundsätzlich außerhalb der Arbeits- oder Nutzungszeiten liegen.

Falls Mitarbeiter nur an bestimmten IT-Systemen innerhalb des LANs arbeiten, so sollten sie sich auch nur an diesen IT-Systemen anmelden können, also die Benutzer-Kennungen auf diese IT-Systeme beschränkt werden.

Unter Unix ist für Terminals der jeweilige Benutzer als Eigentümer des entsprechenden Gerätetreibers einzutragen. Sobald dieser sich ausgeloggt hat, sollte automatisch wieder *root* Eigentümer werden. Nur der jeweilige Benutzer sollte hierfür Leseberechtigung haben. Falls ein Benutzer Nachrichten (z. B. mit *talk*) von anderen Systembenutzern empfangen möchte, muss er ihnen Schreibberechtigung für den Gerätetreiber einräumen. Es ist zu überprüfen, ob dies unbedingt notwendig ist.

Oft kann die Anzahl von gleichzeitigen Anmeldungen unter einem Account von mehreren unterschiedlichen IT-Systemen aus beschränkt werden. Zum Schutz vor dem unbemerktem Eindringen von Angreifern sollte verhindert werden, dass sich ein Benutzer an mehreren IT-Systemen gleichzeitig anmelden kann.

Prüffragen:

- Wurden Zeitfenster, d. h. temporäre Zugangsbeschränkungen, für alle Accounts und Terminals eingerichtet?

# M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Accounts, die über einen längeren Zeitraum nicht benutzt werden, sollten gesperrt und später gelöscht werden. Wenn beim Löschen von Accounts Dateien übrig bleiben, die keinem existierenden Benutzereintrag mehr zugeordnet sind, besteht die Gefahr, dass diese Dateien später eingerichteten Benutzern unberechtigt zugeordnet werden.

Beim Entfernen von Benutzern sind unter Unix die entsprechenden Einträge in */etc/passwd*, */etc/group* und das Heimatverzeichnis des Benutzers zu löschen. Ebenso ist darauf zu achten, dass weitere Benutzereinträge in Dateien wie */etc/hosts*, *shadow*, u. a. gelöscht werden. Die Daten des Heimatverzeichnisses sollten vorher gesichert werden. Bei der Sperrung bzw. auf jeden Fall vor dem Löschen eines Accounts sollte der betroffene Benutzer informiert werden. Beim Löschen von Accounts ist darauf zu achten, dass auch die Dateien des Benutzers gefunden werden, die nicht in seinem Heimatverzeichnis liegen. Dies kann z. B. mit dem Programm *find* und der Option *-uid* erfolgen. Solche Dateien müssen gelöscht oder anderen Benutzern zugeordnet werden. Weiterhin ist darauf zu achten, dass laufende Prozesse und noch anstehende Aufträge gelöscht werden, z. B. unter Unix in der *crontab*.

Ebenso sollten Terminals, die über einen längeren Zeitraum nicht benutzt werden, gesperrt und später entfernt werden.

Unter Unix sind vom System vorgegebene Logins (z. B. *sys*, *bin*, *adm*, *uucp*, *nuucp*, *daemon* und *lp*), die nicht benötigt werden, zu sperren, indem in das zugehörige Passwortfeld in der Datei */etc/passwd* z. B. "LOCKED" eingetragen wird.

Wenn ein neu einzurichtender Benutzer seinen Account nur für einen begrenzten Zeitraum benötigt, sollte dieser nur befristet eingerichtet werden.

Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z. B. jährlich) bei Bedarf zu verlängern.

Ist absehbar, dass ein Benutzer eines lokalen Netzes längere Zeit abwesend ist (Urlaub, Krankheit, Abordnung, ...), so sollte sein Account für diese Zeit im Netz-Server gesperrt werden, so dass das Arbeiten unter seiner Benutzer-Kennung für diese Zeit nicht mehr möglich ist. Jeder Benutzer sollte dem Netzadministrator Zeiten längerer Abwesenheit mitteilen.

Prüffragen:

- Existieren Reglungen zum Identifizieren, Löschen und Sperren von befristet unbenutzten bzw. nicht mehr benötigten Accounts?
- Existiert eine Regelung, um alle Dateien und Verzeichnisse gesperrter und gelöschter Accounts anderen Benutzern zuzuordnen oder zu löschen?
- Existiert eine Regelung zur zeitlichen Befristung von Accounts und Zugangsmerkmalen?

# M 4.18 Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um das Aktivieren des Monitor-Modus und das Booten in den Single-User-Modus zu verhindern, sollten folgende Maßnahmen ergriffen werden:

- Wenn es (abhängig von der Unix-Variante und der zugrunde liegenden Hardware) möglich ist, muss zum Schutz des Unix-Servers ein BIOS-Passwort vergeben werden.
- Beim Booten in den Single-User-Modus sollte das Super-User-Passwort abgefragt werden, um Unberechtigten den Zugang zum Unix-Server zu erschweren.
- Wenn Tastaturschlösser vorhanden sind, sollten diese zum Schutz der Systemkonsole benutzt werden, um den Zugang zum Monitor-Modus zu verhindern.

Diese Maßnahme wird ergänzt durch die Maßnahme M 4.21 *Verhinderung des unautorisierten Erlangens von Administratorrechten*.

Prüffragen:

- Ist der Zugang zum Monitor- und Single-User-Modus angemessen abgesichert?
- Wird beim Booten in den Single-User-Modus das Super-User-Passwort abgefragt?

# M 4.19 Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die hier genannten Maßnahmen gelten für Dateien und Verzeichnisse, für die der Administrator zuständig ist, das heißt für solche, die entweder für alle Benutzer von Bedeutung sind oder die Administrationszwecken dienen. Es reicht nicht aus, die Rechte eines Programms zu überprüfen, es muss auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden (insbesondere zur Vermeidung Trojanischer Pferde).

Die Attribute aller Systemdateien sollten möglichst so gesetzt sein, dass nur der Systemadministrator Zugriff darauf hat. Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

Das s-Bit sollte nur gesetzt sein, wenn unbedingt erforderlich. Bei Shellskripts soll das s-Bit nicht gesetzt sein. Das s-Bit darf nur vom Administrator gesetzt werden, die Notwendigkeit hierfür ist zu begründen und zu dokumentieren.

In Verzeichnissen, in denen alle Benutzer Schreibrechte haben müssen (z. B. */tmp*), sollte das t-Bit (Sticky-Bit) gesetzt sein.

Die Integrität aller bei Unix-Systemdateien und -verzeichnissen gesetzten Attribute sollte regelmäßig verifiziert werden, z. B. mit *Tripwire* (siehe auch M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*).

Prüffragen:

- Werden im Rahmen der Rechtevergabe unter Unix auch indirekt aufgerufene Programme überprüft?
- Sind die Attribute der Systemdateien und -verzeichnisse restriktiv gesetzt?
- Ist das s-Bit nur dort gesetzt, wo es nachvollziehbar erforderlich ist?
- Wird die Rechte- bzw. Attributvergabe bei Systemdateien und -verzeichnissen regelmäßig überprüft?

# M 4.20 Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die hier genannten Maßnahmen gelten für Dateien und Verzeichnisse eines Benutzers (inkl. Mail-Dateien).

Die Benutzer sollten die Attribute ihrer Dateien und Verzeichnisse so setzen, dass andere Benutzer nicht darauf zugreifen können. Wenn anderen Benutzern der Zugriff erlaubt werden soll, sollten entsprechende Benutzergruppen eingerichtet werden. Für benutzerspezifische Konfigurationsdateien wie *.profile*, *.exrc*, *.login*, *.cshrc* sollte nur der jeweilige Eigentümer Rechte besitzen.

Auf Unix-Systemen haben diverse Programme benutzerspezifische Konfigurationsdateien wie *.exrc*, *.emacs* oder *.mailrc*, die nach Programmaufruf automatisch durchlaufen werden und Variablen und Optionen für den Benutzer setzen. Damit in diesen keine trojanischen Pferde installiert werden können, sollte nur der jeweilige Eigentümer Zugriffsrechte besitzen. Die Datei *.exrc* wird gelesen, bevor die Editoren *ex* oder *vi* gestartet werden. Falls sich eine gleichnamige Datei im aktuellen Verzeichnis befindet, wird diese bei einigen Unix-Versionen ausgewertet. Alle eingesetzten Unix-Versionen müssen daraufhin überprüft werden, da damit auch die Ausführung von Betriebssystemkommandos bei jedem Editoraufruf möglich ist.

Das s-Bit sollte nur gesetzt sein, wenn unbedingt erforderlich. Bei Shellskripts soll das s-Bit nicht gesetzt sein. Das s-Bit sollte nur nach Einbeziehung des Administrators gesetzt werden, die Notwendigkeit hierfür ist zu begründen und zu dokumentieren.

### *umask*

Mit *umask* (user file creation mode mask) wird für jeden Benutzer festgelegt, welche Attribute zur Regelung der Zugriffsrechte eine von ihm neu angelegte Datei erhält. In den benutzerspezifischen Konfigurationsdateien wie */etc/profile* oder den *$HOME/.profile*-Dateien sollte *umask* = 0027 (-rw-r-----) oder *umask* = 0077 (-rw-------) eingestellt sein, damit die Dateiattribute für neu angelegte Dateien nur dem Erzeuger (und evtl. der Gruppe) Zugriffsrechte geben.

### Mail-Dateien

Die Attribute der Mail-Dateien sollten regelmäßig daraufhin überprüft werden, ob nur der jeweilige Eigentümer auf die Dateien Zugriff hat. Die Integrität der bei den Unix-Benutzerdateien und -verzeichnissen gesetzten Attribute sollte regelmäßig verifiziert werden, z. B. mit *Tripwire* (siehe auch M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*).

Prüffragen:

- Wissen die Benutzer, dass sie die Attribute von Dateien und Verzeichnissen so setzen sollten, dass Fremdzugriffe durch andere Benutzer verhindert werden?
- Haben auf benutzerspezifische Konfigurationsdateien (zum Beispiel .profile, .exrc) nur die jeweiligen Eigentümer Rechte?

- Sind die benutzerspezifischen Konfigurationsdateien so eingestellt (umask), dass die Dateiattribute für neu angelegte Dateien nur dem Erzeuger (und evtl. der Gruppe) Zugriffsrechte geben?
- Wird die Rechte- bzw. Attributvergabe bei Benutzerdateien und -verzeichnissen regelmäßig überprüft?

# M 4.21 Verhinderung des unautorisierten Erlangens von Administratorrechten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Durch den Befehl *su* kann jeder Benutzer Super-User-Rechte erlangen, wenn er das entsprechende Passwort besitzt. Da die Anzahl fehlerhafter Versuche bei *su* nicht beschränkt ist, besteht ein erhöhtes Risiko, dass das Passwort durch systematisches Probieren mit Hilfe entsprechender Programme herausgefunden wird. Deshalb sollte *su* nur für den Super-User zugänglich sein. Alternativ könnte ein modifiziertes *su* installiert werden, bei dem die Anzahl erfolgloser Versuche beschränkt ist, sich die Wartezeit bis zur nächsten *su*-Aufrufmöglichkeit nach jedem erfolglosen Login-Versuch vergrößert und nach einer bestimmten Anzahl von Fehlversuchen die Ausführmöglichkeit und / oder das Terminal gesperrt wird. Jede Verwendung des Befehls *su* sollte protokolliert werden.

Wenn das System es zulässt, kann der Login-Name des Super-Users anders als *root* genannt werden. Als zusätzliche Super-User-Logins sollten aber nur administrative Logins (siehe M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix*) geschaffen werden.

Der Administrator darf nur von der Konsole aus arbeiten, um zu verhindern, dass bei einem Abhören der Leitung sein Passwort bekannt wird. Unter Solaris kann dies beispielsweise erreicht werden, indem die Datei */etc/default/login* entsprechend konfiguriert wird. Alternativ können Sicherheitsfunktionen verwendet werden, die das Ausspähen von Administratorpasswörtern verhindern. Beispiele für geeignete Mechanismen sind Secure Shell (siehe Maßnahme M 5.64 *Secure Shell*) und Einmalpasswörter (siehe Maßnahme M 5.34 *Einsatz von Einmalpasswörtern*).

Bei BSD-Unix kann sich *root* nur an Terminals einloggen, die in der Datei */etc/ttytab* als *secure* gekennzeichnet sind. Ist diese Option für alle Terminaleinträge entfernt, kann sich ein Administrator an einem Terminal nur mit dem Kommando *su* als *root* einloggen. Es sollte überlegt werden, eine Benutzergruppe einzurichten, auf die die Ausführung des Kommandos *su* beschränkt ist.

Ist bei BSD-Unix die Konsole in der Datei */etc/ttytab* als *secure* gekennzeichnet, wird kein Passwort beim Hochfahren in den Single-User-Modus abgefragt, daher muss dieser Eintrag unbedingt entfernt werden.

Die Datei */etc/ftpusers* enthält die Login-Namen, die sich nicht per ftp anmelden dürfen. Bei ftp werden die Passwörter über eine ungeschützte Klartextverbindung übertragen. Daher sollten administrative Zugänge (*root, bin, daemon, sys, adm, lp, smtp, uucp, nuucp, etc.*) hier eingetragen werden. Bei einigen Standardinstallationen steht root nicht in dieser Datei.

Wenn ein Benutzer bzw. ein Benutzer-Programm eine Super-User-Datei (Dateien mit Eigentümer root und gesetztem s-Bit) ausführt, erhält dieser Benutzer bzw. dieses Programm bei der Ausführung Super-User-Rechte. Das ist für bestimmte Anwendungen erforderlich, kann aber unter Umständen auch missbräuchlich benutzt werden. Deshalb ist darauf zu achten, dass nur die notwendigsten Programmdateien Super-User-Dateien sind und keine weiteren Super-User-Dateien von Dritten hinzugefügt werden.

**Automatisches Mounten von Geräten für austauschbare Datenträger:**

Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann ein Benutzer Super-User-Rechte erlangen. Automatisches Mounten sollte daher restriktiv gehandhabt werden. Manche Unix-Versionen bieten eine Option des *mount*-Befehls, der dazu führt, dass das s-Bit für das entsprechende Filesystem ignoriert wird. Bei austauschbaren Datenträgern sollte überlegt werden, diese Option anzuwenden.

Bei der Freigabe von Verzeichnissen, die von anderen Rechnern gemountet werden dürfen, sind die unter M 5.17 *Einsatz der Sicherheitsmechanismen von NFS* beschriebenen Einschränkungen zu beachten. Es sollten insbesondere keine Verzeichnisse mit *root*-Rechten und nur bei Bedarf Verzeichnisse mit Schreibrechten freigegeben werden.

Diese Maßnahme wird ergänzt durch die Maßnahme M 4.18 *Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus*.

Prüffragen:

- Ist der su-Befehl auf die Super-User-Rolle beschränkt oder so modifiziert, dass er die Anzahl erfolgloser Login-Versuche beschränkt bzw. die Wartezeit zwischen den Versuchen erhöht?
- Wird jede Verwendung des su-Befehls protokolliert?
- Wird über angemessene Sicherheitsmechanismen das Ausspähen von Administratorpasswörtern verhindert (z. B. Leitungsverschlüsselung, Einmalpasswörter)?
- Wird (per /etc/ftpusers) verhindert, dass sich administrative Zugänge (z. B.. root) per ftp anmelden können?
- Wird die unautorisierte Ausführung von Super-User-Dateien verhindert?

# M 4.22 Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Mit Unix-Befehlen wie *ps*, *finger*, *who, last* lassen sich Informationen über einen Benutzer (z. B. Arbeitsverhalten) ermitteln. Viele Unix-Derivate enthalten dazu noch weitere Befehle wie z. B. *listusers* unter Solaris. Es ist zu überlegen, ob das Ausführen dieser Befehle für jeden Benutzer erlaubt sein soll (Datenschutz, Ausspähen von Login-Namen und Ähnlichem). Im Zweifelsfall sollte der Zugriff auf diese Befehle beschränkt werden.

Beim Aufruf von Kommandos dürfen keine sensitiven Informationen als Parameter mit eingegeben werden, wie z. B. ein Passwort, da andere Benutzer mit *ps* diese Angaben sehen können.

Die Protokolldateien wie *wtmp, utmp, wtmpx, utmpx,* etc. sollten nach Möglichkeit durch geeignete Zugriffsrechte vor unbefugtem Auslesen geschützt werden, da hieraus eine Vielzahl von Informationen über die Benutzer herausgelesen werden kann.

Prüffragen:

- Hat die Institution festgelegt, wie mit Unix-Befehlen umgegangen wird, über die Benutzerverhalten ermittelt werden kann (z. B. ps, finger, who, last, listusers)?
- Wird verhindert, dass sensitive Informationen (z. B.. Passwörter) als Kommandoparameter übergeben werden?
- Werden Protokolldateien (z. B. wtmp, utmp, wtmpx, utmpx, etc.) durch eingeschränkte Zugriffsrechte vor unbefugtem Auslesen geschützt?

# M 4.23 Sicherer Aufruf ausführbarer Dateien

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Ausführbare Dateien können direkt gestartet werden. Im Gegensatz hierzu können Anwendungsdaten, wie Textdateien, nur über ein entsprechendes Programm angesehen werden. Unter Windows sind ausführbare Dateien an ihrer Dateiendung (beispielsweise .exe, .com, .vbs, .bat, .cmd) und unter Unix durch Dateirechte (x-Flag) erkennbar.

Es muss sichergestellt werden, dass nur freigegebene Versionen ausführbarer Dateien und keine eventuell eingebrachten modifizierten Versionen (insbesondere Trojanische Pferde) aufgerufen werden (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Ein Angreifer könnte eine ausführbare Datei soweit verändern, dass er die Privilegien des Benutzers erhält, der die Datei ausführt. Um dies zu verhindern, dürfen ausführbare Dateien nur lesbar sein. Ein Schreibzugriff darf nur Administratoren gestattet werden.

Ausführbare Dateien für die Schreibrechte benötigt werden, z. B. weil sie sich in der Entwicklung befinden, dürfen nur in separaten Bereichen verwendet werden. Dasselbe gilt für neue Software, die für einen späteren Einsatz auf einem Produktivsystem getestet werden soll. Hierfür können beispielsweise separate Testsysteme eingesetzt werden oder spezielle Benutzerkonten ohne weitere Privilegien. Nur so kann verhindert werden, dass diese Applikationen Schaden anrichten.

Auch bereits getestete Software kann die Sicherheit beeinträchtigen. Dies betrifft vor allem sehr komplexe Anwendungen wie zum Beispiel Webserver. Schon beim Start von Anwendungen muss sichergestellt werden, dass jeder Prozess nur so viele Rechte erhält wie unbedingt notwendig sind. So kann bei einem erfolgreichen Angriff der eintretende Schaden begrenzt werden. Diese Dienste dürfen, wenn möglich, nicht mit Administrator-Rechten gestartet werden. Hierfür eignen sich ebenfalls Benutzerkonten mit eingeschränkten Privilegien. Über klare Trennungen von Rechten, unter Unix oder Linux beispielsweise durch *chroot*-Umgebungen, die den eintretenden Schaden begrenzen können, muss nachgedacht werden.

Im Weiteren muss sichergestellt werden, dass nur die gewünschte, freigegebene Version ausgeführt werden kann. Ein Angreifer könnte sonst eine modifizierte Datei mit dem selben Namen in ein Verzeichnis kopieren, auf das er Schreibrechte hat. Wird beim Aufruf in den Verzeichnissen nach der Datei gesucht, könnte die modifizierte statt die gewünschte Datei ausgeführt werden.

Bei vielen Betriebssysteme werden die Verzeichnisse, in denen nach den ausführbaren Dateien gesucht werden soll, in der entsprechenden Reihenfolge in der *PATH*-Variable eingetragen. Die Anzahl der angegebenen Verzeichnisse sollte gering und überschaubar gehalten werden. Relative Verzeichnisangaben, die das jeweils aktuelle Arbeitsverzeichnis enthalten, dürfen als Angabe in der *PATH*-Variable nicht enthalten sein. Ausführbare Dateien sollen nur in dafür vorgesehenen Verzeichnissen gespeichert sein. In den in einer *PATH*-Variable enthaltenen Verzeichnissen darf nur der jeweilige Eigentümer Schreibrechte erhalten. Dies muss regelmäßig überprüft werden.

Prüffragen:

- Ist sichergestellt, dass nur freigegebene Versionen ausführbarer Dateien zum Einsatz kommen?
- Ist der Schreibzugriff auf ausführbare Dateien nur Adminstratoren gestattet, während Benutzer nur Lesezugriff erhalten?
- Erhalten Prozesse beim Start der Anwendung nur die unbedingt notwendigen Rechte?
- Werden in den PATH-Variablen nur absolute Verzeichnisangaben verwendet?
- Sind ausführbare Dateien nur in dafür vorgesehenen Verzeichnissen gespeichert?
- Werden die PATH-Einträge regelmäßig überprüft?

# M 4.24 Sicherstellung einer konsistenten Systemverwaltung

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In vielen komplexen IT-Systemen, z. B. unter Unix oder in einem Netz, gibt es eine Administratorrolle, die keinerlei Beschränkungen unterliegt. Unter Unix ist das der Super-User *root,* in einem Novell-Netz der *SUPERVISOR* bzw. *admin*. Durch fehlende Beschränkungen ist die Gefahr von Fehlern oder Missbrauch besonders hoch.

Um Fehler zu vermeiden, soll unter dem Super-User-Login nur gearbeitet werden, wenn es notwendig ist; andere Arbeiten soll auch der Administrator nicht unter der Administrator-Kennung erledigen. Insbesondere dürfen keine Programme anderer Benutzer unter der Administrator-Kennung aufgerufen werden. Ferner sollte die routinemäßige Systemverwaltung (zum Beispiel Backup, Einrichten eines neuen Benutzers) nur menügesteuert durchgeführt werden können.

Durch Aufgabenteilung, Regelungen und Absprache ist sicherzustellen, dass Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Zum Beispiel darf eine Datei nicht gleichzeitig von mehreren Administratoren editiert und verändert werden, da dann nur die zuletzt gespeicherte Version erhalten bleibt.

Wenn die Gefahr des Abhörens von Leitungen zu Terminals besteht, sollte der Administrator nur an der Konsole arbeiten, damit keine Passwörter abgehört werden können. Bei der Administration von Unix-Systemen kann eine verschlüsselte Kommunikation mit dem Protokoll Secure Shell erfolgen. Hiermit ist eine gesicherte Administration von entfernten Arbeitsstationen aus möglich (siehe auch M 5.64 *Secure Shell*).

Für alle Administratoren sind zusätzliche Benutzer-Kennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, sollen die Administratoren ausschließlich diese zusätzliche Benutzer-Kennungen verwenden.

Alle durchgeführten Änderungen sollten dokumentiert werden, um diese nachvollziehbar zu machen und die Aufgabenteilung zu erleichtern (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*). Für die nachträgliche Überprüfung durchgeführter Administratortätigkeiten kann mit dem Unix-Befehl *script* ein Protokoll der eingegebenen Befehle angefertigt werden. Dieser Befehl protokolliert die gesamte Terminal-Sitzung in einer ASCII-Datei. Solch eine Datei kann dann bei Bedarf einem elektronischen oder ausgedruckten Administrations-Journal beigefügt werden.

Prüffragen:

- Werden alle nötigen Vorgaben zur Sicherstellung einer konsistenten Systemverwaltung umgesetzt?
- Werden administrative Tätigkeiten und Systemeingriffe dokumentiert?

# M 4.25 Einsatz der Protokollierung im Unix-System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Protokollmöglichkeiten des einzelnen Unix-Systems sind einzusetzen und gegebenenfalls durch Programme oder Shellskripts zu ergänzen.

Folgende Maßnahmen sollen ergriffen werden:

- Die Protokoll-Dateien müssen regelmäßig ausgewertet werden. Die Auswertung sollte nicht immer zum selben Zeitpunkt erfolgen, um zu verhindern, dass ein Angreifer diese Tatsache ausnutzt. Wenn z. B. der Administrator jeden Tag um 17.00 Uhr die Systemaktivitäten überprüft, kann ein Angreifer um 18.00 Uhr unbemerkt tätig werden.
- Je nach Art der protokollierten Ereignisse kann es erforderlich sein, schnellstmöglich einzugreifen. Damit der Administrator über solche Ereignisse (z. B. Protokolldatei zu groß, wichtige Serverprozesse abgebrochen, mehrfach versuchte *root*-Logins während ungewöhnlicher Tageszeiten, etc.) automatisch informiert wird, sollten halbautomatische Logfileparser für die Alarmierung eingesetzt werden (z. B. *swatch*, *logsurfer* oder *checksyslog*).
- Soweit erforderlich, sollten die Protokolldateien gesichert werden, bevor sie zu groß oder vom System gelöscht werden. Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen beachtet werden müssen.
- Informationen aus Dateien wie *wtmp*, *utmp*, *wtmpx*, *utmpx*, etc. sollten mit Skepsis betrachtet werden, da diese Dateien leicht zu manipulieren sind.
- Die Datei-Attribute der Protokolldateien sollten so gesetzt sein, dass Unberechtigte keine Änderungen oder Auswertungen der Protokolle vornehmen können.
- Folgende Protokolldateien sollten mindestens erstellt und kontrolliert werden: Logins (auch Fehlversuche), Aufruf von *su*, Fehlerprotokollierungsdatei / Protokollierung wichtiger Vorgänge (*errorlog*), Administratortätigkeiten (insbesondere von *root* ausgeführte Befehle). Weitere Einzelheiten finden sich in M 4.106 *Aktivieren der Systemprotokollierung*.
  Der Befehl *last* zeigt Login- und Logout-Informationen wie Zeitpunkt und Terminal für jeden Benutzer an. Der Administrator sollte mit diesem Befehl regelmäßig überprüfen, ob sich Benutzer auf ungewöhnlichem Weg anmelden, z. B. über Modemleitungen oder über FTP.

Wenn auf vielen Systemen Protokolldaten anfallen sollten, empfiehlt sich der Einsatz eines dedizierten Loghosts, der besonders abgesichert ist. Das Weiterleiten (Forward) der Syslog-Meldungen auf diesen Loghost muss in der Syslog-Konfigurationsdatei aktiviert werden (siehe M 4.106 *Aktivieren der Systemprotokollierung*.

Die anfallenden Protokolldaten dürfen nur benutzt werden, um die ordnungsgemäße Anwendung der IT-Systeme zu kontrollieren, nicht für andere Zwecke, insbesondere nicht zur Erstellung von Leistungsprofilen von Benutzern (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Prüffragen:

- Existiert eine Regelung zur Festlegung von protokollierenden Ereignissen (z. B. erfolgreicher Login, nicht erfolgreicher Login, Aufruf von su,

Protokollierung wichtiger Vorgänge, errorlog, administrative Tätigkeiten/ Befehle unter root)?
- Werden die Protokolldateien regelmäßig ausgewertet?
- Werden Tools (Logfileparser) zur halbautomatisierten Auswertung und Alarmierung bei protokollierten Ereignissen eingesetzt?
- Wird die Einhaltung von gesetzlichen und/oder vertraglichen Aufbewahrungsfristen von Protokolldateien gewährleistet?
- Wird ein dedizierter und besonders gesicherter Loghost für Protokolldaten eingesetzt?
- Werden die Protokolldaten der Systeme im Push-Verfahren an den Loghost übertragen?
- Entspricht die Protokollierung den geltenden Datenschutzbestimmungen?

# M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Unix-Betriebssysteme bieten standardmäßig verschiedene Sicherheitseigenschaften an. Diese können jedoch nur zum Erfolg führen, wenn sie sinnvoll eingesetzt werden. Die hierfür notwendigen Einstellungen sollen mit Hilfe von Tools automatisiert überprüft werden, um

- Inkonsistenzen innerhalb eines Unix-Systems erkennen und beseitigen zu können und
- den Systemverwalter in die Lage zu versetzen, das Unix-Betriebssystem unter optimaler Ausnutzung der gegebenen Sicherheitsmechanismen zu verwalten.

Diese Prüfung kann mit im Unix-System vorhandenen Programmen, selbsterstellten Shellskripts oder Public-Domain-Programmen erfolgen. Für einige Unix-Varianten sind auch kommerzielle Programme verfügbar.

**Beispiele:**

- **pwck**
  Dieser Befehl gehört zu den Standard-Betriebssystemkommandos. Mit diesem Befehl nimmt man eine Konsistenzprüfung der Datei */etc/passwd* vor. Es wird überprüft, ob alle notwendigen Einträge vorgenommen wurden, ob das Login-Verzeichnis für den Benutzer existiert und ob das Login-Programm vorhanden ist. Ähnliche Funktionen beinhaltet unter Solaris der Befehl *logins*, mit dem auch Accounts ohne Passwort gefunden werden können.
- **grpck**
  Mit diesem Befehl nimmt man eine Konsistenzprüfung der Datei */etc/group* vor. Er gehört ebenfalls zu den Standard-Betriebssystemkommandos. Es wird überprüft, ob alle notwendigen Einträge vorgenommen wurden, ob alle Mitglieder einer Gruppe auch in der Benutzerpasswortdatei vorhanden sind und ob die Gruppennummer mit der dort angegebenen übereinstimmt.
- **tripwire**
  Mit diesem Programm können Integritätsprüfungen von Dateien durchgeführt werden. Dazu werden Prüfsummen über Dateien gebildet und in einer Datenbank gespeichert. *tripwire* ist in verschiedenen kostenlosen Versionen verfügbar.
- **cops**
  Dieses Public-Domain-Programm dient zur Überprüfung der Sicherheit von Unix-Systemen, z. B. werden verschiedene Systemeinstellungen, Zugriffsrechte, SUID-Dateien etc. überprüft und potentielle Sicherheitslücken aufgezeigt.
- **tiger**
  Mit diesem Public-Domain-Programm können Unix-Systeme ähnlich wie mit *cops* auf Sicherheitslücken überprüft werden.
- **SATAN**
  Mit diesem Public-Domain-Programm kann die Netz-Sicherheit analysiert werden. Es überprüft vernetzte Unix-Systeme auf bekannte, aber oftmals nicht beseitigte Schwachstellen.
- **crack**
  Mit diesem Public-Domain-Programm überprüft man, ob zu einfache, leicht erratbare Passwörter vorhanden sind.

Prüffragen:

- Werden die Sicherheitseinstellungen eines Unix-Systems regelmäßig mit Hilfe von Tools automatisiert überprüft?

# M 4.27 Zugriffsschutz am Laptop

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Jeder Laptop sollte mit einem Zugriffsschutz versehen werden, der verhindert, dass dieser unberechtigt benutzt werden kann. Bei Laptops sollte als Minimalschutz, wenn kein anderer Sicherheitsmechanismus vorhanden ist, der BIOS-Bootschutz aktiviert werden, wenn dessen Nutzung möglich ist. Erst nach Eingabe des korrekten Bootpasswortes wird der Rechner dann hochgefahren. Die im Umgang mit Passwörtern zu beachtenden Regeln sind in M 2.11 *Regelung des Passwortgebrauchs* aufgeführt worden.

Außerdem bieten nahezu alle Betriebssysteme die Möglichkeit, Anmeldepasswörter einzurichten und diese mit geeigneten Restriktionen zu versehen (z. B. Mindestlänge, Lebensdauer, etc.). Da diese Bordmittel nur eine begrenzte Sicherheit bieten, empfiehlt es sich bei Laptops, auf denen sich schnell große Mengen sensitiver Daten sammeln, zusätzliche Sicherheitshard- oder -software einzusetzen. Dazu gehören beispielsweise Chipkarten oder Token, die die Authentikation absichern.

Ist keine Passwortroutine installiert, sollte, wenn keine Verschlüsselung der Daten erfolgt, die Speicherung von schutzbedürftigen Daten auf der Festplatte verboten und deren Speicherung stattdessen nur auf mobilen Datenträgern, also z. B. Disketten oder USB-Sticks, zugelassen werden. Diese sind dann getrennt vom Laptop aufzubewahren, zum Beispiel in der Brieftasche.

Bei kurzen Arbeitsunterbrechungen muss unbedingt ein Zugriffsschutz aktiviert werden, z. B. ein Bildschirmschoner. Ist es absehbar, dass die Unterbrechung länger dauert, ist der Laptop auszuschalten.

Prüffragen:

- Ist ein angemessener Zugriffschutz für die Laptops vorhanden?
- Werden die Regeln für den korrekten Umgang mit dem Zugriffschutz eingehalten?

# M 4.28 Software-Reinstallation bei Benutzerwechsel eines Laptops

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wechselt der Benutzer eines Laptops, so muss sichergestellt sein, dass auf diesem weder schutzbedürftige Daten noch Computer-Viren vorhanden sind. Die Löschung von Daten kann durch vollständiges Überschreiben oder mit Hilfe spezieller Löschprogramme vorgenommen werden. Ein aktuelles Viren-Suchprogramm muss anschließend zum Einsatz kommen. Beide Vorgänge müssen für alle benutzten Datenträger wie Festplatte, Disketten, CDs oder USB-Sticks durchgeführt werden.

Es empfiehlt sich jedoch, die Festplatte des tragbaren PC neu zu formatieren und anschließend die erforderliche Software und Daten neu aufzuspielen. Was hierbei zu beachten ist, ist in M 4.235 *Abgleich der Datenbestände von Laptops* beschrieben.

Prüffragen:

- Wird sichergestellt, das beim Benutzerwechsel eines Laptops evtl. vorhandene schutzbedürftige Daten sicher gelöscht werden?
- Falls der Laptop nach dem Benutzerwechsel nicht neu aufgesetzt wird: Wird sichergestellt, dass sich auf dem System bzw. allen damit verbundenen Datenträgern keine Schadsoftware befindet?

# M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Um zu verhindern, dass aus einem trotz aller Vorsichtsmaßnahmen gestohlenen tragbaren IT-System schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Mit Hilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, in der Lage ist, die Daten zu lesen und zu gebrauchen.

Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne Kenntnis des verwendeten Schlüssels nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, dass der erforderliche Aufwand zum Brechen des Algorithmus bzw. zum Entschlüsseln in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.
- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Passwort zu wählen, sollten die diesbezüglichen Regeln aus M 2.11 *Regelung des Passwortgebrauchs* beachtet werden.
- Der Verschlüsselungsalgorithmus (das Programm), der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Dies kann dadurch geschehen, dass er auf einer Pappkarte in Form einer Scheckkarte aufgeschrieben und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Die kryptographischen Schlüssel sollten auf einem auswechselbaren Datenträger wie z. B. auf Diskette, Chipkarte oder USB-Stick gespeichert werden und getrennt vom tragbaren IT-System aufbewahrt werden (z. B. in der Brieftasche).

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass der Benutzer dies aktiv veranlassen muss. Eine Offline-Verschlüsselung wird explizit vom Benutzer initiiert. Er muss dann auch entscheiden, welche Dateien verschlüsselt werden sollen. Zur Auswahl und Nutzung von kryptographischen Verfahren sollte auch Baustein B 1.7 *Kryptokonzept* beachtet werden.

Für den Bereich der öffentlichen Verwaltung kann das BSI für den Einsatz auf stationären und tragbaren PCs ein Offline-Verschlüsselungsprogramm unter gewissen Randbedingungen zur Verfügung stellen, das den Sicherheitsanforderungen im Bereich des normalen Schutzbedarfs genügt.

Prüffragen:

- Wird ein Verschlüsselungsalgorithmus eingesetzt, der ohne Kenntnis des verwendeten Schlüssels keine Möglichkeit zur Rekonstruktion des Klartextes zulässt?

- Werden die verwendeten Schlüssel zufällig erzeugt? (Alternativ sind die Regeln aus M 2.11 Regelung des Passwortgebrauchs zu beachten)
- Werden Daten und Schlüssel getrennt aufbewahrt?

# M 4.30 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Einige der Standardprodukte im PC-Bereich bieten eine Reihe von nützlichen Sicherheitsfunktionen, deren Güte im einzelnen unterschiedlich sein kann, aber Unbefugte behindern bzw. mögliche Schäden verringern. Im folgenden seien fünf dieser Funktionen kurz erläutert:

- Passwortschutz bei Programmaufruf: das Programm kann nur gestartet werden, wenn vorher ein Passwort korrekt eingegeben wurde. Dies verhindert die unberechtigte Nutzung des Programms.
- Zugriffsschutz zu einzelnen Dateien: das Programm kann nur dann auf eine geschützte Datei zugreifen, wenn das mit dieser Datei verknüpfte Passwort korrekt eingegeben wird. Dies verhindert den unerlaubten Zugriff mittels des Programms auf bestimmte Dateien.
- Automatische Speicherung von Zwischenergebnissen: das Programm nimmt eine automatische Speicherung von Zwischenergebnissen vor, so dass ein Stromausfall nur noch die Datenänderungen betrifft, die nach dieser automatischen Speicherung eingetreten sind.
- Automatische Sicherung der Vorgängerdatei: wird eine Datei gespeichert, zu der im angegebenen Pfad eine Datei gleichen Namens existiert, so wird die zweite Datei nicht gelöscht, sondern mit einer anderen Kennung versehen. Damit wird verhindert, dass versehentlich eine Datei gleichen Namens gelöscht wird.
- Verschlüsselung von Dateien: das Programm ist in der Lage, eine Datei verschlüsselt abzuspeichern, so dass eine unbefugte Kenntnisnahme verhindert werden kann. Die Inhalte der Datei sind damit nur denjenigen zugänglich, die über den verwendeten geheimen Kryptierschlüssel verfügen.
- Automatisches Anzeigen von Makros in Dateien: diese Funktion soll das unbeabsichtigte Ausführen von Makros verhindern (Makro-Viren).

Je nach eingesetzter Software und damit vorhandenen Zusatzsicherheitsfunktionen kann der Einsatz dieser Funktionen sinnvoll sein. Für mobil eingesetzte IT-Systeme bietet sich insbesondere die Nutzung des Passwortschutzes bei Programmaufruf und die automatischen Speicherung an.

- Werden die sicherheitsrelevanten Hinweise in Handbüchern oder Zertifizierungsreports beachtet?

Prüffragen:

- Werden vorhandene Sicherheitsfunktionen in Anwendungsprogrammen genutzt?
- Ist den Benutzern bekannt, welche Sicherheitsfunktionen in den Anwendungsprogrammen existieren?

# M 4.31 Sicherstellung der Energieversorgung im mobilen Einsatz

**Verantwortlich für Initiierung:** Benutzer
**Verantwortlich für Umsetzung:** Benutzer

Um die Energieversorgung eines IT-Systems auch im mobilen Einsatz aufrechterhalten zu können, werden üblicherweise Akkus oder Batterien eingesetzt. Diese können das Gerät je nach Kapazität und Bauweise des mobilen Endgeräts für einen beschränkten Zeitraum, üblicherweise einige Stunden, mit Energie versorgen. Es ist schwierig, diesen Zeitraum genauer abzuschätzen, da er stark vom Alter des Akkumulators und von der Intensität der Nutzung des Endgerätes abhängt. So entlädt der Akku bei mobilen Videokonferenzen deutlich schneller als bei normalen Telefonaten. Damit (insbesondere bei älteren Geräten) nach Abfall der Betriebsspannung keine Daten in flüchtigen Speichern verloren gehen, sollten einige Randbedingungen eingehalten werden:

- Die Warnanzeigen des mobilen Endgerätes (falls vorhanden), die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden. Sie sollten so konfiguriert sein, dass nach der ersten Warnung noch genügend Zeit vorhanden ist, um z. B. wichtige Daten abzuspeichern oder offene Programme zu schließen.
- Falls ein längerfristiger mobiler Einsatz absehbar ist, sind die Akkus vorher vollständig aufzuladen und ggf. Ersatz mitzuführen. Zusätzlich gibt es für viele mobile Endgeräte sogenannte Akku-Packs, die über eine externe Schnittstelle angeschlossen werden können.
- Gerade bei älteren Akkus sind die Gebrauchszeiten verkürzt und die Entladung gegen Ende der Kapazität kann sehr schnell erfolgen. Es müssen daher regelmäßige geöffnete Dateien abgespeichert werden, um Datenverluste zu vermeiden. Da sich solche Akkus auch im Stand-by-Modus schnell entladen können, sollte der Ladezustand regelmäßig kontrolliert werden. Für den Notfall sollten Sicherungen der Konfigurationsdaten des Laptops oder PDAs mitgeführt werden. Es wird empfohlen, den Akku auszutauschen, sobald solche Alterungserscheinungen auftreten.
- Beim Laden sollten die Hinweise im Handbuch des mobilen IT-Systems beachtet werden, damit die Lebensdauer des Akkus nicht beeinträchtigt wird.
- Vor einer Reise bzw. bei der Übergabe eines mobilen IT-Systems ist der ausreichende Ladezustand der Akkus oder Batterien sicherzustellen. Der Ladezustand sollte regelmäßig überprüft werden, da sich ein Akku auch entlädt, wenn er nicht verwendet wird.
- Das Ladegerät sollte immer mitgeführt werden. Nur im Ausnahmefall, beispielsweise bei voraussehbar kurzem mobilen Einsatz, ist es entbehrlich.
- Vor einer Reise bzw. bei der Übergabe eines mobilen IT-Systems ist der ausreichende Ladezustand der Akkus oder Batterien sicherzustellen. Der Ladezustand der Akkus sollte regelmäßig überprüft werden, da sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird.
- Das Ladenetzteil sollte optional mitgeführt werden.

Es empfiehlt sich darüber hinaus, während der Nutzung des mobilen IT-Systems in kurzen Abständen die verarbeiteten Daten auf einem nichtflüchtigen Medium zu speichern. Dazu können auch automatische Datensicherungen in Standardprogrammen benutzt werden.

Wenn eine längere Nutzung des mobilen IT-Systems absehbar ist, z. B. bei Dienstreisen, sollte ein geladener Ersatzakku mitgeführt werden. Der Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des Akkus mit leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs wie Schlüssel oder Ketten verursacht werden.

Jede Art IT-System sollte ausgeschaltet werden, bevor der Akku gewechselt wird, damit der Speicher nicht beschädigt wird.

Prüffragen:

- Sind die Benutzer darüber informiert, wie sie die Energieversorgung im mobilen Einsatz optimal sicherstellen können?
- Werden Ersatzakkus in entsprechenden Hüllen gelagert und transportiert?

# M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche

Neben den in Maßnahme M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten* enthaltenen Hinweisen zur Löschung oder Vernichtung von Datenträgern sind für den Datenträgeraustausch folgende Punkte zu beachten:

Magnetische Datenträger, die für den Austausch bestimmt sind, sollten vor dem Beschreiben mit den zu übermittelnden Informationen physikalisch gelöscht werden. Es soll damit sichergestellt werden, dass keine Restdaten weitergegeben werden, für deren Erhalt der Empfänger keine Berechtigung besitzt.

Eine für den normalen Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Möglich ist auch eine Formatierung des Datenträgers, wenn diese nicht wieder rückgängig gemacht werden kann. Es sollte vermieden werden, nur einzelne Dateien zu löschen, hierbei bleiben häufig Restinformationen erhalten, die die Rekonstruktion der gelöschten Dateien ermöglichen.

In der Regel sind die übertragenen Daten auch für den Empfänger schützenswert. Analog ist auch hier nach dem Wiedereinspielen der Daten eine physikalische Löschung des Datenträgers vorzusehen.

Auf den Einsatz von nicht-löschbaren Datenträgern (wie z. B. WORMs) ist zum Zwecke des Datenaustausches dann zu verzichten, wenn sich darauf weitere, nicht für den Empfänger bestimmte Informationen befinden, die nicht gelöscht werden können.

Prüffragen:

- Stehen den Mitarbeitern Programme zum physikalischen Löschen vor und nach Verwendung von Datenträgern zur Verfügung?
- Erfolgt eine physikalische Löschung zuvor anderweitig verwendeter Datenträgern vor einem Datenträgertausch?

# M 4.33 Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Neben den in Maßnahme M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen sollte unmittelbar vor und unmittelbar nach einer Datenübertragung sowie beim Austausch bzw. beim Versand von Disketten oder anderen Datenträgern eine Viren-Überprüfung durchgeführt werden (siehe Maßnahme M 4.3 *Einsatz von Viren-Schutzprogrammen*). Dabei ist darauf zu achten, dass das eingesetzte Viren-Suchprogramm auch Makro-Viren erkennen kann.

Ein Protokoll der Absender-Überprüfung sollte dem übermittelten Datenträger beigefügt oder einer Datei, die elektronisch versandt wird, angehängt werden. Es empfiehlt sich, dieses Protokoll als Kopie zu verwahren. Der Empfänger hätte anhand dieses Protokolls einen ersten Eindruck von der Integrität der übermittelten Daten. Dies entbindet jedoch nicht von einer erneuten Virenüberprüfung. Der Absender kann andererseits bei eventuellen Beschwerden bezüglich Virenbefall der Daten plausibel machen, dass ein Befall bei ihm unwahrscheinlich war.

Prüffragen:

- Wird vor und nach einem Datenaustausch die Prüfung auf Schadprogramme durchgeführt und protokolliert?

# M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Werden vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen und besteht eine gewisse Möglichkeit, dass diese Daten Unbefugten zur Kenntnis gelangen, von diesen manipuliert werden oder durch technische Fehler verändert werden können, sollte ein kryptographisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung in Betracht gezogen werden.

### Vertraulichkeitsschutz durch Verschlüsselung

Für die Übertragung vertraulicher Informationen bedarf es deren Verschlüsselung. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Ein anerkannter Algorithmus, der für den normalen Schutzbedarf ausreicht, ist der Tripel-DES, der auf dem Data Encryption Standard (DES) basiert. Dieser ist leicht zu programmieren, zumal der Quell-Code in vielen Fachbüchern in der Programmiersprache C abgedruckt ist. Ein anderer anerkannter Algorithmus ist der Advanced Encryption Standard (AES).

Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, müssen das IT-System des Absenders und des Empfängers den Zugriffsschutz auf das Verschlüsselungsprogramm ausreichend gewährleisten. Gegebenenfalls sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, in der Regel verschlossen aufbewahrt und nur bei Bedarf eingespielt und genutzt werden.

### Integritätsschutz durch Checksummen, Verschlüsselung oder Digitaler Signaturbildung

Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muss unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z. B. durch Übertragungsfehler, oder auch gegen Manipulationen geleistet werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummen-Verfahren (z. B. Cyclic Redundancy Checks) oder fehlerkorrigierende Codes zum Einsatz kommen. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus (z. B. Tripel-DES) aus der zu übermittelnden Information einen so genannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z. B. RSA) in Kombination mit einer Hashfunktion und erzeugen eine "Digitale Signatur". Die jeweiligen erzeugten "Fingerabdrücke" (Checksumme, fehlerkorrigierende Codes, MAC, Digitale Signatur) werden zusammen mit der Information an den Empfänger übertragen und können von diesem überprüft werden.

Für die Übermittlung oder den Austausch ggf. notwendiger Schlüssel sei hier auf Maßnahme M 2.46 *Geeignetes Schlüsselmanagement* verwiesen. Weitere Informationen zum Einsatz kryptographischer Verfahren und Produkte finden sich in Baustein B 1.7 *Kryptokonzept*.

Prüffragen:

- Ist das Verschlüsselungsprogramm vor unbefugtem Zugriff geschützt?
- Wird zur Übertragung von vertraulichen Informationen ein Verschlüsselungsalgorithmus verwendet und entspricht dieser Algorithmus dem aktuellen Stand der Technik?
- Wird zur Übertragung von Informationen mit hohem Integritätsanspruch ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt und entspricht dieses Verfahren dem aktuellen Stand der Technik?
- Existiert eine Basis auf welcher den Verschlüsselungs-, Checksummen- und digitalen Signaturverfahren vertraut wird?

# M 4.35 Verifizieren der zu übertragenden Daten vor Versand

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Vor dem Versenden eines Datenträgers ist dieser darauf zu überprüfen, ob die gewünschten Informationen - und auch nur diese - vom Datenträger rekonstruierbar sind. Dies ist sowohl bei Schriftstücken als auch bei elektronischen Datenträgern zu kontrollieren. Auch Briefe und andere analoge Datenträger sollten vor dem Versand noch einmal daraufhin gesichtet werden, ob sie einerseits vollständig sind und andererseits keine zusätzlichen Informationen enthalten, die nicht weitergegeben werden sollen. Dies ist vor allem wichtig, wenn aus Vertraulichkeitsgründen Teile von Vorgängen, wie beispielsweise Namensnennungen, nicht an Dritte übermittelt werden dürfen. Hierfür können diese Teilinformationen z. B. durch Schwärzen unkenntlich gemacht werden. Da geschwärzte Informationen aber häufig ohne größeren Aufwand wieder lesbar gemacht werden können, ist es allerdings besser, diese für die Weitergabe aus den Vorgängen ganz zu entfernen, z. B. indem sie vor dem Ausdrucken in einer Kopie der Ausgangsdatei gelöscht werden. Je nach Schutzbedarf der Informationen gibt es hierfür verschiedene Methoden:

- Dokumente sollten möglichst so strukturiert sein, dass nicht-öffentliche Inhalte einfach abgetrennt werden können, z. B. indem diese nur in einem Anhang erscheinen. Der Anhang sollte dann auch elektronisch in einer eigenen Datei vorliegen, die als vertraulich klassifiziert ist.
- Falls die Dokumente bereits in einer Form vorliegen, die keine saubere Trennung nach Vertraulichkeit zulassen, müssen schutzbedürftige Inhalte vor einer Weitergabe entfernt werden. Ein Grundproblem dabei ist es, alle sensiblen Informationen zu identifizieren und sorgfältig zu entfernen. Da bereits dies in der Praxis häufig nicht funktioniert, sollte möglichst darauf verzichtet werden, solche Dokumente "entschärft" weiterzugeben. Wenn dies trotzdem erforderlich ist, müssen alle kritischen Informationen entfernt und die Sicherheitsstufen der betroffenen Dokumente neu festgelegt werden. In jedem Fall muss vor der Herausgabe der Dokumente ein erneuter Freigabeprozess durchlaufen werden.
- Bei Papierdokumenten werden sensible Informationen häufig nur geschwärzt. Dies ist in folgenden Schritten durchzuführen:
  - Zunächst sind auf einer Papierfassung alle kritischen Informationen sorgfältig und in ausreichender Größe zu schwärzen.
  - Anschließend werden diese geschwärzten Dokumente kopiert.
  - Danach wird überprüft, ob die geschwärzten Passagen auf der Kopie tatsächlich nicht mehr lesbar sind.
  - Wenn dies sichergestellt ist und die Freigabe erteilt wurde, kann die Kopie weitergegeben werden. Das geschwärzte Original darf keinesfalls herausgegeben werden, da geschwärzte Passagen auf dem Original häufig leicht wieder lesbar gemacht werden können.
- Um vertrauliche Informationen in elektronischen Dokumenten zu entfernen, müssen die schutzbedürftigen Passagen zunächst durch andere Zeichen ersetzt und danach geschwärzt werden. Hierfür sollten Zeichenketten fester Länge verwendet werden, beispielsweise "XXXXXXXXXX", damit sich die ursprüngliche Bedeutung auch nicht mehr erraten lässt. Vor der Weitergabe sollte die Dateien daraufhin überprüft werden, ob sie Restinformationen enthalten, z. B. frühere Überarbeitungsstände (siehe auch

M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).

Elektronische Datenträger sind vor der weiteren Verwendung physikalisch zu löschen, wenn vorher andere Daten darauf gespeichert waren (siehe M 4.32 *Physikalisches Löschen der Datenträger vor und nach Verwendung*).

Die korrekte Übertragung kann bei elektronischen Datenträgern überprüft werden, indem ein Programm eingesetzt wird, das die ursprüngliche mit der übertragenen Datei zeichenweise vergleicht (bei einigen Betriebssystemen z. B. mittels des Befehls *comp*).

Vor dem Versand sollten alle Dateinamen auf den Datenträgern aufgelistet werden, um anhand der Namen zu überprüfen, dass nur die für den Empfänger bestimmte Dateien auf diesen Datenträgern enthalten sind.

Prüffragen:

- Ist sichergestellt, dass auf zu versendenden Datenträgern ausschließlich die gewünschten Informationen vollständig enthalten sind?

# M 4.36 Sperren bestimmter Faxempfänger-Rufnummern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Fax-Verantwortlicher, Fax-Poststelle

Besteht die Notwendigkeit, das zufällige oder absichtliche Versenden von Informationen oder Unterlagen per Fax an eine nicht gewünschte Empfängerrufnummer zu verhindern, so bietet die heutige Technik dazu mindestens drei Lösungen:

Bei einigen Faxgeräten bzw. Faxservern ist es möglich, die Versendung von Faxen an bestimmte Faxempfänger-Rufnummern zu unterbinden (positiver Ausschluss) oder alternativ alle Empfängerrufnummern außer einigen ausgewählten Rufnummern zu sperren (negativer Ausschluss).

Die gleiche Art der Berechtigungsvergabe kann auch in modernen TK-Anlagen erreicht werden, vorausgesetzt, das Faxgerät ist über eine solche Anlage ans Telefonnetz angeschlossen.

Wenn ein Faxgerät oder die TK-Anlage eine solche Möglichkeit nicht bietet, so kann zum Beispiel vom Betreiber des öffentlichen Netzes eine Zusatzeinrichtung gemietet werden, die den Verbindungsaufbau zu bestimmten Rufnummern (positiver und negativer Ausschluss) verhindert.

Prüffragen:

- Falls bestimmte Faxadressaten ausgeschlossen werden sollen: Werden am Faxgerät, Faxserver, an der TK-Anlage oder durch den Netzbetreiber bestimmte Faxempfänger-Rufnummern unterbunden bzw. nur bestimmte Rufnummern zugelassen?

# M 4.37 Sperren bestimmter Absender-Faxnummern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fax-Verantwortlicher, Fax-Poststelle

Damit bestimmte Faxsendungen das eigene Faxgerät nicht blockieren können, z. B. bei Überlastung durch spezielle Faxaktionen von Werbeagenturen, kann ggf. eine Sperre bestimmter Sender-Faxnummern realisiert werden.

Einige moderne Faxgeräte (Gruppe 4) sind in der Lage, die übermittelte Senderrufnummer auszuwerten und den Empfang von Faxsendungen ausgewählter Rufnummern zu verweigern. Dies gilt auch für einige Faxserver, sofern diese an das ISDN-Netz angeschlossen sind. Daneben kann auch die Faxabsenderkennung (CSID - Call Subscriber ID) zur Auswertung herangezogen werden. Nachteilig ist allerdings, dass der Faxabsender die Rufnummernübermittlung unterdrücken und die übermittelte Rufnummer sowie die Absenderkennung manipulieren kann.

Eine weitere Möglichkeit besteht darin, dass beim Telefon-Netzbetreiber kostenpflichtig eine geschlossene Benutzergruppe eingerichtet wird, wenn Empfänger und Sender an digitalen Vermittlungsstellen angeschlossen sind. Teilweise wird diese Möglichkeit auch von modernen TK-Anlagen angeboten (vergleiche auch Baustein B 3.401 *TK-Anlage*).

Prüffragen:

- Falls bestimmte Absender-Faxnummern gesperrt werden sollen: Werden bestimmte Sender-Faxnummern am Faxgerät, Faxserver, an der TK-Anlage oder durch den Netzbetreiber unterbunden bzw. nur bestimmte Rufnummern dort zugelassen?

# M 4.38 Abschalten nicht benötigter Leistungsmerkmale

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.39 Abschalten des Anrufbeantworters bei Anwesenheit

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.40 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Viele IT-Systeme sind mit Mikrofonen und teilweise auch mit Kameras ausgestattet. Mikrofon und Kamera eines vernetzten Rechners können von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei haben. Für ein Mikrofon wäre das unter Unix zum Beispiel */dev/audio* für die Soundkarte oder */dev/video* für eine Kamera. Unter Windows bestimmen die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung (*HKEY_LOCAL_MACHINE\HARDWARE*.), wer das Rechnermikrofon oder die Rechnerkamera aktivieren kann. Diese Rechte sind daher sorgfältig zu vergeben. Der Zugriff auf die Gerätedatei sollte nur möglich sein, solange jemand lokal an dem IT-System arbeitet. Wenn die Benutzung eines vorhandenen Mikrofons oder einer Kamera generell verhindert werden soll, müssen diese - wenn möglich - ausgeschaltet oder physikalisch vom Gerät getrennt werden.

Falls das Mikrofon bzw.die Kamera in den Rechner fest eingebaut ist und nur durch Software ein- und ausgeschaltet werden kann, müssen die Zugriffsrechte so gesetzt sein, dass kein Unbefugter sie benutzen kann. Dies kann z. B. erfolgen, indem unter Unix allen Benutzern die Leserechte auf die Gerätedateien */dev/audio*, */dev/video* bzw. unter Windows die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung entzogen werden. Dadurch ist ausgeschlossen, dass ein normaler Benutzer das Mikrofon oder die Kamera benutzen kann, er kann aber weiterhin Audio- oder Video-Dateien abspielen.

Bei IT-Systemen mit Mikrofon bzw. Kamera ist zu prüfen, ob Zugriffsrechte und Eigentümer bei einem Zugriff auf die Gerätedatei verändert werden. Falls dies der Fall ist oder falls gewünscht ist, dass jeder Benutzer Mikrofon oder Kamera benutzen kann und es nicht nur in Einzelfällen durch den Systemadministrator freigegeben werden soll, muss der Administrator ein Kommando zur Verfügung stellen, das

- nur aktiviert werden kann, wenn jemand an dem IT-System angemeldet ist,
- nur durch diesen Benutzer aktiviert werden kann und
- die Zugriffsberechtigungen dem Benutzer nach dem Abmelden wieder entzieht.

Solange der Zugriff auf das Mikrofon oder die Kamera durch kein sicheres Kommando geregelt wird, müssen diese physikalisch vom Rechner oder der Rechner vom Netz getrennt werden.

Rechner mit eingebautem Mikrofon oder Kamera sollten während einer vertraulichen Besprechung aus dem Raum entfernt werden oder zumindest ausgeschaltet werden. Bei einem Laptop sollten alle eventuell vorhandenen Verbindungen zu Kommunikationsnetzen, die nicht benötigt werden, getrennt werden. In den meisten Fällen ist es hierzu am einfachsten, das entsprechende Kabel auszustecken.

Prüffragen:

- Keine betriebliche Notwendigkeit zur Nutzung des Mikrofons: Existiert eine Regelung zur Abschaltung oder physikalischen Trennung des Rechnermikrofons?
- Bei internem Mikrofon bzw. betrieblicher Notwendigkeit: Existieren eindeutige Regelungen zur Rechtevergabe für die Nutzung des Mikrofons?

# M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle

Je nachdem, welche Sicherheitsanforderungen an ein IT-System gestellt werden, reichen eventuell die vorhandenen Sicherheitsfunktionalitäten nicht aus, so dass zusätzlich geeignete Sicherheitsprodukte eingesetzt werden sollten. Typische Beispiele dafür sind Zugangskontrolle, Zugriffsrechteverwaltung und -prüfung, Protokollierung oder Verschlüsselung.

Bei IT-Systemen muss beispielsweise sichergestellt werden, dass

- nur autorisierte Personen das IT-System benutzen können (siehe auch BDSG, Zugangskontrolle). Hierfür sind geeignete Authentisierungsmechanismen auszuwählen.
- die Benutzer auf die Daten nur in der Weise zugreifen können, die sie zur Aufgabenerfüllung benötigen. Hierbei unterstützen geeignete Benutzertrennung und Rechtevergabe.
- Unregelmäßigkeiten und Manipulationsversuche erkennbar werden. Hierbei helfen Protokollierungsfunktionen, Verschlüsselung und digitale Signatur.
- Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle). Hierbei unterstützen beispielsweise Backup-Programme.

Reichen die Protokollierungsmöglichkeiten des IT-Systems nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese nachgerüstet werden. Hierzu gibt es auch verschiedene Gesetze, die dies erfordern. Beispielsweise ist nach BDSG, bei der Eingabekontrolle "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind".

Ist es mit dem IT-System nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann kann z. B. mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

**Empfohlene Mindestfunktionalitäten:**

IT-Systeme sollten mindestens die folgenden Sicherheitseigenschaften besitzen. Wenn diese nicht im Standardumfang vorhanden sind, sollten diese über zusätzliche Sicherheitsprodukte nachgerüstet werden.

- *Identifikation und Authentisierung*: Es sollte eine Sperre des Systems nach einer vorgegebenen Anzahl fehlerhafter Authentisierungsversuche statt finden, die nur ein Administrator zurücksetzen kann. Wird ein Passwort verwendet, sollte das Passwort mindestens acht Stellen umfassen und darf nicht unverschlüsselt im System gespeichert werden.
- *Rechteverwaltung und -kontrolle*: Es sollte eine Rechteverwaltung und -kontrolle auf Festplatten und Dateien vorhanden sein, wobei zumindest zwischen lesendem und schreibendem Zugriff unterschieden werden soll.

Für Benutzer sollte kein Systemzugriff auf Betriebssystemebene möglich sein.
- *Rollentrennungzwischen Administrator und Benutzer*: Es sollte eine klare Trennung zwischen Administrator und Benutzer möglich sein, wobei nur der Administrator Rechte zuweisen oder entziehen können sollte.
- *Protokollierung* der Vorgänge Anmelden, Abmelden und Rechteverletzung sollte möglich sein.
- *Automatische Bildschirmsperre*: Nach zeitweiser Inaktivität der Tastatur oder Maus sollte eine Bildschirmsperre automatisch aktiv werden. Diese sollte sich auch direkt aktivieren lassen. Der erneute Zugriff auf das IT-System darf erst nach erfolgreicher Identifikation und Authentisierung wieder möglich sein.
- *Boot-Schutz* soll verhindern, dass der Rechner unbefugt von anderen Medien gebootet werden kann.

Sollte ein oder mehrere dieser Sicherheitsfunktionalitäten nicht vom Betriebssystem unterstützt werden, so müssen ersatzweise geeignete zusätzliche Sicherheitsprodukte eingesetzt werden.

**Zusätzliche Forderungen** an Sicherheitsprodukte:

- *Benutzerfreundliche Oberfläche* zur Erhöhung der Akzeptanz.
- Aussagekräftige und nachvollziehbare Dokumentation für Administrator und Benutzer.

**Wünschenswerte Zusatzfunktionalität von** Sicherheitsprodukten:

- *Rollentrennung zwischen Administrator, Revisor und Benutzer;* nur der Administrator kann Rechte zuweisen oder entziehen und nur der Revisor hat Zugriff auf die Protokolldaten,
- *Protokollierung* von Administrationstätigkeiten,
- *Unterstützung der Protokollauswertung* durch konfigurierbare Filterfunktionen,
- *Verschlüsselung* der Datenbestände mit einem geeigneten Verschlüsselungsalgorithmus und in einer Weise, dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch des Vorgangs) systemseitig abgefangen wird.

Die Realisierung dieser Funktionalität kann sowohl in Hardware wie auch in Software erfolgen. Bei der Neubeschaffung eines Produktes sollte Maßnahme M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung* berücksichtigt werden.

**Übergangslösung:**

Sollte es nicht möglich sein, kurzfristig ein geeignetes Sicherheitsprodukt zu beschaffen, sind andere geeignete Sicherheitsmaßnahmen zu ergreifen. Diese sind dann typischerweise organisatorischer Natur und müssen von den Benutzern konsequent eingehalten werden. Wenn ein IT-System beispielsweise keine Bildschirmsperre hat, muss dieses in den kurzen Phasen, wo es nicht benutzt wird, ein- oder weggeschlossen werden.

Prüffragen:

- Bei höheren Sicherheitsanforderungen an ein IT-System: Ist der Einsatz zusätzlicher Sicherheitsprodukte geprüft worden?
- Werden organisatorische Maßnahmen ergriffen, falls ein geeignetes Sicherheitsprodukt kurzfristig nicht beschafft werden kann?

# M 4.42 Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler

Mehrere Gründe können zu der Notwendigkeit führen, dass innerhalb der Anwendungsprogramme selbst Sicherheitsfunktionalitäten wie eine Zugangskontrolle, eine Zugriffsrechteverwaltung und -prüfung oder eine Protokollierung implementiert werden müssen:

- Reichen die Protokollierungsmöglichkeiten des IT-Systems einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese Protokollelemente im Anwendungsprogramm implementiert werden. (Beispiel: BDSG, Anlage zum § 9, Eingabekontrolle: "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind".)
- Reicht die Granularität der Zugriffsrechte des IT-Systems einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht aus, um einen ordnungsgemäßen Betrieb zu gewährleisten, so muss eine Zugriffsrechteverwaltung und -kontrolle im Anwendungsprogramm implementiert werden. (Beispiel: eine Datenbank mit einer gemeinsamen Datenbasis. Vorausgesetzt sei, dass je nach Funktion des Benutzers nur Zugriffe auf bestimmte Felder zulässig sind.)
- Ist es mit dem IT-System einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann muss dies bei Bedarf durch zusätzliche Sicherheitsfunktionen im Anwendungsprogramm implementiert werden. Zum Beispiel kann mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

Diese zusätzlichen Anforderungen an IT-Anwendungen müssen schon in der Planung und Entwicklung berücksichtigt werden, da eine nachträgliche Implementation meist aus Kostengründen nicht mehr möglich ist.

Prüffragen:

- Unzureichende Protokollierung zur Beweissicherung: Sind zusätzliche Protokollierungselemente im Anwendungsprogramm implementiert?
- Unzureichende Granularität der Zugriffsrechte: Ist eine zusätzliche Zugriffsrechteverwaltung und -kontrolle im Anwendungsprogramm implementiert?
- Unzureichende Einschränkung der Zugriffsrechte von Administratoren: Sind im Anwendungsprogramm zusätzliche Sicherheitsfunktionen implementiert?

# M 4.43 Faxgerät mit automatischer Eingangskuvertierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Beschaffer

Faxgeräte mit automatischer Eingangskuvertierung verhindern, dass eingegangene Faxe unberechtigt entnommen und unberechtigt gelesen werden. Eingehende Faxe werden so geknickt, dass nur das Faxvorblatt sichtbar bleibt, und dann in einem Klarsichtumschlag eingeschweißt. Danach fällt der Umschlag in ein verschließbares Fach im Faxgerät. Zugriff auf die Umschläge hat normalerweise nur der Berechtigte, der den Schlüssel zu diesem Fach besitzt. Eine unbefugte Kenntnisnahme ist vor Zustellung des Fax nur durch gewaltsames Öffnen des Faches oder Aufreißen des verschweißten Umschlages möglich und wird daher zumindest bemerkt.

Prüffragen:

- Kommen Faxgeräte mit automatischer Eingangskuvertierung zum Einsatz, um zu verhindern, dass Faxe unberechtigt entnommen und gelesen werden?

# M 4.44 Prüfung eingehender Dateien auf Makro-Viren

Diese Maßnahme ist mit Version 2005 entfallen.

# M 4.45 Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.46 Nutzung des Anmeldepasswortes unter WfW und Windows 95

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es muss festgelegt werden, welche Ereignisse protokolliert werden und wer die Protokolle auswertet. Die Protokollierung muss den jeweils geltenden rechtlichen Bestimmungen entsprechen. Für Protokolldaten ist in Deutschland insbesondere die Zweckbindung nach § 14 des BDSG zu beachten.

Für den Einsatz der Protokollierung am Sicherheitsgateway sollten die folgenden Punkte beachtet werden:

- Es muss möglich sein, die Protokolldaten (beispielsweise IP-Adressen) eindeutig einzelnen Rechnern (oder Personen) zuzuordnen. Dabei müssen jedoch die jeweils zutreffenden gesetzlichen Regelungen zum Datenschutz beachtet werden.
- Die Protokolldaten sollten nicht nur auf den einzelnen Komponenten des Sicherheitsgateways, sondern zusätzlich auch auf einem zentralen Protokollierungsserver (Loghost) gespeichert werden, so dass die Gefahr des Datenverlustes durch einen Hacker-Angriff oder durch einen Systemausfall verringert wird.
- Die Übertragung der Protokollinformationen von den Komponenten zum Loghost muss über eine gesicherte Verbindung erfolgen, damit die Protokollinformationen vor ihrer endgültigen Speicherung nicht verändert werden können.
- Wenn bei der Übertragung zum Loghost nicht-vertrauenswürdige Netze passiert werden müssen, so müssen die Daten verschlüsselt werden.
- Die Größe des freien Speicherplatzes auf dem verwendeten Medium sollte regelmäßig kontrolliert werden.
- Bei einem Ausfall der Protokollierung (z. B. aufgrund fehlenden Speicherplatzes auf der Festplatte) sollten alle Funktionen, die Protokolldaten generieren, gesperrt werden. Idealerweise sollte das Sicherheitsgateway jeglichen Verkehr blockieren und eine entsprechende Meldung an den Administrator weitergeben.
- Die Protokolldaten sollten auf einem WORM-Medium ("Write Once, Read Many") gespeichert werden.
- Art und Umfang der Protokollierung sollten sich an der Sensibilität der zu verarbeitenden Daten sowie am Verwendungszweck orientieren.
- Spezielle, einstellbare Ereignisse, wie z. B. wiederholte fehlerhafte Passworteingaben für eine Benutzer-Kennung oder unzulässige Verbindungsversuche, müssen bei der Protokollierung hervorgehoben werden und sollten zu einer unverzüglichen Warnung des Firewall-Administrators führen.
- Die einzelnen Komponenten sollten eine Zeitsynchronisation durchführen, um eine Korrelation der Daten zu ermöglichen. Siehe dazu auch M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*.

Bei kleinen Netzen, in denen nur ein einfaches Sicherheitsgateway eingesetzt wird, kann gegebenenfalls auf einen zusätzlichen Loghost verzichtet werden.

**Umfang der Protokollierung am Paketfilter**

Die Protokollierung am Paketfilter sollte zumindest alle Pakete erfassen, die auf Grund einer Paketfilterregel abgewiesen werden.

Je nach Sicherheitsanforderungen sind eventuell zusätzliche Klassen von Paketen interessant:

- "Ungewöhnliche" Pakete, beispielsweise mit einer fehlerhaften Kombination aus TCP-Flags oder Pakete mit fehlerhaften Header-Informationen. Solche Pakete sollten zwar ohnehin durch eine entsprechende Paketfilterregel abgewiesen und aus diesem Grund bereits von der Protokollierung erfasst werden, aber es wird trotzdem empfohlen, solche Pakete gesondert zu protokollieren, da sie beispielsweise Indizien für sogenannte "Stealth Scans" sein können. Außerdem kann eine Häufung fehlerhafter Pakete auf technische Probleme im Netz hindeuten.
- Bei verbindungsorientierten (beispielsweise TCP-basierten) Protokollen kann es sinnvoll sein, auch akzeptierte Pakete zu protokollieren, die zu einem Verbindungsaufbau gehören (beispielsweise TCP-Pakete, die zum 3-Wege-Handshake gehören), sowie eventuell zusätzlich Pakete, die zum Abbau einer bestehenden Verbindung gehören.
- Bei verbindungslosen Protokollen, über die keine großen Datenmengen übertragen werden (beispielsweise UDP-basierte Protokolle wie DNS) kann es unter Umständen sinnvoll sein, alle Pakete zu protokollieren.

Welche zusätzlichen Klassen von Paketen protokolliert werden hängt in erster Linie vom Schutzbedarf des vertrauenswürdigen Netzes ab. Allerdings bringt die Protokollierung alleine keinen Sicherheitsgewinn, sondern die Informationen müssen auch nach entsprechenden Kriterien ausgewertet werden.

Von den Paketen, für die eine Protokollierung gewünscht wird, sollten mindestens die folgenden Informationen protokolliert werden:

- Quell- und Ziel-IP-Adresse
- Quell- und Zielport oder ICMP-Typ
- Datum und Zeit
- zutreffende Regel des Paketfilters

Wird zusätzlich ein ALG verwendet, so kann auf die Protokollierung der akzeptierten Pakete verzichtet werden, da der Proxy in diesem Fall meist ausreichende Verbindungsinformationen protokolliert.

**Umfang der Protokollierung am Application-Level-Gateway**

Auf dem ALG, der durch den äußeren Paketfilter vor der großen Masse unzulässiger Pakete geschützt wird, sollten für jeden (erfolgreichen oder versuchten) Verbindungsaufbau die folgenden Daten protokolliert werden:

- Quell- und Ziel-IP-Adresse
- Quell- und Zielport
- Dienst
- Datum und Zeit
- Verbindungsdauer
- eventuell Authentisierungsdaten oder ausschließlich Tatsache des Fehlschlagens einer Authentisierung

Es muss möglich sein, für bestimmte Benutzer die Protokollierung abzuschalten, damit nicht wegen einer zu großen Anzahl von Protokolleinträgen wichtige Informationen übersehen werden. Diese Auswahl kann z. B. anhand des Rechteprofils einzelner Benutzer getroffen werden.

Für die einzelnen Protokolle werden darüber hinaus die folgenden Einstellungen empfohlen:

**DNS**
- Ablehnung von Anfragen
- Zulassen von Anfragen
- von anderen Rechnern initiierte ("ausgehende") Zonen-Transfers
- vom ALG initiierte ("eingehende") Zonen-Transfers

Zonen-Transfers werden in der Regel vom Betreiber des DNS-Server verhindert, so dass auf diese Überprüfungen auch verzichtet werden kann.

**FTP**
- Ziel-Adresse (URL)
- Abgelehnte PORT-Befehle
- Name der übertragenen Datei
- Menge der übertragenen Daten
- Statusnachricht

**HTTP**
- Ziel-Adresse (URL)
- Menge der übertragenen Daten
- Verbindungsmethode (z. B. GET, POST, CONNECT)
- Hinweis auf angewandte Filterkriterien
- Statusnachricht

**NNTP**
- Ziel-Adresse (URL)
- Menge der übertragenen Daten
- Statusnachricht

**SMTP**
- E-Mail-Adresse des Absenders und des Empfängers der E-Mail
- Menge der übertragenen Daten
- Hinweis auf angewandte Filterkriterien
- Statusnachricht über Erfolg oder Misserfolg der Weiterleitung

Bei folgenden Modulen braucht keine gesonderte Protokollierung erfolgen:

| **Modul** | **Begründung für Wegfall der Protokollierung** |
|---|---|
| HTTPS | Wird "in Reihe" mit einem HTTP-Proxy geschaltet, der bereits protokolliert. |
| Wartungsmodul | Relevante Protokolldaten fallen nicht an. |
| IDS | Protokolldaten werden auf dem IDS gesondert geliefert. Diese sollten nicht zentral gespeichert werden, um eine Umgehung von Modulen des Sicherheitsgateways zu unterbinden. |

Tabelle: Module ohne gesonderte Protokollierung

Die Protokollierung wird stark vereinfacht, wenn die Software die freie Konfigurierbarkeit der "logging facility" (d.h. eine Kennzeichnung der einzelnen Log-Einträge) ermöglicht. Dadurch ist es möglich, jedem Dienst eine eindeutige Kennung zuzuordnen, anhand derer der Loghost die Protokolldaten auf verschiedene Dateien verteilen kann.

Werden die Protokolldaten über das Netz zu einem zentralen Loghost geschickt, so muss darauf geachtet werden, dass die Log-Einträge verschiedener Rechner und Dienste so gekennzeichnet werden, dass sie eindeutig zugeordnet werden können. Zusätzlich ist es sinnvoll, wenn alle Dienste ihre Protokolldaten fortlaufend nummerieren. Dadurch kann der Verlust bzw. die Manipulation von Protokolldaten erkannt werden.

**Auswertung der Protokolldaten**

Die Auswertung von Protokolldaten kann mit speziellen Tools unterstützt werden ("logfile analyzer"). Diese stellen die Protokolldateien auf unterschiedliche Weise dar, wobei sich die meisten Tools regulärer Ausdrücke bedienen, um relevante Daten aus den Protokolldateien zu extrahieren. Obwohl Listen mit sinnvollen regulären Ausdrücken zum Zwecke der Protokolldatenauswertung existieren, sind im Einzelfall meist Anpassungen notwendig.

Beispiele für verschiedene Ausgaben der Protokolldateien sind:

- Gruppierung und Markierung zusammengehörender Protokolldaten (z. B. LogSurfer)
- Anzeige relevanter Protokolldaten, wobei irrelevante Daten mittels regulärer Ausdrücke ausgeblendet werden können. Auf diese Weise könnten beispielsweise diejenigen Protokolldaten ausgeblendet werden, die eine erfolgreiche Operation (z. B. GET bei HTTP) dokumentieren (z. B. checksyslog).
- Anzeige von Angriffen. Die Analyse der Protokolldaten muss dabei in Echtzeit vorgenommen werden.
- Statistische Analyse der Protokolldaten (z. B. wie oft trat welche Meldung auf).

Neben der reinen Darstellung relevanter Protokolldaten existieren Tools, die abhängig von einer erkannten Auffälligkeit Aktionen (z. B. Ausführen eines Befehls) ermöglichen.

Auffällige Protokolleinträge sind beispielsweise:

- Gehäuft auftretende Anfragen an Ports, auf denen keine Dienste laufen
- Nicht erfolgreiche Zugriffsversuche auf Komponenten des Sicherheitsgateways
- Aus dem nicht-vertrauenswürdigen Netz eintreffende Pakete mit IP-Adressen des vertrauenswürdigen Netzes (Hinweis auf IP-Spoofing)
- Verdächtige, ausgehende Verbindungen von Servern aus dem vertrauenswürdigen Netz. Diese können ein Anzeichen dafür sein, dass nach einem erfolgreichen Einbruch der Angreifer Daten aus dem vertrauenswürdigen Netz nach außen kopiert oder von außen Dateien nachlädt, die er für seine weiteren Aktivitäten braucht.

Die Protokolldateien müssen regelmäßig ausgewertet werden und es sollte festgelegt werden, welche Auswertungen mindestens erfolgen sollen. Darüber hinaus sollten zumindest grobe Richtlinien dafür festgelegt werden, welche Schritte unternommen werden, wenn bei der Auswertung auffällige Einträge festgestellt werden.

Prüffragen:

- Ist festgelegt, welche Ereignisse an den Komponenten des Sicherheitsgateways protokolliert werden?
- Erfolgt eine regelmäßige Auswertung der Protokolldateien?
- Entspricht die Protokollierung den geltenden datenschutzrechtlichen Bestimmungen?

- Erfolgt die Vorhaltung der Protokolldaten zusätzlich zur lokalen Speicherung auf einem zentralen Protokollierungsserver?
- Erfolgt die Übertragung der Protokollinformationen der Komponenten des Sicherheitsgateways über eine gesicherte Verbindung?
- Wird bei Ausfall des Protokollierungsservers eine Alarmierung und Sperrung der Funktionen zur Protokolldatengenerierung vorgenommen?
- Wird bei Ausfall des Protokollierungsservers der Datenverkehr am Sicherheitsgateway blockiert?
- Sind die Protokolldaten vor Veränderung geschützt?
- Decken sich die Art und der Umfang der Protokollierung mit den Vorgaben der Sicherheitsrichtlinien der Organisation?
- Umfasst die Protokollierung an Paketfiltern mindestens folgende Informationen: Quell- und Ziel-IP-Adresse, Quell- und Zielport oder ICMP-Typ, Datum und Zeit sowie die zutreffende Regel des Paketfilters?
- Werden auf dem Application-Level-Gateway alle Verbindungen protokolliert?
- Existieren Eskalationsverfahren für den Fall, dass auffällige Einträge bei der Auswertung der Sicherheitsgateway-Protokolle identifiziert werden?

# M 4.48 Passwortschutz unter Windows-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Zugang zu einem Windows-System ab der Version Windows NT muss für jeden Benutzer durch ein Passwort geschützt und die automatische Anmeldung sollte nicht aktiviert sein. Benutzerkonten ohne Passwort dürfen nicht existieren, da sie eine Schwachstelle im System darstellen. Dies gilt auch für deaktivierte Konten. Gastkonten sind grundsätzlich zu deaktivieren. Es ist wichtig, dass die Benutzer die Schutzfunktion der Passwörter kennen, denn die Mitarbeit der Benutzer trägt zur Sicherheit des gesamten Systems bei. Grundlage für die weiteren Empfehlungen in dieser Maßnahme ist M 2.11 *Regelung des Passwortgebrauchs*.

Die Einrichtung eines neuen Benutzers und die Definition eines Passwortes erfolgt unter Windows NT mit Hilfe des Dienstprogramms *Benutzer-Manager* über das Kommando "Neuer Benutzer". Unter Windows ab Version 2000 ist dazu für Stand-alone-Systeme das Snap-in *Lokale Benutzer und Gruppen* der *Microsoft Management Console* (MMC) zu benutzen. Für IT-Systeme in Active Directory-Domänen erfolgt das Anlegen neuer Benutzer über das MMC Snap-in *Active Directory Benutzer und Computer*. In jedem Fall ist dazu in den Feldern *Kennwort* und *Kennwortbestätigung* ein Anfangspasswort einzugeben. Die Groß- und Kleinschreibung muss beachtet werden. Dabei sollte ein sinnvolles individuelles Anfangspasswort vergeben werden, das den Passwortregeln der Institution entspricht und dem Benutzer mitgeteilt wird. Dies ist auch beim Zurücksetzen des Passwortes durch den Administrator zu beachten. Die immer gleiche Wahl des Anfangspasswortes oder die Verwendung des Benutzernamens als Passwort eröffnet eine Sicherheitslücke, und muss vermieden werden.

Die Option *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* sollte bei allen neuen Konten gesetzt sein, damit das Anfangspasswort nicht beibehalten wird. Dagegen sollte die Option *Benutzer kann Kennwort nicht ändern* nur in Ausnahmefällen verwendet werden, etwa für vordefinierte Konten im Schulungsbetrieb. Die Option *Kennwort läuft nie ab* sollte nur für Benutzerkonten verwendet werden, denen mit Hilfe der Systemsteuerungsoption *Dienste* ein Dienst zugewiesen wird (zum Beispiel das MS Exchange Dienstkonto). Diese Option setzt die Einstellung *Maximales Kennwortalter* in den Richtlinien für Konten außer Kraft und verhindert, dass das Passwort abläuft.

Mit Windows 7 und Windows Server 2008 R2 wurden zwei besondere Konten eingeführt, das v*erwaltete Dienstkonto* und das v*irtuelle Konto*. Im Gegensatz zu den bisher genutzten Konten zur Verwaltung von Diensten wie *lokaler Dienst*, *Netzwerkdienst* oder *lokales System*, können beide Konten zentral verwaltet werden, da sie entweder in der Organisationseinheit "Verwaltete Dienstkonten" innerhalb des Active Directory gespeichert sind (*Verwaltete Dienstkonten),* oder wie das virtuelle Konto als verwaltetes lokales Konto über die Computeridentität in einer Domänenumgebung steuerbar sind. Bei Systemdiensten müssen Kenntwortänderungen demnach nicht von Administratoren konfiguriert werden, da die Änderung automatisch erfolgt. Bisher konnten verwaltete Dienstkonten nicht von mehreren Computern gemeinsam genutzt werden und daher nicht in Serverclustern, in denen ein Dienst auf mehrere Clusterknoten repliziert, verwendet werden. Mit Windows 8 und Windows Server 2012 wurde die Limitierung, dass ein verwaltetes Dienstkonto jeweils nur auf

einem Server eingesetzt werden kann, durch die Einführung von gruppenverwalteten Dienstkonten aufgehoben. Weitere Informationen zu den virtuellen Konten werden in M 4.284 *Umgang mit Diensten ab Windows Server 2003* beschrieben.

**Passwort-Richtlinien**

Mit Windows NT können über den Benutzer-Manager Richtlinien für Benutzerkonten, Benutzerrechte und für die Systemüberwachung festgelegt werden. Unter Windows ab Version 2000 erfolgt das Festlegen der Richtlinien entweder durch das MMC Snap-in *Lokale Sicherheitseinstellungen* oder durch das Snap-in *Gruppenrichtlinien*. Die Parameter und Werte finden sich in den Snap-ins unter *Sicherheitseinstellungen* | *Kontorichtlinien*.

Dabei sollten die Einstellungen der Gruppenrichtlinien für IT-Systeme, die einer Domäne angeschlossen sind, über das Active Directory verteilt und durchgesetzt werden (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows* und M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*). Ab Windows 2000 ist für Kontorichtlinien eine Sicherheitsvorlage zu erstellen (siehe auch M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*).

Die Anforderungen an Passwörter und deren Vergabe unter Windows-Systemen sollten in einer Sicherheitsrichtlinie dokumentiert werden. Die Dokumentation bzw. Richtlinie sollte die Einstellungen der folgenden Tabelle umfassen. Die letzte Spalte enthält Mindestempfehlungen für normalen Schutzbedarf:

| **Windows NT** | **Windows 2000/ XP/2003** | **Ab Windoes Vista und Server 2008** | **Mindestempfehlung** |
|---|---|---|---|
| Maximales Kennwortalter | Maximales Kennwortalter | Maximales Kennwortalter | 90 Tage |
| Minimales Kennwortalter | Minimales Kennwortalter | Minimales Kennwortalter | 1 Tag |
| Minimale Kennwortlänge | Minimale Kennwortlänge | Minimale Kennwortlänge | 8 Zeichen |
| Kennwortzyklus | Kennwortchronik erzwingen | Kennwortchronik erzwingen | 3 Versuchen |
| Konto sperren \| Konto zurücksetzen nach | Zurücksetzungsdauer des Konotsperrungszählers | Zurücksetzungsdauer des Konotsperrungszählers | 30 Minuten |
| Dauer der Sperrung | Kontosperrdauer | Kontosperrdauer | 60 Minuten |
| Benutzer muss sich anmelden, um Kennwort zu ändern | n/v | n/v | Deaktiviert |
| n/v | Kennwort muss Komplexitätsvoraussetzungen entsprechen | Kennwort muss Komplexitätsvoraussetzungen entsprechen | Aktiviert |
| n/v | Kennwörter für alle Domänenbe- | Kennwörter mit umkehrbarer Ver- | Deaktiviert |

| Windows NT | Windows 2000/ XP/2003 | Ab Windoes Vista und Server 2008 | Mindestempfehlung |
|---|---|---|---|
| | nutzer mit umkehrbarer Verschlüsselung speichern | schöüsselung speichern | |

Bei der Festlegung der Einstellungen sind einige systemspezifische Sicherheitsaspekte zu berücksichtigen, die im Folgenden erläutert werden.

Die minimale Passwortlänge für besonders schützenswerte Konten (z. B. Dienstkonten) sollte mehr als 14 Zeichen betragen. Dies funktioniert allerdings nicht unter Windows NT. Hier sollten solche Passwörter in kürzeren Abständen geändert werden. Hohe Passwortlängen oder Passphrasen sind bei steigender Rechenleistung der effektivste Schutz gegen Brute-Force-Angriffe.

Die Passworthistorie sollte grundsätzlich eingeschaltet sein und wenigstens 6 Passwörter umfassen. Damit wird verhindert, dass der Benutzer immer wieder das gleiche Passwort neu vergibt. Die Gültigkeitsdauer des Passwortes sollte auf einen Zeitraum von maximal 6 Monaten begrenzt sein. Durch Festlegung eines Wertes für das *Minimale Kennwortalter* kann verhindert werden, dass Benutzer ihr Passwort mehrfach hintereinander ändern, um so die Historienprüfung zu umgehen. Das *Minimale Kennwortalter* sollte jedoch nicht größer als 1 Tag gewählt werden, um dem Benutzer jederzeit eine Passwortänderung zu ermöglichen.

**Hinweis:** Unter Windows NT darf bei *Minimales Kennwortalter* nicht der Parameter *Sofortige Änderungen erlauben* gewählt werden, da sonst die Prüfung der Passworthistorie abgeschaltet wird.

Benutzerkonten sollten nach wiederholten ungültigen Passworteingaben gesperrt werden, um Versuche zu erschweren, die Passwörter der Benutzer zu erraten (Brute-Force-Angriffe). Mit den Werten aus der Tabelle erfolgt eine Sperrung nach drei ungültigen Anmeldeversuchen, die innerhalb von 29 Minuten unternommen wurden. Hatte ein Benutzer nur zwei ungültige Anmeldeversuche unternommen, erhält er 30 Minuten nach dem letzten Versuch wieder drei neue Anmeldeversuche.

In der Regel sollte eine Kontosperre nur durch einen Administrator aufgehoben werden können. Mit der Einstellung *Kontosperrdauer* wird das Konto nach einem begrenzten Zeitraum automatisch wieder entsperrt. Der Zeitraum darf nicht kürzer als die *Zurücksetzungsdauer des Kontosperrungszählers* sein und sollte keinesfalls 30 Minuten unterschreiten. Prinzipiell verringert eine automatische Entsperrung stark die Sicherheit. Falls der Aufwand für die Benutzerbetreuung und der mögliche Produktivitätsausfall durch gesperrte Benutzerkonten dies nötig machen, muss hierfür ein geeigneter, möglichst hoher Wert als Kompromiss gefunden werden. Bei besonders schützenswerten Konten sollte diese Funktion immer deaktiviert werden.

Es ist zu beachten, dass das vordefinierte Administratorkonto (Built-in Administrator) von dieser automatischen Sperrung ausgenommen ist, um ein völliges Verriegeln des Systems zu vermeiden.

Unter Windows Vista und Windows 7 ist das vordefinierte Administratorkonto (Built-in Administrator) standardmäßig deaktiviert. Die vorgenommene Konfiguration der Passwort-Richtlinien gilt unterschiedslos sowohl für die Gruppe

der Administratoren, als auch für die Standardbenutzer. Wenn die Passwort-Richtlinien so konfiguriert sind, dass Benutzerkonten nach wiederholten ungültigen Passworteingaben gesperrt werden, dann kann ein völliges Verriegeln des Systems nicht ausgeschlossen werden, sofern das vordefinierte Administratorkonto deaktiviert ist.

Soll das vordefinierte Administratorkonto deaktiviert bleiben, sollte dem Problem durch die geeignete Wahl eines Zeitraums für die Einstellung *Kontosperrdauer* begegnet werden. Der Zeitraum ist sorgsam zu wählen, da das Konto leichter geknackt werden kann, wenn es nach einer bestimmten Dauer automatisch wieder aktiviert wird.

Unter Windows NT sollte von der Option *Benutzer muss sich anmelden, um Kennwort zu ändern* kein Gebrauch gemacht werden. Mit der Einstellung *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* führt diese Einstellung dazu, dass neue Benutzer keinen Zugang zum System erhalten.

Werden Passwort-Richtlinien auf Domänenebene eingestellt, ist für Domänen bis Windows Server 2003 keine weitere Differenzierung der Passwort-Anforderungen für Domänenkonten möglich. Nur lokale Konten einzelner Mitgliedsserver können mit eigenen Richtlinien versehen werden. Wenn Betriebsbereiche mit unterschiedlichen Passwort-Anforderungen zwingend erforderlich sind, kann dies nur durch mehrere Active Directory-Forrests umgesetzt werden. Der Aufwand hierfür ist nur selten gerechtfertigt. Daher muss beim Festlegen der Passwort-Anforderungen ein Kompromiss für alle Betriebsbereiche (Dienstkonten, administrative Konten, allgemeine Benutzerkonten, Benutzerkonten von leitenden Personen, Benutzerkonten für die Personalvertretung usw.) gefunden werden.

Seit der Einführung von Windows Server 2008 und dem korrespondierenden Active Directory ist es möglich, verschiedene Passwortrichtlinien (Granulare Kennwort- und Kontosperrungsrichtlinien, englisch *Fine-Grained Password Policy*) innerhalb einer Domäne zu nutzten. Dies bietet die Möglichkeit, besonders schützenswerte oder kritische Konten, wie Domänenadministratoren, mit längeren Passwörtern zu versehen als die restlichen Konten der Domäne. Genau genommen handelt es sich nicht um Richtlinien, sondern um sogenannte Active Directory-Objekte. Diese Objekte heißen *Password Setting Objects (PSO).* Innerhalb eines PSO sind verschiedene Attribute wie "Kennwortchronik erzwingen" oder "Minimale Kennwortlänge" vorhanden. Diese Attribute entsprechen den bekannten Attributen einer bisherigen Passwortrichtlinie. Um granulare Kennwort- und Kontosperrungsrichtlinien innerhalb einer Domäne zu nutzen, müssen mindestens die folgenden Voraussetzungen erfüllt sein:

- Der Funktionsmodus der Domäne muss Windows Server 2008 oder höher entsprechen.
- *PSO* können nicht direkt auf *Organisationseinheiten* (OU) angewendet werden. Sie gelten nur für Benutzerobjekte, globale Sicherheitsgruppen und für inetOrgPerson-Objekte.
- Pro Benutzer kann nur eine *PSO* angewendet werden.
- *PSO* können nur für Benutzer oder Gruppen innerhalb der gleichen Domäne angewendet werden.

Microsoft Windows und andere Software erstellt verschiedene Konten selbst und belegt diese mit Zufallskennwörtern. Auch bei diesen müssen die Richtlinien durchgesetzt werden. Falls die Herstellerdokumentation keine Hinweise dazu enthält, muss die Durchsetzung und Verträglichkeit mit der Software im Einzelfall getestet werden.

Eine weitere Neuerung in Windows 8 ist die Funktion *Konto für zugewiesenen Zugriff einrichten.* Mit dieser Funktion kann die Ausführung einer einzelnen Windows-Store-App für einen Benutzer gesteuert werden. Diese Option ist dafür angedacht, das System für die Kiosk-Nutzung (z. B. für öffentlich zugängliche Terminals) zu konfigurieren. Die Rechte der Benutzer bleiben somit eingeschränkt und verhindern Veränderungen am System. Diese Funktion eignet sich jedoch nicht für die Nutzung klassischer Desktop-Applikationen im Kiosk-Modus. Da die Bindung der App an lokale Benutzerkonten erfolgt, ist eine Konfiguration über Gruppenrichtlinien nicht vorgesehen.

Als Alternative zu klassischen Passwörtern ist seit Windows 8 ist auch die Anmeldung am System mit einem Bildcode oder die Anmeldung mittels einer vierstelligen PIN möglich. Bei der Anmeldung mittels Bildcode muss der Benutzer bei der Anmeldung am System, den Bildcode nachzeichnen (mit dem Finger oder der Maus), den er vorher festgelegt hat. Der Bildcode muss aus mindestens drei gezeichneten Bewegungen bestehen. Diese Anmeldeverfahren bieten nur sehr eingeschränkte Sicherheit und sollten nicht für Systeme mit schützenswerten Daten verwendet werden.

Prüffragen:

- Ist jedes Windows-System und jedes Benutzerkonto durch ein Passwort geschützt?
- Gibt es eine Sicherheitsrichtlinie für die Anforderungen und Vergabe von Passwörtern?
- Ist die automatische Anmeldung deaktiviert?
- Wird die Option Benutzer muss Kennwort bei der nächsten Anmeldung ändern bei allen neuen Konten aktiviert?
- Werden die Einstellungen der Gruppenrichtlinien für Systeme, die einer Domäne angeschlossen sind, über das Active Directory verteilt und durchgesetzt?
- Gibt es für Windows Versionen ab 2000 eine Sicherheitsvorlage für die Kontorichtlinien?
- Sind die Vorgaben für die Benutzerkonten-Richtlinien dokumentiert?
- Ist sichergestellt, dass eine Anmeldung mit Bildcode oder PIN nicht verwendet wird?

# M 4.49 Absicherung des Boot-Vorgangs für ein Windows-System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Windows kann nur dann sicher betrieben werden, wenn vom Systemstart an gewährleistet ist, dass eine geschlossene Sicherheitsumgebung aufgebaut wird. Es dürfen keine Wege an den Sicherheitsfunktionen des Betriebssystems vorbei bestehen. Dies erfordert, dass sich alle durch Windows schützbaren Ressourcen unter der Kontrolle des Betriebssystems befinden. Außerdem darf es keine Möglichkeit geben, fremde Systeme oder offene Systemumgebungen von Disketten-, CD-ROM-Laufwerken oder USB-Speichermedien zu starten, die den durch Windows gebotenen Schutz unterlaufen können. Dazu sind die folgenden Aspekte zu beachten:

- Alle vorhandenen Festplattenpartitionen müssen mit dem Dateisystem NTFS formatiert sein. Partitionen, die mit den Dateisystemen FAT12, FAT16, FAT32, VFAT, oder HPFS formatiert sind, können nicht gegen unbefugte Zugriffe der Benutzer geschützt werden. Dies bedeutet einerseits, dass die auf ihnen abgelegten Daten beliebigen Zugriffen aller Benutzer ausgesetzt sind. Andererseits können diese Partitionen zum unkontrollierten Datenaustausch zwischen Benutzern missbraucht werden.
- Ein ähnliches Risiko stellen Diskettenlaufwerke dar, da Disketten unter NT-basierten Windows-Systemen nur mit dem Dateisystem FAT oder VFAT formatiert werden können. Aus diesem Grund sind Diskettenlaufwerke an allen Rechnern, die nicht unter strikter physischer Kontrolle stehen, grundsätzlich zu sperren (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*). Auf NT-basierten Windows-Clients können die Diskettenlaufwerke auch durch Deaktivieren über die Systemsteuerungsoption *Geräte* bzw. *Computerverwaltung* | *Geräte-Manager*, Gerät *Floppy*, für unprivilegierte Benutzer außer Betrieb gesetzt werden. Hiervon sollte auf Clients ab Windows Vista abgesehen werden (M 4.339 *Verhindern unautorisierter Nutzung von Wechselmedien ab Windows Vista*).
- Verfügt der Rechner über ein offenes Diskettenlaufwerk oder ist es möglich, von einem vorhandenen CD/DVD-Laufwerk zu booten, so besteht die Gefahr, dass der Rechner mit einem anderen Betriebssystem als Windows gestartet wird. Die gleiche Gefährdung ergibt sich, wenn der Rechner von einem USB-Speichermedium gestartet werden kann oder auf einer lokalen Festplatte andere Betriebssysteme installiert sind. Dann kann der Anwender mit verschiedenen Programmen die Sicherheitsmechanismen von Windows umgehen. Inzwischen gibt es mehrere Programme, mit denen sich Dateien, die unter NTFS geschützt sind, von einer DOS-Umgebung oder einer Linux-Umgebung lesen und zum Teil auch ändern lassen. Sowohl unter dem Betriebssystem MS-DOS als auch unter dem Betriebssystem Linux werden die vom Dateisystem NTFS gesetzten Sicherheitsattribute ignoriert.
  Der Anwender hat daher von MS-DOS bzw. von Linux aus Zugriff auf alle Dateien des Rechners. Aus diesem Grund wird empfohlen, neben Windows keine weiteren Betriebssysteme auf lokalen Festplatten zu installieren.
- Clients ab Windows 8 (32- und 64-Bit) unterstützen auf Geräten mit dem Unified Extensible Firmware Interface (UEFI) die Absicherung des Boot-Vorgangs durch UEFI Secure Boot. Hierdurch wird die Integrität des Boot-

loaders vor dem Betriebssystemstart überprüft und ggf. der Start von Schadsoftware verhindert. Auf Systemen mit UEFI Firmware muss UEFI Secure Boot zur Absicherung des Betriebssystemstarts verwendet werden. Die vorinstallierten Schlüssel sollten vorher überprüft werden. Bei Vorfinden nicht vertrauenswürdiger Schlüssel muss nach einer Risikoanalyse die Entscheidung getroffen werden, ob das Schlüsselmanagement fur UEFI Secure Boot selbst übernommen werden muss. Diese Entscheidung sollte dokumentiert werden.

- Im Rahmen einer Neuinstallation von Windows besteht die Möglichkeit, die bestehende Installation des Betriebssystems zu aktualisieren oder eine neue Version parallel zu installieren. Bei der parallelen Installation wird die bestehende Dateistruktur nicht verändert, doch wird das vordefinierte Administratorkonto mit einem neuen Passwort neu angelegt. Dieser "neue" Administrator hat vollen Zugriff auf alle Ressourcen des Rechners und damit auch auf alle Daten und Programme.
  Damit im Bootmenü des Betriebssystems keine alternativen Betriebssysteme eingefügt werden können, dürfen Benutzer nicht in der Lage sein, die Datei *boot.ini* im Wurzelverzeichnis der ersten Platte zu verändern. Um das Booten eines alternativen Betriebssystems über einen Bootmanager auf einem externen Medium wie USB-Stick oder CD/DVD zu unterbinden, darf die Bootreihenfolge nicht verändert werden können. Zum Schutz der Bootreihenfolge sollte ein BIOS-Passwort gesetzt werden. (siehe M 4.149 *Datei- und Freigabeberechtigungen unter Windows* und M 4.247 *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*).
- Mit Hilfe der Installationsprogramme kann für Windows 2000 auch eine Notfalldiskette (siehe M 6.77 *Erstellung von Rettungsdisketten für Windows 2000*) erzeugt und mit dieser eine Systemrekonstruktion durchgeführt werden. Dabei wird der Zugriffsschutz der NTFS-Partition des Betriebssystems aufgehoben. Es ist aus diesem Grund unbedingt erforderlich, die Installationsprogramme, eine eventuell schon vorhandene Notfalldiskette und die Setup-Disketten so zu verwahren, dass sie gegen unbefugten Zugriff geschützt sind. Schutz gegen diese spezifische Bedrohung bietet auch die Sicherung der Diskettenlaufwerke (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*) und die Absicherung des Boot-Vorgangs durch entsprechende Einstellungen im BIOS (siehe oben).
- Für die Systemrekonstruktion wird auf Clients ab Windows XP die Wiederherstellungskonsole (Recovery Console) verwendet. Der Weg über die Notfalldiskette steht nicht mehr zur Verfügung. Die Wiederherstellungskonsole kann entweder von der Installations-CD/-DVD oder den Installations-Disketten gestartet werden. Sie lässt sich auch in das System integrieren, so dass sie beim Systemstart als eine der Boot-Optionen angeboten wird.
- Da die Wiederherstellungskonsole ein mächtiges Werkzeug ist, muss ihr Einsatz durch die entsprechende Einstellung des BIOS und im Allgemeinen durch die Definition der Wiederherstellungskonsole-Richtlinien (siehe M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*) eingeschränkt werden.

Prüffragen:

- Wird der Start des Betriebssystems bei UEFI-basierten Geräten mittels UEFI Secure Boot abgesichert?
- Sind die vorhandenen Schlüssel für UEFI Secure Boot kontrolliert und hinsichtlich Vertrauenswürdigkeit bewertet worden?

- Sind alle vorhandenen Festplattenpartitionen mit dem Dateisystem NTFS formatiert?
- Ist sichergestellt, dass Benutzer den Computer nicht von Disketten-, CD-ROM-Laufwerken oder USB-Speichermedien booten können?
- Ist die Datei boot.ini im Wurzelverzeichnis der ersten Platte vor Veränderungen geschützt?
- Werden die vorhandenen Installationsprogramme, sowie eventuell vorhandene Notfalldisketten und Installationsmedien vor unberechtigtem Zugriff geschützt?

# M 4.50 Strukturierte Systemverwaltung unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.51 Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.52 Geräteschutz unter NT-basierten Windows-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Normalerweise erlauben Windows-Betriebssysteme allen Programmen den Zugriff auf Disketten,CD/DVD-ROMs/RWs und USB-Schnittstellen. Es ist empfehlenswert, diesen Zugriff auf den gerade interaktiv angemeldeten Benutzer zu beschränken, indem die Geräte diesem Benutzer beim Anmelden exklusiv zugeordnet werden.

Im Folgenden wird beschrieben, wie der Zugriff auf Disketten- und CD-ROM-Laufwerke eingeschränkt werden kann. Der Zugriff auf andere Laufwerke für auswechselbare Datenträger sollte auf vergleichbare Weise eingeschränkt werden. Seit Windows Vista und Windows Server 2008 kann der Zugriff auf Wechselmedien durch die Nutzung von Gruppenrichtlinien detailliert gesteuert werden. Es kann nun grundsätzlich festgelegt werden, auf welche Typen von Wechselmedien zugegriffen werden darf, und ob zum Beispiel nur Lesezugriff erlaubt ist. Abhängig von der jeweiligen Umgebung und von den zu konfigurierenden Systemen kann dies entweder im Benutzer- oder im Computerkontext konfiguriert werden. Der Pfad zu den Konfigurationen innerhalb der Sicherheitseinstellungen lautet:

Computerkonfiguration [Benutzerkonfiguration] | Administrative Vorlagen | System | Wechselmedienzugriff

Darüber hinaus kann nun der Zugriff auf die USB-Schnittstellen über sogenannte Geräte-Identifikations-Strings und Geräte-Setup-Klassen genauer konfiguriert werden. Dies ermöglicht eine gezielte Konfiguration, wie zum Beispiel ausschließlich USB-Festplatten zu erlauben, ohne die USB-Schnittstelle vollständig deaktivieren zu müssen. Ab Windows 2000/Server 2003 erfolgt die Konfiguration über die lokalen Sicherheitseinstellungen bzw. über eine Gruppenrichtlinie. Die relevanten Parameter sind unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* zu finden und lauten unter Windows 2000:

Hinweis: Da die Geräte beim Abmelden wieder für den allgemeinen Zugriff freigegeben werden, sind Benutzer darauf hinzuweisen, dass Datenträger vor dem Abmelden aus den Geräten zu entfernen sind.

Sofern Diskettenlaufwerke vollständig abgeschaltet werden sollen, kann dies auch dadurch geschehen, dass in der Computerverwaltung/Gerätemanager ab Windows 2000/Server 2003 dem Gerät "Floppy" die Startart *Deaktiviert* zugewiesen wird. Damit wird das nötige Treiberprogramms nicht geladen. Nach dem nächsten Systemstart steht das Diskettenlaufwerk nicht mehr zur Verfügung, und es kann nur von einem Administrator durch Zuweisen der Startart *System* wieder nutzbar gemacht werden.

Darüber hinaus können Laufwerke in der Regel durch geeignete Konfigurationen innerhalb des Computer-BIOS deaktiviert werden.

Weiterhin erlaubt Windows allen Benutzern den Zugriff auf Bandlaufwerke, so dass jeder Benutzer den Inhalt jedes Bandes lesen und schreiben kann. Normalerweise bringt dies keine Probleme mit sich, da zu einem gegebenen Zeitpunkt jeweils nur ein Benutzer interaktiv angemeldet ist. Sofern dieser jedoch ein Programm laufen lässt, das auch nach dem Abmelden noch auf das

Bandlaufwerk zugreift, so kann dieses Programm möglicherweise auf ein Band zugreifen, das der nächste Benutzer einlegt, der sich anmeldet. Aus diesem Grund sollten Rechner, die sich nicht in einer kontrollierten Umgebung befinden und auf denen vertrauliche Daten verarbeitet werden, neu gestartet werden, ehe das Bandlaufwerk genutzt wird.

Hinweis: Der Einsatz von selbstladenden Bandgeräten, die mehrere Bänder aus einem Reservoir laden können, darf nur unter sehr genau kontrollierten Randbedingungen zugelassen werden. In der Regel sollten derartige Geräte nur zur Datensicherung an einem Server installiert werden. Der interaktive Zugriff normaler Benutzer auf diesen Server ist nicht zulässig (siehe auch M 6.32 *Regelmäßige Datensicherung*).

Weitere Empfehlungen zum geeigneten Umgang mit Laufwerken für Wechselmedien finden sich in M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*.

Prüffragen:

- Wird der Zugriff auf Laufwerke mit Wechselmedien auf den lokal angemeldeten Benutzer beschränkt?
- Werden die Benutzer von Wechselmedien darauf hingewiesen, dass Datenträger vor dem Abmelden aus den Laufwerken zu entfernen sind?

# M 4.53 Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.54 Protokollierung unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.55 Sichere Installation von Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.56 Sicheres Löschen unter Windows-Betriebssystemen

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

### NT-basierte Windows-Betriebssysteme

Das Windows Dateisystem NTFS legt in einer Master Dateitabelle (MFT) alle Dateiinformationen wie Namen, Pfad und Attribute ab. Diese Angaben werden nicht verschlüsselt. Programme, die direkt auf die Festplatte zugreifen, können unter Umgehung der Windows-Sicherheitsmechanismen auf alle Dateien beliebig zugreifen. Dies gilt insbesondere für Programme, die unter einem anderen Betriebssystem als Windows auf demselben IT-System laufen.

Beim Löschen einer Datei unter dem Dateisystem NTFS wird diese nicht physikalisch gelöscht oder überschrieben, sondern lediglich als gelöscht markiert und dem Zugriff für den Benutzer entzogen. Dennoch können gelöschte Dateien mit Programmen, die direkt auf die Festplatte zugreifen, wieder hergestellt werden. Hierzu sind unter Windows Administratorrechte erforderlich. Außerdem kann ein anderes Betriebssystem gestartet werden, um direkten Zugriff auf die Festplatte zu erhalten.

Aus diesen Gründen ist Windows als einziges Betriebssystem zu installieren und zu verhindern, dass andere Betriebssysteme gestartet werden können (siehe M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen* und M M 4.339 *Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista*).

Soll doch ein anderes Betriebssystem gestartet werden können (Multiboot-System), empfiehlt sich der Einsatz eines Programms zur Festplattenverschlüsselung, das mögliche Verletzungen der Vertraulichkeit durch ein anderes Betriebssystem unterbindet. Das in Windows Vista, Windows 7 und Windows Server 2008 enthaltene Programm zur Festplattenverschlüsselung BitLocker ist für Multiboot-Systeme ungeeignet. Es sollte ein für Multiboot-Systeme geeignetes Produkt eines Drittherstellers eingesetzt werden. Alternativ kann unter Windows ab Version 2000 auch das Encrypting File System (EFS) zur Festplattenverschlüsselung eingesetzt werden. EFS unterstützt die Verschlüsselung einzelner Dateien (siehe M 4.147 *Sichere Nutzung von EFS unter Windows*).

### Papierkorb unter Windows

Unter Windows werden Dateien beim Löschen, sofern der Benutzer nicht ausdrücklich ein direktes Löschen verlangt, zunächst in einen benutzerspezifischen Bereich, den sogenannten "Papierkorb", verlagert. Aus diesem Bereich werden sie erst entfernt, wenn der von gelöschten Dateien belegte Speicherplatz die für das betreffende Plattenlaufwerk vorgegebene Größe überschreitet oder wenn der Benutzer explizit den Papierkorb leert. Der Inhalt des Papierkorbs sollte daher regelmäßig gelöscht werden, damit die Festplatte nicht zu voll wird und der Benutzer nicht den Überblick verliert.

Die maximale Größe des für den Papierkorb reservierten Speicherplatzes kann unter "*Eigenschaften*" des Icons "Papierkorb" auf einen geeigneten kleineren Wert, zum Beispiel 2 MByte, eingestellt werden. Dateien mit sensitivem Inhalt sollten nicht in den Papierkorb verschoben, sondern explizit gelöscht werden, indem beim Löschen die Umschalttaste gedrückt gehalten wird.

Unter Windows besteht die Möglichkeit, gelöschte Dateien aus dem Papierkorb wiederherzustellen. Dateien mit besonders sensitivem Inhalt sollten daher vollständig überschrieben werden, statt sie in den Papierkorb zu verschieben (siehe M 2.3 *Datenträgerverwaltung* und B 1.15 *Löschen und Vernichten von Daten*).

Windows XP, Vista, Windows 7 und die Server-Versionen ab Server 2003 bieten die Möglichkeit, Dateien direkt und nicht über den Papierkorb zu löschen. Direktes Löschen von Dateien kann in den Eigenschaften des Papierkorbs (*Dateien sofort löschen*) oder durch das Aktivieren der Richtlinie *Benutzerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Explorer* | *Gelöschte Dateien nicht in Papierkorb verschieben* erzwungen werden. Hierauf sollten die Benutzer hingewiesen werden.

Unter Windows XP, Vista, Windows 7 und den Server-Versionen ab Server 2003 ist es möglich, den gesamten freien Plattenplatz eines Datenträgers oder eines Unterverzeichnisses mit dem Kommando *cipher.exe /w* zu überschreiben. Das Tool *cipher.exe* macht insgesamt drei Schreibdurchgänge und überschreibt den freigegebenen Platz im ersten Durchgang mit 0x0, im zweiten mit 0xF und im dritten mit pseudo-zufälligen Daten. Bei der Benutzung dieses Kommandos sollte jedoch berücksichtigt werden, dass die Inhalte kleiner gelöschter Dateien (unter 4 KB), unüberschrieben bleiben können, wenn sie direkt in der Master File Table (MFT) und nicht in separaten Datenträger-Clustern abgelegt sind. Das Verfahren ist auch geeignet, um verschlüsselte Dateien von unverschlüsselt zwischengespeicherten Datenresten zu bereinigen.

Um vertrauliche Dateien tatsächlich unwiederbringlich zu löschen, sollten spezielle Löschprogramme eingesetzt werden, mit denen alle Restinformationen zu dieser Datei auf dem Datenträger überschrieben werden.

**Schattenkopien**

Windows-Clients ab Vista und Windows-Server ab Server 2003 bieten die Möglichkeit, über sogenannte Schattenkopien (auch Vorgängerversionen genannt) frühere Versionen von Dateien und Verzeichnissen auf einer Festplatte vorzuhalten. Schattenkopien lassen sich für jedes Dateisystem im Eigenschaften-Dialog aktivieren. Bei aktivierten Schattenkopien ist es möglich, gelöschte Dateien und frühere Versionen von Dateien auf dem betroffenen Dateisystem für einen gewissen Zeitraum wiederherzustellen, und zwar auch dann, wenn die Originaldatei mit einem dafür vorgesehenen Programm sicher gelöscht wurde.

Schattenkopien dürfen daher auf Dateisystemen, auf denen ein sicheres Löschen von Dateien erforderlich werden kann, nicht eingesetzt werden. Auch hier kann der Einsatz einer Dateisystemverschlüsselung zusätzlichen Schutz bieten, weil damit auch die Schattenkopien verschlüsselt werden.

Prüffragen:

- Ist sichergestellt, dass Windows als einziges Betriebssystem auf den lokalen Festplatten installiert ist bzw. bei Einsatz eines weiteren Betriebssystems ein Festplattenverschlüsselungsprogramm verwendet wird?
- Sind alle Benutzer darüber informiert, dass über den Papierkorb gelöschte Dateien nicht zuverlässig gelöscht sind?
- Werden zusätzliche Programme zur unwiederbringlichen Löschung, insbesondere bei vertraulichen Daten, eingesetzt?

# M 4.57 Deaktivieren der automatischen CD-ROM-Erkennung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Unter Windows können CD-ROMs automatisch erkannt und bearbeitet werden. Dadurch können auch auf der CD-ROM gespeicherte Programme automatisch auf dem Rechner ausgeführt werden. Die automatische CD-ROM-Erkennung sollte daher *permanent* unterbunden werden.

Unter Windows 95 ist dafür auf der Registerkarte GERÄTEMANAGER unter der Systemsteuerungsoption SYSTEM für die CD-ROM die Eigenschaft *Automatische Benachrichtigung beim Wechsel* zu deaktivieren.

Unter Windows NT 4.0 und Windows 2000 ist für die permanente Deaktivierung der automatischen CD-ROM-Erkennung in der Registrierung der Eintrag *Autorun* im Schlüssel *SYSTEM* \ *CurrentControlSet* \ *Services* \ *CD-ROM* im Bereich *HKEY_LOCAL_MACHINE* auf den Wert *REG_WORD = 0* zu setzen. Unter Windows XP kann dies auch durch das Setzen der Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Autoplay deaktivieren* auf den Wert *Alle Laufwerke* erfolgen. Die Deaktivierung der automatischen CD-ROM-Erkennung kann auch auf Benutzerbasis erfolgen (Richtlinie *Benutzerkonfiguration* | *Administrative Vorlagen* | *System* | *Autoplay deaktivieren*). Die Richtlinien können sowohl in lokalen als auch Active Directory-basierten Gruppenrichtlinien definiert werden.

Falls die automatische CD-ROM-Erkennung nicht generell deaktiviert wird, sollte dies dokumentiert werden. Im Einzelfall kann die automatische CD-ROM-Erkennung *für jede CD-ROM einzeln* durch Drücken der Shift-Taste beim Einlegen verhindert werden. Erfahrungsgemäß wird dies in der Praxis allerdings selten gemacht.

Prüffragen:

- Ist die automatische Erkennung von Wechseldatenträgern wie CD-ROMs dauerhaft deaktiviert?
- Sind die Benutzer im Umgang mit der automatischen CD-ROM-Erkennung geschult, sofern diese nicht generell deaktiviert ist?

# M 4.58 Freigabe von Verzeichnissen unter Windows 95

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.59 Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Moderne ISDN-Karten sowie deren Kommunikationssoftware bzw. das in das Karten-RAM geladene Betriebssystem besitzen zahlreiche, über die reinen ISDN-Funktionalitäten hinausgehende Leistungsmerkmale. Solche"Komfort-Funktionalitäten", welche teilweise auch bei ausgeschaltetem IT-System angesprochen werden können, sind:

- der Empfang und Versand von Faxen,
- Funktionen eines digitalen Anrufbeantworters,
- das Abhören eingegangener Aufzeichnungen des digitalen Anrufbeantworters,
- das Telefonieren über ein im Lieferumfang der Karte enthaltenes Mikrofon bzw. einen enthaltenen Hörer.

Soweit es möglich ist, sollten nicht benötigte Karten-Funktionalitäten deaktiviert werden, am besten durch das Entfernen des jeweiligen Softwaremoduls. Lassen sich Karten-Funktionalitäten lediglich durch Parameter konfigurieren, so muss die korrekte Einstellung der Parameter regelmäßig geprüft werden.

Prüffragen:

- Ist sichergestellt, dass alle nicht benötigten ISDN-Karten-Funktionalitäten deaktiviert werden?
- Werden die korrekten Einstellungen der Parameter der ISDN-Karte regelmäßig überprüft und vorgenommene Änderungen dokumentiert?

# M 4.60 Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Neben Servicefunktionen bzw. der Fernwartung (siehe M 2.108 *Fernwartung der ISDN-Netzkoppelelemente*) können auch Funktionen der Router-Betriebssysteme zu Sicherheitslücken führen. Beispielsweise ist das Aufrufen einer Telnet-Sitzung auf dem Router und das sich anschließende Manipulieren der Management Information Base möglich, wenn dieser mit einem Unix-Betriebssystem ausgestattet ist.

Soweit es möglich ist, sind diese nicht benötigten Funktionalitäten zu deaktivieren, am besten durch das Entfernen des jeweiligen Softwaremoduls. Lassen sich Karten-Funktionalitäten lediglich durch Parameter konfigurieren, so muss die korrekte Einstellung der Parameter regelmäßig geprüft werden.

Prüffragen:

- Ist sichergestellt, dass alle nicht benötigten ISDN-Router-Funktionalitäten deaktiviert werden?
- Werden die korrekten Einstellungen der Parameter von ISDN-Routern regelmäßig überprüft und vorgenommene Änderungen dokumentiert?

# M 4.61 Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sind gemäß Maßnahme M 2.106 *Auswahl geeigneter ISDN-Karten in der Beschaffung* ISDN-Karten mit Sicherheitsfunktionalitäten für das IT-System oder den Router, wie

- Fähigkeit zur Durchführung einer Authentisierung über PAP und CHAP (Password Authentikation Protocol und Challenge Handshake Authentication Protocol, RFC 1994),
- Einsatz eines Verschlüsselungsverfahrens (symmetrisch/asymmetrisch) in Hard- oder Software,
- Möglichkeit der Auswertung von CLIP-Rufnummern (Calling Line Identification Presentation) zur Authentisierung,
- Möglichkeit des Führens einer Rufnummerntabelle für das Durchführen eines Call-Backs und
- Möglichkeit der Protokollierung nicht erfolgreicher Verbindungsaufbauten (Ablehnung aufgrund falscher Rufnummern- oder PAP/CHAP-Authentisierung),

beschafft worden, sollten diese auch geeignet genutzt werden, wie es die Maßnahmen M 5.48 *Authentisierung mittels CLIP/COLP*, M 5.49 *Callback basierend auf CLIP/COLP*, M 5.50 *Authentisierung mittels PAP/CHAP* und M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen* beschreiben. Voraussetzung hierfür ist, dass alle Kommunikationspartner mit ISDN-Karten, die möglichst gleiche Sicherheitsfunktionalitäten aufweisen, ausgestattet werden.

Prüffragen:

- Werden die den ISDN-Komponenten zur Verfügung stehenden Sicherheitsmechanismen genutzt?

# M 4.62 Einsatz eines D-Kanal-Filters

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle

Ein D-Kanal-Filter wird zwischen ISDN-Anschluss (S2M oder S0) und ISDN-Endgerät oder ISDN-TK-Anlage geschaltet. Zum ISDN-Anschluss verhält es sich wie ein ISDN-Endgerät und zum ISDN-Endgerät wie ein ISDN-Anschluss. Der D-Kanal-Filter überwacht den ISDN-D-Kanal auf unzulässige Protokollaktionen und ist damit in der Lage, Manipulationsversuche über den D-Kanal zu detektieren und zu verhindern. Der Einsatz des D-Kanal-Filters ist insbesondere dann sinnvoll, wenn mit qualifizierten Angriffen über Remote-Zugriffe (zum Beispiel bei Fernwartung und -administration) zu rechnen ist.

D-Kanal-Filter schränken weiterhin Leistungsmerkmale und Dienste für Rufnummern bestimmter Kommunikationspartner in der Weise ein, dass es unter konkreten Betriebszuständen nicht zu einem Missbrauch bzw. zur Gefährdung der ISDN-Endeinrichtung kommen kann. Versuche, unberechtigt Leistungsmerkmale und Dienste zu nutzen, werden von D-Kanal-Filtern mit einem Verbindungsabbau (Disconnect, Release) beantwortet und protokolliert.

Weitere Informationen zu dieser vom BSI initiierten Technologie können unter der IT-Grundschutz-Hotline nachgefragt werden.

Prüffragen:

- Werden ISDN-Verbindungen durch den Einsatz eines D-Kanal-Filters geschützt?

# M 4.63 Sicherheitstechnische Anforderungen an den Telearbeitsrechner

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die sicherheitstechnischen Anforderungen an die Telearbeitsrechner richten sich nach dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz und der Daten, auf die die Telearbeiter über den Kommunikationsrechner der Institution zugreifen können. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um diesen Schutz zu gewährleisten. Allgemeine Sicherheitsziele für Telearbeitsrechner sind:

- Telearbeitsrechner dürfen nur von autorisierten Personen benutzt werden können.
  Damit wird sichergestellt, dass nur autorisierte Personen die Daten und Programme, die auf einem Telearbeitsrechner gespeichert sind bzw. auf die über den Kommunikationsrechner zugegriffen werden kann, nutzen können. Autorisierte Personen sind der Administrator des Telearbeitsrechners und der Telearbeiter nebst seines Stellvertreters.
- Telearbeitsrechner dürfen nur für autorisierte Zwecke benutzt werden.
  Damit wird unterstützt, dass die Telearbeiter die Rechner nicht unautorisiert benutzen oder verändern. Beispielsweise dürfen keine ungenehmigten Programme installiert werden. Dies beugt Schäden durch Fehlbedienung und Missbrauch vor.
- Schäden aufgrund eines Diebstahls oder Defektes eines Telearbeitsrechners müssen tolerabel sein.
  Telearbeitsrechner werden üblicherweise in einer wenig gesicherten Umgebung eingesetzt, so dass ein Diebstahl oder Defekt wahrscheinlicher ist als in der geschützten Betriebsumgebung einer Institution. Darunter kann nicht nur die Verfügbarkeit, sondern auch die Vertraulichkeit der gespeicherten Daten leiden. Um die Schäden bei Diebstählen gering zu halten, sollten z. B. die Daten nur verschlüsselt gespeichert werden. Um Schäden durch Defekte zu begrenzen, sollten z. B. regelmäßig Datensicherungen durchgeführt werden.
- Versuchte oder erfolgte Manipulationen am Telearbeitsrechner sollten für den Telearbeiter erkennbar sein.
  Damit wird sichergestellt, dass der Telearbeitsrechner in einem integren Zustand verbleibt, auch wenn Manipulationsversuche nicht ausgeschlossen werden können.

Aus dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz leiten sich die Sicherheitsziele und damit die sicherheitstechnischen Anforderungen an die Telearbeitsrechner ab. Es ist zu dokumentieren, welche der im folgenden beschriebenen sicherheitsrelevanten Funktionalitäten ein Telearbeitsrechner aufweisen muss und wie diese umgesetzt werden.

Für einen Telearbeitsrechner sind daher folgende Funktionalitäten sinnvoll:

- Der Telearbeitsrechner muss über einen **Identifizierungs- und Authentisierungsmechanismus** verfügen. Insbesondere sind folgende Punkte sicherzustellen:
  - Sicherheitskritische Parameter, wie Passwörter, Benutzer-Kennung, usw., müssen sicher verwaltet werden. Passwörter dürfen nie unverschlüsselt auf dem Telearbeitsrechner gespeichert werden.
  - Das Zugangsverfahren muss definiert auf Fehleingaben reagieren. Erfolgt zum Beispiel dreimal hintereinander eine fehlerhafte Authentisierung, ist der Zugang zum Telearbeitsrechner zu sperren oder alternativ sind die zeitlichen Abstände, nach denen ein weiterer Zugangsversuch erlaubt wird, sukzessiv zu vergrößern.
  - Das Setzen bestimmter Minimalvorgaben für die sicherheitskritischen Parameter muss möglich sein. So sollte die Mindestlänge eines Passwortes acht Zeichen betragen.
  - Nach zeitweiser Inaktivität der Tastatur oder Maus muss automatisch eine Bildschirmsperre aktiviert werden, die erst nach erneuter Identifikation und Authentisierung deaktiviert wird.
- Der Telearbeitsrechner muss über eine **Zugriffskontrolle** verfügen. Insbesondere sind folgende Anforderungen umzusetzen:
  - Der Telearbeitsrechner muss verschiedene Benutzer unterscheiden können. Es muss möglich sein, mindestens zwei getrennte Rollen auf dem Telearbeitsrechner einzurichten, nämlich Administrator und Telearbeiter.
  - Mittels einer differenzierten Rechtestruktur (lesen, schreiben, ausführen, ...) muss der Zugriff auf Dateien und Programme regelbar sein.
- Telearbeitsrechner sollten über eine **Protokollierung** verfügen. Es ist sinnvoll, folgende Anforderungen umzusetzen:
  - Der Mindestumfang, den der Telearbeitsrechner protokollieren soll, sollte parametrisierbar sein. Beispielsweise sollten folgende Aktionen inklusive der aufgetretenen Fehlerfälle protokollierbar sein:
    - bei Authentisierung: Benutzer-Kennung, Datum und Uhrzeit, Ergebnis des Anmeldeversuchs, usw.
    - bei der Zugriffskontrolle: Benutzer-Kennung, Datum und Uhrzeit, Ergebnis des Zugriffsversuchs, Art des Zugriffs, was wurde wie geändert, gelesen, geschrieben, usw.
    - Durchführung von Administratortätigkeiten,
    - Auftreten von funktionalen Fehlern.
  - Die Protokollierung darf von Unberechtigten nicht zu deaktivieren sein. Die Protokolle selbst dürfen für Unberechtigte weder lesbar noch modifizierbar sein.
  - Die Protokollierung muss übersichtlich, vollständig und korrekt sein.
- Soll der Telearbeitsrechner über eine **Protokollauswertung** verfügen, können folgende Anforderungen sinnvoll sein:
  - Eine Auswertefunktion muss nach den bei der Protokollierung geforderten Datenarten unterscheiden können (z. B. "Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum").
  - Die Auswertefunktion muss auswertbare ("lesbare") Berichte erzeugen, so dass keine sicherheitskritischen Aktivitäten übersehen werden.

- Telearbeitsrechner sollten über Funktionen zur **Datensicherung** verfügen. Diese sollten u. a. folgende Anforderungen erfüllen:
  - Das Datensicherungsprogramm muss benutzerfreundlich und schnell arbeiten. Es sollte automatisierbar sein.
  - Es muss konfigurierbar sein, welche Daten wann gesichert werden.
  - Es muss eine Option zum Einspielen beliebiger Datensicherungen existieren.
  - Die Funktion muss das Sichern von mehreren Generationen ermöglichen.
  - Datensicherungen von Zwischenergebnissen aus der laufenden Anwendung sollen möglich sein.
- Telearbeitsrechner sollten über eine **Verschlüsselungskomponente** verfügen. Hierfür ist zunächst zu überlegen, welche Funktionalität benötigt wird: die Verschlüsselung ausgewählter Daten (offline) oder automatisch der gesamten Festplatte (online). Grundsätzlich sollte die automatische Verschlüsselung aller Datenträger vorgezogen werden, da dies benutzerfreundlicher und effizienter ist. Dies setzt voraus, dass ein geeignetes Verschlüsselungsprodukt eingesetzt wird und dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch der Verschlüsselung) systemseitig abgefangen wird. Darüber hinaus sind folgende Anforderungen sinnvoll:
  - Der implementierte Verschlüsselungsalgorithmus sollte den Anforderungen aus M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* entsprechen.
  - Das Schlüsselmanagement muss mit der Funktionalität des Telearbeitsrechners harmonieren. Dabei sind insbesondere grundsätzliche Unterschiede der Algorithmen zu berücksichtigen: Symmetrische Verfahren benutzen einen geheim zu haltenden Schlüssel für die Ver- und Entschlüsselung, asymmetrische Verfahren benutzen einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten (geheim zu haltenden) für die Entschlüsselung.
  - Der Telearbeitsrechner muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar, auf dem Telearbeitsrechner abgelegt werden.
- Soll der Telearbeitsrechner über Mechanismen zur **Integritätsprüfung** verfügen, sind folgende Anforderungen sinnvoll:
  - Es sollten Verfahren zur Integritätsprüfung eingesetzt werden, die absichtliche Manipulationen am Telearbeitsrechner bzw. den darauf gespeicherten Daten sowie ein unbefugtes Einspielen von Programmen zuverlässig aufdecken können.
  - Bei der Datenübertragung müssen Mechanismen eingesetzt werden, mit denen absichtliche Manipulationen an den Adressfeldern und den Nutzdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, um unerkannte Manipulationen an den oben genannten Daten vornehmen zu können.
- Der Telearbeitsrechner sollte über einen **Boot-Schutz** verfügen, um zu verhindern, dass unbefugt von auswechselbaren Datenträgern, z. B. von DVD oder USB-Stick, gebootet werden kann (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).
- Es sollte möglich sein, die **Benutzerumgebung** des Telearbeitsrechners **einzuschränken**. Damit soll der Administrator festlegen können, welche Programme der Telearbeiter ausführen kann, welche Peripheriegeräte nutzbar sind und welche Änderungen der Telearbeiter am System vornehmen darf. Darüber hinaus sollte der Telearbeiter Einstellungen, die für den

sicheren Betrieb notwendig sind, nicht unautorisiert ändern und nicht unerlaubt Fremdsoftware aufspielen können.
- Auf dem Telearbeitsrechner muss ein residentes **Computer-Viren-Prüfprogramm** installiert sein, um kontinuierlich den Rechner auf Computer-Viren überprüfen zu können (siehe M 4.3 *Einsatz von Viren-Schutzprogrammen*). Vor dem Einspielen von Daten von auswechselbaren Datenträgern, vor der Weitergabe von Datenträgern bzw. beim Senden und Empfangen von Daten muss ein Virencheck durchgeführt werden (siehe M 4.33 *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung* ).
- Wenn der Telearbeitsrechner über **Fernwartung** administriert werden soll, ist sicherzustellen, dass die Fernadministration nur autorisiert durchgeführt werden kann. Bei der Fernwartung muss eine Authentisierung des Fernwartungspersonals, die Verschlüsselung der übertragenen Daten und eine Protokollierung der Administrationsvorgänge gewährleistet sein.
- Die Software auf einem Telearbeitsrechner sollte **benutzerfreundlich** sein. Sie sollte leicht bedienbar, verständlich und gut erlernbar sein, da Telearbeiter stärker auf sich alleine gestellt sind als andere Mitarbeiter. Insbesondere sollten den Benutzern aussagekräftige und nachvollziehbare Dokumentationen des Betriebssystems und aller installierten Programme zur Verfügung gestellt werden.

Aus den obigen Funktionalitäten sind diejenigen auszuwählen, die aufgrund der Sicherheitsanforderungen an die Telearbeitsrechner benötigt werden. Anhand dieser Funktionalitäten muss dann ein geeignetes Betriebssystem als Plattform ausgewählt werden. Wenn dieses nicht alle benötigten Funktionalitäten unterstützt, müssen dazu Zusatzprodukte eingesetzt werden. Dabei sollten möglichst alle Telearbeitsrechner einer Institution gleich ausgestattet sein, um die Betreuung und Wartung zu erleichtern. Zur sicherheitstechnischen Eignungsprüfung sollte Baustein B 1.10 *Standardsoftware* beachtet werden.

Das Gesamtsystem ist durch die Administratoren so zu konfigurieren, dass maximale Sicherheit erreicht werden kann.

Prüffragen:

- Ist dokumentiert, welche der sicherheitsrelevanten Funktionalitäten ein Telearbeitsrechner aufweisen muss und wie diese umgesetzt werden?
- Ist sichergestellt, dass nur autorisierte Personen auf die Telearbeitsrechner bzw. auf die Kommunikationsrechner zugreifen können?
- Ist sichergestellt, dass Telearbeitsrechner nur für autorisierte Zwecke benutzt werden?
- Ist sichergestellt, dass Manipulationen an den Daten, Telearbeitsrechnern und Kommunikationsrechnern erkannt werden können?

# M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Vor dem Versenden einer Datei per E-Mail oder Datenträgeraustausch bzw. vor dem Veröffentlichen einer Datei auf einem Webserver sollte diese daraufhin überprüft werden, ob sie Restinformationen enthält, die nicht zur Veröffentlichung bestimmt sind. Solche Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich können auch die Aktionen sein, die dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Generell sollte Standard-Software wie z. B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen des Benutzers gespeichert.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, mit dem die Datei erstellt wurde.

Dabei ist darauf zu achten, dass nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z. B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr. Um Restinformationen zu beseitigen,

- kann die Datei in einem anderen Dateiformat abgespeichert werden, z. B. als "Nur-Text" oder als HTML,
- können die Nutzdaten in eine zweite Instanz derselben Standard-Software kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte. Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie.

Um der Weitergabe von Informationen vorzubeugen, die ursprünglich mit Wissen der Ersteller eingebracht worden sind, wie z. B. als "verborgen" formatierter Text, dessen Vorhandensein dann aber vergessen wurde, kann es sinnvoll sein, die Datei ausdrucken. Dabei sollten dann alle Optionen aktiviert werden, die beim Drucken versteckte Informationen mitausgeben.

**Restinformationen/Slack-Bytes**

Beim Datenträgeraustausch kann sogenannter Slack-Space ein Problem darstellen. Jedes Betriebssystem hat eine kleinste physikalische Speichereinheit mit festgelegter Größe. Unter DOS ist dies ein Sektor und umfasst 512 Byte. Bei Unix-Systemen ist dies ein Block, die Größe eines Blocks hängt dabei von der eingesetzten Unix-Variante ab. Unter DOS werden die einzelnen Sektoren einer Partition logisch zu Zuordnungseinheiten (Cluster) zusammengefasst. Wie viele Sektoren einen Cluster bilden, hängt von der Größe der Partition ab. Wird eine Datei geöffnet, werden ihr ein oder mehrere Cluster zugeordnet.

Die letzte Zuordnungseinheit wird dabei nicht vollständig benutzt, wenn die Dateigröße der zu speichernden Datei nicht zufällig ein Vielfaches der Clustergröße ist.

Dies verbraucht Speicherplatz. Der durchschnittliche Speicherplatzverbrauch hierdurch steigt mit der Clustergröße. Da diese wiederum mit der Partitionsgröße steigt, sollten Partitionen nicht zu groß sein. Hierzu ein Beispiel: Bei einer Partitionsgröße zwischen 1024 und 2047 MB hat ein einzelner Cluster 32 KB. Damit gehen durchschnittlich bei jeder Datei 16 KB Speicherplatz verloren.

Ein anderes Problem hierbei ist, dass (bei DOS-basierten Betriebssystemen) die restlichen Bytes des letzten Clusters bzw. Blocks mit zufällig im Hauptspeicher stehenden Bytes aufgefüllt werden, sogenannten Slack-Bytes. Diese können sinnlose Einträge, Informationen über die Dateistruktur, aber auch Passwörter enthalten. Auch bei einem Kopiervorgang von einem Datenträger auf den anderen kann die Datei je nach Clustergröße mit Slack-Bytes aufgefüllt werden.

Vor der Weitergabe von Dateien sollte sichergestellt werden, dass diese keine Slack-Bytes mehr enthalten. Dies kann mit Hilfe eines geeigneten Editors (z. B. Hex-Editor) überprüft werden.

Daneben haben viele Windows-Applikationen das Problem, dass das jeweilige Programm bei der Bearbeitung einer Datei den in Anspruch genommenen Speicherplatz nicht durchgehend mit Applikationsdaten überschreibt, sondern dass Lücken entstehen können, die ebenfalls alte Datenbestände des IT-Systems enthalten.

**Verborgener Text / Kommentare**

Eine Datei kann Textpassagen enthalten, die als "versteckt" oder "verborgen" formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche Zusatzinformationen gelöscht werden.

**Änderungsmarkierungen**

Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten.

**Versionsführung**

In praktisch allen aktuellen Office-Suites gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in **einer** Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu riesigen Dateien führen, z. B. wenn Graphiken mitgeführt werden. Auf keinen Fall sollte die Option "Version beim Schließen automatisch speichern" gewählt werden, da hier bei jedem Schließen einer Datei die komplette Vorgängerversion zusätzlich gespeichert wird.

**Dateieigenschaften**

Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei späteren Suchen helfen sollen, Dateien wieder zu finden.

Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, Bearbeiter (nicht nur der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selber angelegt und können nicht durch den Bearbeiter beeinflusst werden. Andere Informationen müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält.

**Schnellspeicherung**

Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt somit weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil ist jedoch, dass die Datei unter Umständen Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungsoptionen abgeschaltet werden.

Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor eine weitere Anwendung ausgeführt wird, die viel Speicherplatz in Anspruch nimmt,
- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und
- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

Prüffragen:

- Werden die Benutzer hinsichtlich der Gefahren von Rest- und Zusatzinformationen in Dateien informiert?
- Werden stichprobenhafte Überprüfungen der Dateien auf enthaltene Restinformationen durchgeführt?
- Werden die Zusatzinformationen von Dateien von Standart-Software ermittelt und überprüft vor der Weitergabe?
- Wird vor der Weitergabe von Dateien darauf geachtet das diese keine Slack-Bytes enthalten?
- Wird auf die Speicherung verschiedener Versionen eines Dokumentes in einer Datei verzichtet?

# M 4.65 Test neuer Hard- und Software

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Vor dem Einsatz neuer Hardware-Komponenten oder neuer Software in der Produktivumgebung müssen diese auf speziellen Testsystemen kontrolliert werden. Neben der Lauffähigkeit des Produktes ist dabei insbesondere zu überprüfen, dass der Einsatz neuer Komponenten keine negativen Auswirkungen auf die laufenden IT-Systeme hat. Da vor erfolgreichen Tests Schadfunktionen nicht ausgeschlossen werden können und da bei Tests Fehler provoziert werden, sind immer **vom Produktionsbetrieb isolierte** Testsysteme zu verwenden.

Der Einsatz isolierter Testsysteme ist auch erforderlich, um selbstextrahierende Dateien, die z. B. per E-Mail empfangen wurden, auf Schadfunktionen zu prüfen.

Generelle Verfahrensweisen für die Software-Abnahme und -Freigabe inklusive des Testens sind in Baustein B 1.10 *Standardsoftware* beschrieben. Erst nach bestandenem Test dürfen neue Komponenten für die Installation auf Produktionssystemen freigegeben werden.

Prüffragen:

- Werden alle neuen IT-Komponenten vor dem Einsatz getestet?
- Werden die Tests ausschließlich auf isolierten Testsystemen durchgeführt?

# M 4.66 Novell Netware - Sicherer Übergang ins Jahr 2000

Diese Maßnahme ist mit Version 2004 entfallen.

# M 4.67 Sperren und Löschen nicht benötigter Datenbank-Accounts

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wenn ein neu einzurichtender Benutzer seinen Datenbank-Account nur für einen befristeten Zeitraum benötigt, sollte dieser auch nur befristet eingerichtet werden, falls die Datenbank eine solche Möglichkeit zur Verfügung stellt. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z. B. jährlich) bei Bedarf zu verlängern.

Darüberhinaus sollte die Datenbankadministration schnellstmöglichst über das endgültige Ausscheiden eines Benutzers informiert werden. Spätestens am letzten Arbeitstag des Benutzers ist dessen Account zu sperren.

Auch wenn Benutzer in ein anderes Aufgabengebiet, einen anderen Zuständigkeitsbereich oder andere Projekte wechseln, müssen die dafür nicht mehr benötigten Datenbank-Accounts gesperrt oder die Zugriffsrechte entsprechend angepasst werden.

Weiterhin sollte regelmäßig geprüft werden, ob vorhandene Datenbank-Accounts tatsächlich benötigt werden. Insbesondere sollten hierbei auch nicht benötigte Standard-Accounts gesperrt werden.

Prüffragen:

- Werden Datenbank-Accounts befristet eingerichtet, mindestens wenn der Benutzer diesen nur für einen befristeten Zeitraum benötigt und die technische Möglichkeit besteht?
- Wird regelmäßig überprüft, ob vorhandene Datenbank-Accounts mit den spezifizierten Zugriffsrechten noch benötigt werden?
- Werden nicht benötigte Datenbank-Accounts, insbesondere auch Standard-Accounts, gesperrt bzw. die Zugriffsrechte entsprechend angepasst?

# M 4.68 Sicherstellung einer konsistenten Datenbankverwaltung

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Datenbankverwaltung steht im Zentrum des Betriebskonzepts eines Datenbanksystems (DBS), auf dessen Grundlage unter anderem die konsistente Datenbankverwaltung sichergestellt werden soll. Im Betriebskonzept müssen alle für den Betrieb des DBS wichtigen Prozesse mit fest definierten Ausgangspunkten, Durchführungsreihenfolgen und Zielen sowie die zur Durchführung der Prozesse berechtigten Rollen mit ihren Rechten und Pflichten definiert sein.

Im weiteren Verlauf des Projekts müssen darüber hinaus den definierten Rollen reale Personen zugeordnet werden.

In der Rollenbeschreibung werden die Aufgaben, Zugriffsrechte und Befugnisse der Rollen beschrieben, die zur Durchführung bestimmter Funktionen notwendig sind (siehe auch M 2.132 *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen*). Im Datenbank-Managementsystem (DBMS) sind die definierten Rollen als Benutzergruppen einzurichten, denen die rollenspezifische Rechte zuzuordnen sind. Den Benutzergruppen werden gemäß Rollenprofil die zuständigen Benutzer über ihre Benutzerkennung zugeordnet.

Besonders zu beachten sind nachfolgende Hinweise:

- Der Systemadministrator ist ein spezieller Benutzer in der Rechteverwaltung des Datenbanksystems, der bereits nach der Installation des DBMS zur Verfügung steht. Dieser Benutzer unterliegt prinzipiell keinerlei Beschränkungen bei der Nutzung des Datenbanksystems, wodurch ein Risiko für Fehler oder Missbrauch besteht. Diese Kennung darf nur von dem kleinen Kreis der System-Administratoren für explizit festgelegte Administrationsaufgaben, wie die Einrichtung von Datenbank-Administratoren für einzelne Datenbanken genutzt werden.
- Die Benutzergruppen der Datenbank-Administratoren für einzelne Datenbanken und somit auch die jeweils zugeordneten Benutzer unterliegen prinzipiell keinerlei Beschränkungen bei Nutzung und Manipulation der Datenbanken in ihrem Zuständigkeitsbereich, wodurch ein generelles Gefahrenpotential besteht. Die Rechte, die für diese Aufgaben notwendig sind, müssen daher wie der Personenkreis, der mit diesen Rechten ausgestattet wird, klar definiert und dokumentiert sein.
- In vielen Fällen arbeiten die Administratoren auch als Benutzer auf einer Datenbank, da sie neben ihrer Administratorentätigkeit Benutzeraufgaben wahrnehmen oder die Datenbank für die Ablage und Verwaltung von Dokumentationen im Administrationsumfeld nutzen. In diesem Fall ist für sie, neben der Administratorenkennung, eine normale Benutzerkennung anzulegen, die für solche Arbeiten mit der Datenbank genutzt wird. Die Administratorenkennung darf nur für Administrationstätigkeiten genutzt werden.
- Die Zuordnung eines Benutzers zu mehreren Benutzergruppen sollte genau geplant werden, da der Benutzer die Summe der Berechtigungen aller Benutzergruppen erhält, denen er zugeordnet ist.

Zusätzlich sollte durch eine klare Aufgabenteilung, verbindliche Regelungen sowie Absprachen zwischen den Administratoren sichergestellt werden, dass Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Dabei sollten folgende Bedingungen erfüllt sein:

- Die Art und Weise der Durchführung von Änderungen sowie deren Dokumentation ist festzulegen.
- Art, Umfang und Grund der Änderungen sind zu beschreiben.
- Änderungen an Datenbankobjekten oder Daten sind prinzipiell durch den Verantwortlichen der IT-Anwendung genehmigungspflichtig. Handelt es sich dabei um ein zentrales Datenbankobjekt, so erfordert eine Änderung die Zustimmung aller Verantwortlichen der betroffenen IT-Anwendungen.
- Der Zeitpunkt der geplanten Änderungen ist festzulegen und bekannt zu geben.
- Vor der Durchführung von Änderungen muss die Datenbank komplett gesichert werden.
- Für den laufenden Betrieb sollte ein Kontrollintervall festgelegt werden, in dem die Dokumente/Protokolle auf Aktualität und Korrektheit überprüft werden (siehe auch M 4.69 *Regelmäßiger Sicherheitscheck der Datenbank*).

Um Gefährdungen der Datenbankintegrität und Inkonsistenzen einzelner Datensätze zu vermeiden, sollten alle Datenbankobjekte einer Anwendung unter die ausschließliche Verwaltung einer eigens für die jeweilige Anwendung eingerichteten Benutzergruppe gestellt werden. Dieser Benutzergruppe dürfen ausschließlich Anwender zugeordnet werden, die direkte Zugriffsrechte auf die Datenbankobjekte der betreffenden Anwendung zu ihrer Aufgabenerfüllung benötigen. Außerdem sollte der für die jeweilige Anwendung zuständige Datenbankadministrator Mitglied dieser Benutzergruppe sein.

Prüffragen:

- Sind alle für den Betrieb des Datenbanksystems wichtigen Prozesse zur Administration und Nutzung der Datenbank und die zur Durchführung dieser Prozesse berechtigten Rollen mit ihren Rechten und Pflichten in einem Betriebskonzept definiert?
- Verfügt jeder Datenbank-Administrator über eine zusätzliche Benutzer-Kennung mit eingeschränkten Rechten für nicht-administrative Tätigkeiten auf der Datenbank?
- Gibt es verbindliche Regelungen für Administratoren, die inkonsistente oder unvollständige Eingriffe in die Datenbank verhindern (u. a. Dokumentation von Änderungen an der Datenbank, Genehmigungspflicht von Änderungen, Komplettsicherung vor Änderungen, regelmäßige Prüfungen)?

# M 4.69 Regelmäßiger Sicherheitscheck der Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Datenbankadministrator sollte regelmäßig, jedoch mindestens einmal monatlich einen Sicherheitscheck des Datenbanksystems (DBS) durchführen, der durch das Betriebskonzept geregelt sein sollte. In Abhängigkeit der Prüfungsergebnisse sollten entsprechende Maßnahmen ergriffen werden, um Abweichungen von den Vorgaben des Betriebskonzepts abzustellen. Diese Maßnahmen und die Zuständigkeiten für die Umsetzung sollten ebenfalls im Betriebskonzept festgelegt sein.

Folgende Aspekte sollten im Rahmen des Sicherheitschecks mindestens überprüft werden, wobei die mit (*) markierten Punkte meist durch entsprechende Skripte automatisiert werden können:

- Werden die im Betriebskonzept vorgegebenen Nachweise (z. B. Dokumentation von Änderungen) korrekt erstellt?
- Sind die erforderlichen und geplanten Sicherungs- und Sicherheitsmechanismen aktiv und greifen sie auch?
- Gibt es Datenbank-Benutzer mit leicht zu ermittelndem oder keinem Passwort? (*)
- Gibt es Benutzer, die die ihnen zugewiesenen Rechte nicht mehr für ihre Aufgabenerfüllung benötigen?
- Wer darf bzw. kann außer dem Datenbank-Administrator auf die Dateien der Datenbank-Software bzw. auf die Dateien der Datenbank auf Betriebssystemebene zugreifen? (*)
- Wer hat außer dem Datenbank-Administrator Zugriff auf die System-Tabellen der Datenbanken?
- Wer darf mit einem interaktiven SQL-Editor auf die Datenbank zugreifen?
- Welche Benutzer-Kennungen haben modifizierende Zugriffsrechte auf die Datenbankobjekte der Anwendungen? (*)
- Welche Benutzer-Kennungen haben lesende und / oder modifizierende Zugriffsrechte auf die Daten der Anwendungen? (*)
- Welche Benutzer besitzen die gleichen Rechte wie der Datenbank-Administrator? (*)
- Verfügt das Datenbanksystem über ausreichend freie Ressourcen? (*)

Prüffragen:

- Erfolgt regelmäßig ein Sicherheitscheck des Datenbanksystems?
- Werden aufgrund der Ergebnisse des Sicherheitschecks des Datenbanksystems notwendige Maßnahmen zur Beseitigung von Abweichungen eingeleitet?
- Ist die Durchführung des Sicherheitschecks im Betriebskonzept zum Datenbanksystem geregelt?

# M 4.70 Durchführung einer Datenbanküberwachung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Verfügbarkeit, die Datenbankintegrität und die Vertraulichkeit der Daten gewährleisten zu können, ist eine regelmäßige und in angemessen definierten Überwachungszeiträumen durchzuführende Datenbanküberwachung erforderlich. Dabei zu beachtende Aspekte, die im folgenden kurz erläutert werden, sind unter anderen die Datenfragmentierung innerhalb der Datenbank, das aktuelle Datenvolumen und dessen Veränderung hinsichtlich der vorhandenen Ressourcen (Füllgrad) sowie die Auslastung der Datenbank.

**Datenfragmentierung**

Die Datenbank ist in regelmäßigen Zeitabständen hinsichtlich einer möglichen Fragmentierung zu überprüfen, um gegebenenfalls Maßnahmen, wie z. B. eine Reorganisation der Datenbank, planen und durchführen zu können.

Die Speicherplatzverwaltung in einem Datenbankmanagementsystem (DBMS) geschieht in der Regel in Form von Blöcken fester Größe, d. h. eine Veränderung (meist Vergrößerung) des Speicherplatzes erfolgt nur in Blöcken. Datensätze werden dabei auf eine minimale Anzahl von Blöcken verteilt abgespeichert. Prinzipiell werden Daten hinzugefügt, indem zuerst freie Blöcke belegt und wenn nötig zusätzlich neue Blöcke angelegt werden. Beim Löschen werden die zugehörigen Blöcke wieder freigegeben und stehen für neue Daten zur Verfügung.

Im Laufe der Zeit entsteht durch Datenveränderungen im Speicherbereich eine Abfolge von belegten und unbelegten Blöcken sowie eine immer größere Anzahl unvollständig belegter Blöcke. Darüberhinaus werden die Datensätze physikalisch weit über die Speichermedien verteilt. Diese Fragmentierung erhöht nicht nur den Speicherbedarf, sondern verlangsamt auch Datenbankoperationen, da Datensätze und freier Speicherplatz erst über einen größeren Speicherbereich gesucht werden müssen.

Sollte die Fragmentierung der Datenbank aufgrund der oben genannten Gründe eine festgelegte Grenze überschreiten, muss eine Reorganisation durchgeführt werden. Datenbank-Hersteller und Drittanbieter stellen zur Unterstützung dieser Aufgaben Administrations- und Hilfsprogramme zur Verfügung.

**Datenvolumen und Füllgrad**

Um einer zu starken bzw. zu raschen Fragmentierung vorzubeugen, erlauben einige Datenbankmanagementsysteme durch Definition bestimmter Parameter bereits beim Anlegen der Tabellen, eine bestimmte Menge zusammenhängender Blöcke zu reservieren. Damit steigt bei gleichem Datenvolumen der Füllgrad.

Die Datenbankdateien sollten regelmäßig hinsichtlich ihres Datenvolumen und Füllgrades überwacht werden. Dabei wird regelmäßig überprüft, ob sich das Datenvolumen zusammen mit dem Füllgrad im vorgegebenen Rahmen verändert. Ist das Wachstum größer als erwartet, kann es unter Umständen zu Speicherengpässen kommen. Aus den Beobachtungen sollten Maßnahmen, wie z. B. eine Erweiterung der Speicherkapazitäten, abgeleitet werden.

**Beispiel:**

Bei einer Oracle-Datenbank wird jeder Tabelle eine feste Anzahl von Extents (im Sprachgebrauch von Oracle: logische Größeneinheit) zugeordnet. Die Daten einer Tabelle werden in mindestens einem Extent abgelegt. Sobald die Kapazität eines Extents ausgeschöpft ist, legt das DBMS automatisch ein weiteres Extent an. Beim Erstellen einer Tabelle können dabei folgende Werte definiert werden:

- Größe des ersten und nachfolgenden Extents in Bytes
- Wachstum aller weiteren Extents in Prozent, wobei diese Zahl in Relation zur Größe des zweiten Extents steht
- Maximale Anzahl an Extents, die für die Tabelle angelegt werden dürfen
- Reservierte Blöcke für spätere Änderungen in Prozent

Wenn durch Anlage weiterer Extents der freie Speicherbereich innerhalb eines Tablespaces (siehe Beispiel in G 2.39 *Mangelhafte Konzeption eines DBMS*) zu gering wird, muss ein neuer Tablespace hinzugefügt werden. Eine Verringerung der Anzahl der Tablespaces ist nur durch vollständige Reorganisation möglich.

**Auslastung**

Darüber hinaus ist die Auslastung der Datenbank regelmäßig zu prüfen, insbesondere im Hinblick auf die eingestellten Obergrenzen (siehe M 4.73 *Festlegung von Obergrenzen für selektierbare Datensätze*).

Welche Informationen für eine konkrete Datenbanküberwachung relevant sind, hängt von deren spezieller Funktionsweise, also von der eingesetzten Datenbank-Standardsoftware ab. Dementsprechend sind auch individuelle Maßnahmen einzuleiten, die die Datenbankkonfiguration dahingehend modifizieren, dass sie den Anforderungen hinsichtlich Zugriffsgeschwindigkeiten, durchzuführender Transaktionen usw. gerecht wird.

Eine Automatisierung der Datenbanküberwachung kann in vielen Fällen mit Hilfe von Skripten durchgeführt werden. Eine Voraussetzung ist allerdings, dass die Informationen in auswertbarer Form von der eingesetzten Datenbank-Software zur Verfügung gestellt werden.

Prüffragen:

- Wird die Datenbank regelmäßig hinsichtlich einer möglichen Datenfragmentierung überwacht und überprüft?
- Werden die Datenbankdateien regelmäßig hinsichtlich ihres Datenvolumens und Füllgrades überwacht und überprüft?
- Wird die Datenbank regelmäßig hinsichtlich ihrer Auslastung überwacht und überprüft?

# M 4.71 Restriktive Handhabung von Datenbank-Links

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Über Datenbank-Links (DB-Links) besteht die Möglichkeit, von einer Datenbank innerhalb eines DBMS aus auf die Daten einer anderen Datenbank, gegebenenfalls in einem anderen DBMS, zuzugreifen. Um einen angemessenen Schutz der Daten zu gewährleisten, sollte diese Technik nur im Rahmen eines entsprechenden Berechtigungskonzepts angewendet werden. In diesem Konzept muss unter anderem die Kontrolle der Berechtigungen eines Benutzers bei der Verwendung von DB-Links geregelt werden.

So kann festgelegt werden, dass ein Benutzer prinzipiell die Möglichkeit erhält, auf eine fremde Datenbank zuzugreifen, wenn dort die gleiche Benutzer-Kennung existiert, mit der sich der Benutzer an der lokalen Datenbank anmeldet. Einen weitergehenderen Schutz erhält man durch die Möglichkeit, einen DB-Link mit expliziter Angabe einer Benutzer-Kennung und eines Passwortes zu erstellen.

Nachfolgende Aspekte sollten im Hinblick auf DB-Links in einem Berechtigungskonzept geregelt werden:

- Im allgemeinen sollte nur der Administrator das Recht besitzen, mittels der entsprechenden CREATE-Kommandos DB-Links zu erstellen. Insbesondere gilt dies für DB-Links, die von allen Datenbankbenutzern genutzt werden dürfen (sogenannte PUBLIC DB-Links). Die Berechtigung zur Erstellung von DB-Links sollte dagegen für normale Benutzer-Kennungen nicht vergeben werden.
- Die Anzahl von parallel nutzbaren DB-Links eines Benutzers sollte begrenzt werden, um die Belastung der Datenbank-Server unter Kontrolle halten zu können (siehe M 4.73 *Festlegung von Obergrenzen für selektierbare Datensätze*). Ansonsten kann ein Angreifer dies ausnutzen, um den Durchsatz der Datenbank-Server zu reduzieren oder diese sogar vollständig zu überlasten.
- Eine Dokumentation der vom Administrator angelegten DB-Links ist unabdingbar. Die Dokumentation sollte neben der Verbindungsart (über eine spezielle Benutzer-Kennung oder unter der Voraussetzung, dass die jeweilige aktuelle Datenbank-Kennung ebenfalls für die verbundene Datenbank angelegt wurde) auch beinhalten, welcher Benutzerkreis in der Lage ist, den entsprechenden DB-Link zu nutzen.

Prüffragen:

- Gibt es ein Berechtigungskonzept für die Verwendung von Datenbank-Links?
- Besitzt ausschließlich der Administrator das Recht zur Erstellung von Datenbank-Links?

# M 4.72 Datenbank-Verschlüsselung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler

In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln. Dabei kann zwischen einer Online- und einer Offline-Verschlüsselung unterschieden werden:

- Bei einer Online-Verschlüsselung werden die Daten während des laufenden Betriebs ver- und entschlüsselt, ohne dass die betroffenen Benutzer davon etwas merken. Dafür können Tools eingesetzt werden, mit denen entweder auf Betriebssystemebene die gesamte Festplatte verschlüsselt wird, oder solche, mit denen nur die Anwendungsdaten der Datenbank verschlüsselt werden.
- Bei einer Offline-Verschlüsselung werden die Daten erst nach ihrer Bearbeitung verschlüsselt und vor ihrer Weiterverarbeitung wieder entschlüsselt. Dies wird im allgemeinen mit Tools durchgeführt, die nicht in das Datenbanksystem integriert sind, und kann insbesondere für Datensicherungen oder Datenübertragungen sinnvoll sein. Dabei ist zu beachten, dass genügend Platz auf der Festplatte vorhanden ist, da die Ver- bzw. Entschlüsselung nur dann erfolgreich ausgeführt werden kann, wenn auf der Festplatte genügend Platz für das Original und die verschlüsselte Version der Datenbank verfügbar ist.

Darüber hinaus besteht die Möglichkeit, Daten weiterhin im Klartext in der Datenbank abzuspeichern, beim Zugriff über ein Netz jedoch eine verschlüsselte Datenübertragung zu realisieren. Dies kann z. B. durch die *Secure Network Services* der Oracle SQL*Net Produktfamilie durchgeführt werden.

Welche Daten mit welchem Verfahren zu verschlüsseln sind, ist am besten bereits bei der Auswahl der Datenbank-Standardsoftware festzustellen (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*). Dabei sollten die Anforderungen hinsichtlich der Verschlüsselung von Datenbeständen mit den entsprechenden Leistungsmerkmalen der Datenbank-Software verglichen werden. Als Mindestanforderung sollte sie in jedem Fall sicherstellen, dass die Passwörter der Benutzer-Kennungen der Datenbank verschlüsselt abgelegt sind.

Falls die Anforderungen durch keine der am Markt verfügbaren Datenbank-Standardsoftware abgedeckt werden können, sollte man den Einsatz von Zusatzprodukten prüfen, um die entsprechende Sicherheitslücke zu schließen. Falls auch keine Zusatzprodukte erhältlich sind, muss ein Konzept für die Umsetzung einer Verschlüsselungsstrategie erstellt werden, das im Unternehmen bzw. in der Behörde umgesetzt wird.

Prüffragen:

- Sofern die Informationen der Datenbank es erfordern, werden von der Datenbank oder durch Zusatzprodukte geeignete Techniken zur Verschlüsselung bereitgestellt und genutzt?

# M 4.73 Festlegung von Obergrenzen für selektierbare Datensätze

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Anwendungsentwickler

Um den Zugriff auf ein Datenbanksystem besser kontrollieren zu können und um die Performance zu verbessern, sollten Obergrenzen für bestimmte Parameter von Datenbank-Systemen festgelegt werden.

Zudem kann durch diese Maßnahme die Wahrscheinlichkeit bestimmter Arten von Denial-of-Service-Attacken (siehe G 5.65 *Verhinderung der Dienste eines Datenbanksystems*) verringert werden.

Beispiele sind:

- die Festlegung von Obergrenzen für Datensätze, die im Rahmen eines Datenzugriffs selektiert werden können
- die maximale Anzahl von Anmeldungen pro Benutzer-Kennung
- der maximale Anspruch auf CPU-Zeit pro Anmeldung
- die Gesamtdauer einer Datenbankverbindung
- die maximal zulässige inaktive Zeit während einer Anmeldung

Dabei sind vor allem folgende Hinweise zu beachten:

**Festlegung von Obergrenzen für selektierbare Datensätze**

Insbesondere wenn große Datenmengen in einer Datenbank abgelegt wurden, sollte eine maximale Anzahl von Datensätzen definiert werden, die im Rahmen eines Datenzugriffs selektiert werden können.

Existieren solche Obergrenzen nicht, kann ein Benutzer gezielt oder unbeabsichtigt beliebig umfangreiche Selektierungen durchführen. Dies behindert nicht nur den einzelnen Benutzer in seiner Arbeit, sondern führt unter Umständen auch bei allen anderen Benutzern der Datenbank zu langen Wartezeiten. Werden die Datensätze dabei selektiert um sie zu modifizieren, sind sie solange für alle anderen Benutzer gesperrt, bis die Transaktion beendet ist.

Die Obergrenzen müssen im Rahmen der Anwendungen definiert werden, die auf die Datenbank zugreifen. Dabei müssen geeignete Kontrollen bzw. Sperren realisiert werden, die die Einhaltung der Obergrenzen überwachen. Stellt eine Anwendung Suchfunktionalitäten bereit, so sollte die uneingeschränkte Suche generell abgelehnt und die Eingabe von Suchkriterien gefordert werden.

Sollte zwischen Anwendungsprogramm und Datenbank eine große Distanz liegen (z. B. Anbindung über Internet) sollten Ergebnisse in Blöcken ausgetauscht werden, für die ebenfalls Obergrenzen festzulegen sind.

**Beispiel:**

Ein Anwendungsprogramm greift über eine Internetverbindung auf eine Datenbank zu. Die vom Anwendungsprogramm an die Datenbank übergebenen Abfragen liefern potentiell sehr große Datenmengen zurück. Um nicht Gefahr zu laufen, durch zu große Ergebnisblöcke die Übertragung an die Anwendung zu verlangsamen, wird auf der Datenbank die Abfrage in einer Prozedur gekapselt. Diese Prozedur überträgt bei jedem Aufruf eine festgelegte Menge von Daten (beispielsweise 5 Datensätze), bis alle Ergebnisse vollständig über-

tragen sind. Die Anwendung schickt in einer Schleife Anfragen an das DBMS und setzt die erhaltenen Teilergebnisse wieder zusammen oder kann eventuell auch schon Teilergebnisse anzeigen.

**Festlegung von Ressourcenbeschränkungen**

Eine weitere Möglichkeit, die von einigen Herstellern angeboten wird, ist die Festlegung von Ressourcenbeschränkungen in Bezug auf die Benutzung einer Datenbank.

**Beispiele:**

Mit folgendem Kommando wird in einer Oracle-Datenbank für die Datenbankkennung "Meier" der temporäre Tablespace "Temp" auf 100 MB begrenzt:

ALTER USER Meier TEMPORARY TABLESPACE Temp QUOTA 100M ON Temp;

Mit dem nachfolgenden Befehl wird ein Profil "Tester" erstellt, das die Anzahl der Sessions, die maximale CPU-Zeit pro Session, die maximale Zeit einer Datenbankverbindung und die maximale Leerlaufzeit (IDLE) begrenzt. Dieses Profil kann dann einzelnen Benutzern zugeordnet werden.

CREATE PROFILE Tester LIMIT

SESSIONS PER USER 2,
CPU _PER_SESSION 6000,
IDLE_TIME 30,
CONNECT_TIME 500;

Eine Ingres-Datenbank erlaubt beispielsweise für Benutzer und Gruppen das Setzen von Grenzen für die maximale Ein- und Ausgabe je Abfrage oder für die Anzahl von Sätzen pro Abfrage.

Weiterhin kann die Anzahl der Benutzer beschränkt werden, die gleichzeitig auf die Datenbank zugreifen dürfen. Je nach Lizenzmodell kann durch deren Begrenzung mittels Parametereinstellungen im DBMS unter Umständen auch gewährleistet werden, dass die maximal zur Verfügung stehende Zahl an Lizenzen für die Datenbank-Software nicht überschritten wird.

Außerdem verursachen viele parallel zugreifende Benutzer eine hohe Arbeitslast, der der Datenbank-Server eventuell nicht gewachsen ist. Hierdurch verlängert sich die durchschnittliche Dauer einer Transaktion. Ist in diesem Fall eine Erweiterung der Ressourcen des Datenbanksystems nicht möglich oder nicht gewünscht, schafft hier eine Begrenzung der maximal möglichen parallelen Benutzerzugriffe ebenfalls Abhilfe.

Auf der anderen Seite kann eine Begrenzung der maximal möglichen parallelen Benutzerzugriffe auch zu starken Einbußen bei der Performance für die Benutzer führen. Diese Funktionalität sollte deshalb nur nach genauer Prüfung oder temporär, beispielsweise in einmalig auftretenden Spitzenzeiten, eingesetzt werden.

Wenn die Zahl der Datenbankbenutzer zunimmt und absehbar ist, dass die aktuellen Ressourcen zukünftig die Anforderungen an die Performance nicht mehr erfüllen können oder dass mehr Lizenzen benötigt werden, ist eine entsprechende Erweiterung vorzusehen und zu planen.

Die absehbaren Anforderungen sollten bereits während der Auswahl einer Datenbank-Standardsoftware geklärt werden, um gegebenenfalls ein Kon-

zept zur Umsetzung der Ressourcenbeschränkungen zu erstellen (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*).

Prüffragen:

- Wurden Obergrenzen für bestimmte Parameter (z. B. selektierbare Datensätze, Ressourcenbeschränkungen für Benutzer) von Datenbank-Systemen festgelegt und dokumentiert?

# M 4.74 Vernetzte Windows 95 Rechner

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 4.75 Schutz der Registry unter Windows-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In der Registry eines Windows-Systems werden alle wichtigen Konfigurations- und Initialisierungsinformationen gespeichert. Dort wird unter anderem die SAM-Datenbank verwaltet, die die Benutzer- und Computerkonten enthält. Dies gilt insbesondere für Rechner, die keiner Domäne angeschlossen sind, oder Domänen-Rechner, auf denen auch lokale Konten benutzt werden.

Die Registry eines Windows-Systems besteht aus mehreren Dateien, die sich in dem Verzeichnis *%SystemRoot%\SYSTEM32\Config* befinden. Aus diesem Grund sollten die Zugriffsrechte auf dieses Verzeichnis und die darin enthaltenen Dateien so gesetzt werden, wie dies in M 4.149 *Datei- und Freigabeberechtigungen unter Windows* und M 4.247 *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista* vorgeschlagen wird.

Zur Erhöhung des Schutzes sollten unmittelbar nach der Installation von Windows-Betriebssystemen die folgenden sicherheitsrelevanten Teile der Registry durch expliziten Eintrag von Zugriffsrechten mit Hilfe des Registry-Editors besonders geschützt werden. Dies erfolgt mit Hilfe der Programme *regedt32.exe* oder *regedit.exe* im Windows-Systemverzeichnis *%SystemRoot%\SYSTEM32.* Die Einstellungen sollten so erfolgen, dass die Gruppe *Jeder* für diese Teile der Registry nur über die Zugriffsrechte *Wert einsehen*, *Teilschlüssel auflisten*, *Benachrichtigen* und *Zugriff lesen* verfügt:

- Im Bereich HKEY_LOCAL_MACHINE gilt das für folgende Schlüssel:
  \Software\Windows3.1MigrationStatus (mit allen Unterschlüsseln)
  \Software\Microsoft\RPC (mit allen Unterschlüsseln)
  \Software\Microsoft\Windows NT\CurrentVersion
- Unter dem Schlüssel \Software\Microsoft\Windows NT\CurrentVersion\ sind das diese Einträge:
  + Profile List+ AeDebug
  + Compatibility
  + Drivers
  + Embedding
  + Fonts
  + FontSubstitutes
  + GRE_Initialize
  + MCI
  + MCI Extensions
  + Port (mit allen Unterschlüsseln)
  + WOW (mit allen Unterschlüsseln)
- und im Bereich HKEY_CLASSES_ROOT ist folgender Bereich zu schützen:
  \HKEY_CLASSES_ROOT (mit allen Unterschlüsseln)

Die entsprechenden Einstellungen für Zugriffsrechte auf die Registry unter Windows XP, Vista und Windows 7 sind in M 4.247 *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista* zu finden.

In einer Windows Server 2003 Domäne sollte der Zugriff auf die Schlüssel HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE und HKEY_USERS durch Gruppenrichtlinien über das Active Directory konfiguriert werden.

Dabei ist sorgfältig vorzugehen, da fehlerhafte Einstellungen in der Registry dazu führen können, dass das System nicht mehr lauffähig ist und nach dem nächsten Starten eventuell nicht mehr bootet. Die hier genannten Einstellungen sollten daher zunächst auf ein Testsystem angewendet und auf ihre Lauffähigkeit in der aktuellen Umgebung kritisch geprüft werden, ehe sie allgemein eingesetzt werden.

**Netzzugriff auf die Registry**

Sofern diese Funktionalität nicht gebraucht wird, sollte auch der Zugriff über das Netz auf die Registry gesperrt werden. Dies ist ab Windows NT 4.0 möglich, indem der Eintrag *winreg* im Schlüssel /*System/CurrentControlSet/Control/SecurePipeServers* im Bereich HKEY_LOCAL_MACHINE entsprechend konfiguriert wird.

Prüffragen:

- Wurde der Zugriff durch die Gruppe Jeder auf die Registry eingeschränkt?
- Werden Änderungen an der Registry vorher auf einem Testsystem ausführlich getestet?

# M 4.76 Sichere Systemversion von Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.77 Schutz der Administratorkonten unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Durchführung von Änderungen an einem IT-System im Echtbetrieb ist immer als kritisch einzustufen und entsprechend sorgfältig muss hierbei vorgegangen werden.

Bevor mit Änderungen am System begonnen wird, muss als erstes die alte Konfiguration gesichert werden, sodass sie schnell verfügbar ist, wenn Probleme mit der neuen Konfiguration auftreten.

Bei vernetzten IT-Systemen müssen die Benutzer rechtzeitig über die Durchführung von Wartungsarbeiten in geeigneter Weise, wie z. B. durch einen Eintrag im Intranet oder per E-Mail, informiert werden, damit sie zum einen ihre Planung auf eine zeitweise Systemabschaltung einrichten können, und zum anderen nach Änderungen auftretende Probleme richtig zuordnen können.

Die Konfigurationsänderungen sollten immer nur schrittweise durchgeführt werden. Zwischendurch sollte immer wieder überprüft werden, ob die Änderungen korrekt durchgeführt wurden und das IT-System sowie die betroffenen Applikationen noch lauffähig sind.

Bei Änderungen an Systemdateien ist anschließend ein Neustart durchzuführen, um zu überprüfen, ob sich das IT-System korrekt starten lässt. Für Problemfälle sind alle für einen Notstart benötigten Datenträger vorrätig zu halten, z. B. Boot-Medien, Start-CD-ROM.

Vor Konfigurationsänderungen sollten von allen eventuell betroffenen Dateien und Verzeichnissen Datensicherungen angefertigt werden. Komplexere Konfigurationsänderungen sollten möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen sollten nach dem Vier-Augen-Prinzip überprüft werden, bevor sie in den Echtbetrieb übernommen werden.

Bei IT-Systemen mit hohen Verfügbarkeitsanforderungen ist auf Ersatzsysteme zurückzugreifen bzw. zumindest ein eingeschränkter IT-Betrieb zu gewährleisten. Das Vorgehen kann sich dabei idealerweise nach dem Notfall-Handbuch richten.

Die durchgeführten Konfigurationsänderungen sollten Schritt für Schritt notiert werden, so dass bei auftretenden Problemen das IT-System durch sukzessive Rücknahme der Änderungen wieder in einen lauffähigen Zustand gebracht werden kann (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Prüffragen:

- Werden die Benutzer über Wartungsarbeiten in geeigneter Weise informiert?
- Werden von allen Dateien, an denen Änderungen vorgenommen werden müssen, Datensicherungen angelegt?

# M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei vielen aktiven Netzkomponenten kann über einen lokalen Zugriff die Administration der Komponenten erfolgen. Solch ein lokaler Zugriff ist zumeist über einen seriellen Anschluss realisiert. Für einen sicheren lokalen Zugriff sind die folgenden Maßnahmen zu beachten:

- Die aktiven Netzkomponenten und ihre Peripheriegeräte, wie z. B. angeschlossene Terminals, müssen sicher aufgestellt werden (siehe M 1.29 *Geeignete Aufstellung eines IT-Systems*),
- der lokale Zugriff zur Administration der lokalen Komponenten muss softwaretechnisch und/oder mechanisch gesperrt werden,
- ein eventuell vorhandenes Standardpasswort für den lokalen Zugriff muss sofort nach Inbetriebnahme geändert werden (zur Auswahl des neuen Passwortes siehe M 2.11 *Regelung des Passwortgebrauchs*),
- die Sicherheitseigenschaften dauerhaft angeschlossener Terminals oder Rechner, wie z. B. automatische Bildschirmsperre oder Auto-Logout, sind zu aktivieren.
- jeder autorisierte Administrator sollte über eine eigene Benutzerkennung verfügen.

Eine lokale Administration bietet folgende Vorteile:

- Die Gefahr des Abhörens von Passwörtern wird reduziert.
- Auch bei einem Ausfall des Netzsegmentes, in dem sich die aktive Komponente befindet, oder bei einem Ausfall des gesamten Netzes ist eine Administration weiterhin möglich.

Eine lokale Administration bietet allerdings auch folgende Nachteile:

- Aktive Netzkomponenten können im Allgemeinen so konfiguriert werden, dass eine lokale oder eine zentrale Administration der aktiven Netzkomponenten möglich ist. Für die Auswahl der Konfigurationsmethode kann jedoch keine generelle Empfehlung gegeben werden. Zu berücksichtigen ist jedoch, dass bei der Konfiguration für eine ausschließlich lokale Administration keine zentrale Administration der aktiven Netzkomponenten mehr möglich ist. Diese muss dann immer vor Ort direkt an den entsprechenden Komponenten vorgenommen werden. In diesem Fall erhöht sich auch die Reaktionszeit im Störungsfall, da unter Umständen längere Wege bis zum Standort der Komponente zurückzulegen sind.
- Der lokale Zugriff ist durch die Realisierung über eine serielle Schnittstelle im Allgemeinen langsamer als ein Fernzugriff über das Netz.

Prüffragen:

- Ist der lokale Zugriff zur Administration der aktiven Netzkomponenten softwaretechnisch und/oder mechanisch abgesichert?
- Werden Standardpasswörter vor Inbetriebnahme des IT-Systems geändert?
- Sind die Sicherheitsmechanismen dauerhaft angeschlossener Komponenten (z. B. automatische Bildschirmsperre, Auto-Logout) aktiviert?

# M 4.80 Sichere Zugriffsmechanismen bei Fernadministration

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Viele aktive Netzkomponenten können über einen Netzzugriff fernadministriert oder überwacht werden. Der Zugriff erfolgt entweder über verbindungsorientierte oder verbindungslose Protokolle. Hierzu gehören:

- Protokolle zur reinen Datenübertragung, beispielsweise um neue Firmware-Versionen oder Konfigurationsdateien zu übertragen, z. B. FTP, TFTP (von letzterem wird prinzipiell abgeraten) oder RCP (siehe auch M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*),
- Protokolle zur interaktiven Kommunikation, z. B. SSH,
- Protokolle für das Netzmanagement, z. B. SNMP.

Für eine sichere Fernadministration von Netzkomponenten ist Folgendes zu beachten:

- Zur interaktiven Kommunikation dürfen nur sichere Protokolle, wie zum Beispiel SSH oder HTTPs eingesetzt werden. Unsichere Protokolle, wie beispielsweise Telnet oder HTTP dürfen entweder nicht verwendet werden oder nur in einem eigens dafür vorgesehenen Administrationsnetz (Out-of-Band-Management).
- Für interaktive Kommunikationsprotokolle sollte die Auto-Logout-Option der Netzkomponente aktiviert werden, um Verbindungen nach einem definierten Zeitraum ohne Nutzeraktivität zu sperren oder zu beenden.
- Auch zur Datenübertragung (Backup von Firmware-Versionen oder Konfigurationsdateien) dürfen nur sichere Protokolle, wie zum Beispiel SCP eingesetzt werden. Unsichere Protokolle, wie zum Beispiel TFTP, FTP oder RCP dürfen nur in einem isolierten Administrationsnetz genutzt werden.
- SNMP sollte nur ab der Version 3 (SNMPv3) eingesetzt werden, da erst ab dieser stärkere Authentisierung und Verschlüsselung unterstützt werden. Wird SNMP in einer unsicheren Version (SNMPv1 oder SNMPv2) eingesetzt, dann nur in Verbindung mit Out-of-Band-Management. SNMPv1 und SMMPv2 dürfen keinesfalls außerhalb isolierter Administrationsnetze verwendet werden, weil sie keine ausreichenden Möglichkeiten zur Absicherung der Kommunikation bieten.
- Alle Standardpasswörter bzw. Community-Namen der Netzkomponenten müssen gegen sichere Passwörter bzw. Community-Namen ausgetauscht werden (siehe M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*). Die Kopplung von Community-Namen und Passwort betrifft bei vielen aktiven Netzkomponenten die Protokolle FTP, Telnet und SNMP.
- Viele Komponenten bieten auch die Möglichkeit, den Zugriff auf die Administrationszugänge (Management-Interface) auf der Basis von MAC- oder IP-Adressen einzuschränken. Soweit möglich, sollte diese Option genutzt werden, um den Zugriff nur von dedizierten Managementstationen aus zu gestatten.

Bei den meisten der genannten Protokolle ist zu beachten, dass die Übertragung der Passwörter bzw. Community-Namen im Klartext erfolgt, also prinzipiell abgehört werden kann (siehe hierzu M 5.61 *Geeignete physische Segmentierung* und M 5.62 *Geeignete logische Segmentierung*).

Prüffragen:

- Werden zur interaktiven Kommunikation und zur Datenübertragung nur sichere Protokolle eingesetzt?
- Ist für interaktive Kommunikationsprotokolle die Auto-Logout-Option der Netzkomponenten aktiviert?
- Sofern SNMP eingesetzt wird: Wird mindestens SNMPv3 eingesetzt?
- Sofern unsichere Protokolle eingesetzt werden: Werden diese nur in einem eigens dafür vorgesehenen Administrationsnetz (Out-of-Band-Management) verwendet?
- Werden Standardpasswörter bzw. Community-Namen vor Inbetriebnahme der aktiven Netzkomponenten geändert?
- Bei Verwendung von Komponenten, bei denen der Zugriff auf MAC- oder IP-Adressen beschränkt werden kann: Wird der Zugriff nur von dedizierten Managementstationen gestattet?

# M 4.81 Audit und Protokollierung der Aktivitäten im Netz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Revisor

Eine angemessene Durchführung von Protokollierung, Audit und Revision ist ein wesentlicher Faktor der Netzsicherheit.

Eine *Protokollierung* innerhalb eines Netzmanagement-Systems oder an bestimmten aktiven Netzkomponenten erlaubt es, gewisse (im Allgemeinen zu definierende) Zustände für eine spätere Auswertung abzuspeichern. Typische Fälle, die protokolliert werden können, sind z. B. die übertragenen fehlerhaften Pakete an einer Netzkomponente, ein unautorisierter Zugriff auf eine Netzkomponente oder die Performance eines Netzes zu bestimmten Zeiten. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz.

Unter einem *Audit* wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Dies kann online oder offline erfolgen. Bei einem Online-Audit werden die Ereignisse mit Hilfe eines Tools (z. B. einem Netzmanagement-System) in Echtzeit betrachtet und ausgewertet. Bei einem Offline-Audit werden die Daten protokolliert oder aus einer bestehenden Protokolldatei extrahiert. Zu den mit Hilfe eines Offline-Audits überwachten Faktoren gehören häufig auch Daten über Nutzungszeiten und angefallene Kosten.

Bei der *Revision* werden die beim (Offline-) Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeitern (Vier-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und die Arbeit der Administratoren zu kontrollieren.

Die mit einem Netzmanagement-System möglichen Protokollierungs- und Audit-Funktionen sind in einem sinnvollen Umfang zu aktivieren. Neben Performance-Messungen zur Überwachung der Netzlast sind dabei insbesondere die Ereignisse (Events) auszuwerten, die von einem Netzmanagement-System generiert werden, oder spezifische Datensammler (z. B. RMON-Probes) einzusetzen, mit denen sicherheitskritische Ereignisse überwacht und ausgewertet werden können.

Bei der Protokollierung fallen zumeist sehr viele Einträge an, sodass diese nur mit Hilfe eines Werkzeuges sinnvoll ausgewertet werden können. Beim Audit liegt die Fokussierung auf der Überwachung von sicherheitskritischen Ereignissen. Zusätzlich werden beim Audit häufig auch Daten über Nutzungszeiträume und anfallende Kosten erhoben.

Dabei sind für ein Audit insbesondere folgende Vorkommnisse von Interesse:

- Daten über die Betriebsdauer von IT-Systemen (wann wurde welches IT-System ein- bzw. wieder ausgeschaltet?),
- Zugriffe auf aktive Netzkomponenten (wer hat sich wann angemeldet?),
- sicherheitskritische Zugriffe auf Netzkomponenten und Netzmanagement-Komponenten mit oder ohne Erfolg,
- Verteilung der Netzlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance des Netzes.

Weiterhin sollten folgende Vorkommnisse protokolliert werden:

- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können,
- Unzulässige Änderungen der IP-Adresse eines IT-Systems (in einem TCP/IP-Umfeld).

Ein Audit kann sowohl online als auch offline betrieben werden. Bei einem Online-Audit werden entsprechend kategorisierte Ereignisse direkt dem Auditor mitgeteilt, der ggf. sofort Maßnahmen einleiten kann. Dafür müssen Ereignisse in geeignete Kategorien eingeteilt werden, damit der zuständige Administrator oder Auditor auf wichtige Ereignisse sofort reagieren kann und nicht unter einer Flut von Informationen den Überblick verliert. Ist Rollentrennung notwendig? Bei einem Offline-Audit werden die Daten aus den Protokolldateien oder speziellen Auditdateien mit Hilfe eines Werkzeuges für Auditzwecke aufbereitet und durch den Auditor überprüft. Im letzteren Fall können Maßnahmen zur Einhaltung oder Wiederherstellung der Sicherheit nur zeitverzögert eingeleitet werden. Im Allgemeinen wird eine Mischform aus Online- und Offline-Audit empfohlen. Dabei werden für das Online-Audit die sicherheitskritischen Ereignisse gefiltert und dem Auditor sofort zur Kenntnis gebracht. Zusätzlich werden weniger kritische Ereignisse offline ausgewertet.

Für Protokollierung und Audit können die Standard-Managementprotokolle, wie z. B. SNMP und das darauf aufsetzende RMON, aber auch spezifische Protokolle des eingesetzten Netzmanagement-Produkte verwendet werden.

Auf keinen Fall dürfen Benutzer-Passwörter im Rahmen eines Audits oder einer Protokollierung gesammelt werden! Dadurch wird ein hohes Sicherheitsrisiko erzeugt, falls es zu einem unberechtigten Zugriff auf diese Informationen kommt. Auch falsch eingegebene Passwörter sollten nicht protokolliert werden, da sie sich von den gültigen Passwörtern meist nur um ein Zeichen bzw. um eine Vertauschung zweier Zeichen unterscheiden.

Es muss weiterhin festgelegt werden, wer die Protokolle und Audit-Daten auswertet. Hierbei muss eine angemessene Trennung zwischen Ereignisverursacher und -auswerter (z. B. Administrator und Auditor) vorgenommen werden. Weiterhin ist darauf zu achten, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Für alle erhobenen Daten ist insbesondere die Zweckbindung nach § 14 BDSG zu beachten.

Die Protokoll- oder Auditdateien müssen regelmäßig ausgewertet werden. Sie können sehr schnell sehr umfangreich werden. Um die Protokoll- oder Auditdateien auf ein auswertbares Maß zu beschränken, sollten die Auswertungsintervalle daher angemessen, aber dennoch so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist.

Prüffragen:

- Ist die Protokollierung der Aktivitäten im Netz geregelt, z. B. von definierten Ereignissen und Zuständen innerhalb eines Netzmanagement-Systems oder an bestimmten aktiven Netzkomponenten?
- Ist die Auditierung und Auswertung von definierten Ereignissen im Netz geregelt?
- Existieren zur Auswertung von Auditdaten geeignete Werkzeuge?
- Werden regelmäßig Revisionen im Netz durchgeführt, um Unregelmäßigkeiten beim Betrieb von IT-Systemen und Netzen aufzudecken?

- Sind die mit einem Netzmanagement-System möglichen Protokollierungs- und Audit-Funktionen in einem sinnvollen Umfang aktiviert?
- Ist gewährleistet, dass auf sicherheitskritische Ereignisse sofort reagiert wird?
- Wird verhindert, dass Benutzer-Passwörter im Rahmen von Netz-Audits oder der Protokollierung gesammelt werden?
- Werden die Datenschutzbestimmungen im Rahmen der Protokollierung und Auditierung im Netz eingehalten?

# M 4.82 Sichere Konfiguration der aktiven Netzkomponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Neben der Sicherheit von Serversystemen und Endgeräten wird die eigentliche Netzinfrastruktur mit den aktiven Netzkomponenten in vielen Fällen vernachlässigt. Gerade zentrale aktive Netzkomponenten müssen jedoch sorgfältig konfiguriert werden. Denn während durch eine fehlerhafte Konfiguration eines Serversystems nur diejenigen Benutzer betroffen sind, die die entsprechenden Dienste dieses Systems nutzen, können bei einer Fehlkonfiguration eines Routers größere Teilnetze bzw. sogar das gesamte Netz ausfallen oder Daten unbemerkt kompromittiert werden.

Im Rahmen des Netzkonzeptes (siehe M 2.141 *Entwicklung eines Netzkonzeptes*) sollte auch die sichere Konfiguration der aktiven Netzkomponenten festgelegt werden. Dabei gilt es insbesondere Folgendes zu beachten:

- Für Router und Layer-3-Switching muss ausgewählt werden, welche Protokolle weitergeleitet und welche gesperrt werden. Dies kann durch die Implementation geeigneter Filterregeln geschehen.
- Weiterhin muss festgelegt werden, welche IT-Systeme in welcher Richtung über die Router kommunizieren. Auch dies kann durch Filterregeln realisiert werden.
- Sofern dies von den aktiven Netzkomponenten unterstützt wird, sollte festgelegt werden, welche IT-Systeme Zugriff auf die Ports der Switches des lokalen Netzes haben. Hierzu wird die MAC-Adresse des zugreifenden IT-Systems ausgewertet und auf ihre Berechtigung hin überprüft.

Für aktive Netzkomponenten mit Routing-Funktionalität ist außerdem ein geeigneter Schutz der Routing-Updates erforderlich. Diese sind zur Aktualisierung der Routing-Tabellen erforderlich, um eine dynamische Anpassung an die aktuellen Gegebenheiten des lokalen Netzes zu erreichen. Dabei sind zwei verschiedene Sicherheitsmechanismen zu unterscheiden:

- Passwörter
  Die Verwendung von Passwörtern schützt die so konfigurierten Router vor der Annahme von Routing-Updates durch Router, die nicht über das entsprechende Passwort verfügen. Hierdurch können also Router davor geschützt werden, falsche oder ungültige Routing-Updates anzunehmen. Der Vorteil von Passwörtern gegenüber den anderen Schutzmechanismen ist ihr geringer Overhead, der nur wenig Durchsatz und Rechenzeit benötigt.
- Kryptographische Prüfsummen
  Prüfsummen schützen vor der unbemerkten Veränderung von gültigen Routing-Updates auf dem Weg durch das Netz. Zusammen mit einer Sequenznummer oder einem eindeutigen Bezeichner kann eine Prüfsumme auch vor dem Wiedereinspielen alter Routing-Updates schützen.

Die Auswahl eines geeigneten Routing-Protokolls ist die Voraussetzung für einen angemessenen Schutz der Routing-Updates. RIP-2 (Routing Information Protocol Version 2, RFC 2453) und OSPF (Open Shortest Path First, RFC 1583) unterstützen Passwörter in ihrer Basis-Spezifikation und können durch Erweiterungen auch kryptographische Prüfsummen verwenden.

Prüffragen:

- Wird die sichere Konfiguration der aktiven Netzkomponenten im Rahmen des Netzkonzeptes festgelegt?
- Sind bei Routern und Layer-3-Switchen die erlaubten Protokolle und Verkehrsflüsse durch geeignete Filterregeln implementiert?
- Unterstützen die aktiven Netzkomponenten "Port Security" als Sicherheitsfunktion, um den Zugriff auf Ports der Netzkomponenten auf freigegebene MAC-Adressen der IT-Systeme zu beschränken?
- Entsprechen die Schutzmechanismen der eingesetzten Routing-Protokolle (z. B. im Rahmen des Routing-Updates) dem Stand der Technik?

# M 4.83 Update/Upgrade von Soft- und Hardware im Netzbereich

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Dies betrifft beispielsweise die Betriebssoftware von aktiven Netzkomponenten wie z. B. Switches oder Router, aber auch eine Netzmanagement-Software. Ein Update ist insbesondere dann notwendig, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Netzes haben, wenn Fehlfunktionen wiederholt auftauchen oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Auch ein Upgrade von Hardware kann in bestimmten Fällen sinnvoll sein, wenn z. B. eine neue Version eines Switches eine höhere Transfer- und Filterrate bietet. Durch diese Maßnahmen kann der Grad der Verfügbarkeit, der Integrität und der Vertraulichkeit unter Umständen erhöht werden.

Bevor jedoch ein Upgrade oder ein Update vorgenommen wird, muss die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau geprüft werden. Dies geschieht am sinnvollsten in einem physisch separaten Testnetz, bevor das Update oder Upgrade in den produktiven Einsatz übernommen wird (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*).

Prüffragen:

- Ist der Umgang mit Updates/Upgrades von Soft-und Hardware im Netzbereich bzw. für die verwendeten Netzkomponenten geregelt?
- Werden die Updates bzw. Upgrades vor einem produktiven Einsatz auf Interoperabilität mit den bereits vorhandenen Komponenten überprüft?

# M 4.84 Nutzung der BIOS-Sicherheitsmechanismen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Moderne BIOS-Varianten, z. B. UEFI (Unified Extensible Firmware Interface), bieten eine Vielzahl von Sicherheitsmechanismen an, mit denen sich die Systemadministration vertraut machen sollte. Auf keinen Fall sollten ungeschulte Benutzer BIOS-Einträge verändern, da hierdurch schwerwiegende Schäden verursacht werden können.

- **Schreibschutz:** Viele Mainboards besitzen einen Hardware-Schreibschutz für das BIOS (meist in Form eines Jumpers auf dem Mainboards). Sofern ein solcher Schreibschutz existiert, sollte er genutzt werden und nur bei notwendigen BIOS-Änderungen entfernt werden, z. B. nach einem nötigen BIOS-Update (siehe M 6.27 *Sicheres Update des BIOS*). Anschließend sollte er wieder gesetzt werden.
- **Passwortschutz:** Bei den meisten BIOS-Varianten kann ein Passwortschutz aktiviert werden. Dieser ist teilweise verhältnismäßig einfach überwindbar, sollte aber auf jeden Fall benutzt werden, wenn keine anderen Zugriffsschutzmechanismen zur Verfügung stehen.
  Meist kann ausgewählt werden, ob das Passwort vor jedem Rechnerstart oder nur vor Zugriffen auf die BIOS-Einstellungen überprüft werden soll. Teilweise können sogar verschiedene Passwörter für diese Prüfungen benutzt werden. Um zu verhindern, dass Unbefugte die BIOS-Einstellungen ändern, sollte das Setup- oder Administrator-Passwort immer aktiviert werden.
- **Boot-Reihenfolge:** Die Boot-Reihenfolge sollte so eingestellt sein, dass nur vom Datenträger mit dem vorgesehenen Betriebssystem gebootet werden kann. Das Booten von anderen Datenträgern sollte verhindert werden. Dies schützt vor einer Infektion mit bestimmten Schadprogrammen, falls versehentlich ein Datenträger im System vergessen wurde.
  Ohne eine Umstellung der Boot-Reihenfolge können auch Zugriffsschutzmechanismen (siehe M 4.1 *Passwortschutz für IT-Systeme*) und weitere Sicherheitsmaßnahmen umgangen werden. Ein Beispiel hierfür ist das Starten eines anderen Betriebssystems, so dass gesetzte Sicherheitsattribute ignoriert werden (siehe M 4.49 *Absicherung des Boot-Vorgangs für ein Windows-System*).
  Generell sollte durch einen Boot-Versuch überprüft werden, ob die Umstellung der Boot-Reihenfolge wirksam ist, da einige Controller die interne Reihenfolge außer Betrieb nehmen und eine getrennte Einstellung erfordern.
- **Virenschutz, Virus-Warnfunktion:** Wird diese Funktion aktiviert, verlangt der Rechner vor einer Veränderung des Boot-Sektors bzw. des MBR (Master Boot Record) eine Bestätigung, ob diese Änderung durchgeführt werden darf. Wird die Virus-Warnfunktion von der BIOS-Version unterstützt, sollte diese Funktion als zusätzlicher Schutz aktiviert werden.

Prüffragen:

- Ist das BIOS so konfiguriert, dass die BIOS-Einstellungen nur nach Eingabe eines Passworts bzw. nach Entfernen eines Hardware-Schreibschutzes geändert werden können?
- Wurde getestet, dass die im BIOS eingestellte Boot-Reihenfolge zum Booten von der Festplatte führt?

- Ist die Virus-Warnfunktion des BIOS zum Schutz vor unbeabsichtigten Veränderungen des Boot-Sektors oder des MBR (Master Boot Record) aktiviert?

# M 4.85 Geeignetes Schnittstellendesign bei Kryptomodulen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Ein Kryptomodul sollte so beschaffen und konfigurierbar sein, dass der gesamte Informationsfluss von und zu dem Modul oder gar ein unmittelbarer physikalischer Zugriff auf den Datenbestand des Moduls kontrolliert bzw. eingeschränkt werden kann. Je nach Anwendungsfall bzw. Schutzbedarf empfiehlt sich die Verwendung von physikalisch getrennten Ein- und Ausgabeports. In jedem Fall sollten die Modulschnittstellen so aufgebaut sein, dass die einzelnen Datenkanäle logisch voneinander verschieden sind, obwohl sie möglicherweise einen gemeinsamen Ein- oder Ausgangsport teilen. Im Zusammenhang mit dem Schlüsselmanagement des Kryptomoduls muss gewährleistet sein, dass die Ausgabekanäle von der internen Schlüsselgenerierung bzw. dem Eingabeport für die manuelle Schlüsseleingabe zumindest logisch getrennt sind. In vielen Fällen werden zum Anschluss einer externen Versorgungsspannung bzw. eines externen Versorgungstakts und zur ausschließlichen Verwendung von Reparatur- oder Wartungsaufgaben separate Schnittstellen zur Verfügung stehen. Aus der Perspektive des Kryptomoduls ist daher die folgende Aufteilung und Verwendung zweckmäßig:

- Dateneingabeschnittstelle, die all diejenigen Eingabedaten des Kryptomoduls führt, die im Modul weiterverarbeitet oder bearbeitet werden (z. B. kryptographische Schlüssel, Authentisierungsinformationen, Statusinformationen von anderen Kryptomodulen, Klartextdaten etc.).
- Datenausgabeschnittstelle, die all diejenigen Daten des Kryptomoduls führt, die vom Modul an dessen Umgebung gelangen sollen (z. B. verschlüsselte Daten, Authentisierungsinformationen, Steuerinformationen für andere Kryptomodule, etc.).
- Steuereingabeschnittstelle, die sämtliche Steuerbefehle, -signale und -daten zur Ablaufsteuerung und Einstellung der Betriebsweise des Moduls führt.
- Statusausgabeschnittstelle, die alle Signale, Anzeigen und Daten an die Umgebung abführt, um den inneren Sicherheitszustand des Kryptomoduls anzuzeigen.

Und schließlich

- Maintenance-Schnittstelle, die ausschließlich Wartungs- und/oder Reparaturzwecken dient.

Die Dokumentation für eine Kryptokomponente sollte eine Beschreibung sämtlicher Komponenten enthalten (Hard-, Firm- und/oder Software).

Ferner sollte die Dokumentation die komplette Spezifikation der Modulschnittstellen beinhalten zuzüglich der physikalischen oder logischen Ports, manuellen oder logischen Steuereinheiten, physikalischen oder logischen Anzeigeelementen sowie deren physikalischen, logischen oder elektrischen Eigenschaften. Wenn eine Kryptokomponente eine Maintenance-Schnittstelle enthält, sollte die Dokumentation auch die vollständige Spezifikation der durchzuführenden Wartungsprozesse zur Verfügung stellen. Alle physikalischen und logischen Ein- und Ausgabekanäle innerhalb des Moduls müssen explizit offengelegt sein. Neben der konkreten Einbindung der Kryptokomponente in eine vorgesehene Einsatzumgebung ist auch die Bedienung und Benutzung der Kryptokomponente zu beschreiben.

Die Dokumentation sollte weiterhin eine Zusammenstellung der Sicherheitsfunktionalität enthalten und womöglich die Abhängigkeit von Hard-, Firm- oder Software aufzeigen, die je nach Konzeption der Kryptokomponente nicht unmittelbar zum Lieferumfang der Kryptokomponente gehören.

Die Dokumentation über die Modulschnittstellen sind vom Modulhersteller zur Verfügung zu stellen. Die Dokumentation wird beispielsweise von einem Administrator benötigt, der beabsichtigt, das Kryptomodul in seine Systemumgebung zu integrieren, oder von einem Evaluator, der eine Sicherheitsbeurteilung des Kryptomoduls vornehmen möchte.

Prüffragen:

- Sind die eingesetzten Kryptomodul so konfigurierbar, dass der gesamte Informationsfluss und Zugriffe kontrolliert bzw. eingeschränkt werden kann?
- Ist die Dokumentation der Kryptokomponente und ihrer Modulschnittstellen vollständig?
- Sind die durchzuführenden Wartungsprozesse für Kryptokomponenten vollständig dokumentiert?

# M 4.86 Sichere Rollenteilung und Konfiguration der Kryptomodule

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Viele kryptographische Sicherheitskomponenten bieten die Möglichkeit, dass mehrere Nutzerrollen sowie die zugehörigen Handlungen, die durch das autorisierte Personal ausgeführt werden können, unterschieden werden können. Abhängig vom Schutzbedarf sind hierzu Zugriffskontroll- und Authentisierungsmechanismen erforderlich, um verifizieren zu können, ob ein Nutzer zur Ausführung des gewünschten Dienstes auch tatsächlich autorisiert ist. In Bezug auf die unterschiedlichen Rollen bietet sich folgende Unterteilung an:

- Benutzerrolle, der die Benutzung und Verwendung der Sicherheitskomponente obliegt (z. B. Endteilnehmer, Benutzer).
- Operatorrolle, die für die Installation und das Kryptomanagement verantwortlich ist (z. B. Sicherheitsadministrator).

Und zumindest eine

- Maintenance-Rolle, die für Wartungs- und Reparaturarbeiten zuständig ist (z. B. Wartungstechniker, Revisor).

Bei Kryptokomponenten, bei denen die Benutzer- und die Administratorrolle getrennt werden kann, sollte diese Möglichkeit auch genutzt werden und durch die Administration Grundeinstellungen vorgegeben werden, wie z. B. Passwortlänge oder Schlüssellänge, sodass die Benutzer nicht aus Bequemlichkeit oder Unkenntnis unsichere Einstellungen wählen können.

Neben den unterschiedlichen Rollen gilt es entsprechend auch die verschiedenen Handlungen bzw. die von der Sicherheitskomponente bereitgestellten Dienste zu unterscheiden. Ein Kryptomodul sollte zumindest folgende Dienste zur Verfügung stellen:

- Statusanzeige zur Ausgabe des momentanen Status der Kryptokomponente,
- Selbsttest zur Initialisierung und Durchführung von selbständigen Selbsttests,
- Bypass zur Aktivierung und Deaktivierung eines Bypass mittels dessen durch das Kryptomodul Klarinformationen bzw. ungesicherte Daten transportiert werden.

Zur erforderlichen Authentisierung des Personals gegenüber der Sicherheitskomponente bieten sich eine Vielzahl von unterschiedlichen Techniken an: Passwort, PIN, kryptographische Schlüssel, biometrische Merkmale etc. Die Kryptokomponente sollte so konfiguriert sein, dass bei jedem Rollenwechsel oder bei Inaktivität nach einer bestimmten Zeitdauer die Authentisierungsinformationen erneut eingegeben werden müssen. Ferner empfiehlt sich an dieser Stelle eine Beschränkung der Authentisierungsversuche (z. B. indem der Fehlbedienungszähler auf 3 gesetzt wird).

Prüffragen:

- Werden die administrativen Möglichkeiten von Kryptokomponenten genutzt, um sichere Grundeinstellungen vorzugeben?
- Erfordert ein Rollenwechsel oder längere Inaktivität eine erneute Authentisierung an der Kryptokomponente?

# M 4.87 Physikalische Sicherheit von Kryptomodulen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Wie in M 2.165 *Auswahl eines geeigneten kryptographischen Produktes* beschrieben, können Kryptomodule in Software, Firmware oder Hardware realisiert sein. Firmware- bzw. Hardware-Produkte werden insbesondere dann gewählt, wenn das Kryptomodul besonders manipulationsresistent sein soll.

Unter diesem Gesichtspunkt sollte das Kryptomodul unter Verwendung von physikalischen Sicherheitsmaßnahmen oder unter Ausnutzung entsprechender Materialeigenschaften so konstruiert sein, dass ein unautorisierter physikalischer Zugriff auf Modulinhalte erfolgreich verhindert werden kann. Dies soll möglichen technischen Manipulationen oder sonstigen Beeinträchtigungen im laufenden Betrieb vorbeugen. In Abhängigkeit von der Sicherheitsstufe des Kryptomoduls sind hierzu beispielsweise die Verwendung von Passivierungsmaterialien, geeignete Tamperschutzmaßnahmen oder mechanische Schlösser in Betracht zu ziehen. Eine automatische Notlöschung, die eine aktive Löschung oder die Vernichtung aller im Klartext enthaltenen sensitiven Schlüsseldaten und -parameter bewerkstelligen kann, innerhalb des Kryptomoduls nach identifizierten Angriffsversuchen, zählt ebenfalls in diese Maßnahmenkategorie.

Mit dem Einsatz von diversen Sensoren und Überwachungseinrichtungen lässt sich sicherstellen, dass das Kryptomodul - was Spannungsversorgung, Taktung, Temperatur, mechanische Beanspruchung, elektromagnetische Beeinträchtigung etc. anbelangt - in seinem vorgesehenen Arbeitsbereich betrieben wird.

Zur Aufrechterhaltung seiner beabsichtigten Funktionalität sollte das Kryptomodul Selbsttests initiieren und durchführen können. Diese Tests können sich auf folgende Bereiche erstrecken: Algorithmentests, Software und Firmwaretests, Funktionstests, statistische Zufallstests, Konsistenztests, Bedingungstests sowie Schlüsselgenerierungs- und -ladetests. Im Anschluss an ein negatives Testergebnis sollte dem Benutzer des Kryptomoduls eine entsprechende Fehlermeldung signalisiert und ein entsprechender Fehlerzustand eingenommen werden. Erst nach Behebung der Fehlerursache(n) darf eine Freischaltung aus diesem Fehlerzustand möglich sein.

Beim Einsatz von Softwareprodukten muss die physikalische Sicherheit des Kryptomoduls durch das jeweilige IT-System bzw. dessen Einsatzumgebung geleistet werden. Sicherheitstechnische Anforderungen an solche IT-Systeme können den systemspezifischen Bausteinen entnommen werden.

Eine Softwarelösung sollte Selbsttests durchführen können, um Modifikationen durch Trojanische Pferde oder Coputer-Viren erkennen zu können.

Prüffragen:

- Ist sichergestellt, dass ein unautorisierter physikalischer Zugriff auf Modulinhalte des Kryptomoduls verhindert wird?
- Können Hard- und Softwareprodukte als Kryptomodule Selbsttests durchführen?

# M 4.88 Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Beim Einsatz von Kryptomodulen spielt deren Einbindung ins bzw. Abhängigkeit vom jeweiligen Betriebssystem des Hostsystems eine wesentliche Rolle. Das Zusammenwirken von Betriebssystem und Kryptomodul muss gewährleisten, dass

- das Kryptomodul nicht abgeschaltet oder umgangen werden kann (z. B. durch Manipulation oder Austausch von Treibern),
- die angewendeten oder gespeicherten Schlüssel nicht kompromittiert werden können (z. B. durch Auslesen von RAM-Bereichen),
- die zu schützenden Daten **nur** mit Wissen und unter Kontrolle des Anwenders auch unverschlüsselt auf Datenträgern abgespeichert werden können bzw. das informationsverarbeitende System verlassen (z. B. bei Netzanbindung),
- Manipulationsversuche am Kryptomodul erkannt werden.

Je nach Art des Kryptomoduls (Hardware- oder Software-Realisierung, Einbindungsstrategie in die IT-Komponente etc.), den Einsatzbedingungen und dem Schutzbedarf der zu sichernden Daten können sich unterschiedlich starke Anforderungen bzgl. der Betriebssystem-Sicherheit ergeben. Bei in Software realisierten Kryptomodulen ist der Einsatz eines sicheren Betriebssystems besonders wichtig. Kommerzielle PC-Betriebssysteme sind in der Regel derart komplex und kurzen Innovationszyklen unterworfen, dass die Daten- bzw. Systemsicherheit kaum nachweisbar oder beweisbar ist. Eine Ausnahme können proprietäre oder für spezielle Anwendungen optimierte Betriebssysteme bilden (z. B. spezielle Betriebssysteme in Kryptogeräten). Daher ist es beim Einsatz von kryptographischen Produkten auf Standard-Betriebssystemen wie z. B. zur Dateiverschlüsselung oder zur E-Mail-Absicherung wichtig, dass alle Standardsicherheitsmaßnahmen für dieses Betriebssystem umgesetzt sind. Die sicherheitstechnischen Anforderungen an diese IT-Systeme können den jeweiligen systemspezifischen Bausteinen entnommen werden, so etwa für Clients oder Server in Schicht 3.

In Hardware realisierte Kryptomodule können so konstruiert sein, dass sie Mängel der Betriebssystem-Sicherheit kompensieren oder vollständig ausräumen. Hier liegt die Verantwortung zur Erfüllung der o. g. Anforderungen allein beim Kryptomodul. Es muss z. B. erkennen können, ob unverschlüsselte Daten berechtigt oder unberechtigt am Modul vorbei auf Datenträger oder andere Geräteschnittstellen geschrieben werden. Der Anwender muss in Übereinstimmung mit der für sein Umfeld individuell erstellten Sicherheitspolitik entscheiden, welche Kombination Betriebssystem / Kryptomodul erforderlich ist.

Prüffragen:

- Ist gewährleistet, dass die installierten Kryptomodule nicht unbemerkt abgeschaltet oder umgangen werden können?
- Ist im Zusammenwirken von Betriebssystem und Kryptomodulen gewährleistet, dass die kryptographischen Schlüssel nicht kompromittiert werden können?

# M 4.89 Abstrahlsicherheit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Jedes elektronische Gerät strahlt mehr oder weniger starke elektromagnetische Wellen ab. Diese Abstrahlung ist als Störstrahlung bekannt und ihre maximal zulässige Stärke ist im Allgemeinen gesetzlich geregelt, in Deutschland ist dies das Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Bei Geräten, die Informationen verarbeiten (PC, Drucker, Faxgerät, Modem, usw.) kann diese Störstrahlung auch die gerade verarbeiteten Informationen mit sich führen. Derartige informationstragende Abstrahlung wird bloßstellende Abstrahlung genannt. Wird die bloßstellende Abstrahlung in einiger Entfernung, z. B. in einem Nachbarhaus oder auch in einem in der Nähe abgestellten Fahrzeug empfangen, kann daraus die Information rekonstruiert werden. Die Vertraulichkeit der Daten ist damit in Frage gestellt. Die Grenzwerte des EMVG reichen im allgemeinen nicht aus, um das Abhören der bloßstellenden Abstrahlung zu verhindern. Hierzu müssen in aller Regel zusätzliche Maßnahmen getroffen werden.

Bloßstellende Abstrahlung kann einen Raum auf unterschiedliche Weise verlassen:

- In Form von elektromagnetischen Wellen, die sich wie Rundfunkwellen durch den freien Raum ausbreiten.
- Als leitungsgebundene Abstrahlung entlang metallischer Leiter (Kabel, Klimakanäle, Heizungsrohre).
- Durch Überkoppeln von einem Datenkabel in parallel hierzu verlegte Kabel. Auf dem Parallelkabel breitet sich die Abstrahlung aus und kann von diesem noch in großer Entfernung abgegriffen werden.
- Als akustische Abstrahlung, z. B. bei Druckern. Die Detailinformationen des Druckvorgangs breiten sich über Schall beziehungsweise Ultraschall aus und können mit Mikrofonen aufgenommen werden.
- In Form von akustischer Überkopplung auf andere Geräte. Die Schallwandlung in elektrische Signale erfolgt dabei durch schallempfindliche Geräteteile, die unter bestimmten Voraussetzungen ähnlich wie ein "Mikrofon" arbeiten können. Die weitere Ausbreitung erfolgt dann entlang metallischer Leiter oder auch in Form elektromagnetischer Raumstrahlung.
- Bloßstellende Abstrahlung kann auch durch eine äußere Manipulation von Geräten verursacht werden. Wird z. B. ein Gerät mit Hochfrequenzenergie bestrahlt, können die im Gerät ablaufenden elektrischen Vorgänge die eingestrahlten Wellen so beeinflussen, dass diese nun die verarbeitete Information mit sich tragen.

In allen Fällen hat die Installation, also die Verkabelung der Geräte untereinander und mit dem Stromversorgungsnetz, einen wesentlichen Einfluss auf die Ausbreitung und damit auch auf die Reichweite der Abstrahlung.

Vom BSI werden Schutzmaßnahmen entwickelt, welche die Gefährdung ohne wesentliche Kostensteigerung wirksam reduzieren. Dazu gehören:

- **Zonenmodell**
  Das Zonenmodell berücksichtigt die Ausbreitungsbedingungen für bloßstellende Abstrahlung bei den jeweiligen Gebäude- und Geländeverhältnissen. Dabei wird die Abschwächung der Abstrahlung auf ihrem Weg vom verursachenden IT-Gerät zum potentiellen Empfänger messtechnisch erfasst. Abhängig von den Gegebenheiten am Einsatzort können gegebe-

nenfalls Geräte eingesetzt werden, an denen nur geringfügige oder gar keine Sonderentstörmaßnahmen durchgeführt wurden.

- **Quellenentstörung**
  Die Quellenentstörung bewährt sich besonders bei der Neuentwicklung von IT-Produkten. Hier wird die bloßstellende Abstrahlung bereits am Entstehungsort innerhalb des Gerätes unterdrückt oder so verändert, dass sie nicht mehr auswertbar ist. Durch diese Methode kann z. B. auch der Einsatz kostengünstiger Kunststoffgehäuse möglich werden, mit vernachlässigbar geringen Auswirkungen auf den Serienpreis.
- **Kurzmessverfahren**
  Die Erarbeitung von Kurzmessverfahren und Manipulationsprüfverfahren erlaubt, auch nach Wartung, Reparatur oder möglichen unberechtigten Zugriffen die Abstrahlsicherheit mit geringem Aufwand sicherzustellen.
- **Einsatz abstrahlarmer bzw. abstrahlgeschützter Geräte**
  Hersteller von PC-Bildschirmen werben häufig mit dem Begriff "abstrahlarm" nach MPR II, TCO oder SSI. Diese Richtlinien berücksichtigen jedoch ausschließlich mögliche gesundheitsschädliche Auswirkungen der Gerätestrahlung. Die Messverfahren und Grenzwerte für die Strahlung sind daher für den Nachweis bloßstellender Abstrahlung ungeeignet und ermöglichen wie auch Messungen zur elektromagnetischen Verträglichkeit (EMV) keine Bewertung der Sicherheit gegen unberechtigtes Mitlesen der Daten. Daneben werden aber auch speziell abstrahlgeschützte IT-Systeme angeboten. Ein detailliertes Prüfkonzept des BSI dient zur abgestuften Prüfung von IT-Geräten bzw. -Systemen. Grundgedanke dieses Konzeptes ist es, den Umfang der Schutzmaßnahmen so gut wie möglich an die vom Anwender angenommene Bedrohungslage anzupassen, um so bei minimiertem Kostenaufwand ein Optimum an Abstrahlsicherheit zu erzielen. Ursprünglich wurde das Prüfkonzept des BSI zum Schutz staatlicher Verschlusssachen entwickelt, der Einsatz kann aber auch in der Privatwirtschaft sinnvoll sein, wenn Daten mit hohem Schutzbedarf bezüglich Vertraulichkeit geschützt werden sollen. So kann z. B. in vielen Fällen ein nach dem Zonenmodell geprüftes und für den Einsatz in den Zonen 1-3 zugelassenes Gerät (sog. "Zone 1-Gerät") bereits einen hinreichenden Schutz gegen unberechtigtes Abhören vertraulicher Daten infolge bloßstellender Abstrahlung bieten. Bei hohem oder sehr hohem Schutzbedarf in Bezug auf die Vertraulichkeit sollte deshalb geprüft werden, ob der Einsatz abstrahlarmer bzw. abstrahlgeschützter Geräte zweckmäßig oder sogar erforderlich ist. Ob ein Hersteller abstrahlgeschützte Geräte gemäß dieser sog. "TEMPEST"-Kriterien in seinem Lieferprogramm anbietet, sollte durch eine Rückfrage beim Hersteller, beim BSI bzw. durch Einsicht in die offizielle Produktübersicht BSI TL 03305, welche auf der Internetseite des BSI unter dem Stichwort *Publikationen* verfügbar ist, geklärt werden. Dabei gehört zu der Aussage, dass für ein Gerät eine TEMPEST-Zulassung vorliegt, immer auch die Aussage des Zulassungsgrades (z. B. zugelassen für den Einsatz in den Zonen 1-3 gemäß Zonenmodell).

Prüffragen:

- Wurde überlegt, ob zusätzliche Maßnahmen zur Abstrahlsicherheit erforderlich sind?

# M 4.90 Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

**Das OSI-Referenzmodell nach ISO**

Kryptographische Verfahren können auf den verschiedenen Schichten des ISO/OSI-Referenzmodells implementiert werden. Dieses Modell, welches in Maßnahme M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung* dieses Handbuchs kurz erläutert wird, definiert vier transportorientierte Schichten und drei anwendungsorientierte Schichten. Instanzen einer Schicht in verschiedenen Systemen kommunizieren über Protokolle miteinander. Jede Schicht bietet der nächst höheren Schicht ihre Dienste an. Das kann neben den üblichen Kommunikationsdiensten auch ein Sicherheitsdienst sein. Welcher Sicherheitsdienst in welcher Schicht des Schichtenmodells platziert werden sollte und welche Mechanismen dazu genutzt werden können, ist im Teil 2 der ISO 7498 (Security Architecture) beschrieben.

Auch wenn konkrete Kommunikationssysteme, Referenzmodelle oder Protokolle sich nicht immer konform zum ISO-Referenzmodell verhalten, so hilft die Kenntnis des ISO-Referenzmodells bei der Beurteilung von Sicherheitsfunktionen von Produkten und erleichtert damit auch die systematische Erstellung "sicherer" Gesamtsysteme.

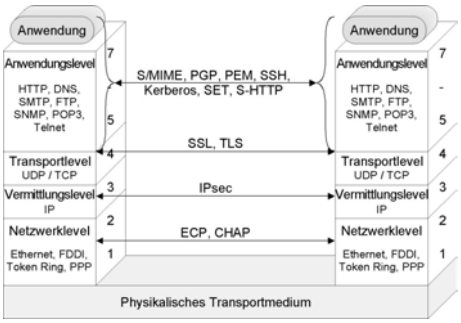



Abbildung: Beurteilung von Sicherheitsfunktionen von Produkten mit Hilfe der Kenntnis des ISO-Referenzmodells

Im Folgenden soll erläutert werden, welche Vor- bzw. Nachteile mit dem Einsatz von kryptographischen Verfahren auf den jeweiligen Schichten verbunden sind.

Kryptographische Verfahren werden zur Sicherung verschiedener bei der Kommunikation anfallender Informationen eingesetzt, also um Informationen zu verschlüsseln, mit kryptographischen Prüfsummen zu versehen oder zu signieren. Zum einen können die vom Benutzer zu übermittelnden Daten gesichert werden, zum anderen aber auch Informationen, die sich beim Informationsaustausch implizit ergeben (z. B. Verkehrsflussinformationen).

Sicherheitsbeziehungen können für verschiedene Sicherheitsdienste in verschiedenen OSI-Schichten gleichzeitig existieren. Oberhalb der Schicht, in der ein Sicherheitsdienst realisiert ist, liegen die Informationen (bezüglich dieses

Dienstes) ungesichert vor. Kryptographische Mechanismen (Verschlüsselung, digitale Signatur, kryptographische Prüfsummen) liefern Beiträge zur Realisierung wichtiger Sicherheitsdienste (Authentizität, Vertraulichkeit, Integrität, Kommunikations- und Datenursprungsnachweise).

Hierzu wird zunächst ein Überblick über die Gesichtspunkte gegeben, die für oder gegen den Einsatz von kryptographischen Verfahren auf den verschiedenen OSI-Schichten sprechen:

| **Verwendung von kryptographischen Verfahren auf** | | | |
|---|---|---|---|
| **oberen Schichten:** | | **unteren Schichten:** | |
| +: | sinnvoll, wenn die Anwendungsdaten nahe der Anwendung geschützt werden sollen bzw. der "unsichere Kanal" möglichst kurz gehalten werden soll | +: | sinnvoll für die Kopplung zweier Netze, die als sicher gelten, über eine unsichere Verbindung, z. B. Kopplung zweier Liegenschaften über öffentliche Netze |
| +: | auf jeden Fall immer dann, wenn die Daten nicht auf den tieferen Schichten geschützt werden | +: | zur Sicherung eines Netzes gegen unbefugte Zugriffe |
| +: | sinnvoll bei vielen, wechselnden Kommunikationspartnern an verschiedenen Standorten | +: | immer dann, wenn Verkehrsflussinformationen geschützt werden sollen, z. B. Adressinformationen |
| +: | Benutzer können sie nach eigenen Anforderungen einsetzen | +: | alle höherliegenden Header- und die Benutzerinformationen sind verschlüsselt |
| +: | Absicherung näher am Benutzer und für diesen erkennbarer | +: | transparent für Benutzer, geringeres Fehlbedienungsrisiko |
| -: | höhlen Absicherung durch Firewalls aus | +: | einfacheres Schlüsselmanagement |
| -: | werden häufig fehlbedient | -: | Schutz nur bis in die Schicht, in der die Sicherheits- |

| **Verwendung von kryptographischen Verfahren auf** | | | |
|---|---|---|---|
| | | | protokolle realisiert sind |
| -: | basiert häufig auf Software, kryptographische Schlüssel und Algorithmen sind einfacher manipulierbar | -: | häufig Hardware, also teuer und unflexibel |
| -: | höhere Abhängigkeit vom Betriebssystem bzw. darunter liegender Hardware | -: | bietet häufig keine Ende-zu-Ende Sicherheit |

Tabelle: Verwendung von kryptographischen Verfahren auf die OSI-Schichten

Ein einfaches Schlüsselmanagement ergibt sich i.d.R. dann, wenn Gruppenschlüssel verwendet werden können, z. B. beim Aufbau von sicheren Teilnetzen (VPNs), bei denen die Zugänge mit Kryptogeräten versehen werden.

Kryptographische Produkte für die unteren Schichten liegen im Anschaffungspreis meist deutlich über solchen für obere Schichten, dafür werden allerdings auch weniger benötigt. Außerdem ist der Administrations- und Implementierungsaufwand meist niedriger, da Sicherheitsdienste nicht in verschiedensten Anwendungen implementiert werden müssen. Auch "exotische" Anwendungen - ohne eigene Sicherheitsfunktionalität - können dadurch gesichert Daten austauschen.

In vielen Fällen bietet sich auch eine Kombination von kryptographischen Diensten auf verschiedenen Schichten an. Dies hängt von den jeweiligen Sicherheitsanforderungen und den Einsatzbedingungen ab, wie Kosten, Performance und inwieweit entsprechende Komponenten erhältlich sind. Entscheidende Faktoren sind auch die angenommenen Gefährdungen, gegen die die implementierten Sicherheitsdienste wirken sollen, sowie die zugrunde liegende Systemarchitektur.

**Sicherheits-Endgeräte <-> Sicherheits-Koppelelemente**

Sicherheitssysteme können als Endgerät bzw. Teil eines Endgeräts oder als Koppelelement bzw. Teil eines Koppelelements ausgelegt sein. Koppelelemente sind z. B. aktive Netzkomponenten wie Router oder Gateways.

Im Unterschied zu Endgeräten weisen Sicherheits-Koppelelemente gewöhnlich zwei Netzschnittstellen auf, die auf einer für dieses System typischen Schicht über ein Kryptomodul (Hard- oder Software) gekoppelt sind. Eine Schnittstelle ist mit dem "sicheren" Netz verbunden (z. B. Hausnetz), die andere Schnittstelle mit einem als "unsicher" bewerteten Netz (z. B. öffentliche Netze).

Sicherheits-Endgeräte haben den Vorteil, dass die Sicherheitsmechanismen gut an die Anforderungen der Anwendung angepasst werden können. Typische SicherheitsEndgeräte sind Kryptotelefone, Kryptofaxgeräte oder hard-/

softwarebasierte Sicherheitslösungen für PCs. Sicherheits-Endgeräte bieten i.d.R. Lösungen für einzelne Arbeitsplätze. Teilweise unterstützen diese Lösungen lediglich einen Dienst. Die Grenzen sind hier jedoch fließend (Telefonie über Internet-PC, Kryptotelefon mit Dateneingang). In Endgeräten ist im Gegensatz zum Koppelelement die Wahl der Sicherheitsschicht nicht eingeschränkt, da Endgeräte grundsätzlich vollständig sind, also über 7 Schichten verfügen.

Sicherheits-Koppelelemente sind häufig derart leistungsfähig konstruiert, dass sie größere Arbeitseinheiten bis hin zu ganzen Liegenschaften absichern können. Dabei versuchen die Hersteller solcher Systeme möglichst viele Dienste bzw. übergeordnete Protokolle zu unterstützen, damit eine universelle Verwendung möglich ist. Auch die weitgehende Unabhängigkeit von den Betriebssystemen der Endgeräte liefert einen Beitrag zur universellen Einsetzbarkeit von Koppelelementen. Natürlich können auch einzelne Endgeräte durch Sicherheits-Koppelelemente abgesichert werden. Jedoch führt die höhere Leistungsfähigkeit der Geräte häufig zu höheren Kosten. Bei Koppelelementen handelt es sich definitionsgemäß um unvollständige OSI-Systeme. Daher ist auch die Implementierung von Sicherheitsdiensten auf die Schichten beschränkt, die das Koppelelement aufweist.

Auch Mischformen sind im Einsatz. Das setzt voraus, dass Sicherheits-Endgeräte und Sicherheits-Koppelelemente aufeinander abgestimmt sind, insbesondere bezüglich der verwendeten Sicherheitsmechanismen und Sicherheitsparameter (z. B. kryptographische Schlüssel).

**Nutzer-, Steuer- und Managementinformationen**

Ein Anwender ist hauptsächlich an der Übermittlung von Nutzerinformationen an entfernte Anwender interessiert. Je nach konkretem Referenzmodell (z. B. ISDN) werden aber zwischen den Systemen (Endgeräte, Koppelelemente) zudem Steuer-, Signalisier- und Managementinformationen zwecks Aufbau/Abbau von Verbindungen, Aushandeln von Dienstgüteparametern, Konfiguration und Überwachung des Netzes durch Netzbetreiber, usw. übertragen.

Das jeweilige Netz hat dabei die Aufgabe, Benutzerinformationen unverändert und unausgewertet zu übertragen, d. h. Benutzerinformationen müssen nur von den Endgeräten interpretiert werden können. Damit lassen sich diese Informationen unabhängig von der übrigen Netzinfrastruktur sichern, notfalls sogar unter Verwendung proprietärer Sicherheitsfunktionen (geschlossene Benutzergruppe). Steuer-, Signalisier- und Managementinformationen der Transportschichten müssen von Netzelementen des Netzbetreibers ausgewertet, geändert oder erzeugt werden können. Damit entziehen sich diese Informationen einer vom Netzbetreiber unabhängigen Sicherung (z. B. Verschlüsselung) weitgehend. Die Sicherung dieser Informationen erfordert neben entsprechenden Standards die vertrauensvolle Zusammenarbeit mit dem Netzbetreiber. Bedrohungen können sich dadurch ergeben, dass Sicherheitsfunktionen von Produkten falsch eingeschätzt werden. Bei der Auswahl von Kryptogeräten ist genau zu prüfen, welche Informationsanteile gesichert oder gefiltert werden. Ebenso ist im Umkehrschluss zu überprüfen, welche Informationen trotz des Einsatzes von Kryptogeräten ungesichert bleiben und in wieweit dies zu tolerieren ist.

**Beispiel:** Beim ISDN erfolgt die Übertragung der Benutzerinformationen in der Regel über die B-Kanäle. Aber auch der D-Kanal, welcher primär für die Signalisierung genutzt wird, kann zur Übertragung paketierter Daten verwendet werden. Ist das Ziel die Sicherung aller Benutzerdaten, so reicht im Fall der

Übertragung von paketierten Daten über den D-Kanal die Absicherung der B-Kanäle offensichtlich nicht aus.

**Sicherheit in leitungsvermittelten Netzen**

Bei leitungsvermittelten Netzen werden durch den Verbindungsaufbau Kanäle definierter Bandbreite eingerichtet, die den Kommunikationspartnern exklusiv zur Verfügung stehen. Nach Einrichten der Verbindung erfolgt die Übertragung der Nutzdaten, anschließend der Verbindungsabbau. Der Netzbetreiber kann Festverbindungen einrichten, bei denen dann der durch den Teilnehmer gewöhnlich durchzuführende Verbindungsauf- und -abbau entfällt. Ein Beispiel für ein leitungsvermitteltes Netz ist ISDN.

Durch den Verbindungsaufbau werden Nutzdatenkanäle auf OSI-Schicht 1 zwischen den Kommunikationspartnern eingerichtet, die beim ISDN B-Kanäle heißen. Um die Vertraulichkeit der übertragenen Nutzdaten zu gewährleisten, kann dieser Kanal verschlüsselt werden. Soll darüber hinaus der Signalisierungskanal abgesichert werden, bei N-ISDN also der D-Kanal (Schicht 1-3), so muss bedacht werden, dass als Gegenstellen eines Endgeräts sowohl das Endgerät des Kommunikationspartners als auch Vermittlungsstellen des Netzbetreibers auftreten können. Der D-Kanal wird normalerweise nicht verschlüsselt, da hierzu besondere Anforderungen an den Netzbetreiber zu stellen wären. In diesem Fall sollte man die Überwachung und Filterung des D-Kanals vorsehen (siehe auch M 4.62 *Einsatz eines D-Kanal-Filters*).

**Leitungsverschlüssler:** Als Sonderfall muss die Verschlüsselung synchroner vollduplex Festverbindungen gesehen werden, da in diesem Fall die Vertraulichkeit - auch des Verkehrsflusses - gewährleistet werden kann. Stehen keine Daten zur Übertragung an, werden Fülldaten verschlüsselt, sodass auf der Leitung immer ein kontinuierliches "Rauschen" zu sehen ist. Der Leitungsverschlüssler stellt eine Alternative zur Verlegung geschützter Leitungen dar.

**Sicherheit in paketvermittelten Netzen**

Bei paketvermittelten Netzen ist zwischen verbindungsorientierter und verbindungsloser Paketvermittlung zu unterscheiden. Bei der verbindungsorientierten Paketvermittlung wird während der Verbindungsaufbauphase eine virtuelle Verbindung eingerichtet, wodurch der Datenpfad durch das Paketnetz im Anschluss festgelegt ist. Datenpakete werden nach dem Verbindungsaufbau auf Basis der zugeordneten virtuellen Kanalnummer auf dem selben Pfad durch das Netz geroutet. Sende- und/oder Empfängeradressen sind hierzu nicht mehr erforderlich. Ein Beispiel hierfür ist das X.25-Netz.

Bei verbindungsloser Paketvermittlung gibt es keine Verbindungsauf und -abbauphasen. Datenpakete werden - unter anderem ausgestattet mit Quell- und Zieladresse - einzeln vermittelt. Dies ist typisch für LAN-Datenverkehr.

Die Wahl der Schicht, in der die Sicherheitsmechanismen wirken, bestimmt, welche Informationsanteile gesichert werden. Je niedriger die gewählte Sicherheitsschicht, desto umfangreicher die Informationssicherung. Beim Durchlauf der Benutzerdaten durch die Instanzen der Schichten 7 bis 1 (Sender) werden den Daten zusätzliche Steuerinformationen hinzufügt. Geht es also nicht nur um die Sicherung von Benutzerdaten, sondern auch um die Sicherung des Verkehrsflusses, so bietet sich die Wahl einer niedrigen OSI-Schicht an. Andererseits gilt: je niedriger die gewählte OSI-Schicht, desto weniger Koppelelemente (Repeater, Bridge, Switch, Router, Gateway) lassen sich transparent überwinden.

| Koppelelement | höchste Schicht des Koppelelements |
|---|---|
| Repeater | 1 |
| Bridge, Layer-2-Switch | 2 |
| Router, Layer-3-Switch, X.25-Packet Handler | 3 |
| Gateway | 7 |

Tabelle: Gegenüberstellung: Koppelelement - ISO-Schicht

Sollen Sicherheitsdienste über Koppelelemente hinweg wirken, dann sind sie in einer Schicht zu implementieren, die oberhalb der höchsten (Teil-) Schicht der Koppelelemente liegt. Dadurch wird sichergestellt, dass die Übermittlungseinrichtungen die gesicherten Informationen unverarbeitet/ uninterpretiert weiterleiten können.

Beispiele und Folgen fehlerhafter Netzkonfigurationen:

**Beispiel 1:** Sämtliche Endgeräte zweier über Router und öffentliche Kommunikationsnetze gekoppelter LANs sollen zur Gewährleistung der Vertraulichkeit - insbesondere im Bereich öffentlicher Kommunikationsnetze - mit Schicht-2-Verschlüsselungskomponenten ausgestattet werden. Der Router muss zur Weiterleitung der LAN-Datenpakete über das öffentliche Netz die Adressen der Schicht 3 auswerten. Da sämtliche Schicht-3-Daten jedoch durch die Schicht-2-Verschlüsselung verborgen sind, kann die Auswertung der Schicht-3-Adressen nicht erfolgreich durchgeführt werden. Dadurch wird die Datenübertragung verhindert. Zur Abhilfe müssen hier die Verschlüsselungskomponenten für Schicht 3 (obere Teilschicht) oder höher eingesetzt werden.

**Beispiel 2:** Ein Großteil des Schriftverkehrs einer Institution soll zukünftig elektronisch über X.400 (Schicht 7) abgewickelt werden. Zur Sicherung der Datenintegrität plant die Institution den Einsatz von Schicht-4-Kryptokomponenten in den Endgeräten (hier PCs). Zum Zweck der Sicherung werden die Datenpakete beim Sender auf Schicht 4 mit kryptographischen Prüfsummen versehen, welche von der zugehörigen Schicht-4-Kryptokomponente des Empfängers geprüft wird. Nur Datenpakete mit korrekten Prüfsummen sollen zugestellt werden. Falls aber nicht alle MTAs (Message Transfer Agents, also die Vermittler für elektronische Mitteilungen auf Schicht 7) ebenfalls mit interoperablen Kryptokomponenten ausgestattet sind, können die MTAs ohne Kryptokomponente keine gültigen Prüfsummen erzeugen, so dass nachfolgende MTAs oder Endgeräte mit Kryptokomponente die Daten laut Vorgabe verwerfen müssen.

Aber selbst wenn sämtliche genutzten MTAs ebenso wie die Endgeräte mit interoperablen Kryptokomponenten und Sicherheitsparametern ausgestattet sind, ist die Datenintegrität nicht sichergestellt. Dann kann die abschnittsweise Sicherung der Daten zwar gewährleistet sein, eine Verfälschung der Daten innerhalb der MTAs ist jedoch unbemerkt möglich. Ferner könnten (je nach Protokoll) einzelne Schicht-4-Datenpakete verloren gehen, was zu Lücken in der Gesamtnachricht führt, deren Unversehrtheit eigentlich gesichert werden sollte. Eine Abhilfe ist hier die Integritätssicherung der Daten auf Schicht 7.

Wie die Beispiele zeigen, ist genau zu untersuchen, welche Netztopologie vorliegt und welche Netzbereiche wie gesichert werden müssen, damit eine ange-

passte Lösung mit den gewünschten (Sicherheits-)Merkmalen gefunden werden kann.

**Abschnittsweise Sicherheit <-> Ende-zu-Ende-Sicherheit**

Benutzer von Kommunikationssystemen erwarten häufig, dass Sicherheitsdienste durchgängig erbracht werden (Ende-zu-Ende-Sicherheit), also von der Eingabe der Information (Daten, Sprache, Bilder, Text) am Endgerät A bis zur Ausgabe der Information an einem entfernten Endgerät B. Ist kein durchgehender Sicherheitsdienst gewährleistet, so existieren - abgesehen von den beteiligten Endgeräten - weitere Systeme, auf denen die Informationen ungesichert vorliegen. Existiert beispielsweise keine Ende-zu-Ende-Verschlüsselung zur Sicherung der Vertraulichkeit einer Kommunikationsbeziehung zwischen zwei Teilnehmern, so liegen die Daten in mindestens einem weiteren Netzelement unverschlüsselt vor. Solche Netzelemente müssen lokalisiert und durch zusätzliche Maßnahmen abgesichert werden. Personal, welches Zugriff auf insbesondere solche ungesicherten Netzelemente hat (z. B. Administrator), muss entsprechend vertrauenswürdig sein. Sicherheitsdienste werden in diesem Fall nicht durchgängig, sondern abschnittsweise erbracht. Auf die angemessene Sicherung aller relevanten Abschnitte ist zu achten.

**Mehrfache Sicherung auf verschiedenen OSI-Schichten**

Gegen eine Mehrfachsicherung der zu übertragenden Informationen auf verschiedenen OSI-Schichten ist nichts einzuwenden, wenn gewisse Regeln befolgt werden, die bei standardkonformen Produkten jedoch implizit gewährleistet sind. Insbesondere bei der Verschlüsselung sind die aus der Schule bekannten Klammerregeln anzuwenden. So entspricht das Verschlüsseln dem Öffnen einer Klammer, das Entschlüsseln dem Schließen einer Klammer. Innerhalb der Klammer können nun wiederum weitere Sicherheitsmechanismen zur Anwendung kommen.

Nachteilig kann sich die Mehrfachsicherung dadurch auswirken, dass der Datendurchsatz aufgrund zusätzlicher Operationen reduziert wird oder dass sich die übertragbare Nutzdatenmenge dadurch vermindert, dass zusätzliche Daten zur Erhöhung der Redundanz (z. B. kryptographische Prüfsummen) übertragen werden müssen. Auch durch Daten, die vor der Übermittlung über Kryptosysteme gesichert werden, z. B. digital signierte Dokumente, ergibt sich implizit eine Mehrfachsicherung. Dadurch erhöht sich die Sicherheit der Datenübertragung hinsichtlich der verwendeten Sicherheitsdienste.

Oft lässt sich die Sicherheit des Gesamtsystems erst durch die Kombination mehrerer Sicherheitsprotokolle oder Sicherheitsprodukte erreichen. Sind z. B. anwendungsnahe Sicherheitslösungen verfügbar, deren vertrauenswürdige Implementierung jedoch nicht (von unabhängiger Seite) überprüft wurde (z. B. Evaluierung nach ITSEC, CC) und existieren gleichzeitig vertrauenswürdige transportorientierte Sicherheitsprodukte zur Absicherung unsicherer Netzabschnitte zwischen entfernten Liegenschaften, so kann durch die Kombination der Maßnahmen u. U. eine den Anforderungen genügende Gesamt-Sicherheitslösung geschaffen werden. Nachteilig wirken sich dabei meist der erhöhte Administrationsaufwand und/oder erhöhte Anschaffungskosten aus.

# M 4.91 Sichere Installation eines Systemmanagementsystems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Installation eines Systemmanagementsystems erfordert eine umfangreiche und sorgfältige Planung. Nach erfolgter Systemanalyse (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagement-Systems*), Festlegung der Managementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) und Auswahl eines geeigneten Managementsystems (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*) muss die Installation des Produktes detailliert geplant und entsprechend umgesetzt werden. In Abhängigkeit von der dem Management-Produkt zugrunde liegenden Architektur ist für das lokale Netz die konkrete Managementsystemkonfiguration zu erstellen, die insbesondere der formulierten Managementstrategie Rechnung trägt.

Zur Installation der meisten Managementsysteme muss auf den beteiligten Rechnern Managementsoftware installiert werden, die die Kommunikation zwischen Managementkonsole oder -servern und dem lokalen Rechner übernimmt. Oft müssen auf den zentralen Rechnern (Server oder Gateways) auch Datenbanksysteme installiert werden, in denen die Managementinformationen von der Managementsoftware persistent abgelegt werden. Je nach Produkt ist hier auch die Einbindung eines schon vorhandenen Datenbanksystems möglich. Generell stellt die zusätzlich zu installierende Software Anforderungen an die lokalen Ressourcen des Rechners. Daher ist bei der Planung zu beachten, welche Systemressourcen lokal vorhanden sind. Unter Umständen müssen einzelne Systeme aufgerüstet werden. Diese Kosten sollten bei der Auswahl des Management-Produktes berücksichtigt werden.

Neben diesen Kriterien, die im wesentlichen den geregelten technischen Ablauf des Systems garantieren sollen, ist aus Sicherheitsgesichtspunkten die dem Managementsystem zugehörige Software und die entsprechenden Daten in die Schutzbedarfsfeststellung gemäß IT-Grundschutz (siehe BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise*) aufzunehmen und der Schutzbedarf als "hoch" bis "sehr hoch" einzustufen. Die Kompromittierung des Managementsystems kann nicht nur den Ausfall des gesamten Netzes nach sich ziehen; durch unbemerkte Veränderungen am System kann vielmehr beträchtlicher Schaden entstehen, der sehr schnell existenzbedrohende Formen annehmen kann.

Insbesondere ist bei der Installation auf folgende Punkte zu achten:

- Alle Rechner, auf denen Managementinformationen gelagert werden, sind besonders zu sichern:
  - Es sind die Maßnahmen der Bausteine aus Schicht 3, je nach vorliegendem System, durchzuführen.
  - Insbesondere sind die Betriebssystemmechanismen so zu konfigurieren, dass auf die lokal gespeicherten Managementinformationen nicht unberechtigt zugegriffen werden kann.
  - Der Zugang zur Managementsoftware ist nur den berechtigten Administratoren und Revisoren zu gestatten.
  - Der Zutritt zu den Rechnern sollte beschränkt werden.
- Die Kommunikation zwischen den Managementkomponenten sollte verschlüsselt erfolgen - sofern dies vom Produkt unterstützt wird - um zu ver-

hindern, dass Managementinformationen mitgehört und gesammelt werden können. Unterstützt das Produkt keine Verschlüsselung, so sind gesonderte Maßnahmen zu ergreifen, um die Kommunikation abzusichern (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

Prüffragen:

- Sind die lokal gespeicherten Managementinformationen vor unberechtigtem Zugriff geschützt?
- Ist der Zugang zur Managementsoftware nur den berechtigten Administratoren und Revisoren gestattet?
- Ist der Zutritt zu den Rechnern mit Managementsoftware beschränkt?
- Ist die Kommunikation zwischen den Managementkomponenten verschlüsselt oder durch andere Maßnahmen angemessen abgesichert?

# M 4.92 Sicherer Betrieb eines Systemmanagementsystems

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für den sicheren Betrieb eines Systemmanagementsystems, welches auch aus verschiedenen Management-Tools (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*) bestehen kann, ist die sichere Konfiguration aller beteiligten Komponenten zu prüfen und sicherzustellen (siehe auch M 4.91 *Sichere Installation eines Systemmanagementsystems*). Hierzu ist es nötig, die jeweiligen Betriebssysteme der Komponenten, die durch das Systemmanagementsystem verwaltet werden und damit Teile des Systems in Form von Software und/oder Daten installiert haben, entsprechend zu sichern. Zur Absicherung gehört dabei auch die sichere Aufstellung der Rechner, die zentrale Aufgaben für das Managementsystem erfüllen (Managementserver, Rechner mit Managementdatenbanken). Daneben muss für die sichere Datenübertragung Sorge getragen werden (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

Auf die folgenden Punkte ist insbesondere während des laufenden Betriebs eines Managementsystems zu achten:

- Im Rahmen der Fortschreibung der Systemdokumentation müssen die durch das Managementsystem neu hinzugekommenen Hard- und Softwarekomponenten dokumentiert werden.
- Auch Änderungen am Managementsystem selbst müssen dokumentiert und/oder protokolliert werden.
- Die Fortschreibung gilt in gleicher Weise für das Notfallhandbuch. Insbesondere sind einerseits die Anlauf- und Recovery-Pläne zu modifizieren, da viele Standardfunktionen der verwalteten Betriebssysteme nach Einführung eines Managementsystems nun nur noch mit Hilfe der Funktionen des Managementsystems erfolgen können. Andererseits muss das Notfallhandbuch aber auch Anweisungen dafür enthalten, wie das System ohne Managementsystem (etwa bei Totalausfall zentraler Komponenten) innerhalb kurzer Zeit in hinreichendem Maße (Notbetriebsregelung) verfügbar gemacht werden kann (siehe auch Baustein B 1.3 *Notfallmanagement*).
- Ein Zugriff auf die Komponenten oder Daten des Managementsystems erfolgt in der Regel ausschließlich durch das Managementsystem selbst oder berechtigte andere Systemmechanismen (z. B. Datensicherungssystem). Daher ist der Zugriff für normale Benutzer zu unterbinden. Dies gilt im Normalfall auch für die Rolle des lokalen Administrators eines einzelnen Rechners. Muss in Ausnahmefällen tatsächlich direkt auf einem Rechner auf die lokalen Komponenten des Managementsystems zugegriffen werden (z. B. bei Crashrecovery oder Neuinstallation von Komponenten, sofern das Managementsystem dies nicht im Rahmen des Managements unterstützt), so sollte diese Berechtigung explizit und nur für die Durchführung dieser Aufgabe erteilt werden.
- Im Rahmen der Sicherheitspolitik müssen die Befugnisse festlegt sein. Auch für den Bereich Management ergibt sich eine Rollentrennung Administrator und Revisor - je nach Produkt auch zwischen Administratoren mit unterschiedlichen Rechten (z. B. Arbeitsgruppenadministrator, Bereichsadministrator). Es empfiehlt sich, bestimmte Rollen zu definieren und gemäß diesen verschiedenen Rollen Benutzer mit entsprechenden Berech-

tigungen einzurichten. Dadurch werden dem Zugreifenden lediglich die Rechte auf Komponenten oder Daten des Managementsystems erlaubt, die für seine momentane Aufgabe nötig sind. Je nach Managementsystem geschieht die Einrichtung der Benutzer im Managementsystem oder in der Benutzerverwaltung der Rechner. Da die existierenden Systeme nicht direkt die Definition unterschiedlicher Rollen (etwa Administrator und Revisor) vorsehen, müssen die Rollen bestmöglich durch das Einrichten unterschiedlicher Benutzerkonten (z. B. "Administrator", "Revisor", "RechnerAdmin", "Datenschutzbeauftragter") mit entsprechenden Berechtigungen nachgebildet werden. Je nach System ist diese Nachbildung der Rollen nur unvollständig und mit einigem Aufwand möglich, da u. U. für jede Systemkomponente (Dateien, Programme) die Berechtigungen für die einzelnen Rollen explizit vergeben und gewartet werden müssen.

- Der Zugang zur Managementsoftware ist durch sichere Passwörter zu schützen. Die Passwörter sollten gemäß Sicherheitspolitik regelmäßig geändert werden.
- Funktionen der Managementsoftware, die gemäß Managementstrategie nicht zum Einsatz kommen sollen, sind - wenn möglich - zu sperren.
- Die Protokollierungsdateien sind in regelmäßigen Abständen auf Anomalien (z. B. Ausführung von Funktionen, die nicht zum Einsatz kommen sollen) zu untersuchen. Hier empfiehlt sich der Einsatz von Protokoll-Analysatoren, die entweder in das Managementprodukt integriert oder auch als Zusatzsoftware erhältlich sein können und die (meist) regelgesteuert im Bedarfsfall Alarmmeldungen (z. B. Mail, Pager) erzeugen können.
- Das Managementsystem ist in Abständen Integritätstests zu unterziehen, so dass unberechtigte Änderungen so früh wie möglich entdeckt werden können. Dies gilt insbesondere für sämtliche Konfigurationsdaten des Managementsystems.
- Wird über das Systemmanagementsystem auch Software verteilt, so sind auch die zu verteilenden Programmdaten regelmäßig auf Veränderungen zu überprüfen, um das Verteilen modifizierter Software über das gesamte Netz zu verhindern.
- Das Managementsystem sollte auf sein Verhalten bei einem Systemabsturz getestet werden. Je nach Management- und Sicherheitspolitik muss ein automatischer Neustart des Managementsystems oder lokaler Teilkomponenten des Systems sichergestellt werden. Damit wird verhindert, dass Rechner, die dem Managementsystem angeschlossen sind, längere Zeit nicht für das Management zugreifbar sind (siehe auch M 6.57 *Erstellen eines Notfallplans für den Ausfall des Managementsystems*).
- Beim Systemabsturz dürfen die Managementdatenbanken nicht zerstört werden oder in einen inkonsistenten Zustand gelangen, damit vermieden wird, dass ein möglicher Angreifer provozierte Inkonsistenzen zum Angriff nutzen kann. Dazu muss das Managementsystem entweder auf ein Datenbanksystem zurückgreifen, das entsprechende Recovery-Mechanismen unterstützt, oder diese Mechanismen selbst implementieren (siehe M 2.170 *Anforderungen an ein Systemmanagement-System*). Werden diese Mechanismen von dem gewählten System nicht zur Verfügung gestellt (z. B. beim Einsatz von mehreren Management-Tools), sollten die Rechner, die Managementinformationen speichern, maximal möglich (auch physikalisch) gesichert werden (siehe die Bausteine der Schicht 3).
- Das Managementsystem sollte einen geeigneten Backup-Mechanismus zur Sicherung der Managementdaten enthalten oder mit einem Backup-System zusammenarbeiten. Beim Einspielen alter Datenbestände aus einer Datensicherung ist darauf zu achten, dass diese in der Regel manuell nachbearbeitet werden müssen, um der aktuellen Systemkonfiguration zu entsprechen.

- Auch mittels Backup-Verfahren gesicherte Managementdatenbestände sind so zu lagern, dass kein unberechtigter Dritter Zugriff darauf erlangen kann. In der Regel sind die Daten nicht in sicherer Form auf dem Backupdatenträger gespeichert, so dass sie von jedem, der über das Backup-Programme und ein entsprechendes Laufwerk verfügt, eingesehen werden können.
- Die Aufteilung in Managementdomänen und deren Zuständigkeiten sollte in regelmäßigen Abständen auf Gültigkeit hin untersucht werden. Dies gilt insbesondere für den Fall innerbetrieblicher Umstrukturierungen.

Prüffragen:

- Werden Änderungen am Managementsystem und neu hinzugekommene Hard- und Softwarekomponenten dokumentiert sowie das Notfallhandbuch entsprechend aktualisiert?
- Ist der Zugriff auf Komponenten oder Daten des Managementsystems ausschließlich diesem vorbehalten und der Zugriff für normale Benutzer unterbunden bzw. sind für Ausnahmefälle explizite Berechtigungen vergeben?
- Sind differenzierte Rollen mit Rechten auf Komponenten oder Daten des Managementsystems für unterschiedliche Aufgaben definiert?
- Werden sichere Passwörter für die Managementsoftware eingesetzt und regelmäßig geändert?
- Sind alle Funktionen der Managementsoftware gesperrt, die gemäß der Managementstrategie nicht zum Einsatz kommen sollen?
- Werden die Protokollierungsdateien der Managementsoftware regelmäßig auf Unregelmäßigkeiten hin untersucht?
- Werden in regelmäßigen Abständen Integritätstests des Managementsystems durchgeführt, um frühzeitig unberechtigte Änderungen zu entdecken?
- Im Fall der Softwareverteilung durch das Systemmanagementsystem: Werden in regelmäßigen Abständen Integritätstests der Programmdaten durchgeführt, um frühzeitig unberechtigte Änderungen zu entdecken?
- Ist das Managementsystem auf das Verhalten bei einem Systemabsturz getestet, um längere Zeiten der Nichtverfügbarkeit vermeiden?
- Sind Mechanismen vorhanden, die sicherstellen, dass nach einem Systemabsturz des Managementsystems die Managementdatenbanken konsistent bleiben?
- Existiert ein Backup-Verfahren zur Sicherung der Managementdaten?
- Wird die Aufteilung in Managementdomänen und deren Zuständigkeiten regelmäßig auf Gültigkeit hin überprüft?

# M 4.93 Regelmäßige Integritätsprüfung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine regelmäßige Kontrolle des Dateisystems, der Dateiattribute und der Prozessinformationen sowie weiterer wichtiger Elemente der Systemkonfiguration (beispielsweise unter Windows die Registry) auf unerwartete Veränderungen hilft dabei, Inkonsistenzen zu erkennen. Die Erkennung solcher Inkonsistenzen kann zur Vorbeugung gegen Systeminstabilitäten eingesetzt werden. Es können dadurch aber auch Angriffe zeitnah entdeckt werden. Sollte tatsächlich ein Angriff vorliegen, ist es wichtig, das Vorgehen des Angreifers zu rekonstruieren. Dies dient einerseits dazu, Manipulationen an Daten aufzudecken, und andererseits dazu, verborgene Hintertüren zu erkennen, die ein Angreifer für einen späteren Zugriff auf den Rechner installiert haben könnte.

### Berechnung kryptographischer Prüfsummen

Zur Erkennung von Manipulationen können Programme genutzt werden, die kryptographische Prüfsummen über einen Großteil der Dateien des Systems oder über andere Ressourcen berechnen. Zu unterscheiden sind dabei Integritätsprüfungsprogramme, welche nur auf Dateiebene arbeiten, und solche, die auch Prozesse und spezielle Konfigurationsdaten, wie die Windows-Registry oder Datenstrukturen des Kernels, überprüfen können. Es wird empfohlen, darauf zu achten, dass diese Werkzeuge auch zentral administriert und überwacht werden können. Außerdem müssen die vom Programm verwendeten kryptographischen Mechanismen dem Stand der Technik entsprechen.

Einige Programme stellen lediglich fest, ob Veränderungen am Dateisystem durchgeführt wurden. Hierzu prüfen sie, ob die Zugriffsrechte, das Datum der letzten Modifikation oder die Inhalte der jeweiligen Datei geändert wurden. Modifikationen werden erkannt, indem die vorher erstellte kryptographische Prüfsumme mit der aktuell berechneten Prüfsumme verglichen wird. Mit einer speziellen Einstellung kann in vielen Fällen auch ein nur lesender Zugriff auf die Datei bemerkt werden.

### Schutz der Prüfsummendatei

Um zu verhindern, dass das Integritätsprüfungsprogramm selbst oder die Datei, welche die Prüfsummen des Systems enthält, von einem Angreifer oder durch Schadsoftware verfälscht werden können, sollten sich diese auf einem schreibgeschützten Datenträger befinden. Allerdings muss die Prüfsummendatei bei erlaubten Veränderungen am Dateisystem ebenfalls geändert werden, so dass sich CDs, DVDs oder Wechselplatten für diesen Zweck empfehlen. Alternativ kann die Prüfsummendatei auch über das Netz schreibgeschützt zur Verfügung gestellt werden. Bei einer Verwaltung des Integritätsprüfungsprogramms über das Netz sollte dieser Weg auch bevorzugt werden. Einige Schadprogramme tarnen sich, so dass sie mit Methoden des manipulierten Betriebssystems nicht erkannt werden können. Daher ist es im Verdachtsfall sinnvoll, das System mittels eines manipulationsfreien Betriebssystems zu untersuchen. Dieses kann beispielsweise von einer CD-ROM gestartet werden, die von einem vertrauenswürdigen Referenzsystem erzeugt wurde.

### Prüfintervall und Prüfumfang

Eine Integritätsprüfung sollte regelmäßig, beispielsweise jede Nacht, durchgeführt werden. Die Wahl eines geeigneten Prüfintervalls hängt stark vom Einsatzzweck des jeweiligen IT-Systems beziehungsweise der Einsatzumge-

bung ab. Bei der Durchführung von Integritätsprüfungen ist außerdem der Verbrauch an Speicherplatz und Rechenzeit, der für die Überprüfung der Prüfsummen notwendig ist, zu berücksichtigen. Der Einsatz des Integritätsprüfungsprogramms darf den ordnungsgemäßen Betrieb nicht beeinträchtigen.

Im normalen Betrieb jedes größerenIT-Systems ergeben sich ständig kleinere und größere Änderungen an Systemdateien. Generell ist es daher empfehlenswert, das Integritätsprüfungsprogramm so zu konfigurieren, dass nur Veränderungen an relevanten Dateien erfasst werden. Anderenfalls besteht die Gefahr, dass sehr viele Änderungsmeldungen ausgelöst werden, die auf ganz normale betriebliche Abläufe und nicht auf Angriffsversuche zurückzuführen sind (false positives). Als Folge kann es passieren, dass die Protokolldateien nicht mehr zeitnah ausgewertet werden können.

**Prozessinformationen im Arbeitsspeicher**

Neben dateibasierten Integritätsprüfungen gibt es auch die Möglichkeit, Prozessinformationen aus dem Arbeitsspeicher gegen eine Liste erlaubter Prozesse (Whitelist) zu prüfen. Auf diese Weise lassen sich auch bestimmte Manipulationen erkennen, die keine Spuren im Dateisystem hinterlassen. Andererseits gibt es Manipulationen, die nicht die Prozesse selbst, sondern nur deren Konfiguration betreffen. Solche Manipulationen lassen sich unter Umständen leichter durch eine Integritätsprüfung der Konfigurationsdateien aufdecken. Integritätsprüfungen des Dateisystems und des Arbeitsspeichers haben somit teilweise unterschiedliche Schutzwirkungen. Ein Vorteil der Prüfung von Prozessinformationen im Arbeitsspeicher ist, dass dazu nur wenige oder keine Festplattenzugriffe nötig sind, die deutlich langsamer sind als Arbeitsspeicherzugriffe. Dadurch kann wesentlich häufiger geprüft werden als bei einer dateibasierten Methode, bei der viele Informationen von der Festplatte gelesen werden müssen. So können unerwünschte Programme meist schneller entdeckt werden als bei einer dateibasierten Integritätsprüfung.

**Benachrichtigung**

Eine Benachrichtigung über das Ergebnis sollte, auch wenn keine Veränderungen festgestellt wurden, automatisch per E-Mail oder einen ähnlichen Weg an den Administrator erfolgen. Vorab sollte festgelegt werden, welche Maßnahmen einzuleiten sind, wenn ein Integritätsverlust festgestellt wird. Wichtig ist beispielsweise, ob automatische oder manuelle Aktionen durchgeführt werden.

Prüffragen:

- Entsprechen die verwendeten kryptographischen Mechanismen der Integritätsprüfung dem Stand der Technik?
- Werden die Prüfsummendatei und das Prüfprogramm selbst ausreichend vor Manipulationen geschützt?
- Ist sichergestellt, dass wichtige Hinweise auf einen Integritätsverlust nicht in einer Fülle irrelevanter Änderungsmeldungen (false positives) untergehen?

# M 4.94 Schutz der Webserver-Dateien

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Dateien und Verzeichnisse auf einem Webserver müssen gegen unbefugte Veränderungen, aber auch - je nach Sicherheitsanforderungen - gegen unbefugten lesenden Zugriff geschützt werden. Werden Inhalte auf dem Webserver dynamisch erzeugt, so gilt dies zusätzlich und ganz besonders für die Programme (Skripte oder Server-Erweiterungen), die dafür verwendet werden.

### Generelle Aspekte

Generell muss zwischen zwei verschiedenen Aspekten unterschieden werden, nämlich dem Schutz vor unbefugtem Zugriff lokaler Benutzer und dem Schutz vor unbefugtem Zugriff von außen über das Web.

### Schutz vor unbefugten Veränderungen

Auf vielen Webservern ändern sich nur die Protokolldateien ständig, alle anderen Dateien sind statisch. Dies trifft insbesondere auf Systemprogramme und die Webseiten zu. Webseiten werden zwar regelmäßig aktualisiert, sollten aber nicht auf dem Webserver selber bearbeitet werden.

Die Schreib- und Leserechte der Web-Dateien sollten als lokale Dateien nur berechtigten Benutzern Zugriff erlauben. Daher sollte bereits bei der Planung des Webangebots ein Benutzer- und Rollenkonzept erstellt werden (siehe auch M 2.176 *Geeignete Auswahl eines Internet Service Providers*).

Um sicherzustellen, dass keine Dateien auf dem Webserver unbemerkt abgeändert werden können, können über alle statischen Dateien und Verzeichnisse Prüfsummen gebildet werden, siehe auch M 4.93 *Regelmäßige Integritätsprüfung*. Diese sollten dann regelmäßig überprüft werden.

Um zu verhindern, dass Web-Dateien überhaupt von Unbefugten geändert werden können, können statische Daten auf einem schreibgeschützten Speichermedium (z. B. CD-ROM oder Festplatte mit Schreibschutz) gespeichert werden.

Falls das Webangebot nicht nur aus statischen HTML-Dateien besteht, sondern bestimmte Inhalte dynamisch erzeugt werden, so müssen die dazu benutzten Programme (beispielsweise CGI-Skripte, Java Server Pages) besonders sorgfältig programmiert werden, um zu verhindern, dass auf diesem Weg ein unbefugter Zugriff oder gar eine Kompromittierung des Servers erfolgen kann.

Auf dem Server müssen solche Programme vor unbefugtem Zugriff geschützt werden. Nur die Benutzer oder Benutzergruppen, die unbedingt Zugriff auf diese Programme oder Skripte brauchen (etwa Entwickler oder Administratoren), dürfen eine Schreibberechtigung haben. Normalerweise dürfen die Programme nicht für den Benutzer schreibbar sein, unter dessen Kennung der Webserver-Prozess ausgeführt wird. Für normale Benutzer sollten insbesondere Skripte nicht lesbar sein, da diese eventuell sensitive Informationen wie Authentisierungsdaten für den Zugriff auf Datenbanken enthalten können. Gleiches gilt für eventuell vorhandene Konfigurationsdateien.

**Schutz vor unbefugtem Zugriff über das Internet**

Der Zugriff über das Web auf Dateien oder Verzeichnisse eines Webservers kann auf verschiedene Arten gesteuert werden.

Welche Arten der Zugriffssteuerung unterstützt werden und wie diese implementiert sind hängt vom verwendeten Serverprodukt ab. Die folgenden Möglichkeiten sind verbreitet und werden von den meisten Webservern und Clients unterstützt.

**Authentisierung von Clients über IP-Adressen**

Der Zugriff auf Web-Dateien kann bei vielen Servern auf frei wählbare IP-Adressen, Teilnetze oder Domänen beschränkt werden. Die Authentisierung über numerische IP-Adressen bietet nicht den Schutz kryptographischer Verfahren, da sie über einen auf IP-Spoofing basierenden Angriff unwirksam gemacht werden kann. Bei IP-Spoofing fälscht ein Angreifer IP-Pakete, um vorzugeben, von einem vertrauenswürdigen IT-System zu kommen (siehe G 5.48 *IP-Spoofing*). Über eine Firewall kann jedoch verhindert werden, dass Externe vortäuschen können, Interne zu sein. Wird der Zugriff nicht auf numerische IP-Adressen oder Teilnetze sondern auf bestimmte Rechnernamen oder Domainnamen beschränkt, ist außerdem die Gefährdung durch DNS-Spoofing (siehe G 5.78 *DNS-Spoofing*) zu betrachten.

Wenn der Web-Browser über einen Proxy-Server auf den Webserver zugreift, ist zu bedenken, dass der Webserver nur die IP-Adresse des Proxy erfährt. Ein Proxy kann aber nur dann als vertrauenswürdig angesehen werden, wenn alle IT-Systeme und Benutzer, die hinter ihm verborgen sind, ebenfalls vertrauenswürdig sind.

Wenn der Zugriff auf Web-Dateien auf vorgegebene IP-Adressen, Teilnetze oder Domänen beschränkt wird, kann es daher sinnvoll sein, diese zusätzlich mit einem Passwort zu schützen.

**Passwortschutz**

Eine weitere Möglichkeit der Zugriffssteuerung, die in praktisch allen Webservern implementiert ist, stellt der Schutz über Benutzernamen und Passwörter dar. Der Benutzer gibt beim erstmaligen Zugriff auf ein entsprechend geschütztes Verzeichnis in seinem Browser einen Benutzernamen und ein Passwort an, das zum Zugriff auf die entsprechende Ressource berechtigt. Über das Protokoll HTTP lässt sich ein Passwortschutz (Benutzer-Authentisierung) auf verschiedene Arten realisieren, die sich im Bezug auf Implementierungsaufwand und Sicherheit unterscheiden.

In Abhängigkeit von den Sicherheitsanforderungen muss eine geeignete Methode zur Benutzer-Authentisierung ausgewählt werden. Bei höheren Sicherheitsanforderungen sollte SSL oder TLS zur Verschlüsselung der Datenübertragung und gegebenenfalls auch zur Benutzer-Authentisierung über Client-Zertifikate eingesetzt werden. Näheres ist in M 4.176 *Auswahl einer Authentisierungsmethode für Webangebote* beschrieben, Informationen zu SSL und TLS finden sich in M 5.66 *Clientseitige Verwendung von SSL/TLS*.

**Dateiverschlüsselung**

Eine weitere Möglichkeit zum Schutz von Web-Dateien ist es, Dateien verschlüsselt auf einem Webserver abzulegen, so dass nur diejenigen die Daten lesen können, die im Besitz des richtigen kryptographischen Schlüssels sind. Dieses Vorgehen bietet zusätzlich den Schutz vor unbefugtem lokalem Zu-

griff, verlangt allerdings ein entsprechendes, unter Umständen aufwendiges, Schlüsselmanagement.

Prüffragen:

- Werden Dateien und Verzeichnisse auf einem Webserver vor unbefugtem Lesen und Schreiben geschützt?
- Integritätsprüfung von Dateien und Verzeichnissen durch Prüfsummen: Werden die Prüfsummen der Dateien und Verzeichnisse regelmäßig überprüft?
- Erzeugung dynamischer Inhalte: Sind die Programme zur Inhaltserzeugung sicher programmiert und sicher auf dem Server gespeichert, so dass unbefugte Zugriffe auf den Server durch sie nicht erfolgen können?
- Sind Skripte und Konfigurationsdateien für normale Benutzer nicht lesbar?
- Bei Authentisierung von Clients über Rechner oder Domainnamen: Werden Maßnahmen gegen DNS-Spoofing und Pharming getroffen?
- Authentisierung von Clients über IP-Adressen: Werden Verbindungen von Proxy-Servern nur dann als vertrauenswürdig angesehen wenn alle IT-Systeme hinter dem Proxy auch vertrauenswürdig sind?
- Schutz der WWW-Dateien durch Passwörter: Wird in Abhängigkeit von den Sicherheitsanforderungen eine geeignete Methode zur Benutzer-Authentisierung gewählt?

# M 4.95 Minimales Betriebssystem

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Rechner in einem sicherheitskritischen Umfeld sollten so konzipiert sein, dass sie möglichst wenig Angriffspunkte bieten. Da heutige Betriebssysteme standardmäßig viele Netzdienste bereitstellen, reicht für den Betrieb eines sicheren Servers ein gut konzipierter Serverdienst (z. B. ein SSL-basierter Webserver) nicht aus. Vielmehr muss auch das Betriebssystem abgesichert werden, da ansonsten über eine Schwachstelle im Betriebssystem die Sicherheitsfunktionen des Serverdienstes umgangen werden könnten. Ein sogenanntes minimales Betriebssystem zeichnet sich dadurch aus, dass es im Idealfall keinen einzigen Netzdienst zur Verfügung stellt. Ein potentieller Angreifer kann also eine Schwachstelle in einem Netzdienst dieses Betriebssystems nicht ausnutzen. Und sollte ein Angreifer doch durch eine Schwachstelle Zugriff auf den Rechner bekommen haben, so wird er durch das Minimalsystem weiter behindert. Je weniger Programme ein Angreifer auf einem Zielrechner vorfindet, desto schwieriger wird es für ihn, weitere Schwachstellen in dem Zielrechner zu finden bzw. auszunutzen. Außerdem erleichtert dies die Pflege eines Servers sehr stark, da die Patches bzw. Service Packs für Diensteprogramme nicht mehr eingespielt werden müssen, wenn diese nicht vorhanden sind.

Im folgenden wird die Konfiguration eines Betriebssystems anhand eines Internet-Servers beschrieben, da hier im allgemeinen sehr hohe Sicherheitsanforderungen an das Betriebssystem gestellt werden müssen.

Ein Internet-Server hat meist nur eine einzige Aufgabe: stabil eine bestimmte Anzahl von Diensten (z. B. die Bereitschaft, E-Mail entgegenzunehmen) anderen Rechnern zur Verfügung zu stellen. Das zugrunde liegende Betriebssystem sollte keine weiteren Dienste anbieten. Deshalb sollte bei der Installation eines Internet-Servers folgendes Vorgehen eingehalten werden:

**1. Grundinstallation des Betriebssystems**

Kann man bei der Installation den Umfang der zu installierenden Pakete beeinflussen, so sollten schon hier nur die notwendigen Pakete eingespielt werden. Die Notwendigkeit bestimmter Pakete ist allerdings nicht immer zu erkennen, so dass zumindest die offensichtlich überflüssigen Pakete nicht eingespielt werden sollten.

**2. Abschalten nicht benötigter Programme**

Beim Start eines Rechners werden eine Vielzahl von Programmen automatisch gestartet. Einige dieser Programme sind für einen Internet-Server völlig überflüssig und sollten deaktiviert werden. Die Deaktivierung kann durch das Verhindern des automatischen Starts erfolgen (Startskripte unter Unix, Autostart und Dienstemanager unter Windows NT) und durch zusätzliches Löschen der entsprechenden Programme. Aus Gründen der Sicherheit wird das Löschen empfohlen, da dann ein Angreifer die Dienste nicht wieder reaktivieren kann. Allerdings ist es manchmal sehr schwierig, alle zu einem bestimmten Dienst gehörigen Dateien zu finden und zu löschen, so dass im Zweifel das Löschen unterbleiben sollte.

**3. Konfiguration der Netzparameter**

Falls dies nicht schon bei der Installation geschehen ist, müssen die Netzparameter des Internet-Servers eingestellt werden. Relevant für die Sicherheit

des Internet-Servers sind unter anderem die Wahl eines *Default Gateways* und eines *Domain Name Servers*. Findet beispielsweise die Kommunikation des Internet-Servers mit dem Internet über einen Proxy (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*) statt, so ist ein *Default Gateway* überflüssig. Ohne ein *Default Gateway* ist eine direkte Antwort vom Internet-Server ins Internet nicht möglich, so dass bei Umgehung des Proxies keine Kommunikation, d. h. auch kein Angriff, stattfinden kann. Auch DNS ist für einen Internet-Server häufig überflüssig und sollte möglichst vermieden werden, da dies einen direkten Kommunikationskanal zum Betriebssystem ermöglicht (siehe M 4.96 *Abschaltung von DNS*). Zusätzlich gibt es noch eine Vielzahl von Parametern, die den sogenannten TCP/IP-Stack direkt beeinflussen, z. B. die maximale Größe von IP-Paketen. Diese Parameter sind extrem stark vom jeweiligen Betriebssystem abhängig, so dass hier nur das Abschalten von IP-Forwarding erwähnt werden kann. Weitere Änderungen könnten beispielsweise die Stabilität gegenüber fehlerhaften IP-Paketen oder aber auch den Netzdurchsatz erhöhen.

**4. Abschalten nicht benötigter Netzdienste**

Einige benötigte Diensteprogramme stellen eine Vielzahl weiterer Dienste bereit (insbesondere ist hier der *inetd* unter Unix gemeint). Die entsprechenden Konfigurationsdateien sind auf die notwendigen Netzdienste einzuschränken (siehe auch M 5.16 *Übersicht über Netzdienste*).

**5. Installation von Sicherheitsprogrammen**

Das Betriebssystem sollte um zusätzliche Sicherheitsprogramme erweitert werden, falls diese nicht schon Teil des Betriebssystems sind. Insbesondere sinnvoll sind ein Integritätsprüfprogramm (siehe M 4.93 *Regelmäßige Integritätsprüfung*) und ein Softwarepaketfilter (bei Windows NT schon enthalten). Empfehlenswert sind zusätzlich Programme zur Virensuche und zur Auswertung der Protokolleinträge. Ist eine Fernadministration des Internet-Servers gewünscht, so muss ein entsprechendes Sicherheitsprodukt installiert werden, z. B. der Secure Shell Daemon (siehe M 5.64 *Secure Shell*), und regelmäßig die Sicherheit des Systems überprüft werden (siehe auch M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*).

**6. Konfiguration und Überprüfung der Netzdienste**

Idealerweise stellt ein minimales Betriebssystem keinen einzigen Netzdienst zur Verfügung und ist somit von außen nicht angreifbar. Gerade in größeren Netzen ist dieses Vorgehen aufgrund der Administration nicht mehr praktikabel, so dass ein Fernzugang notwendig ist. Ob der Internet-Server Dienste bereitstellt, kann sowohl unter Unix als auch Windows NT mit dem Befehl *netstat -a* überprüft werden. Jeder der aufgelisteten Dienste sollte in seiner Konfiguration so eingeschränkt werden, dass nur berechtigte Rechner auf ihn zugreifen können (z. B. ist der Fernzugang zum Internet-Server auf die Rechner des Netzmanagements einzuschränken).

**7. Löschen nicht mehr benötigter Programme**

Sobald die Installation eines minimalen Betriebssystems abgeschlossen ist, sollten verschiedene Programme gelöscht werden, die einem potentiellen Angreifer hilfreich sein könnten. Insbesondere sind eventuell vorhandene Compiler zu entfernen, da diese einem Angreifer ein wertvolles Hilfsmittel sein könnten. Außerdem sind Compiler auf Internet-Servern auch deshalb nicht sinnvoll, da diese Rechner Produktionsmaschinen sind und Programmentwicklung und Tests auf anderen Rechnern durchgeführt werden sollten. Ebenfalls denkbar

ist das Löschen aller Editoren, was einem Angreifer die Manipulation von Konfigurationsdateien sehr stark erschweren würde. Allerdings ist dann auch die Administration komplizierter. Bei Änderungen an Konfigurationsdateien muss dann jeweils wieder ein Editor installiert werden oder aber, und dies ist empfehlenswert, die Konfigurationsdateien müssen auf einem anderen Rechner editiert und dann überspielt werden.

Ein minimales Betriebssystem sollte natürlich kein Selbstzweck sein. Für einen Internet-Server muss selbstverständlich noch der eigentliche Serverdienst installiert werden. Ob dies am Ende der obigen Liste geschieht oder beispielsweise zwischen den Punkten 6 und 7 oder auch direkt nach Punkt 1, hängt von der jeweiligen Installation ab. Problematisch wird es, wenn die Installation wegen fehlender Betriebssystempakete fehlschlägt, da man dann die fehlenden Pakete suchen und selber nachinstallieren muss. Besser wäre es, der Hersteller des Serverdienstes gäbe die Betriebssystemabhängigkeiten an, so dass das Minimalsystem von Anfang an darauf ausgerichtet werden könnte.

Auch ein mit einem Minimalsystem konfigurierter Rechner ist nicht gänzlich vor Angriffen geschützt. Die wahrscheinlichste Ursache für einen erfolgreichen Angriff ist sicherlich der Serverdienst, aber auch das Minimalsystem selber ist noch angreifbar, insbesondere nämlich der TCP/IP-Stack, der die Netzpakete zur Applikation weiterleiten muss. Nahezu alle bisher bekannt gewordenen Angriffe gegen den TCP/IP-Stack betrafen allerdings nur die Verfügbarkeit, indem die betroffenen Rechner abstürzten, d. h. ein Eindringen in Rechner ist noch nicht beobachtet worden. Um auch diese Gefahr weiter zu verkleinern, sollte auch M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* umgesetzt werden.

Prüffragen:

- Bieten Rechner in einem sicherheitskritischen Umfeld möglichst wenig Angriffspunkte?
- Installation des Betriebssystems: Werden nur benötigte Pakete mit eingespielt?
- Starten des Rechners: Werden nicht benötigte Programme deaktiviert oder schon vorher gelöscht?
- Werden die benötigten Dienstprogramme so weit wie möglich in ihren Funktionen eingeschränkt und können nur berechtigte Rechner auf die Dienstprogramme zugreifen?
- Sind auf den Betriebssystemen Sicherheitsprogramme wie z.B. Softwarepaketfilter oder Integritätsprüfprogramme installiert?
- Fernadministration: Sind entsprechende Sicherheitsprodukte installiert und wird die Sicherheit der Systeme regelmäßig überprüft?

# M 4.96 Abschaltung von DNS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Internet-Server braucht normalerweise kein DNS (Domain Name System), um Informationen zur Verfügung zu stellen, es sei denn, über ihn wird die E-Mail versandt, wovon aber abzuraten ist (siehe dazu auch M 4.97 *Ein Dienst pro Server*). So wird bei den meisten Webservern DNS nur dazu verwendet, in den jeweiligen Protokolldateien Rechnernamen statt IP-Adressen einzutragen. Diese Umwandlung von IP-Adressen zu Rechnernamen könnte auch später bei der Analyse der Protokolldateien durchgeführt werden. Zwar ist dann der Umgang mit den Protokolldateien etwas umständlicher, aber die Vertrauenswürdigkeit der Protokolldaten steigt. Die Zuordnung zwischen einer IP-Adresse und einem Rechnernamen ist nämlich weder eindeutig noch statisch. Ein Verzicht auf DNS gibt zusätzlich Schutz vor DNS-Spoofing (siehe M 5.59 *Schutz vor DNS-Spoofing bei Authentisierungsmechanismen*) und erhöht häufig die Performance des Internet-Servers.

Folgendes Szenario zeigt mögliche negative Auswirkungen:

Ein Angreifer verfügt über eine eigene Domain mit einem Test-PC. Dieser Test-PC ist gleichzeitig auch DNS-Server für diese Domain. Mit dem Test-PC baut er eine Verbindung zu einem Internet-Server auf. Der Internet-Server kennt am Anfang der Verbindungsanfrage nur die IP-Adresse des Test-PCs und versucht, sich über DNS den Rechnernamen des Test-PCs zu verschaffen. Zu diesem Zweck muss das Betriebssystem eine Verbindung mit einem DNS-Server aufnehmen, der sich wiederum die Daten von dem Test-PC holen muss, da dieser der DNS-Server der Angreifer-Domain ist. Anstatt nun dem DNS-Server des Internet-Servers zu antworten, kann der Angreifer nun auch direkt eine beliebige Antwort zum Internet-Server selber schicken (unter Verwendung von IP-Spoofing, siehe G 5.78 *DNS-Spoofing*). Auf diese Weise kann der Angreifer nicht nur Daten zu dem eigentlichen DNS-Server schicken, sondern auch direkt zum Internet-Server. Eventuelle Fehler in dessen Betriebssystem könnten so ausgenutzt werden.

**Hinweis:** Soll beispielsweise der Zugriff auf einen Webserver nur einer bestimmten Domain erlaubt sein, z. B. nur *.de, so kann allerdings nicht auf DNS verzichtet werden. Jedoch ist ein solcher Zugriffsschutz sehr schwach und daher nicht empfehlenswert.

Prüffragen:

- Wurde der Möglichkeit der DNS Abschaltung untersucht?

# M 4.97 Ein Dienst pro Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Viele Schwachstellen in IT-Systemen sind einzeln nicht für einen potentiellen Angreifer ausnutzbar. Häufig wird erst durch die Kombination von Schwachstellen ein erfolgreiches Eindringen in einen Rechner möglich. Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste kann es deshalb zweckmäßig sein, auf einem Rechner nur *einen* Dienst zu betreiben. Dies betrifft vor allem Server, die Dienste auch ins Internet oder in andere Fremdnetze anbieten.

Beispielsweise kann das Sicherheitsniveau dadurch gesteigert werden, dass sowohl der Webserver als auch der E-Mailserver jeweils auf eigenständigen, dedizierten Rechnern, die als Minimalsystem ausgelegt sind (siehe auch M 4.95 *Minimales Betriebssystem*), betrieben werden.

Außerdem sind einzelne Dienste auch unterschiedlich in ihrer Sicherheitseinstufung. So ist ein erfolgreiches Eindringen in einen Webserver unter Umständen sehr ärgerlich, insbesondere wenn der Angreifer die extern verfügbaren Webseiten abändert. Zugriff auf vertrauliche Informationen ist dem Angreifer hierdurch aber meist nicht möglich. Ist der Webserver aber gleichzeitig der E-Mailserver, so kann der Angreifer unter Umständen den gesamten E-Mail-Verkehr mitlesen, was möglicherweise viel schlimmere Auswirkungen hat.

Die Aufteilung kann sogar noch verstärkt werden, indem für einen einzelnen Dienst verschiedene Aufgaben auf unterschiedliche Rechner verteilt werden. So könnte es beispielsweise einen E-Mailserver A geben, der E-Mails aus dem Internet annimmt und in das interne Netz weiterleitet, und einen anderen E-Mailserver B, der E-Mails aus dem internen Netz an das Internet weiterleitet. Da die Kommunikationsaufnahme aus dem Internet nur mit dem E-Mailserver A möglich ist, kann ein Angreifer auch nur diesen direkt attackieren. Der E-Mailserver A darf selber keine E-Mails in das Internet verschicken, deshalb kann dieser Rechner auch nicht für E-Mail-Spamming missbraucht werden.

Eine Aufteilung verschiedener Dienste auf unterschiedliche Rechner hat unter anderem folgende Vorteile:

- Leichtere Konfiguration der einzelnen Rechner
- Einfachere und sicherere Konfiguration eines vorgeschalteten Paketfilters
- Erhöhte Widerstandsfähigkeit gegenüber Angriffen
- Erhöhte Ausfallsicherheit

Durch ein geeignetes zentrales Systemmanagement kann der zusätzliche Administrationsaufwand, der durch die höhere Anzahl der Rechner entsteht, begrenzt werden.

**Virtualisierung**

Im Falle von sicherheitskritischen Diensten sollten auch in virtuellen IT-Systemen jeweils nur ein Dienst betrieben werden, wie dies auch für physische Systeme gilt. Ein virtuelles IT-System selbst ist jedoch in diesem Sinne kein "Dienst" eines Virtualisierungsservers. Daher können auf einem Virtualisierungsserver mehrere virtuelle IT-Systeme betrieben werden. Je nachdem, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) der Virtualisierungsserver beruht, kann allerdings die Varianz der durch die virtuellen IT-Systeme bereitgestellten Dienste eingeschränkt sein. Ob das ein-

gesetzte Virtualisierungsprodukt geeignet ist, unterschiedliche Dienste in virtuellen IT-Systemen auf einem Virtualisierungsserver bereitzustellen, muss für das konkrete Produkt geprüft werden. Als Kriterien sind hierfür die Stärke der Isolation und der Kapselung der virtuellen IT-Systeme auf dem Virtualisierungsserver heranzuziehen (siehe M 3.72 *Grundbegriffe der Virtualisierungstechnik*). Je stärker die virtuellen IT-Systeme auf dem Virtualisierungsserver isoliert sind, desto eher eignet sich das Virtualisierungsprodukt dazu, unterschiedliche Dienste in den verschiedenen virtuellen IT-Systemen zu betreiben. Die folgenden Grundsätze lassen sich für eine erste Beurteilung heranziehen:

- Auf Virtualisierungsservern mit einer Betriebssystemvirtualisierungslösung sollten in der Regel nur virtuelle IT-Systeme mit einer Funktion bereitgestellt werden. So sollten auf einem solchen Virtualisierungsserver beispielsweise ausschließlich Webserver oder ausschließlich Mailserver, aber keine Mischung aus diesen Gruppen betrieben werden. Bei einigen Produkten zur Betriebssystemvirtualisierung ist die Isolation der virtuellen IT-Systeme allerdings stark genug, so dass von dieser Vorgabe abgewichen werden kann.
- Auf Virtualisierungsservern mit einer Servervirtualisierungslösung ist es meist zulässig, virtuelle IT-Systeme mit unterschiedlichen Diensten zu betreiben. Es können also unter Umständen Webserver und Mailserver auf einem Virtualisierungsserver in jeweils getrennten virtuellen IT-Systemen gemeinsam bereitgestellt werden.

Auf einem Virtualisierungsserver selbst sollten allerdings neben der Virtualisierungssoftware und damit direkt verbundener Dienste (Verwaltungsdienst für die Virtualisierung etc.) keine weiteren Dienste betrieben werden.

Prüffragen:

- Wird darauf geachtet, nur einen Dienst pro Server anzubieten?

# M 4.98 Kommunikation durch Paketfilter auf Minimum beschränken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Paketfilter sind IT-Systeme mit spezieller Software, die die Informationen der unteren Schichten des OSI-Modells filtern und entsprechend spezieller Regeln Pakete weiterleiten oder abfangen (siehe M 2.74 *Geeignete Auswahl eines Paketfilters*).

Die Konfiguration eines Paketfilters, der zum Schutz von Internet-Servern eingesetzt wird, sollte sehr restriktiv sein, um die Widerstandsfähigkeit gegen Angriffe zu maximieren. Zwar sollte sich ein gut konfigurierter Internet-Server (siehe M 4.95 *Minimales Betriebssystem*) selbst vor Angriffen schützen können, jedoch ist die Software eines Internet-Servers viel komplexer und fehleranfälliger als die eines auf Sicherheit konzipierten Paketfilters. Der Paketfilter sollte nur diejenigen Kommunikationskanäle durchlassen, die für die Funktion der Internet-Server notwendig sind. Insbesondere ist nicht nur die Kommunikation zu kontrollieren, die vom Internet zum Internet-Server initiiert wird, sondern auch die Kommunikation, die der Internet-Server zum Internet hin aufbauen darf. Für viele Angriffe ist es eine notwendige Voraussetzung, dass der angegriffene Rechner neue Verbindungen zum Internet hin aufbauen kann. Ist dies nicht möglich, sind auch viele Angriffe nicht erfolgreich. So war 1997 ein Angriff auf News-Server sehr verbreitet, bei dem sich der Angreifer über einen Fehler in einem News-Daemon per E-Mail wichtige Systeminformationen zuschicken lassen konnte. Hätten die angegriffenen Rechner nicht die Berechtigung zum Verschicken von E-Mails gehabt, so hätte der Angreifer auch keine Rückmeldung bekommen und der Angriff wäre nicht erfolgreich gewesen.

Im Folgenden werden einige Beispiele für die Konfiguration von Paketfiltern für verschiedene Internet-Server dargestellt.

- Webserver:
  - Internet darf auf Port 80, beziehungsweise 443 für SSL/TLS, des Webservers TCP
  - Webserver darf ins Internet von Port 80, beziehungsweise 443 für SSL/TLS, TCP/ack, sonst nichts!
- News-Server:
  - Newsfeed-Server dürfen auf Port 119 des News-Servers TCP
  - News-Server darf von Port 119 auf Newsfeed-Server TCP/ack
  - News-Server darf auf Port 119 der Newsfeed-Server TCP
  - Newsfeed-Server dürfen von Port 119 auf den News-Server TCP/ack
- Mailserver (Provider stellt E-Mail-Gateway zur Verfügung):
  - Mailserver des Providers darf auf Port 25 des Mailservers TCP
  - Mailserver darf von Port 25 auf Mailserver des Providers TCP/ack
  - Mailserver darf auf Port 25 des Mailservers des Providers TCP
  - Mailserver des Providers darf von Port 25 auf Mailserver TCP/ack
- Mailserver (eigenes Verschicken ins Internet):
  - Internet darf auf Port 25 des Mailservers TCP
  - Mailserver darf von Port 25 ins Internet TCP/ack

  - Mailserver darf auf Port 25 im Internet TCP
  - Internet darf von Port 25 auf den Mailserver TCP/ack
- DNS-Server:
  - Resolving DNS-Server darf auf Port 53 des Advertising DNS-Servers UDP
  - Advertising DNS-Server darf auf alle Ports des Resolving DNS-Servers UDP (nur bei stateless Firewall nötig)
  - Resolving DNS-Server darf auf Port 53 seines Forwarders UDP
  - Forwarder darf auf alle Ports des Resolving DNS-Servers UDP (nur bei stateless Firewall nötig)
  - Externes Netz darf auf Port 53 des Advertising DNS-Servers UDP
  - Advertising DNS-Server darf auf alle Ports externer DNS-Server UDP und TCP (nur bei stateless Firewall nötig)
  - Internes Netz darf auf Port 53 des Resolving DNS-Servers UDP
  - Resolving DNS-Server darf auf alle Ports des internen Netzes UDP (nur bei stateless Firewall nötig)
  - Primary DNS-Server darf auf Port 53 seiner Secondary DNS-Server UDP und TCP
  - Secondary DNS-Server darf auf Port 53 seines Primary DNS-Server UDP und TCP

Werden nur diese Regeln implementiert, ist eine Kommunikationsaufnahme aus dem Internet auf die freigegebenen Dienste beschränkt. Können die Kommunikationspartner noch weiter eingeschränkt werden (siehe obige Beispiele), so kann ein Angreifer gar keine direkte Verbindung zu dem Internet-Server aufbauen.

**Hinweis:** Obige Regeln können bewirken, dass der Internet-Server nicht von jedem Rechner aus erreicht werden kann, da ICMP nicht durchgelassen wird. Deshalb empfiehlt es sich, den ICMP Subtype *icmp unreachable* vom Internet hin zum Internet-Server durchzulassen.

Prüffragen:

- Lässt der Paketfilter nur die benötigten Kommunikationskanäle offen?

# M 4.99 Schutz gegen nachträgliche Veränderungen von Informationen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Dateien, die an Dritte weitergegeben werden, können von diesen im Allgemeinen auch weiterbearbeitet werden. Dies ist nicht immer im Sinne des Erstellers. Daher wäre ein Schutz gegen nachträgliche Veränderungen, auszugsweise Weitergabe oder Verarbeitung wünschenswert.

Häufig steht man vor dem Problem, dass Informationen über das Internet oder andere Netze Dritten zwar zur Verfügung gestellt, aber nicht hundertfach ausgedruckt oder nahtlos in andere Werke integriert werden sollen.

Hierzu gibt es verschiedene Lösungen, die teilweise auch miteinander kombiniert werden können. Beispiele hierfür sind:

- Die Verwendung von digitalen Signaturen, um unbemerkte Änderungen an Dateien zu verhindern (siehe auch M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen* oder M 3.23 *Einführung in kryptographische Grundbegriffe*).
- Das Hinzufügen von Copyright-Vermerken zu Informationen, wie Broschüren oder Dateien auf Webseiten. Diese können wie folgt lauten: "Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen des Urheberrechtsgesetzes ohne Zustimmung des Autors ist unzulässig und strafbar." sowie "Copyright (©) 7/2009 by BSI".
- Die Verwendung von Dateiformaten, die nachträgliche Änderungen bzw. auszugsweise Weiterverarbeitung erschweren. Hierfür kann z. B. Postscript genutzt werden oder die Sicherheitseigenschaften von Anwendungsprogrammen, z. B. bei PDF-Dateien.

Viele Anwendungsprogramme bieten Sicherheitsmechanismen an, um den weiteren Umgang mit den erstellten Dateien einzuschränken. Im Folgenden werden einige solcher Sicherheitsmechanismen am Beispiel von PDF-Dateien vorgestellt. Da die Sicherheitsmechanismen der verschiedenen Anwendungsprogramme sehr unterschiedlich ausgeprägt sind und teilweise sogar von Version zu Version variieren, ist es wichtig, die Mitarbeiter darüber zu informieren, wie diese zu benutzen sind und welche Schritte vor der Weitergabe von elektronischen Dokumenten zu beachten sind. Es ist häufig sinnvoll, einen Mitarbeiter (plus Vertreter) gründlich hierzu auszubilden. Dieser sollte dann alle weiterzugebenden Dokumente entsprechend der Sicherheitsvorgaben bearbeiten oder als Ansprechpartner zur Verfügung stehen.

### Schutz von PDF-Dokumenten

PDF-Dokumente können bei der Erstellung mit Zugriffsbeschränkungen versehen werden. So kann z. B. das Öffnen, Drucken oder Kopieren von PDF-Dateien eingeschränkt werden.

- Häufig sollen in einem Dokument vor dessen Veröffentlichung einzelne Passagen unkenntlich gemacht werden. Eine beliebte, aber extrem fehlerträchtige Methode ist es, Textpassagen elektronisch zu "schwärzen".

Die so übermalten Informationen sind allerdings in vielen Fällen einfach auslesbar. Daher ist dies unbedingt zu unterlassen (siehe auch G 3.13 *Weitergabe falscher oder interner Informationen*).

- Durch die Verwendung von kryptographischen Verfahren können PDF-Dokumente signiert oder so verschlüsselt werden, dass nur bestimmte Anwender diese benutzen können.
- Es können PDF-Sicherheitsrichtlinien erstellt werden. Diese kann jeder Benutzer für sich erstellen oder es können von der Institution vorgegebene Sicherheitsrichtlinien verwendet werden, hierfür ist ein Adobe Policy Server erforderlich.
- Dateischutz
  Mit Adobe Acrobat, also der verbreitetsten Anwendung, mit der PDF-Dateien erstellt und nachbearbeitet werden können, ist die Vergabe von zwei Arten von Passwörtern möglich. Die einen werden zum Öffnen des Dokuments, die anderen zum Ändern der Sicherheitsattribute benötigt. Bei der Vergabe eines Passwortes wird zunächst danach gefragt, zu welchen Programmversionen die Schutzfunktion kompatibel sein soll. Bis zur Version "Adobe 5.0 und höher" ist dabei nur eine 40-Bit-Verschlüsselung mit RC4 möglich, ab "Adobe 5.0 und höher" ist eine 128-Bit-Verschlüsselung mit RC4 und ab "Adobe 7.0 und höher" ist eine 128-Bit-Verschlüsselung mit AES vorgesehen. Es sollte darauf geachtet werden, mindestens mit 128 Bit zu verschlüsseln, da der Dokumentenschutz sonst einfach ausgehebelt werden kann.
  Über die Sicherheitsattribute können unter anderem folgende Funktionen eingeschränkt werden:

  - Öffnen des Dokuments
  - Drucken
  - Ändern des Dokuments
  - Kopieren von Texten, Bildern oder anderen Inhalte
  - Zugriff auf Metadaten eines Dokuments
  - Notizen und Formularfelder hinzufügen oder ändern

  So können sehr einfach die Rechte beschränkt werden, so dass niemand mit Cut and Paste die Inhalte einer Veröffentlichung übernehmen kann. Wenn im Extremfall sogar das Ausdrucken verhindert wird, kann die Datei nur online gelesen werden.

Es sollte genau überlegt werden, welche Metadaten die Datei enthalten soll. Hier kann es beispielsweise erwünscht sein, einer Datei eine Vielzahl von Metadaten mitzugeben, damit dieses über Suchmaschinen gefunden werden kann. Es kann aber auch sinnvoll sein, keine Metadaten weiterzugeben, beispielsweise sollte der Name des Autors entfernt werden, wenn ein Dokument anonymisiert weitergegeben werden soll.

Leider bietet dies nur einen rudimentären Schutz, da PDF-Dateien (abhängig von der Programmversion, mit der sie erstellt wurden) auch mit Programmen geöffnet werden können, die diese Sicherheitsattribute ignorieren. Solange z. B. Drucken erlaubt wird, kann das Dokument sogar jederzeit wieder in eine PDF-Datei ohne jegliche Einschränkungen verwandelt werden.

Prüffragen:

- Werden ausreichende Sicherheitsmaßnahmen ergriffen, damit Dateien nicht unbemerkt verändert werden können?

# M 4.100 Sicherheitsgateways und aktive Inhalte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eines der größten Probleme bei der Konzeption eines Sicherheitsgateways ist die Behandlung der Probleme, die durch die Übertragung aktiver Inhalte zu den Rechnern im zu schützenden Netz entstehen. Derzeit existieren noch keine brauchbaren Programme, die eine ähnlich wirksame Erkennung von Schadfunktionen in ActiveX-Controls, Java-Applets oder Scripting-Programmen ermöglichen, wie sie im Bereich der Computer-Viren möglich ist.

Die Größe der Gefährdung, die von aktiven Inhalten für die Rechner im zu schützenden Netz ausgeht, lässt sich anhand des folgenden Beispiels darstellen: Ein Java-Applet bzw. der Browser darf gemäß der Java-Spezifikationen eine Netzverbindung zu dem Server aufbauen, von dem es geladen worden ist. Diese zur Zeit noch recht wenig benutzte Möglichkeit ist eine zentrale Voraussetzung, wenn Netz-Computer (NC) oder ähnliches eingesetzt werden sollen, die auch ohne spezielle Initiierung durch den Anwender Programme vom Server laden müssen. Um diese Eigenschaft trotz der Verwendung eines Paketfilters vollständig unterstützen zu können, müssen sehr viel mehr Ports freigeschaltet werden oder es muss ein dynamischer Paketfilter eingesetzt werden. Ist das der Fall, können Java-Applets verwendet werden, um kaum zu kontrollierende IP-Verbindungen aufbauen zu können.

Die Kontrolle aktiver Inhalte kann auf verschiedene Weise geschehen:

**1. Zentrale Filterung der aktiven Inhalte auf dem Sicherheitsgateway**

Sämtliche als schädlich eingestuften Inhalte werden von einer Komponente des Sicherheitsgateways (in der Regel vom ALG) gefiltert, so dass keine potenziell schädlichen Programme mehr auf den Client-Rechnern eintreffen.

Aktive Inhalte werden über spezielle Tags innerhalb einer HTML-Seite eingebunden. In der Regel werden aktive Inhalte anhand der entsprechenden Tags aus einer HTML-Seite erkannt und gelöscht, oder sie werden durch einen Textbaustein ersetzt, der dem Anwender einen Hinweis über die Tatsache der Filterung gibt. Das Problem besteht dabei darin, dass wegen der komplexen Möglichkeiten der aktuellen HTML-Spezifikation oft nicht alle zu löschenden Tags von den Sicherheitsproxies erkannt werden.

Weiterhin ist problematisch, dass beispielsweise Java-Applets nicht notwendigerweise als Datei mit der Endung .class verschickt werden müssen. Stattdessen können auch komprimierte Dateien eingesetzt werden, die z. B. die Endung .jar (Java-Archive) haben. Das bedeutet, dass ein Java-Filter auch alle von den verwendeten Browsern unterstützten Dateiendungen für Java-Dateien kennen muss. Zusätzliches Schadenspotential resultiert auch aus der Möglichkeit, JavaScript aus Java heraus auszuführen. Ähnliche Probleme existieren im Zusammenhang mit Flash-Objekten, .NET Assemblies und anderen aktiven Inhalten.

Es sollte unbedingt beachtet werden, dass auch aktive Inhalte außerhalb von Webseiten gefiltert werden müssen, beispielsweise in HTML-E-Mails.

**2. Dezentrale Abwehr auf den angeschlossenen Clients**

Die Ausführung aktiver Inhalte sollte normalerweise durch entsprechende Einstellungen im Browser unterbunden werden. Die Umsetzung einer Whitelist-Strategie für aktive Inhalte wird von verschiedenen Browsern in unterschiedlicher Weise und mehr oder weniger gut unterstützt (Beispiele: Zonenmodell des Microsoft Internet Explorers, Browser-Profile bei Mozilla). Idealerweise sollte ein Browser die Möglichkeit bieten, die Ausführung bestimmter Typen aktiver Inhalte getrennt für einzelne Server oder Domains freigeben oder verbieten zu können.

Dabei ist allerdings zu beachten, dass es auf Grund von Schwachstellen in den Browsern Angreifern möglich sein kann, entsprechende Einschränkungen zu umgehen.

Java-Applets, Acitve-X Objekte und mit Einschränkungen auch Javascript können mit einer digitalen Signatur versehen werden. Die Signatur dient dazu, die Integrität und Authentizität des jeweiligen aktiven Inhalts zu schützen. Werden ausschließlich signierte aktive Inhalte zugelassen, so bietet dies eine erhöhte Sicherheit vor Schadfunktionen. Diese Sicherheit ist jedoch nur indirekt, da der Nutzer auf die Vertrauenswürdigkeit der Signaturstelle, die in Zusammenarbeit mit dem Anbieter der aktiven Inhalte die Signatur erstellt, angewiesen ist.

Selbst die vollständige Deaktivierung der Ausführung aktiver Inhalte bietet aber nur einen begrenzten Schutz vor bösartigen aktiven Inhalten. Aufgrund der Vielzahl von Software-Schwachstellen in den Browsern können die Sicherheitseinstellungen umgangen werden, so dass der intendierte Schutz tatsächlich nicht oder nicht in vollem Umfang existiert.

**3. Installation von Anti-Viren-Software und Personal Firewalls auf den Clients**

Anti-Viren-Produkte können vor Viren, Makroviren und Trojanischen Pferden schützen, die durch aktive Inhalte automatisch heruntergeladen wurden. Sie bieten einen guten Schutz vor bereits bekannten Schadprogrammen. Mehr zu Anti-Viren-Produkten findet sich in Baustein B 1.6 *Schutz vor Schadprogrammen*.

Personal Firewalls sind Programme, die auf dem Client-Rechner installiert werden und dort meist mehrere Funktionen wahrnehmen. Sie bieten meist neben der Funktion eines lokalen Paketfilters weitere Funktionen an. Beispielsweise bieten einige Personal Firewalls die Möglichkeit einer Überwachung anderer Programme, die versuchen eine Netz-Verbindung aufzubauen. Solche Verbindungsaufnahmen können dann meist entweder automatisch anhand festgelegter Regeln oder im Einzelfall vom Benutzer selbst erlaubt oder verboten werden. In einigen Fällen bieten sie auch sogenannte "Sandboxen", die die Ausführung aktiver Inhalte kontrollieren und auf unbedenkliche Operationen beschränken können.

Personal Firewalls bieten zusammen mit Anti-Viren-Programmen einen recht guten Schutz vor bösartigen aktiven Inhalten.

Allerdings muss berücksichtigt werden, dass die richtige Konfiguration dieser Programme zusätzlichen Administrationsaufwand erfordert, und dass Personal Firewalls selbst Sicherheitslücken aufweisen können, die das System gefährden.

Bei allen drei Optionen ist eine Sensibilisierung der Benutzer zusätzlich notwendig. Zudem muss sichergestellt werden, dass die Einstellungen auf den Clients bei allen unter Punkt 2 und 3 genannten Schutzvorkehrungen nicht versehentlich oder absichtlich vom Benutzer deaktiviert oder umgangen werden können.

| Vorteile der zentralen Filterung | Vorteile der dezentralen Filterung |
|---|---|
| - Einfache Installation und Administration, da die Filtersoftware nur einmal installiert werden muss.<br>- Einfache Protokollierung und Auswertung, da im Gegensatz zur dezentralen Filterung keine Protokolldaten von mehreren Rechnern zusammengeführt werden müssen.<br>- Im Gegensatz zur dezentralen Filterung ist keine triviale Manipulation der Filtersoftware durch den Benutzer möglich.<br>- Filterprogramme für aktive Inhalte auf dem ALG sind dedizierte Sicherheitsprodukte. Der Schutz vor aktiven Inhalten auf den Clients (z. B. im Browser) ist hingegen oft fehlerhaft implementiert.<br>- Die Verwendung der Filtersoftware ist unabhängig von der Software auf den Clients möglich. Es entstehen keine Kompatibilitätsprobleme mit der auf den Clients eingesetzten Software | - Im Vergleich zur zentralen Filterung höhere Ausfallsicherheit, da die Filterung dezentral erfolgt.<br>- Schutz vor verschlüsselten aktiven Inhalten. Bei Filterung auf dem Endgerät können aktiven Inhalte erkannt werden, da sie auf dem Endgerät entschlüsselt werden.<br>- Die Ausführung von aktiven Inhalten kann unabhängig vom Sicherheitsgateway abgeschaltet werden.<br>- Es entstehen keine Kompatibili-tätsprobleme, die sich durch den Einsatz einer zentralen Filter-software auf dem ALG ergeben könnten. |

Tabelle: Vorteile der zentralen beziehungsweise dezentralen Filterung

**Empfehlung**

Die Entscheidung, wie mit aktiven Inhalten in Webseiten umgegangen wird, hängt in erster Linie vom Schutzbedarf der betreffenden Clients ab. Die folgende Tabelle kann bei der Festlegung der individuellen Strategie als Grundlage dienen:

| Schutzbedarf der Clients | Empfehlung |
|---|---|
| Normal | Allgemein: Deaktivierung aktiver Inhalte im Browser und Freischaltung nur für vertrauenswürdige Websites.<br>Virenscanner auf dem Client (siehe auch Baustein B 1.6 *Schutz vor Schadprogrammen*).<br>Eine Filterung aktiver Inhalte auf dem Sicherheitsgateway mit Freischaltung für vertrauenswürdige Websites (Whitelist) ist empfehlenswert. |
| Hoch | Deaktivierung aktiver Inhalte im Browser und Freischaltung nur für vertrauenswürdige Websites. |

| Schutzbedarf der Clients | Empfehlung |
|---|---|
| | Virenscanner auf dem Client (siehe auch Baustein B 1.6 *Schutz vor Schadprogrammen*).<br>Filterung aktiver Inhalte auf dem Sicherheitsgateway mit Freischaltung für vertrauenswürdige Websites (Whitelist). Zusätzlich Filterung von Cookies (Whitelist).<br>Die Kriterien, für welche Websites aktive Inhalte freigeschaltet werden, sollten deutlich restriktiver sein als bei normalem Schutzbedarf.<br>Eine ergänzende Sicherheitsanalyse wird empfohlen, um sicher zu stellen, dass ein angemessenes Sicherheitsniveau erreicht wurde |
| Bei zusätzlichen oder speziellen Anforderungen | Einsatz einer Personal Firewall auf dem Client. |

Tabelle: Empfehlungen für den Umgang mit aktiven Inhalten in Webseiten

Die Entscheidung für eine bestimmte Vorgehensweise und die Gründe, die dafür ausschlaggebend waren, sollten nachvollziehbar dokumentiert werden.

Eine zu "liberale" Einstellung oder gar eine generelle Freigabe aktiver Inhalte ist auch bei normalem Schutzbedarf nicht zu empfehlen. Die möglichen Schäden, die durch bösartige aktive Inhalte in Verbindung mit Schwachstellen in Webbrowsern oder im unterliegenden Betriebssystem entstehen können, sind dafür zu gravierend. Falls für bestimmte, Anwendungen aktive Inhalte zwingend nötig sind, sollten sie nur für die betreffenden Server freigegeben werden.

Bei Neuentwicklungen browserbasierter Anwendungen oder bei einer Weiterentwicklung einer bestehenden Anwendung, die aktive Inhalte im Browser benötigt, sollte kritisch hinterfragt werden, ob die Verwendung der aktiven Inhalte wirklich notwendig ist. Oft lassen sich aktive Inhalte bei gleichwertiger Funktionalität durch serverseitig dynamisch erzeugte Webseiten ersetzen.

Prüffragen:

- Findet eine Filterung aktiver Inhalte statt?
- Sind Anforderungen definiert, welche aktiven Inhalte als schädlich einzustufen sind?
- Entspricht die Umsetzung zur Filterung aktiver Inhalte der als schädlich eingestuften Inhalte den Sicherheitszielen der Organisation?
- Ist auf den Clients zum Schutz gegen Schadprogramme ein Anti-Viren-Produkt installiert?
- Ist auf den Clients zum Schutz gegen aktive Inhalte eine Personal Firewall eingerichtet?
- Sind die Benutzer für den Umgang mit aktiven Inhalten sensibilisiert?

# M 4.101 Sicherheitsgateways und Verschlüsselung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Da im Internet die Daten über nicht vorhersagbare Wege und Knotenpunkte verschickt werden, sollten die versandten Daten möglichst nur verschlüsselt übertragen werden. Eine Verschlüsselung des Datenverkehrs über das Internet kann auf zwei verschiedene Arten realisiert werden:

- Verschlüsselung auf dem Sicherheitsgateway bzw. auf Netzkoppel-elementen, die zum Aufbau sicherer Teilnetze eingesetzt werden kann
- Verschlüsselung auf den Endgeräten, die z. B. von Benutzern bedarfsabhängig eingesetzt wird

Beide Verfahren haben spezifische Vor- und Nachteile, die je nach Anwendungszusammenhang für die eine oder die andere Variante sprechen.

### Verschlüsselung durch das Sicherheitsgateway

Um mit externen Kommunikationspartnern Daten über ein offenes Netz auszutauschen und / oder diesen Zugriff auf das eigene Netz zu geben, kann der Aufbau von virtuellen privaten Netzen (VPNs) sinnvoll sein. Dafür sollten alle Verbindungen von und zu diesen Partnern verschlüsselt werden, damit Unbefugte keinen Zugriff darauf nehmen können. Zum Aufbau von verschlüsselten Verbindungen können eine Vielzahl von Hard- und Softwarelösungen eingesetzt werden. Sollen hierbei nur wenige Liegenschaften miteinander verbunden werden, sind insbesondere Hardware-Lösungen basierend auf symmetrischen kryptographischen Verfahren eine einfache und sichere Lösung.

Möglichkeiten zur Einbindung von VPN-Komponenten in Sicherheits-gateways finden sich in M 4.224 *Integration von VPN-Komponenten in ein Sicherheitsgateway*.

Die Ver- und Entschlüsselung kann gegebenenfalls auf verschiedenen Geräten erfolgen. So könnte eine Hardware-Lösung im Paketfilter als Schlüsselgerät arbeiten. Dies ist insbesondere dann sinnvoll, wenn keine unverschlüsselte Kommunikation über dieses Gerät gehen soll.

Die Integration der Verschlüsselung auf dem ALG hat den Vorteil einer leichteren (zentralen) Benutzerverwaltung. Zudem kann ein Angreifer, der einen externen Informationsserver unter seine Kontrolle gebracht hat, die verschlüsselte Kommunikation nicht belauschen.

### Verschlüsselung auf den Endgeräten

Zum Schutz der Vertraulichkeit bestimmter Daten, insbesondere bei der Versendung von E-Mails, bietet sich auch der Gebrauch von Mechanismen an, die eine Ende-zu-Ende-Verschlüsselung ermöglichen.

Hierfür wird beim Dienst E-Mail zum Beispiel das frei verfügbare Programmpaket PGP (Pretty Good Privacy) sehr häufig eingesetzt (siehe M 5.63 *Einsatz von GnuPG oder PGP*), für den Zugriff auf andere Rechner das Secure-Shell Protokoll (SSH). Für eine vertrauenswürdige Datenübertragung mit ausgewählten Partnern im Internet sollten nur Übertragungsprogramme und -protokolle verwendet werden, die eine Verschlüsselung der übertragenen Daten unterstützen. Unsichere Klartextprotokolle wie Telnet und FTP sollten ohne

zusätzliche Maßnahmen (etwa Tunneln über eine verschlüsselte Verbindung oder ein echtes VPN) nicht mehr in öffentlichen Netzen eingesetzt werden.

Die Ende-zu-Ende-Verschlüsselung der Daten stellt andererseits aber auch ein großes Problem für den wirksamen Einsatz von Filtermechanismen eines Sicherheitsgateways dar. Wenn die Übertragung verschlüsselter Daten über das Sicherheitsgateway zugelassen wird (z. B. SSL), sind Filter auf der Anwendungsschicht nicht mehr in der Lage, die Nutzdaten beispielsweise auf Viren oder andere Schadprogramme zu kontrollieren. Auch die Protokollierungsmöglichkeiten werden durch eine Verschlüsselung stark eingeschränkt.

Eine Lösung dieses Problems kann darin bestehen, den Datenverkehr temporär vom Sicherheitsgateway entschlüsseln zu lassen. Beispielsweise existieren für SSL entsprechende Proxies, die die SSL-Verbindung am Sicherheitsgateway terminieren und den entschlüsselten Datenstrom für eine Filterung zugänglich machen. Gegebenenfalls können die Daten dann wieder für die Übertragung zum Endgerät verschlüsselt werden.

Eine generelle Empfehlung für oder gegen den Einsatz von Verschlüsselung über das Sicherheitsgateway kann nicht gegeben werden. Dies hängt von den Anforderungen im Einzelfall ab, daher sollte eine Bewertung im Anwendungszusammenhang erfolgen.

| **Auf dem Sicherheitsgateway:** | **Auf den Endgeräten:** |
|---|---|
| + Zentrale Datenprüfung<br>+ Zentrale Schlüsselverteilung<br>+ Detailliertes Accounting<br>- Zugriff vom Sicherheitsgateway auf internes Netz<br>- Keine Ende-zu-Ende-Sicherheit | + Ende-zu-Ende Sicherheit<br>+ Keine Protokollprobleme<br>+/- benutzerabhängig<br>- Keine Kontrollmöglichkeiten auf dem Sicherheitsgateway<br>- Oft werden Public-Key-Infrastrukturen benötigt |

Tabelle: Vor- und Nachteile der verschiedenen Realisierungsmöglichkeiten

Wird für bestimmte Dienste oder Protokolle festgelegt, dass eine Ende-zu-Ende-Verschlüsselung eingesetzt (bzw. zugelassen) werden soll, so kann es erforderlich werden, für die Endgeräte zusätzliche Maßnahmen zu ergreifen. Dies sollte im Rahmen einer ergänzenden Sicherheitsbetrachtung geprüft werden.

Prüffragen:

- Bestehen auf Basis der Sicherheitsvorgaben der Organisation Anforderungen an das Sicherheitsgateway, wann die Kommunikation mit externen Partnern verschlüsselt erfolgen muss?

# M 4.102 C2-Sicherheit unter Novell 4.11

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.103 DHCP-Server unter Novell Netware 4.x

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.104 LDAP Services for NDS

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.105 Erste Maßnahmen nach einer Unix-Standardinstallation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die meisten Unix-Systeme entsprechen nach einer Standardinstallation nicht den Anforderungen an einen sicheren Systembetrieb. Hier werden von den Herstellern häufig zu viele sicherheitskritische Dienste und Konfigurationen aktiviert bzw. mit zu weitreichenden Rechten versehen.

Die folgende Übersicht soll exemplarisch zeigen, wie eine Standardinstallation abgesichert werden kann:

- Vor der Installation sind die Administratoren entsprechend zu schulen, insbesondere hinsichtlich der Sicherheitsaspekte. In diesem Rahmen sollten sie sich über alle potentiellen Sicherheitslücken des eingesetzten Betriebssystems und der darauf installierten Applikationen kundig machen (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Dazu kann es auch sinnvoll sein, entsprechende Mailinglisten zu abonnieren.
- Nach der Installation sollte die Administrator-Kennungen mit guten Passwörtern geschützt werden (siehe M 2.11 *Regelung des Passwortgebrauchs*) oder eine Zwei-Faktor-Authentisierung eingebunden werden.
- Es sollte überprüft werden, welche Dienste auf dem IT-System ausgeführt werden. Dies kann z. B. mit dem Befehl *netstat -a | grep LISTEN* überprüft werden. Nicht benötigte Dienste sollten deaktiviert oder entfernt werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*).
- Wenn das System nicht als Mailserver fungiert, sollte der Maildaemon als Netzdienst deaktiviert werden. Wenn Mail **lokal** auf dem System zugestellt werden soll, kann sendmail mit der Option *-q15* oder als Cron-Prozess gestartet werden:

  ```
  1 * * * * /usr/sbin/sendmail -q 2>&1 >/dev/null
  ```

  Die Mail-Queue wird in regelmäßigen Abständen geleert und die Mail lokal zugestellt.
- Die aktuellste *sendmail*-Version sollte installiert werden (siehe auch M 4.107 *Nutzung von Hersteller- und Entwickler-Ressourcen* und M 5.19 *Einsatz der Sicherheitsmechanismen von sendmail*). Alternativ kann auch auf Public-Domain-Mailprogramme wie z. B. qmail zurückgegriffen werden. Die laufende *sendmail*-Version kann mit dem Befehl *telnet localhost 25* herausgefunden werden.
- Nach der Standardinstallation sollten die verfügbaren Security-Patches des Herstellers installiert werden (siehe auch M 4.107 *Nutzung von Hersteller- und Entwickler-Ressourcen*). Danach ist unbedingt zu überprüfen, dass durch die Patch-Installation keine nichtbenötigten Dienste aktiviert wurden.
- Die Filesysteme sollten möglichst restriktiv im- bzw. exportiert werden. Es ist darauf zu achten, dass Filesysteme nicht für alle schreibbar exportiert werden.
- Wenn zum Einsatz von *NIS* keine Alternativen existieren, sollte *NIS+* eingesetzt werden, das über erweiterte Sicherheitsmechanismen verfügt.
- Wenn *tftp* verfügbar sein muss, dann sollte es mit der Option *-s* gestartet werden, damit nicht jede Datei vom System kopiert werden kann (siehe auch M 5.21 *Sicherer Einsatz von telnet, ftp, tftp und rexec* und M 5.72 *Deaktivieren nicht benötigter Netzdienste*).

- Die Protokollierungsfunktion des *inetd* sollte mit *-t* aktiviert werden, damit jeder Verbindungsaufbauversuch protokolliert wird (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*). Hilfreich ist die Installation der Public-Domain-Tools xinetd oder TCP-Wrapper. Mit diesen Tools können u. a. alle Verbindungsversuche frühzeitig protokolliert werden, noch bevor der angesprochene Daemon via *inetd* gestartet wird.
- Protokolldateien sollten täglich bzw. wöchentlich untersucht werden. Zur halb-automatischen Auswertung sollten Analyseprogramme wie *swatch*, *logdaemon* oder *logsurfer* installiert werden (siehe M 2.64 *Kontrolle der Protokolldateien*).
- Regelmäßig sollten Sicherheitschecks beispielweise mit Programmen zur Integritätsprüfung oder Audit-Werkzeugen durchgeführt werden.
- Neben allen anderen nicht benötigten Diensten sollten *rshd*, *rlogind*, *rexecd* unbedingt deaktiviert werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*). Zur Konvertierung von RPC-Programmnummern in Portadressen wird von den meisten Herstellern das Programm rpcbind mit ausgeliefert. Als Ergänzung bzw. als Ersatz sollte der Daemon *portmapper* eingesetzt werden, wenn er für die vorliegende Plattform verfügbar ist. Alle Clients, die diese Dienste benutzen, sollten für normale Anwender nicht ausführbar gemacht werden. Weitere Authentisierungsverfahren, die auf Hostnamen beruhen, sollten vollkommen abgelöst werden.
- *Telnet* sollte durch *ssh* ersetzt werden. *ssh* ermöglicht eine stark verschlüsselte und authentisierte interaktive Verbindung zwischen zwei Systemen. *ssh* ist als Ersatz für *telnet*, *rsh*, *rlogin* und *rcp* zu verstehen. X-Window kann dadurch auch abgesichert übertragen werden (siehe auch M 5.64 *Secure Shell*).
- *Xauth* ist *xhost* vorzuziehen - es sollte niemals "xhost +" verwendet werden (siehe auch M 4.9 *Einsatz der Sicherheitsmechanismen von X-Window*).
- Aus der Konfigurationsdatei */etc/inetd.conf* sollten alle nicht benötigten Einträge entfernt werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*, ).
- Die Konfigurationsdatei */etc/syslog.conf* ist für die Aktivierung der Protokollfunktionen zu modifizieren (siehe M 4.106 *Aktivieren der Systemprotokollierung*).
- Eine Liste aller world-writable Dateien und Verzeichnisse kann mit folgenden Befehlen erstellt werden:

  ```
  find / -type f -perm -22 -exec ls -l {} \;
  find / -type d -perm -22 -exec ls -ld {} \;
  ```

  Die Ergebnisse sollten regelmäßig mit dem Installationszustand verglichen werden.
- Vor der Inbetriebnahme sollte ein Programm zur Integritätsprüfung installiert werden. Vor Aufnahme des Wirkbetriebs sollte eine Checksummenübersicht von den kritischen Systembereichen des installierten Systems erstellt werden. Die erstellte Übersicht sollte auf einem nichtbeschreibbaren Datenträger gespeichert werden.
- */var* sollte eine große Partition sein, damit ein vorsätzliches Produzieren von Protokolldaten das Unix-System nicht zum Stillstand bringt.

Alle durchgeführten Veränderungen sollten sorgfältig dokumentiert werden und unter allen Systemadministratoren abgestimmt werden. Diese Dokumentation kann in Papierform erfolgen oder in einer Datei auf dem jeweiligen System geführt werden. Sie sollte aber jederzeit eingesehen und aktualisiert werden können (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Prüffragen:

- Werden zur Integritätssicherung des IT-Systems Checksummen von kritischen Systembereichen vor Aufnahme des Wirkbetriebs erstellt und gesichert?
- Werden Protokollierungsfunktionen in angemessenem Umfang aktiviert?
- Werden vorhandene Optionen und Systemeinstellungen zur Steigerung des Sicherheitsniveaus genutzt?
- Ist sichergestellt, dass Filesysteme nur restriktiv im- bzw. exportierbar sind (z. B. nicht für alle schreibbar exportierbar)?
- Wird nach Änderungen (z. B. Einspielen von Updates und Patches) überprüft, dass weiterhin nur benötigte Dienste aktiviert sind?
- Werden vor der Inbetriebnahme alle verfügbaren Security-Patches installiert?
- Werden die Dienste des IT-Systems auf das notwendige Maß reduziert?

# M 4.106 Aktivieren der Systemprotokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die systemeigene Unix-Protokollierung *syslog* dient dem Festhalten von Informationen, die vom Betriebssystem oder von Anwendungsprozessen generiert werden. Sicherheitsrelevante Ereignisse, wie versuchte Anmeldung bzw. Ausführung des Befehls *su* sollten unbedingt protokolliert werden und einer späteren Auswertung zur Verfügung stehen.

Der erforderliche Daemon *syslogd* wird in der Regel automatisch gestartet und über die Datei */etc/syslog.conf* konfiguriert. Durch geeignete Rechtevergabe muss sichergestellt werden, dass nur Systemadministratoren diese Datei ändern können und dass die Protokolldateien in */var/log* und */var/adm* nur von Systemadministratoren gelesen werden können. Alle Änderungen an */etc/syslog.conf* sind zu dokumentieren. Bei der Anpassung an das vorliegende IT-System sollte zunächst alles protokolliert werden, danach können bei Bedarf stufenweise einzelne Bereiche deaktiviert werden. Durch eine ausreichende Dimensionierung der */var*-Partition ist sicherzustellen, dass ausreichend Platz für die Protokolldateien zur Verfügung steht. Das folgende Beispiel für eine Konfigurationsdatei ist in Anlehnung an eine SunOS-Konfiguration erstellt worden und definiert eine ausführliche Protokollierung in verschiedenen Dateien.

```
#ident "@(#)syslog.conf 1.3 93/12/09 SMI" /* SunOS 5.0 */
#
# Alle Meldungen werden zu einem Loghost geschickt, der in der Datei
# /etc/hosts definiert werden muss.
#
# Es muss TAB als Separator verwendet werden!
#
# Test: . syslogd mit der Option "-d" starten
# . syslogd mit kill -HUP nach jeder Änderung dieser Datei starten
# . die Logdatei muss vor dem Start/Neustart bereits existieren
# . mit/usr/ucb/logger können Testmeldungen für jede facility
# und priority generiert werden
#
*.err;kern.warning;auth.err;daemon.err /dev/console
*.alert;kern.err;daemon.err operator
*.alert root
# zeigt emerg-Meldungen auf Terminals an (verwendet WALL)
*.emerg *
#
kern.info ifdef(`LOGHOST', /var/log/kernlog, @loghost)
user.info ifdef(`LOGHOST', /var/log/userlog, @loghost)
mail.info ifdef(`LOGHOST', /var/log/maillog, @loghost)
daemon.info ifdef(`LOGHOST', /var/log/daemonlog, @loghost)
auth.info ifdef(`LOGHOST', /var/log/authlog, @loghost)
lpr.info ifdef(`LOGHOST', /var/log/lprlog, @loghost)
news,uucp.info ifdef(`LOGHOST', /var/log/newslog, @loghost)
cron.info ifdef(`LOGHOST', /var/log/cronlog, @loghost)
#
## alle anderen "local" Nachrichten, für eigene Programme
local0,local1.info ifdef(`LOGHOST', /var/log/locallog, @loghost)
local2,local3,local4.info ifdef(`LOGHOST', /var/log/locallog, @loghost)
```

```
local5,local6,local7.info ifdef(`LOGHOST', /var/log/locallog, @loghost)
#
# alle Alarme und höher werden in eine separate Datei geschrieben:
*.err ifdef(`LOGHOST', /var/log/alertlog, @loghost)
#
# Beispiel Log levels:
# ------------------------------------
# 'su root' failed for .. auth.err
# ROOT LOGIN REFUSED ON ... auth.err
# 'su root' succeeded for.. auth.notice
```

Prüffragen:

- Werden unter Unix sicherheitsrelevante Ereignisse, wie versuchte Anmeldung bzw. Ausführung des Befehls su, protokolliert?
- Ist sichergestellt, dass die Konfigurationsdatei zur Protokollierung (/etc/syslog.conf) nur vom Systemadministrator geändert werden kann?
- Ist sichergestellt, dass die Protokolldateien (in /var/log bzw. /var/adm) nur für den Systemadministrator lesbar sind?
- Werden alle Änderungen in der Konfigurationsdatei zur Protokollierung (/etc/syslog.conf) nachvollziehbar dokumentiert?
- Ist sichergestellt, dass die Partition für die Protokolldaten ausreichend dimensioniert ist?

# M 4.107 Nutzung von Hersteller- und Entwickler-Ressourcen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die meisten Hersteller von IT-Systemen oder IT-Komponenten bieten diverse Unterstützungs- und Informationsangebote für die Anwender ihrer Produkte. Dazu gehören beispielsweise Hilfestellungen zur Problembehebung (Support, Hotline, Updates, Patches, etc.) und Informationsmöglichkeiten über Sicherheitlösungen (Web-Seiten, Newsgroups, Mailinglisten, etc.). Einige dieser Angebote sind kostenfrei, andere nicht.

Dienstleister

Die Angebote gehen typischerweise von den jeweiligen Herstellern aus, vor allem bei Standardsoftware. Es gibt jedoch auch zahlreiche Angebote von Dienstleistern. Dies gilt insbesondere für Open Source Software, für die die Entwickler oftmals keinen kommerziellen und vertraglich garantierten Support anbieten. Viele Entwickler von Open Source Software benennen jedoch qualifizierte externe Dienstleister in ihren Informationsangeboten. Oftmals sind Mitarbeiter der Dienstleister auch an der Entwicklung der Open Source Software beteiligt. Dadurch sind die Dienstleister in der Lage, Unterstützungsleistungen in einer Qualität anzubieten, die der einer klassischen Herstellerunterstützung entspricht. Auch Hersteller von proprietärer Software arbeiten oft eng mit Dienstleistern zusammen und weisen diese Dienstleister als Partner aus oder zertifizieren deren Dienstleistungen.

Bereits bei der Beschaffung von IT-Systemen oder -Produkten sollte überlegt werden, welche Unterstützungsangebote zusätzlich in Anspruch genommen werden sollen, insbesondere wenn dies laufende Kosten verursacht. Weiter ist zu überlegen, ob der Hersteller selbst oder ein Dienstleister beauftragt wird. Bei der Auswahl eines Dienstleisters ist zu beachten, dass ein größerer Dienstleister mehrere Anwendungen betreuen kann. Allerdings sind größere Dienstleister oft nicht spezialisiert genug, um für jedes Produkt qualitativ gleichwertige Unterstützungsleistungen bieten zu können.

Es sollte sichergestellt sein, dass für **alle** eingesetzten IT-Systeme und -Produkte regelmäßig überprüft wird, ob neue Informationen über Sicherheitsprobleme und Lösungsmöglichkeiten seitens der Hersteller oder anderer Quellen vorhanden sind. Dies ist besonders bei allen Server-Betriebssystemen wichtig, da eine Sicherheitslücke auf einem Server wesentlich mehr Schäden verursachen kann als auf einem Client.

Sicherheitsspezifische Updates

Sicherheitsspezifische Updates sollten nur von vertrauenswürdigen Stellen bezogen werden, zum Beispiel vom Hersteller, von den Entwicklern, von vertrauenswürdigen Dienstleistern oder CERTs (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Die Updates sind mittels kryptographischer Methoden zu überprüfen, soweit die Dateien entsprechend verschlüsselt bzw. signiert angeboten werden.

Damit jederzeit auf sicherheitsrelevante Hinweise zugegriffen werden kann, sollte für alle eingesetzten Betriebssysteme und alle wichtigen IT-Produkte eine Übersicht geführt werden. Aus dieser sollte hervorgehen, unter welchen WWW-Adressen sicherheitsspezifische Updates und Patches bzw. Informa-

tionen gefunden werden können. Diese Adressen sind meist in der Produktdokumentation zu finden. Sehr oft wird auf der Web-Seite von Herstellern oder Anbietern direkt auf diese Informationen verwiesen. Erfahrungsgemäß verändern sich Links häufig, sodass es wichtig ist, diese regelmäßig auf ihre Korrektheit zu überprüfen und, wenn es erforderlich ist, zu aktualisieren.

Prüffragen:

- Wurde geprüft, welche Unterstützungsleistungen für ein Produkt angeboten werden und ob es sinnvoll ist, diese in Anspruch zu nehmen?
- Wird für alle eingesetzten IT-Systeme und Produkte regelmäßig überprüft, ob neue Informationen über Sicherheitsprobleme und Lösungsmöglichkeiten seitens der Hersteller oder anderer Quellen vorliegen?
- Sind Maßnahmen zum Schutz der Integrität von Patches und Updates getroffen worden?
- Existiert eine aktuelle Übersicht über die eingesetzten IT-Produkte und der jeweiligen Support-Möglichkeiten?

# M 4.108 Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.109 Software-Reinstallation bei Arbeitsplatzrechnern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei Arbeitsplatzrechnern kann es häufiger zu Problemen mit dem Betriebssystem oder den Anwendungen kommen, die nur durch den Benutzersupport wieder behoben werden können. Dies kann z. B. durch Softwarefehler, Konfigurationsänderungen, Aufspielen neuer Software oder Computer-Viren verursacht werden.

Damit die Administratoren bei den oben beschriebenen Problemen auf den Benutzerrechnern nicht zeitaufwendig nach Fehlern suchen müssen, sollte eine Software-Reinstallation der Standardkonfiguration vorgenommen werden.

Dafür muss zunächst der Rechner eindeutig identifiziert werden und dann über eine entsprechende Dokumentation oder ein Programm anhand dieser Identifikation genau ermittelt werden, welche Software in welcher Konfiguration auf genau diesem Rechner installiert werden muss. Dabei ist es hilfreich, wenn sich die Systeme weitestgehend gleichen, zumindest in Bereichen mit ähnlicher Aufgabenstellung.

Es empfiehlt sich, die Festplatte des Arbeitsplatzrechners neu zu formatieren und anschließend die erforderliche Software und Daten neu aufzuspielen.

Eine Software-Reinstallation kann auf verschiedene Weise durchgeführt werden, so gibt es z. B. spezielle Programme, die eine vorgegebene Konfiguration von einem Server auf den neu zu installierenden Arbeitsplatzrechnern überspielen. Hierbei ist zu beachten, dass solche Arbeiten meist in zweierlei Hinsicht zeitkritisch sind: Die Neueinrichtung sollte möglichst schnell erfolgen können, damit das IT-System wieder verfügbar ist, und das Netz sollte möglichst wenig belastet werden. Dies ist insbesondere bei Schulungsrechnern oder PC-Pools wichtig.

Natürlich kann eine Reinstallation auch "von Hand" vorgenommen werden. Zu diesem Zweck sollte als erstes eine Standardinstallation vorgenommen werden. Im Anschluss daran werden die Besonderheiten der einzelnen Rechner kopiert, wie spezielle Gerätetreiber, andere Konfigurationsdateien oder spezielle Software. Dafür müssen diese allerdings vorkonfiguriert verfügbar sein, z. B. auf dem Netz oder auf mobilen Datenträgern. Ein aktuelles Viren-Suchprogramm muss anschließend zum Einsatz kommen.

Prüffragen:

- Ist ein Verfahren festgelegt, um Arbeitsplatzrechner bei Bedarf schnell neu installieren zu können?
- Ist bei Reinstallation von IT-Systemen das betroffene IT-System und die erforderliche Konfiguration eindeutig identifizierbar?
- Ist der Reinstallationsprozess so gestaltet, dass das betroffene IT-System möglichst schnell wieder verfügbar ist?
- Ist der Reinstallationsprozess so gestaltet, dass das Netz der Organisation möglichst wenig belastet wird?

# M 4.110 Sichere Installation des RAS-Systems

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.319 *Sichere Installation von VPN-Endgeräten* integriert.

# M 4.111 Sichere Konfiguration des RAS-Systems

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.320 *Sichere Konfiguration eines VPNs* integriert.

# M 4.112 Sicherer Betrieb des RAS-Systems

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.321 *Sicherer Betrieb eines VPNs* integriert.

# M 4.113 Nutzung eines Authentisierungsservers bei Remote-Access-VPNs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Für Remote-Access-VPNs (RAS-VPNs) mit vielen Benutzern muss darüber nachgedacht werden, wie die Benutzerverwaltung für entfernte Zugänge (englisch: Remote Access) effizient durchgeführt werden kann. In der Regel muss jeder RAS-Benutzer auch eine Systemidentität (Benutzerkonto des Betriebssystems) erhalten und bei der Nutzung eines solchen Benutzerkontos identifiziert und authentisiert werden. In einigen Betriebssystemen (z. B. aktuellen Windows-Versionen) ist direkt eine RAS-Funktionalität und eine gemeinsame Benutzerverwaltung integriert. Bei mittleren und großen Netze, die organisatorisch meist in mehrere Teilnetze aufgeteilt sind (Domänen, Verwaltungsbereiche), besteht in vielen Fällen das Problem, dass in jedem Verwaltungsbereich eine getrennte Verwaltung der Benutzerdaten durchgeführt wird. Sollen sich Benutzer auch an fremden Teilnetzen anmelden können, müssen hier Querberechtigungen (Cross-Zertifikate, Vertrauensstellungen) oder ein zentraler Verzeichnisdienst eingerichtet und gepflegt werden. Eine weitere Alternative ist, dass die Benutzer zusätzlich ein Benutzerkonto in dem anderen Teilnetz erhalten, dies erschwert aber die Verwaltung der Benutzerdaten. Insbesondere im RAS-Kontext haben sich spezielle Authentisierungssysteme herausgebildet, die auch für den "normalen" Authentisierungsprozess bei der Systemanmeldung genutzt werden können. Typische Vertreter sind beispielsweise RADIUS, TACACS, TACACS+und andere LDAP-basierte Verzeichnisdienste.

Prinzipiell besitzen diese Systeme folgenden Aufbau:

- Die Authentisierungsdaten der Benutzer werden durch einen zentralen Server verwaltet.
- Das Programm zur Systemanmeldung wendet sich zur Überprüfung der vom Benutzer eingegebenen Authentisierungsdaten an den Authentisierungsserver.
- Zur Kommunikation zwischen Anmeldeprozess und Authentisierungsserver wird in der Regel ein abgesichertes Protokoll eingesetzt.

Der Anmeldeprozess muss dazu die Nutzung externer Authentisierungsserver unterstützen. Weiterhin muss die Netzadresse des zu benutzenden Authentisierungsservers in den Konfigurationsdaten des Anmeldeprozesses korrekt eingetragen sein. Will sich ein Benutzer nun am System anmelden, laufen grob vereinfacht folgende Schritte ab, gleichgültig, ob er dazu eine RAS-Verbindung benutzt oder sich direkt im LAN befindet:

- Findet ein Verbindungsaufbau mit dem System- oder RAS-Anmeldeprozess statt, kontaktiert dieser den Authentisierungsserver und informiert ihn über den eingegangenen Verbindungswunsch eines Benutzers. Der Authentisierungsserver sendet, sofern ein "Challenge-Response" Verfahren zum Einsatz kommt, eine so genannte "Challenge" an den Prozess zurück, der diese an den Benutzer weiterleitet.
- Der Benutzer authentisiert sich gegenüber dem VPN-Client, beispielsweise durch Passworteingabe oder ein Token.
- Der Anmeldeprozess leitet die Authentisierungsdaten (meist transparent für den Benutzer) an den Authentisierungsserver weiter.

- Der Authentisierungsserver verifiziert die Benutzerdaten und signalisiert dem Anmeldeprozess das Ergebnis der Überprüfung.
- Der Zugang zum (Access-)Netz wird nach erfolgreicher Überprüfung gewährt.

Durch die Verwendung von zentralen Authentisierungsservern kann erreicht werden, dass einerseits die Authentisierungsdaten konsistent verwaltet werden und andererseits bessere Authentisierungsmechanismen genutzt werden können, als sie von den Betriebssystemen standardmäßig unterstützt werden. Hier sind insbesondere Chipkarten- und Token-basierte Mechanismen zu nennen. Je nach System erzeugen diese z. B. Einmalpasswörter, die auf einem Display angezeigt werden und die der Benutzer als Passwort angeben muss.

Für mittlere und große Netze wird die Verwendung von Authentisierungsservern insbesondere im RAS-Bereich empfohlen, da diese eine wesentlich höhere Sicherheit bei der Benutzer-Authentisierung bieten. Berücksichtigt werden muss jedoch, dass auch diese Server administriert und gewartet werden müssen. Ein Authentisierungsserver muss so im Netz platziert werden, dass er einerseits performant erreicht werden kann, aber andererseits auch vor unberechtigten Zugriffen geschützt ist.

Prüffragen:

- Ist für den RAS-Zugang und für den Zugang zu Systemen und Anwendungen eine konsistente Benutzerverwaltung gewährleistet?
- Erfüllen die genutzten Authentisierungsverfahren des RAS-VPN die festgelegten Sicherheitsanforderungen?
- Falls eigenständige Authentisierungsserver zum Einsatz kommen: Werden diese Authentisierungsserver sicher betrieben und vor unberechtigten Zugriffen geschützt?

# M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Hierzu gehören:

**Zugriff auf die SIM-Karte**

Die SIM-Karte kann durch eine vier- bis achtstellige PIN gegen unberechtigten Zugriff geschützt werden. Mit dieser PIN identifiziert sich der Teilnehmer gegenüber der Karte. Gelangt ein Unbefugter in den Besitz einer SIM-Karte, kann er ohne Kenntnis der PIN diese Karte nicht aktivieren. Um eine missbräuchliche Benutzung der SIM-Karte zu verhindern, sollte daher unbedingt die PIN-Abfrage aktiviert werden, sodass die PIN nach dem Einschalten des Mobiltelefons eingegeben werden muss. Die PIN sollte nicht zusammen mit dem Mobiltelefon bzw. der SIM-Karte aufbewahrt werden.

Bei der Auslieferung ist meist die PIN-Abfrage deaktiviert und eine PIN voreingestellt. Bei der ersten Benutzung sollte unbedingt die PIN geändert und aktiviert werden. Hierbei sollte keine triviale oder leicht vorhersagbare PIN gewählt werden (1111, Geburtsdatum, etc.).

**Hinweis:** Auf der Tastatur der meisten Mobiltelefone sind unter den Ziffern Buchstaben unterlegt. Dies kann dazu benutzt werden, sich statt PINs Passwörter auszuwählen, die leichter zu merken sind, aber natürlich auch wieder nicht zu einfach sein sollten. Beispiel: "4AUGEN" entspricht der PIN "428436".

Nach dreimaliger falscher PIN-Eingabe wird die SIM-Karte in der Regel gesperrt. Um diese Sperre aufheben zu können, muss ein achtstelliger Entsperrcode eingegeben werden. Dieser wird häufig auch als PUK (Personal Unblocking Key) oder Super-PIN bezeichnet. Nach zehnmaliger Falscheingabe der PUK wird die Karte unbrauchbar. Dieser Entsperrcode wird normalerweise in einem PIN-Brief zusammen mit der SIM-Karte ausgeliefert. Er sollte äußerst sorgfältig und vor unbefugtem Zugriff geschützt aufbewahrt werden. Die PUK darf auf keinen Fall zusammen mit dem Mobiltelefon aufbewahrt werden.

Neben der PIN gibt es mit der PIN2 noch eine weitere Geheimzahl, mit der der Zugriff auf bestimmte Funktionen der SIM-Karte abgesichert werden kann. Sie wird häufig benutzt für Konfigurationsänderungen der SIM-Karte, die nicht vom Benutzer selbst durchgeführt werden können, z. B. Nutzungsrestriktionen. Dies kann aber beispielsweise auch ein Firmentelefonbuch sein, das nur nach der Eingabe der PIN2 geändert werden kann. Die PIN2 hat einen eigenen Entsperrcode (PUK2).

**Zugriff auf das Mobiltelefon**

Darüber hinaus gibt es im Allgemeinen noch einen Sicherheitscode für das Mobiltelefon (Geräte-PIN), um den Zugriff auf bestimmte Funktionen zu schützen. Auch dieser sollte schnellstmöglich auf einen individuell gewählten Wert gesetzt werden. Er sollte notiert und vor unbefugtem Zugriff geschützt aufbewahrt werden. Alternativ bieten moderne Mobiltelefone einen Zugriffsschutz per Passwort, Gesten, Fingerabdruck oder Gesichtserkennung. Das Mobilte-

lefon sollte so eingestellt werden, dass der Sicherheitscode nach einigen Minuten Untätigkeit erneut eingegeben werden muss. Es sollte eine PIN, ein Passwort oder, eine Geste nach der jeweiligen Sicherheitsrichtlinie der Institution gewählt werden. Alternativ kann ein Fingerabdruckscanner benutzt werden. Da eine Gesichtserkennung bereits mit einfachen Fotos vom Gesicht des Benutzers getäuscht werden kann, sollte dieses Verfahren nicht eingesetzt werden.

**Diebstahlschutz durch zusätzliche Applikationen**

Moderne Mobiltelefone bieten die Möglichkeit, durch zusätzliche Applikationen das Mobiltelefon bei Verlust oder Diebstahl zu orten, seine Daten zu löschen bzw. es komplett zu sperren. Es sollte eine passende Applikation ausgewählt und eingesetzt werden. Die betreffenden Mitarbeiter sollten im Umgang mit dieser Applikation geschult werden.

**Zugriff auf Mailbox**

Beim Netzbetreiber kann für jeden Teilnehmer eine Mailbox eingerichtet werden, die unter anderem als Anrufbeantworter dient. Da die Mailbox von überall und auch von beliebigen Endgeräten aus abgefragt werden kann, muss sie mit einer PIN vor unbefugtem Zugriff geschützt werden. Bei der Neueinrichtung vergibt der Netzbetreiber hierzu eine voreingestellte PIN. Diese sollte unbedingt sofort geändert werden.

**Weitere Kennwörter**

Neben den diversen oben aufgeführten Geheimnummern kann es für verschiedene Nutzungsarten noch weitere Kennwörter geben. Dies ist z. B. der Fall beim Zugriff auf Benutzerdaten beim Netzbetreiber. So muss bei Fragen an die Hotline wegen der Abrechnung unter Umständen ein Kennwort genannt werden. Auch kostenpflichtige Dienstleistungen wie z. B. der Abruf von Informationen oder die Durchführung bestimmter Konfigurationen seitens des Netzbetreibers bzw. Mobilfunkanbieters werden häufig durch zusätzliche Kennwörter geschützt. Diese sollten, wie alle anderen Passwörter auch, sorgfältig ausgewählt, sicher aufbewahrt und nicht an Dritte weitergegeben werden.

Generell sollte mit allen PINs und Passwörtern sorgfältig umgegangen werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs*).

**Hinweis:** Angreifer haben in jüngster Zeit wiederholt versucht, telefonisch die PIN oder PUK von Mobilfunknutzern zu erfragen, indem sie sich als Mitarbeiter eines Netzbetreibers ausgegeben und einen technischen Defekt vorgetäuscht haben. Über Geheimnummern sollte **nie** telefonisch Auskunft gegeben werden!

Es gibt viele verschiedene Sicherheitsmechanismen bei Mobiltelefonen. Welche hiervon vorhanden sind bzw. wie diese aktiviert werden können, ist abhängig vom eingesetzten Mobiltelefon, von der SIM-Karte und vom gewählten Netzbetreiber. Daher sollten die Bedienungsanleitung und die Sicherheitshinweise des Netzbetreibers sorgfältig daraufhin ausgewertet werden. Beim Einsatz von Firmentelefonen empfiehlt es sich, die wichtigsten Sicherheitsmechanismen sowohl vorzukonfigurieren als auch auf einem übersichtlichen Handzettel zu dokumentieren.

Einige Modelle bieten auch die Möglichkeiten von Kennwort geschützten SIM-Locks. Dadurch kann z. B. zusätzlich verhindert werden, dass das Gerät nach einem Diebstahl mit einer anderen SIM-Karte problemlos weiter betrieben wer-

den kann. Weiterhin kann mit einem SIM-Lock verhindert, dass in ein unbeaufsichtigtes Gerät eine SIM mit Schadpotential eingelegt wird.

Prüffragen:

- Wurden die notwendigen Sicherheitsmechanismen für die Nutzung von Mobiltelefonen ausgewählt und auf den Geräten vorkonfiguriert?
- Welche Sicherheitsmechanismen sind für die Nutzung von Mobiltelefonen vorgeschrieben?
- Sind die Benutzer über die notwendigen Sicherheitsmechanismen für die Nutzung von Mobiltelefonen informiert?

# M 4.115 Sicherstellung der Energieversorgung von Mobiltelefonen

**Verantwortlich für Initiierung:** Administrator, Benutzer
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Akkus von Mobiltelefonen können das Gerät je nach Kapazität und Bauweise des Telefons für einen beschränkten Zeitraum, üblicherweise einige Stunden, mit Energie versorgen. Damit ein Mobiltelefon im Bedarfsfall jederzeit verfügbar ist bzw. keine Daten in flüchtigen Speichern verloren gehen, sollten einige Randbedingungen beachtet werden:

- Die Warnanzeigen des Mobiltelefons, die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden.
- Falls ein längerfristiger mobiler Einsatz absehbar ist, sollte ein Ladegerät mitgeführt werden. Ist kein Ladegerät verfügbar, kann das Mobiltelefon gegebenenfalls über das Datenkabel an einer USB-Schnittstelle eines PCs oder Laptops aufgeladen werden. Dies dauert in der Regel deutlich länger als mit einem Ladegerät. Es sollte auch bedacht werden, dass durch diese Form des Aufladens auch eine Datenverbindung möglich ist und Daten abfließen oder verändert werden können.
- Beim Laden sollten die Hinweise im Handbuch zum Mobiltelefon beachtet werden, insbesondere sollte die Lebensdauer des Akkus nicht beeinträchtigt werden.
- Bei der Übergabe eines Mobiltelefons ist der ausreichende Ladezustand der Akkus sicherzustellen. Der Ladezustand der Akkus sollte regelmäßig überprüft werden, da sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird.

Wenn eine längere Nutzung des Mobiltelefons absehbar ist, z. B. bei Dienstreisen, kann auch gegebenenfalls ein geladener Ersatzakku mitgeführt werden. Der Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des Akkus mit leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs wie Schlüssel oder Ketten verursacht werden. Wenn die Akkus nicht getauscht werden können, z. B. weil dieser fest verbaut ist, könnte auch auf externe Akku-Packs zurückgegriffen werden.

Ein Mobiltelefon sollte ausgeschaltet werden, bevor der Akku gewechselt wird, damit der Speicher nicht beschädigt wird.

Ein Mobiltelefon sollte keinen extremen Temperaturen ausgesetzt werden. Insbesondere der Akku, aber auch das Display können anderenfalls ihre Funktionsfähigkeit einbüßen. Da die Temperatur in Autos über Nacht oder beim Parken in der Sonne stark schwanken kann, sollten weder Mobiltelefone noch Akkus in geparkten Autos zurückgelassen werden.

Um den Akku des Mobiltelefons zu schonen, sollten Bluetooth, IrDA, WLAN, GPS, und Mobilfunk-Internetverbindung nur bei Bedarf aktiviert werden.

Prüffragen:

- Wurden ausreichende Sicherheitsmaßnahmen für die Sicherstellung der Energieversorgung von Mobiltelefonen getroffen?

# M 4.116 Sichere Installation von Lotus Notes/Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Voraussetzung für die sichere Installation von Lotus Notes/Domino ist die Planung der Rahmenbedingungen des Einsatzes, beschrieben in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino*. Anschließend erfolgt die Installation der Lotus Notes/Domino-Komponenten auf den relevanten Servern und Clients. Dazu müssen sichere Installationsverfahren sowie eine schutzbedarfsorientierte Absicherung der Installationsumgebung und der Installationsmedien festgelegt und eingehalten werden.

Es ist sinnvoll, zwischen Installationsverfahren bei Neuinstallation der gesamten Lotus Notes/Domino-Plattform und Installationsverfahren bei Anpassungen (Software-Upgrades, Patches) und Migrationen zu unterscheiden.

**Neuinstallation**

Bei einer Neuinstallation von Lotus Notes/Domino ist aus Sicherheitssicht Folgendes zu beachten:

- Die bei einer Neuinstallation einzuhaltenden Installationsverfahren sind festzulegen und zu dokumentieren. Dabei sind allgemeine Regelungen bezüglich der Verfahren festzulegen sowie spezielle Regelungen zu der Installation von Servern, Serverdiensten und Clients. Zu den allgemeinen Regelungen gehören beispielsweise die Festlegung der Verantwortung für die Initiierung und Durchführung von Neuinstallationen, Freigabe- und Kontrollverfahren für das Installationsverfahren an sich und die dafür erforderlichen Konfigurationen (z. B. Vier-Augen-Prinzip) sowie die Regelungen zur Produktionsfreigabe.
- Sind bereits allgemeine Regelungen zu Installationsverfahren vorhanden, kann auf diese verwiesen werden. In diesem Fall sind jedoch die Spezifika der Lotus Notes/Domino-Plattform zu ergänzen.
- Das Installationsverfahren bei Neuinstallation muss sicherstellen, dass eine ausreichende Dokumentation des Installationsvorganges und eine ausreichend fein granulare Protokollierung kritischer Teilschritte erfolgen. Diese Dokumentation ist erforderlich für die Erkennung von Manipulationen an den installierten Komponenten, aber auch bei der Fehlersuche.
- Werden automatisierte Installationsverfahren genutzt, ist eine detaillierte Dokumentation der verwendeten Parameter, Skripte etc. zu erstellen. Es ist eine geeignete Prüfung und Freigabe sowohl der Installationspakete als auch der installierten Komponenten zu etablieren.
- Das Installationsverfahren muss sicherstellen, dass nach der Installation nur die dazu berechtigten Administratoren auf die installierten Verzeichnis- und Dateistrukturen über das Betriebssystem oder administrative Tools zugreifen können. Dazu sind die Rechtestrukturen entsprechend anzupassen.
- Es ist sicherzustellen, dass nur berechtigte Administratoren und Wartungstechniker physischen Zugang zu den Domino-Servern haben, auch bereits während der Installation.
- Auswahl einer passenden Grundinstallation: Da ein Domino-Server unterschiedlich eingesetzt werden kann, ist schon bei der Installation darauf zu achten, dass die für den gedachten Einsatzzweck am besten geeignete Grundinstallation gewählt wird. So kann z. B. zwischen der vordefinierten Installation *Domino Utility Server* (ohne Messaging Dienste, gedacht

als reiner Applikations-Server), *Domino Messaging Server* (ohne Anwendungsdienste, gedacht als reiner Messaging-Server) und *Domino Enterprise Server* (alle Dienste) ausgewählt werden. Über die Installations-Option *Customize Domino Server* ist eine fein granulare Anpassung der Grundinstallation möglich. Die Auswahl der passenden Grundinstallation und insbesondere die fein granulare Anpassung an den geplanten Einsatzzweck ist Vorbedingung für eine sichere Konfiguration und Härtung.

**Anpassungen (Upgrades) und Migrationen**

Als Anpassung (Upgrade) wird hierbei eine reine Softwareanpassung bezeichnet, also eine Änderung des im Einsatz befindlichen Releases der Lotus Notes/Domino-Software oder einzelner Komponenten der Software einschließlich der für die Lotus Notes/Domino-Plattform zugekauften oder eigenentwickelten Komponenten.

Unter einer Migration wird sowohl eine Softwareanpassung mit Änderungen der Nutzdatenbestände (beispielsweise bei Formatänderungen der Datenbestände, Änderungen der verwendeten Datenbanken, Datenbereinigungen und Konsolidierungen) wie auch der Wechsel von einer anderen Plattform für E-Mail und Zusammenarbeit hin zur Lotus Notes/Domino-Plattform verstanden.

Bei Anpassungen (Upgrades) und Migrationen von Lotus Notes/Domino ist aus Sicherheitssicht Folgendes zu beachten:

- Die bei Upgrades und Migrationen einzuhaltenden Installationsverfahren sind festzulegen und zu dokumentieren.
- Für Anpassungen (Upgrades) können Verfahren eingesetzt werden, die abgeänderte (vereinfachte) Varianten des Verfahrens zur Neuinstallation darstellen.
- Bei Migrationen muss ein zusätzlicher Schwerpunkt auf die Gewährleistung der definierten Verfügbarkeit, Vertraulichkeit und Integrität der Nutzdaten gesetzt werden.
- Größere Upgrades und Migrationen können für die Lotus Notes/Domino-Plattform in Phasen durchgeführt werden. So ist sowohl ein Teil-Update abgeschlossener Domänen möglich (z. B. für Konzerne oder Institutionen mit mehreren Standorten) wie auch eine schichtorientierte Vorgehensweise, bei der z. B. zuerst das Update der Clients und anschließend das Update der Serverkomponenten vorgenommen wird. Alle phasenorientierten Vorgehensweisen bergen das Risiko von Inkompatibilitäten zwischen Komponenten der alten und neuen Releasestände und sind daher sehr sorgfältig, unter Berücksichtigung der entsprechenden Empfehlungen des Herstellers, zu planen. Rückfallstrategien sind in jedem Fall vorzusehen.
- Es ist zu berücksichtigen, dass nach Upgrades und Migrationen die Rechte der installierten Verzeichnis- und Dateistrukturen anzupassen sind, um sicherzustellen, dass nur die dazu vorgesehenen Administratoren Zugriff auf die betriebssystemseitig installierten Elemente von Lotus Notes/Domino haben.
- Eine Bewertung der geänderten Eigenschaften der neuen Releases, insbesondere der Mechanismen im Umfeld der Replikation und der Push-Mechanismen für Policies in Richtung der Clients, ist erforderlich, um unerwünschte Seiteneffekte nach einer Migration, die erst den Benutzern auffallen, zu vermeiden.

**Absicherung der Installationsumgebung und Installationsmedien**

Generell sind Installationsumgebungen und Installationsmedien gegen Manipulation vor oder während des Installationsvorgangs abzusichern (siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Dies gilt insbesondere auch für die Installation von Lotus Notes/Domino-Komponenten.

Gängige Verfahren sind z. B. die Abkopplung der Server, auf denen Installationen durchgeführt werden, vom Netz und die durchgängige Verwendung integritätsgesicherter Originalmedien des Herstellers für die Installation. Da dies jedoch mit erhöhtem administrativem Aufwand verbunden ist und insbesondere in großen Institutionen oder bei Providern oft nicht der gängigen Praxis entspricht, können alternative Sicherheitsmaßnahmen genutzt werden. So ist für Software, die nicht auf Originalmedien, sondern per elektronischer Kanäle vom Hersteller bezogen wird (z. B. Download, automatische Softwareaktualisierung durch den Hersteller, E-Mail etc.), in jedem Fall ein Installationsverfahren zu etablieren, das eine angemessene Integritätsprüfung der Software beinhaltet. Die Qualität der verwendeten Mechanismen, wie z. B. die zur Integritätssicherung verwendeten Hashes, muss den Schutzbedarf der zu installierenden Komponente berücksichtigen.

Für Lotus Notes/Domino bietet der Hersteller die Möglichkeit des elektronischen Bezugs der Software über HTTP-Download oder über die Nutzung eines speziellen Dowload-Applets (*Download Director*). Letzteres bietet erhöhte Sicherheit und entspricht laut Herstellerangaben den Anforderungen der Common Criteria für Softwaredownloads. Da kein vom Hersteller angebotener transparenter Mechanismus zur Integritätsüberprüfung einzelner Komponenten vorhanden ist, sollten bei hohem oder sehr hohem Schutzbedarf von Lotus Notes/Domino Maßnahmen getroffen werden, um sicherzustellen, dass der Download nicht kompromittiert werden kann. Es ist sicherzustellen, dass während des Downloads kein weiterer Zugriff (auch kein administrativer) auf das Zielverzeichnis/Ziellaufwerk erfolgen kann und dass nach erfolgreichem Download eine Integritätssicherung mittels entsprechender Hashes erfolgt.

Werden in der Institution zentrale Ablagen für Installationsmedien genutzt (Installationslaufwerke, Installationsserver), ist für diese eine dem Schutzbedarf der Medien entsprechende Absicherung vorzusehen. Hierzu gehören unter anderem entsprechende Maßnahmen zum Zugriffsschutz, zur Integritätssicherung und zur Gewährleistung der Verfügbarkeit. Wenn technisch und aus Administrationsgesichtspunkten möglich, sind die Installationslaufwerke sowie Installationsserver nur zeitlich eingeschränkt für Installationsvorgänge freizugeben.

**Kritische Vorgänge bei Installation, Anpassungen und Migrationen**

Bei der Installation des Lotus Domino Servers sind die Vorgänge zur Erzeugung wesentlicher technischer Elemente der Domänen- und Zertifikatshierarchie kritisch, da eine Kompromittierung dieser Elemente zu einer Kompromittierung der gesamten Domino/Notes-Sicherheitsmechanismen führen kann. Folgendes ist aus Sicherheitssicht zu berücksichtigen:

- Die Notes-IDs, die in diesem Zusammenhang erzeugt werden (Certifier-ID, Server-IDs, Administrator-IDs), sind mit komplexen Zugangspasswörtern zu versehen.
- Diese Notes-IDs sollten nicht im Namens- und Adressbuch gespeichert werden, sondern in Dateien, die durch betriebssystemseitige Sicherheitsmechanismen (z. B. betriebssystemseitige Zugriffsbeschränkungen) und zusätzliche Sicherheitskomponenten (z. B. Host-based IDS) geschützt vorgehalten werden.
- Ist ein automatisches Starten des Domino-Servers vorgesehen, so darf die Server-ID keinen Passwortschutz haben und muss daher über betrie-

bssystemseitige Zugriffschutzmechanismen und entsprechende Überwachung vor unberechtigtem Zugriff geschützt werden.
- Das Vorgehen bei der Installation der Elemente der Zertifikatshierarchie hat gemäß dem Konzept zur Domänen- und Zertifikatshierarchie von Lotus Notes/Domino zu erfolgen (siehe M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*). Dieses kann bei entsprechendem Schutzbedarf von Lotus Notes/Domino z. B. auch ein Vier-Augen-Prinzip zur Nutzung der Certifier-ID vorsehen, sodass in diesem Fall die Certifier-ID durch ein entsprechendes Mehrfachpasswort zu schützen ist.
- Es ist zu berücksichtigen, dass die technischen Elemente der Zertifikatshierarchie nicht nur in Bezug auf Integrität und Vertraulichkeit, sondern auch in Bezug auf Verfügbarkeit direkte Auswirkungen auf die entsprechenden Schutzziele von Lotus Notes/Domino haben. So sind für alle wichtigen IDs (Certifier-ID, Server-ID, Administrator-ID) Sicherungskopien vorzusehen, die getrennt vom System zugriffsgeschützt aufzubewahren sind.

**Nutzung der erweiterten Zugriffskontrolle (xACL)**

Lotus Notes/Domino bietet seit der Version 6 die Möglichkeit, erweiterte ACLs (*extended ACLs* oder *xACLs*) für ein Domino Directory oder einen Extended Directory Catalog aufzusetzen. Die mit Hilfe der xACLs implementierten zusätzlichen Möglichkeiten des Zugriffsschutzes ermöglichen z. B. Delegation administrativer Tasks, eingeschränkt auf Organisationseinheiten und weitergehenden Schutz auf Feldebene für NRPC, HTTP, LDAP, POP3 und IMAP-Zugriffe. Dadurch kann z. B. das Auslesen von Passwort-Hashes per HTTP-Zugriff auf Personendokumente in der names.nsf verhindert werden. Die Technote 1244808 des Herstellers beschreibt die dazu nötigen Schritte.

Für alle Lotus Notes/Domino-Systeme mit hohem oder sehr hohem Schutzbedarf bezüglich Vertraulichkeit oder Integrität ist die Nutzung der xACLs zu planen und umzusetzen. Durch die Aktivierung der xACLs wird automatisch der Eintrag der Gruppe ANONYMOUS in den ACLs auf NO ACCESS gesetzt.

Werden keine xACLs genutzt, ist bei der Domino-Installation die Gruppe ANONYMOUS standardmäßig auf NO ACCESS zu setzen. Sollen für einzelne Datenbanken anonyme Zugriffe erlaubt werden, ist dies auf Datenbankebene explizit freizuschalten.

Prüffragen:

- Sind definierte und dokumentierte Installationsverfahren für Neuinstallationen, Anpassungen und Migrationen von client- und serverseitigen Komponenten (Lotus Notes und Lotus Domino) vorhanden?
- Wird während des Installationsvorgangs (auch während Anpassungen und Migrationen) gemäß den definierten Verfahren protokolliert und eine Sicherung bzw. Archivierung der Installationsdokumentation und Installationsprotokolle vorgenommen?
- Sind detaillierte Vorgaben für alle erwähnten kritischen Vorgänge bei der Installation, Anpassung und Migration vorhanden?
- Wird sichergestellt, dass während der Installation, Anpassung oder Migration nur die beteiligten Administratoren Zugriff auf die entsprechenden Verzeichnisse und Ressourcen haben?
- Sind Installationsumgebungen und Installationsmedien gegen Manipulation vor oder während des Installationsvorgangs abgesichert?

- Wurde bewertet, ob der Einsatz der erweiterten Zugriffskontrolle (xACL) gerechtfertigt ist, und wird diese bei entsprechendem Schutzbedarf genutzt?
- Wenn keine erweiterte Zugriffskontrolle genutzt wird, wurde dann bei der Domino-Installation die Gruppe ANONYMOUS auf NO ACCESS gesetzt?

# M 4.117 Sichere Konfiguration eines Lotus Notes Servers

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.118 Konfiguration als Lotus Notes Server

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.119 Einrichten von Zugangsbeschränkungen auf Lotus Notes Server

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.120 Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.121 Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.122 Konfiguration für den Browser-Zugriff auf Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.123 Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.124 Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.125 Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.126 Sichere Konfiguration eines Lotus Notes Clients

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.127 Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 4.128 Sicherer Betrieb der Lotus Notes/Domino-Umgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Der sichere Betrieb der Lotus Notes/Domino-Umgebung umfasst alle Regeltätigkeiten, die zur Aufrechterhaltung der Funktionsfähigkeit der Lotus Notes/Domino-Umgebung vonnöten sind. Dazu gehört die Administration von Lotus Notes/Domino, die Durchführung von Upgrades und Migrationen, die regelmäßige Datensicherung und bei Bedarf Datenarchivierung sowie die Tätigkeiten zur Überwachung des Betriebs und der Sicherheit der Plattform. Änderungen an den Diensten, die außerhalb von Upgrades und Migrationen stattfinden (z. B. die Aktivierung bislang nicht genutzter Dienste, Inbetriebnahme neuer Datenbanken und Ähnliches), sind vergleichbar mit dem Verfahren bei Upgrades und Migrationen durchzuführen. Dies beinhaltet die Einhaltung der Vorgaben zur Dokumentation (einschließlich der systemseitigen Protokollierung der vorgenommenen Änderungen und Archivierung der Protokolle) und Einhaltung der Vorgaben für kritische Administrationstätigkeiten (z. B. Vier-Augen-Prinzip oder Freigabeverfahren für Dienste oder Komponenten wie Datenbanken oder Schnittstellen).

**Betriebskonzept**

Der sichere Betrieb der Lotus Notes/Domino-Umgebung erfordert ein Betriebskonzept, das alle angesprochenen betriebsrelevanten Themenfelder ausreichend detailliert regelt. Das Betriebskonzept muss auf weitere betriebsrelevante Konzepte (siehe M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*) verweisen.

**Datensicherung**

Eine regelmäßige Datensicherung ist Teil eines sicheren Betriebs und ist in einem Datensicherungskonzept zu dokumentieren. Dieses ist nicht Teil der Notfallvorsorge, sondern Teil des regulären Betriebs der Plattform, ist aber mit der Notfallplanung abzustimmen. Wird diese Vorgehensweise zur Datensicherung auch im Rahmen der Archivierung genutzt, so muss das Datensicherungskonzept mit dem in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* beschriebenen Archivierungskonzept abgestimmt werden.

Da Lotus Notes/Domino seine Informationen (sowohl Nutzdaten als auch interne Verwaltungsdaten, Konfigurationen, Protokolle etc.) in proprietären Datenbanken hält, muss das Datensicherungskonzept neben der Sicherung von Konfigurationsdateien (wie notes.ini) auch die Sicherung dieser Datenbanken abdecken. Allgemeine Empfehlungen zur Sicherung von Datenbanken finden sich in der Maßnahme M 6.49 *Datensicherung einer Datenbank*.

Folgende Besonderheiten der Lotus Notes/Domino-Plattform sind zu berücksichtigen:

- Ab Domino Release 5 und dem ODS (*On-Disc Structure*) 41 unterstützt Lotus Notes/Domino die Transaktionsprotokollierung für Datenbanken. Dies ist nicht nur wegen der erweiterten Möglichkeiten der inkrementellen Datensicherung über die Sicherung und das Nachfahren von Transaktionsprotokollen von Bedeutung, sondern auch wegen der Reparatur beschädigter Datenbanken über ein Einspielen des Backups und der Transaktionsprotokolle.

- Die Transaktionsprotokollierung ist für alle Datenbanken mit hohem Schutzbedarf in Bezug auf Verfügbarkeit oder Integrität, insbesondere auch für die Systemdatenbanken von Lotus Notes/Domino, einzurichten. Dabei sind insbesondere die Parameter *Protokollierungsart*, *Automatisches Fixup von beschädigten Datenbanken* und *Leistung zur Laufzeit bzw. beim Neustart* für den Einsatzzweck angemessen zu konfigurieren.
- In den neueren Domino-Versionen ist es möglich, Lotus Notes/Domino-Datenbanken in einer DB2-Datenbank abzulegen und über die Lotus Notes/Domino-Plattform darauf zuzugreifen. Wird diese Möglichkeit genutzt, muss das Sicherungskonzept für Lotus/Notes Domino auch die Sicherung der genutzten DB2-Datenbanken beinhalten.
- Datensicherungen komplexer Betriebsumgebungen mit umfangreichen Abhängigkeiten, die z. B. durch die Verwendung von Replikation entstehen können, sollten möglichst nicht manuell, sondern unter Verwendung dafür geeigneter Sicherungstools durchgeführt werden. Tools des Herstellers der zu sichernden Plattform (im diesem Fall Tivoli Storage Manager und Tivoli Data Protection for Domino) sind oftmals auf die Eigenheiten der Plattform abgestimmt, daher sind die Inkompatibilitätsrisiken geringer als bei Tools von Fremdanbietern.

**Anwendungsentwicklung für die Lotus Notes/Domino-Plattform**

Wird Anwendungsentwicklung für die Lotus Notes/Domino-Plattform betrieben, gehören zum sicheren Betrieb der Plattform auch die Verfahren zur Überführung der Anwendungen in den Betrieb. Diese müssen nicht nur gewährleisten, dass eine formell richtige Übergabe stattfindet, sondern auch, dass die geforderten Schritte zur Absicherung der Anwendungsentwicklung umgesetzt wurden.

Der Betrieb einer Lotus Notes/Domino-Umgebung mit Eigenentwicklung ist anders abzusichern als der einer Standard-Umgebung, insbesondere auch unter Berücksichtigung der Thematik "Altlagen" und "Produktivnahme von Eigenentwicklungen".

Wie allgemein üblich hat auch für die Lotus Notes/Domino-Plattform eine angemessene Trennung zwischen Entwicklungsumgebungen, Umgebungen für Test und Qualitätssicherung und Produktivumgebungen zu erfolgen. Es ist vielfach möglich, als Entwicklungsumgebungen und Umgebungen für Test und Qualitätssicherung Lotus Notes/Domino-Umgebungen unter Verwendung von Virtualisierung zu nutzen, auch unter dem Aspekt niedrigerer Lizenzkosten (siehe dazu M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*). Abhängig vom Schutzbedarf kann auch über Virtualisierung eine ausreichende Trennung der Umgebungen realisiert werden.

Bei der Trennung der Umgebungen ist zu berücksichtigen, dass in der Regel kein Zugriff mit Entwicklerclients (Domino Designer) auf die Produktivumgebungen zuzulassen ist. Sollte ein Entwicklerzugriff auf eine Produktionsumgebung aus betrieblichen Erfordernissen in Ausnahmesituationen benötigt werden, sind im Vorfeld im Rahmen des Betriebskonzepts Verfahren zu definieren, die die Überwachung und Qualitätssicherung dieses Zugriffs sicherstellen. Der Zugriff hat transparent und anhand der Protokollierung nachvollziehbar zu erfolgen.

Die Verfahren, um eigenentwickelte Anwendungen in den Produktivbetrieb zu übernehmen, müssen sicherstellen, dass:

- eine formelle Abnahme der Anwendung durch die Verantwortlichen erfolgt,

- fachliche Tests, Integrationstests und Performanztests der Anwendung in ausreichendem Maß durchgeführt wurden,
- die in die Produktivumgebung eingebrachten Objekte und die getesteten Objekte übereinstimmen,
- die in die Produktivumgebung eingebrachten Objekte frei von Schadsoftware (siehe hierzu auch B 1.6 *Schutz vor Schadprogrammen*) sind und
- die Richtlinie für die Anwendungsentwicklung für die Notes/Domino-Plattform (siehe M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*) bei der Entwicklung nachvollziehbar angewendet wurde.

Bei zugekauften Anwendungen für die Lotus Notes/Domino-Umgebung sollten im Rahmen der Möglichkeiten vergleichbare Qualitätsmaßstäbe gelten wie für Eigenentwicklungen, wobei die Einhaltung der Richtlinie für die Anwendungsentwicklung durch entsprechende Aussagen und Zertifizierungen des Herstellers zu ersetzen ist.

**Anwendungsintegration mit der Lotus Notes/Domino-Plattform**

Anwendungsintegration mit Lotus Notes/Domino (siehe M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*) kann die Sicherheitsanforderungen an die Plattform im Betrieb völlig verändern.

Clientseitige Anwendungsintegration kann den Schutzbedarf des Lotus Notes Clients bezüglich aller drei Grundwerte erhöhen. Dies gilt auch für die Nutzung spezieller Integrationskomponenten wie das gemeinschaftlich mit SAP entwickelte Produkt *Alloy* zum Zugriff auf SAP-Systeme aus Lotus Notes. Dies hat in der Regel Auswirkungen auf die Konfiguration und Nutzung des Notes Clients. Die in M 4.229 *Sicherer Betrieb von Smartphones, Tablets und PDAs* geforderte sichere Konfiguration des Clients muss dies berücksichtigen. Der sichere Betrieb der Plattform ist um eine entsprechende clientseitige Protokollierung und Auswertung, mit Fokus auf die clientseitig integrierten Anwendungen, zu ergänzen.

Serverseitige Anwendungsintegration kann beispielsweise über die Nutzung von DB2-Datenbanken für Notes-Daten realisiert werden, oder aber über die Nutzung spezieller Integrationskomponenten. Daneben gibt es weitere Integrationslösungen über den Domino DIIOP-Dienst, Domino XML (DXL) und Domino JSP, die insbesondere die Integration mit der Websphere-Middleware unterstützen. Die Nutzung von Web Services der eigenen Institution oder von Fremdanbietern über die entsprechenden Schnittstellen von Lotus Notes/Domino fällt auch unter diese Betrachtungen.

Bei serverseitiger Anwendungsintegration erhöht sich der Schutzbedarf der entsprechenden Notes/Domino-Anwendungen und Dienste entsprechend unter Berücksichtigung des Schutzbedarfs der über die Integration eingebundenen Anwendungen und Dienste. Dies ist sowohl bei der serverseitigen Konfiguration der Dienste des Domino-Servers aus M 4.116 *Sichere Installation von Lotus Notes/Domino* zu berücksichtigen wie auch in der Festlegung der in M 4.132 *Überwachung der Lotus Notes/Domino-Umgebung* zu monitorenden Parameter und Ereignisse. Auch die Parameter für das in M 4.427 *Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino* beschriebene Logging sind anzupassen.

Anwendungsintegration ist daher, wie unter M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* gefordert, konzeptionell im Rahmen einer Richtlinie für die Anwendungsintegration zu betrachten. Die Einhaltung der Richtlinie ist bei der Produktivnahme der Integrationslösung zu prüfen.

Ist der Betrieb der Lotus Notes/Domino-Umgebung (oder einzelner Komponenten hiervon) ausgelagert, verbleibt die Verantwortung für die Gewährleistung eines sicheren Betriebs bei der auslagernden Institution, während die Durchführung der dazu erforderlichen Regeltätigkeiten bei der Institution und/oder einem oder mehreren Dienstleistern stattfindet. Der IT-Grundschutz-Baustein B 1.11 *Outsourcing* beschreibt die für eine Auslagerung oder Teilauslagerung erforderlichen besonderen Sicherheitsmaßnahmen.

**Upgrades und Migrationen im Betrieb**

Für den sicheren Betrieb der Lotus Notes/Domino-Umgebung sind die in M 4.116 *Sichere Installation von Lotus Notes/Domino* angeführten Hinweise zu Upgrades und Migrationen zu berücksichtigen.

**Administrationstätigkeiten**

Die administrativen Tätigkeiten sind nach Möglichkeit anhand eines Administrationshandbuches, das die in M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* angesprochene Planung administrativer Tätigkeiten dokumentiert, durchzuführen. Insbesondere bei Auslagerungen ist dies das Mittel, um eine nachvollziehbare Qualität kritischer Administrationstätigkeiten zu gewährleisten. Der Detaillierungsgrad dieses Administrationshandbuches ist abhängig vom Schutzbedarf der Lotus Notes/Domino-Plattform. Die Verbindlichkeit des Administrationshandbuches für die Durchführung administrativer Tätigkeiten ist sicherzustellen, entweder über die Verabschiedung als institutionseigene Richtlinie oder, bei ausgelagerter Administration, über die Aufnahme in die Vereinbarungen zur Erbringung der Dienstleistung.

**Überwachung im Betrieb**

Eine Überwachung der Lotus Notes/Domino-Umgebung im Betrieb ist erforderlich. Die Maßnahmen M 4.132 *Überwachung der Lotus Notes/Domino-Umgebung* und M 4.427 *Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino* beschreiben weitere Aspekte, die als Teil des sicheren Betriebs der Lotus Notes/Domino-Plattform umzusetzen sind.

**Nutzung von Lotus Notes/Domino als führendes System für institutionsweites Identitätsmanagement**

Die Zertifikatshierarchie (PKI) von Lotus Notes/Domino kann als Basis des institutionsweiten Identitätsmanagements genutzt werden. Dies hat in der Regel sehr große Auswirkungen auf den Schutzbedarf der Lotus Notes/Domino-Umgebung, da das Identitätsmanagement in der Regel der Kern des zentralen Berechtigungsmanagements ist. Eine solche Situation erfordert im Betrieb meistens einen im Hinblick auf alle Grundwerte strikt abgesicherten, dedizierten Domino-Server, der die dafür erforderlichen Dienste bereitstellt.

Die erforderliche Planung für die Nutzung der Zertifikatshierarchie von Lotus Notes/Domino als Basis des ist bereits in der Maßnahme M 2.206 *Planung des Einsatzes von Lotus Notes/Domino* unter den Punkten "Architekturplanung unter Berücksichtigung von Sicherheitsaspekten", "Planung der Rolle von Notes/Domino im institutionsweiten Identitätsmanagement", "Planung der Domänen- und Zertifikatshierarchie" umrissen.

Aus betrieblicher Sicht müssen insbesondere die administrativen Prozesse rund um die Zertifikatshierarchie sowie die Überwachung, Protokollierung und Auswertung und die Archivierung den erhöhten Schutzbedarf des Servers, der die Dienste der Zertifikatshierarchie bereitstellt, berücksichtigen.

**Anbindung von Lotus Notes/Domino an ein externes, zentrales Identitätsmanagement**

Die Anbindung von Notes/Domino an ein externes, zentrales Identity-Management von Fremdanbietern (wie z. B. den *Oracle Identity Manager*, das *Microsoft Identity and Access Management*, *Novell eDirectory*) oder des eigenen Herstellers (*IBM Tivoli Identity Management*) ändert den Schutzbedarf der Lotus Notes/Domino Zertifikatshierarchie.

Abhängig vom Schutzbedarf der Lotus Notes/Domino-Umgebung wird die Schnittstelle zur Anbindung an das externe Identitätsmanagement in der Regel im Hinblick auf alle Grundwerte entsprechend hohen Schutzbedarf aufweisen. Dies ist in den betrieblichen Prozessen, insbesondere in der Administration, Überwachung, Protokollierung und Auswertung entsprechend zu berücksichtigen. Bei Umsetzung von M 6.73 *Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung* ist der Ausfall des externen Identitätsmanagements bzw. der Anbindung an das externe Identitätsmanagement angemessen zu berücksichtigen.

Prüffragen:

- Ist ein dokumentiertes Betriebskonzept oder eine vergleichbare Betriebsdokumentation für die Lotus Notes/Domino-Umgebung vorhanden?
- Berücksichtigt das Datensicherungskonzept die Größe und Komplexität der zu sichernden Datenbanken?
- Ist die Vorgehensweise zur Produktivnahme von Anwendungen für die Lotus Notes/Domino-Umgebung dokumentiert?
- Ist die Vorgehensweise bei den wesentlichen Administrationstätigkeiten im Betrieb dokumentiert?
- Werden die Domino-Server, auf denen der CA-Prozess (Zertifizierungsprozess) läuft, bei entsprechender Nutzung der Domino-Zertifikatsinfrastruktur entsprechend überwacht und protokolliert?
- Ist bei Nutzung der Domino-CA (Certificate Authority, Zertifizierungsstelle) für weitere Anwendungen außerhalb der Lotus Notes/Domino-Plattform der erhöhte Schutzbedarf von Lotus Notes/Domino berücksichtigt?
- Ist bei einer vorhandenen Lotus Notes/Domino-Anbindung an ein externes, zentrales Identitätsmanagement dies in dem Betriebshandbuch entsprechend berücksichtigt?

# M 4.129 Sicherer Umgang mit Notes-ID-Dateien

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.128 *Sicherer Betrieb der Lotus Notes/Domino-Umgebung* integriert.

# M 4.130 Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.128 *Sicherer Betrieb der Lotus Notes/Domino-Umgebung* integriert.

# M 4.131 Verschlüsselung von Lotus Notes Datenbanken

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* integriert.

# M 4.132 Überwachung der Lotus Notes/ Domino-Umgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine angemessene Überwachung der Lotus Notes/Domino-Umgebung ist erforderlich, um den definierten Schutzbedarf im Betrieb abbilden zu können. Die Überwachung leistet einen Beitrag zur Erkennung von Fehlfunktionen oder Angriffen.

Abhängig vom definierten Schutzbedarf der Lotus Notes/Domino-Umgebung ist eine angemessene Überwachung einzurichten, die entsprechend zu dokumentieren ist (z. B. in dem in M 4.128 *Sicherer Betrieb der Lotus Notes/Domino-Umgebung* erwähnten Betriebskonzept).

Die Überwachung der Lotus Notes/Domino-Umgebung kann durch externe Monitoring-Tools erfolgen, die auf Netz-, Betriebssystem- und teilweise auch Anwendungsebene relevante Parameter und Prozesse prüfen. Eine tiefe Integration des Monitoring-Tools und der zu überwachenden Anwendung ist in der Regel möglich, wenn Tools desselben Herstellers (in diesem Fall die Tivoli-Produktfamilie) genutzt werden.

Sicherheitskomponenten wie Sicherheitsgateways, IDS-Systeme, Content-Security-Appliances und ähnliche können auch einen Beitrag zum Monitoring leisten. Hier ist eine entsprechende Zusammenarbeit der für die Sicherheitskomponenten Verantwortlichen mit den Verantwortlichen für den Betrieb der Lotus Notes/Domino-Umgebung erforderlich.

Die Lotus Notes/Domino-Plattform stellt eine Reihe von Überwachungsfunktionen sowohl auf Domänenebene (Domino Domain Monitoring) wie auch auf Serverebene (Domino Server-Überwachung und Server Health Monitoring, abgebildet durch die Integration von Basisfunktionen des IBM Tivoli Analyzers) bereit. Eine Überwachung ist unter anderem über die Serverkonsole, die Administratorkonsole und den Domino Server Monitor möglich. Weiterhin stellt die Plattform umfangreiche Überwachungsfunktionen bereit, die zur Unterstützung des Performance-Tuning gedacht sind, wie den Domino Configuration Collector.

Über Fault Recovery stehen Mechanismen bereit, die die automatische Wiederherstellung und den Wiederanlauf im Fehlerfall unterstützen. Die Nutzung dieser Funktionen erfordert umfangreiche konzeptionelle Vorarbeiten und eine sorgfältige Parametrisierung.

Prüffragen:

- Findet eine Überwachung des Betriebs der Lotus Notes/Domino-Umgebung über geeignete Überwachungsmechanismen oder -tools statt?
- Ist die Parametrisierung der Überwachungsmechanismen dokumentiert?

# M 4.133 Geeignete Auswahl von Authentikationsmechanismen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Identifikations- und Authentikationsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden. Die Identifikation und Authentisierung muss vor jeder anderen Interaktion zwischen IT-System und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben (sie prüfen oder ändern können). Bei jeder Interaktion muss das IT-System die Identität des Benutzers feststellen können.

Vor der Übertragung von Nutzerdaten muss der Kommunikationspartner (Rechner, Prozess oder Benutzer) eindeutig identifiziert und authentisiert sein. Erst nach der erfolgreichen Identifikation und Authentisierung darf eine Übertragung von Nutzdaten erfolgen. Beim Empfang von Daten muss deren Absender eindeutig identifiziert und authentisiert werden können. Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.

Es gibt verschiedene Techniken, über die die Authentizität eines Benutzers nachgewiesen werden kann. Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern)
- Passwörter
- Token wie z. B. Zugangskarten
- Biometrie

Für sicherheitskritische Anwendungsbereiche sollte starke Authentisierung verwendet werden, hierbei werden zwei Authentisierungstechniken kombiniert, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bezeichnet. Beide eingesetzten Authentisierungstechniken müssen sich auf dem Stand der Technik befinden.

Im Folgenden werden verschiedene Kriterien aufgezeigt, die bei der Auswahl von Identifikations- und Authentikationsmechanismen beachtet werden sollten. Nicht alle marktgängigen Systeme erfüllen alle Kriterien, diese sollten aber bei der Auswahl entsprechend berücksichtigt werden. Viele IT-Produkte beinhalten bereits neben ihrer eigentlichen Funktionalität Authentikationsmechanismen, beispielsweise Betriebssysteme. Hier ist zu überprüfen, ob diese den Ansprüchen genügen oder ob sie um zusätzliche Funktionalitäten erweitert werden müssen. Auch dazu eignen sich die folgenden Kriterien.

**Administration der Authentikationsdaten**

Es müssen Sicherheitsfunktionen bereitstehen, um Authentikationsdaten für Benutzer anlegen und verändern zu können. Diese Funktionen sollten nur von autorisierten Administratoren ausgeführt werden können. Bei der Verwendung von Passwörtern sollten autorisierte Benutzer ihre eigenen Authentikationsdaten innerhalb festgesetzter Grenzen verändern können. Das IT-System sollte einen geschützten Mechanismus zur Verfügung stellen, damit Benutzer ihre

Passwörter selbstständig verändern können. Dabei sollte es möglich sein, eine Mindestlebensdauer für Passwörter vorzugeben.

Nach einer erfolgreichen Anmeldung sollte den Benutzern Zeit und Ort seines letzten erfolgreichen Zugriffs angezeigt werden.

**Schutz der Authentikationsdaten gegen Veränderung**

Das IT-System muss die Authentikationsdaten bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung schützen. Dies kann beispielsweise durch Verschlüsselung der Passwortdateien und durch Nicht-Anzeigen der eingegebenen Passwörter geschehen. Die Authentikationsdaten sind getrennt von Applikationsdaten zu speichern.

**Systemunterstützung**

Beim Einsatz von organisationsweiten Authentikationsverfahren sollten diese nur auf Servern betrieben werden, deren Betriebssystem einen adäquaten Schutz gegen Manipulationen bietet. Bei der Auswahl von Authentikationsverfahren sollte darauf geachtet werden, dass diese möglichst plattformübergreifend eingesetzt werden können.

**Fehlerbehandlung bei der Authentikation**

Das IT-System sollte Anmeldevorgänge nach einer vorgegeben Anzahl erfolgloser Authentikationsversuche beenden können. Nach Ende eines erfolglosen Anmeldevorgangs muss das IT-System den Benutzer-Account bzw. das Terminal sperren können bzw. die Verbindung unterbrechen. Nach erfolglosen Authentikationsversuchen sollte das IT-System jeden weiteren Anmeldeversuch zunehmend verzögern (Time-delay). Die Gesamtdauer eines Anmeldeversuchs sollte begrenzt werden können.

**Administration der Benutzerdaten**

Das IT-System sollte die Möglichkeit bieten, den Benutzern verschiedene Voreinstellungen zuweisen zu können. Diese sollten angezeigt und verändert werden können. Die Möglichkeit, Benutzerdaten zu verändern, muss auf den autorisierten Administrator beschränkt sein. Wenn die Administration der Benutzerdaten über eine Kommunikationsverbindung erfolgen soll, muss diese ausreichend kryptographisch gesichert sein.

**Definition der Benutzereinträge**

Das IT-System muss die Umsetzung der Sicherheitsrichtlinie ermöglichen, indem für jeden Benutzer die entsprechenden Sicherheitseinstellungen gewählt werden können.

Ein Authentikationsverfahren sollte auch erweiterbar sein, z. B. um die Unterstützung starker Authentikationstechniken wie dem Einsatz von Token oder Chipkarten (siehe auch M 5.34 *Einsatz von Einmalpasswörtern*).

**Umfang der Benutzerdaten**

Neben Benutzernamen und Rechteprofil sollten noch weitere Informationen über jeden Benutzer hinterlegt werden (siehe auch M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*):

- Es sollte mindestens Vorname und Nachname eines Benutzers in der Benutzerverwaltung aufgenommen werden. Zusätzlich ist auch Telefon- und Raumnummer hilfreich.

- Um mit dem Benutzer in Kontakt zu treten, sollten zusätzlich auch Informationen wie E-Mail-Adresse, Telefonnummer und geographischer Standort (Adresse, Raumnummer) erfasst werden.
- Zusätzlich sollte erfasst werden, wie lange die Benutzerkennung gültig sein soll. Ist die Benutzerkennung abgelaufen, sollte sie gesperrt werden.

**Passwortgüte**

Wenn Passwörter zur Authentikation eingesetzt werden, sollte das IT-System Mechanismen bieten, die folgende Bedingungen erfüllen (siehe M 2.11 *Regelung des Passwortgebrauchs*):

- Es wird gewährleistet, dass jeder Benutzer individuelle Passwörter benutzt (und diese auch selbst auswählen kann).
- Es wird überprüft, dass alle Passwörter den definierten Vorgaben genügen (z. B. Mindestlänge, keine Trivialpasswörter). Die Prüfung der Passwortgüte sollte individuell regelbar sein. Beispielsweise sollten vorgegeben werden können, dass die Passwörter mindestens ein Sonderzeichen enthalten müssen oder bestimmte Zeichenkombinationen verboten werden.
- Das IT-System generiert Passwörter, die den definierten Vorgaben genügen. Das IT-System muss die so erzeugten Passwörter dem Benutzer anbieten.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden. Die Lebensdauer eines Passwortes sollte einstellbar sein.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Nach der Installation bzw. der Neueinrichtung von Benutzern sollte das Passwort-System einen Passwort-Wechsel nach der Erst-Anmeldung erzwingen.

**Biometrie**

Unter Biometrie im hier verwendeten Sinn ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale zu verstehen. Um biometrische Verfahren für die Authentisierung einsetzen zu können, werden zusätzliche Peripherie-Geräte benötigt, die die Benutzer auf Grundlage besonderer Merkmale eindeutig authentisieren können. Eine oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris
- Fingerabdruck
- Gesichtsproportionen
- Stimme und Sprachverhalten
- Handschrift
- Tippverhalten am Rechner

Neben einer Vielzahl von biometrischen Merkmalen und darauf basierenden biometrischen Verfahren bestehen darüber hinaus auch große Unterschiede zwischen den verfügbaren konkreten biometrischen Systemen und Produkten. Die Leistungsfähigkeit von biometrischen Verifikationssystemen ist sehr unterschiedlich. Bei einem Einsatz in sicherheitskritischen Bereichen muss darauf geachtet werden, dass das biometrische System eine akzeptable Erkennungsleistung und eine hohe Sicherheit bietet. Es darf nicht möglich sein, dass dieses mit Hilfe von Nachbildungen (z. B. einer Gesichtsmaske, Wachsnachbildung des Fingers, Kontaktlinsen mit Irismuster...) überlistet werden kann.

**Authentisierung mit Token**

Eine weitere Alternative bieten Authentikationstoken, also handliche Datenträger, die als sicherer Speicherplatz für die für die Authentikation benötigten Informationen wie z. B. kryptographischer Schlüssel dienen. Typische Beispiele für Authentikationstoken sind Chipkarten, USB-Sticks oder taschenrechnerähnliche Geräte zur Erzeugung von Einmal-Passwörtern.

**Anforderungen an Authentikationsmechanismen für Benutzer**

Das IT-System muss vor jeder anderen Benutzertransaktion die Benutzeridentität überprüfen. Das IT-System sollte darüber hinaus das Wiedereinspielen von Authentikationsdaten für Benutzer oder das Einspielen gefälschter oder kopierter Benutzerauthentikationsdaten erkennen und verhindern können. Das IT-System darf die Authentikationsdaten erst dann überprüfen, wenn sie vollständig eingegeben wurden.

Es sollte für jeden Benutzer individuell einstellbar sein, wann und von wo er auf das IT-System zugreifen darf.

**Protokollierung der Authentisierungsmechanismen**

Authentisierungsvorgänge sind in einem sinnvollen Umfang zu protokollieren. Die Protokolldateien sollten in regelmäßigen Abständen von den Administratoren überprüft werden. Das IT-System muss die folgenden Ereignisse protokollieren können:

- Ein- und Ausschalten der Protokollierung.
- Jeden Versuch, auf Mechanismen zum Management von Authentikationsdaten zuzugreifen.
- Erfolgreiche Versuche, auf Authentikationsdaten zuzugreifen.
- Jeden Versuch, unautorisiert auf Benutzer-Authentikationsdaten zuzugreifen.
- Jeden Versuch, auf Funktionen zur Administration von Benutzer-Einträgen zuzugreifen.
- Änderungen an Benutzereinträgen.
- Jeden durchgeführten Test auf Passwort-Güte.
- Jede Benutzung von Authentisierungsmechanismen.
- Jede Konfiguration der Abbildung von Authentisierungsmechanismen zu spezifischen Authentikationsereignissen.
- Die Installation von Authentisierungsmechanismen.

Jeder Protokollierungseintrag sollte Datum, Uhrzeit, Art des Ereignisses, Bezeichnung des Subjektes sowie Erfolg bzw. Misserfolg der Aktion enthalten.

Prüffragen:

- Ist sichergestellt, dass jede weitere Interaktionen mit dem System oder der Anwendung erst nach erfolgreicher Identifikation und Authentisierung möglich ist?
- Kommen dem Schutzbedarf angemessene Identifikations- und Authentisierungsmechanismen zum Einsatz?
- Können Authentisierungsdaten für Benutzer ausschließlich von autorisierten Administratoren angelegt bzw. verändert werden?
- Werden die Authentisierungsdaten durch das IT-System bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung geschützt?

- Können die eingesetzten Authentisierungsmechanismen Anmeldevorgänge nach einer vorgegebenen Anzahl von Fehlversuchen beenden?
- Werden abgelaufene Benutzerkennungen automatisch gesperrt?
- Werden Authentisierungsvorgänge in einem für die Institution angemessenen Umfang protokolliert?

# M 4.134 Wahl geeigneter Datenformate

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Leiter IT

Es gibt eine Vielzahl von unterschiedlichen Datenformaten, die von den verschiedenen IT-Anwendungen unterstützt werden. Diese sind allerdings im Allgemeinen nicht kompatibel, also untereinander austauschbar. Leider können häufig nicht einmal IT-Anwendungen mit demselben Aufgabenfeld (z. B. Textverarbeitungssysteme) mit den Datenformaten ähnlicher Produkte umgehen. Dieses Problem wird noch dadurch gesteigert, dass oft Anwendungsprogramme nach einem Versionswechsel die Datenformate ihrer Vorgänger nicht mehr verarbeiten können.

Daher muss bei der Beschaffung neuer Anwendungsprogramme untersucht werden, welche Datenformate unterstützt werden und wie verbreitet die unterstützten Datenformate sind. Da viele wichtige Vorgänge dauerhaft elektronisch gespeichert werden sollen, ist es ebenso wichtig zu hinterfragen, welche "Lebensdauer" von einem Datenformat erwartet wird. Generell sollte bei jedem Systemwechsel überprüft werden, ob alle gespeicherten Daten mit den neuen IT-Systemen oder Anwendungen noch verarbeitet werden können.

Ebenso muss aber auch bei jeder Nutzung eines Anwendungsprogramms überlegt werden, in welchem Format die bearbeiteten Daten gespeichert werden sollen. Dabei sollte immer berücksichtigt werden, wer und zu welchem Zeitpunkt diese Daten lesen können soll.

Bei der Wahl von Datenformaten für den Dateiaustausch sollte auch hinterfragt werden, ob diese Sicherheitsrisiken mit sich bringen können. Beispielsweise können bei bestimmten Datenformaten unerwünschte Zusatzinformationen in den Dateien enthalten sein (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*). Dateien, die in bestimmten Datenformaten erstellt wurden, können auch andere sicherheitsrelevante Probleme wie Makros und damit die Gefahr von Makro-Viren mit sich bringen (siehe M 4.3 *Einsatz von Viren-Schutzprogrammen*).

Die Überlegungen dazu, welche Datenformate für welche Zwecke geeignet sind und in der Institution unterstützt werden sollen, sollten geeignet dokumentiert und kommuniziert werden.

Prüffragen:

- Wird bei der Beschaffung von Anwendungsprogrammen darauf geachtet, welche Datenformate unterstützt werden?
- Wird bei der Beschaffung von Anwendungsprogrammen darauf geachtet, ob die unterstützten Datenformate die Anforderungen der Organisation hinsichtlich der Lebensdauer des Formates erfüllen?
- Wird bei der Auswahl des Datenformats für den Dateiaustausch berücksichtigt, welche zusätzlichen Informationen gespeichert werden?

# M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Systemdateien bzw. -verzeichnisse sind Dateien und Verzeichnisse, für die der Administrator zuständig ist. Diese sind entweder für alle Benutzer von Bedeutung oder sie dienen Administrationszwecken.

Auf Systemdateien sollten möglichst nur die Systemadministratoren Zugriff haben. Der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden. Auch Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen. Die Vergabe von Zugriffsrechten auf Systemdateien sollte grundsätzlich restriktiv und nur in Übereinstimmung mit den hausinternen Sicherheitsrichtlinien erfolgen (siehe auch M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*).

Systemdateien sollten getrennt von Applikationsdaten und Benutzerdateien gespeichert werden (siehe auch M 2.138 *Strukturierte Datenhaltung*). Dies sorgt für eine bessere Übersicht und erleichtert auch die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes.

Der Zugriff auf Systemdateien sollte immer protokolliert werden. Überflüssige, also nicht benötigte Systemdateien sollten vom System entfernt werden, damit sie nicht für Angriffe missbraucht werden können und auch nicht ständig auf Integrität kontrolliert werden müssen.

Bei der restriktiven Vergabe von Zugriffsrechten reicht es nicht aus, nur die Rechte eines Programms zu überprüfen. Zusätzlich muss auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden.

Die Integrität aller Systemdateien und -verzeichnisse, sowie die Korrektheit der Zugriffsrechte sollte nach Möglichkeit regelmäßig verifiziert werden. Für viele Betriebssysteme gibt es dafür Tools, mit denen solche Prüfungen schnell und zuverlässig durchgeführt werden können.

Prüffragen:

- Wird der Zugriff auf Systemdateien auf einen möglichst kleinen Kreis von Administratoren beschränkt?
- Sind Systemverzeichnisse so eingerichtet, dass sie den Benutzern nur die benötigten Privilegien zur Verfügung stellen?
- Erfolgt die Vergabe von Zugriffsrechten restriktiv und im Einklang mit den organisationseigenen Sicherheitsrichtlinien?
- Wird die Rechtevergabe aller Programme inklusive der von diesen aufgerufenen weiteren Programme überprüft?
- Wird der Zugriff auf Systemdateien immer protokolliert?

# M 4.136 Sichere Installation von Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.137 Sichere Konfiguration von Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.138 Konfiguration von Windows Server als Domänen-Controller

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Domänen-Controller stellen in einem Netz auf Basis der Serverbetriebssysteme Windows 2000 Server und Windows Server 2003 (im Folgenden unter dem Begriff Windows-Server zusammengefasst) die zur Verwaltung einer Windows-Server Domäne nötigen Dienste zur Verfügung, unter denen der Active Directory Dienst (Active Directory Service, ADS) die wichtigste Rolle einnimmt. In der Regel wird von einem Domänen-Controller auch der Namensdienst DNS (Domain Name Service) angeboten, ohne den das Active Directory nicht betrieben werden kann. Im DNS werden von Windows Referenzen auf wichtige Windows-Server Ressourcen gehalten, deren Integrität für das korrekte Funktionieren einer Windows-Server Domäne essentiell sind. Da ein Domänen-Controller als Anmeldeserver fungiert, führt er den dazu notwendigen Kerberos-Dienst aus. Die Kerberos-Komponenten auf dem Domänen-Controller bewahren zudem die im Rahmen des Authentisierungs-Protokolls genutzten geheimen Schlüssel auf.

Da jedem Domänen-Controller daher eine wichtige Rolle zukommt und durch ihn schützenswerte Daten gespeichert werden, sind für die Konfiguration folgende Punkte zu beachten. Daneben gelten auch für einen Domänen-Controller die in der Maßnahme M 4.137 *Sichere Konfiguration von Windows 2000* und M 4.139 *Konfiguration von Windows 2000 als Server* beschriebenen Aspekte entsprechend.

- Die Sicherheit eines Domänen-Controllers leitet sich hauptsächlich aus zwei wesentlichen Bereichen ab: der Sicherheit der Betriebssystemkonfiguration und der Sicherheit des Active Directory, welches auf eigene Sicherheitsmechanismen zurückgreift (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*). Die Sicherheitseinstellungen des Betriebssystems erfolgen im Wesentlichen durch Gruppenrichtlinien, die Sicherheitseinstellungen des Active Directory erfordern entsprechende Planung und Umsetzung (siehe M 2.229 *Planung des Active Directory*, M 2.231 *Planung der Gruppenrichtlinien unter Windows*).
- An einem Domänen-Controller dürfen sich nur berechtigte Administratoren lokal anmelden. Ein Benutzerbetrieb auf einem Domänen-Controller darf nicht erlaubt werden. Nach einer Standardinstallation ist es normalen Benutzern daher nicht gestattet, sich lokal an einem Domänen-Controller anzumelden.
- Ein Domänen-Controller sollte neben den zwingend notwendigen Standard Domänen-Controller Diensten, wie z. B. Active Directory, Kerberos und DNS, keine weiteren Infrastrukturdienste (z. B. DFS, DHCP) anbieten. Insbesondere vom Betrieb eines DHCP-Servers auf einem Domänen-Controller muss aus Sicherheitsgründen abgeraten werden (siehe auch Microsoft Dokumentation zu DNS und DHCP). Beide Dienste laufen unter den gleichen Berechtigungen ab. Dadurch können - stark vereinfacht dargestellt - die Zugriffsrechte auf DNS-Daten nicht mehr durchgesetzt werden, wenn der DHCP-Dienst Veränderungen an DNS-Daten durchführt.
- Ein Domänen-Controller sollte keine (Applikations-) Serverdienste anbieten, da bei Fehlern in den Serverprogrammen eine Kompromittierung des Domänen-Controllers und damit der gesamten Windows-Server Domäne möglich ist.

Domänen-Controller sollten so sicher wie möglich konfiguriert werden. Nach der Standardinstallation sollte die Vorlagendatei *secdc.inf* (unter Windows 2003 Server *securedc.inf*) oder *hisecdc.inf* angewandt werden. Die Vorlagendateien finden sich im Windows-Server Systemverzeichnis unter *%windir%\security\templates* und können entweder von der Kommandozeile mittels des Kommandos *secedit* konfiguriert werden, oder über die MMC-Plug-ins *Sicherheitsvorlagen* und *Sicherheitskonfiguration und -analyse* angesehen oder angewandt werden. Je nach Umfeld müssen die durch die Vorlagen *secdc.inf* (unter Windows Server 2003 *securedc.inf*) bzw. *hisecdc.inf* vorgenommen Einstellungen angepasst werden. Dies kann beispielsweise erforderlich sein, wenn im Netz noch Altsysteme, z. B. OS/2, vorhanden sind, die weniger sichere Einstellungen bieten. Weitere Hinweise zur Planung der Sicherheitseinstellungen finden sich in M 2.231 *Planung der Gruppenrichtlinien unter Windows*. Als ergänzendes Regelwerk für die Migration von Windows NT Server auf Windows 2003 Server empfiehlt sich die im Microsoft Download Center (http://www.microsoft.com/downloads) erhältliche Migrationshilfe "*Migrating from Windows NT Server 4.0 to Windows Server 2003*". Diese beschreibt detailiert alle für die Umstellung erforderlichen Konfigurationsanpassungen.

- Die Konfiguration des Kanals, der zur Kommunikation von Verwaltungsdaten zwischen Rechnern einer Windows-Server Domäne genutzt wird, sollte so sicher wie möglich sein (siehe dazu M 5.89 *Konfiguration des sicheren Kanals unter Windows*).
- Wenn möglich, sollte ein Domänen-Controller im *native mode* betrieben werden, damit alle Windows-Client-Mechanismen (ab Windows 2000) voll ausgenutzt werden können. Dies sind beispielsweise universelle Gruppen, Gruppenschachtelung und die Vergabe der RAS-Zugangsberechtigung über eine Gruppenzugehörigkeit. Ein Umschalten in den *native mode* ist dann möglich, wenn in der Domäne kein Windows NT BDC (Backup-Domänen-Controller) betrieben wird. Der Betrieb von Windows NT Servern und Workstations ist auch im *native mode* möglich. Zu beachten ist, dass eine Rückkehr in den *mixed mode* und damit zu einer NT-Domäne danach nicht mehr möglich ist.
- Kann ein Domänen-Controller in den so genannten Active-Directory-Restore-Modus gebootet werden, so ist es möglich, Veränderungen am AD durchzuführen, indem z. B. alte Zustände (teilweise oder vollständig) von Backup-Medien geladen werden. Diese Veränderungen lassen sich so einspielen, dass sie nach dem regulären Booten durch die Active-Directory-Replikation an alle anderen Domänen-Controllern einer Domäne propagiert werden. Es ist daher sicherzustellen, dass der Active-Directory-Restore-Modus durch ein geeignetes Passwort geschützt ist und Arbeiten in diesem Modus nur unter Einhaltung des Vier-Augen-Prinzips erfolgen. Der Active-Directory-Restore-Modus ist kommandozeilenbasiert und Tippfehler können gravierende Folgen haben, z. B. Löschen oder Überschreiben des falschen Active-Directory-Zweiges. Daher bietet das Vier-Augen-Prinzip hier neben der Tätigkeitskontrolle auch eine Sicherheit durch die Kontrolle aller Eingaben durch zwei Personen.
- Die Domänen-Controller der Forest-Root-Domäne (FRD) sind aufgrund der Sonderstellung der FRD besonders schutzbedürftig.

Generell ist für jeden Domänen-Controller immer die physikalische Sicherheit zu gewährleisten, z. B durch Aufstellung in einem Serverraum.

Prüffragen:

- Sind für alle Domänen-Controller restriktive Zugriffsrechte auf Betriebssystemebene vergeben?
- Wird der Domänen-Controller im native mode betrieben?

- Ist sichergestellt, dass der Active-Directory-Restore-Modus durch ein geeignetes Passwort geschützt ist und Arbeiten in diesem Modus nur unter Einhaltung des Vier-Augen-Prinzips erfolgen?

# M 4.139 Konfiguration von Windows 2000 als Server

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.140 Sichere Konfiguration wichtiger Windows 2000 Dienste

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.141 Sichere Konfiguration des DDNS unter Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.142 Sichere Konfiguration des WINS unter Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.143 Sichere Konfiguration des DHCP unter Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.144 Nutzung der Windows 2000 CA

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.145 Sichere Konfiguration von RRAS unter Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Nach der Installation und initialen Konfiguration gemäß den im Vorfeld geplanten Windows Konzepten und Sicherheitsrichtlinien erfolgt der Betrieb von Windows-Systemen in der Regel im Netzverbund. Die Sicherheit eines solchen Netzes hängt einerseits von den eingestellten Konfigurationsparametern ab. Sie wird andererseits auch maßgeblich durch die Art und Weise der Konfigurationsänderungen bestimmt, die im laufenden Betrieb erfolgen müssen. Dabei sind insbesondere Seiteneffekte zu berücksichtigen, die unter Umständen unbeabsichtigt zu Sicherheitslücken führen können.

Die Windows Client-Versionen bieten eine Reihe von Werkzeugen und Mechanismen an, die die Administratoren bei der Aufrechterhaltung der Sicherheit eines laufenden Systems unterstützen können:

- *Windows File Protection (WFP)* beziehungsweise *Windows Resource Protection (WRP)* ist ein Systemmechanismus von Windows, der sicherstellt, dass Systemdateien unverändert im Originalzustand verbleiben. Der Mechanismus nutzt zwei Komponenten: Den so genannten *SystemFileChecker* (*sfc.exe*), der die Systemdateien, beispielsweise beim Systemstart, auf ihre Integrität hin überprüft und veränderte Dateien durch zwischengespeicherte Originaldateien ersetzt. Weiterhin existiert ein Überwachungsmechanismus, der Systemdateien nach dem Versuch eines schreibenden Zugriffs wieder durch die Originalversion ersetzt. Der Mechanismus kann auch so konfiguriert werden, dass die veränderte Datei nach einer entsprechenden Bestätigung beibehalten wird. Die Konfiguration erfolgt durch *sfc.exe* über die Kommandozeile:
- Windows XP:
- - *sfc /SCANNOW*: Überprüft sofort alle geschützten Systemdateien.
  - *sfc /SCANONCE*: Überprüft alle geschützten Systemdateien einmal beim nächsten Neustart.
  - *sfc /SCANBOOT*: Überprüft alle geschützten Systemdateien bei jedem Start.
  - *sfc /REVERT*: Setzt den Mechanismus auf die Standardeinstellungen zurück.
  - *sfc /PURGECACHE*: Leert den Dateicache.

- Ab Windows Vista:
- - *sfc /SCANNOW*: Überprüft die Integrität aller geschützten Systemdateien und repariert Dateien mit Problemen, falls nötig.
  - *sfc /VERIFYONLY*: Überprüft die Integrität aller geschützten Systemdateien. Es erfolgt keine Reparatur.
  - *sfc /SCANFILE*: Überprüft die Integrität der angegebenen Datei, und repariert die Datei, wenn Probleme gefunden werden. Es muss ein vollständiger Pfad angegeben werden.
  - *sfc /VERIFYFILE*: Überprüft die Integrität der angegebenen Datei. Es erfolgt keine Reparatur.
  - *sfc /OFFBOOTDIR*: Gibt den Speicherort des Offline-Startverzeichnisses für Offline-Reparaturen an.
  - *sfc /OFFWINDIR*: Gibt den Speicherort des Offline-Windows-Verzeichnisses für Offline-Reparaturen an.

Um die oben genannten Schritte durchführen zu können, werden Administratorenrechte benötigt.

- Mit Windows XP wurde die automatische Systemwiederherstellung eingeführt. Dieser Mechanismus kann zum Wiederherstellen eines früheren Systemzustands verwendet werden, wenn beispielsweise eine Softwareinstallation fehlschlägt und das System in einen instabilen Zustand gerät. In Abhängigkeit von lokalen Umständen und insbesondere von der implementierten Softwareverteilungs-Strategie kann der Einsatz der automatischen Systemwiederherstellung beispielsweise im Testumfeld vorteilhaft sein.
  Windows Vista bietet mit *Systemsteuerung* | *Sichern und Wiederherstellen* und der Option *Den gesamten Computer anhand eines Abbildes von Windows Complete PC-Sicherung und Wiederherstellung wiederherstellen* zwei Möglichkeiten der Wiederherstellung eines beschädigten Systems an. Ab Windows 7 sind diese Einstellungen (in der Desktop-Ansicht) unter folgendem Pfad zu finden: *Systemsteuerung* | *Wiederherstellung* | *Systemwiederherstellung öffnen*.
  Systemwiederherstellungen dürfen nur von verantwortlichen Administratoren durchgeführt werden. Die Konfiguration des wiederhergestellten Systems muss auf Konformität mit den geltenden Sicherheitsrichtlinien geprüft werden, um die Sicherheit des Informationsverbundes nicht zu gefährden. Es ist besonders darauf zu achten, dass keine kritischen Patches, Updates oder Einstellungen zurückgesetzt werden. Diese sind gegebenenfalls erneut zu installieren und zu konfigurieren.
- Windows enthält mit dem Kommandozeilen-basierten Sicherheitseditor *secedit.exe* und dem MMC Snap-in *Sicherheitskonfiguration und -analyse* Werkzeuge zur Konfiguration der Sicherheitseinstellungen von Windows Client-Rechnern. Diese Sicherheitskonfiguration kann auch in einer Datenbank gespeichert werden, gegen die ein Rechner auf Konformität getestet werden kann. Dazu wird zunächst mit dem MMC Snap-in *Sicherheitskonfiguration und -analyse* eine Datenbank erzeugt (*Vorgang/Datenbank öffnen*, neuen oder existierenden Datenbanknamen eingeben). Diese kann mit einer Sicherheitsvorlage *(.inf*-Datei, siehe MMC Snap-in *Sicherheitsvorlagen*) initialisiert werden. Mittels *Vorgang/ Computer jetzt analysieren* und *Vorgang/System jetzt konfigurieren* kann eine Analyse oder Konfiguration des Systems anhand der Einstellungen der Datenbank erfolgen. Die Datenbank selbst liegt in Dateiform vor *(.sdb*-Datei) und kann auf andere Systeme übertragen werden. Allerdings sind die Aussagen bei Abweichungen von Zugriffsrechten auf Datei- oder Registry-Ebene wenig hilfreich, da lediglich die Abweichung dokumentiert wird, nicht jedoch, welche Zugriffsrechte abweichen.
- Die Sicherheitseinstellungen eines Windows Clients werden beim Betrieb in einer Domäne in der Regel durch die Anwendung von Gruppenrichtlinien beziehungsweise den in einem Objekt enthaltenen Einstellungen festgelegt. Auf diese Weise lassen sich die Sicherheitseinstellungen auch für große Windows-Netze effizient und zentral verwalten. Änderungen von Group Policy Objects (GPO) Einstellungen finden zentral an einem Domänen-Controller statt und werden dann an die betroffenen Rechner verteilt. Der GPO-Mechanismus kann so konfiguriert werden, dass periodisch ein Update der GPO-Einstellungen erfolgt, damit die veränderten Einstellungen wirksam werden können (siehe auch M 2.231 *Planung der Gruppenrichtlinien unter Windows* und M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*).
- Die Sicherheit des Systemzugangs kann durch die Verwendung einer Smartcard-basierten Anmeldung erhöht werden. Die Authentisierung erfolgt dann nicht über einen Benutzernamen und ein möglicherweise schwaches Passwort, sondern über ein Zertifikat, welches auf einer phy-

sischen Chipkarte gespeichert ist. Windows kann so konfiguriert werden, dass Anmeldungen sowohl über die Eingabe von Benutzername und Passwort als auch über eine Chipkarte möglich sind, oder ausschließlich mit Chipkarte. Generell können nur Microsoft-konforme Zertifikate genutzt werden sowie Chipkarten, die von Windows-Betriebssystemen unterstützt werden. Mit der Einführung von Windows 8 und Windows Server 2012 wird die Möglichkeit gegeben, solche Zertifikate auf virtuellen Chipkarten zu speichern. Diese simulieren die Funktionalität einer physischen Chipkarte und nutzen dafür das Trusted Platform Module (TPM), das im jeweiligen IT-System integriert sein muss. Bei dieser Variante ist zu beachten, dass eine solche Smartcard immer mit dem System verbunden ist (z. B. sich bei einem Diebstahl des Gerätes dann auch im Besitz des Diebes befindet). Sicherer ist hier der Einsatz eines echten zweiten Faktors für die Authentisierung. Eine weitere Möglichkeit, Unbefugten den Systemzugang zu verwehren, ist der Einsatz einer Festplattenverschlüsselung und einer Authentisierung des Benutzers vor dem Start des Betriebssystems.
- Beim Einsatz von kryptographischen Funktionen auf den Clients (Festplattenverschlüsselung, sonstige Verschlüsselungs- und Signaturverfahren) muss ein besonderes Augenmerk auf die Sicherung der kryptographischen Schlüssel gegen unbefugten Zugriff gerichtet werden. Die Speicherung der Schlüssel im TPM bietet hier einerseits einen hohen Schutz, koppelt aber andererseits die Schlüssel an das eingesetzte System, so dass ein Verlust durch Hardware-Defekte droht.

Die Sicherheit eines Informationsverbunds basiert immer auch auf der physikalischen Sicherheit der IT-Systeme und Netzkomponenten. Diese muss für den Betrieb eines Windows Client-Systems sichergestellt sein. Für den sicheren Betrieb eines Windows Client-Systems ist generell Folgendes zu beachten:

- Die Sicherheit von Windows hängt wesentlich von der Sicherheit des Active Directory ab. Die hier enthaltenen Informationen müssen einerseits vor unberechtigter Veränderung geschützt und andererseits konsistent gehalten werden. Dies erfordert insbesondere bei Veränderungen entsprechende Sorgfalt. Es empfiehlt sich dringend, im Rahmen der Sicherheitsplanung nicht nur Werte oder Wertebereiche für Parameter festzulegen, sondern auch innerbetriebliche oder administrative Abläufe zu definieren, die geeignet sind, die festgelegte Sicherheitsrichtlinie umzusetzen. So sollte zum Beispiel festgelegt werden, welche Schritte beim Löschen oder Anlegen eines neuen Benutzerkontos durchzuführen sind, damit die notwendigen Veränderungen korrekt ausgeführt werden. Weitere Informationen zum sicheren Betrieb von Windows Clients in einem Active Directory sind in B 5.16 *Active Directory* beschrieben.

Neben der Sicherheit des Active Directory und der Systemsicherheit, die durch die im Active Directory festgelegten Parameter bedingt wird, muss auch die Sicherheit wichtiger Systemdienste gewährleistet werden. Hierbei spielt die Sicherheit von DNS, WINS, DHCP, RAS sowie Kerberos eine besonders große Rolle.
Auch hier muss bei Änderungen sichergestellt werden, dass die geltenden und festgelegten Sicherheitsrichtlinien nicht verletzt werden. Hinweise zur Konfiguration dieser Dienste finden sich in M 4.246 *Konfiguration der Systemdienste auf Clients ab Windows XP* und den darin referenzierten Maßnahmen.

- Für die Verwaltung eines Windows Client-Systems stehen standardmäßig die so genannten Snap-ins der Microsoft Management Console (MMC-Snap-ins) zur Verfügung. MMC Snap-ins stellen Verwaltungsmodule dar, die über eine standardisierte Schnittstelle in die MMC integriert werden können. Der Zugriff auf die verschiedenen MMC Snap-ins muss daher re-

glementiert werden. Normalen Benutzern sollte der Zugriff auf Systemverwaltungswerkzeuge generell untersagt werden. Als Ausnahme ist hier jedoch das MMC Snap-in zur Verwaltung von Zertifikaten zu nennen, welches auch von normalen Benutzern zum Verwalten der eigenen Zertifikate genutzt werden muss. Der Zugriff auf die einzelnen MMC Snap-ins lässt sich granular über GPO-Einstellungen regeln.

- Die Verwaltungstools zum Zugriff auf die lokale Registry eines Rechners (*regedt32* und *regedit*) sollten nicht für normale Benutzer zugreifbar sein. Auch dies lässt sich durch GPO-Einstellungen erreichen (siehe M 4.75 *Schutz der Registry unter Windows-Systemen*).
- Die Sicherheit eines Windows-Netzes hängt von vielen Faktoren ab. Insbesondere können Sicherheitslücken durch Zusatzapplikationen entstehen, die entweder falsch konfiguriert sind oder Fehler in der Programmierung enthalten. Oft ergeben sich Probleme erst durch den gemeinsamen Betrieb mehrerer Anwendungen. Aus diesem Grund sind vor Einführung einer neuen Applikation Tests durchzuführen, die einen ersten Hinweis darauf geben, ob offensichtliche Probleme bestehen. Vollständige Sicherheit kann jedoch nicht erreicht werden, da insbesondere der Test auf Fehler durch Seiteneffekte in anderen Applikationen schwierig durchzuführen und extrem aufwendig ist.
- Auch wenn Änderungen sorgfältig und unter Einhaltung aller Vorsichtsmaßnahmen erfolgen, kann die Existenz von Sicherheitslücken in einem komplexen System nie ganz ausgeschlossen werden. Aus diesem Grund sollte immer eine geeignete Systemüberwachung stattfinden (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems* und M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008* Überwachung von Clients ab Windows Vista und Servern ab Windows Server 2008). Dabei muss die Stärke und Genauigkeit der Überwachung der Gefährdungslage angepasst sein. Die Art und Weise der Überwachung kann nur im konkreten Fall festgelegt werden. Generell sollten auch die Tätigkeiten von Administratoren durch die Überwachung erfasst werden. Zusätzlich empfiehlt sich eine regelmäßige Überprüfung, damit eventuelle Lücken, die durch Veränderungen des Systems entstehen können, aufgedeckt werden.
- Unter Sicherheitsgesichtspunkten sind auch Änderungen in der Domänenstruktur kritisch. Daher sind diese nur nach sorgfältiger Planung durchzuführen. Es ist schon bei der initialen Planung zu berücksichtigen, dass eine Windows Domänenstruktur (Aufteilung in Domänen, Trees, Forests) nachträglich nur wenige Veränderungen erlaubt (siehe M 2.229 *Planung des Active Directory*).
- Auch unter Sicherheitsgesichtspunkten ist es wichtig, dass alle den Betrieb eines Windows Client-Systems betreffenden Richtlinien, Regelungen und Prozesse dokumentiert werden. Dazu sollten Betriebshandbücher erstellt werden, die bei Systemänderungen aktualisiert werden müssen. Da die Betriebshandbücher sicherheitsrelevante Informationen enthalten, sind sie so aufzubewahren, dass einerseits Unbefugte keinen Zugriff auf sie erlangen können, jedoch andererseits für befugte Administratoren ein einfacher Zugriff besteht.

Die aufgeführten Empfehlungen können nur allgemeinen Charakter besitzen, da die Aufrechterhaltung der Systemsicherheit auch von lokalen Gegebenheiten abhängt. Daher müssen schon in der Planungsphase eines Windows-Netzes entsprechende Richtlinien zum sicheren Betrieb erstellt werden, die die lokalen Anforderungen berücksichtigen. Unter Umständen kann es vorkommen, dass gewisse Sicherheitsmechanismen nicht optimal sicher konfiguriert werden können. Dies ist zum Beispiel der Fall, wenn "alte" Applikationen weiter betrieben werden müssen, die nur für schwache oder keine Authentisie-

rung ausgelegt sind. Hier muss durch entsprechend ausgleichende Gegenmaßnahmen an anderer Stelle, oder auf organisatorischer Ebene, eine zufrieden stellende Sicherheit garantiert werden.

Die Sicherheit eines Windows-Systems im laufenden Betrieb hängt wesentlich vom Kenntnisstand der Administratoren ab. Daher ist die Schulung und Fortbildung der Systemverwalter eine wichtige Schutzmaßnahme (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*), da potenzielle Sicherheitslücken nur von kompetenten Administratoren entdeckt und vermieden werden können. Daneben müssen auch die normalen Benutzer in Sicherheitsaspekten geschult werden (siehe auch M 3.28 *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*), damit potenzielle Gefahren bekannt sind und zur Verfügung stehende Sicherheitsmechanismen richtig eingesetzt werden können.

Prüffragen:

- Sind Stärke und Genauigkeit der Systemüberwachung von Windows Client-Betriebssystemen der Gefährdungslage angepasst?
- Ist der Zugriff auf alle Administrationswerkzeuge für Benutzer von Windows Client-Betriebssystemen unterbunden worden?
- Werden vor der Einführung neuer Applikationen auf Windows Client-Betriebssystemen Funktions- und Sicherheitstests durchgeführt?
- VoIP im WLAN: Ist ein qualifizierter Schutz des WLAN gewährleistet?

# M 4.147 Sichere Nutzung von EFS unter Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Unter Windows steht das Dateisystem EFS (Encrypting File System - verschlüsselndes Dateisystem) zur Verfügung, das die Verschlüsselung einzelner Dateien unterstützt, die dafür gekennzeichnet werden müssen. Die Dateiverschlüsselung mittels EFS basiert auf einem hybriden Mechanismus, der asymmetrische und symmetrische Verschlüsselungsverfahren gemischt einsetzt:

- Zur reinen Datenverschlüsselung wird ein schnelles symmetrisches Verfahren benutzt. Der dabei benutzte Schlüssel (der sogenannte File Encryption Key, FEK) wird zufällig erzeugt.
- Windows 2000 und Windows XP vor Service Pack 1 setzen standardmäßig das DESX-Verfahren ein, eine abgewandelte Form des DES-Algorithmus. Windows XP kann auf das Triple-DES-Verfahren nach FIPS 140-1 umgestellt werden. Der Einsatz des Triple-DES-Verschlüsselungsalgorithmus ermöglicht vor allem Verschlüsselung mit größeren Schlüssellängen. Die Aktivierung des Algorithmus erfolgt in den Gruppenrichtlinien unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Systemkryptographie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden*. Ab Windows XP Service Pack 1 kommt der AES-Algorithmus mit 256-Bit langen Schlüsseln zum Einsatz. Der verwendete Verschlüsselungsalgorithmus kann durch den Registry-Eintrag *HKLM\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\EFS\AlgorithmID* festgelegt werden: 0x6603 für Triple-DES, 0x6604 für DESX und 0x6610 für AES.
- Die Aktivierung des Triple-DES-Verschlüsselungsalgorithmus betrifft standardmäßig nicht nur das EFS, sondern auch IPSec. Durch einen neuen Eintrag in die Registrierungsdatenbank (DWORD Name: *AlgorithmID*, Wert *0x6603*, unter *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS*) wird die Benutzung von Triple-DES auf EFS beschränkt.
- Beim Einsatz in einer gemischten Umgebung (Windows 2000 und spätere Windows-Versionen) ist zu beachten, dass Windows 2000-Systeme ohne High-Encryption-Pack (bzw. vor Service Pack 2) nicht auf Dateien zugreifen können, die mit dem Triple-DES-Algorithmus verschlüsselt wurden. Dokumente, die mit AES verschlüsselt wurden, können nicht von Windows 2000-Systemen und Windows XP-Systemen ohne Service Pack 1 gelesen werden. Diese Probleme treten im Normalbetrieb jedoch nur auf, wenn die verschlüsselten Daten nicht auf dem Originalrechner entschlüsselt werden, wie es beim Verwenden von Wechsellaufwerken mit NTFS oder WebDAV mit EFS möglich ist.
- Zur Verschlüsselung des FEK wird das asymmetrische RSA-Verfahren eingesetzt. Die Verschlüsselung des FEK erfolgt mit dem öffentlichen Schlüssel des Benutzers, der die Datei verschlüsselt. Damit kann der FEK nur noch mit dem privaten Schlüssel dieses Benutzers entschlüsselt und zum Entschlüsseln der Dateiinhalte verwendet werden. Seit Windows 7 und Server 2008 R2 kann der FEK zusätzlich durch das Elliptic-Curve-Cryptosystems-Verfahren (ECC) verschlüsselt werden. Das Verfahren ermöglicht den Einsatz von kürzeren Schlüsseln. Ab Windows 7 und Server 2008 R2 werden RSA und ECC Hybrid verwendet, um Kompatibilität zu vorherigen Windows Versionen zu erhalten. Die Schlüssellänge für

die Verfahren wird in der Gruppenrichtlinie: *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für öffentliche Schlüssel* | *Verschlüsselndes Dateisystem* konfiguriert. Dabei sollte mindestens der voreingestellte Wert von 2048 Bit für RSA und 256 Bit für ECC verwendet werden. Diese Einstellungen werden auch standardmäßig genutzt. Je nach Vertraulichkeitsanforderung an die zu verschlüsselnden Daten können auch größere Schlüssellängen gewählt werden.

Alle zur Ver- oder Entschlüsselung benötigten Schlüssel werden von Windows während der Benutzung in einem Hauptspeicherbereich abgelegt, der nicht in die Auslagerungsdatei verlagert wird. Dadurch soll gewährleistet werden, dass die Schlüssel nicht kompromittiert werden können, wenn ein unberechtigter Dritter Zugriff auf die Auslagerungsdatei erhält. Kritisch ist in diesem Zusammenhang die Verwendung des Ruhezustandes (*Hibernation Modus*), da der gesamte Hauptspeicherbereich in einer unverschlüsselten Datei (hiberfil.sys) gespeichert wird, die dann notwendigerweise auch das Schlüsselmaterial enthält. Aus diesem Grund sollte der Ruhezustand bei Verwendung von EFS unter Windows-Versionen vor Windows Vista und Windows Server 2008 nicht verwendet werden. Dies ist besonders bei mobilen Systemen wichtig. Sofern zusätzlich BitLocker aktiv zur Festplattenverschlüsselung auf den Systemen eingesetzt wird, erfolgt eine Verschlüsselung der Ruhezustandsdatei. Der ab Windows Vista verfügbare hybride Standbymodus sollte aus dem gleichen Grund nicht verwendet werden. Dieser speziell für Desktop-Systeme entwickelte Energiesparmodus speichert wie der Ruhezustand den Inhalt des Arbeitsspeichers auf die Festplatte, bevor das System in den Standby-Zustand versetzt wird. Clientseitig ab Windows Vista und serverseitig ab Server 2008 kann als Abhilfe die Auslagerungsdatei verschlüsselt werden: *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für öffentliche Schlüssel* | *Verschlüsselndes Dateisystem.* Klick mit der rechten Maustaste und Wahl von *Eigenschaften* im dann angezeigten Menü aktivieren.

Die Verschlüsselung mittels EFS kann jeder Benutzer pro Datei oder Verzeichnis einstellen. Über den korrekten Umgang mit EFS sollten die Benutzer geschult werden, ebenso sind sie über die potenziellen Schwächen dieser Art der Verschlüsselung zu informieren. Folgendes gilt es hierbei zu beachten:

- Das Kopieren oder Verschieben von EFS-verschlüsselten Dateien von einem NTFS- auf ein FAT/FAT32 entschlüsselt die Dateien, da FAT/FAT32 keine Verschlüsselung unterstützt. Zusätzlich werden die NTFS-Berechtigungen, die für die Datei vergeben sind, entfernt.
- Ein Verschieben von verschlüsselten Dateien zwischen NTFS-Laufwerken auf dem gleichen Computer behält die Verschlüsselung und auch die NTFS-Berechtigungen bei.
- Sollen die verschlüsselten Dateien auch einem anderen Computer zugreifbar sein, ist es erforderlich, das EFS-Zertifikat mitsamt Schlüssel zu exportieren und auf dem Zielcomputer zu importieren.
- EFS funktioniert nicht mit komprimierten Ordnern.

Durch die Nutzung von EFS wird ein Sicherheitsgewinn erzielt. Die Benutzer sollten sich allerdings bewusst sein, dass trotz des Verschlüsselns von Klartextdateien ein Restrisiko besteht, dass die Daten der gelöschten Klartextdatei teilweise oder ganz wiederhergestellt werden können. Dazu ist jedoch spezielle Software und der Zugriff auf die Festplatte des jeweiligen Rechners notwendig.

Damit die mittels EFS verschlüsselten Dateien beim Verlust des privaten Schlüssels nicht vollständig verloren sind, kann eine zusätzliche Verschlüsselung des FEK mit dem öffentlichen Schlüssel des so genannten Wiederher-

stellungsagenten (englisch *Recovery Agent*) erfolgen. Dadurch ist eine Entschlüsselung der Daten auch unter dem Benutzerkonto des Wiederherstellungsagenten möglich. Prinzipiell kann ein beliebiges Benutzerkonto als Wiederherstellungsagent eingesetzt werden. Unter Windows 2000 ist die Angabe eines Wiederherstellungsagenten obligatorisch, unter Windows ab Version XP dagegen nicht. Als Standardvorgabe wird von Windows 2000 das Administratorkonto genutzt.

Beim Einsatz von EFS ist Folgendes aus Sicherheitssicht zu beachten:

- EFS ist völlig transparent für den Benutzer. Unter Windows 2000 bemerkt ein Benutzer damit jedoch auch keinen Unterschied zwischen verschlüsselten und unverschlüsselten Dateien. Daher ist besondere Aufmerksamkeit gefordert, dass sensitive Dateien auch tatsächlich verschlüsselt werden. Ab Windows XP / Server 2003 werden die verschlüsselten Dateien im Windows Explorer standardmäßig in einer anderen Farbe angezeigt. Dies kann im Windows Explorer durch die Option *Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen* unter *Extras* | *Ordneroptionen* | *Ansicht* bzw. *Organisieren* | *Ordner- und Suchoptionen* | *Ansicht* gesteuert werden. Ab Windows Vista / Server 2008 hängt der zu verwendende Befehlspfad von der eingestellten Ansicht des Windows Explorer ab.
- EFS-verschlüsselte Dateien werden in der Grundeinstellung nicht in den Index der Windows-Suchfunktion aufgenommen. Wenn die verschlüsselten Dateien dennoch für die schnelle Suche indiziert werden sollen, muss der Index ebenfalls durch Verschlüsselungsmechanismen geschützt werden. Sonst könnten sensitive Daten aus dem Index im Klartext ausgelesen werden. Daher sollten EFS-verschlüsselte Dateien nicht für die Windows-Suche indiziert werden.
- Aufgrund der Transparenz für Benutzer ist der Schutz der EFS-Dateiverschlüsselung so stark wie das Passwort des jeweiligen Benutzerkontos. Kann sich ein unbefugter Dritter erfolgreich unter einem Benutzerkonto anmelden, so hat er Zugriff auf alle verschlüsselten Dateien dieses Benutzerkontos. Auch aus diesem Grund sollten, starke Passwörter für jedes Benutzerkonto verwendet werden. Da Windows erlaubt, eigene Passwortfilter zu nutzen, kann auf diesen Mechanismus zurückgegriffen werden, um die Verwendung starker Passwörter technisch zu erzwingen.
- EFS ist eine Dateiverschlüsselung und keine Ordnerverschlüsselung. Allerdings kann ein Ordner zur Verschlüsselung markiert werden, dann werden alle im Ordner befindlichen Dateien oder auch Dateien, die neu in einem solchen Ordner erzeugt werden, verschlüsselt. Es ist jedoch prinzipiell möglich, auch unverschlüsselte Dateien in einem solchen Ordner zu halten und zu erzeugen (siehe nächster Absatz). Verschlüsselte Dateien können außerdem an jeder Stelle im Dateibaum existieren und sind nicht an Ordner gebunden, die zur Verschlüsselung gekennzeichnet sind.
- Obwohl EFS keine Ordnerverschlüsselung ist, empfiehlt es sich, verschlüsselte Dateien in speziellen Ordnern vorzuhalten und Ordner für die Verschlüsselung zu kennzeichnen. Dies erleichtert das Arbeiten mit verschlüsselten Dateien.
- Das Verschlüsselungsmerkmal ist ein Dateiattribut, das wie alle anderen Dateiattribute behandelt wird, das heißt beim Verschieben von Dateien bleiben die Dateiattribute unverändert. Dies führt dazu, dass Dateien nicht automatisch verschlüsselt werden, wenn sie in einen Ordner verschoben werden, der für die Verschlüsselung gekennzeichnet ist. Die Voreinstellung für den Windows Explorer ist jedoch, dass auch verschobene Dateien verschlüsselt werden. Dieses Verhalten lässt sich über eine Gruppenrichtlinie steuern. Allerdings gilt dies gilt nicht für das Arbeiten unter der

Kommandozeile von Windows. Benutzer müssen auf die Gefahr hingewiesen werden, dass Dateien in Ordnern, die für die Verschlüsselung gekennzeichnet sind, auch unverschlüsselt sein können.

- Die Verschlüsselung einer Datei bietet keine Zugriffskontrolle. Insbesondere können verschlüsselte Dateien durch Dritte gelöscht werden, falls die Zugriffsrechte dies erlauben. Neben der Verschlüsselung einer Datei müssen daher auch entsprechende Einstellungen für die Zugriffskontrolle vorgenommen werden.
- Der zentral gesteuerte Einsatz von EFS wird durch die Verwendung von Gruppenrichtlinien ermöglicht, die unter anderem zur Definition der Wiederherstellungsagenten eingesetzt werden.
- Damit EFS unter Windows 2000 eingesetzt werden kann, muss immer ein Wiederherstellungsagent definiert sein. Es empfiehlt sich, dafür ein spezielles Konto anzulegen, das ausschließlich für diesen Zweck genutzt wird. Insbesondere sollte dafür kein Administratorkonto verwendet werden, um die Befugnisse des Administrators zu beschränken.
  In Abhängigkeit vom ermittelten Schutzbedarf sollte darüber nachgedacht werden, für die Benutzung des entsprechenden Kontos ein Vier-Augen-Prinzip einzuführen, zum Beispiel durch Passwortteilung.
- Ein unter Windows 2000 mit Mitteln einer leeren Wiederherstellungsrichtlinie durchgesetztes Verschlüsselungsverbot funktioniert ab Windows XP nicht mehr. Das Verschlüsselungsverbot wird unter Windows XP durch das Deaktivieren der Option *Benutzer dürfen das verschlüsselnde Dateisystem benutzen* in den Eigenschaften der Richtlinie *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien öffentlicher Schlüssel* | *Dateisystem wird verschlüsselt* | *Eigenschaften* | *Benutzer dürfen das verschlüsselnde Dateisystem benutzen* erreicht. Ab Windows Vista / Server 2003 kann die Nutzung von EFS unter *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für öffentliche Schlüssel* | *Verschlüsselndes Dateisystem* durch einen Klick mit der rechten Maustaste und Wahl von *Eigenschaften* im dann angezeigten Menü konfiguriert werden.
- Die Nutzung eines separaten Wiederherstellungsagenten bietet keinen vollständigen Schutz vor dem Administrator, da dieser immer das Passwort eines Benutzers zurücksetzen kann, um sich nachfolgend als Benutzer anzumelden und auf dessen verschlüsselte Dateien zuzugreifen. Unter Windows XP gilt dies jedoch nur für Domänenkonten. Wird unter Windows XP das Kennwort für ein lokales Benutzerkonto zurückgesetzt, so wird der Zugriff auf seine verschlüsselten Dateien für alle gesperrt. Um den Verlust der verschlüsselten Daten eines lokalen Benutzers zu vermeiden, bietet Windows XP die sogenannte Kennwortrücksetzungs-Diskette (Password Reset Disk, PRD) an. Die Erstellung einer solchen Kennwortrücksetzungs-Diskette für ein Domänen-Benutzerkonto ist laut Microsoft nicht möglich.
- Der private Schlüssel des Wiederherstellungsagenten sollte vom System gelöscht werden, nachdem er auf ein Speichermedium exportiert worden ist. Das Speichermedium muss an einem sicheren Ort aufbewahrt werden und der Zugriff sollte nach dem Vier-Augen-Prinzip erfolgen. Es empfiehlt sich, eine gesondert und sicher aufbewahrte Sicherungskopie des Schlüssels anzulegen.
- Beim Einsatz von EFS ist es wichtig, alle privaten Schlüssel zu sichern. Hierzu müssen alle Profildaten auf allen Rechnern, das heißt alle Verzeichnisse unterhalb von *Dokumente und Einstellungen/ <Benutzername>*, die auch alle Benutzerschlüssel und Zertifikate enthalten, durch den Backup-Mechanismus erfasst werden.
- Wird EFS ohne serverseitig gespeichertes Benutzerprofil (*roaming profile*) eingesetzt, so werden in Abhängigkeit von unterschiedlichen lokalen Pro-

filen unterschiedliche Schlüssel zum Ver- und Entschlüsseln des FEK benutzt, da diese im Profil eines Benutzers (verschlüsselt) gespeichert werden. Auch in diesem Fall ist es wichtig, alle Schlüssel zu sichern. Insbesondere können verschlüsselte Daten von einem Rechner, die auf Band gesichert wurden, nicht auf einem anderen Rechner wieder eingespielt werden, da eine erfolgreiche Entschlüsselung aufgrund unterschiedlicher Schlüssel nicht möglich ist.

- Der Einsatz einer PKI zum Ausstellen von EFS-Zertifikaten kann in einem Unternehmen oder einer Behörde sinnvoll sein. Insbesondere bei der Verwendung von serverseitig gespeicherten Benutzerprofilen verspricht dies eine einfachere Schlüsselverwaltung und -Sicherung.
- Das Verschlüsseln von Systemdateien (Dateien mit gesetztem Systemattribut) und komprimierten Dateien ist unter Windows XP nicht möglich. Des Weiteren können komprimierte Dateien ab Windows Vista / Server 2003 verschlüsselt werden. Dabei wird die Kompression rückgängig gemacht.
- Die Windows Boot-Datei *autoexec.bat* muss vor Verschlüsselung geschützt werden, indem für Benutzer der Schreibzugriff unterbunden wird. Ansonsten ist eine Denial-of-Service-Attacke möglich.
- Werden verschlüsselte Daten nach der Entschlüsselung mit Programmen, wie einem Texteditor, bearbeitet oder gedruckt, so werden in der Regel temporäre Dateien erzeugt, die Daten im Klartext enthalten. Diese können, je nach Programm, auch nach der Bearbeitung weiter bestehen. Damit ist je nach Speicherort (Temp-Verzeichnisse oder Spool-Bereich) und Zugriffsberechtigung auch ein Zugriff durch unautorisierte Dritte möglich.
- Um eine größere Sicherheit bei der Verarbeitung von EFS-verschlüsselten Dateien zu erreichen, sollte überlegt werden, ob es zweckmäßig ist, auch Verzeichnisse, die typischerweise temporäre Daten enthalten (Temp, Spool), für die Verschlüsselung zu kennzeichnen. Es ist zu berücksichtigen, welche Datenmengen in diesen Verzeichnissen abgelegt werden und welche Programme diese Verzeichnisse nutzen. Bei sehr häufigen Zugriffen auf große Datenmengen kann die Verschlüsselung zu einem Performanceverlust führen. Die Verschlüsselung des Temp-Verzeichnisses kann unter Umständen Probleme bei Updates verursachen.
- Ab Windows Vista/Server 2003 können zur EFS-Verschlüsselung auch die Zertifikate anderer Benutzer eingesetzt werden, um den Zugriff auf die verschlüsselten Daten zu ermöglichen.
- Ab Windows XP wurde die Möglichkeit zur Verschlüsselung von Offlinedateien eingeführt. Der gesamte Speicher für Offlinedateien, der Dateien aller Benutzer enthält, wird mit einem computerspezifischen Schlüssel verschlüsselt. Die Verschlüsselung ist transparent für Benutzer und kann nur von Administratoren aktiviert oder deaktiviert werden. Die Aktivierung erfolgt in den Einstellungen des Windows Explorers oder durch die Definition der entsprechenden Gruppenrichtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Offlinedateien* | *Offlinedateicache verschlüsseln*.
- Mit EFS verschlüsselte Daten werden auf dem Rechner ver- und entschlüsselt, auf dem diese Daten gespeichert sind. Dies bedeutet insbesondere, dass Daten, die auf einem Server verschlüsselt gespeichert werden, beim Zugriff durch einen Client im Klartext über das Netz übertragen werden (SMB-Protokoll). Müssen die Daten in Abhängigkeit vom ermittelten Schutzbedarf auch während der Übertragung geschützt sein, so sind zusätzliche Maßnahmen zur Absicherung der Netzkommunikation erforderlich. Hierfür können zum Beispiel EFS mit WebDAV (Web Digital Authoring and Versioning), SSL oder IPSec verwendet werden, siehe dazu auch M 5.90 *Einsatz von IPSec unter Windows*.
- Windows XP führte mit WebDAV einen neuen Mechanismus zum Arbeiten mit Dateien über das Web-Sharing ein. Wird EFS mit WebDAV verwen-

det, so wird eine lokal verschlüsselte Datei in verschlüsselter Form zum Server übertragen und dort gespeichert. Eine über WebDAV angeforderte Datei wird ebenfalls in verschlüsselter Form vom Server übertragen und lokal entschlüsselt. Somit ist durch die Verwendung von WebDAV eine verschlüsselte Übertragung über das Netz möglich.
- Wird EFS für lokale Benutzerkonten eingesetzt, muss die Registry-Verschlüsselung mittels des Kommandos *syskey* unter Verwendung eines Passwortes erfolgen. Nur so können die lokalen Kontenpasswörter vor dem Zurücksetzen durch "Hacker-Werkzeuge" geschützt werden.
- EFS ist nur bei richtiger Anwendung eine kostengünstige Alternative zur Dateiverschlüsselung mit anderen Werkzeugen. EFS kann beispielsweise auf Laptops eingesetzt werden, um die fehlende physikalische Sicherheit auszugleichen, so dass Daten vor dem unbefugten Zugriff an den Betriebssystemmechanismen vorbei geschützt werden können. Der Einsatz von EFS ist jedoch nicht in jedem Fall zweckmäßig, so dass für den jeweiligen Einsatzzweck entschieden werden muss, ob EFS benutzt werden soll.

Alternativ zu einer Verschlüsselung auf Dateisystemebene vermeidet der Einsatz einer vollständigen Festplattenverschlüsselung die oben beschriebenen Nachteile von EFS. Dies gilt insbesondere für mobile Rechner (siehe M 2.442 *Einsatz von Client-Betriebssytemen ab Windows Vista auf mobilen Systemen*).

Prüffragen:

- Wurden der Ruhezustand (Hibernation Modus) und der hybride Standbymodus bei Verwendung von EFS und Nutzung von Windows Versionen vor Windows Vista und Windows Server 2008 deaktiviert?
- Werden starke Passwörter für die Windows Benutzerkonten erzwungen?
- Sind mit EFS verschlüsselte Dateien zusätzlich durch restriktive Zugriffsrechte geschützt?
- Wurde ein dediziertes Konto für den Wiederherstellungsagenten erzeugt und dessen privater Schlüssel gesichert und aus dem System entfernt?
- Existieren von allen privaten Schlüsseln Datensicherungen?
- Wird die Registry-Verschlüsselung mit Passwort mittels des Tools syskey verwendet, wenn EFS mit lokalen Konten eingesetzt wird?
- Wird verhindert, dass die Windows Boot-Datei autoexec.bat verschlüsselt werden kann?
- Sind alle Windows Benutzer im korrekten Umgang mit EFS geschult?
- Ist der Einsatz von EFS ausreichend zur Erfüllung der betrieblichen Anforderungen an die Vertraulichkeit?

# M 4.148 Überwachung eines Windows 2000/XP Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Revisor

Die Überwachung von Rechnersystemen ist ein wichtiges Mittel zur Aufrechterhaltung der Systemsicherheit und Systemintegrität. Nur so können mögliche Sicherheitslücken, Verstöße gegen die geltenden Sicherheitsrichtlinien oder gar Angriffe durch Außen- und Innentäter entdeckt und geeignete Gegenmaßnahmen eingeleitet werden.

Die Überwachung eines Windows 2000/XP Systems muss schon in der Planungsphase berücksichtigt werden, damit die relevanten Parameter entsprechend den Anforderungen festgelegt werden können. Damit unter Windows 2000/XP eine Überwachung erfolgen kann, muss diese zunächst generell aktiviert werden. Dies gilt insbesondere für die Datei- und Registry-Überwachung. Die Aktivierung und die Konfiguration der Überwachungskomponenten erfolgt dabei über folgende Gruppenrichtlinienparameter:

**Allgemeine Aktivierung der Überwachungsfunktionen:**

Es können jeweils die Werte *Keine Überwachung* oder *Erfolgreich* und/oder *Fehlgeschlagen* eingestellt werden.

| **Computer Richtlinien / Lokale Richtlinien / Überwachungsrichtlinien** | |
|---|---|
| **Parameter** | **Empfehlung** |
| Prozessverfolgung überwachen | Die Prozessverfolgung ist im allgemeinen nicht sinnvoll und sollte nur für Debugging-Zwecke aktiviert werden. |
| Rechteverwendung überwachen | Die Verwendung von Benutzerrechten sollte überwacht werden. |
| Richtlinienänderungen überwachen | Das Verändern von Richtlinieneinstellungen (GPOs) ist eine sicherheitskritische Operation und sollte überwacht werden. |
| Systemereignisse überwachen | Aktiviert die Protokollierung der Boot-Ereignisse. |
| Anmeldeereignisse überwachen | Die Protokollierung der Anmeldeereignisse auf dem lokalen Rechner (z. B. Arbeitsplatzrechner) sollte aktiviert sein. |
| Anmeldeversuche überwachen | Die Protokollierung der Anmeldeversuche auf dem Domänen-Controller, der die Authentisierung des Benutzers durchführt, sollte aktiviert sein. |
| Kontenverwaltung überwachen | Änderungen in den Konteneinstellungen sind sicherheitskritische Ereignisse und sollten überwacht werden. |
| Objektzugriff überwachen | Diese Option sollte aktiviert werden, da hierdurch die Protokollierung von |

| | |
|---|---|
| **Computer Richtlinien / Lokale Richtlinien / Überwachungsrichtlinien** | |
| | Datei- und Registry-Zugriffen möglich wird. |
| Active Directory Zugriff überwachen | Dies ist nur auf Domänen-Controllern relevant. Änderungen am AD sollten überwacht werden. |

Tabelle: Computer-, Lokale-, Überwachungsrichtlinien

**Einstellungen für die Protokolldateien:**

| **1. Computer Richtlinien / Lokale Richtlinien / Zuweisen von Benutzerrechten** | |
|---|---|
| **Parameter** | **Empfehlung** |
| Verwalten von Überwachungs- und Sicherheitsprotokollen | Dieses Recht ermöglicht<br>- die Konfiguration der Audit-Einstellungen für die einzelnen Objekte (Dateien, Registry, Active Directory),<br>- das Ansehen bzw. Löschen des Sicherheitsprotokolls.<br>Welcher Benutzergruppe (bzw. -gruppen) dieses Recht eingeräumt wird, hängt vom Überwachungskonzept ab. Prinzipiell sollte dieses Recht restriktiv vergeben werden. Es sollte dabei jedoch beachtet werden, dass<br>- auch zur Diagnose und Behebung von nicht sicherheitsrelevanten Problemen der Zugriff auf das Sicherheitsprotokoll notwendig sein kann,<br>- Administratoren sich dieses Benutzerrecht auch selbst einräumen können, wenn es ihnen entzogen wird. Es empfiehlt sich daher, diesen Vorgang zu protokollieren (Option *Rechteverwendung überwachen*). |
| **2. Computer Richtlinien / Lokale Richtlinien / Ereignisprotokoll** | |
| - Aufbewahrungsmethode des Anwendungsprotokolls<br>- Aufbewahrungsmethode des Sicherheitsprotokolls<br>- Aufbewahrungsmethode des Systemprotokolls | Je nach Protokollierungskonzept kann gewählt werden zwischen<br>*Nach ... Tagen*,<br>*Überschreiben* und<br>*Nicht überschreiben*. |
| - Anwendungsprotokoll aufbewahren für | Anzahl der Tage, wenn die Aufbewahrungsmethode *Nach ... Tagen* gewählt wurde. |

| **1. Computer Richtlinien / Lokale Richtlinien / Zuweisen von Benutzerrechten** | |
|---|---|
| - Sicherheitsprotokoll aufbewahren für<br>- Systemprotokoll aufbewahren für | |
| Windows 2000:<br><br>- Gastkontozugriff auf Anwendungsprotokoll einschränke<br>- Gastkontozugriff auf Sicherheitsprotokoll einschränke<br>- Gastkontozugriff auf Systemprotokoll einschränken<br><br>Windows XP:<br><br>- Lokalen Gastkontozugriff auf Anwendungsprotokoll verhindern<br>- Lokalen Gastkontozugriff auf Sicherheitsprotokoll verhindern<br>- Lokalen Gastkontozugriff auf Systemprotokoll verhindern | Die Zugriffsbeschränkung für das Gastkonto sollte aktiviert werden. |
| - Maximale Größe des Anwendungsprotokolls<br>- Maximale Größe des Sicherheitsprotokolls<br>- Maximale Größe des Systemprotokolls | Die Größe muss so gewählt werden, dass je nach Aufbewahrungsmethode auch bei überdurchschnittlicher Systemaktivität genügend Platz zur Verfügung steht.<br>Dies ist besonders wichtig für das Sicherheitsprotokoll, da sonst eine zeitliche Lücke in der Sicherheitsüberwachung des Systems entstehen kann.<br>Vorschläge für die hier vorzunehmenden Einstellungen finden sich in M 2.231 *Planung der Gruppenrichtlinien unter Windows* bzw. M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*. Diese müssen jedoch den realen Bedingungen (Tests im Probebetrieb) angepasst werden. |
| Windows 2000:<br>System bei Erreichen der max. Sicherheitsprotokollgröße herunterfahren | Im Normalbetrieb ist dies mit Vorsicht zu behandeln. Diese Option ist jedoch in Hochsicherheitsbereichen sinnvoll, wenn Nachweisführung vor Verfügbarkeit geht. In jedem Fall muss der Einsatz genau abgewogen werden. |

Tabelle: Einstellungen für Protokolldateien

Im Rahmen der Überwachung sind allgemein auch folgende Aspekte zu berücksichtigen:

- Der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat sollten frühzeitig in die Planung mit einbezogen werden, da bei einer Überwachung meist auch personenbezogene Daten erfasst werden, um im Fal-

le einer Sicherheitsverletzung zuverlässig den Verursacher feststellen zu können.
- Damit die Überwachungskomponenten Protokolleinträge generieren, muss die Überwachung über die relevanten Gruppenrichtlinieneinstellungen aktiviert werden.
- Windows 2000/XP stellt zur Überwachung lediglich eine Protokoll-Funktionalität zur Verfügung: Systemkomponenten und Applikationen erzeugen Statusmeldungen, die in drei Protokolldateien (System-, Applikations- und Sicherheitslog) gesammelt werden. Eine dedizierte Auditing-Architektur zur Online-Überwachung existiert nicht. Die Protokolldateien werden jeweils lokal gespeichert und müssen im Wesentlichen von Hand ausgewertet werden.
- Der Aufbau einer zentralen Sammelstelle von Protokolldateien mit entsprechend automatisierter Auswertung kann durch Produkte von Drittherstellern erreicht werden. Wird ein Werkzeug zum Netz- und Systemmanagement eingesetzt (siehe auch Baustein B 4.2 *Netz- und Systemmanagement*), so ist es - je nach Produkt - möglich, die Windows 2000/XP Protokolle direkt in dieses Werkzeug zu importieren.
- Über die Windows 2000/XP Auditing-Einstellungen können Zugriffe auf Dateien oder Registry-Schlüssel im Sicherheitsprotokoll aufgezeichnet werden.
- Durch die Überwachung fallen je nach Einstellung große Datenmengen an. Zusätzlich führt eine intensive Überwachung zu Performanceverlusten. Dadurch kann im Extremfall ein System so überlastet werden, dass ein geregelter Betrieb nicht mehr möglich ist. Aus diesem Grund müssen die geeigneten Überwachungsparameter im Rahmen eines Testbetriebes überprüft und gegebenenfalls angepasst werden. Es ist zu beachten, dass die Anpassung auch Einfluss auf das gesamte Überwachungskonzept haben kann, da bestimmte Überwachungsaufgaben nicht mehr durchführbar sind. Dies gilt insbesondere dann, wenn zusätzliche Produkte eingesetzt werden, die hohe Anforderungen an die protokollierten Ereignisse stellen. Dies sind z. B. Programme, die eine automatische Analyse der Protokolldaten auf Verhaltensanomalien, etwa für die Erkennung von Angriffen, durchführen.

Im Rahmen der Überwachung von Systemfunktionen empfiehlt sich auch die regelmäßige Kontrolle der AD-Replikation, durch die Konfigurationsänderungen weitergereicht werden. Dazu können einerseits AD-Werkzeuge, wie *repadmin.exe* oder *showreps.exe*, genutzt werden, andererseits sollten das ADS-Log (Active Directory Service) und das FRS-Log (File Replication Service) auf Fehlermeldungen hin überprüft werden. Fehler in der Replikation haben meist zur Folge, dass Konfigurationsänderungen nicht überall durchgeführt werden. Dadurch besteht die Gefahr, dass einem Benutzer ungeeignete oder zu viele Rechte zugestanden werden.

Die Systemzeit spielt eine wichtige Rolle bei der Systemüberwachung und der Auswertung protokollierter Daten. Insbesondere wenn mehrere Systeme überwacht werden, sollte die Systemzeit auf allen Rechnern synchronisiert werden. Windows 2000 führte den Zeitdienst *W32Time* (Windows-Zeitgeber) ein. Dieser Dienst ist für die Zeitsynchronisierung verantwortlich.

In einer Active Directory-Umgebung ist der autorisierende Domain Controller der Zeitgeber für die Domänenmitglieder. Der Windows Zeitdienst ist hierarchisch aufgebaut: Der Domain Controller der Stammdomäne (Root Domain), der die PDCE FSMO Rolle innehat, wird zum zentralen Zeitgeber für die gesamte Active Directory-Infrastruktur. Der Domain Controller kann mit dem Kommando net time /setsntp:<zeitquelle> so konfiguriert werden, dass er eine externe Zeitquelle zum Synchronisieren verwendet. Die Zeitquelle kann sich

innerhalb oder außerhalb des eigenen Netzes befinden, wobei eine interne Zeitquelle bevorzugt eingesetzt werden sollte. Wird eine Zeitquelle außerhalb des eigenen Netzes verwendet, muss ihre Vertrauenswürdigkeit sichergestellt sein.

Client-Rechner, die keine Domänenmitglieder sind, benutzen standardmäßig den Microsoft Zeitserver *time.windows.com*. Sie können aber auch mit dem Kommando *net time* oder über die Registrierung (*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers*) so konfiguriert werden, dass sie eine andere Zeitquelle verwenden.

Prüffragen:

- Wurde ein bedarfsgerechtes Überwachungskonzept für Windows entworfen und umgesetzt?
- Entsprechen die Parameter zur Systemüberwachung den Anforderungen der Institution?
- Deckt sich die geforderte Konfiguration der Überwachungskomponenten unter Windows mit den eingesetzten Gruppenrichtlinienparametern?
- Decken sich die vergebenen Rechte zur Verwaltung der Überwachungs- und Sicherheitsprotokolle mit den Sicherheitsrichtlinien der Institution?
- Werden der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat in die Planung einer Überwachung mit einbezogen?
- Ist eine regelmäßige Synchronisation der Systemzeit gewährleistet?

# M 4.149 Datei- und Freigabeberechtigungen unter Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Windows-Betriebssysteme mit NT-Kern nutzen das Dateisystem NTFS. Die Mechanismen zur Zugriffssteuerung unterscheiden sich dabei kaum. Die folgende Tabelle gibt einen Überblick der möglichen Zugriffsrechte auf Dateien. Diese erlauben ab Windows XP eine wesentlich detailliertere Konfiguration, als es bei den Vorversionen möglich ist.

| **Zugriffsrechte für Ordner** | **Zugriffsrechte für Dateien** |
|---|---|
| Ordner durchsuchen | Dateien ausführen |
| Ordner auflisten | Daten lesen |
| Attribute lesen | Attribute lesen |
| Erweiterte Attribute lesen | Erweiterte Attribute lesen |
| Dateien erstellen | Datienen schreiben |
| Ordner erstellen | Daten anhängen |
| Attribute schreiben | Attribute schreiben |
| Erwiterte Attribute schreiben | Erweiterte Attribute schreiben |
| Unterordner und Dateien löschen | |
| Löschen | Löschen |
| Besitz übernehmen (vor Windows 7 ist diese Einstellung mit "Besitzrechte übernehmen" betitelt) | Besitz übernehmen (vor Windows 7 ist diese Einstellung mit "Besitzrechte übernehmen" betitelt) |

Tabelle: Überblick der Zugriffsrechte für Ordner und Dateien

Die Zugriffsrechte können auf Dateien oder Ordner angewandt werden. Im Rahmen der Rechtevererbung ist es möglich, dass Rechte eines Ordners an Dateien und/oder Unterordner weitergereicht werden, sodass eine einfache Möglichkeit besteht, die Zugriffsberechtigungen in einem ganzen Teildateibaum durch die Änderung an einer Stelle zu wechseln. Das Vererben an die Objekte in einem Verzeichnis kann gezielt durch folgende sieben Einstellungen kontrolliert werden, die angeben, auf welche Objekte die Zugriffsrechte vererbt werden sollen:

- Nur diesen Ordner
- Diesen Ordner, Unterordner und Dateien
- Diesen Ordner, Unterordner
- Diesen Ordner, Dateien
- Nur Unterordner und Dateien
- Nur Unterordner
- Nur Dateien

Durch die Option *Berechtigungen nur für Objekte und/oder Container in diesem Container übernehmen* kann zudem erreicht werden, dass die Rechte nicht rekursiv in den jeweiligen Unterbaum weitervererbt werden, sondern nur auf die Objekte im aktuellen Verzeichnis.

Zur Steuerung der Rechteübernahme auf Objekte beim Einsatz des Vererbungsmechanismus stehen zwei weitere Optionen zur Verfügung:

| **Funktion** | **Erlauben oder Blockieren der Vererbung für untergeordnete Objekte** |
|---|---|
| Windows XP | Berechtigung übergeordneter Objekte auf untergeordnete Objekte, sofern anwendbar, vererben |
| Windows Vista / Windows 7 | Alle Berechtigungseinträge für untergeordnete Objekte durch vererbbare Berechtigungseinträge von diesem Objekt ersetzen |
| Windows 8 | Vererbung aktivieren |

| **Funktion** | **Erzwingen der Vererbung von Berechtigungen auf untergeordnete Objekte** |
|---|---|
| Windows XP | Berechtigungen für alle untergeordneten Objekte durch die angezeigten Einträge, sofern anwendbar, ersetzen |
| Windows Vista / Windows 7 | Alle Berechtigungen für untergeordnete Objekte durch vererbbare Berechtigungen von diesem Objekt ersetzen |
| Windows 8 | Alle Berechtigungseinträge für untergeordnete Objekte durch vererbbare Berechtigungseinträge von diesem Objekt ersetzen |

Stehen die beiden Rechte in Konflikt miteinander, so wird die erzwungene Übernahme der vererbten Rechte durchgesetzt.

Ab Windows XP sind die *Zugriffseinstellungen für [Ordner- oder Dateiname]* in *Erweiterte Sicherheitseinstellungen für [Ordner- oder Dateiname]* umbenannt und um die Registerkarten *Überwachung* und *Effektive Berechtigungen* erweitert worden.

Die Überwachung des Zugriffs auf Objekte, wie Dateien und Ordner lässt sich ab Windows XP über die Registerkarte *Überwachung* konfigurieren. Hierbei ist es beispielsweise möglich, fehlerhafte Zugriffe auf einen Ordner zu überwachen. Diese Zugriffsüberwachung kann an alle, im Ordner enthaltenen Ordner und Dateien, vererbt werden.

Die Überprüfung der Rechte eines Benutzers erfolgt ab Windows XP mittels der Registerkarte *Effektive Berechtigungen*, deren Bezeichnung ab Windows 8 in *Effektiver Zugriff* geändert wurde. Es kann für jede Datei und jeden Ordner überprüft werden, welche effektiven Berechtigungen ein Anwender oder eine Gruppe haben. Diese effektiven Berechtigungen können aufgrund von Vererbung oder Zugehörigkeit eines Benutzers zu verschiedenen Gruppen unterschiedlich sein.

Diese Fülle an unterschiedlichen Dateiberechtigungen im Zusammenspiel mit den unterschiedlichen Vererbungsmechanismen macht die Verwaltung von

Zugriffsrechten für den Benutzer unübersichtlich. Im Normalfall empfiehlt sich daher, nur die zusammengesetzten Standardzugriffsrechte zu verwenden:

| **Ordner** | **Dateien** | **entspricht** |
|---|---|---|
| Vollzugriff | Vollzugriff | alle Einzelberechtigungen |
| Ändern | Ändern | Lesen, Ausführen ergänzt um Schreiben und Löschen |
| Lesen, Ausführen | Lesen, Ausführen | Lesen ergänzt um Datei ausführen |
| Ordnerinhalt auflisten | - | Lesen ergänzt um Ordner durchsuchen |
| Lesen | Lesen | Daten lesen, Attribute lesen, erweiterte Attribute lesen, Berechtigungen lesen |
| Schreiben | Schreiben | Daten schreiben, Daten anhängen, Attribute schreiben, erweiterte Attribute schreiben |

Tabelle: Standardzugriffsrechte

Im Rahmen der Planung des Windows Einsatzes ist auch das Berechtigungs- und Zugriffskonzept für Dateien und Ordner zu entwerfen, durch das die detaillierten Zugriffsrechte festgelegt werden. Dabei sind die organisatorischen und geschäftlichen Anforderungen zu berücksichtigen. Generell empfiehlt es sich, für die Windows-Systemdateien restriktive Rechte zu vergeben.

Als Ausgangskonfiguration für Clients ab Windows XP können die folgenden Berechtigungsvorgaben genutzt werden, die auf jeden Fall an die lokalen Gegebenheiten angepasst werden müssen. Die vorgeschlagenen Einstellungen gehen davon aus, dass die Benutzerkennung *Hauptbenutzer* (*Power-User*) nicht verwendet wird, da administrative Belange durch Administratoren mit entsprechenden Berechtigungen im Rahmen des Administrationskonzeptes abgedeckt werden. Aus diesem Grund ist die Kennung *Hauptbenutzer* aus allen Zugriffslisten zu entfernen. Zusätzlich empfiehlt sich im Rahmen des Administrationskonzeptes eine Gewaltenteilung, so dass die administrativen Berechtigungen auf entsprechende Konten aufgeteilt werden. Im Folgenden wird jedoch davon ausgegangen, dass die Gruppe *Administratoren* die gesamte administrative Gewalt hat. Die Berechtigungen gelten nur für die angegebenen Verzeichnisse oder Dateien und sind nicht für die Vererbung gedacht.

| **Verzeichnis** | **Rechte** |
|---|---|
| Stammverzeichnis der Systempartition | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt auflisten; Lesen |
| \WINDOWS | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>ERSTELLER-BESITZER: Spezielle Berechtigungen |

| Verzeichnis | Rechte |
|---|---|
| | Benutzer: Lesen, Ausführen; Ordnerinhalt auflisten; Lesen |
| WINDOWS\REPAIR | Administratoren: Vollzugriff |
| WINDOWS\SYSTEM32\CONFIG | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Ordnerinhalt auflisten |
| WINDOWS\SYSTEM32\SPOOL | Administratoren:Vollzugriff<br>SYSTEM: Vollzugriff<br>ERSTELLER-BESITZER: Spezielle Berechtigungen<br>Benutzer: Lesen, Ausführen; Ordnerinhalt auflisten; Lesen |

Tabelle: Berechtigungsvorgaben für Verzeichnisse unter Windows XP

| Verzeichnis / Datei | Rechte |
|---|---|
| boot.inintldr | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff |
| autoexex.batconfig.sys | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen |
| \WINDOWS\Temp | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: spezielle Berechtigungen |
| PROGRAMME | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt auflisten; Lesen |
| Dokumente und Einstellungen | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt auflisten; Lesen |

Tabelle: Berechtigungsvorgaben für Dateien unter Windows XP

Die Berechtigungsvorgaben für Verzeichnisse für Clients ab Windows Vista dokumentiert folgende Tabelle:

| Verzeichnis | Rechte |
|---|---|
| Stammverzeichnis der Systempartition | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt auflisten; Lesen |
| \WINDOWS | Administratoren: spezielle Berechtigungen Ordner durchsuchen / Dateien asuführen, Ordner auflisten / Dateien lesen, Attribute lesen, Erweiterte Attribute lesen, Dateien erstellen / Dateien schreiben, Ordner erstellen / Daten anhängen, Attribute schreiben / Erweiterte Attribute schreiben, Löschen, Berechtigungen |

| Verzeichnis | Rechte |
|---|---|
| | lesen Auf die Unterordner haben Administratoren Vollzugriff<br>SYSTEM: wie Administratoren<br>Benutzer: Lesen, Ausführen; Ordnerinhalt anzeigen; Lesen<br>TrustedInstaller: Ordnerinhalt anzeigen |
| WINDOWS\SYSTEM32\CONFIG | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt anzeigen; Lesen<br>ERSTELLER-BESITZER: Vollzugriff<br>TrustedInstaller: Ordnerinhalt anzeigen |
| WINDOWS\SYSTEM32\SPOOL | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt anzeigen; Lesen<br>ERSTELLER-BESITZER: Vollzugriff<br>TrustedInstaller: Ordnerinhalt anzeigen |

Tabelle: Berechtigungsvorgaben für Verzeichnisse für Clients ab Windows Vista

In obiger Tabelle wird der *TrustedInstaller* erwähnt, siehe dazu M 4.341 *Integritätsschutz ab Windows Vista* im Abschnitt Windows Ressource Protection und TrustedInstaller für weitergehende Hinweise.

Die Berechtigungsvorgaben für Dateien von Clients ab Windows Vista dokumentiert folgende Tabelle:

| Verzeichnis / Datei | Rechte |
|---|---|
| Bootmgr BCD | SYSTEM: lesen, ausführen<br>Administratoren: lesen, ausführen<br>TrustedInstaller: Vollzugriff |
| autoexec.batconfig.sys | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen<br>TrustedInstaller: Vollzugriff |
| TEMP | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Spezielle Berechtigungen |
| PROGRAMME | Administratoren: spezielle Berechtigungen Ordner durchsuchen / Dateien asuführen, Ordner auflisten / Dateien lesen, Attribute lesen, Erweiterte Attribute lesen, Dateien erstellen / Dateien schreiben, Ordner erstellen / Daten anhängen, Attribute schreiben / Erweiterte Attribute schreiben, Löschen, Berechtigungen |

| Verzeichnis / Datei | Rechte |
|---|---|
| | lesen Auf die Unterordner haben Administratoren Vollzugriff<br>SYSTEM: wie Administratoren<br>Benutzer: Lesen, Ausführen; Ordnerinhalt anzeigen; Lesen<br>TrustedInstaller: Ordnerinhalt anzeigen |
| Benutzer | Administratoren: Vollzugriff<br>SYSTEM: Vollzugriff<br>Benutzer: Lesen, Ausführen; Ordnerinhalt anzeigen; Lesen |

Tabelle: Berechtigungsvorgaben für Dateien von Clients ab Windows Vista

**Freigabe für den Netzzugriff**

Windows erlaubt es, Verzeichnisse und die darin enthaltenen Dateien über eine Freigabe für den Netzzugriff zur Verfügung zu stellen. Dabei erfolgt die Zugriffskontrolle zweistufig. Es können Zugriffsberechtigungen für die Netzfreigabe selbst eingerichtet werden. Sie bestimmen, wer generell auf die Netzfreigabe zugreifen darf.

Sind die Benutzer für die Berechtigungsvergabe beispielsweise auf eigene oder Projektdateien zuständig, so müssen sie entsprechend geschult werden. Anderenfalls können unsichere Dateizugriffsrechte unter Umständen zur Kompromittierung eines Einzelsystems oder, im schlimmsten Fall, zur Kompromittierung des Informationsverbundes führen.

Eine Berechtigungsvergabe an die vorkonfigurierte Benutzergruppe *Jeder* (insbesondere *Vollzugriff*, *Schreiben/Ändern*) sollte grundsätzlich vermieden werden. Soll der Zugriff für alle Benutzer möglich sein, empfiehlt sich stattdessen die Verwendung der ebenfalls vorkonfigurierten Gruppe *Authentifizierte Benutzer*. Weiterhin wirken die oben beschriebenen, auf Dateisystemebene angegebenen Zugriffsrechte auf Dateien und Verzeichnisse. Berechtigungen auf Netzfreigaben können nur über die Rechte:

- Vollzugriff,
- Ändern und
- Lesen

gesteuert werden. Eine feinere Kontrolle ist jedoch an dieser Stelle nicht notwendig.

Um Datei-, Verzeichnis- und Freigabeberechtigungen festzulegen, sollten folgende Regeln beachtet werden:

- Freigaben auf Arbeitsplatzrechnern sind zu vermeiden.
- Freigaben auf Domänen-Controllern sind ebenfalls zu vermeiden, da Domänen-Controller sensitive Daten speichern.
- Alle nicht vermeidbaren Freigaben auf Arbeitsplatzrechnern und Domänen-Controllern sind zu begründen und zu dokumentieren und sollten nur nach einer vorherigen Risikoabwägung erfolgen.
- Für alle Freigaben und die dadurch zugreifbaren Daten müssen die Zugriffsberechtigungen so restriktiv wie möglich vergeben werden.
- Es sollte überlegt werden, das Benutzerkonto *Jeder* zu entfernen und stattdessen das Benutzerkonto *Authentifizierte Benutzer* zu verwenden.
- Das Zugriffskonzept muss dokumentiert sein.

Prüffragen:

- Wurde ein bedarfsgerechtes Berechtigungs- und Zugriffskonzept für Windows erstellt?
- Sind die Berechtigungen aller Verzeichnisse und Dateien auf allen, von einem älteren Windows-Betriebssystem aktualisierten, Rechnern überprüft worden?
- Sind die eingestellten Datei- und Verzeichnisberechtigungen von freigegebenen Verzeichnissen für den Netzzugriff geeignet? Wurden die Freigaben so restriktiv wie möglich vergeben?

# M 4.150 Konfiguration von Windows 2000 als Workstation

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 4.151 Sichere Installation von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Installation des Internet-PC müssen eine Reihe von Entscheidungen getroffen werden, die Auswirkungen auf die IT-Sicherheit des Systems haben.

**Hardware**

Die Hardware des Internet-PCs ist so zu konfektionieren, dass nur die im Einsatzkonzept vorgesehenen Komponenten vorhanden sind. Gegebenenfalls müssen nicht vorgesehene Laufwerke oder Schnittstellen, z. B. Diskettenlaufwerke oder interne Modems, entfernt oder deaktiviert werden (siehe auch M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).

Die Boot-Reihenfolge sollte im System-BIOS so eingestellt werden, dass der Computer nur vom Datenträger mit dem vorgesehenen Betriebssystem startet Soll das IT-System beispielsweise von einer nicht wiederbeschreibbaren CD- oder DVD-ROM gestartet werden, sollte *CD-ROM Drive* eingestellt werden. Befindet sich das Betriebssystem auf der Festplatte "C", sollte *C: A:*, *C only* oder *Harddisk first/only* gewählt werden.

Der Zugang zum System-BIOS sollte durch ein Passwort geschützt werden. Falls ein Betriebssystem ohne zwingende Benutzer-Authentisierung eingesetzt wird, z. B. Windows 9x/ME, kann darüber nachgedacht werden, auch ein Boot-Passwort im BIOS zu aktivieren. Dies bietet einen gewissen Schutz vor Missbrauch durch Gelegenheitstäter.

**Betriebssystem**

Im Anschluss an die Installation der Hardware wird das im Einsatzkonzept vorgesehene Betriebssystem installiert. Zu beachten ist dabei, dass gängige Betriebssysteme unterschiedliche Sicherheitsfunktionen bieten. Windows NT-basierte Betriebssysteme und Linux verfügen beispielsweise über eine wirksame Benutzertrennung und Zugriffsrechte. Diese Funktionen stehen bei Windows 9x/ME nur ansatzweise oder gar nicht zur Verfügung, sind jedoch wichtig für die Trennung von Administrator- und Benutzerbereichen.

Grundsätzlich sollten nur die Betriebssystem-Komponenten installiert werden, die auch wirklich für den festgelegten Einsatzbereich benötigt werden. Besonders kritisch zu prüfen sind hierbei "Dienste" (Windows) bzw. "Daemons" (Linux). Ein Internet-PC sollte in der Regel keine Dienste im Internet anbieten (siehe auch M 5.72 *Deaktivieren nicht benötigter Netzdienste*).

Nach der Installation des Betriebssystems müssen alle evtl. vergebenen Standardpasswörter geändert werden. Unter Linux betrifft dies insbesondere das *root*-Passwort, sofern die verwendete Distribution hierfür ein Standardpasswort vergibt.

Vor der Inbetriebnahme müssen alle aktuellen sicherheitsrelevanten Patches bzw. Updates eingespielt werden. Für Windows-Betriebssysteme sind entsprechende Informationen auf den WWW-Seiten der Firma Microsoft (*www.microsoft.com*) erhältlich. Falls Linux eingesetzt wird, sollte zunächst beim Hersteller der verwendeten Distribution nach verfügbaren Patches und

Updates gesucht werden. Falls das Angebot des Herstellers unzureichend ist, sollten weitere Quellen hinzugezogen werden, z. B. *www.linuxdoc.org*.

Weitere Empfehlungen hierzu finden sich in M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* und M 4.107 *Nutzung von Hersteller- und Entwickler-Ressourcen*.

Für Windows-Betriebssysteme gelten darüber hinaus folgende Empfehlungen:

- Das jeweils aktuelle Service Pack sollte eingespielt werden.
- Als einziges Netzprotokoll sollte TCP/IP installiert werden.
- An das TCP/IP-Protokoll für den Internet-Zugang sollten keine Dienste gebunden werden.
- Die Datei- und Druckerfreigabe sollte deaktiviert werden. Es sollten keine *Shares* zur Verfügung gestellt werden.
- Bei Verwendung des Internet Explorers sollte unter *Extras* | *Internetoptionen* | *Verbindungen* die Funktion *Vor dem Wählen Systemsicherheit prüfen* aktiviert werden, falls diese Option angeboten wird.
- Der Windows Scripting Host (WSH) sollte deinstalliert werden, wenn dies bei der verwendeten Konfiguration möglich ist. Anderenfalls sollten die dem WSH zugeordneten Dateitypen, beispielsweise *.vbs* und *.js*, einem Editor zugewiesen werden.
- Der Microsoft Personal Web Server sollte deaktiviert, möglichst sogar deinstalliert werden.
- Die automatische CD-ROM-Erkennung sollte deaktiviert werden (siehe auch M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*).
- Falls die verwendete Windows-Version eine Benutzertrennung unterstützt, sollten alle nicht benötigten Benutzerkonten, z. B. *Gast*, deaktiviert oder gelöscht werden. Unter Windows NT kann dies über den *Benutzer-Manager* erfolgen. Das *Administrator*-Konto sollte umbenannt und mit einem starken Passwort geschützt werden.
- Beim Einsatz von Windows 9x/ME kann darüber nachgedacht werden, einen passwortgeschützten Bildschirmschoner zu verwenden. Dies bietet einen gewissen Schutz gegen unberechtigte Zugriffe.
- Als Standardvorgang beim Doppelklick auf eine Datei vom Typ *.reg* sollte *Bearbeiten* (mit Editor öffnen) und nicht *Zusammenführen* eingestellt werden. Unter Windows ME kann das entsprechende Dialogfeld über den Explorer via *Extras* | *Ordneroptionen* | *Dateitypen* erreicht werden.
- Es sollte geprüft werden, ob anstelle der Standardnamen für System- und Datenverzeichnisse bzw. -dateien abweichende Pfadnamen verwendet werden können. Schadprogramme suchen in vielen Fällen nach bestimmten Dateien in Standardverzeichnissen, so dass durch diese Änderung ggf. ein zusätzlicher Schutz erreicht werden kann. Es ist jedoch zu berücksichtigen, dass dies zu Inkompatibilitäten mit bestimmten Programmen führen kann.

Bei der Verwendung von Linux sollten folgende Empfehlungen berücksichtigt werden:

- Der Daemon *inetd* sollte nicht gestartet werden. Je nach Distribution wird dies über Änderungen an den rc-Startdateien oder über spezielle Administrationstools konfiguriert.
- Der *Portmap Daemon* und der *Name Service Caching Daemon* sollten nicht gestartet werden.
- Falls die verwendete Distribution spezielle Dienste zur Fernadministration installiert, z. B. *linuxconf* oder *swat*, so sollten diese deaktiviert werden.
- *Apache* oder andere WWW-Server-Software sollte deinstalliert werden.

- Das Programm *sendmail* sollte nicht im Server-Modus gestartet werden. Auch andere Daemons für den Empfang von E-Mail über das Protokoll SMTP sollten deinstalliert oder zumindest deaktiviert werden. Sofern benötigt, sollte E-Mail stattdessen via POP3 oder IMAP abgeholt werden.
- Als zusätzliche Sicherheitsmaßnahme gegen Angriffe aus dem Internet kann die Paketfilterfunktion *ipchains* bzw. *iptables* von Linux eingesetzt werden. Einige Distributionen enthalten hierfür vorkonfigurierte Pakete.

Als zusätzliche Sicherheitsmaßnahme kann eine so genannte *Personal Firewall* installiert werden. Damit diese auch wirksam ist, muss sie sorgfältig für den jeweiligen Einsatzzweck konfiguriert werden. Insbesondere muss das Programm so eingestellt werden, dass die Benutzer nicht mit einer Vielzahl von Warnmeldungen belästigt werden, die sie nicht interpretieren können. Weitere Empfehlungen finden sich in M 5.91 *Einsatz von Personal Firewalls für Clients* .

**Client-Programme**

Neben dem eigentlichen Betriebssystem sollten auf dem Internet-PC nur die zusätzlichen Programme installiert werden, die für die Nutzung der im Einsatzkonzept festgelegten Internet-Dienste erforderlich sind.

Falls die Nutzung des World Wide Web im Einsatzkonzept vorgesehen ist, muss ein WWW-Browser installiert werden. Gängige Browser-Programme sind der *Internet Explorer*, *Firefox*, *Chrome*, *Safari* und *Opera*. Empfehlungen zur sicheren Konfiguration dieser Browser finden sich der Maßnahme M 5.93 *Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs*.

Falls vom Internet-PC aus E-Mails gesendet oder empfangen werden sollen, muss entweder ein E-Mail-Client installiert werden oder es muss auf einen WWW-basierten E-Mail-Dienst (z. B. GMX oder Web.de) zurückgegriffen werden. Gängige E-Mail-Clients sind *Outlook, Outlook Express, Thunderbird* oder *KMail*. Empfehlungen zur sicheren Konfiguration dieser Programme finden sich in der Maßnahme M 5.94 *Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs*.

Falls im Einsatzkonzept vorgesehen ist, weitere Internet-Dienste zu nutzen, z. B. Internettelefonie oder Instant Messaging, müssen unter Umständen weitere Client-Programme installiert werden.

Alle Programme sollten so konfiguriert werden, dass sie optimale Sicherheit bieten, und die Benutzer sollten in deren sichere Nutzung eingewiesen werden.

**Tools**

Im Hinblick auf den sicheren Betrieb eines Internet-PCs müssen in der Regel zusätzliche Tools installiert werden, die nicht Bestandteil des Betriebssystems sind.

Unverzichtbar ist der Einsatz eines Viren-Schutzprogramms auf jedem Internet-PC. Solche Programme sind von verschiedenen Herstellern erhältlich. Wichtig ist, dass die zugehörigen Datenbanken, auf deren Grundlage diese Tools arbeiten, regelmäßig aktualisiert werden. Gängige Viren-Schutz-

programme stellen hierfür spezielle Funktionen zur Verfügung. Dabei ist zu beachten, dass dies nicht zentral gesteuert werden kann, wenn die Internet-PCs nicht untereinander vernetzt sind. Weitere Empfehlungen zum Schutz

vor Schadprogrammen finden sich in M 4.3 *Einsatz von Viren-Schutzprogrammen*.

Zur Datensicherung für einen Internet-PC gibt es unterschiedliche Konzepte (siehe auch M 6.79 *Datensicherung beim Einsatz von Internet-PCs*). In vielen Fällen wird hierfür jedoch ein eigenständiges Tool benötigt, dass das erforderliche Backup automatisch oder halbautomatisch erledigt. Oft lassen sich Datensicherung und Datentransport vom oder ins Hausnetz über das gleiche Medium realisieren. Wichtig ist hierbei eine ordnungsgemäße Verwaltung der eventuell benötigten Datenträger.

Bei der Übertragung über das Internet können Daten unter Umständen mitgelesen oder manipuliert werden. Um diesen Gefährdungen entgegenzuwirken, können kryptographische Verfahren eingesetzt werden. Beispielsweise existieren eine Reihe von Tools, mit denen E-Mails verschlüsselt und signiert werden können. Weiterhin besteht die Möglichkeit, sichere Kanäle zu bekannten Kommunikationspartnern aufzubauen, beispielsweise über so genannte Virtuelle Private Netze (VPNs). Planungshinweise zum Einsatz kryptographischer Verfahren finden sich in Baustein B 1.7 *Kryptokonzept*.

Informationen im Internet werden nicht nur im HTML-Format angeboten, sondern z. B. auch als Word-, Excel-, PowerPoint- oder PDF-Dateien. Wenn solche Dateien direkt auf dem Internet-PC betrachtet werden sollen, müssen hierfür geeignete Viewer-Programme installiert werden. Diese Viewer sollten nach Möglichkeit nicht in der Lage sein, Makro-Befehle auszuführen. Insbesondere sollte nach Möglichkeit kein Office-Paket auf dem Internet-PC installiert werden. Falls dies dennoch zwingend erforderlich ist, sollten alle integrierten Funktionen zum Schutz vor Makro-Viren aktiviert werden.

Für alle installierten Betriebssystem- und Software-Komponenten sollten die jeweils verfügbaren sicherheitsrelevanten Patches bzw. Updates eingespielt werden. Diese sollten aus vertrauenswürdigen Quellen, beispielsweise direkt vom Hersteller, bezogen werden (siehe auch M 4.152 *Sicherer Betrieb von Internet-PCs*).

Nachdem alle Betriebssystem- und Software-Komponenten installiert sind, sollte ein Abbild ("Image") dieser Grundkonfiguration gesichert werden. Dies erlaubt es, das System schnell wiederherzustellen, wenn die Installation durch Abstürze, fehlgeschlagene Konfigurationsänderungen oder Manipulationen unbrauchbar wird (siehe auch M 6.79 *Datensicherung beim Einsatz von Internet-PCs*).

**Surf-CD**

Eine andere Möglichkeit sicher im Internet zu surfen, bietet die Nutzung einer Surf-CD, die alle notwendigen Komponenten enthält, um den Rechner mit der Surf-CD zu starten. So bleibt das eigentliche Betriebssystem des Clients unberührt, da das Betriebssystem auf der CD nicht auf lokale Festplatten zugreifen kann. Solche CDs werden beispielsweise regelmäßig fertig über Computerzeitschriften oder im Internet als Programmpakete angeboten. Solche Surf-CDs enthalten typischerweise nur ein gehärtetes Betriebssystem und die für die Internetnutzung absolut notwendigen Programme, um potentielle Sicherheitslücken zu minimieren.

Prüffragen:

- Werden bei der Installation von Internet-PCs alle erforderlichen Sicherheitsaspekte strikt umgesetzt?

- Wurden alle nicht benötigten Laufwerke, Schnittstellen, Dienste und Programme bei Internet-PCs deaktiviert?
- Sind auf allen Internet-PCs ein aktuelles Viren-Schutzprogramm und eine Personal Firewall installiert?

# M 4.152 Sicherer Betrieb von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um den sicheren Betrieb eines Internet-PCs zu gewährleisten, müssen Maßnahmen zur Wartung und Pflege des Systems umgesetzt werden. Anderenfalls besteht die Gefahr, dass beispielsweise durch Veränderungen an der Konfiguration Sicherheitslücken entstehen oder bekannt gewordene Software-Schwachstellen für Angriffe von innen oder außen ausgenutzt werden. Beim Betrieb eines Internet-PCs sollten daher die folgenden Aufgaben wahrgenommen werden:

- **Installation von Patches und Updates zur Behebung sicherheitsrelevanter Schwachstellen**
  Häufig werden Fehler in Software-Produkten bekannt, die dazu führen können, dass die Sicherheit der IT-Systeme, auf denen diese Produkte installiert sind, beeinträchtigt wird. Diese Software-Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen hierzu in der Regel so genannte Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.
  Die Administration des Internet-PCs sollte sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren und dagegen veröffentlichte Patches bzw. Updates installieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Wichtig ist dabei, dass Patches und Updates - wie jede andere Software - nur aus vertrauenswürdigen Quellen bezogen werden dürfen, möglichst direkt vom Hersteller bzw. Anbieter. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden.
- **Regelmäßige Kontrolle und Überwachung des Internet-PCs**
  Die Installation und Konfiguration eines Internet-PCs ist in der Regel nicht statisch, sondern ändert sich im laufenden Betrieb. Benutzer können beispielsweise Lesezeichen auf besuchte Internet-Seiten anlegen, E-Mails oder Downloads abspeichern und Dateitypen mit Anzeigeprogrammen verknüpfen. Viele Programme nehmen teilweise auch selbständig erhebliche Änderungen an der Konfiguration vor. Schließlich können sich auch Angriffe oder Angriffsversuche durch Änderungen an der Installation oder Konfiguration des Internet-PCs bemerkbar machen.
  Die Administration muss daher regelmäßig überprüfen, ob die Installation und die Konfiguration des Internet-PCs den Vorgaben bzw. Sollwerten entspricht. Hierzu ist z. B. zu prüfen,

  - ob die Hardware-Konfiguration des Internet-PCs verändert wurde,
  - ob Software-Komponenten entfernt oder zusätzlich installiert wurden,
  - ob Einstellungen des BIOS, des Betriebssystems oder der Programme unerlaubt verändert wurden und
  - ob es Hinweise darauf gibt, dass lokal gespeicherte Daten nicht den Richtlinien entsprechen, z. B. aufgrund der Pfad- oder Dateinamen.

  Weiterhin sollten sporadisch die zur Verfügung stehenden Protokollierungsmechanismen, z. B. *Ereignisanzeige* unter Windows NT, *syslog* unter Linux, *Verlauf* im Internet Explorer, ausgewertet werden. Diese Protokolle können Hinweise auf Angriffe, Angriffsversuche und missbräuchliche

Nutzung des Internet-PCs, z. B. Zugriffe auf unerlaubte Internet-Seiten, liefern. Dabei ist jedoch zu berücksichtigen, dass einige dieser Protokolle leicht manipuliert werden können.
Bewusste Verstöße gegen die Sicherheitsrichtlinien werden naturgemäß ungern in der Öffentlichkeit unternommen. Um einen Missbrauch zusätzlich zu erschweren, kann der Internet-PC daher auch an einem Ort mit Publikumsverkehr aufgestellt werden, beispielsweise in einer Bibliothek.
Bei der Kontrolle oder Überwachung des Internet-PCs müssen die Bestimmungen zum Datenschutz und zur betrieblichen Mitbestimmung beachtet werden. Daher sollten alle Maßnahmen hierzu frühzeitig mit dem Personalrat und dem Datenschutzbeauftragten abgestimmt werden.

- **Regelmäßige Neuinstallation des Systems**
  Eine weitere Möglichkeit, unerwünschten Veränderungen an der Installation oder Konfiguration des Internet-PCs entgegenzuwirken, ist die regelmäßige Neuinstallation des Systems. Solche Neuinstallationen beugen auch Systemabstürzen vor, die durch beschädigte oder instabile Installationen verursacht werden. Die Zeitabstände zwischen den Neuinstallationen müssen individuell anhand der Anforderungen an die Integrität des Internet-PCs festgelegt werden.
  Falls solche Neuinstallationen in kurzen Zeitabständen durchgeführt werden sollen, empfiehlt es sich, ein Abbild ("Image") des Systems herzustellen, das dann als ganzes installiert werden kann. Andernfalls entsteht u. U. ein erheblicher Arbeitsaufwand, da jedes Mal das System anhand der einzelnen Software-Komponenten und der Konfigurationsparameter rekonstruiert werden muss.
  Die Vorgehensweise bei der Neuinstallation muss auf jeden Fall mit dem Datensicherungskonzept für den Internet-PC (siehe M 6.79 *Datensicherung beim Einsatz von Internet-PCs*) abgestimmt sein. Andernfalls besteht die Gefahr, dass bei der Neuinstallation Daten verloren gehen, die nicht rekonstruiert werden können.

Prüffragen:

- Werden Internet-PCs regelmäßig mit den aktuellen Patches und Updates ausgestattet und werden diese ausschließlich aus vertrauenswürdigen Quellen bezogen?
- Erfolgt eine regelmäßige Prüfung, ob Installation und Konfiguration von Internet-PCs den Vorgaben entsprechen?
- Werden bei einer Kontrolle bzw. Überwachung von Internet-PCs die Bestimmungen zum Datenschutz und zur betriebliche Mitbestimmung eingehalten?

# M 4.153 Sichere Installation von Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach erfolgter Planung eines eDirectory-Verzeichnissystems (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*) muss eDirectory auf den relevanten Servern installiert werden. Während der Installationsphase ist ein eDirectory-Server nicht vollständig konfiguriert, sodass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Es empfiehlt sich daher, die erstmalige Konfiguration entweder in einer geschützten Umgebung durchzuführen oder alternativ eine vorbereitete Standardkonfiguration aufzuspielen.

Abbildung: eDirectory Installationsprogramm

Bei der Installation eines eDirectory-Servers in einen bereits bestehenden Verzeichnisbaum muss dessen genauer Kontext spezifiziert werden. Eine spätere Verschiebung des Servers innerhalb des Baums ist nur mit größerem Aufwand zu bewerkstelligen.

Während der Installation erfolgt u. a. auch die erstmalige Konfiguration der lokalen Sicherheitseinstellungen. Die wichtigsten Grundeinstellungen beziehen sich auf

- die Definition des eDirectory-Baums,
- die eDirectory-Zugriffsberechtigungen,
- die eDirectory-Vererbungseinstellungen und
- die Sicherheitseinstellungen für den LDAP-Zugriff.

Während der Installation lassen sich diese Einstellungen zum Teil vorgeben, ein Teil wird jedoch zunächst mit Standardwerten initialisiert. Bei Servern, die

als Erstes einen neuen eDirectory-Baum repräsentieren, muss zunächst die Zertifikatsserver-Komponente von eDirectory installiert werden, bevor ein durch SSL geschützter LDAP-Zugriff verwendet werden kann. Die Alternative hierzu ist, dass der eDirectory-Server einem bereits bestehenden eDirectory-Baum beitritt.

Je nachdem, welche eDirectory-Module zum Einsatz kommen, ist für jedes Modul eine sichere Installationskonfiguration einzurichten, die den Zugriff verhindert, solange sich der Server in der erstmaligen Konfigurationsphase befindet und bis die festgelegten Sicherheitsrichtlinien umgesetzt worden sind. Weitere Empfehlungen hierzu finden sich in M 4.155 *Sichere Konfiguration von Novell eDirectory*.

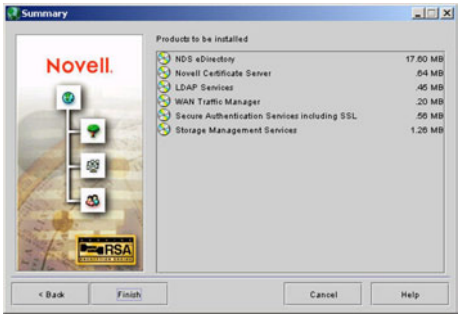



Abbildung: Zusammenfassung der Installation

Generell ist bei der Installation aus Sicherheitssicht Folgendes zu beachten:

- Die geltenden Zugriffseinstellungen für das Verzeichnissystem nach einer eDirectory-Installation hängen davon ab, ob die Software neu installiert wurde oder ob ein Upgrade erfolgt ist.
- Weitere Upgrade-Mechanismen können die Standardeinstellungen verändern, z. B. die Einbeziehung einer Windows NT-Domäne in einen eDirectory-Baum.
- Soll ein neuer Server in einen existierenden eDirectory-Baum aufgenommen werden, so erlaubt es der implizite Vererbungsmechanismus, die erstmalige Konfiguration deutlich abzukürzen.
- Bei der Installation der eDirectory-Server ist besondere Sorgfalt erforderlich, da diese im späteren Betrieb sensitive Daten speichern.

eDirectory-Server dürfen nur auf Servern installiert und betrieben werden, die sich in einer physikalisch sicheren Umgebung befinden (siehe auch M 1.29 *Geeignete Aufstellung eines IT-Systems*). Dies gilt insbesondere für eDirectory-Server, auf denen die Partition mit dem Security-Container abgelegt ist.

Prüffragen:

- Wird die die erstmalige Konfiguration von Novell eDirectory in einer geschützten Umgebung durchgeführt?

# M 4.154 Sichere Installation der Novell eDirectory Clientsoftware

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach der Planung eines eDirectory-Systems (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*) und der Installation der eDirectory-Server (siehe M 4.153 *Sichere Installation von Novell eDirectory*) muss die eDirectory-Clientsoftware auf den relevanten Rechnern installiert werden. Während der Installationsphase ist die eDirectory-Clientsoftware noch nicht vollständig konfiguriert, sodass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Es empfiehlt sich daher, die erstmalige Konfiguration entweder in einer geschützten Umgebung durchzuführen oder alternativ eine vorbereitete Standardkonfiguration aufzuspielen.

Die Installation der eDirectory-Clientsoftware erfolgt naturgemäß nicht unabhängig von den eDirectory-Servern. Die Installation kann erst dann als abgeschlossen gelten, wenn die Server-Anbindung erfolgt ist.

Schon bei der Installation der eDirectory-Clientsoftware sind sicherheitsrelevante Aspekte zu berücksichtigen. In der Regel genügt eine Standardinstallation nicht den geltenden Sicherheitsanforderungen, sodasss direkt danach eine sichere Konfiguration der Software erfolgen sollte.

Je nach eingesetztem Betriebssystem gibt es verschiedene Clientsoftware: Windows (der Novell Client), Linux sowie Sun Solaris. Nach erfolgter Installation wird dem Benutzer die Eingabemaske für das eDirectory-Login angezeigt (unter Windows der Novell Client):

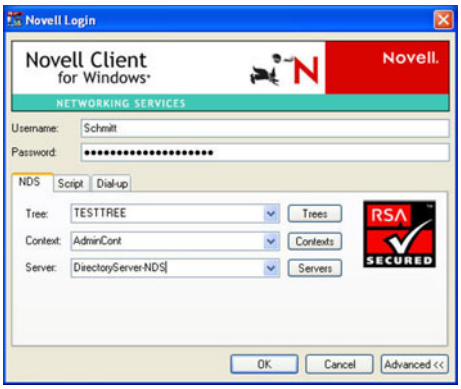



Abbildung: Eingangsmaske des eDirectory-Login

Die Installation beschränkt sich nicht nur auf die Clientsoftware, sondern betrifft in der Regel auch die zugrunde liegenden Betriebssysteme. Auch hierbei gilt, dass der Installationsprozess erst dann als abgeschlossen betrachtet werden kann, wenn direkt nach der Betriebssystem-Installation eine sichere Konfiguration erfolgt. Empfehlungen zur sicheren Installation und Konfiguration des Betriebssystems finden sich in den entsprechenden Bausteinen.

Für jedes Modul ist eine sichere Installationskonfiguration einzurichten, die den Zugriff verhindert, solange sich der Rechner in der erstmaligen Konfigurationsphase befindet und bis die festgelegten Sicherheitsrichtlinien umgesetzt

worden sind. Weitere Empfehlungen hierzu finden sich in M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*.

Prüffragen:

- Werden bei der Installation der eDirectory-Clientsoftware auch die sicherheitsrelevanten Aspekte berücksichtigt?
- Wird für jedes eDirectory Modul eine sichere Installationskonfiguration eingerichtet, die den Zugriff verhindert, solange sich der Rechner in der erstmaligen Konfigurationsphase befindet und bis die festgelegten Sicherheitsrichtlinien umgesetzt worden sind?

# M 4.155 Sichere Konfiguration von Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Konfiguration von eDirectory kann um eine Vielzahl weiterer Module erweitert werden, deren Funktionen über einen reinen Verzeichnisdienst hinausgehen. Dazu gehören:

- das *LDAP-Servermodul*, das einen Zugriff auf die Benutzerinformationen für LDAP-Clients erlaubt,
- das *iMonitor-Tool*, welches den administrativen Zugriff über einen Web-Browser gestattet,
- das *SLP-Modul* (Service Location Protocol), welches Service-URLs verwaltet und in das Ressourcenmanagement einbezieht,
- die *ConsoleOne* als Administrationsplattform des eDirectory,
- der *Zertifikatsserver*, der stets bei der Erstinstallation eines eDirectory-Servers innerhalb eines eDirectory-Baums installiert wird,
- eventuell eingesetzte Zusatzmodule, wie z. B. das Modul zur Unterstützung von *Groupwise*.

Daraus ergibt sich ein Bündel an Konfigurationsaufgaben, das noch durch folgende Themen ergänzt wird:

- Konfiguration der Verzeichnisbaumhierarchie,
- Konfiguration der Objekt-Zugriffsrechte,
- Konfiguration der Vererbungsfilter,
- Konfiguration der Sicherheitsäquivalenzen zwischen einzelnen Objekten bzw. Objektklassen,
- Konfiguration der Administrationsrollen,
- Konfiguration der Delegation von Administrationsaufgaben,
- Konfiguration der Benutzer und der Benutzergruppen,
- Verteilung der Key Management Objekte (KMOs),
- Konfiguration des Client-Zugriffs auf das eDirectory,
- Konfiguration der Partitionierung der eDirectory-Verzeichnisdatenbank,
- Konfiguration der Repliken des eDirectory-Verzeichnisdienstes,
- Konfiguration der DirXML-Schnittstelle zur Synchronisation mit fremden Verzeichnisdiensten,
- Konfiguration der Systemüberwachung.

Dies alles betrifft originär die eDirectory-Software. Es darf jedoch nicht vergessen werden, dass auch das zugrunde liegende Betriebssystem sicher konfiguriert werden muss, insbesondere was den Serverzugriff, die Netzanbindung und das Dateisystem betrifft.

Je nach Einsatzszenario und dem vom eDirectory-Server angebotenen Funktionsumfang muss überprüft werden, welche Zusatzmodule für den Betrieb von eDirectory benötigt werden und genutzt werden sollen. Nicht genutzte Module sollten nicht installiert werden, da jedes installierte Modul bei Fehlkonfiguration Sicherheitsprobleme verursachen kann.

Für jedes aktivierte Modul muss eine entsprechende Sicherheitsplanung durchgeführt werden. Anschließend ist diese durch geeignete Konfigurationsparameter umzusetzen (siehe auch M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*).

eDirectory bietet weitgehende Möglichkeiten zur Konfiguration des Benutzerzugangs für die einzelnen im Verzeichnis angelegten Benutzerkonten. Neben der individuellen Konfiguration einzelner Benutzerkonten können auch Templates verwendet werden, um eine Vielzahl von Benutzerkonten identisch zu konfigurieren. Die vorhandenen Einstellungsmöglichkeiten umfassen u. a.

- eine Beschränkung der Zeiten, zu denen eine Anmeldung an das Benutzerkonto möglich ist,
- eine Beschränkung der IP-Adressen, von denen aus eine Anmeldung möglich ist,
- eine Begrenzung der Anzahl gleichzeitiger Anmeldungen an ein Benutzerkonto,
- Anforderungen an die Passwortlänge und die Gültigkeitsdauer von Passwörtern.

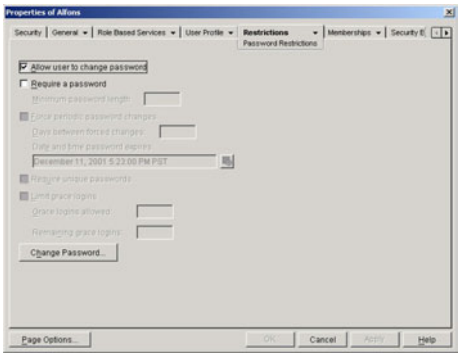



Abbildung: Eigenschaften von Alfons

Außerdem gibt es die Möglichkeit, Benutzerkonten direkt zu deaktivieren oder sie nach Ablauf einer bestimmten Zeit automatisch deaktivieren zu lassen.

Die Sicherheit eines eDirectory-Systems hängt außerdem von der Sicherheit der zum Zugriff benutzten Clientsoftware ab. Daher müssen für die sichere Konfiguration eines eDirectory-Systems auch die Client-seitigen Rechner und Programme einbezogen werden. Empfehlungen hierzu sind gesondert in Maßnahme M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware* zusammengefasst. Besondere Schutzmaßnahmen sind für die administrativen Zugänge zum eDirectory zu realisieren.

Ein eDirectory-System besteht in der Regel nicht nur aus einem eDirectory-Server, sondern aus einem ganzen Serververbund (siehe auch M 2.236 *Planung des Einsatzes von Novell eDirectory*). Die Verzeichnisdatenbank kann dabei in Form von einzelnen Partitionen auf verschiedene Server verteilt werden. Weiterhin können die einzelnen Server die Verzeichnisdatenbanken untereinander replizieren. Dadurch, dass mehrere Kopien einer Datenbank-Partition auf unterschiedlichen Servern vorliegen, kann eine Lastverteilung erreicht werden. Damit die Aktualität der Verzeichniskopien sichergestellt ist, müssen Veränderungen an den Daten zwischen den Servern ausgetauscht werden. Es muss daher ein Replikationskonzept erstellt werden. Unter anderem sind dabei folgende Aspekte zu berücksichtigen:

- Welcher Server hält die Master-Replica einer eDirectory-Partition?
- Welche Replikationstypen werden konfiguriert?
- Auf welche Server soll das eDirectory-Verzeichnis repliziert werden?
- Welche Informationen des eDirectory-Verzeichnisses sollen repliziert werden (Definition von Filtern)?

- Sollen Änderungen an Replikaten des Verzeichnisses erlaubt sein und sollen diese auf das Original übertragen werden (Definition als Typ *Read/ Write* oder als *Read-Only*)?

Da ein System in der Regel ständig Veränderungen durch den laufenden Betrieb unterworfen ist, muss auch die Sicherheit permanent überprüft und neu konfiguriert werden. Hinweise dazu finden sich in M 4.159 *Sicherer Betrieb von Novell eDirectory*.

Prüffragen:

- Sind alle eDirectory Module gemäß der ihnen zugedachten Rolle konfiguriert?
- Sind besondere Schutzmaßnahmen für die administrativen Zugänge zum eDirectory realisiert?

# M 4.156 Sichere Konfiguration der Novell eDirectory Clientsoftware

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach der Planung und Installation eines eDirectory-Systems (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*) muss das Verzeichnissystem inklusive seiner Clientsoftware auf den relevanten Rechnern konfiguriert werden.

Aufgrund der Vielzahl möglicher Applikationen und Dienste, die als Clientsoftware für eDirectory in Betracht kommen, wird im Folgenden nicht detailliert auf spezifische Konfigurationsmöglichkeiten eingegangen. Unter anderem ist es auch möglich, eigene Clientsoftware zu erstellen, die mit eDirectory über die standardisierte LDAP-Schnittstelle kommuniziert.

Die folgenden, generischen Hinweise sollten in jedem Fall beachtet werden:

- Zur Absicherung der jeweiligen Client-Installation sind die relevanten Maßnahmen der IT-Grundschutzhand-Kataloge für das jeweilige zugrunde liegende Betriebssystem anzuwenden.
- Soll die Clientsoftware zum eDirectory eine mittels SSL geschützte LDAP-Verbindung aufbauen, muss der Client ein entsprechendes Wurzelzertifikat erhalten, anhand dessen er die Authentizität des SSL-Serverzertifikats überprüfen kann.

Die Administration von eDirectory erfolgt über das Programm *ConsoleOne* von einem Client aus. Die Sicherheit der eDirectory-Installation hängt auch von der Integrität der zur Administration verwendeten Clients ab. Die Absicherung dieser Clients ist daher besonders wichtig.

Zum einen muss für administrativ genutzte Clientsoftware die Integrität der jeweiligen Betriebssystemplattform geschützt werden. Dafür können z. B. Zugriffsbeschränkungen auf Systemdateien eingerichtet werden, sofern solche Beschränkungen nicht bereits in der Voreinstellung des Betriebssystems vorhanden sind. Neben dem Schutz der unterliegenden Betriebssystemplattform des Clients ist auch ein Schutz der Administrationssoftware selbst erforderlich. Durch die Vergabe geeigneter Zugriffsbeschränkungen müssen die Verzeichnisse, in denen die *ConsoleOne* und die entsprechende Zusatzsoftware installiert sind, vor Manipulationen oder Überschreiben geschützt werden.

Speziell für den *Novell Client für Windows* ist das Zusatzmodul NMAS (Novell Modular Authentication Services) verfügbar. Dies erlaubt die Konfiguration zusätzlicher Authentisierungsmethoden (z. B. mittels Smartcard, Biometrie, RADIUS-Protokoll) für den Zugriff auf das eDirectory. Auch Kombinationen von Authentisierungsmethoden sind nutzbar. Auf Seite des eDirectory lassen sich bei Verwendung dieses Moduls Zugriffsrechte in Abhängigkeit der verwendeten Authentisierungsmethode konfigurieren.

Prüffragen:

- Geschützte LDAP-Verbindung von Clientsoftware zum eDirectory mittels SSL: Besitzt der Client ein entsprechendes Wurzelzertifikat?

# M 4.157 Einrichten von Zugriffsberechtigungen auf Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Verzeichnisdienst eDirectory speichert in der Regel sehr viele sensitive Unternehmens- und Benutzerdaten. Es ist deshalb unerlässlich, diese Informationen nur ausdrücklich autorisierten Applikationen, Benutzern und Administratoren zugänglich zu machen. Dazu ist es notwendig, eine zuvor erstellte Sicherheitsrichtlinie, die Regelungen für die Zugriffsberechtigungen enthalten muss (siehe M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*), konsequent und konsistent umzusetzen.

Die Rechtevergabe erfolgt bei eDirectory über *Access Control Lists* (ACLs). Zugriffsberechtigungen können dabei sowohl auf Objekt- als auch auf Attributsebene vergeben werden. Folgende Objektrechte (bzw. Privilegien) stehen zur Verfügung: *Browse, Create, Delete, Rename* und *Supervisor*. Attributsrechte sind: *Compare, Read, Add or Delete Self, Write, Supervisor* sowie *Inheritance Control*. Rechte können grundsätzlich nur im positiven Sinne vergeben werden, d. h. der Zugriff wird explizit erlaubt. Ein ausdrücklicher Ausschluss eines Benutzers mittels einer Zugriffsliste kann nicht definiert werden.

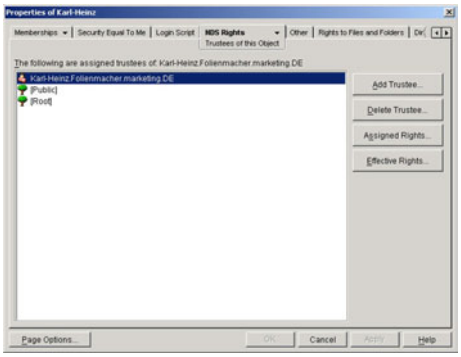



Abbildung: Rechtevergabe unter Novell eDirectory

Zugriffsberechtigungen werden explizit durch so genannte *Trustee-Assignments* vergeben. Für ein Zielobjekt wird dabei eingetragen, welche weiteren Objekte darauf zugreifen dürfen, d. h. *Trustees* dieses Zielobjekts sind. Umgekehrt kann man auch die Sicht eines zugreifenden Objekts einnehmen und so ablesen, auf welche Zielobjekte dieses Objekt zugreifen darf.

Zugriffsberechtigungen vererben sich entsprechend der Baumhierarchie des Verzeichnisdienstes. Dies gilt allerdings zunächst nur für die Objektrechte, die Attributsrechte vererben sich nur, wenn dies explizit konfiguriert wird. Die automatische Vererbung von Zugriffsberechtigungen von Objekten auf deren Kindobjekte kann reglementiert werden durch die Konfiguration so genannter Masken oder *Inherited Rights Filter* (IRF). Damit lässt sich die Vererbung der Zugriffsberechtigungen einschränken. Da über das *Self*-Recht eigene Attributswerte verändert werden können, ist es aus Sicherheitssicht kritisch und sollte ebenfalls mit Hilfe des Filters kontrolliert werden.

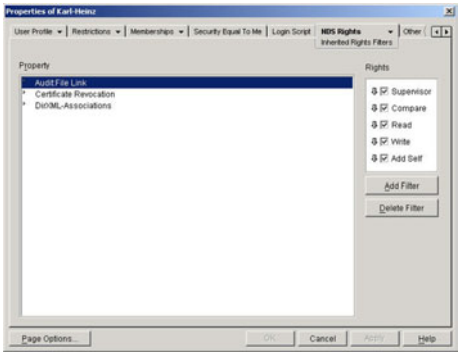



Abbildung: Rechte zuweisen

Bei einer Partitionierung des Verzeichnisbaums entsteht zunächst eine Lücke in der Vererbungskette, welche allerdings automatisch durch das Anhängen einer *inherited ACL* geschlossen wird.

Eine weitere Möglichkeit zur Vergabe von Zugriffsberechtigungen auf eDirectory-Objekte besteht in der Zuweisung einer so genannten Sicherheitsäquivalenz eines Objektes zu einem anderen Objekt. So kann definiert werden, dass auf Objekt X zumindest die gleichen Zugriffsmöglichkeiten existieren wie auf Objekt Y. Sämtliche Trustees von Objekt Y werden damit automatisch auch zu Trustees von Objekt X.

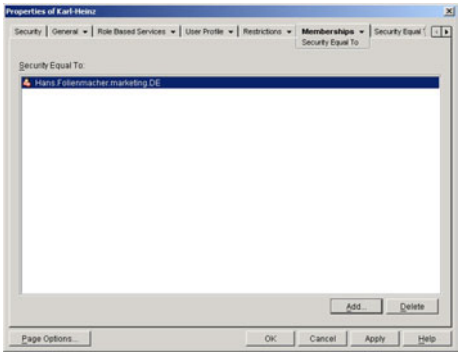



Abbildung: Gruppen-Mitgliedschaften einrichten

Wirksam bei einem Zugriffsversuch werden die so genannten *effektiven Rechte*, d. h. diejenigen Zugriffsberechtigungen, die sich gemäß den oben genannten Mechanismen als Endresultat ergeben. Diese effektiven Rechte werden bei jedem Zugriff dynamisch berechnet bzw. im Cache des Servers gehalten. Der Administrator hat über die Managementkonsole *ConsoleOne* die Möglichkeit, sich diese aktuell gültigen effektiven Rechte auf einzelne Objekte anzeigen zu lassen.

Ein wichtiger Aspekt bei der Rechtevergabe im eDirectory ist die Konfiguration der Benutzer und der Benutzergruppen (Organizational Roles). Durch geeignete Definition der Benutzer- und Administratorgruppen lässt sich die Rechtevergabe transparenter und einfacher gestalten. Dies ist zu empfehlen, da generell eine hohe Komplexität in der Administration die Gefahr durch Fehlkonfigurationen erhöht. Zur vereinfachten und konsistenten Konfiguration der Benutzer und Benutzergruppen (Organizational Roles) sollten *Templates* (Vorlagen) verwendet werden.

eDirectory erlaubt eine rollen- und funktionsbasierte Administration. Dazu werden so genannte RBS-Objekte (*Role Based Service*) und anschließend RBS-

Jobobjekte sowie RBS-Funktionsobjekte definiert. Dies erfordert eine Schemaerweiterung des Verzeichnisdienstes. Mit Hilfe der RBS-Funktionsobjekte werden die Aufgaben definiert, die von Mitgliedern einer zugewiesenen Benutzergruppe (Administratorengruppe) durchgeführt werden können. Auf diese Weise wird auch die Delegation von Administrationsaufgaben ermöglicht.

Bei einer eventuellen Zusammenführung zweier oder mehrerer eDirectory-Bäume zu einem Gesamtbaum sind anschließend die resultierenden effektiven Rechte zu kontrollieren. Auch bei der Verschiebung von Partitionen innerhalb eines eDirectory-Baums ist dies zu berücksichtigen. Ebenso müssen die Zugriffsberechtigungen kontrolliert und eventuell nachkonfiguriert werden, wenn z. B. eine Windows NT-Domäne in einen eDirectory-Baum durch Migration übernommen wurde.

Prüffragen:

- Wird die eDirectory Sicherheitsrichtlinie hinsichtlich der Regelungen für die Zugriffsberechtigungen konsequent und konsistent umgesetzt?
- Werden zur Konfiguration von Benutzern und Benutzergruppen (Organizational Roles) Templates (Vorlagen) verwendet?

# M 4.158 Einrichten des LDAP-Zugriffs auf Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

LDAP (Lightweight Directory Access Protocol) ist ein Protokoll zum Zugriff auf Daten eines Verzeichnisdienstes. LDAP wurde ursprünglich als Alternative zu DAP (Directory Access Protocol) entwickelt, das im Rahmen des X.500-Directory-Standards definiert wurde. Das zugrunde liegende Datenmodell und die innerhalb des Protokolls möglichen Operationen wurden dabei im Wesentlichen vom X.500-Standard übernommen. Die aktuelle Version des Protokolls, LDAP Version 3, hat sich inzwischen zum dominierenden Standard für den Zugriff auf Verzeichnisdienste entwickelt.

eDirectory verfügt über eine LDAP-Schnittstelle. Dies ermöglicht z. B. die folgenden Einsatzszenarien:

- eDirectory wird im Internet platziert, z. B. als so genannte eBusiness-Plattform oder einfach als Zertifikatsdatenbank. Die Benutzer greifen über das Internet mit Hilfe eines geeigneten, LDAP-fähigen Software-Clients darauf zu.
- eDirectory wird im Intranet einer Organisation zur Verwaltung von Benutzerkonten oder Ressourcen im Netz eingesetzt. Dann sind neben direkten Benutzerzugriffen über einen LDAP-Client auch Zugriffe von Netzapplikationen möglich. Außer über die Novell-eigenen Protokolle können diese Zugriffe ebenso über die LDAP-Schnittstelle erfolgen.

In beiden Fällen ist der LDAP-Zugriff entsprechend der zuvor definierten Sicherheitsrichtlinie (siehe M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*) zu konfigurieren.

**Anonymer LDAP-Zugriff**

eDirectory erlaubt prinzipiell eine anonyme Anmeldung von LDAP-Clients. In der Voreinstellung hat dabei der LDAP-Client die Zugriffsrechte, die für das Objekt [Public] im eDirectory eingetragen sind. Das Objekt [Public] ist ein virtuelles Objekt, das lediglich der Rechtevergabe im eDirectory dient. Jeder Zugriff auf Objekte im Verzeichnisbaum erfolgt automatisch mindestens mit den Rechten, die diesem Objekt eingeräumt werden.

In der Voreinstellung verfügt [Public] über das Recht *Browse* auf dem gesamten Baum.

Sollen anonymen Benutzern auf einzelne Teilbereiche des Verzeichnisbaums weitergehende Zugriffe eingeräumt werden, so sollte dafür ein gesondertes Benutzerkonto angelegt werden. Dieses Benutzerkonto muss dann als so genannter *Proxy-User* für den anonymen LDAP-Zugriff eingetragen werden. Dieses Konto darf kein Passwort erfordern, damit ein anonymer Zugang möglich ist. Es muss ferner darauf geachtet werden, dass dieses Benutzerkonto auch kein Passwort einrichten kann, da der anonyme Zugang sonst durch einen einzelnen Client blockiert werden könnte.

Bereits bei der Planung des Einsatzes eines Verzeichnisdienstes muss entschieden werden, welche Daten über eine anonyme Anmeldung zugänglich sein dürfen (siehe auch M 2.238 *Festlegung einer Sicherheitsrichtlinie für No-*

*vell eDirectory*). Entsprechend dieser Entscheidung müssen die Zugriffsrechte für den Proxy-User im eDirectory konfiguriert werden.


Abbildung: Zugriffsrechte für Proxy-User

**Einsatz von Novell eDirectory als LDAP-Server im Internet**

Wird eDirectory als LDAP-Server im Internet eingesetzt, so sollten die entsprechenden Server durch eine Firewall geschützt werden. Diese sollte so konfiguriert werden, dass nur die zum Betrieb der LDAP-Server notwendigen Datenpakete zu den LDAP-Servern weitergeleitet werden. Meist wird es sich dabei um TCP-Pakete an die Ports 389 und 636 handeln, die standardisierten Port-Nummern für LDAP bzw. LDAP über SSL.

Für Daten, auf die nicht anonym zugegriffen werden darf, ist eine Authentisierung des jeweiligen LDAP-Clients notwendig. Das Ergebnis einer erfolgreichen Authentisierung ist ein *NDS User Bind* des LDAP-Clients an das eDirectory. Der jeweilige Client authentisiert sich also als im eDirectory-Verzeichnis eingetragener Benutzer.

Um zu verhindern, dass Kennwörter im Klartext über das Internet übertragen werden, sollte für die entsprechende LDAP-Gruppe der Schalter *allowing cleartext passwords* nicht gesetzt sein (siehe auch M 5.97 *Absicherung der Kommunikation mit Novell eDirectory*). Dies entspricht auch der Voreinstellung von eDirectory. Mit dieser Einstellung sind anonyme LDAP-Verbindungen ebenso möglich wie eine Benutzeranmeldung mit LDAP über SSL.

Grundsätzlich wird empfohlen, SSL für die Kommunikation und Übertragung einzusetzen. Hierbei werden die Optionen *ein-* sowie *zweiseitige Authentisierung* unterstützt. Zweiseitige Authentisierung bedeutet, dass auch der Client in Besitz eines gültigen Zertifikats sein muss und dass auf Basis des zugehörigen privaten Schlüssels ein *Session-Key* generiert wird. Dies ist die sicherste Konfiguration. Alternativ kann die Client-Authentisierung jedoch auch über ein Passwort erfolgen. Durch die Verwendung einer verschlüsselten SSL-Verbindung zum Server ist die Vertraulichkeit des Passworts bei der Übertragung gewährleistet. In jedem Fall müssen die Benutzer das CA-Wurzelzertifikat in ihren LDAP-Client, z. B. einen Browser, importieren, damit die eingerichteten Vertrauensbeziehungen auch lokal nachvollzogen werden können.

Wird kein SSL verwendet, so können die Benutzerpasswörter im Klartext über das Internet an das eDirectory übertragen werden (siehe auch M 5.97 *Absicherung der Kommunikation mit Novell eDirectory*). Dies sollte aber vermieden werden. Um es ausdrücklich zu unterbinden, muss die Option *allowing cleartext passwords* auf *disabled* geschaltet sein.

**Konfiguration des LDAP-Zugriffes bei Schemaänderungen**

eDirectory bietet die Möglichkeit, die innerhalb von LDAP verwendeten standardisierten Objektklassen auf andere im eDirectory intern verwendete Objektklassen abzubilden. Diese Eigenschaft wird relevant, wenn LDAP-Clients bei der Suche standardisierte LDAP-Objektklassen verwenden, die entsprechenden Daten sich jedoch in Attributen von eDirectory-Objektklassen mit anderen

Namen befinden. Bei der erstmaligen Verwendung von LDAP-Clients oder bei Änderungen des eDirectory-Schemas sollte daher überprüft werden, ob die Abbildung der LDAP-Objektklassen auf eDirectory-Objektklassen schlüssig ist und die verwendeten LDAP-Applikationen damit korrekt funktionieren.

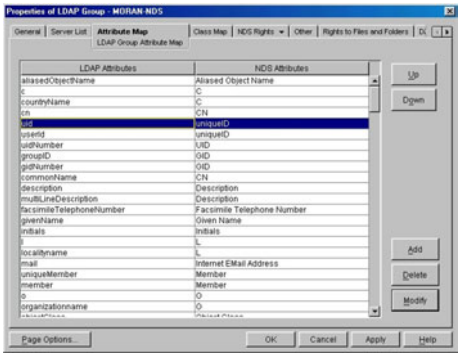


Abbildung: Eigenschaften der LDAP-Gruppe

Prüffragen:

- Ist für die LDAP-Gruppe der Schalter allowing cleartext passwords nicht gesetzt, so dass Kennwörter nicht im Klartext übertragen werden?
- Sind alle eDirectory-Server, die vom Internet aus über LDAP angesprochen werden können, durch eine Firewall geschützt?
- Ist sichergestellt, dass Proxy-User (Konto für den anonymen LDAP-Zugriff) über ihr Benutzerkonto kein Passwort einrichten können?

# M 4.159 Sicherer Betrieb von Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Sicherheit eines komplexen Systems muss im Betrieb permanent aufrecht erhalten werden, da sich im laufenden Betrieb notwendige Veränderungen ergeben. Es genügt daher nicht, eine sichere Anfangskonfiguration einzustellen (siehe M 4.153 *Sichere Installation von Novell eDirectory*, M 4.155 *Sichere Konfiguration von Novell eDirectory* sowie die entsprechenden Maßnahmen M 4.154 *Sichere Installation der Novell eDirectory Clientsoftware* und M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*).

Nach der Installation und erstmaligen Konfiguration gemäß den im Vorfeld festgelegten eDirectory-Konzepten und Sicherheitsrichtlinien erfolgt der Betrieb von eDirectory-Servern in der Regel im Netzverbund. Die Sicherheit eines solchen Netzes hängt dabei einerseits von der anfangs eingestellten Konfiguration ab. Sie wird jedoch auch maßgeblich durch die Art und Weise der Konfigurationsänderungen bestimmt, die im laufenden Betrieb erfolgen müssen. Dabei sind insbesondere auch Seiteneffekte zu berücksichtigen, die unter Umständen unbeabsichtigt zu Sicherheitslücken führen können.

Folgende Aspekte sind im laufenden Betrieb für ein eDirectory-Verzeichnissystem aus Sicht der Informationssicherheit zu beachten:

- Der eDirectory-Zertifikatsserver spielt eine wesentliche Rolle für die Zugriffskontrollmechanismen des Verzeichnisses. Der Zertifikatsserver wird auf dem ersten eDirectory-Server eines eDirectory-Baums installiert. Für jedes neue Objekt im eDirectory wird automatisch ein eigenes Schlüsselpaar generiert und auf dem Zertifikatsserver abgelegt. Der sichere Betrieb dieses "ersten eDirectory-Servers" im Baum ist deshalb besonders wichtig. Zu schützen sind nicht nur die sensitiven Daten, die sich auf diesem befinden, sondern vor allem auch dessen Verfügbarkeit. Es ist deshalb dringend anzuraten, die Replizierung des eDirectory auf verschiedene Server zu konfigurieren, insbesondere sollte wenigstens eine vollständige *Read/Write-Replica* existieren. Wird der "Hauptserver" aus einem wichtigen Grund heruntergefahren oder fällt dieser dauerhaft aus, so kann die nächstgelegene *Read/Write-Replica* zur *Master-Replica* erklärt und der Betrieb damit aufrecht erhalten werden.
- Die Sicherheit eines IT-Systems basiert immer auch auf der physikalischen Sicherheit der Server und Netzkomponenten. Diese muss auch für den Betrieb von eDirectory sichergestellt sein. Entsprechende Maßnahmen finden sich in Schicht 2, beispielsweise in den Bausteinen B 2.4 *Serverraum* oder B 2.9 *Rechenzentrum*.
- Veränderungen in einem eDirectory-Verzeichnissystem ergeben sich insbesondere dann, wenn fremde eDirectory- oder LDAP-Verzeichnisse in einen bestehenden eDirectory-Baum importiert werden. Diese neu importierten Verzeichnisse sind in der Regel noch nicht in die bestehenden Sicherheitsstrukturen eingebunden.
  Damit die definierte Sicherheitsrichtlinie auch weiterhin konsistent umgesetzt ist, muss die Konfiguration der Sicherheitseinstellungen umgehend nachgeholt werden. Die Berechtigungen zum Import neuer Verzeichnisse

und zum Erzeugen von Verzeichnis-Repliken müssen restriktiv vergeben werden.
- Um den Sicherheitszustand eines Systems nachvollziehen zu können, ist es notwendig, dieses zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die potentiell zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept ist dabei auch als Teil des Sicherheitskonzeptes anzusehen. Komplexe Systeme wie eDirectory können in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Überwachung muss automatisch durch entsprechende Systemkomponenten oder Produkte von Drittherstellern erfolgen. Dabei ist auch die Konfiguration der Systemüberwachung regelmäßig an das sich verändernde System anzupassen. Die Empfehlungen zur Überwachung sind in M 4.160 *Überwachen von Novell eDirectory* zusammengefasst.
- Ein wichtiger Aspekt der Systemsicherheit eines eDirectory-Systems ist die konsistente Verwaltung von Benutzern und Berechtigungen. Das administrative Konzept hat dabei Auswirkungen auf die Komplexität der durchzuführenden Aufgaben. Da es bei komplexen Abläufen leicht zu Fehlern kommen kann, sollten die administrativen Aufgaben möglichst einfach gestaltet werden. Dies trägt zur Aufrechterhaltung eines sicheren Systemzustands bei. Deshalb ist ein gruppenbasiertes Zugriffskonzept unerlässlich. Dadurch wird die Verwaltung von Zugriffsrechten auf Datenbanken wesentlich vereinfacht und weniger fehleranfällig.

Auch unter Sicherheitsgesichtspunkten ist es wichtig, dass alle den Betrieb eines eDirectory-Systems betreffenden Richtlinien, Regelungen und Prozesse dokumentiert werden. Dazu sollten Betriebshandbücher erstellt und bei Systemänderungen aktualisiert werden. Da die Betriebshandbücher sicherheitsrelevante Informationen enthalten, sind sie so aufzubewahren, dass Unbefugte keinen Zugriff auf sie erlangen können. Befugte Administratoren sollten die Handbücher jedoch leicht einsehen können.

Die aufgeführten Empfehlungen können an dieser Stelle nur allgemeinen Charakter haben, da die Aufrechterhaltung der Systemsicherheit auch von lokalen Gegebenheiten abhängt. Daher müssen schon in der Planungsphase eines eDirectory-Verzeichnisbaums entsprechende Richtlinien zum sicheren Betrieb erstellt werden, die die lokalen Anforderungen berücksichtigen. Unter Umständen kann es auch vorkommen, dass bestimmte Mechanismen nicht optimal sicher konfiguriert werden können. Dies ist z. B. der Fall, wenn "alte" Applikationen weiter betrieben werden müssen, die nur auf schwache oder keine Authentisierung ausgelegt sind. Hier muss dann durch alternative Gegenmaßnahmen an anderer Stelle, z. B. auf organisatorischer Ebene, eine angemessene Sicherheit erreicht werden.

Potentielle Sicherheitslücken können nur von kompetenten Administratoren entdeckt bzw. vermieden werden. Daher ist die Schulung und Fortbildung der Systemverwalter eine wichtige Schutzmaßnahme (siehe auch M 3.29 *Schulung zur Administration von Novell eDirectory*). Daneben müssen auch die normalen Benutzer in Sicherheitsaspekten geschult werden (siehe auch M 3.30 *Schulung zum Einsatz von Novell eDirectory Clientsoftware*), damit potentielle Gefahren bekannt sind und die zur Verfügung stehenden Sicherheitsmechanismen richtig eingesetzt werden können.

Die Sicherheitseinstellungen und die Protokolldateien eines Servers sollten regelmäßig überprüft werden. Dies kann manuell oder werkzeuggestützt erfolgen. Anderenfalls besteht die Gefahr, dass Abweichungen von den Sicherheitsrichtlinien und Sicherheitsprobleme nicht frühzeitig erkannt und dadurch

auch nicht rechtzeitig behoben werden (siehe auch M 4.160 *Überwachen von Novell eDirectory*).

**Beispiel: gruppenbasiertes Zugriffskonzept**

Ein Mitarbeiter wechselt die Abteilung, wodurch eine Anpassung der Zugriffsrechte erforderlich ist. Werden benutzerbezogene *Access Control Lists* (ACLs) genutzt, so muss jedes Verzeichnis überprüft werden, um den Benutzer gegebenenfalls aus der ACL auszutragen bzw. neu einzutragen. Werden dagegen gruppenbezogene ACLs verwendet, so muss der Benutzer lediglich in der Benutzerverwaltung aus den relevanten Gruppen aus- bzw. eingetragen werden. Die Änderung kann zentral am Benutzer-Objekt erfolgen.

Prüffragen:

- Wird der eDirectory-Zertifikatsserver auf verschiedene Server repliziert?
- Werden die Sicherheitseinstellungen nach Änderungen am eDirectory-Verzeichnissystem angepasst?
- Sind alle den Betrieb eines eDirectory-Systems betreffenden Richtlinien, Regelungen und Prozesse dokumentiert und auf dem aktuellen System-Stand?
- Werden die Sicherheitseinstellungen und die Protokolldateien eines eDirectory-Servers regelmäßig überprüft?

# M 4.160 Überwachen von Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT, Revisor

Um den Sicherheitszustand eines Systems nachvollziehen zu können, ist es notwendig, dieses kontinuierlich zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept ist dabei auch als Teil des Sicherheitskonzeptes anzusehen.

Komplexe Systeme wie eDirectory können dabei in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Kontrolle muss automatisch durch entsprechende Systemkomponenten oder Produkte von Drittherstellern erfolgen. Dabei ist auch die Konfiguration der Systemüberwachung regelmäßig an das sich verändernde System anzupassen.

eDirectory stellt für die Systemüberwachung das Werkzeug *iMonitor* zur Verfügung. Dies ist eine Client-Server-Anwendung, bei der auf einigen (oder allen) eDirectory-Servern der iMonitor-Dienst läuft. Die Clients können über einen Browser darauf zugreifen, der hierfür HTML Version 3 unterstützen muss. Der Zugreifende muss sich gegenüber den iMonitor-Services authentisieren und erhält nach erfolgreicher Erkennung Zugriff auf die iMonitor-Daten, wobei die für ihn konfigurierten Rechte gelten.

Die Informationen, die der iMonitor-Dienst über einen eDirectory-Server zur Verfügung stellt, könnten u. U. von Unbefugten dazu genutzt werden, gezielt nach Sicherheitslücken in einer bestehenden eDirectory-Installation zu suchen. Aus diesem Grund wird empfohlen, den Zugriff auf den iMonitor-Dienst nur mit aktivierter SSL-Verschlüsselung zu erlauben, besonders wenn von außerhalb des eigenen Behörden- bzw. Unternehmensnetzes aus zugegriffen werden kann. Dazu muss auf dem Client das entsprechende Server-Zertifikat in den Browser importiert werden.

Es gibt zwei verschiedene Operationsmodi des iMonitor-Zugriffs: den *direkten Modus* und den *Proxymodus*. Beim direkten Modus ist der Browser direkt mit dem eDirectory-Server verbunden, dessen Statusdaten abgefragt werden. Auf dem eDirectory-Server müssen dabei die iMonitor-Services aktiviert sein. Beim Proxymodus wird auf einen Server zugegriffen, auf dem die iMonitor-Services zur Verfügung stehen, die eigentliche Information wird aber von einem anderen Server abgefragt.

Der direkte Modus besitzt gegenüber dem Proxymodus u. a. den Vorteil, dass er weniger Bandbreite benötigt und die serverzentrierten Funktionalitäten in vollem Umfang zur Verfügung stehen. Aus Sicht der Informationssicherheit ist jedoch der Proxymodus zu bevorzugen, damit nicht alle eDirectory-Rechner diese direkte Zugriffsmöglichkeit gestatten. Dabei sollte eine feste Einwahladresse verwendet werden, die dann entsprechend kontrolliert und geschützt werden muss.

Das *NDS Trace Utility* dient der Erfassung eDirectory-spezifischer Ereignisse in eine eigene Protokolldatei. Damit kann eine Protokollierung sämtlicher eDirectory-Ereignisse erreicht werden. Ferner gibt es das Zusatzmodul NAAS

(Novell Advanced Auditing Service), womit sich eine automatisierte Auswertung der eDirectory-spezifischen Ereignisse realisieren lässt.

Im Rahmen der Überwachung sind auch folgende Aspekte zu beachten:

- Der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat sollten frühzeitig in die Planung mit einbezogen werden, da eine Überwachung meist auch personenbezogene Daten erfassen muss, damit im Fall einer Sicherheitsverletzung zuverlässig der Verursacher festgestellt werden kann.
- Neben den eDirectory-spezifischen Ereignissen müssen auch Ereignisse des Betriebssystems beobachtet und protokolliert werden, um ein vollständigeres Bild über die Systemabläufe zu erhalten. Empfehlungen und Hinweise zur Protokollierung auf Betriebssystem-Ebene finden sich in den jeweiligen Bausteinen.
- Eine zentrale Sammelstelle für Protokolldateien mit entsprechend automatisierter Auswertung kann durch Produkte von Drittherstellern aufgebaut werden. Wird ein Werkzeug zum Netz- und Systemmanagement eingesetzt (siehe auch Baustein B 4.2 *Netz- und Systemmanagement*), so ist es - je nach Produkt - möglich, die eDirectory-Protokolle direkt in dieses Werkzeug zu integrieren.
- Durch die Überwachung fallen je nach Einstellung große Datenmengen an. Diese müssen nicht nur regelmäßig ausgewertet, sondern aus Platzgründen auch gelöscht oder auf andere Datenträgern ausgelagert werden. Zusätzlich führt eine intensive Überwachung u. U. zu Performanceverlusten. Dadurch kann ein Server unter Umständen so überlastet werden, dass ein geregelter Betrieb nicht mehr möglich ist. Aus diesem Grund müssen die geeigneten Überwachungsparameter im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst werden. Es ist zu beachten, dass die Anpassung auch Einfluss auf das gesamte Überwachungskonzept haben kann, da bestimmte Überwachungsaufgaben u. U. nicht mehr durchführbar sind. Dies gilt besonders, wenn zusätzliche Produkte eingesetzt werden, die hohe Voraussetzungen an die protokollierten Ereignisse stellen. Beispiele hierfür sind Programme, die eine automatische Analyse der Protokolldaten auf Verhaltensanomalien, etwa für die Erkennung von Angriffen, durchführen.

Im Rahmen der Überwachung der Systemfunktionen empfiehlt sich außerdem eine regelmäßige Kontrolle der eDirectory-Replikation, durch die Konfigurationsänderungen weitergeleitet werden. Fehler in der Replikation haben meist zur Folge, dass Konfigurationsänderungen nicht überall durchgeführt werden und so z. B. einem Benutzer zu viele Rechte zugestanden werden.

Prüffragen:

- Ist ein Überwachungskonzept zum eDirectory vorhanden?
- Wird die Konfiguration der Systemüberwachung zum eDirectory regelmäßig an das sich verändernde System angepasst?
- Erfolgt, im Rahmen der Überwachung der Systemfunktionen, eine regelmäßige Kontrolle der eDirectory-Replikation?

# M 4.161 Sichere Installation von Exchange-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine sichere Installation aller Komponenten ist immer eine Grundvoraussetzung für den reibungslosen und sicheren Betrieb des Systems. Wie für jedes komplexe Client-Server-System muss auch die Installation von Exchange-Servern und Outlook-Clients geplant und getestet werden. Die Installation sollte auf Basis der Einsatzplanung von Exchange und Outlook und der festgelegten Sicherheitsrichtlinie erfolgen (siehe M 2.247 *Planung des Einsatzes von Exchange und Outlook*). Da sich Exchange-Systeme sehr stark in die Windows Umgebung integrieren, speziell in das Active Directory, müssen die entsprechenden spezifischen Sicherheitsrichtlinien berücksichtigt werden.

Die Systeme, auf denen Exchange/Outlook installiert werden soll, müssen geeignet abgesichert sein. Die Installation kann erst dann als abgeschlossen angesehen werden, wenn die Exchange/Outlook-Systeme in einen sicheren Zustand überführt wurden. Dadurch wird sichergestellt, dass in der anschließenden Konfigurationsphase nur berechtigte Administratoren auf das Exchange-System zugreifen können.

Für die Installation eines Exchange-Systems sind außerdem die in M 4.356 *Sichere Installation von Groupware-Systemen* beschriebenen Aspekte zu berücksichtigen.

**Microsoft-Hinweise für die Installation umsetzen**

Die Installationsanleitung von Microsoft Exchange enthält in der Regel eine Vielzahl von Verweisen auf Microsoft-Hinweise, in denen wichtige Informationen für die Installation oder zur Problemlösung bei Installationsproblemen enthalten sind. In der Regel verweisen die in der Dokumentation genannten Microsoft-Hinweise selbst auch wieder auf weitere Dokumente, so dass eine beträchtliche Informationsmenge zusammenkommen kann. Die Hinweise sind im Vorfeld der Installation zu sichten. In der Regel ist es zunächst ausreichend, ausgehend von der Installationsdokumentation die dort angegebenen Hinweise zu lesen und einen weiteren Iterationsschritt durchzuführen. Oft wird bei Referenzen auf weitere Informationen explizit angegeben, ob diese verpflichtend abzuarbeiten sind oder nur unter bestimmten Bedingungen angewandt werden sollen. Es wird dringend empfohlen, alle relevanten Informationen tatsächlich abzuarbeiten, da es sonst leicht zu Fehlinstallationen kommen kann.

Insbesondere wenn die Installation zwar abgeschlossen wird, dabei jedoch Fehler aufgetreten sind, ist es möglich, dass Teilfunktionen eines Microsoft-Exchange-Systems nicht korrekt arbeiten. Dies kann auch sicherheitsrelevante Auswirkungen haben, so dass immer eine fehlerfrei abgeschlossene Installation anzustreben ist. Fehlermeldungen können nur dann ignoriert werden, wenn dies explizit durch die Installationsanleitung oder Microsoft Hinweise angegeben wird.

Es wird empfohlen, die Microsoft Hinweise auszudrucken und nach der Abarbeitung der Systemdokumentation beizulegen (siehe M 2.480 *Nutzung der Exchange- und Outlook-Dokumentation*).

Aktuelle Microsoft-Exchange-Sicherheitsleitfäden berücksichtigen

Für immer mehr Produkte von Microsoft stehen Sicherheitsleitfäden zur Verfügung. Obwohl diese unterschiedlich in der Qualität der Sicherheitsempfehlungen sind, ist es sinnvoll, die Leitfäden für die zu installierenden Microsoft-Komponenten zu verwenden. Die Sicherheitsleitfäden werden in Abständen aktualisiert, so dass es sich lohnt, neuere Leitfäden für bereits installierte Systeme zu berücksichtigen.

Die sichere Installation einer Microsoft Exchange 2010-Infrastruktur wird im Microsoft Technet unter "Deploying Exchange 2010: Exchange 2010 Help" beschrieben. Installationsempfehlungen für eine sichere Microsoft Outlook 2010-Anwendung werden unter "Deploy Office 2010" gegeben.

Prüffragen:

- Wurden alle für den Betrieb des Exchange-Systems benötigten Komponenten sicher installiert?
- Sind alle relevanten Microsoft-Hinweise für die Installation von Microsoft Exchange umgesetzt worden?

# M 4.162 Sichere Konfiguration von Exchange-Servern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach der Installation eines Exchange-Servers muss die Software sicher konfiguriert werden, aufbauend auf den Vorgaben aus dem Sicherheitskonzept. Bevor ein Administrator nach der erfolgreichen Installation von Exchange mit der Konfiguration fortfährt, sollten die allgemeinen Empfehlungen hier zur Administration umgesetzt werden.

Bei der eigentlichen Konfiguration des Exchange-Servers ist dann vor allem auf folgendes zu achten:

### Administratives

Die Zugriffsrechte auf Exchange Objekte müssen auf das notwendige Maß beschränkt werden, siehe M 4.163 *Zugriffsrechte auf Exchange-Objekte*. Insbesondere sind die Administrator-Rechte festzulegen.

### Begrenzung der maximalen Nachrichtengröße

Als eine der möglichen Maßnahmen zum Schutz gegen DoS-Attacken (Denial of Service) sollten maximal zulässige Größen sowohl für eingehende als auch für ausgehende Nachrichten definiert werden. Die maximal zulässige Größe sollte auf der Basis der Anforderungen der Institution beschränkt werden. Außerdem muss festgelegt werden, welche Reaktionen bei Erreichen des Richtwerts erfolgen sollten. Bei ausgehender Mail sollten beispielsweise die Sender darüber informiert werden, dass der Richtwert überschritten wurde und die Nachricht nicht ausgeliefert wurde. Bei eingehender Mail könnten die Empfänger informiert werden, dass eine Nachricht nicht zugestellt wurde. Es wird empfohlen, den Richtwert von 10 MByte nicht zu unterschreiten.

### Umgang mit Sondernachrichten

Automatische Lese- und Empfangsbestätigungen, sowie automatisch generierte Abwesenheitsnachrichten (Out-of-Office-Meldungen) können zu Denial-of-Service-Attacken oder zu unbeabsichtigten Speicherplatzproblemen führen. Sofern im Unternehmen bzw. in der Behörde die Verwendung von E-Mail-Bestätigungen und Out-of-Office-Meldungen nicht explizit gewünscht ist, wird empfohlen, den Einsatz dieser Sondernachrichten in der Exchange-Gesamtorganisation komplett zu verbieten. In den Standardeinstellungen sollten alle Sondernachrichtentypen deaktiviert werden.

### Konfiguration der Exchange-Konnektoren

In einer Umgebung mit mehreren Servern muss die Sicherheit der Nachrichtenübertragung gewährleistet werden, was eine entsprechende Konfiguration der Routing-Konnektoren bedeutet. Die Verbindungen zwischen Servern einer Routing-Gruppe werden während der Installation automatisch konfiguriert. Die Einstellungen der einzelnen Konnektoren müssen jedoch manuell angepasst werden, um ein höheres Sicherheitsniveau zu erreichen.

Es ist zu beachten, dass für die Konfiguration der Exchange-Konnektoren nicht nur Exchange-Administratorrechte, sondern auch Windows-Administratorrechte erforderlich sind.

**Authentisierung zwischen Exchange-Servern und SMTP-Relay-Hosts**

Für die Weiterleitung einkommender und ausgehender Nachrichten kann in der DMZ einer Institution ein S/MIME-Relay-Host eingerichtet werden. Öffentliche SMTP-Verbindungen (von außen zum SMTP-Relay-Host) können prinzipiell nicht verschlüsselt werden, wenn fremde SMTP-Server mit dem SMTP-Relay-Host in der DMZ im Klartext kommunizieren. Der Relay-Host in der DMZ und die Server im internen Netz sollte sich jedoch gegenseitig authentisieren. Der SMTP-Konnektor muss entsprechend konfiguriert werden.

Zugriff auf den Exchange-Server über HTTP (Outlook Web Access, OWA)

Von der Benutzung der OWA-Funktionalität im Exchange-Umfeld wird grundsätzlich abgeraten. Soll den Benutzern der Zugriff auf Exchange-Server über HTTP dennoch ermöglicht werden, müssen die Empfehlungen aus M 5.129 *Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen* umgesetzt werden. Organisationsintern muss dazu festgelegt werden, ob OWA eingesetzt werden darf oder nicht.

**Zugriff von MAPI-Clients auf Exchange Server über das Internet**

Es wird empfohlen, den Benutzern keinen direkten Zugriff auf die Exchange-Postfächer und den globalen Katalog über das Internet zu gestatten. Sollte dies aus anderen Gründen doch erlaubt werden, so muss das Sicherheitsgateway (Firewall) der Institution entsprechend konfiguriert werden, siehe M 2.481 *Planung des Einsatzes von Exchange für Outlook Anywhere*.

**Konfiguration der POP3 und IMAP Netzprotokolle**

Der Zugriff auf einen Exchange-Server kann unter anderem über die Protokolle POP3 und IMAP4 stattfinden. Entscheidet sich eine Institution, diese Protokolle einzusetzen, so sollten Einstellungen zur Authentisierung und Verschlüsselung vorgenommen sowie Zugriffseinschränkungen auf Basis der IP-Adressen oder Domänennamen definiert werden. Dies erfolgt in den jeweiligen Protokolleinstellungen für die Dienste POP3 und IMAP.

**Authentisierung**

Als Authentisierungsmechanismus sollte die integrierte Windows Authentisierung der HTTP Basic-Authentisierung vorgezogen werden. Die HTTP Basic-Authentisierung sollte nur in Verbindung mit TLS-Verschlüsselung eingesetzt werden.

**Verschlüsselung**

Die Verschlüsselung der Verbindungen wird empfohlen, wenn sensitive Daten über ungeschützte Kommunikationswege übertragen werden oder HTTP Basic Authentisierung zum Einsatz kommen soll.

**Nachrichtenformat**

Nachrichten im HTML-Format können auch aktive Elemente enthalten, was ein Sicherheitsrisiko für Clients darstellt. Deshalb wird empfohlen, den Exchange-Server so zu konfigurieren, dass dieser HTML-Nachrichten über SMTP, POP3 und IMAP4 als einfache Textnachrichten ausliefert.

**Sichere Konfiguration der Exchange-Datenbanken**

Die von einem Groupware-System zur Speicherung genutzte Datenbank enthält alle Groupware-Informationen dieses Systems (dies schließt im Allgemei-

nen Passwörtern lokaler Benutzer, Systemdateien und Transaktionslogs nicht mit ein). Die Kommunikation zwischen Groupware-System und Datenbank erfolgt über Anfragen, die über das lokale Netz übertragen werden, sofern Datenbank und die Groupware-Systemkomponenten nicht auf demselben Rechner installiert werden. Wenn die Datenbank nicht auf demselben System betrieben wird, muss die Datenbank besonders gut geschützt werden.

Folgendes ist zu beachten:

- Auf die Informationsspeicher darf nur vom Microsoft-Exchange-System selbst zugegriffen werden, z. B. durch Paketfilter.
- Direkte Datenbankverbindungen von anderen Systemen oder Clients sind durch ein Sicherheitsgateway (Firewall) zu unterbinden.

In Abhängigkeit vom Einsatzszenario können noch weitere Maßnahmen notwendig sein. Die Liste ist daher geeignet zu erweitern. Es wird empfohlen, die Empfehlungen von Microsoft zur Absicherung der Exchange-Datenbank umzusetzen. Details dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Protokollierung**

Der Betrieb eines Exchange-Systems muss protokolliert werden, siehe M 4.270 Protokollierung von Exchange-Systemen.

Weitere Hinweise, wie die Anforderungen aus dieser Maßnahme konkret umgesetzt werden können, finden sich für die Version 2010 beispielsweise in folgenden Informationen des Microsoft Technet:

- Die Einschränkung der Zugriffsberechtigungen wird unter "Permissions: Exchange 2010 Help" beschrieben.
- Die Einstellungen zur Umsetzung von Richtlinien der Nachrichtenübermittlung und Compliance werden unter "Messaging Policy and Compliance: Exchange 2010 Help" beschrieben.
- Die Einrichtung der notwendigen Konnektoren wird unter "Transport Server Post-Deployment Tasks: Exchange 2010 Help" beschrieben.
- Die sichere Konfiguration von Outlook Web Access wird unter "Understanding Security for Outlook Web Access: Exchange 2007 Help" (analog Exchange 2007) beschrieben.
- Die Zugriffsregelungen auf Datenbanken eines Mailbox-Servers werden unter "Permissions to Manage Mailbox Servers: Exchange 2010 Help" beschrieben. Die sichere Konfiguration von Datenbanken eines Mailbox-Servers wird unter "Securing Mailbox Servers: Exchange 2010 Help" beschrieben.

Prüffragen:

- Wurde der Exchange-Server entsprechend der Vorgaben aus dem Sicherheitskonzept sicher konfiguriert?
- Wurden die Zugriffsrechte für Administratoren der Exchange Installation festgelegt?
- Ist organisationsintern geklärt, ob der Zugriff via Outlook Web Access auf E-Mail-Konten erlaubt ist?
- Ist die Datenbank des Microsoft Exchange-Systems durch eine Firewall vor direkten Zugriffen Dritter geschützt?

# M 4.163 Zugriffsrechte auf Exchange-Objekte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Zugriffsberechtigungen auf Exchange-Objekte müssen auf der Grundlage der Sicherheitsrichtlinie festgelegt werden.

### Einrichtung der Benutzerberechtigungen für die Exchange-Administration

Grundsätzlich sollte die Administration auf dem Gruppen- und nicht dem Personenprinzip aufgebaut werden: Berechtigungen sollten für Gruppen und nicht für einzelne Benutzerkonten vergeben werden. Dadurch wird die Verwaltung erheblich erleichtert und übersichtlicher gestaltet und eine mögliche Fehlerquelle beseitigt. Auch die Exchange-Administratoren sollten dabei über Gruppenmitgliedschaften verwaltet werden. Dafür muss deren Rollen klar definiert sein.

### Serverseitige Benutzerprofile

Es wird empfohlen, bei Microsoft Exchange serverseitige Benutzerprofile zu verwenden. Besitzt ein Benutzer ein serverseitiges Profil, werden die Benutzereinstellungen bei jeder Anmeldung an der Domäne in die lokale Konfiguration ("Registry") der Arbeitsstation übernommen. Somit kann ein rechnerunabhängiger Zugriff auf Exchange-Daten erreicht werden.

### Standard-NTFS-Berechtigungen anpassen

Die Standard-NTFS-Berechtigungen auf das Exchange-Verzeichnis müssen angepasst werden, so dass nur autorisierten Administratoren und Systemkonten der Zugriff auf sensitive Daten in diesem Verzeichnis (z. B. Datenbanken und Transaktionsprotokolle) erlaubt ist.

Ist die Benutzung von Outlook Web Access (OWA) geplant, muss für die Gruppe der authentisierten Benutzer ("Authenticated Users") Lese- und Ausführrecht gewährt werden.

Weitere Hinweise, wie die Anforderungen aus dieser Maßnahme konkret umgesetzt werden können, finden sich für die Version 2010 beispielsweise in folgenden Informationen des Microsoft Technet:

- Das rollenbasierte Zugriffsmodell auf Exchange Objekte wird in "Understanding Permissions: Exchange 2010 Help" erläutert.
- Für einfache E-Mail-Benutzer werden die Zugriffsrechte unter "Managing End Users: Exchange 2010 Help" behandelt.

Prüffragen:

- Wurde die Rolle Exchange-Administrator definiert und eine entsprechende Benutzergruppe eingerichtet?
- Wurden die Zugriffsberechtigungen auf Exchange-Objekte auf der Grundlage der Sicherheitsrichtlinie festgelegt?

# M 4.164 Browser-Zugriff auf Exchange 2000

Diese Maßnahme ist mit der 13. Ergänzungslieferung entfallen.

# M 4.165 Sichere Konfiguration von Outlook

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

### Allgemeine Empfehlungen

Es wird empfohlen, Einstellungen in der Microsoft Exchange/Outlook-Umgebung soweit wie möglich durch Administratoren vornehmen zu lassen. Nur in Ausnahmefällen, in denen dies nicht möglich ist, sollten die Einstellungen durch Benutzer vorgenommen werden.

Einstellungen, die durch Administratoren zentral vorgegeben werden, müssen vor Änderungen durch Benutzer geschützt werden, so dass diese das vorgegebene Sicherheitsniveau nicht durch Fehlkonfigurationen abschwächen können. Leider ist dies nicht für alle Einstellungen möglich. Besteht diese Möglichkeit, so wird in den nachfolgenden Empfehlungen darauf hingewiesen.

### Sichere Konfiguration des zugrunde liegenden Betriebssystems

Als Voraussetzung für eine sichere Konfiguration von Microsoft Outlook ist zunächst das zugrunde liegende Betriebssystem sicher zu konfigurieren. Für die allgemeine Konfiguration und Administration von Clients bietet Windows den Richtlinien-Mechanismus an. Es wird empfohlen, diese Richtlinien zu nutzen, da so eine zentrale Administration erreicht werden kann.

### Administrationswerkzeuge

Die Administration bzw. Konfiguration von Microsoft Outlook kann zu unterschiedlichen Zeitpunkten stattfinden: noch vor der eigentlichen Verteilung und Installation von Microsoft Outlook (sogenannte Vorkonfiguration) oder dann, wenn Outlook bereits verteilt ist. Durch Administrationswerkzeuge für Outlook, wie dem Custom Installation Wizard, hat der Administrator beispielsweise die Möglichkeit, eine vorkonfigurierte Version der Outlook-Software für die spätere Verteilung und Installation zentral zu erzeugen.

Für mittlere und große Unternehmen bzw. Behörden wird empfohlen, Administrationswerkzeuge zur Konfiguration und Administration von Outlook-Clients zu verwenden. Der Einsatz von Administrationswerkzeugen erleichtert die Arbeit der Administratoren und verhilft zu einem gleichmäßig hohen Sicherheitsniveau in der Institution. Für kleine Institutionen sollte geprüft werden, ob sich der Einsatz von Administrationswerkzeugen lohnt.

### Verwenden von Benutzerprofilen

Sofern mehrere Benutzer einen PC gemeinsam verwenden, kann für jeden Benutzer ein eigenes Outlook-Profil mit den benutzerspezifischen Einstellungen angelegt werden. In diesem Fall sind die unterschiedlichen Outlook-Profile durch den Administrator einzurichten und gegeneinander abzusichern. Die Benutzerprofile können dabei entweder serverseitig oder auf dem Client abgelegt werden.

Es wird generell empfohlen, serverseitige Benutzerprofile zu verwenden. Es muss dabei beachtet werden, dass Offline-Arbeit (bei der die Daten in einer rechnerlokalen Kopie existieren) nicht möglich ist, wenn serverseitige Profile verwendet werden. Wird dies explizit gewünscht, müssen die Outlook-Profile auf dem Client abgelegt werden. Es ist dabei zu beachten, dass Veränderun-

gen am Profil dann jeweils nur für den lokalen Rechner gelten, so dass ein Benutzer unter Umständen auf verschiedenen Rechnern mit unterschiedlichen Profilen arbeitet.

Auch wenn Outlook-Profile lokal abgelegt werden, wird empfohlen, die Benutzerprofile von einem Exchange-Administrator erzeugen und verteilen zu lassen, damit eine sichere und konsistente Vorkonfiguration erfolgen kann.

**Outlook-relevante Daten sicher lagern**

Outlook-Daten werden in erster Linie im Postfachordner auf dem Exchange-Server gehalten. Es ist jedoch auch möglich, Outlook-Daten lokal auf dem Client zu speichern, wenn z. B. mit Offline-Ordnern (d. h. mit einer lokalen Kopie des serverseitigen Postfachordners) gearbeitet wird oder wenn der Benutzer lokal eigene persönlichen Ordner angelegt hat. Die auf den Clients gehaltenen Outlook-Daten sind generell einem höheren Risiko ausgesetzt als die serverseitig abgelegten Informationen, da für deren Schutz auch der Benutzer zuständig ist. Dieser muss für eigene persönliche Ordner die Sicherheit (z. B. Dateizugriffsrechte) selbst konfigurieren. Es ist deshalb in der Sicherheitsrichtlinie für Outlook festzulegen, ob Outlook-Daten auf den Benutzersystemen gehalten werden dürfen oder nicht. Es wird empfohlen, Outlook-Daten prinzipiell nicht clientseitig zu speichern. Dies schließt jedoch auch aus, dass mit Offline-Ordnern gearbeitet wird.

Kann auf das Arbeiten mit Offline-Ordnern nicht verzichtet werden, so sind die folgenden Empfehlungen für den Schutz der lokal abgelegten Outlook-Ordner zu berücksichtigen. Outlook speichert Informationen in persönlichen Ordnern (.pst-Dateien) sowie im Offline-Ordner (.ost-Dateien), die in diesem Fall auf der lokalen Festplatte des Clients liegen. Es ist zu beachten, dass zusätzlich Daten in den Systemverzeichnissen, den Installationsverzeichnissen von Outlook sowie in den Windows Benutzerprofilen abgelegt werden. Diese sind daher mit restriktiven Zugriffsrechten zu versehen.

**Lokale Outlook-Ordner verschlüsseln**

Es wird empfohlen, lokale Outlook-Ordner (d. h. persönliche Ordner und Offline-Ordner) zu verschlüsseln. Grundsätzlich ist hier die Maßnahme M 4.131 *Verschlüsselung von Lotus Notes Datenbanken* umzusetzen.

Als zusätzlicher Schutz wird empfohlen, den Offline-Ordner bzw. persönliche Ordner in einem eigenen Verzeichnis zu speichern und dieses mit restriktiven Zugriffsrechten zu versehen. Das Verzeichnis sollte nur für den jeweiligen Benutzer zugreifbar sein.

**Kennwortschutz der lokalen persönlichen Outlook-Ordner nicht nutzen**

Für die persönlichen Ordner kann ein Kennwortschutz aktiviert werden, dessen Verwendung jedoch wenig sinnvoll ist. Dieser Kennwortschutz ist schwach und kann mit im Internet verfügbaren Werkzeugen ausgehebelt werden.

Verlangt die Sicherheitsrichtlinie der Institution zusätzlich, dass bestimmte Passwörter hinterlegt werden müssen, so steht der mit dem Kennwortschutz verbundene Sicherheitsgewinn in keinem Verhältnis zum administrativen Aufwand.

Von der Verwendung des Kennwortschutzes wird deshalb abgeraten.

**Zugriffsberechtigungen auf zentrale Outlook-Ordner**

In einer Exchange-Umgebung können persönliche Ordner für andere Benutzer zugreifbar gemacht werden. Es wird generell empfohlen, Zugriffsberechtigungen restriktiv zu vergeben, so dass nur die unbedingt notwendigen Berechtigungen bestehen. Als sichere Grundeinstellung wird empfohlen, nur dem Besitzer und dessen Vertreter den Zugriff zu gestatten.

**Sicherer Umgang mit dem Outlook Journal**

Das Journal erfasst auf einer Zeitskala Aktivitäten, die mit Outlook durchgeführt wurden. Dazu gehören nicht nur gesendete und empfangene E-Mails, Termine und Aufgaben, sondern auch Aktivitäten im Zusammenhang mit Kontakten und Office-Dokumenten.

Journaleinträge können manuell erstellt oder auch automatisch generiert werden. Aus Sicherheitssicht muss beachten werden, dass die im Journal eingetragenen oder automatisch generierten Einträge vertrauliche Informationen und Datei-Verknüpfungen enthalten können. Daher wird empfohlen, Einträge nicht automatisch zu erzeugen.

Im Rahmen der organisatorischen Sicherheitsrichtlinien sollte festgelegt werden, welche Dateien als Verknüpfungen in den Journaleinträgen zugelassen sind.

**Schutz persönlicher Daten gegenüber Systemadministratoren**

Lokal gehaltene persönliche Outlook-Daten (.pst-Dateien) sind durch Administratoren jederzeit einsehbar. Vertraulichkeit gegenüber den Administratoren kann daher nur durch Verschlüsselung erreicht werden.

Beim Einsatz eines dateibasierten Verschlüsselungssystems wird empfohlen, eine Sicherheitsrichtlinie für das Hinterlegen der verwendeten Schlüssel zu definieren, damit der Zugriff auf die verschlüsselten Daten in Notsituationen möglich ist.

**Authentisierung**

Es wird empfohlen, nicht auf die automatischen Anmeldeverfahren der eingesetzten Microsoft Betriebssysteme zurückzugreifen. In diesem Fall wird der Benutzer beim Zugriff auf den Exchange Server explizit aufgefordert, seinen Benutzernamen und sein Passwort anzugeben. In keinem Fall darf das Benutzerkennwort gespeichert werden. Anderenfalls besteht die Gefahr, dass die gespeicherten Kennwörter bei einem lokalen Zugriff auf das Benutzersystem mit öffentlich im Internet verfügbaren Werkzeugen ausgelesen werden.

**Verschlüsselung der Kommunikation**

Wenn Outlook als MAPI-Client eines Exchange-Servers eingesetzt wird, kann die in diesem Fall genutzte RPC-Kommunikation (Remote Procedure Call) zwischen Client und Exchange-Server durch Verschlüsselung geschützt werden. Ob diese Kommunikationsverschlüsselung genutzt wird, muss durch die Sicherheitsrichtlinie für Outlook festgelegt werden.

Die Verschlüsselung ist besonders dann zu empfehlen, wenn die Kommunikation zwischen den Outlook-Clients und dem Exchange-Server über unsichere Netze erfolgt.

**Umgang mit potentiell gefährlichen Dateianhängen**

Dateianhänge dürfen prinzipiell nicht automatisch aus E-Mails heraus geöffnet werden.

Generell wird der Einsatz eines Filters auf einem E-Mail-Gateway oder einem Sicherheitsgateway (Firewall) empfohlen, um E-Mails auf potentiell gefährliche E-Mail-Anhänge zu kontrollieren und diese, wenn nötig, In Quarantäne zu verschieben oder zu löschen. Wird jedoch E-Mail-Verschlüsselung eingesetzt, so sind die auf einem E-Mail-Gateway eingesetzten Filter nicht mehr wirksam. In diesem Fall können E-Mail-Filter auf den Clients eingesetzt werden, die E-Mails nach der Entschlüsselung kontrollieren. Ob lokale E-Mail-Filter eingesetzt werden, muss im Einzelfall entschieden werden. Es ist zu beachten, dass hierdurch zusätzlicher Administrationsaufwand für die Verteilung, Installation und Wartung der Filter-Software entsteht.

Der zusätzliche Einsatz sogenannter Personal Firewalls auf den Clients kann das erreichbare Sicherheitsniveau erhöhen. Diese erlauben Beschränkungen für das Ausführen auf Betriebssystemebene und stellen für ausführbare E-Mail-Anhänge Quarantäne-Bereiche oder Sandboxen (d. h. kontrollierte Ablaufumgebungen) zur Verfügung. Auch hier muss der Einsatz eines solchen Produktes sorgfältig geprüft werden, da zusätzlicher Administrationsaufwand anfällt.

Vom Einsatz lokal installierter Produkte, wie E-Mail-Filter oder Personal Firewalls, wird abgeraten, wenn:

- diese nicht zentral konfiguriert und administriert werden oder
- die vorgegebene Konfiguration durch den Benutzer geändert werden kann oder
- die Konfiguration sogar durch den Benutzer erfolgen muss.

**Vorschaufenster deaktivieren**

Wird das Vorschaufenster bzw. die Autovorschau von Outlook genutzt, werden E-Mails automatisch angezeigt und damit die in ihnen vorhandenen aktiven Inhalte automatisch ausgeführt. Es wird daher empfohlen, das Vorschaufenster und die Autovorschau zu deaktivieren.

**Sicherheitseinstellungen für die Makroverarbeitung in Outlook**

Es wird empfohlen, nur signierte Makros auszuführen, deren Signaturen mit Hilfe bestimmter Zertifikate überprüft werden konnte. Es muss beachtet werden, dass auch hier auf die sogenannten Authenticode-Einstellungen des Microsoft Internet Explorers zurückgegriffen wird. Änderungen wirken sich dadurch auf alle Programme aus, die diese Einstellungen nutzen.

Es wird empfohlen, die Liste der vertrauten Herausgeber zentral zu verwalten und diese mittels Windows-Gruppenrichtlinien zu verteilen. Die zugehörige Richtlinie ist eine Benutzerrichtlinie, so dass für verschiedene Benutzer-Gruppen unterschiedliche Voreinstellungen festgelegt werden können. Es muss sichergestellt werden, dass die Voreinstellungen gegen Veränderungen durch den Benutzer gesperrt sind. Es muss beachtet werden, dass die Makro-Einstellungen nur für VBA-Makros gelten, also für mit Visual Basic for Applications (VBA) erstellte Makros, nicht jedoch für Visual Basic Script.

Dürfen Benutzer die Liste der vertrauenswürdigen Herausgeber selbst aufbauen und verändern, so zeigt sich folgendes Verhalten: Wird ein signiertes VBA-Makro geöffnet und befindet sich das zugehörige Zertifikat nicht in der Liste

der vertrauenswürdigen Quellen, kann der Benutzer entscheiden, ob das Zertifikat in die Liste aufgenommen werden soll oder nicht. Einträge in der Liste vorhandener Zertifikate können auch durch den Benutzer gelöscht werden. Diese Entscheidungen sind sicherheitsrelevant und sollten in der Regel nicht von den Benutzern getroffen werden. Für den Einsatz in Unternehmen und Behörden wird dieses Vorgehen daher nicht empfohlen.

Die Entwicklung eigener Makro-Erweiterungen wird in M 2.379 *Software-Entwicklung durch Endbenutzer* behandelt.

**Konfiguration der E-Mail-Filterregeln**

Unerwünschte E-Mails wie Spam-Mails können das produktive Arbeiten stören. Outlook bietet die Möglichkeit, solche unerwünschten E-Mails mittels spezieller Filterregeln auszufiltern. Es wird jedoch empfohlen, Filtereinstellungen nicht durch Benutzer in der Outlook Client-Software vornehmen zu lassen, sondern das Filtern auf dem Server durchzuführen. Dies hat den Vorteil, dass alle E-Mails konsistent gefiltert werden und beschränkt den administrativen Aufwand auf einen definierten Punkt. Ist eine serverseitige Filterung nicht erwünscht, so wird empfohlen, dass der Administrator die Filterregeln zentral erzeugt.

**Restriktive Stellvertreterberechtigungen**

Outlook/Exchange erlaubt es, für Zeiten der Abwesenheit (z. B. Urlaub oder Krankheit) Stellvertreter zu definieren, die dann die Bearbeitung von E-Mails im Namen des Benutzers übernehmen können. Diese Stellvertreter erhalten Zugriff auf das Postfach bzw. einzelne Outlook-Ordner des jeweiligen Benutzers und können "im Auftrag" E-Mails verschicken. Die Zugriffsberechtigungen für Stellvertreter können für die einzelnen Bestandteile des Outlook-Ordners (Kalender, Kontakte, Posteingang etc.) separat vergeben werden. Die Konfiguration erfolgt in den jeweiligen Objekteigenschaften. Die Stellvertreter-Regelungen sollten in den unternehmens- bzw. behördenweiten Richtlinien verankert sein.

**E-Mails nicht automatisch weiterleiten und verschieben**

Der Regelassistent, mit dem die Filterregeln eingestellt werden, kann auch benutzt werden, um E-Mails automatisch an andere Benutzer weiterzuleiten . Durch unbedacht eingerichtete Weiterleitungen besteht jedoch die Gefahr des Daten- bzw. Vertraulichkeitsverlustes. Dies kann z. B. dann vorkommen, wenn E-Mails unerwartet vertrauliche Mitteilungen enthalten und aufgrund falscher Regeln an Dritte weitergeleitet werden. Es wird daher empfohlen, E-Mails nicht automatisiert weiterzuleiten.

**Erweiterte Funktionalität von Outlook deaktivieren**

Der Outlook-Formulardesigner stellt eine Entwicklungsumgebung für Workflow-Anwendungen auf Basis von Outlook-Verzeichnissen dar. Hierdurch können Sicherheitsprobleme entstehen, da dem Formularentwickler z. B. ActiveX-Steuerelemente zur Verfügung stehen. Normale E-Mail-Anwender benötigen diese Möglichkeit nicht. Es wird daher empfohlen, den Outlook-Formulardesigner auf den Clients zu deaktivieren.

**Nutzung von Folder-Add-Ins und COM-Add-Ins untersagen**

Outlook gestattet es seinen Benutzern standardmäßig, selbständig Add-Ins zu installieren, um den Funktionsumfang von Outlook zu erweitern. Da dabei in

der Regel ausführbarer Code in Form von EXE- oder DLL-Dateien eingebunden wird, müssen Erweiterungen immer zur Verwendung freigegeben werden.

Es muss organisatorisch geregelt werden, dass Benutzer keine eigenen Add-Ins aus dem Internet laden und verwenden.

**Ordner Gelöschte Objekte automatisch Leeren**

Wird der Ordner gelöschte Objekte automatisch geleert, wenn Outlook beendet wird, so hat dies Vor- und Nachteile. Der Hauptvorteil liegt darin, dass der Ordner dann keine "gelöschten" vertraulichen Daten enthält und kein zusätzlicher Speicherplatz verbraucht wird. Der wesentliche Nachteil besteht darin, dass dadurch Daten verloren gehen können. In Umgebungen, in denen häufig vertrauliche Daten über E-Mail ausgetauscht werden, sollte der Ordner gelöschte Objekte automatisch geleert werden.

**Umgang mit Sondernachrichten**

Automatisierte Lese- und Empfangsbestätigungen können zu - gegebenenfalls unbeabsichtigten - Denial-of-Service-Angriffen führen. Sofern die E-Mail-Richtlinie einer Organisation nicht explizit die Verwendung von E-Mail-Bestätigungen vorsieht, wird empfohlen, auf Lese- und Empfangsbestätigungen zu verzichten.

Automatisch generierte Abwesenheitsnachrichten übermitteln zum einen die Information der Abwesenheit eines Mitarbeiters nach außen und können zum anderen als ein Ansatzpunkt für einen Denial-of-Service-Angriff genutzt werden. Es ist deshalb organisationsintern festzulegen, ob diese Funktionalität genutzt werden soll.

**Word als E-Mail-Editor vermeiden**

Unter Microsoft Outlook wird Word standardmäßig als E-Mail-Editor genutzt. Da auch Word-Makros ein Sicherheitsproblem darstellen können, wird davon abgeraten, Microsoft Word als E-Mail-Editor zu nutzen. In der Behörde bzw. im Unternehmen sollte durch eine Richtlinie einheitlich geregelt sein, welcher Editor für E-Mails genutzt wird.

**Weitere Aspekte**

Wird eine E-Mail-Verschlüsselung wie S/MIME eingesetzt, so werden die verschlüsselten Nachrichten in der Regel auch verschlüsselt in das Backup übernommen. Um sicherzustellen, dass später auf diese Informationen zugegriffen werden kann, z. B. im Rahmen einer Reparaturmaßnahme nach einem Notfall, müssen die verwendeten Schlüssel ebenfalls in die Datensicherung einbezogen werden. Weitere Informationen hierzu finden sich in M 6.82 Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen.

**Entfernen schutzbedürftiger Detailinformationen aus eigenen E-Mail-Headern**

Die Header ausgehender E-Mails können Informationen beinhalten, welche nach Möglichkeit nicht nach außen gegeben werden sollten. Dazu zählen beispielsweise Informationen zum Betriebssystem und zur E-Mail-Software des eingesetzten E-Mail-Servers. Serverseitig können Detailinformationen entfernt werden, siehe auch M 4.162 *Sichere Konfiguration von Exchange-Servern*.

**Einsatz eines Virenscanners**

Der Einsatz eines Viren-Schutzprogramms wird in jedem Fall empfohlen. Den größten Schutz bietet dabei eine kombinierte Gateway-Client-Lösung, die sowohl server- als auch clientseitige Komponenten beinhaltet. Es muss gewährleistet sein, dass alle Dateianhänge einer E-Mail geprüft werden. Dies gilt auch für komprimierte oder verschlüsselte Anhänge.

**Software- und Systempflege**

Die zuständigen Administratoren sollten sich regelmäßig im Internet über neu entdeckte Schwachstellen in Exchange/Outlook informieren. Die verfügbaren Patches sollten zunächst innerhalb einer Testumgebung und dann für den Produktivbetrieb eingespielt werden.

Außerdem empfiehlt es sich, für die konkrete Umsetzung der Anforderungen aus dieser Maßnahme die Informationen aus dem Microsoft Technet hinzuziehen. Beispielsweise wird die sichere Konfiguration von Microsoft Outlook 2010 im Sicherheitsleitfaden zu Microsoft Office 2010 vorgestellt: "Security and protection for Office 2010 Beta". Sicherheitsanforderungen ergeben sich direkt aus den Anleitungen für Administratoren für Microsoft Outlook unter "Configuration and deployment of Office 2010 Beta".

Prüffragen:

- Werden Änderungen von administrativen Einstellungen von Outlook durch Benutzer verhindert?
- Ist der Umgang mit Benutzerprofilen für Outlook geregelt?
- Werden Anhänge so behandelt, dass diese nicht automatisch geöffnet werden?

# M 4.166 Sicherer Betrieb von Exchange-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach der Installation und Konfiguration der eingesetzten Exchange-Server müssen Maßnahmen zu deren sicheren Betrieb ergriffen werden.

### Administrative Aspekte

Bei der Administration und der Vergabe von Berechtigungen sollte stets das Prinzip des geringsten Privilegs ("least privilege") beachtet werden. Dies gilt vor allem in Bezug auf die Exchange-Administratoren: Jeder Administrator sollte nur diejenigen Rechte erhalten, die zur Wahrnehmung seiner Aufgaben notwendig sind.

Es wird empfohlen, administrative Tätigkeiten auf Betriebssystemebene und Exchange-Anwendungsebene soweit wie möglich zu trennen. Es sollte jedoch beachtet werden, dass dies nicht uneingeschränkt möglich ist: Für einige Aufgaben benötigen Exchange-Administratoren auch lokale Administratorrechte (so z. B. zum Starten und Stoppen von Diensten).

### Software- und Systempflege

Eine wichtige Voraussetzung für den sicheren Betrieb von IT-Systemen ist, dass alle sicherheitsrelevanten Service Packs, Updates und Patches für das Softwareprodukt eingespielt werden. Es ist daher erforderlich, dass sich die Administratoren regelmäßig über neu bekannt gewordene Schwachstellen in der eingesetzten Exchange und Betriebssystemen informieren und geeignete Maßnahmen zu deren Beseitigung zeitnah umsetzen. Vor dem Einspielen eines Service Packs, Updates oder Patches in das Produktivsystem sollte dies jedoch zunächst in einer Testumgebung geschehen. So kann überprüft werden, ob unerwünschte Seiteneffekte zu erwarten sind. Darüber hinaus sollten die Konfigurationseinstellungen des Gesamtsystems regelmäßig daraufhin überprüft werden, ob sie den Vorgaben entsprechen und den Sicherheitsanforderungen genügen.

### Konfiguration der Exchange-Konnektoren

In einer Umgebung mit mehreren Mail-Servern muss die Sicherheit der Nachrichtenübertragung gewährleistet werden, was eine entsprechende Konfiguration der Routing-Konnektors bedeutet. Die Verbindungen zwischen Servern einer Routing-Gruppe werden während der Installation automatisch konfiguriert. Die Einstellungen der einzelnen Konnektoren müssen jedoch manuell angepasst werden, um ein höheres Sicherheitsniveau zu erreichen.

Es ist zu beachten, dass für die Konfiguration der Exchange-Konnektoren nicht nur Exchange-Administratorrechte, sondern auch Windows-Administratorrechte erforderlich sind.

### Datensicherung

Als Grundlage für die schnelle Wiederherstellung der Daten, z. B. nach einem Systemausfall, muss regelmäßig eine Datensicherung des Exchange-Systems und des Active Directory angelegt werden (siehe M 6.149 *Datensicherung unter Exchange*).

**Ausfallsicherheit und Notfallplanung**

Als Vorsorge sollte schließlich eine praktikable Notfallplanung vorliegen. Die Notfallplanung für Microsoft Exchange-Systeme muss sich in die Notfallplanung des jeweiligen Windows-Server-Netzes (siehe M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*) integrieren. Für den sicheren und unterbrechungsfreien Betrieb von Microsoft Exchange muss der Global Catalog Server stets erreichbar sein. Um die Auswirkung des Ausfalls eines Microsoft Exchange-Systems zu verringern, können Exchange-Daten durch Partitionierung auf mehrere Server verteilt werden. Der Ausfall eines einzelnen Servers betrifft dann nur einen Teil der Daten. Die Partitionierung ist bedarfsgerecht zu planen und durchzuführen.

Für das aktuelle eingesetzte Exchange-System müssen ein Notfallplan und ein Wiederanlaufplan erstellt werden. Die hier zu erfassenden Details für die notwendigen Notfall- und Wiederanlaufmaßnahmen sind bei jeder Exchange Version sehr speziell. Beispielsweise bietet Microsoft Exchange Server 2010 umfassende Hochverfügbarkeitsfunktionen, mit denen Schäden in Notfallsituationen reduziert werden können. Diese sind im Microsoft Technet unter "High Availability and Site Resilience: Exchange 2010 Help" beschrieben. Als Disaster-Recovery-Optionen werden vor allem das Restaurieren eines Servers (siehe "Recover an Exchange Server: Exchange 2010 Help") und das Restaurieren von Daten über eine Recovery Datenbank (siehe "Restore Data using a Recovery Database: Exchange 2010 Help") angeführt. Daher ist es wichtig, die jeweiligen Notfall-Vorkehrungen durch entsprechende Notfallübungen zu testen.

**Schutz vor Denial-of-Service-Attacken (DoS)**

Als Schutz vor DoS-Attacken wird empfohlen, Einschränkungen der maximal möglichen Nachrichten- bzw. Speichergrößen einzuführen. Dies gilt vor allem für eingehende Verbindungen.

Ein weiterer Mechanismus ist die Filterung von Nachrichten. Damit können zwar keine großangelegten Spam-Angriffe abgewehrt werden, jedoch kann dieser Mechanismus für die Filterung einzelner Absender sinnvoll eingesetzt werden.

Wie diese Anforderungen konkret umzusetzen sind, kann den Informationen aus dem Microsoft Technet entnommen werden, beispielsweise für die Version 2010 in folgenden Dokumenten:

- Antispam und Antivirus-Funktionen werden unter "Managing Anti-Spam and Antivirus Features: Exchange 2010 Help" beschrieben.
- Der Einsatz von Antivirus-Lösungen, Betriebssystemhärtung und Softwarepflege werden im Sicherheitshandbuch betrachtet ("Exchange 2010 Security Guide: Exchange 2010 Help").
- Relevante Details zu unterstützten Datensicherungsoptionen und Ausfallsicherheit finden sich unter "Understanding Backup, Restore and Disaster Recovery: Exchange 2010 Help".
- Die Überwachung und Protokollierung eines Exchange Servers 2010 wird über das Microsoft Operations Framework (siehe "Monitoring and Operations Management: Exchange 2007 Help") analog Microsoft Exchange 2007 realisiert. Spezifische Monitoring-Funktionen werden in "Monitoring Exchange 2010: Exchange 2010 Help" beschrieben.

Prüffragen:

- Wurden geeignete Maßnahmen zur Gewährleistung des sicheren Betriebs der Exchange-Systeme ergriffen?
- Werden alle sicherheitsrelevanten Updates zeitnah eingespielt?
- Existieren aktuelle Notfall- und Wiederanlaufpläne für das Exchange-System?

# M 4.167 Überwachung und Protokollierung von Exchange 2000 Systemen

Diese Maßnahme ist mit der 13. Ergänzungslieferung entfallen. Die Inhalte wurden in M 4.166 *Sicherer Betrieb von Exchange-Systemen* integriert.

# M 4.168 Auswahl eines geeigneten Archivsystems

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Archivverwalter, Leiter IT

Die Auswahl eines Archivsystems erfolgt auf der Grundlage der im Archivierungskonzept (siehe hierzu M 2.243 *Entwicklung des Archivierungskonzepts*) festgeschriebenen Vorgaben.

Typischerweise werden folgende Mindestanforderungen an das einzusetzende Archivsystem gestellt, wobei individuelle organisationsspezifische Anforderungen zu ergänzen sind:

- Anbindung an die vorhandene Systemumgebung
  Das Archivsystem sollte die erforderlichen Schnittstellen zur Anbindung an die vorliegende Systemumgebung (Netz, Server, Clients, Systemmanagement) aufweisen. Systeme zur Datenein- und -ausgabe, wie Scanner, Textverarbeitung, Drucker, etc., sind typischerweise nicht Bestandteil des Archivsystems, sondern werden auf Anwendungsebene bereitgestellt.
- Anbindung an ein Dokumentenmanagementsystem
  Das Archivsystem sollte Schnittstellen zur Anbindung an ein Dokumentenmanagementsystem (DMS) aufweisen.
- Versionierung von Dokumenten
  Das Archivsystem sollte die mehrfache Speicherung von Dokumenten in unterschiedlichen Fassungen unterstützen (Versionierung).
- Zugriffsschutz auf die archivierten Daten
  Durch das Archivsystem sollte ein Zugriffsschutz auf die archivierten Daten und die Funktionen des Archivsystems umgesetzt werden können. Dies sollte auf der Grundlage eines vorgegebenen Berechtigungskonzepts erfolgen.
- Mehrstufiges, rollenbasiertes Berechtigungskonzept
  Bei einer rollenbasierten Rechtevergabe werden Zugriffsrechte nicht an konkrete Benutzer vergeben, sondern an definierte Benutzergruppen (Rollen). Im Gegensatz zu normalen Berechtigungsgruppen werden in einem rollenbasierten Zugriffsmodell auch Rollenkonflikte berücksichtigt. Dies bedeutet zum Beispiel, dass eine Person nicht gleichzeitig die Rolle des Administrators und des Revisors einnehmen kann.
- Protokollierung
  Das Archivsystem sollte eine Protokollierung ermöglichen, die alle Vorgänge rund um die Archivierung nachvollziehbar macht (siehe auch M 4.172 *Protokollierung der Archivzugriffe*). Dabei sollte es auch möglich sein, kritische Ereignisse zu definieren und einen Administrator zu benachrichtigen, wenn solche auftreten.
- Einrichtung eines Benutzerkontos für die Revision
  Für Zugriffe im Rahmen der regelmäßigen Revision des Archivsystems sollte ein entsprechendes Benutzerkonto mit den für die Revision notwendigen Rechten eingerichtet werden. Die konkrete Rechtevergabe ist organisationsintern festzulegen. Im Rahmen der Revision werden typischerweise Leserechte (read-only) auf Konfigurationsdaten und Protokolldaten eingerichtet.
- Erweiterbarkeit des Archivsystems
  Das Archivsystem sollte erweiterbar sein, damit es bei Änderungen der Anforderungen angepasst werden kann. Die Erweiterbarkeit betrifft vor allem die eingesetzten Speicherkomponenten und Speichermedien, aber

auch sonstige Hardware-Änderungen sowie die Archivsystem-Software und Nutzungslizenzen.

- Geringe Zugriffszeit
  Für das Archivsystem wird typischerweise eine geringe Zugriffsverzögerung und gleichzeitig eine hohe Bandbreite bei der Übertragung und Bereitstellung der angeforderten Dokumente verlangt. Die Anforderungen sind organisationsspezifisch zu ermitteln. Hierbei ist neben der Einbindung in die vorhandene Systemumgebung auch das abzusehende Benutzerverhalten zu berücksichtigen.
  Die festgelegten Anforderungen wirken sich auf die Auswahl der Archivmedien und der Speicherlaufwerke aus. Ebenso können die Anforderungen die Auswahl und Dimensionierung von Cache-Komponenten beeinflussen.
- Ausreichende Kapazität der Archivmedien
  Die Archivmedien sollten eine ausreichende Kapazität aufweisen. Sowohl die mehrfache Speicherung von Dokumenten zur Versionierung als auch die zu erwartende Datenmenge sollten bei der Kapazitätsplanung berücksichtigt werden.
- Systemgesteuertes Einlegen oder Entnehmen von Archivmedien
  Das Archivsystem sollte generell eine systemgestützte Entnahme der Archivmedien aus Laufwerken unterstützen. Hierdurch soll gewährleistet werden, dass Archivmedien nur nach kontrollierter Offline-Schaltung (unmount) sowie unter Beachtung entsprechender Zugriffsrechte entnommen werden und die Entnahme protokolliert werden kann. Gleiches gilt für die Online-Schaltung (mount) von Archivmedien. Dies ist erforderlich, damit eine konsistente Verwendung der Archivmedien sichergestellt ist.
  Für Notfälle sehen in der Regel alle Archivsysteme und Laufwerke manuelle Möglichkeiten vor, Archivmedien zu entnehmen.
- Kapazitätsüberwachung der Archivmedien
  Die Restkapazität der in Benutzung befindlichen Archivmedien muss laufend überwacht werden. Bei Unterschreiten einer Restkapazitätsgrenze muss eine Signalisierung bzw. Alarmierung erfolgen.
- Alarmierung und Signalisierung
  Das Archivsystem muss die Signalisierung von Systemmeldungen an übergreifende Systemmanagement-Umgebungen gestatten. Wenn keine Anbindung an eine Systemmanagement-Umgebung vorgesehen ist, so sollte eine individuelle Alarmierung über E-Mail, SMS oder SNMP möglich sein.
- Einhaltung von Standards
  Die Einhaltung von Standards erleichtert die Interoperabilität zwischen einzelnen Komponenten. Dies ist erforderlich, weil damit gerechnet werden muss, dass im Betriebszeitraum einzelne Komponenten ausgetauscht werden müssen oder das System erweitert werden soll.
  Standards sind in folgenden Bereichen relevant:

    - Archivmedien und Aufzeichnungsverfahren (siehe M 4.169 *Verwendung geeigneter Archivmedien*),
    - Dateiformate und Komprimierungsverfahren (siehe M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*),
    - Dokumentenmanagementsysteme (siehe M 2.259 *Einführung eines übergeordneten Dokumentenmanagements*).

Es sollte überlegt werden, die Daten durch Verschlüsselung und digitale Signatur zu schützen. Dies wird jedoch typischerweise nicht durch das Archivsystem implementiert, sondern auf Anwendungsebene, z. B. durch das Dokumentenmanagementsystem.

Eine Ausnahme bildet die Grundverschlüsselung von Archivmedien durch das Archivsystem. Hierdurch soll ein Missbrauch des Archivmediums außerhalb des Archivsystems verhindert werden. Diese Grundverschlüsselung wird jedoch für den IT-Grundschutz nicht gefordert.

Prüffragen:

- Erfüllt das ausgewählte Archivsystems die im Archivierungskonzept formulierten Anforderungen?

# M 4.169 Verwendung geeigneter Archivmedien

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die dauerhafte elektronische Archivierung von Dokumenten erfordert den Einsatz geeigneter Datenträger (Archivmedien). Für die Wahl der Archivmedien sollten folgende Fragen berücksichtigt werden:

- Welches Datenvolumen soll archiviert werden?
- Welche Zugriffszeiten sind im Mittel zu erbringen?
- Wie hoch ist die Zahl gleichzeitiger Zugriffe im Mittel?
- Welche Aufbewahrungsfristen sollen durch das Archivmedium abgedeckt werden?
- Sollen Daten "revisionssicher" gespeichert werden?

In den folgenden Abschnitten werden typische Archivmedien und deren Einsatzbereiche beschrieben. Für die Datenträger werden üblicherweise magnetische, magnetooptische oder optische Speichertechnologien verwendet. Die Vorzüge und Nachteile der Technologien sind in den jeweiligen Abschnitten beschrieben.

Sämtliche beschriebenen Archivmedien sind anfällig gegenüber physikalischen Beschädigungen, etwa durch

- Wasser,
- Feuer bzw. Hitzeentwicklung,
- Verkratzen des Mediums durch das Laufwerk infolge Verschmutzung oder Herunterfallen,
- Zerknittern und Aufreißen des Mediums im Bandlaufwerk sowie
- Sabotage und Diebstahl.

Archivmedien müssen daher sorgsam aufbewahrt und vor den genannten Einflüssen geschützt werden. Außerdem muss der unbefugte Zugriff auf die Datenträger verhindert werden. Hierzu wird, abhängig vom konkreten Einsatzszenario des elektronischen Archivs, die Anwendung der im Baustein B 2.5 *Datenträgerarchiv* bzw. B 2.7 *Schutzschränke* beschriebenen Maßnahmen zum Schutz der Datenträger empfohlen.

### Digitale magnetische Systeme

Bei magnetischen Speichersystemen wird durch gezielte lokale Veränderung eines magnetisierten Grundmediums ein Speichereffekt erzielt. Die Magnetisierung kann durch ein Lesegerät erfasst, die gespeicherten Daten können dadurch gelesen werden. Durch erneutes Einwirken eines Magnetfeldes können die gespeicherten Daten verändert werden. Dies erfolgt gezielt durch Verwendung eines Schreib-/Lesegerätes oder ungezielt durch starke externe Magnetfelder (z. B. elektromagnetische Felder in der Nähe von Transformatoren oder großen Spulen). Dies kann auch unabsichtlich geschehen.

Magnetische Datenträger sind anfällig gegenüber Angriffen mit starken Magnetfeldern, die auf das Speichermedium einwirken. Da das magnetisierte Grundmedium typischerweise als Verbundwerkstoff aus Kunststoffen sowie einer metallischen (magnetisierbaren) Beschichtung hergestellt wird, ist außerdem auch bei sorgsamer Behandlung mit langfristigen Veränderungen zu rechnen. Diese können z. B. durch Zersetzung (durch Weichmacher in Kunst-

stoffen), Aufquellen (Ablösung von Kunststoff- und Metallschichten) oder Oxydation (der Metallschicht) bedingt sein.

Aufgrund der verwendeten Technologie sind magnetische Speicher zudem stets wiederbeschreibbar bzw. löschbar und daher ohne zusätzliche Sicherungsverfahren prinzipiell nur für die kurzfristige Archivierung geeignet, bei der kein Schutz gegen Veränderung bzw. Wiederbeschreiben von Dokumenten durch das Medium erbracht werden muss. Dies schließt typischerweise die Verwendung als Archivmedium aus, wenn eine revisionssichere Archivierung gefordert wird. Dagegen können magnetische Systeme für Datensicherungen und als Cachemedien eingesetzt werden.

Die Revisionssicherheit kann mit hohem Aufwand durch den Einsatz kryptographischer Verfahren, die eine Veränderung an den Daten erkennen lassen, erreicht werden (z. B. Signierung).

Typische magnetische Speicher sind Festplatten, Disketten und (Magnet-) Bandmedien.

- **Disketten**
  Disketten, die derzeit in Abmessungen von 3,5 Zoll, früher auch 5,25 Zoll und größer, angeboten werden, weisen eine geringe Kapazität von 1,44 MB auf. Der Einsatz von Disketten als Archivmedium wird nur für sehr kleine Archive empfohlen, in denen keine revisionssichere (schreibgeschützte) Archivierung gefordert wird.
- **Festplatten**
  In Festplatten sind typischerweise das Speichermedium und das Schreib-/Lese-Laufwerk zusammen in einer Einheit untergebracht. Sie sind daher fehleranfällig gegen mechanische Ausfälle, wie z. B. des Laufwerkantriebs. Durch die physikalische Kapselung wird eine dichtere Anordnung der Magnetmedien bei gleichzeitigem Schutz vor Staubpartikeln ermöglicht, so dass Festplatten im Gegensatz zu Disketten-Laufwerken über mehrere Schreib-Lese-Einheiten verfügen.
  Festplatten weisen typischerweise eine hohe Kapazität und eine geringe Zugriffszeit bei hoher Übertragungsrate auf. Aufgrund der verwendeten Speichertechnologie eignen sie sich nicht für eine dauerhafte, revisionssichere Ablage von Dokumenten. Festplatten finden dagegen Verwendung als Datenträger für das Archivsystem selbst und in Cachesystemen.
- **Magnetbänder**
  Magnetbänder bestehen aus einem aufgewickelten Magnetstreifen, der in der Regel an einem Schreib-Lesekopf sequentiell vorbeigeführt wird. Magnetband und Schreib-Lese-Einheit sind typischerweise nicht miteinander verbunden.
  Magnetbänder weisen technologisch bedingt eine sehr lange Zugriffszeit und eine sehr geringe Übertragungsrate auf. Ihre Speicherdichte und Platzverbrauch sind jedoch vergleichbar mit Festplatten.
  Magnetbänder eignen sich für die Speicherung großer Datenmengen, auf die nur selten und sequentiell zugegriffen werden muss. Sie sind daher geeignet für Backups, bei denen eine mittelfristige, jedoch nicht langfristige Stabilität erwartet wird. Da auch Magnetbänder prinzipiell überschrieben, gelöscht oder durch zufälligen Einfluss von Magnetfeldern verändert werden können, eignen sie sich nicht für die revisionssichere Speicherung von Daten.

Die folgende Tabelle gibt einen kurzen Überblick über die Eignung magnetischer Speichermedien für die elektronische Archivierung:

| Medium | Format und Kapazität | Standard | Verwendung |
|---|---|---|---|
| Diskette | 3,5 - 5,25 Zoll, bis 1,44 MB | de facto | Kurzfristig für sehr kleine Archive, nicht revisionssicher |
| Festplatte | 2,5 - 5,25 Zoll, über 100 GB | Herstellernormen | Kurzfristig für kleine Archive und Cachesysteme, nicht revisionssicher |
| Magnetband | über 80 GB | Herstellernormen | Mittelfristig für Archive mittlerer Größe, nicht revisionssicher |

Tabelle: Eignung magnetischer Speichermedien

**Digitale optische Systeme**

Bei optischen Speichersystemen wird ein Speichereffekt dadurch erzielt, dass das optische Verhalten eines Grundmediums gezielt verändert werden kann. Die Speicherung erfolgt typischerweise durch Veränderung des Grundmediums, indem in eine ebene Grundschicht ("Land") gezielt Vertiefungen ("Pits") erzeugt oder simuliert werden, die beim Lesevorgang ein unterschiedliches optisches Verhalten eines gezielt ausgesandten Laserstrahls hervorrufen. Hieraus lassen sich Bitmuster interpretieren.

Während der Lesevorgang typischerweise bei allen optischen Medien gleich ist (die Wellenlänge des verwendeten Lasers kann sich allerdings unterscheiden), bestehen beim Speichervorgang wesentliche technologische Unterschiede.

- **CD-ROM**
  Die Erzeugung von CD-ROMs (Compact Disk Read Only Memory) erfolgt mechanisch durch Stempelung mit einem Master-Datenträger. Die auf CD-ROM gespeicherten Daten sind typischerweise nicht mehr nachträglich änderbar (WORM). Die Produktion solcher Datenträger ist jedoch nur bei hoher Stückzahl rentabel. Als Archivmedien eignen sich solche Datenträger nicht, da in elektronischen Archiven typischerweise nur eine sehr geringe Stückzahl produziert wird, die nicht rentabel ist. Es gibt jedoch Ausnahmen, z. B. "Jahrgangsarchive" als Beilage zu großflächig verteilten Zeitschriften.
  Für CD-ROMs sind mehrere Standards definiert, wodurch eine breite Herstellerunterstützung besteht. Ihre Speicherkapazität beträgt typischerweise bis zu 650 MB.
- **CD-Recordables (CD-Rs)**
  CD-Rs bestehen im Gegensatz zu CD-ROMs aus einer zusätzlichen Schicht (typischerweise Cyanin oder Phtalocyanin), bei der durch Auspunkten ("Brennen") mit einem Laser eine Lichtreflexion erzeugt werden kann, so dass beim Lesen des Datenträgers ein ähnlicher optischer Effekt wie bei einer CD-ROM erzielt wird. Die Speicherkapazität beträgt typischerweise bis zu 700 MB. Die einmal "gebrannten" Punkte können nicht wieder gelöscht werden. Vorteil gegenüber der mechanischen Stempe-

lung des Datenträgers ist die individuelle Anpassbarkeit. Die Nachteile sind:

- CD-Recordables können in beschränktem Umfang nachträglich geändert werden, da es prinzipiell möglich ist, durch Überbrennen der CD-R weitere Brennpunkte zu erzeugen und dadurch unter Umständen auch gezielte Datenveränderungen bis hin zur Unlesbarmachung der CD-R vorzunehmen. Es können jedoch keine bereits ausgepunkteten Bereiche wieder rückgängig gemacht werden. CD-Rs sind demnach gegenüber der allgemeinen Auffassung keine "echten" Write-Once-Medien (WORM), sondern lediglich nicht-löschbare Datenträger.
- Bei fehlerhaftem Brennvorgang kann eine Lichtreflexion vorgetäuscht werden, die in seltenen Fällen durch eine nur vorübergehende Reaktion der Zwischenschicht erzeugt wird. CD-Rs müssen daher nach einigen Tagen verifiziert werden, um diesen Effekt auszuschließen.
- Bei CD-Rs besteht ein sehr geringes Restrisiko, dass durch spontane Kristallisation der Oberfläche gespeicherte Daten zufällig verändert werden.

  CD-ROMs sind zwar nur einmal beschreibbar, es können aber in weiteren Brennvorgängen mehrere Sitzungen (Sessions) darauf angelegt werden. Bei der Verwendung als Archivmedien ist hiervon unbedingt abzusehen, da dies die Lesbarkeit und Korrektheit der zuerst archivierten Daten gefährden kann.

- **CD-Rewritables (CD-RWs)**

  CD-RWs nutzen ähnlich wie CD-Rs eine Zwischenschicht, die jedoch aus einem aufwändigeren Material (aus Silber, Indium, Antimon und Tellur) besteht, das gezielt in zwei unterschiedlich lichtreflektierende Zustände versetzt werden kann. Dies hängt ab von der Intensität des benutzten Lasers. CD-RWs sind daher mehrfach wiederbeschreibbar bzw. löschbar, bei fehlerhaften Laufwerken auch versehentlich. Sie eignen sich daher nicht für Archive, in denen eine revisionssichere Speicherung der Daten gefordert wird. Die Speicherkapazität beträgt typischerweise bis zu 700 MB.

  Als Archivmedium weist die CD-RW-Technologie analog zur CD-R Schwachstellen auf:

  - Bei fehlerhaftem Brennvorgang kann eine Lichtreflexion vorgetäuscht werden, die in seltenen Fällen durch eine nur vorübergehende Reaktion der Zwischenschicht erzeugt wird. CD-RWs müssen daher nach einigen Tagen verifiziert werden, um diesen Effekt auszuschließen.
  - Bei CD-RWs besteht ein sehr geringes Restrisiko, dass durch spontane Kristallisation der Oberfläche gespeicherte Daten zufällig verändert werden.

- **DVD**

  DVD-Medien (Digital Versatile Disk) sind eine technologische Weiterentwicklung der Compact Disk (CD). DVDs erlauben eine wesentlich höhere Speicherdichte von 4,7 bis zu 17 GB, je nach Hersteller. Das DVD-Format ist im Gegensatz zur CD nicht standardisiert, weshalb derzeit unterschiedliche DVD-Varianten auf dem Markt erhältlich sind.

  Bei einigen DVD-Varianten können Daten übereinander in zwei unterschiedlichen Medienschichten gespeichert werden, die separat mit unterschiedlich fokussierten Lasern gelesen werden können (Dual Layer DVD). DVDs sind derzeit auch als DVD-Recordable (DVD-R) erhältlich. Es wird erwartet, dass künftig auch DVD-RWs am Markt angeboten werden. Für die elektronische Archivierung ist - analog zur CD - insbesondere die Vari-

ante DVD-Recordable interessant, da hierdurch eine revisionssichere Ablage bei hoher Speicherkapazität ermöglicht wird. Allerdings sind dabei dieselben Einschränkungen hinsichtlich des Überschreibschutzes wie bei der CD-R zu beachten.

Neben den weitverbreiteten CD- und DVD-Medien gibt es für die elektronische Archivierung weitere standardisierte optische Medien, die von Herstellern großer Speichersysteme verwendet werden. Die folgende Tabelle gibt einen Überblick über erhältliche Medienformate und die zugehörigen Standards:

| **Format** | **Kapazität** | **Normierung** |
|---|---|---|
| 3,5 Zoll | | ANSI X3.213 |
| CD (5,25 Zoll) | 650 - 700 MB | ISO 9660 |
| DVD (5,25 Zoll) | 4,7 - 17 GB | ISO 13346 |
| 5,25 Zoll, RW | 1 - 2,6 GB | ISO 10089 |
| 5,25 Zoll, WORM | 1 - 2,6 GB | ISO 9171, ANSI X3.191, ANSI X3.211, ANSI X3.214 |
| 12 Zoll | 2,6 - 16 GB | herstellerspezifisch, keine Norm |
| 14 Zoll, WORM | 6,8 - 25 GB | ANSI X3.200 und ISO/IEC 10885 |

Tabelle: Erhältliche Medienformate

Die bei diesen Medien verwendete Technologie gleicht grundsätzlich dem bei CD-R (DVD-R) und CD-RW (DVD-RW) verwendeten optischen Verfahren. Die wesentlichen Unterschiede bestehen in der Verarbeitung zuverlässigerer Materialien und erweiterten Garantieerklärungen der Hersteller. Diese garantieren für wiederbeschreibbare Medien eine Datenstabilität zwischen 10 und 100 Jahren und für WORM-Medien zwischen 30 und 100 Jahren, je nach Hersteller und unter jeweiliger Vorgabe optimaler Einsatzbedingungen.

Auch bei den hier beschriebenen WORM-Medien kann technologisch bedingt nachträgliches Überschreiben bislang nicht genutzter Bereiche nicht ausgeschlossen werden. Es handelt sich demnach auch hier nicht um "echte" Write-Once-Medien, sondern lediglich um nicht-löschbare Datenträger.

Die betreffenden Hersteller bieten in der Regel nicht einzelne Medien an, sondern komplette Speicherlösungen, bei denen meist eine automatische Datenträgerverwaltung erfolgt. Die Speichermedien sind dann mechanisch an die jeweilige Herstellerlösung angepasst und mit einem Gehäuse versehen, so dass sie in den entsprechenden Robotersystemen (Jukeboxen) verwendet werden können.

| **Medium** | **Format und Kapazität** | **Verwendung in Archiven** | **Revisionssicherheit** |
|---|---|---|---|
| CD-ROM | 5,25 Zoll, 650 MB | nicht empfohlen | ja |
| CD-R | 5,25 Zoll, 700 MB | kleine Archive | ja* |
| CD-RW | 5,25 Zoll, 700 MB | kleine Archive | nein |
| DVD | 5,25 Zoll, | nicht empfohlen | ja |

| Medium | Format und Kapazität | Verwendung in Archiven | Revisionssicherheit |
|---|---|---|---|
| | 4 - 17 GB | | |
| DVD-R | 5,25 Zoll,<br>4 - 17 GB | mittelgroße Archive | ja* |
| DVD-RW | 5,25 Zoll,<br>4 - 17 GB | mittelgroße Archive | nein |
| ISO 9171-WORM Medien | 5,25 Zoll,<br>1,3 - 2,6 GB | mittelgroße bis große Archive | ja* |
| ISO 10089-RW Medien | 5,25 Zoll,<br>1,3 - 2,6 GB | mittelgroße bis große Archive | nein |
| 12 Zoll RW, herstellerspezifisch | 12 Zoll,<br>2,6 - 16 GB | große Archive | nein |
| 12 Zoll WORM, herstellerspezifisch | 12 Zoll,<br>2,6 - 16 GB | große Archive | ja* |
| 14 Zoll Medien, herstellerspezifisch | 14 Zoll,<br>6,8 - 25 GB | große Archive | unbekannt |

(* Technologisch bedingt ist ein Überschreiben dieser Medien prinzipiell nicht vollständig zu verhindern. WORM-Medien werden jedoch im Allgemeinen als revisionssicher angesehen.)

Tabelle: Überblick über die Eignung optischer Speichermedien für die elektronische Archivierung

**Magneto-Optische Systeme**

Bei der magneto-optischen (MO) Speichertechnologie werden gespeicherte Daten, ähnlich wie bei optischen Speichern, durch Abtasten eines Speichermediums mit einem Laserstrahl gelesen. Im Gegensatz zu CD-ähnlichen Speichern wird der optische Effekt jedoch nicht durch Vertiefungen in der Oberfläche des Speichermediums verursacht, sondern durch eine Magnetschicht, deren Partikel beim Durchlaufen und Reflexion des Laserstrahls als Polarisationsfilter wirken. Die Polarisation der Oberfläche lässt sich punktuell beeinflussen, indem ein Magnetfeld angelegt wird, das nur an einer (wiederum durch einen Laser) speziell aufgeheizten Region des Speichermediums wirkt. In einem Schreibprozess werden die Regionen der Medienoberfläche gezielt unterschiedlich polarisiert.

Die folgende Tabelle gibt einen Überblick über erhältliche Medienformate und die zugehörigen Standards:

| Format | Kapazität | Normierung |
|---|---|---|
| 3,5 Zoll Format | 128 - 256 MB | ISO Norm 10090 |
| 5,25 Zoll, RW | 1,3 - 9,1 GB | ANSI Norm X3.212 |
| 5,25 Zoll, WORM | 1,3 - 9,1 GB | ISO/IEC 11560, ANSI Norm X3.220 |

Tabelle: Medienformate

Auch bei den hier beschriebenen WORM-Medien kann technologisch bedingt ein nachträgliches unbefugtes Überschreiben (Brennen) bislang ungenutzter Bereiche nicht ausgeschlossen werden. Es handelt sich demnach auch hier nicht um "echte" Write-Once-Medien, sondern lediglich um nicht-löschbare Datenträger.

Magneto-optische Systeme weisen eine hohe Langzeitstabilität (nach Herstellerangaben mehr als 30 Jahre) und eine hohe Speicherkapazität von bis zu 9,1 GB je Medium auf. Die folgende Tabelle gibt einen kurzen Überblick über die Eignung magneto-optischer Speichermedien für die elektronische Archivierung:

| **Medium** | **Kapazität** | **Verwendung in Archiven** | **Revisions-sicherheit** |
|---|---|---|---|
| 3,5 Zoll Format | 128 - 256 MB | nicht empfohlen | nein |
| 5,25 Zoll, RW | 1,3 - 9,1 GB | mittelgroße Archive | nein |
| 5,25 Zoll, WORM | 1,3 - 9,1 GB | mittelgroße Archive | ja* |

(* Technologisch bedingt ist ein Überschreiben der Medien prinzipiell nicht vollständig zu verhindern. WORM-Medien werden jedoch im Allgemeinen als revisionssicher angesehen.)

Tabelle: Speichermedien für elektronische Archivierung

Unabhängig von der Art des gewählten Archivmediums sollte grundsätzlich nach der Speicherung eine Verifikation durchgeführt werden. Zum einen sollte diese durch das System erfolgen, um zu überprüfen, ob ein genaues Abbild der zu speichernden Daten angelegt wurde. Zum anderen sollte aber auch stichprobenartig immer wieder durch den Archivverwalter geprüft werden, ob auch alle für die Archivierung vorgesehen Daten archiviert und nicht durch Fehlkonfigurationen übersehen wurden.

Prüffragen:

- Sind die genutzten Archivmedien für das zu archivierende Datenaufkommen geeignet (z. B. in Bezug auf das zu archivierende Datenvolumen, mittlere Zugriffszeiten und mittlere gleichzeitige Zugriffe auf das Archivsystem)?
- Sind die genutzten Archivmedien für Langzeitarchivierung (z. B. in Bezug auf Revisionssicherheit und Lebensdauer) geeignet?

# M 4.170 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für die Archivierung elektronischer Dokumente müssen geeignete Datenformate gewählt werden. Das Datenformat sollte langfristig eine originalgetreue Reproduktion der Archivdaten sowie ausgewählter Merkmale des ursprünglichen Dokumentmediums (z. B. Papierformat, Farben, Logos, Seitenzahl, Wasserzeichen, Unterschrift) ermöglichen. Die derzeit verwendeten Datenformate sind hierfür unterschiedlich geeignet, ihre Eignung hängt sehr stark vom Einsatzzweck der archivierten Daten und ihren Ursprungsmedien ab. Bei einem Wechsel des Medien- und Datenformats können jedoch in der Regel nicht alle Strukturmerkmale des Ursprungsmediums gleichzeitig abgebildet werden.

Da im Vorfeld meist nicht absehbar ist, welche Merkmale des Originaldokuments bei einer späteren Reproduktion nachgewiesen werden sollen und mit welcher Nachweiskraft dies erfolgen soll, werden Dokumente typischerweise in mehreren elektronischen Datenformaten gleichzeitig archiviert. Dadurch soll eine möglichst hohe Überdeckung der Merkmale des Originaldokuments erreicht werden. Der Konvertierungsvorgang wird häufig als Rendition bezeichnet.

Für die Wahl geeigneter Datenformate sind folgende Kriterien maßgeblich:

- das Datenformat sollte möglichst langfristige Relevanz haben,
- die Dokumentstruktur sollte eindeutig interpretiert werden können,
- der Dokumentinhalt sollte elektronisch weiterverarbeitet werden können,
- Beachtung gesetzlicher Vorschriften,
- die Grammatik und Semantik des Datenformates muss ausführlich dokumentiert sein, so dass eine spätere Migration problemlos möglich ist,
- Merkmale des Originaldokuments (elektronisch oder in Papierform) sollen später eindeutig nachweisbar sein, auch wenn das Originaldokument nicht mehr vorhanden ist.

Typischerweise wird neben einer strukturellen Repräsentation (in einer Strukturbeschreibungssprache) bei Papierdokumenten auch eine graphische Repräsentation des Dokuments archiviert. Hinzu kommen unter Umständen elektronische Signaturen zur Beglaubigung der Authentizität.

In den folgenden Abschnitten werden einige typische Datenformate beschrieben und ihre Eignung für die elektronische Archivierung diskutiert.

### A. Strukturformate

#### SGML

SGML (Standard Generalized Markup Language) ist eine Dokumentenbeschreibungssprache, die die logische Struktur und den Inhalt von elektronischen Dokumenten beschreibt. SGML ist als ISO-Norm 8879 standardisiert.

Neben der Struktur (Syntax) von Dokumenten beschreibt SGML insbesondere die Semantik der Strukturelemente des elektronischen Dokuments. SGML bildet jedoch nicht die konkrete Darstellung und Formatierung der Dokumentinhalte bei der Wiedergabe ab.

Wichtige Merkmale von SGML sind:

- Die Semantik der SGML-Elemente wird separat in der so genannten DTD (Document Type Definition) definiert. Die DTD dient als Grundlage für den Dokumentenaustausch zwischen Institutionen bzw. Applikationen.
- SGML ist für die unabhängige Darstellung und Speicherung von strukturierten Textdokumenten geeignet, da die Layout-Informationen vom Dokumenteninhalt getrennt behandelt werden.
- SGML kann direkt für die Abbildung von Strukturen in Dokumenten-Management-Systemen verwendet werden.

SGML kann als Format für die Langzeitarchivierung von elektronischen Dokumenten genutzt werden. Bei der Archivierung ist jedoch unbedingt auch die Semantikspezifikation (DTD) zu archivieren. Da SGML keinerlei Layout-Informationen beinhaltet, wird empfohlen, zusätzlich zu SGML-Dokumenten eine graphische Repräsentation des Ursprungsdokuments zu archivieren, z. B. im Format TIFF.

**HTML**

HTML (Hyper Text Markup Language) ist eine Strukturbeschreibungssprache für elektronische Dokumente. HTML basiert auf einer Untermenge der SGML-Beschreibungselemente und hat sich zum Standard für die Darstellung und den Dokumentenaustausch im World Wide Web entwickelt.

HTML bietet eine sehr eingeschränkte Zahl möglicher Strukturmerkmale für Dokumente und ist als SGML-Spezialisierung mit impliziter DTD zu verstehen.

Wichtige Merkmale von HTML sind:

- In HTML können Dokumentteile durch "Hyperlinks" zu einer Gesamtdokumentstruktur zusammengefügt werden. Hierdurch können in den laufenden Text Bilder und Textteile eingebunden werden, die physikalisch auf verteilten Servern gelagert sind. Es ist aufgrund der dynamischen Anbindung möglich, dass sich ohne Kenntnis des Dokumentinhabers Teile des Gesamtdokuments ändern, da hinzugelinkte Unterkapitel oder Bilder verändert wurden oder nicht erreichbar sind.
- HTML ist auf die bestehenden Strukturmerkmale festgelegt. Weder die Syntax noch die Semantik der so genannten HTML-Tags kann individuell ergänzt oder erweitert werden.
- Aufgrund der mangelhaften Flexibilität von HTML ist es bei Veränderungen der Anforderungen notwendig, den HTML-Standard zu überarbeiten. Dies erfolgte in den letzten Jahren regelmäßig durch das zuständige Standardisierungsgremium (W3C-Konsortium). Daneben wurden eigenmächtige Erweiterungen durch Hersteller von HTML-Browsern vorgenommen. Auch zukünftig ist mit ständigen Erweiterungen der Sprache zu rechnen.

HTML wird als Format für die Langzeitarchivierung nicht empfohlen. Es ist nicht für die Archivierung geeignet, da aufgrund der mangelhaften syntaktischen und semantischen Flexibilität auch künftig in kurzen zeitlichen Abständen Erweiterungen des HTML-Standards zu erwarten sind.

Es ist zudem nicht geeignet, da aufgrund der dynamischen Struktur der HTML-Dokumente eine Archivierung des Gesamtdokuments erfolgen muss, d. h. inklusive aller verlinkten Bilder, Subdokumente und Querverweise. Bei der Archivierung von HTML-Dokumenten dürfen keine aktiven Links zu nicht archivierten Dokumentteilen mehr vorhanden sein, da nicht sichergestellt werden kann, dass solche externen Dokumentteile bei späteren Reproduktionen zur Verfügung stehen.

**XML**

Aufgrund der eingeschränkten Funktion von HTML wurde vom W3C eine Möglichkeit geschaffen, die Vorteile der Sprache SGML zu nutzen, gleichzeitig aber nicht deren volle Komplexität einzubringen. XML wurde als Teilmenge von SGML entwickelt.

Wichtige Merkmale von XML sind:

- In XML können - im Gegensatz zu HTML - Tags und Attribute neu definiert werden. Hierdurch können Anpassungen an der Syntax und Semantik der Beschreibungselemente vorgenommen werden.
- Analog zu HTML können Links in die Dokumentenstruktur integriert werden. Somit können auf einfache Art und Weise bestehende Dokumente referenziert und z. B. Bilder in Dokumente eingebunden werden.
- XML kann direkt in neueren Web-Browsern angezeigt werden. Zur Darstellung wird eine separate Definition des Layouts in Form der Beschreibungssprache XSL (Extensible Stylesheet Language) benötigt.

XML kann als Format für die Langzeitarchivierung von elektronischen Dokumenten genutzt werden. Bei der Archivierung sind jedoch unbedingt auch die Semantikspezifikation (DTD - Document Type Definition) und ggf. auch die Layout-Informationen, in XSL beschrieben, zu archivieren.

**PDF**

PDF (Portable Document Format) ist ein Dokumentformat, bei dem neben der Strukturinformation von elektronischen Dokumenten auch wesentliche Layout-Informationen mitgespeichert werden.

PDF wurde von der Firma Adobe auf Basis des Datenformats PostScript entwickelt.

Das Erscheinungsbild wird dabei durch einen Datenstrom beschrieben, der eine Reihe von graphischen Objekten enthält. Durch diese Beschreibung ist ein Dokument vollkommen festgelegt. Die Entscheidung über das Erscheinungsbild wird dabei zum Zeitpunkt der Erstellung des Dokuments getroffen und ist dann fixiert. Gegenüber einer rein bildlichen Darstellung (Pixeldarstellung) benötigen Dokumente im PDF-Format meist deutlich weniger Speicherplatz.

Zielsetzung beim Einsatz von PDF ist, das Erscheinungsbild eines elektronischen Dokuments unabhängig von der zur Erstellung benutzten Anwendungs-Software, der Hardware-Plattform oder dem Betriebssystem zu bewahren. PDF eignet sich daher primär für die Archivierung von Dokumenten, bei denen eine Abbildung in Papierform vorgesehen ist bzw. die den Charakter von Briefen und Geschäftsdokumenten haben.

Speziell für die Anforderungen der Langzeitarchivierung wurde mit PDF/A eine Version von PDF als ISO 19005-1:2005 genormt. PDF/A (A steht hier für Archivierung) definiert eine stabile Untermenge von PDF, mit der zu archivierende Dokumente so beschrieben werden können, dass alle erforderlichen Informationen in der Datei selber enthalten sind und zwar vollständig, eindeutig, zugänglich und erschließbar.

PDF/A kann als Format für die Langzeitarchivierung von elektronischen Dokumenten genutzt werden. Hierbei ist die Konformität der Dokumente zur PDF/A-Spezifikation zu überprüfen.

**B. Bildformate**

**TIFF**

Das Format TIFF (Tagged Image File Format) wird zur Speicherung gerasterter Bilder verwendet. Eine TIFF-Datei besteht aus einem Datei-Header und der Bildinformation. Der Header enthält so genannte Tags, in denen Eigenschaften des aufgezeichneten Bildes gespeichert sind, z. B. Auflösung oder verwendete Kompressionsverfahren.

Wichtige Merkmale von TIFF sind:

- Bildinformationen können sowohl in Schwarz/Weiß als auch in Grauabstufungen verlustfrei gespeichert werden, jedoch nur dann, wenn eine Farbtiefe von 24 Bit (Truecolor) gewählt wird. Nur in dieser Stufe können alle Graustufen wiedergegeben werden. Um Farbinformationen originalgetreu aufzunehmen und zu speichern, ist jedoch eine regelmäßige Feineinstellung der optischen Sensoren notwendig, damit die Farbinformation nicht durch Farbverschiebungen verfälscht werden. Dies kann z. B. durch einen Farbabgleich mit Weiß als Referenzfarbe erfolgen.
- Alle gängigen Graphik- und Präsentationsprogramme unterstützen das TIFF Format. Darüber hinaus wird es auch von Archiv- und Workflow-Systemen unterstützt.
- Faxgeräte benutzen TIFF als gängiges Datenformat.
- Die Bilddaten können komprimiert abgespeichert werden. TIFF ist mit den meisten Kompressionsverfahren kompatibel. Zwei der wichtigsten Kompressionsverfahren werden hier kurz angesprochen:

  - ITU/CCITT - Gruppe 4:
    Die ITU-Kompression benutzt TIFF als Eingangsformat. Dabei wird bei normalen Textdokumenten ein Kompressionsfaktor von etwa 1:40 erreicht. Es ist damit ideal geeignet für Schwarz/Weiß-Dokumente. Die Kompression ist verlustfrei.
    Die ITU-Kompression ist im Bereich der Archivierung weltweit standardisiert.
  - JBIG:
    JBIG ist ein verlustfreies Kompressionsverfahren für Schwarz/Weiß-Bilder im TIFF-Format. Es ist in der ISO/IEC-Norm 11544 standardisiert. Im Vergleich zur ITU-Gruppe-4-Kompression arbeitet es bis zu 70% effektiver.
    JBIG ist derzeit nicht so weit verbreitet wie das ITU-Verfahren und wird nicht von allen Herstellern unterstützt.

TIFF ist in komprimierter Form als Format für die Langzeitarchivierung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Es wird empfohlen, ein verlustfreies Kompressionsverfahren zu verwenden, z. B. ITU/CCITT-Gruppe 4, um den benötigten Speicherbedarf zu minimieren.

**GIF**

Das Format GIF (Graphics Interchange Format) wird zur Speicherung gerasterter Bilder verwendet.

Wichtige Merkmale von GIF sind:

- Alle gängigen Graphik- und Präsentationsprogramme unterstützen das GIF-Format. Darüber hinaus wird es auch von Archiv- und Workflow-Systemen unterstützt.
- Die Konvertierung in GIF ist verlustbehaftet, es gehen zugunsten einer geringen Dateigröße Bildinformationen verloren.

- Die Verwendung des Formats GIF in Applikationen ist lizenzpflichtig.

Der Einsatz des Formats GIF wird für die Langzeitarchivierung nicht empfohlen, jedoch kann GIF für die kurz- und mittelfristige Archivierung eingesetzt werden.

**JPEG**

JPEG wurde von der *Joint Photographic Experts Group* entwickelt und eignet sich besonders für Farb- und Grauwertbilder. In diesem Bereich ist die JPEG-Kompression auch effektiver als die ITU-Gruppe-4-Kompression.

JPEG kann anhand einiger Parameter unterschiedlich konfiguriert werden. Je nach Einstellung werden dann unterschiedliche Kompressionsraten erreicht. Allerdings können auch Verluste auftreten.

Wichtige Merkmale von JPEG sind:

- Alle gängigen Graphik- und Präsentationsprogramme unterstützen das Format JPEG.
- Die Konvertierung in JPEG ist in einigen Kompressionsstufen verlustbehaftet, es können dann zugunsten einer geringen Dateigröße wesentliche Bildinformationen verloren gehen.

JPEG ist als Format für die Langzeitarchivierung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Für eine revisionssichere Archivierung wird empfohlen, bei der Auswahl der Kompressionsstufe eine verlustfreie Kompression zu wählen.

**C. Audio- und Video-Formate**

Bei der digitalen Verarbeitung von Audio- und Videodaten entstehen schon bei zeitlich kurzen Aufzeichnungen sehr große Datenmengen. Daher gewinnt eine effektive Kompression an Bedeutung.

Verlustfreie Kompressionsverfahren für Audio- und Videodaten erreichen derzeit jedoch nur Kompressionsraten von etwa 2:1. Gebräuchlicher sind Verfahren, die eine Kompressionsrate bis zu 200:1 erreichen, jedoch nicht verlustfrei arbeiten. Der durch die Kompression entstehende, teilweise erhebliche Datenverlust wird typischerweise in Kauf genommen, solange er mit dem menschlichen Auge bzw. Ohr nicht wahrnehmbar ist bzw. nicht als störend empfunden wird.

Die Eignung verlustbehafteter Kompressionsverfahren für die Archivierung von Video- und Tonmaterial ist anwendungsspezifisch zu prüfen.

Im Folgenden werden einige typische Formate vorgestellt:

**MPEG**

Innerhalb der ISO ist die *Motion Pictures Expert Group* (MPEG) für die Bearbeitung weltweiter Standards zur Kompression digitalisierter Bewegtbilder verantwortlich.

Derzeit sind drei verschiedene Verfahren bekannt:

- MPEG1: Dieses Format gibt es in drei verschiedenen Layern. Layer 3 ist in der Kurzform MP3 bekannt und als Kompression für Audiodaten verbreitet.
- MPEG2: Dieses Format ist derzeit für die Speicherung von Videodaten auf DVD in Gebrauch und als Standard akzeptiert.

- MPEG4: Dieses Format befindet sich noch in der Entwicklung und ist noch nicht abschließend standardisiert.

**ITU H.261**

Im Jahr 1990 wurde der Standard H.261 von der ITU zur Kodierung von Videosignalen verabschiedet. Die Kodierung nach H.261 ist für die Übertragung auf ISDN-Kanälen optimiert und entwickelt worden.

**ITU H.263**

Der ITU-Standard H.263 ist eine Weiterentwicklung des Standards H.261 aus dem Jahr 1995/96. Er ist ursprünglich für Datenraten kleiner als 64 kbit/s entwickelt worden. Dieser Beschränkung existiert heute nicht mehr. Die Bildqualität wurde gegenüber dem Standard H.261 bei deutlich verbesserter Kompression erheblich gesteigert.

Prüffragen:

- Ermöglicht das gewählte Datenformat eine langfristige und originalgetreue Reproduktion der Archivdaten sowie ausgewählter Merkmale des ursprünglichen Dokumentmediums?
- Kann die Dokumentstruktur des ausgewählten Datenformats zur Archivierung eindeutig interpretiert und elektronisch verarbeitet werden?
- Sind die Syntax und Semantik der verwendeten Datenformate für die Archivierung dokumentiert?
- Wird ein verlustfreies Bild-Kompressionsverfahren für revisionssichere Archivierung verwendet?

# M 4.171 Schutz der Integrität der Index-Datenbank von Archivsystemen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Index-Datenbank ist besonders wichtig für das korrekte Funktionieren eines Archivsystems. In ihr sind die Verweise auf sämtliche archivierten Dokumente abgelegt. Fehlende oder beschädigte Einträge in der Index-Datenbank können dazu führen, dass archivierte Dokumente nicht oder nur mit sehr hohem Aufwand wiedergefunden und Geschäftsvorgängen zugeordnet werden können.

Daher muss für einen ordnungsgemäßen Archivbetrieb die Integrität der Index-Datenbank sichergestellt werden und überprüfbar sein. Zur Integritätssicherung sind folgende Empfehlungen zu berücksichtigen:

**Redundante Ablage der Indexeinträge**

In Abhängigkeit von der Archivgröße sind folgende Abstufungen vorzusehen:

Bei *kleinen Archiven mit geringem Datenaufkommen* und geringen Anforderungen an die Antwortzeiten ist es ausreichend, eine tägliche Datensicherung der Index-Datenbank vorzunehmen. Die Datensicherung sollte gemäß Baustein B 1.4 *Datensicherungskonzept* vorgenommen werden.

Bei *Archiven mit hohem Datenaufkommen* sowie hohen Anforderungen an die Antwortzeit sollte die Index-Datenbank selbst redundant ausgelegt, d. h. gespiegelt sein. Auch hier ist zusätzlich eine tägliche Datensicherung durchzuführen. Die gespiegelten Teil-Datenbanken sollten in unterschiedlichen Brandabschnitten aufgestellt sein.

**Regelmäßige Integritätsprüfung**

Die Index-Datenbank sollte regelmäßig (mindestens wöchentlich, bei großen Archiven täglich) geprüft werden, ob sie konsistent und integer ist. Alle in der Index-Datenbank referenzierten Dokumente müssen auf den Archivmedien auffindbar sein. Integritätsverletzungen müssen dokumentiert und zeitnah behoben werden.

In regelmäßigen Abständen (z. B. monatlich) sollte zudem geprüft werden, ob die Datensicherungen der Index-Datenbank lesbar und wiederverwendbar sind. Bei redundant ausgelegten Datenbanken sollte getestet werden, ob die Funktionsübergabe bei Ausfall eines Teils ordnungsgemäß funktioniert.

Alle Ergebnisse der regelmäßigen Integritätsprüfung sollten ebenfalls archiviert werden, damit Datenänderungen später nachvollzogen werden können.

Prüffragen:

- Ist die Integrität der Index-Datenbank von Archivsystemen sichergestellt und überprüfbar?
- Erfolgt eine regelmäßige Datensicherung der Index-Datenbank des Archivsystems?
- Wird regelmäßig überprüft, ob die Datensicherungen der Index-Datenbank wiederherstellbar sind?

- Ist bei mittleren und großen Archiven die Index-Datenbank redundant ausgelegt?
- Befinden sich bei Archiven mit hohem Datenaufkommen die gespiegelten Datenbankteile in unterschiedlichen Brandabschnitten?

# M 4.172 Protokollierung der Archivzugriffe

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Zugriffe auf elektronische Archive sind zu protokollieren. Hierdurch soll die Nachvollziehbarkeit der Aktivitäten gewährleistet und eventuelle Fehlerkorrekturen ermöglicht werden. Die folgende Aufzählung gibt einen Überblick darüber, welche Arten von Ereignissen mit Hilfe der Protokollierung erkannt werden können:

- Vertraulichkeits- bzw. Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer,
- fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- Ausschalten des Servers im laufenden Betrieb,
- Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen,
- defekte Datenträger,
- Verlust gespeicherter Daten,
- Datenverlust bei erschöpftem Speichermedium,
- Manipulation an Daten oder Software,
- unberechtigtes Kopieren der Datenträger,
- Manipulation eines Kryptomoduls,
- Kompromittierung kryptographischer Schlüssel und
- unberechtigtes Überschreiben oder Löschen von Archivmedien.

Der Umfang der Protokollierung richtet sich einerseits nach den Anforderungen an die Nachvollziehbarkeit und Authentizität der in Archiven gespeicherten Dokumente. Andererseits müssen auch die organisationsintern abgestimmten Regelungen, z. B. zum Datenschutz, beachtet werden.

Sofern möglich, sollten mindestens folgende Daten protokolliert werden:

- Datum und Uhrzeit des Zugriffs,
- Clientsystem, von dem aus zugegriffen wurde,
- Archivbenutzer und ausgeübte Benutzerrolle,
- ausgeführte Aktionen sowie
- eventuelle Fehlermeldungen und -codes.

Die Zeitdauer der Aufbewahrung der Protokolldaten ist im Archivierungskonzept festzulegen.

Die Protokolldaten müssen unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei deren Auftreten ein Administrator zu benachrichtigen ist. Solche Vorfälle sollten umgehend signalisiert werden, z. B. unter Nutzung vorhandener Systemmanagement-Umgebungen. Außerdem ist es wichtig, dass die Benachrichtigung rollenbezogen, nicht personenbezogen erfolgt. Wird beispielsweise eine E-Mail an eine konkrete Person geschickt, bleibt die Nachricht unter Umständen unbeachtet, wenn diese Person nicht anwesend ist.

Folgende Ereignisse weisen bei der Archivierung typischerweise eine hohe Kritikalität auf und sollten daher permanent protokolliert, überwacht und bei Auftreten umgehend signalisiert werden:

- Kopieren von Archivmedien,

- Kopieren von Archivsystem-Datenträgern,
- Löschen oder Löschmarkierung von Datensätzen,
- Offline-Schaltung von Archivmedien in Archivsystemen,
- Entnahme von Archivmedien aus dem Archivsystem,
- Einlegen von Archivmedien,
- Online-Schalten von Archivmedien,
- Fehler oder Probleme beim Zugriff auf das Archiv,
- Systemfehler und Timeouts,
- Katastrophenszenarien (Brand, unzulässige Temperatur, Wasser etc.), die in der Regel durch externe Sensorik gemeldet werden.

Nach der Signalisierung sollte das Ereignis sofort geprüft und gegebenenfalls weiter eskaliert werden. Typischerweise erfolgt eine erste Eskalation an den Leiter IT. Organisationsspezifisch können jedoch auch andere Eskalationsprozesse vorgesehen sein.

Prüffragen:

- Werden Zugriffe auf elektronische Archive protokolliert?
- Werden organisationsinterne Regelungen, zum Beispiel zum Datenschutz, bei der Protokollierung von Archivzugriffen beachtet?
- Werden, falls möglich, zu jedem Zugriff Datum, Uhrzeit, Benutzer, Clientsystem und die ausgeführten Aktionen sowie Fehlermeldungen protokolliert?
- Ist die Aufbewahrungsdauer der Protokolldaten im Archivierungskonzept festgelegt?
- Werden Protokolldaten von Archivzugriffen unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet?
- Sind kritische Ereignisse bei Archivzugriffen und deren rollenbezogene Signalisierung definiert?
- Werden kritische Ereignisse sofort nach der Signalisierung geprüft und, falls nötig, laut den organisationsspezifischen Eskalationsprozessen weiter eskaliert?

# M 4.173 Regelmäßige Funktions- und Recoverytests bei der Archivierung

**Verantwortlich für Initiierung:** Archivverwalter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Archivverwalter, Leiter IT

Durch verschiedene Ursachen in den Bereichen Datenträger, Hardware und beim Programmablauf kann es bei der Archivierung zu Datenverlusten kommen. Regelmäßige Funktions- und Recoverytests sind daher unumgänglich.

Datenträger unterliegen ebenso wie alle anderen Archivierungskomponenten Verschleißerscheinungen und sollten daher mindestens einmal jährlich auf Lesbarkeit und Integrität geprüft werden.

Werden Fehler auf einem Archivmedium festgestellt, so ist unverzüglich sicherzustellen, dass die betroffenen Dateien aus dem Backup-Bestand wieder hergestellt werden. Wenn fehlerhafte Archivdatenträger ausgetauscht werden müssen, so sind diese nach der Kopie der darauf enthaltenen Daten sicher zu löschen bzw. zu vernichten (siehe auch M 2.167 *Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten*). Der gesamte Vorgang ist zu dokumentieren.

Alle Hardwarekomponenten, insbesondere die mechanischen Teile des Archivs, müssen regelmäßig auf einwandfreie Funktion geprüft werden. Nur so kann gewährleistet werden, dass archivierte Datenbestände den geforderten Verfügbarkeitsanforderungen entsprechen und beim Schreiben und Lesen der Daten die Datenintegrität gegeben ist.

Der Archivierungsvorgang selbst kann fehlerhaft verlaufen. Mögliche Ursachen können sein: Konfigurationsfehler, Softwarefehlfunktionen (z.B. beim Einsatz neuer Programme), Probleme mit den Speichermedien oder Änderungen und Fehler in der Ablaufsteuerung. Einmal pro Tag ist daher zu überprüfen, ob alle Archivierungsprozesse fehlerfrei abgelaufen sind. Dies kann durch Auswertung von Log-Dateien sowie stichprobenartige Ansicht der erstellten Archivmedien durch den Administrator geschehen.

Die notwendigen Integritätsprüfungen der Index-Datenbank sind in Maßnahme M 4.171 *Schutz der Integrität der Index-Datenbank von Archivsystemen* beschrieben.

Prüffragen:

- Gibt es regelmäßige Funktions- und Recoverytests bei der Archivierung?
- Werden Archivierungsdatenträger mindestens einmal jährlich auf Lesbarkeit und Integrität geprüft?
- Existiert ein eingespieltes Verfahren, um auf Fehler auf Archivmedien zu reagieren (von Wiederherstellung der Daten bis hin zur sicheren Löschung fehlerhafter Archivmedien)?
- Werden alle Hardwarekomponenten des Archivsystems regelmäßig auf ihre einwandfreie Funktion geprüft?
- Wird die Fehlerfreiheit aller Archivierungsprozesse einmal pro Tag überprüft?

# M 4.174 Vorbereitung der Installation von Windows NT/2000 für den IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.175 Sichere Konfiguration von Windows NT/2000 für den IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.176 Auswahl einer Authentisierungsmethode für Webangebote

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für E-Commerce- und E-Government-Anwendungen, personalisierte Webangebote oder nur allgemein zur Realisierung von Zugriffsbeschränkungen auf bestimmte Bereiche eines Webangebots werden Mechanismen zur Identifikation und Authentisierung verschiedener Benutzer benötigt.

In Abhängigkeit von den konkreten Anforderungen an den Schutz der Informationen vor unbefugtem Zugriff und die Qualität der Authentisierung muss eine geeignete Methode ausgewählt werden. Die Wahl der Authentisierungsmethode und die Gründe, die zu der Wahl geführt haben, sollten dokumentiert werden.

**Authentisierungsmethoden bei HTTP**

Das Protokoll HTTP/1.1 sieht zwei verschiedene Methoden zur Benutzerauthentisierung vor.

Die erste Methode ist die so genannte *Basic-Access-Authentisierung*. Dabei sendet der Client den Benutzernamen und das Passwort *Base64*-kodiert im so genannten *Authorization Header* des HTTP-Requests an den Server. *Base64* ist eine Methode zur Kodierung von Binärdaten in 7-Bit ASCII, die hier zur Übertragung von Sonderzeichen über die HTTP-Schnittstelle genutzt wird. Das Passwort ist somit zwar nicht auf den ersten Blick ablesbar, kann aber von einem potentiellen "Lauscher" problemlos ermittelt werden, da es unverschlüsselt ist. Daher ist dieser Authentisierungstyp allenfalls für sehr geringe Vertraulichkeitsanforderungen zu gebrauchen.

Die zweite Methode zur HTTP-Authentisierung ist die *Digest-Authentisierung*. Bei dieser Art der Authentisierung muss auf dem Server das Passwort des Benutzers im Klartext vorliegen. Der Client erhält vom Server einen Zufallsstring, die so genannte Challenge. Aus dieser Challenge und dem Passwort des Benutzers errechnet der Client nach einem standardisierten Verfahren einen so genannten *Digest*, der dann zur Authentisierung an den Server gesandt wird. Da der Server sowohl über den von ihm generierten Zufallsstring, als auch über das Passwort des Benutzers verfügt, kann er den Digest ebenfalls berechnen und so die Authentisierung durchführen. Da bei der Digest-Authentisierung das Passwort nicht über das Netz verschickt wird, eignet sich diese Methode für einen etwas höheren Schutzbedarf.

Ein Problem bei der Verwendung der oben genannten Authentisierungsmethoden ist die Sicherheit der Passwortdaten auf dem Server: Bei Verwendung der Digest-Authentisierung müssen die Authentisierungsdaten der Benutzer auf dem Webserver im Klartext vorhanden sein. Bei Verwendung der Basic-Authentisierung wird meist ein Hash-Wert des Passwortes gespeichert. Eine Sicherung der Passwortdateien auf dem Server vor unbefugtem Zugriff ist daher besonders wichtig.

Neben der HTTP-Authentisierung existiert ein weiterer Weg, Zugriffskontrolle über das HTTP-Protokoll zu realisieren: die Authentisierung kann nicht über den Webserver selbst, sondern über eine serverseitige Anwendung durchge-

führt werden. Dabei werden Benutzername und Passwort über normale HTML Formulare eingegeben und von der Anwendung überprüft. Dieses Verfahren ist häufig bei Internet-Angeboten realisiert. Es sollte jedoch stets beachtet werden, dass Passwörter oder PINs, die im Klartext über das Internet übertragen werden, leicht mitgelesen werden können. Zudem werden natürlich auch sämtliche Daten, selbst wenn sie auf authentisierte Anfragen hin ausgeliefert werden, unverschlüsselt übermittelt.

Manche Webangebote identifizieren die Benutzer über spezielle Cookies, die im Browser gespeichert werden. Da Cookies bei der Verwendung von HTTP ebenfalls im Klartext übertragen werden, ist diese Methode für die Authentisierung beim Zugriff auf schutzbedürftige Informationen ebenfalls nicht geeignet. Da im Zusammenhang mit Cookies noch weitere Sicherheitsprobleme existieren, sollte diese Methode generell nicht verwendet werden.

**Verwendung von SSL**

Wenn im Rahmen von E-Government- oder E-Commerce-Angeboten höhere Anforderungen an die Sicherheit der Authentisierung und die Vertraulichkeit der übertragenen Daten bestehen, dann sollte die Übertragung durch die Verwendung von SSL abgesichert werden (siehe auch M 5.66 *Verwendung von SSL*).

Bei der Verwendung von SSL gibt es zwei verschiedene Betriebsarten: bei der ersten Variante besitzt nur der Server ein Zertifikat. Dies dient dem Benutzer dazu, zu erkennen, dass er wirklich mit dem "richtigen" Server verbunden ist, und ermöglicht nach dem Aufbau einer verschlüsselten Verbindung die sichere Übertragung von Authentisierungsinformationen und Anwendungsdaten.

Ein Server-Zertifikat enthält neben dem Namen der Zertifizierungsstelle auch den Namen des Servers, für den es gültig ist. Es kann von einer Wurzelzertifizierungsstelle (Root-CA) ausgestellt sein oder auch selbst erzeugt werden, beispielsweise mit den im OpenSSL Paket enthaltenen Tools.

Zertifikate, die nicht von einer Wurzelzertifizierungsstelle ausgestellt wurden, die dem Browser bekannt ist, werden vom Browser meist nicht ohne weiteres akzeptiert, sondern der Benutzer muss explizit bestätigen, dass das betreffende Zertifikat akzeptiert werden soll.

Bei der zweiten Variante, verfügt auch der Benutzer über ein Zertifikat, das auf dem Client-Rechner vorhanden sein muss, und das der Browser zur Authentisierung an den Server schickt. Voraussetzung dafür ist jedoch, dass die Zertifizierungsstellen, deren Zertifikate verwendet werden, vertrauenswürdig sind. Dass diese Art der Authentisierung in der Praxis nicht häufiger verwendet wird, liegt an dem Aufwand, der zur Umsetzung einer solchen Lösung erforderlich ist. Die serverseitige Konfiguration ist relativ einfach: Neben der Konfiguration des Webservers für SSL muss ein SSL-Server-Zertifikat beschafft und implementiert werden. Der Aufwand, der für jeden einzelnen Benutzer zu betreiben ist, ist jedoch relativ hoch: Jeder Benutzer muss über ein SSL-Client-Zertifikat verfügen, das jeweils im Browser des Benutzers installiert ist. Dies führt zu einer gewissen Einschränkung der Bequemlichkeit, da einer der großen Vorteile der normalen Webserver-Nutzung gerade darin besteht, dass der Zugriff von praktisch jedem beliebigen Rechner aus erfolgen kann. Werden Client-Zertifikate zur Authentisierung benutzt, so ist diese Flexibilität deutlich eingeschränkt, weil das Client-Zertifikat meist nicht überall vorhanden ist. Andererseits kann in bestimmten Situationen, etwa beim Einsatz eines Intranet-Webservers, genau dies erwünscht sein.

Eine häufig verwendete Methode der Benutzerauthentisierung für Webangebote ist die Kombination von formularbasierter Authentisierung und SSL-verschlüsselter Datenübertragung. Diese Methode bietet, wenn die gewählte SSL-Verschlüsselung ausreichend stark gewählt wird, bei vertretbarem Aufwand (Benutzerverwaltung in der Webanwendung und Implementierung eines SSL-geschützten Zugriffs auf den Webserver) ein Sicherheitsniveau, das auch für höhere Sicherheitsanforderungen angemessen ist.

In M 5.160 *Authentisierung gegenüber Webservern* werden die verschiedenen Möglichkeiten der Benutzerauthentisierung bei Webservern vorgestellt und in der folgenden Tabelle zusammengefasst:

| **Methode** | **Sicherheits-niveau** | **Aufwand für Implementierung** | **Serveranforderungen** | **Kommentare** |
|---|---|---|---|---|
| Standard-Authentisierung | Niedrig | Niedrig | Benutzerverwaltung | Authentisierungsinformationen und Daten werden unverschlüsselt übertragen! |
| Formularbasierte Authentisierung ohne gesicherte Übertragung | Niedrig | Niedrig bis mittel | Implementierung in der jeweiligen Anwendung | Authentisierungsinformationen und Daten werden unverschlüsselt übertragen! |
| Digest-Authenti-sierung | Mittel | Niedrig | Benutzerverwaltung | Daten werden unverschlüsselt übertragen. |
| Formularbasierte Authentisierung über SSL | Hoch | Mittel bis hoch | SSL-Unterstützung im Server, Implementierung in der jeweiligen Anwendung | Authentisierungsinformationen und Daten werden verschlüsselt übertragen! |
| Zertifikatbasierte Authentisierung über SSL | Hoch bis sehr hoch | Hoch bis sehr hoch | Installation von Server-Zertifikaten. Zertifikatsverwaltung, Public-Key Infrastruktur. | Wird hauptsächlich für sichere Transaktionen über das Internet verwendet. |

Tabelle: Benutzerauthentisierung bei Webservern

Der Microsoft Internet Information Server bietet darüber hinaus noch eine weitere Methode, bei der die Windows-Benutzeranmeldung benutzt wird. Diese Methode funktioniert allerdings nur mit dem Microsoft Internet Explorer als Client.

Beim Aufbau einer SSL-Verbindung wird der zu verwendende Verschlüsselungsmodus zwischen Client und Server ausgehandelt. Unter den zur Verfügung stehenden Algorithmen befinden sich auch solche, die nicht mehr als sicher angesehen werden können. Insbesondere gibt es auch den so genannten Null-Encryption-Modus, bei dem keine Verschlüsselung stattfindet. Bei der Konfiguration des Webservers für die Verwendung von SSL muss darauf geachtet werden, dass der Server keinen der schwachen Algorithmen und insbesondere nicht den Null-Encryption-Modus akzeptiert. Andernfalls könnte es dazu kommen, dass scheinbar eine sichere Verbindung aufgebaut wird (es wird https verwendet), die jedoch in Wirklichkeit zu schwach oder gar nicht verschlüsselt ist. Eine solche Situation könnte von einem Angreifer bewusst herbeigeführt werden, um Authentisierungsinformationen und andere Daten abzuhören. Daher sollte in der SSL-Konfiguration des Webservers die Verwendung des Null-Encryption-Modus und der schwachen Algorithmen abgeschaltet werden.

Prüffragen:

- Wurden/Sind die Authentisierungsmethode für Webangebote und die Gründe für deren Auswahl dokumentiert?
- Digest-Authentisierung: Werden Passwortdateien auf dem Webserver vor dem Zugriff Unbefugter geschützt?
- Bei hohen Anforderungen an die Vertraulichkeit: Wird die Authentisierung und die Übertragung von Daten bei Webangeboten durch SSL abgesichert?
- Bei SSL-Verwendung: Werden schwache kryptographische Algorithmen vom Webserver nicht akzeptiert?

# M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Änderungsmanager

Durch unvorsichtiges Ausführen von Programmen, die aus "unsicheren" Quellen stammen, kann beträchtlicher Schaden entstehen. Schadsoftware (so genannte *Malware*) kann beispielsweise Programme zum Ausspähen von Passwörtern, Trojanische Pferde oder Backdoors auf einem Computer installieren, oder ganz einfach Daten beschädigen oder löschen.

Typische Quellen für solche Schadsoftware sind beispielsweise Programme, die sich als Bildschirmschoner, Virenscanner oder sonstige Hilfsprogramme ausgeben, und per E-Mail unter gefälschten Absenderadressen an sehr viele Empfänger verschickt werden. Oft laden auch unvorsichtige Anwender die Programme aus dem Internet herunter und installieren sie ohne Überprüfung.

Zwei Beispiele, bei denen durch die Überprüfung vorhandener digitaler Signaturen Schaden hätte vermieden werden können, sind ein Vorfall vom März 2002, bei dem die Distribution des Pakets *OpenSSH* auf dem ftp-Server des OpenSSH-Projekts manipuliert wurde, und ein ähnlicher Vorfall vom September 2002, bei dem dies mit der Distribution des Mailservers *sendmail* geschah. In beiden Fällen wurden in die Distributionen Trojanische Pferde eingeschleust, die zu einer Kompromittierung des Rechners führen konnten, auf dem die Pakete kompiliert wurden. In beiden Fällen hätte eine Überprüfung der vorhandenen digitalen Signaturen die Manipulation aufdecken können.

Selbst wenn ansonsten keine Verschlüsselungs- oder Signaturtechniken zum Einsatz kommen, sollte die Nutzung in dem Umfang, wie er in dieser Maßnahme beschrieben wird, in Erwägung gezogen werden.

Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, besonders dann, wenn sie nicht auf Datenträgern geliefert, sondern beispielsweise aus dem Internet heruntergeladen wurde. Dies gilt besonders für Updates oder Patches, die normalerweise nicht mehr auf Datenträgern ausgeliefert werden. Die meisten Hersteller und Distributoren bieten zu diesem Zweck Prüfsummen an, die zumindest eine Prüfung der Integrität eines Paketes erlauben. Die Prüfsummen werden dabei meist auf den Webseiten der Hersteller veröffentlicht oder auch per E-Mail verschickt. Um die Integrität eines heruntergeladenen Programms oder einer Archivdatei zu verifizieren, wird dann die veröffentlichte Prüfsumme mit einer von einem entsprechenden Programm lokal erzeugten Prüfsumme verglichen.

Falls zu einem Softwarepaket Prüfsummen angeboten werden, so sollten diese vor der Installation des Paketes überprüft werden.

Eine Überprüfung der Authentizität kann mit Prüfsummen jedoch nicht erfolgen. Daher werden in vielen Fällen für Programme oder Pakete digitale Signaturen angeboten. Die zur Überprüfung der Signatur benötigten öffentlichen Schlüssel sind wiederum meist auf den Webseiten des Herstellers oder von Public-Key-Servern verfügbar. Häufig werden die Prüfsummen mit einem der Programme PGP oder GnuPG erzeugt.

Ergibt die Prüfung, dass es sich um eine gültige Signatur des jeweiligen Herstellers handelt, so resultiert daraus ein deutlich höherer Grad an Vertrauenswürdigkeit für das Paket, als lediglich durch das Vorhandensein einer Prüfsumme.

Das bei Linux-Distributionen verbreitete Paketverwaltungssystem RPM (Redhat Package Manager) hat ebenso wie das Paketverwaltungssystem der Debian-Distribution bereits eine integrierte Überprüfungsfunktionalität.

Manchmal führen selbst die eingebauten Software-Updatemechanismen des jeweiligen Betriebssystems oder der Anwendungssoftware keine Prüfsummenvergleiche durch. Wenn möglich, sollte allerdings bei jedem Softwarepaket vor dem Einspielen ein Prüfsummencheck durchgeführt werden.

Ferner sind nicht alle Prüfsummenvergleiche ohne Mitwirkung der Anwender durchführbar, da die hierfür erforderlichen Checksummen, Signaturen oder Zertifikate von den Herstellern nicht auf eine einheitliche Weise bereitgestellt werden. Daher ist häufig eine manuelle Verifikation auf den Herstellerseiten oder die Anpassung der URLs in der Patch- und Änderungssoftware nötig.

Falls zu einem Softwarepaket digitale Signaturen verfügbar sind, sollten diese auf jeden Fall vor der Installation des Pakets überprüft werden.

Ein prinzipielles Problem bei der Verwendung digitaler Signaturen stellt die Verifikation der Authentizität des verwendeten Schlüssels selbst dar. Trägt der öffentliche Schlüssel keine Signatur einer bekannten vertrauenswürdigen Person oder Organisation (etwa eines Trustcenters), so bieten die mit dem entsprechenden privaten Schlüssel erzeugten Signaturen keine wirkliche Sicherheit, dass das Softwarepaket tatsächlich vom Entwickler, Hersteller oder Distributor stammt. Daher sollten die öffentlichen Schlüssel, sofern sie nicht zertifiziert sind, möglichst aus einer anderen Quelle als das Softwarepaket selbst bezogen werden, beispielsweise von einer CD-ROM des Herstellers, von einem anderen Spiegelserver, auf dem das Paket ebenfalls heruntergeladen werden kann, oder von einem Public Key Server.

Zur Überprüfung von Prüfsummen und digitalen Signaturen müssen die entsprechenden Programme lokal vorhanden sein. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert sein. Außerdem müssen die Administratoren genügend Zeit haben, die entsprechenden Programme im Arbeitsalltag einzusetzen und sich mit der Bedienung vertraut zu machen.

Von einem Bezug von Patches und Änderungen per E-Mail ist aus verschiedenen Gründen abzuraten. Die Herkunft von E-Mails ist ohne Einsatz zusätzlicher Sicherheitsmechanismen schwer festzustellen und die Empfängeradressen in den Institutionen sind oft Verteilerlisten, deren Adresse leicht zu erraten ist. Patches und Änderungen können außerdem mittlerweile sehr umfangreich sein. Viele Unternehmen und Behörden haben die Größe von E-Mail-Anhängen beschränkt und verbieten unter Umständen zudem die Annahme ausführbarer Anhänge. Ferner werden durch die großen Datenmengen die E-Mail-Systeme unnötig belastet. Daher kann eine rechtzeitige Verfügbarkeit der Software-Änderungen, welche besonders bei Sicherheitspatches kritisch sein kann, via E-Mail nicht ausreichend gewährleistet werden.

Des Weiteren bieten einige Hersteller an, Änderungen und Patches dem Kunden direkt auf Datenträgern zuzusenden. Auch in diesem Fall sollten die Patches und Änderungen möglichst anhand von Prüfsummen oder digitalen Si-

gnaturen verifiziert werden, denn Absender-Angaben auf Postsendungen und Hersteller-Logos auf CDs und DVDs lassen sich leicht fälschen.

Ein weiterer Aspekt zur Prüfung der Echtheit der Aktualisierung können vom Hersteller veröffentlichte Nachrichten auf seiner Webseite, per Newsletter oder über ähnliche Kanäle sein. Einige Hersteller haben Zyklen und Zeitpunkte etabliert, zu denen in der Regel systematisch Informationen über Änderungen veröffentlicht werden.

Prüffragen:

- Wurde nachgeprüft, ob für die eingesetzten Softwarepakete Prüfsummen oder digitale Signaturen verfügbar sind?
- Wird Software einer Integritäts- und Authentizitätsprüfung unterzogen, bevor sie innerhalb der Institution verwendet wird?
- Sind die notwendigen Programme zur Überprüfung von Prüfsummen oder digitalen Signaturen verfügbar?

# M 4.178 Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.179 Schutz von sicherheitskritischen Dateien beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.180 Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.181 Ausführen des IIS in einem separaten Prozess

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.182 Überwachen des IIS-Systems

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.183 Sicherstellen der Verfügbarkeit und Performance des IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.184 Deaktivieren nicht benötigter Dienste beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.185 Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.186 Entfernen von Beispieldateien und Administrations-Scripts des IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.187 Entfernen der FrontPage Server-Erweiterung des IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.188 Prüfen der Benutzereingaben beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.189 Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.190 Entfernen der RDS-Unterstützung des IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.191 Überprüfung der Integrität und Authentizität der Apache-Pakete

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.192 Konfiguration des Betriebssystems für einen Apache-Webserver

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.193 Sichere Installation eines Apache-Webservers

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.194 Sichere Grundkonfiguration eines Apache-Webservers

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.195 Konfiguration der Zugriffssteuerung beim Apache-Webserver

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.196 Sicherer Betrieb eines Apache-Webservers

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.197 Servererweiterungen für dynamische Webseiten beim Apache-Webserver

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 4.198 Installation einer Applikation in einem chroot Käfig

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zur Erhöhung der Sicherheit kann eine Applikation in einem sogenannten chroot-Käfig installiert werden. Durch den Systemaufruf *chroot()* wird unter Unix der Zugriff einer bestimmten Applikation auf einen Teil des Dateibaums beschränkt. Dies geschieht dadurch, dass alle Zugriffe, die dieser Applikation und die von ihr aufgerufenen Applikationen auf das Dateisystem durchführt, relativ zu dem Verzeichnis erfolgen, das beim Aufruf der Funktion *chroot()* angegeben wurde. Das Verzeichnis wird so zur Wurzel eines virtuellen Dateibaums, der als *chroot-Käfig* oder *chroot jail* bezeichnet wird. Auf darüber liegende Verzeichnisse und Dateien kann nicht zugegriffen werden. Somit können beispielsweise mehrere Dienste auf einem Server voneinander abgeschottet werden.

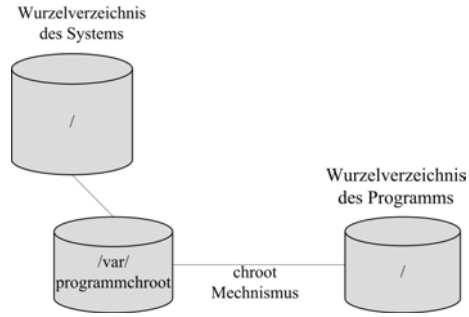


Abbildung: Wurzelverzeichnis

Neben dem Systemaufruf *chroot()* steht auch ein ausführbares Programm gleichen Namens zur Verfügung, das zum Start beliebiger Applikationen in einem solchen chroot-Käfig genutzt werden kann. Wenn es beispielsweise einem Angreifer gelingt, eigenen Programmcode im Prozessraum der Applikation auszuführen, würde der unmittelbare Schaden dadurch begrenzt werden, dass der Angreifer keinen direkten Zugriff auf das eigentliche Betriebssystem erhält. Es existieren Möglichkeiten, aus einem chroot-Käfig auszubrechen. Ein Angreifer muss aber erst erkennen, dass er sich in einem chroot-Käfig befindet. Dadurch wird ein Angriff verzögert. Während dieser Zeit kann eventuell der Angriff erkannt und Gegenmaßnahmen können eingeleitet werden.

Der chroot-Käfig muss Kopien aller Dateien enthalten, die zur Ausführung der Applikation notwendig sind. Welche Dateien dies sind, muss anhand der vorhandenen Dokumentation geprüft werden. Im Normalfall sind dies folgende Dateien und Verzeichnisse: *dev, lib, usr/bin, var, var/run, etc*, und die applikationsspezifischen Dateien und Verzeichnisse.

Wird in Betracht gezogen, eine Applikation in einem chroot-Käfig zu installieren, so muss ausreichend Zeit für Planung und Tests vorgesehen werden. Bei der Installation muss dokumentiert werden,

- welches das Wurzelverzeichnis des chroot-Käfigs ist und
- welche Betriebssystemkomponenten im chroot-Käfig zur Verfügung gestellt werden.

Insbesondere müssen einige *Device Files* im chroot-Käfig angelegt werden, des Weiteren werden entsprechend angepasste Versionen der Dateien */etc/*

*passwd* und */etc/group* benötigt. Aus diesen Dateien sollten alle nicht benötigten Einträge bis auf den Benutzer und die Gruppe unter denen die Applikation betrieben werden soll, entfernt werden. Je nach Betriebssystem können noch weitere Einträge, die in den Dateien verbleiben sollten, erforderlich sein.

Prüffragen:

- Wurde die Konfiguration des chroot-Käfigs ausreichend dokumentiert?
- Wurden alle nötigen Daten in den chroot-Käfig kopiert?

# M 4.199 Vermeidung problematischer Dateiformate

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

E-Mail ist mittlerweile der wichtigste Übertragungsweg für Schadsoftware. Eine rein textbasierte E-Mail ohne Anhänge ist dabei ungefährlich. Gefährlich wird es erst, wenn E-Mail-Anhänge ausgeführt werden, die E-Mail HTML-basiert ist oder die Mail-Empfänger über Links in der E-Mail auf manipulierte Webseiten gelockt werden (siehe unten). Prinzipiell können E-Mails Anhänge in beliebiger Art und Menge beigefügt werden. Durch ein Zuviel an Anhängen kann die Verfügbarkeit eines E-Mail-Clients oder des E-Mail-Servers beeinträchtigt werden (siehe G 5.75 *Überlastung durch eingehende E-Mails*). Die größere Gefahr sind aber Anhänge, die ausführbaren Code enthalten und damit ungeahnte Nebeneffekte auslösen können.

### Anhänge

Anhänge, die ausführbaren Code enthalten, können ungeahnte Nebeneffekte auslösen. Aus diesem Grund muss eine Regelung für den Umgang mit Dateiformaten, die als potentiell problematisch eingeschätzt werden, erstellt werden. Wichtig ist, dass alle Betroffenen sich der Problematik bewusst sind und entsprechend vorsichtig mit diesen Dateiformaten umgehen.

Zum Schutz vor der unbeabsichtigten Ausführung von Schadcode sollten die E-Mail-Clients so eingestellt werden, dass Anhänge nicht versehentlich gestartet werden können, sondern das Programm vor der Ausführung warnt bzw. zumindest nachfragt, ob die Datei geöffnet werden soll. Das Betriebssystem bzw. der E-Mail-Client sollte außerdem so eingerichtet sein, dass Dateien zunächst nur in Viewern oder anderen Darstellungsprogrammen angezeigt werden, die eventuell in den Dateien enthaltenen Programmcode, wie Makros oder Skripte, nicht ausführen.

Sollte ein Benutzer eine E-Mail mit einem potentiell gefährlichen Anhang erhalten, so sollte er sicherstellen, dass die Quelle der E-Mail vertrauenswürdig ist. Dies lässt sich durch Verwendung von kryptographischen Signaturen durch den Versender und durch sachgemäße Überprüfung der Signatur durch den Empfänger realisieren. Auch sollte der Versender von potentiell gefährlichen Anhängen dafür sorgen, dass sein versendeter Anhang tatsächlich ungefährlich ist. Dazu gehört mindestens eine Prüfung mit einem Virenscanner mit aktuellen Schadcode-Signaturen.

### Problematische Dateiformate

Für den Umgang mit Dateiformaten, die als potentiell problematisch eingeschätzt werden, können verschiedene Regelungen getroffen werden. Wichtig ist aber auf jeden Fall, dass alle Betroffenen sich der Problematik bewusst sind und entsprechend vorsichtig mit diesen Dateiformaten umgehen.

Die restriktivste Form ist es, das Öffnen aller als problematisch eingestuften Dateiformate zu verbieten bzw. diese am E-Mail-Gateway herauszufiltern. Dies führt allerdings erfahrungsgemäß zu großen Akzeptanzproblemen seitens der Kunden und der Mitarbeiter. Besser ist es im allgemeinen, einerseits die Mitarbeiter für die Problematik zu sensibilisieren und zum Mitdenken anzuregen und sie andererseits technisch zu unterstützen, indem die Gefährdungspotentiale durch entsprechende Konfiguration und Sicherheitswerkzeu-

ge minimiert werden (siehe auch M 2.224 *Vorbeugung gegen Schadprogramme*, M 5.69 *Schutz vor aktiven Inhalten*).

Im Folgenden werden einige Einschätzungen verschiedener Dateiformate gegeben. Diese können sich allerdings jederzeit ändern, wenn z. B.ein Hersteller seinem Produkt neue Features hinzufügt, die ungeplante Nebenwirkungen haben, bzw. ein Tüftler solche Nebenwirkungen herausfindet.

- Als weitgehend harmlos gelten bisher ASCII-, GIF-, JPEG-formatierte Dateien.
- Als möglicherweise gefährlich sollten die folgenden Dateiformate behandelt werden: alle Dateiformate von Office-Paketen wie Microsoft Office, Star Office oder Open Office mit integrierter Makrosprache, z. B. Word, Excel, Powerpoint (.DOC, .XLS, .PPT, ODT usw.) und alle Dokumente, die interpretierbaren/ausführbaren Code enthalten können, wie z.B. PDF, CHM. Besonders kritisch sind alle ausführbaren Programme (wie .COM, .EXE, .PIF) oder Skript-Sprachen (.VBS, .JS, .BAT unter Windows, ebenso wie Perl- oder Shellskripte unter Unix), Registrierungsdateien (.REG) sowie Bildschirmschoner (.SCR).
  Vorsichtshalber sollte für alle diese Dateitypen eine "ungefährliche" Standardapplikation festgelegt werden, mit der diese zwar geöffnet werden, innerhalb deren aber eventuelle Computer-Viren keinen Schaden auslösen können. Beispielsweise sollten Dateitypen wie *.VBS, *.JS oder *.BAT grundsätzlich mit einem einfachen, nicht makrofähigen Texteditor geöffnet werden.
  Windows-Betriebssysteme sollten außerdem so konfiguriert sein, dass bei Registrierungsdateien (.REG) als Standardvorgang *Bearbeiten* statt *Zusammenführen* eingestellt ist. Dadurch wird die Datei zunächst in einem Editor dargestellt und nicht der Registrierungsdatenbank hinzugefügt, wenn sie aktiviert wird.
- Mit Zusatzmaßnahmen als vertretbar angesehen werden können: HTML, wenn ein JavaScript-Filter oder andere Sicherheitsvorkehrungen eingesetzt werden, RTF (mit COM-Object-Filter), ZIP (hier sollten die Benutzer allerdings gewarnt werden, dass die enthaltenen Dateien problematisch sein können), PDF (dabei ist darauf zu achten, dass der PDF-Reader auf dem Endgerät als Standard installiert ist und nicht Adobe Acrobat).

Eine als Anlage mitversandte komprimierte Datei kann sich als Mailbombe erweisen, die nach dem Auspacken Unmengen von Unterverzeichnissen anlegt oder sehr viel Festplattenplatz beansprucht. Archive, also mit Packprogrammen komprimierte Dateien, sollten niemals ohne vorhergehende Prüfung ausgepackt werden. Dazu gehört die Sichtung des Inhaltsverzeichnisses auf Art und Größe der komprimierten Dateien und die Überprüfung auf Schadsoftware. Selbstextrahierende Archive, also solche mit Endungen wie *.EXE, sollten niemals aufgerufen werden, da vor dem Auspacken der Inhalt nicht geprüft kann.

**HTML-Mails**

Immer mehr E-Mails sind heutzutage auch HTML-formatiert. Dies ist einerseits oft lästig, weil nicht alle E-Mail-Clients dieses Format anzeigen können. Andererseits kann dies aber auch dazu führen, dass bereits bei der Anzeige solcher E-Mails auf dem Client ungewollte Aktionen ausgelöst werden, da HTML-Mails eingebetteten JavaScript- oder VisualBasic-Skript-Code enthalten können.

Über im HTML-Quelltext eingebettete Bilder lässt sich auch eine Rückkopplung vom E-Mail-Client zum Spammer realisieren. Wird das eingebettete Bild durch Anzeige der E-Mail aus der Quelle im Internet nachgeladen, weiß der Spammer, dass seine E-Mail gelesen wurde und bekommt somit eine Bestäti-

gung, dass der Empfänger gültig ist und Spam-E-Mails liest. Das automatische Nachladen von HTML-Objekten sollte im E-Mail-Client unterbunden werden.

Durch Kombination verschiedener Sicherheitslücken in E-Mail-Clients und Browsern ist es in der Vergangenheit immer wieder zu Sicherheitsproblemen mit HTML-formatierten E-Mails gekommen (siehe auch G 5.110 *Web-Bugs*). Ein Beispiel hierfür findet sich unter anderem im CERT-Advisory CA-2001-06 (unter *http://www.cert.org/advisories/CA-2001-06.html*).

Generell sollten möglichst keine HTML-formatierten E-Mails oder solche mit aktiven Inhalten versendet werden. Außerdem sollte die Möglichkeit überprüft werden, in eingehenden E-Mails enthaltene aktive Inhalte herauszufiltern, beispielsweise an der Firewall.

Weiterhin sollten E-Mail-Clients gewählt werden, bei denen HTML-formatierte E-Mails als solche zu erkennen sind, damit die Benutzer diese nicht unbewusst öffnen.

Generell sollte eine Vorgabe innerhalb einer Institution zum Umgang mit HTML-formatierten E-Mails erstellt werden. Beim Empfang von HTML-formatierten E-Mails sollte festgelegt werden, ob diese

- unverändert an die Benutzer weitergeleitet und die Benutzer für den verantwortungsvollen und vorsichtigen Umgang mit solchen E-Mails geschult und sensibilisiert werden,
- mit Hilfe von serverseitigen Tools in ein reines Textformat umgewandelt und danach mit einem entsprechenden Hinweis an die Benutzer weitergeleitet werden (dabei können allerdings Informationen verloren gehen),
- nicht direkt an die Benutzer weitergeleitet werden, sondern an einen besonderen Arbeitsplatz, wo sie mit besonderen Sicherheitsvorkehrungen vom Empfänger eingesehen werden können (je nach E-Mail-Aufkommen kann dies allerdings einen nicht akzeptablen Aufwand mit sich bringen).

Grundsätzlich sollten alle Benutzer für diese Problematik sensibilisiert sein.

Wer auf Nummer sicher gehen will, der konfiguriert den E-Mail-Client so, dass er standardmäßig eine E-Mail nur als Text anzeigt.

Prüffragen:

- Gibt es Vorgaben für den Umgang mit HTML-formatierten E-Mails und für den Umgang mit Dateianhängen an E-Mails?

# M 4.200 Umgang mit USB-Speichermedien

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Über die USB-Schnittstelle lassen sich eine Vielzahl von Zusatzgeräten an PCs anschließen. Beispiele sind Festplatten, CD/DVD-Brenner und Memory-Sticks. USB-Memory-Sticks bestehen aus einem USB-Stecker und einem Speicherchip. Trotz großer Speicherkapazität sind sie so handlich, dass sie beispielsweise in Form von Schlüsselanhängern hergestellt werden und in jede Hosentasche passen. Die Preise sind so stark gefallen, dass USB-Sticks auch im Privatbereich Disketten überflüssig machen können. In modernen Betriebssystemen sind die Treiber für USB-Massenspeichergeräte bereits integriert, so dass zum Betrieb keine Softwareinstallation mehr notwendig ist. Im Allgemeinen bezieht sich diese Maßnahme nicht ausschließlich auf USB-Speichermedien, sondern generell auf alle USB-Geräte, die Daten speichern können. Unter anderem können auch USB-Drucker und USB-Kameras zum Speichern der Daten "missbraucht" werden. Dies gilt insbesondere für "intelligente" USB-Geräte wie PDAs, die jede beliebige USB-Identität annehmen können, wenn sie mit spezieller Software ausgestattet sind.

Ähnlich wie über Disketten können über USB-Speichermedien unkontrolliert Informationen und Programme ein- oder ausgelesen werden. Daher ist mit USB-Speichermedien generell genauso wie mit herkömmlichen Speichermedien umzugehen. Der Zugriff auf Diskettenlaufwerke kann relativ einfach verhindert werden (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*). Der Betrieb von USB-Speichermedien lässt sich dagegen nur sehr schwer verhindern, wenn die USB-Schnittstelle für andere Geräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Deswegen ist es meist nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren. Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Alternativ kann das Hinzufügen von Geräten überwacht werden. Beim Anschluss von Datenspeichern an externen Schnittstellen werden oftmals vom Betriebssystem Treiber bzw. Kernelmodule geladen oder Einträge in Konfigurationsdateien (wie der Windows-Registry) erzeugt, die detektiert werden können. Nachdem die Veränderungen festgestellt wurden, kann dann beispielsweise eine Protokolldatei erstellt oder ein Administrator benachrichtigt werden. Dies alles kann jedoch nur mit Hilfe von Zusatzsoftware realisiert werden. Hierfür ist entweder eine Eigenentwicklung oder ein Drittprodukt notwendig.

Im Folgenden werden die technischen Details für Windows 2000 und XP beschrieben.

**Gerätetreiber deaktivieren**

- **Windows 2000**
  Unter Windows 2000 kann das Starten des Gerätetreibers für USB-Speichermedien deaktiviert werden. Mit dieser Möglichkeit wird dem Standard-Benutzer die Möglichkeit, USB-Massenspeichergeräte hinzuzufügen, komplett entzogen, da er die Startart des Gerätetreibers nicht verändern kann. Auch einem Standard-Benutzer mit erschlichenem Administratorkennwort wird der Datendiebstahl zumindest schwerer gemacht.

USB-Sticks werden unter Windows 2000 als USB-Massenspeichergeräte registriert. Zum Ausführen wird der Gerätetreiber als Dienst gestartet.
In der Registrierung kann hinterlegt werden, wie der Dienst gestartet wird (Manuell, Automatisch oder Deaktiviert). So wird unter *HKLM/System/CurrentControlSet/Services* der Dienst *USBStor* als Gerätetreiber für die USB-Massenspeichergeräte bereitgestellt. Die unterschiedlichen Startarten können unter dem Unterschlüssel Start eingestellt werden. Die Festlegung, dass das Starten des Gerätetreibers USBStor deaktiviert (0x00000004) ist, verhindert, dass Massenspeichergeräte installiert oder hinzugefügt werden können.

- **Windows XP**
  Windows XP verhält sich anders als Windows 2000. Wird ein dem Rechner bekanntes Massenspeichergerät hinzugefügt, wird der Treiber geladen, und wenn in der Registrierung die Startart auf deaktiviert steht, wird der Einsatz des Massenspeichergeräts verhindert. Sobald jedoch ein dem Rechner unbekanntes USB-Massenspeichergerät hinzugefügt wird, werden neue Treiber installiert und die Einstellungen des Dienstes USBStor in der Registrierung überschrieben. Die Startart wird dabei auch wieder zurückgesetzt, so dass unter Windows XP der Einsatz von USB-Massenspeichergeräten nicht global verhindert werden kann.
  Ab Service Pack 2 bietet Windows XP die Möglichkeit, zumindest den Schreibzugriff auf USB-Blockspeichergeräte zu unterbinden. Damit wird die USB-Schnittstelle einem CD-ROM-Laufwerk gleichgesetzt, das nur das Lesen eines Mediums erlaubt. Die Deaktivierung des Schreibzugriffs erfolgt durch das Erstellen des Registrierungs-Schlüssels *HKLM\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect*, der auf den Wert 1 gesetzt wird.

**Überwachen des Rechners**

- **Windows 2000/XP**
  Sehr vielversprechend ist unter beiden Betriebssystemen die Möglichkeit, die Registrierung zu überwachen und damit nur auf das Hinzufügen zu reagieren. Ein Missbrauch würde sofort auffallen.
  Wenn das Hinzufügen von neuen Geräten beobachtet wird, können Aktionen initiiert werden. Jedes neue USB-Gerät wird in der Registrierung unter *HKLM\System\CurrentControlSet\Enum\USB* aufgeführt. Mit Hilfe eines Skriptes oder Programms könnte dieser Schlüssel daraufhin überwacht werden, ob ein Gerät unerlaubt hinzugefügt wird. Es kann eine Positivliste für erlaubte Geräte in dem Programm abgearbeitet werden, so dass auf möglicherweise benötigte Geräte nicht reagiert wird. Wird das unerlaubte Hinzufügen eines Geräts erkannt, kann eine Aktion (Herunterfahren des Systems, Benachrichtigen des Administrators per net send oder E-Mail) ausgeführt werden. Für eine solche Überwachung der Registrierung ist spezielle Software notwendig, die ein Drittprodukt sein oder aus Eigenentwicklung stammen kann.

Prüffragen:

- Wird der Anschluss von USB-Geräten protokolliert und werden diese Protokolle regelmäßig ausgewertet?

# M 4.201 Sichere lokale Grundkonfiguration von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sämtliche Konfigurationsarbeiten an Routern und Switches müssen entsprechend der erstellten Sicherheitsrichtlinie (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*) durchgeführt werden und wie in M 2.281 *Dokumentation der Systemkonfiguration von Routern und Switches* beschrieben dokumentiert und kommentiert werden.

**Betriebssystem**

Da Router und Switches durch ihren Einsatz im Netz eine besonders große Anzahl von Kommunikationspartnern und damit potentiellen Angreifern haben, ist bei der Auswahl, Einrichtung und Pflege des Betriebssystems besondere Sorgfalt notwendig.

Zunächst ist es wichtig, sich einen Überblick über die benötigten und angebotenen Funktionen zu verschaffen. Das Ziel bei der Auswahl sollte sein, eine möglichst stabile Version zu betreiben. Hierbei ist zu beachten, dass mit dem Alter eines Releases in der Regel auch die Zahl der Angriffsmöglichkeiten (Exploits) zunimmt. Andererseits kann ein sehr neues Release (insbesondere mit völlig neuen Funktionen) noch Unzulänglichkeiten oder neue Fehler enthalten.

Im Zweifelsfall ist es meist besser, eine ältere Version einzusetzen, falls diese den funktionalen Anforderungen noch genügt. Allerdings müssen für diese unbedingt die aktuellen Sicherheitspatches eingespielt werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Versionen, für die vom Hersteller keine Sicherheitspatches mehr zur Verfügung gestellt werden, sollten nicht mehr eingesetzt werden.

**Offline-Grundkonfiguration**

Bevor ein Router oder Switch an das Produktions-Netz angeschlossen wird, muss eine sichere Grundkonfiguration hergestellt werden. Viele Geräte werden vom Hersteller mit einer Default-Konfiguration ausgeliefert, die vor allem auf eine schnelle Inbetriebnahme mit möglichst umfassender Funktionalität ausgerichtet ist und in der so gut wie keine Sicherheitsmechanismen aktiv sind. Daher muss die Überprüfung der Default-Einstellungen und die Grundkonfiguration offline oder nur in einem eigens dafür eingerichteten und besonders gesicherten Testnetz erfolgen.

Oft ist es möglich, die Konfiguration mit entsprechenden Programmen auf einem Management-Rechner zu erstellen und beispielsweise mit einer Speicherkarte auf das neue Gerät zu übertragen. Ist nur eine Übertragung über das Netz möglich, so darf dies nur im Testnetz oder im Administrationsnetz geschehen.

Bei der Konfiguration muss beachtet werden, dass unter Umständen nicht jedes Administrations- oder Konfigurationswerkzeug (Konsole, Webschnittstelle, externes Konfigurationsprogramm) alle relevanten Informationen anzeigt.

So kann es beispielsweise vorkommen, dass die Systembefehle zur Anzeige einer Konfiguration auf Routern und Switches nicht alle Parameter anzeigen.

Daher ist es wichtig, anhand der vorhandenen Dokumentation nachzuvollziehen, dass auch alle relevanten Einstellungen vorgenommen wurden.

Es bietet sich an, die Grundkonfiguration in zwei Schritte zu unterteilen:

- Lokale Konfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf das Gerät selbst beziehen (beispielsweise Benutzerkonten oder -rollen, Passwörter, Protokolldateien, Einstellungen für Konsolenzugang und serielle Schnittstelle, etc.). Die entsprechenden Schritte sind im Anschluss beschrieben.
- Netzkonfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf die Funktion des Gerätes im Netz beziehen (beispielsweise Dienste und Protokolle, Einrichtung von Access-Control-Listen (ACLs), VLANs etc.). Die entsprechenden Schritte sind in M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches* beschrieben.

**Benutzerkonten und Passworte**

Die Möglichkeiten für die Einrichtung von Benutzern und Rollen und das Zuweisen von Berechtigungen unterscheiden sich von Hersteller zu Hersteller (gelegentlich auch zwischen einzelnen Geräten oder Software-Releases) teilweise erheblich. Daher ist es empfehlenswert, entsprechend dem vorgegebenen Rechte- und Rollenkonzept für die Administration der aktiven Netzkomponenten ein detailliertes Konzept für die jeweiligen Geräte zu erstellen.

Auf Routern und Switches einiger Hersteller (z. B. Cisco) sind werksmäßig mehrere Benutzerkonten (Accounts) mit abgestuften Berechtigungen für die Administration vorhanden. Andere Geräte sind werksmäßig nur mit einem Benutzerkonto für Administrationszwecke voreingestellt. Voreingestellte Benutzerkonten haben allgemein bekannte Standardnamen und Passwörter, gelegentlich sind Administrations-Accounts sogar ganz ohne Passwort vorkonfiguriert. Auf einschlägigen Internet-Seiten können Listen mit herstellerspezifischen Standard-Accounts und Passwörtern heruntergeladen werden.

Bei der Inbetriebnahme des Geräts müssen diese Standard-Benutzerkonten, falls möglich, geändert werden. In jedem Fall müssen aber die Passwörter der Standard-Accounts geändert werden. Nicht benutzte Benutzerkonten müssen deaktiviert werden.

Entsprechend dem Rechte- und Rollenkonzept müssen anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden.

Leider werden bei vielen aktiven Netzkomponenten Passwörter im Klartext in den Konfigurationsdateien gespeichert. Insbesondere falls dies der Fall ist, müssen Konfigurationsdateien vor unbefugtem Zugriff besonders geschützt werden. Wo immer es möglich ist, eine verschlüsselte Speicherung von Passwörtern zu konfigurieren, sollte von dieser Möglichkeit Gebrauch gemacht werden. Weitergehende Aspekte sind in M 1.43 *Gesicherte Aufstellung aktiver Netzkomponenten*, M 4.204 *Sichere Administration von Routern und Switches* und M 6.91 *Datensicherung und Recovery bei Routern und Switches* beschrieben.

**Login-Banner**

Beim Login wird auf den Geräten meist eine relativ ausführliche Login-Nachricht angezeigt. In dieser Login-Nachricht sind oft Informationen (beispielsweise Modell- oder Versionsnummer, Software-Release-Stand oder Patchlevel) enthalten, die einem potentiellen Angreifer von Nutzen sein können.

Sofern das Gerät es zulässt, sollte die Standard-Loginnachricht durch eine angepasste Version ersetzt werden, die diese Informationen nicht mehr enthält. Die Modell- und Versionsnummer des Geräts und die Version des Betriebssystems darf unter keinen Umständen vom Login-Banner verraten werden. Stattdessen sollten folgende Informationen bei einer Anmeldung am Gerät angezeigt werden:

- Jeglicher Zugriff darf nur durch autorisiertes Personal erfolgen.
- Alle Arbeiten sind entsprechend der Sicherheitsrichtlinie durchzuführen.
- Das Gerät ist in zentrale Kontrollmechanismen, wie beispielsweise in ein Netzmanagementsystem (NMS) zur Protokollierung und Erkennung von Verstößen gegen die Sicherheitsrichtlinie eingebunden.
- Verstöße gegen die Sicherheitsrichtlinie werden disziplinarisch / strafrechtlich verfolgt.

**Protokollierung**

Sicherheitsmaßnahmen in bezug auf die Protokollierung auf Netzkomponenten und der Einbindung von Zeitinformationen mit Hilfe von NTP sind in M 4.205 *Protokollierung bei Routern und Switches* beschrieben.

**Schnittstellen**

Nicht genutzte Schnittstellen auf Routern sind zu deaktivieren. Bei Switches sollten alle nicht genutzten Ports entweder deaktiviert oder einem eigens dafür eingerichteten "Unassigned-VLAN" zugeordnet werden.

**Backup der Konfiguration**

Die Konfigurationsdateien der Grundkonfiguration bilden die Basis für die weitere Konfiguration. Es wird empfohlen, sowohl von den mit dem Gerät ausgelieferten Default-Konfigurationsdateien als auch von den Dateien, die das Ergebnis der Grundkonfiguration darstellen, Sicherungskopien zu erstellen.

In M 6.91 *Datensicherung und Recovery bei Routern und Switches* werden weitere Aspekte zur Sicherung von Konfigurationsdateien beschrieben.

Prüffragen:

- Werden Konfigurationsänderungen an den Routern und Switches gemäß der bestehenden Sicherheitsrichtlinie durchgeführt und so dokumentiert, dass Konfigurationsänderungen nachvollzogen werden können?
- Werden für alle eingesetzten Router und Switches Sicherheitspatches durch die Hersteller zur Verfügung gestellt und werden diese eingespielt?
- Werden die Default-Einstellungen der Router und Switches vor dem Einsatz im Produktions-Netz überprüft und mit einer sicheren Grundkonfiguration ausgestattet?
- Erfolgt die Grundkonfiguration der Router und Switches offline bzw. nur ein einem eigens dafür eingerichteten und besonders gesicherten Testnetz?
- Existieren gerätespezifische Konzepte für die Einrichtung des vorgegebenen Rechte- und Rollenkonzeptes?
- Sind die Passwörter der Standardkonten auf den Routern und Switches geändert und entsprechen sie den Sicherheitsrichtlinien der Organisation?
- Sind nicht benutzte Benutzerkonten auf den Routern und Switches deaktiviert?
- Sofern auf den Routern und Switches die Passwörter im Klartext in den Konfigurationsdateien gespeichert werden: Sind die Konfigurationsdateien vor dem unbefugten Zugriff besonders geschützt?

- Werden die Passwörter auf den Routern und Switches sofern möglich verschlüsselt gespeichert?
- Sind die Standard-Loginmeldungen auf den Routern und Switches sofern möglich durch eine angepasste Version ersetzt, so dass kein Rückschluss auf die eingesetzten Versionen möglich ist?
- Sind nicht genutzte Schnittstellen auf Routern und Switches deaktiviert oder einem dafür eingerichteten "Unassigned-VLAN" zugeordnet?
- Werden Backups sowohl vor als auch nach der erfolgreichen Grundkonfiguration durchgeführt?

# M 4.202 Sichere Netz-Grundkonfiguration von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

### Remote-Zugriff

Für die Administration aktiver Netzkomponenten über das Netz wird oft noch Telnet als Standardmöglichkeit angeboten. Oft gibt es auch eine Administrationsmöglichkeit über SNMP oder den Zugriff über eine HTTP-Schnittstelle. Alle diese Protokolle haben den Nachteil, dass sowohl Benutzername und Passwort als auch die Nutzdaten im Klartext über das Netz übertragen werden (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*).

Daher ist für die Administration entweder ein eigenes Administrationsnetz (Out-of-Band-Management) einzurichten, oder es dürfen nur Protokolle benutzt werden (beispielsweise ssh2), die eine gesicherte Authentisierung und verschlüsselte Übertragung unterstützen.

Soll SNMP außerhalb eines eigenen Administrationsnetzes eingesetzt werden, so darf nur SNMPv3 benutzt werden.

### Authentisierungsserver

In großen Netzen sollten Router und Switches möglichst für die Nutzung von Authentisierungsservern unter Verwendung von Einmal-Passwörtern konfiguriert werden. Beispiele hierfür sind RADIUS oder TACACS+. Weitergehende Aspekte sind in M 4.204 *Sichere Administration von Routern und Switches* beschrieben.

### Management-Interface und Administrationsnetz

Einige Geräte bieten die Möglichkeit, ein eigenes logisches Interface zur Administration (Management-Interface) zu konfigurieren. Bei Switches sollte dieses Interface einem eigenen VLANN zugeordnet werden, das ausschließlich für administrative Zwecke verwendet wird (Out-of-Band Management) und dem ausschließlich Management-Interfaces angehören. Bei Routern sollten ACLs so konfiguriert werden, dass der Zugriff auf das Management-Interface von der Management-Station aus mit definierten Protokollen erlaubt ist. Alle nicht benötigten Dienste sind für das Management-Interface zu deaktivieren.

Weitere Schritte zur Einrichtung eines Administrationsnetzes (Out-of-Band-Management) sind in M 4.204 *Sichere Administration von Routern und Switches* beschrieben.

### Deaktivierung unnötiger Netzdienste

Hersteller aktiver Netzkomponenten legen oft in erster Linie Wert auf eine möglichst einfache Inbetriebnahme und Konfiguration der Komponenten. Daher sind in der Default-Konfiguration meist eine Vielzahl von Diensten aktiviert. Es sollten nur Dienste aktiviert sein, die für den Betrieb notwendig sind. Nicht benötigte Dienste auf den Routern und Switches müssen deaktiviert werden, weil sie ein erhöhtes Risiko darstellen.

Die Einstellungen zu den in der nachfolgenden Tabelle genannten Diensten gelten oft für das gesamte System und nicht explizit für einzelne Schnittstellen / Ports der Geräte. Generell dürfen diese Dienste nicht aus unsicheren Netzen erreichbar sein. Dies ist durch entsprechende Access-Control-Lists sicherzustellen.

In der folgenden Tabelle ist eine Anzahl von Diensten aufgeführt, die oft auf aktiven Netzkomponenten vorhanden sind. Für jeden Dienst ist eine Empfehlung angegeben, wie mit dem Dienst normalerweise verfahren werden sollte.

| **Dienst** | **Beschreibung** |
|---|---|
| FINGER | Der Finger-Dienst zeigt die augenblicklich auf einem Gerät angemeldeten Benutzer an. Er hat keinen praktischen Nutzen und sollte deaktiviert werden. |
| BOOTP | Einige Router und Switches unterstützen BOOTP (Bootstrap-Protocol), sowohl als Server als auch als Client. Damit ist es anderen Komponenten möglich, von diesen Geräten zu booten. BOOTP besitzt keine Funktionen zur Authentisierung oder Verschlüsselung und sollte deaktiviert werden. |
| HTTP | Eine große Anzahl von Routern und Switches können mit Hilfe von HTTP administriert werden.<br>Dieser Dienst sollte in öffentlichen Netzen auf jeden Fall deaktiviert und allenfalls in einem isolierten Administrationsnetz verwendet werden. |
| SNMP | SNMP ist ein Administrations- und Netzmanagement-Protokoll. Bis einschließlich der Version SNMPv2 sind die Sicherheitsfunktionen nicht ausreichend. Die Variante SNMPv3 besitzt stärkere Authentisierungs- und Verschlüsselungsoptionen.<br>Dieser Dienst sollte möglichst nur in einem isolierten Administrationsnetz genutzt werden. SNMPv1 und SNMPv2 dürfen keinesfalls außerhalb isolierter Administrationsnetze verwendet werden. |
| TELNET | Telnet wird oft als Standard-Administrationsschnittstelle für Router und Switches verwendet.<br>Dieser Dienst sollte durch SSH (siehe unten) ersetzt werden. In öffentlichen Netzen darf Telnet nicht zur Administration aktiver Netzkomponenten verwendet werden. |
| NTP | Das Network Time Protocol NTP dient zur Synchronisation der Systemzeit. |

| Dienst | Beschreibung |
|---|---|
| | Einige Router oder Switches können als Zeitserver für andere Geräte fungieren. NTP besitzt keine Sicherungsfunktionen und sollte daher nicht in öffentlichen Netzen verwendet werden. Es sollte ein interner NTP-Server installiert sein, der über ein Administrationsnetz angesprochen wird. |
| DNS | Einige Router oder Switches unterstützen die Funktion eines DNS-Clients zur Namensauflösung, beispielsweise im Zusammenhang mit der Protokollierung. Eine Namensauflösung ist bei aktiven Netzkomponenten normalerweise nicht notwendig und bietet keinen echten Nutzen. Daher sollte DNS deaktiviert werden. |
| CDP | CDP ist ein proprietäres Layer 2 Protokoll zwischen Cisco Routern und Switches. Es sollte zumindest auf Endgeräte-Ports deaktiviert werden. |
| TFTP | Einige Router und Switches unterstützen das Booten von einem TFTP-Server. TFTP bietet keine Sicherheitsmechanismen.<br>Diese Funktion sollte nur genutzt werden, wenn ein interner TFTP-Server in einem isolierten Administrationsnetz installiert ist. |
| SSH1 | SSH1 ist eine alte Variante des Secure Shell Protokolls, die Sicherheitslücken aufweist. Sie sollte daher nicht verwendet werden. Falls ein Gerät nur SSH1 anbietet, so sollte der Zugriff nur über ein isoliertes Administrationsnetz erfolgen. |
| SSH2 | SSH2 ein sicherer Ersatz für Telnet über öffentliche Netze zur Administration von Routern und Switches eingesetzt werden kann. Trotzdem ist es empfehlenswert, auch den SSH-Zugang durch entsprechende ACLs zusätzlich abzusichern. |

Tabelle: Dienste von aktiven Netzkomponenten

Auf Schnittstellen von Switches, aber in erster Linie auf Interfaces von Routern in öffentlichen Netzen sollten außerdem die folgenden Einstellungen zusätzlich berücksichtigt werden.

Dabei kann jedoch keine allgemeine Vorgehensweise vorgegeben werden, sondern es werden nur Empfehlungen für verschiedene Aspekte gegeben.

Wenn in bestimmten Fällen von diesen Empfehlungen abgewichen wird, so sollte aber stets klar sein, wieso.

| Dienst | Beschreibung, Einstellung |
|---|---|
| IP source routing | Diese Funktion erlaubt es einem IP-Paket, die Route zum Ziel vorzugeben. Diese Funktion wird für eine Vielzahl von Angriffen verwendet. Deshalb sollte diese Funktion deaktiviert werden. |
| IP directed broadcast | Dieser Dienst kann für DOS-Attacken ausgenutzt werden. Deshalb sollte diese Funktion deaktiviert werden. |
| ICMP redirects | Diese ICMP-Funktion kann verwendet werden, um Informationen über Netze herauszufinden. Deshalb muss diese Funktion zumindest an externen Interfaces von Routern deaktiviert werden. |
| ICMP unreachable notifications | Diese ICMP-Funktion kann verwendet werden, um Informationen über Netze herauszufinden. Deshalb muss diese Funktion zumindest an externen Interfaces von Routern deaktiviert werden. |
| ICMP mask reply | Diese ICMP-Funktion kann verwendet werden, um Informationen über Netze herauszufinden. Deshalb muss diese Funktion zumindest an externen Interfaces von Routern deaktiviert werden. |

Tabelle: Einstellung der Dienste

**Anti-Spoofing**

Border-Router stellen den Übergang von internen Netzen zu externen Netzen dar. Auf Border-Routern sollten Sicherheitsmaßnahmen ergriffen werden, die IP-Spoofing (siehe auch G 5.48 *IP-Spoofing*) verhindern. Dies kann beispielsweise durch die Einrichtung entsprechender ACLs erreicht werden. Eine mögliche Variante ist folgender Ansatz:

- An den externen Schnittstellen werden solche Pakete blockiert, deren Absender-IP-Adresse im internen Netz liegt
- An den internen Schnittstellen werden solche Pakete blockiert, deren Absender-IP-Adresse nicht im internen Netz liegt.

Zumindest bei Paketen, die auf Grund der zweiten Regel blockiert werden, ist eine entsprechende Protokollierung und gegebenenfalls eine Alarmierung der zuständigen Administratoren empfehlenswert. Die Tatsache, dass eine Station innerhalb des eigenen Netzes offensichtlich gefälschte Pakete verschickt, ist nämlich ein klares Indiz dafür, dass entweder eine falsche Konfiguration oder gar ein Sicherheitsproblem vorliegt.

**Loopback-Interface**

Einige Router-Modelle (beispielsweise von Cisco) bieten die Möglichkeit, ein Loopback-Interface einzurichten. Die dem Loopback-Interface zugewiesene IP-Adresse kann vom Router als Quelladresse für Protokolle wie Syslog, NTP oder wichtiger Dienste zur Administration benutzt werden. Dadurch kann einebessere Absicherung des Routers erreicht werden, weil die Quell-Adresse im IP-Paket immer die IP-Adresse des Loopback-Interfaces ist.

**Routing-Protokolle**

Es sollten nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung unterstützen. In demilitarisierten Zonen dürfen keine dynamischen Routing-Protokolle eingesetzt werden, stattdessen müssen statische Routen eingetragen werden.

Die Verwendung von Routing-Protokollen sollte zusätzlich durch die Einrichtung von ACLs abgesichert sein. Mehr Informationen finden sich in M 5.112 *Sicherheitsaspekte von Routing-Protokollen*.

**Access Control Lists**

Die Verwendung von Access Control Lists (ACLs) zur Einschränkung des Zugriffes auf Routern und zur netzübergreifenden Paketfilterung ist in M 5.112 *Sicherheitsaspekte von Routing-Protokollen* beschrieben.

**Spanning Tree**

Das Spanning Tree Protocol (STP, IEEE 802.1d) wird von Switches und Bridges verwendet, um Schleifenbildungen innerhalb des Netzes auf der OSI-Schicht 2 zu vermeiden. Es werden BPDUs (Bridge Protocol Data Units) ausgesendet, um die Root-Bridge (basierend auf MAC-Adresse und Priorität) zum Systemstart und bei Topographie-Änderungen zu bestimmen. Dieses Protokoll bietet keine Authentisierung. Deshalb sollte STP zumindest auf allen Endgeräte-Ports deaktiviert werden. In der Konfiguration muss eine eindeutige Root-Bridge festgelegt werden.

**VLANs und Trunking**

Trunking ermöglicht es, VLANs über mehrere Switches auszudehnen. Die Steuerung von Trunking wird durch den Standard IEEE 802.1q oder durch unterschiedliche proprietäre Trunking-Protokolle realisiert. Dabei wird pro Switch ein physischer Port (Trunk-Port) für die Inter-Switch-Kommunikation reserviert. Diese logische Verbindung zwischen den Switches wird als Trunk bezeichnet.

Trunk-Ports können auf alle VLANs zugreifen. Das heißt, dass der Zugang zu einem Trunk-Port den Zugriff auf alle VLANs dieses Trunks ermöglicht. Manche Geräte bieten allerdings auch die Möglichkeit, den Zugriff eines Trunk-Ports auf bestimmte VLANs zu beschränken ("VLAN Pruning"). Sofern ein Switch eine solche Möglichkeit bietet, ist es empfehlenswert, dies zu nutzen. Auf Endgeräte-Ports sollte Trunking möglichst deaktiviert werden.

Das Default-VLAN darf nicht für ein produktives VLAN verwendet werden.

Wird das proprietäre Protokoll VTP (VLAN Trunking Protocol) des Herstellers Cisco verwendet, so sollte unbedingt die von VTP unterstützte Authentisierung verwendet werden.

**Freie Ports**

Für nicht benutzte Ports sollte ein eigenes VLAN ("Unassigned-VLAN") eingerichtet werden. Nach Möglichkeit sollten nicht genutzte Ports allerdings ganz deaktiviert werden, da die VLAN-Port-Zuweisung nur wenig zusätzliche Sicherheit bietet.

Ist es gewünscht, bestimmte Ports für den freien Anschluss verschiedener Geräte vorzusehen, so ist es empfehlenswert, für diese Ports eine Sicherung zu implementieren, die erst nach einer Anmeldung den Zugang zum Netz gewährt.

Ein solcher Zugangsschutz kann beispielsweise über den Standard IEEE 802.1x implementiert werden. Der Standard 802.1x wird inzwischen von vielen Switches und den meisten Rechner-Betriebssystemen unterstützt. Darüber hinaus existiert eine Reihe weiterer, teils proprietärer Lösungen, bei denen die Endgeräte auf der Basis ihrer MAC-Adresse oder über andere Mechanismen gegenüber der aktiven Netzkomponente authentisiert werden können, bevor der Zugang zum Netz freigeschaltet wird.

Prüffragen:

- Erfolgt die Administration der Router und Switches ausschließlich über vertrauenswürdige Pfade?
- Sofern SNMP außerhalb des Administrationsnetzes eingesetzt wird: Wird SNMPv3 bei den Routern und Switches eingesetzt?
- Sind die auf den Routern und Switches zur Verfügung gestellten Dienste auf die benötigten begrenzt?
- Ist sichergestellt, dass nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung unterstützen?
- Wird in demilitarisierten Zonen auf den Einsatz von dynamischen Routing-Protokollen verzichtet und werden stattdessen statische Routen genutzt?
- Werden die Routing-Protokolle durch die Einrichtung von ACLs zusätzlich abgesichert?
- Ist das Spanning Tree Protocol auf den Endgeräte-Ports der Switches deaktiviert?
- Ist in der Konfiguration der Switches bei Nutzung des Spanning Tree Protocol eine eindeutige Root-Bridge festgelegt?
- Wird, sofern möglich, das VLAN Pruning eingesetzt, um den Zugriff eines Trunk-Ports auf bestimmte VLANs zu beschränken?
- Ist das VLAN Trunking auf den Endgeräte-Ports deaktiviert?
- Ist sichergestellt, dass das Default-VLAN nicht für ein produktives VLAN verwendet wird?
- Sofern das VLAN Trunking Protocol (VTP) verwendet wird: Wird die von VTP unterstützte Authentisierung verwendet?

# M 4.203 Konfigurations-Checkliste für Router und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zusammenfassend können anhand der folgenden Konfigurations-Checkliste die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden. Es muss jedoch festgehalten werden, dass die sichere Konfiguration von Routern und Switches stark vom Einsatzzweck abhängt. Beispielsweise muss auf Border-Routern die Einrichtung von ACLs, Anti-Spoofing-Konfiguration, etc. berücksichtigt werden. Deshalb sollte die folgende Tabelle lediglich als allgemeine Anleitung verwendet werden. Sicherheitsmaßnahmen, die auf Router anzuwenden sind, gelten auch für Switches, sofern diese Routing-Funktionen unterstützen und soweit diese Funktionen genutzt werden.

| **Konfigurations-Checkliste für Router und Switches** | |
|---|---|
| Erstellung einer Sicherheitsrichtlinie für Router und Switches | |
| Prüfung und gegebenenfalls Update des Betriebssystems | |
| Die Router- und Switchkonfiguration offline speichern, sichern und gegen unbefugten Zugang schützen (Nutzung eines TFTP-Servers nur in Verbindung mit Out-of-Band-Management (eigenes Administrationsnetz)) | |
| Dokumentation und Kommentierung der Konfiguration | |
| Konfiguration von Passwortschutz für alle Zugänge (Konsole, VTY, etc.) | |
| Einrichtung eines Session-Timeouts | |
| Keine Trivial-Passworte verwenden | |
| Verschlüsselte Speicherung der Passworte | |
| Einrichtung eines physischen Zugangsschutzes für den Konsolenanschluss | |
| Für Administrationszwecke soweit möglich TELNET durch SSH ersetzen | |
| Möglichst RADIUS oder TACACS+ zur Authentisierung verwenden | |
| Einschränkung der Administrationszugänge (z. B. SSH, SNMP, TELNET) durch ACLs, Nutzung von SNMP und TELNET nur in Verbindung mit Out-of-Band-Management (eigenes Administrationsnetz), bei SNMP Änderung der Community-Strings | |

| **Konfigurations-Checkliste für Router und Switches** | |
|---|---|
| Deaktivieren unnötiger Netzdienste | |
| Bei Routern nicht benötigte Schnittstellen abschalten, bei Switches nicht benötigte Ports in "Unassigned VLAN" oder ebenfalls deaktivieren | |
| Kritische Schnittstellendienste und Protokolle sperren | |
| Protokollierung einschalten | |
| Genaue Uhrzeit auf den Geräten einstellen (interner NTP-Server) | |
| Einbinden der Zeitinformation bei der Protokollierung | |
| Auswerten, Überprüfen und Archivieren der Protokolldateien entsprechend der Sicherheitsrichtlinie | |
| SNMP möglichst deaktivieren, Nutzung nur in Verbindung mit Out-of-Band-Management (Administrationsnetz) oder Verwendung von SNMPv3 | |
| Überprüfung der Default-Einstellungen | |
| Einrichtung eines Login-Banners | |
| Deaktivierung von CDP auf Endgeräte Ports | |
| **Speziell für Switches:** | |
| Bei Nutzung von VTP: Authentisierung verwenden | |
| Deaktivierung von Trunk-Negotiation auf Endgeräte-Ports | |
| Das Default-VLAN darf nicht genutzt werden | |
| Einrichtung eines eigenen VLANs für alle Trunk-Ports | |
| Einrichtung eines Unassigned-VLANs für alle unbenutzten Ports | |
| Deaktivierung von STP (Spanning Tree) auf Endgeräte-Ports | |
| Festlegung einer Root-Bridge | |
| **Speziell für Router:** | |
| Erstellung einer Kommunikationsmatrix des netzübergreifenden Datenverkehrs | |
| Begrenzen des netzübergreifenden Datenverkehrs in Abgleich mit Kommunikationsmatrix durch Zugriffslisten | |

| **Konfigurations-Checkliste für Router und Switches** | |
|---|---|
| Blockieren von unbekannten Adressen durch Zugriffslisten (ACLs) | |
| Falls erforderlich (insbesondere in der DMZ): Konfiguration statischer Routen | |
| Konfiguration von Integritätsmechanismen der verwendeten Routing Protokolle | |

Prüffragen:

- Werden sicherheitsrelevante Einstellungen auf Routern und Switches anhand einer Konfigurations-Checkliste geprüft?
- Werden in der Konfigurations-Checkliste die unterschiedlichen Anforderungen der Router und Switches berücksichtigt?

# M 4.204 Sichere Administration von Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es gibt unterschiedliche Zugriffsmöglichkeiten, um Router und Switches zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert, Router und Switches in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration praktisch nicht gewährleistet werden kann.

Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt werden, und die Administration darf nur entsprechend der Sicherheitsrichtlinie durchgeführt werden. Alle nicht verwendeten Administrationsschnittstellen sollten deaktiviert werden. Im folgenden werden einige Punkte beschrieben, die bei der Administration beachtet werden sollten.

Zusätzlich sollte wenn möglich der Administrationszugriff durch die Einrichtung von Access Control Lists (ACLs) eingeschränkt werden (siehe auch M 5.111 *Einrichtung von Access Control Lists auf Routern*).

**Remote-Administration**

Eine Vielzahl von aktiven Netzkomponenten bietet die Möglichkeit der Remote-Administration mit Hilfe des Dienstes Telnet. Die Nutzung von Telnet birgt allerdings die Gefahr des Ausspähens von Authentisierungsdaten, da sämtliche Daten im Klartext übertragen werden und somit der Datenverkehr inklusive des Benutzernamens und Passwortes mitgelesen werden kann (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*). Oft wird zur Remote-Administration auch SNMP verwendet. Die Varianten SNMPv1 und SNMPv2 bieten ebenfalls keine ausreichenden Möglichkeiten zur Absicherung der Kommunikation. Erst SNMPv3 bietet Sicherheitsmechanismen, die einen Einsatz auch außerhalb abgeschotteter Administrationsnetze erlauben.

Bei Remote-Zugriff auf Routern und Switches muss in jedem Fall eine Absicherung der Kommunikation erfolgen. Dies kann beispielsweise durch die Nutzung des Dienstes SSH anstatt Telnet (siehe M 5.64 *Secure Shell*) oder durch die Schaffung eigener LAN-Segmente, die ausschließlich für Administrationszwecke genutzt werden, erreicht werden (siehe Abschnitt Administrationsnetz).

Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten soweit möglich keine unsicheren Protokolle verwendet werden.

**Webserver**

Viele Geräte bieten die Möglichkeit, Administrationsarbeiten mit Hilfe des Dienstes HTTP über ein Browser-Interface durchzuführen. Auf dem Router bzw. dem Switch ist in diesem Fall ein HTTP-Server gestartet, der Zugriff erfolgt von beliebigen Clients über Web-Browser.

Die Standardeinstellungen für den Zugriff auf das Web-Interface sind nicht bei allen Herstellern einheitlich. Idealerweise sollte der Zugriff in der Grund-

einstellung deaktiviert sein, es ist aber auch möglich, dass dieser Dienst ungeschützt ohne Eingabe von Benutzerinformationen verwendet werden kann. Dies ist bei der Inbetriebnahme der Geräte zu prüfen, gegebenenfalls muss die Konfiguration entsprechend geändert werden.

Wie bei der Nutzung des Dienstes TELNET wird auch beim HTTP der Benutzername und das Passwort im Klartext übertragen. Zudem sind eine Reihe von Exploits bekannt, die Schwachstellen der HTTP-Server der unterschiedlichen Hersteller ausnutzen. Daher wird von der Nutzung des HTTP-Dienstes für Administrationszwecke dringend abgeraten. Der HTTP-Server sollte nach Möglichkeit bei der Erstkonfiguration des Systems deaktiviert werden, sofern der Zugriff nicht über ein gesondertes Management-Netz erfolgt.

Manche Geräte bieten zusätzlich zum Zugriff über HTTP auch die Möglichkeit, über HTTPS auf das Web-Interface zuzugreifen. Sofern diese Möglichkeit besteht, sollte HTTPS in jedem Fall der Vorzug vor HTTP gegeben werden.

Bei der Nutzung des Web-Interfaces muss außerdem beachtet werden, dass oft nicht alle Konfigurationseinstellungen auf diesem Weg zugänglich sind.

**Administrationsnetz (Out-of-Band-Management)**

Um den Risiken bei der Remote-Administration entgegen zu wirken, bieten einige Geräte die Möglichkeit, einen eigenen logischen Port (Management-Interface) zur Administration zu konfigurieren. Bei Switches sollte dieser Port einem VLAN zugeordnet werden, welches ausschließlich für administrative Zwecke verwendet wird (Out-of-Band-Management) und dem ausschließlich Management-Interfaces angehören. Das Management-Netz sollte komplett von anderen Teilen des Netzes getrennt werden. Dadurch werden Schwachstellen wie unverschlüsselt übertragene Anmeldeinformationen bei den für administrative Aufgaben zur Anwendung kommenden Protokollen wie TELNET oder die veralteten SNMP-Varianten kompensiert.

Access Control Lists (ACLs) sind so zu konfigurieren, dass der Zugriff auf das Management-Interface nur der Management-Station erlaubt ist. Alle nicht benötigten Dienste sind für das Management-Interface zu deaktivieren.

**Netzmanagement-Systeme**

Aktive Netzkomponenten werden normalerweise in ein zentrales Netzmanagement-System eingebunden. Zusätzlich zum vorigen Abschnitt müssen in diesem Fall die Sicherheitsmaßnahmen, die im Baustein B 4.2 *Netz- und Systemmanagement* beschrieben sind, beachtet werden.

**Zentraler Authentisierungsserver**

An Stelle lokal auf dem Gerät zu konfigurierender Zugriffs- und Rechtekontrolle kann dies auch über einen zentralen Server erfolgen. Bei großen Umgebungen mit einer hohen Anzahl von aktiven Netzkomponenten ist die lokale Konfiguration nur bedingt praktikabel. Der Aufwand für die Administration und für viele parallel zu pflegende Berechtigungen ist dann sehr hoch.

Auf dem zentralen Server werden dabei einheitlich alle Zugriffe und Berechtigungen verwaltet. Die sensitiven Daten sind nicht mehr auf den Geräten selbst gespeichert und müssen nicht einzeln gepflegt werden. Stattdessen sind alle Informationen verschlüsselt in einer Datenbank abgelegt und lassen sich übersichtlich verwalten. Ein solcher Server bietet zudem erweiterte Möglichkeiten zur Protokollierung, beispielsweise können Anzahl und Zeitpunkt von Einwahl- oder Zugriffsvorgängen und übertragene Datenmengen dokumen-

tiert werden. Beispiele hierfür sind RADIUS und TACACS+ (Terminal Access Controller Access Control System). Die Authentisierung sollte in komplexen Netzen mit einer Vielzahl von aktiven Netzkomponenten durch einen zentralen Authentisierungsserver abgesichert werden.

Für den Fall, dass kein Authentisierungsserver genutzt werden kann (beispielsweise beim Ausfall des Servers oder bei Netzproblemen), sollte trotzdem ein lokaler Zugriff konfiguriert sein. Dieser ist durch ein nur für diesen Zweck zu nutzendes Passwort abzusichern.

Für lokale Zugänge, die nicht eigens für den Fall eingerichtet wurden, dass der Authentisierungsserver nicht zur Verfügung steht, sollten der Authentisierungsserver nach Möglichkeit genutzt werden, da ansonsten die Benutzer, die sich lokal anmelden, die zentrale Autorisierung und Überwachung umgehen.

**Berechtigungsverwaltung für Benutzerkonten und Systemkommandos**

Die Berechtigungsverwaltung kann je nach Hersteller auf unterschiedlichen Ebenen und mit unterschiedlichen Graden der Granularität erfolgen. Bei der Berechtigungsverwaltung von Systemkommandos können Kommandos, die nur bestimmten Nutzern oder Gruppen zugänglich sein sollen, in einer Berechtigungsstufe zusammengefasst bzw. dieser zugeordnet werden. Dies ist beispielsweise vom Hersteller Cisco bereits für zwei Stufen vorkonfiguriert:

1. Die Zuordnung von Systemkommandos zu Berechtigungsstufen.
2. Die Zuordnung von Benutzerkonten zu Berechtigungsstufen.

Der Zugriff auf eine Berechtigungsstufe wird durch ein Passwort abgesichert. Ein Nutzer muss für den Zugriff auf ein entsprechend abgesichertes Systemkommando zunächst in die Berechtigungsstufe wechseln und das zugehörige Passwort eingeben. Dann ist er in der Lage, alle dieser Stufe zugeordneten Kommandos auszuführen. Die Berechtigungsvergabe für Benutzerkonten erfolgt, indem der Nutzer einer Berechtigungsstufe zugeordnet wird. Generell sollte gelten, dass jedem Nutzer nur die minimal notwendigen Berechtigungen zugeteilt werden. Somit lassen sich analog der folgenden Beispiele unterschiedliche Rollen definieren:

- Ein Read-Only Account dient dazu, die Einstellungen des Geräts einzusehen. Änderungen der Konfiguration sind nicht möglich.
- Der Read-Write Account erlaubt die Änderung und Betrachtung der meisten Einstellungen des Geräts, Sicherheits- und Passwort-Einstellungen gehören nicht dazu.
- Der Read-Write-All Account ist für die umfassende Kontrolle inklusive Sicherheitseinstellungen, Zugriffspassworte und Web-basierte Managementzugriffe vorgesehen.
- Zudem sind spezielle Accounts für die Verwaltung von Layer-2- und Layer-3-Funktionen möglich.

Ein Benutzer ist somit nach seiner Anmeldung am Gerät automatisch einer Berechtigungsstufe zugeordnet, alternativ muss er nach der Anmeldung dediziert die zu nutzende Berechtigungsstufe und das zugehörige Passwort eingeben. Für sicherheitskritische Rollen sollte stets eine Absicherung des Zugriffs über einen zentrale Authentisierungsserver eingerichtet werden.

Die Möglichkeiten der Zuordnung von Berechtigungen zu Benutzern und Rollen können sogar so weit gehen, dass für jeden einzelnen Befehl Berechtigungen vergeben werden können, die jedes Mal vor der Ausführung über den Autorisierungsserver überprüft werden.

Bei der Erstellung des Rechte- und Rollenkonzepts für die Administration der aktiven Netzkomponenten müssen die Möglichkeiten der einzelnen Systeme in Betracht gezogen werden. Wie fein die Berechtigungsstufen im Einzelfall unterschieden werden, sollte unter Berücksichtigung von Einsatzzweck und Schutzbedarf festgelegt werden. Als Faustregel kann dabei gelten: "So fein wie nötig, so einfach wie möglich." Zu grobe Unterteilungen bieten keine angemessene Sicherheit, andererseits können zu feine Unterteilungen die Effizienz der Arbeit beeinträchtigen und bringen die Gefahr von Fehlern mit sich.

**Passwortverschlüsselung**

Router und Switches sollten die Möglichkeit unterstützen, Passwörter verschlüsselt in Konfigurationsdateien abzulegen (siehe auch M 2.280 *Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches*). Beispielsweise kann dies bei Cisco-Geräten mit dem Befehl *enable secret* erreicht werden.

Die Verschlüsselung von Passwörtern ist insbesondere dann wichtig, wenn Konfigurationsdateien über das Netz übertragen oder in zentralen Servern gespeichert werden.

Wenn das Gerät die Passwortverschlüsselung unterstützt, sollte diese Funktion unbedingt genutzt werden. Dabei sollte das Verschlüsselungsverfahren berücksichtigt werden, da einige Geräte unterschiedliche Verfahren unterstützen. Insbesondere bei älteren Betriebssystemen werden noch schwache Verschlüsselungsverfahren angewendet, die eventuell aus Gründen der Kompatibilität auch in neueren Versionen noch unterstützt werden. Hier sollte bei einer Migration auf ein neues Gerät oder eine neue Betriebssystemversion geprüft werden, ob die neuere Version stärkere Verschlüsselungsverfahren unterstützt.

Zudem bestehen für alle Geräte Prozeduren, die es zwar nicht ermöglichen, verschlüsselte Passworte wieder lesbar zu machen, die aber das Rücksetzen von Passwörtern durchführen.

Einige Dienste können nicht durch eine Passwort-Verschlüsselung abgesichert werden. Hierzu gehören SNMPv1 und SNMPv2, RADIUS und TACACS+. Die Passwörter der letztgenannten Dienste sollten somit immer einmalig sein, für keinen weiteren Dienst verwendet und regelmäßig geändert werden. SNMPv1 und SNMPv2 sollten allenfalls in Verbindung mit Out-of-Band-Management (siehe oben: Administrationsnetz) genutzt werden und möglichst durch SNMPv3 ersetzt werden.

**Session-Timeouts**

Sämtliche Zugriffsarten können durch die Vergabe von Passwörtern geschützt werden. Diese Absicherung kann jedoch wirkungslos werden, wenn Sessions unbeaufsichtigt sind, beispielsweise wenn ein angemeldeter Administrator seinen Rechner verlässt und dabei vergisst, die Session zu beenden oder die Bildschirmsperre zu aktivieren. Aus diesem Grund ist es empfehlenswert, Time-Outs einzurichten, um Verbindungen nach einem definierten Zeitraum ohne Nutzeraktivität zu beenden oder zu sperren. Dabei sollte eine Timeout-Zeit von 10 Minuten nicht überschritten werden.

Prüffragen:

- Sind die Router und Switches in ein zentrales Netzwerkmanagement-System eingebunden?

- Ist die Kommunikation für Remote-Zugriffe auf Router und Switches entsprechend abgesichert?
- Sind ACLs definiert, die den Zugriff auf das Management-Interface der Router und Switches nur von einer Management-Station erlaubt?

# M 4.205 Protokollierung bei Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Router und Switches bieten in der Regel Möglichkeiten zur Protokollierung. Die Auswertung dieser Informationen ermöglicht die Beurteilung der korrekten Funktion des Geräts und das Erkennen von Angriffsversuchen. Mit Hilfe der Protokollierungsinformationen kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden.

Daher sollte die Protokollierung immer genutzt und sorgfältig eingerichtet werden. Die sorgfältige Konfiguration ist besonders wichtig, da nur bei einer sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert werden können. Hierzu gehören vor allem das Erkennen abgewiesener Zugriffsversuche und Änderungen der Konfiguration.

Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Organisation abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

Folgende Informationen sollten nach Möglichkeit protokolliert werden:

- Konfigurationsänderungen
- Reboots
- Systemfehler
- Statusänderungen pro Interface, System und Netzsegment
- Login-Fehler (zumindest dann, wenn sie wiederholt auftreten)
- Verstöße gegen ACL-Regeln (abgewiesene Zugriffsversuche)

Insbesondere der letzte Punkt sollte für jede ACL aktiviert werden, um alle fehlgeschlagenen Versuche zu erfassen und falsch oder nicht korrekt konfigurierte Regeln erkennen zu können.

Je nach Hersteller können einige Aspekte möglicherweise nicht durch die Protokollierung erfasst werden. Beispiele sind

- Änderung von Berechtigungen
- Passwortänderungen
- Änderungen über SNMP
- Speicherung einer neuen Konfiguration in das NVRAM

In diesem Fall sollten andere Möglichkeiten der Überprüfung in Betracht gezogen werden, um zumindest feststellen zu können, dass Änderungen vorgenommen wurden.

In der Regel sind die zu protokollierenden Informationen unterschiedlichen Klassen zugeordnet. Dies ermöglicht eine Filterung der Protokollierung, indem in der Konfiguration die auszugebende Protokollierungsklasse angegeben wird.

Neben einer geeigneten Speicherung der Informationen kommt der möglichst zeitnahen Auswertung besondere Bedeutung zu. Hierfür existieren un-

terschiedliche Ausgabemöglichkeiten, die abgestimmt auf die individuellen Bedürfnisse auch in Kombination miteinander angewendet werden können:

**Nutzersession**

Die Protokollierungsinformationen können in einer bestehenden Nutzersession angezeigt werden. Hierzu müssen die Protokollierung und die Sitzung entsprechend konfiguriert werden.

**Speicher**

Protokollierungsinformationen lassen sich im systemeigenen RAM ablegen. Die Größe des dafür erforderlichen Speichers hängt stark vom Typ und Einsatzzweck des Gerätes ab, so dass an dieser Stelle keine konkreten Vorschläge gemacht werden können. Eine Speicherung der Protokollierungsinformationen auf einem zentralen Server (syslog) ist gegenüber der Speicherung im RAM zu bevorzugen.

**SNMP**

Herstellerabhängig lassen sich auf Routern und Switches für eine Vielzahl von Ereignissen SNMP-Nachrichten generieren, die von einem bestehenden Netzmanagementsystem erkannt, angezeigt und verarbeitet werden können. Dies ermöglicht eine automatisierte Auswertung.

**Ausgabe an der Konsole**

Die Ausgabe der Protokollierung an der Konsole erlaubt keine dauerhafte Speicherung kann daher lediglich eine Ergänzung zu anderen Methoden darstellen.

**Zentraler Authentisierungsserver**

Bei der Nutzung eines zentralen Authentisierungsservers, zum Beispiel mittels TACACS+ oder RADIUS, kann die dort implementierte Protokollierung (Accounting) genutzt werden, um Nutzeraktivitäten zu dokumentieren.

**Syslog**

Die Protokollierungsinformationen können über das Netz auf einen eigenen syslog-Server (beispielsweise auf einem Unix-Rechner) übertragen werden. Dies dient der zentralen Sammlung und Archivierung der Protokollierungsinformationen, da auf den Netzkomponenten oft keine ausreichenden Betriebsmittel dafür vorhanden sind. Dadurch können an einer zentralen Stelle relevante Informationen erfasst und ausgewertet werden. Außerdem bietet dies den Vorteil, dass bei einer Kompromittierung eines Gerätes die bereits übertragenen Protokollierungsinformationen vom Angreifer nicht verändert oder gelöscht werden können.

Die Übertragung zum syslog-Server erfolgt meist unverschlüsselt über TCP oder UDP, so dass ein Mithören auf dem Übertragungsweg möglich ist. Somit kann durch das Versenden von Informationen aus dem internen Netz die Vertraulichkeit der im internen Netz vorhandenen Informationen gefährdet werden. Daher sollte überlegt werden, die Übertragung über ein eigenes Netz (Administrationsnetz) abzuwickeln.

**NTP**

Alle Protokollierungsinformationen sollten mit einem korrekten Zeitstempel versehen sein. Nur so ist eine effektive Auswertung dieser Daten, insbeson-

dere bei der Analyse von versuchten oder erfolgten Angriffen, sichergestellt. Aus diesem Grunde sollten im internen Netz entsprechende Server eingerichtet werden, die allen Systemen die korrekte Zeit bereitstellen. Dies kann beispielsweise auf Basis des NTP-Dienstes geschehen. Dazu sollte in Erwägung gezogen werden, im internen Netz einen eigenen Zeit-Server einzurichten, der beispielsweise auf einem eigenen Rechner angesiedelt ist, der mit einer Funkuhr verbunden ist. Alternativ kann ein geeigneter Rechner als NTP-Proxy dienen und die Zeitinformation seinerseits per NTP von einem Zeit-Server im Internet (beispielsweise von der Physikalisch-Technischen Bundesanstalt (PTB)) bezieht. Im Zweifelsfall sollte die erste Lösung (interner Zeitserver mit Funkuhr) bevorzugt werden, insbesondere in Netzen mit hohem Schutzbedarf. Keinesfalls sollten alle Geräte individuell per NTP direkt Anfragen an Zeitserver im Internet stellen.

Prüffragen:

- Werden personenbezogene Daten in den Protokolldateien nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet?
- Ist der Umfang der Protokollierung und die Kriterien für deren Auswertung dokumentiert und abgestimmt?
- Sind Vorgaben definiert, wie eine zeitnahe Auswertung der Protokollinformationen durchzuführen ist?
- Werden die Protokollierungsinformationen mit einem korrekten Zeitstempel versehen?

# M 4.206 Sicherung von Switch-Ports

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In Abhängigkeit vom Schutzbedarf eines Netzes ist es oft wünschenswert, dass nur ganz bestimmte vertrauenswürdige Clients Zugang zum Netz erhalten. Zu diesem Zweck bieten viele Switches eine Reihe von Möglichkeiten, mit denen selbst dann, wenn ein Angreifer beispielsweise Zugang zu einer Netz-Anschlussdose erlangt hat, ein Zugriff auf das Netz verhindert werden kann.

### MAC-Address Notification

Viele Switches bieten die Möglichkeit zu protokollieren, wenn sich die an einem Port angeschlossene MAC-Adresse ändert. Diese Option bietet zwar keine Zugriffskontrolle, kann aber zur Entdeckung von Angriffen wichtig sein. Beispielsweise kann eine Nachricht an den Administrator verschickt werden, wenn sich eine MAC-Adresse ändert.

### MAC-Locking

Die verbreitetste Methode zur Absicherung von Switch-Ports ist das sogenannte MAC-Locking. Dabei wird am Switch festgelegt, dass an einem bestimmten physischen Port des Switches nur Clients mit ganz bestimmten MAC-Adressen (im Extremfall nur eine einzige MAC-Adresse) zugelassen sind. Erhält der Switch einen Ethernet-Frame mit einer anderen MAC-Adresse, so wird dieser nicht in das Netz weitergeleitet, sondern verworfen. Auf diese Weise kann in "statischen" Netzen ein relativ guter Schutz erreicht werden.

Allerdings ist die Pflege der entsprechenden Tabellen aufwändig. Daher ist es nicht sinnvoll, MAC-Locking bei größeren Installionen einzusetzen. Außerdem bietet MAC-Locking keinen Schutz vor einem Angreifer, der zunächst eine zugelassene MAC-Adresse ermittelt hat und beim Anschluss seines Gerätes diese Adresse verwendet (siehe auch G 5.113 *MAC-Spoofing*).

### IEEE 802.1X

Im Standard IEEE 802.1X wird eine Methode beschrieben, die eingesetzt werden kann, um eine ortsbasierte Netzzugangskontrolle für LAN und WLAN zu realisieren. Bevor einem IT-System Zugang zu einem nach dem IEEE 802.1X konfigurierten Netz gewährt wird, muss sich das neue Gerät (im Standard "Supplicant", auf deutsch Bittsteller, genannt) an einem Authentikator anmelden.

Der Authentikator ist für gewöhnlich ein Netzkoppelelement, also z. B. ein Switch, Router oder WLAN Access Point. Der Authentikator überprüft die übermittelten Authentisierungsdaten mit Hilfe eines Authentisierungsservers (häufig ein RADIUS-Server) und gibt je nach Ausgang dieser Überprüfung den Zugriff auf das Netz frei oder verwehrt ihn. Ohne eine erfolgreiche Authentisierung ist keine IP-basierte Kommunikation möglich.

Damit eine Port-basierte Authentisierung erfolgen kann, wird innerhalb des IEEE-Standards 802.1X das Extensible Authentication Protocol (EAP, RFC 3748) verwendet. Hierbei handelt es sich nicht um ein eigenes Authentisierungsverfahren, sondern um einen Rahmen, in den die eigentlichen Authentisierungsverfahren (EAP-Typen) eingebettet werden. Der Standard 802.1X sagt nichts darüber aus, welche tatsächliche EAP-Methode genutzt werden sollte. EAP unterstützt eine Reihe von Authentisierungsmethoden, so dass

abhängig vom Schutzbedarf der Informationen Passwörter, Zertifikate oder Zwei-Faktor-Authentisierungen genutzt werden können.

Mittlerweile sind schätzungsweise 40 EAP-Methoden bekannt. Hierzu gehören beispielweise EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-MSCHAPv2, EAP-LEAP, EAP-MD5. Weitere EAP-Methoden sind im Standard IEEE 802.1X und in der Technischen Richtlinie Sicheres WLAN des BSI beschrieben.

Generell ist es in größeren Installationen sinnvoll, zur Benutzerauthentisierung EAP gemäß IEEE 802.1X zu verwenden. Aufgrund der bekannten Sicherheitsprobleme wie Anfälligkeit gegenüber Man-in-the-Middle- bzw. Wörterbruchangriffen sollten EAP-MD5 und EAP-LEAP nicht mehr verwendet werden. Weiterhin ist es empfehlenswert in einem Netz mit einem hohen Schutzbedarf bezüglich der Vertraulichkeit eine starke port-basierte Zugriffskontrolle z. B. mittels EAP-TLS einzurichten.

**Andere Verfahren**

Je nach Hersteller existieren andere Verfahren, über die eine Zugriffskontrolle auf Switch-Ports realisiert werden kann. Beispielsweise gibt es die Möglichkeit, dass der Benutzer sich über ein Web-Interface anmeldet. Dabei läuft auf dem Switch ein Webserver, der die eingegebenen Authentisierungsdaten an einen Authentisierungsserver weiterleitet. Dabei muss allerdings beachtet werden, dass durch den auf dem Switch laufenden Webserver eventuell neue Gefährdungen entstehen.

Bei Geräten, die IEEE 802.1X oder andere Verfahren zur Zugriffskontrolle unterstützen ist es außerdem wichtig, den Default-Status vorzugeben, in dem sich ein Port normalerweise befindet.

Wenn eine port-basierte Zugriffskontrolle eingerichtet werden soll, so muss im Rahmen der Planung des Einsatzes der Switches geklärt werden, ob sowohl der Switch selbst als auch die vorgesehenen Clients die entsprechenden Protokolle und Authentisierungsmethoden unterstützen. Außerdem sollte vorab getestet werden, ob das Zusammenspiel von Clients, Switches und Authentisierungsserver reibungslos funktioniert. In der Sicherheitsrichtlinie und den Betriebsanweisungen für die aktiven Netzkomponenten sollten die zu verwendenden Verfahren und Default-Einstellungen dokumentiert werden.

Prüffragen:

- Erfolgt je nach Schutzbedarf eine port-basierte Zugriffskontrolle auf den Switches?

# M 4.207 Einsatz und Sicherung systemnaher z/OS-Terminals

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Steuerung und Kontrolle eines z/OS-Betriebssystems erfolgt über die *HMC*-Konsole (*Hardware Management Konsole),* über verschiedene *MCS*-Konsolen (*Multiple ConsoleSupport*), eventuell über *Extended MCS*-Konsolen und darüber hinaus, falls erforderlich, über Monitor-Konsolen. Weitere Informationen zu den Konsolen finden sich in der Maßnahme M 3.39 *Einführung in die zSeries-Plattform*.

**HMC-Konsolen**

*HMC*-Konsolen sind über ein LAN mit den *Support Elements* (SEs) des zSeries-Systems verbunden. Sie erlauben sicherheitskritische Eingriffe in die Hardware, den Microcode und die Konfiguration des gesamten z/OS-Systems. Die folgenden Hinweise sind zu beachten:

**Voreingestellte IBM-Kennungen**

Die mitgelieferten Passwörter der voreingestellten IBM-Kennungen müssen gegen neue Passwörter ausgetauscht werden (dies gilt auch für alle Kennungen von Nicht-IBM-Produkten). Hierbei ist M 2.11 *Regelung des Passwortgebrauchs* zu beachten.

**Schutz der HMC-Konsole**

Die HMC-Konsole sollte in einem Raum betrieben werden, der gegen unbefugten Zutritt geschützt ist.

Der Zugang zur HMC-Konsole muss logisch geschützt werden. Für den logischen Schutz sollte die Login-Funktion durch personenbezogene Kennungen mit Passwort gesichert werden.

Der *IBM Product Engineering* Zugriff ist während der normalen Produktion zu deaktivieren.

**Verbindung mit den Support Elements**

Die HMC-Konsole sollte über ein dediziertes LAN mit den *Support Elements* verbunden sein. Wenn ein anderes LAN mitbenutzt wird, sollte eine feste Zuordnung zwischen *Support Element* und HMC-Konsole definiert werden, z. B. durch entsprechende Einstellung in der *Domain-Security*-Funktion.

**Remote-Anbindung**

Wenn die HMC-Konsolen über eine Remote-Anbindung betrieben werden sollen, müssen entsprechende Schutzmaßnahmen für den Remote Access-Zugang vorgesehen werden. In diesem Fall ist Baustein B 4.4 *VPN* anzuwenden.

**Autorisierungs-Modi**

Das Personal sollte verschiedenen Autorisierungs-Modi zugeordnet werden. Diese Modi sollten wie folgt eingesetzt werden:

- Access Administrator

Dieser Modus ist nur an die Administratoren der HMC-Konsolen zu vergeben. Er darf nicht für normale Benutzer vergeben werden. Dieser Modus sollte nur wenigen Mitarbeitern zur Verfügung stehen.

- Operator
  Dieser Modus ist den normalen Bedienern zuzuordnen, die z. B. ein zSeries-Betriebssystem starten oder stoppen sollen (Initial Microcode Load oder Initial Program Load).
- Advanced Operator
  Dieser Modus wird normalerweise nicht benötigt, da die wesentlichen Betriebs-Funktionen in *Operator* enthalten sind und die anderen Funktionen, wie z. B. *Customization*, normalerweise unter *System Programmer* angesiedelt werden.
- System Programmer
  Dieser Modus sollte nur den Bedienern zugeordnet werden, die als System-Programmierer tätig sind und in dieser Funktion Anpassungen in der HMC-Konsole vornehmen.
- Service Representative
  Dieser Modus ist nur dem Service-Techniker vorbehalten und darf nicht anderweitig vergeben werden.

**Web-Server**

Die HMC-Konsole besitzt einen eigenen Web-Server, der einen eingeschränkten Funktionsumfang der HMC-Konsole für den Zugang über einen Web-Browser anbietet. Auf Netzebene sollten alle nicht autorisierten Zugänge zum Web-Server der HMC-Konsole gesperrt werden. Der Web-Server der HMC-Konsole sollte deaktiviert werden, wenn die Web-Schnittstelle zur HMC-Konsole nicht genutzt wird.

**Standard-Einstellungen**

Die vom Hersteller mitgelieferten Standard-Einstellungen der HMC-Konsole sollten geändert werden, so dass Benutzern nur die Darstellungen zugeordnet werden, die sie für ihre Arbeit auch benötigen (*Customize User Control Process* in der *HMC*-Konsole).

**Wartungsarbeiten**

Es ist eine Vorgehensweise für die Benutzung der HMC-Konsole, bzw. der *Support Elements*, durch Techniker für Wartungszwecke einzurichten. Es ist sicherzustellen, dass nach Beendigung der Wartungsarbeiten die HMC-Konsole mit einer Betriebskennung aktiviert wird und nicht weiter mit der hoch autorisierten Technikerkennung betrieben wird.

**Schulung**

Das für den Betrieb der *HMC*-Konsolen eingesetzte Personal ist für die Benutzung der Konsole zu schulen, besonders in Bezug auf die komplexeren Funktionen. Dadurch sollen gravierende Fehlbedienungen vermieden werden.

Es sollte überlegt werden, ob Übungen an der HMC-Konsole die Sicherheit erhöhen, da die Konsole im Betrieb nur selten benötigt wird.

**Support Elements (SEs)**

Die *Support Elements* (zwei IBM Laptops) befinden sich im Gehäuse der zSeries-Hardware und sind mit den Ressourcen der Hardware fest verbunden. Von diesen *Support Elements* aus können die gleichen Kommandos wie von der *HMC*-Konsole ausgeführt werden.

**Zugang**

Der Zugang zu den *Support Elements* muss physisch geschützt werden. Dies ist in der Regel dadurch gewährleistet, dass die zSeries-Systeme in einem Rechenzentrum betrieben werden, das gegen unbefugten Zutritt geschützt ist. Das Hardware-Schloss der zSeries-Hardware bietet keinen ausreichenden Schutz.

**Wartung**

Die *Support Elements* werden auch von den Hardware-Technikern des Herstellers zu Wartungszwecken genutzt. Nach Beendigung der Wartungstätigkeiten sollten die Türen der zSeries-Hardware abgeschlossen und ggf. weitere Sicherheitsmechanismen wieder aktiviert werden.

**MCS-Konsolen (Multiple Console Support)**

Die *MCS*-Konsolen (aus historischen Gründen auch immer noch MVS-Konsolen genannt) bieten direkten Zugriff auf das Betriebssystem (MCS mit eigenem Input/Output-Protokoll, SMCS via VTAM seit z/OS V1R1). Die folgenden Sicherheitsmechanismen sind für MCS- und SMCS-Konsolen vorzusehen:

**Login**

Es ist zu prüfen, ob der Schutz über *AUTH*-Definition im Member *CONSOL00* ausreicht oder ob *MCS*-Konsolen so definiert werden, dass ein Login mit Kennung und Passwort erforderlich ist, bevor die Konsole benutzt werden kann. Für *SMCS*-Konsolen, die auch Remote eingesetzt werden, ist ein Login-Vorgang in jedem Fall notwendig.

**Physischer Schutz**

Wenn kein Login mit Kennung und Passwort für die MCS-Konsole eingerichtet wird, muss sie in einem Raum betrieben werden, der vor unbefugtem Zutritt geschützt ist. Ausgenommen hiervon sind Konsolen, die so definiert sind, dass nur unkritische *Display*-Funktionen möglich sind.

Da die *MCS-Masterkonsole* nicht über Kennung und Passwort geschützt werden kann, muss diese Konsole in jedem Fall in einem Raum betrieben werden, der vor unbefugtem Zutritt geschützt ist.

Das z/OS-Betriebssystem macht die erste verfügbare Konsole zur Masterkonsole, soweit keine anderen Definitionen vorliegen. Die Zuordnung der Masterkonsole ist im Member *CONSOL00* sovorzunehmen, dass eine physisch geschützte Konsole zur Masterkonsole wird. Eine zweite MCS-Konsole, die durch das automatische Umschalten der primären MCS-Masterkonsole im Fehlerfall zum *Master* wird, ist auf die gleiche Weise wie die primäre MCS-Masterkonsole zu schützen.

**Logischer Schutz**

Es muss durch entsprechende Definitionen sichergestellt werden, dass MCS-Konsolen, die in nicht zutrittsgeschützten Räumen betrieben werden, nur von autorisierten Benutzern verwendet werden können. Dies kann über die Konfigurations-Parameter *AUTH=xxx* oder *LOGON=REQUIRED* im Member *CONSOL00* vorgenommen werden.

Sind die MCS-Konsolen auf andere Weise ausreichend geschützt und wird ein Audit der Operatoren nicht gefordert, kann statt *LOGON=REQUIRED* auch die Definition *LOGON=OPTIONAL* im Member *CONSOL00* verwendet werden.

**Individuelle Autorisierungen**

Für *MCS*-Konsolen mit *Login*-Prozess sollte überlegt werden, jeder Kennung individuelle Autorisierungen zuzuordnen. Dies ermöglicht die Einteilung in unterschiedliche Operator-Gruppen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*), was bei der Vorgehensweise ohne Authentisierung nicht möglich ist. Ansonsten stehen die Funktionen der Konsole für jeden offen, der physischen Zugang zur MCS-Konsole hat.

**Extended MCS-Konsolen**

Über die *Extended MCS-Konsole* stehen zum Beispiel MCS-Konsolen unter TSO (*Time Sharing Option*) via *System Display and Search Facility* (für JES2) oder *Flasher* (für JES3) zur Verfügung. Für diese Konsolen sollten die folgenden Hinweise beachtet werden:

**RACF-Definitionen**

Zum Schutz der MVS-Kommandos sind entsprechende RACF-Definitionen (Klasse *OPERCMDS*) einzusetzen. Ob die *Extended MCS*-Konsole benutzt werden darf, welche Kennung die *Extended MCS*-Konsole benutzen darf und welche Kommandos verfügbar sind, muss separat in RACF definiert werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). In jedem Fall muss sichergestellt sein, dass die Konsol-Services und die dabei verwendeten z/OS-Kommandos nur von Anwendern benutzt werden können, die in RACF entsprechend autorisiert worden sind. Dies gilt für alle Applikationen, die mit *Extended MCS*-Konsolen arbeiten.

**RSF-Konsole (Remote Support Facility)**

RSF (*Remote Support Facility*) ermöglicht es dem zSeries-System, automatisch mit dem Hersteller Verbindung aufzunehmen und den dortigen Technikern Fehler des laufenden Systems zu melden (Hard- und Software). Darüber hinaus erlaubt es die RSF-Funktion prinzipiell auch, dass der Hersteller Microcode-Modifikationen in das System laden kann. RSF ist eine zusätzliche Funktion der HMC-Konsole (*Host Management Console*) und ist über eine Wählverbindung an das Telefonnetz angeschlossen.

Für die RSF-Funktion sind die folgenden Hinweise zu berücksichtigen:

**Grundsätzliche RSF-Überlegung**

Es ist zu überlegen, ob eine Funktion wie RSF überhaupt gewünscht wird und welche Teilfunktionen davon benötigt werden. Der Einsatz der Funktion muss mit dem für die Systeme zuständigen Hardware-Support über den Wartungsvertrag abgestimmt werden. RSF (und ähnliche Funktionen bei Festplatten von anderen Herstellern) wird normalerweise für die Fehlererkennung von Hard- und Firmware eingesetzt und erhöht deutlich die Reaktionsfähigkeit auf auftretende Fehler. Ob die Fernwartung durch RSF aktiviert werden soll, muss der Betreiber des Rechenzentrums entscheiden.

**Wählverbindung zum Hersteller**

Fehlermeldungen werden von der HMC-Seite aus initiiert, dabei wird eine Wählverbindung zum Hersteller aufgebaut. Es ist im Rahmen der Anpassung

der HMC-Definitionen sicherzustellen, dass die eingetragene Telefonnummer korrekt ist und nur von autorisiertem Personal geändert werden darf.

**Microcode-Anpassung**

Wird eine Microcode-Anpassung (oder sonstige Modifikation der Firmware) durch den Hersteller angefordert, so ist der *IBM Product Engineering* Zugriff für den vereinbarten Zeitraum zu aktivieren. Die Verbindung wird dabei durch *Dial-In* hergestellt. Nach Ablauf der Wartungsarbeiten ist er wieder zu deaktivieren, um das Missbrauchsrisiko zu minimieren.

**Dokumentation**

Die RSF-Installation und deren Einsatz ist nachvollziehbar zu dokumentieren.

Prüffragen:

- Wurden die mitgelieferten Passwörter der voreingestellten IBM-Kennungen des z/OS-Systems gegen neue Passwörter ausgetauscht?
- Ist der Zutritt und Zugang zur HMC-Konsole, zur MCS-Masterkonsole, zu den (Extended) MCS-Konsolen und zu den Support Elements der zSeries-Systeme angemessen geschützt?
- Falls ein Remote Access-Zugang zu den HMC-Konsolen im z/OS-System existiert: Ist der Fernzugang angemessen geschützt?
- Wurde dem Personal für die z/OS-Systeme die Autorisierungs-Modi zugewiesen, die für ihre jeweiligen Aufgaben geeignet sind?
- Sind auf Netzebene alle nicht autorisierten Zugänge zum Web-Server der HMC-Konsole im z/OS-System gesperrt?
- Wenn die Web-Schnittstelle zur HMC-Konsole nicht genutzt wird: Wird der Web-Server der HMC-Konsole deaktiviert?
- Sind den Benutzern für die HMC-Konsole im z/OS-System nur die Darstellungen zugeordnet, die sie für ihre Arbeit auch benötigen?
- Ist eine Vorgehensweise für die Benutzung der HMC-Konsole bzw. der Support Elements für Wartungszwecke festgelegt?
- Ist das für den Betrieb der HMC-Konsolen zum z/OS-Systems eingesetzte Personal für die Benutzung der Konsole geschult?
- Entsprechen die RSF-Einstellungen der zSeries-Systeme den Vorgaben der Institution?
- Ist die RSF-Installation und deren Einsatz zum zSeries-System nachvollziehbar dokumentiert?

# M 4.208 Absichern des Start-Vorgangs von z/OS-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Startvorgang eines z/OS-Systems erfolgt beginnend mit dem IML-Ablauf (*Initial Microcode Load*) über den IPL-Ablauf (*Initial ProgramLoad*) eines z/OS-Betriebssystems bis hin zum Starten der einzelnen *System Tasks*. Für den Startvorgang sollten die folgenden Hinweise beachtet werden:

### IML- und IPL-Parameter

Die IML- und IPL-Parameter müssen dem *Operating*-Personal bekannt sein. Eine aktuelle Dokumentation muss vorliegen.

### Fallback-Konfiguration

Es muss immer eine Fallback-Konfiguration vorliegen. Mit der Fallback-Konfiguration muss das System vor der letzten Änderung erfolgreich gestartet worden sein.

### IOCDS-Datei

Es muss eine gültige IOCDS-Datei (*Input/Output Configuration DataSet*) im HMC-Dialog (*Host Management Console*) verfügbar sein, mit der das System gestartet werden kann.

### LPAR

Das zu startende System muss als LPAR (*Logical Partition*) auf der zSeries-Hardware eingerichtet und entsprechend konfiguriert sein.

### MVS-Master-Konsole

Es muss eine MVS-Master-Konsole (*Multiple Virtual Systems*) verfügbar sein, damit die Nachrichten während der NIP-Phase (*Nucleus Initialization Program*) kontrolliert werden können. Zusätzlich muss eine Backup-Konsole definiert sein, auf die der *Master* automatisch umgeschaltet werden kann, wenn die normale Master-Konsole aus technischen Gründen nicht verfügbar ist (siehe M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*).

### Automationsverfahren

Werden Automationsverfahren eingesetzt, muss eine Dokumentation vorliegen, welche *System Tasks* in welcher Reihenfolgen zu starten sind. Auch die notwendigen Kommandos müssen dokumentiert sein, um eventuelle Fehler der Automation (oder auch deren Komplettausfall) zumindest teilweise kompensieren zu können.

### Abschluss des Startvorgangs

Es sollte eine Nachricht an das Ende des Startvorgangs platziert werden, die anzeigt, dass der Startvorgang abgeschlossen ist.

### Prüfliste

Es sollte eine aktuelle Prüfliste vorliegen, die nach dem Startvorgang zur Überprüfung des System-Status herangezogen werden kann. Die Überprü-

fung stellt sicher, dass das z/OS-System wie vorgesehen ohne Fehler aktiviert worden ist (Soll/Ist-Vergleich). Wenn Automationsverfahren existieren, können auch Funktionen aus diesen Verfahren dazu benutzt werden.

Prüffragen:

- Sind die aktuellen IML- und IPL-Parameter dokumentiert und dem Operating-Personal bekannt?
- Sind eine MVS-Master-Konsole und eine Backup-Konsole vorhanden, um Nachrichten während des Start-Vorgangs des z/OS-Systems zu kontrollieren.
- Ist eine Backup-Konsole im z/OS-System definiert, auf die der Master automatisch umgeschaltet werden kann, wenn die normale Master-Konsole nicht verfügbar ist?
- Zeigt eine Nachricht am Ende des Startvorgangs den Abschluss des Startvorgangs des z/OS-Systems an?
- Liegt eine aktuelle Prüfliste vor, die nach dem Startvorgang des z/OS-Systems zur Überprüfung des System-Status herangezogen werden kann?

# M 4.209 Sichere Grundkonfiguration von z/OS-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das z/OS-Betriebssystem verwaltet und benutzt verschiedene Autorisierungsmechanismen. Bei fehlerhaftem Einsatz oder Missbrauch dieser Mechanismen kann sich dies auf die Integrität des gesamten Systems auswirken. Sie müssen deshalb in der Grundkonfiguration berücksichtigt werden. Es handelt sich dabei im Wesentlichen um die folgenden Funktionen:

- APF-autorisierte Dateien (*Authorized Program Facility*),
- SVCs (*SuperVisor Calls*),
- Ressourcen-Schutz,
- Parmlib-Definitionen,
- System Prozeduren (*Started Tasks*) und
- JES2-Definitionen.

Empfehlungen für das Sicherheitssystem RACF (*Resource Access Control Facility*) sind in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben. Darüber hinaus ist M 4.220 *Absicherung von Unix System Services bei z/OS-Systemen* für die Grundkonfiguration zu berücksichtigen.

Um die Integrität des z/OS-Betriebssystems zu schützen, sind die folgenden Empfehlungen zu berücksichtigen:

**APF-Autorisierungen**

Über APF-autorisierte Dateien ist es möglich, sich Zugriff zu privilegierten Operationen zu verschaffen (z. B. *MODESET SVC*). In der Folge lassen sich dadurch Funktionen benutzen, für die der Anwender normalerweise nicht autorisiert ist. So ist es jederzeit möglich, sich im Supervisor-Modus Zugriff zu privilegierten Hauptspeicherbereichen zu verschaffen und dort hoch privilegierte Attribute (z. B. *SPECIAL* im *ACEE - Accessor Environment Element*) der eigenen Kennung zuzuordnen. Für APF-Dateien ist das Folgende zu beachten:

- Alle APF-Dateien müssen über vollqualifizierte generische RACF-Profile (wie auch in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben) geschützt werden, d. h. trotz der Benutzung von generischen Profilen sollte der komplette Dateiname als Profilname benutzt werden.
- Alle APF-Dateien werden im Parmlib-Member *PROGnn* mit Volume-Angaben (bzw. Angabe *SMS*) definiert. Es dürfen keine Einträge existieren, zu denen es keine Datei gibt, da sonst die Gefahr besteht, dass eine andere Datei untergeschoben wird.
- Zugriff zu den APF-Dateien dürfen nur Mitarbeiter haben, zu deren Aufgaben die Wartung des Systems gehört. Die Anzahl dieser Mitarbeiter ist auf ein Minimum zu beschränken. Eine Vertreterregelung muss vorgesehen sein.
- APF-Dateien sind regelmäßig auf Veränderungen zu überprüfen, um Missbrauch und Missbrauchsversuche möglichst frühzeitig zu entdecken. Änderungen an diesen Dateien sollten unter Produktionsbedingungen nur über angemeldete Wartungsfenster erfolgen.
- Es ist zu überlegen, ob der Einsatz eines Real-Time-Monitors hilft, Missbrauch schneller zu entdecken, und somit zur Erhöhung der Sicherheit beitragen kann (siehe M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). In jedem Fall sollten mindestens manuelle Kontrollen der Zu-

griffe auf APF-Dateien durchgeführt werden, etwa durch Auswertung von SMF-Sätzen (*System Management Facility*).
- Alle APF-Dateien sollten ohne *Extents* angelegt werden.
- Es sollte berücksichtigt werden, dass alle in der *LINKLIST* definierten Dateien bei Benutzung des Parameters *LNKAUTH=LNKLST* im Member *IEASYSxx* vom System standardmäßig als APF-Dateien angesehen werden. Auch für diese Dateien müssen deshalb die oben beschriebenen Sicherheitsmechanismen aktiviert werden.

**User SVCs (SuperVisor Calls)**

*User-SVCs* (alle SVC-Nummern ab 200) erhalten die Kontrolle im *SuperVisor*-Status mit *Key 0* (diesentspricht dem *Kernel-Modus* bei einigen anderen Betriebssystemen), d. h. User-SVCs haben Zugriff auf alleSpeicherbereiche und alle Operationendes z/OS-Betriebssystems. Für *User-SVCs* ist deshalb das Folgende zu beachten:

- Alle Dateien, die SVC-Programme bereitstellen, müssen über vollqualifizierte generische RACF-Profile (wie auch in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben) geschützt werden.
- Alle SVCs werden im Parmlib-Member *IEASVCxx* definiert. Da ein SVC durch die notwendigen internen Sicherheitsmechanismen nicht sehr klein sein kann, deutet ein *User-SVC*-Modul mit kleiner Länge eventuell auf ein Sicherheitsproblem hin. Solche *User-SVCs* müssen von der Systemprogrammierung darauf untersucht werden, ob sicherheitskritische Lücken vorhanden sind. In früheren Jahren wurden oft SVCs mit unzureichenden Sicherheitsmechanismen eingesetzt, z.B. sogenannte *Autorisierungs-SVCs*, um autorisierte Funktionen aus nicht-autorisierten Umgebungen heraus ausführen zu können. Falls solche SVCs noch existieren, sollten sie nach Möglichkeit entfernt oder ersetzt werden.
- Werden *User-SVCs* im Rahmen von Produkten mitgeliefert, sollten beim Hersteller die Sicherheitsmechanismen der mitgelieferten SVCs erfragt werden. Dies ist besonders wichtig, wenn das gelieferte SVC-Modul sehr klein ist, denn das ist eventuell ein Hinweis auf fehlende interne Prüfungen.
- Zugriff auf SVC-Dateien dürfen nur Mitarbeiter haben, zu deren Aufgaben die Wartung des Systems gehört. Die Anzahl dieser Mitarbeiter ist zu minimieren. Dabei muss jedoch sichergestellt werden, dass mindestens ein Vertreter Zugriff hat.

**Ressourcen**

Ressourcen des z/OS-Betriebssystems (z.B. Dateien, Programme, Funktionen usw.) sind über RACF zu schützen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Darüber hinaus sollten folgende Empfehlungen beachtet werden:

- Für die *Class Descriptor Table* (CDT) sollten installationsspezifische Einträge nur im Modul *ICHRRCDE* vorgenommen werden. Als wichtige Parameter sind *DFTUACC* (hier wird *NONE* empfohlen) und *OPER* (hier wird *NO* empfohlen) zu beachten. Die *Dataset Name Table* (DSNT) muss die Dateinamen der RACF-Datenbanken enthalten.
- Die *Authorized Caller Table* (AUT) sollte laut Empfehlung von IBM leer sein. Dabei handelt es sich um eine alte Funktion, die heute durch die Klasse *Program* ersetzt worden ist, aber noch existiert. Ausnahmen müssen begründet sein.
- Die *TSO Authorized command and program table* in der Parmlib (*IKJTSOxx*) darf nur die Kommando- und Programm-Namen enthalten, die für die Ausführung unter TSO (*Time Sharing Option*) notwendig sind.
- Die *Started Procedure Table* (*ICHRIN03*) sollte nur noch wenige Einträge für Notfälle enthalten, ansonsten sollte für die Definition der autorisierten

*Started Tasks* die RACF Klasse *STARTED* benutzt werden. Das Attribut *PRIVILEGED* sollte vermieden, *TRUSTED* nur eingesetzt werden, wenn erforderlich (z.B. bei JES2). Die Tabelle sollte einen generischen Eintrag für alle *Started Tasks* enthalten, die nicht definiert sind, um sicherzustellen, dass diese Tasks nicht lauffähig sind.
- Die *RACF Router Table* muss synchron zur CDT gepflegt werden.
- RACF bietet zwei Algorithmen zum Verschlüsseln des Passwortes an, den *Masking Algorithm* und die DES-Verschlüsselung (*Data Encryption Standard*). Die RACF-Passwörter sollten DES-verschlüsselt werden, da dies einen besseren Schutz bietet als das *Masking*. Gesteuert wird dies über den RACF-Exit *ICHDEX01*. RACF-spezifische Empfehlungen sind in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* zu finden.

**IPL-Parameter-Datei**

In der IPL-Parameter-Datei (*Initial Program Load*) stehen die wesentlichen Informationen, die zum Initialisieren des z/OS-Betriebssystems benötigt werden. Diese Datei muss über RACF geschützt werden, die Zahl der für diese Datei autorisierten Mitarbeiter muss klein gehalten werden. Es ist jedoch darauf zu achten, dass Vertretungsregeln eingeführt sind.

**Parmlib-Definitionen**

In den Parameter-Dateien des z/OS-Betriebssystems (*SYSn.PARMLIBs*, es können mehrere vorhanden sein) werden wesentliche Definitionen des Betriebssystems abgelegt. Alle Parmlib-Dateien sind mittels RACF-Profil zu schützen. Der Zugriff darf nur den Mitarbeitern erlaubt sein, die im Rahmen ihrer Tätigkeit diese Dateien bearbeiten. Es ist zu überlegen, ob verschiedene Parameter-Dateien mit unterschiedlichem RACF-Schutz eingesetzt werden sollen, da in der Parmlib Definitionen mit unterschiedlichem Schutzbedarf existieren. Sicherheitskritische Member der Parmlib sind zum Beispiel (ohne Sortierung):

- BPXPRMxx
- CLOCKxx
- COMMNDxx
- CSVLLA00
- IEASYSxx
- IEFSSNxx
- IKJTSOxx
- MSTJCLxx
- PROGxx
- SCHEDxx
- SMFPRMxx

Der Zugriff auf diese Definitionen muss auf die notwendigen Mitarbeiter beschränkt werden. Vertretungsregeln müssen in Kraft sein.

**System-Prozeduren**

Alle wichtigen Prozeduren der *Started Tasks* stehen in speziellen Bibliotheken, die entweder über die MSTJCLxx-Definitionen, oder über die JES2/3-Definitionen dem System bekannt gegeben werden. Diese Dateien, z. B. *SYS1.PROCLIB*, müssen über RACF-Profile geschützt werden, die nur autorisierten Mitarbeitern Zugriff auf die Definitionen gewähren.

Besonders wichtig ist der Schutz von allgemeinen, d. h. von allen Mitarbeitern benutzten Login-Prozeduren, da hier die Gefahr des Missbrauchs besonders groß ist (siehe Maßnahme M 4.213 *Absichern des Login-Vorgangs unter z/OS*). Der schreibende/ändernde Zugriff sollte auf die Systemadministratoren

beschränkt werden, darüber hinaus benötigt nur JES2/3 einen lesenden Zugriff.

Diese Schutzvorkehrungen gelten auch für alle in allgemeinen Login-Prozeduren verwendeten Script-Dateien (TSO CLISTs oder REXX EXECs), da auch hier die Gefahr des Missbrauchs besonders groß ist.

**JESx Definitionen (Job Entry Subsystem)**

Zum Schutz der *Job Entry Subsysteme* JES2 und JES3 müssen hauptsächlich die folgenden Ressourcen durch RACF abgesichert werden:

- JES-eigene Dateien,
- Input von anderen Quellen (z. B. anderen Knoten),
- Jobnamen,
- System Input/Output auf der JES-Spool und
- Output für andere Knoten oder Remote Workstations.

Die folgenden RACF-Funktionen sollten eingesetzt werden, um die Sicherheit von JES2/3 zu erhöhen:

- BATCHALLRACF
  (Erzwingen der Kennung bei Batch-Jobs)
- EARLYVERIFY
  (nur noch *Early Verify* möglich)
- XBMALLRACF
  (Unterstützung des Execution Batch Monitors)
- NJEUSERID
  (Zuordnung der *Default Userid* bei *Network Job Entry* Funktionen)
- UNDEFINEDUSER
  (Zuordnung der *Undefined Userid* bei *Network Job Entry* Funktionen)

Darüber hinaus stellt RACF eine Reihe von *General Resource Classes* für JES2/3 zur Verfügung, die zum Schutz von JES-Funktionen eingesetzt werden sollten:

- OPERCMDS
- JESSPOOL
- SURROGAT
- NODES
- WRITER

Prüffragen:

- Ist sichergestellt, dass nur Mitarbeiter, zu deren Aufgaben die Wartung des z/OS-Systems gehört, Zugriff zu den APF- und SVC-Dateien haben?
- Existiert eine Vertreterregelung für die Grundkonfiguration der z/OS-Systeme?
- Werden im z/OS-System die APF-Dateien regelmäßig auf Veränderungen überprüft?
- Sind alle APF-Dateien im z/OS-System ohne Extents angelegt?
- Sind die Ressourcen des z/OS-Betriebssystems über RACF geschützt?
- Sind die IPL-Parameter-Datei und alle Parmlib-Dateien über RACF im z/OS-System geschützt?
- Ist der Zugriff auf Parmlib-Dateien im z/OS-System auf die Mitarbeiter begrenzt, die diese Dateien regulär bearbeiten müssen?
- Sind alle wichtigen System-Prozeduren über RACF-Profile im z/OS-System so geschützt, dass nur autorisierten Mitarbeitern der Zugriff auf die Definitionen möglich ist?
- Sind die Job Entry Subsysteme JES2 bzw. JES3 durch RACF geschützt?

# M 4.210 Sicherer Betrieb des z/OS-Betriebssystems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein z/OS-Betriebssystem läuft im Normalfall weitgehend autonom ohne Eingriffe durch das Bedienungspersonal. Zur Absicherung des Betriebes gibt es jedoch einige Maßnahmen, die notwendigerweise ergriffen werden müssen, wenn die Funktionalitäten eines z/OS-Betriebssystems ohne Probleme zur Verfügung stehen sollen:

**Überwachung**

*HMC-Kontrolle*

Die HMC (*Host Management Console*) ist regelmäßig auf dort gemeldete Fehler (Hardware, Microcode, Software) zu untersuchen. Fehler, die dem Hersteller durch die RSF-Funktion (*Remote Support Facility*) gemeldet werden, sollten in der Betriebsorganisation bekannt sein, bevor der Hersteller anruft.

*WTOR-Überwachung*

WTOR-Nachrichten (*Write To Operator with Reply*) des z/OS-Betriebssystems müssen überwacht werden, um sicherzustellen, dass neu hinzugekommene Anfragen des Betriebssystems, falls erforderlich, sofort beantwortet werden. Analog gilt dies auch für wichtige WTO-Nachrichten (*Write To Operator*) des Betriebssystems oder seiner Komponenten, die unter Umständen ein sofortiges Reagieren erfordern.

*System Tasks*

Es muss sichergestellt werden, dass alle geplanten *System Tasks* aktiv sind. Dies ist meist an bestimmten Nachrichten während des Starts oder an Reaktionen der jeweiligen *System Task* auf Abfragen zu erkennen. Es reicht meist nicht aus, nur deren Vorhandensein durch *Display*-Kommandos zu kontrollieren, sondern es sollte auch die Reaktion der *System Task* geprüft werden.

*Kapazitätskontrolle*

Es muss sichergestellt werden, dass die Kapazitätsgrenzen des Systems nicht überschritten werden. Dies bedeutet, dass die planerischen Vorgaben eingehalten werden sollten, was regelmäßig zu überprüfen ist.

*Überwachung der Sicherheitsverletzungen*

Die Einhaltung der Sicherheitsvorgaben muss überwacht werden. Sicherheitsverletzungen müssen über die definierten Mechanismen gemeldet werden (siehe M 2.292 *Überwachung von z/OS-Systemen*).

*System-Auslastung*

Die Systemauslastung muss mit geeigneten Mitteln überwacht werden, bei Überlastung sind korrektive Maßnahmen erforderlich, z. B. das Reduzieren der JES2/3 *Initiators* (*Job Entry Subsystem*).

Es ist zu überlegen, ob neben den standardmäßig vorhandenen Funktionen (RMF - *Resource Measurement Facility*) zusätzliche, spezielle Monitore eingesetzt werden sollen, um das System noch effizienter zu überwachen.

*Automation System*

Es ist zu überlegen, ob eine Automationsfunktion (als Eigenentwicklung oder als fertiges Produkt) eingesetzt werden sollte, um die trivialen Überprüfungen des Systems regelmäßig durchzuführen. Dazu gehört z. B. der Soll-/Ist-Vergleich aktiver Tasks und aktiver NJE-Verbindungen sowie offene Replies, System-Performance, JES2/3 Queue-Belegung und mehr. Dies ermöglicht eine einheitliche *System Alive*-Nachricht statt vieler unstrukturierter Nachrichten, wodurch die Kontrolle wesentlich erleichtert werden kann.

Werden mehrere z/OS-Systeme zentral von einer Funktion überwacht, sollte überlegt werden, die Ausnahme-Informationen (*Events*) an einer Konsole darzustellen (*AlertManagement*). Verschiedene Hersteller bieten entsprechende Programme im Rahmen ihrer Automationspakete an.

*Automation Batch-Jobs*

Es ist zu überlegen, ob eine Automationsfunktion für die Kontrolle der Batch-Jobs eingesetzt werden soll. Ab einer bestimmten Anzahl von zu kontrollierenden Batch-Jobs ist dies unabdingbar, da sonst eine konsistente Überwachung nicht mehr zu realisieren ist. Job-Scheduler, die tausende von Batch-Jobs kontrollieren können, sind von verschiedenen Herstellern erhältlich.

*Reduzieren der Systemnachrichten*

Systemnachrichten sollten so reduziert werden, dass nur wirklich wichtige Nachrichten dargestellt werden. Der Einsatz von Nachrichten-Filtern ist im Rahmen von Automationsfunktionen zu empfehlen (MPF - *Message Processing Facility*).

*Focal Point Konzept*

Wenn viele z/OS-Betriebssysteme eingesetzt werden, ist zu überlegen, eine zentrale Kontrollstelle (*Focal Point*) einzurichten.

**Absicherung der Betriebsfunktionen**

Informationssicherheit ist keine Einmal-Angelegenheit, sie muss im laufenden Betrieb immer wieder überprüft und auch an die Gegebenheiten angepasst werden. Solche Anpassungen erfordern im laufenden Betrieb oft sicherheitsrelevante Aktionen, die entsprechend geschützt werden müssen. Für den sicheren Betrieb eines z/OS-Systems müssen deshalb folgende Empfehlungen berücksichtigt werden:

*Kontrollierte Wartungsarbeiten*

An einem laufenden z/OS-System dürfen keine die Produktion beeinflussenden Wartungsarbeiten und Änderungen außerhalb des Wartungsfensters durchgeführt werden. Alle Änderungen, ob geplant oder ungeplant, müssen über ein Change-Management-Verfahren mit allen beteiligten Fachverantwortlichen abgestimmt werden. Der Change-Plan sollte zur Nachverfolgbarkeit archiviert werden.

*Software Installation durch SMP/E*

Eine Software-Installation darf erst nach einer Anmeldung über das Change-Management-Verfahren durchgeführt werden. Um Fehler zu vermeiden, muss zur Software-Installation ein Verfahren wie SMP/E (*System Management Process Enhanced*) eingesetzt werden.

*Dynamische Änderungen*

Viele sicherheitsrelevante Änderungen lassen sich heute dynamisch, d. h. während des Betriebs, vornehmen, ohne dass ein IPL (*Initial Program Load*) notwendig wäre. Dynamische Änderungen am System dürfen nur während geplanter Wartungsarbeiten, bzw. auf Antrag, ausgeführt werden. Besonders sicherheitsrelevante dynamische Befehle, wie z. B. *SETAPF*, *REFRESH LLA*, *MODIFY*, *CONFIG*, *FORCE* oder *SET*, müssen über entsprechende RACF-Profile geschützt werden. Sie dürfen nur von geschultem Personal auszuführen sein.

*SDSF*

SDSF (*System Display and Search Facility*) muss so geschützt werden, dass Unberechtigte keine Systemkommandos missbrauchen können. So darf es z. B. nicht möglich sein, beliebig viele *Initiators* zu aktivieren. Weiterhin muss die Prioritäten-Steuerung für Jobs im System in SDSF geschützt werden (Zuordnung von *WLM-Service-Klassen*). Es darf Anwendern nicht erlaubt sein, die Priorität ihrer Batch-Jobs zu ändern, um z. B. für sich eine bessere Performance zu erhalten.

Diese Empfehlung gilt analog auch für *Flasher*, eine JES3-Unterstützung, die in dieser Hinsicht der SDSF-Funktionalität entspricht.

*Schutz der Konsolen*

Der Schutz der Konsolen ist in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*) beschrieben. Es muss durch entsprechende RACF-Definitionen verhindert werden, dass sich Mitarbeiter unberechtigt Zugang zu einer EMCS (*Extended Multiple Console Support*) verschaffen können.

*Schutz der MVS-Kommandos*

z/OS-System-Kommandos dürfen nur von berechtigten Personen ausgeführt werden. Diese Kommandos müssen über entsprechende RACF-Profile geschützt sein. Es muss festgelegt werden, welche Mitarbeiter die Berechtigung für bestimmte System-Kommandos benötigen und diese ausführen dürfen. So ist zu überlegen, ob z. B. das Stoppen und Starten von Tasks allein durch das *Operating* zu erfolgen hat.

*HCD*

Bestimmte Hardware-Einstellungen können während des Betriebs eines z/OS-Systems nachträglich definiert werden. Dies erfolgt durch den HCD-Prozess (*HardwareConfiguration Definition*). Die Aktivierung des neuen IO-CDS (*Input/Output Configuration Dataset*) sollte jedoch nur im Rahmen des Change-Managements durchgeführt werden.

Bei der Definition von Hardware muss darauf geachtet werden, dass es nicht vorkommt, dass Ressourcen über mehrere Einzelsysteme *Shared* definiert werden. Ein Zugriff auf die gleiche Festplatte von zwei unterschiedlichen Einzelsystemen aus sollte beispielsweise nicht möglich sein. Bei *Parallel-Sy-*

*splex*-Konfigurationen gehört *Resource-Sharing* zur Architektur und ist deshalb - bei sachgerechter Konfiguration - kein Problem.

*Operation (Betrieb)*

Es sollte überlegt werden, für das *Operating* zwei RACF-Gruppen einzurichten, eine für langjährig erfahrene Operatoren und eine zweite für neue (noch unerfahrene) Mitarbeiter. Alle Mitarbeiter sollten nur die Rechte erhalten, die sie benötigen. Sie müssen für ihre Aufgaben ausreichend geschult sein. Besonders sicherheitskritische Aufgaben sollten erfahrenen Mitarbeitern übertragen werden.

Prüffragen:

- Wird unter z/OS die Host Management Console regelmäßig auf dort gemeldete Fehler untersucht?
- Werden WTOR-Nachrichten überwacht, um sicherzustellen, dass neu hinzugekommene Anfragen des z/OS-Betriebssystems, falls erforderlich, sofort beantwortet werden?
- Ist sichergestellt, dass alle geplanten System Tasks des z/OS-Systems aktiv sind?
- Werden die Systemauslastung und die Einhaltung der geplanten Kapazitätsgrenzen des z/OS-Systems geeignet überwacht?
- Wird die Einhaltung der Sicherheitsvorgaben zum z/OS-System überwacht?
- Werden z/OS-Systemnachrichten so reduziert, dass nur wichtige Nachrichten dargestellt werden?
- Werden Wartungsarbeiten am z/OS-System über ein nachvollziehbares Change-Management-Verfahren mit allen beteiligten Fachverantwortlichen abgestimmt?
- Wird zur Software-Installation unter z/OS ein Verfahren wie SMP/E eingesetzt?
- Sind die z/OS-System-Kommandos über entsprechende RACF-Profile geschützt, so dass nur berechtigte Personen diese Kommandos ausführen können?
- Werden die Mitarbeiter, die für das Operating des z/OS-Systems verantwortlich sind, ausreichend geschult?

# M 4.211 Einsatz des z/OS-Sicherheitssystems RACF

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die sichere Konfiguration eines z/OS-Systems erfolgt durch Definitionen von Betriebssystem-Komponenten und zentral über das Sicherheitssystem RACF (*Resource Access Control Facility*). In dieser Maßnahme werden Empfehlungen für den Einsatz von RACF erläutert. Informationen für die Sicherung der z/OS-Definitionen können der Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* entnommen werden.

In RACF werden die Kennungen der Anwender und die Zugriffsmöglichkeiten auf unterschiedliche Ressourcen in Form von Profilen verwaltet. Diese stehen als *Dataset* Profile, *General Resource* Profile, *Group* Profile und deren Verbindungen sowie als *User* Profile zur Verfügung.

Für die Verwaltung von RACF sind die folgenden Regeln zu berücksichtigen:

### Wesentliche RACF-Einstellungen

*SETROPTS Definitionen*

Die zentrale Konfiguration des RACF erfolgt in den *SETROPTS* Einstellungen. Hier werden allgemeingültige systemweite Einstellungen für das RACF vorgenommen. Da hier sehr viele Parameter veränderbar sind und sich teilweise gegenseitig beeinflussen, müssen die Einstellungen gut konzipiert und durchdacht sein. Nachfolgend eine Aufzählung der wichtigsten Parameter, die über das Kommando *SETROPTS* gesetzt werden müssen.

| ***Resource Access Policies* für allgemeine Resource-Klassen** | |
|---|---|
| CLASSACT | Access Authorization Checking |
| AUDIT | schaltet Protokollfunktion für Klassen an |
| RACLIST | definiert, welche Profile in den Speicher geladen werden |
| GENERIC | aktiviert *Generic Profile Checking* |
| NOADSP | verhindert diskrete Profile |
| PROTECTALL | stellt sicher, dass RACF-Profile erstellt werden |
| WHEN | erlaubt konditionalen Schutz für Programme |
| CMDVIOL | protokolliert alle RACF-Verstöße |
| OPERAUDIT | kontrolliert Kennungen mit Attribut *OPERATIONS* |
| ERASE | löscht Dateninhalt nach Löschen einer Datei |
| u. a. | |

Tabelle: *Resource Access Policies* für allgemeine Resource-Klassen

| ***Password Policies* für die Behandlung der Passwörter** | |
|---|---|
| INTERVAL | Gültigkeitsdauer des aktuellen Passworts |
| REVOKE | Anzahl ungültiger Anmelde-Versuche vor dem Sperren |
| RULE | definiert Passwort-Regeln |
| u. a. | |

Tabelle: *Password Policies* für die Behandlung der Passwörter

Die RACF-Grundeinstellung ist wesentlich für die Sicherheit des z/OS-Betriebssystems und relativ komplex. Da hier u. U. mehr als 30 Parameter definiert oder aktiviert werden müssen, ist eine ausführliche Planung notwendig. Diese stellt sicher, dass die Parameter richtig gesetzt werden und vermeidet so potentielle Sicherheitslücken. Zur Unterstützung des Planungsvorgangs bietet der Hersteller einen *RACF Security Planner* an (auch im Internet). Der *RACF Security Planner* gibt auch Empfehlungen für die RACF-Grundeinstellung.

*Voreingestelltes RVARY-Passwort*

Das voreingestellte Passwort für das RVARY-Kommando, z. B. für den SWITCH der RACF-Datenbanken, muss verändert werden und darf nicht auf dem voreingestellten Wert stehen.

*Einsatz von RACF-Exits*

Es ist zu untersuchen, ob *RACF-Exits* benötigt werden. Durch verschiedene *Exits* lässt sich erreichen, dass RACF Sicherheitsprüfungen übergeht oder zusätzliche Sicherheitsprüfungen durchführt. Geänderte und eigene *Exits* sind zu dokumentieren. Dabei sind Funktion und Grund für den Einsatz anzugeben. Werden *Exits* eingesetzt, sind sie zu überwachen (siehe M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*).

**RACF-Kennungen**

*Begrenzung der Anmeldeversuche*

Eine in RACF angelegte Kennung erlaubt dem Anwender die Authentisierung gegenüber dem z/OS-System. Zum Schutz gegen Brute-Force-Attacken ist die Anzahl der Anmeldeversuche zu begrenzen, damit die Kennung automatisch gesperrt werden kann (maximal 3 bis 5 Versuche).

*Anlegen einer Kennung*

Für das Anlegen einer Kennung muss ein Verfahren existieren. Das Verfahren muss sicherstellen, dass nur Personen, die den Zugang zu dem jeweiligen System für ihre Arbeit benötigen, und deren Vertreter eine Kennung erhalten. Das Verfahren kann z. B. über ein Formblatt oder automatisiert ablaufen. In jedem Fall muss der Systemverantwortliche den Antrag genehmigen.

*Segmente einer Kennung*

Es sind nur die Segmente einer Kennung im RACF zu aktivieren, die der Anwender für seine Tätigkeit auch benötigt (z. B. *TSO*, *Netview*, *DCE* oder *OMVS*).

*Freischaltung einer Kennung*

Zum Freischalten einer gesperrten Kennung ist ein Verfahren einzuführen. Der Anwender muss sich gegenüber der freischaltenden Stelle, wie Call Center oder User Helpdesk, eindeutig identifizieren und seinen Anspruch nachweisen. Erst daraufhin darf die Kennung des Anwenders freigeschaltet werden.

*TSO-Segment Daten*

Die Daten aus dem TSO-Segment (*Time Sharing Option*), wie z. B. Name der Logon-Prozedur, Account-Nummer oder Speicherplatz, sollten durch RACF-Profile vor dem Überschreiben durch den Anwender geschützt werden. Dadurch kann der Anwender nur mit der vorgeschriebenen Umgebung arbeiten. Ausnahmefälle müssen begründet und dokumentiert werden.

*Sperren wegen Inaktivität*

Die Kennung eines Anwenders sollte aus Sicherheitsgründen nach einer bestimmten Zeitspanne der Inaktivität gesperrt werden, z. B. nach 90 Tagen. Von dieser Regelung auszunehmen sind Verfahrens-Kennungen, beispielsweise Notfall-Kennungen und STC-Kennungen. Es ist zu überlegen, nach einem noch längeren Zeitraum, z. B. 180 Tagen, die gesperrten Kennungen daraufhin zu überprüfen, ob sie gelöscht werden können. Wird ein solcher Löschvorgang durchgeführt, muss sichergestellt werden, dass die Ergebnisse des Löschvorgangs protokolliert werden und die RACF-Administration darüber informiert ist. Die Protokolle müssen gesichert abgespeichert werden und dienen der Nachvollziehbarkeit durch die RACF-Administration.

*Löschen einer Kennung*

Die Kennungen von Anwendern werden entweder auf Antrag gelöscht oder als Ergebnis von internen Überprüfungen. Beim Löschen einer Kennung muss darauf geachtet werden, dass neben der Kennung in RACF alle entsprechenden Zuordnungen und auch der ALIAS-Eintrag dieser Kennung im Masterkatalog gelöscht werden. Die Dateien dieser Kennung müssen entweder ebenfalls gelöscht oder einer anderen Kennung zugeordnet werden.

*Limitierung restriktiver Kennungen*

Kennungen mit hohen Rechten sollten nur dann vergeben werden, wenn die Mitarbeiter diese Berechtigungen tatsächlich für ihre Arbeit benötigen. Weitere Informationen hierzu finden sich in der Maßnahme M 2.289 *Einsatz restriktiver z/OS-Kennungen*.

*RACF-Gruppen und -Gruppenstruktur*

Berechtigungen sollten nicht direkt an eine Kennung vergeben werden. Anwender mit gleichen Aufgaben sollten in Gruppen zusammengefasst werden und über diese Gruppen die Berechtigungen erhalten. Eine Trennung der Gruppenstruktur ist zu empfehlen, z. B. nach dem folgenden Schema:

| **Trennung der Gruppenstruktur** | |
|---|---|
| Organisationsgruppen | Zuordnung der Kennungen zu Organisationseinheiten der Behörde bzw. des Unternehmens, beispielsweise ORGA |

| **Trennung der Gruppenstruktur** | |
|---|---|
| Funktionsgruppen | Über diese Gruppen erhalten die Anwender ihre Rechte anhand der Aufgaben (Funktion) im System, beispielsweise FUNKT. |
| Ressourcen-Gruppen | zur Verwaltung der Datei-Ressourcen. Für jedes angelegte Dateiprofil im RACF muss eine Gruppe oder eine Kennung existieren. Gruppen sind zu empfehlen, da diese nicht zum Einstieg in das System missbraucht werden können, z. B. RES. |

Tabelle: Trennung der Gruppenstruktur

Nachfolgend eine beispielhafte Darstellung der Gruppenstruktur:

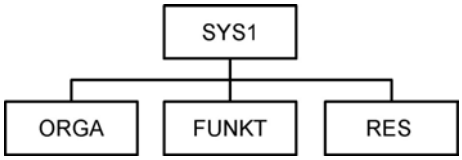



Abbildung: Prinzipaufbau der empfohlenen Gruppenstruktur im RACF

Der Name der Gruppe SYS1 ist fest vorgegeben. Sie ist immer die oberste Gruppe. In dieser Gruppe befindet sich nur der *IBMUSER*, der bei einer Neuinstallation benötigt wird. Zum Umgang mit dem *IBMUSER* siehe Maßnahme M 2.289 *Einsatz restriktiver z/OS-Kennungen*.

Die *Owner*-Struktur der Gruppen im RACF ist durchgängig anzulegen. In diesem Beispiel ist SYS1 der *Owner* der Gruppen ORGA, FUNKT und RES. Für weitere Untergruppen sollte als *Owner* der jeweilige Gruppenname der übergeordneten Gruppe gewählt werden. Der hierarchische Aufbau vereinfacht die Übersicht beim Einsatz der Berechtigungen *Group-Special*, *Group-Operations* und *Group-Auditor*.

**Schutz durch RACF-Definitionen**

*Schutz von Started Tasks*

*Started Tasks* sind mit einer Kennung im RACF mit dem Attribut *PROTECTED* anzulegen. Das Attribut *PROTECTED* verhindert dabei den Missbrauch der Kennung zum normalen Login. *Started Tasks* sind in der RACF-Klasse *STARTED* zu definieren und zu schützen. Weitere Informationen über *Started Tasks* finden sich in der Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*.

*Schutz von sicherheitskritischen Programmen*

Sicherheitskritische Programme sind mit der RACF-Klasse *PROGRAM* zu schützen. Der Zugang zu diesen Programmen ist nur Anwendern zu gewähren, die diese Programme für ihre Tätigkeit benötigen, sowie deren Vertretern. Weitere Informationen zum Umgang mit sicherheitskritischen Programmen sind in M 4.215 *Absicherung sicherheitskritischer z/OS-Dienstprogramme* zu finden.

*Schutz von Dateien*

Dateien werden im RACF über Dateiprofile geschützt. Dies betrifft sämtliche Systemdateien sowie alle Dateien der produktiven Anwendungen. Für den Schutz von Dateien sollten die folgenden Regeln beachtet werden:

- Dateien müssen generell über generische Dateiprofile im RACF geschützt werden. Diskrete Dateiprofile sind zu vermeiden.
- Kein Dateiprofil sollte mit *Universal Access* (UACC) größer *NONE* angelegt werden. Es sollte durch organisatorische oder technische Mechanismen verhindert werden, dass Anwender für die eigenen Dateiprofile den UACC-Wert verändern können.
- *General Resource*-Profile sollten nur dann mit UACC größer *NONE* angelegt werden, wenn dies unbedingt erforderlich ist. Dies sollte nachvollziehbar dokumentiert werden.
- In einem Produktions-System dürfen Dateiprofile und *General Resource*-Profile nicht im *Warning*-Modus laufen, da sonst kein echter Schutz der Ressourcen gewährleistet ist, denen diese Profile zugeordnet sind. Beim Einsatz des *Warning*-Modus auf einem Test-System ist darauf zu achten, dass die Performance des Systems nicht gravierend negativ beeinflusst wird (durch das Generieren von MVS-Nachrichten und SMF-Records).
- Um den Aufwand der RACF-Pflege zu begrenzen, sind Standards für die Erstellung und Benutzung von Dateinamen und RACF-*General Resources* notwendig (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Hochautorisierte Dateien, wie z. B. APF-, SVC-Dateien, *Parmlibs* und *Proclibs*, dürfen nur über voll qualifizierte generische Dateiprofile geschützt werden. Weitere Informationen zum Schutz dieser Dateien sind in M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* zu finden.
- Die RACF-Datenbank, die Backup-RACF-Datenbank und deren Sicherheitskopien sind mit UACC (*NONE*) zu schützen. Zugriffsrechte auf diese Dateien (selbst nur lesend) sind auf ein Minimum zu beschränken, um Brute-Force-Attacken auf die in der Datenbank gespeicherten Passwörter soweit wie möglich zu verhindern.

*HFS-Dateien*

Die HFS-Dateien (*Hierarchical File System*) des USS-Subsystems (*Unix System Services*) müssen im z/OS wie normale MVS-Datasets über RACF geschützt werden. Informationen zum Schutz der Files im USS sind in M 4.220 *Absicherung von Unix System Services bei z/OS-Systemen* enthalten.

**Mandantenfähigkeit unter z/OS**

In vielen Installationen ist es üblich, dass sich mehrere Kunden (Mandanten) ein z/OS-System teilen. Da sie somit auf dem gleichen System arbeiten, muss das z/OS-System mandantenfähig sein. Dies bedeutet unter anderem, dass ein Kunde nicht auf die Daten eines anderen Kunden zugreifen und somit auch nicht deren Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann.

Für die Mandantenfähigkeit sind folgende Hinweise zu beachten:

*Trennung durch RACF-Profile*

Die Daten und Anwendungen der Mandanten müssen durch RACF-Profile getrennt werden. Hierzu ist ein RACF-Konzept zur Mandantentrennung zu erstellen.

*Absicherung der Betriebssysteme*

Keiner der Mandanten darf ändernden Zugriff auf Dateien des z/OS-Betriebssystems haben. Solche Änderungen dürfen nur durch den Betreiber des z/OS-Systems erfolgen.

*Kennungen mit hohen Berechtigungen*

Hohe Berechtigungen im RACF (*SPECIAL, OPERATIONS, AUDITOR*) dürfen nur von Mitarbeitern des System-Betreibers verwendet werden. Es sollte überlegt werden, dem Kunden auf Wunsch die Berechtigungen *Group-Special*, *Group-Operations* und *Group-Auditor* zur Verfügung zu stellen. Hierzu muss ein Gruppenkonzept (*Owner*-Konzept) speziell für jeden Kunden erstellt werden.

*Einsatz von RACF-Security-Labels*

Es ist zu überlegen, *RACF-Security-Labels* für die Trennung der Kundenumgebungen zu verwenden, um die Mandantentrennung genauer durchsetzen zu können.

*Abstimmung Wartungsfenster*

Die Wartungsfenster, in denen das z/OS-System nicht zur Verfügung steht, sind mit allen Kunden, die auf dem betroffenen System arbeiten, abzustimmen.

Prüffragen:

- Ist das z/OS-Sicherheitssystem RACF hinsichtlich seiner Einstellungen und Parameter ausführlich geplant und konzipiert?
- Wurde das voreingestellte Passwort für das RVARY-Kommando im z/OS-System durch eines neues Passwort ersetzt?
- Werden geänderte und eigene RACF-Exits unter z/OS dokumentiert?
- Werden eingesetzte RACF-Exits unter z/OS überwacht?
- Ist bei den in RACF angelegten Kennungen zum Schutz gegen Brute-Force-Attacken die Anzahl der Anmeldeversuche bei der Authentisierung gegenüber dem z/OS-System begrenzt?
- Existiert ein Verfahrem zum Anlegen und Freischalten von Kennungen in RACF?
- Werden RACF-Kennungen im z/OS-System nach einer festgelegten Zeitspanne der Inaktivität gesperrt?
- Werden sicherheitskritische Programme des z/OS-Systems mit der RACF-Klasse PROGRAM geschützt?
- Sind hochautorisierte Dateien (z. B. APF-, SVC-Dateien, Parmlibs und Proclibs) über voll qualifizierte generische Dateiprofile geschützt?
- Werden die Daten und Anwendungen der Mandanten durch RACF-Profile im z/OS-System getrennt?
- Werden Wartungsfenster für das z/OS-System mit allen Kunden abgestimmt, die auf dem betreffenden System arbeiten?

# M 4.212 Absicherung von Linux für zSeries

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Auf zSeries-Systemen kann auch das Betriebssystem Linux eingesetzt werden. Zur Absicherung des Betriebssystems ist in diesem Fall zusätzlich der Baustein B 3.102 *Server unter Unix* bzw. Baustein B 3.204 *Client unter Unix* anzuwenden. Darüber hinaus sind im Folgenden einige zSeries-spezifische Besonderheiten beschrieben, die zu berücksichtigen sind.

**Betriebsarten von Linux unter zSeries**

Es sind drei unterschiedliche Methoden zum Betrieb von Linux unter zSeries möglich.

*Linux Native auf zSeries Hardware*

Das Linux-Betriebssystem wird als Single-System auf der zSeries-Hardware betrieben. Dies bedeutet, dass die gesamte zSeries-Hardware vom Linux-System benutzt wird.

*Linux in einer zSeries LPAR*

Bei dieser Variante erfolgt der Betrieb von Linux in einer *LPAR* (*Logical Partition*) auf der zSeries-Maschine. Der *LPAR*-Mode erlaubt den Betrieb von mehreren unabhängigen Betriebssystem-Installationen auf der gleichen zSeries-Hardware. Jede einzelne Partition verhält sich wie eine unabhängige Hardware. Auf diesen *LPARs* können unter anderem *z/OS* oder *Linux* als Betriebssystem installiert werden.

*Linux unter dem Träger-System z/VM*

Es können mehrere Linux-Installationen auf einem zSeries-Rechner oder innerhalb einer LPAR unter dem Träger-System z/VM betrieben werden. Das z/VM stellt sogenannte virtuelle Maschinen zur Verfügung, unter denen die einzelnen Linux-Installationen unabhängig von einander betrieben werden können.

**Absicherung der Terminals**

Die SE (*Support Elements*) und die HMC (*Hardware Management Console*) sind, wie in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals* empfohlen, zu sichern.

**Absicherung von Linux unter z/VM**

Für den Betrieb von Linux unter z/VM sollten zusätzlich folgende Empfehlungen berücksichtigt werden:

- Für z/VM müssen die aktuellen Patch-Stände eingehalten werden. Es ist darauf zu achten, nicht mit veralteten Systemen zu arbeiten.
- Die Berechtigungen des z/VM Systemadministrators sind sehr hoch. Er kann unter z/VM weitere virtuelle Maschinen einrichten oder löschen. Dies beinhaltet eine Vertrauensstellung, in der dem Administrator bewusst sein muss, dass er für die Sicherheit der Systeme mitverantwortlich ist.

- Nach der Installation von z/VM müssen das voreingestellte Login-Passwort und das voreingestellte *Minidisk*-Passwort sofort geändert werden.
- Unter z/VM definierte virtuelle Maschinen sollten nur die für die jeweiligen Aufgaben notwendigen Ressourcen erhalten, beispielsweise *Minidisks*, Adressen usw. Die Zugriffe werden über z/VM kontrolliert. Die strenge Trennung der virtuellen Maschinen muss eingehalten werden.
- Auch unter z/VM dürfen nur die benötigten Dienste gestartet werden. Nicht benötigte Dienste sind zu deaktivieren.
- Die Sicherheitsadministration von z/VM muss über *RACF für z/VM* erfolgen. *RACF für z/VM* dient als Security Manager und kann nur die Rechte der z/VM-Benutzer verwalten. Darüber hinaus sollten *Virtual Machines*, *Minidisks* und - falls gewünscht - auch Terminals über RACF *Resource Profile* geschützt werden. Zugriff auf diese Ressourcen dürfen nur diejenigen Anwender erhalten, die diese Rechte im Rahmen ihrer Tätigkeit benötigen. RACF kann jedoch nicht die Rechte der Linux-Benutzer und deren Zugriffe auf Systemressourcen innerhalb des Linux-Betriebssystems verwalten. Linux-Benutzer werden nach erfolgreichem Aktivieren des virtuellen Linux-Systems von den normalen Linux-Sicherheitsmechanismen kontrolliert. Sicherheitskritische System-Kommandos von z/VM (wie z. B. *CP DIAL*) sollten über RACF geschützt werden.
- Zur Verwaltung der Dateien und Verzeichnisse von z/VM ist zu überlegen, das Utility *DIRMAINT* einzusetzen. Es erlaubt eine übersichtliche Verwaltung der Anwenderverzeichnisse und hilft dadurch bei der Vermeidung von Administrationsfehlern. *DIRMAINTs* Sicherheitsmechanismen sollten immer auf *RACF für z/VM* basieren. Kommandos und Nachrichten im Rahmen der *DIRMAINT*-Administration sollten unter Audit-Kontrolle stehen.
- Die *Journaling*-Funktion von z/VM und die *Audit*-Funktionen von RACF sollten für Audits eingesetzt werden (siehe auch M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*).
- Es sollten die unter Unix bzw. Linux üblichen Standardmechanismen zur Absicherung von TCP/IP-Anbindungen eingesetzt werden. Darüber hinaus ist zu überlegen, ob zusätzlich die von Linux unterstützten *KERBEROS Authentication Services* oder *Secure SocketLayer* (SSL) eingesetzt werden sollen.
- Die Linux-Definitionen sollten so eingestellt sein, dass der Aufruf rekursiver Funktionen nicht zur Überlastung des Betriebssystems führen kann (siehe auch G 3.69 *Fehlerhafte Konfiguration der Unix System Services unter z/OS*).

**Linux-Authentisierung über z/OS RACF**

Es ist zu überlegen, die Authentisierung von Linux-Benutzern über ein zentrales z/OS RACF mittels LDAP (*Lightweight Directory Access Protocol*) und ein Linux PAM (*Pluggable Authentication Module*) durchzuführen. Dies kann besonders bei einer hohen Anzahl zu administrierender Linux-Systeme zu einer erheblichen Reduzierung des Verwaltungsaufwands für die Kennungen führen.

**Linux und Krypto-Hardware von zSeries-Maschinen**

zSeries-Systeme können mit optionalen kryptographischen Prozessor-Karten vom Typ PCICA (*Peripheral Component Interconnect Cryptographic Accelerator*) oder PCICC (*Peripheral Component Interconnect Cryptographic Coprocessor*) ausgestattet werden. Diese Karten dienen der Performance-Verbesserung von Krypto-Funktionen und zur sicheren Verwahrung von digitalen Schlüsseln. Beide Karten werden auch von Linux unterstützt. Da Linux das CCF (*Cryptographic Coprocessor Feature*) nicht unterstützt, sollte über-

legt werden, diese Krypto-Karten einzusetzen. Dies kann unter allen oben beschriebenen Installationsvarianten erfolgen. Unter z/VM können die Krypto-Karten von mehreren Linux-Systemen gleichzeitig und unabhängig von einander verwendet werden.

**Kommunikation von Linux unter zSeries-Hardware**

Die Kommunikation von Betriebssystemen, *z/OS* oder *Linux*, die entweder im *LPAR-Mode* oder unter *z/VM* auf derselben zSeries-Hardware installiert sind, sollte über interne Kanäle erfolgen, d. h. über *HiperSockets* oder virtuelle CTC-Verbindungen (*Channel-to-Channel*). Diese ermöglichen eine schnelle TCP/IP-Verbindung zwischen den Betriebssystem-Installationen. Im Vergleich mit der Kommunikation über das lokale Netz werden hierdurch die Fehler- und Angriffsmöglichkeiten reduziert, da die Informationen direkt innerhalb derselben Hardware von System zu System fließen.

Prüffragen:

- Wird z/VM auf zSeries-Systemen immer auf dem aktuellen Patch-Stand gehalten?
- Wurden nach der Installation von z/VM auf zSeries-Systemen das voreingestellte Login-Passwort und das Minidisk-Passwort durch neue Passwörter ersetzt?
- Sind unter z/VM auf zSeries-Systemen alle nicht benötigten Dienste deaktiviert?
- Werden die Journaling-Funktion von z/VM und die Audit-Funktionen von RACF auf zSeries-Systemen für Audits eingesetzt?
- Erfolgt die Kommunikation von Betriebssystemen (z/OSoder Linux), die im LPAR-Mode oder unter z/VM auf derselben zSeries-Hardware installiert sind, über interne Kanäle?

# M 4.213 Absichern des Login-Vorgangs unter z/OS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Zugang zu z/OS-Systemen - insbesondere der Login-Vorgang - muss geschützt werden. Hierzu sind folgende Empfehlungen zu beachten:

- Alle nicht für den Zugang benötigten Dienste und Ports sollten gesperrt sein. Es sollte überlegt werden, den Zugriff auf die benötigten Dienste und Ports durch RACF-Profile auf die autorisierten Zugriffsmöglichkeiten zu beschränken.
- Der Umgang mit Passwörtern sollte wie in Maßnahme M 2.11 *Regelung des Passwortgebrauchs* beschrieben erfolgen. Beim Zugang aus öffentlichen Netzen (Internet) zu z/OS-Systemen muss verhindert werden, dass alle Kennungen durch Falscheingabe von Passwörtern gesperrt werden. Dies kann zur Zeit nur durch den Einsatz von digitalen Zertifikaten gelöst werden. Es ist zu überlegen, ob die Automation des *RACF Reply* bei Kennungen mit dem Attribut *SPECIAL* aus Sicherheitsgründen unterbleiben sollte. Dies verhindert, dass alle Kennungen mit *SPECIAL* Attribut automatisch gesperrt werden können.
- Die Datei *SYS1.UADS* dient dazu, dass beim Ausfall des RACF noch eine Möglichkeit zum Systemzugang besteht. In diese Datei darf nur der *IBMUSER* oder ein (oder mehrere) *Notuser* eingetragen sein.

Darüber hinaus gelten die in M 4.15 *Gesichertes Login* beschriebenen Empfehlungen.

Prüffragen:

- Wird der Zugang zu z/OS-Systemen insbesondere der Login-Vorgang geschützt?
- Sind alle nicht für den Zugang benötigten Dienste und Ports im z/OS-System gesperrt?

# M 4.214 Datenträgerverwaltung unter z/OS-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um den Schutz von Festplatten und Bändern in z/OS-Systemen gewährleisten zu können, sind die nachfolgenden Empfehlungen zu berücksichtigen.

**Festplatten**

- Die Festplatten sind über entsprechende RACF-Profile (*Resource Access Control Facility*) und RACF-Klassen zu schützen. Es ist im RACF ein Profil für den Schutz des VTOC (*Volume Table of Content*) der Festplatte anzulegen. Das Arbeiten mit generischen Profilen - z. B. VTOC.** - ist möglich und zu überlegen.
- Der *Master-Katalog* ist durch ein RACF-Profil zu schützen, Mitarbeiter sind mit *READ* zu autorisieren. Ein schreibender Zugriff ist nur den Mitarbeitern zu erlauben, die dies im Rahmen ihrer Tätigkeit wirklich benötigen (z. B. beim Anlegen eines *ALIAS*).
- Zur Verwaltung und Erhaltung der Übersicht über die Festplatten in den Festplattenschränken ist ein Plattenbelegungsplan notwendig. Dieser Plattenbelegungsplan muss mindestens folgende Informationen enthalten:

  - Adresse der Festplatte,
  - Name der Festplatte,
  - Name des SMS-Festplatten-Pools, zu dem die Festplatte gehört (wenn SMS) und
  - Name des Plattenschranks, in dem die Festplatte generiert wurde.

  Dies ist schriftlich zu dokumentieren.
- Die Programme zum Verwalten der Festplatten (z. B. Initialisieren, Umkopieren von Daten u. a.) müssen geschützt werden. Die Programme dürfen nur von Mitarbeitern ausführbar sein, die diese Berechtigung für ihre Tätigkeit benötigen. Die Benutzung des Attributs *OPERATIONS* durch Programme sollte vermieden werden, weitere Informationen über dieses Attribut sind in M 2.289 *Einsatz restriktiver z/OS-Kennungen* zu finden, wenn es doch benötigt wird.
- Die Administrationsfunktion des ISMF (*Interactive Storage Management Facility*) muss über RACF-Profile geschützt sein. Nur berechtigte Anwender dürfen diese Funktionalitäten nutzen.
- z/OS-Befehle, mit denen Festplatten und Bänder in das System eingefügt, bzw. aus dem System herausgelöst werden können, sind über entsprechende RACF-Profile zu schützen. Sie dürfen nur von berechtigten Anwendern ausgeführt werden (siehe auch M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*).
- Die ACS-Routinen (*Automatic Class Selection*) des SMS (*System Managed Storage*) müssen geschützt sein und dürfen nur von berechtigten Anwendern angepasst werden. Es sollten Sicherungskopien der ACS-Dateien zur Verfügung stehen, die in einer Notfall-Situation zurückgespielt werden können.

**Magnetbänder**

- Der Schutz von Magnetbändern muss über entsprechende RACF-Profile und RACF-Klassen gewährleistet werden.

- Beim Einsatz von Verwaltungsprogrammen für Magnetbänder sind die Besonderheiten dieser Programme beim Schutz von Magnetbändern zu beachten (z. B. Einsatz von *TAPEVOL* und *TAPEDSN* Klasse).
- Durch entsprechende Vorkehrungen und Regelungen muss gewährleistet werden, dass genügend Bandstationen zur Verfügung stehen und diese nicht unnötig lange durch Belegung blockiert werden.
- Um den Schutz der Daten auf Magnetbändern zu gewährleisten, muss die Funktion *Bypass Label Processing* bei z/OS-Systemen gesperrt werden. Hierzu ist in der *General Ressource* Klasse *FACILITY* ein Profil mit dem Namen *ICHBLP* einzutragen. Dieses Profil ist mit *UACC=NONE* zu schützen. Zugang zu dieser Funktion darf nur in begründeten Ausnahmefällen temporär gewährt werden.

**HSM (Hierarchical Storage Manager)**

- Die Konfiguration des HSM erfolgt in einem Member (*ARCCMDxx*). Hier müssen auch die Kennungen der Administratoren für den HSM eingetragen sein. Die Datei, die dieses Member enthält, muss durch ein entsprechendes RACF-Profil geschützt werden, so dass nur die zuständigen Mitarbeiter Zugriff haben.
- Die Dateien, die auf Migrationsstufe 2 sind, befinden sich auf Magnetbändern. Diese Bänder müssen geschützt werden und dürfen nur von HSM bearbeitet werden.
- Es ist zu überlegen, wann die Backup-Sicherungen durch den HSM ausgeführt werden, um Behinderungen der Produktion durch *ENQUEUES* und *RESERVES* zu vermeiden. Ferner ist festzulegen, welche Platten gesichert werden sollen und wie die Plattensicherung erfolgen soll (*Full Volume* oder *Incremental* Speicherung).

Prüffragen:

- Werden die Festplatten und Magnetbänder des z/OS-Systems über entsprechende RACF-Profile und RACF-Klassen geschützt?
- Ist der Master-Katalog des z/OS-Systems durch ein RACF-Profil geschützt?
- Existiert ein Plattenbelegungsplan für das z/OS-System?
- Sind Befehle bzw. Programme zum Verwalten von Festplatten und Bändern des z/OS-Systems geschützt, so dass die Programme nur von Mitarbeitern ausführbar sind, die diese Berechtigung für ihre Tätigkeit benötigen?
- Sind im z/OS-System die Administrationsfunktionen des ISMF über RACF-Profile geschützt, so dass nur berechtigte Anwender diese Funktionalität nutzen können?
- Sind die ACS-Routinen des SMS im z/OS-System so geschützt, dass nur berechtigte Anwender diese anpassen können?
- Existierten Sicherungskopien der ACS-Dateien im z/OS-System?
- Ist die Datei, die das Member zur Konfiguration des HSM unter z/OS enthält, durch ein entsprechendes RACF-Profil geschützt, so dass nur zuständige Mitarbeiter Zugriff haben?

# M 4.215 Absicherung sicherheitskritischer z/OS-Dienstprogramme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In z/OS-Systemen stehen den Systemprogrammierern, RACF-Administratoren und Storage-Managern Dienstprogramme zur Verfügung, über die bei entsprechender Autorisierung tiefgreifende Änderungen am z/OS-System durchgeführt werden können. Für eine sichere Benutzung dieser Programme müssen folgende Empfehlungen berücksichtigt werden:

### Absichern sicherheitskritischer Programme

Sicherheitskritische Dienstprogramme müssen über das RACF-Sicherheitssystem (*Resource Access Control Facility*) entsprechend geschützt werden. Sie dürfen nur von den dafür vorgesehenen Mitarbeitern benutzt werden können. Ebenso sind die *Alias*-Namen der Programme zu schützen.

Nachfolgend eine Auswahl sicherheitskritischer Dienstprogramme:

- AMASZAP, AMASPZAP, IMASZAP
- ADRDSSU
- SYSIEH
- SMFDUMP
- ICKDSF
- IEHATLAS
- IEHINITT
- PGTFPF00
- IRRDBU00
- ICHDSM00
- IRRUT100, IRRUT200, IRRUT300, IRRUT400
- RESOLVE

### Schutz von kritischen TSO-Kommandos

TSO-Kommandos (*Time Sharing Option*), hinter denen sich sicherheitskritische Programme verbergen, müssen über das Member *TSOKEY00* (in der z/OS *Parmlib*) entsprechend gesichert werden, damit nur autorisierte Mitarbeiter diese Kommandos benutzen können.

### Unerlaubtes Installieren sicherheitskritischer Programme

Es muss sichergestellt werden, dass Fremdprogramme nicht unerlaubt installiert werden können. So sind im Internet einige Programme erhältlich, die sehr tief in das z/OS-System eingreifen können. Auch haben viele Systemprogrammierer selbstgeschriebene Programme, die ihre Arbeit erleichtern, aber u. U. sehr tiefgreifende Änderungen am z/OS-System vornehmen können. Ein unkontrolliertes Installieren und Ausführen dieser Programme muss durch entsprechende Schutzvorkehrungen unterbunden werden (siehe hierzu Maßnahmen M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* und M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Werden solche Programme dennoch benötigt, so dürfen sie nur über den offiziellen Installationsprozess in das System eingebracht werden.

Prüffragen:

- Sind sicherheitskritische z/OS-Dienstprogramme über das RACF-Sicherheitssystem so geschützt, dass diese nur von den dafür vorgesehenen Mitarbeitern benutzt werden können?
- Sind TSO-Kommandos, hinter denen sich sicherheitskritische z/OS-Programme verbergen, über das Member TSOKEY00 gesichert, sodass nur autorisierte Mitarbeiter diese Kommandos benutzen können?
- Wird im z/OS-System sichergestellt, dass Fremdprogramme nicht unerlaubt installiert werden können?

# M 4.216 Festlegung der Systemgrenzen von z/OS

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für den Betrieb eines z/OS-Systems ist es wichtig, die Systemgrenzen für die maximale Belastung der Ressourcen festzulegen. Folgende Hinweise sind zu beachten:

### Kommunikation der Systemgrenzen

Die Systemgrenzen, deren Planung in Maßnahme M 2.286 *Planung und Einsatz von zSeries-Systemen* beschrieben wird, müssen den betroffenen Administratoren und Anwendungseignern bekannt sein. Zu den Systemgrenzen zählen Angaben wie die maximale Größe einer Datei, der maximal zur Verfügung stehende Hauptspeicher, die maximale Größe von Dateien für FTP-Übertragungen (*File Transfer Program*), die Anzahl von LPARs (*Logical Partitions* auf einem zSeries-Mainframe), die Anzahl von Systemen in einem *Parallel-Sysplex-Cluster* und ähnliche Festlegungen. Systemgrenzen müssen bekannt sein und berücksichtigt werden, um Fehler beim Ablauf von Anwendungen zu vermeiden.

### Magnetband-Stationen

Die Anzahl der zur Verfügung stehenden Magnetband-Stationen sollte mit den Anforderungen der betroffenen Anwendungseigner abgestimmt sein. Damit nicht zu viele gleichzeitige Belegungen von Magnetband-Stationen erfolgen, müssen die Zeiten, an denen Anwendungen auf Magnetband-Stationen zugreifen, unter den betroffenen Anwendungsentwicklern und -verantwortlichen abgestimmt sein.

### Festplatten

Die benötigte Kapazität an Festplatten muss von den Anwendungseignern geplant und festgelegt sein. Das *Space-Management* muss darauf achten, dass der Speicherplatz auf den Festplatten ausreicht. Ist dies nicht der Fall, so ist der jeweilige Anwendungseigner zu informieren (zu *Space Management* siehe M 2.295 *Systemverwaltung von z/OS-Systemen*).

### Initiators

Die *Initiators*, die im JES2 (*Job Entry Subsystem*) aktiviert sind, steuern die parallele Verarbeitung von Batch-Jobs. Ihre Anzahl muss an die Hardware-Voraussetzungen angepasst sein. Die Zahl und die damit verbundenen Restriktionen müssen den Anwendungseignern bekannt sein.

### TSO-Anwender und Adressräume

Die maximale Anzahl der TSO-Anwender und die maximale Anzahl der zu startenden Adressräume müssen an die Hardware-Voraussetzungen angepasst sein.

### Einsparungspotential

Es ist zu überlegen, ob System-Ressourcen eingespart werden können, wenn nach einer Zeit der Inaktivität eines Anwenders (z. B. 30 Minuten) dieser Anwender automatisch durch das System abgemeldet wird. Dabei ist zu prüfen,

ob dies zu Problemen mit den betriebenen Applikationen führt. Die Anwender sind über eine entsprechende Regelung zu informieren.

Prüffragen:

- Sind die Systemgrenzen von z/OS für die maximale Belastung der Ressourcen festgelegt?
- Sind den Administratoren und Anwendungseignern die Systemgrenzen des z/OS-Systems bekannt?
- Ist die Anzahl der im z/OS-System zur Verfügung stehenden Magnetband-Stationen mit den Anforderungen der betroffenen Anwendungseignern abgestimmt?
- Ist die benötigte Kapazität an Festplatten mit den Anwendungseignern des z/OS-Systems geplant und festgelegt?

# M 4.217 Workload Management für z/OS-Systeme

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Die Verwaltung der Ressourcen in einem *Parallel Sysplex Cluster* (aberauch in einem Einzelsystem) erfolgt durch die Komponente WLM (*Work Load Manager*) des z/OS-Betriebssystems. Für die Sicherheit des WLM-Einsatzes sind die folgenden Hinweise zu beachten:

### Schutz der *Couple-Datasets*

Die für WLM notwendigen *Couple-Datasets* sind durch entsprechende RACF-Profile (*Resource Access Control Facility*) zu schützen. Für die WLM-Arbeitsdateien - ein oder mehrere PDS-Dateien (*Partitioned Datasets*) - gelten die gleichen Regeln. Das Dienstprogramm zum Anlegen der Dateien ist über das RACF *Facility*-Profil *MVSADMIN.WLM.POLICY* zu schützen.

### Schutz des Modify-Kommandos

Es ist möglich, WLM-Optionen dynamisch durch ein *Modify*-Kommando zu verändern. Dieses Kommando darf nur autorisierten Mitarbeitern, wie entsprechend geschulten Operatoren oder Systemprogrammierern, zur Verfügung stehen.

### Schutz des Reset-Kommandos

Das *Reset*-Kommando muss so geschützt werden, dass nur autorisierte Mitarbeiter WLM-Regeln für laufende Jobs ändern können.

### Schutz der WLM-Applikation

Die WLM-Definitionen werden durch einen ISPF-basierenden WLM-Dialog gepflegt (*Interactive System Productivity Facility*). Der Zugang zu der WLM-Applikation sollte über das RACF *Facility*-Profil *MVSADMIN.WLM.POLICY* geschützt werden und nur autorisierten Mitarbeitern zur Verfügung stehen (Service- und Kapazitäts-Management).

### Übereinstimmende Autorisierung

Definierte WLM-Vorgaben (z. B. die *Service Class*) können sowohl über MVS-Kommandos als auch über die SDSF-Schnittstelle (*System Display and Search Facility*) geändert werden. Es muss sichergestellt werden, dass die Berechtigungen zum Ändern des WLM über MVS-Kommandos und über das SDSF gleich sind.

Prüffragen:

- Sind die für WLM von z/OS-Systemen notwendigen Couple-Datasets durch entsprechende RACF-Profile geschützt?
- Steht das Modify-Kommando, das WLM-Optionen unter z/OS dynamisch verändern kann, nur den hierzu autorisierten Mitarbeitern zur Verfügung?
- Ist das Reset-Kommando so geschützt, dass nur autorisierte Mitarbeiter WLM-Regeln für laufende Jobs des z/OS-Systems ändern können?
- Ist der Zugang zu der WLM-Applikation des z/OS-Systems über das RACF Facility-Profil MVSADMIN.WLM.POLICY geschützt?

- Steht die WLM-Applikation des z/OS-Systems nur autorisierten Mitarbeitern zur Verfügung?
- Sind die Berechtigungen zum Ändern des z/OS-WLM über MVS-Kommandos und über das SDSF gleich?

# M 4.218 Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Anwendungsentwickler

Das z/OS-System arbeitet in der Regel mit dem EBCDIC-Zeichensatz (*Extended Binary Coded Decimal Interchange Code*). Dies gilt sowohl für die MVS-Dateien (*Multiple Virtual Storage*), als auch für die HFS-Dateien (*Hierarchical File System*). Ausnahmen sind lediglich im zFS-Filesystem möglich. Windows- und Unix-Systeme arbeiten meist mit dem ASCII-Zeichensatz (*American Standard Code for Information Interchange*). Bei der Kommunikation zwischen den unterschiedlichen Systemen müssen folgende Regeln beachtet werden:

- Sollen Textdateien übertragen werden, müssen Umsetzungs-Tabellen eingesetzt werden, die eine Zeichensatz-Konvertierung durchführen. Diese Tabellen werden im z/OS-Betriebssystem mitgeliefert. Es ist jedoch darauf zu achten, dass die richtige Tabelle verwendet wird.
- Bei der Übertragung von Binärdaten muss sichergestellt werden, dass die Konvertierung ausgeschaltet ist, da sonst die Daten nachher unbrauchbar sind.
- Beim Daten-Transfer von Unix- oder Windows-Systemen in ein HFS (*Hierarchical File System*) des z/OS-Systems - und umgekehrt - über FTP (*File Transfer Protocol*) muss darauf geachtet werden, dass die richtige Konvertierungs-Option beim Transfer aktiviert ist.
- Es ist besonders beim Übertragen von Programm-Quellcode zu überprüfen, dass wirklich alle Zeichen (und hier speziell einige Sonderzeichen) richtig übersetzt werden, damit nicht unbemerkte Programmfehler durch die Konvertierung entstehen. Beispielsweise führen falsche Zeichen in Konstantendefinitionen in einigen Fällen nicht zu einem Compiler-Fehler, sondern machen sich erst bei der Ausführung eventuell sehr viel später bemerkbar.

Prüffragen:

- Wird bei der Übertragung von Textdateien zwischen z/OS-Systemen und anderen Systemen darauf geachtet, dass die eventuell erforderliche Zeichensatz-Konvertierung durchgeführt wird?
- Falls beim Datenaustausch mit z/OS-Systemen eine Zeichensatz-Konvertierung erforderlich ist: Wird die jeweils korrekte Umsetzungstabelle verwendet?
- Ist bei der Übertragung von Binärdaten zwischen z/OS-Systemen und anderen Systemen sichergestellt, dass die Zeichensatz-Konvertierung ausgeschaltet ist?
- Wird beim Daten-Transfer zwischen z/OS-Systemen und anderen Systemen über FTP darauf geachtet, dass die jeweils richtige Konvertierungsoption beim Transfer aktiviert ist?
- Wird bei der Übertragung von Programm-Quellcode zwischen z/OS-Systemen und anderen Systemen überprüft, dass alle Zeichen richtig übersetzt werden?

# M 4.219 Lizenzschlüssel-Management für z/OS-Software

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Verantwortliche der einzelnen Anwendungen

Einige Software-Hersteller benutzen sogenannte *Activation-Keys* (Lizenzschlüssel), um die Nutzung ihrer Programme zu steuern. Diese Lizenzschlüssel laufen oft nach bestimmten Zeiten ab und müssen durch den Systembetreiber erneuert werden. Die folgenden Hinweise sind hierbei zu berücksichtigen:

**Erneuerung von Lizenzschlüsseln**

Es ist ein Verfahren einzurichten, so dass Lizenzschlüssel rechtzeitig erneuert werden. Andernfalls besteht die Gefahr, dass Software-Funktionen durch abgelaufene Lizenzschlüssel plötzlich nicht mehr zur Verfügung stehen.

Die Laufzeiten der Lizenzschlüssel sind zu dokumentieren. Die Dokumentation muss allen betroffenen Administratoren zur Verfügung stehen.

Es ist zu überlegen, ob die Gültigkeit der Lizenzschlüssel regelmäßig kontrolliert werden sollte.

**Warnung vor Ablauf der Lizenz**

Sollte Software im Einsatz sein, die ohne Warnung nach Ablauf des Lizenzschlüssels die Funktion einstellt, sollte mit dem Hersteller verhandelt werden, um eine Verbesserung der Situation zu erreichen. Die Software sollte z. B. rechtzeitig vor dem Ablaufen des Lizenzschlüssels warnen oder den Einsatz von Notschlüsseln erlauben.

Prüffragen:

- Ist für die z/OS-Software ein Verfahren eingerichtet, um die Lizenzschlüssel rechtzeitig zu erneuern?
- Sind die Laufzeiten der Lizenzschlüssel für die z/OS-Software dokumentiert?
- Wird vor dem Ablauf einer Lizenz von der z/OS-Software eine Warnung ausgegeben?

# M 4.220 Absicherung von Unix System Services bei z/OS-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

*Unix System Services* (USS) ist ein *Posix*-kompatibles Subsystem, das unter dem z/OS-Betriebssystem läuft. Für den generellen Schutz der *Unix System Services* müssen die im Baustein B 3.102 *Server unter Unix* beschriebenen Maßnahmen umgesetzt werden. Weiterhin müssen einige zusätzliche Sicherheitsaspekte berücksichtigt werden:

**Doppelte UID-Vergabe**

Es muss sichergestellt werden, dass UIDs nicht doppelt vergeben werden, da sonst keine genaue Zuordnung zur MVS-User-ID möglich ist.

**HFS-Dateien**

HFS-Dateien (*Hierarchical File System*), die das Unix-Dateisystem beinhalten, sind über RACF-Datei-Profile zu schützen. Auf diese RACF-Profile sollte nur die *Unix Started Task* Zugriff erhalten. Ein Backup der HFS-Dateien sollte über HSM-Funktionen (*Hierarchical Storage Manager*) erfolgen. HFS-Dateien sollten jedoch nicht durch HSM migriert werden. Diese Empfehlungen gelten ebenfalls für zFS-Dateien.

Das *ROOT*-Dateisystem sollte mit der Option *READ-ONLY* gemounted sein.

Es ist zu überlegen, HFS-Dateien von Anwendern über die RACF-Profile der Kennung des jeweiligen Anwenders zu schützen. Um zu verhindern, dass jeder Anwender mit eigener HFS-Datei die Befehle *mount* und *umount* ausführen muss, sollte überlegt werden, die *Automount*-Funktion einzusetzen.

**Member BPXPRMxx**

Die wesentlichen USS-Parameter werden in der *Parmlib* im Member *BPXPRMxx* definiert. Einige Parameter beschreiben die zur Verfügung stehenden Ressourcen (z. B. *MAXPROCSYS* oder *MAXPROCUSER*). Diese Parameter müssen entsprechend der Leistungsfähigkeit der zSeries-Hardware bzw. LPAR eingestellt werden, um eine Überlastung des Systems zu verhindern.

Es sollten symbolische Variablen zur Definition dieses Members verwendet werden.

**APF-Autorisierung**

Es sollte im USS-Dateisystem keine APF-Autorisierung (*Authorized Program Facility*) über das *File Security Packet* (FSP) geben. Statt dessen sollten die Module von APF-Dateien des z/OS-Betriebssystems geladen werden.

**Superuser UID(0) und UNIXPRIV**

Viele System-Kommandos, für deren Nutzung unter anderen Unix-Systemen die Berechtigung *Superuser* (UID 0) nötig ist, können bei USS über die RACF-Profile in der RACF-Klasse *UNIXPRIV* geschützt werden. Dies bedeutet, dass die Rechte der Administration durch RACF verwaltet werden können und so die *Superuser*-Berechtigung nur in sehr wenigen Ausnahmefällen vergeben

werden muss. Die Empfehlungen zum Umgang mit *Superuser*-Rechten sind in M 2.289 *Einsatz restriktiver z/OS-Kennungen* aufgeführt.

**RACF-Profile BPX.xxx der Klasse FACILITY**

Zur Absicherung vieler USS-Funktionen sollten zusätzlich zu den Profilen in der Klasse *UNIXPRIV* die RACF-Profile *BPX.xxx* der Klasse *FACILITY* eingesetzt werden. Dadurch können in vielen Fällen höhere Autorisierungen vermieden werden (z. B. UID 0).

**Audit und Monitoring**

Für das Audit und Monitoring der USS sollten die gleichen Mechanismen wie für z/OS genutzt werden. Die Vorgänge im USS schreiben SMF-Sätze. Zugriffsverletzungen werden in RACF-Nachrichten übersetzt und erzeugen Meldungen im *Syslog*. Beide Quellen sollten, wie in Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS* beschrieben, ausgewertet werden. Einige Unix-Tasks, wie z. B. der mitgelieferte Webserver, schreiben Protokoll-Informationen in eigene Dateien. Diese sollten ebenfalls ausgewertet werden, falls die entsprechenden Programme aktiviert sind.

**Zeichensatzkonvertierung**

Es sollten die Empfehlungen in M 4.218 *Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen* beim Einsatz des USS-Subsystems beachtet werden.

Prüffragen:

- Ist sichergestellt, dass die UIDs unter USS im z/OS-System nicht doppelt vergeben werden?
- Sind zFS- und HFS-Dateien, die das Unix-Dateisystem beinhalten, unter z/OS über RACF-Datei-Profile geschützt?
- Wird das Root-Dateisystem für USS des z/OS-Systems mit der Option READ-ONLY gemounted?
- Ist sichergestellt, dass es im USS-Dateisystem des z/OS-Systems keine APF-Autorisierung über das File Security Packet gibt?
- Werden für das Audit und Monitoring der USS die gleichen Mechanismen wie für z/OS genutzt?

# M 4.221 Parallel-Sysplex unter z/OS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Ein *Parallel-Sysplex-Cluster* ist ein Systemverbund aus mehreren z/OS-Systemen, die nach außen hin als ein System erscheinen. Dabei können die z/OS-Systeme auf einer oder auch auf mehreren LPARs (*Logical Partitions*) laufen. Zur Synchronisierung sind alle Systeme dieses Verbunds über eine *Coupling Facility* verbunden. Bei der Benutzung mehrerer LPARs muss zur Synchronisierung der System-Zeit (*Clock*) ein sogenanntes *Timer Facility* eingesetzt werden. Weitere Informationen hierzu finden sich in M 3.39 *Einführung in die zSeries-Plattform*. *Parallel-Sysplex-Cluster* kommen zum Einsatz, wenn hohe Anforderungen an die Verfügbarkeit und Skalierbarkeit bestehen.

Alle z/OS-Systeme eines *Parallel-Sysplex-Clusters* werden vom gleichen Festplattensatz geladen. Die einzelnen z/OS-Betriebssysteme werden über individuelle Systemdefinitionen unterschieden.

Beim Einsatz von *Parallel-Sysplex-Clustern* sollten folgende Empfehlungen beachtet werden:

**Einsatz der Coupling Facility**

Die *Coupling Facility* (CF) verbindet die LPARs untereinander. Sie stellt auch einen gemeinsam nutzbaren Speicher zur Verfügung, der in verschiedene Objekte, sogenannte *Coupling Facility Structures*, aufgeteilt ist. Der Zugriff auf die CF erfolgt über XES (*Cross-System Extended Services*). Es gibt drei verschiedene Speichertypen, die in der CF definiert werden können:

*Cache Structures*

Diese Struktur stellt hochperformanten Speicher für die gemeinsame Nutzung durch mehrere Anwender zur Verfügung. Werden Daten von der Festplatte gelesen, wird eine Kopie in den eigenen lokalen Speicherpuffer geschrieben. Darüber hinaus kann optional eine weitere Kopie in die *Cache Structure* der *Coupling Facility* gestellt werden.

*List Structures*

Diese Struktur erlaubt es mehreren Anwendern, Informationen miteinander zu teilen, die in Listen (*Message passing*) oder Warteschlangen (*Queues of work*) verfügbar sind.

*Lock Structures*

Diese Struktur kann verwendet werden, um die Benutzung von Ressourcen im *Shared*- oder *Exclusive*-Modus über alle LPARs zu steuern.

*Einsatz*

Wird der Betrieb eines *Parallel-Sysplex-Clusters* erwogen, z. B. aus Verfügbarkeitsgründen, sollte die *Coupling Facility* möglichst mit *Data Sharing* eingesetzt werden. Dies gilt zumindest für JES2/3 (*Job Entry Subsystem*), RACF (*Resource Access Control Facility*), VTAM (*Virtual Telecommunication Access Method*), *System Logger*, CICS, IMS und DB2. Es sollte geprüft werden, ob eine redundante Auslegung der *Coupling Facility* erforderlich ist, um den Anforderungen an die Verfügbarkeit des Gesamtsystems Rechnung zu tragen.

*Coupling Facilities* werden über die HMC (*Host Management Console*) definiert und initialisiert. Empfehlungen zum Einsatz dieser Konsole finden sich in M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*.

**Couple Datasets**

Die *Couple Datasets* werden von XCF (*Cross-System Coupling Facility*) benutzt, um Informationen über die LPARs, Gruppen oder Member zu kontrollieren. Alle LPARs des *Parallel-Sysplex*-Verbundes müssen auf diese Datasets zugreifen können. Der Einsatz von *Alternate CoupleDatasets* ist zu empfehlen. Unter z/OS müssen die *Couple Datasets* über RACF geschützt werden. Es sollten nur die Mitarbeiter verändernden Zugriff darauf erhalten, die im Rahmen ihrer Tätigkeit die Dateien bearbeiten, sowie deren Vertreter (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

Zum Formatieren der *Couple Datasets* steht das Utility *IXCL1DSU* zur Verfügung. Dieses Programm sollte über RACF geschützt werden (Class *PROGRAM*). Das administrative Utility *XCMIAPU* erlaubt die Definition der *CFRM-Policy* (*Coupling Facility Resource Management*). Es sollte über ein entsprechendes *Facility*-Profil im RACF geschützt werden, so dass nur autorisiertes Personal Zugriff darauf hat. Weitere Empfehlungen zum Schutz kritischer Programme finden sich in M 4.215 *Absicherung sicherheitskritischer z/OS-Dienstprogramme*.

**Sysplex-Kommandos**

Zur Administration und Kontrolle stellt das z/OS-Betriebssystem das System-Kommando *SETXCF* zur Verfügung. Es unterstützt unter anderem die folgenden Aktivitäten:

- Definieren der *Couple Datasets*
- Umschalten zwischen *Primary*- und *Backup-Couple Dataset*
- Aktivieren einer neuen *CFRM-Policy*
- Start der *PATHIN*- oder *PATHOUT*-Verbindung
- Ändern der Struktur-Größe (*Structure Size*)
- *Rebuild* der Struktur nach Struktur-Fehlern

Zum Schutz dieses Kommandos (und aller anderen den *Parallel-Sysplex-Cluster* unterstützenden Kommandos) müssen entsprechende RACF-Profile definiert werden (siehe M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*).

**XCF Kontrolle**

RMF (*Resource Measurement Facility*) erzeugt einen sogenannten *XCF Activity Report*. Es ist zu überlegen, diesen Report zur Überwachung des Nachrichtenverkehrs zwischen den z/OS-Betriebssystemen einzusetzen, um Kommunikationsengpässe und *Deadlock*-Situationen rechtzeitig erkennen und präventive Maßnahmen ergreifen zu können.

**Einheitliche RACF-Datenbank**

Für alle LPARs des gesamten *Parallel-Sysplex-Clusters* sollte eine RACF-Datenbank mit einheitlichen RACF-Definitionen verwendet werden.

**Standards**

Um die Übersichtlichkeit und Wartbarkeit zu verbessern, sollten in folgenden Bereichen Standards eingeführt werden:

- Die Parameter-Member der *PARMLIBs* sollten standardisiert werden. Alle Namen müssen im *Parallel-Sysplex*-Verbund eindeutig sein. Hierzu gehören: Dataset-Namen, Subsystem-Namen, Prozedur-Namen, VTAM *Application IDs* (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Sämtliche Systemeinstellungen der lokalen Definitionen in *PARMLIB* und *PROCLIB* sollten einheitlich sein. Es ist empfehlenswert, dass der strukturelle Aufbau der einzelnen Definitions-Member identisch ist.
- Die SMS-Struktur (*System Managed Storage*) muss im gesamten *Parallel-Sysplex*-Verbund einheitlich sein.
- Auf allen LPARs sollte eine möglichst einheitliche System-Software eingesetzt werden (eventuell ist hierdurch eine Anpassung der Software-Lizenzen notwendig).

**Dimensionierung**

Es muss auf die richtige Dimensionierung der Caches der Festplatten-Steuereinheiten, der Work-Platten, der Strukturen in der *Coupling Facility* und der *SPOOL*-Platten geachtet werden. Die Größe der Bereiche ergibt sich in erster Linie aus der Art und den Anforderungen der Anwendungen, die auf dem *Parallel-Sysplex*-Verbund laufen. In vielen Fällen enthalten auch die Dokumentationen der Software-Hersteller Hinweise hierzu.

**Serialisierung**

Es muss ein GRS-Verbund (*Global Resource Serialization*) eingerichtet werden, um die System-Aktionen serialisieren zu können. Der GRS-Modus muss im Member *IEASYSnn* der *PARMLIB* definiert sein (*RING*- oder *STAR*-Modus). Es sollte, wenn möglich, der modernere *STAR*-Modus gewählt werden, da diese Topologie durch die auf den *Couple Datasets* gespeicherten *Resource Name Lists* (RNLs) meist eine schnellere Verarbeitung bietet. Auch in Bezug auf die Verfügbarkeit ist der *STAR*-Modus in der Regel vorteilhafter.

Achtung: Der *STAR*-Modus ist nur mit *Coupling Facility* möglich.

**Hochverfügbarkeit durch Redundanz**

Bei hohen oder sehr hohen Anforderungen an die Verfügbarkeit sollte geprüft werden, ob die folgenden Redundanzmechanismen zweckmäßig sind:

- RACF mit Primary- und Backup-Datenbank
- Zweite Coupling Facility
- Alternate Couple Datasets
- Zweiter Timer (gekoppelt über Hochverfügbarkeitseinrichtung *FC 4048*, mit eigenem Stromkreis)
- Backup-Systemumgebung, damit im Fehlerfall ein System-Reboot ohne Zeitverzögerung erfolgen kann
- CTC-GRS-Ring (Kanalverbindung *ESCON* / *General Resource Serialization*)
- Backup-MCS-Masterkonsole (*Multiple Console Support*)
- Datensicherung von wichtigen Kontrolldateien, wenn möglich, mit der Option *Concurrent Copy* realisieren (Utility *ADRDSSU*)

Weitere Hinweise finden sich in M 6.93 *Notfallvorsorge für z/OS-Systeme*.

**Festplattenzugriffe**

Bei den Festplattenzugriffen sind folgende Empfehlungen zu beachten:

- Im *Parallel-Sysplex*-Verbund sollten keine Festplatten außerhalb des Verbundes zur Verfügung stehen. Festplatten, die nicht zum Verbund gehören, sollten nur für Recovery-Maßnahmen *Online* gesetzt werden können.
- Der Zugriff auf Festplatten des *Parallel-Sysplex*-Verbundes von anderen, nicht zum Verbund gehörenden Systemen sollte unter Produktionsbedingungen nicht möglich sein.
- Es ist zu überlegen, ob die Option *Enhanced Catalog Sharing* eingesetzt werden soll, wenn hohe Performance-Anforderungen vorliegen.
- Test-/Entwicklungs-Systeme und Produktions-Systeme sollten möglichst nicht im selben *Parallel-Sysplex-Cluster* betrieben werden.
- Das Betriebssystem sollte für alle z/OS-Systeme im *Parallel-Sysplex-Cluster* von einem Systemplatten-Satz geladen werden.

**Symbolische Variablen**

Es sollten symbolische Variablen an möglichst vielen Stellen der *PARM-LIB*-Definitionengenutzt werden. Dies hilft, Fehler bei der Systemadministration zu vermeiden und erleichtert das *System-Cloning*.

**System Logger**

Der *System Logger* sollte mit *Staging Dataset* eingesetzt werden. (Im Fehlerfall wird auf diese Datasets von anderen Systemen im Verbund aus zugegriffen.)

**Reduzierung der Konsol-Nachrichten**

Um die Konsol-Meldungen zu reduzieren und überschaubar zu halten, wird empfohlen, die Message-Filterung zu aktivieren (siehe M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*). Dies ist besonders wichtig, da alle Nachrichten von allen z/OS-Betriebssystemen eines *Parallel-Sysplex-Clusters* auf einer MVS-Konsole angezeigt werden.

Prüffragen:

- Bei Einsatz eines Parallel-Sysplex-Clusters unter z/OS: Wird geprüft, ob eine redundante Auslegung der Coupling Facility erforderlich ist, um den Anforderungen an die Verfügbarkeit des Gesamtsystems Rechnung zu tragen?
- Wird der Zugriff auf die Couple Datasets unter z/OS über RACF geschützt?
- Wird das administrative z/OS-Utility XCMIAPU über ein entsprechendes Facility-Profil im RACF geschützt, so dass nur autorisiertes Personal Zugriff hat?
- Wird für alle LPARs des gesamten Parallel-Sysplex-Clusters unter z/OS eine RACF-Datenbank mit einheitlichen RACF-Definitionen verwendet?
- Ist die System Managed Storage-Struktur im gesamten Parallel-Sysplex-Verbund unter z/OS einheitlich?
- Bei Einsatz eines Parallel-Sysplex-Clusters unter z/OS: Ist ein GRS-Verbund zur Serialisierung von System-Aktionen eingerichtet?
- Werden im Parallel-Sysplex-Cluster unter z/OS ausschließlich Festplatten innerhalb des Verbundes zur Verfügung gestellt?
- Wird der Zugriff auf Festplatten des Parallel-Sysplex-Clusters unter z/OS von Systemen außerhalb des Verbundes verhindert?

# M 4.222 Festlegung geeigneter Einstellungen von Sicherheitsproxies

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In dieser Maßnahme werden Empfehlungen zu Standardeinstellungen der wichtigsten Sicherheitsproxies zusammengestellt. Die vorgeschlagenen Einstellungen können allerdings die Funktionalität der betreffenden Inhalte einschränken (z. B. können eventuell Web-Seiten aufgrund des fehlenden JavaScript nicht mehr bedient werden) und müssen deshalb auf die eigenen Bedürfnisse angepasst werden.

**HTTP**

Die Filterung aktiver Inhalte in Webseiten ist ein zentraler Punkt bei der Sicherheit der Clients (siehe auch M 4.100 *Sicherheitsgateways und aktive Inhalte*). Für Clients mit hohem Schutzbedarf bezüglich der Vertraulichkeit sollten aktive Inhalte in Webseiten grundsätzlich ausgefiltert werden. Gegebenenfalls können in Einzelfällen für vertrauenswürdige Websites aktive Inhalte zugelassen werden (Whitelist Strategie). Die entsprechenden Whitelists dürfen aber nicht zu umfangreich werden und müssen regelmäßig überprüft und gepflegt werden.

Folgende weitergehende Einstellungen werden für HTTP-Proxies empfohlen:

- Sperrung des HTTPS-Verkehrs, falls kein HTTPS-Proxy eingesetzt wird,
- Komplette Sperrung von Cookies (eventuell Freischaltung einzelner Webseiten),
- Filtern bzw. Ersetzen der Browserkennung,
- Filtern folgender Informationen aus dem Request-HTTP-Header:
  - Referer (falls beim Surfen eine Domain verlassen wird)
  - Via
  - From
- Filtern folgender Informationen aus dem Response-HTTP-Header:
  - Server
- Prinzipiell Freigabe aller URLs. Ggf. Sperrung einzelner, bedenklicher URLs und
- Einschränkung auf notwendige MIME-Typen.
  Hinweis: Die Whitelist-Strategie "Alles sperren, was nicht explizit erlaubt ist" kann auf die Sperrung bzw. Freigabe von MIME-Typen nur schlecht angewendet werden. Aufgrund der Vielzahl der von Web-Seiten verwendeten MIME-Typen ist sehr schwierig, die relevanten Typen zu sperren und gleichzeitig die Funktionalität des Dienstes WWW wenigstens einigermaßen zu erhalten. Eine pragmatische Vorgehensweise ist die Sperrung besonders bedenklicher MIME-Typen. Um einen hohen Schutz zu erhalten, muss eine solche Sperrliste allerdings ständig vom Administrator auf dem Laufenden gehalten werden.

**HTTPS**

Bezüglich der Filterung von Schadprogrammen sollte wie beim HTTP-Proxy verfahren werden.

Ein HTTPS-Proxy ist die zentrale Entscheidungsinstanz für die Akzeptanz von Zertifikaten und nimmt den Benutzern weitgehend die Kontrolle über die Zertifikate ab. Aus diesem Grunde sind die Einstellungen des HTTPS-Proxies bezüglich der Vorgehensweise bei "problematischen" Zertifikaten besonders wichtig. Die folgende Tabelle gibt Vorschläge zur Einstellung in verschiedenen Fällen:

| **Entscheidung** | **Vorschlag zur Einstellung** |
|---|---|
| Akzeptieren von Zertifikaten, die von einer Zertifizierungsstelle ausgestellt wurden. | Den in weit verbreiteten Browsern eingetragenen Zertifizierungsstellen kann vertraut werden. Dabei wird davon ausgegangen, dass die Vertrauenswürdigkeit der Zertifizierungsstellen durch den Hersteller der Browser überprüft wurde.<br>Trotzdem sollte regelmäßig geprüft werden, ob alle Zertifizierungsstellen noch vertrauenswürdig sind.<br>Gegebenenfalls können zusätzliche Zertifizierungsstellen hinzugefügt werden. Dies darf aber nur nach sorgfältiger Prüfung der Vertrauenswürdigkeit der Zertifizierungsstelle geschehen. |
| Akzeptieren von Zertifikaten, die nicht von einer Zertifizierungsstelle ausgestellt wurden ("self signed certificates"). | Selbst erstellte Zertifikate dienen ausschließlich zur Verschlüsselung und bieten keine Funktionen zur Sicherstellung der Authentizität einer Web-Site.<br>Solche Zertifikate sollten nur in Ausnahmefällen nach einer expliziten Überprüfung akzeptiert werden. |
| Tunneln von Webseiten (d. h. bei diesen besteht Ende-zu-Ende-Verschlüsselung). | Beim Tunneln wird die Filterung auf Schadprogramme umgangen. Daher sollte Tunneln nur ausnahmsweise zugelassen werden, wenn zu der betreffenden Gegenseite ein besonders hohes Vertrauen besteht. |
| Akzeptieren von Zertifikaten, bei denen der "Common Name" des Zertifikats nicht mit der aufgerufenen URL übereinstimmt. | Stimmen der "Common Name" des Zertifikats und URL nicht überein, so ist dies prinzipiell ein Indiz für eine Manipulation.<br>Solche Zertifikate sollten prinzipiell nicht akzeptiert werden. |
| Akzeptieren von Zertifikaten trotz abgelaufenen Gültigkeitszeitraums. | Vertrauenswürdige Web-Sites sind gut betreut und besitzen immer ein gültiges Zertifikat.<br>Zertifikate mit abgelaufenen Gültigkeitszeitraum sollten daher prinzipiell nicht akzeptiert werden. |

Tabelle: Vorschläge zur Einstellung

**SMTP**

Auch im Zusammenhang mit SMTP (d. h. dem Dienst E-Mail) sollte M 4.100 *Sicherheitsgateways und aktive Inhalte* beachtet werden.

In verschiedene Sicherheitsproxies sind Spam-Filter integriert. Allerdings reichen die Fähigkeiten dieser Filter oft nicht an die Funktionalität dedizierter Spam-Filter (d. h. eigenständiger Komponenten) heran. Die Integration eines dedizierten Spam-Filters in das Sicherheitsgateway ermöglicht somit oft eine effektivere Filterung von E-Mails.

Derzeit existieren keine Verfahren, die "nützliche" E-Mails von Spam-Mails sicher unterscheiden können. Der Einsatz eines Spam-Mail-Filters ist deshalb nur dann zu empfehlen, wenn die Liste der verworfenen E-Mails ständig (in der Regel täglich) von einem Mitarbeiter nach versehentlich verworfenen E-Mails ("false positives") durchsucht wird.

Vorschläge zu Konfiguration und Betrieb des Spam-Filters:

- Der Spam-Filter sollte gesperrte E-Mails nicht an den Absender zurückschicken bzw. eine Meldung über die Tatsache der Sperrung ausgeben, da der Spam-Absender in diesem Fall weitere Informationen über die Existenz seiner Adressaten erhält.
- Ein automatisches Löschen von E-Mails kann aus verschiedenen (unter anderem aus rechtlichen) Gründen problematisch sein. Der Spam-Filter sollte daher keine E-Mails automatisch löschen, sondern sie stattdessen mit einem Hinweis versehen, dass es sich vermutlich um eine Spam-Mail handelt. Anhand dieses Hinweises kann der Mail-Client bzw. der Benutzer selbst eine Sortierung in unterschiedliche Postfächer oder Verzeichnisse vornehmen.
- Die Betreuung des Spam-Filters sollte durch organisationsinterne Mitarbeiter erfolgen. Wird die Filterung als Dienst eingekauft, ergeben sich eventuell (datenschutz-) rechtliche Probleme.
- Vor dem Einsatz von Spam-Filtern sollte eine umfassende rechtliche Zulässigkeitsprüfung im Einzelfall vorgenommen werden. Die allgemeine rechtliche Lage beim Einsatz von Spam-Filtern ist derzeit noch unklar. Die Einführung von Spam-Filtern sollte zudem mit der Betriebsleitung und dem Betriebsrat abgesprochen werden.
- Appliances zur Spam-Filterung können den Installationsaufwand verringern. Diese Produkte bieten oft umfassende Updatemöglichkeiten zur Verbesserung der Erkennungsrate.
- Bei eingehenden E-Mails sollte kontrolliert werden, ob Server des vertrauenswürdigen Netzes als Mail-Relay missbraucht werden. Dabei wird bei eingehenden E-Mails überprüft, ob die Empfängerdomain zum vertrauenswürdigen Netz gehört. Bei ausgehenden E-Mails sollte die Absenderdomain zum vertrauenswürdigen Netz gehören.
- Ausgehende E-Mails sollten ebenfalls kontrolliert werden. Dadurch kann der Schaden begrenzt werden, wenn trotz aller Sicherheitsmaßnahmen ein Client im internen Netz mit einem E-Mail-Wurm infiziert wird. Auf diese Weise kann eine Infektion oft auch sofort entdeckt werden.
- Auffällige E-Mail-Adressen sollten gesperrt werden.

Wird kein Spam-Filter in das Sicherheitsgateway integriert, so sollten die Mitarbeiter beim sicheren Umgang mit Spam-Mails geschult werden. Hinweise an die Mitarbeiter könnten sein:

- Spam-Mails ungelesen löschen,
- Unsubscribe-Funktion von Spam-Mails nicht verwenden,

- Mit dem Absender "fraglicher" vor dem Öffnen Rücksprache halten, falls dieser bekannt ist und
- Einige Provider wünschen die Zusendung von besonders auffälligen bzw. gefährlichen Spam-Mails. In Ausnahmefällen kann auch eine Benachrichtigung des Providers sinnvoll sein.

**Filterung von Dateianhängen**

Folgende Dateianhänge werden in den meisten Arbeitsumgebungen nicht benötigt und könnten gefiltert werden (geordnet nach der Art der Bedrohung):

Zugriff auf das gesamte System:

- * .bat (DOS-Batch-Datei)
- * .vbx (Visual-Basic-Datei)
- * .com (Windows-Anwendung)
- * .hta (HTML-Applikationen)
- * .inf (Installationsskript)
- * .js (Jscript-Datei)
- * .jse (Kodierte Jscript-Datei)
- * .wsh (Windows-Scripting-Host-Skript)
- * .vbs (Visual-Basic-Datei)
- * .vbe (Kodierte Visual-Basic-Datei)

Ausführung beliebiger Anwendungen:

- * .lnk (Link-Datei)
- * .chm (Kompilierte HTML-Datei)
- * .pif (Programm-Information-File)
- * .rm (RealMedia-Datei)

Weitere Probleme:

- * .mdb (Access-Datenbank. Können Makroviren beinhalten.)
- * .reg (Registry-Datei. Kann Veränderungen an der Registry vornehmen.)

Diese Liste ist zwangsläufig unvollständig. Es existieren viele weitere Dateitypen, mit denen ein Endgerät kompromittiert werden kann, die teilweise für Arbeitsvorgänge unbedingt benötigt werden (z. B. .html, .xls, .pdf). Das Filtern von Dateien alleine anhand von Dateiendungen oder MIME-Typen kann alleine keine ausreichende Sicherheit erzeugen, da Dateien mit Schadprogrammen oft mit unbedenklichen Endungen versehen und trotzdem ausgeführt werden.

**Telnet**

Telnet sollte nur noch in Ausnahmefällen verwendet und nach Möglichkeit durch ein sichereres Protokoll wie beispielsweise SSH ersetzt werden. Muss Telnet aus zwingenden Gründen trotzdem noch eingesetzt werden, so müssen mit Hilfe des ALG oder der Paketfilter die erlaubten Verbindungen auf ein Minimum beschränkt werden.

**FTP**

FTP sollte wie Telnet ebenfalls nur noch in Ausnahmefällen verwendet und die erlaubten Verbindungen müssen ebenfalls mit entsprechenden Filterregeln oder Access-Control-Lists auf ein Minimum beschränkt werden.

Folgende Protokollbefehle sollten gefiltert werden:

- PORT (Filterung verhindert aktives FTP)

**POP3**

Bei POP3 sollte M 4.100 *Sicherheitsgateways und aktive Inhalte* beachtet werden.

Prüffragen:

- Sind die Einstellungen der Sicherheitsproxies zur Nutzung der unterschiedlichen Protokolle mit den Bedürfnissen der Organisation abgestimmt?
- Erfolgt die Nutzung von SMTP über die Integration eines dedizierten Spam-Filters in das Sicherheitsgateway?
- Erfolgt eine Filterung von Dateianhängen durch das Sicherheitsgateway?
- Sind die umgesetzten Sicherheitsmaßnahmen bei der Nutzung von Proxies und zur Filterung von Dateianhängen nachvollziehbar dokumentiert?

# M 4.223 Integration von Proxy-Servern in das Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

**HTTPS-Sicherheitsproxy**

Der HTTPS-Proxy sollte den eintreffenden Datenverkehr entschlüsseln, der Inhaltefilterung zuleiten und daraufhin den Datenverkehr wieder verschlüsseln. Der temporär unverschlüsselte Datenverkehr kann auf unerwünschte Inhalte untersucht werden.

Im besten Fall wird ein HTTPS-Proxy vom eingesetzten Application Level Gateway (ALG) unterstützt. Dann bietet sich der in Abbildung dargestellte, relativ einfache Aufbau an. Hier wird der Übersichtlichkeit halber der Fall betrachtet, in dem der Datenverkehr auf einer eigenen Komponente gefiltert wird. Vielfach wird die Filterung jedoch vom Hersteller bereits in das ALG integriert.

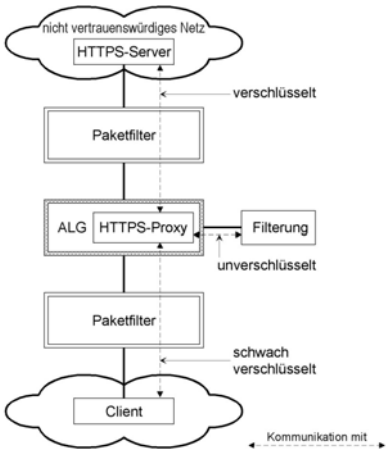



Abbildung: Integration eines internen HTTPS-Proxies

| Vorteile "HTTPS-Proxy auf ALG" | Nachteile "HTTPS-Proxy auf ALG" |
|---|---|
| - Einfache Einrichtung, da in der Regel Konfigurationsoberflächen zur Verfügung stehen.<br>- Gegenüber einem externen HTTPS-Proxy ergibt sich eine geringere Anzahl an Kommunikationsbeziehungen zwischen den an der SSL-Entschlüsselung und an der Inhaltefilterung beteiligten Modulen (da die Daten das ALG nicht verlassen müssen). | - Die Komplexität von SSL begünstigt Fehler bei der Entwicklung der Proxy-Software, was zu Schwachstellen führen kann. Durch Fehler in der SSL-Implementierung kann dann möglicherweise das gesamte ALG übernommen werden.<br>- Der maximale Datendurchsatz wird aufgrund der rechenintensiven Schlüsselverarbeitung und der daraus resultierenden verstärkten Auslastung des ALG verringert. |

Tabelle: Vorteile und Nachteile von HTTPS-Proxy auf ALG

Falls das ALG keinen HTTPS-Proxy anbietet, ergibt sich der in der Abbildung dargestellte Aufbau. Der HTTPS-Proxy befindet sich hier in einer eigenen

DMZ. In der Abbildung ist abweichend von der vorhergehenden Abbildung der Fall dargestellt, bei dem Schadinhalte vom ALG gefiltert werden.

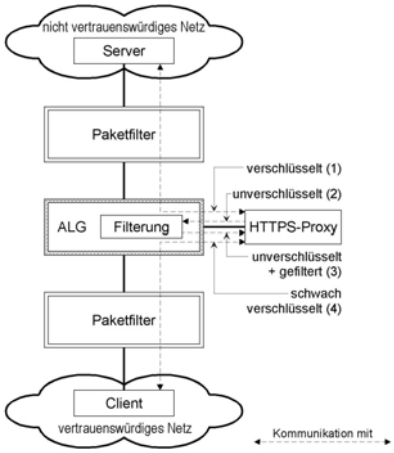



Abbildung: Integration eines externen HTTPS-Proxies

| Vorteile "HTTPS-Proxy in DMZ" | Nachteile "HTTPS-Proxy in DMZ" |
|---|---|
| - Die Produktauswahl ist unabhängig vom ALG möglich.<br>- Entlastung des ALGs, da die rechenintensive Schlüsselverwaltung auf einem eigenen Rechner stattfindet. | - Auf dem ALG müssen mehrere Proxies eingerichtet werden.<br>- Fehlkonfigurationen werden aufgrund der komplexen Kommunikationsbeziehungen der beteiligten Komponenten begünstigt.<br>- Erhöhte Latenzzeiten gegenüber einem auf dem ALG integrierten HTTPS-Proxy beim Abruf von Daten, da mehrere TCP- bzw. UDP-Verbindungen zwischen den einzelnen Modulen aufgebaut werden müssen. |

Tabelle: Vorteile und Nachteile von HTTPS-Proxy in DMZ

Die Stärke der Verschlüsselung innerhalb des vertrauenswürdigen Netzes könnte bei beiden vorgestellten Lösungen dem Schutzbedarf und der Vertrauenswürdigkeit der Teilnehmer angepasst werden, unter Umständen kann hier zur Steigerung der Performance auf eine Verschlüsselung im vertrauenswürdigen Netz verzichtet werden oder ein weniger rechenintensives, schwächeres Verschlüsselungsverfahren eingesetzt werden.

**Caching-Proxy**

Bei der Nutzung von Diensten könnte der Zugriff auf das nicht-vertrauenswürdige Netz auf bestimmte Proxies (z. B. Caching-Proxy für HTTP) beschränkt werden. Die Clients können den ("Zwangs-") Proxy nicht umgehen, um nach außen zu kommunizieren, da die IP-Adresse des Clients vom Sicherheitsgateway abgewiesen wird (nur die IP-Adresse des Caching-Proxy wird vom Sicherheitsgateway akzeptiert).

| Vorteile von ("Zwangs-") Caching-Proxies | Nachteile von ("Zwangs-") Caching-Proxies |
|---|---|
| - Umfangreiche Möglichkeiten zur Protokollierung des HTTP-Verkehrs, falls nur ein einstufiges Si- | - Kompletter Ausfall von HTTP/ HTTPS bei Ausfall des Proxies. Eine vorübergehende In- |

| Vorteile von ("Zwangs-") Caching-Proxies | Nachteile von ("Zwangs-") Caching-Proxies |
|---|---|
| cherheitsgateway verwendet wird (bestehend aus einem Paketfilter).<br>- Erweiterte Filtermöglichkeiten, falls nur ein einstufiger Aufbau bestehend aus einem Paketfilter eingesetzt wird. Mit einem Caching-Proxy lassen sich beispielsweise filtern:<br>  - Cookies,<br>  - URLs,<br>  - HTTP-Referrer,<br>  - HTTP-Via und<br>  - HTTP-Server.<br>- Reduzierung des übertragenen Datenvolumens aufgrund der Caching-Funktionalität.<br><br>Anmerkung: In der Regel werden Caching-Proxies nicht unter Sicherheitsaspekten entwickelt. Ein dedizierter Sicherheitsproxy sollte den Caching-Proxies nach Möglichkeit vorgezogen werden. | betriebnahme unter Verzicht auf den Proxy erfordert umfangreiche Konfigurationsarbeiten (die Sperrlisten auf dem Paketfilter müssen geändert werden und die Proxyeinstellungen der Clients müssen angepasst werden, falls der Caching-Proxy nicht transparent betrieben wurde). In der Regel ist deshalb eine redundante Auslegung des Proxies notwendig. |

Tabelle: Vorteile und Nachteile von Zwangs-Caching-Proxies

**Reverse Proxy**

"Reverse Proxies" werden im Zusammenhang mit der Bereitstellung von (Web-) Servern auch zur Erreichung folgender Sicherheitsziele verwendet:

- Einschränkung der Kommunikationsverbindungen, die aus dem nicht-vertrauenswürdigen Netz kommend über einen Sicherheitsproxy geleitet werden müssen. Dadurch wird die Administration des Sicherheitsgateways erleichtert und die Wahrscheinlichkeit von Fehlkonfigurationen verringert.
- Verschleierung der Identität des Webservers (mehrere, zur Lastverteilung genutzte Web-Server erscheinen vom nicht-vertrauenswürdigen Netz aus gesehen unter einer IP-Adresse).
- Abfangen von Fehlermeldungen des Webservers, die einem Angreifer Hinweise zur Kompromittierung des Systems liefern könnten (eigentlich handelt es sich hierbei um einen Workaround, da der Webserver dieses Problem selber abfangen sollte).
- Zusätzliche Abschottung des Webservers, d. h. ein Angreifer kann u. U. die Informationen einer Transaktion mitlesen, aber keinen Zugriff auf den Webserver erlangen.
- Abkoppelung des IP-Stacks des Servers vom nicht-vertrauenswürdigen Netz.
- Filterung unerwünschter, aus dem nicht-vertrauenswürdigen Netz stammender Anfragen an den Webserver.
- Erhöhung der Verfügbarkeit aufgrund von Lastverteilung und Lastminderung durch Caching.

In der folgenden Abbildung ist eine Situation dargestellt, in der zwei Server zum Zugriff aus dem nicht-vertrauenswürdigen Netz bereitgestellt werden. In

dem abgebildeten Szenario müssen zwei Kommunikationsverbindungen über das ALG und den externen Paketfilter hinweg freigeschaltet werden.

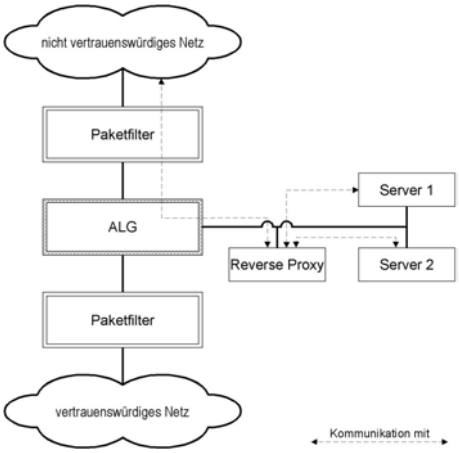



Abbildung: Reverse Proxy zur Vermeidung vieler Kommunikationsbeziehungen über das ALG hinweg. Reverse Proxy und die Server stehen in einer DMZ.

Die in der vorigen Abbildung dargestellten Kommunikationsbeziehungen lassen sich mit Hilfe eines Reverse Proxy reduzieren. In Abbildung ist aus dem nicht-vertrauenswürdigen Netz nur der Zugriff auf den Reverse Proxy gestattet, Server 1 und 2 sind vor Zugriff gesperrt. Auf beide Server kann nur der Reverse Proxy zugreifen.

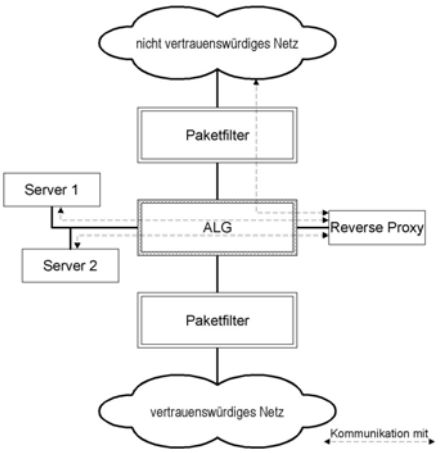



Abbildung: Reverse Proxy zur Vermeidung vieler Kommunikationsbeziehungen über das ALG hinweg. Reverse Proxy und die Server stehen in verschiedenen DMZ.

Zur Erhöhung der Serversicherheit können die Server auch in einer eigenen DMZ betrieben werden, wo sie durch einen Sicherheitsproxy vom Reverse Proxy getrennt werden. Die Übernahme eines Servers wird hierdurch zusätzlich erschwert, allerdings erhöht sich die Anzahl der Kommunikationsbeziehungen über das ALG.

Prüffragen:

- Betrifft den Einsatz eines Reverse-Proxy: Existieren Maßnahmen bei Ausfall des Reverse-Proxy?

- Entspricht der Einsatz der Proxies den Sicherheitsvorgaben der Organisation?
- Betrifft den Einsatz eines Caching-Proxy: Deckt sich der Einsatz des Caching-Proxy mit den Vorgaben der Sicherheitsrichtlinien der Organisation?
- Betrifft den Einsatz eines Caching-Proxy: Existieren Maßnahmen bei Ausfall des Caching-Proxy?
- Existieren Maßnahmen die bei Ausfall eines Proxies getroffen werden?
- Betrifft den Einsatz eines Reverse-Proxy: Deckt sich die Umsetzung des Reverse-Proxy mit den Anforderungen der Sicherheitsvorgaben der Organisation?

# M 4.224 Integration von VPN-Komponenten in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für die Sicherheit eines VPNs ist die Integration der VPN-Endpunkte in die Sicherheitsgateways essentiell. Die optimale Platzierung der VPN-Komponenten ist dabei abhängig von mehreren Faktoren:

- Schutzbedarf des VPN-Gateways vor Angriffen aus dem nicht-vertrauenswürdigen Netz
- Notwendigkeit der Kontrolle und Flusssteuerung der Datenübertragung der Zugriffe aus dem nicht-vertrauenswürdigen Netz auf Systeme und Dienste im vertrauenswürdigen Netz
- Schutzbedarf der übertragenen Daten

Die bekanntesten Protokolle zum Aufbau von VPNs sind IPSec, TLS/SSL, PPTP und L2TP. Daher werden im Folgenden solche VPNs betrachtet. Die hier dargestellten Empfehlungen lassen sich jedoch auch auf die meisten anderen Verfahren übertragen. Die Entscheidung für ein bestimmtes Verfahren hängt von der jeweiligen Anwendung und vom Einsatzgebiet ab. Es kann durchaus zweckmäßig sein, dass eine Institution mehrere VPNs mit unterschiedlichen VPN-Protokollen und Kryptoverfahren betreibt.

Die Entscheidung, welche Verfahren eingesetzt und wie die einzelnen VPN-Komponenten angeordnet werden sollen, ist zu dokumentieren.

**VPNs mittels IPSec oder TLS/SSL**

Der Ort der Integration des VPN-Gateways relativ zum Paketfilter des Sicherheitsgateways hängt davon ab, wie viele Schnittstellen dem VPN-Gateway zur Verfügung stehen.

- VPN-Gateways mit einer Schnittstelle:
  Bei einem hohen Angriffspotenzial sollte das VPN-Gateway durch einen Paketfilter geschützt am Application-Level-Gateway (ALG) platziert werden. Der äußere Paketfilter schützt gegen IP-Spoofing-Attacken, da aus dem nicht-vertrauenswürdigen Netz eingehende Pakete mit der IP-Adresse des VPN-Gateways als Absenderadresse vom äußeren Paketfilter nicht weitergeleitet werden. Der entschlüsselte Datenverkehr muss auf dem Weg in das vertrauenswürdige Netz das ALG und den inneren Paketfilter passieren. Da entschlüsselte Verbindungen nur an der DMZ-Schnittstelle des ALG und nicht an der Schnittstelle des ALG zum nicht-vertrauenswürdigen Netz erlaubt werden, ist ein unberechtigter Verbindungsaufbau aus dem nicht-vertrauenswürdigen Netz gegenüber den vorangehenden Varianten deutlich erschwert.

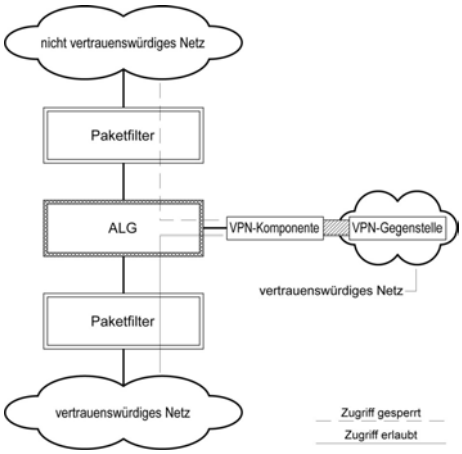



Abbildung 1: Platzierung einer VPN-Komponente mit einer Schnittstelle

- VPN-Gateways mit zwei Schnittstellen:
  Bei VPN-Gateways mit zwei Schnittstellen sollte das VPN-Gateway mit einer Netzschnittstelle am äußeren Paketfilter und mit der anderen Schnittstelle am ALG verbunden werden. Durch die Platzierung des VPN-Gateways am äußeren Paketfilter wird die VPN-Komponente durch den äußeren Paketfilter gegen Angriffe aus dem nicht-vertrauenswürdigen Netz geschützt. Aus dem nicht-vertrauenswürdigen Netz werden nur Verbindungen zum VPN-Gateway zugelassen, die für die VPN-Kommunikation erforderlich sind. Der entschlüsselte Datenverkehr kann auf Anwendungsebene kontrolliert und eingeschränkt werden, da die Verbindungen über das ALG geleitet werden. Zusätzlich kann der entschlüsselte Datenverkehr durch den internen Paketfilter kontrolliert und eingeschränkt werden.

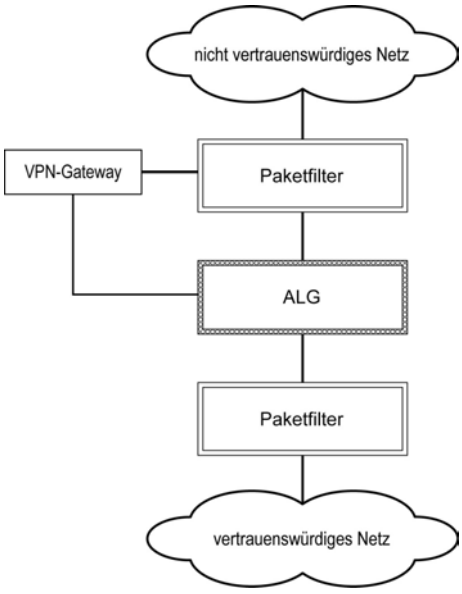



Abbildung 2: Platzierung einer VPN-Komponente mit zwei Schnittstellen

**VPNs mittels Layer-2-Protokollen**

Layer-2-VPNs können beispielsweise mit Hilfe der Protokolle PPTP (Point to Point Tunneling Protocol) und L2TP (Layer 2 Tunneling Protocol) realisiert werden. Sie werden häufig verwendet, um VPNs über öffentliche Telekommunikationsnetze, beispielsweise GSM oder ISDN, aufzubauen. Zur Netztren-

nung sollte auch für Layer-2-VPNs ein ALG zwischen dem LAN und der VPN-Anbindung verwendet werden.

Bei der Anbindung verschiedener Nutzergruppen mit verschiedenen Rechten sollte jeder Nutzergruppe ein eigener Schlüsselkreis zugeordnet werden, um die Vertraulichkeit der übertragenen Daten zwischen den Nutzergruppen sicherzustellen.

Prüffragen:

- Sind die VPN-Komponenten so in das Sicherheitsgateway integriert, dass der Datenverkehr wirksam kontrolliert und gefiltert werden kann?
- Ist die Entscheidung dokumentiert, wie die VPN-Komponenten in das Sicherheitsgateway zu integrieren sind?

# M 4.225 Einsatz eines Protokollierungsservers in einem Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei komplizierteren Sicherheitsgateways fallen oft große Mengen verschiedener Protokollierungsinformationen der verschiedenen Komponenten an. Um die Auswertung der Protokolle zu erleichtern ist es empfehlenswert, an zentraler Stelle einen Protokollierungsserver (Loghost) zu betreiben, der die Protokolldaten der an das Sicherheitsgateway angeschlossenen Komponenten aufnimmt. Die Daten lassen sich so einfach zueinander in Beziehung setzen und erleichtern damit die regelmäßige, anlassunabhängige Auswertung und ermöglichen im Falle eines Ausfalls das Auffinden des Verursachers (siehe auch M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*).

Problematisch ist die Platzierung des zentralen Loghosts, denn er muss einerseits von sämtlichen Komponenten des Sicherheitsgateways aus zu erreichen sein, andererseits darf er keinen unberechtigten Zugriff aus dem nichtvertrauenswürdigen Netz ermöglichen.

Wird der Loghost kompromittiert, so erleichtert er aufgrund der zentralen Aufstellung im Sicherheitsgateway die Kompromittierung der anderen Komponenten erheblich. Ein zentraler Loghost im Sicherheitsgateway sollte daher nur diese Funktion wahrnehmen und nicht noch für weitere Aufgaben (etwa als Administrationsrechner) verwendet werden.

Im Zusammenhang mit Logdaten sollte folgendes beachtet werden:

- Der zentrale Loghost sollte die Daten redundant ablegen.
- Die Protokollierung sollte, wenn möglich, zusätzlich lokal auf den einzelnen Komponenten des Sicherheitsgateways erfolgen. Da hierdurch die Leistung der Komponente nicht merklich sinkt, sollte diese Sicherung als zusätzlicher Ausfallschutz eingeschaltet werden.

Ein weiteres wichtiges Element der Protokollierung stellt die Alarmierung bei definierten, kritischen Ereignissen dar. Auch hier ist darauf zu achten, dass die Weiterleitung der Alarmmeldungen zu einer zentralen Instanz möglich ist.

Wichtigstes Kriterium bei der Platzierung eines Loghosts ist, dass keine zusätzlichen Schwachstellen entstehen, wie z. B. die Möglichkeit zur Umgehung von Sicherheitskomponenten. Zudem ist zu berücksichtigen, dass die Protokolldaten zur Speicherung auf einem zentralen Loghost möglichst wenige Komponenten des Sicherheitsgateways überqueren müssen. Werden Protokolldaten über Proxies versendet, so erscheinen diese in den Protokolldateien mit der IP-Adresse des Proxies, so dass der eigentliche Absender nicht mehr unmittelbar zu erkennen ist, wenn nicht die Protokollierungsfunktionen auf den einzelnen Komponenten eine entsprechende Kennzeichnung der Daten ermöglichen.

Im Idealfall werden Loghosts in einem eigenen Administrationsnetz platziert. Auf den Loghost wird dann ausschließlich aus dem Adminstrationsnetz heraus zugegriffen.

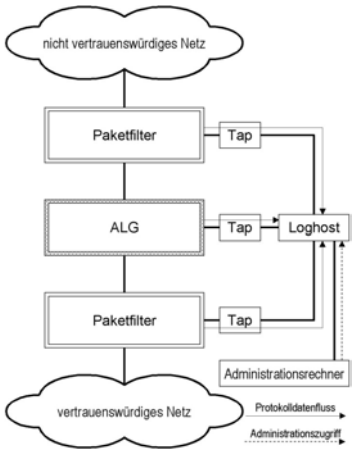



Abbildung 1: Platzierung des Loghost im Administrationsnetz

Steht kein eigenes Administrationsnetz zur Verfügung, so muss der Loghost im Produktivnetz betrieben werden. In Abhängigkeit von der Struktur des Sicherheitsgateways ergeben sich damit zwei empfohlene Platzierungen für einen zentralen Loghost:

**Platzierung bei einfachen Sicherheitsgateways**

Bei einem einfachen Sicherheitsgateway, das nur aus einem einzelnen Paketfilter besteht, bietet es sich an, den Loghost in einer eigenen DMZ des Paketfilters zu platzieren. In der Regel bieten Paketfilter eine ausreichende Anzahl an Netzschnittstellen oder sind leicht erweiterbar, so dass eine spezielle Loghost-DMZ zum Einsatz kommen kann.

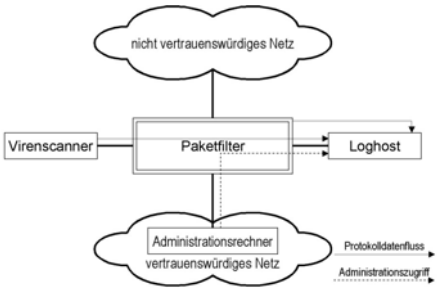



Abbildung 2: Platzierung des Loghost bei einfach strukturierten Sicherheitsgateways

**Platzierung bei komplexen Sicherheitsgateways**

Bei komplexeren Strukturen von Sicherheitsgateways ist es in der Regel notwendig, die Protokolldaten über einen Proxy zum Loghost zu leiten.

Prinzipiell ist dabei zwischen der Platzierung des Loghosts in einer eigenen DMZ und der Platzierung des Loghosts in einer gemeinsamen DMZ mit anderen Modulen des Sicherheitsgateways zu unterscheiden.

Die folgende Abbildung zeigt eine Lösung, bei der ein zentraler Loghost in einer eigenen DMZ platziert wurde und von zwei getrennten Sicherheitsgateways gemeinsam genutzt wird.

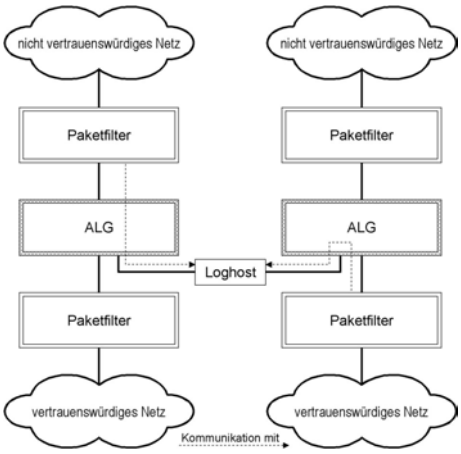



Abbildung 3: Platzierung des Loghost in einer dedizierten DMZ.

Die Platzierung des Loghost in einer eigenen DMZ hat den Vorteil, dass sie bei einer Kompromittierung des Loghosts dem Angreifer nur wenig weitere Angriffsmöglichkeiten eröffnet, da die einzigen direkt erreichbaren Module des Sicherheitsgateways die ALGs sind. Diese sind in der Regel jedoch besonders gegen Angriffe geschützt.

Bei der abgebildeten Lösung ist zudem zu beachten, dass durch die Integration des Loghost eine "Querverbindung" zwischen den beiden vertrauenswürdigen Netzen geschaffen wurde, die ohne Integration des Loghost nicht existiert hätte. Hierzu ist eine eigene Risikoabschätzung notwendig. Gegebenenfalls muss auf die Querverbindung verzichtet werden, was den Einsatz von zwei getrennten Loghosts zur Folge hat, deren Protokolldaten eventuell zu Analysezwecken zusammengeführt werden müssen.

Bei der Lösung, die in der folgenden Abbildung dargestellt ist befinden sich weitere Module des Sicherheitsgateways in der gleichen DMZ wie der Loghost. Diese können weitere Angriffspunkte nach der Übernahme des Loghost bieten, da es sich nicht notwendigerweise um speziell entwickelte Sicherheitsprodukte handelt. Möglicherweise können diese Module deshalb besonders einfach übernommen werden.

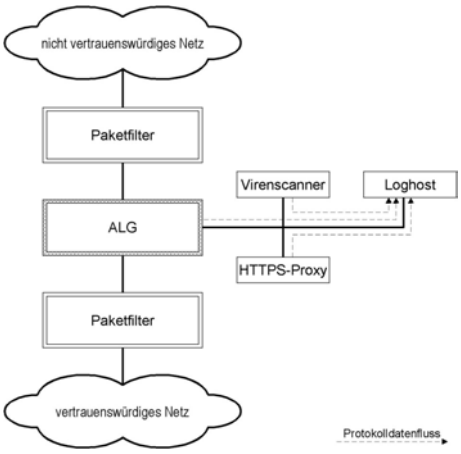



Abbildung 4: Platzierung des Loghost

in einer DMZ, die weitere Komponenten des Sicherheitsgateways enthält.

Die Lösung, bei der der Loghost in einer eigenen DMZ platziert wird, ist deshalb dieser Lösung vorzuziehen.

Die Platzierung des Loghost in einer DMZ mit weiteren Komponenten ist nur dann ratsam, wenn das ALG keine ausreichende Anzahl an Netzschnittstellen zur Verfügung stellt.

Die folgende Tabelle fasst die Empfehlungen zusammen:

| **Struktur des Sicherheitsgateway** | **Schutzbedarf** | **Platzierung des Loghosts** |
|---|---|---|
| Nur Paketfilter | normal | Loghost in einer eigenen DMZ des Paketfilters |
| Komplexes Sicherheitsgateway (P-A-P) | normal | Loghost in einer gemeinsamen DMZ mit anderen Komponenten akzeptabel.<br>Eigene DMZ für den Loghost empfohlen |
| Gemeinsame Nutzung eines Loghosts durch mehrere Sicherheitsgateways | hoch | Loghost in einer eigenen DMZ |

Tabelle: Empfehlungen

Prüffragen:

- Wird der Zugriff auf den Protokollserver aus nicht-vertrauenswürdigen Netzen verhindert?
- Wird der Protokollserver ausschließlich zur Speicherung der Protokolldaten des Sicherheitsgateway genutzt?
- Werden die Protokollierungsinformationen redundant hinterlegt?
- Existiert ein zentrales Alarmierungssystem für im Vorfeld definierte kritische Ereignisse?
- Besteht ein Konzept zur Bestimmung der erforderlichen netzwerktechnischen Platzierung des Protkollierungsservers anhand der Struktur des Sicherheitsgateways?

# M 4.226 Integration von Virenscannern in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Schadsoftware wie Viren, Würmer und Trojanische Pferde (im Folgenden vereinfachend unter dem Begriff "Viren" zusammengefasst) können zum einen zentral auf dem Sicherheitsgateway und zum anderen verteilt auf den Arbeitsplatz-PCs und Servern (d. h. den Endsystemen von Kommunikationsbeziehungen über das Sicherheitsgateway hinweg) gefiltert werden.

Eine zentrale Filterung auf dem Sicherheitsgateway kann einen dezentralen Virenschutz nicht vollständig ersetzen, da unter Umständen Schadsoftware auch auf anderen Wegen (beispielsweise über Wechseldatenträger) auf die Systeme gelangen kann.

Eine zentrale Filterung ist derzeit in der Regel nur beim Einsatz eines Application-Level-Gateways möglich.

**Filterung direkt durch das ALG**

Sofern das eingesetzte ALG eine entsprechende Option anbietet ist es meist sinnvoll, die Prüfung auf Schadsoftware direkt auf dem ALG durchzuführen.

**Filterung durch das Sicherheitsgateway beim Einsatz eines ALG**

ALGs bieten oft eine Schnittstelle, mit denen sich Virenschutzprogramme von Drittanbietern anbinden lassen. Das Virenschutzprogramm nimmt die Daten entgegen und übergibt dem ALG eine Meldung über das Ergebnis der Virenfilterung. Das ALG verarbeitet die Daten dann in Abhängigkeit vom Ergebnis der Überprüfung.

Somit bietet sich für die Integration des Virenscanners der in der nachfolgenden Abbildung dargestellte Aufbau an, in dem der Virenscanner "neben" dem ALG in der DMZ des Sicherheitsgateway platziert wird. Bei diesem Aufbau sollten einige Punkte beachtet werden, da der Rechner mit dem Virenschutzprogramm durch diese Aufgabe besonders stark gefährdet ist:

- Der Rechner mit dem Virenschutzprogramm muss besonders sicher konfiguriert werden, beispielsweise durch eine besonders restriktive Konfiguration des Betriebssystems ("Härten"). Die Sicherheitsanforderungen sind (mindestens) genau so hoch wie an die sonstigen Komponenten des Sicherheitsgateway.
- Der Rechner muss durch entsprechende Paketfilterregeln möglichst gut vom Rest des Netzes getrennt werden. Insbesondere sollten von diesem Rechner keine ausgehenden Verbindungen, weder ins interne noch ins externe Netz, von den Paketfiltern erlaubt werden. Im Idealfall kann der Rechner direkt mit dem ALG kommunizieren, über den er den zu prüfenden Datenstrom erhält und an den er die gefilterten Daten zurück liefert. Darüber hinaus sind nur noch Verbindungen aus einem gesonderten Administrationsnetz zu dem Rechner erlaubt.
- Die regelmäßige Integritätsprüfung des Systems sollte in kurzen Abständen erfolgen.
- Eventuell sollte der Rechner mit einem host-basierten Intrusion-Detection-System ausgerüstet werden, so dass eine eventuelle Kompromittierung möglichst sofort erkannt werden kann.

- Die Administration des Rechners muss über eine entsprechend abgesicherte Verbindung erfolgen.

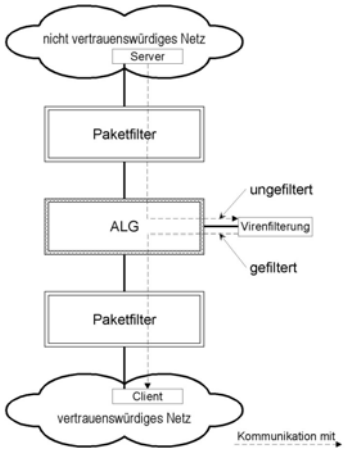



Abbildung: Integration einer Viren-Filterung

**Filterung auf den Endgeräten (beim Einsatz eines Paketfilters)**

Da Paketfilter keine Schnittstelle zu Virenfiltern besitzen, ist beim Einsatz eines einstufigen Sicherheitsgateways, das nur aus einem Paketfilter besteht normalerweise keine zentrale Virenfilterung durch das Sicherheitsgateway möglich. In diesem Fall kann der Schutz vor Schadprogrammen nur durch den Einsatz von Virenfiltern auf den Arbeitsplatzrechnern oder den jeweiligen Servern des vertrauenswürdigen Netzes (beispielsweise E-Mail-Server, Newsserver) realisiert werden.

Zum Thema Virenschutz ist außerdem Baustein B 1.6 *Schutz vor Schadprogrammen* zu berücksichtigen.

Prüffragen:

- Erfolgt zusätzlich zum dezentralen Virenschutz eine zentrale Filterung auf dem Sicherheitsgateway?
- Betrifft die Anbindung eines Virenschutzprogramms an das Application-Level-Gateway: Ist der externe Rechner zur Virenprüfung im Vergleich zu den Komponenten des Sicherheitsgateway abgesichert?

# M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In vielen Situationen ist es bei vernetzten Systemen wichtig, dass alle bei einem Vorgang betroffenen Rechner eine korrekte Systemzeit besitzen. Insbesondere bei der Auswertung von Protokollierungsinformationen ist dies von zentraler Bedeutung, beispielsweise um Fehlermeldungen, die auf einen Angriff über das Netz hindeuten, richtig korrelieren zu können, oder wenn bei Anwendungen, die über mehrere Rechner verteilt sind, Synchronisationsprobleme auftreten. Auch verteilte Dateisysteme und zentrale Authentisierungsdienste sind auf Zeitsynchronizität angewiesen.

Für die korrekte Einstellung der Systemzeit bieten die meisten Betriebssysteme die Möglichkeit, über das Protokoll NTP (Network Time Protocol Version 3, RFC 1305) oder SNTP (Simple Network Time Protocol Version 4, RFC 2030) auf einen externen Zeitserver zuzugreifen. Windows-Rechner in einer Active Directory Infrastruktur gleichen zudem die Systemzeit mit dem Domänencontroller ab.

Im Internet existiert eine verteilte Infrastruktur von öffentlichen NTP Zeitservern. In Deutschland bieten beispielsweise die Physikalisch-Technische Bundesanstalt (PTB) in Braunschweig und verschiedene Universitäten einen solchen Dienst an.

Da NTP ein Klartextprotokoll ohne kryptographische Sicherungen ist, sollte es nur innerhalb des eigenen Netzes eingesetzt werden. Falls die Zeitserver-Infrastruktur im Internet genutzt werden soll, so sollte dafür ein eigener Rechner vorgesehen werden, der als einziger die NTP-Informationen von den ausgewählten Zeitservern bezieht. Die Rechner im lokalen Netz synchronisieren ihre Systemuhr dann mit dem lokalen NTP-Proxy. Am Sicherheitsgateway sollte NTP in diesem Fall nur für den NTP-Proxy-Server freigeschaltet werden. Insbesondere in Netzen mit hohem Schutzbedarf sollten keinesfalls alle Geräte individuell per NTP direkt Anfragen an Zeitserver im Internet stellen.

Alternativ kann ein Rechner im internen Netz mit einem Funkuhr-Modul ausgestattet als lokaler Zeitserver eingesetzt werden. Im Zweifelsfall sollte dieser Lösung der Vorzug gegeben werden.

Falls für die Zeitsynchronisation auf externe Quellen (Funkuhren, öffentliche NTP-Zeitserver, etc.) zurückgegriffen wird, muss sichergestellt werden, dass die empfangenen Zeit-Informationen nicht ungeprüft übernommen werden. Die Software des lokalen Zeit-Servers beziehungsweise NTP-Proxys muss eine Plausibilitätsprüfung vornehmen, bevor sie die empfangenen Zeit-Informationen übernimmt und an die anderen Rechner im Netz weitergibt. Ein Beispiel für eine solche Plausibilitätsprüfung ist, dass sprunghafte Änderungen, die eine vorher festgelegte maximale Zeitdifferenz überschreiten, nicht übernommen werden.

Prüffragen:

- Erfolgt der NTP-Abgleich der Sicherheitsgateways ausschließlich mit einem zentralen NTP-Proxyserver?

- Findet eine regelmäßige Plausibilitätsprüfung der empfangenen Zeit-Informationen auf dem NTP-Proxy statt, bevor diese übernommen und weitergegeben werden?
- Werden NTP-Informationen durch einen eigenen NTP-Proxyserver zur Verfügung gestellt, welcher sich regelmäßig mit der Zeitserver-Infrastruktur im Internet oder durch ein Funkuhr-Modul abgleicht?

# M 4.228 Nutzung der Sicherheitsmechanismen von Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Administrator

Smartphones, Tablets oder PDAs und zugehörige Anwendungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Alle Benutzer müssen sich über Wirkung und Grenzen der Sicherheitswerkzeuge im Klaren sein.

### Zugriffsschutz für Smartphone, Tablet oder PDA

Heute besitzen alle mobilen Endgeräte eine Zugriffssicherung, die meistens über eine Passwortabfrage realisiert ist. Auch wenn nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher sind, wie es wünschenswert wäre, sollten sie benutzt werden, solange nichts Besseres vorgegeben ist.

Im Auslieferungszustand der Geräte ist meist die Passwortabfrage deaktiviert und oft ein triviales Passwort voreingestellt. Bei der ersten Benutzung muss daher das Passwort geändert und aktiviert werden, sodass zumindest bei jedem Einschalten des Gerätes eine Passwort-Eingabe erforderlich ist. Für diese Passwörter und PINs sollten dieselben Regeln gelten wie für Passwörter zu sonstigen IT-Systemen (siehe M 2.11 *Regelung des Passwortgebrauchs*). Auf keinen Fall dürfen sie zu kurz oder zu einfach gewählt sein. Die Passwörter dürfen keinesfalls zusammen mit dem Smartphone, Tablet oder PDA aufbewahrt werden.

Viele Smartphones, Tablets oder PDAs lassen sich über die USB-Schnittstelle mit einem PC sehr leicht administrieren und stellen über USB oder sogar die Luftschnittstelle weitreichende Systemfunktionen (sogenannte Debugging-Funktionen) bereit. Diese Schnittstelle muss deaktiviert werden, wenn sie nicht benutzt wird, da sonst ohne Kenntnis des Benutzers Daten ausgelesen oder beliebige Anwendungen installiert oder deinstalliert werden können.

### Automatische Sperre / Pausenschaltung

Smartphones, Tablets oder PDAs sehen im Allgemeinen auch die Möglichkeit einer automatischen Sperre vor, die sich bei Arbeitsunterbrechungen nach kurzer Zeit selbst aktiviert. Erst nach Eingabe des entsprechenden Passwortes ist die weitere Nutzung des Endgerätes möglich. Ist eine Pausenschaltung vorhanden, so sollte sie unbedingt genutzt werden. Der Zugriffsschutz sollte sich bereits nach einer kurzen Phase von Inaktivität einschalten, zu empfehlen sind hier maximal 5 Minuten.

### Benutzer-Information

Damit ein ehrlicher Finder eines Smartphones, Tablets oder PDAs weiß, an wen er sich wenden kann, sollte das Endgerät so eingerichtet werden, dass nach dem Einschalten eine entsprechende Information auf dem Bildschirm erscheint. Bei privat genutzten Smartphones, Tablets oder PDAs sollte hier möglichst nicht die vollständige Privatadresse angegeben werden, damit ein Dieb nicht auch noch diese Information für einen Einbruch bei einer vermuteten Abwesenheit des Benutzers ausnutzen kann. In der Regel reichen der Name und eine E-Mail-Adresse aus. Wenn diese Funktion nicht systemseitig

zur Verfügung steht, sollte eine entsprechende Applikation installiert oder ein eigens gestalteter Sperrbildschirmbild dafür verwendet werden.

**Weitere Sicherheitsmechanismen**

Es gibt viele verschiedene Sicherheitsmechanismen bei Smartphones, Tablets oder PDAs wie Verschlüsselung oder zeitgesteuerte Deaktivierung. Welche hiervon vorhanden sind bzw. wie diese aktiviert werden können, ist abhängig vom eingesetzten Endgerät. Daher sollte die Bedienungsanleitung sorgfältig daraufhin gelesen werden. Sollen auf einem Smartphone, Tablet oder PDA vertrauliche und besonders zu schützende Daten gespeichert werden, so sollten diese verschlüsselt werden. Bietet das Endgerät keine eingebaute Verschlüsselungsfunktion, so sollte ein zusätzliches Verschlüsselungsprodukt eingesetzt werden.

Beim Einsatz von Smartphones, Tablets oder PDAs in Behörden oder Unternehmen empfiehlt es sich, die wichtigsten Sicherheitsmechanismen sowohl vorzukonfigurieren als auch auf einem übersichtlichen Handzettel verständlich für die Benutzer zu dokumentieren. Wenn möglich sollte dieser Zettel auch in elektronischer Form auf dem Endgerät an einer leicht zu findenden Stelle hinterlegt werden.

Prüffragen:

- Verfügen die eingesetzten Smartphones, Tablets oder PDAs über Einschalte-Passwörter? Sind diese aktiviert?

# M 4.229 Sicherer Betrieb von Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die sinnvolle Nutzung von Smartphones, Tablets oder PDAs erfordert im Allgemeinen eine Kopplung mit anderen IT-Systemen, beispielsweise dem Arbeitsplatzrechner, einen Serverdienst für die Geräteverwaltung oder -steuerung oder einen Cloud-Dienst. Die Installation und Konfiguration der dafür benötigten Hard- und Software sollte zentral geregelt sein und durchgeführt werden. Ohne entsprechende Tests und Freigaben sollte keinerlei Installation erfolgen. Bei vielen Smartphones und Tablets ist die Synchronisation mit Cloud-Diensten voreingestellt und erfolgt nahezu automatisch. Es muss verhindert werden, dass ungewollt Daten zu diesen Diensten abfließen. Dies ist insbesondere bei jeder neu installierten Anwendung zu prüfen. Gegebenenfalls sind entsprechende Gegenmaßnahmen zu ergreifen.

Sicherheitsmechanismen und -einstellungen für mobile Endgeräte sollten festgelegt und für die Benutzer verständlich dokumentiert werden, damit sie die Geräte korrekt benutzen können. Daher ist explizit zu verbieten, dass die Konfiguration geändert wird. Außerdem müssen die Benutzer für Sinn und Zweck der gewählten Einstellungen sensibilisiert werden. Soweit technisch möglich, sollten Sicherheitsmechanismen so gewählt und konfiguriert werden, dass die Benutzer möglichst wenig Einflussmöglichkeiten haben. Dies ist in der Regel am einfachsten durch eine zentrale Mobile Device Management-(MDM)Lösung möglich. MDM-Lösungen können Passwortrichtlinien erlassen, Konfigurationen überprüfen, installierte Anwendungen verwalten und den Patch-Stand vom Betriebssystem und der Virenschutz-Software überprüfen. Es wird empfohlen eine MDM-Lösung einzusetzen oder zumindest zu prüfen, ob damit der sichere Betrieb von Smartphones, Tablets und PDAs am effizientesten erreicht wird (siehe auch M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs*).

Smartphones, Tablets und PDAs sind in der Regel nicht in der Lage, verschiedene Benutzerkonten bereitzustellen. Daher gibt es auch im Allgemeinen keine ausgefeilten Mechanismen zur Rollentrennung. Das bedeutet insbesondere, dass es selten Bereiche gibt, die nur für Administratoren zugänglich sind. Benutzer können also nicht ohne Weiteres daran gehindert werden, sicherheitsrelevante Konfigurationsänderungen durchzuführen. Dies kann nur durch entsprechende Regelungen und Sensibilisierung der Benutzer erreicht werden. Hilfreich ist es außerdem, regelmäßig die Einstellungen zu kontrollieren bzw. diese durch Administrationstools bei der Synchronisierung wieder auf die vorgegebenen Werte zurückzusetzen.

Die Sicherheit aller zur Synchronisation mit dem Smartphone, Tablet oder PDA benutzten Endgeräte ist wesentlich für die Sicherheit des jeweiligen mobilen Geräts. Wenn auf den stationären Endgeräten Daten oder Programme manipuliert worden sind, können diese auf das Smartphone, das Tablet oder den PDA durchgereicht werden, ohne dass dies erkannt werden kann.

Die Synchronisationssoftware sollte so konfiguriert werden, dass vor der Installation von Programmen eine Rückfrage beim Benutzer erfolgt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen. Es sollte protokolliert werden, welche Programme und Daten jeweils transferiert bzw. aktuali-

siert wurden und diese Protokolle sollten zumindest sporadisch auf ungewöhnliche Einträge überprüft werden.

Für die Auswahl und Installation von Applikationen ist ein geeignetes Test- und Freigabeverfahren umzusetzen (siehe M 4.467 *Auswahl von Applikationen für Smartphones, Tablets und PDAs*). Werden in einer Behörde oder einem Unternehmen private Smartphones, Tablets oder PDAs dienstlich benutzt, sind solche Verfahren, wenn überhaupt, viel schwieriger umzusetzen.

In der Sicherheitsrichtlinie sollte festgehalten werden, welche Daten und Programme auf den Smartphones, Tablets oder PDAs gespeichert werden dürfen. Davon hängen auch weitere Sicherheitsmaßnahmen ab. Beispielsweise hat ein Tablet, auf dem ausschließlich weniger schützenswerte Daten gespeichert werden, einen anderen Schutzbedarf als ein Endgerät, auf dem kryptografische Schlüssel und Zugangsparameter für IT-Systeme und Netze abgelegt sind.

Es gibt Schadprogramme, die speziell für Smartphones, Tablets oder PDAs konzipiert worden sind. Sie lesen persönliche Daten aus, rufen kostenpflichtige Servicerufnummern an oder versenden SMS-Spam. Einige Schadprogramme sind auch darauf spezialisiert, Authentisierungsinformationen, beispielsweise die mobile TAN für Online-Banking, an Kriminelle weiterzuleiten. Die meisten Hersteller von Viren-Schutzprogrammen haben deswegen Virenscanner für Smartphones, Tablets oder PDAs in die Produktpalette mit aufgenommen. Nicht vergessen werden darf in diesem Zusammenhang auch der Virenschutz aufseiten der zur Synchronisation eingesetzten Endgeräte oder Diensteanbieter. Auch diese müssen mit aktuellen Virenschutz-Programmen ausgestattet sein. Dies muss insbesondere auch für private PCs oder Laptops gelten, mit denen das dienstliche Endgerät eventuell auch synchronisiert wird.

Wenn über Smartphones, Tablets oder PDAs Internet-Dienste genutzt werden, muss jede Datenverbindung zur Institution verschlüsselt werden, beispielsweise durch ein VPN. Zudem sollte der E-Mail-Client und Web-Browser SSL bzw. TSL beherrschen und hierüber auch verschlüsselt kommunizieren, beispielsweise für den Zugriff auf unternehmens- oder behördeninterne Server. Einige der für mobile Endgeräte verfügbaren Browser unterstützen auch aktive Inhalte, also Java, ActiveX und/oder Javascript. Wie bei anderen IT-Systemen ist auch hier zu beachten, dass je nach Art dieser Programme mit ihrem Ausführen eventuell ein Sicherheitsrisiko verbunden sein kann. Daher sollten aktive Inhalte im Web-Browser im Regelfall abgeschaltet sein und nur aktiviert werden, wenn diese aus einer vertrauenswürdigen Quelle kommen, also z. B. von den WWW-Seiten eines ihnen bekannten Anbieters.

Da kleine und mobile Geräte häufig verloren werden, müssen für den Einsatz in einer Institution Bestandsverzeichnisse angelegt werden. Sie sollten mindestens folgende Informationen enthalten: Identifizierungsmerkmale wie Gerätenummern oder Inventarnummern, Art des Gerätes, Betriebssystem, Installationsdatum und Konfigurationsbesonderheiten, Aufstellungsort (wenn stationär), Benutzer sowie Administratoren.

Prüffragen:

- Wird die Installation und Konfiguration von Hard- und Software für die Kopplung von PDAs mit IT-Systemen zentral durchgeführt und geregelt?
- Existiert eine verständliche PDA-Sicherheitsrichtlinie für Benutzer?
- Gibt es ein Test- und Freigabeverfahren für PDA-Applikationen?
- Wird die PDA-Synchronisation protokolliert und sporadisch überprüft?

- Sind PDAs und die zur Synchronisation eingesetzten PCs mit aktuellen Virenschutz-Programmen ausgestattet?
- Gibt es ein PDA-Bestandsverzeichnis?

# M 4.230 Zentrale Administration von Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Administration mobiler Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Mit solchen Tools können dann beispielsweise zentrale Vorgaben an die Passwortgestaltung umgesetzt oder auch der Zugriffsschutz beim Synchronisationsvorgang verbessert werden. Daher sollte ein solches Mobile Device Management (MDM)-Tool eingesetzt werden.

Grundsätzlich ist eine gut überlegte Einbindung in die vorhandene IT-Umgebung notwendig, um die Benutzer durch den Komfort eines MDM-Tools davon abzuhalten, unkontrollierte und damit potenziell unsichere Smartphones, Tablets oder PDAs in die Unternehmens-IT einzuschleppen. Durch eine zentrale Administration können nicht nur Software und Informationen verteilt, sondern auch die organisationseigenen Sicherheitsrichtlinien durchgesetzt werden, z. B. für Authentikation, Zugriff oder Datensicherung.

Beim Einsatz eines MDM-Tools werden Smartphones, Tablets oder PDAs typischerweise nicht mehr mit einem lokalen Endgerät synchronisiert, sondern mit einem Server. Daher können Daten dann nicht nur von einer Station aus abgeglichen werden, sondern von allen mit dem Server verbundenen Geräten. Diese Synchronisation muss kryptografisch abgesichert sein. In vielen Fällen werden die Daten nicht mehr kabelgebunden, sondern per Funktechnik, z. B. über ein WLAN, synchronisiert. Daher sollte beispielsweise darauf geachtet werden, dass hierfür nur kryptografisch abgesicherte WLANs verwendet werden. Ist die Leitung jedoch durch eine verschlüsselte VPN-Verbindung geschützt, kann auch über ein nicht gesichertes WLAN (z. B. in Cafés oder Hotels) synchronisiert werden.

Bei der Synchronisation über einen Server lassen sich aber auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen Mobile Device Management sind unter anderem:

- Über Personal Information Manager (PIM) können Termine verwaltet und Adressbücher geführt werden, und dies nicht nur für einzelne Benutzern, sondern auch für Arbeitsgruppen. Das Management der PIM-Daten, anderer Informationen und der Applikationen, die auf den diversen Endgeräten vorhanden sein sollen, kann zentral gesteuert werden. Dadurch können z. B. Applikationen remote installiert und konfiguriert werden.
- Es können aber auch zentrale Adressen-Sammlungen und andere Daten gepflegt und weitergegeben werden. Dies erleichtert besonders bei einer Vielzahl von mobilen Mitarbeitern, die unterwegs eingepflegten Daten den anderen Mitarbeitern schnell und komfortabel zur Verfügung zu stellen.
- Daten können zentral gesichert werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso kann vorgegeben werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.
- Auch Rückmeldungen über den Status der Smartphones, Tablets oder PDAs sind möglich, sodass Diagnosen aus der Ferne durchgeführt werden können.

- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich organisationsspezifisch einstellbare Passwortregeln und andere Sicherheitsregeln vorgeben.
- Wenn die MDM-Lösung für verschiedene Benutzungskontexte, wie z. B. privat und dienstlich, ausgelegt ist (siehe M 4.468 *Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs*), kann sie beide Bereiche voneinander trennen. Dies geschieht vielfach über eine Container-Lösung, bei der im Container eine Verwaltung privater PIM-Daten möglich ist oder sogar Anwendungen installiert werden können.
- Viele MDM-Lösungen bieten auch spezielle Maßnahmen für den Fall an, dass das Endgerät verloren geht. So können Smartphones und Tablets mit solchen Programmen aus der Ferne gelöscht, gesperrt und lokalisiert werden. Diese Funktionen sollten von der zentralen Stelle, bei der der Verlust des Endgerätes gemeldet wird, in Absprache mit dem Benutzer und nach vorher klar definierten Regeln ausgeführt werden (siehe M 2.306 *Verlustmeldung* und M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*).

Diese Funktionen können im Allgemeinen nicht nur über die bei älteren Geräten oft gebräuchlichen Dockingstationen, sondern auch über andere Schnittstellen wie WLAN oder Bluetooth angeboten werden.

Ein Tool zum zentralen Management von Smartphones, Tablets und PDAs sollte möglichst alle in der Organisation eingesetzten Betriebssysteme dieser mobilen Endgeräte unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt natürlich für die eingesetzte Groupware und E-Mail-Plattform.

Prüffragen:

- Werden Tools für das zentrale PDA-Management eingesetzt?

# M 4.231 Einsatz zusätzlicher Sicherheitswerkzeuge für Smartphones, Tablets oder PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Es gibt diverse Zusatzwerkzeuge, mit denen die Sicherheit von PDAs verbessert werden kann. Diese bieten erweiterte Sicherheitsfunktionen wie beispielsweise

- Verschlüsselung des Dateisystems und der Speicherkarteninhalte oder auch nur einzelner Dateien oder Datenbanken,
- Verbesserung der Authentisierung, z. B. durch einfachere oder sicherere Authentisierungsverfahren,
- Absicherung der Verbindung zu anderen Komponenten, z. B. durch Verschlüsselung der Kommunikation oder durch Erzeugung von Einmalpasswörtern für die Anmeldung über externe IT-Systeme,
- Virenschutz und
- Verhinderung des unautorisierten Zugriffs auf das Gerät.

Dadurch kann die PDA-Sicherheit bis zu einem gewissen Grad erhöht werden. Dafür müssen die Benutzer die erweiterten Sicherheitsmechanismen aber auch genau kennen. Sie sollten zum einen über deren Nutzen und Schwächen informiert sein und zum anderen über deren Handhabung. Generell sollte aber allen Anwendern klar sein, dass es nahezu unmöglich ist, auf einer unsicheren Plattform mit schwachen Sicherheitsmechanismen eine zuverlässig sichere Applikation zu implementieren. Für viele der PDA-Sicherheitsprodukte sind schon Warnmeldungen über Sicherheitslücken herausgegeben worden. Auch mit der verfügbaren Zusatz-Sicherheitssoftware für PDAs werden nur einige, aber nicht alle vorhandenen Sicherheitsprobleme beim PDA-Einsatz behoben.

Trotzdem sollte geprüft werden, inwieweit solche Tools für den jeweiligen Einsatzzweck sinnvoll sind, da sie helfen, das Gefährdungspotential zu senken. Der Einsatz solcher Tools ist vor allem dann anzuraten, wenn PDAs als Sicherheitstoken oder für die Speicherung sensibler Daten eingesetzt werden. So gibt es beispielsweise Tools zur Verbesserung des Zugriffsschutzes, zur Verschlüsselung einzelner Dateien oder des gesamten Systems und für eine zentrale Administration.

Prüffragen:

- Wurde geprüft, ob der Einsatz zusätzlicher Sicherheitswerkzeuge für PDA sinnvoll ist?
- Werden die Benutzer im Umgang mit den zusätzlichen Sicherheitswerkzeugen geschult?

# M 4.232 Sichere Nutzung von Zusatzspeicherkarten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Da bei mobilen Endgeräten wie PDAs der vorhandene Speicherplatz beschränkt ist, können die meisten Modelle mit externen Speichermedien erweitert werden. Verbreitet sind hierfür Speicherkarten, z. B. SD-, MMC oder auch Compact Flash Cards, die den Vorteil haben, schnell gewechselt werden zu können. Diese Karten benötigen keine Batterie zur Datenspeicherung, wodurch der Verlust der gespeicherten Daten durch Strommangel wegfällt. Sie eignen sich dadurch auch, um unterwegs Backups durchzuführen, was vor allem dann sinnvoll ist, wenn ein PDA-Benutzer häufig lange abwesend ist. Wie generell für Datensicherungen gilt auch hier, dass diese sicher verwahrt werden müssen. Wenn die Memory-Cards im PDA oder anderswo unbeaufsichtigt zurückgelassen werden können, können Unbefugte diese benutzen, um die darauf gespeicherten Daten auszulesen. Dies geht mit einem Laptop und einem geeigneten Adapter im Handumdrehen. Wenn anschließend die Memory-Card wieder zurückgelegt wird, werden dabei nicht einmal Spuren hinterlassen.

Um die Daten auf externen Speicherkarten zu schützen, ist es empfehlenswert, diese mit entsprechenden Zusatztools zu verschlüsseln. Solange dies nicht der Fall ist, sollten die Speicherkarten auch unterwegs immer beaufsichtigt werden.

Prüffragen:

- Werden Zusatzspeicherkarten sicher aufbewahrt?

# M 4.233 Sperrung nicht mehr benötigter RAS-Zugänge

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.322 *Sperrung nicht mehr benötigter VPN-Zugänge* integriert.

# M 4.234 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Mitarbeiter

IT-Systeme und Datenträger sind dem ständigen Wandel der Technik unterworfen. Daher werden sie häufiger ausgetauscht als viele andere Arbeitsmaterialien. Bevor IT-Systeme oder Datenträger außer Betrieb genommen werden, muss geklärt werden, wie dies ablaufen soll und wie mit den darauf gespeicherten Informationen umzugehen ist. Es muss vor allem sichergestellt werden, dass weder wichtige Daten, die eventuell auf diesen gespeichert sind, verloren gehen, und noch dass vertrauliche Daten auf den Datenträgern zurück bleiben.

Bevor IT-Systeme oder Datenträger ausgesondert werden, müssen sie gesichtet werden, ob sich darauf noch Daten befinden, die noch benötigt werden. Diese müssen dann auf anderen Datenträgern gesichert bzw. archiviert werden. Es sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.

Bei der Außerbetriebnahme eines IT-Systems sollte außerdem geprüft werden, ob noch Datensicherungsmedien vorhanden sind, die während seines Betriebs benutzt wurden. Auch diese müssen gelöscht oder unbrauchbar gemacht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.

Danach muss geklärt werden, ob die IT-Systeme oder Datenträger vernichtet oder an Dritte weitergegeben werden sollen. Häufig werden IT-Systeme nach der Aussonderung weiterverwendet, beispielsweise können ausrangierte IT-Systeme an andere Abteilungen weitergegeben werden, an Mitarbeiter verschenkt oder verkauft werden. Außerdem muss geregelt werden, wie darauf gespeicherte Informationen entweder zur weiteren Verwendung gesichert oder zuverlässig entfernt werden.

Falls Datenträger an Externe weitergegeben werden sollen, müssen diese sicher überschrieben werden. Auch wenn auf den ersten Blick keine schützenswerten Informationen mehr vorhanden sind, können die Daten unzureichend gelöscht worden sein, so dass noch Restinformationen zu finden sind. Es muss sichergestellt sein, dass alle Daten und Anwendungen vorher sorgfältig gelöscht wurden (siehe auch M 2.433 *Überblick über Methoden zur Löschung und Vernichtung von Daten*).

Wurden auf dem Datenträger Daten mit hohem Schutzbedarf gespeichert, führen die Verfahren, um diese Daten zuverlässig zu löschen, häufig zur physikalischen Zerstörung der Datenträger.

Bei der Regelung der Außerbetriebnahme von IT-Systemen und Datenträgern dürfen auch die Geräte nicht vergessen werden, die nicht unbedingt als IT-Systeme wahrgenommen werden, aber eine Vielzahl vertraulicher Daten enthalten können, wie Mobiltelefone, Drucker, Kopierer oder Faxgeräte. Beispielsweise sollte bei Weitergabe oder Verkauf von Faxgeräten darauf geachtet werden, dass die internen Speicher für Telefaxverbindungsdaten und Telefaxin-

halte sicher gelöscht werden. Außerdem sollten alle Kennzeichnungen und Aufkleber von den Geräten und Datenträgern entfernt werden, die Hinweise auf deren vorigen Verwendungszweck geben, wie beispielsweise Etiketten mit IP-Adressen und Rechnernamen.

Ebenso müssen auch die IT-Systeme und Speichermedien sicher gelöscht und entsorgt werden, deren Betrieb und/oder Wartung ausgelagert wurde. Deren sichere Außerbetriebnahme inklusive Entsorgung oder Rückgabe muss in den entsprechenden Verträgen geregelt sein.

Die Vorgehensweise für die Außerbetriebnahme von IT-Systemen und Datenträgern innerhalb der Institution muss nachvollziehbar dokumentiert sein. Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme von IT-Systemen abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden. Es empfiehlt sich, dass die einzelnen Schritte vom jeweils Zuständigen schriftlich bestätigt werden.

Prüffragen:

- Existiert eine klar definierte Vorgehensweise zur Außerbetriebnahme von IT-Systemen und Datenträgern?
- Werden bei allen Arten von IT-Systemen und Datenträgern vor einer Aussonderung alle gespeicherten Daten sorgfältig gelöscht?
- Wird die geregelte Außerbetriebnahme von IT-Systemen und Datenträgern innerhalb der Institution nachvollziehbar dokumentiert?

# M 4.235 Abgleich der Datenbestände von Laptops

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Wenn ein Laptop unterwegs eingesetzt wird, ist es wichtig, alle erforderlichen Daten und Anwendungen in der aktuellsten Version verfügbar zu haben. Ebenso sollten unterwegs bearbeitete Daten zügig auf IT-Systemen innerhalb des IT-Verbunds der Behörde bzw. des Unternehmens gespeichert werden, damit es nicht zu inkonsistenten Datenbeständen kommt. Der einfachste Weg hierfür ist der regelmäßige Abgleich der Datenbestände von Laptops, beispielsweise über Tools zur Synchronisation von Dateien und Verzeichnissen zwischen Laptops und Arbeitsplatzrechnern oder Servern.

Dafür sollte überlegt werden, welche Informationen an welchen Stellen gespeichert sind, also auf welchen Servern und in welchen Verzeichnissen. Bei der ersten Sichtung zeigt sich meist, an wie vielen verschiedenen Stellen in einem IT-Verbund sich die für einen Arbeitsplatz relevanten Informationen befinden.

Damit Synchronisationsvorgänge nicht zu lange dauern, sollten dafür Tools ausgewählt werden,

- über die Dateien und Verzeichnisse nach vorher festgelegten Kriterien automatisch abgeglichen und aktualisiert werden können,
- die über Filtermöglichkeiten komplette Verzeichnisse oder auch einzelne Dateien von einem Kopiervorgang ausschließen können,
- die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.

Synchronisationstools sollten außerdem möglichst benutzerfreundlich sein und trotzdem einen guten Schutz vor fehlerhafter Bedienung gewährleisten. Synchronisationsvorgänge sollten zugriffsgeschützt sein, bei Laptops kann dies über bereits vorhandene Zugriffsschutz-Verfahren erfolgen.

Damit über die Synchronisation keine Manipulationen vorgenommen werden können, sollten die Benutzer regelmäßig die relevanten Verzeichnisse daraufhin inspizieren, ob sich dort ihnen unbekannte Dateien befinden. Die Synchronisationssoftware sollte so konfiguriert werden, dass vor der Installation von Programmen eine Rückfrage beim Benutzer erfolgt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen, auch die Informationen, welche Dateien jeweils transferiert werden, können entscheidende Hinweise enthalten. Die Synchronisation sollte protokolliert werden. Die Synchronisationsprotokolle sollten dann regelmäßig zumindest überflogen werden, um festzustellen, ob unbefugte Synchronisationsvorgänge stattgefunden haben.

Prüffragen:

- Gibt es eine geregelte Vorgehensweise für die Übernahme von Daten mobiler IT-Systeme in den Informationsverbund der Institution?
- Bei Anwendung eines Synchronisationstools: Können Synchronisationskonflikte aufgelöst werden?
- Bei Anwendung eines Synchronisationstools: Wird der Synchronisationsvorgang protokolliert?
- Bei Anwendung eines Synchronisationstools: Sind die Benutzer angewiesen, die Synchronisationsprotokolle zu prüfen?

# M 4.236 Zentrale Administration von Laptops

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Administration für mobile Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Durch eine zentrale Administration können nicht nur Software und Informationen verteilt, sondern auch die organisationseigenen Sicherheitsrichtlinien durchgesetzt werden, z. B. für Authentisierung, Zugriff oder Datensicherung.

Beim Einsatz von Software zum zentralen Laptop-Management erfolgt die Synchronisation der Laptops dann typischerweise nicht mehr mit einem lokalem Endgerät, sondern mit einem Server. Daher können Daten dann nicht nur von einer Station aus abgeglichen werden, sondern von allen mit dem Server verbundenen.

Bei der Synchronisation über einen Server lassen sich aber auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen Laptop-Management sind unter anderem:

- Datensicherungen können zentral durchgeführt werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso können Vorgaben gemacht werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.
- Es besteht die Möglichkeit, Rückmeldungen über den Status der Laptops zu erhalten und Diagnosen remote durchführen zu können.
- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich organisationsspezifisch einstellbare Passwortregeln und andere Sicherheitsregeln vorgeben.

Ein Tool zum zentralen Laptop-Management sollte möglichst alle in der Organisation eingesetzten Laptop-Betriebssysteme unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt ebenso natürlich für die eingesetzte Groupware und E-Mail-Plattform.

Prüffragen:

- Existiert eine geeignete Vorgehensweise für die zentrale Administration von Laptops?

# M 4.237 Sichere Grundkonfiguration eines IT-Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Grundeinstellungen, die vom Hersteller oder Distributor eines Betriebssystems vorgenommen werden, sind meist nicht auf Sicherheit optimiert, sondern auf eine einfache Installation und Inbetriebnahme sowie oft darauf, dass jeder Anwender möglichst einfach auf möglichst viele Features des Betriebssystems zugreifen kann. Beim Einsatz von IT-Systemen (egal, ob als Client oder Server) in Behörden oder Unternehmen ist dies oft nicht wünschenswert.

Der erste Schritt bei der Grundkonfiguration muss daher sein, die Grundeinstellungen zu überprüfen und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie anzupassen. Die Grundkonfiguration ist naturgemäß relativ stark vom eingesetzten Betriebssystem abhängig. Aus diesem Grund sind in den betriebssystemspezifischen Bausteinen entsprechende detailliertere Maßnahmen enthalten.

Ziele einer sicheren Grundkonfiguration sollten sein, dass

- das System gegen "einfache" Angriffe über das Netz abgesichert ist,
- kein normaler Benutzer durch reine Neugierde oder gar zufällig Zugriff auf sensitive Daten erlangen kann, die nicht für ihn bestimmt sind,
- kein normaler Benutzer beim normalen Arbeiten mit dem System durch reine Bedienungsfehler oder Leichtsinn ("Was passiert eigentlich, wenn ich diese Datei lösche?") schwerwiegenden Schaden am System oder an Daten anderer Benutzer verursachen kann, und dass
- auch für die Arbeiten der Systemadministratoren die Auswirkungen kleinerer Fehler so weit wie möglich begrenzt sind.

Die Einstellungen, die im Rahmen der Grundkonfiguration überprüft und angepasst werden sollten, betreffen insbesondere die folgenden Bereiche:

- Einstellungen für Systemadministratoren
  Die Kennungen, unter denen Systemadministratoren arbeiten, sollten besonders stark abgesichert werden.. Dies betrifft beispielsweise die Einstellungen für die Benutzerumgebung wie
- Suchpfade für Programme und Dateien,
- Umgebungsvariablen und die
- Konfiguration bestimmter Programme.
  Diese Einstellungen sollten überprüft und gegebenenfalls angepasst werden. Außerdem sollten die Einstellungen für die Benutzerverzeichnisse von Systemadministratoren so gewählt werden, dass normale Benutzer keinen Zugriff darauf haben.
- Einstellungen für die Systemverzeichnisse und -dateien
  Bei der Grundkonfiguration muss überprüft werden, ob die Berechtigungen für Systemverzeichnisse und -dateien den Vorgaben der Sicherheitsrichtlinie entsprechen. Auf einem Server sollten für die Berechtigungen der Systemverzeichnisse und -dateien relativ restriktive Einstellungen gewählt werden.
- Einstellungen für Benutzerkonten
  Im Rahmen der Grundkonfiguration sollte überprüft werden, welche Standardeinstellungen für Benutzerkonten gelten. Die Einstellungen müssen gegebenenfalls entsprechend der Sicherheitsrichtlinie angepasst werden. Dies betrifft im Wesentlichen dieselben Parameter wie für Systemadmini-

strator-Konten, für normale Benutzer können aber unter Umständen andere Einstellungen sinnvoll sein.

- Bereinigung der Benutzerdatenbank
  Oft wird im Rahmen der Standardinstallation eines Betriebssystems eine größere Anzahl von Benutzerkonten eingerichtet, die für den Betrieb nicht in jedem Fall notwendig sind. Daher sollte im Rahmen der Grundkonfiguration geprüft werden, welche Benutzerkonten wirklich gebraucht werden. Nicht benötigte Benutzerkonten sollten entweder gelöscht oder zumindest so deaktiviert werden, so dass unter dem betreffenden Konto keine Anmeldung am System möglich ist.
- Überprüfung der Dienste
  Die Standardinstallation eines Betriebssystems enthält oft eine Reihe von Programmen und Diensten, die normalerweise nicht benötigt werden und die gerade deswegen eine Quelle von Sicherheitslücken sein können. Dies gilt insbesondere für Netzdienste. Nach der Installation sollte deswegen überprüft werden, welche Dienste auf dem System installiert und aktiviert sind. Nicht benötigte Dienste sollten deaktiviert oder ganz deinstalliert werden.
  Die Überprüfung auf laufende Dienste kann einerseits lokal mit den Mitteln des installierten Betriebssystems und bei Netzdiensten andererseits von außen durch einen Portscan von einem anderen System aus erfolgen. Durch eine Kombination beider Methoden kann weitgehend ausgeschlossen werden, dass das System noch weitere ungewollte Netzdienste anbietet.
- Einstellungen für den Zugriff auf das Netz
  Im Rahmen der Grundkonfiguration sollten auch die Einstellungen für den Zugriff auf das Netz sowie wichtige externe Dienste getroffen und dokumentiert werden. Dies betrifft beispielsweise (sofern nicht bereits bei der Installation geschehen):
- Vergabe der IP-Adresse und Konfiguration der grundlegenden Netzparameter oder Konfiguration des Zugriffs auf einen Server, der automatisch, beispielsweise über DHCP (Dynamic Host Configuration Protocol) Netzeinstellungen verteilt. Für Server wird allerdings von der Verwendung von DHCP abgeraten.
- Konfiguration des Zugriffs auf einen DNS-Server und gegebenenfalls andere Namensdienste und die
- Konfiguration des Zugriffs auf verteilte Dateisysteme, Datenbanken oder sonstige externe Dienste.
- Zusätzlicher Schutz durch einen lokalen Paketfilter
  Server und Clients mit hohem Schutzbedarf sollten zusätzlich zum Schutz durch die organisationsweiten Sicherheitsgateways oder Paketfilter, die das interne Netz segmentieren, mit einem lokalen Paketfilter oder einer Personal Firewall abgesichert werden. Entsprechende Funktionalitäten sind in praktisch allen modernen Betriebssystemen vorhanden.
  Im Rahmen der Grundkonfiguration sollte zumindest für Server mit hohem Schutzbedarf ein entsprechender Schutz durch einen lokalen Paketfilter realisiert werden. Auch für Server mit normalem Schutzbedarf wird der Schutz durch einen lokalen Paketfilter empfohlen. Gegebenenfalls kann in diesem Fall eine "liberalere" Konfiguration gewählt werden.
  Für Clients wird der Einsatz eines lokalen Paketfilters oder einer Personal Firewall dann empfohlen, wenn diese einen hohen oder sehr hohen Schutzbedarf im Bezug auf die Vertraulichkeit oder Integrität besitzen.
  Genauere Informationen zur Einrichtung eines lokalen Paketfilters finden sich in M 4.238 *Einsatz eines lokalen Paketfilters*, zu einer Personal Firewall in M 5.91 *Einsatz von Personal Firewalls für Clients* .
- Deaktivierung von "Call Home"-Funktionen

Einige Betriebssysteme und Anwendungen senden Informationen, beispielsweise über aufgetretene Fehler oder über die Systemkonfiguration , direkt an den Hersteller, damit dieser zukünftig das Produkt an die Bedürfnisse der Anwender anpassen kann. Hierfür wird eine Datenverbindung über Datennetze, wie dem Internet, zu den Servern des Herstellers aufgebaut. Eine solche Form des Datenabflusses kann kritisch sein, vor allem, wenn die Anwender nicht über die Häufigkeit und Inhalte der Datenweitergabe informiert werden.

Generell sollte dieser oft unerwünschte Informationsaustausch unterbunden werden. Ob und wie Informationen versendet werden, kann in der Regel den Lizenzvereinbarungen der eingesetzten Software entnommen werden.

Viele Applikationen bieten die Möglichkeit, diese "Call Home"-Funktion zu deaktivieren. Nur in begründeten Ausnahmefällen sollte diese aktiviert bleiben. Nach Updates sollte überprüft werden, ob die "Call Home"-Funktion weiterhin deaktiviert ist.

Durch lokale Paketfilter oder dem zentralen Sicherheitsgateway (Firewall) kann ebenfalls der Verbindungsaufbau mit dem Hersteller unterbunden werden. Beispielsweise könnten auf Grundlage der Zieladressen oder der Portnummern die Datenverbindungen abgewiesen werden. Hierbei ist zu beachten, dass die Berücksichtigung aller Applikationen aufwändig ist und automatische Update-Funktionen, falls benötigt, dann oft nicht mehr zur Verfügung stehen.

- Deaktivieren nicht benötigter Schnittstellen

  In einer Grundkonfiguration sind üblicherweise alle vorhandenen oder auch potentiell nachrüstbaren Schnittstellen aktiviert. Häufig werden nicht alle davon benötigt und sollten daher entfernt oder deaktiviert werden. Einige dieser Schnittstellen können auch potentielle Sicherheitsprobleme mit sich bringen, denen durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden muss. Schnittstellen, deren Nutzung kontrolliert werden sollte, sind beispielsweise Bluetooth, WLAN, Firewire, eSATA (externer SATA-Festplattenanschluss) und IrDA (Infrared Data Association). Was dabei zu beachten ist, findet sich in den entsprechenden Maßnahmen.
- Verzeichnisbasierte Ausführungskontrolle

  Bei aktuellen Betriebssystemen ist eine verzeichnis- oder partitionsbasierte Ausführungskontrolle möglich. Dabei werden die Ausführungsrechte für alle Dateien in einem Verzeichnis und allen Unterverzeichnissen unterbunden. Beispielsweise kann dies auf windowsbasierten Betriebssystemen durch entsprechende Gruppenrichtlinien mit "Richtlinien für Softwareeinschränkung" erreicht werden. Auf Linux-Systemen kann die Festplatte zweckdienlich partitioniert und mit passenden mount-Optionen "ro" (read only) und "noexec" (no execute) eingebunden werden. Für hohen Schutzbedarf existieren darüber hinaus Werkzeuge, die dateibezogene Berechtigungen im Betriebssystem festlegen.

  Die verzeichnis- oder partitionsbasierte Ausführungskontrolle sorgt bei geeigneter Konfiguration dafür, dass Benutzer
  - aus Verzeichnissen, in die sie schreiben dürfen, keine Programme starten können und
  - in Verzeichnisse, aus denen sie Anwendungen starten dürfen, nicht schreiben können.

  Dadurch wird es Benutzern erschwert, eine Programmdatei auszuführen, die sie aus dem Internet geladen oder von einem USB-Stick kopiert haben.
- Monitoring

  Um auf kritische Systemereignisse reagieren zu können, können diese durch Monitoring beobachtet werden. Hierfür werden in der Regel Statusinformationen von einem zentralen IT-System abgerufen, auf dem die Er-

eignisse ausgewertet werden. Über die Schnittstelle, die benötigt wird, um die Systemereignisse vom IT-System abzurufen, können aber oft Systemeinstellungen des Betriebssystems verändert werden, z. B. über SNMP (Simple Network Management Protocol). Ist eine solche Modifikation nicht gewünscht, dann sollten diese Merkmale deaktiviert werden.

- Schutz vor Buffer Overflows
  Um Betriebssystem und Applikation vor möglichen Buffer Overflows zu schützen, sollten entsprechende Speicherschutzmechanismen aktiviert werden, sofern diese von der verwendeten Hardware (CPU) und dem Betriebssystem unterstützt werden. Beispielsweise kann mit Executable Space Protection (ESP) verhindert werden, dass Programme aus nicht dafür zugelassenen Bereichen des Arbeitsspeichers ausgeführt werden.
- Anlegen einer Integritätsdatenbank
  Nach Abschluss der Grundkonfiguration wird empfohlen, mit einem entsprechenden Tool eine Integritätsdatenbank anzulegen. Bei manchen Betriebssystemen gehören entsprechende Programme bereits zum Umfang einer Standardinstallation. Die Integritätsdatenbank sollte nicht auf dem System selbst, sondern auf einem schreibgeschützten Datenträger (beispielsweise CD-R) oder einem anderen, besonders gesicherten System gespeichert werden. Bei einem Verdacht auf eine Kompromittierung des Systems lassen sich anhand der erzeugten Prüfsummen Dateien identifizieren, die von einem Angreifer modifiziert wurden. Bei den regelmäßigen Überprüfungen der Systemintegrität (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*) dient diese Datenbank als Referenz für einen definierten, sicheren Zustand des Systems.

Es sollte dokumentiert werden, welche Einstellungen im Rahmen der Grundkonfiguration überprüft wurden, sowie ob und gegebenenfalls wie sie geändert wurden. Die Dokumentation muss so beschaffen sein, dass im Notfall auch eine andere Person als der eigentliche Administrator ohne vorherige Kenntnis des Systems anhand der Dokumentation nachvollziehen kann, was getan wurde. Im Idealfall sollte es möglich sein, alleine mit Hilfe der Dokumentation das System wiederherzustellen.

Prüffragen:

- Wird eine sichere Grundkonfiguration aller eingesetzten IT-Systeme entsprechend den Vorgaben der Sicherheitsrichtlinie vorgenommen?
- Wurden nicht benötigte Benutzerkonten, Dienste und Schnittstellen deaktiviert oder entfernt?

# M 4.238 Einsatz eines lokalen Paketfilters

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das gesamte Netz einer Organisation sollte durch ein entsprechendes Sicherheitsgateway geschützt sein. Server, die Dienste nach außen hin anbieten, sollten in einer Demilitarisierten Zone (DMZ) aufgestellt werden. Trotzdem ist es empfehlenswert, auch auf jedem Rechner entsprechende Zugriffsbeschränkungen auf Anwendungs- oder Netzebene einzurichten. Dies gilt auch für Server, die nur intern genutzt werden und nicht zuletzt auch für Clients.

Ein lokaler Paketfilter kann einen Rechner gegen Angriffe schützen, die aus dem selben Subnetz heraus gestartet werden. Außerdem kann ein solcher Paketfilter dazu benutzt werden, eine feiner abgestufte Zugriffskontrolle für einzelne Dienste zu realisieren, als dies beispielsweise mit Paketfiltern nur an Netzübergängen möglich ist.

Darüber hinaus kann ein lokaler Paketfilter auch dazu benutzt werden, ausgehende Netzverbindungen zu beschränken und so die Folgen einer Kompromittierung des Systems zu begrenzen. Ein solcher Schutz kann zwar eventuell von einem Angreifer nach einer erfolgreichen Kompromittierung des Rechners deaktiviert werden, andererseits wird ein Angreifer auf diese Weise zumindest behindert. Auf diese Weise kann entscheidende Zeit bei der Entdeckung und für mögliche Reaktionen gewonnen werden.

Zuletzt kann die Protokollfunktion eines lokalen Paketfilters es ermöglichen, bestimmte Angriffe überhaupt zu entdecken.

Praktisch alle aktuellen Betriebssysteme bieten die Möglichkeit, Filter zu definieren, die alle empfangenen oder zu sendenden Pakete nach bestimmten Regeln untersuchen und behandeln. Die Filtermöglichkeiten unterscheiden sich dabei zwischen den einzelnen Betriebssystemen teilweise erheblich. Praktisch immer können jedoch Regeln basierend auf der Quell- und Zieladresse des Pakets sowie auf dem verwendeten Protokolltyp (TCP/IP, UDP/IP, ICMP etc.) sowie gegebenenfalls dem Quell- oder Zielport definiert werden. Mit Hilfe von Paketfilterregeln können so beispielsweise Pakete, die von bestimmten Rechnern oder aus bestimmten Subnetzen stammen, gezielt verworfen werden.

Manche Serveranwendungen besitzen eigene Mechanismen, um den Zugriff auf den Dienst für einzelne IP-Adressen oder Adressbereiche zu erlauben oder zu verbieten. Gegenüber diesen Mechanismen hat ein lokaler Paketfilter auf Betriebssystemebene den Vorteil, dass er den Dienst selbst gegen mögliche Angriffe schützt, die zu einer Kompromittierung führen, bevor die eingebaute Zugriffsbeschränkung überhaupt wirksam werden kann.

Prinzipiell sollten alle Server mit hohem Schutzbedarf mit einem lokalen Paketfilter geschützt werden.

Es gibt zwei allgemeine Strategien, mit der Paketfilter-Regeln implementiert werden können: Die Blacklist-Strategie erlaubt alle Arten von Verbindungen, die nicht bestimmte Ausschlusskriterien erfüllen (Freizügige Strategie: "Alles ist erlaubt, was nicht explizit verboten ist"). Der Vorteil liegt dabei in einem

eventuell geringeren Aufwand bei der Administration und der Fehlersuche. Ein schwerwiegender Nachteil ist jedoch, dass vergessene Regeln, die den Zugriff auf nicht geschützte Netzdienste ermöglichen, als Grundlage für einen Angriff dienen können.

Demgegenüber werden bei der Whitelist-Strategie alle Arten von Verbindungen blockiert, die nicht zu einer Liste erlaubter Dienste gehören (Restriktive Strategie: "Alles ist verboten, was nicht explizit erlaubt ist").

Die Whitelist-Strategie bietet die größere Sicherheit und sollte daher grundsätzlich verwendet werden, wenn nicht wichtige Gründe dagegen sprechen. Der Nachteil liegt in einem tendenziell höheren Administrationsaufwand, da bei jeder Änderung der Anforderungen neue Regeln definiert werden müssen. In Ausnahmefällen, beispielsweise wenn ein Protokoll nicht auf fest definierten Ports arbeitet, kann auf die Blacklist-Strategie zurückgegriffen werden.

Es ist empfehlenswert, auf allen Servern im Rahmen der Grundkonfiguration einen lokalen Paketfilter mit einem Basis-Regelwerk einzurichten, bei dem grundsätzlich alle Verbindungsanfragen von außen abgewiesen werden. Dieses Regelwerk sollte aktiv sein, wenn das System ans Netz angeschlossen wird. Je nachdem welche Dienste von dem System angeboten werden sollen, können nach deren Konfiguration die dafür benötigten Protokolle und Ports freigeschaltet werden. Auch für Clients sollte dieses Vorgehen zumindest dann in Betracht gezogen werden, wenn diese besondere Anforderungen an die Sicherheit stellen.

Paketfilter erlauben meist ein detailliertes Protokollieren des Netzverkehrs. Das Aufsetzen eines lokalen Paketfilters ist daher auch in sicheren Netzen, die mit einem Sicherheitsgateway von einem unsicheren Netz wie dem Internet getrennt sind, sinnvoll, denn gewonnen Informationen können für die Erkennung von Angriffen hilfreich sein. Allerdings muss dabei darauf geachtet werden, dass keine Datenschutzbestimmungen verletzt werden. Gegebenenfalls sollten die entsprechenden Stellen (Datenschutzbeauftragter, Belegschaftsvertretung oder andere) beteiligt werden.

**Problem ICMP**

Das *Internet Control Message Protocol* ICMP wird dazu verwendet, Nachrichten über Fehler bei der Übertragung von IP-Paketen zu übermitteln. Beispielsweise existieren Nachrichten, die dem Sender eines Pakets mitteilen, dass das Zielnetz nicht erreichbar ist oder dass das Paket zu groß war, um an das Zielsystem weitergeleitet zu werden. Die Funktion der Tools *ping* und *traceroute* beruhen ebenfalls auf ICMP.

Neben vielen nützlichen Eigenschaften gibt es jedoch einige ICMP-Nachrichtentypen, mit denen Angreifer sich wichtige Informationen über ein Netz verschaffen und diese direkt für Angriffe benutzen können. Leider ist der radikale Ansatz, ICMP grundsätzlich am Sicherheitsgateway zu blockieren, ebenfalls keine befriedigende Lösung, da bestimmte Funktionen dann nicht mehr verfügbar sind. Auf *ping* und *traceroute* kann zwar in der Regel auf normalen Arbeitsplatzrechnern und Servern verzichtet werden, eine globale Blockierung von ICMP kann aber zu Beeinträchtigungen führen, die schwer zu diagnostizieren sind. Daher sollte überlegt werden sowohl am Sicherheitsgateway, als auch beim lokalen Paketfilter eine selektive ICMP-Filterung vorzunehmen, sofern dieser die entsprechenden Möglichkeiten zur Verfügung stellt. Dies sollte stets unter der Berücksichtigung des Einsatzzweckes des Rechners (Server oder Arbeitsplatzrechner), dessen Schutzbedarfs und die am Sicherheitsgateway getroffenen Maßnahmen geschehen. Beispielsweise kann für das interne

Netz eine größere Zahl von Nachrichtentypen zugelassen werden, als für das externe Netz.

Mehr Informationen zur Filterung von ICMP finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)* und speziell in M 5.120 *Behandlung von ICMP am Sicherheitsgateway*.

**Umsetzung und Überprüfung**

Welche Möglichkeiten der Filterung und Protokollierung zur Verfügung stehen, unterscheidet sich je nach Betriebssystem. Vor dem Aufsetzen eines lokalen Paketfilters sollte die vorhandene Dokumentation zu Rate gezogen werden.

Bei der Einrichtung von Paketfilterregeln sollte mit großer Sorgfalt vorgegangen werden, da ein Fehler in einer Regel unter Umständen dazu führen kann, dass sich ein Administrator, der über das Netz auf dem Rechner arbeitet, auf diese Weise "aussperrt" und die Korrekturen von der Systemkonsole aus vornehmen muss.

Nach dem Aktivieren des lokalen Paketfilters sollte einerseits geprüft werden, ob die benötigten Dienste noch erreichbar sind, andererseits sollte mit einem Portscan überprüft werden, ob die restlichen Ports alle blockiert sind.

**Beispiel: lokale Paketfilterregeln für einen Webserver**

Im nachfolgenden Beispiel werden lokale Paketfilterregeln für einen Rechner vorgeschlagen, der als Webserver in einer DMZ aufgestellt ist. Dabei wird davon ausgegangen, dass die Administration des Servers von einem Arbeitsplatzrechner aus über eine ssh-Verbindung erfolgt und die Dateien für das Webangebot ebenfalls über eine ssh-Verbindung auf den Rechner übertragen werden.

Für den Webserver wurde die Namensauflösung per DNS abgeschaltet, daher ist kein Zugriff auf einen DNS-Server erforderlich. UDP kann daher vollständig blockiert werden. Vom Webserver aus wird normalerweise kein *ping* oder *traceroute* benötigt, sondern es wird nur der ICMP-Nachrichtentyp 3 (*Destination unreachable*) zugelassen. Für eine leichtere Diagnose im internen Netz können eventuell noch andere ICMP-Nachrichtentypen (beispielsweise Typ 8 und Typ 0: *Echo request* und *Echo reply*) erlaubt werden. Im Beispiel werden für das interne Netz eingehende *Echo requests* und ausgehende *Echo replies* erlaubt: Dies ermöglicht es, den Webserver aus dem internen Netz heraus "anzupingen".

Wichtig ist weiter, dass die ssh-Verbindungen nur zum Webserver hin erfolgen, und nicht von diesem ausgehen. Das gleiche gilt für Verbindungen zum TCP-Port 80, der zum Webserver-Prozess gehört: Es werden eingehende Verbindungen zu diesem Port zugelassen, aber keine ausgehenden Verbindungen. Dies bedeutet, dass prinzipiell keine ausgehenden Verbindungsanfragen (nur das TCP SYN-Flag ist gesetzt) benötigt werden, sondern dass nur ausgehende TCP-Pakete erlaubt sind, die zu einer bestehenden Verbindung gehören (das TCP ACK-Flag ist gesetzt). Das Sperren ausgehender Verbindungsanfragen dient, wie oben erläutert, dem Zweck, einen Angreifer, der sich beispielsweise über eine Sicherheitslücke im Webserver-Dienst Zugang zum Rechner verschafft hat, zumindest aufzuhalten. Der Angreifer kann diese Sperre zwar deaktivieren, sie bietet aber insbesondere dann einen zusätzlichen Sicherheitsgewinn, wenn sie mit entsprechenden Protokollierungs- und Alarmierungsfunktionen kombiniert wird.

| Quell-Adresse:Port | Ziel-Adresse:Port | Protokoll | TCP-Flags oder ICMP-Typ | Entscheidung |
|---|---|---|---|---|
| intern:* | Webserver:22 (ssh) | TCP | SYN oder ACK | Akzeptieren |
| extern:* | Webserver:22 | TCP | alle | Blockieren |
| Webserver:22 | intern:* | TCP | ACK | Akzeptieren |
| alle:* | Webserver:80 (http) | TCP | SYN oder ACK | Akzeptieren |
| Webserver:80 | alle:* | TCP | ACK | Akzeptieren |
| alle | Webserver, nicht 22 oder 80 | TCP | alle | Blockieren |
| Webserver:* | alle:* | TCP | ohne ACK | Blockieren |
| alle | alle | UDP | - | Blockieren |
| alle | Webserver | ICMP | Typ 3 | Akzeptieren |
| Webserver | alle | ICMP | Typ 3 | Akzeptieren |
| intern | Webserver | ICMP | Typ 8 | Akzeptieren |
| Webserver | intern | ICMP | Typ 0 | Akzeptieren |
| Webserver | alle | ICMP | andere | Blockieren |
| alle | Webserver | ICMP | andere | Blockieren |

Tabelle: Beispielkonfiguration für einen Paketfilter

In der Tabelle steht * für einen beliebigen Port.

Eine noch höhere Sicherheit kann in diesem Beispiel erreicht werden, wenn die internen Adressen, von denen aus ein Zugriff per ssh erlaubt sein soll, weiter eingeschränkt werden. Falls beispielsweise nur zwei Administratoren von ihren beiden Arbeitsplatzrechnern aus zugreifen, dann könnte der Zugriff auf die Adressen dieser beiden Rechner beschränkt werden.

Detailliertere Informationen zu Paketfiltern finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)*.

Prüffragen:

- Werden auf IT-Systemen lokale Zugrifssbeschränkungen auf Netz- und Anwendungsebene umgesetzt?
- Ist die Sicherheitsstrategie der lokalen Firewall gemäß dem Whitelist-Verfahren restriktiv?
- Ist für die Konfiguration eines lokalen Paketfilters eine Grundkonfiguration vorgesehen?
- Werden Maßnahmen zur lokalen ICMP-Filterung eingesetzt?
- Wird das lokale Firewall-Regelwerk regelmäßig überprüft?
- Wird die Richtlinie zum Einsatz einer lokalen Firewall regelmäßig aktualisiert?

# M 4.239 Sicherer Betrieb eines Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der sichere Betrieb eines Servers hängt von einer Reihe von Faktoren ab. Besonders wichtig ist dabei, dass die Administration des Servers mit der gebotenen Sorgfalt auf einem sicheren Zugang erfolgt.

Im Folgenden werden einige allgemeine Punkte beschrieben, die für einen sicheren Betrieb eines Servers beachtet werden sollten. Für einzelne Betriebssysteme werden in entsprechenden Maßnahmen der betreffenden Bausteine spezifischere Hinweise gegeben.

**Administrationszugänge**

Es gibt unterschiedliche Zugriffsmöglichkeiten um Server zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert, auch die Server in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration kaum gewährleistet werden kann. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt werden und die Administration darf nur entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Allgemein ist es wichtig, einen Überblick darüber zu erhalten, welcher Teil der Administration eines Servers normalerweise

- lokal über die Konsole,
- remote über das Netz, aber unter Nutzung der Standardmechanismen des Betriebssystems, oder
- über ein zentrales netzbasiertes Administrationswerkzeug

durchgeführt werden soll. Es wird empfohlen, für die verschiedenen Nutzungsarten eine Übersicht zu erstellen, welche Administrationstätigkeiten auf welchem Weg durchgeführt werden können. Insbesondere ist es wichtig festzuhalten, ob bestimmte Tätigkeiten auf einem bestimmten Weg normalerweise nicht durchgeführt werden dürfen.

- Lokale Administration
  Ein Server sollte prinzipiell in einem Serverraum oder zumindest einem abschließbaren Serverschrank aufgestellt sein. Für den Teil der Administration, der trotzdem teilweise lokal über die Konsole erfolgen soll oder muss, müssen entsprechende Vorgaben dafür gemacht werden, wer Zugang zur Konsole erhält, welche Art der Authentisierung für den lokalen Zugang genutzt werden darf und welche anderen Vorgaben berücksichtigt werden müssen.
- Remote-Administration
  Meist wird ein Server nicht lokal an der Konsole sondern von einem Arbeitsplatzrechner aus über das Netz administriert. Um zu verhindern, dass dabei Authentisierungsinformationen der Administratoren und Konfigurationsdaten der Server abgehört oder gar von einem Angreifer manipuliert werden, sollte die Administration nur über sichere Protokolle (beispielsweise nicht über Telnet, sondern über SSH, nicht über HTTP, sondern über HTTPS) erfolgen. Alternativ kann ein eigenes Administrationsnetz eingerichtet werden, das vom dem restlichen Netz getrennt ist.
  Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung

der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten, soweit möglich, keine unsicheren Protokolle verwendet werden.

- Administration über ein zentrales Managementsystem
  Falls für die Administration des Servers ein zentrales Managementsystem genutzt werden soll, so sollten für diesen Zugangsweg analoge Vorüberlegungen angestellt werden, wie für die Remote-Administration. Zusätzlich ist es wichtig, dass das zentrale Managementsystem selbst entsprechend sicher konfiguriert und administriert wird. Entsprechende Hinweise finden sich im Baustein B 4.2 *Netz- und Systemmanagement*.

**Routinetätigkeiten bei der Administration**

Es wird empfohlen, für die üblichen Routinetätigkeiten der Administratoren entsprechend der Sicherheitsrichtlinie für den Server Hinweise für die Administration zu erstellen. Dies umfasst beispielsweise Tätigkeiten wie

- Anlegen und Löschen von Benutzern,
- Installation und Deinstallation von Programmen,
- Einspielen von Sicherheitsupdates und Patches (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*),
- Einspielen sonstiger Updates und Patches,
- Regelmäßige Überprüfung des Betriebszustandes des Systems (beispielsweise Auslastung des Systems, verbleibender freier Plattenplatz),
- Überprüfung der Logdaten auf ungewöhnliche Einträge (siehe auch M 5.9 *Protokollierung am Server*) und
- Regelmäßiger Integritätscheck mit entsprechenden Tools (siehe auch M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*).

**Tests von Konfigurationsänderungen**

Verschiedene Serverprogramme bieten die Möglichkeit, Konfigurationsänderungen vor dem Wirksamwerden zumindest auf technische Korrektheit zu überprüfen. Dies hilft zu vermeiden, dass ein Serverprogramm nach einer fehlerhaften Konfigurationsänderung nicht mehr startet und so zu einem Ausfall des betreffenden Dienstes führt. Sofern solche Möglichkeiten vorhanden sind, sollten die Administratoren mit deren Benutzung vertraut sein und sie auch tatsächlich wahrnehmen.

**Dokumentation von Arbeiten am System**

Änderungen an der Systemkonfiguration oder an der Konfiguration von Serverprogrammen müssen dokumentiert werden. Die Dokumentation muss so beschaffen sein, dass im Falle von Problemen nachvollziehbar ist, was die letzte Änderung war und wann sie von wem durchgeführt wurde. Dabei ist es wichtig, dass die Dokumentation so beschaffen ist, dass sie nicht nur von den Administratoren selbst nachvollzogen werden kann, sondern notfalls auch von einem "fachkundigen Dritten", der mit dem täglichen Betrieb des betreffenden Systems nichts zu tun hat. Außerdem sollte es anhand der Dokumentation möglich sein, eine frühere Konfiguration zu reproduzieren.

Für Änderungen an textbasierten Konfigurationsdateien bieten sich zu diesem Zweck Revisionsverwaltungssysteme an. Zusätzlich sollte direkt in den Konfigurationsdateien durch kurze Kommentare die Auswirkungen und die Funktionsweise der neuen Konfigurationseinstellungen erläutert werden. Für andere Konfigurationsmechanismen existieren teilweise ähnliche Werkzeuge oder die betreffende Software bietet bereits standardmäßig entsprechende Funktionalitäten an. Wird ein zentrales Administrationssystem genutzt, so sollten entsprechende Funktionen vorhanden sein und auch genutzt werden.

Prüffragen:

- Entsprechen die Zugänge (lokaler Zugriff über die Konsole, Remote Zugriff über das Netzwerk, Zugriff über ein zentrales Managementsystem) für administrative Tätigkeiten an den IT-Systeme der Sicherheitsrichtlinie?
- Entsprechen die verwendeten Protokolle und Pfade der Administrationszugänge dem Stand der Technik?

# M 4.240 Einrichten einer Testumgebung für einen Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für Server mit hohen Sicherheitsanforderungen sollte eine Testumgebung eingerichtet werden, in der Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf dem Produktionssystem vorab getestet werden können. Dies betrifft sowohl Sicherheitspatches und -updates als auch normale Updates, die vom Hersteller herausgegeben werden.

Die Testumgebung muss so beschaffen sein, dass sie eine "funktional äquivalente" Installation von Hard- und Software erlaubt. Dies bedeutet nicht notwendigerweise, dass zu einem teuren Serverrechner ein zweites, identisch konfiguriertes System beschafft werden muss. Zum Testen von Konfigurationsänderungen, Updates und Patches von Anwendungsprogrammen und Serversoftware genügt meist ein technisch deutlich sparsamer ausgestattetes System.

Es sollte jedoch auch die Möglichkeit bestehen, neue Gerätetreiber vor dem Einspielen zu testen. Daher kann es gegebenenfalls vorteilhaft sein, für verschiedene Arten von Tests unterschiedliche Testsysteme zu nutzen, etwa ein System für Tests systemnaher Programme oder von Betriebssystempatches und ein anderes für Tests im Zusammenhang mit der eigentlichen Serversoftware. In einem solchen Fall ist es jedoch wichtig sich bewusst zu sein, dass auf diese Weise gewisse Arten von Wechselwirkungen zwischen Betriebssystemumgebung und Serversoftware nicht abgedeckt werden können. Bei besonderen Anforderungen an die Sicherheit und Zuverlässigkeit eines Servers kann es deswegen erforderlich werden, tatsächlich ein zweites, identisch konfiguriertes System als Testumgebung zur Verfügung zu haben.

Für verschiedene typische und häufiger wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testen abgearbeitet werden können und die neben der reinen Dokumentation des Tests oft auch zu einer Erhöhung der Effizienz und zur Vermeidung von Fehlern beitragen können.

Alle Tests sollten so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

Prüffragen:

- Bei hohem Schutzbedarf: Existiert eine Testumgebung um Konfigurationsänderungen, Updates und Patches auf Interoperabilität zu testen?
- Erlaubt die Testumgebung der IT-Systeme eine "funktional äquivalente" Installation von Hard- und Software?
- Erlaubt die Testumgebung der IT-Systeme eine Installation von Gerätetreibern und systemnahen Programmen vergleichbar den Wirksystemen?
- Werden Checklisten für typische und häufig wiederkehrende Testfälle verwendet?

# M 4.241 Sicherer Betrieb von Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der sichere Betrieb von Clients hängt von einer Reihe von Faktoren ab. Besonders wichtig ist dabei auch bei Clients, dass die Administration mit der gebotenen Sorgfalt und ausschließlich über sichere Zugänge erfolgt.

Im Folgenden werden einige wichtige Punkte beschrieben, die für einen sicheren Betrieb von Clients unabhängig vom Betriebssystem beachtet werden sollten. Für einzelne Betriebssysteme werden in den entsprechenden Maßnahmen der betreffenden Bausteine spezifischere Hinweise gegeben.

**Administrationszugänge**

Es gibt unterschiedliche Zugriffsmöglichkeiten, um Clients zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert und oft unumgänglich, die Clients in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration nicht gewährleistet werden kann. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt und die Administration nur entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Es wird empfohlen, für die verschiedenen Administrationstätigkeiten eine Übersicht zu erstellen, welche Arbeiten auf welchem Weg durchgeführt werden können. Vor allem ist es wichtig festzuhalten, ob bestimmte Tätigkeiten auf einem bestimmten Weg normalerweise nicht durchgeführt werden dürfen.

- Lokale Administration
  Die Administration von Clients direkt durch Zugriff über die Konsole ist nur für eine kleine Zahl von Rechnern handhabbar und wird in Umgebungen mit einer größeren Anzahl von Clients meist einen Ausnahmefall darstellen. Muss ein Administrator ausnahmsweise doch lokal an einem Client-Rechner arbeiten, ist es beispielsweise wichtig, dass der Administrator bei der Authentisierung über ein Passwort darauf achtet, dass dieses nicht ausgespäht werden kann. Gegebenenfalls sollte überlegt werden, für solche Arbeiten Einmalpasswörter oder ähnliches zu verwenden.
- Administration mit Hilfe eines Bootmediums
  Für bestimmte Administrationsarbeiten, die lokal an einem Client-Rechner vorgenommen werden sollen kann es vorteilhaft sein, ein externes Boot-Medium einzusetzen, von dem der Rechner gestartet wird (siehe auchM 6.24 *Erstellen eines Notfall-Bootmediums*). Dies bietet den Vorteil, dass der Administrator sich einer "sauberen" Systemumgebung sicher sein kann. Allerdings hat diese Methode auch eine Reihe von Nachteilen, beispielsweise einen höheren Aufwand. Außerdem ist es auf diese Weise meist nicht möglich, bestimmte Fehlermeldungen, die im laufenden Betrieb auftreten, nachzuvollziehen.
- Remote-AdministrationClients werden häufig von Administrationsrechnern aus über das Netz administriert. Um zu verhindern, dass dabei Authentisierungsinformationen der Administratoren abgehört oder gar von einem Angreifer manipuliert werden, sollte die Administration nur über sichere Protokolle (beispielsweise nicht über Telnet, sondern über SSH, nicht über HTTP, sondern über HTTPS) erfolgen.

Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Si-

cherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten soweit möglich keine unsicheren Protokolle verwendet werden.

- Administration über ein zentrales Managementsystem
  Falls für die Administration ein zentrales Managementsystem genutzt werden soll, so müssen für diesen Zugangsweg analoge Vorüberlegungen angestellt werden, wie für die Remote-Administration. Zusätzlich ist es wichtig, dass das zentrale Managementsystem selbst entsprechend sicher konfiguriert und administriert wird.

**Routinetätigkeiten bei der Administration**

Es wird empfohlen, für die üblichen Routinetätigkeiten der Administratoren entsprechend der Sicherheitsrichtlinie Hinweise für die Administration zu erstellen. Dies umfasst beispielsweise Tätigkeiten wie

- Anlegen und Löschen von Benutzern,
- Installation und Deinstallation von Programmen,
- Einspielen von Sicherheitsupdates und Patches (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*),
- Einspielen sonstiger Updates und Patches oder
- Regelmäßiger Integritätscheck mit entsprechenden Tools (siehe auch M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*).

**Tests von Konfigurationsänderungen**

Konfigurationsänderungen an Clients sollten nach Möglichkeit auf einem Referenzsystem getestet werden, bevor sie auf die einzelnen Rechner verteilt werden (siehe auch M 4.242 *Einrichten einer Referenzinstallation für Clients*). Werden (etwa im Rahmen einer Fehlersuche) Änderungen lokal auf einzelnen Clients durchgeführt, so sollte auf jeden Fall geprüft werden, ob durch die Änderungen die sonstigen Funktionen des Clients nicht beeinträchtigt werden.

**Dokumentation von Arbeiten an den Systemen**

Änderungen an der Systemkonfiguration der Clients oder an der Konfiguration von Anwendungen müssen dokumentiert werden. Die Dokumentation sollte auch bei Clients idealerweise so beschaffen sein, dass im Falle von Problemen nachvollziehbar ist, was die letzte Änderung war und wann und von wem sie durchgeführt wurde. Bei Clients ohne hohe

Sicherheitsanforderungen kann aber auch die Dokumentation einzelner funktionierender Konfigurationsstände (beispielsweise zu bestimmten Zeitpunkten) ausreichend sein, ohne dass es unbedingt notwendig ist, jeden einzelnen Schritt nachzuvollziehen. Trotzdem wird empfohlen, die Dokumentation so zu gestalten, dass alle Änderungen nachvollziehbar sind.

**Protokollierung**

Sicherheitsrelevante Ereignisse, die bei Clients auftreten, sollten aus vielen Gründen protokolliert werden. Zum einen hilft eine aktivierte Protokollierung, potentielle Schwachstellen frühzeitig erkennen und damit beseitigen zu können. Zum anderen kann Protokollierung dabei helfen, Verstöße gegen Sicherheitsvorgaben zeitnah zu erkennen oder Nachforschungen über einen Sicherheitsvorfall vorzunehmen. Die Protokollierung von Clients sollte im Protokollierungskonzept integriert werden (siehe M 2.500 *Protokollierung von IT-Systemen*).

Prüffragen:

- Werden die zur Administration von Clients verwendeten Methoden in der Sicherheitsrichtlinie beschrieben?
- Werden bei der Remote-Administration bzw. bei Nutzung eines Managementsystems ausschließlich sichere Protokolle verwendet?
- Existieren Vorgaben für die Dokumentation von Änderungen und werden diese umgesetzt?

# M 4.242 Einrichten einer Referenzinstallation für Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es wird empfohlen, für Clients eine Referenzinstallation zu erstellen, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Clients bei den Anwendern vorab getestet werden können. Dies betrifft die Grundeinstellungen des Systems, Sicherheitspatches und -updates und auch normale Updates, die vom Hersteller herausgegeben werden.

Darüber hinaus kann eine solche Referenzinstallation gegebenenfalls auch dazu genutzt werden, die Installation neuer Clients zu vereinfachen, indem eine entsprechend vorkonfigurierte Installation auf geeignete Art und Weise auf den zu installierenden Rechner überspielt wird ("klonen"). Im Idealfall brauchen anschließend nur noch wenige Einstellungen angepasst zu werden. Eine Referenzinstallation, die zum Klonen von Clients verwendet wird, muss mit besonderer Sorgfalt konfiguriert und getestet werden.

Die Referenzinstallation muss so beschaffen sein, dass die wesentlichen Parameter der Hard- und Softwareplattform für alle Systeme, die von dieser Referenzinstallation abgeleitet werden, die selben sind. Dies bedeutet nicht notwendigerweise, dass deswegen auf sämtlichen Clients eine identische Hard- und Softwarekonfiguration bestehen muss. Die Konfiguration verschiedener Clients muss aber hinreichend ähnlich sein, damit der Referenzcharakter der Installation erhalten bleibt.

Bei Tests von Anwendungsprogrammen und Einstellungen, die die Anwender auf den Clients betreffen, ist es darüber hinaus besonders wichtig, dass die Administratoren diese nicht mit Administratorrechten durchführen, sondern unter einer Benutzerkennung, der die selben Berechtigungen besitzt und für den die selben Einstellungen für die Benutzerumgebung gewählt wurden, wie die Anwender, die mit dem System arbeiten sollen.

Gegebenenfalls kann es vorteilhaft sein, für verschiedene Arten von Tests unterschiedliche Testsysteme zu nutzen, etwa ein oder mehrere Systeme für Tests von Gerätetreibern oder systemnaher Programme und von Betriebssystempatches, und ein anderes für Tests im Zusammenhang mit Anwendungsprogrammen. In einem solchen Fall ist es jedoch wichtig, sich bewusst zu sein, dass auf diese Weise gewisse Arten von Wechselwirkungen zwischen Betriebssystemumgebung und Anwendungsprogrammen nicht abgedeckt werden können. Bei besonderen Anforderungen an die Sicherheit der Clients kann es deswegen erforderlich werden, tatsächlich für bestimmte Einsatzszenarien nur identisch ausgestattete und konfigurierte Systeme einzusetzen.

Für verschiedene typische und häufiger wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testen abgearbeitet werden können und die neben der reinen Dokumentation des Tests oft auch zu einer Erhöhung der Effizienz und zur Vermeidung von Fehlern beitragen können.

Alle Tests sollten so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dies ist insbesondere bei Tests von Sicherheitsupdates und von neuen Gerätetreibern notwendig, bei denen eine fehlerhafte Konfiguration oder ein Fehlschlagen der Installation dazu führen kann, dass die betroffenen Clients keinen Zugang mehr zum Netz erhalten

oder gar überhaupt nicht mehr starten. Gerade in solchen Fällen kann eine aussagekräftige Dokumentation die notwendige Zeit für die Fehlersuche und -beseitigung wesentlich verkürzen.

Prüffragen:

- Existiert eine dokumentierte Referenzinstallation für Clients?
- Existieren Checklisten für Testfälle?
- Bei hohen Schutzbedarfen: Besteht für jeden Clienttyp eine eigene Referenzinstallation, mit der Wechselwirkungen von Programmen/ Updates ausgeschlossen werden können?

# M 4.243 Verwaltungswerkzeuge unter Windows Client-Betriebssystemen

**Verantwortlich für Initiierung:** Administrator
**Verantwortlich für Umsetzung:** Administrator

Das Kommandozeilen-basierte Tool *secedit* ist bereits aus Windows 2000 bekannt. Es ermöglicht das Automatisieren von Aufgaben bei der Konfiguration der Sicherheitseinstellungen. Mit diesem Tool können unter anderem Vorlagen automatisch erstellt, angewandt und analysiert werden. Eines seiner wichtigsten Merkmale ist die Fähigkeit, einen Abgleich der geltenden Gruppenrichtlinieneinstellungen mit einem Mustersatz zu erstellen. Es sollte beachtet werden, dass ein Teil der *secedit*-Funktionalität unter Windows XP in das Tool *gpupdate* ausgelagert wurde. Wird unter Windows Vista und Windows 7 *secedit* von der Kommandozeile aus aufgerufen, muss der Kommandozeilen-Prozess mit expliziten Administrator-Rechten ("Als Administrator ausführen") gestartet worden sein.

Die Analyse der aktuell geltenden Einstellungen kann auch mit dem MMC Snap-in *Sicherheitskonfiguration und -analyse* durchgeführt werden. Die Ergebnisse werden im Gegensatz zu *secedit* graphisch aufbereitet und präsentiert. Es ist zu beachten, dass weder das *secedit*-Tool noch das MMC Snap-in *Sicherheitskonfiguration- und -analyse* zur Konfiguration und Analyse der definierten Parameter in administrativen Vorlagen verwendet werden können.

Die Bearbeitung von Sicherheitsvorlagen erfolgt unter Windows XP, Windows Vista und Windows 7 mit dem MMC Snap-in *Sicherheitsvorlagen*. Da die Sicherheitsvorlagen einfache Textdateien sind, können sie auch mit einem gewöhnlichen Texteditor bearbeitet werden. Dies kann unter anderem für die Spezifizierung zusätzlicher Registry-Schlüssel notwendig sein.

Ändern sich die Einstellungen einer Gruppenrichtlinie, so werden die Konfigurationsänderungen nur mit einer Verzögerung wirksam, die durch die Verarbeitungseinstellungen der Gruppenrichtlinien vorgegeben wird. Um die Änderungen für einen Benutzer oder Computer unverzüglich zu verbreiten, kann ab Microsoft Windows XP das Kommandozeilenwerkzeug *gpupdate* benutzt werden. Dieses Tool ersetzt das von Windows 2000 bekannte Kommando *secedit /refreshpolicy*.

Das Kommandozeilentool *gpresult* kann auf einem Windows Client ab Windows XP benutzt werden, um das Resultat aller eingerichteten Gruppenrichtlinien aufzulisten. Es dient unter anderem dazu herauszufinden, was bei der Anmeldung eines bestimmten Benutzers auf einem bestimmten Computer passiert (*gpresult /r /s:computername /u:benutzername*). Dieses Werkzeug kann vor allem zur Fehlersuche oder zur Dokumentation der geltenden Einstellungen verwendet werden.

Eine ähnliche Funktionalität wie *gpresult* bietet auch das MMC Snap-in *Richtlinienergebnissatz* (*rsop.msc*). Dieses Tool kann nicht nur zur Dokumentation der aktuell geltenden Einstellungen verwendet werden (Protokollierungsmodus), sondern auch, um mögliche andere Szenarien durchzuspielen (Planungsmodus).

Damit lässt sich eine Richtlinienimplementierung simulieren, die vor allem in der Design-Phase immens wichtig ist und vor vielen Implementierungsfehlern,

insbesondere bei komplexen Gruppenrichtlinien-Strukturen und -Hierarchien, bewahren kann.

Das von Microsoft frei verfügbare Tool *Group Policy Management Console* (*GPMC*) bietet deutlich bessere Verwaltungsmöglichkeiten für Gruppenrichtlinien im Active Directory als die Standard Snap-ins von Windows 2000 und XP. Das Tool ist bei einer Standardinstallation von Windows Vista bereits enthalten. Dieses Tool stellt weitergehende Funktionalitäten zur Verfügung, welche für die Verwaltung der Gruppenrichtlinien im Active Directory sehr wichtig sind:

- Erstellen, Verlinken und Löschen von GPOs
- Importieren der Einstellungen aus gesicherten Gruppenrichtlinienobjekten,
- Erstellung von GPO-Reports, die unter anderem für Dokumentationszwecke verwendet werden können und
- Sichern und Wiederherstellen von GPOs.
  Nicht zuletzt bietet *GPMC* eine Scripting-Schnittstelle, die bei einer Vielzahl administrativer Aufgaben sinnvoll eingesetzt werden kann. Der Einsatz von *GPMC* wird daher in Active Directory-Umgebungen dringend empfohlen. Ab Windows 7 wurde das GPMC durch das RSAT (Remote Server Administration Tool) ersetzt.

Das *GPOAccelerator-Tool* unterstützt die Konfigurationen von Gruppenrichtlinien für den Betrieb von Windows Vista Clients in einer Domäne, wenn die Domänen-Controller noch nicht unter Windows Server 2008 betrieben werden. Die Konfiguration der Gruppenrichtlinien muss dann von einem Windows Vista Client aus erfolgen. Auf dem Client kann ein Domänenadministrator mit dem *GPOAccelerator-Tool* die notwendigen Konfigurationen der Gruppenrichtlinien erstellen. Im Anschluss müssen diese in den *sysvol*-Ordner des Domänen-Controllers übertragen werden. Das *GPO Accelerator-Tool* wird seit Windows 7 durch die *Microsoft Security Compliance Manager Suite* ersetzt.

Ein weiteres sinnvolles Tool ist der Migrationstabellen-Editor *mtedit*, der im Lieferumfang des *GPMC* enthalten ist. Dieses Tool ermöglicht eine bequeme Erstellung von Migrationstabellen, die beim domänenübergreifenden Kopieren oder Importieren einer Sicherheitsrichtlinie verwendet werden können. Durch die Verwendung von Migrationstabellen lassen sich domänenspezifische Informationen wie Gruppennamen oder SIDs modifizieren.

Zur Konfiguration von Überwachungsrichtlinien steht unter Windows Vista und Windows 7 das Werkzeug *auditpol* zur Verfügung.

Microsoft stellt mit dem *Baseline Security Analyzer* (MBSA) ein Tool zur Verfügung, das für die automatische Auswertung der Patch-Stände eingesetzt werden kann. Der Einsatz dieses Tools verschafft den Administratoren einen aktuellen Überblick über den Patch-Stand der Systeme und trägt somit wesentlich zur Gesamtsicherheit bei (siehe M 4.249 *Windows Client-Systeme aktuell halten*).

Der "Problem Steps Recorder" (Problemaufzeichnung, PSR) von Microsoft erleichtert es den Benutzern, entstehende Probleme für Administratoren sinnvoll und nachvollziehbar zu dokumentieren. Das Tool steht ab Windows 7 zur Verfügung und dokumentiert, sobald es aktiviert wurde, sämtliche Eingaben des Benutzers. Das Tool generiert Screenshots des betroffenen IT-Systems und markiert sowie beschreibt die Eingaben des Benutzers. Zusätzlich kann der Benutzer einem Screenshot eigene Kommentare hinzufügen, um das Problem detaillierter zu beschreiben. Der PSR generiert eine ZIP-Datei die eine MHT-

Datei enthält, in der das Problem beschrieben wird. Es sollte grundlegend in einer Anweisung festgelegt werden, dass:

- Fenster mit vertraulichen Bildschirminhalten während der Problemaufzeichnung geschlossen oder minimiert werden sollten,
- keine Passworte oder sonstigen Authentisierungsdaten und
- keine vertraulichen Informationen eingegeben werden.

Weiterhin ist für die Übertragung der generierten ZIP/MHT-Datei ein hinsichtlich des Inhaltes dieser Datei angemessen sicherer Kommunikationsweg zu wählen.

Alle diese Werkzeuge sollten unbedingt von Administratoren bei der Fehlersuche oder während der Design- und Test-Phasen eingesetzt werden. Die Verwendung dieser Tools hilft, Konfigurationsschwächen zu entdecken und zu vermeiden.

Prüffragen:

- Werden die Verwaltungswerkzeuge der Windows Client-Betriebssysteme entsprechend den Anforderungen eingesetzt?

# M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Sicherheit eines Arbeitsplatzrechners hängt im Wesentlichen davon ab, ob ein Benutzer administrativ auf den Rechner einwirken kann, welche Funktionen den Benutzern verfügbar gemacht werden und ob die Benutzer die ihnen zur Verfügung gestellten Sicherheitsmechanismen korrekt nutzen.

Bei der Konfiguration von Clients ab Windows XP sind folgende Aspekte aus Sicherheitssicht zu berücksichtigen:

- Die entsprechenden Überwachungsrichtlinien müssen definiert sein (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems* und M 4.344 *Überwachung von Client ab Windows Vista und Server ab Windows Server 2008*). Die gesammelten Protokolldaten müssen auch regelmäßig ausgewertet werden.
- Beim Einsatz in einer Active Directory Umgebung sollten die Rechte zum Hinzufügen von Arbeitsstationen zur Domäne eingeschränkt werden. Ausschließlich berechtigte administrative Benutzer dürfen diese Zuständigkeit besitzen. Die Einschränkung des Rechts erfolgt über die Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Zuweisen von Benutzerrechten* | *Hinzufügen von Arbeitsstationen zur Domäne*.
- Beim Einsatz von Client-Betriebssystemen ab Windows XP auf mobilen Rechnern entstehen zusätzliche Sicherheitsrisiken, die durch besondere Vorkehrungen gemindert werden sollten (siehe M 2.328 *Einsatz von Windows XP auf mobilen Rechnern*, M 2.442 *Einsatz von Windows ab Windows Vista auf mobilen Systemen*, sowie B 3.3 *Laptop*).

**Datenhaltung und Verarbeitung**

Es empfiehlt sich, bei vernetzten Clients keine lokalen Daten auf Arbeitsplatzrechnern zu halten. Dies erleichtert die zentrale Administration und Steuerung von Sicherheitsvorgaben ebenso wie die Datensicherung. Daneben ergibt sich der Sicherheitsvorteil, dass bei Kompromittierung des Systems lokal keine sensitiven Daten vorzufinden sind, da sie sich auf einem Server befinden, der in der Regel besser als ein Client geschützt ist. In Einzelfällen kann es notwendig sein, dass Daten aus Sicherheitsgründen lokal auf dem Arbeitsplatz gespeichert werden müssen, wenn beispielsweise nur der Arbeitsplatzbenutzer darauf zugreifen darf und/oder keine Übertragung über das Netz erfolgen soll. Dann ist der Arbeitsplatz jedoch nicht als Standardarbeitsplatz anzusehen, so dass besondere Regelungen für solche Arbeitsplätze geplant und umgesetzt werden müssen. Beispiele für entsprechende Maßnahmen sind eine starke Absicherung der Clients ("hardening") sowohl lokal als auch im Netz, eine Festplattenverschlüsselung und die Einbindung der Clients in ein zentrales Backup-Konzept.

Vertrauliche Daten müssen sicher verarbeitet werden. Nicht nur der direkte Zugriff auf die Daten muss entsprechend dem Berechtigungskonzept eingeschränkt sein. Es muss auch dafür Sorge getragen werden, dass kein unautorisierter Zugriff auf die temporären Inhalte möglich ist. Viele Anwendungen erstellen bei der Verarbeitung temporäre Dateien, die im Gegensatz zu Originaldaten möglicherweise nicht ausreichend geschützt sind. Daher ist die re-

gelmäßige Bereinigung von Verzeichnissen, in denen temporäre Dateien abgelegt werden (z. B. *Temp*, *Tmp* und das Drucker-Spool-Verzeichnis), sehr empfehlenswert. Dies kann unter anderem mit einem Skript realisiert werden, das beim Herunterfahren des Systems ausgeführt wird (siehe M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*). Die Auslagerungsdatei wird beim Herunterfahren des Systems durch die Richtlinie *Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems löschen* in Gruppenrichtlinienobjekten gelöscht. Ab Windows Vista ist dafür die Einstellung *Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen* unter *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* verantwortlich.

**Softwareeinschränkungen**

Durch die gezielte Systemkonfiguration soll vermieden werden, dass normale Benutzer administrative Tätigkeiten ausführen können. Dies kann durch die Zugriffsrechte auf Dateien und die Registry sowie durch die Berechtigung zum Starten der Konfigurationswerkzeuge, wie der Microsoft Management Konsole, erreicht werden. Diese Einstellungen werden über Gruppenrichtlinien verwaltet und sollten schon in die Planung der Gruppenrichtlinien einfließen. Der Einsatz von Richtlinien für Softwareeinschränkungen (englisch Software Restriction Policies, SRP) und AppLocker ab Windows 7 kann in dieser Hinsicht zusätzliche Sicherheit bringen.

Software-Installationen sind ausschließlich von berechtigten Administratoren durchzuführen. Die Installationsmöglichkeiten für normale Benutzer sind soweit wie möglich einzuschränken (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*). Die Installationen, die mittels des Windows-Installers durchgeführt werden, lassen sich durch die Definition geeigneter Gruppenrichtlinien unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Installer* einschränken. Ob und in welchem Umfang Installationen eingeschränkt werden sollten, hängt von der Software-Installationsrichtlinie des Unternehmens oder der Behörde ab. Es sollte bedacht werden, dass diese Einstellungen nur den Windows-Installer betreffen und nicht verhindern, dass Benutzer anderweitig Programme installieren oder aktualisieren können.

Die mit Windows XP eingeführte Technologie der Softwareeinschränkungen ermöglicht es, die auf einem Computer ausführbaren Programme zu begrenzen. Durch die Definition von Richtlinien für Softwareeinschränkungen im Computerteil einer GPO (*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für Softwareeinschränkungen*) wird entweder die Summe der erlaubten (Positivliste) oder der verbotenen Programme (Negativliste) spezifiziert.

In einer Positivliste sollten nicht nur die Anwendungen, sondern alle für den Regelbetrieb benötigten Systemprogramme erlaubt sein.

Programme können in einer Regel der Softwareeinschränkungen durch einen voll- oder teilqualifizierten Pfad-Namen, einen Hashwert, eine digitale Signatur oder Zertifikat oder durch die Programmzone (beispielsweise *Internet*, *Lokaler Rechner*) identifiziert werden. Eine Regel ist nicht nur auf gewöhnliche ausführbare Dateien, sondern unter anderem auch auf DLLs, ActiveX-Steuerelemente, Windows-Installer Dateien sowie auf VBScript Dateien anwendbar.

Die zur Verfügung stehenden Konfigurationsmöglichkeiten für Ausführungsbeschränkungen mittels SRP sind sehr variabel und ermöglichen die Realisierung einer Vielzahl von Einsatzszenarien. Dieser Vorteil wird jedoch mit ei-

nem entsprechenden Administrationsaufwand erkauft, da die definierten Regeln schnell komplex und unübersichtlich werden. Umfangreiche Planung und ausgiebiges Testen sind unabdingbar, wenn ein Unternehmen oder eine Behörde Richtlinien zur Softwareeinschränkungen implementieren möchte.

Eine weitere Möglichkeit, die Nutzung von Anwendungen einzuschränken, bieten Windows Vista und Windows 7 mit dem *Jugendschutz* sowie Windows 8 mit *Family Safety. Family Safety* enthält neben dem *Jugendschutz* der Vorgängerversionen auch Webaktivitätsberichte. Zu beachten ist, dass *Family Safety* nicht für den professionellen Einsatz konzipiert und nicht in einer Domänenumgebung verfügbar ist. Wenn in der Institution Minderjährige Zugang zu Clients haben, sollten die durch *Family Safety* ermöglichten Einschränkungen durch alternative Maßnahmen durchgesetzt werden. Weitere Informationen sind in der Maßnahme M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung* zu finden.

**Sichere Konfiguration von Windows 8-Apps**

Windows 8-Apps unterscheiden sich neben den Funktionsanforderungen und deren Beziehbarkeit auch in der Sicherheitskonfiguration gegenüber den Desktop-Anwendungen. Es sollte daher entschieden werden, ob und welche Windows-Apps in der Institution zugelassen werden. Weiterführende Materialien hierzu finden sich im *Hilfsmittel zum Baustein Windows 8* im Kapitel Einsatz von Apps unter Windows 8.

Die sichere Konfiguration von Windows 8-Apps funktioniert in der Regel nicht wie bei den Desktop-Anwendung zentral über die Gruppenrichtlinien. Hier sind ergänzende Maßnahmen erforderlich, z. B. mit Hilfe des Werkzeugs *AppLocker*, das sich wiederum auf Gruppenrichtlinien stützt. Über AppLocker können *Ausführbare Regeln*, *Windows Installer-Regeln*, *Skript-Regeln* sowie *App-Paket-Regeln* konfiguriert und erzwungen werden. Ziel dieser Regeln ist es, die vollständige Kontrolle darüber zu behalten, welche Windows-Apps von den Benutzern ausgeführt werden können.

Die Konfiguration des AppLocker erfolgt unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Anwendungssteuerungsrichtlinien* | *Applocker.* Weitere Informationen hierzu finden sich in der Maßnahme *M 4.419 Anwendungssteuerung ab Windows 7 mit AppLocker*.

**Dienste**

Windows Vista, Windows 7 und Windows 8 sind keine Server-Betriebssysteme und sollten nur für Clients verwendet werden sowie keine Anwendungen oder Dienste im Netz zur Verfügung stellen. Unter anderem sollten die normalen Arbeitsplatzrechner neben den administrativen Standardfreigaben keine Verzeichnisfreigaben zur Verfügung stellen. Auch die administrativen Freigaben sollten deaktiviert werden, wenn sie nicht zur Administration verwendet werden. Dazu muss der Wert *AutoShareWks*=0 unter *HKLM\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters* erstellt werden.

Sind aus bestimmten Gründen Freigaben auf den Clients erforderlich, darf der mit Windows XP eingeführte Mechanismus der einfachen Dateifreigabe nicht benutzt werden, um die hiermit verbundenen Sicherheitsrisiken zu vermeiden. Ist die einfache Dateifreigabe auf einem Client aktiviert, werden alle Benutzer, die über das Netz auf diesen Computer zugreifen, dem Gastkonto zugeordnet. Die Berechtigungen für den Zugriff auf die Freigabe müssen jedoch sehr restriktiv vergeben werden. Es ist zu beachten, dass die einfache Dateifreigabe standardmäßig nur auf Einzelclients möglich ist, die keiner Domäne angehö-

ren. Auf Clients, die als Domänenmitglieder installiert wurden, ist die einfache Dateifreigabe standardmäßig deaktiviert. Ab Windows 7 ist die Ordnerfreigabe über das Kontextmenü zu erreichen und trägt die Bezeichnung *Freigeben für*. Um einen Ordner in einer Domänenumgebung freizugeben, werden Administrationsrechte benötigt.

Die Gesamtsicherheit eines IT-Systems hängt auch von den eingesetzten Systemdiensten ab. Hinweise zur sicheren Dienstkonfiguration können in M 4.246 *Konfiguration der Systemdienste auf Clients ab Windows XP* gefunden werden.

Bei Clientsystemen ab Windows 7 kann ein IT-System als dedizierter Printserver verwendet werden. In diesem Fall darf dieses IT-System für keine anderen Zwecke eingesetzt werden. Die Hardware des IT-Systems und die Zugangssicherheit müssen die entsprechenden Serveranforderungen erfüllen (siehe unter anderem B 3.101 *Allgemeiner Server*). Alle Anwendungsfunktionen müssen deaktiviert werden.

**Benutzerkonten**

Die Benutzerkonten für Clients ab Windows XP dürfen nur von einer dazu berechtigten Person verwendet werden, das heißt, das Benutzerkonto ist einem Benutzer eindeutig zuzuordnen. Dies hat vor allem aus Gründen der Nachvollziehbarkeit zu erfolgen. Sammelkonten sollten nach Möglichkeit keine Verwendung finden. Dies ist auf organisatorischer Ebene zu gewährleisten.

Wird ein neues Benutzerkonto im Active Directory angelegt, ist auf die richtige Zuordnung zu einer Organisationseinheit zu achten, da hierüber die korrekten Sicherheitseinstellungen für dieses Benutzerkonto festgelegt werden. Die an einen Benutzer vergebenen Rechte resultieren neben den Gruppenmitgliedschaften unter anderem aus den Gruppenrichtlinien, die mit der Organisationseinheit des Benutzers verknüpft sind.

Erfolgt die Administration der Clientsysteme ab Windows XP über personalisierte Benutzerkonten, kann das integrierte Administrator-Konto gesperrt werden. Bei einer Standardinstallation ab Windows Vista ist dies grundsätzlich der Fall.

In jedem Fall sollte das Administratorkonto umbenannt werden. Das Deaktivieren oder Umbenennen des integrierten Administratorkontos kann in der Benutzerverwaltung oder durch die Richtlinien der *Konten: Administratorkontostatus* und *Konten: Administrator umbenennen* (unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) erfolgen. Vor dem Deaktivieren des Administratorkontos ist eine Testphase empfehlenswert, in der ausschließlich über die personalisierten Benutzerkonten administriert wird.

Alle Windows Versionen enthalten standardmäßig ein Gastkonto. Das Gastkonto sollte nicht genutzt werden, sondern immer ein dediziertes Konto für Benutzer verwenden. Das Gastkonto ist zu deaktivieren, wobei trotzdem ein komplexes Kennwort für das Konto vergeben werden sollte. Bei einer Standardinstallation ab Windows Vista ist das Gastkonto bereits deaktiviert, jedoch ist kein Kennwort vergeben. Durch das Setzen eines Kennworts besteht auch im Falle eines zufälligen oder unberechtigten Aktivierens des Gastkontos ein entsprechender Kennwortschutz. Um das Gastkonto umzubenennen und zu deaktivieren, können entweder die lokale Benutzerverwaltung oder die Richtlinien *Konten: Gastkontenstatus* und *Konten: Gastkonto umbenennen* (unter

*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) verwendet werden.

Das unter Windows XP standardmäßig angelegte Konto für den Support-Benutzer (*SUPPORT_388945a0*) wird normalerweise in Behörden- und Unternehmensumgebung nicht verwendet und sollte daher gelöscht werden. Zum Löschen dieses Kontos dient die lokale Benutzerverwaltung. Bei Clientsystemen ab Windows Vista ist das Benutzerkonto für den Support-Benutzer nicht mehr vorhanden.

Beim Betrieb eines Windows-Systems in der Domäne sollten nach Möglichkeit keine weiteren lokalen Benutzerkonten angelegt werden. Generell sollten lokal nur die unbedingt notwendigen Konten angelegt sein. Eine Überprüfung lokaler Benutzerkonten hat in regelmäßigen Abständen zu erfolgen.

Entsprechend M 4.2 *Bildschirmsperre* muss für jeden Benutzer der Kennwortschutz für den Bildschirmschoner aktiviert werden. Ist der Standby-Modus möglich, so muss die Kennworteingabe auch beim Reaktivieren des Systems aus dem Standby-Modus erforderlich sein. Bei Windows XP unter *Systemsteuerung* | *Energieoptionen* | *Erweitert* | *Kennwort beim Reaktivieren aus dem Standbymodus anfordern* und ab Windows Vista unter *Systemsteuerung* | *Energieoptionen* | *Kennwort bei Reaktivierung anfordern*.

Die Anforderungen in M 2.11 *Regelung des Passwortgebrauchs* und M 4.15 *Gesichertes Login* müssen umgesetzt werden. Dies betrifft vor allem Länge, Qualität und Änderungsintervalle der Kennwörter sowie die Anzahl der Fehlversuche und das Sperren der Benutzerkonten.

**Anmeldung absichern**

Der Systemzugang muss auf autorisierte Personen beschränkt sein. Die Vergabe entsprechender Benutzerrechte hat dementsprechend restriktiv zu erfolgen (siehe M 4.247 *Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista*). Ein administrativer Zugriff über das Netz sollte grundsätzlich nur berechtigtem administrativem Personal erlaubt werden. Des Weiteren muss die Anmeldung über das Netz an lokalen Benutzerkonten ohne Kennwort untersagt werden. Dies wird durch das Aktivieren der Richtlinie *Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken* (unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) erreicht.

Die automatische Benutzeranmeldung muss auf allen Windows-Installationen deaktiviert sein. Administrative Benutzer müssen sich explizit authentisieren. In der Wiederherstellungskonsole darf ein automatischer Login ebenfalls nicht gestattet und der Zugriff auf Daten außerhalb der Systemverzeichnisse muss eingeschränkt werden. Anderenfalls können unautorisierte Datenzugriffe stattfinden, die zudem nicht protokollierbar sind. Um dies zu erreichen, sind folgende Richtlinien zu deaktivieren: *Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen* und *Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen* (unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*).

Bei einer Standardinstallation von Clientsystemen ab Windows Vista ist das Konto des Built-In Administrator deaktiviert. Da dieses Konto in einer Standardinstallation kein Kennwort besitzt, sollte für den Built-In Administrator nachträglich ein Kennwort vergeben werden.

Alle Benutzer müssen explizit authentisiert werden, bevor ihnen der Zugang zum System gewährt wird. Die Tastenkombination STRG+ALT+ENTF sollte bei der Anmeldung erzwungen werden (Richtlinie deaktivieren: *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Interaktive Anmeldung: Kein STRG+ALT+ ENTF erforderlich*). Dies gewährleistet, dass tatsächlich das originale Anmeldefenster und kein "Nachbau" benutzt wird.

Außerdem sollte der Name des zuletzt angemeldeten Benutzers in der Anmeldemaske nicht angezeigt werden (Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*).

Es wird weiterhin empfohlen, allen Benutzern, die sich lokal anzumelden versuchen, eine Warnmeldung anzuzeigen. Der genaue Text der Warnmeldung ist anhand der konkreten Umstände und im Einzelfall festzulegen. Der Text der Warnmeldung und der Nachrichtentitel werden mit Hilfe der Richtlinien *Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen* und *Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wollen* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* eingerichtet.

Anmeldeinformationen für Domänenkonten werden standardmäßig zwischengespeichert, sodass sich ein Benutzer auch bei Nichtverfügbarkeit des Domain-Controllers an seinem Client anmelden kann. Die Anzahl solcher zwischengespeicherten Kontoinformationen wird in der Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen* festgelegt und sollte nach Möglichkeit minimiert werden. Die Parametereinstellung ist anhand konkreter Umstände und im Einzelfall festzulegen.

**Systemeinstellungen**

Die Autostart-Funktionalität ist in der Standardinstallation von Windows aktiviert und stellt ein Sicherheitsrisiko dar, da gefährliche Inhalte ohne Benutzerinteraktion zur Ausführung kommen können. Aus diesem Grund ist die Autostart-Funktionalität für alle Laufwerke zu deaktivieren (siehe auch M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung* und M 4.339 *Verhindern unautorisierter Nutzung von Wechselmedien ab Windows Vista*). Hierfür muss bei Windows XP die Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *AutoPlay deaktivieren* aktiviert und der Wert *Alle Laufwerke* eingestellt werden. Für Clientsysteme ab Windows Vista ist die Einstellung unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows Komponenten* | *Richtlinien für die automatische Wiedergabe* | *AutoPlay deaktivieren* zu finden.

Interne Systemobjekte (wie z. B. Mutexe und Semaphore, die zur Synchronisation unterschiedlicher Threads und Prozesse dienen) besitzen eigene Zugriffsrechte. Diese Zugriffsrechte können durch die Definition einer speziellen Richtlinie verstärkt werden, sodass nicht-administrative Benutzer keine Änderungsrechte an Objekten haben, die nicht von ihnen erstellt wurden (*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Systemobjekte: Standardberechtigungen interner Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken*.

Normalerweise erlaubt Windows sowohl lokalen als auch entfernten Zugriff auf Disketten und CD-ROMs. Wie in M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen* für Windows XP empfohlen wird, sollte der Zugriff jedoch

auf den gerade angemeldeten Benutzer beschränkt werden. Seit Windows Vista kann dies durch die Nutzung von Gruppenrichtlinien gesteuert werden.

**Selbstständige Internetkommunikation von Windows unterbinden**

Mehrere Windows Dienste und Anwendungen nehmen in der Standardkonfiguration selbsttätig und vom Benutzer unbemerkt Kontakt zu Servern im Internet auf. Dabei werden system- und/oder benutzerspezifische Daten an Microsoft oder andere Anbieter übermittelt.

Die nachfolgende Liste gibt einen Überblick über Dienste und Anwendungen, die selbsttätig Daten an Microsoft übertragen. Diese Liste erhebt keinen Anspruch auf Vollständigkeit.

- Internet Explorer
- Windows Store
- Windows Apps
- Windows Media Player
- Windows Defender
- Handschriftproben
- Windows Zeitdienst
- Hilfe- und Supportcenter
- Windows Update
- Gerätemanager
- Windows Aktivierung und Registrierung
- Aktualisierung der Stammzertifikate
- Ereignisanzeige
- Webdienst Assoziation
- Fehlerberichterstattung
- das Netzwerkverbindungssymbol ab Windows Vista (Der Status des Internetzugriffs wird regelmäßig aktualisiert, indem Testdaten an einen Microsoft-Server gesendet werden.)

Für die meisten der oben aufgeführten Dienste und Anwendungen wird das Abschalten der Datenübertragung empfohlen. Dies kann durch entsprechendes Umkonfigurieren von Registry und Programmoptionen, Änderungen im Dateisystem oder durch Sicherheitsgateway-Filter erfolgen. Seit der Einführung des Windows XP Service Pack 2, wurde die Verwaltbarkeit dieser Funktionalitäten deutlich verbessert. Eine neue Kategorie der Gruppenrichtlinien wurde unter *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Internetkommunikationsverwaltung* eingeführt.

**Aktivieren bzw. Einbinden von Sicherheitsfunktionen der Hardware**

Für jede am Windows-System angeschlossene und aktivierte Hardware sollte ein Treiber installiert sein.

Für Sicherheitsfunktionen wie Biometriegeräte, Smartcards und Festplattenverschlüsselung sollten nur aktuelle und von Microsoft zertifizierte Treiber verwendet werden. Falls möglich, sollte solche Hardware zusammen mit den in Windows integrierten Sicherheits-APIs verwendet werden, zum Beispiel das Biometrie-Framework und die Smartcard-Authentisierung.

Nach Möglichkeit sollten die vorhandenen Speicherschutzmechanismen wie z. B. die Datenausführungsverhinderung (DEP) oder Speicherrandomisierung (ASLR) für alle Programme und Dienste genutzt werden. Dies kann beispielsweise mit Microsofts Enhanced Mitigation Experience Toolkit (EMET) erreicht werden, das in den Hilfsmitteln zum Baustein *Client unter Windows 8* näher beschrieben ist.

**Basiseinstellungen für Group Policy Objects (GPOs)**

Die Basiseinstellungen für Gruppenrichtlinienobjekte unter Windows Gruppenrichtlinienobjekte sind in M 4.245 *Basiseinstellungen für Windows Group Policy Objects* beschrieben.

Prüffragen:

- Werden die in der Überwachungsrichtlinie festgelegten Sicherheitseinstellungen umgesetzt?
- Werden bei einem Einsatz in einer Active Directory Umgebung die Rechte zum Hinzufügen von Arbeitsstationen zur Domäne eingeschränkt?
- Wird verhindert, dass Windows Clients Anwendungen, Windows Apps oder Dienste im Netz zur Verfügung stellen?
- Ist sichergestellt, dass Windows Benutzerkonten nur von einer dazu berechtigten Person verwendet werden können?
- Werden die Zugriffsrechte und Installationsmöglichkeiten für normale Benutzer unter Windows restriktiv vergeben?
- Wurde das Gastkonto deaktiviert und mit einem komplexen Kennwort versehen?
- Ist das unter Windows XP standardmäßig angelegte Konto für den Support-Benutzer gelöscht worden?
- Wurde darauf geachtet, dass nur die unbedingt notwendigen Konten unter Windows vorhanden sind?
- Sind die automatische Benutzeranmeldung und der automatische Login in der Wiederherstellungskonsole deaktiviert worden?
- Wurde der Systemzugang auf autorisierte Personen beschränkt?
- Wurde eine entsprechende Warnmeldung für Benutzer konfiguriert, die sich lokal anzumelden versuchen?
- Wird die selbstständige Kommunikation von Windows Diensten und Anwendungen unterbunden?
- Wurde bei Clientsystemen ab Windows Vista für den Built-In Administrator ein Kennwort angelegt?
- Ist die Autostart-Funktionalität für alle Laufwerke deaktiviert worden?
- Ist die Datenausführungsverhinderung (DEP) für alle Programme und Dienste (Opt-Out Modus) aktiviert worden?

# M 4.245 Basiseinstellungen für Windows Group Policy Objects

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Mit jeder neuen Windows Client- und Server-Betriebssystemversion erscheinen auch weitere, neue Group Policy Objects. Unter den Hilfsmitteln des IT-Grundschutzes befinden sich Vorgaben für Windows XP und Windows Server 2003, die Sicherheitseinstellungen in Tabellenform enthalten. Diese können als Ausgangsbasis für die Sicherheitseinstellungen innerhalb einer Gruppenrichtlinie dienen. Die vorgeschlagenen Werte resultieren unter anderem aus Anforderungen von M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen* und M 5.123 *Absicherung der Netzkommunikation unter Windows*. Die Vorgaben für die Berechtigungsvergabe sind in M 4.247 *Restriktive Berechtigungsvergabe ab Windows Vista* und in den Hilfsmitteln des IT-Grundschutzes zu finden.

Mit den neueren Windows-Versionen werden die Einstellungsmöglichkeiten über Group Policy Objects immer komplexer. Auf der BSI-Webseite finden sich hier bei den *Hilfsmitteln/Informationen externer Anwender* technische Sicherheitsvorlagen, die die Vorgaben der IT-Grundschutz-Kataloge berücksichtigen und mit Hilfe des Security Compliance Managers von Microsoft an die eigene IT-Umgebung angepasst werden können.

Die angegebenen Werte müssen auf jeden Fall an die lokalen Bedingungen angepasst werden. Im Rahmen des Gruppenrichtlinienkonzeptes sind die einzelnen Werte zudem auf unterschiedliche Gruppenrichtlinienobjekte zu verteilen und jeweils an den Verwendungszweck anzupassen. Dadurch können für einzelne Einträge auch jeweils unterschiedliche Werte zustande kommen.

Werden die angegebenen Basiseinstellungen angepasst und insbesondere abgeschwächt, so sind mögliche sicherheitsrelevante Auswirkungen zu untersuchen, die aus diesen Änderungen resultieren.

Prüffragen:

- Wurden die Basiseinstellungen für die Windows Group Policy Objects an eigene Anforderungen angepasst?
- Wurden mögliche sicherheitsrelevante Auswirkungen untersucht, die sich aus dem Abschwächen der Basiseinstellungen der Windows Group Policy Objects ergeben?

# M 4.246 Konfiguration der Systemdienste auf Clients ab Windows XP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die sichere Konfiguration einzelner Systemdienste, die auf einem IT-System ausgeführt werden, trägt wesentlich zur Gesamtsicherheit des Informationsverbunds bei. Systemprozesse, die nicht im Benutzerkontext laufen, funktionieren unabhängig von Benutzerkonten und angemeldeten Benutzern und stellen wichtige Basisfunktionen für die Windows-Komponenten bereit. Jeder nicht benötigte, aber aktivierte Dienst kann eine Gefahrenquelle sein. Daher ist vor der Konfiguration von Windows-Clients eine Bedarfsanalyse durchzuführen. Es dürfen ausschließlich benötigte Dienste zur Ausführung kommen. Für eine zentralisierte Konfiguration der Dienste wird in einer Active Directory-Umgebung der Einsatz entsprechender Gruppenrichtlinien empfohlen. Dafür werden einzelne Dienste im Computerteil eines Gruppenrichtlinienobjektes unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Systemdienste* im Gruppenrichtlinienverwaltungs-Editor aktiviert oder deaktiviert. Die Deaktivierung der Dienste kann aber auch lokal auf dem jeweiligen System durch den Administrator vorgenommen werden.

In einer Windows Server 2003 Domänenstruktur können die Windows Vista- und Windows 7-spezifischen Konfigurationen der Dienste nur bei Einsatz des *GPOAccelerator-Tool* über Gruppenrichtlinien konfiguriert werden. Dieses betrifft:

- die Konfiguration der Startart *Automatisch (Verzögerter Start)* für die Dienste und
- die Konfiguration der unter Windows Vista und Windows 7 neu hinzu gekommenen Dienste.

Das GPOAccelerator-Tool wurde mittlerweile vollständig vom Microsoft Security Compliance Manager (MS SCM) ersetzt. Wie auch sein Vorgänger ist der SCM dafür geeignet, den Administrator bei der Konfiguration und der Umsetzung von Sicherheitsrichtlinien für Clients (ab Windows XP SP3), Server (ab Windows Server 2003 SP3) und Anwendungen (Exchange, Office und Internet Explorer) zu unterstützen. Hierfür stellt der SCM mehrere Sicherheitsvorlagen bereit, die entsprechend angepasst werden können. Nachdem der Administrator eine sogenannte Custom-Baseline mit den geforderten Sicherheitseinstellungen erstellt hat, besteht die Möglichkeit, diese als Gruppenrichtlinie auf einem Domänen-Controller zu importieren und von dort auf Domänensysteme anzuwenden. Der SCM stellt ebenfalls das Werkzeug LocalGPO bereit, das es dem Administrator erlaubt, die vorher erstellte Sicherheitsrichtlinie auf Standalone-Systeme zu importieren und anzuwenden, um so eine einheitliche Client-Konfiguration erzielen zu können. Zur Konfiguration von Systemdiensten ist der SCM ebenso geeignet.

Weitere Details zum Tool *GPOAccelerator* und *Microsoft Security Compliance Manager* sind in der Maßnahme M 4.243 *Verwaltungswerkzeuge unter Windows Client-Betriebssystemen* beschrieben.

Gerade bei neueren Betriebssystemen wie z. B. Windows 7 und Windows 8 wird ein Überprüfen und Deaktivieren von unnötigen Diensten immer wichtiger, da diese Betriebssysteme immer mehr neue Funktionen mit sich bringen, die oftmals gar nicht zum Einsatz kommen, aber dennoch ein gewisses An-

griffspotenzial durch einen aktiven Dienst bieten. Aus diesem Grund setzt Microsoft den Starttyp vieler Dienste bereits standardmäßig auf "manuell", was bewirkt, dass der Dienst nur gestartet wird, sobald er auch tatsächlich erforderlich ist oder eine Abhängigkeit zu einem anderen Dienst hat.

Zu jedem Dienst liefert Microsoft in der Dienste-Verwaltung über Gruppenrichtlinien oder mit dem SCM eine ausführliche Beschreibung, was dieser bezweckt. Aufgrund der Beschreibung sollte jeder Administrator selbst nachvollziehen können, ob der Dienst für die Umgebung, in der das System betrieben wird, notwendig ist.

Unter den Hilfsmitteln zum IT-Grundschutz werden Vorgaben für die Konfiguration der Systemdienste aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen dienen können. Es sei darauf hingewiesen, dass die Konfiguration einzelner Systemdienste immer von lokalen Gegebenheiten oder Anforderungen abhängt und daher in diesem spezifischen Kontext zu sehen ist. Im Einzelfall muss gegebenenfalls aufgrund lokaler Gegebenheiten auf weniger sichere Konfigurationen ausgewichen werden. Dann sollten aber zusätzliche Schutzmaßnahmen eingeleitet werden, die die fehlende Sicherheit in der Dienstkonfiguration ausgleichen. Beispiele hierfür sind der Einsatz einer zusätzlichen Firewall oder auch organisatorische Maßnahmen.

Zur Absicherung von Diensten unter Windows-Server-Betriebssystemen kann auch der seit Windows Server 2003 integrierte Security Configuration Wizard genutzt werden. Dieser ist in der Lage, anhand der zugewiesenen Server-Rolle zu entscheiden, welche Systemdienste zu aktivieren oder zu deaktivieren sind. Eine mit dem Assistenten erstellten Sicherheitsrichtlinie lässt sich dann auch auf andere Systeme anwenden.

Sofern für die auf dem Client laufenden Dienste ein Konto benötigt wird, empfiehlt sich der Einsatz der ab Windows 7 verfügbaren *Verwalteten Dienstkonten*. Diese Konten können über das Active Directory der Domäne verwaltet werden und ermöglichen eine Kennwortverwaltung über die Domäne, in dem das AD regelmäßig automatisierte Kennwortänderungen durchführt.

Prüffragen:

- Wurde eine Bedarfsanalyse unter Windows bezüglich der erforderlichen Systemdienste durchgeführt?
- Sind alle nicht benötigten Dienste unter Windows deaktiviert?
- Werden für die erforderlichen Systemdienste vorzugsweise *Verwaltete Dienstkonten* der Domäne eingesetzt?

# M 4.247 Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Insgesamt können unter Windows Berechtigungen in folgenden Bereichen vergeben werden:

- Dateisystem,
- Registrierung,
- Systemberechtigungen bzw. Benutzerberechtigungen,
- Berechtigungen für den Zugriff auf Freigaben in Client/Server-Netzen und Heimnetzen,
- Rechte zum Ausführen von Dateien, Skripten und Installationen,
- Integritätsstufen.

Alle Berechtigungen sind grundsätzlich restriktiv zu vergeben, das heißt die so genannten Need-to-know- oder Least-Privilege-Strategien müssen umgesetzt werden (siehe auch M 4.149 *Datei- und Freigabeberechtigungen unter Windows*). Dies betrifft ausnahmslos alle Bereiche, in denen Berechtigungen vergeben werden können. Das im Vorfeld der Einführung von Windows spezifizierte Berechtigungskonzept muss umgesetzt werden (siehe M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*).

Für hohe bis sehr hohe Schutzbedarfsanforderungen einzelner Anwendungen können die Berechtigungen über die oben genannten Maßnahmen hinaus eingeschränkt werden, wobei dann die Funktionalität und eventuell auch die Stabilität eingeschränkt wird. Bei Clients ab Windows Vista kann der Aufwand für Entwicklung und Test eines eingeschränkten, stabil laufenden Systems sehr hoch werden.

Im Folgenden werden Empfehlungen zu den oben genannten Bereichen gegeben:

**Dateisystem und Registrierung**

Die Sicherheitsgruppe *Jeder* sollte nicht verwendet werden. Für das Systemlaufwerk, üblicherweise Laufwerk C:, sollte die Sicherheitsgruppe *Authentifizierte Benutzer* in keinem der vorinstallierten Dateiordner hinzugefügt werden. Diese Gruppe sollte außerdem aus den Sicherheitseinstellungen des Stammordners entfernt werden.

In einigen Ordnern des Systemlaufwerks wird von Windows und anderer Software das Recht "Schreiben" - besonders im Ordner C:\ProgramData - an die Sicherheitsgruppe *Jeder* vergeben. Dies ermöglicht bestimmte anonyme Netzzugriffe und Skriptoperationen, welche meist nicht benötigt werden und ein Risiko darstellen. Daher sollte dieses Schreibrecht nachträglich von den einzelnen Unterordnern entfernt werden. Um diese Ordner zu finden, kann zum Beispiel das Tool *AccessChk* verwendet werden.

Bestehen hohe oder sehr hohe Schutzbedarfsanforderungen hinsichtlich der Integrität oder Vertraulichkeit, sollte nur Software installiert werden, die zu den Integritätsebenen (engl. Integrity Level), zur Ordnerstruktur und zu den standardmäßig eingeschränkten Berechtigungen von Clients ab Windows Vista

kompatibel ist. Auskunft darüber erteilen der Hersteller oder Microsoft. Weiterhin wird empfohlen, dedizierte Gruppen für einzelne Anwendungen zu definieren. Entsprechend sind die Zugriffsberechtigungen auf Software und Daten im Dateisystem und in der Registry zu vergeben. Dabei sind nicht nur systemspezifische, sondern auch anwendungsspezifische Verzeichnisse und Dateien zu identifizieren, die einem besonderen Schutzbedarf unterliegen.

Besteht ein sehr hoher Schutzbedarf hinsichtlich der Vertraulichkeit oder Integrität, sollte die Vererbung der Standardberechtigungen in Systemordnern, anderen Ordnern des Systemlaufwerks sowie in Registry-Schlüsseln deaktiviert werden, um explizite Berechtigungen für Programmdateien und Programmdaten zu vergeben. Sicherheitsgruppen wie *Authentifizierte Benutzer* oder *Administratoren* müssen dann entfernt und durch explizite Benutzerkonten ersetzt werden. Die Besitzer-Einträge von allen Ordnern, Dateien und Schlüsseln, die nicht auf *System* oder *TrustedInstaller* lauten, sollten bei einer höheren Schutzbedarfsanforderung als normal ebenfalls auf ein explizites Benutzerkonto gesetzt werden. Dadurch ist ein Angriff über andere kompromittierte Konten ausgeschlossen. Allerdings wird das System irreparabel zerstört, falls Berechtigungen falsch gesetzt werden. Der Entwicklungs- und Testaufwand ist daher nur bei sehr hohen Schutzbedarfsanforderungen sinnvoll.

Analyse-Werkzeuge von Drittanbietern wie *AccessChk* helfen dabei, abweichenden Rechte in Ordnerstrukturen und der Registry zu finden.

**Integritätsstufen**

Der ab Windows Vista verfügbare Kompatibilitätsmodus, das *Application Compatibility Toolkit* von Microsoft sowie bestimmte, auf .NET basierende Software von Drittanbietern, können einen Anwendungsprozess auf eine höhere Integritätsstufe (siehe M 4.341 *Integritätsschutz ab Windows Vista*) heben. Für hohe oder sehr hohe Schutzbedarfsanforderungen sollten solche Anwendungen unter Ausschluss weiterer Anwendungen auf isolierten Clients ausgeführt werden, um diese nicht zu gefährden. Ist dies organisatorisch nicht möglich, empfiehlt es sich, die Programmdateien und -daten gemäß dem Abschnitt Dateisystem und Registrierung in restriktiv abzusichern.

Bestehen hohe oder sehr hohe Schutzbedarfsanforderungen, sollte die Ausführung von Komponenten, die Integritätsstufen überspringen können, unterbunden werden. Dazu gehören zum Beispiel der Windows Installer und der Kompatibilitätsmodus von Windows sowie Software zur Steuerung und Aufzeichnung der Benutzerschnittstelle (Snipping-Tool, Remote-Unterstützung, VNC, Makro-Rekorder). Solche Komponenten setzen die Systemeigenschaft *UIAccess=TRUE*. Auskunft darüber erteilt der Software-Hersteller. Updates und Software können allerdings nicht installiert werden, solange der Windows Installer deaktiviert ist.

Bestehen hohe oder sehr hohe Schutzbedarfsanforderungen, kann es weiterhin sinnvoll sein, bestimmte Programmteile auf der Integritätsstufe *Gering* auszuführen. Beispielsweise bewirkt der Befehl *icacls java.exe /setintegritylevel L*, dass ein Java-Programm aus unbekannter Quelle auf der Verbindlichkeitsstufe *Gering* ausgeführt wird. Allerdings sind solche Einschränkungen mit erheblichem Aufwand für Anpassung und Test der Anwendungen verbunden.

Aufwendige programmspezifische Anpassungen der Berechtigungen und Integritätsstufen können durch Software von Drittherstellern erleichtert werden.

**Systemberechtigungen bzw. Benutzerberechtigungen**

Im Produktionsbetrieb sollten sämtliche Systemberechtigungen mittels Domänencontroller und Gruppenrichtlinien durchgesetzt werden. Keine Systemberechtigung darf auf *Nicht konfiguriert* stehen. Ansonsten könnte sie von jedem Konto mit lokalen Administratorrechten manipuliert werden.

Als Grundlage für die Erstellung der Gruppenrichtlinien empfiehlt es sich, die bei den Hilfsmitteln zum IT-Grundschutz verfügbaren Templates für den Security Compliance Manager zu verwenden und an die eigenen Anforderungen anzupassen.

**Berechtigungen für Freigaben in Client/Server-Netzen und Heimnetzen**

Freigabeberechtigungen sollten nicht an integrierte Systemgruppen wie *Authentifizierte Benutzer* oder *Jeder* erteilt werden. Weiterhin empfiehlt es sich, auf Clients alle lokalen Benutzerkonten zu deaktivieren und ausschließlich Domänenkonten mit Kerberos-Authentisierung zu verwenden.

Die Funktion *Heimnetzgruppen* ist für erhöhte Sicherheitsanforderungen nicht geeignet (siehe M 4.423 *Verwendung der Heimnetzgruppen-Funktion ab Windows 7*).

**Starten von Programmen, Skripten und Installationen**

Bestehen hohe oder sehr hohe Schutzbedarfsanforderungen, sollte der Windows Installer im Normalbetrieb deaktiviert sein. Dadurch können Updates sowie ein Großteil der Software nicht installiert werden. Zur Deaktivierung dient die Gruppenrichtlinie unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Installer* | *Windows Installer deaktivieren (Immer)*.

Prüffragen:

- Wurden alle Berechtigungen restriktiv nach den so genannten Need-to-know- oder Least-Privilege-Strategien vergeben?
- Wurde für Anwendungen unter Windows ein restriktives Berechtigungskonzept definiert und umgesetzt?
- Wurde der Sicherheitsgruppe "Jeder" das Schreibrecht innerhalb von Systemordnern entzogen?
- Werden Freigabeberechtigungen nicht an integrierte Systemgruppen wie Authentifizierte Benutzer oder Jeder erteilt?
- Sind die restriktiven Berechtigungen mit dem Patchmanagement und dem Netz- und Systemmanagement abgestimmt?

# M 4.248 Sichere Installation von Windows Client-Betriebssystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Grundlegend erreichen die Out-Of-the-Box-Installationen ab Windows Vista nicht immer ein für den professionellen Einsatz angemessenes Sicherheitsniveau. Ein eigenes Setup muss daher geplant und genutzt werden.

Während der Installationsphase ist ein Windows-System nicht vollständig konfiguriert (siehe M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* ), so dass auch die gewünschten Sicherheitseinstellungen gegebenenfalls noch nicht aktiviert sind. Die Installation und die initiale Konfiguration eines Windows-Systems sollten daher nach Möglichkeit in einer geschützten Umgebung erfolgen. Für die Erstinstallation sollten Antwortdateien und Policy-Templates herangezogen werden, da die händische Installation riskant ist. Die vorhandenen Checklisten sollten stets aktuell gehalten werden. Wo dies nicht möglich ist, beispielsweise bei der Vor-Ort-Installation von Arbeitsplatz-Systemen (lokal oder über das Netz), sollte alternativ eine vorbereitete (und vorkonfigurierte) Standardkonfiguration aufgespielt werden. Ab Windows 7 sollte diese Art der Installation stets bevorzugt werden. Beim Einsatz von Systemabbildern, den sogenannten Images-Files, ist darauf zu achten, dass vor einer Überführung des IT-Systems in den produktiven Betrieb alle zum Zeitpunkt der Überführung veröffentlichen Updates und Patches installiert werden. Ein Windows-System sollte komplett aktualisiert und mit bereits für die Institution freigegebenen Updates versorgt sein, bevor es in den produktiven Betrieb geht -insbesondere bevor es sich mit dem Internet oder Drittnetzen verbinden darf.

Ist ein Windows-System nicht in eine Active Directory-Domänenstruktur integriert, muss die Konfiguration der Gruppenrichtlinien, die auch die Sicherheitseinstellungen enthalten, lokal auf dem IT-System erfolgen. Dies sollte bei den Microsoft Betriebssystemen ab Windows Vista manuell oder skriptbasiert durchgeführt werden. Wie genau die Einstellungen vorgenommen werden, ist in der Planungsphase zu entscheiden.

Der Mechanismus der Gruppenrichtlinien ermöglicht eine schnellere, zuverlässigere, vollständige und vertraulichere initiale Konfiguration, wenn das IT-System in die Domäne aufgenommen wird. Nach dem Beitritt zur Domäne muss das IT-System-Objekt in die entsprechende Organisationseinheit (Organisational Unit, OU) im Active Directory verschoben werden. Bleibt das IT-System im standardmäßig zugewiesenen Active Directory-Container *Computer*, werden ausschließlich Standort- und Domänen-GPOs aber keine OU-GPOs angewandt, da an diesen Active Directory-Container keine OU-Gruppenrichtlinienobjekte angehängt werden können. Es ist auch darauf zu achten, dass das IT-System nach dem Verschieben in eine neue OU neu gestartet wird. Auf diese Weise werden an diese OU gelinkte GPOs auf das IT-System geladen und angewandt.

Nach der erfolgten Installation sollte sichergestellt werden, dass die entsprechenden Sicherheitseinstellungen auch tatsächlich angewandt worden sind. Dabei sind installierte Komponenten, angewandte Richtlinien, Berechtigungen

im Dateisystem und in der Registrierung, zugewiesene Benutzerrechte und erlaubte Systemdienste zu überprüfen.

Für Windows Vista und Windows 7 gilt ergänzend, dass das Betriebssystem nach der erfolgten Installation aktiviert werden muss. Ein nur installiertes und nicht aktiviertes Windows Vista ohne Service Pack 1 (SP1) ist nach Ablauf einer definierten Kulanzfrist (Grace Period) von 30 Tagen nicht mehr arbeitsfähig. Der Vista Client fällt zwangsweise in den so genannten Reduced Functionality Mode (RFM), in dem nur noch eingeschränkte Funktionalitäten zur Verfügung stehen. Mit dem Erscheinen des Service Pack 1 für Windows Vista hat Microsoft den RFM zurückgenommen. Anstelle des RFM zeigen Windows Vista und Windows 7 nun entsprechende Warnmeldungen an, die allerdings ebenfalls geeignet sind, kritische Arbeiten an einem Windows Vista oder Windows 7 System zu behindern oder zu verzögern.

Bei Clients ab Windows 8 (außer Enterprise) muss der Produkt-Schlüssel nun schon während der Installation eingegeben werden. Bei Windows 8 Enterprise werden anstatt des Produkt-Schlüssels die Mechanismen KMS (Key Management Service) und MAK (Multi Activation Key) eingesetzt.

Das Thema Aktivierung wird in M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* und M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* vertieft.

**Domänenmitgliedschaft**

Um ein IT-System zu einer Domäne hinzuzufügen, muss entweder ein entsprechendes Computerkonto in der Domäne vorbereitet worden sein oder das Computerkonto wird beim Beitritt erzeugt. Dazu sind entsprechende administrative Berechtigungen notwendig, mit denen restriktiv umgegangen werden muss. Ob das Computerkonto vor oder während der Installation erstellt werden soll, ist in Abhängigkeit von der gängigen Praxis des Unternehmens oder der Behörde zu entscheiden.

Zukünftige Domänenmitglieder sollten während der Installation in die Domäne aufgenommen und nicht erst als Einzelsystem installiert werden. Dadurch wird beispielsweise gewährleistet, dass die einfache Dateifreigabe deaktiviert bleibt und keine zusätzlichen lokalen Benutzer mit administrativen Berechtigungen angelegt werden.

**Unbeaufsichtigte Installationen**

Windows bietet einen Mechanismus zur unbeaufsichtigten Installation des Betriebssystems. Hierbei wird die Installation unter Verwendung einer vorgefertigten Antwortdatei und ohne Interaktion mit dem Administrator durchführt. Diese Antwortdatei, die die notwendigen Installationseingaben enthält, wird im Vorfeld einer Windows XP Installation mit dem Installations-Manager *Setup Manager* erstellt.

Clients ab Windows Vista nutzen zur unbeaufsichtigten Installation des Betriebssystems die Antwortdatei *Unattend.xml*. Diese Antwortdatei kann mit dem *Windows-Systemabbild-Manager* erstellt und geändert werden. Der *Windows-Systemabbild-Manager* ist Bestandteil des *Windows Automated Installation Kit (WAIK)*. Das WAIK ist nicht auf den Installationsmedien von Clients ab Windows Vista enthalten, kann jedoch über die Internetseiten von Microsoft bezogen werden. Im neuen Bereitstellungswerkzeug *Business Desktop Deployment (BDD)* für Clients ab Windows Vista ist das WAIK bereits enthal-

ten. Das BDD enthält Funktionen um das Betriebssystem ab Windows Vista zu planen, aufzubauen, zu testen und bereitzustellen. Das Windows Assessment and Deployment Kit (Windows ADK) ist der Nachfolger des WAIK. Mit Hilfe des ADK und seinen Tools kann das Windows-Betriebssystemen personalisiert, bewertet und bereitgestellt werden. Für Betriebssysteme ab Windows 8 stellt Microsoft auf seiner Homepage das Deployment Kit (MDT), eine Sammlung von Tools, Prozessen und Anleitungen in einer grafischen Oberfläche, zur Verfügung.

Werden Windows-Systeme unbeaufsichtigt installiert, so ist Folgendes zu berücksichtigen:

- Sensitive Informationen wie Kennwörter in Antwortdateien müssen vor unberechtigter Einsichtnahme geschützt sein. Die verwendeten Kennwörter sind beim Erstellen der Antwortdatei mit dem Installations-Manager *Setup Manager* oder bei Clients ab Windows Vista mit dem *Windows-Systemabbild-Manager* zu verschlüsseln.
- Der Umgang mit Kennwörtern für die Aufnahme in die Domäne, die in einem Installationsskript oder einer Antwortdatei verwendet werden, muss definiert sein. Da sich diese Funktion nicht verschlüsseln lässt, sollte ein IT-System über die Windows Bereitstellungsdienste (Windows Deployment Services WDS) der Domäne beitreten.
- Das Administrator-Kennwort darf im Rahmen der unbeaufsichtigten Installationen unter Windows XP nicht leer sein, da sonst die automatische Anmeldung selbsttätig aktiviert wird. Bei Clients ab Windows Vista wird die automatische Anmeldung im Rahmen der unbeaufsichtigten Installationen nur durch eine entsprechende Konfiguration der zugehörigen vorgefertigten Antwortdatei aktiviert.
- Nach der Installation müssen die Skripte sowie alle Dateien mit vertraulichem Inhalt umgehend sicher gelöscht werden (siehe auch M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*).

**Angepasste Installationsmedien**

Wenn Windows von möglicherweise veralteten Originalmedien installiert wird, müssen nach der Installation die existierenden Patches, Service Packs und Updates gesondert eingespielt werden. Dies verlängert die Installationszeit und erhöht das Risiko eines erfolgreichen Angriffs auf das IT-System, da es sich für eine gewisse Zeit nicht auf dem aktuellen Stand befindet. Um die Updates gleich bei der Installation einzuspielen und das Risiko eines erfolgreichen Angriffs zu mindern, kann eine der beiden, mit Windows XP eingeführten, Installationsfunktionen verwendet werden:

- integrierte Installation (auch Slipstream-Installation bezeichnet) oder
- kombinierte Installation.

Bei Clients ab Windows Vista können Updates während der Installation mit dem Bereitstellungswerkzeug BDD beziehungsweise MDT 2010 eingespielt werden. Bei der integrierten Installation wird Windows zusammen mit einem Service Pack installiert. Die kombinierte Installation ermöglicht die Installation des Betriebssystems zusammen mit Hotfixes und zusätzlichen Anwendungen im unbeaufsichtigten Modus.

Für eine integrierte Installation wird ein neues Installationsmedium erstellt. Dabei werden die Originaldateien durch Dateien des Service Packs überschrieben. Mögliche Installationsmedien sind optische Datenträger wie CD-ROM oder DVD, Netz-Distributionsfreigaben oder Installationsordner der Remoteinstallationsdienste (RIS) beziehungsweise die Windows Deployment Services

(WDS). Es ist zu beachten, dass ein Service Pack, das im integrierten Modus installiert wurde, nicht deinstalliert werden kann.

Ein kombiniertes Installationsmedium wird erstellt, indem zusätzliche Installationsdateien in das Original-Installationsmedium integriert werden. Die Antwortdatei für die unbeaufsichtigte Installation (standardmäßig wird sie *Unattend.txt* beziehungsweise bei Clients ab Windows Vista *AutoUnattend.xml* genannt) und *cmdlines.txt* müssen entsprechend angepasst werden. Die genaue Vorgehensweise ist der Dokumentation von Microsoft zu entnehmen.

Der Einsatz von angepassten Installationsmedien ist grundsätzlich zu empfehlen. Welches der beiden Verfahren bei einem Unternehmen oder einer Behörde eingesetzt werden soll, ist im Einzelfall zu entscheiden. Für Windows XP ist dabei M 2.329 *Einführung von Windows XP SP2* zu beachten.

Seit Windows Vista ist zur Verteilung lediglich die Anpassung des WIM-Images erforderlich. Das WIM-Image ist ein Betriebssystem-Abbild mit dem Format WIM. Dieses wird entweder auf Wechseldatenträgern oder im Netz bereitgestellt. Für zeitnahe Änderungen und Updates werden während des Installationsprozesses eine Serverfreigabe oder ein WSUS-Server abgefragt. Dies ist aber nicht zwingend notwendig.

**Systemkomponenten**

Bei der Installation des Systems ist zu gewährleisten, dass nur die benötigten Systemkomponenten installiert werden. Je nach existierenden geschäftlichen Anforderungen der Institution können weitere Komponenten installiert werden, die in der Tabelle in den Hilfsmitteln zum IT-Grundschutz als *Optional* markiert wird. Von der Installation der Windows-Komponenten, die mit *Deaktiviert* markiert sind, ist aus Sicherheitssicht abzuraten.

**TPM-Nutzung ab Windows 8**

Je nach Einsatzentscheidung aus M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* muss das TPM in den Firmware-Einstellungen abgeschaltet oder ggf. für die Verwendung initialisiert werden. Die genaue Vorgehensweise hierbei sowie die anschließenden Nutzungsmöglichkeiten des TPMs durch das Betriebssystem unterscheiden sich je nach Firmware-Version, Version des TPMs und Version des Betriebssystems.

Prüffragen:

- Ist sichergestellt, dass Windows-Systeme erst nach der vollständigen Installation, Konfiguration und dem Einspielen aller Patches und Updates produktiv ins Netz gehen?
- Wird gewährleistet, dass bei der Installation von Windows-Systemen nur die benötigten Systemkomponenten installiert werden?
- Ist sichergestellt, dass die erforderlichen Windows-Sicherheitseinstellungen nach der Installation auch tatsächlich konfiguriert werden (installierte Komponenten, angewandte Richtlinien, Berechtigungen im Dateisystem/ Registry, zugewiesene Benutzerrechte, erlaubte Systemdienste usw.)?
- Sind Kennwörter in Installationsskripten und Konfigurationsdateien geschützt und wurden diese nach der Installation vom System gelöscht?
- Wird bei einer unbeaufsichtigten Installation von Windows ein Administrator-Kennwort vergeben?
- Sind die Vor- und Nachteile des Einsatzes eines TPM abgewogen und eine Entscheidung zur Verwendung im Betriebssystem getroffen worden?

# M 4.249 Windows Client-Systeme aktuell halten

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Die Vergangenheit hat gezeigt, dass sicherheitsrelevante Updates oder Patches, die Microsoft regelmäßig veröffentlicht, zeitnah installiert werden müssen. In der Praxis führt dies jedoch öfter zu Problemen, da die Updates einerseits so schnell wie möglich eingespielt werden müssen, sie andererseits vor der Installation ausgiebig getestet werden sollen. Für dieses Problem existiert keine allgemeingültige Lösung. Hier ist ein geeigneter Kompromiss einzugehen, der den Anforderungen an Sicherheit und Praktikabilität gerecht wird.

M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* muss bei der Planung berücksichtigt sein.

- Es muss ein Prozess für den Umgang mit Patches und Updates auf organisatorischer Ebene etabliert sein (z. B. im Rahmen des Änderungsmanagements).
- Der Prozess muss nicht nur Updates und Patches für Windows-Systeme, sondern auch für eingesetzte Anwendungen (z. B. Microsoft Internet Explorer, Microsoft Office und insbesondere Software von Drittherstellern) berücksichtigen.
- Administratoren müssen sich regelmäßig über Schwachstellen und verfügbare Sicherheits-Updates informieren.
- Das Einspielen und Prüfen der Updates auf einem Test-System muss sichergestellt werden.
- Es muss eine Strategie zum Wiederherstellen der Funktionsfähigkeit der Systeme im Problemfall vorhanden sein.

**Überprüfung des Patch-Standes**

Um existierende Windows-Systeme aktuell zu halten, muss der aktuelle Patch-Stand der Systeme mit den von Microsoft verfügbaren Updates verglichen werden. Microsoft stellt mit dem *Baseline Security Analyzer* (MBSA) ein Tool zur Verfügung, das für die automatische Auswertung der Systemstände eingesetzt werden kann. Der Einsatz dieses oder eines vergleichbaren Tools verschafft den Administratoren einen aktuellen Überblick über den Patch-Stand der Systeme und trägt somit wesentlich zur Gesamtsicherheit bei. Das MBSA-Tool kann so konfiguriert werden, dass die Überprüfung nicht gegen einen Microsoft-Server im Internet, sondern gegen intern aufgesetzte Microsoft Windows Server Update Services (WSUS) erfolgt. Auf diese Weise wird der Ist-Zustand der Systeme mit dem unternehmensspezifischen Soll-Zustand verglichen. Diese Vorgehensweise wird vor allem für Tests verwendet, ob die im Unternehmen freigegebenen Patches und Updates auf allen Systemen installiert sind. Durch die Integration von MBSA in Microsoft Systems Management Server (SMS) können die Testergebnisse auch direkt in der SMS-Datenbank gespeichert werden.

Das MBSA-Tool besitzt eine graphische Bedienungsoberfläche (*mbsa.exe*), kann aber auch über die Kommandozeile gesteuert werden (*mbsacli.exe*). Mit Letzterem lässt sich das Tool in einen automatisierten Prozess integrieren, so dass die Ergebnisse ebenfalls automatisch (z. B. mit Skripten) weiterverarbeitet werden können.

Mit dem MBSA-Tool kann der Patch-Stand des Betriebssystems und weiterer Anwendungen von Microsoft wie Microsoft Office, Exchange Server, Microsoft

Internet Explorer (hier speziell auch die Zonen-Konfiguration) überprüft werden. Die Überprüfungen können lokal und weitgehend auch entfernt durchgeführt werden.

**Aktualisierungsmethoden**

Zum Aktualisieren eines Windows Systems kann die integrierte *Automatische Updates* Funktionalität von Windows verwendet werden oder die Updates und Patches werden mittels anderer (externer) Software-Verteilungsmechanismen installiert. Nach welcher Strategie verfahren werden soll, ist anhand der konkreten Umstände und im Einzelfall festzulegen. Wird ein externer Software-Verteilungsmechanismus verwendet, so ist die *Automatische Updates* Funktionalität zu deaktivieren, damit durch ihren parallelen Einsatz keine negativen Wechselwirkungen entstehen können.

Wird die automatische Aktualisierung von Windows verwendet, so stehen folgende Konfigurationsmöglichkeiten zur Verfügung:

- Updates werden automatisch heruntergeladen und entsprechend dem definierten Zeitplan installiert (in Windows XP ohne Service Pack 1 steht diese Funktionalität erst in der aktualisierten Version von *Automatische Updates* Software zur Verfügung).
- Updates werden automatisch heruntergeladen, es findet jedoch keine automatische Installation statt. Der Benutzer wird über zur Verfügung stehende Updates informiert.
- Beim Vorhandensein neuer Updates erfolgt lediglich eine Benachrichtigung des Administrators, die Updates werden nicht heruntergeladen.
- ab Windows Vista können Updates, die empfohlen, aber nicht kritisch sind, kurzfristig direkt an einzelnen Clients von der automatischen Installation ausgenommen werden (*Windows Update* | *Einstellungen ändern* | *Empfohlene Updates*). Im Normalfall sollte die Auswahl der Updates jedoch zentral mittels Softwareverteilung gesetzt werden.

Von der manuellen Installation der Updates sollte abgesehen werden. Um die Zeitspanne zwischen dem Bekanntwerden und dem Schließen einer Sicherheitslücke möglichst kurz zu halten, wird die automatische Installation von freigegebenen Updates mit dem *Automatische Updates* Mechanismus oder einem externen Software-Verteilungsmechanismus empfohlen.

Da aus Sicherheitssicht direkte Verbindungen ins Internet zu vermeiden sind und die zu installierenden Updates zuerst in Testsystemen getestet werden sollten, wird eine direkte Aktualisierung von Windows-Systemen von externen Quellen (z. B. Microsoft) beim Einsatz des *Automatische Updates* Mechanismus nicht empfohlen. Stattdessen sollten die Windows-Systeme durch die entsprechende Konfiguration angewiesen werden, einen institutionsinternen Update-Server zu benutzen. Auf diese Weise lässt sich der folgende sinnvolle Ablauf einer Aktualisierung realisieren:

- Administratoren werden über die Bereitstellung eines Updates benachrichtigt.
- Das Update wird heruntergeladen und auf Testsystemen installiert.
- Nach erfolgreich abgeschlossenen Tests wird das Update für interne Update-Server freigegeben.
- Windows-Rechner laden das freigegebene Update von einem internen Update-Server herunter und installieren es.

**Anwendungssoftware und Tools**

Die Update-Funktionen von Anwendungssoftware und Tools funktionieren häufig nicht mit normalen Benutzerberechtigungen und zeigen dem Benutzer

störende oder verwirrende Meldungen an. Solche Meldungen sollten vom Administrator vermieden werden, zum Beispiel, indem die Update-Pakete in Softwareverteilungssysteme eingebunden werden oder *Geplante Tasks* (Windows XP) beziehungsweise *Aufgabenplanung* (ab Vista) genutzt wird.

**Benutzer informieren**

Auf viele Updates folgen ein Neustart und einige automatische Systemaktivitäten, die die Arbeitsgeschwindigkeit für einige Zeit beeinträchtigen. Nach Neustarts können Meldungen oder Fortschrittsanzeigen, erscheinen, die für manche Benutzer verwirrend sind. Der erfolgreiche Abschluss der Prozesse darf jedoch nicht gefährdet werden, etwa durch manuell ausgelöste Neustarts. Daher sollten Benutzer vor größeren Updates über mögliche Beeinträchtigungen informiert werden. Weiterhin sollten stichprobenartig Rückmeldungen von den Benutzern eingeholt werden und in die Verbesserung des Update-Zyklus einfließen.

**Verifikation der Systeme**

Nach einem Upgrade oder einer größeren Systemänderung (z. B. dem Einspielen eines neuen Service Packs) sollten für einige Tage die Windows-Protokolle und Software-Protokolle auf bisher unbekannte Fehler beobachtet werden. Stichprobenartig sollten auch einige Clients daraufhin überprüft werden, ob

- alle Updates erfolgreich installiert wurden (Windows Systemprotokoll),
- anwendungsspezifische Berechtigungen und Sicherheitseinstellungen noch korrekt sind (manuell oder mit Hilfe von Sicherheitsvorlagen), besonders in den Windows-Ordnern, bei Netzwerk und Firewall und
- ob Anwendungen, Schutzsoftware und -hardware korrekt funktionieren.

Prüffragen:

- Gibt es einen regelmäßigen Abgleich mit dem aktuellen Patch-Stand der Systeme und den von Microsoft verfügbaren Updates?
- Informieren sich die Administratoren regelmäßig über Schwachstellen und verfügbare Sicherheits-Updates?
- Ist die Strategie für die Aktualisierung von Windows Client-Systemen festgelegt?
- Berücksichtigt die definierte Update-Strategie für Windows Client-Systeme auch anwendungsspezifische Updates, zum Beispiel von Drittherstellern?
- Ist die Vertrauenswürdigkeit der Update-Quellen für Windows Client-Systeme gewährleistet?
- Ist gewährleistet, dass nur getestete und freigegebene Updates auf Windows Client-Systemen installiert werden?
- Gibt es eine Strategie zur Wiederherstellung der Funktionsfähigkeit der Systeme bei Problemen oder Fehlern?

# M 4.250 Auswahl eines zentralen, netzbasierten Authentisierungsdienstes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

IT-Systeme aller Art sollten grundsätzlich sicherstellen, dass sich alle Benutzer, die darauf zugreifen möchten, authentisieren müssen. Nur so kann verhindert werden, dass unautorisierte Personen Zugriff auf die Dienste erlangen, die das System anbietet, oder auf die Daten, die auf dem System gespeichert sind. Eine Ausnahme bilden nur solche IT-Systeme, die allgemein zugänglich sein sollen wie öffentliche Informationsdienste (beispielsweise öffentliche Webserver) oder Ähnliches.

Nachdem die Authentisierung erfolgreich abgelaufen ist, muss das System sicher stellen, dass die Benutzer nur auf solche Dienste und Daten Zugriff erhalten, für die sie entsprechende Berechtigungen besitzen.

Oft soll die Authentisierung nicht lediglich für einen einzelnen Dienst oder auf einem einzelnen System erfolgen, sondern es sollen zumindest für verschiedene Dienste und auf unterschiedlichen Systemen dieselben Authentisierungsdaten (etwa Benutzername und Passwort) genutzt werden können. In einem solchen Fall ist ein zentraler, netzbasierter Authentisierungsdienst erforderlich, damit die Authentisierungsdaten nicht auf jedem beteiligten System einzeln verwaltet und aktualisiert werden müssen.

Den Extremfall stellt hier das sogenannte "Single Sign-On" dar, bei dem eine Authentisierung zentral für alle Dienste eines IT-Verbunds erfolgt. Dies hat den Vorteil, dass die Benutzer sich nur einmal anmelden müssen. Die Benutzer benötigen nur jeweils ein Passwort oder Token und müssen sich somit nicht verschiedene Passwörter merken oder eine Vielzahl von Token aufbewahren. Andererseits wird einem Angreifer aber der Zugriff auf alle Dienste des IT-Verbunds ermöglicht, wenn er sich einmal als Benutzer anmelden konnte.

Soll ein zentrales, netzbasiertes Authentisierungssystem eingesetzt werden, so ist eine sorgfältige Planung besonders wichtig, da die Funktion und die Sicherheit eines solchen Systems entscheidende Faktoren für die Sicherheit des gesamten IT-Verbundes sind.

Die zentrale Authentisierung kann durch einen Einsatz eines zentralen Authentisierungssystems wie Kerberos erreicht werden. Kerberos bietet im weiterem den Vorteil, dass neben Unix-Systemen auch unter Windows-Betriebssysteme eine Kerberos-Authentisierung verwendet werden kann.

Auf wichtige Empfehlungen, die für die Auswahl und den Einsatz eines netzbasierten Authentisierungsdienstes berücksichtigt werden müssen, wird im Folgenden tiefer eingegangen:

**Verschlüsselung der Netz-Protokolle**

Im Gegensatz zu einer lokalen Benutzerverwaltung werden kritische Informationen, die für eine netzbasierte Authentisierung benötigt werden, über ein LAN oder WAN übertragen. Daher ist es zwingend erforderlich, dass diese Informationen nicht mitgelesen oder verändert werden können.

Außerdem muss sichergestellt werden, dass ein Angreifer sich nicht anmelden kann, indem er aufgezeichnete Anmeldeinformationen wieder einspielt. Daher müssen die Anmeldeinformationen, die für die Authentisierung zwischen Server und Client ausgetauscht werden, verschlüsselt und zusätzlich, beispielsweise mit Challenge-Response-Verfahren, dynamisiert werden.

**Schutz des Authentisierungsservers**

Generell werden alle für eine Authentisierung benötigten Informationen auf einem zentralen Server abgelegt. Daher ist sicherzustellen, dass keine unautorisierten Personen an diese kritischen Informationen gelangen können. Ein Authentisierungsserver muss also auf allen Ebenen sorgfältig geschützt werden (der Schutzbedarf ist vergleichbar mit dem eines Sicherheitsgateways). Hierzu gehört unter anderem:

- Er sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann der Authentisierungsserver alternativ in einem Serverschrank aufgestellt werden (siehe Baustein B 2.7 *Schutzschränke*).
- Er darf sich nur innerhalb eines geschützten Netzes befinden.
- Auf einem Authentisierungsserver sollten nur die dafür erforderlichen Dienste verfügbar sein und möglichst keine weiteren Dienste angeboten werden, zumindest keine mit niedrigerem Schutzbedarf, wie z. B. ein Webserver. Außerdem dürfen nur Programme installiert sein, die für die Funktionsfähigkeit nötig sind.
- Für die Konzeption und den Betrieb eines Authentisierungsservers muss geeignetes Personal mit ausreichend Ressourcen zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Authentisierungsservers darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt oft viel Zeit in Anspruch. Die Administratoren müssen fundierte Kenntnisse der eingesetzten IT-Komponenten besitzen und entsprechend geschult werden.
- Nur Administratoren dürfen sich auf diesem System anmelden können. Die Vergabe von Administrationsrechte muss sorgfältig dokumentiert sein. Besonders sicherheitskritische Eingriffe sollten möglichst im Vieraugenprinzip erfolgen. Administratoren sollten für die Anmeldung starke Authentisierungsmethoden benutzen.
- Die Administration des Authentisierungsservers darf nur über einen gesicherten Zugang möglich sein, also z. B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz (Administrationsnetz).
- Die korrekte Konfiguration eines Authentisierungsservers ist wesentlich für dessen sicheren Betrieb. Fehler in der Konfiguration können zu Sicherheitslücken oder Ausfällen führen. Die bestmögliche Konfiguration muss sorgfältig dokumentiert sein.
- Betriebssystem und Programme eines Authentisierungsservers müssen jederzeit auf einem sicheren Patch-Stand sein.
- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*). Im Fehlerfall muss der Authentisierungsserver abgeschaltet werden.
- Es muss klar dokumentiert sein, welche Ereignisse protokolliert werden müssen (M 5.9 *Protokollierung am Server*), wo diese gespeichert werden und wie und in welchen Abständen sie ausgewertet werden.
- Authentisierungsserver müssen in das organisationsweite Datensicherungskonzept sowie in das Notfallvorsorgekonzept integriert sein. Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet

werden, dass Benutzer- und Rechteverwaltung auf dem aktuellsten Stand sind.
- Für einen sicheren Betrieb eines Authentisierungsservers sind die umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre korrekte Einhaltung zu überprüfen. Durch regelmäßige Audits muss der sichere Betrieb überprüft werden.

Weiterhin ist bei einer zentralen Verwaltung ein Ausfall des Servers oder des Netzes zu berücksichtigen, was nach einem Denial-Of-Service-Angriff der Fall sein kann. Wenn alle weiteren Rechner im Netz von dem Server für eine Authentisierung abhängig sind, weitet sich der Denial-Of-Service-Angriff auf alle Systeme im Netz aus. Daher wird der Einsatz eines hochverfügbaren Systems empfohlen, das mit dem Einsatz eines redundanten Servers (siehe M 6.43 *Einsatz redundanter Windows-Server*) realisiert werden kann.

Da eine verlässliche Authentikation für die Sicherheit jedes Netzes eine zentrale Rolle spielt, ist der sichere und ordnungsgemäße Betrieb des Authentisierungsservers besonders wichtig. Daher muss das gewählte Vorgehen in die bestehende organisationsweite Sicherheitsleitlinie integriert werden.

**Passwörter**

Analog zur Maßnahme M 2.11 *Regelung des Passwortgebrauchs* sind geeignete Vorkehrungen für eine hohe Passwortgüte zu treffen.

**Protokollierung**

Das Authentisierungssystem muss die aus der Maßnahme M 5.9 *Protokollierung am Server* bekannten Ereignisse erfassen können.

Alle Logdateien sollten zentral auf dem Server abgelegt werden. Da dies die Erstellung detaillierter Benutzerprofile ermöglicht, muss aus Gründen des Datenschutzes verhindert werden, dass diese Informationen von unautorisierten Personen ausgelesen werden können.

Wird ein zentraler Protokollierungsserver eingesetzt, sollte gewährleistet werden, dass die übertragenen Daten nicht abgehört werden können. Dies kann beispielsweise durch den Einsatz von Übertragungsprotokollen, die die Verschlüsselung der Daten ermöglichen, eine VPN-Verbindung oder durch ein separates Netz zwischen den zentralen Authentisierungsserver und dem Protokollierungsserver erfolgen.

Prüffragen:

- Wurde bei Einsatz von einem zentralen netzbasierten Authentisierungsdienst der Einsatz sorgfältig geplant?
- Wurden die für die Auswahl eines zentralen, netzbasierten Authentisierungsdienstes relevanten Sicherheitsanforderungen dokumentiert?

# M 4.251 Arbeiten mit fremden IT-Systemen

**Verantwortlich für Initiierung:** Benutzer, IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Benutzer

Häufig ist es erforderlich, auch unterwegs auf elektronische Informationen verschiedenster Art zugreifen zu können, z. B. um Terminkalender abgleichen zu können, E-Mails zu verschicken oder einzelne Dateien abrufen zu können. Hierfür ist es häufig das einfachste, fremde IT-Systeme oder Kommunikationsanbindungen zu benutzen, also beispielsweise

- aus einem Internet-Cafe Dateien herunterzuladen,
- in einem Büro einer besuchten Institution über deren PCs oder deren Intranet oder
- über WLAN über einen Hotspot im Hotel auf das Firmennetz zuzugreifen.

Hierbei sollte sich aber jeder Benutzer darüber im Klaren sein, das dies fremdadministrierte IT ist und daher zusätzliche Sicherheitsmaßnahmen zu ergreifen sind. Es sollte immer davon ausgegangen werden, dass das Sicherheitsniveau der fremden Umgebung nicht bekannt ist und damit als niedrig eingeschätzt werden muss. Jeder Mitarbeiter sollte sich bewusst sein, dass fremde Rechner und fremde Umgebungen grundsätzliche höhere Sicherheitsrisiken darstellen. Selbst wenn das Sicherheitsniveau einen ausgezeichneten Eindruck macht, kann dies ein Trugschluss sein.

Beispielsweise kann die momentane Netzumgebung schlechter geschützt sein als der eigene Laptop, so dass damit Probleme wie z. B. Computer-Viren oder Trojanische Pferde importiert werden können. Es kann sich auch herausstellen, dass in einer besuchten Institution ein völlig anderes Verständnis von Sicherheit herrscht, so dass kein Konsens über Sicherheitsziele, Sicherheitsniveau und Sicherheitsmaßnahmen existiert.

In mobilen Netzen kann es passieren, dass die Netzteilnehmer ständig wechseln, also neue hinzukommen und andere das Netz verlassen. Damit ist es schwer, nachzuvollziehen, wer zu einem bestimmten Zeitpunkt ebenfalls in diesem Netz aktiv war. Mobile Netze sind dadurch anfällig für Angriffe, die unter Umständen nicht einmal nachvollziehbar sind, und alle Aussagen über ein vorhandenes Sicherheitsniveau sind sehr schwierig.

Bevor sich Benutzer in fremden Netzen anmelden oder Dienstleistungsangebote nutzen, sollten sie sich darüber Gedanken machen, wie vertrauenswürdig diese sind. Extrem günstige Angebote könnten speziell dazu eingerichtet worden sein, um Daten auf mobilen Endgeräte auszuspähen oder zu manipulieren. Beispielsweise könnte ein Angreifer einen kostenfreien Internet-Zugang oder WLAN-Zugang zur Verfügung stellen, um so auf einfache Weise die von dort übertragenen Daten mitlesen zu können.

Auch bei der Nutzung verhältnismäßig einfacher, überschaubarer Dienstleistungen müssen die Benutzer die unerlässliche Sorgfalt bewahren. Beispielsweise kann es unterwegs erforderlich sein, Ausdrucke vom Laptop aus anzufertigen. Dazu können dann etwas Druckdienste in Hotels, in Internetcafes oder Kopierläden genutzt werden oder auch auf die Drucker in einer besuchten Firma zugegriffen werden. Dabei werden allerdings mit dem Druckjob zumindest auch die gedruckten Informationen Externen zugänglich gemacht, nämlich den jeweiligen Dienstleistern. Die zu druckende Datei muss an den

Drucker übertragen werden und wird dabei unter Umständen auf IT-Systemen zwischengespeichert. Ausdrücke können unbemerkt mehrfach angefertigt werden oder es kann schlicht Papier am Drucker liegen bleiben.

Daher sollten Benutzer folgende Empfehlungen beachten, bevor sie mit fremden IT-Systemen arbeiten oder Dienstleistungsangebote nutzen:

- Sie sollten sich über vorhandene Sicherheitsmaßnahmen informieren.
- Sie sollten sich genau überlegen bzw. sich an den Vorgaben und Regelungen für die mobile IT-Nutzung orientieren und fremde IT-Systeme oder Dienstleistungsangebote nicht für alle denkbaren Aktionen und Daten benutzen.
- Sobald die Arbeit beendet wurde, sollten bei einem fremden Rechner grundsätzlich alle währenddessen entstandenen temporären Daten gelöscht werden. Dies ist allerdings meistens nicht einfach, da bei vielen Betriebssystemen temporäre Daten an einer Vielzahl von Stellen entstehen. Außerdem kann es bei fremden IT-Systemen auch vorkommen, dass die Zugriffsrechte ein Löschen aller entstandenen Daten nicht zulassen. Zumindest sollte der Zwischenspeicher (Cache) gelöscht werden.
- Auf keinen Fall sollten Browser-Funktionen zur "Auto-Vervollständigung" von Benutzernamen und Passwörtern genutzt werden, damit nachfolgende Benutzer keine einfache Möglichkeit vorfinden, sich unter diesem Benutzernamen irgendwo anzumelden.

Prüffragen:

- Sind alle Mitarbeiter darüber informiert, was sie bei der Nutzung fremder IT beachten sollten?
- Wissen alle Mitarbeiter, dass sie bei fremden IT-Systemen nach Beendigung der Arbeiten grundsätzlich alle währenddessen entstandenen temporären Daten löschen müssen?
- Wissen alle Mitarbeiter, dass sie auf keinen Fall Browser-Funktionen zur "Auto-Vervollständigung" oder Speicherung von Passwörtern nutzen dürfen?

# M 4.252 Sichere Konfiguration von Schulungsrechnern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um Sicherheitsprobleme und die ungewünschte Nutzung von Schulungsrechnern zu vermeiden, sind eine minimale Konfiguration der Rechner und eine restriktive Rechtevergabe (siehe M 2.63 *Einrichten der Zugriffsrechte* und M 4.135 *Restriktive Vergabe von Zugriffsrechten auf Systemdateien*) erforderlich. Empfehlungen zur Konfiguration von Schulungsrechnern können der Maßnahme M 4.95 *Minimales Betriebssystem* entnommen werden.

Vor dem Einsatz von Schulungsrechnern sollte festgelegt werden, welche Anwendungen und Kommunikationsschnittstellen in der jeweiligen Schulung genutzt werden sollen. Durch die Festlegung einer Standardkonfiguration für die Schulungsrechner (siehe M 2.69 *Einrichtung von Standardarbeitsplätzen*) kann der Installationsaufwand minimiert und ein Mindestniveau an Sicherheit für die Schulungsrechner gewährleistet werden. Vor jeder Schulung muss überprüft werden, ob die Konfiguration der Rechner für die Zwecke der Schulung geeignet ist. Um hier auf langwierige Prüfungen verzichten zu können, ist es sinnvoll, Schulungsrechner vor jedem Einsatz über entsprechend vorbereitete Pakte neu zu installieren (siehe M 4.109 *Software-Reinstallation bei Arbeitsplatzrechnern*).

Von Schulungsrechnern sollten Informationen wie Schulungs- oder Prüfungsunterlagen nicht unkontrolliert kopiert werden können und es sollten auch keine zusätzlichen Dateien oder Programme aufgespielt werden können (z. B. Spickzettel für Prüfungen). Daher sollten einerseits restriktive Zugriffsrechte für die Benutzer dieser Rechner vergeben werden und andererseits das Überspielen von Daten auf externe Medien verhindert werden (siehe auch M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).

Es ist außerdem zu überlegen, ob und in welchem Umfang es notwendig ist, Datensicherungen durchzuführen, beispielsweise wenn Übungsaufgaben oder Prüfungsergebnisse gesichert werden sollen.

Auf den Schulungsrechnern sollten zusätzliche Sicherheitsprogramme installiert werden, falls diese nicht schon Teil des Betriebssystems sind. Vor allem sinnvoll sind ein Integritätsprüfprogramm (siehe M 4.93 *Regelmäßige Integritätsprüfung*) und ein Softwarepaketfilter. Empfehlenswert sind zusätzlich Programme zur Virensuche und zur Auswertung der Protokolleinträge.

Prüffragen:

- Wird bei Schulungsrechnern eine minimale Konfiguration sowie eine restriktive Rechtevergabe umgesetzt?
- Ist festgelegt, welche Anwendungen und Kommunikationsschnittstellen von Schulungsrechnern in der jeweiligen Schulung genutzt werden sollen?
- Werden auf Schulungsrechnern restriktive Zugriffsrechte für die Benutzer vergeben und das Überspielen von Daten auf externe Medien verhindert?

# M 4.253 Schutz vor Spyware

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 4.254 Sicherer Einsatz von drahtlosen Tastaturen und Mäusen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Drahtlose Tastaturen und Mäuse sind Peripheriegeräte, die kabellos über Funk- oder Infrarot-Schnittstellen mit einem Empfängermodul kommunizieren, das über COM-Port, PS2-Schnittstelle oder USB-Anschluss mit dem Rechner verbunden ist.

Da keine galvanische Verbindung zum Rechner besteht, müssen kabellose Eingabegeräte über eine eigene Spannungsversorgung in Form von Batterien oder Akkus verfügen. Für eine lange Betriebsdauer ist eine geringe Leistungsaufnahme dieser Geräte unumgänglich. Nach dem heutigen Stand der Technik haben Geräte mit Infrarot-Technik einen höheren Energieverbrauch als solche mit Funkschnittstelle.

Die Betriebsfrequenzen der Systeme liegen alle in lizenzfreien Frequenzbereichen. Die Mehrzahl der Funkmäuse und Funktastaturen senden im 27 MHz-Band und verfügen über zwei Funkkanäle, einige kabellose Geräte arbeiten im 2,4 GHz-Bereich.

Die Reichweite der Funksysteme beträgt typischerweise 2 bis 5 Meter. Hier ist im Gegensatz zu den Systemen auf Basis der Infrarot-Technik keine direkte Sichtverbindung zwischen Sender und Empfänger notwendig. Die Reichweite ist extrem abhängig von den Umgebungsbedingungen. Andere im gleichen Frequenzbereich sendende Geräte wie z. B. Sprechfunkgeräte, Funkspielzeug, funkgesteuerte Antriebe für Garagentore oder WLAN-Verbindungen im 2,4 GHz-Bereich können den Betrieb der Systeme empfindlich stören und die Reichweite reduzieren. Metallische Hindernisse (Stahlarmierungen, Stahlschränke und Ähnliches) können zum Versagen der Technik führen.

Hersteller von Funk-Anwendungen geben als Reichweite Entfernungen an, in denen die Datenübertragung ihrer Geräte sicher funktioniert. Diese Funktionalitätsreichweite ist aber im Falle von Geräten, die nur mit billiger Empfangstechnik ausgestattet sind, in der Regel kleiner als die Entfernung, in der die ausgesendeten Signale mit Hilfe von Richtantennen und hochwertiger Empfängerelektronik noch empfangen, aufgezeichnet und ausgewertet werden können. Eine Abhörgefährdung in einer größeren Entfernung als die Funktionalitätsreichweite kann daher nicht ausgeschlossen werden.

Ein Problem der funkbasierten Eingabegeräte ist die mangelnde Abhörsicherheit. Die ausgesendeten Funksignale können von Dritten empfangen und aufgezeichnet werden. Sind diese Funksignale nicht sicher verschlüsselt, können diese Daten leicht ausgewertet werden. Es gibt auf dem Markt zahlreiche Funktastatursysteme, welche die aus den Tastenanschlägen resultierenden Signale völlig unverschlüsselt und damit für Dritte abhörbar übertragen. Hier reicht häufig schon ein zweiter Empfänger vom selben Hersteller aus, um die empfangenen Signale auf einem anderen Rechner sichtbar zu machen.

Systeme, die auf Basis der Infrarot-Technik kommunizieren, verwenden meistens den IrDA-Standard der Infrared Data Association. Im IrDA-Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs spezifiziert. Die Daten werden nur auf Protokollebene gegen Übertragungsfehler mittels Prüfsummenverfahren gesichert. Sicherheitsmechanismen wie Authentisierung, kryptographischer Integritätsschutz und Verschlüsselung sind

nicht vorhanden. In gewissem Rahmen wird die Übertragung durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und die benötigte Sichtverbindung geschützt. Das Sicherheitsniveau dieser Systeme liegt allerdings, aufgrund der möglichen Streustrahlung, unter dem der kabelgebundenen Eingabegeräte.

Einige Hersteller bieten Produkte mit proprietären Sicherheitslösungen an. Über die Sicherheit solcher Lösungen kann keine Aussage getroffen werden, da die eingesetzten Algorithmen in der Regel von den Herstellern unter Verschluss gehalten werden.

Damit baugleiche Geräte nebeneinander betrieben werden können, haben die meisten Hersteller ihre Geräte mit verschiedenen Erkennungsnummern ausgerüstet. Hierbei werden verschiedene Prinzipien verwendet, z. B. wird aus einem Pool von IDs ein bestimmter Wert fest für ein Gerät vergeben oder es wird bei einem Batteriewechsel die ID durch die Software neu erwürfelt.

Auf dem Markt sind erste Produkte erhältlich, die über Bluetooth kommunizieren. Bei korrekter Implementierung und Konfiguration der Bluetooth-Sicherheitsmerkmale bieten diese im Allgemeinen einen höheren Schutz als Funksysteme mit proprietärer Technik.

Abschließend sei erwähnt, dass bei Tastaturen durch die elektromagnetische Abstrahlung der Tastaturmatrix und des Verbindungskabels eine Abhörgefährdung besteht (siehe auch M 4.89 *Abstrahlsicherheit*). Dies gilt auch für kabellose Tastaturen. Die Abhörgefährdung ist aber bei kabelgebundenen Tastaturen im Allgemeinen wesentlich geringer als die Abhörgefahr durch den Einsatz von Funkkommunikationsstrecken bei kabellosen Eingabegeräten.

Zahlreiche Funktastaturen und Funkmäuse senden ihre Informationen über Funk oder Infrarot-Licht ohne Sicherheitsvorkehrungen zu den Rechnern. Ohne großen Aufwand können diese Informationen von Dritten mitgelesen oder gegebenenfalls sogar manipuliert werden. Vom Einsatz solcher Systeme ist aus Sicht der Informationssicherheit daher generell abzuraten.

Für Systeme mit proprietären Sicherheitsmaßnahmen, die kein Sicherheitszertifikat aufweisen, ist der Sicherheitswert nicht einschätzbar. Der Nutzer geht hierbei das Risiko ein, dass die nicht evaluierte Lösung des Herstellers nur eine minimale Sicherheit bietet, die aber bei weitem nicht ausreicht, um seine Daten effektiv zu schützen.

Drahtlose Systeme, die auf Standards wie Bluetooth basieren und bei denen die Sicherheitsmechanismen korrekt implementiert und aktiviert worden sind, bieten im Vergleich einen höheren Schutz. In sensiblen Bereichen sollten jedoch grundsätzlich besser keine Funk-Tastaturen, Funk-Mäuse und Infrarot-Produkte eingesetzt werden.

Prüffragen:

- Ist die Verwendung von kabellosen Eingabegeräten mit den Sicherheitsrichtlinien der Organisation vereinbar?
- Wird in Bereichen mit höherem Schutzbedarf auf die Verwendung kabelloser Eingabegeräte verzichtet?

# M 4.255 Nutzung von IrDA-Schnittstellen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die Infrared Data Association (IrDA) hat Spezifikationen veröffentlicht, in der zunächst die unteren Schichten eines Protokolls für eine Infrarot-Schnittstelle definiert wurden. Dabei wird infrarotes Licht als Träger für den Datenaustausch über kurze Distanzen verwendet. Mittlerweile stellt IrDA auch höhere Protokolle für unterschiedliche Einsatzbereiche zur Verfügung. IrDA wird heute von allen gängigen Betriebssystemen unterstützt, allerdings verliert diese Schnittstelle im Vergleich zu Bluetooth, WLAN oder USB zunehmend an Bedeutung.

Im IrDA-Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs spezifiziert. Die Daten werden nur auf Protokollebene mittels Prüfsummenverfahren gegen Übertragungsfehler gesichert. Sicherheitsmechanismen wie Authentisierung, kryptografischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Diese müssten gegebenenfalls auf Applikationsebene implementiert werden. In gewissem Rahmen wird die Übertragung durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und Notwendigkeit einer Sichtverbindung geschützt. Das Sicherheitsniveau dieser Systeme liegt allerdings, aufgrund der möglichen Streustrahlung, unter dem der kabelgebundenen Eingabegeräte. Gleichzeitig ist die geringe Reichweite aber auch eine Gefährdung für die Verfügbarkeit, da die Kommunikation bei kurzfristigem Verlust der Sichtverbindung sofort unterbrochen wird. Andere, nicht vom Netzbetreiber abhängige Funkschnittstellen wie WLAN oder Bluetooth haben diese Nachteile nicht und bieten zusätzliche Sicherungsfunktionen wie Verschlüsselung und Authentisierung der Endgeräte. Daher sollte nach Möglichkeit die IrDA-Schnittstelle nicht verwendet werden.

Sofern dies doch geschieht, sollte die IrDA-Schnittstelle nur bei konkretem Bedarf aktiviert werden. Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. So nimmt beispielsweise ein Mobiltelefon mit aktivierter IrDA-Schnittstelle SMS-Mitteilungen zum Versand an. An einen PDA oder Laptop können auch Programme über IrDA geschickt werden, die unter Umständen Schadfunktionen enthalten. Außerdem belastet eine eingeschaltete IrDAIrDA-Schnittstelle die Batterie bzw. den Akku des mobilen Gerätes zusätzlich.

Da die Kopplung nur in einem sehr eingeschränkten Bereich möglich ist, kann die Kommunikation meist nicht mitgehört werden. Das bestehende geringe Restrisiko aufgrund der Streustrahlung der IrDA-Komponenten kann durch den Einsatz von zusätzlichen Sicherheitsmechanismen (z. B. Authentisierung und Verschlüsselung auf Applikationsebene) oder den Ersatz von IrDA durch leitungsgebundene Übertragung weiter minimiert werden.

Prüffragen:

- Werden IrDA-Schnittstellen bei allen IT-Komponenten deaktiviert, solange sie nicht benötigt werden?

# M 4.256 Sichere Installation von SAP Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für die Installation eines SAP Systems sind die nachfolgend beschriebenen Aspekte zu berücksichtigen, denn schon in der Installationsphase werden wichtige Weichen für dessen Sicherheit gestellt.

### Verwendete Betriebssysteme absichern

Die Komponenten eines SAP Systems werden als Programme auf einem IT-System installiert und in Form von Prozessen ausgeführt. Damit ist die Sicherheit des genutzten Betriebssystems auch wichtig für die Sicherheit des SAP Systems (siehe auch M 4.257 *Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene*). Die Bausteine der IT-Grundschutz-Kataloge, die für die genutzten IT-Systeme relevant sind, müssen daher in die Modellierung einbezogen und angewendet werden. Außerdem sollten die IT-Systeme gehärtet werden (Hardening), also nicht benötigte Dienste und Programme deaktiviert oder besser entfernt werden.

Hinweise auf weitere Informationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

### Nur benötigte Komponenten installieren

Ein SAP System besteht potentiell aus vielen Komponenten unterschiedlichster Ausprägung. Ungenutzte Komponenten jeglicher Art bergen jedoch Sicherheitsrisiken, da diese oftmals vergessen werden und daher ohne angepasste Konfiguration sind.

Für ein SAP System muss insbesondere entschieden werden, ob nur ein oder beide Stacks benötigt werden, sofern die eingesetzte Systemversion die separate Installation noch unterstützt. Ist dies nicht der Fall, muss der nicht benötigte Stack-Teil so abgesichert werden, dass dessen Funktionen nicht unberechtigt genutzt werden können.

### Wahl von sicheren Passwörtern

Schon während der Installation müssen wichtige Authentisierungsdaten eingegeben werden. Dies sind beispielsweise Passwörter für technische Benutzer, die von den SAP Systemkomponenten (z. B. der Komponente, die die Verbindung zwischen Java-Stack und ABAP-Stack realisiert) zur Authentisierung bei internen Kommunikationsverbindungen genutzt werden.

Es ist darauf zu achten, dass dabei sichere Passwörter gewählt werden. Die Passwörter sollten sich an den internen Passwortvorgaben orientieren. Es ist auch dann ein neues Passwort einzugeben, falls die Installationsroutine bereits ein Passwort vorgibt.

Im Rahmen der Risikobetrachtung für das SAP System ist zu bedenken, dass der Administrator, der das SAP System installiert und die Passwörter festlegt, dadurch die Möglichkeit besitzt, die Sicherheitsmechanismen des SAP Systems zu unterwandern. Die technischen Benutzer, für die die Passwörter anzugeben sind, besitzen in der Regel hohe Privilegien. Daher müssen die Passwörter nach der Installation durch vertrauenswürdige Administratoren verändert werden. Alternativ kann die Passworteingabe im Vier-Augen-Prinzip

erfolgen, wobei je einer von zwei Administratoren die Hälfte des Passwortes eingibt. Dies gilt insbesondere in Outsourcing-Szenarien.

Bei der Passwortlänge ist zu beachten, dass ABAP- und Java-Stack unterschiedliche Restriktionen besitzen: Für den ABAP-Stack können Passwörter maximal aus 8 Zeichen bestehen. Groß- und Kleinschreibung wird dabei nicht unterschieden. Für den Java-Stack gelten diese Beschränkungen nicht. Bei der Passworteingabe ist daher zu berücksichtigen, ob der zugehörige technische Benutzer im ABAP- oder Java-Stack angelegt wird.

Die eingestellten Passwörter sind gemäß der geltenden Passwortrichtlinie zu dokumentieren und aufzubewahren. Hinweise zur Passwortgestaltung finden sich auch in M 2.11 *Regelung des Passwortgebrauchs*.

**Installationsquellen absichern**

In der Regel werden SAP Systeme nicht direkt von CD oder DVD installiert. Vielmehr wird eine Verzeichnisstruktur lokal oder im Netz genutzt, um die Daten anzubieten, die zur Installation benötigten werden. Die Daten der CD- bzw. DVD-Medien werden dann dorthin kopiert. Es wird empfohlen, die Daten nicht lokal auf dem Rechner zu halten, auf dem das SAP System installiert wird, sondern auf einem separaten Rechner. Auf die Daten kann dann über das Netz zugegriffen werden. In großen Behörden und Unternehmen kann dieses Verzeichnis genutzt werden, um zusätzliche SAP Systeme zu installieren. Werden die Systeme nicht in einem separaten und abgeschirmten Netzsegment installiert, so ist es sinnvoll, den Installationsrechner vom Netz zu nehmen, solange er nicht benötigt wird.

Es wird empfohlen den Zugriff auf die Installationsquellen mit Mitteln des Betriebssystems abzusichern, so dass nur berechtigte Administratoren darauf zugreifen können. Unberechtigte Benutzer dürfen insbesondere keine schreibenden Rechte auf die Installationsquellen besitzen, damit die enthaltenen Daten nicht verändert werden können.

Werden die Installationsquellen lokal auf den Rechnern des SAP Systems vorgehalten, so wird empfohlen, diese nach Abschluss der Installation zu löschen.

**SAP Hinweise für die Installation umsetzen**

Die Installationsanleitung eines SAP Systems enthält in der Regel eine Vielzahl von Verweisen auf SAP Hinweise, in denen wichtige Informationen für eine reibungslose Installation oder zur Problemlösung bei Installationsproblemen enthalten sind. In der Regel verweisen die in der Dokumentation genannten SAP Hinweise selbst auch wieder auf weitere SAP Hinweise, so dass eine beträchtliche Informationsmenge zusammenkommen kann. Die Hinweise sind im Vorfeld der Installation zu besorgen. In der Regel ist es zunächst ausreichend, ausgehend von der Installationsdokumentation die dort angegebenen Hinweise zu lesen und einen weiteren Iterationsschritt durchzuführen. Oft wird bei Referenzen auf weitere Informationen explizit angegeben, ob diese verpflichtend abzuarbeiten sind oder nur unter bestimmten Bedingungen angewandt werden sollen. Es wird dringend empfohlen, alle relevanten Informationen tatsächlich abzuarbeiten, da es sonst leicht zu Fehlinstallationen kommen kann.

Insbesondere wenn die Installation zwar abgeschlossen wird, dabei jedoch Fehler aufgetreten sind, ist es möglich, dass Teilfunktionen eines SAP Systems nicht korrekt arbeiten. Dies kann auch sicherheitsrelevante Auswirkungen haben, so dass immer eine fehlerfrei abgeschlossene Installation anzu-

streben ist. Fehlermeldungen können nur dann ignoriert werden, wenn dies explizit durch die Installationsanleitung oder SAP Hinweise angegeben wird.

SAP Hinweise sind über den SAP Service Marktplatz (siehe M 2.265 *Geeigneter Einsatz digitaler Signaturen bei der Archivierung*) zu erreichen. Es wird empfohlen, die SAP Hinweise auszudrucken und nach der Abarbeitung der Systemdokumentation beizulegen.

**Aktuelle SAP Sicherheitsleitfäden berücksichtigen**

Für immer mehr Produkte von SAP stehen Sicherheitsleitfäden zur Verfügung. Obwohl diese unterschiedlich in der Qualität der Sicherheitsempfehlungen sind, ist es sinnvoll, die Leitfäden für die zu installierenden SAP Komponenten zu verwenden. Die Sicherheitsleitfäden werden in Abständen aktualisiert, so dass es sich lohnt, neuere Leitfäden für bereits installierte Systeme zu berücksichtigen.

Die Sicherheitsleitfäden stehen vornehmlich für aktuelle System- und Produktversionen zur Verfügung. Es lohnt sich jedoch auch für Betreiber von älteren R/3 Systemen, die Sicherheitsleitfäden für neuere Produkt-Versionen zu nutzen, da viele Empfehlungen direkt anwendbar sind oder leicht adaptiert werden können.

Die existierenden SAP Sicherheitsleitfäden sind über den SAP Service Marktplatz (siehe M 2.346 *Nutzung der SAP Dokumentation*) erreichbar.

**Sichere Installation und Konfiguration der Datenbank**

Die Datenbank, die das SAP System nutzt, um alle Informationen persistent zu speichern, ist eine kritische Komponente, die vor unberechtigtem Zugriff unbedingt geschützt werden muss. Neben den allgemeinen Aspekten einer sicheren Datenbank-Installation sind die spezifischen Empfehlungen in der Maßnahme M 4.269 *Sichere Konfiguration der SAP System Datenbank* zusammengefasst. Die Sicherheit von Datenbanken wird auch im Baustein B 5.7 *Datenbanken* behandelt.

**Sichere Installation und Konfiguration der SAP Systemlandschaft**

Entsprechend der Planung der Systemlandschaft (siehe M 2.341 *Planung des SAP Einsatzes*) müssen die betroffenen SAP und Nicht-SAP Komponenten (z. B. Firewalls) installiert und konfiguriert werden.

Prüffragen:

- Werden bei der Installation des SAP-Systems die IT-Systeme gehärtet (Hardening), also nicht benötigte Dienste und Programme deaktiviert beziehungsweise entfernt?
- Wird bei der Installation des SAP-Systems der eventuell Nicht benötigte Stack-Teil gegen unberechtigte Nutzung abgesichert?
- Orientiert sich die Passwortauswahl bei der SAP-Installation an den internen Passwortvorgaben?
- Werden bei der SAP-Installation auch dann neue Passwörter eingegeben, wenn die Installationroutine bereits ein Passwort vorgibt?
- Werden die während der SAP-Installation vergebenen Passwörter durch vertrauenswürdige Administratoren geändert?
- Sind die SAP-Installationsquellen abgesichert, so dass nur berechtigte Administratoren darauf zugreifen können?
- Werden die Installationshinweise zur SAP-Installation im Vorfeld und während der Installation berücksichtigt?

- Erfolgt die sichere Installation und Konfiguration der betroffenen SAP und Nicht-SAP Komponenten entsprechend der Planung?

# M 4.257 Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Während der SAP Installation werden durch das Installationsprogramm zunächst Daten aus den Installationsquellen (z. B. Verzeichnis im Netz, CD/DVD) in ein Installationsverzeichnis (z. B. /sapinst) extrahiert. In diesem werden auch alle Aktivitäten während der Installation protokolliert.

Je nach Installationsprogramm können in den Protokolldateien auch schützenswerte Informationen enthalten sein. Dazu zählen die Informationen über die gewählten SAP System-IDs (SAPSID), Informationen über den lokalen Rechner (z. B. IP-Adresse, Rechnername), Namen der gewählten technischen Benutzer. Aber auch die Passwörter, die während der Installation eingegeben wurden, können im Klartext enthalten sein. Dies gilt insbesondere für ältere Installer-Versionen.

Daher wird nach Abschluss der Installation folgendes Vorgehen empfohlen:

- Das gesamte Installationsverzeichnis ist zu sichern. Die Sicherung sollte so erfolgen, dass auf die Daten nicht von unberechtigten Personen zugegriffen werden kann.
- Bei Problemen mit der SAP Installation müssen die gesicherten Daten und Protokolle durch SAP Experten gesichtet werden. Hierfür können diese an SAP gesandt oder durch SAP Berater eingesehen werden. Daher müssen in diesem Fall berechtigte Administratoren auf die Daten zugreifen können. Werden die Daten an SAP gesandt oder von Dritten eingesehen, so ist zu bedenken, dass damit diese Personen schützenswerte Systeminformationen erhalten. Daher muss eine entsprechende Vertraulichkeitsvereinbarung geschlossen werden.
- Das gesicherte Installationsverzeichnis kann danach auf dem installierten System gelöscht werden.

Je nach Schutzbedarf des SAP Systems kann es sinnvoll sein, die Protokolldaten vor dem Zugriff durch Dritte auf Klartextpasswörter zu untersuchen und diese zu löschen oder zu maskieren. Dies wird von neueren Installer-Versionen bereits bei der Protokollerstellung umgesetzt, so dass dadurch keine Beeinträchtigung der Support-Leistung erfolgt, falls die so veränderten Protokolldateien im Support-Fall genutzt werden.

Prüffragen:

- Wird nach Abschluss der SAP-Installation das gesamte Installationsverzeichnis gesichert?
- SAP-Installationsverzeichnisses keine unberechtigten Personen zugreifen können?
- Erforderliche Kenntnisnahme von SAP-Daten durch Dritte: Wird mit Dritten eine entsprechende Vertraulichkeitsvereinbarung geschlossen?
- Wird nach der SAP-Installation das Installationsverzeichnis auf dem installierten System gelöscht?

# M 4.258 Sichere Konfiguration des SAP ABAP-Stacks

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der ABAP-Stack ist die traditionelle Ausführungsumgebung eines SAP Systems. Dies trifft insbesondere auf die Systemversionen zu, die allgemein mit dem Begriff SAP R/3 bezeichnet werden, da die R/3 Komponenten und Module im ABAP-Stack ausgeführt werden.

Die initiale Konfiguration des ABAP-Stacks ist aufwendig und umfasst viele Einzelschritte. Der Aufwand erhöht sich, wenn neben der Konfiguration der reinen SAP Basis auch Applikationen und Module konfiguriert werden müssen, wie das in R/3-Systemen notwendig ist. Hier müssen alle relevanten Behörden- oder Unternehmensprozesse durch Konfiguration (Customizing) oder Anpassungen im ABAP-Code nachgebildet werden.

Im Folgenden werden die aus Sicherheitssicht wichtigsten Schritte aufgezeigt, die bei der initialen Konfiguration des ABAP-Stacks durchzuführen sind. Die Darstellung beschränkt sich auf die Konfiguration der SAP Basis und geht damit nicht auf Module oder Applikationen ein.

### Mandant für den Betrieb festlegen

Zunächst muss ein Mandant für den Betrieb des SAP Systems festgelegt werden. Als "Mandant" (engl. Client) wird in einem SAP System eine technische Unterteilung verstanden. Dies ist nicht mit dem Mandantenbegriff im Sinne von "Kunde" zu verwechseln. Nach der Installation dürfen die existierenden Standardmandaten mit den Nummern 000 (SAP Referenzmandant), 001 (Produktionsvorbereitungsmandant), und 066 (Earlywatch-Mandant) nicht genutzt werden.

Ein SAP System kann mehrere Mandanten mit unterschiedlichen Verwendungszwecken enthalten. Alle Mandanten eines SAP Systems hängen jedoch über den SAP Referenzmandanten zusammen, in dem Konfigurationen erfolgen, die global für das gesamte SAP System gelten.

Aus Sicherheitssicht ist zu fordern, dass Mandanten mit sehr unterschiedlichen Sicherheitsanforderungen nicht zusammen in einem SAP System betrieben werden. So darf etwa ein Produktivmandant nie zusammen mit einem Entwicklungsmandanten in einem SAP System betrieben werden. Beim gemeinsamen Betrieb können Entwickler auch mandanten-unabhängige Objekte ändern, so dass dies direkt Auswirkungen auf den Produktivmandanten hat. Daher ist eine Separation zwingend erforderlich.

### Sicherheitsrelevante IMG-Aktivitäten durchführen

Der SAP Implementation Guide (IMG, SAP Reference IMG) ist eine von SAP vordefinierte, systeminterne Liste, die die Konfigurationsschritte enthält, die zur Konfiguration eines SAP Systems durchzuführen sind. Die Liste ist hierarchisch aufgebaut und jeweils auf die verwendete Systemversion und die installierten Komponenten abgestimmt. Daneben besteht die Möglichkeit, eigene IMGs zu erstellen (Projekt IMGs), in denen nur die im Rahmen der Systemverwendung notwendigen Konfigurationsschritte aus dem SAP Reference IMG enthalten sind. IMGs bieten zudem die Möglichkeit festzuhalten, welche Konfi-

gurationen bereits durchgeführt wurden, so dass dadurch der Konfigurationsstatus vorgehalten werden kann.

In M 2.346 *Nutzung der SAP Dokumentation* findet sich ein Hinweis auf die SAP IMG Dokumentation, die zu beachten ist. Alle im Rahmen der Planung festgelegten IMG-Aktivitäten (siehe auch M 2.341 *Planung des SAP Einsatzes*) müssen abgearbeitet werden.

Folgende IMG-Aktivitäten sind immer durchzuführen:

- HTTP-Services aktivieren bzw. deaktivieren, falls diese für den späteren Einsatz nicht benötigt werden (Transaktion: SICF), siehe dazu auch , M 5.127 *Absicherung des SAP Internet Connection Framework (ICF)*.
- Berechtigungen für IDOC-Schnittstelle vergeben (Transaktion: PFCG), siehe dazu auch M 5.128 *Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle*.
- Berechtigungen für RFC-Schnittstellen vergeben (Transaktion PFCG), siehe dazu auch M 2.342 *Planung von SAP Berechtigungen* und , M 5.126 *Absicherung der SAP RFC-Schnittstelle*.
- IDOC-Administration einstellen (Transaktion: OYEA), siehe dazu auch , M 5.128 *Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle*.
- Content-Server Administration (Transaktion: CSADMIN), siehe dazu auchM 5.129 *Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen*.
- Profilparameter für den Internet Connection Manager (ICM) konfigurieren (Transaktion SMICM, Springen, Parameter)
- Proxy-Konfiguration definieren (Transaktion SM30 mit THTTP)
- Alle Aktivitäten unter dem Stichwort "Systemadministration" sind durchzuführen.

Durch die IMG-Aktivitäten werden unter anderem auch die nachfolgend beschriebenen Maßnahmen berührt. Da diese jedoch aus Sicherheitssicht eine große Relevanz aufweisen, werden sie hier explizit aufgeführt.

**Profilparameter anpassen**

Über Profilparameter können grundsätzliche Funktionen eines SAP Systems konfiguriert werden. Daher müssen im Rahmen der Konfiguration auch die Profilparameter an die Bedürfnisse angepasst werden. Da Profile in mehreren Ausprägungen existieren (z. B. Start-Profil, Default-Profil, Instanz-Profil), müssen sich Administratoren mit dem Profil-Mechanismus vertraut machen.

Generell ist für jeden einzelnen Profilparameter die zu verwendende Einstellung zu definieren. Folgende Parameter verdienen dabei aus Sicherheitssicht besondere Aufmerksamkeit:

- alle Parameter mit dem Präfix "auth/"
- alle Parameter mit dem Präfix "login/"
- alle Parameter mit dem Präfix "snc/", sofern SNC eingesetzt wird
- alle Parameter mit dem Präfix "ssf/", sofern SSF eingesetzt wird

Für die Profil-Verwaltung sollte die Transaktion RZ10 verwendet werden. Das manuelle Ändern auf Dateisystemebene sollte unterbleiben. Für die Anzeige der Profilparameter kann auch der Report RSPARAM benutzt werden, der über die Transaktion SE38 aufgerufen wird. Die Profil-Dateien sind auf Betriebssystemebene vor unberechtigtem Zugriff zu schützen.

Hinweise auf Detailinformationen zum Umgang mit Profilen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Systemänderbarkeit konfigurieren**

Je nach Rolle eines SAP Systems muss die Systemänderbarkeit eingestellt werden. Durch die Einstellung wird bestimmt, ob Änderungen an internen System-Komponenten und Applikationskomponenten überhaupt erlaubt sind oder nicht. Dies betrifft beispielsweise den ABAP-System-Code, generell alle Objekte im Data Dictionary (DDIC) sowie den Objektnamensraum.

Für Produktiv-Systeme wird empfohlen, die Systemänderbarkeit global auf "nicht änderbar" zu setzen. Damit können Änderungen nur noch über das Transportsystem eingespielt werden. Dies ist für Produktiv-Systeme wünschenswert, damit Änderungen nur über definierte Prozeduren und Abläufe erfolgen. Wichtig ist hier, einen geordneten Änderungsmanagementprozess zu definieren und einzuhalten, siehe M 4.272 *Sichere Nutzung des SAP Transportsystems*.

Für Test- und Qualitätssicherungssysteme sollten die gleichen Einstellungen wie im Produktivsystem verwendet werden, also global "nicht änderbar". Änderungen sind im Entwicklungssystem vorzunehmen und nach dem Durchlauf des Qualitätssicherungsprozesses in das Qualitätssicherungs- und final in das Produktiv-System zu transportieren.

Für Entwicklungssysteme sollten die Komponenten, die durch die Entwicklung nicht betroffen werden, auf "nicht änderbar" gesetzt werden. Die Komponenten, in denen entwickelt wird, müssen hingegen auf "änderbar" gesetzt werden.

Die Einstellungen der Systemänderbarkeit können über die Transaktion SE06 oder SE03 erreicht werden.

Hinweise auf detaillierte Informationen zum Thema finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Mandanten-Konfiguration durchführen**

Neben der übergreifenden Änderbarkeit des SAP Systems können auch einzelne Mandanten gegen Veränderungen mandantenabhängiger Eigenschaften geschützt werden. Diese Einstellung ist für alle produktiven Mandanten zu benutzen. Durch die Einstellungen wird auch beeinflusst, ob Mandanten-Veränderungen automatisch aufgezeichnet werden, so dass Einstellungsveränderungen nach der Prüfung automatisch als Transportauftrag verfügbar sind und in andere Mandanten transportiert werden können, die mit den gleichen Einstellungen betrieben werden sollen.

Das Änderungsmanagement-Konzept muss festlegen, nach welchem Schema Änderungen zwischen Mandaten verteilt werden und welche Mandanten welchen Verwendungszweck (z. B. Produktivmandant, Testmandant, Entwicklungsmandant) besitzen.

Die Einstellungen erfolgen über die Transaktion SCC4. Für die eigenen Produktivmandanten sind folgende Einstellungen empfohlen (Hinweis: Die angegebenen Bezeichnungen der Einstellungswerte finden sich so in der abgekürzten Schreibweise im SAP System.):

- Rolle des Mandanten: "Produktiv"
- Änderungen und Transporte für mandantenabhängige Objekte: "keine Änderung erlauben"
- Änderungen an mandantenübergreifenden Objekten: "keine Änderungen von Repository- und mand.unabh. Cust.-Obj."

- Schutz bzgl. Mandantenkopierer und Vergleichstool: "Schutzstufe 2: kein Überschreiben, keine ext. Verfügbarkeit"
- Einschränkungen beim Starten von CATT und eCATT: "eCATT und CATT nicht erlauben"

Entsprechende Einstellungen sollten im Test- und Akzeptanzsystem gelten. Für andere Mandanten (Entwicklung, Schulung, Demo) sind die Einstellungen geeignet zu definieren.

Administratoren müssen sich mit den Auswirkungen der Mandanten-Konfiguration sehr genau vertraut machen. Hinweise auf entsprechende Detail-Dokumentation findet sich in M 2.346 *Nutzung der SAP Dokumentation*,.

**Ausführbare Betriebssystemkommandos absichern**

Der ABAP-Stack bietet die Möglichkeit an, Betriebssystemkommandos auszuführen. Die Kommandos werden mit den Betriebssystemrechten des technischen Betriebssystembenutzers ausgeführt, unter dem das SAP System abläuft. Dies sind in der Regel weitreichende Administratorrechte.

Der Zugriff auf diese Funktionalität muss daher abgesichert werden. Insbesondere das Anlegen oder Verändern von Kommandos muss verhindert werden. Daher sollten folgende Hinweise umgesetzt werden:

- Die Berechtigungen, externe Betriebssystemkommandos auszuführen (Berechtigung S_LOG_COM) oder zu pflegen, (Berechtigung S_RZL_ADM mit ACTVT=01) sind restriktiv zu vergeben.
- Der Zugriff auf die Transaktion SM49 "Externe Betriebssystemkommandos ausführen" ist auf die berechtigten Administratoren einzuschränken.
- Der Zugriff auf die Transaktion SM69 "Externe Betriebssystemkommandos pflegen" ist auf die berechtigten Administratoren einzuschränken.
- Für die Betriebssystemkommandos besteht die Möglichkeit, die beim Aufruf genutzten Parameterwerte vorzugeben und zu verhindern, dass zusätzliche Parameter angehängt werden können. Von dieser Möglichkeit sollte Gebrauch gemacht werden. Dies trifft insbesondere für selbst definierte Kommandos zu.

Hinweise auf Detailbeschreibungen zum Absichern der Betriebssystemkommandos finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Passwortqualität sicherstellen**

Damit die Passwortqualität beim Zugang zum SAP System sichergestellt wird, sind die folgenden Hinweise zu berücksichtigen.

Es sollte eine minimale Passwortlänge definiert werden. Dazu dient der Profilparameter "login/min_password_lng". Es wird ein Wert von 8 Zeichen empfohlen. Dieser Wert stellt gleichzeitig die maximale Passwortlänge des ABAP-Stacks dar.

Für Passwörter sollten Komplexitätskriterien definiert werden. Dies sind über die folgenden Profilparameter einstellbar:

- login/min_password_diff:
  Mindestanzahl der unterschiedlichen Zeichen zwischen neuem und altem Passwort
- login/min_password_digits:
  Mindestanzahl von Ziffern im Passwort
- login/min_password_letters:
  Mindestanzahl von Buchstaben im Passwort
- login/min_password_specials:

Mindestanzahl von Sonderzeichen im Passwort

Bei der Definition von Komplexitätskriterien ist darauf zu achten, dass konsistente Vorgaben eingestellt werden.

Für Passwörter sollte eine maximale Gültigkeitsdauer vorgegeben werden, so dass eine regelmäßige Passwortänderung erzwungen wird. Dies wird über den Profilparameter "login/password_expiration_time" konfiguriert, der die Anzahl der Tage angibt, nach denen das Passwort zu ändern ist. Empfehlenswert sind Werte zwischen 60 und 90 Tagen.

Es können verbotene Passwörter definiert werden. Diese sind in der Tabelle USR40 über die Transaktion SM31 zu pflegen. Hierüber sollten typische Trivial-Passwörter verhindert werden.

Die eingestellten Werte sind entsprechend der geltenden Passwortrichtlinie zu wählen.

**Schutz vor Passwort-Attacken konfigurieren**

Es wird empfohlen, das SAP System vor Passwort-Attacken zu schützen, indem nach einer Anzahl von Anmelde-Fehlversuchen die Verbindung unterbrochen wird. Die Anzahl wird durch den Profilparameter "login/fails_to_session_end" konfiguriert.

Um wiederholt angegriffene Benutzerkonten vor weiteren Angriffen zu schützen, wird empfohlen, Benutzerkonten nach einer Anzahl von Anmelde-Fehlversuchen zu sperren. Die Anzahl wird durch den Profilparameter "login/fails_to_user_lock" konfiguriert.

Es muss außerdem entschieden werden, ob gesperrte Benutzerkonten automatisch wieder um Mitternacht entsperrt werden oder ob dies manuell durch den Benutzer-Administrator erfolgen muss. Das Verhalten wird über den Profilparameter "login/failed_user_auto_unlock" gesteuert.

Die eingestellten Werte sind entsprechend der geltenden Passwortrichtlinie zu wählen.

**Mehrfachanmeldungen verhindern**

SAP Systeme können verhindern, dass das gleiche Benutzerkonto für mehrere parallele Anmeldungen verwendet wird. In der Regel sind in Produktiv-Systemen Mehrfachanmeldungen durch die gleiche Person nicht sinnvoll und sollten daher unterbunden werden. Das Verhalten kann für SAPGui- und RFC-Sitzungen separat gesteuert werden wird über die Profilparameter "login/disable_multi_gui_login" und "login/disable_multi_rfc_login" definiert.

Bevor Mehrfachanmeldungen über RFC unterbunden werden, muss sichergestellt sein, dass parallele Sitzungen mit demselben technischen Benutzerkonto ausgeschlossen sind.

**Single Sign-On sicher konfigurieren**

Werden mehrere SAP Systeme betrieben, so kann die Benutzeranmeldung über den SAP Single Sign-On (SSO) Mechanismus vereinfacht werden. Eine wiederholte Passwort-Eingabe ist dann nicht mehr notwendig, da nach einem erfolgreichen Login vom SAP System ein Single Sign-On Ticket ausgestellt wird, welches den Zugriff auf andere SAP Systeme ohne erneutes Login er-

laubt. Ob und zwischen welchen SAP Systemen der Single Sign-On Mechanismus genutzt wird, muss in der Planungsphase festgelegt werden.

Folgende sicherheitsrelevante Aspekte sind zu bedenken, wenn Single Sign-On verwendet wird:

- Single Sign-On sollte nur zwischen vertrauenswürdigen Systemen konfiguriert werden. Insbesondere Single Sign-On Szenarien über Unternehmens- oder Behördengrenzen hinweg sind unter Sicherheitsgesichtspunkten zu vermeiden.
- Es empfiehlt sich, pro Szenario nur ein System für die zentrale Anmeldung einzusetzen, das SSO-Tickets ausstellt. Alle anderen Systeme sollten SSO-Tickets nur akzeptieren.
- Besonders wichtig ist, dass die Kommunikation zwischen dem Browser des Benutzers und dem SAP System verschlüsselt wird. Ansonsten besteht potentiell die Gefahr, dass Angreifer das SSO-Ticket abhören und damit ohne Anmeldung auf das SAP System zugreifen können.

Folgende Profilparameter regeln die SSO-Konfiguration für ein SAP System:

- login/accept_sso2_ticket:
  System akzeptiert SSO-Tickets.
- login/create_sso2_ticket:
  System stellt SSO-Tickets aus.
- login/ticket_expiration_time:
  Gültigkeitsdauer der ausgestellten SSO-Tickets in Stunden
- login/ticket_only_by_https:
  SSO-Tickets werden nur beim Zugriff über HTTPS ausgestellt.
- login/ticket_only_to_host:
  SSO Tickets werden nur bei Zugriffen auf das ausstellende System verwendet.

Für die Konfiguration von SSO sind zusätzliche administrative Tätigkeiten durchzuführen, die über die Transaktionen SSO2, SSO2_ADMIN (SSO2_ACL) und STRUSTSSO2 gemanagt werden können. SAP empfiehlt, die Transaktion SSO2 zu nutzen.

Hinweise auf Detailinformationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Neben dem SAP SSO-Mechanismus über Tickets können auch externe Systeme für SSO genutzt werden. Diese müssen dann jedoch über die SNC-Schnittstelle (Secure Network Communication) eingebunden sein. Für Windows-basierte Umgebungen (ab Windows 2000) wird auf die Möglichkeit hingewiesen, Single Sign-On über Kerberos zu nutzen. In diesem Fall erfolgt die Anmeldung nur am Windows-System. Beim Zugriff auf das SAP System ist dann keine Eingabe von Benutzername und Passwort mehr notwendig. Der verwendete Windows-Kerberos SNC-Provider ist standardmäßig und ohne Mehrkosten verfügbar. Es muss jedoch bedacht werden, dass der Windows Kerberos SNC-Provider keine Verschlüsselung der Kommunikation anbietet. Daher ist nur SNC-basierte Authentisierung verfügbar. Ab Windows 2000 besteht jedoch standardmäßig die Möglichkeit, IPSec zwischen Rechnern einzusetzen und so eine generelle Verschlüsselung der Kommunikation zu erreichen. Ob dies eine mögliche Variante ist, um Single Sign-On in einem Unternehmen oder einer Behörde umzusetzen, muss jeweils entscheiden werden.

Weitere Maßnahmen zu SNC finden sich in M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*, SAP Informationsquellen in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Werden die existierenden Standardmandanten des SAP Systems im Betrieb nicht genutzt?
- Ist sichergestellt, dass Mandanten mit sehr unterschiedlichen Sicherheitsanforderungen nicht zusammen in einem SAP System betrieben werden?
- Sind die Administratoren mit dem Profil-Mechanismus im SAP System vertraut?
- Sind die Profil-Dateien des SAP Systems auf Betriebssysstemebene vor unberechtigtem Zugriff geschützt?
- Ist für das SAP Produktiv-System der Parameter zur Systemänderbarkeit auf "nicht änderbar" gesetzt?
- Sind für die Test- und Qualitätssysteme die gleichen Einstellungen wie im SAP Produktivsystem verwendet worden, also global "nicht änderbar"?
- Sind die SAP Komponenten des Entwicklungssystems, die durch die Entwicklung nicht betroffen sind, auf nicht änderbar gesetzt?
- Sind im SAP System die Einstellungen für alle produktiven Mandanten so gewählt, dass sie gegen Veränderungen mandantenabhängiger Eigenschaften geschützt sind?
- Wird bei der SAP Mandanten Konfiguration im Änderungsmanagement-Konzept festgelegt, nach welchem Schema Änderungen zwischen Mandanten verteilt werden?
- Sind die SAP Administratoren mit den Auswirkungen der Mandanten-Konfiguration vertraut?
- Wird im SAP System der Zugriff auf ausführbare Betriebssystemkommandos abgesichert, insbesondere das Anlegen oder Verändern von Kommandos?
- Ist die Passwortqualität im SAP System technisch sichergestellt?
- Sind die SAP Systeme so konfiguriert, dass nach einer Anzahl von Anmelde-Fehlversuchen die Verbindung unterbrochen wird?
- Ist das SAP System so eingestellt, dass Mehrfachanmeldungen für das gleiche Benutzerkonto verhindert werden?
- Ist festgelegt, zwischen welchen SAP Systemen der SAP Single Sign-On Mechanismus genutzt wird?

# M 4.259 Sicherer Einsatz der ABAP-Stack Benutzerverwaltung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der sichere Einsatz der ABAP-Stack Benutzerverwaltung ist Voraussetzung für die Systemsicherheit, da damit bestimmt wird, wer prinzipiell Zugriff auf ein SAP System hat. Folgende Aspekte sind beim Einsatz der Benutzerverwaltung mindestens zu bedenken. Je nach Einsatzszenario müssen auch weitere Themen berücksichtigt werden, die durch die spezifischen Anforderungen im Unternehmen oder der Behörde bestimmt werden. Dabei sind auch Anforderungen zu beachten, die sich aus rechtlichen Bestimmungen ergeben.

Hinweise auf SAP Dokumente zur Benutzerverwaltung in SAP Systemen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

### Namenskonvention für Benutzer

Benutzernamen müssen eindeutig sein. Daher ist eine Namenskonvention festzulegen, die dies auch dann garantiert, wenn Personen den gleichen Namen besitzen. In der Regel bestehen im Unternehmen oder der Behörde schon eindeutige Identifikationen für Mitarbeiter, etwa in Form der Personalnummer, die dazu benutzt werden können.

Es ist sinnvoll, Klassen von Benutzern zu bilden (z. B. Interne, Externe, Partner, technische Benutzer) und diese Klassen auch in den Benutzernamen zu kodieren.

### Eindeutige Benutzerzuordnung

Durch das Benutzerverwaltungskonzept ist sicherzustellen, dass derselbe Benutzernamen in unterschiedlichen Systemen immer dieselbe Person bezeichnet.

Es ist durch geeignete organisatorische Maßnahmen auszuschließen, dass ein Benutzerkonto durch mehrere Personen genutzt wird (Account-Sharing).

### Einrichten eines Notfalladministrators

Für Notfälle sollte ein SAP Konto eingerichtet werden, dass für die Notfalladministration verwendet wird. Es empfiehlt sich, dieses mit einer normalen Bezeichnung zu versehen, damit keine gezielten Angriffe auf dieses Benutzerkonto provoziert werden. Das Konto SAP* darf nicht zur Administration oder Notfalladministration verwendet werden.

Der Notfalladministrator ist in der Regel mit weitreichenden Berechtigungen ausgestattet und ist daher mit einem sicheren Passwort zu versehen. Im Rahmen der Notfallplanung sind Prozeduren zu definieren, wie das Konto zu benutzen ist (siehe M 2.341 *Planung des SAP Einsatzes* und M 6.97 *Notfallvorsorge für SAP Systeme*). Das Passwort des Notfalladministrators sollte an einem sicheren Ort (z. B. Safe) aufbewahrt werden. Der Zugriff auf das Passwort sollte im 4-Augen Prinzip erfolgen.

**Absichern der Standardbenutzer**

In einem SAP System sind mehrere Standardbenutzer verfügbar, die abgesichert werden müssen. Betroffen sind die Benutzer:

- SAP*
- DDIC
- EARLYWATCH
- SAPCPIC
- TMSADM
- SAPSYS
- WF-BATCH (wird erst durch das automatische Workflow-Customizing erstellt)

Zur Absicherung gehören folgende Aktionen:

- Ändern des Passwortes (siehe auch unten)
- Deaktivieren der Benutzerkennung
- Die Benutzerkennungen sollten nur für kurze Zeit aktiviert werden, um bestimmte Aktivitäten (z. B. System-Update) durchzuführen. Für das geregelte Vorgehen, sind entsprechende Prozesse notwendig. Diese müssen sicherstellen, dass die Benutzerkennungen nach Abschluss der Arbeiten wieder deaktiviert werden.
- Zuordnung der Benutzer zur Gruppe SUPER.

Nachdem Benutzerkennungen deaktiviert wurden, kann es zu Funktionseinbußen kommen. Ob eine zeitweise oder doch dauerhafte Aktivierung notwendig ist, hängt vom Verwendungszweck des Systems ab und muss im Einzelfall entschieden werden. Das zusätzliche Risiko durch einen aktivierten Standardbenutzer mit unter Umständen bekanntem Standardpasswort ist dabei zu berücksichtigen.

Das Löschen der Benutzer SAP* und DDIC wird nicht empfohlen, da diese automatisch z. B. beim Anlegen eines neuen Mandaten neu erzeugt werden. Für den Benutzer SAP* kann dieses Verhalten durch den Profilparameter "logon/no_automatic_user_sapstar" beeinflusst werden. Es wird empfohlen, den Parameter zu aktivieren.

Bevor der Benutzer SAP* deaktiviert wird, muss ein alternatives Benutzerkonto für die Notfalladministration erfolgreich eingerichtet sein.

Bei der Installation neuer Komponenten können zusätzliche Standardbenutzer angelegt werden. Diese sind dann nach der Installation entsprechend abzusichern.

Hinweise auf SAP Dokumentationen zum Umgang mit Standardbenutzern in SAP Systemen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Ändern von Standardpasswörtern**

Die Standardbenutzer (siehe oben) sind mit Standardpasswörtern ausgestattet. Diese sind zu ändern, um zu verhindern, dass die Benutzerkennungen unbefugt genutzt werden.

Nach der Passwortänderung kann es jedoch dazu kommen, dass Systemfunktionen nicht mehr oder nicht mehr korrekt ausgeführt werden können. Dies ist beispielsweise für die Benutzer TMSADM (siehe auch SAP Hinweis 139854) und SAPCPIC der Fall. Wird die betroffene Systemfunktion häufig genutzt, so muss der Standardbenutzer unter Umständen mit dem Standardpasswort betrieben werden. Dies ist im Rahmen der Risikobewertung zu berücksichtigen.

Für die Benutzer SAP* und DDIC ist zu berücksichtigen, dass diese z. B. beim Erzeugen neuer Mandanten automatisch neu angelegt werden, falls diese Benutzerkennungen gelöscht wurden. Dabei werden die neuen Benutzerkennungen mit den Standardpasswörtern ausgestattet.

Der Report RSUSR003 kann über die Transaktion SE38 dazu genutzt werden, um in allen Mandanten eine Prüfung auf die Existenz, den Sperrstatus und auf Standardpasswörter für die Benutzer SAP*, DDIC, SAPCPIC und EARLYWATCH durchzuführen.

**Verwaltungsverfahren**

Bei der Benutzerverwaltung ist zu berücksichtigen, welches Verwaltungsverfahren eingesetzt wird. Wird die zentrale Benutzerverwaltung eingesetzt, so sollten Benutzerkennungen nicht lokal angelegt werden.

Die geplanten Prozesse und Verfahren (siehe M 2.341 *Planung des SAP Einsatzes*) für die dezentrale oder zentrale Benutzerverwaltung müssen umgesetzt und eingehalten werden. Die Prozesse sollten dabei auch Regelungen zur Behandlung von Ausnahmen enthalten.

Folgende Aspekte sind für das eingesetzte Verwaltungsverfahren zu berücksichtigen:

- Für die Basis-Administration muss ein spezielles Rollenkonzept entwickelt werden.
- Im Rahmen der Planung des Verwaltungskonzeptes müssen Prozessbeschreibungen zum Änderungsmanagement von Rollen und Berechtigungen erstellt werden. Dabei ist zu berücksichtigen:
  - Die jeweiligen Verantwortlichen für die Geschäftsprozesse müssen in den Zustimmungsprozess für Rollenänderungen und Rollenzuordnungen einbezogen werden.
  - Mit dem Werkzeug "SAP GRC Access Control" oder mit Werkzeugen anderer Hersteller können Geschäftsprozessrisiken analysiert werden, die möglicherweise dadurch entstehen, dass Rollen verändert werden oder dass Benutzern neue Rollen zugeordnet werden.

Prüffragen:

- Sind für Benutzernamen im SAP System Namenskonventionen festgelegt, die eindeutige Benutzer-Zuordnungen garantieren?
- Wird im SAP System ein SAP Konto eingerichtet, das für die Notfalladministration verwendet wird?

# M 4.260 Berechtigungsverwaltung für SAP Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Sicherheit der in einem SAP System verarbeiteten Geschäftsdaten wird sehr stark durch die eingestellten Berechtigungen für Benutzer und Administratoren bestimmt. Diese legen fest, welche Funktionen (im SAP Jargon auch Transaktionen genannt) von einem bestimmten Benutzer aufgerufen und damit, welche Daten eingesehen bzw. verändert werden können. Daher sind die konfigurierten Berechtigungen und deren Verwaltung ein sehr wichtiger Bestandteil der Systemsicherheit, vor allem vor dem Hintergrund möglicher Betrugshandlungen durch interne Mitarbeiter.

Das SAP Berechtigungssystem ist sehr flexibel, dadurch aber auch komplex in der Konfiguration. Im Gegensatz zu Betriebssystemen, in denen Berechtigungen direkt auf Objekten (z. B. Dateien) vergeben werden, arbeiten SAP Systeme nach dem Ausweisprinzip: Beim Zugriff auf Funktionen wird geprüft, ob der Benutzer Berechtigungen eines bestimmten Typs besitzt. Ist dies der Fall, wird geprüft, ob die eingetragenen Werte den Anforderungen entsprechen, die zum Ausführen der aufgerufenen Funktion notwendig sind. Die geprüften Berechtigungstypen und Werte werden dabei durch den Programmierer der Funktion bestimmt und können auch die Daten berücksichtigen, die beim aktuellen Aufruf an die Funktion übergeben wurden. Zusätzlich entscheidet zum Schluss der Programmierer einer Funktion, ob er eine eigentlich notwendige Berechtigungsprüfung implementiert oder nicht.

Für die Verwaltung von Berechtigungen sollten die folgenden Empfehlungen berücksichtigt werden. Die Liste ist an die lokalen Bedürfnisse und Anforderungen anzupassen und zu erweitern.

### Schulung

Administratoren die für die Verwaltung von Benutzerkennungen, Rollen, Profilen oder Berechtigungen verantwortlich sind, müssen zwingend Schulungen zum SAP Berechtigungskonzept und zur Berechtigungsverwaltung (Vorgehen, Werkzeuge, richtige Verwendung) erhalten oder das entsprechende Verständnis nachweisen. Nur so wird erreicht, dass die Berechtigungsverwaltung versiert durchgeführt werden kann.

### Trennen der Verantwortlichkeiten (Vier-Augen-Prinzip)

Das Verwaltungskonzept muss so ausgelegt sein, dass die Verantwortlichkeiten möglichst getrennt werden. Folgendes sollte dabei beachtet werden:

- Es sollte ein Benutzeradministrator vorgesehen werden. Dieser sollte Benutzerkennungen anlegen, verändern und Rollen zuordnen können. Das Anlegen oder Verändern von Rollen oder Profilen darf dem Administrator nicht erlaubt sein. SAP bietet hierzu die Vorlage SAP_ADM_US an.
- Es sollte ein Rollenadministrator vorgesehen werden, der Rollen anlegen und verändern kann, der jedoch keine Benutzer oder Profile anlegen oder verändern darf. SAP bietet hierzu die Vorlage SAP_ADM_AU an.
- Es sollte ein Profiladministrator vorgesehen werden. Dieser darf für vorhandene Rollen Profile generieren, die keine kritischen Systemberechtigungen enthalten (etwa S_USER*), da diese zur Benutzer- und Rollenverwaltung berechtigen. SAP bietet hierzu die Vorlage SAP_ADM_PR an.

- Diese Administratoren sind der Gruppe SUPER zuzuordnen.
- Es sollte ein Administrator-Administrator definiert werden. Dieser verwaltet die Benutzer-, Rollen-, und Profil-Administratoren. Der Administrator-Administrator sollte dem Profil S_A.SYSTEM zugeordnet werden, das zur Verwaltung von Benutzern in der Gruppe SUPER benötigt wird. Der Administrator-Administrator sollte nur im Vier-Augen-Prinzip genutzt werden. Er kann beispielsweise durch den Benutzer-Administrator gesperrt und bei Bedarf für die Dauer der Nutzung entsperrt werden.

Durch die Trennung (sofern technisch richtig umgesetzt) wird erreicht, dass sich die Administratoren nicht selbst Berechtigungen zuordnen können und für sie auf diese Weise nur die ihnen zugeordneten Aufgaben ausführbar sind.

In kleineren Unternehmen oder Behörden kann es aufgrund eingeschränkter Personalverfügbarkeit vorkommen, dass keine Trennung vorgenommen werden kann und alle Aufgaben durch eine Person ausgeführt werden. Alle Daten im SAP System können dann durch den Administrator unbemerkt eingesehen und verändert werden. Generell ist dies als sicherheitskritisch zu bewerten, so dass zusätzliche Kontrollen notwendig sind. Gleiches gilt allgemein auch im Kontext wichtiger finanz- und bilanzrelevanter Prozesse sowie bei der Verarbeitung personenbezogener Daten, wo beispielsweise eine entsprechende Funktionstrennung vorhanden sein muss. Kann diese nicht erreicht werden, müssen geeignete Kontrollen auf organisatorischer Ebene definiert und deren Durchführung sichergestellt werden. Entsprechende Prüfungen auf das Vorhandensein von Kontrollen finden beispielsweise auch im Kontext von Sarbanes Oxley Act bezogenen Prüfungen statt.

Die von SAP vorgegebenen und ausgelieferten Rollen sind sorgfältig gegen die eigenen Anforderungen zu prüfen und anzupassen.

Hinweise auf SAP Dokumentationen zum Aufbau der Berechtigungsverwaltung und zu relevanten Berechtigungen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Werkzeuge zur Berechtigungsverwaltung**

Berechtigungen, Profile und Rollen können auch manuell verwaltet werden. Von diesem Vorgehen wird jedoch aus Sicherheitsgründen dringend abgeraten, da aufgrund der zu verwaltenden Objektmengen bei manueller Pflege immer Berechtigungsprobleme entstehen. Der Einsatz des Profilgenerators (Transaktion PFCG) wird daher dringend empfohlen. Insbesondere dürfen dann keine manuellen Veränderungen an den Profilen erfolgen.

Administratoren müssen sich mit den Mechanismen und Verfahren beim Einsatz des Profilgenerators vertraut machen, damit eine korrekte Berechtigungsvergabe erfolgt. So muss beispielsweise der Profilgenerator zunächst über die Transaktion SU25 initialisiert werden. Insbesondere die Verwendung und Pflege von Prüfkennzeichen (Transaktion SU24) muss bekannt sein. In Testläufen können fehlende Berechtigungen (diese sind beispielsweise über die Transaktion SU53 oder über Berechtigungstraces mit ST01 feststellbar) erkannt werden.

Neben den systeminternen Werkzeugen zur Berechtigungsverwaltung werden von Drittherstellern auch externe Werkzeuge zur Benutzer- und Berechtigungsverwaltung angeboten. Diese sind in der Regel mit einer komfortableren Benutzungsschnittstelle ausgestattet, da diese direkt auf dem Betriebssystem ablaufen. Ob solche Werkzeuge als Alternative zu den systeminternen Werk-

zeugen genutzt werden, ist jeweils im Einzelfall unter Kosten/Nutzen-Aspekten zu entscheiden.

Hinweise auf SAP Dokumentationen zur Berechtigungsverwaltung mit dem Profilgenerator finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Applikationsspezifische Berechtigungsverwaltung**

Einige Produkte und Applikationen nutzen zusätzlich zum SAP Standardberechtigungskonzept auch noch eigene Berechtigungskonzepte und -verwaltungswerkzeuge (z. B. das SAP Customer Relationship Management, mySAP CRM oder das Modul Human Capital Management, HCM). Dies ist bei der Verwaltung auch zu berücksichtigen, da zusätzliche Verwaltungsschritte und -arbeiten notwendig sind. Insbesondere muss bedacht werden, dass das Produkt oder die Applikation nur dann sicher betrieben werden kann, wenn auch die applikationsspezifischen Berechtigungen über die applikationsspezifischen Verwaltungswerkzeuge sicher konfiguriert wurden. Generell ist dabei auch auf minimale Berechtigungen, Rollentrennung und auf Trennung von Aufgaben und Verantwortlichkeiten zu achten. So darf beispielsweise in einem CRM-System ein Warenbestellkorb nicht durch die gleiche Person zur Bestellung freigegeben werden, die den Warenkorb erzeugt hat.

Generell spielt auf Applikationsebene das Thema Geschäftsrisikomanagement eine wichtige Rolle: Bei der Vergabe von Berechtigungen definiert unter anderem auch das Risikomanagement die Kriterien für die Vergabe von Berechtigungen.

Prüffragen:

- Existiert ein Rollenkonzept zur Verwaltung des SAP-Systems?
- Wurden die von SAP vorgegebenen und ausgelieferten Rollen gegen die eigenen Anforderungen geprüft und angepasst?
- Sind die SAP Administratoren mit den Mechanismen und Verfahren beim Einsatz des SAP Profilgenerators vertraut?

# M 4.261 Sicherer Umgang mit kritischen SAP Berechtigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Berechtigungen, die im Sinne der Sicherheit oder aus rechtlicher oder betriebswirtschaftlicher Sicht kritische Operationen erlauben, werden von SAP "kritische Berechtigung" genannt. Betroffen sind z. B. Operationen, die zu Betrug führen können oder über die wichtige Daten und Konfigurationen gelesen oder modifiziert werden können.

Die Vergabe von kritischen SAP Berechtigungen muss generell mit besonderer Sorgfalt erfolgen. Der Umgang mit kritischen SAP Berechtigungen ist daher im Vorfeld zu planen. Organisatorische und technische Maßnahmen sowie Prozesse müssen dann sicherstellen, dass das gewünschte Sicherheitsniveau umgesetzt wird. Im Folgenden wird bewusst keine Liste mit kritischen SAP Berechtigungen angegeben, da diese immer unvollständig wäre und damit Administratoren in falscher Sicherheit wiegt. In der Regel wird dann darauf verzichtet, die Liste zu prüfen und zu erweitern. Die Identifikation kritischer SAP Berechtigungen für den konkreten Einsatz eines SAP Systems ist jedoch ein wichtiger Schritt, der auf jeden Fall durchgeführt werden muss.

**Kritische SAP Berechtigungen, Profile, Rollen identifizieren**

Kritische SAP Berechtigungen hängen aufgrund des SAP Berechtigungskonzeptes auch von den Feldern und Feldwerten von Berechtigungsobjekten ab. Dies gilt insbesondere für Berechtigungen, die in Applikationen oder Modulen zum Einsatz kommen und damit aus betriebswirtschaftlicher Sicht als kritisch zu betrachten sind. Es wird daher empfohlen, kritische Felder in Berechtigungsobjekten zu identifizieren, um so die betroffenen Berechtigungsobjekte zu identifizieren. Nur so kann überhaupt eine spätere Prüfung erfolgen, und nur bei Kenntnis der Berechtigungsobjekte kann die Prüfung automatisiert werden. Beispiele für kritische Felder in Berechtigungsobjekten sind Felder für Kosten-Center, Buchungskreis, Profit-Center oder Werk.

Kritische SAP Berechtigungen sind auch alle Berechtigungen, die im Rahmen der SAP System-Administration verwendet werden. Dies sind alle Berechtigungen die von Berechtigungsobjekten abgeleitet sind und mit dem Präfix "S_" beginnen.

Neben Berechtigungen lassen sich auch kritische Profile und Rollen identifizieren, die bereits im Auslieferungszustand enthalten sind. Alle Profile, die auf "_ALL" enden, sind als kritisch anzusehen, da damit in der Regel alle Berechtigungen erteilt werden, die für einen Teilbereich im System, einer Applikation oder eines Moduls relevant sind. Alle Rollen, die die Zeichenkette "ADM" enthalten, sind als kritisch anzusehen, da diese in der Regel administrative Rollen bezeichnen.

Bei der Identifikation kritischer SAP Berechtigungen, Profile und Rollen ist zu bedenken, dass SAP für Namen zwar ein Konzept vorschlägt, dies aber durch Applikationen oder eigene Entwicklungen nicht immer berücksichtigt wird. Daher können auch kritische Berechtigungen, Profile und Rollen bestehen, die nicht in das vorgenannte Namensschema passen.

Manuell ist die Identifikation kritischer SAP Berechtigungen insgesamt schwierig. Es sind jedoch von SAP und Drittherstellern Werkzeuge verfügbar, die

automatisiert auf kritische Berechtigungen prüfen können. Dabei sind die kritischen SAP Berechtigungen in der Regel durch den Hersteller der Prüfsoftware vordefiniert.

Hinweise auf SAP Dokumentationen zu Berechtigungsprüfungen finden sich in M 2.346 *Nutzung der SAP Dokumentation*. Bei der Identifikation kritischer Berechtigungen ist entsprechendes Wissen über die zugrunde liegenden Berechtigungsprüfungen notwendig.

**Anpassen kritischer SAP Berechtigungen, Profile, Rollen**

Sind die kritischen SAP Berechtigungen, Profile und Rollen identifiziert, so sollten diese gemäß der Berechtigungsplanung angepasst werden. Insbesondere bei der Anpassung von Profilen und Rollen zur Systemverwaltung müssen die damit verbundenen Effekte für Systemfunktionen berücksichtigt werden. Nach der Anpassung ist daher zu prüfen, ob das gewünschte Systemverhalten erreicht wurde oder ob es zu Fehlfunktionen kommt. Dieser Anpassungsprozess kann bei stärkeren Veränderungen an den vorgegeben Berechtigungen, Profilen oder Rollen aufwendig und zeitintensiv sein und sollte nicht im Produktivsystem durchgeführt werden.

**Verwendung kritischer SAP Systemberechtigungen einschränken**

Im Rahmen der Berechtigungsplanung müssen die Regeln für den Umgang mit kritischen SAP Berechtigungen, Profilen und Rollen festgelegt werden. Folgende Empfehlungen sind dabei zu berücksichtigen:

- Die Profile SAP_ALL, SAP_NEW* und S_DEVELOP* dürfen in einem Produktivsystem nicht genutzt werden.
- Administrative Berechtigungen, Profile und Rollen dürfen entsprechend der Berechtigungsplanung (siehe M 2.342 *Planung von SAP Berechtigungen*) nur an administrative Benutzer vergeben werden. Auf ausreichende Rollentrennung ist dabei zu achten.

Hinweise auf weitere Informationen dazu finden sich in, M 2.346 *Nutzung der SAP Dokumentation*.

**Liste mit kritischen SAP Berechtigungen pflegen**

Sind die kritischen SAP Berechtigungen identifiziert, so empfiehlt es sich, diese Liste im SAP System zu pflegen. Dann kann automatisiert geprüft werden, welchen Benutzern kritische SAP Berechtigungen zugeordnet wurden. Die Pflege der Liste kritischer SAP Berechtigungen erfolgt über die Transaktion SU96. Über den Report "RSUSR009" lassen sich die Benutzer anzeigen, die eine der kritischen SAP Berechtigungen besitzen.

Auch bestimmte Kombinationen von unkritischen SAP Berechtigungen können kritisch sein, da sie beispielsweise in der Kombination ermöglichen, dass eine oder mehrere als kritisch eingestufte Transaktionen aufgerufen werden können. Ein SAP System bietet hier die Möglichkeit an, automatisiert nach Benutzern zu suchen, die die Berechtigungen besitzen, bestimmte Kombinationen von Transaktionen aufzurufen. Dazu ist über die Transaktion SU98 (Pflege der Tabelle SUKRI) eine Liste der kritischen Kombinationen zu pflegen. Über den Report "RSUSR008" lassen sich dann die Benutzer identifizieren, die die kritischen SAP Berechtigungskombinationen besitzen.

In neueren SAP Systemen (ab Version 6.20) sollte der Report RSUSR008_009_new genutzt werden, der die Funktionen der Reports RSUSR008 und RSUSR009 ersetzt.

Die im Auslieferungszustand eines SAP Systems enthaltenen Listen für die kritischen SAP Berechtigungen und Transaktionskombinationen sind nur als Beispiel anzusehen und sollten nicht für die Überprüfungen genutzt werden. Die Listen müssen selbst aufgebaut und gepflegt werden. Diese können beispielsweise auch bei Sarbanes Oxley Act bezogenen Prüfungen begutachtet werden.

In diesem Kontext bietet SAP für die NetWeaver Plattform mit dem SAP GRC Access Control kostenpflichtig ein entsprechendes Zusatz-Prüfwerkzeug an, so dass entsprechende Risiken automatisiert erkannt werden können. Prüfwerkzeuge sind auch von Drittherstellern erhältlich.

Prüffragen:

- Sind die kritischen SAP Berechtigungen, Profile und Rollen identifiziert und gemäß der Berechtigungsplanung angepasst?
- Werden Tabellen mit kritischen SAP Berechtigungen und kritischen Kombinationen von Transaktionen im SAP System gepflegt?

# M 4.262 Konfiguration zusätzlicher SAP Berechtigungsprüfungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein SAP System erlaubt es, die vorkonfigurierten Berechtigungsprüfungen (siehe dazu M 2.342 *Planung von SAP Berechtigungen*) zu verändern. Berechtigungsprüfungen können deaktiviert werden. Es können auch zusätzliche Berechtigungsprüfungen erfolgen. Im Rahmen der Berechtigungsplanung ist diese Möglichkeit zu berücksichtigen. Generell ist bei Veränderungen an den Berechtigungsprüfungen Folgendes zu bedenken:

**Deaktivieren von Berechtigungsprüfungen**

Werden vorhandene Berechtigungsprüfungen deaktiviert, so kann dies die Sicherheit des SAP Systems gefährden, da damit Zugriffskontrollen abgeschaltet werden. Bevor Prüfungen deaktiviert werden, müssen die Auswirkungen auf die Sicherheit sorgfältig geprüft werden.

Hinweise auf weitere Informationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Erzeugen von Transaktionen für den Start von Programmen oder Reports**

Programme und Reports können beispielsweise über die Transaktion SE38 (ABAP Editor) gestartet werden. Nicht jedem Programm oder Report ist jedoch ein Transaktionscode zugeordnet. Sollen bestimmte Programme oder Reports Benutzern verfügbar gemacht werden, so empfiehlt sich, diese über eine Transaktion verfügbar zu machen. Dies hat den Vorteil, dass der Zugriff auf die Transaktion und damit das Programm oder den Report über Berechtigungen vom Typ S_TCODE geschützt werden können. Zusätzlich kann der Zugriff auf die Transaktion SE38 gesperrt werden, da damit prinzipiell beliebiger Code ausgeführt werden kann.

Auch bei diesem Vorgehen ist zu beachten, dass weiterhin die durch den Profilgenerator erzeugten Berechtigungen zum Aufruf von Programmen oder Reports gepflegt werden müssen. Dazu sind die vom Berechtigungsobjekt S_PROGRAM abgeleiteten Berechtigungen in den Rollen-Berechtigungsprofilen entsprechend der Berechtigungsplanung zu modifizieren.

**Einsatz von Parametertransaktionen**

Über neu angelegte Parametertransaktionen können für Transaktionen Werte oder Wertebereiche für die Aufrufparameter vorgegeben werden. Die neu angelegten Parametertransaktionen (Transaktion SU93) können dann über eigene Berechtigungen (Berechtigungsobjekt S_TCODE) zugriffsbeschränkt werden.

Es ist in diesem Zusammenhang wichtig zu berücksichtigen, dass der Einsatz von Parametertransaktionen nicht als Sicherheitsverfahren geeignet ist, um den Zugriff auf Funktionen der Transaktion oder auf Daten zu beschränken. Generell muss der Zugriff, beispielsweise auf Programme, Reports oder Tabellen, immer über die entsprechenden Berechtigungsobjekte (S_PROGRAM für Programme und Reports, S_TABU_DIS für Tabellen) eingeschränkt werden.

**Anpassen der ABAP-Berechtigungsgruppen**

Für Programme, Reports und Tabellen können so genannte Berechtigungsgruppen definiert werden. Damit kann eine Gruppierung erfolgen, so dass der Zugriff auf die Programme, Reports oder Tabellen einer Gruppe über ein Berechtigungsobjekt gesteuert werden kann.

Folgendes ist beim Einsatz von ABAP-Berechtigungsgruppen zu beachten:

- Der Zugriff wird immer auf alle Objekte einer Gruppe reglementiert.
- Die Berechtigungsgruppe stellt eine zusätzliche Prüfung dar. Die normalen Berechtigungsprüfungen, die das Programm oder der Report durchführt, werden davon nicht berührt.
- Werden Berechtigungsgruppen genutzt, so kann in der Planung mit einer groben Gruppierung, etwa bezüglich einzelner Applikationen oder Module, begonnen werden. Diese können dann entsprechend dem gewünschten Schutzbedarf weiter verfeinert werden.
- Die genaue Funktionsweise von Berechtigungsgruppen und deren Verwaltung muss Planern und durchführenden Administratoren bekannt sein.

Hinweise auf weitere Informationen zur Konfiguration von Berechtigungsgruppen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Eigene zusätzliche Berechtigungsobjekte**

Werden im Unternehmen oder der Behörde eigene (ABAP-) Programme entwickelt oder der Programm-Code vorhandener Programme modifiziert, so können auch Berechtigungsprüfungen für neue, selbst definierte Berechtigungsobjekte eingebaut werden. Damit diese durch den Profilgenerator berücksichtigt werden, müssen die Prüfkennzeichen über die Transaktion SU24 definiert und entsprechend angepasst werden. Dies ist im Rahmen der Change-Management Prozesse zu umzusetzen.

**Veränderungen dokumentieren**

Alle Veränderungen an der Berechtigungsprüfung sind zu dokumentieren.

Prüffragen:

- Werden SAP Berechtigungsprüfungen nur nach sorgfältiger Prüfung deaktiviert?
- Werden die durch den SAP Profilgenerator erzeugten Berechtigungen zum Aufruf von Programmen oder Reports entsprechend der Berechtigungsplanung gepflegt?
- Sind die genaue Funktionsweise von SAP Berechtigungsgruppen und deren Verwaltung den Planern und durchführenden Administratoren bekannt?

# M 4.263 Absicherung von SAP Destinationen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein SAP System kann neben der Server-Rolle, in der es seine Funktionen zum Zugriff anbietet, auch die Client-Rolle annehmen, in der es auf Funktionen anderer SAP Systeme zugreift. Destinationen beschreiben dabei die unterschiedlichen Zielsysteme und enthalten alle zum Zugriff notwendigen Informationen. Generell sind dies der Rechnername oder die IP-Adresse, das zu verwendende Protokoll und Nummer des Kommunikationsports, die die Netzverbindung zum Zielsystem beschreiben.

Für Destinationen können aber auch Authentisierungsinformationen hinterlegt werden. Beim Zugriff auf die Destination werden diese dann zur Anmeldung am Zielsystem genutzt. Sind keine Authentisierungsinformationen hinterlegt, so müssen diese durch den aufrufenden Benutzer angegeben werden. Die entfernte Ausführung erfolgt dann unter den Berechtigungen des angegebenen Benutzers. In diesem Zusammenhang werden im Kontext von Destinationen, auf die über RFC (Remote Function Call) zugegriffen wird, üblicherweise folgende Begrifflichkeiten verwendet:

- RFC-Benutzer: Der Benutzer, der im Server-System aktiv ist und bestimmte Berechtigungen besitzt.
- RFC-Service-Benutzer: Ein RFC-Benutzer wird dann Service-Benutzer genannt, wenn die Anmeldedaten (Benutzer und Kennwort) beim Client gespeichert sind.

Destinationen werden in einer mandantenunabhängigen Tabelle gehalten, daher hat jeder Benutzer Zugriff auf alle Destinationen im SAP System. Somit muss der Zugriff auf die Destinationen abgesichert werden. Folgende Empfehlungen sind für Destinationen zu berücksichtigen:

### Speichern von Authentisierungsinformationen

Authentisierungsinformationen sollten nur dann hinterlegt werden, wenn dies nicht zu vermeiden ist. Es ist dabei abzuwägen, ob der Schutz des benutzten Passwortes oder der Schutz des Zielsystems vor unberechtigten Zugriffen überwiegt. Es ist zu beachten, dass für RFC-Destinationen, die aus Programmen heraus genutzt werden, die Authentisierungsinformationen hinterlegt werden müssen, sofern das Server-System nicht für die so genannte Trusted-RFC-Kommunikation konfiguriert ist, so dass generell alle RFC-Aufrufe aus den vertrauten SAP System ohne Authentisierung erfolgen können.

Werden Authentisierungsinformationen hinterlegt, so sollte ausschließlich ein Benutzer vom Typ Kommunikation gewählt werden. Insbesondere sollten keine Dialog-Benutzer eingetragen werden, da sonst über die Destination eine interaktive Anmeldung ohne Passworteingabe möglich ist.

Die Möglichkeit, Passwörter unverschlüsselt zu speichern, sollte nicht benutzt werden.

### Zugriff auf Destinationen

Der Zugriff auf Destinationen muss eingeschränkt werden, so dass nur berechtigte Benutzer darauf zugreifen können.

Der Zugriff auf Destinationen kann über das Berechtigungsobjekt S_ICF gesteuert werden. Folgende Berechtigungsfelder sind für das Berechtigungsobjekt definiert, die für die Zugriffssteuerung benutzt werden:

- ICF_FIELD: Typ des zu schützenden Objekts
  Dieses Feld kann folgende Werte beinhalten:
  - SERVICE: für Verwendung von ICF-Services
  - DEST: für Verwendung von RFC-Destinationen (ab 6.20)
- ICF_VALUE: Wert des zu schützenden ICF-Objektes
  Dieses Feld enthält den Wert des entsprechenden Objektes. Die Werte, die geschützt werden sollen, werden in der Transaktion SICF für ICF-Services und in der Transaktion SM59 für RFC-Destinationen gepflegt.

Folgendes ist dabei zu beachten:

- Destinationen müssen nach Einsatzszenarien gruppiert werden. Benutzern kann dann der Zugriff auf alle im Szenario benötigten Destinationen erlaubt werden. Probleme treten jedoch dann auf, wenn Destinationen in mehreren Szenarien eingesetzt werden, da pro Destination nur eine Zuordnung zu genau einer Gruppe möglich ist. In diesem Fall muss eine weitere Unterteilung erfolgen.
- Der Zugriff auf Destinationen mit unterschiedlichem Schadenspotential muss über getrennte Berechtigungen gesteuert werden.

Es ist zu bedenken, dass eine Destination für viele Zwecke genutzt werden kann. Der Zugriffsschutz kann daher nur als Einstiegshürde dienen. Schlussendlich muss der Schutz des Zielsystems durch die aufgerufenen Funktionen selbst und die Berechtigungsvergabe im Zielsystem erfolgen.

Dies gilt insbesondere für Destinationen, auf die über Trusted-RFC zugegriffen wird (dann auch "Trusted Destination" genannt). In diesem Fall werden die Berechtigungen über die Berechtigungsobjekte S_RFC und S_RFCACL gesteuert.

Hinweise auf Detailinformationen zur Zugriffssteuerung auf Destinationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Unbenutzte Destinationen absichern**

Für nicht benutzte Destinationen muss entschieden werden, ob diese nur vorübergehend oder gar nicht mehr genutzt werden. Im ersten Fall sind die Destinationen zu deaktivieren, im zweiten Fall sind die Destinationen zu löschen.

**Übertragen von Destinationen in andere Systeme**

Werden Destinationen von einem System in ein anderes System übertragen, so werden auch die in Destinationen gespeicherten Authentisierungsdaten übertragen. Diese Destinationen können dann im System, in das sie importiert wurden, sofort zum erfolgreichen Zugriff auf das in der Destination angegebene Zielsystem benutzt werden. Dies ist beim Übertragen von Destinationen (z. B. bei Systemkopien) zu berücksichtigen.

**Zugriff auf Destinationspflege und -tabelle einschränken**

Die Pflege von Destinationen erfolgt über die Transaktion SM59. Es wird empfohlen, den Zugriff auf diese Transaktion auf die berechtigten Administratoren einzuschränken (Berechtigungsobjekt S_TCODE).

Es ist zu bedenken, dass die RFC-Destinationsdaten in der Tabelle RFCDES abgelegt werden. Hinterlegte Passwörter sind dabei kodiert gespeichert, im

SAP System sind jedoch alle Informationen vorhanden, um die Passwörter zu dekodieren. Der direkte Tabellenzugriff ist daher ebenso einzuschränken (siehe M 4.264 *Einschränkung von direkten Tabellenveränderungen in SAP Systemen*).

**THOST Tabelle absichern**

In der Tabelle THOST werden symbolische Rechnernamen (SAP Name), die innerhalb des SAP Systems verwendet werden, auf DNS-Rechnernamen (Netz-Name) abgebildet. Der Zugriff auf die Tabellenpflege (Transaktion SM55 oder über SE16) muss daher auf die berechtigten Administratoren eingeschränkt werden (Berechtigungsobjekt S_TCODE).

Auf die Konsistenz der SAP Namen mit den Netz-Namen ist zu achten, damit auf die jeweils richtigen IT-Systeme zugegriffen wird.

Prüffragen:

- Werden die Destinationen im SAP System so abgesichert, dass nicht jeder Benutzer Zugriff auf alle Destinationen hat?
- Werden Benutzer-Anmeldeinformationen für Destinationen nur dann gespeichert, wenn andere Lösungen nicht in Frage kommen?
- Wurden bei der Hinterlegung von Authentisierungsinformationen im SAP System ausschließlich Benutzer vom Typ Kommunikation gewählt (und keine Benutzer vom Typ Dialog)?
- Werden Passwörter im SAP System nur verschlüsselt gespeichert?
- Wird der Zugriff auf Destinationen mit unterschiedlichem Schadenspotential über getrennte Berechtigungen gesteuert?
- Haben nur berechtigte SAP Administratoren Zugriff auf die Transaktion SM59 zur Pflege von Destinationen?
- Ist der direkte Tabellenzugriff auf die RFC-Destinationsdaten auf berechtigte SAP Administratoren eingeschränkt?
- Ist der direkte Tabellenzugriff auf die symbolischen Rechnernamen in der Tabelle THOST auf berechtigte SAP Administratoren eingeschränkt?
- Wurde auf die Konsistenz der SAP-Namen mit den Netz-Namen geachtet?

# M 4.264 Einschränkung von direkten Tabellenveränderungen in SAP Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Alle Daten eines SAP Systems werden in den Tabellen der Datenbank des SAP Systems gehalten. Bei der Nutzung erfolgen die Tabellenveränderungen z. B. durch die aufgerufenen Transaktionen, Programme oder RFC-Bausteine.

**Berechtigungen auf Tabellen-Zugriffstransaktionen einschränken**

Im SAP System besteht die Möglichkeit, auch direkt auf die Inhalte von Tabellen lesend oder verändernd zuzugreifen. Der Zugriff auf Tabellen und Tabelleninhalte kann durch unterschiedliche Transaktionen erfolgen. Dies sind beispielsweise SE16 Data Browser, SE80 Workbench, SE84 Repository Browser, SM30 Pflege Tabellensichten, SM31 Pflege Tabellen, SE11 Data Dictionary, SQVI Quick Viewer.

Je nach Version des SAP Systems und je nachdem, welche Applikationen und Module installiert sind, können auch zusätzliche Transaktionen oder Reports existieren, die direkte Tabellenzugriffe erlauben.

Der Zugriff auf die oben genannten Transaktionen sollte mindestens eingeschränkt werden, so dass nur die berechtigten Administratoren oder Benutzer diese aufrufen können. Die Liste der Transaktionen, die aus diesem Grund zugriffsbeschränkt werden sollten, muss entsprechend der lokalen Systemausprägung erweitert werden. Der Zugriff wird über das Berechtigungsobjekt S_TCODE konfiguriert.

Es wird empfohlen, regelmäßig zu prüfen, welche Benutzer auf die in diesem Sinne kritischen Transaktionen zugreifen können. Dazu kann beispielsweise das Benutzer-Informationssystem (Transaktion SUIM) genutzt werden, über das Benutzer nach unterschiedlichen Suchkriterien aufgelistet werden können.

Über die Transaktion S_BCE_68001398 können direkt die Benutzer aufgelistet werden, die auf eine bestimmte Transaktion Zugriff besitzen. Diese Transaktion kann für Einzeltests benutzt werden.

**Berechtigungen für den Tabellenzugriff konfigurieren**

Können die Transaktionen für den direkten Tabellenzugriff nicht beschränkt werden, so besteht die Möglichkeit, Tabellenzugriffe über direkte Berechtigungen auf Tabellen zu steuern. Die dabei benutzten Berechtigungsobjekte sind S_TABU_DIS, S_TABU_CLI und S_TABU_LIN. Über das Berechtigungsobjekt S_TABU_DIS können Berechtigungen auf mandantenbezogene Tabellen-Gruppen vergeben werden. Diese werden in der Tabelle TBRG definiert und fassen einzelne Tabellen zu Gruppen zusammen. Für jede Tabellen-Gruppe wird über die Tabelle TDDAT eine zugehörige Berechtigungsgruppe definiert. Für die Zugriffssteuerung werden die Namen der Tabellen-Berechtigungsgruppen als Werte in den Parameter DIBERCLS aufgenommen. Die erlaubten Operationen werden über den Parameter ACTVT gesteuert. Über das Berechtigungsobjekt S_TABU_CLI können analog Berechtigungen auf mandantenunabhängige Tabellen-Gruppen vergeben werden.

Es ist unbedingt notwendig, Berechtigungsobjekte S_TABU_DIS und S_TABU_CLI für die Zugriffskontrolle auf Tabellen einzusetzen, wenn der Zugriff auf Transaktionen, die direkten Tabellenzugriff erlauben, nicht ausgeschlossen ist.

Mittels S_TABU_LIN lassen sich Berechtigungen auf einzelne Tabellenzeilen vergeben. Dieser Mechanismus erfordert jedoch zusätzliche Customizing-Einstellungen. Hierzu müssen so genannte Organisationskriterien definiert und aktiviert werden. Auf Grund der Komplexität der Definition der Autorisierungsreichweiten wird dieses Objekt in der Praxis eher selten verwendet.

Eine häufig genutzte Variante, den Zugriff auf bestimmte Tabellen zuzulassen, ist die Definition von Parametertransaktionen. Dadurch werden Transaktionen definiert, die andere Transaktionen mit vordefinierten Werten aufrufen. Im vorliegenden Fall wird dann die Transaktion SE16 direkt mit dem gewünschten Tabellennamen aufgerufen. Der Tabellenname wird dann als Wert für den Parameter "DATABROWSE-TABLENAME" in den Vorschlagswerten definiert. Parametertransaktionen werden über die Transaktion SE93 definiert. Bei diesem Vorgehen ist zu beachten, dass trotzdem die Zugriffsberechtigungen für Tabellen über S_TABU_DIS vergeben werden müssen, da Parametertransaktionen nicht zur Zugriffssteuerung geeignet sind.

Hinweise auf SAP Dokumentationen dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Haben nur berechtigte SAP Administratoren oder SAP Benutzer direkten Zugriff auf Tabellen-Transaktionen?
- Wird regelmäßig überprüft, welche SAP Benutzer auf kritische Tabellen-Transaktionen zugreifen können?

# M 4.265 Sichere Konfiguration der Batch-Verarbeitung im SAP System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Im Rahmen der Hintergrundverarbeitung (Batch-Verarbeitung) werden in der Regel Abläufe (Batch-Jobs) automatisiert durchgeführt. Zusätzlich können Arbeiten zeitgesteuert ausgeführt werden. Folgendes ist bei der Konfiguration zu bedenken:

- Batch-Jobs werden über die Transaktion SM36 gesteuert. Auf diese Transaktion sollten nur berechtigte Batch-Administratoren Zugriff besitzen.
- Über die folgenden Berechtigungsobjekte erfolgt die Verwaltung der Batch-Verarbeitung. Die Vergabe der Berechtigungen ist generell über das Berechtigungskonzept zu regeln.

  - Die Ausprägung des Berechtigungsobjektes S_BTCH_ADM mit Wert "Y" ermöglicht Vollzugriff auf die Batch-Administration.
    Es ist zu beachten, dass keine weiteren Einschränkungen erfolgen können. Ein Benutzer mit dieser Berechtigung kann immer alle Verwaltungsoperationen ausführen und darf nur an wenige Administratoren (z. B. Batch-Verwalter, Stellvertreter) vergeben werden.
  - Die Ausprägung des Berechtigungsobjektes S_BTCH_JOB mit Wert "LIST" ermöglicht es einem Batch-Verwalter, die von Batch-Jobs erzeugten Spool-Aufträge anzuzeigen. Da darin die Ausgabedaten des Batch-Jobs enthalten sind, muss im Rahmen des Berechtigungskonzeptes entschieden werden, unter welchen Umständen und durch wen diese Berechtigung verwendet werden darf.
  - Benutzer können immer - ohne besondere Berechtigungen besitzen zu müssen - eigene Jobs erzeugen und verwalten. Folgende Berechtigungsobjekte können für spezielle Operationen verwendet werden, die ohne die Berechtigung nicht möglich sind:

    - S_BTCH_JOB: Erlaubt je nach Wert-Einstellung Folgendes:

      - Wert "DELE": Jobs anderer Benutzer löschen
      - Wert "LIST": Spool-Aufträge anzeigen
      - Wert "PROT": Job-Protokolle ansehen, auch für andere Benutzer
      - Wert "SHOW": Job-Details anzeigen
      - Wert "RELE": Jobs anderer Benutzer freigeben

      Da es sich bei den betroffenen Operationen um kritische Operationen handelt, muss die Verwendung sorgfältig geplant werden. In der Regel dürfen diese Berechtigungen nicht an normale Benutzer vergeben werden.
    - S_BTCH_NAM: Ein Benutzer kann Batch-Jobs unter den Berechtigungen eines anderen Benutzers ausführen. Die Benutzer, unter denen der Batch-Job ausgeführt werden kann, sind in der Berechtigung anzugeben. Die Vergabe der Berechtigung ist unter Sicherheitsgesichtspunkten als kritisch zu betrachten und nur für Batch-Administratoren sinnvoll, um beispielsweise Batch-Jobs unter technischen Benutzern ablaufen zu lassen.

- Da die Batch-Verarbeitung im Hintergrund und automatisiert erfolgt, findet sie in der Regel unbemerkt statt. Auswirkungen, hervorgerufen durch unautorisierte Veränderungen an der Batch-Verarbeitung, können daher längere Zeit unbemerkt bleiben. Eine restriktive Berechtigungsvergabe ist daher notwendig.
- Die Hintergrund-Verarbeitung wird in der Regel unter den Berechtigungen des Benutzers durchgeführt, der einen Batch-Job erzeugt. Insofern greifen die konfigurierten Berechtigungen des Benutzers.
- Werden Batch-Jobs unter den Berechtigungen technischer Benutzer ausgeführt, so sind die Berechtigungen der technischen Benutzer zu beschränken. Es empfiehlt sich nicht, einen technischen Batch-Benutzer mit dem Profil SAP_ALL auszustatten.
- Der Zugriff auf die Verwaltung der Batch-Verarbeitung sollte nur für die berechtigten Administratoren möglich sein.
- Durch die Batch-Verarbeitung kann Last auf einem SAP System erzeugt werden. Es muss daher entschieden werden, ob normale Benutzer Batch-Jobs starten dürfen oder ob diese durch den Batch-Administrator freigegeben und eingeplant werden, nachdem der Batch-Job vom Benutzer erzeugt wurde.

Hinweise zu SAP Dokumentationen zur Batch-Verarbeitung finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Haben nur berechtige SAP Administratoren Zugriff auf die Transaktion SM36, um Batch Jobs zu steuern?
- Haben nur die notwendigen SAP Administratoren Vollzugriff auf die Batch-Administration?
- Ist im Rahmen des Berechtigungskonzeptes festgelegt, welche Batch-Verwalter die Berechtigung haben, die von Batch-Jobs erzeugten Spool-Aufträge anzuzeigen?
- Haben nur Batch-Administratoren die Berechtigung, einen Batch-Job unter den Berechtigungen eines anderen Benutzers auszuführen?
- Haben nur berechtigte SAP Administratoren Zugriff auf die Verwaltung der Batch-Verarbeitung?

# M 4.266 Sichere Konfiguration des SAP Java-Stacks

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Java-Stack eines SAP Systems erlaubt es, Java-basierte Technologien einzusetzen. Diese werden vornehmlich in Web-basierten Szenarien genutzt. Im Gegensatz zum ABAP-Stack ist der Java-Stack relativ neu und dessen Funktionen finden sich weniger häufig im Einsatz. Die neuen Java-basierten Technologien ergänzen jedoch die ABAP-Welt, so dass die Bedeutung des Java-Stacks in Zukunft weiter zunehmen wird. Zwar werden viele geschäftsrelevante Funktionen weiterhin im ABAP-Stack ablaufen, aber die Frontend-Komponenten werden in Java implementiert sein. Der Java-Stack wird durch einen Applikationsserver gebildet, der die J2EE (Java 2 Enterprise Edition) Spezifikation umsetzt.

Da Java- und ABAP-Stack im NetWeaver ApplicationServer integriert sind und miteinander über den JavaConnector (JCo) kommunizieren können, muss ein installierter Java-Stack abgesichert werden. Dabei kommen jedoch im Vergleich zum ABAP-Stack völlig unterschiedliche Sicherheitsmechanismen und -konzepte zum Einsatz.

Im Folgenden werden die aus Sicherheitssicht wichtigsten Schritte aufgezeigt, die bei der initialen Konfiguration des Java-Stacks durchzuführen sind. Die Darstellung beschränkt sich auf die Konfiguration des Applikationsservers und geht damit nicht auf sonstige installierte Applikationen ein.

### Java-Stack Installation

Der Java-Stack sollte für SAP System Versionen, die eine separate Installation erlauben (Versionen bis 6.40), nur dann installiert werden, wenn Java-basierte Produkte oder Applikationen zum Einsatz kommen.

Kann der Java-Stack nicht separat installiert werden und wird nicht genutzt, so muss die Konfiguration so erfolgen, dass kein Zugriff auf den Java-Stack möglich ist. Dazu sollten alle Dienste des Java-Stacks deaktiviert werden.

### Schulung zum Java-Stack

Administratoren, die den Java-Stack administrieren, müssen Kenntnisse in der Architektur und den Sicherheitskonzepten der J2EE-Architektur besitzen. Hier sind insbesondere Kenntnisse bezüglich der statischen Konfiguration der Sicherheit für J2EE-konforme Objekte notwendig, die über das Administrationswerkzeug durch den Administrator durchgeführt wird. Es kommt dabei ein rollenbasiertes Sicherheitskonzept zum Einsatz. Zu beachten ist, dass SAP den J2EE Java Authentication and Authorization Service (JAAS) mit den SAP spezifischen User Management Engine (UME) Funktionalitäten erweitert hat. Damit wurde die statische Konfiguration der Sicherheitseinstellungen um eine dynamische Konfigurationsmöglichkeit durch den Programmcode erweitert, die über die UME steuerbar ist. In der UME können daher beispielsweise erlaubte Aktionen in den Programmen zu Rollen zusammengefasst werden. Benutzern kann dann diese Rolle zugeordnet werden, so dass sie damit die benötigten Berechtigungen erhalten.

Administratoren muss zudem bewusst sein, dass der Java-Stack mit einer separaten Benutzer- und Berechtigungsverwaltung ausgestattet ist, so dass hier

immer administrative Aufgaben durchgeführt werden müssen. Empfohlen ist hier der Einsatz der UME (siehe auch M 2.341 *Planung des SAP Einsatzes*), da damit die administrativen Tätigkeiten verringert werden.

**Nicht benötigte Dienste abschalten**

Der Java-Stack bietet eine Fülle von Diensten an. Nicht alle werden zum Betrieb in jedem Szenario benötigt. Daher sollten aus Sicherheitsgründen alle nicht benötigten Dienste deaktiviert werden. Problematisch dabei ist, dass Dienste voneinander abhängig sein können. Es kann zudem zwischen System-Diensten und Nicht-System-Diensten unterschieden werden. Die Verwaltung des Java-Stacks erfolgt über ein eigenes Werkzeug, den so genannten "Visual Administrator". Hier können auch die einzelnen Dienste verwaltet werden. Die Dienste finden sich dabei im "Server"-Abschnitt des Objekt-Baumes, der als Navigationshilfe im Visual Administrator dient. Die Detailinformationen zu einem Dienst werden angezeigt, sobald er selektiert wird.

Folgendes Vorgehen wird empfohlen:

- Zunächst wird der Dienst festgestellt, der die Technologie zum Ausführen der benötigten Applikation anbietet (z. B. Dienst servlet_jsp für Servlet-basierte Applikationen).
- Dann müssen die Abhängigkeiten des Dienstes festgestellt werden. Es muss dazu geklärt werden, welche anderen Dienste aktiviert sein müssen, damit der betrachtete Dienst ausgeführt werden kann. Dies ist aus der Registerkarte "Abhängigkeiten" in den Diensteigenschaften zu ersehen. In der Regel werden nur die Dienste mit starkem Abhängigkeitsverhältnis benötigt.
- Für die gefundenen Dienste muss nach gleichem Verfahren vorgegangen werden, bis sich die Liste der Dienste nicht mehr erweitert.
- Die Dienste, die nicht in der Liste erscheinen, können deaktiviert werden. Es ist zu beachten, dass bestimmte Dienste für den Betrieb des Java-Stacks benötigt werden.
- Nicht benötigte Applikationen können gestoppt oder deinstalliert werden. Dies erfolgt über den Dienst "deploy".
- Nicht benötigte Applikations-"Aliase", die über den Dienst "http" verwaltet werden, können deaktiviert werden.
- Nachdem Dienste oder Applikationen deaktiviert wurden, ist zu prüfen, ob die benötigten Dienste oder Applikation noch lauffähig sind.
- Falls die Applikation oder der Java-Stack nicht mehr lauffähig ist, sollten die Java-Stack Protokolle analysiert werden. In der Regel finden sich Fehlermeldungen, die auf den benötigten, aber deaktivierten Dienst hindeuten. Ansonsten kann nur durch Versuche die benötigte Kombination herausgefunden werden.
- Für Systemdienste muss das Startverhalten "always" über die XML-Konfigurationsdatei "runtime.xml" im Betriebssystem im jeweiligen Dienstverzeichnis oder das GUI-basierte "Configurations"-Werkzeug verändert werden (Wert: "never" oder "manual").

Da sich der Java-Stack mit jeder Version verändert und insbesondere Unterschiede in der Dienstanzahl und -funktion bestehen, kann an dieser Stelle keine verbindliche Liste angegeben werden.

Hinweise auf SAP Dokumentationen zu den Diensten und deren Funktion finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Standardinhalte entfernen**

Alle Standardinhalte wie Dokumentationen (etwa Dienst deploy: sap.com/...docs.examples), Beispielprogramme (etwa Dienst deploy: sap.com/...htmlb.ear) oder statische HTML-Seiten sollten deinstalliert werden.

**HTTP-Dienst absichern**

Der HTTP-Dienst sollte abgesichert werden, wozu unter anderem die folgenden Punkte gehören:

- Verzeichnisanzeige nicht zulassen
- nicht benötigte Aliase deaktivieren
- HTTP PUT (Hochladen von Daten) nicht erlauben

Hinweise auf SAP Dokumentationen zu den Diensten und deren Funktion finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Kryptographische Funktionsbibliothek installieren**

Damit für den Java-Stack starke kryptographische Verfahren genutzt werden können, sollte eine kryptographische Funktionsbibliothek installiert werden, die starke Verfahren anbietet. Hier kann auch auf freie Implementierungen aus dem Java-Umfeld zurückgegriffen werden. Generell ist beim Einsatz von kryptographischen Funktionsbibliotheken auf die Kompatibilität mit dem Java-Stack und auf die Lizenzbestimmungen des Anbieters zu achten.

Auch Java-Stack-Komponenten wie der Secure-Storage, der zur sicheren Ablage von Daten durch System-Dienste und Applikationen dient, benötigen kryptographische Verfahren. Daher kann eine adäquate Sicherheit nur nach der Installation der kryptographischen Funktionsbibliothek erreicht werden.

**Authentisierungsmodule konfigurieren**

Für die Authentisierung beim Zugriff auf den Java-Stack können mehrere Authentisierungsverfahren eingesetzt werden. So sind neben dem Benutzernamen und Passwort-Verfahren auch Zertifikate oder Single Sign-On Tickets für die Authentisierung konfigurierbar. Dabei kann die Reihenfolge der verwendeten Verfahren bestimmt werden und ob ein bestimmtes Verfahren zur alleinigen Authentisierung ausreichend ist.

Im Rahmen des Berechtigungskonzeptes ist daher zu entscheiden, welche Verfahren wie einzusetzen sind. Falls notwendig, können weitere Verfahren über zusätzliche Bibliotheken von Drittherstellern eingebunden werden. Dabei wird die durch den Java-Standard spezifizierte JAAS-Schnittstelle genutzt.

**Zugriff auf Systemressourcen beschränken**

Durch das Berechtigungskonzept muss bestimmt werden, welche Benutzer oder Gruppen auf die Systemressourcen des Java-Stacks zugreifen dürfen und welche Zugriffsoperationen (z. B. Lesen, Schreiben, Auflisten) erlaubt werden sollen. Die konfigurierbaren Operationen hängen dabei vom Typ der Ressource ab. Es empfiehlt sich daher, die Detail-Planung anhand eines konkreten Java-Stacks - etwa nach der Installation - durchzuführen. Weitere Informationen finden sich in M 4.268 *Sichere Konfiguration der SAP Java-Stack Berechtigungen*.

**Zugriff auf die Administrationsschnittstelle einschränken**

Der Java-Stack wird über mehrere Schnittstellen administriert:

- Visual-Administrator
  Der Visual-Administrator kommuniziert über die P4-Schnittstelle mit dem Java-Stack. Der Zugriff auf die P4-Schnittstelle (standardmäßig Port 50004 für die Instanz 00) muss daher vor unberechtigten Zugriffen durch eine Firewall geschützt werden. Da das P4-Protokoll auch über HTTP getunnelt werden kann (standardmäßig Port 50001 für die Instanz 00), ist auch dieser Port zu schützen.
- Telnet-Dienst des Java-Stacks (standardmäßig Port 50008 für die Instanz 00)
  Wird dieser kommandozeilenbasierte Zugriff nicht genutzt, so sollte der Telnet-Dienst deaktiviert werden. Kommt Telnet zum Einsatz, so dürfen nur berechtigte Administratoren auf den Dienst zugreifen. Die Telnet-Ressource (security-Dienst, Resources, root/system/telnet) ist daher so zu konfigurieren, dass als "GrantedUsers" nur die Gruppe der berechtigten Administratoren eingetragen ist.
- Dateisystem, in dem Konfigurationsdateien abgelegt werden
  Die Verzeichnisse und Dateien der Java-Stack-Installation sind mit restriktiven Zugriffsbeschränkungen auszustatten. (Hinweis: Je nach Java-Stack-Version finden sich unterschiedliche Datei-System-Layouts. Die Entwicklung geht dahin, die Konfigurationen des Java-Stacks nur noch in der Datenbank zu halten).

Der Zugriff auf die Administrationswerkzeuge (Visual Administrator, Configtool) ist auf die berechtigten Administratoren einzuschränken. Es ist jedoch zu bedenken, dass die Werkzeuge über das Netz arbeiten, so dass Angreifer eigene Programminstallationen nutzen können. Es empfiehlt sich daher, die Beschränkung auf Netzebene so zu konfigurieren, dass auf die administrativen Ports (siehe oben) nur von bestimmten Rechnern aus zugegriffen werden kann. Dies schließt zwar einen Angriff nicht vollständig aus, erschwert ihn jedoch.

**Passwortqualität sicherstellen**

Für die Benutzer des Java-Stacks sollten starke Passwörter konfiguriert werden. Die Möglichkeiten, die Passwortqualität sicherzustellen, unterscheiden sich in den einzelnen Java-Stack Versionen.

Als Mindestanforderung ist die minimale Passwortlänge auf einen Wert einzustellen, der durch die Passwortrichtlinie vorgegeben wird. Die Passwortlänge sollte mindestens 8 Zeichen betragen (Konfiguration für alle Benutzer über "Set Filter").

Auch ein maximales Alter für Passwörter sollte eingestellt werden, das den Vorgaben der Passwortrichtlinie entspricht. Dies wird über die Eigenschaften von Benutzern konfiguriert. Hier sind 90 Tage zu empfehlen.

**Java-Stack Single Sign-On sicher konfigurieren**

Damit auf den Java-Stack über Single Sign-On zugegriffen werden kann, müssen die Zertifikate der Systeme importiert werden, von denen Single Sign-On Tickets akzeptiert werden sollen. Dabei ist darauf zu achten, dass Single Sign-On Tickets nur von vertrauenswürdigen Systemen akzeptiert werden (siehe auch M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*).

Prüffragen:

- Werden die SAP Administratoren, die den Java-Stack administrieren, in der Architektur und den Sicherheitskonzepten der J2EE-Architektur geschult?
- Werden alle nicht benötigten Dienste des Java-Stack im SAP System deaktiviert?
- Wird der HTTP-Dienst im SAP System geeignet abgesichert?
- Ist für den SAP Java-Stack eine kryptographische Funktionsbibliothek installiert, die starke Verfahren anbietet?
- Ist im SAP Berechtigungskonzept festgelegt, welche Benutzer oder Gruppen auf die Systemressourcen des Java-Stacks zugreifen dürfen und welche Zugriffsoptionen (z. B. Lesen, Schreiben, Auflisten) erlaubt sind?
- Ist der Zugriff auf die Java-Stack Administrationswerkzeuge (Visual Administrator, Configtool) auf berechtigte SAP Administratoren beschränkt?
- Ist das SAP-Netz so konfiguriert, dass auf administrative Ports nur von bestimmten Rechnern aus zugegriffen werden kann?
- Stellt die Konfiguration des SAP Systems eine ausreichende Passwortqualität für Benutzer des Java-Stacks sicher?

# M 4.267 Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der SAP Java-Stack besitzt eine eigene Benutzerverwaltung, die unabhängig vom ABAP-Stack eingesetzt werden kann. Folgendes ist dabei zu beachten:

**Benutzer-Speicher konfigurieren**

Der Java-Stack verwaltet seine Benutzer in einem Benutzer-Speicher, der ab Version 6.30 konfiguriert werden kann. Zur Auswahl stehen im Wesentlichen die Java-Stack Datenbank oder die User Management Engine (UME). Wird die UME eingesetzt, kann als Benutzer-Speicher auch ein LDAP-Verzeichnis oder ein ABAP-Stack genutzt werden.

In der Regel empfiehlt es sich, als Benutzer-Speicher den ABAP-Stack über die UME zu nutzen. Auf diese Weise können die Benutzer im ABAP-Stack verwaltet werden. Der Zugriff auf den ABAP-Stack erfolgt über den JavaConnector (JCo) unter den Berechtigungen des ABAP-Stack-Benutzers SAPJSF.

Im Rahmen der Einsatz-Planung ist zu entscheiden, welcher Benutzer-Speicher zum Einsatz kommen soll.

**Notfall-Administrator anlegen**

Wie für den ABAP-Stack muss auch für den Java-Stack ein Notfall-Administrator angelegt werden. Für diesen müssen die gleichen organisatorischen Schutzmechanismen gelten wie für den Notfall-Administrator des ABAP-Stack (siehe M 4.259 *Sicherer Einsatz der ABAP-Stack Benutzerverwaltung*).

**Standardbenutzer absichern**

Die Java-Stack Standardbenutzer Administrator, System und Guest müssen wie folgt abgesichert werden:

- Es muss ein sicheres Passwort gewählt werden. Je nach Version erfolgt dies während der Installation oder muss manuell nach der Installation vergeben werden.
  Das Gast-Konto (Benutzer Guest) muss deaktiviert sein.

**Konzeption zur Benutzerverwaltung**

Im Rahmen der Planung ist ein Konzept zur Benutzerverwaltung zu erstellen, das auch den Java-Stack berücksichtigt. Dabei ist unter anderem zu bedenken, dass die Benutzer in der Regel nur über das Werkzeug Visual-Admin verwaltet werden. Standardmäßig muss dabei die Anmeldung unter Administrator-Rechten (Mitgliedschaft in der Gruppe "Administrators") erfolgen. Dies bedeutet, dass sich beispielsweise Help-Desk-Mitarbeiter unter administrativen Berechtigungen verbinden. Dies kann zwar durch Rekonfiguration der internen Berechtigungsstrukturen eingeschränkt werden, diese ist jedoch aufwendig und verhindert nicht alle administrativen Tätigkeiten.

Alternativ kann die Benutzerverwaltung auch über die Web-Schnittstelle der UME erfolgen, falls diese zum Einsatz kommt.

Der Java-Stack erlaubt es, dass sich unbekannte Benutzer selbst registrieren können. Im Rahmen der Konzeption ist zu entscheiden, ob diese Funktion

eingesetzt werden soll. Dabei ist eine sorgfältige Risikobetrachtung durchzuführen, da sich selbstregistrierte Benutzer nach der Registrierung gegenüber dem Java-Stack authentisieren können. Zwar besitzen die Benutzer dann in der Regel noch keine weiteren Berechtigungen, sind jedoch Applikationen mit Sicherheitsschwächen installiert (z. B. keine Berechtigungsprüfung beim Zugriff über bestimmte URLs), so können diese unter Umständen durch selbstregistrierte Benutzer ausgenutzt werden. Insbesondere im Internet-Einsatz ist diese Funktion kritisch zu bewerten. Um die Selbstregistrierung zu unterbinden, muss die UME Eigenschaft "ume.logon.selfreg" auf den Wert "FALSE" gesetzt werden. Die Konfiguration erfolgt über die Properties-Datei im Dateisystem oder über das Java Stack Werkzeug "Configtool". Generell muss der Einsatz der Selbstregistrierung sorgfältig geplant werden, von einer standardmäßigen Nutzung muss daher abgesehen werden. Es wird empfohlen, dass der Einsatz der Selbstregistrierung durch das Sicherheitsmanagement genehmigt werden muss.

**Zugriff auf UME Web-Schnittstelle**

Die UME Web-Schnittstelle erlaubt die Benutzerverwaltung über einen Browser. Wird diese Funktion eingesetzt, ist Folgendes zu berücksichtigen:

- Standardmäßig können Benutzer und Administratoren auf die UME Web-Schnittstelle zugreifen. Für normale Benutzer ist dann die Verwaltung des eigenen Benutzerkontos möglich (z. B. Passwortänderung). Für Benutzer der Gruppe "Administrators" ist die Verwaltung von Benutzern möglich (z. B. Benutzer anlegen).
- Auf die UME Web-Schnittstelle zur Benutzerverwaltung sollten nur berechtigte Administratoren zugreifen können. Dies kann durch entsprechende Authentisierungsanforderungen auf die Zugriffs-URL realisiert werden.
- Es sollte überlegt werden, ob die UME Web-Schnittstelle nur von Client-Rechnern berechtigter Administratoren zugreifbar sein sollte.
- Nutzen Applikationen die UME zum Speichern von benutzerbezogenen Eigenschaften (UME-Properties), so ist zu bedenken, dass diese durch die Benutzer selbst verändert werden können, wenn ihnen der Zugriff auf die UME Web-Schnittstelle gewährt wird.

Ob und unter welchen sicherheitsrelevanten Randbedingungen die UME Web-Schnittstelle eingesetzt werden soll, ist in der Planungsphase zu entscheiden.

Prüffragen:

- Ist festgelegt worden, welcher Benutzerspeicher unter SAP zum Einsatz kommt (Java-Stack Datenbank oder User Management Engine)?
- Ist das Gast-Konto (Benutzer Guest) für den Java-Stack im SAP System deaktiviert?
- Wird die UME Web-Schnittstelle sicher verwendet, falls diese eingesetzt wird?

# M 4.268 Sichere Konfiguration der SAP Java-Stack Berechtigungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Planung und Konfiguration der SAP Java-Stack Berechtigungen ist Folgendes zu berücksichtigen:

- Das SAP Java-Stack Berechtigungskonzept unterscheidet sich fundamental vom Berechtigungskonzept des ABAP-Stacks, da hier die Konzepte der Java Spezifikation J2EE umgesetzt sind.
- Für die korrekte und sichere Konfiguration sind detaillierte Kenntnisse des J2EE-Sicherheitsmodells und der -Sicherheitskonzepte notwendig. Daher sollte die Konfiguration nur durch geschulte Administratoren erfolgen.
- Die Konfiguration der Zugriffbeschränkungen auf Ressourcen und für Java Protection Domains (Code Security) erfolgt über den "security" Service.
- Zugriffsbeschränkungen auf die JNDI-Objekte (Java Objekt Registratur und Namensdienst) erfolgen über den "naming" Dienst.
- Zugriffsbeschränkungen auf Java Bean-Methoden erfolgen über den "ejb" Dienst jeweils in den Eigenschaften der einzelnen Bean-Objekte auf der Registrierkarte "Security".
- Die jeweils verfügbaren Objekte hängen von den installierten Applikationen ab.
- Die Gruppe "root", die in Versionen vor 6.40 verfügbar ist, bezeichnet nicht eine Gruppe von Administratoren, sondern alle Benutzer. Die Gruppe entspricht daher eher der vergleichbaren Windows-Gruppe "Jeder/Everyone".
- Nach der Installation müssen die voreingestellten Berechtigungen geprüft und unter Umständen entsprechend dem erstellten Berechtigungskonzept abgeändert werden.

Generell sind die Berechtigungen restriktiv zu vergeben. Im Rahmen der Berechtigungsplanung muss jeweils entschieden werden, welcher Benutzer welche Berechtigung auf welche Objekte besitzt.

Prüffragen:

- Sind die Administratoren ausreichend zur Konfiguration der SAP Java-Stack Berechtigungen geschult?
- Wurden nach der Installation des SAP Java-Stacks die voreingestellten Berechtigungen entsprechend dem Berechtigungskonzept angepasst?
- Sind die Berechtigungen des SAP Java-Stacks restriktiv vergeben?

# M 4.269 Sichere Konfiguration der SAP System Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die von einem SAP System zur Speicherung genutzte Datenbank enthält alle Informationen eines SAP Systems. Die Kommunikation zwischen SAP System und Datenbank erfolgt über SQL-Anfragen, die über das lokale Netz übertragen werden, sofern Datenbank und die SAP Systemkomponenten nicht auf demselben Rechner installiert werden. Daher muss die Datenbank möglichst gut geschützt werden. Folgendes ist zu beachten:

- Die gemeinsame Installation von SAP System und Datenbank auf einem Rechner ist allgemein nur für kleine Unternehmen und Behörden sinnvoll. Für größere Institutionen ist die getrennte Installation vorzuziehen, da der Datenbankrechner so optimal auf die Last- und Performanzanforderungen separat ausgelegt werden kann.
- Kein Datenbank-Administrator darf Zugriff auf die Tabellen des SAP Systems besitzen. Die Datenbank-Berechtigungen sind zu prüfen und entsprechend anzupassen. Es ist dabei zu berücksichtigen, dass es typischerweise immer einen Datenbank-Administrator gibt, der Vollzugriff auf alle Datenbanken in der Institution und damit Tabellen besitzt.
- Auf die Datenbank darf nur vom SAP System selbst zugegriffen werden. Dies bedeutet insbesondere:
  - Direkte Datenbankverbindungen von anderen Systemen oder Clients sind durch eine Firewall zu unterbinden.
  - Die Datenbank sollte vom SAP System exklusiv genutzt werden. Andere Applikationen dürfen hier keine eigenen Tabellen erzeugen. Insbesondere sind Datenbank-Verknüpfungen zwischen der Datenbank und den Tabellen des SAP Systems und anderen Datenbanken auszuschließen.
- Auf dem Datenbank-Rechner für das SAP System dürfen keine anderen Dienste oder Applikationen ablaufen. Ausnahmen bilden hier Werkzeuge zur Betriebssystemüberwachung. Werden diese eingesetzt, so ist sicherzustellen, dass Verbindungsversuche nur authentisiert und von bestimmten Rechnern (Administrations-Server, Administrator-Client) erfolgen.
- Das vom SAP System genutzte Datenbank-Konto ist mit einem sicheren Passwort zu versehen.
- Das verwendete Datenbank-Produkt ist sicher zu konfigurieren.
  - Nicht benötigte Funktionen und Dienste sind abzuschalten. Dies betrifft insbesondere HTTP-basierte Zugriffsschnittstellen wie Applikationsserver, die die Datenbanken zum Zugriff über eine Web-Schnittstelle anbieten. In der Regel werden hier auch administrative Möglichkeiten angeboten.
  - Standardbenutzer sind zu deaktivieren oder zu löschen, sofern diese nicht für administrative Operationen benötigt werden.
  - Alle Passwörter von Standardbenutzern sind zu ändern, auch wenn diese Konten deaktiviert wurden.

In Abhängigkeit vom Einsatzszenario können noch weitere Maßnahmen notwendig sein. Die Liste ist daher geeignet zu erweitern.

Es wird empfohlen, die Empfehlungen von SAP zur Absicherung der Datenbank umzusetzen. Details dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Sind die Datenbank-Berechtigungen so eingestellt, dass kein Datenbank-Administrator Zugriff auf die Tabellen des SAP Systems besitzt?
- Ist die Datenbank des SAP Systems durch eine Firewall vor direkten Zugriffen Dritter geschützt?
- Ist sichergestellt, dass die Datenbank exklusiv vom SAP System genutzt wird?
- Ist das vom SAP System genutzte Datenbank-Konto mit einem sicheren Zugriffsschutz versehen?
- Ist die Datenbank des SAP Systems sicher konfiguriert?

# M 4.270 SAP Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Damit die Systemfunktionen und die Systemsicherheit eines SAP Systems überwacht werden können, müssen Ereignisse protokolliert werden. Ein SAP System bietet dazu viele Möglichkeiten an. Es ist zu beachten, dass sich die vorliegende Maßnahme mit der Protokollierung im Sinne von "Monitoring des SAP Basissystems unter dem Gesichtspunkt der IT Sicherheit" beschäftigt. Betriebswirtschaftliche Prüfungen (Audits) sind nicht Gegenstand der Maßnahme.

SAP Dokumentationen mit Detailbeschreibungen zu den Systemüberwachungsfunktionen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Generell ist für die Protokollierung Folgendes zu beachten.

**Protokollierungskonzept**

Es muss ein Protokollierungskonzept erstellt werden. Das Konzept muss den ABAP- und Java-Stack berücksichtigen. Im Konzept ist festzulegen, welche Protokolldaten im SAP System gesammelt werden. Da bei der Protokollierung auch personenbezogene Daten anfallen können, sind der Datenschutzbeauftragte und der Personal- oder Betriebsrat in die Planung einzubeziehen.

**Sicherheit der Protokolldaten**

Die protokollierten Daten können wichtige Systeminformationen und personenbezogene Daten enthalten. Der Zugriff auf die Protokolldaten muss daher eingeschränkt werden. Dies kann Einstellungen sowohl innerhalb des SAP Systems als auch außerhalb des SAP Systems (z. B. auf Dateiebene) notwendig machen.

**Wichtige Systemereignisse auswerten**

Wichtige Systemereignisse werden im Systemlog protokolliert. Die Ereignisse sollten regelmäßig ausgewertet werden. Dazu kann die Transaktion SM21 genutzt werden. Es ist zu bedenken, dass über diese Transaktion auch auf Systemlogs entfernter SAP Systeme zugegriffen werden kann, sofern die Berechtigung dazu besteht. Der Zugriff auf die Transaktion SM21 ist daher auf die berechtigten Administratoren zu beschränken.

Beim Betrieb mehrerer SAP Systeme empfiehlt es sich, eine zentrale Protokollierung einzusetzen, so dass die Auswertung auf einem System erfolgen kann.

**Verwendung von Traces einschränken**

Traces erlauben es, Systemaktivitäten bei einem Zugriff genau zu protokollieren. Dabei können unter Umständen auch die verarbeiteten Daten - etwa über das Protokollieren der SQL-Anfragen an die Datenbank oder die über die ALE-Schnittstelle übergebenen Dokumente - eingesehen werden.

Für produktive Systeme dürfen Traces daher nicht genutzt werden. Fehleranalysen sollten im Test- oder Entwicklungssystem erfolgen. Müssen Traces in einem Produktivsystem eingesetzt werden, so ist dies über ein entsprechendes Ausnahmeverfahren zu regeln.

Der Zugriff auf die Trace-Transaktionen - darunter fallen die meisten Transaktionen mit dem Präfix "ST" (die Liste dieser Transaktionen mit Kurzbeschreibung kann über die Transaktion SE93 angezeigt werden) - ist daher einzuschränken (Berechtigungsobjekt S_TCODE).

**Aktivieren der Änderungsverfolgung für Tabellen**

Die Datenbank-Tabellen des SAP Systems halten alle System- und Geschäftsdaten. Im Rahmen des Protokoll- und Audit-Konzeptes ist daher festzulegen, für welche Tabellen eine Änderungsverfolgung aktiviert werden soll. In der Regel protokollieren die SAP Anwendungen alle für eine Nachvollziehbarkeit notwendigen Daten. Für die SAP Basis gilt: Customizing-Tabellen, also Tabellen, die durch den Kunden verändert werden können, werden mit aktivierter Änderungsverfolgung ausgeliefert. Dadurch können die Änderungen an den Tabellen nachvollzogen werden. Dies ist auch für Unternehmen wichtig, die dem Sarbanes Oxley Act unterliegen, da so im Rahmen von Kontrollen geprüft werden kann, welche Benutzer welche Veränderungen durchgeführt haben.

Es ist dabei zu bedenken, dass die Änderungsverfolgung nur für Tabellen aktiviert werden kann, für die der Entwickler dies vorgesehen hat. Das Aktivieren erfolgt im Data Dictionary (DDIC), wo für die betroffene Tabelle die Option "Datenänderungen protokollieren" einzustellen ist (Transaktion SE13). Zusätzlich muss die Protokollierung im Systemprofil aktiviert werden. Dazu ist der Parameter "rec/client" zu konfigurieren, über den eingestellt wird, für welche Mandanten die Änderungsverfolgung aktiviert wird (Einstellmöglichkeiten: OFF / mmm/ nnn,mmm,... / ALL).

Die Änderungsverfolgung wird für Produktiv- und Customizing-Mandanten empfohlen. Die Einstellung "ALL" ist nicht sinnvoll. Dies führt beispielsweise bei Updates zu Performanzeinbußen, da auch der Mandant 000 und mögliche Test-Mandaten betroffen sind.

Hinweise auf weitere Informationen zur Änderungsverfolgung sind in M 2.346 *Nutzung der SAP Dokumentation*.

**Zugriff auf die Monitoring-Werkzeuge einschränken**

Der Zugriff auf die durch das SAP System angebotenen Monitoring-Werkzeuge ist auf die berechtigten Administratoren einzuschränken. In der Regel kann dies über die Beschränkung des Zugriffs auf die Transaktionen und die Berechtigungseinstellungen erfolgen.

Es ist zu beachten, dass einige Monitoring-Werkzeuge auch Web-Schnittstellen zum Zugriff anbieten, wie etwa der ABAP-Stack Message-Server Monitor oder die Monitore des Java-Stacks (z. B. SQL-Trace, Systeminfo).

**Einsatz des SAP Security Audit Log**

Das SAP Security Audit Log zeichnet wichtige sicherheitsrelevante Systemereignisse auf. Der Einsatz ist daher sicherzustellen. Die Konfiguration erfolgt über die Transaktion SM19. Die Transaktion SM18 dient zum Löschen alter Log-Dateien, die Transaktionen SM20 und SM20N dienen zur Auswertung. Das Security Audit Log erlaubt so genannte dynamische Konfigurationen, deren Einstellungen zur Laufzeit verändert werden können und so genannte statische Konfigurationen, für die bei Einstellungsänderungen ein System-Neustart durchgeführt werden muss.

Für die Konfiguration der zu protokollierenden Ereignisse sollte Folgendes beachtet werden:

- Alle Ereignisse der Klasse "kritisch" sollten aktiviert werden.
- Alle Ereignisse der Klasse "schwerwiegend" sollten aktiviert werden.
- Für die Ereignisse der Klasse "unkritisch" muss entschieden werden, ob diese protokolliert werden sollen. Dabei ist zu bedenken, dass darunter auch Ereignisse sind, die sehr viele Protokolleinträge erzeugen. Ist das Security Audit Log voll, werden keine Einträge mehr protokolliert.

Der Zugriff auf die Transaktionen SM18, SM19, SM20 und SM20N sollte auf die berechtigten Administratoren eingeschränkt sein. Das Security Audit Log muss regelmäßig ausgewertet werden.

Prüffragen:

- Existiert ein Protokollierungskonzept für die SAP Protokollierung, das u. a. festlegt, welche Aktivitäten des SAP Systems und der Benutzer zu protokollieren sind?
- Ist der Zugriff auf die administrativen Funktionen und die Protokolldaten des SAP Systems eingeschränkt?
- Werden die (z. B. im Systemlog) protokollierten Systemereignisse des SAP Systems regelmäßig ausgewertet?
- Ist die Verwendung von Traces im SAP System eingeschränkt?
- Ist im Rahmen des Protokoll- und Audit-Konzeptes festgelegt, für welche Tabellen eine Änderungsverfolgung aktiviert werden soll?
- Ist der Zugriff auf die verwendeten Monitoring-Werkzeuge der SAP Systeme auf die berechtigten Administratoren eingeschränkt?
- Wird das SAP Security Audit Log eingesetzt?

# M 4.271 Virenschutz für SAP Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter Entwicklung, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Mit der Version SAP NetWeaver 04 wurde die Möglichkeit geschaffen, ein externes Anti-Viren-Programm an SAP Systeme anzuschließen. Damit ist es allen Anwendungen im ABAP- und Java-Stack möglich, die verarbeiteten Daten auf Computer-Viren scannen zu lassen. Dazu wurde die "Viren Scanner Schnittstelle" für Anti-Viren-Programme definiert, die jedoch durch die jeweiligen Programme explizit angesprochen werden muss.

Bei Eigenentwicklungen oder bei Zusatzsoftware von Drittherstellern für SAP Systeme sollte darauf geachtet werden, dass die Schnittstelle für Anti-Viren-Programme unterstützt wird. Dies gilt für den Einsatz in Szenarien, in denen Daten in ein SAP System geladen und anderen Benutzern zum Herunterladen angeboten werden. Es wird empfohlen, in die Beschaffungskriterien für Software von Drittherstellern für SAP Systeme eine Prüfung aufzunehmen, ob diese die Schnittstelle für Anti-Viren-Programm unterstützen.

Der Einsatz der Anti-Viren-Programme im SAP Umfeld ist mit dem behörden- oder unternehmensweiten Computer-Viren-Schutzkonzept abzustimmen.

Hinweise auf Dokumentationen zur Schnittstelle für Anti-Viren-Programme finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Wird bei Eigenentwicklungen oder Zusatzsoftware von Drittanbietern für SAP Systeme darauf geachtet, dass, die Schnittstelle für Anti-Viren-Programme unterstützt wird?
- Ist der Einsatz der Anti-Viren-Programme im SAP Umfeld mit dem institutionsweiten Schadsoftware-Schutzkonzept abgestimmt?

# M 4.272 Sichere Nutzung des SAP Transportsystems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Über das SAP Transportsystem (Transport Management System, TMS) erfolgt das Einspielen neuer Funktionalitäten oder veränderter Objekte in den ABAP-Stack. Da dies grundsätzlich ein Risiko darstellt, muss das Transportsystem möglichst sicher konfiguriert und benutzt werden. Folgende Aspekte sind daher für das Transportmanagementsystem zu berücksichtigen:

Generell müssen Personen, die Transporte erstellen, prüfen und durchführen, mit den Konzepten und Verfahren des SAP Transportmechanismus (Transport Organizer, Transport Management System) vertraut sein.

### Berechtigungen im Transportsystem

Über den Schutz der Transaktionen, die für das Transportsystem genutzt werden, und durch Berechtigungen ist sicherzustellen, dass nur die berechtigten Personen auf das Transportsystem zugreifen können. Unter anderem sind folgende Transaktionen betroffen: SE01, SE03, SE06, SE09, SE10, STMS*

### Transportverzeichnis schützen

Die zu transportierenden Daten werden als Dateien im Transportverzeichnis im Dateisystem abgelegt. Der Zugriff auf das Transportverzeichnis muss daher auf Betriebssystem- und Netzebene eingeschränkt werden, so dass nur berechtigte Personen und nur berechtigte entfernte Instanzen Zugriff besitzen. Es ist dabei zu beachten, dass alle Instanzen einer Transportdomäne Zugriff auf das gleiche Transportverzeichnis haben müssen.

Es ist zu bedenken, dass unberechtigte Veränderungen an den Transportdateien zu Fehlfunktionen beim Import oder auch zu weiteren Sicherheitsproblemen führen können.

### Sichere Übertragung von Transporten

Transporte werden aus dem Dateisystem in ein SAP System geladen. Dabei kann ein zentrales Transportverzeichnis, auf das über das lokale Netz zugegriffen wird, genutzt werden. Alternativ ist es auch möglich, Transportdateien über Dateitransfermechanismen (z. B. ftp, sfpt, scp) manuell oder zeitgesteuert zu übertragen.

Da Transportdateien vor unberechtigter Kenntnisnahme und Veränderungen geschützt werden müssen, sollte der eingesetzte Übertragungsmechanismus die Sicherheit der Daten beispielsweise durch Verschlüsselung gewährleisten.

Hinweise auf Dokumentationen zum Transportmanagementsystem finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Sind die zuständigen Personen mit den Konzepten und Verfahren des SAP Transportmechanismus (Transport, Organizer, Transport Management System) vertraut?
- Ist sichergestellt, dass nur die berechtigten Personen Zugriff auf das Transportsystem von SAP haben?

- Ist der Zugriff auf das Transportverzeichnis des SAP Systems eingeschränkt, auch auf Betriebssystem- und Netzebene?
- Werden Transportdateien des SAP Systems vor unberechtigter Kenntnisnahme und Veränderungen geschützt?

# M 4.273 Sichere Nutzung der SAP Java-Stack Software-Verteilung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Java-Stack nutzt ein eigenes Software-Verteilungsverfahren, das sich vom ABAP-Stack Transportsystem unterscheidet. Der so genannte Software Deployment Manager (SDM) dient dazu, neue Software in den JAVA-Stack einzuspielen. Der SDM ist Client-/Server-basiert aufgebaut, so dass Änderungen auch aus der Entfernung eingespielt werden können. Neben den allgemeinen Anforderungen (siehe M 2.221 *Änderungsmanagement*) ist Folgendes im Kontext der Software-Verteilung (Deployment) unter Sicherheitsgesichtspunkten zu bedenken:

- Es muss ein Konzept für die SAP Software-Verteilung geplant und erstellt worden sein. Das Software-Verteilungskonzept muss auf die Java-Besonderheiten abgestimmt sein, da hier im Vergleich zum ABAP-Stack unterschiedliche Verfahren und Werkzeuge eingesetzt werden müssen.
- Für den Test-, Validierungs- und Abnahmeprozess sind die Verantwortlichkeiten zu definieren.
- Durch Entwickler oder andere Personen dürfen keine Software-Verteilungen direkt aus den Entwicklungsumgebungen in Produktivsysteme erfolgen. Es ist zu bedenken, dass die SAP Entwicklungsumgebung Software direkt in den Java-Stack laden kann. Dies ist durch technische Maßnahmen (z. B. Firewall) auszuschließen.
- Der für die Software-Verteilung eingesetzte Software Deployment Manager (SDM) Dienst muss sicher betrieben werden. Ältere Versionen des SDM bieten nu eine schwache Absicherung, da nur ein Benutzer unterstützt wird und keine weiteren Berechtigungen vergeben werden können.
- Die SDM-Server-Komponente sollte nicht permanent laufen, sondern nur bei Bedarf gestartet werden.

Quellen für SAP Dokumentationen finden sich in M 2.341 *Planung des SAP Einsatzes*.

Prüffragen:

- Existiert ein auf die Java-Besonderheiten abgestimmtes Konzept für die SAP Software-Verteilung?
- Sind Verantwortlichkeiten und Prozesse etabliert, welche die Sicherheit bei der SAP Software-Verteilung gewährleisten?
- Wird technisch verhindert, dass Software-Verteilungen direkt aus der Entwicklungsumgebung in das SAP Produktivsystem erfolgen können?

# M 4.274 Sichere Grundkonfiguration von Speichersystemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Sämtliche Konfigurationsarbeiten an Speichersystemen müssen entsprechend der erstellten Sicherheitsrichtlinie (siehe M 2.525 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen*) durchgeführt werden und wie in M 2.358 *Dokumentation der Systemeinstellungen von Speichersystemen* beschrieben dokumentiert und kommentiert werden.

**Betriebssystem**

Speichersysteme, die als NAS-Systeme betrieben werden können, sind spezialisierte Server, die intern von einem Betriebssystem verwaltet werden. Dieses Betriebssystem ist üblicherweise eine eingeschränkte und leistungsgesteigerte Version eines Standard-Betriebssystems.

Auch bei SAN-Systemen, die aus einer Vielzahl von Einzelkomponenten bestehen können, werden gegebenenfalls einzelne Komponenten durch Standard-nahe Systeme verwaltet.

Vor allem bei diesen Betriebssystemen aber auch bei herstellerspezifischen "unbekannten" Systemen muss vor Inbetriebnahme sichergestellt sein, dass ein aktueller Stand aller Software- und Firmwarekomponenten hergestellt wird, um bestmögliche Stabilität des Systems und auch Schutz gegen Angriffe wie z. B. durch Schadprogramme sicherzustellen.

**Grundkonfiguration**

Bevor ein Speichersystem in die IT-Produktion integriert wird, muss eine sichere Grundkonfiguration hergestellt werden. Viele Geräte werden vom Hersteller mit einer Default-Konfiguration ausgeliefert, die vor allem auf eine schnelle Inbetriebnahme mit möglichst umfassender Funktionalität ausgerichtet ist und in der so gut wie keine Sicherheitsmechanismen aktiv sind. Daher muss die Überprüfung der Default-Einstellungen und die Grundkonfiguration offline, in einem eigens dafür eingerichteten und besonders gesicherten Testnetz oder über das Administrationsnetz, erfolgen.

Bei der Konfiguration muss beachtet werden, dass unter Umständen nicht jedes Administrations- oder Konfigurationswerkzeug (Konsole, Webschnittstelle, externes Konfigurationsprogramm) alle relevanten Informationen anzeigt.

Daher ist es wichtig, anhand der vorhandenen Dokumentation nachzuvollziehen, dass auch alle relevanten Einstellungen vorgenommen wurden. Es ist wünschenswert, wenn Konfigurationswerkzeuge alle Konfigurationsschritte am Speichergerät mindestens in lokalen Logdateien, besser noch auf einem zentralen Logging-System auswertbar dokumentieren.

Es bietet sich an, die Grundkonfiguration in folgende Schritte zu unterteilen:

- Lokale Konfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf das Gerät selbst beziehen (beispielsweise Einstellung von RAID-Levels, Zuordnung von Festplatten zu Volumes, Zuordnung von Backup-Geräten zu Speichergeräten), Einstellungen zur Protokollierung, Einstellungen für Konsolenzugang etc.

- Netzkonfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf die Einbindung des Geräts in das lokale Netz, das Administrationsnetz und das Speichernetz beziehen. Dienste zur Administration wie telnet, tftp, oder http, bei denen Anmeldung und alle Informationen im Klartext ausgetauscht werden, sollten durch die verschlüsselten Äquivalente ssh, sftp und https ersetzt werden.
- Bei SAN-Systemen muss die interne Segmentierung des Netzes durch Zoning und Port-Binding vorgenommen werden. Den angeschlossenen Servern sollten nur die tatsächlich benötigten Ressourcen des SAN zugeordnet werden.
- Die Administration der Speichersysteme sollte in die zentrale Rechteverwaltung eingebunden werden (z. B. Active Directory, LDAP, Radius,...).

**Benutzerkonten und Passwörter**

Die Möglichkeiten für die Einrichtung von Benutzern und Rollen und das Zuweisen von Berechtigungen unterscheiden sich von Hersteller zu Hersteller teilweise erheblich. Daher ist es empfehlenswert, entsprechend dem vorgegebenen Rechte- und Rollenkonzept für die Administration der Speichergeräte ein detailliertes Konzept für die jeweiligen Geräte zu erstellen.

Oft sind ein oder mehrere Administrationszugänge mit allgemein bekannten Standardnamen und Passwort oder sogar ohne Passwort vorkonfiguriert. Auf einschlägigen Internet-Seiten können Listen mit herstellerspezifischen Standard-Accounts und Passwörtern heruntergeladen werden.

Bei der Inbetriebnahme des Geräts müssen diese Standard-Benutzerkonten, falls möglich, geändert werden. In jedem Fall müssen aber die Passwörter der Standard-Accounts geändert werden. Nicht benutzte Benutzerkonten müssen deaktiviert werden.

Entsprechend dem Rechte- und Rollenkonzept müssen anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden.

Konfigurationsdateien müssen vor unbefugtem Zugriff besonders geschützt werden. Auch wenn z. B. eine verschlüsselte Speicherung von Passwörtern sichergestellt ist, müssen solche Dateien vor unberechtigtem Lesen geschützt werden, da sie geschäftskritische Informationen enthalten und auch verschlüsselte Passwörter häufig in recht kurzer Zeit durch passende Programme entschlüsselt werden könnten.

Passwortrichtlinien der Institution bezüglich Länge, Stärke und Änderungshäufigkeit sind also unbedingt zu beachten.

**Login-Banner**

Jenseits des Administrationsnetzes sollten keinesfalls Login-Nachrichten eines Speichersystems sichtbar werden. In diesen Login-Nachrichten sind oft Informationen (beispielsweise Modell- oder Versionsnummer, Software-

Release-Stand oder Patchlevel) enthalten, die einem potentiellen Angreifer von Nutzen sein können.

Sollte es sich nicht vermeiden lassen, dass auch im Intranet der Institution ein Login möglich ist, sollte die Standard-Loginnachricht durch eine angepasste Version ersetzt werden, die keine internen Informationen enthält. Die Modell- und Versionsnummer des Geräts und die Version des Betriebssystems darf unter keinen Umständen vom Login-Banner verraten werden. Stattdes-

sen sollten folgende Informationen bei einer Anmeldung am Gerät angezeigt werden:

- Jeglicher Zugriff darf nur durch autorisiertes Personal erfolgen.
- Alle Arbeiten sind entsprechend der Sicherheitsrichtlinie durchzuführen.
- Das Gerät ist in zentrale Kontrollmechanismen, wie beispielsweise in ein Netzmanagementsystem (NMS) zur Protokollierung und Erkennung von Verstößen gegen die Sicherheitsrichtlinie eingebunden.
- Verstöße gegen die Sicherheitsrichtlinie werden disziplinarisch / strafrechtlich verfolgt.

**Protokollierung**

Die interne Protokollierung auf dem Speichersystem muss so konfiguriert werden, dass vor allem Informationen, die zur Früherkennung von Problemen benötigt werden, leicht sichtbar werden.

Das Speichersystem und die zur Administration und Protokollierung genutzten Rechner sollten durch Nutzung eines NTP-Servers zeitlich synchronisiert werden.

Es ist generell ratsam, alle IT-Systeme der Institution per NTP auf eine einheitliche Zeit zu synchronisieren.

**Schnittstellen**

Nicht genutzte Schnittstellen auf Speichersystemen sind zu deaktivieren. Das bedeutet, dass nicht genutzte Anschlüsse (z. B. eine serielle Schnittstelle zum Anschluss eines Terminals) nicht verkabelt und Dienste, die nicht genutzt werden sollen, explizit deaktiviert werden sollten.

**Test der Konfiguration**

Zum Abschluss des Testbetriebes sollten Standardsysteme und auch die Absicherung des Administrationsnetzes durch einen Sicherheitscheck geprüft werden.

**Backup der Konfiguration**

Die Konfigurationsdateien der Grundkonfiguration bilden die Basis für die weitere Konfiguration. Es müssen sowohl von der mit dem Gerät ausgelieferten Default-Konfiguration als auch von den Daten, die das Ergebnis der Grundkonfiguration darstellen, Sicherungskopien hergestellt und geschützt aufbewahrt werden.

Diese bilden die Grundlage für einen Wiederanlauf nach gravierenden Störungen (siehe M 6.98 *Notfallvorsorge und Notfallreaktion für Speicherlösungen*).

Prüffragen:

- Wurden alle Konfigurationsarbeiten gem. der Sicherheitsrichtlinie für das Speichersystem ausgeführt?
- Ist anhand der vorhandenen Dokumentation nachvollziehbar ob alle relevanten Einstellungen vorgenommen werden?
- Werden bei der Inbetriebnahme von Speichersystemen nicht benötigte Benutzerkonten deaktiviert, Standard-Passwörter im Einklang mit der Passwortrichtlinie geändert bzw. neue Accounts angelegt?
- Werden die vorgegebenen Benutzerkonten- bzw. -rollen entsprechend des Rechte- und Rollenkonzepts eingerichtet?

- Ist die interne Protokollierung des Speichernetzes so konfiguriert, dass Informationen, die der Früherkennung von Problemen dienen, schnell erkannt werden?
- Sind nicht genutzte Schnittstellen des Speichersystems deaktiviert?
- Speichersystem-Hardware: Werden die Default-Konfiguration, die ermittelte Grundkonfiguration und die aktuelle Konfiguration redundant und geschützt aufbewahrt?

# M 4.275 Sicherer Betrieb einer Speicherlösung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine Speicherlösung läuft im Normalfall weitgehend autonom, ohne dass Administratoren eingreifen müssen. Zur Absicherung des Betriebs gibt es jedoch einige Maßnahmen, die ergriffen werden müssen, wenn die Funktionalität einer Speicherlösung ohne Probleme dauerhaft und ohne Unterbrechung zur Verfügung stehen soll. Realisiert wird die Überwachung des Betriebs durch ein Managementsystem (siehe M 2.359 *Überwachung und Verwaltung von Speicherlösungen*).

**Überwachung**

- Anwendungen, Systemprogramme:
  Es muss sichergestellt werden, dass Dienstprogramme störungsfrei laufen. Hierzu gehören z. B. die Antiviren-Software oder Scheduler, die automatisierte Aufgaben wie die automatische Datensicherung steuern können.
- Kapazitätskontrolle und Systemauslastung:
  Es muss sichergestellt werden, dass Kapazitätsgrenzen von Speichersystemen nicht überschritten werden und Engpässe auf Speichersystemen oder im Speichernetz so rechtzeitig erkannt werden, dass Gegenmaßnahmen getroffen werden können.
- Überwachung kritischer Ereignisse:
  Es muss überwacht werden, dass sicherheitskritische Einstellungen nicht verändert und alle Sicherheitsvorgaben eingehalten werden. Ereignisse, die gegen wesentliche Sicherheitsregeln verstoßen, müssen unübersehbar gemeldet werden.
- Reduzieren der Systemnachrichten:
  Systemnachrichten sollten so reduziert werden, dass nur wirklich wichtige Nachrichten dargestellt werden.

**Organisatorische Maßnahmen**

Im Rahmen des sicheren Betriebs ist eine Unterscheidung hinsichtlich regelmäßiger Aufgaben und anlassgesteuerter Aufgaben, wie sie beispielsweise im Zusammenhang mit Sicherheitsvorfällen, dem Einspielen von Patches oder der Änderung von Berechtigungen auftreten, vorzunehmen.

Um Änderungen und Wartungsarbeiten an einer Speicherlösung durchführen zu können, die eine Betriebsunterbrechung zur Folge haben, sind im Rahmen der Planung des Betriebs der Speicherlösung (M 2.526 *Planung des Betriebs der Speicherlösung*) Wartungsfenster zu definieren.

An einer laufenden Speicherlösung dürfen keine die Produktion beeinflussenden Wartungsarbeiten und Änderungen außerhalb eines Wartungsfensters durchgeführt werden. Alle Änderungen, ob geplant oder ungeplant, müssen über ein Änderungsmanagementverfahren mit allen beteiligten Fachverantwortlichen abgestimmt werden. Der Änderungsplan sollte zur Nachvollziehbarkeit archiviert werden.

Insbesondere Updates von Firmware oder Betriebssystem von Speichersystemen und Netzkomponenten einer Speicherlösung dürfen nur innerhalb eines Wartungsfensters durchgeführt werden.

Notwendige relevante Änderungen an der Konfiguration oder an interner Software der Speicherlösung müssen unbedingt aktuell dokumentiert werden. Diese Dokumentation muss vor allem für die Behandlung von Störungen und in Notfallsituationen eindeutig und leicht verfügbar sein.

Insbesondere nach Änderungen der Systemkonfiguration sind die Logdateien von Komponenten zur Datensicherung und Archivierung gesondert zu kontrollieren. Es sind außerplanmäßige Tests dahingehend vorzunehmen, ob Daten vom Backup wiederhergestellt werden können (siehe dazu auch M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*).

**Absicherung der Systemverwaltung**

Das Managementsystem für die Speicherlösung ist selbst so abzusichern, dass ein Zugriff unberechtigter Anwender nicht möglich ist.

Prüffragen:

- Erfolgt eine Überwachung des Betriebs der Speicherlösung hinsichtlich der Verfügbarkeit der internen Anwendungen, der Systemauslastung und kritischer Ereignisse?
- Werden Änderungen nur über das Änderungsmanagement aktiviert?
- Sind Wartungsfenster im Betrieb der Speicherlösung vorgesehen?
- Werden Wartungsarbeiten, wie Updates, nur während der dafür vorgesehenen Zeitfenster durchgeführt?

# M 4.276 Planung des Einsatzes von Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Vor der Einführung von Windows Server 2003 sind umfangreiche Planungen durchzuführen, damit eine geregelte und auch sichere Einführung sowie in Folge ein sicherer Betrieb ermöglicht wird. Dabei ist zu gewährleisten, dass die festgelegten Sicherheitsrichtlinien (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*) eingehalten werden und so eine richtlinienkonforme Umsetzung erfolgt. Hierbei ist zu beachten, dass Windows Server 2003 in der Standardinstallation ohne bereits vorinstallierte Softwarekomponenten zur Verfügung steht, um den Betrieb später nicht benötigter Komponenten zu vermeiden. In Abhängigkeit des Einsatzszenarios ist zu definieren, für welche Serverrolle Windows Server 2003 geplant wird und welche Softwarekomponenten hierfür gegebenenfalls zusätzlich installiert werden müssen.

Die im Zusammenhang mit der Einführung bzw. dem Betrieb von Active Directory stehenden Fragestellungen bzw. Planungsschritte werden hier nur ansatzweise berücksichtigt.

**Grobkonzept**

Die Planung eines Windows Server 2003 erfolgt in mehreren Schritten. Ein definierter Anforderungskatalog gemäß M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* erleichtert die Planung erheblich und ist zu empfehlen.

Die konkrete Planung kann nach dem Prinzip des Top-Down-Entwurfes erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifischen Teilkonzepten festgelegt. Im Grobkonzept werden beispielsweise folgende typische Fragestellungen behandelt:

- Wird ein neues Netz aufgebaut oder wird ein bestehendes Netz migriert?
- Soll ein existierendes Windows-Netz (z. B. basierend auf Windows 2000 Server) vollständig oder nur teilweise nach Windows Server 2003 migriert werden?
- Handelt es sich um einen zusätzlichen einzuführenden Server oder um das Upgrade eines existierenden Servers (siehe M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003*)?
- Welche Komponenten, z. B. Dateiserver, Druckserver, DNS-Server, werden ersetzt, welche bleiben erhalten?
- Müssen existierende Verfahren oder Komponenten, wie z. B. ein bestehendes Kerberos-System oder auch eine bestehende PKI, in Windows Server 2003 integriert werden? Hier sind u. a. die Interoperabilität mit anderen IT-Systemen sowie der angebotene Funktionsumfang zu berücksichtigen.
- Wird die geplante Konfiguration des Servers der zu erwartenden Datenmenge und Spitzenlast gerecht?
- Ist das Lizenzierungsmodell ausreichend und geeignet für das Bereitstellungskonzept und das Notfallkonzept?
- Ist ein Mischbetrieb von Windows Server 2003 und anderen Betriebssystemen, wie Windows 2000, Windows 95, Novell oder Unix, notwendig? Ist dies der Fall, so hat dies u. a. Einfluss auf die im System verwendeten

Authentisierungsverfahren, die abhängig von den anderen eingesetzten Betriebssystemen auch Schwachstellen aufweisen und damit die Sicherheit der Windows-Server-2003 Umgebung insgesamt herabsetzen können. Der Sicherheitsstandard in der Mischumgebung sollte in einer Sicherheitsrichtlinie festgelegt sein.

**Rollenplanung**

Im Rahmen der Erstellung von Teilkonzepten sollten die Serverrollen festgelegt werden. Das Bedienkonzept von Windows Server 2003 definiert mittels verschiedener Konfigurationsassistenten konkrete Rollen, welche zunächst als Ausgangsbasis für die Planung berücksichtigt werden sollten. Die Rollen sind in Abhängigkeit des Einsatzszenarios und der Anforderungsdefinition zu planen. In Teilkonzepten für die einzelnen Rollen müssen die spezifischen Anforderungen berücksichtigt werden, wie z. B. zu erwartende Datenmenge und Last, Kommunikationsprotokolle und -schnittstellen, Zugriffskonzept, Konfiguration der jeweiligen Betriebssystemkomponenten usw.

**Rollen (Auswahl)**

| **Serverrolle** | **Serverkonfigurations-Assistent** | **Manuelle Konfiguration** | **Sicherheitskonfigurations-Assistent** |
|---|---|---|---|
| Dateiserver | x | | x |
| Druckserver | x | | |
| Anwendungsserver | x | | x |
| Mailserver | x | | |
| Terminalserver | x | | x |
| RAS/VPN-Server | x | | x |
| Domänencontroller | x | | x |
| DNS-Server | x | | x |
| DHCP-Server | x | | x |
| Streaming Media-Server | x | | x |
| WINS-Server | x | | x |
| Web-Server | | x | x |
| Remote Installations-Server | | x | x |
| Bastion-Host | | x | |
| Zertifikatsserver | | x | x |

Der Sicherheitskonfigurations-Assistent unterstützt eine große Zahl weiterer Serverrollen von Microsoft-Produkten, z. B. die Rolle des Datenbankservers.

**Kombination von Serverrollen**

Rollen können kombiniert werden, um sowohl Beschaffungskosten als auch den Administrationsaufwand zu verringern. Kombinationsmöglichkeiten sind hauptsächlich durch folgende Aspekte beschränkt:

- Sicherheit/Schutzbedarf des IT-Systems

- designbedingte Beschränkungen von Windows Server 2003
- Skalierbarkeitsanforderungen
  Nachfolgende Möglichkeiten der Rollenverteilung sind Empfehlungen. In jedem Fall sind die geplanten Rollenkombinationen zu testen.

  - **Anwendungsserver, Zertifikatsserver, Webserver, RAS/VPN-Server:**
    Diese Rollen sollten hauptsächlich aus Gründen der Sicherheit jeweils getrennt von anderen Rollen verwendet werden.
  - **Terminalserver, Druckserver:**
    Diese Rollen sind hauptsächlich aus Design- und Skalierbarkeitsgründen von anderen Rollen zu trennen. Zum Beispiel werden auf Druckservern Treiber von anderen Herstellern installiert, die die Verfügbarkeit des Servers beeinträchtigen können.
  - **Bastion Host:**
    Ein Bastion-Host ist ein abzusichernder Computer, der direkt mit dem Internet verbunden ist. Bastion-Hosts werden in der Regel als Webserver, DNS-Server, FTP-Server, SMTP-Server und als NNTP-Server eingesetzt. Die Rolle des Bastion-Hosts eignet sich für Server im exponierten Bereich und sollte nicht mit anderen Serverrollen kombiniert werden.
- Kombinationen
  Infrastrukturdienste können gemeinsam auf einem Server betrieben werden. Kommt Active Directory zum Einsatz, empfiehlt sich die Integration von DNS auf den Domänencontrollern. Bei erhöhten Sicherheitsanforderungen in mittleren und großen Umgebungen sollte WINS nicht auf dem Domänencontroller integriert werden.
  In vielen Fällen bietet es sich an, einem Dateiserver weitere Rollen hinzuzufügen, z. B. Infrastrukturdienste. Auch die Rolle des Streaming-Media-Servers könnte von einem Dateiserver übernommen werden.

Die Verwendung von Remoteinstallationsdiensten (RIS) ist auf einem Dateiserver möglich, zum Beispiel im Rahmen von Helpdesk-Szenarien. Hierbei kann jedoch die Sicherheit des Servers durch die Remoteinstallationsdienste beeinträchtigt werden.

Die Dienste der Mailserverrolle können für bestimmte administrative oder infrastrukturelle Einsatzzwecke mit anderen Rollen kombiniert werden. Hier sollte seitens der Anforderungsdefinition klar von der Rolle des Bastion-Hosts unterschieden werden.

- **Weitere Serverapplikationen und -dienste**
  Die Internet Information Services (IIS) enthalten Basisdienste für verschiedene Serverrollen (z. B. Webserver) und stellen selbst keine eigene Serverrolle dar. Bei der Planung sollte unter Sicherheitsgesichtspunkten zwischen statischen und dynamischen IIS-Komponenten unterschieden werden.
  Weitere Serverrollen können durch Zusatzsoftware bereitgestellt werden. Die Verträglichkeit mit den Standardrollen ist im Einzelfall abzuwägen, dabei sind die bei den oben zur Kombination von Rollen beschriebenen möglichen Konflikte zu berücksichtigen. Die Planung sollte auf Basis der Ergebnisse des Software-Auswahlprozesses (siehe B 1.10 *Standardsoftware*) erfolgen.
  16-bit-Anwendungen und sonstige veraltete Software, die keine Sicherheitsmechanismen auf Anwendungsebene bieten bzw. die Mechanismen von Windows Server 2003 nicht unterstützen, stellen ein erhöhtes Sicherheitsrisiko für den Server dar. Daher sind besondere Anforderungen der Absicherung auf Daten- und Netzwerkebene bei der Planung der Windows

Server 2003 Umgebung zu berücksichtigen. Dies ist sowohl technisch als auch organisatorisch relevant.

- **Rollen in heterogenen Umgebungen**
  Heterogene Serverumgebungen mit vorhandenen Diensten und Rollen beeinflussen ebenfalls die Rollenplanung, vor allem wenn vorhandene Dienste in Windows Server 2003 überführt, konsolidiert oder wenn bestimmte Rollen parallel auf verschiedenen Plattformen realisiert werden sollen (das klassische Beispiel hierfür ist DNS). Letztlich ist die Rollenplanung auch vom Format und den Migrationsmöglichkeiten vorhandener Datenbestände und Produktionssysteme und der damit verbundenen mittel- und langfristigen Strategie abhängig.

**Überlegungen zur Konfiguration des Servers**

Die Dimensionierung der Hardware erfolgt unter den Gesichtspunkten Performance, Verfügbarkeit und Serverrolle.

Für die Performance sollten die Mindestanforderungen des Herstellers sowie der Anforderungskatalog berücksichtigt werden. Lastsimulationstools von der Microsoft-Website oder von Serverherstellern ermöglichen eine Vorhersage des Lastverhaltens von Windows Server 2003 Komponenten. Insbesondere die Maximalzahl gleichzeitiger Benutzer ist sorgfältig und prognostisch einzuschätzen. Bei hoher Benutzerzahl bzw. Nutzungsintensität ist die Zusammenfassung mehrerer Server zu einem Cluster zu erwägen.

Die geplanten Serverrollen und Serverapplikationen, die voraussichtliche Last sowie die zu erwartende Datenmenge entscheiden über weitere Parameter der Hardwarekonfiguration. Wichtige Parameter sind z. B. die Aufteilung von Festplatten-Arrays und das Partitionslayout. Die Einrichtung unabhängiger Festplatten-Arrays (RAID-Level) ist aus Performance- und Verfügbarkeitsgründen für bestimmte Serverrollen zu empfehlen, z. B. Dateiserver oder Datenbankserver. Die Software-RAID-Varianten von Windows Server 2003 ermöglichen es, kurzfristig und kostengünstig eine Datenredundanz zu konfigurieren. Sie eignen sich jedoch nicht für Performance-Steigerung und können auch einen Plattenausfall im laufenden Betrieb meist nicht kompensieren. Hardware-RAID-Level sind bei der Planung in jedem Fall zu bevorzugen.

Die Planung des Partitionslayouts sollte sich am zu erwartenden Datenaufkommen und an der logischen Trennung verschiedener Datenarten orientieren. Z. B. ist eine Partition sinnvoll, die nur das Betriebssystem und Programmdateien enthält. Nutzdaten oder temporäre Daten sollten auf separate Partitionen, die sich gegebenenfalls auf anderen Disk Arrays befinden, verteilt werden. Bei Windows Server 2003 mit Service Pack 1 oder früher sind Datenträgerkontingente nur auf Partitions- bzw. Volumeebene konfigurierbar.

**Netzanbindung**

Im Rahmen der Einsatzplanung von Windows Server 2003 ist es notwendig, in Abhängigkeit der gewählten Serverrolle eine geeignete Netzanbindung zu berücksichtigen. Die benötigten Kommunikationsprotokolle können aus der Serverrolle(n) abgeleitet werden. Hier ist zu prüfen, ob die Kommunikationsprotokolle mit dem Netzkonzept, den Sicherheitsrichtlinien für die Kommunikationsprotokolle und gegebenenfalls dem Konzept für die Sicherheitsgateways in Konflikt stehen. Der Datendurchsatz am Server kann aufgrund des zu erwartenden Zugriffsaufkommens durch Clients dimensioniert werden. Im Fall von verschlüsselten Zugriffen sind die Performanceeinbußen zu berücksichtigen. Entsprechend sollte die Leistungsfähigkeit skaliert werden, z. B. durch schnellere Prozessoren und Netzwerkadapter oder softwareseitig mit Hilfe des

Netzlastenausgleichs in einem Cluster unter Windows Server 2003. Sowohl die Kommunikationsprotokolle als auch der Datendurchsatz sind wesentliche Merkmale der Verfügbarkeit und müssen sorgfältig geplant werden.

Bei der Planung eines Servers, auf den über unsichere Netze zugegriffen werden kann oder der sich in einer besonders exponierten Lage befindet, zum Beispiel Webserver mit Anbindung zum Internet, müssen erhöhte Sicherheitsanforderungen beachtet werden. Bei der Planung für Server in exponierter Lage kann prinzipiell analog zur Planung von Servern im geschützten Bereich vorgegangen werden, jedoch ist bei allen Planungsaspekten von einer stark erhöhten Bedrohung durch Einbruchsversuche, Denial-of-Service-Attacken oder sonstigen Kompromittierungsversuchen auszugehen. Außerdem muss konzeptionell festgelegt werden, wie der oder die Server vom lokalen Netz isoliert werden und wie gegebenenfalls die Kommunikation mit dem lokalen Netz abgesichert werden kann. Als Beispiel sind Sicherheitsgateways und DMZ-Anordnung zu nennen.

Grundsätzlich nicht empfehlenswert ist der Einsatz von Mitgliedsservern einer geschützten Active-Directory-Umgebung in exponierter Lage oder DMZ. Die Sicherheitskontexte sollten entsprechend getrennt werden.

**Möglichkeiten des Zugriffs**

Bei der Einsatzplanung ist auch zu berücksichtigen, welche Zugriffswege ermöglicht werden müssen bzw. sollen (NetBIOS-Freigaben, WebDAV, DFS usw.). Hinsichtlich der Absicherung der Kommunikation sind gegebenenfalls die Maßnahmen M 4.277 *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern* und M 5.132 *Sicherer Einsatz von WebDAV unter Windows Server 2003* zu berücksichtigen. Die Notwendigkeit jedes zugelassenen Zugriffswegs ist zu begründen.

**Überlegungen zur Administration des Servers**

Im Rahmen der Planung des Einsatzes sollten folgende weiterführende Aspekte berücksichtigt werden. Eigene Teilkonzepte hierfür sind zu empfehlen, vorhandene Konzepte sollten ergänzt werden.

- Planung der Administration (M 2.364 *Planung der Administration ab Windows 2003*), dies beinhaltet auch eventuell erforderliche Zusatzsoftware für die Administration
- Überwachung (Monitoring, Protokollierung, Auswertung), siehe M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*
- Patchmanagement, Updates
- Bereitstellung (M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003*, M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003*)
- Übernahme bestehender Daten

Festlegungen zu diesen Aspekten sollten in der Sicherheitsrichtlinie für Windows Server 2003 getroffen und bei der weiteren Planung berücksichtigt werden. Vor dem produktiven Einsatz sollte die Richtlinie in verbindlicher Form vorliegen.

**Lizenzmodell**

Geeignete Lizenzmodelle sind abhängig vom Einsatz der Windows-Systeme. Für die Lizenzkontrolle wird Windows Server 2003 vom Hersteller mit Produktschlüssel und Produktaktivierung ausgeliefert. Es ist darauf zu achten, dass der betrachtete IT-Verbund ausreichend lizenziert ist und das für das einzelne Windows Server 2003 System eine aktivierbare oder aktivierungsfreie Instal-

lationsquelle und Lizenz verfügbar ist. Dies ist gegebenenfalls im Bereitstellungskonzept und im Notfallkonzept zu berücksichtigen.

Prüffragen:

- Werden bei Einsatz von Windows Server 2003 die Sicherheitsrichtlinien der Organisation berücksichtigt und umgesetzt?
- Wurden bei Windows Server 2003 die Serverrollen nach Abhängigkeit des Einsatzszenarios und der Anforderungsdefinition geplant?
- Ist bei Windows Server 2003 die Kompatibilität zwischen den Standard-Serverrollen und zusätzlichen Serverrollen sichergestellt?
- Fehlende Sicherheitsmechanismen auf Anwendungsebene: Sind die besonderen Anforderungen zur Absicherung auf Daten- und Netzwerkebene bei der Planung der Windows Server 2003 Umgebung berücksichtigt?
- Sind bei der Dimensionierung der Hardware für Windows Server 2003 die Bereiche Performance, Verfügbarkeit und Serverrollen berücksichtigt?
- Sind die eingesetzten Kommunikationsprotokolle mit dem Netzkonzept und den Sicherheitsrichtlinie abgestimmt, um Konflikten entgegenzuwirken?
- Wurden für Windows Server 2003 in exponierter Lage erhöhte Sicherheitsanforderungen definiert?
- Sind Richtlinien und Maßnahmen definiert, wie exponierte Windows Server 2003 vom lokalen Netz isoliert und abgesichert werden?
- Sind die auf den Windows Servern 2003 zur Verfügung stehenden Zugriffswege auf das erforderliche Maß reduziert und dokumentiert?
- Stehen für Windows Server 2003 die erforderlichen Mengen an Lizenzen und Installationsquellen zur Verfügung?

# M 4.277 Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows-Servern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die grundlegenden Protokolle für die netzinterne Kommunikation zwischen Windows-Servern und -Clients sind SMB, RPC und LDAP. Diese Protokolle sind eng mit der Sicherheitsarchitektur von Windows verzahnt und profitieren von den integrierten Techniken, um eine sichere Kommunikation zu gewährleisten.

Grundsätzlich muss die Verwendung der Klartextanmeldung, unter Windows Standardauthentisierung genannt, unterbunden werden. Gleiches gilt für einige andere Anmeldeverfahren mit schwacher Verschlüsselung, die mit allgemein verfügbaren Auditwerkzeugen leicht kompromittiert werden können. Die Anmeldung muss also hinreichend stark verschlüsselt sein, sowohl bei der Kommunikation innerhalb einer Windows-Umgebung als auch zwischen Windows und anderen IT-Systemen wie Samba oder Mac OS X.

Bei der Planung muss berücksichtigt werden, dass einige erforderliche Sicherheitseinstellungen für SMB, RPC und LDAP nach einer Standardinstallation nicht gesetzt sind. Hinweise zu den Einstellungen sind unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *RPC, SMB und LDAP unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*). Die Sicherheitseinstellungen sollten überprüft und gegebenenfalls angepasst werden. Diese Einstellungen gelten ebenso für Windows Server 2008. Einige der erweiterten Einstellungen sind dort, abhängig von der Rolle (AD oder Member Server), bereits als Standard gesetzt (insbesondere im Bereich Verschlüsselung und LM-Hashes), der Großteil muss aber angepasst werden.

Neben den dort genannten Einstellungen sollten für Windows Server 2003 mindestens die Standard-Sicherheitseinstellungen von Service-Pack 1 aktiv sein (siehe *Windows Default Security and Services Configuration.xls* aus dem *Microsoft Security Guide* "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*" Version 2.0 vom 27. Dezember 2005).

**Kompatibilität**

Die nach einer Standardinstallation vorzunehmenden Sicherheitseinstellungen sind mit den in G 2.114 *Uneinheitliche Windows-Server-Sicherheitseinstellungen bei SMB, RPC und LDAP* bei SMB, RPC und LDAP beschriebenen Risiken verbunden. In einem heterogenen Netz sollten diese Einstellungen erst durch das Änderungsmanagement freigegeben werden, nachdem die Verträglichkeit mit allen beteiligten Systemtypen erfolgreich in einem isolierten Testsystem erprobt wurde. Im Test sollte auch die Verfügbarkeit bei hoher Last erprobt werden. Mit Systemtypen sind hier Clients und Server unterschiedlicher Windows-Versionen und Service-Packs sowie unterschiedlicher Betriebssystem-Plattformen gemeint. Ausführliche Kompatibilitätshinweise sind im *Microsoft Knowledge Base Artikel 823659* Revision 22 vom 10. Dezember 2010 (oder einer späteren Revision) dokumentiert. Die deutsche Revision ist üblicherweise einige Revisionen älter und enthält, bedingt durch die automatische Übersetzung, oft missverständliche Formulierungen, sie sollte daher nicht als Referenz verwendet werden.

Einige grundlegende Kompatibilitätshinweise, geeignete Werkzeuge sowie Hinweise zur Vorgehensweise bei der Aktivierung sind in den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *RPC, SMB und LDAP unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

**Sicherheitsvorlage**

Die Einstellungen sind in einer Sicherheitsvorlage für diesen Server einzustellen, siehe dazu M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* und M 2.491 *Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008*.

**Dokumentation**

Eine minimale Dokumentation muss zumindest die wirksame Sicherheitsvorlage für jeden Server und deren Inhalt enthalten. Falls einzelne Einstellungen nicht flächendeckend übernommen werden, so sind die jeweiligen Bereiche abzugrenzen, zu begründen und auf alternative Sicherheitsmaßnahmen zu verweisen, zum Beispiel auf eine stärkere Isolierung des oder der Server oder die Aktivierung von IPSec (siehe M 5.90 *Einsatz von IPSec unter Windows*).

Prüffragen:

- Wird auf die Verwendung der Standardauthentisierung, sowie anderen Anmeldeverfahren mit schwacher Verschlüsselung verzichtet und stattdessen eine Anmeldung mit hinreichend starker Verschlüsslung zwingend gefordert?
- Sind auf den Windows Servern die aktuellsten Service-Packs installiert und die Standard-Sicherheitseinstellungen konfiguriert?
- Werden die vorgenommenen Sicherheitseinstellungen unter Windows Server im Vorfeld auf ihre Verträglichkeit mit allen beteiligten Systemtypen überprüft und die Verfügbarkeit unter hoher Last erprobt?
- Sind die wirksamen Sicherheitsvorlagen für jeden Server dokumentiert?

# M 4.278 Sichere Nutzung von EFS unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Das verschlüsselnde Dateisystem (Encrypting File System, EFS) von Windows Server 2003/XP ist für Benutzer ein einfach zu bedienendes Mittel zum anwendungsunabhängigen Arbeiten mit verschlüsselten Dateien. Es eignet sich am besten für einzelne Benutzer und exponierte Client-Computer, die zeitweise außerhalb der geschützten IT-Umgebung zum Einsatz kommen. Die Hauptintention ist das Herstellen von Vertraulichkeit für dedizierte lokale Daten. Grundlagen sind M 4.147 *Sichere Nutzung von EFS unter Windows* zu entnehmen.

Weniger geeignet ist EFS für die großflächige Verschlüsselung von zentralisierten Benutzerdaten auf Remote-Servern, beispielsweise Dateiservern. Dies ist nur mit spezieller Planung der Schlüsselverwaltung zu realisieren. Einen erheblichen Aufwand für die Sicherung und den Schutz großer Datenmengen und einer Vielzahl von Benutzerschlüsseln muss in Kauf genommen werden.

**Unterschiede bei der Implementierung**

Zu Beginn der Planung sollte klar unterschieden werden, ob mit EFS die Verschlüsselung von servergespeicherten Dateien im Netz angeboten werden soll oder ob es nur darum geht, Sitzungsdaten und vertrauliche administrative Daten lokal auf dem Server zu verschlüsseln. In letzterem Fall funktioniert der Server wie ein Client-Computer mit aktiviertem EFS und es sollte die Maßnahme M 4.147 *Sichere Nutzung von EFS unter Windows* umgesetzt werden. Es sollte jedoch mit der Verschlüsselung von Statusinformationen des Systems (z. B. DNS-Zonendateien, Druckerwarteschlange auf Druckservern), Protokolldateien (z. B. IIS-Protokoll) und den gemeinsamen temporären Ordnern (*C:\WINDOWS\Temp*) äußerst sparsam umgegangen werden. Hier sind Tests unter lastähnlichen Bedingungen zu empfehlen, bevor die Verschlüsselung für solche kritischen Dateien eingeschaltet wird, sonst kann durch G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS* der gesamte Server gestört werden.

Eine Möglichkeit, mit EFS die Sicherheit von administrativen Sitzungen auf dem Server zu erhöhen, stellt das Verschlüsseln von Sitzungsdaten (z. B. temporäre Verzeichnisse, Desktop-Ordner, *Eigene Dateien*, Druckerwarteschlange) und vertraulichen Arbeitsdaten wie zum Beispiel Dokumentationsunterlagen dar. Dies ist weniger kritisch, da im Zweifel nur das Profil nicht mehr funktioniert und zentrale Dienste unberührt bleiben. Anwendungen erstellen regelmäßig zur Laufzeit temporäre Kopien von Dateien. Es ist zu prüfen, welche Ordner von Anwendungen für temporäre Dateien verwendet werden. Für diese Ordner kann EFS aktiviert werden, damit diese Daten nicht während der Bearbeitung von unberechtigten Dritten eingesehen werden können.

EFS als Verschlüsselungsdienst für Remote-Dateien (servergespeicherte Dateien im Netz) sollte nur aktiviert werden, wenn ein sehr hoher Schutzbedarf hinsichtlich der Vertraulichkeit von Daten auf dem Server erforderlich ist und die zusätzlichen Risiken und der Aufwand dafür gerechtfertigt sind. Dies ist in einer Richtlinie für die IT-Umgebung festzuschreiben. Der Einsatzbereich für EFS ist genau zu definieren. Hierzu ist auch die Gefährdung G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS* zu beachten.

Wird EFS im Zusammenhang mit WebDAV-Freigaben verwendet, findet die Verschlüsselung einer Datei nicht auf dem Server, sondern auf dem Client statt. Die verschlüsselte Datei kann dann auf der WebDAV-Freigabe per HTTP-Transfer abgelegt werden. EFS braucht dazu nicht auf dem Server aktiviert zu werden. Für den Benutzer bestehen dann die gleichen Risiken wie bei der lokalen Verschlüsselung von Daten auf seinem Client. In der oben genannten Richtlinie muss festgehalten werden, in wie weit der Administrator zentrale Mittel zur Wartung, Sicherung und Wiederherstellung solcher Daten bei Schlüsselverlust bereitstellen soll. Je weitgehender dies gefordert wird, desto höher sind die Anforderungen und der Aufwand für das zentrale Schlüsselmanagement.

Die Aktivierung von EFS im Behörden- oder Unternehmensumfeld ist nur mit der gleichzeitigen Nutzung einer Public Key Infrastructure (PKI) und der Konfiguration von Wiederherstellungsagenten zu empfehlen.

**EFS deaktivieren**

Nach einer Standardinstallation von Windows Server 2003 ist EFS aktiv. Ein Wiederherstellungsagent ist nicht konfiguriert. EFS sollte für den normalen Betrieb in der Sicherheitsrichtlinie des Servers deaktiviert werden:

*Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | *Richtlinien öffentlicher Schlüssel* | Eigenschaften von *Verschlüsselndes Dateisystem* | *Benutzer dürfen das Verschlüsselnde Dateisystem verwenden* deaktivieren

In einer Active-Directory-Umgebung sollte diese Einstellung durch eine Gruppenrichtlinie für alle Server- und Clientcomputer vorgegeben werden.

Wenn EFS nachträglich auf einem laufenden System deaktiviert wird, empfiehlt es sich, das System nach noch verschlüsselten Datenbeständen zu durchsuchen. Dies kann z. B. mit dem Programm *EFSinfo.exe* aus den *Support Tools* für Windows Server 2003 durchgeführt werden.

Beispiel für Befehl an der Kommandozeile: efsinfo /s:c:\

**Rollentrennung für den DRA**

Eine geeignete Rollentrennung verhindert, dass Administratoren uneingeschränkt auf verschlüsselte Daten zugreifen können. Eine kritische Rolle spielt der Datenwiederherstellungsagent (Data Recovery Agent, DRA), mit dem Daten zentral und unabhängig von den verschlüsselnden Benutzern wiederhergestellt werden können. Datenwiederherstellungsagenten werden in Form spezieller Sicherheitszertifikate erzeugt. Folgende Bedingungen sollten für einen DRA eingehalten werden:

- Das vordefinierte Administratorkonto darf nicht mit einem DRA-Zertifikat versehen werden
- Benutzerkonten, die die Rolle eines DRA übernehmen, sollten generell keine Administratorrechte besitzen
- Es sind so wenige Datenwiederherstellungsagenten wie möglich zu erstellen
- Es ist stets ein separates Konto für den Einsatz als DRA zu verwenden

Der private Schlüssel des DRA sollte kennwortgeschützt auf einen externen Datenträger exportiert und vom System gelöscht werden. Der Datenträger mit der Sicherung des privaten Schlüssels ist in einem Bereich mit geschütztem Zugang (Tresor) zu verwahren. Zur Erhöhung der Sicherheit können die Kennwörter getrennt von den Datenträgern aufbewahrt werden.

Es sollte erwogen werden, ein Hardware-Sicherheitsmodul (HSM, siehe B 1.7 *Kryptokonzept*) einzusetzen, um die Sicherheit des privaten Schlüssels eines DRA zu erhöhen.

**Datensicherung**

Das Dienstkonto für die Datensicherung sollte keinerlei EFS- oder Wiederherstellungszertifikat besitzen und somit Daten nur verschlüsselt lesen und auf das Sicherungsmedium schreiben können.

**Abgelaufene DRA-Zertifikate**

Abgelaufene DRA-Zertifikate bleiben weiterhin sicherheitskritisch, weil sie

- Zugriff auf alle bisher verschlüsselten Daten ermöglichen (gefährdete Vertraulichkeit).
- die einzige Wiederherstellungsmöglichkeit für den bisher verschlüsselten Datenbestand auf dem Server sind (gefährdete Verfügbarkeit).

Vor Ablauf des alten DRA-Zertifikats muss ein neues hinzugefügt werden, da unmittelbar nach Ablauf die Verschlüsselung nicht mehr funktioniert. Für den neuen DRA müssen die gleichen Sicherheitsmaßnahmen umgesetzt werden (siehe oben). Dies ist bei Planung und Betrieb zu berücksichtigen.

Die Entsorgung eines alten DRA-Zertifikats ist nur ratsam, nachdem der gesamte Datenbestand entschlüsselt und mit einem neuen DRA wieder verschlüsselt wurde. Dies kann, abhängig von der Datenmenge und -organisation, einen erheblichen Aufwand und ein erhebliches Risiko für die Verfügbarkeit und Integrität der Daten mit sich bringen und sollte nur in Ausnahmefällen durchgeführt werden, z. B. wenn die Schlüsselstärke des bisherigen DRA-Zertifikats als nicht mehr ausreichend erachtet wird.

**Zentrales Schlüsselmanagement**

EFS erfordert ein definiertes zentrales Schlüsselmanagement. Der Einsatz einer Public Key Infrastructure (PKI) ist dringend empfohlen, damit nicht selbst signierte Zertifikate des lokalen Servers oder Clients benutzt werden. Weitere Informationen zu diesem Thema sind unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *Schutz der Zertifikatsdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Es ist außerdem empfehlenswert, das automatische Verlängern der EFS-Zertifikate zu erlauben, da nach deren Ablauf sonst auf selbst signierte Zertifikate zurückgegriffen wird.

Es ist notwendig, einen Wiederherstellungsagenten festzulegen, um Gefahren wie G 4.55 *Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP* vorzubeugen. Der Assistent hierfür ist unter

*Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | *Richtlinien öffentlicher Schlüssel* | *Verschlüsselndes Dateisystem* | *Menüpunkt Aktion* | *Datenwiederherstellungs-Agenten erstellen...*

aufzurufen.

Das Risiko des Verlusts der Benutzerschlüssel kann weiter verringert werden, indem die Archivierung der privaten Schlüssel auf der Zertifizierungsstelle zugelassen wird, welche die EFS-Zertifikate ausstellt. Allerdings können die Schlüssel durch die zentrale Speicherung einem erhöhten Missbrauchsrisiko ausgesetzt sein. Dadurch entsteht ein deutlich höherer organisatorischer

und administrativer Aufwand für die Zertifizierungsdienste, insbesondere für Schlüsselwiederherstellungsagenten, Rollentrennung und Schutz der Zertifizierungsstelle insgesamt.

**Wiederherstellungsstation**

In größeren IT-Verbünden sollte die Einrichtung einer Wiederherstellungsstation erwogen werden, welche in einem Bereich mit gesicherter Zugangskontrolle verwahrt und nur im Bedarfsfall aktiviert wird. Die zu entschlüsselnden Dateien können mit einem Sicherungswerkzeug wie *ntbackup* auf die Wiederherstellungsstation übertragen und dort mit dem Schlüssel des DRA wiederhergestellt werden. Der DRA-Schlüssel kann auf der Wiederherstellungsstation verbleiben. Ein weiterer Vorteil der Verwendung einer Wiederherstellungsstation ist, dass der Schlüssel auf der Wiederherstellungsstation nicht durch nicht vertrauenswürdige Software gefährdet werden kann.

Für die Wiederherstellungsstation kann Virtualisierungstechnologie eingesetzt werden. Das heißt, das gesamte Betriebssystem wird in einer simulierten Hardware-Umgebung installiert. Diese virtuelle Umgebung kann leicht auf einem Wechseldatenträger gespeichert und sicher verwahrt werden.

**Schulung**

Zur Funktion und den Risiken von EFS muss der Benutzer geschult werden. Mit geschulten Benutzern und einem Schlüsselmanagement kann durch die Nutzung von EFS ein Sicherheitsgewinn erzielt werden.

Prüffragen:

- Sind die Mittel zur Wartung, Sicherung und Wiederherstellung von EFS-Daten für die Administratoren bei Schlüsselverlust definiert?
- Ist sichergestellt, dass das vordefinierte Administratorkonto nicht mit einem DRA-Zertifikat versehen ist?
- Ist sichergestellt, dass die Benutzerkonten, die die Rolle eines DRA übernehmen generell keine Administratorrechte besitzen?
- Sind die Anzahl der Datenwiederherstellungsagenten auf das erforderliche Minimum begrenzt?
- Wird für den Einsatz von DRA stets ein separates Konto verwendet?
- Werden bei Ablauf alter DRA-Zertifikate rechtzeitig neue DRA-Zertifikate erstellt?
- Sind die Benutzer im Umgang mit EFS und den damit entstehenden Risiken geschult?
- Werden abgelaufene DRA-Zertifikate sicher aufbewahrt?

# M 4.279 Erweiterte Sicherheitsaspekte für Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für IT-Verbünde mit erhöhtem Schutzbedarf, in denen Windows Server 2003 eingesetzt wird, sind zusätzliche Maßnahmen zur Erreichung eines solchen Schutzniveaus erforderlich. Damit ist nicht nur die Erhöhung der Verfügbarkeit des Systems insgesamt gemeint (Redundanz, Hochverfügbarkeitscluster), sondern auch gezielte Maßnahmen zum erhöhten Schutz der Vertraulichkeit und Integrität von Anwendungen, Daten und Datenverkehr im Netz. Die Maßnahmen können unter Umständen eine Einschränkung von Funktionalität oder Interoperabilität bedeuten. Deshalb sollte auf jeden Fall eine Testumgebung zur Verfügung stehen, um die gewünschte Funktionalität sicherzustellen.

Die nachfolgend erläuterten Aspekte sind bereichsübergreifend und keinesfalls erschöpfend. Je nach Rolle des Servers, Einsatzszenario und entsprechender Gefährdungslage sind weitere Vorkehrungen zu treffen. In den spezifischen Maßnahmen für Windows Server 2003 werden dazu weitere Anhaltspunkte genannt.

**Produktaktivierung**

Die Online-Produktaktivierung benötigt eine aktive Internetverbindung und das HTTP-Protokoll. Während der Installationsphase sollte diese Verbindung nur über ein Sicherheits-Gateway mit Proxyserver realisiert werden, d. h. die Option *AutoActivate* darf ausschließlich gemeinsam mit der Option *ActivateProxy* verwendet werden. Dazu muss die Antwortdatei manuell editiert werden. Die Aktivierung kann auch später skriptgesteuert (z. B. im Post-Installationsskript) oder manuell ausgelöst werden.

Bei hohem Schutzbedarf des Servers kann auf die telefonische Aktivierung ausgewichen werden.

**Verschlüsselung**

Durch *IPSec* können alle IP-basierten Kommunikationsverbindungen von und zu einem Client abgesichert werden. Dabei ist es möglich, die Endpunkte der Kommunikation zu authentisieren und die Datenpakete signiert und verschlüsselt zu übertragen, so dass die Integrität und Vertraulichkeit der Daten bei erhöhten Anforderungen an die Sicherheit gewährleistet werden kann. Das Teilkonzept für eine IPSec-Infrastruktur sollte den erhöhten Administrationsaufwand berücksichtigen und setzt eine Verträglichkeitsprüfung mit den beteiligten Systemen in einer Testumgebung voraus.

Falls Verschlüsselung gemäß den Richtlinien FIPS (Federal Information Processing Standard) der US-amerikanischen Behörde NIST (National Institute of Standards and Technology) für das *SSL/TLS-Protokoll* und für das *Encrypting File System* (EFS) benötigt wird, kann dies unter

Konsole *Lokale Sicherheitsrichtlinie* | *Lokale Richtlinien Sicherheitsoptionen* | *Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden*

eingestellt werden. Die Aktivierung bedeutet sichere Verschlüsselung (z. B. 3DES), aber nicht unbedingt immer höchstmögliche Schlüssellänge. Beispielsweise wird AES (beim EFS) nicht berücksichtigt.

Generell darf der erhöhte Rechenaufwand und der mögliche Einfluss auf das Lastverhalten des Servers nicht vernachlässigt werden.

Weiterhin sollte *Systemkryptografie: Starken Schlüsselschutz für auf dem Computer gespeicherte Benutzerschlüssel erzwingen* mindestens auf *Benutzer wird zur Eingabe aufgefordert, wenn der Schlüssel zum ersten mal verwendet wird* setzen. Dadurch wird bei Zugriff auf den privaten Schlüssel eines Sicherheitszertifikats die Kennworteingabe erzwungen.

**Hochverfügbarkeit**

Bei hohen Verfügbarkeitsanforderungen kann es erforderlich sein, nicht nur Teile der Serverhardware, sondern den gesamten Server redundant auszulegen und in einem Hochverfügbarkeits-Cluster zusammenzufassen. Windows Server 2003 Enterprise Edition unterstützt mittels des *Clusterdienstes* acht Knoten in einem Cluster, die je nach Anforderung für Hochverfügbarkeit und Lastverteilung optimiert werden können. Jeder der redundanten Server sollte einheitlichen Hardwareanforderungen gerecht werden. Die Planung des Clusters muss bei der Rollenplanung berücksichtigt werden, da bestimmte Dienste nur eingeschränkt clusterfähig sind.

Der *Netzwerklastenausgleich* wird nicht nur von der Enterprise Edition, sondern auch von der Web Edition und der Standard Edition unterstützt.

**Denial-of-Service**

Um sich gegen DoS-Attacken abzusichern, sollten die TCP/IP-Einstellungen des Servers (siehe Hilfsmittel zum IT-Grundschutz, *Absichern von IP-Protokollen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) überprüft und gegebenenfalls gesetzt werden. Zum Setzen der Registrierungsschlüssel wird die Verwendung von administrativen Vorlagen empfohlen (siehe M 2.368 *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*). Diese Vorkehrungen sollten auf jeden Fall ausgeführt werden, wenn der Server in einer exponierten Umgebung eingesetzt wird, z. B. als Sicherheits-Gateway oder in einer Demilitarized Zone (DMZ). Innerhalb einer geschützten IT-Umgebung sind sie optional.

Der Einsatz als Webserver oder als sogenannter *Bastion Host* (öffentlich erreichbarer Computer des Unternehmensnetzes) erfordert weitere spezifische Schutzmaßnahmen, die z. B. im Baustein B 5.10 *Internet Information Server* beschrieben sind.

**Plug and Play**

Ein weiteres Gefahrenpotential stellt die automatische Hardware-Erkennung (*Plug and Play*) dar, falls der Server nicht hinreichend vor unbefugtem Zugang geschützt ist. Im Normalfall genügt es, alle nicht benötigten Anschlüsse zu deaktivieren (z. B. im *BIOS* und im Windows-*Gerätemanager*). Laufwerke für Wechseldatenträger sollten entfernt oder verschlossen werden oder durch Software-Werkzeuge von Drittherstellern kontrolliert werden. Windows Server 2003 stellt entsprechende Funktionalitäten nur sehr eingeschränkt zu Verfügung.

Die vollständige Umgehung von *Plug and Play* ist in Windows Server 2003 nicht vorgesehen und beeinträchtigt die Systemstabilität. Der Testaufwand und das Risiko sind nur bei besonders hohen Sicherheitsanforderungen gerechtfertigt.

**Ressourcenberechtigungen**

Die standardmäßigen Ressourcenberechtigungen in den Systemordnern und an Systemobjekten sind restriktiv, sollten aber bei sehr hohem Schutzbedarf gehärtet werden. Hierzu werden die Berechtigungen für bestimmte Standardgruppen entzogen und explizit an bestimmte Benutzerkonten vergeben.

Die Einstellung in der Konsole *Lokale Sicherheitsrichtlinie* | *Lokale Richtlinien Sicherheitsoptionen* | *Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden* steht standardmäßig auf *Administratorgruppe*. Besitzer haben immer besondere Berechtigungen auf ihr Objekt. Außerdem kann die Überwachung von Gruppen als Besitzer von Objekten nicht optimal gelöst werden. Die Einstellung *Administratorengruppe* sollte durch *Objektersteller* ersetzt werden. Dies verschlechtert jedoch die Administrierbarkeit des Servers erheblich.

Prüffragen:

- Bei Produktaktivierung: Erfolgt diese online ausschließlich über ein Sicherheits-Gateway mit Proxy-Server oder wird im Bedarfsfall auf eine telefonische Aktivierung ausgewichen?
- Bei Einsatz verschlüsselter IP-basierter Kommunikationsverbindungen: Sind der erhöhte administrative und technische Aufwand mit der Sicherheitsrichtlinie der Organisation abgestimmt und dokumentiert?
- Sind nicht benötigte Hardware-Anschlüsse und Laufwerke für Wechseldatenträger vom Windows Server 2003 entfernt oder verschlossen worden?

# M 4.280 Sichere Basiskonfiguration ab Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die sichere Basiskonfiguration muss während der Bereitstellung des Servers, bei Änderungen der Serverkonfiguration und bei Änderungen von Vorgaben und Richtlinien durchgeführt werden. Außerdem empfiehlt es sich, die Durchsetzung der Einstellungen turnusmäßig zu überprüfen, um Fehleinstellungen durch alltägliche Administrationsarbeiten oder sonstige Einflüsse zu vermeiden.

Die notwendigen Einstellungen sind zu identifizieren, zum Beispiel in Form einer Checkliste. In der Liste sollten die bei der Grundschutzmodellierung gefundenen Maßnahmen berücksichtigt werden.

**Standard-Sicherheitseinstellungen und Sicherheitsvorlagen**

Für die gefundenen Einstellungen sollten nach Möglichkeit Sicherheitsvorlagen und administrative Vorlagen (siehe M 2.368 *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*) erstellt werden. Dadurch wird der Grad an Standardisierung und Automatisierung der Basiskonfiguration erhöht. Außerdem können die Einstellungen später leichter überprüft und revisioniert werden. Die Basiskonfiguration kann mit relativ wenig Aufwand dokumentiert werden, indem die Vorlagen exportiert und der Dokumentation beigefügt werden. Darauf aufbauend kann ein Freigabeprozess für die Basiskonfiguration im IT-Änderungsmanagement (siehe M 2.221 *Änderungsmanagement*) etabliert werden.

Die genannten Aspekte setzen voraus, dass die Standardeinstellungen von Windows Server 2003 und Server 2008 nicht willkürlich verändert wurden. Standard-Gruppenmitgliedschaften sollten belassen, Basisrechte für systeminterne Konten (z. B. NT-Autorität) sollten nicht verändert werden. Standardberechtigungen in Subkomponenten wie WMI und den Komponentendiensten sollten erhalten bleiben. Abweichungen sollten in Form von Checklisten und Vorlagen geplant, begründet und durchgeführt werden, insbesondere wenn die Abweichung eine Verschlechterung des Sicherheitsstandards bewirken könnte. Als Referenz für Standardeinstellungen dienen die mitgelieferten Sicherheitsvorlagen, hauptsächlich *defltsv.inf* (für Server) und *defltdc.inf* (für Domänencontroller) im Ordner *C:\WINDOWS\inf*. In der Vorlage *setup security.inf* (Ordner *C:\WINDOWS\security\templates*) sind alle Einstellungen nach Abschluss des Setup-Programms festgehalten. Unter Windows Server 2008 sind nur noch die Sicherheitsvorlagen

- *Defltbase.inf*
- *Defltsv.inf* (Für Server)
- *Defltdc.inf* (Für Domänencontoller)

verfügbar. Diese Vorlagen werden ausschließlich im Verzeichnis *%systemroot%\inf* der Windows Installation gespeichert.

Weitere Informationen sind in M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* zu finden.

Für die Konfiguration von Windows Server 2008 sollte als zentrales Verwaltungstool *Microsoft Security Compliance Manager* eingesetzt werden, um Vorlagedateien zu steuern und zu bearbeiten (Siehe Maßnahmen M 2.491 *Nut-*

*zung von Rollen und Sicherheitsvorlagen unter Windows Server 2008* und M 4.416 *Einsatz von Windows Server Core*).

Weitere Referenzen sind die Konfigurationsvorlagen des Sicherheitskonfigurations-Assistenten (ab Windows Server 2003 Service-Pack 1), die Tabelle Windows Default Security and Services Configuration.xls (aus der Herstellerdokumentation "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP" Version 2.0 ), die Maßnahmen des IT-Grundschutzes sowie sonstige Dokumentationsunterlagen des Herstellers.

Ab Windows Server 2008 sind die Einstellungen des Dokuments *Windows Server 2008 Security Baseline Settings* zu beachten. Diese Tabelle ist Teil des *Security Compliance Management Toolkit.*

In den weiteren Abschnitten dieser Maßnahme werden einige Einstellungen und Vorgaben aufgezählt. Sie sind nicht in anderen Maßnahmen für Windows Server 2003 oder Windows Server 2008 enthalten, beeinflussen aber die Sicherheit der Basiskonfiguration. Sie sollten beim Erstellen der Checkliste ebenfalls berücksichtigt werden.

**Wichtige sicherheitsrelevante Funktionen**

Festplattenpartitionen sollten bei der ersten Formatierung ausschließlich mit NTFS formatiert werden. Das Setup-Programm von Windows Server 2003 und Windows Server 2008 nimmt während der Installation unter Umständen eine Konvertierung der Systempartition vor. Auf einem produktiven System sollte das nachträgliche Konvertieren von FAT32-Partitionen jedoch vermieden und gleich NTFS gewählt werden.

Aus der Auslagerungsdatei des Arbeitsspeichers können unverschlüsselte Daten extrahiert werden. Die Auslagerungsdatei sollte bei jedem Herunterfahren automatisch gelöscht werden:

*Start | Systemsteuerung | Verwaltung | Konsole Lokale Sicherheitsrichtlinie öffnen | auswählen des Knotens Lokale Richtlinien | Sicherheitsoptionen | Herunterfahren: Auslagerungsdatei des Virtuellen Arbeitsspeichers löschen*

Weitere Gefahrenpotentiale stellen die automatische Hardware-Erkennung (Plug and Play) sowie Autorun-Funktionen (Automatisches Starten von Programmen) dar, falls der Server nicht hinreichend vor unbefugtem Zugang geschützt ist. Alle nicht benötigten Anschlüsse sollten deaktiviert werden (z. B. im BIOS und im Windows-Gerätemanager). Es ist auch zu überlegen, ob Laufwerke für Wechseldatenträger entfernt oder physikalisch verschlossen werden. Alternativ kann die Verwendung von Wechselmedien durch Software-Werkzeuge von Drittherstellern kontrolliert werden. Windows bietet hierfür bis einschließlich Windows Server 2003 keine eigenen ausreichenden Mittel. Erst mit der Einführung von Windows Server 2008 können über Gruppenrichtlinienobjekte Wechseldatenträger zumindest teilweise konfiguriert werden (siehe M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen*).

Der sichere Betrieb von mehreren Servern setzt eine synchrone Systemzeit voraus. Sie sollte mit der Zeit der anderen IT-Systeme im Informationsverbund synchronisiert sein. Hierfür kann der im System vorhandene Client für das Network Time Protocol (NTP) genutzt werden.

Besitzer haben immer besondere Berechtigungen auf ihre Objekte. Erstellt ein administrativer Benutzer ein Objekt, ist standardmäßig die lokale Sicherheitsgruppe "Administratoren" der Besitzer. Für Gruppen als Besitzer von Objekten

kann die Überwachung nicht optimal gelöst werden. Datenträgerkontingente werden ebenfalls anhand des Dateibesitzes diskreter Benutzer gesteuert. Durch Gruppen als Besitzer von Dateien kommen irreführende Kontingenteinträge und Screeningergebnisse (ab Windows Server 2003 R2) zustande.

Diese Problematik sollte in erster Linie durch geeignete Konzepte gelöst werden, welche sich mit den Bereichen Überwachungseinstellungen, Berechtigungen (z. B. Berechtigungskonzept) und Datenträgerkontingente (z. B. Teilkonzept für einen Dateiserver) befassen.

Wenn keine Kompatibilität zu Windows NT 4.0, Windows ME/98 oder früher benötigt wird, sollte überlegt werden, die anonyme Aufzählung von Freigaben zu deaktivieren:

*Start* | *Systemsteuerung* | *Verwaltung* | *Konsole Lokale Sicherheitsrichtlinie öffnen* | *auswählen des Knotens Lokale Richtlinien* | *Sicherheitsoptionen* | *Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben* setzen auf *Aktiviert*

**Weitere Sicherheitskomponenten**

Auf unveränderten Windows-Server-Installationsdatenträgern befindet sich eine eingeschränkte Kommandozeilenumgebung (Wiederherstellungskonsole), die auf dem Server alternativ zum Betriebssystem gestartet werden kann. Damit kann die Konfiguration des installierten Windows-Betriebssystems manipuliert werden. Für die Authentisierung wird das Kennwort des in der Windows-Server-Installation standardmäßig vordefinierten Administratorkontos abgefragt. Dies funktioniert unabhängig davon, ob das Konto umbenannt oder deaktiviert wurde. Die Wiederherstellungskonsole kann auch direkt auf die Festplatte installiert werden und verhält sich wie ein zusätzlich installiertes Betriebssystem. In beiden Fällen stellt dies eine Möglichkeit für den potenziellen Missbrauch des Bootvorgangs dar. Die Installation der Wiederherstellungskonsole sollte daher nicht willkürlich erfolgen, sondern in einer Richtlinie geregelt werden. Die Sicherheitseinstellungen nach einer Standardinstallation (*Start* | *Systemsteuerung* | *Verwaltung* | *Konsole Lokale Sicherheitsrichtlinie öffnen* | *auswählen des Knotens Lokale Richtlinien* | *Sicherheitsoptionen* |*Wiederherstellungskonsole)* sollten beibehalten werden.

Nach einer Standardinstallation ist die verstärkte Sicherheitskonfiguration für Internet Explorer aktiv (*Systemsteuerung* | *Software* | *Windows-Komponenten*). Diese Komponente sollte nur deaktiviert werden, falls eine Internet-Explorer-basierte Applikation (eines Drittherstellers), die auf dem Server benötigt wird, nicht damit kompatibel ist.

Die Windows-Firewall wird ab Windows Server 2003 mit Service-Pack 1 beim Boot-Vorgang gemeinsam mit dem TCP/IP-Protokoll geladen und aktiviert, wodurch das TCP/IP-Protokoll bereits während des Bootvorgangs besser geschützt wird. Der Dienst Windows-Firewall/Gemeinsame Nutzung der Internetverbindung muss dafür auf die Startart "Automatisch" gesetzt sein. Es gilt zu beachten, dass die Firewall auf einem Windows Server 2008 im Gegensatz zu Windows Server 2003 den Datenverkehr in beide Flussrichtungen, also auch ausgehend filtert. Dies ist für die eventuell notwendige Kommunikation von Applikationen zu berücksichtigen.

Nach dem Bootvorgang ist die Firewallfunktionalität (nicht der Dienst selbst) standardmäßig wieder inaktiv. Bei Sicherheitsvorfällen im lokalen Netz (sich ausbreitende Schadprogramme oder Angriffe von innen) ist der Server unge-

schützt. Daher sollte überlegt werden, die Aktivierung der Windows-Firewall bei einer sicheren Basiskonfiguration zu berücksichtigen.

Hierzu können gezielt die typischen Dienste und Funktionen in der lokalen Gruppenrichtlinie (*Start* | *Ausführen...* | *gpedit.msc*) freigeschaltet werden (*Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Netzwerkverbindungen* | *Windows Firewall*) oder die Konfiguration mittels des mit Windows 2003 eingeführten *Security Configuration Wizard* (SCW) durchgeführt werden. Die Windows-Firewall unterstützt RPC-Dienste, welche über die vordefinierten Konten Lokales System, Lokaler Dienst und Netzwerkdienst laufen, beispielsweise für die Remote-Administration. Zusatzsoftware mit RPC-Diensten muss vorher getestet werden.

**Nicht benötigte Funktionen abschalten**

Auf einem Windows-Server-System sind häufig Basis- und Hilfsfunktionen aktiv, die nicht in jedem Fall benötigt werden. Es gilt das Prinzip: Funktionen so weit wie möglich deaktivieren, um die Angriffsfläche und unnötige Risiken zu minimieren. Möglicherweise sinkt dadurch die Flexibilität von Windows Server 2003 und der Administrationsaufwand steigt. Aus Sicherheitsgründen sollten deaktivierte Funktionen trotzdem nur mit entsprechender Begründung und Dokumentation wieder aktiviert werden.

Es sollte genau überlegt werden, welche Funktionen für den konkreten Einsatz eines Windows Servers 2003 oder Windows Server 2008 benötigt werden, um nur diese zu aktivieren. Hinweise zu nicht benötigten Funktionen sind auch in der Herstellerdokumentation "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP" Version 2.0 vom 27. Dezember 2005 oder später und in der erwähnten Excel-Datei Windows Default Security and Services Configuration.xls zu finden.

Hinweis: Durch zu restriktives Abschalten von Diensten kann das System in einen nicht lauffähigen Zustand geraten. Zum Erhalt der Verfügbarkeit des Systems ist ein entsprechender Testaufwand zu betreiben.

**Dokumentation**

Die Dokumentation der Basiskonfiguration sollte den Anforderungen des Änderungsmanagements entsprechen. Sie sollte alle verwendeten Vorlagen mit Versionsnummer und Beschreibung enthalten. Für jeden Server sollte ersichtlich sein, welche Vorlagen bei ihm wirken.

Prüffragen:

- Gibt es eine Checkliste oder ein anderes Dokument, worin alle notwendigen Einstellungen dokumentiert sind?
- Gibt es, falls nötig, für alle notwendigen Einstellungen Sicherheitsvorlagen und administrative Vorlagen?
- Sind die Standardeinstellungen zu Gruppenmitgliedschaften, für systeminterne Konten und für Berechtigungen unverändert?
- Ist die Systemzeit mit der Zeit der anderen IT-Systeme im Informationsverbund synchronisiert?
- Gibt es ein Konzept, welches verhindert, dass keine Gruppen die Besitzer von Objekten sind?
- Gibt es eine Richtlinie zur Wiederherstellungskonsole?
- Sind alle nicht benötigten Funktionen abgeschaltet?
- Gibt es eine Dokumentation für das Änderungsmanagement?

- Wird zur Bearbeitung von Sicherheitsvorlagen der Microsoft Security Compliance Manager eingesetzt?

# M 4.281 Sichere Installation und Bereitstellung von Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Bereitstellung umfasst die Schritte nach Planung und Beschaffung des Servers oder einer Gruppe von Servern bis zur Aufnahme des produktiven Betriebs. Besonders kritisch ist die Installation des Betriebssystems. Während dieser Phase greifen die Schutzmechanismen von Windows Server 2003 nicht. Viele Vorgaben aus Sicherheitsrichtlinien können erst auf einem installierten Server durchgesetzt werden. Andererseits werden wichtige Parameter für den späteren Betrieb schon durch die Installation festgelegt. Daher muss ein Installationskonzept gemäß M 2.318 *Sichere Installation eines IT-Systems* erstellt werden, das dem spezifischen Verhalten von Windows Server 2003 Rechnung trägt. Bei einer Gruppe von Servern oder bei wiederkehrenden Installationen gewinnt die Automatisierung und Standardisierung von Installationen an Bedeutung, außerdem haben die vorhandene IT-Umgebung und eventuell vorhandene Software-Management-Systeme Einfluss auf die Installation und Bereitstellung. Solche Betrachtungen sprengen oft den Rahmen eines Installationskonzepts für den einzelnen Server. Daher ist die Erstellung eines umfassenderen, wiederverwendbaren Bereitstellungskonzepts zu empfehlen, welches die bestehenden Installationskonzepte berücksichtigt. Die Konzepte für Installation und Bereitstellung sollten so angelegt sein, dass dem Administrator eine konkrete Handlungsanweisung für seinen jeweiligen Installationsauftrag zur Verfügung steht.

Neben der manuellen Installation von einem unveränderten Windows-Server-2003-Datenträger sind zwei grundlegende Bereitstellungsvarianten zu unterscheiden: Festplattenabbild (Image) und Installation von einer Installationsquelle mittels Setup-Programm. Mit beiden Varianten ist eine Automatisierung und Standardisierung auf unterschiedliche Art und Weise möglich.

In der Abbildung werden für die weiteren Betrachtungen diese Bereitstellungsvarianten exemplarisch als zwei mögliche Pfade zugrunde gelegt:

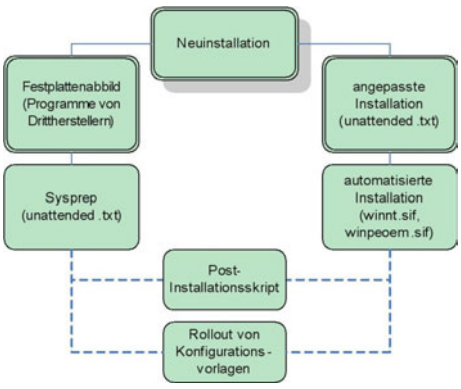



Abbildung: Bereitstellungspfade

Aus der Abbildung können die grundlegenden Mittel für die Bereitstellung und die Reihenfolge abgeleitet werden, in welcher die Mittel vorbereitet werden. Das Szenario kann variiert und durch Zusatz-Software ergänzt werden. Der

Administrator sollte zumindest in der Anwendung der hier gezeigten Mittel geschult sein, da sie fast allen Verfahren zugrunde liegen.

**Für das Installationskonzept zu berücksichtigende Aspekte**

Im Installationskonzept für den einzelnen Server müssen eine Reihe von Faktoren berücksichtigt werden:

- Bootvorgang und Initiierung der Installation
- Treiber für Massenspeichergeräte und gegebenenfalls Netzwerktreiber müssen beim Bootvorgang zur Verfügung gestellt werden
- Art der Installationsquelle (Datenträger, Netzwerk)
- Service Packs in die Installationsquelle integrieren (sog. *slipstreamed*)
- Bereitstellung des Produktschlüssels
- Hardware-Treiber zur Verfügung stellen
- Einspielen von Produktaktualisierungen (Patches)
- gegebenenfalls Domänenbeitritt
- Serverrollen konfigurieren
- sicherheitsrelevanten Einstellungen vornehmen, gemäß Sicherheitsrichtlinien
- Produktaktivierung von Windows Server 2003

Für ein Bereitstellungskonzept werden diese und weitere Aspekte systemübergreifend betrachtet. Eine Orientierungshilfe findet sich unter den Hilfsmitteln zum IT-Grundschutz (siehe *Bereitstellungskonzept von Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Die gängigen Produkte für Softwaremanagement und -verteilung integrieren und automatisieren einige Basismechanismen von Windows Server 2003, z. B. Antwortdateien oder Treiberbereitstellung. Nachfolgend werden daher einige allgemeingültige Sicherheitsaspekte erläutert.

**Sicherheitsaspekte**

Ein Festplattenabbild wird von einem vollständig installierten lauffähigen Server gezogen und auf einen anderen Server gespiegelt. Ein Manko dieses Verfahrens ist die identische Sicherheitskennung (SID) von gespiegelten Systemen. Für Authentisierungsvorgänge in einer Windows-Umgebung sind eindeutige SIDs zwingend erforderlich. Das Verfahren zur nachträglichen Änderung der SID (*Sysprep* oder Programme von Drittanbietern) greift tief in das System ein und berührt sämtliche sicherheitskritischen Objekte. Außerdem ist ein Festplattenabbild unflexibel gegenüber Änderungen der Hard- und Softwarekonfiguration. Gespiegelte Systeme müssen aktiviert werden, daher sind Mehrfach- oder Volumenlizenzprogramme zu empfehlen. In geeigneten Testverfahren sollte der zuverlässige Betrieb der gespiegelten Systeme nachgewiesen werden.

Abbilder ermöglichen einen hohen Grad an Standardisierung sowie Schutz vor Installationsproblemen. Sie können leicht verwaltet und archiviert werden. Softwaremanagementprogramme können bei der Aufspielung von Festplattenabbildern gewisse Systemparameter anpassen, weitere Anpassung erfolgen durch *Sysprep* (mit Antwortdatei) und Post-Installationsskripte. Die Vorteile dieses Konzeptes kommen bei einer großen Anzahl von Abbildern mit jeweils geringem Anpassungsbedarf zum Tragen.

Automatisierte angepasste Installationen basieren auf einer Antwortdatei für den Installationsvorgang. Sie bieten hohe Flexibilität und Modularität für Hard- und Softwarekonfiguration und sind mit geringem Aufwand anzupassen. Der Installationsverlauf ist anfälliger für Fehler oder Kompromittierungsversuche,

allerdings wird für jede Installation ein individuelles Protokoll generiert. Für vollständige Automation sind Lizenzprogramme mit einheitlichem Produktschlüssel zu empfehlen.

Am Ende der Installation sollten die Installationsprotokolle gesichert werden. Dies sind *setuplog.txt* und alle Dateien mit der Erweiterung *.log*, im Systemstammverzeichnis (meist *C:\WINDOWS*), sowie alle *.log*-Dateien in *C:\WINDOWS\security\logs*. Die Datei *setuperr.log* muss immer ausgewertet werden.

Antwortdateien (*unattended.txt*, *winnt.sif, winpeoem.sif, ini*-Dateien usw.) enthalten kritische Konfigurationsinformationen, die von unbefugten Personen für Einbruchsversuche missbraucht werden können. Installationsmedien oder Installationsquellen mit angepassten Antwortdateien sollten daher immer vor unbefugtem Zugriff geschützt aufbewahrt bzw. mit eingeschränkten Berechtigungen versehen werden. Zum Erstellen der Antwortdateien dient der Setup Manager (Datei *SetupMgr.exe* auf der Installations-CD bzw. CD1 bei Windows Server 2003 R2 in *\SUPPORT\TOOLS\DEPLOY.CAB*). Der Zugriff sollte auf Administratoren beschränkt werden sowie einer Versionskontrolle unterliegen.

Besonders wichtig ist Planung der Installationskonten, die während der Bereitstellungsphase verwendet werden sollen. Diese sind ähnlich kritisch wie administrative Konten und sollten entsprechend überwacht werden. Sie sollten mit minimalen Berechtigungen versehen werden, die Möglichkeiten der Anmeldung sollten eingeschränkt sein.

Das Laden von Produktaktualisierungen schon während des Installationsprozesses erhöht die Sicherheit. Dennoch sollten die Aktualisierungen nicht direkt aus dem Internet (*Windows Update*) geladen werden. Vorzugsweise sollte *Dynamic Update* verwendet werden, welches auf eine lokale Quelle zugreift und die individuelle und bewusste Freigabe von Aktualisierungen ermöglicht. Dazu muss die Option *DUShare* manuell in die Antwortdatei eingetragen werden. *DUShare* verweist auf einen Ordner der Installationsquelle, der Update-Pakete in Form von *.cab*-Dateien enthält.

Alternativ zu diesem Verfahren können Produktaktualisierungen nach der Installation mit Hilfe von *Windows Update* und Post-Installationsskripten von einem lokalen Update-Server eingespielt werden. Eines der beiden beschriebenen Verfahren sollte im Bereitstellungskonzept definiert werden.

Hinweis: Die Herstellerdokumentation zum Thema Antwortdateien ist in den Dateien *ref.chm* und *deploy.chm* auf der Installations-CD bzw. CD1 bei Windows Server 2003 R2 in *\SUPPORT\TOOLS\DEPLOY.CAB* zu finden.

Ab Windows Server 2003 mit Service Pack 1 ist während und nach der Installation die lokale Firewall solange aktiv und restriktiv eingestellt, bis der Aktualisierungsprozess einmal durchlaufen wurde. Erst danach ist die volle Konnektivität gegeben. Dieser Modus schützt den Server, wenn Produktaktivierung und -aktualisierung direkt über das Internet vorgenommen werden. Für geringen Schutzbedarf genügt dieses Szenario, jedoch ersetzt es nicht ein isoliertes Installationsnetz.

**Konformität mit Sicherheitsrichtlinien**

Die Konformität mit den aktuellen Sicherheitsrichtlinien bei Aufnahme des produktiven Betriebs muss durch den Bereitstellungsvorgang gewährleistet werden. Sicherheitsvorlagen werden meist durch Gruppenrichtlinien und Active Directory auf den Server übertragen und aktiviert. Alternativ oder zusätzlich können die Vorlagen mit Hilfe von Post-Installationsskripten eingespielt wer-

den. Die fertige Installation muss mit den aktuellen Vorlagen und den sonstigen aktuellen Sicherheitsvorgaben getestet werden. Das Durchsetzen der Vorlagen und Einstellungen sollte Teil des Installations- bzw. Bereitstellungskonzeptes sein.

**Dokumentation**

Das Bereitstellungskonzept ist ausführlich und verständlich zu dokumentieren. Es sollte für jeden Server eine aktuelle Installationsanweisung geben.

Prüffragen:

- Bei einer hohen Anzahl von Windows Server 2003 Systemen: Existiert zusätzlich zum Installationskonzept ein umfassenderes, wiederverwendbares Bereitstellungskonzept?
- Werden die Installationsprotokolle der Windows Server 2003 gesichert und die erzeugten Fehlermeldungen ausgewertet?
- Betrifft die skriptgesteuerte Installation von Windows Server 2003 Systemen: Ist in dem Bereitstellungskonzept die Installation per Image beziehungsweise per Antwortdatei berücksichtigt?
- Erfolgt die Installation neuer Systeme über gesonderte Konten und sind diese mit den minimal erforderlichen Berechtigungen versehen.
- Ist in dem Bereitsstellungskonzept das Einspielen von Patches und Updates auf dem neu erstellten Windows Server 2003 System definiert?
- Betrifft die skriptgesteuerte Installation von Windows Server 2003 Systemen: Ist sichergestellt, dass die Antwortdateien keine Klartextkennwörter aus der Produktivumgebung beinhalten?

# M 4.282 Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Internet Information Services (IIS) 6.0 sind eine wichtige Komponente von Windows Server 2003, ohne die viele wichtige Funktionen des Betriebssystems nicht oder nur eingeschränkt zur Verfügung stehen. Die IIS wurden seit Version 5 um neue Technologien erweitert, modularisiert und größtenteils aus dem Betriebssystemkern ausgegliedert. Dieses neue Systemdesign macht die IIS robuster und das Betriebssystem weniger anfällig. Die IIS sind in Windows Server 2003 im Kontext eines Anwendungsservers für Web-basierte Anwendungen integriert. Dementsprechend heißt die Komponente in Windows Server 2003 *Anwendungsserver*. Die IIS sind eine Teilkomponente des Anwendungsservers. Die Komponente *Anwendungsserver* ist nach einer Standardinstallation des Betriebssystems vollständig deaktiviert.

Die im Folgenden beschriebenen Empfehlungen gehen nicht näher auf die sichere Installation eines Anwendungsservers oder Intranet/Internet-Servers (siehe hierzu B 5.10 *Internet Information Server*) ein. Sie sollten stattdessen immer dann angewendet werden, wenn eine andere Windows Server 2003 Komponente oder eine zusätzliche Applikation die Installation der IIS als Hilfsdienst anfordert. Diese Maßnahme weist auf die einzelnen Punkte hin, die bei einer sicheren Konfiguration der IIS-Basis-Komponente beachtet werden müssen. Konkrete Einstellungen zu den hier aufgeführten Hinweisen sind unter den Hilfsmitteln zum IT-Grundschutz (siehe *Absichern der IIS-Basis-Komponente unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*)zu finden.

### Welche Komponenten können installiert werden?

Auf dem Server sollten nur der *COM+-Netzwerkzugriff* sowie die *Internetinformationsdienste* (IIS) aktiviert sein. Für letztere ist die Aktivierung auf *Gemeinsame Dateien*, *Informationsdienste-Manager* und *WWW-Dienst* einzuschränken; optional darf lediglich noch *Internetdrucken* verwendet werden.

### Weitere IIS-Dienste neben dem HTTP-Server

Unter *Anwendungsserver* sind die verbreiteten Protokolle SMTP, NNTP und FTP sowie der Message-Queuing-Dienst aufgelistet. Einige Werkzeuge und Serveranwendungen fordern deren Installation an. Mit diesen Protokollen und Diensten sind weitere Gefährdungen verbunden, so dass neben den hier genannten Empfehlungen noch weitere Maßnahmen gemäß den Ergebnissen der Modellierung nach IT-Grundschutz umzusetzen sind (siehe auch M 5.131 *Absicherung von IP-Protokollen unter Windows Server 2003*).

Auf einem Domänencontroller für Active Directory sollten nur die notwendigen IIS-Dienste und -Protokolle installiert sein.

### Absichern der Basiskonfiguration

Die Installationsroutine der IIS legt im Stammverzeichnis des Systemlaufwerks die Verzeichnisse *C:\Inetpub* und *C:\Inetpub\wwwroot* an. Beide Ordner sollten umbenannt werden. Die Sicherheitsgruppe *Benutzer* ist aus den Sicherheitseinstellungen von *C:\Inetpub\wwwroot* und allen darunter liegenden Ord-

nern zu entfernen. Der Ordner *AdminScripts* sollte in ein benutzerdefiniertes Verzeichnis verschoben werden. Generell ist auf alle Beispiel- und Testskripte auf dem produktiven Server zu verzichten, egal ob sie aus eigener Feder, aus dem Internet oder aus Softwareentwicklungspaketen stammen.

Dieselben Vorkehrungen gelten auch für folgende Ordner, sofern diese vorhanden sind:

- *C:\inetpub\ftproot* (FTP-Server)
- *C:\inetpub\mailroot* (SMTP-Server)
- *C:\inetpub\nntpfile* (NNTP-Server)

Alle virtuellen Standardserver, die Standardwebsite und die Standard-FTP-Site sind zu beenden, wenn sie nicht benötigt werden. Es ist zu empfehlen, die Standardwebsite grundsätzlich deaktiviert zu lassen und neue Websites nur für klar definierte Einsatzzwecke hinzuzufügen, z. B. für WebDAV-Freigaben.

Viele virtuelle Verzeichnisse im Internetinformationsdienste-Manager verweisen auf Funktionen des Betriebssystems, beispielsweise Internetdrucken oder Zertifikatsdienste. Die Basisverzeichnisse sind daher meist Systemordnern des Betriebssystems zugeordnet. Daher sollte generell die Sicherheitsgruppe *Benutzer* aus den Sicherheitseinstellungen der jeweiligen Basisverzeichnisse entfernt werden. Wenn bestimmte Ressourcen auch für Benutzer zur Verfügung stehen sollen, z. B. Internetdrucken oder das IIS-basierte Ändern des Benutzerkennworts, so ist ein entsprechendes Berechtigungskonzept zu planen und umzusetzen. Allgemeines zu Berechtigungen in Webservern wird in M 4.360 *Sichere Konfiguration eines Webservers* beschrieben.

**Umgang mit dynamischen Inhalten**

Die Zertifizierungsdienste und andere Windows-Komponenten enthalten z. T. grafische Benutzeroberflächen, die mit ASP laufen. Es ist daher nicht immer möglich, ASP zu deaktivieren. In Windows Server 2003 sind die Einflussmöglichkeiten von ASP auf das Betriebssystem standardmäßig stark eingeschränkt (aktiviertes *IISLockdown*). Unter kontrollierten Bedingungen ist daher ohne größeren Aufwand ein sicherer Betrieb dieser Komponenten möglich. Dies bedeutet vor allem, dass ASP ausschließlich für administrative und infrastrukturelle Zwecke aktiviert wird. Zudem existieren ein geeignetes Administrationskonzept und eine entsprechende Sicherheitsrichtlinie. Der Zugriff auf Benutzerebene wird eingeschränkt, protokolliert und kontrolliert. Ansonsten ergeben sich weitere Risiken, für die entsprechende Maßnahmen umgesetzt werden müssen (siehe B 5.10 *Internet Information Server*). Zum ausführen von dynamische Inhalte startet IIS eigenständige Prozesse. Mehrere Anwendungen sollten durch ein geeignete Prozessmanagement isoliert voneinander betrieben werden.

**Zugriff einschränken und absichern**

Der Zugriff auf die virtuellen Server und Verzeichnisse ist standardmäßig nicht eingeschränkt, obwohl die IIS-Dienste nur vom lokalen Computer oder von bestimmten Clients im Netz abgefragt werden. Außerdem wird die Klartextübermittlung von Kennwörtern nicht verhindert. Daher sollten restriktivere Einstellungen als Grundeinstellung vorgegeben werden.

**Authentisierungsmethoden**

Im LAN stellt die *Integrierte Windows-Authentifizierung* die sicherste und komfortabelste Methode dar. Sie funktioniert mit den meisten gängigen Browsern, z. B. Internet Explorer und Firefox. Ist ein Teil des LAN durch einen Sicher-

heits-Gateway abgeschirmt, so muss die Unterstützung für die *Integrierte Windows-Authentifizierung* überprüft werden.

Sofern die Sicherheitsrichtlinie es zulässt und Gefährdungen (siehe G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*) ausreichend berücksichtigt werden, kann in bestimmten Bereichen auf *Digest-Authentifizierung* (verschlüsseltes Senden der Anmeldeinformationen nach RFC 2617 unter Verwendung von Domänencontrollern) ausgewichen werden. Ist dies nicht möglich, muss die gesamte Verbindung über einen verschlüsselten Kanal aufgebaut werden (siehe unten).

Voraussetzungen für *Digest-Authentifizierung* sind

- Active Directory mit der Windows-Server-2003-Schemaerweiterung
- Windows Server 2003 auf allen Domänencontrollern der lokalen Active-Directory-Site
- HTTP-1.1-Unterstützung auf Clients (z. B. MS Internet Explorer ab Version 5)
- HTTP-1.1-Unterstützung auf Sicherheits-Gateways

In Windows Server 2003 wurde Digest als Security Service Provider Interface (SSPI) integriert (*erweiterte Digest-Authentifizierung*). Voraussetzung ist, dass sowohl IIS als auch Domänencontroller unter Windows Server 2003 laufen. Auf dem Server mit IIS muss das SSPI für Digest mit Hilfe eines Skriptes erzwungen werden, da Windows Server 2003 auf das ältere Digest-Modul von Windows 2000 zurückschaltet oder die Authentisierung ganz fehlschlägt, sobald die Konfiguration der Windows-Domäne nicht homogen ist.

Der Aufruf auf der Kommandozeile lautet:

*cscript adsutil.vbs SET W3SVC/UseDigestSSP wahr*

Das Konfigurationsskript *adsutil.vbs* befindet sich im Verzeichnis *AdminScripts*. Informationen zum Verwenden von Skripten sind in M 2.367 *Einsatz von Kommandos und Skripten ab Windows Server 2003* zu finden.

**Verschlüsselung in einem sicherem Kanal (SSL/TLS)**

Der sichere Kanal ist oft der einzige Weg, um bei Administrationswerkzeugen von Drittherstellern eine verschlüsselte Kennwortübertragung zu erreichen.

Jede Webseite, nachfolgend virtueller Server genannt, muss mit einem gültigen Zertifikat ausgestattet sein und die verschlüsselte Kommunikation über einen sicheren Kanal ermöglichen.

Für Server mit hohem oder sehr hohem Schutzbedarf kann die Anforderung von Clientzertifikaten aktiviert werden. Mit Hilfe weiterer Systeme wie z. B. Chipkarten besteht damit die Möglichkeit, eine zwei-Faktor-Authentisierung zu realisieren.

**Überwachung**

Auf allen virtuellen Servern und Webseiten muss im Eigenschaften-Dialogfenster die Protokollierung aktiviert werden. Die Standardeinstellung von einer Protokolldatei pro Tag sollte belassen werden, sofern die Sicherheitsrichtlinie für den Server keine längerfristigen Protokolle vorschreibt. Ab Windows Server 2003 mit Service Pack 1 sollte zudem die Metabase-Überwachung eingestellt werden. Dazu dient das Konfigurationsskript *iiscnfg.vbs*.

Der Kommandozeilenaufruf

*iiscnfg.vbs /enableaudit W3SVC/<Bezeichner>/ROOT*

aktiviert die Überwachung auf der Webseite-Konfiguration und den untergeordneten virtuellen Verzeichnissen. Der *<Bezeichner>* ist die Nummer des virtuellen Servers. Diese ist im Internetinformationsdienste-Manager unter dem Knoten *Websites* neben den aufgelisteten Websites dokumentiert. Schließlich muss die Gruppenrichtlinie für die Objektüberwachung auf dem Server aktiviert bzw. wirksam sein (siehe auch M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*).

**Dokumentation**

Es sollte mindestens dokumentiert werden, welcher Server Zugriffspunkt für welches administrative Werkzeug ist, welche Authentisierungsmethoden dafür eingestellt sind und auf welche weiteren Ressourcen das Werkzeug gegebenenfalls Zugriff benötigt. Abweichungen von den genannten Grundeinstellungen bzw. vom Installationsstandard sollten dokumentiert und begründet werden.

Prüffragen:

- Sind auf allen Windows Servern nur die notwendigen IIS-Dienste und -Protokolle installiert?
- Wurde die Basiskonfiguration der der IIS-Basis-Komponente unter Windows Server 2003 abgesichert und der Zugriff auf die virtuellen Server und Verzeichnisse eingeschränkt?
- Wurde die Protokollierung unter Windows Server 2003 auf allen virtuellen Servern und Webseiten aktiviert?
- Ist die Konfiguration der IIS-Basis-Komponente unter Windows Server 2003 dokumentiert?

# M 4.283 Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Aktualisierung einer Vorgängerversion auf Windows Server 2003 hat meist verschiedene Gründe und verfolgt mehrere Ziele. Die Ausgangspositionen sind dabei organisatorisch und technisch sehr vielfältig. Deshalb ist die umfassende und sorgfältige Planung einer Serveraktualisierung unter Berücksichtigung der zu erreichenden Ziele unerlässlich. Die Forderungen in M 2.315 *Planung des Servereinsatzes* und M 2.319 *Migration eines Servers* sind zu beachten. Für die Migration eines Windows NT-Servers gelten grundsätzlich auch die Festlegungen aus M 2.233 *Planung der Migration von Windows NT auf Windows 2000*.

### Vor- und Nachteile verschiedener Migrationspfade

Bei der Entscheidung für einen Migrationspfad sind besonders die Vor- und Nachteile der Aktualisierung eines bestehenden Servers (In-place Upgrade) gegen die einer Neuinstallation sorgfältig abzuwägen. So weicht unter Umständen ein aktualisierter Server auf Grund übernommener "Altlasten" oder alter Konzepte erheblich von den Sicherheitsstandards eines neu installierten Windows Server 2003 Systems ab. Maßgeblich ist auch die Ausgangsversion des aktualisierten Servers. Die Standardsicherheitseinstellungen eines aktualisierten Windows Server 2003 entsprechen nicht den Standardeinstellungen der Neuinstallation. Die Einstellungen werden vom Setup-Programm je nach Ausgangsversion und Service Pack unterschiedlich gesetzt. Wird also Windows NT 4.0 Server auf Windows Server 2003 aktualisiert, dann unterscheiden sich die resultierenden Einstellungen von denen eines von Windows 2000 Server aus aktualisierten Windows-Server-2003-Systems.

Für die Durchsetzung einer homogenen Sicherheitsrichtlinie müssen abhängig von der Ausgangssituation (Version, Rolle, Konfiguration) die Sicherheitskonfigurationen angepasst werden.

Die Aktualisierung eines bestehenden Servers erfordert im Allgemeinen weniger Aufwand, da die vorhandenen Benutzer, Gruppen und Rechte beibehalten werden. Dateien und Anwendungen müssen nicht neu installiert werden.

Eine Neuinstallation mit frisch formatierten Festplatten ist hingegen leistungsfähiger. Die Datenträgerpartitionen können den aktuellen Bedürfnissen angepasst werden. Für Server, bei denen die Verfügbarkeitsanforderungen sehr hoch sind, ist eine Neuinstallation zu empfehlen. Anderenfalls sollte nach vorheriger Datensicherung auf jeden Fall eine komplette Defragmentierung der Partitionen erfolgen.

### Vorbereitungen

Die Herstellerinformationen, insbesondere die mitgelieferten Dokumentationen auf den Installationsmedien (z. B. Verzeichnis *\DOC* auf dem Windows Server 2003 Installationsmedium) sind zu beachten. Vor einer Aktualisierung muss geprüft werden, ob die Voraussetzungen dafür erfüllt sind. Dazu gehört die Upgrade-Fähigkeit der unterschiedlichen Versionen der Betriebssysteme. Die Systemanforderungen und Hardwarekompatibilität sind beim Her-

steller nachzulesen oder mittels *Setup* vom Windows Server 2003 Installationsmedium mit *Systemkompatibilität prüfen* zu kontrollieren. Neben diesen empfohlenen Herstelleranforderungen sind die produktiv benötigten Kapazitäten (Festplatte, Arbeitsspeicher usw.) zu berücksichtigen. Informationen über die vorhandenen Geräte und Treiber helfen unter Umständen bei erforderlichen manuellen Eingriffen. Es wird empfohlen, ein Inventarverzeichnis für den Server anzulegen, in dem Angaben zu dessen Komponenten (wie Bezeichnung, Typ, Anzahl, IRQ, E/A-Adresse, etc.) dokumentiert sind. Sofern Treiber für diese Komponenten vom Hersteller angeboten werden, sollten diese vorab beschafft werden.

Der Einsatz von Windows Server 2003 erfordert gegebenenfalls den Einsatz neuer Treiber, die möglicherweise nur mit neueren BIOS-Versionen lauffähig sind, wodurch ein Update des BIOS notwendig wird. Dies sollte jedoch erst geschehen, nachdem recherchiert wurde, welche Treiberversionen welche BIOS-Stände benötigen.

Befinden sich auf dem zu aktualisierenden Server

- Cluster,
- Volumensätze,
- Spiegelsätze,
- Stripesets oder
- FAT/FAT32-Partitionen

bedürfen diese der besonderen Berücksichtigung, wobei die Nutzung von FAT grundsätzlich nicht zu empfehlen ist.

Software, welche auf dem aktualisierten Server weiter betrieben werden soll, ist vorab auf ihre Kompatibilität zu testen. Dazu gehören u.a. Virenschutzprogramme, Backup- und Managementsysteme sowie Verschlüsselungsanwendungen.

Die Namen, Namensdienste und Netzwerkeinstellungen der zu migrierenden Server sind so zu wählen, dass in allen Phasen keine Konflikte oder zusätzliche Gefährdungen auftreten.

Hinweise hierzu finden sich unter den Hilfsmitteln zum IT-Grundschutz (siehe *DNS/WINS/DHCP als Infrastrukturdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Ein produktiver Windows Server 2003 sollte (abgesehen von der Wiederherstellungskonsole) grundsätzlich nur eine Betriebssysteminstallation beherbergen und ausschließlich NTFS-Partitionen besitzen.

Es sollte überlegt werden, aus den Erkenntnissen und Anforderungen der Planungsphase eine Prüfliste zu erstellen, welche in einer Testmigration und vor allem nach der durchgeführten Migration dem dokumentierten Funktionsnachweis dient.

**Durchführung**

Nach dem erfolgreichen Abschluss aller Tests sollte die Migration eines produktiven Servers mit dem Geschäftsbetrieb abgestimmt werden. Zum angekündigten Termin ist der Server für den Installationsvorgang aus dem Produktivbetrieb zu entfernen. Für eine aktuelle vollständige Datensicherung ist zu sorgen.

Für die Installation darf nur Software aus sicheren Quellen verwendet werden (M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Upda-*

*tes*). Aktuelle Servicepacks, Sicherheitspatches und Treiber müssen zur Verfügung stehen. Deren Bereitstellung auf geeigneten Wechselmedien wie CD oder DVD ist am sichersten und auch später nachvollziehbar.

Während der Installation ist ein aktiver Netzwerkanschluss am Server notwendig. Der serielle Anschluss einer evtl. vorhandenen unterbrechungsfreien Stromversorgung ist wegen möglicher Komplikationen bei der Schnittstellenerkennung vorsorglich zu trennen.

Die Option eines *dynamischen Updates* über das Internet sowie eine unbeaufsichtigte Aktualisierung sind zu vermeiden, denn beim Aktualisieren von produktiv genutzten Servern sind meist Besonderheiten zu berücksichtigen, die individuelle Entscheidungen und Eingriffe erfordern. Internetverbindungen während einer Serverinstallation erfordern zusätzliche Sicherheitsmaßnahmen und schaffen vermeidbare Gefährdungen. Außerdem kann ihre Verfügbarkeit nicht garantiert werden.

**Hilfsmittel**

Die Servermigration auf neue Hardware wird durch Werkzeuge von Microsoft unterstützt. Vor dem Einsatz von diesen Tools und Werkzeugen ist mit dem Hersteller die Unterstützung bei Problemen zu klären Sie sind besonders sorgfältig auszuwählen und vor ihrer Anwendung zu testen. Es können ebenso Werkzeuge von Drittanbietern einbezogen werden.

- Das *File Server Migration Toolkit* (FSMT) dient zur Migration und Konsolidierung der Daten älterer Dateiserver. Neben den Daten werden mit *FSMT* auch die Berechtigungen auf NTFS- und Freigabe-Ebene übertragen.
- Der *Microsoft Print Migrator* überträgt Druckertreiber und deren Konfiguration jedoch ohne Sicherheitsberechtigungen.
- Für die Migration und Konsolidierung von Domänen steht das *Active Directory Migration Tool* (ADMT) zur Verfügung.
- Für die Migration eines Betriebssystems und der installierten Anwendungen eines physischen Servers in eine virtuelle Maschine unter MS Virtual Server 2005 kann das Tool *Virtual Server Migration Toolkit* (VSMT) genutzt werden.

**Nacharbeiten**

Nach Abschluss wesentlicher Arbeitsschritte, z. B. nach einem Neustart des Windows Server 2003, sind die Ereignisanzeigen auf kritische Fehler und Hinweise zu prüfen.

Abhängig von der Produktversion und den Lizenzbedingungen ist gegebenenfalls eine Produktaktivierung erforderlich. Hinweise hierzu finden sich unter den Hilfsmitteln zum IT-Grundschutz (siehe *Auswahl geeigneter Lizenzierungsmethoden für Windows XP/Server 2003* in *Hilfsmittel zum Windows Server 2003*).

**Sicherheitskonfiguration**

Die Sicherheitskonfiguration unter Windows Server 2003 wird mit verschiedenen Werkzeugen durchgeführt, deren Konfigurationsbereiche sich teilweise überschneiden. Es können eigene Richtlinien und Vorlagen definiert werden.

- Nach einer Aktualisierung ist mit Hilfe des *Sicherheitskonfigurations-Assistenten* (SCW) eine vorbereitete Sicherheitskonfiguration auf den Server anzuwenden. Die Rolle des betroffenen Servers muss zu diesem Zeitpunkt definiert sein.

- Mit der *Microsoft Management Console* (MMC) werden mittels *Sicherheitskonfiguration und -Analyse* bzw. *Sicherheitsvorlagen* Vorlagen für Sicherheitseinstellungen erstellt und gegebenenfalls angewendet. Die Anwendung dieser Vorlagen ist auch über Gruppenrichtlinien möglich. Im *Sicherheitshandbuch für Windows Server 2003* (online beim Hersteller verfügbar) stehen empfohlene Sicherheitsvorlagen, Beschreibungen und Dokumentationsvorlagen zur Verfügung. Diese Vorschläge müssen jedoch in jedem Fall an die spezifischen Anforderungen angepasst werden. Hilfestellung hierzu bieten die Maßnahmen M 4.280 *Sichere Basiskonfiguration ab Windows Server 2003* und M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*.

Nach jeder Sicherheitskonfiguration sind die Ereignisanzeigen zu kontrollieren.

Unter Windows Server 2003 ist der Internet-Explorer standardmäßig auf erhöhte Sicherheit eingestellt. Die daraus resultierenden Einschränkungen können durch Übernahme von Internetadressen in die Zone *vertrauenswürdige Sites* bzw. der UNC-Pfade in die Zone *Lokales Intranet* aufgehoben werden. Der Benutzer muss dafür die erforderlichen Berechtigungen für die Konfiguration des Internet-Explorers besitzen.

Unter Windows Server 2003 wurden zusätzliche lokale Gruppen und Benutzer, z. B. *Remotedesktopbenutzer*, *Netzwerkkonfigurations-Operatoren*, *Support_388945a0* (deaktiviert), eingerichtet, welche beachtet und berücksichtigt werden müssen.

Der Verzeichnispfad für Benutzerprofile hat sich gegenüber Windows NT 4.0 verändert. Vorhandene Skripte und Verfahren sind gegebenenfalls diesbezüglich anzupassen.

Prüffragen:

- Ist der Migrationspfad auf Windows Server 2003 Systeme mit den Sicherheitsrichtlinien der Organisation abgestimmt und dokumentiert?
- Wurde die Upgrade-Fähigkeit auf Windows Server 2003 im Vorfeld überprüft (Treiber, Erfüllung der Hardware-Anforderungen der Hersteller etc.) und in einer Prüfliste dokumentiert?
- Erfolgt nach Installation von Windows Server 2003 eine Sicherheitskonfiguration zur Systemhärtung?

# M 4.284 Umgang mit Diensten ab Windows Server 2003

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Dienste werden unter Windows unter dem Sicherheitskontext bestimmter Konten ausgeführt (sogenannte Dienstkonten). Zugriffe auf Ressourcen erfolgen mittels des Dienstkontos, ähnlich wie bei einem Benutzer mit Benutzerkonto. Einmal gestartet bleiben Dienste prinzipiell aktiv, also bleibt auch das zugehörige Dienstkonto dauerhaft angemeldet oder die Anmeldung wird regelmäßig durch die zentrale Dienstesteuerung erneuert. Auf Servern handelt es sich meist um betriebskritische zentrale Dienste. Dienstkonten sind daher exponierter als normale Benutzerkonten. Sofern Abhängigkeiten zwischen Diensten existieren, kann auch ein kompromittierter, scheinbar weniger wichtiger Dienst einen betriebskritischen Dienst zum Absturz bringen. Aus diesen Gründen sollten Dienste und Dienstkonten unter Beachtung spezieller Regeln administriert werden.

- Für Dienstkonten sollte niemals das vordefinierte Administratorkonto verwendet werden.
- Jeder Dienst sollte mit einem eigenen Dienstkonto laufen.

Ein kompromittiertes Dienstkonto mit hohem Berechtigungsniveau kann leichter isoliert werden, wenn es nicht für mehrere Dienste verwendet wird. In der Praxis betreiben Serverapplikationen möglicherweise eine Gruppe von Diensten im Kontext desselben Kontos. Hier muss im Einzelfall abgewogen werden, ob dies mit dem Schutzbedarf des Systems vereinbar ist und inwieweit unterschiedliche Dienstkonten zugewiesen werden können, ohne die gewünschte Funktionalität zu beeinträchtigen.

Eine Ausnahme bilden die speziellen, vordefinierten Konten NT AUTHORITY\LocalService und NT AUTHORITY\NetworkService. Sie werden von der internen Dienstesteuerung verwaltet und stellen jedem Dienst einen isolierten Sicherheitskontext zur Verfügung. Die Authentisierung wird systemintern durch die Dienstesteuerung geregelt. Kennworteintragungen werden ignoriert.

- Jedes Dienstkonto sollte nur mit den minimal erforderlichen Berechtigungen ausgestattet sein.

Deshalb sind vorrangig die vordefinierten Konten NT AUTHORITY\LocalService für lokal agierende Dienste und NT AUTHORITY\NetworkService für Dienste mit Netzwerkzugriff in Betracht zu ziehen. Sie haben standardmäßig die gleichen Berechtigungen wie die vordefinierte Gruppe *Authentifizierte Benutzer* (normale Benutzer).

Mit Windows Server 2008 R2 wurden zwei besondere Konten eingeführt: das verwaltete Dienstkonto und das virtuelle Konto.

- Verwaltete Dienstkonten sind unter Windows Server 2008 R2 verwaltete Domänenkonten, die eine automatische Kennwortverwaltung bieten. Darüber hinaus können Klassen von Domänenkonten erstellt werden, diese können für Verwaltungsaufgaben an Nicht-Administratoren delegiert werden. Dieser Kontentyp wird in der Regel zur Verwaltung von Anwendungen wie SQL-Server oder des IIS eingesetzt.
- Virtuelle Konten sind unter Windows Server 2008 R2 verwaltete lokale Konten. Für diese Konten ist keine Kennwortverwaltung erforderlich. Innerhalb einer Domäne erfolgt die Anmeldung an Ressourcen des Netzes mit der Computeridentität.

Im Gegensatz zu den bisher genutzten Konten zur Verwaltung von Diensten wie *lokaler Dienst*, *Netzwerkdienst* oder *lokales System* kann das verwaltete Dienstkonto zentral verwaltet werden, da es in der Organisationseinheit "Verwaltete Dienstkonten" innerhalb des Active Directory gespeichert ist.

Es ist zu beachten, dass die neue Funktion der Dienstkonten auf dem zu verwaltenden System Windows Server 2008 R2 erfordert. Pro System kann nur ein verwaltetes Dienstkonto eingesetzt werden. Darüber hinaus muss sich die Domäne für eine vollständige Nutzung der Funktionen im sogenannten Windows Server 2008 R2 Modus befinden (*Domänenfunktionsebene*). Für Domänen, die sich im Modus Windows Server 2003 oder 2008 befinden, müssen gegebenenfalls weitere Konfigurationsschritte durchgeführt werden.

Bis einschließlich Windows Server 2008 sind lokale Konten den Domänenkonten vorzuziehen. Werden Domänenkonten verwendet, sollten sie mit so wenigen Domänenberechtigungen wie möglich ausgestattet werden, und es sollte für eine entsprechende Verfügbarkeit von Domänencontrollern gesorgt werden. Dienstkonten sollte die lokale Anmeldung verweigert werden (*Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | *Lokale Richtlinien* | *Zuweisen von Benutzerrechten* | *Lokal anmelden verweigern* oder in einer Domänengruppenrichtlinie). Ab Windows Server 2008 R2 sollten zur Administration von Dienstkonten die schon erwähnten Konten *verwaltetes Dienstkonto* und das *virtuelle Konto g*enutzt werden.

- Als Faustregel gilt, dass Applikationen mit Diensten auf Administrator-Niveau auf einem eigenen Server zu betreiben sind. Je höher die Anzahl solcher Applikationen auf einem Server ist, desto geringer ist das erreichbare Sicherheitsniveau. Als Beispiel sind Backup-Server oder Domänencontroller zu nennen, welche ihre Kerndienste nur mit vollen administrativen Berechtigungen ausüben können.
- Die voreingestellten Konten für die in Windows enthaltenen Dienste sollten nicht verändert werden.
- Unnötige oder potenziell gefährliche Dienste sollten deaktiviert werden.
- Viele Skripte und sonstige ausführbare Dateien können als Dienst installiert und ausgeführt werden. Dies ist im Normalfall kein empfohlenes Vorgehen.
- Im Einzelfall muss geklärt werden, wie das Verhalten von als Dienst ausgeführten Prozessen (Skripte oder Programme) die Systemstabilität und -sicherheit beeinflusst. Beispielsweise kann *Dienst beenden* oder *Dienst neu starten* zu beschädigten Daten führen, weil der Prozess auf solche Ereignisse nicht selbst reagieren kann, sondern einfach gelöscht wird. Der Einsatz eines solchen Verfahrens sollte in einer Testumgebung erprobt worden sein. Es sollte erwogen werden, starke Überwachungseinstellungen (System Access Control List, SACL) für die Dienstkonten zu setzen, um unvorhergesehenes Verhalten erkennen zu können.
- Für Kennwörter von Dienstkonten sind die üblichen Festlegungen für Benutzerkennwörter teilweise ungeeignet. Die folgende Tabelle zeigt beispielhaft die Standardeinstellungen nach der Installation. Daher ist für die Dienstkonten eine eigene, mit den Sicherheitsrichtlinien der Organisation abgestimmte Kennwortrichtlinie zu definieren.

| **Kennwortrichtlinie** | **Standardeinstellung auf Domänencontrollern** | **Tauglichkeit für Dienstkonten** |
|---|---|---|
| Kennwortchronik | 24 | ja |
| Maximales Kennwortalter (in Tagen) | 42 | ungeeignet |

| Kennwortrichtlinie | Standardeinstellung auf Domänencontrollern | Tauglichkeit für Dienstkonten |
|---|---|---|
| Minimales Kennwortalter (in Tagen) | 1 | ja |
| Minimale Kennwortlänge | 7 | nicht ausreichend |
| Kennwort muss festgelegten Anforderungen an Komplexität entsprechen? | Aktiviert | ja |
| Kennwörter mit umkehrbarer Verschlüsselung speichern | Deaktiviert | ja |

Das Kennwort sollte eine zweistellige Kennwortlänge besitzen (Es sind bis 127 Zeichen möglich). Es darf nicht automatisch ablaufen (Option *Kennwort läuft nie ab* in den Eigenschaften des Kontos), sondern sollte während regelmäßiger Wartungszyklen geändert werden. Ein Verfahren zum Ändern der Kennwörter sollte definiert sein und die Kennwörter sicher hinterlegt werden, siehe hierzu M 2.22 *Hinterlegen des Passwortes*. Bei einer größeren Anzahl von Diensten und Servern kann es sehr aufwendig werden, Kennwörter (inklusive Funktionstest der Dienste) zu ändern und zu hinterlegen, so dass der Sicherheitsgewinn unter Umständen nicht mehr gegeben ist. Hilfsprogramme für die Kennwortverwaltung von Dienstkonten können Hilfestellung leisten, stellen aber ihrerseits ein Risiko dar. Das maximale Alter von Kennwörtern und das Verfahren für deren Verwaltung sollte in Abhängigkeit des Schutzbedarfs und des Aufwandes festgelegt sowie in einer Richtlinie dokumentiert werden.

Dokumentation

Zu allen Diensten, die nicht mit einem vordefinierten Konto laufen, sind die Dienstkonten sowie deren Berechtigungen zu vermerken.

Prüffragen:

- Haben alle Dienstkonten nur die minimal benötigten Rechte?
- Wurde ein Verfahren zum Ändern der Kennwörter der Dienstkonten definiert?
- Ist sichergestellt, dass für Dienstekonten niemals der Built-in-Administrator verwendet wird?
- Wird nach Möglichkeit jeder Dienst mit einem separaten Dienstkonto betrieben?
- Werden ab Windows Server 2008 R2 zur Administration von Dienstkonten die neu eingeführten Kontentypen Verwaltetes Dienstkonto und Virtuelles Konto eingesetzt?
- Wurde für die Dienstkonten eine eigene Kennwortrichtlinie definiert und mit den Sicherheitsrichtlinien der Organisation abgestimmt?
- Sind die vorgenommenen Einstellungen bei den Dienstkonten dokumentiert?

# M 4.285 Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Standardinstallation von Windows Server 2003 enthält verschiedene Funktionen, die als Clientzubehör von Windows XP bekannt sind. Auf einem Server werden sie nicht benötigt und sollten deinstalliert oder, falls Deinstallation nicht möglich, zumindest deaktiviert werden, um die Angriffsfläche zu verringern und die damit verbundenen unnötigen Risiken zu reduzieren.

**Deinstallieren von Programmen unter *Start* | *Alle Programme* | *Zubehör***

- Als Administrator am Server anmelden
- Sicherheitskopie der Datei *C:\WINDOWS\inf\sysoc.inf* anlegen, z. B. als *Kopie von sysoc.inf*
- Folgende Zeilen in *C:\WINDOWS\inf\sysoc.inf* ändern und abspeichern:
  *OEAccess=ocgen.dll,OcEntry,oeaccess.inf,hide,7*
  ändern in
  *OEAccess=ocgen.dll,OcEntry,oeaccess.inf,,7*
  und
  *MultiM=ocgen.dll,OcEntry,multimed.inf,HIDE,7*
  ändern in
  *MultiM=ocgen.dll,OcEntry,multimed.inf,,7*
- Zu *Start* | *Systemsteuerung* | *Software* | *Windowskomponentenhinzufügen/entfernen* wechseln und folgende Checkboxen deaktivieren:
  - Outlook Express
  - Zubehör und Dienstprogramme / Multimedia / Audiorecorder
  - Zubehör und Dienstprogramme / Multimedia / Mediaplayer
  - Zubehör und Dienstprogramme / Kommunikation / Telefon

Hinweis: Durch die Schritte 1 bis 3 werden die Software-Optionen in Schritt 4 erst sichtbar gemacht.

**Deaktivieren von Mediaplayer, Outlook Express und Netmeeting**

Die Deinstallationsroutinen der integrierten Komponenten Mediaplayer, Outlook Express und Netmeeting entfernen die Programme nicht vollständig, das ungewollte Ausführen ist weiterhin möglich. Deshalb sollten diese Programme mit Hilfe der Richtlinien für Softwareeinschränkungen (siehe M 4.286 *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003*) deaktiviert werden.

Werden Active Directory und Gruppenrichtlinien verwendet, so muss die Wirksamkeit der Einstellungen auf dem einzelnen Server durch korrekte Konfiguration der Gruppenrichtlinien sichergestellt sein (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows*).

**Anpassen der lokalen Softwareeinschränkungsrichtlinie:**

- Die lokale Sicherheitsrichtlinie über *Start* | *Systemsteuerung* | *Verwaltung* | *LokaleSicherheitsrichtlinie* öffnen
- In den Zweig *Richtlinien für Softwareeinschränkungen* | *ZusätzlicheRegeln* wechseln

- Neue Pfadregeln mit der Sicherheitsstufe *Nicht erlaubt* für folgende Pfade *hinzufügen:*
  *%HKEY_LOCAL_MACHINE*
  *\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%*
  *\NetMeeting*
  *%HKEY_LOCAL_MACHINE*
  *\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%*
  *\Outlook Express*
  *%HKEY_LOCAL_MACHINE*
  *\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%*
  *\Windows Media Player*

Falls eines der deaktivierten Programme bisher beim Start des Betriebssystems automatisch geladen wurde, können Fehlermeldungen auftreten. Die entsprechenden Autostart-Funktionen sollten vor der Aktivierung der Richtlinie abgeschaltet werden, z. B. mit *msconfig.exe*.

Weiterhin sollte die Internetkommunikation für Windows-Client-Komponenten eingeschränkt werden. Dazu ist in der lokalen Gruppenrichtlinie (*Start* | *Ausführen*... | *gpedit.msc*) der Zweig *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Internetkommunikationsverwaltung* | *Internetkommunikationseinstellungen* auszuwählen. Hier sollten alle Funktionen deaktiviert werden. Nur *Automatische Aktualisierung von Stammzertifikaten* und *Windows Update* sollten aktiviert bleiben, solange hierfür kein alternatives Verfahren für den Server festgelegt wurde.

Wenn weitere nicht benötigte Client-Anwendungen und -Funktionen auf dem Server aktiv sind, dann sind auch diese zu deinstallieren bzw. zu deaktivieren.

Prüffragen:

- Sind alle auf dem Windows Server 2003 System nicht benötigten Dienste und Programme deinstalliert beziehungsweise deaktiviert, insbesondere die Client-Funktionen?

# M 4.286 Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bedingt unter anderem durch die intensive Nutzung des Internets (WWW, E-Mail usw.) werden Benutzer häufig mit unbekannter Software konfrontiert. Dabei müssen die Benutzer entscheiden, ob sie diese Software einsetzen möchten. Schadprogramme z. B. tarnen sich häufig als so genannte Trojanische Pferde, um Benutzer dazu zu verführen, diese zu installieren und auszuführen. Für den einzelnen Benutzer ist es oft schwierig zu entscheiden, welche Software er ausführen kann und soll. Durch Softwareeinschränkungsrichtlinien kann die IT-Umgebung vor nicht erwünschter oder nicht vertrauenswürdiger Software geschützt werden.

Nach einer Standardinstallation von Windows Server 2003 sollte zumindest eine lokale Softwareeinschränkungsrichtlinie erzeugt werden:

*Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | im Kontextmenü von *Richtlinien für Softwareeinschränkung* die Option *Neue Richtlinien für Softwareeinschränkungen erstellen* auswählen

Einstellungen unter *Vertrauenswürdige Herausgeber*:

- *Administratoren des lokalen Computers* aktivieren
- *Herausgeber* und *Zeitstempel* aktivieren

*Designierte Dateitypen* sind die Dateitypen, auf die die Softwareeinschränkungsrichtlinien Wirkung haben. Deshalb sollte die Liste *designierte Dateitypen* regelmäßig aktualisiert werden. Als Referenz kann zum Beispiel die Virenschutz-Richtlinie des IT-Verbunds dienen, in welcher kritische Dateierweiterungen definiert sind.

Die anderen Einstellungen sollten im Normalfall auf den Standardwerten belassen werden. Insbesondere die vordefinierten Regeln sollten nicht verändert werden, da das System sonst in einen unbenutzbaren Zustand versetzt werden kann. Die Richtlinien sollten immer für alle Benutzer gelten, die Administratoren eingeschlossen.

**Arten zusätzlicher Regeln**

| Regeltyp | Erklärung | Zuverlässigkeit der Sicherheitsmaßnahme |
|---|---|---|
| Hashregel | Bei Zugriff auf eine Datei wird ihr Hashwert berechnet und mit einem zuvor hinterlegten Hashwert verglichen. Die Regel greift bei identischen Hashwerten. Wird der Dateiinhalt allerdings zwischendurch manipuliert, ändert sich auch der Hashwert, und | mittel |

| Regeltyp | Erklärung | Zuverlässigkeit der Sicherheitsmaßnahme |
|---|---|---|
| | die Regel greift nicht mehr! | |
| Zertifikatsregel | Die Zertifikatsregel identifiziert Software anhand eines Authenticode-Zertifikats des Softwareherausgebers und lässt die Ausführung in Abhängigkeit der Sicherheitsstufe auch in geschützten Bereichen des Servers zu. | mittel |
| Pfadregel | Die Pfadregel identifiziert Software über einen angegebenen Dateipfad. Durch Verschieben des Programms verliert die Regel ihre Gültigkeit. | gering |
| Internetzonenregel | Zonenregeln gelten nur für .msi-Dateien (Windows Installer-Pakete) | gering |

**Einsatz der Softwareeinschränkungsrichtlinie**

Die Richtlinie zur Softwareeinschränkung erfordert eine ausführliche Planung sowie hinreichende Tests in einer Testumgebung, vor allem, wenn die Sicherheitsebene *Nicht erlaubt* als Standard gesetzt wird. Bei der Umsetzung sollte bevorzugt mit Hash- und Zertifikatsregeln gearbeitet werden, da die Pfad- und Internetzonenregeln nur einen geringen Schutz vor Ausführung von Programmen und Programmbibliotheken geben. Außerdem sollte die *Microsoft Knowledge Base* hinzugezogen werden, um dort dokumentierte unerwartete und unerwünschte Effekte bei der Anwendung von Hashregeln ausschließen zu können.

In der Softwareeinschränkungsrichtlinie können die DLL-Bibliotheken von vorn herein mit blockiert werden. In diesem Fall müssen eine hohe Zahl von Regeln für ausdrücklich zugelassene Bibliotheken definiert werden. Zugriffe auf DLL-Bibliotheken treten während der Programmausführung häufig auf, und jedes Mal muss die komplette Liste abgearbeitet werden. Performance-Auswirkungen sollten daher ebenfalls berücksichtigt werden.

Die Anwendung der Richtlinie sollte vornehmlich auf exponierten Servern mit hohen Sicherheitsanforderungen wie so genannten *Bastion Hosts* (öffentlich erreichbare Computer des Unternehmensnetzes) durchgeführt werden, um die Angriffsmöglichkeiten durch Schadprogramme zu minimieren. Die aktivierte Richtlinie mit entsprechend eingerichteten Regeln kann Virenschutzprogramme nicht ersetzen. Zur Abwehr von Sicherheitsvorfällen, z. B. im Zusammenhang mit Schadprogrammen, kann die Richtlinie zur Softwareeinschränkung als vorsorgliche Schutzmaßnahme oder Notfallmaßnahme angewendet werden.

Wenn eine Softwareeinschränkungsrichtlinie mittels Gruppenrichtlinien des Active Directory verteilt wird, sollte hierfür ein separates Gruppenrichtlinien-Objekt erstellt werden. Die Regeln in den Standardgruppenrichtlinien sollten nicht verändert werden. Wenn sich unerwartete und unerwünschte Effekte

im laufenden Betrieb herausstellen, kann das separate Gruppenrichtlinien-Objekt problemlos deaktiviert werden, und es greifen die Standardregeln.

**Dokumentation**

Alle Regeln außer den vordefinierten sollten dokumentiert werden. Der jeweilige Zweck sollte ebenfalls dokumentiert werden.

Prüffragen:

- Wird nach der Installation von Windows Server 2003 Systemen eine lokale Softwareeinschränkungsrichtlinie erzeugt, die unter Anderem eine aktuelle Liste designierter Dateitypen enthält?
- Werden die Richtlinien zur Softwareeinschränkung unter Windows Server 2003 im Vorfeld innerhalb einer Testumgebung überprüft?
- Wird in der Softwareeinschränkungsrichtlinie unter Windows Server 2003 bevorzugt mit Hash- und Zertifikatsregeln gearbeitet?

# M 4.287 Sichere Administration der VoIP-Middleware

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei VoIP-Middleware handelt es sich grundsätzlich um Server-Systeme, die mit den gleichen Sicherheitsmaßnahmen zu schützen sind, wie sie auch für andere Serversysteme eingesetzt werden. Darüber hinaus sind weitere Sicherheitsmaßnahmen anzuwenden, die den besonderen Bedrohungen bei VoIP-Systemen gerecht werden.

Vor der Inbetriebnahme müssen die VoIP-Komponenten sicher konfiguriert werden. Das Vorgehen bei der Erstinstallation ist zu dokumentieren. Im Folgenden werden einige Punkte vorgestellt, die für eine sichere Konfiguration und Administration berücksichtigt werden müssen.

**Leistungsmerkmale**

VoIP-Systeme bieten, wie auch traditionelle TK-Systeme, eine Vielzahl verschiedener Leistungsmerkmale. Es sollte vor Inbetriebnahme eines VoIP-Systems geklärt sein, welche Leistungsmerkmale und Funktionalitäten vorhanden sind und welche benötigt werden (siehe M 2.372 *Planung des VoIP-Einsatzes*). Die nicht benötigten sowie die sicherheitskritischen Leistungsmerkmale müssen deaktiviert werden. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und Wechselsprechen.

**Administration und Zugänge**

Administration und Konfiguration der Middleware ist immer an der Konsole oder über gesicherte Verbindungen durchzuführen. Die Administration kann beispielsweise über eine Secure Shell (SSH) oder eine verschlüsselte VPN-Verbindung erfolgen.

Viele VoIP-Systeme ermöglichen eine Konfiguration über eine Web-Oberfläche. Der dabei installierte Web-Server kann ein zusätzliches Sicherheitsrisiko darstellen. Daher ist es empfehlenswert, den Web-Server für eine mögliche Web-basierte Konfigurationsoberfläche nicht auf der kritischen Middleware, wie Gateways und Gatekeeper zu betreiben. Eine Web-basierte Konfiguration sollte immer gesichert erfolgen, beispielsweise durch den Einsatz von SSL oder TLS.

Bei der Planung des Administrationskonzeptes sollte ein Rollenkonzept vorgesehen sein, das verschiedene Berechtigungsstufen umfasst. Jeder Rolle sollten im Sinne einer Vertretungsregelung mindestens zwei Personen zugeordnet werden.

Sehr oft bietet es sich an, die VoIP-Komponenten, wie Softphones oder Middleware-Applikationen, auf Standard-PCs mit allgemein verbreiteten Betriebssystemen zu installieren. Die Administration der Betriebssysteme ist, wenn möglich, von der Administration der VoIP-Applikationen personell zu trennen.

Konfigurationsänderungen sollten durch das System so protokolliert werden, dass Manipulationen zeitnah nachvollzogen werden können. Die Protokolldaten selber müssen so abgesichert werden, dass Manipulationen an ihnen ausgeschlossen sind. Hierauf sollten auch Administratoren möglichst keine Zu-

griffsmöglichkeiten haben. Zum Schutz der Protokolldaten können diese z. B. auf WORM-Medien gespeichert werden oder der Zugriff kann auf Revisoren beschränkt werden.

**Backup**

Ein umfassendes Datensicherungskonzept ist eine zentrale Anforderung zur Sicherstellung bzw. zur raschen Wiederherstellung der Verfügbarkeit, aber auch, um die Integrität jederzeit überprüfen zu können. Dabei ist darauf zu achten, dass bei der Sicherung personenbezogener Daten, wie beispielsweise privater Verbindungsdaten, diese so abgelegt werden, dass sie vor unbefugtem Zugriff geschützt sind, also beispielsweise verschlüsselt.

**Sicherheit der Software**

Es ist darauf zu achten, dass die eingesetzte Software immer auf einem aktuellen Stand ist und etwaige sicherheitsrelevante Patches unverzüglich aufgespielt werden. Dies gilt insbesondere auch für das eingesetzte Betriebssystem.

Es muss gewährleistet werden, dass nur Original-Updates und -Patches eingespielt werden. Dies gilt sowohl für die Beschaffung, beispielsweise von den Internetseiten eines Herstellers, als auch für die Übertragung auf die VoIP-Komponenten. Durch folgende Maßnahmen können die Manipulationen bei der Übertragung erschwert beziehungsweise entdeckt werden:

- Vergleich von Prüfsummen
- Nutzung von sicheren Kommunikationswegen
- Verwendung von Zertifikaten

Für die Verlässlichkeit des Gesamtsystems ist eine korrekt implementierte Software von großer Bedeutung. Insbesondere die vitalen Funktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gateway-Funktion in das digitale Fernsprechnetz, sollten daher einem besonderen Evaluierungsprozess unterzogen werden.

Wünschenswert ist es deshalb, dass die Software für die Basisfunktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gateway-Funktion in das digitale Fernsprechnetz, nach einem bewährten Modell entwickelt und möglichst auch von einer unabhängigen Instanz überprüft wurde.

**Betriebssystemsicherheit**

Die VoIP-Komponenten sollten so konzipiert werden, dass verschiedene Dienste auf verschiedenen Servern betrieben werden (siehe auch M 4.97 *Ein Dienst pro Server*). Allerdings ist insbesondere bei kompakten Stand-alone-Systemen, die meist nur aus einer Hardware-Komponente bestehen, die vollständige Trennung von Diensten nicht immer möglich.

Das eingesetzte Betriebssystem sollte als minimales Betriebssystem (siehe M 4.95 *Minimales Betriebssystem*) ausgelegt sein und die Anzahl der auf der Middleware ausgeführten Applikationen so klein wie möglich gehalten werden. Jede zusätzliche Applikation kann Schwachstellen enthalten, die für Angriffe ausgenutzt werden können. Daher ist genau zu prüfen, welche Applikationen benötigt werden. Nicht benötigte Anwendungen sind zu deinstallieren. Software, die nur zur Installation benötigt wird, sollte im Anschluss gelöscht werden (beispielsweise Compiler). Nicht benötigte Netzdienste sind ebenfalls zu

deaktivieren und der Zugriff auf die verbleibenden Netzdienste ist durch lokale Paketfilter zu beschränken.

Prüffragen:

- Wird die Default-Konfiguration der VoIP-Komponenten vor der produktiven Inbetriebnahme abgeändert?
- Sind sicherheitskritische und nicht benötigte Leistungsmerkmale wie Aufschalten auf ein bestehendes Gespräch "Raumüberwachung" und "Wechselsprechen" deaktiviert?
- Wird die Middleware nur an der Konsole oder über gesicherte Verbindungen administriert und konfiguriert?
- Einsatz von VoIP-Middleware: Gibt es ein Administrationskonzept das ein Rollenkonzept mit verschiedenen Berechtigungsstufen enthält?
- Entspricht die Administration der Betriebssystemebene und der VoIP-Applikationsebene dem Rollenkonzept und der Berechtigungsstruktur?
- Einsatz von VoIP-Middleware: Sind Sicherheitsvorfälle aus den Protokolldaten ersichtlich?
- Sind die Protokolldaten durch geeignete Sicherheitsmaßnahmen geschützt?
- Einsatz von VoIP-Middleware: Sind Backups, die personenbezogene Daten beinhalten, vor unbefugtem Zugriff geschützt?
- Einsatz von VoIP-Middleware: Werden die eingesetzten Software-Komponenten durch regelmäßige Updates aus vertrauenswürdigen Quellen auf dem Stand der Technik gehalten?
- Einsatz von VoIP-Middleware: Existiert eine Regelung zur Dienste- und Servertrennung?
- Wird das System, durch den Einsatz eines minimalen Betriebssystems und der Verwendung von ausschließlich "notwendigen Applikationen", ausreichend gehärtet?
- Wird untersucht welche Applikationen benötigt werden und werden nicht benötigte Applikationen und Netzdienste deinstalliert, deaktiviert oder der Zugriff beschränkt?

# M 4.288 Sichere Administration von VoIP-Endgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wie die VoIP-Middleware müssen auch die VoIP-Endgeräte zahlreiche Sicherheitsvorgaben erfüllen. Ein Unterschied zwischen den Sicherheitsmaßnahmen der Middleware besteht darin, wie diese sicher konfiguriert werden.

### Vertrauenswürdige Firmware-Updates

Viele VoIP-Endgeräte bieten die Möglichkeit zum automatischen Update ihrer Firmware. Es muss sichergestellt werden, dass neue Firmware nur nach erfolgreicher Überprüfung der Authentizität und Integrität des Codes auf die Endgeräte aufgespielt wird. Falls der Hersteller für die Updates Prüfsummen zur Verfügung stellt oder die Update-Pakete digital signiert, müssen die Prüfsummen oder Signaturen vor der Installation überprüft werden. Stellt der Hersteller keine Prüfsummen bereit, muss sichergestellt sein, dass Updates nur über vertrauenswürdige Quellen bezogen werden.

### Vertrauenswürdiges Konfigurieren und Digitale Zertifikate

Die meisten VoIP-Endgeräte bieten verschiedene Möglichkeiten zur Konfiguration. Beispiele hierfür sind die lokale Konfiguration am Endgerät, die Webbasierte Konfiguration durch Zugriff auf einen im Endgerät integrierten Webserver sowie die automatische Konfiguration durch "Ziehen" (Pull) der Konfiguration von einem http(s)- oder TFTP-Server.

Die lokale Konfiguration wird in der Praxis selten eingesetzt. Sie sollte mit einem Passwort geschützt sein. Falls sie nicht genutzt werden soll, sollte sie deaktiviert werden. Der Zugang zur Web-basierten Konfiguration sollte ebenfalls nur mit einem Passwort möglich sein und über eine gesicherte Verbindung, beispielsweise über SSL oder TLS, erfolgen. Ein zusätzlicher Schutz wird durch die Verwendung eines Client-Zertifikats zur Authentisierung der Clients erreicht.

Die automatische Konfiguration über einen TFTP-Server sollte nicht gewählt und stattdessen deaktiviert werden, da sie nicht ausreichend sicher ist. Insbesondere die automatische Auswahl eines TFTP-Servers während des DHCP-Bootvorganges bietet zahlreiche Angriffsmöglichkeiten.

Eine automatische Konfiguration sollte grundsätzlich über einen https-Server erfolgen. Der https-Server sollte sich mit einem Zertifikat authentisieren, das vom Endgerät vor dem Laden der Konfiguration überprüft werden kann. Üblicherweise wird das Server-Zertifikat bei der Erstinbetriebnahme manuell auf die Endgeräte installiert.

### Sicherheitsfunktionalität

Viele VoIP-Telefone bieten die Möglichkeit zur passwortbasierten ein- oder mehrstufigen Zugangskontrolle (z. B. personenbezogenes Login oder Passwort für Amtsberechtigung). Es ist zu entscheiden, ob die Benutzer nur mit einer vorherigen Anmeldung das Telefon benutzen dürfen. Bei aktiviertem Passwortschutz sollten dann nur Notrufdienste zur Verfügung stehen. Um eine Nutzung durch unautorisierte Personen zu verhindern, müssen die Benutzer dann auch bei kurzfristiger Abwesenheit das Telefon sperren.

Sicherheitsfunktionalitäten, wie beispielsweise Anmeldepasswörter oder Passwörter für Amtsberechtigungen, müssen vor dem Produktiveinsatz ausführlich getestet werden, ob sie auch korrekt implementiert sind. Diese Authentisierungsmechanismen sollten von den Benutzern verwendet werden. Allerdings müssen sie über die Schwächen informiert werden. Anderenfalls besteht die Gefahr, dass nur eine Scheinsicherheit besteht.

Softphones werden in der Regel auf einem Standard-PC, der weitere Aufgaben erfüllt, betrieben. Dieser muss ebenfalls so administriert werden, dass er ein angemessenes Sicherheitsniveau erreicht. Hierzu gehören beispielsweise auch Maßnahmen, dass das Mikrofon nicht durch Dritte aktiviert werden kann. Wird diese Anforderung nicht umgesetzt, könnte das Mikrofon durch einen Angreifer zum Abhören missbraucht werden.

Durch die umfangreiche Angriffsfläche, die komplexe Arbeitsplatzsysteme bieten können, dürfen bei einem hohen oder sehr hohen Schutzbedarf keine Softphones eingesetzt werden.

In der Dokumentation der Komponenten sind oft Informationen zu finden, welche weiteren Sicherheitsfunktionen unterstützt werden. Es ist zu dokumentieren, welche Sicherheitsfunktionen aktiviert wurden.

Prüffragen:

- Werden die Authentizität und die Integrität von Firmware, Updates und Patches vor dem Einspielen auf die Endgeräte überprüft?
- Werden nicht benötigte Funktionen der Endgeräte per Konfigurationseinstellungen deaktiviert?
- Bei Einsatz der lokalen Konfiguration: Ist der Zugriff auf die lokale Konfiguration durch anerkannte Zugangsmerkmale geschützt?
- Bei Einsatz der webbasierten Konfiguration: Ist der Zugriff auf die webbasierten Konfiguration über sichere Pfade und Zugangsmerkmale abgesichert?
- Bei Einsatz der automatischen Konfiguration: Erfolgt vor der Konfiguration eine beidseitige Authentisierung der Kommunikationspartner?
- Bei Nutzung der Anmeldefunktion: Sperren die Nutzer ihr Endgerät bei Abwesendheit und sind Notrufdienste auch ohne Anmeldung verfügbar?
- Werden die Sicherheitsfunktionalitäten der Endgeräte vor dem produktiven Einsatz getestet?
- Einsatz von Softphones: Entspricht das Sicherheitsniveau des IT-Systems, auf dem das Softphone betrieben wird, den Sicherheitsanforderungen der Organisation?
- Bei hohem oder sehr hohem Schutzbedarf: Wird auf den Einsatz von Softphones verzichtet?
- Werden die eingesetzten Sicherheitsmechanismen und die verwendeten Parameter dokumentiert?

# M 4.289 Einschränkung der Erreichbarkeit über VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In den wenigsten Fällen ist es ratsam, dass direkt aus dem Internet auf die VoIP-Komponenten einer Behörde beziehungsweise eines Unternehmens zugegriffen werden kann. Ein direkter Zugriff, beispielsweise durch den Verbindungsaufbau auf eine interne IP-Adresse, kann einem Angreifer zahlreiche Möglichkeiten eröffnen. Daher ist zu entscheiden, wie externen Gesprächspartnern die Kontaktaufnahme über die VoIP-Architektur ermöglicht werden soll.

Zunächst ist zu prüfen, ob überhaupt der direkte Aufbau einer VoIP-Verbindung von außerhalb unterstützt werden soll. Oft ist es ausreichend, dass die Kontaktaufnahme über ein leitungsvermittelndes Telefonnetz stattfindet. In diesem Fall dürfen keine internen VoIP-Komponenten aus dem öffentlichen Datennetz erreichbar sein. Auf das Gateway, das zwischen dem öffentlichen, leitungsvermittelnden Telefonnetz und dem lokalen VoIP-Netz betrieben wird, sollte vom öffentlichen Datennetz ebenfalls kein Zugriff möglich sein. Bei einem generellen Verzicht auf die Erreichbarkeit über VoIP von außen ergeben sich aber Nachteile für externe Gesprächspartner. Besitzen diese einen Anschluss an ein öffentliches Datennetz, müssen sie dennoch über das öffentliche, leitungsvermittelnde Telefonnetz eine Verbindung aufbauen. Die hierfür anfallenden Kosten sind in der Regel höher als die für ein direkter Verbindungsaufbau zu einer VoIP-Adresse, wie einer SIP-URL. Da diesem Nachteil jedoch viele Vorteile, besonders bei sicherheitskritischen Anwendungsfällen, gegenüberstehen, sollte die Erreichbarkeit über VoIP von außen kritisch betrachtet werden.

Werden Verbindungen von außen nur über das öffentliche, leitungsvermittelnde Telefonnetz zugelassen, so kann auch SPIT (Spam over IP-Telephone) vermieden werden. Da SPIT dann nicht kostengünstig über das Datennetz übermittelt werden kann, fallen die gleichen Kosten wie bei einem Anruf bei einem Benutzer an, der nicht VoIP einsetzt.

Soll dennoch ein Verbindungsaufbau von oder in das öffentliche Datennetz gewünscht werden, ist die Entscheidung inklusive der Restrisiken zu dokumentieren. Außerdem müssen entsprechende Sicherheitsmaßnahmen ergriffen werden. Beispielsweise kann der gesamte Datenverkehr über einen Konzentrator geleitet werden, der wie ein Proxy-Server Verbindungsanfragen annimmt und an das nächste System, wie beispielsweise einen weiteren Server oder direkt an ein Endgerät, weiterleitet. Bei dem Einsatz eines Konzentrators sollten folgende Punkte beachtet werden:

- Sowohl die Signalisierungs- als auch die Sprachinformationen zwischen dem öffentlichen und privaten Datennetz müssen über den Konzentrator geleitet werden. Der Aufbau von individuellen Verbindungen sollte unterbunden werden. Die Paketfilter und Sicherheitsgateways müssen dementsprechend konfiguriert werden, so dass die VoIP-Kommunikation mit externen Kommunikationspartnern nur über einen Konzentrator stattfinden kann. Beispielsweise kann der Konzentrator innerhalb der demilitarisierten Zone (DMZ) des Sicherheitsgateways betrieben werden. Auf diese Weise könnte der direkte Verbindungsaufbau aus dem lokalen Netz ins öffentliche Netz beziehungsweise aus dem öffentlichen Netz ins lokale Netz vermieden werden.

- Wegen eines fehlenden Signalisierungsstandards empfiehlt es sich, so viele Signalisierungsprotokolle wie möglich nach außen zu unterstützen. Daher sollte der Konzentrator als Gateway zwischen den im lokalen Datennetz verwendeten Protokoll und den Protokollen, die für externe Benutzer zur Verfügung stehenden, betrieben werden können.
- Um einem Missbrauch entgegenzuwirken, sollte ein Gesprächsaufbau aus dem internen in das externe Datennetz nur nach einer Authentisierung am Konzentrator möglich sein.
- Bei Verbindungen innerhalb des lokalen Datennetzes sollte der Konzentrator nicht beteiligt werden.
- Es muss festgelegt werden, welche Funktionen neben der Sprachkommunikation externen Teilnehmern angeboten werden sollen.
- Der Konzentrator sollte Signalisierungs- und Sprachpakete, die nicht protokollkonform (Beispiele sind zu große Datenpakete) sind, erkennen und abweisen.
- Da direkt auf den Konzentrator aus dem öffentlichen Datennetz zugegriffen werden kann, sollte die sicherheitskritische Konfiguration im Vordergrund stehen.
- Gesprächsteilnehmer aus dem öffentlichen Datennetz müssen die IP-Adresse des Konzentrators kennen, um eine Verbindung zu ihm aufbauen zu können. Daher bietet es sich an, die Adresse des Konzentrators durch einen entsprechenden Eintrag im DNS-Server der Behörde beziehungsweise des Unternehmens zu veröffentlichen.
- Der Empfang, die Bearbeitung und die Weiterleitung der Sprach- und Signalisierungsinformationen können hohe Ressourcen beanspruchen. Daher sollte sowohl die Netzanbindung als auch die Systemressourcen ausreichend dimensioniert werden.
- Werden hohe Anforderungen an die Verfügbarkeit der Erreichbarkeit gestellt, sollte der Konzentrator redundant ausgelegt werden können. Bei einer redundanten Auslegung zur Lastverteilung müssen die verbleibenden Systeme genügend Ressourcen bereitstellen, um einen möglichen Ausfall ausgleichen zu können.

Viele Hersteller bieten hierfür teilweise proprietäre Systeme an. Als Alternative im Open-Source-Umfeld erfüllt die Software-Telefonanlage Asterisk, die als Appliance betrieben kann, viele diese Anforderungen. Ein weiterer Vorteil beim Einsatz eines Konzentrators ist die Vermeidung der Probleme, die bei der Verwendung von NAT (Network Adress Translation) auftreten.

Prüffragen:

- Existiert eine Regelung zur Kontaktaufnahme für externe Gesprächspartner?
- Kontaktaufnahme durch ein leitungsvermittelndes Telefonnetz: Wird der Zugriff auf die VoIP-Architektur gemäß der Sicherheitsrichtlinie beschränkt?
- Erlaubter Verbindungsaufbau aus dem oder in das öffentliche Datennetz: Sind Sicherheitsmaßnahmen entsprechend der Sicherheitsrichtlinie umgesetzt?
- Erlaubter direkter Verbindungsaufbau zwischen Endgerät und Datennetz: Existiert eine Risikoanalyse für die VoIP-Schnittstelle?
- Einsatz eines Konzentrators: Laufen alle Signalisierungsinformationen und Sprachinformationen zwischen dem öffentlichem und dem privatem Datennetz nur über den autorisierten Konzentrator?

# M 4.290 Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wird ein IP-Datennetz für VoIP genutzt, ergeben sich zusätzliche Anforderungen, insbesondere auch an die Sicherheit des Netzes. Oftmals ist die strikte Trennung von Sprach- und Datennetzen nicht möglich, da beispielsweise Softphones von Arbeitsplatzrechnern aus dem Datennetz auf den VoIP-Server im Sprachnetz zugreifen, Groupware-Clients das direkte Wählen von Rufnummern gespeicherter Kontakte aus der Applikation ermöglichen oder VoIP-Server mit Verzeichnisdiensten, wie LDAP (Lightweight Directory Access Protocol) gekoppelt werden. Hinzu kommt eventuell die Vernetzung geografisch getrennter Behörden-, Unternehmens- bzw. Organisationsstandorte, die beispielsweise einen zentralen VoIP-Server für die organisationsweite Kommunikation verwenden und gleichzeitig diese Verbindung für den Austausch von Daten nutzen.

Ein Sicherheitsgateway soll ein internes, sicheres System vor unberechtigten Zugriffen aus einem unsicheren Netz schützen und gleichzeitig berechtigte Zugriffe zu den geschützten Bereichen zulassen. Was als sicheres bzw. unsicheres Netz gilt, welche Ressourcen schützenswert sind und wie sie zu schützen sind, wird in den Sicherheitsrichtlinien der Organisation festgelegt (siehe hierzu auch B 3.301 *Sicherheitsgateway (Firewall)*).

Bei der Planung der VoIP-Nutzung sollte überprüft werden, ob das bestehende Sicherheitsgateway für den Einsatz von VoIP angepasst werden kann. Anderenfalls muss ein zusätzliches Sicherheitsgateway hierfür beschafft und installiert werden.

**Auswahl und Anforderungen an ein Sicherheitsgateway**

Die Leistungsfähigkeit des eingesetzten Sicherheitsgateways bei der Nutzung von VoIP beeinflusst nicht nur den Schutz, sondern auch die Qualität der übertragenen Sprache. Durch die Verarbeitung vieler kleiner Datenpakete, die bei VoIP üblich sind, wird das Sicherheitsgateway stark belastet, wodurch Delay und Jitter der übertragenen Sprachsignale direkt beeinflusst werden.

Werden Signalisierungs- und Sprachdaten über das Sicherheitsgateway hinaus geleitet, sollte ein VoIP-fähiges Sicherheitsgateway verwendet werden, das in der Lage ist, die verwendeten Signalisierungsprotokolle mit dem gesamten Rufauf- und -abbau zu analysieren und die jeweiligen Zustände zu speichern. Anhand der Protokolldaten (z. B. die zu verwendenden UDP-Ports für die mit RTP übertragenen Sprachdaten) werden die benötigten Ports für die Dauer der Kommunikation geöffnet.

Im Weiterem hängt die Auswahl des richtigen Systems von den folgenden Faktoren ab:

- Wie groß ist das Netz?
- Welche Systemkomponenten stehen zur Verfügung? Ermöglichen bestehende Switches eine VLAN-Trennung von Sprach- und Datennetzen? Unterstützen bestehende Router Zugriffslisten (ACLs) oder Funktionalitäten von Sicherheitsgateways?
- Welche Sicherheitsgateways werden bereits im Datennetz eingesetzt?

- Ist nur eine auf das LAN begrenzte IP-Telefonie oder auch die Internet-Telefonie geplant?
- Wie umfassend sind die Kenntnisse des betreuenden IT-Personals?
- Welche VoIP-Systemkomponenten werden eingesetzt?
- Welcher finanzielle Rahmen steht für die Umsetzung der Sicherheitsziele zur Verfügung?

**Konzeption eines Sicherheitsgateways**

Unabhängig davon, ob ein bestehendes Sicherheitsgateway für die Nutzung von VoIP verändert oder ob ein neues System beschafft werden soll, kann es aus folgenden Komponenten bestehen:

- **Zustandsloser Paketfilter (Stateless Packet Filter)**
  Einfache Paketfilter können auf Routern, Layer-3-Switches bzw. Sicherheitsgateways zur Trennung von Daten- und Sprachnetz eingesetzt werden, wobei ihre Filterfunktionalität gegenüber zustandsbasierenden Filtern bzw. Application Level Gateways deutlich eingeschränkt ist.
- **Zustandsbasierende Filterung (stateful packet inspection)**
  Zustandsbasierende Paketfilter können die für eine Kommunikation benötigten Rückpakete dynamisch durchlassen und so ein erhöhtes Maß an Sicherheit für ein Netz bereitstellen. Sie speichern Zustände einer Verbindung ab und können so Rückpakete, die zu einer bestehenden Verbindung gehören, durchlassen, ohne das dafür explizite Zugriffslisten konfiguriert werden müssen.
- **Application Level Gateway (ALG)**
  Ein Application Level Gateway kann im Gegensatz zu den vorgenannten Systemen nicht nur auf IP-Adressen und Ports, sondern auch auf der Applikationsebene filtern. Der Vorteil eines Application Level Gateways macht sich gerade bei der Übertragung von RTP-Paketen bemerkbar. Die für die RTP-Übertragung zu verwendenden UDP-Ports werden im Rahmen der Signalisierung (mittels SDP) zwischen den Endpunkten ausgetauscht. Diese Ports variieren in der Regel bei jedem neuen Gespräch und müssen an dem Sicherheitsgateway freigegeben werden. Da das ALG den Austausch der Protokollnachrichten verfolgt, in denen die IP-Adressen und die zu verwendenden UDP-Ports vereinbart werden, kann es dynamisch Filter anpassen, die den betreffenden RTP-Strom passieren lassen.

Vergleicht man zustandslose Paketfilter, zustandsorientierte Paketfilter und ALGs miteinander, so empfiehlt es sich aufgrund der Vorteile möglichst ein ALG einzusetzen. Um eingehenden RTP-Verkehr zu ermöglichen, müssen zustandslose und zustandsorientierte Sicherheitsgateways große Portbereiche dauerhaft öffnen, damit RTP-Pakete mit Sprachdaten durchgelassen werden können. Eine solche Konfiguration stellt ein erhebliches Sicherheitsrisiko dar.

Application Level Gateways hingegen öffnen nur die tatsächlich benötigten Ports für die Dauer der Kommunikation und bieten daher weniger potentielle Angriffsmöglichkeiten.

Die Verwendung von Protokollen wie IAX (InterAsterisk eXchange) erleichtert die Konzeption des Sicherheitsgateways. Da hierbei sowohl die Signalisierungs- und die Medientransportinformationen über einen Nachrichtenstrom übertragen werden, wird nur ein festgelegter Port benötigt. Aufgrund der fehlenden Portaushandlung müssen keine dynamischen Portfilterungen durchgeführt werden.

**Konfiguration eines Sicherheitsgateways**

Die bei der Nutzung von VoIP eingesetzten Sicherheitsgateways unterscheiden sich kaum von klassischen Sicherheitsgateways. Für deren Aufbau und sicheren Betrieb sind die im Baustein B 3.301 *Sicherheitsgateway (Firewall)* beschriebenen Maßnahmen umzusetzen.

Die VoIP-spezifischen Einstellungen müssen analog zu den Maßnahmen aus diesem Baustein vorgenommen werden, wie diese konkret umzusetzen sind, ist der Dokumentation des eingesetzten Produktes zu entnehmen.

Prüffragen:

- Existiert eine Regelung zur Absicherung des VoIP-Dienstes durch ein Sicherheitsgateway?

# M 4.291 Sichere Konfiguration der VoIP-Middleware

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Funktion und die Sicherheit der VoIP-Middleware wird wesentlich durch die eingestellten Konfigurationsparameter bestimmt. Sehr oft werden mehrere unabhängige VoIP-Komponenten, wie Gatekeeper und Gateways, benötigt. Das nicht abgestimmte Ändern eines Konfigurationsparameters bei einer Komponente kann daher im Zusammenspiel mit den anderen Komponenten zu Fehlfunktionen führen.

Die für die VoIP-Komponenten zuständigen Administratoren müssen nach der Inbetriebnahme zahlreiche weitere Änderungen vornehmen können. Verlassen Mitarbeiter die Behörde oder das Unternehmen oder kommen neue hinzu, müssen Änderungen vorgenommen werden. Auch bei einem Wechsel in ein anderes Netzsegment, beispielsweise durch einen Umzug in ein anderes Gebäude, müssen Anpassungen durchgeführt werden können. Daher sollte eine Konfigurationsoberfläche gewählt werden, über die die Administratoren diese Anpassungen effizient vornehmen können.

In der Regel werden den Mitarbeitern jeweils ein Benutzername und ein Passwort für die VoIP-Nutzung zugewiesen. Bei der Nutzung von VoiceMails kann an dieser Stelle eine E-Mail-Adresse eingetragen werden. Es ist darauf zu achten, dass die Benutzer Passwörter auswählen, die nicht zu kurz oder leicht zu erraten sind. Einstellungen, die nur sichere Passwörter akzeptieren, sollten aktiviert werden. Benutzer, die nur stationäre Geräte mit einer gleichbleibenden IP-Adresse besitzen, sollten sich nur mit dem Gerät, dem diese IP-Adresse zugewiesen wurde, anmelden dürfen.

Bei der Zuordnung zwischen Benutzernamen und Telefonnummer müssen eventuell vorhandene interne Vorgaben beachtet werden. Die Vergabe von Telefonnummern, die keinem Benutzer zugeordnet werden, spielt eine weitere Rolle. Ein Beispiel hierfür sind für Besucher frei zugängliche Telefone in Konferenzräumen. Prinzipiell sollten diese Telefonanschlüsse so wenig Privilegien wie möglich erhalten. In der Regel ist die Beschränkung, dass nur interne Gesprächsteilnehmer angerufen werden können, akzeptabel und ausreichend.

Oft kann festgelegt werden, welcher Benutzer welche Signalisierungsprotokolle verwenden darf. Wenn es möglich ist, sollten alle Benutzer nur ein Protokoll verwenden dürfen, da dies den Administrationsaufwand verringert. Unterstützen die Endgeräte verschlüsselte Signalisierungsprotokolle, sollte darauf geachtet werden, dass eine unverschlüsselte Anmeldung nicht möglich ist.

Den Benutzern des TK-Systems können bestimmte Rechte (Privilegien) zugeordnet oder entzogen werden. Beispielsweise kann das recht eingeschränkt werden, ins Ausland oder kostenpflichtige Service-Rufnummern anzurufen. Bei der Konfiguration muss das Ziel verfolgt werden, dass jeder Benutzer nur die Privilegien erhält, die für ihn vorgesehen sind.

Kleine, selbstentwickelte und den Gegebenheiten angepasste Makros können den Administratoren die Konfiguration erleichtern. Diese Makros sind ausführlich zu dokumentieren. Bei dem Einsatz der Makros ist darauf zu achten, dass sie vor dem Einsatz einer ausführlichen Qualitätssicherung unterzogen und gründlich getestet wurden. Anderenfalls besteht beispielsweise die Gefahr,

dass solche Makros schwer auffindbare Konfigurationsmängel erzeugen oder unerwünschte Seiteneffekte mit sich bringen.

Während der Konfiguration muss darauf geachtet werden, dass zusätzliche und nicht zwingend benötigte Dienste deaktiviert werden beziehungsweise bleiben. Anderenfalls besteht die Gefahr, dass diese Dienste für Angriffe ausgenutzt werden.

Zahlreiche Ereignisse können protokolliert werden. Über die Signalisierungsinformationen kann beispielsweise ausgewertet werden, welcher Benutzer wie lange mit wem telefoniert hat. Werden die Medieninformationen nicht direkt zwischen den Endgeräten, sondern über die Middleware ausgetauscht, ist eine zentrale Auswertung der Gesprächsinhalte grundsätzlich möglich. Einerseits können Protokollierungsfunktionen zur Nachvollziehbarkeit des VoIP-Betriebs beitragen. Andererseits muss verhindert werden, dass Protokollierungsfunktionen für Verletzungen der Informationssicherheit oder des Datenschutzes missbraucht werden.

Es muss deshalb systematisch und verbindlich festgelegt werden, welche Informationen protokolliert werden und wie die regelmäßige Auswertung der Protokolldaten erfolgt. Dabei ist in jedem Fall der Datenschutzbeauftragte und der Personal- beziehungsweise Betriebsrat zu beteiligen. Treten bei der Auswertung Unstimmigkeiten auf, müssen diese näher beleuchtet und die Ursachen gegebenenfalls beseitigt werden.

Alle Einstellungen sind durch eine regelmäßige Revision zu überprüfen.

Prüffragen:

- Existiert eine geeignete Konfigurationsoberfläche mit der Administratoren effizient Anpassungen und Einstellungen vornehmen können?
- Existiert eine Regelung zur Verwendung von Passwörtern mit einer anerkannten Güte?
- Bei Einsatz von stationären Geräten mit definierter IP-Adresse: Existiert eine Regelung zur restriktiven Anmeldung von Geräten und Benutzern?
- Existiert eine Regelung für den restriktiven Einsatz von Signalisierungsprotokollen?
- Erhält jeder Benutzer nur die notwendigen Privilegien?
- Existiert eine Regelung für den Einsatz von Sicherheitsmechanismen und Protokollen?
- Werden nicht benötigte Dienste der VoIP-Middleware deaktiviert?
- Existiert eine Regelung zur datenschutzkonformen Protokollierung und Auswertung von Informationen?
- Auswertung von Protokollen: Existiert eine Regelung zur Überprüfung und Behebung von Auffälligkeiten?

# M 4.292 Protokollierung bei VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei einer Kommunikation über VoIP können zahlreiche Informationen protokolliert werden. Meist müssen bestimmte Statusinformationen der VoIP-Middleware protokolliert werden, um für einen reibungslosen Betrieb zu sorgen. Erst die regelmäßige Auswertung dieser Protokolldaten ermöglicht es, die korrekte Funktion der Geräte zu beurteilen und Angriffsversuche zu erkennen. Mit Hilfe der Protokolldaten kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden.

Die sorgfältige Konfiguration der Protokollierungsfunktionen ist besonders wichtig, da nur eine sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert.

Je nach Art der protokollierten Ereignisse kann es erforderlich sein, schnellstmöglich einzugreifen. Daher müssen die Protokolldaten regelmäßig ausgewertet werden.

Einerseits können Protokollierungsfunktionen zur Nachvollziehbarkeit des VoIP-Betriebs beitragen. Andererseits besteht die Gefahr, dass Protokollierungsfunktionen für Verletzungen der Informationssicherheit oder des Datenschutzes missbraucht werden. Es muss deshalb verbindlich festgelegt und dokumentiert werden, welche Informationen protokolliert werden und wie die regelmäßige Auswertung der Protokolldaten erfolgt. Dabei ist in jedem Fall der Datenschutzbeauftragte und der Personal- beziehungsweise Betriebsrat zu beteiligen (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollten dokumentiert und innerhalb der Institution abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

### Protokollierung der Signalisierung

Durch die Auswertung der Signalisierung können zahlreiche Informationen ermittelt werden. An einem Sip-Proxy, Gatekeeper oder Gateway sollten folgende Daten aufgezeichnet werden:

- wer mit wem telefoniert hat,
- wie lange telefoniert wurde,
- ob der Empfänger das Gespräch entgegen genommen hat,
- von welchem Netz und welcher IP-Adresse aus das Gespräch geführt wurde,
- welche Medientransportprotokolle und welcher Codec ausgehandelt wurden.

Diese Informationen können beispielsweise für eine Kostenabrechnung oder für eine Optimierung der VoIP-Infrastruktur genutzt werden.

### Protokollierung des Medientransports

Durch die Protokollierung an einer geeigneten Stelle im Netz können unter bestimmten Bedingungen die eigentlichen Gesprächsinhalte aufgezeichnet werden. Bei Gesprächen, die das Netz über eine definierte Stelle verlassen, wie beispielsweise über einen Proxy, könnte die Protokollierung direkt an dieser Stelle vorgenommen werden.

Bei internen Gesprächen ist häufig kein Proxy erforderlich. Auch in diesem Fall ist eine Aufzeichnung der Gesprächsinhalte in der Regel möglich, beispielsweise an den beteiligten Endgeräten oder Routern.

Werden die kryptographischen Schlüssel bei einem wirksam verschlüsselten Medientransport direkt von den beteiligten Gesprächsteilnehmern ausgehandelt, können weniger Informationen an zentraler Stelle erfasst werden.

**Protokollierung der Systemstatusinformationen**

Neben den oben genannten Punkten sollten folgende Informationen nach Möglichkeit an der VoIP-Middleware protokolliert werden:

- Alle direkten Anmeldungen auf der Appliance beziehungsweise auf dem IT-System,
- Veränderungen der Konfiguration,
- Fehlerhafte Anmeldungen am VoIP-Dienst,
- Systemfehler,
- Auslastung,
- Änderungen an der Benutzerverwaltung (Anlegen oder Löschen von Benutzern, Änderungen der Zuordnung zwischen Benutzer und Telefonnummer, etc.),
- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können und
- wichtige Systemereignisse des IT-Systems, auf dem die VoIP-Applikation betrieben wird. Weitere Informationen hierzu sind dem entsprechenden IT-Grundschutz-Baustein zum Betriebssystem entnehmen.

**Zentrale Verwaltung der Protokolldaten**

Es ist zu empfehlen, die Protokolldaten über das Netz auf einen eigenen syslog-Server zu übertragen. Dies dient der zentralen Sammlung, Archivierung und Auswertung der Protokolldaten, da auf den VoIP-Applicances oft keine ausreichenden Betriebsmittel dafür vorhanden sind. Außerdem bietet dies den Vorteil, dass bei einer Kompromittierung eines Gerätes die bereits übertragenen Protokolldaten vom Angreifer nicht direkt verändert oder gelöscht werden können.

Falls die Übertragung zum syslog-Server unverschlüsselt erfolgt, ist ein Mithören auf dem Übertragungsweg möglich. Daher sollten die Protokolldaten entweder nur am Server selber gespeichert werden, oder verschlüsselt oder über ein eigenes Netz (Administrationsnetz) übertragen werden.

**Zeitsynchronisation**

Alle Protokolldaten sollten möglichst mit einem korrekten Zeitstempel versehen sein. Nur so ist eine effektive Auswertung dieser Daten, insbesondere bei der Analyse von versuchten oder erfolgten Angriffen, möglich. Deshalb sollten im internen Netz entsprechende Server eingerichtet werden, die allen Systemen die korrekte Zeit bereitstellen. Dies kann beispielsweise auf Basis des NTP-Dienstes geschehen (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*).

Prüffragen:

- Existiert eine Regelung zur zeitnahen Auswertung von Protokollierungsdaten?
- Existiert eine Regelung zur Verbesserung des Sicherheitsniveau auf Grundlage der Protokollauswertung?

- Existiert eine Regelung zur Festlegung von Inhalten und Umfang der zu protokollierenden Ereignisse und Informationen?
- Entsprechen die verwendeten Protokolle und Pfade zur Protokollierung und Administration dem Stand der Technik?
- Existiert eine Regelung zur einheitlichen Konfiguration und Überwachung von Parametern?

# M 4.293 Sicherer Betrieb von Hotspots

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter IT

**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Zweck eines Hotspots ist im Allgemeinen (fremden) Benutzern einen einfachen Zugang zum Internet zu erlauben. Um einen Hotspot dauerhaft und sicher betreiben zu können, ist eine erfolgreiche Authentisierung aller Benutzer am Hotspot erforderlich. Gebräuchliche und ansatzweise sichere Verfahren sind beispielsweise:

- **Webauthentisierung**
  Hierbei gibt der Benutzer über eine Webschnittstelle seine Zugangsdaten (IP-Adresse, Benutzername, Passwort etc.) ein. Dies sollte natürlich über SSL/TLS verschlüsselt erfolgen. Nach einer erfolgreichen Anmeldung wird der Zugang für den Client freigeschaltet.
- **PPTP (Point to Point Tunnel Protocol)**
  PPTP ist ein typisches Tunneling-Protokoll für VPNs, also Protokollen, die verwendet werden, um Daten bei der Übertragung zu verschlüsseln, durch den Tunnel zu übertragen und die Verbindung zu verwalten. Als kryptographische Verfahren stehen bei PPTP RC4 mit 40 oder 128 Bit zur Verschlüsselung sowie PAP oder CHAP zur Authentisierung zur Auswahl. In gängigen Implementierungen dieses Tunnel-Verfahrens wurden Sicherheitslücken entdeckt, insbesondere in Zusammenhang mit schwachen Passwörtern. Ohne zusätzliche Sicherheitsmechanismen sollte PPTP daher nicht eingesetzt werden.
- **IPSec**
  IPSec bietet starke kryptographische Verfahren und eine gegenseitige Authentisierung der Kommunikationspartner. Diese sollte sinnvollerweise auf Zertifikaten basieren. Deren Verwendung ist aber einerseits noch nicht in allen IPsec-Implementationen vorgesehen, zum anderen müssen diese erst geeignet generiert und verteilt werden (typisches PKI-Problem).
- **WLAN-spezifische Sicherheitsmechanismen wie WEP, IEEE 802.1X, WPA, WPA2, TKIP, IEEE 802.11i**
  Bei allen WLAN-spezifischen Sicherheitsmechanismen soll für Sicherheit auf der Funkstrecke gesorgt werden. Diese müssen geeignet kombiniert werden. Aufgrund der schnellen Entwicklung in diesen Bereichen sind wegen des Verbreitungsgrads bzw. der Sicherheitsmängel dieser Verfahren nicht alle für die Verwendung bei Hotspots geeignet.

Hotspot-Anbieter sollten geeignete Authentisierungsverfahren anbieten.

Beim Betrieb von Hotspots sollten außerdem folgende Sicherheitsmaßnahmen umgesetzt werden:

- Access Points, die als Hotspot betrieben werden sollen, dürfen nicht direkt mit einem LAN verbunden werden, sondern nur über ein Sicherheitsgateway.
- Die Kommunikation von WLAN-Clients untereinander, die sogenannte Inter-Client-Kommunikation, sollte komplett unterbunden werden.
- Die Funkschnittstelle sollte mit Funk-Analyse-Systemen überwacht werden, um fremde Access Points und Hotspots zu erkennen.
- Die Authentisierungsdaten sollten über die Funkstrecke, also zwischen WLAN-Client und Access Point immer verschlüsselt übertragen werden. Bei der weiteren Übertragung der Daten von einem Hotspot-Access Point zu den Authentisierungssystemen (beispielsweise einem RADIUS-Server)

sind geeignete Verschlüsselungsverfahren wie SSL oder IPSec anzuwenden, vor allem bei der Nutzung öffentlicher Netze.
- Falls für die Authentisierung Zertifikate verwendet werden, sollten diese von einer geeigneten Zertifizierungsinstanz signiert sein. Außerdem sollte der Fingerprint des Serverzertifikats veröffentlicht werden, damit Benutzer die Echtheit überprüfen können.
- Jeder Betreiber eines Hotspots sollte mindestens ein geeignetes Verfahren zur Verschlüsselung der Funkstrecke anbieten, damit die Benutzer ihre Daten vor unbefugtem Mitlesen schützen können. Nicht alle Benutzer haben allerdings ein ausgeprägtes Interesse am Schutz ihrer Daten und Systeme. Es können auch die technischen Voraussetzungen für die Nutzung von angebotenen Verschlüsselungsverfahren fehlen. Daher sollte deren Nutzung optional sein. Die Benutzer sollten aber unbedingt auf die Möglichkeit und die Vorteile der verschlüsselten Übertragung hingewiesen werden.
- Viele Benutzer wollen über einen Hotspot beispielsweise per VPN auf das Netz der eigenen Institution zugreifen. Hierfür müssen diese die organisationseigenen Sicherheitsvorgaben umsetzen können. Daher sollte die technische Ausgestaltung des Hotspots die Nutzung typischer Sicherheitsmaßnahmen wie IPsec ermöglichen.

Außerdem sollten Hotspot-Betreiber regelmäßig die Protokolle daraufhin überprüfen, ob hier Unregelmäßigkeiten zu erkennen sind, also beispielsweise die Zahl der Benutzer die der angemeldeten Gäste übersteigt.

Anbieter von öffentlichen Hotspots haben darüber hinaus die jeweiligen gesetzlichen und regulatorischen Vorgaben zu beachten.

Den Benutzern sind in geeigneter Weise vorab die Nutzungsbedingungen mitzuteilen. In den Nutzungsbedingungen sollten Hinweise darüber zu finden sein, ob die Nutzung kostenfrei oder kostenpflichtig ist (mit Angabe der entsprechenden Preise), aber auch, welche Leistungen, vor allem welche Sicherheitsmechanismen, bei der Verwendung des Hotspots angeboten werden. Der Benutzer muss bestätigen, dass er die Nutzungsbedingungen zur Kenntnis genommen hat und akzeptiert. Bei einer Webauthentisierung könnten die Nutzungsbedingung beispielsweise auf einer Webseite präsentiert und die Zustimmung zu den Nutzungsbedingungen eingeholt werden.

Die Sicherheitsrichtlinien, die Hotspot-Benutzer beachten sollten, sind in M 2.389 *Sichere Nutzung von Hotspots* beschrieben.

Prüffragen:

- Ist sichergestellt, dass die Freischaltung des Clients erst nach erfolgreicher Anmeldeprozedur erfolgt?
- Einsatz von Zertifikaten zur Authentisierung: Sind die eingesetzten Zertifikate von einer öffentlichen Zertifizierungsinstanz signiert?
- Wird seitens des Hotspots-Betreibers ein Verfahren zur Verschlüsselung der WLAN-Kommunikation angeboten?
- Wird der Einsatz eines VPN innerhalb des WLAN unterstützt?
- Erfolgt seitens des Hotspot-Betreibers eine regelmäßige Auswertung der Protokolldaten, um beispielsweise Unregelmäßigkeiten rechtzeitig zu erkennen?
- Erfolgt der Betrieb von öffentlichen Hotspots unter Beachtung der gesetzlichen und regulatorischen Vorgaben?
- Werden die Benutzer in geeigneter Weise vorab über die Nutzungsbedingungen des Hotspots informiert (z. B. Kosten, Leistungen,

Sicherheitsmechanismen) und muss diese zur Kenntnis nehmen und akzeptieren?
- Sind die Nutzungsbedingungen des Hotspots für jeden Benutzer transparent und verständlich?
- Existiert eine Regelung zum Schutz des kabelgebundenen LAN ?
- Wird die Inter-Client-Kommunikation unterbunden?
- Wird die Funkschnittstelle überwacht, um fremde Access Points und Hotspots zu erkennen?
- Entsprechen die genutzten Kommunikationsprotokolle und Schnittstellen bei der Authentisierung dem aktuellen Stand der Technik?

# M 4.294 Sichere Konfiguration der Access Points

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Keinesfalls dürfen Access Points in der Konfiguration des Lieferzustandes verwendet oder mit Einstellungen z. B. für SSID (Service Set Identifier), Zugangskennwörter oder kryptographischen Schlüssel versehen werden, die in den Handbüchern des Produktes genannt werden.

Folgende Einstellung sollten vorgenommen bzw. auf individuelle, sichere Werte geändert werden:

- Soweit möglich, sollte ein administrativer Zugriff auf die Access Points über die Luftschnittstelle generell deaktiviert werden.
- Alle Administrationspasswörter sollten möglichst komplex sein und regelmäßig gewechselt werden.
- Unsichere Administrationszugänge (z. B. über Telnet, HTTP) sollten möglichst abgeschaltet werden. Ein administrativer Zugriff muss in jedem Fall über eine verschlüsselte Verbindung erfolgen (z. B. über SSL oder SSH).
- Die voreingestellte SSIDs, kryptographische Schlüssel oder Passwörter müssen gleich nach Inbetriebnahme geändert werden.
- Die SSID sollte keinen Hinweis auf den Inhaber oder den Zweck eines WLAN geben. Ebenso sollte die SSID nicht auf "Any" gesetzt sein, da sonst jede beliebige WLAN-Komponente an der Kommunikation teilnehmen kann.
- Der SSID-Broadcast sollte deaktiviert werden, damit die Existenz des WLAN nicht unnötig mitgeteilt wird. Ferner sollte die Assoziation via SSID-Broadcast deaktiviert sein, damit der Client explizit die gewünschte SSID bei der Assoziierung angeben muss.
- Es müssen geeignete Verschlüsselungsmechanismen aktiviert werden. Gleichzeitig muss sichergestellt sein, dass alle Komponenten im WLAN diese unterstützen. Es darf nicht möglich sein, mit WLAN-Komponenten Verbindungen aufzubauen, die keine oder nur unzureichende Verschlüsselungsmechanismen besitzen.
- Kryptographische Schlüssel sollten möglichst zufällig gewählt und regelmäßig gewechselt werden. Es sollte ein komplexer Pre-Shared Key (PSK) bei der Nutzung von WPA-PSK bzw. WPA2-PSK verwendet werden. Falls kryptographische Schlüssel wie der PSK über ein Passwort generiert wird, so sollte hierfür ein Passwort hoher Komplexität mit mindestens 20 Zeichen gewählt werden.
- Zur Einschränkung der zugelassenen Kommunikationspartner eines Access Point sollten Access Control Lists (ACLs) auf MAC-Adress-Ebene verwendet werden. Dies ist insbesondere bei kleinen bis sehr kleinen WLAN-Installationen hilfreich. Als alleiniges Instrument kann sie aber besonders im WLAN (durch die leichte Abhörbarkeit) im Allgemeinen nicht für ein ausreichendes Maß an Sicherheit sorgen, da MAC-Adressen einfach geändert werden können. ACLs im WLAN können daher nur als eine schwache, ergänzende Zusatzmaßnahme gesehen werden, deren Einsatz vor allem in speziellen Situationen sinnvoll ist. Da der Sicherheitsgewinn begrenzt ist, sollte in größeren Netzen abgewogen werden, ob der Sicherheitsgewinn den entstehenden Administrationsaufwand rechtfertigt.
- Der DHCP (Dynamic Host Configuration Protocol) Server im Access Point sollte, falls vorhanden und technisch möglich, abgeschaltet werden, d. h. es sollten statische IP-Adressen vergeben und der zulässige IP-

Adressraum möglichst klein gehalten werden. Der DHCP Server wird einem Eindringling andernfalls automatisch eine gültige IP-Adresse zuweisen.
- Beim Einsatz mehrerer Access-Points sind die benutzten Frequenzkanäle benachbarter Access-Points möglichst überlappungsfrei zu wählen.
- Änderungen an der Systemkonfiguration müssen getestet und dokumentiert werden.
- Es muss regelmäßig überprüft werden, ob alle sicherheitsrelevanten Updates und Patches eingespielt worden sind. Auch für die zugehörigen Gerätetreiber der WLAN-Hardware auf den WLAN-Clients ist dies zu berücksichtigen. Eine neue Software-Version oder ein Patch sollte erst nach einem angemessenen Test im WLAN eingespielt werden. Es ist in der Praxis schon vorgekommen, dass nach einen Software-Update die WLAN-Kommunikation nur noch eingeschränkt oder sogar gar nicht mehr möglich war.
  Es sollten Melde- und Informationsprozeduren im Änderungsmanagement spezifiziert werden, die beschreiben, wer und wie bei derartigen Änderungen zu informieren ist. Ebenso ist die Dokumentation der WLAN-Infrastruktur anzupassen.
- Wenn WLAN-Komponenten längere Zeit nicht benutzt werden, sollten sie abgeschaltet werden. Access Points sollten außerhalb der Arbeitszeiten (beispielsweise nachts und am Wochenende) automatisch deaktiviert werden.

Diese Aufgaben können durch den Einsatz einer WLAN-Management-Software und durch Einbindung in ein zentrales Netz-Management sinnvoll unterstützt und überwacht werden.

Prüffragen:

- Ist die SSID des Access Points so gewählt, dass kein Hinweis auf den Inhaber und den Verwendungszweck gegeben ist?
- Ist der SSID Broadcast deaktiviert?

# M 4.295 Sichere Konfiguration der WLAN-Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Damit WLANs sicher betrieben werden können, müssen auch alle damit gekoppelten Clients sicher konfiguriert sein. Geeignete Sicherheitsempfehlungen für Clients sind in den Bausteinen der Schicht 3 *IT-Systeme* beschrieben. Zusätzlich sollten folgende WLAN-spezifischen Sicherheitsmaßnahmen ergriffen werden:

- Voreingestellte SSIDs, kryptographische Schlüssel und Passwörter müssen direkt nach Inbetriebnahme geändert werden. Passwörter sollten so gewählt werden, dass sie nur schwer zu erraten sind.
- Der Ad-hoc-Modus sollte abgeschaltet werden, damit Clients nur über einen Access Point miteinander kommunizieren können, nicht direkt untereinander.
- Schutzbedürftige Daten auf mobilen Endgeräten sollten verschlüsselt werden. Hierfür gibt es eine Vielzahl hardware- oder softwarebasierender Produkte, die es erlauben, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte zu verschlüsseln, so dass nur diejenigen, die über eine Zugriffsberechtigung verfügen, die Daten entschlüsseln können.
- Die WLAN-Schnittstellen von Clients sollten generell deaktiviert sein, solange diese nicht tatsächlich genutzt werden. Vor allem sollte dies immer dann erfolgen, wenn die Clients in einem kabelgebundenen LAN angemeldet sind. Der Zugriff von einem Client auf das hausinterne LAN über die üblichen internen Anbindungen sollte also nur dann möglich sein, wenn keine WLAN-Aktivitäten erfolgen. Ansonsten bietet dies Angreifern die Möglichkeit, über die WLAN-Schnittstelle auf eventuell ins Hausnetz bestehende (und authentisierte) Verbindungen zuzugreifen.
- Beim Aufbau von VPN-Verbindungen sollte diverse Sicherheitsvoraussetzungen auf Client-Seite erfüllt sein. So sollte es nicht möglich sein, neben einer VPN-Verbindung andere Kommunikationsschnittstellen parallel zu nutzen, damit nicht über unsichere Kanäle die als sicher betrachtete VPN-Anbindungen ausgehöhlt wird. Außerdem ist es empfehlenswert, gewisse Mindest-Sicherheitsmaßnahmen bei den Clients nicht nur vorauszusetzen, sondern sie besser auch noch zu überprüfen, bevor ein Zugriff über VPN gestattet wird. Dafür empfehlen sich Tools, die die Einhaltung der Sicherheitsrichtlinien auf den Clients überprüfen, bevor der Server weitere Kommunikation erlaubt.
- Es muss regelmäßig überprüft werden, ob alle sicherheitsrelevanten Updates und Patches eingespielt worden sind. Das Einspielen eines größeren Software-Updates auf WLAN-Clients über das WLAN kann problematisch sein, da die Bandbreite im WLAN im Vergleich zum kabelbasierten LAN deutlich geringer ist. Die Installation eines Updates dauert damit nicht nur erheblich länger, sondern auch andere Nutzer des WLANs können spürbar behindert werden, da WLAN ein Shared Medium ist. Wenn möglich, sollte daher ein Client für die Installation eines größeren Software-Update an ein kabelbasiertes LAN angeschlossen werden. Ergänzend kann die Übertragung von Software Updates auf der Luftschnittstelle niedriger priorisiert werden, sofern die hierdurch verlängerte Installationszeit praktikabel ist. Auf diese Weise werden andere WLAN-Anwendung nicht mehr signifikant durch das Software-Update gestört.

Es sollte regelmäßig kontrolliert werden, dass sicherheitsrelevante Einstellungen nicht geändert worden sind.

Es muss klar geregelt werden, ob und unter welchen Rahmenbedingungen WLAN-Clients an fremden Netzen angemeldet werden dürfen (siehe M 4.251 *Arbeiten mit fremden IT-Systemen*), vor allem wenn diese Zugriff auf die Produktivumgebung haben oder auf diesen vertrauliche Informationen gespeichert sind.

WLAN-Clients sollten grundsätzlich nicht in unsicheren Umgebungen, wie z. B. öffentliche Hotspots oder nur durch WEP gesicherte WLANs, betrieben werden. WLAN-Clients, die Daten hohen Schutzbedarfs verarbeiten, dürfen nur in WLANs eingesetzt werden, die vollständig unter eigener Kontrolle betrieben werden und entsprechend sicher konfiguriert wurden. Die Nutzung in anderen WLANs ist zu untersagen.

Alle Benutzer von WLAN-Komponenten sollten über potentielle Risiken und Probleme bei der Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen informiert sein. Alle Benutzer müssen die Sicherheitsrichtlinie zur WLAN-Nutzung kennen (siehe M 2.382 *Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung*). Niemand sollte auf ein internes WLAN zugreifen dürfen, der nicht vorher den in der WLAN-Sicherheitsrichtlinie festgehaltenen Nutzungsbedingungen schriftlich zugestimmt hat.

Prüffragen:

- Ist der Ad-hoc-Modus an den WLAN-Clients generell abgeschaltet?
- Werden schutzbedürftige Daten auf mobilen Endgeräten verschlüsselt?
- Werden die WLAN-Schnittstellen nur dann aktiviert, wenn sie tatsächlich benötigt werden?
- Ist sichergestellt, dass bei bestehender VPN-Verbindung keine anderen Kommunikationsschnittstellen parallel genutzt werden können?
- Werden die WLAN-Clients regelmäßig mit allen sicherheitsrelevanten Updates und Patches versorgt?
- Erfolgt eine regelmäßige Prüfung, dass alle sicherheitsrelevanten Einstellungen an den WLAN-Clients nicht geändert worden sind?
- Existiert eine Regelung zur Anbindung von WLAN-Clients an fremde Access Points und Netze?
- Bei hohem Schutzbedarf an Vertraulichkeit: Existiert eine Regelung zur ausschließlichen Anbindung von WLAN-Clients an Access Points und Netze, die unter der vollen Kontrolle der Organisation stehen?

# M 4.296 Einsatz einer geeigneten WLAN-Management-Lösung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Damit bei allen WLAN-Komponenten eine aus Sicherheitssicht optimale Konfiguration gewährleistet ist, sollten diese sorgfältig administriert werden. Da die Administration bei großen WLANs aufwendig und komplex sein kann, ist der Einsatz von WLAN-Systemmanagement-Tools sinnvoll. Diese sollten möglichst auch in vorhandene IT- und Netzmanagement-Tools integriert werden können.

Generell ist die Realisierung einer Management-Lösung zu empfehlen, die neben einer Überwachung des WLAN auch eine Online-Dokumentation ermöglichen kann. Je nach Leistungsumfang sollte es folgende Möglichkeiten bieten:

- Dokumentation der Firmware-Stände der Access Points
- Dokumentation der Firmware-Stände und Treiber der WLAN-Adapter der WLAN-Clients
- Dokumentation der Sicherheitskonfigurationen
- Dokumentation von ortsspezifischen Konfigurationen
- Historienverwaltung von Konfigurationsänderungen

Damit die Administratoren einen Überblick über alle stationären und mobilen Systeme und Anwendungen erhalten, und dies möglichst einfach, sollte eine Systemmanagement-Lösung mobile Endgeräte und deren Anwendungen automatisch inventarisieren können. Jedes Endgerät sollte von der Management-Software in die Konfigurations- und Kontrollprozesse einbezogen werden, sobald es am Netz angemeldet wird. Die Nutzung dieser Funktionen richtet sich nach den Festlegungen im Betriebshandbuch.

Das Management-System sollte darüber hinaus über eine Alarm- und Fehlerbehandlung verfügen. Hierbei sollten folgende Aufgaben durch die Administratoren durchgeführt werden können:

- Auswertung und Bewertung von Alarmen, z. B. eine Häufung von fehlgeschlagenen Authentisierungsversuchen an einem Access Point
- Auswertung von Statistiken zur Fehlersuche
- Auslösung von Maßnahmen bei einem vermuteten Sicherheitsvorfall
- Anpassung von Schwellwerten zur Alarmauslösung an eine geänderte WLAN-Nutzung

Es sollte ein geeignetes Netzmanagement-Protokoll ausgewählt werden, beispielsweise SNMPv3 (siehe auch M 2.144 *Verwendung von SNMP als Netzmanagement-Protokoll*).

Die aufgezeichneten Protokolldaten sollten regelmäßig, spätestens einmal monatlich, ausgewertet werden. Der Umfang der Protokollierung ist mit der Personalvertretung und dem Datenschutzbeauftragten abzustimmen. Die WLAN-Management-Software bzw. die allgemeine Netz-Management-Lösung sollte Filtermöglichkeiten bieten, um die Protokolldaten besser auswerten zu können.

Prüffragen:

- Werden in der WLAN-Management-Lösung die Firmware-Stände der eingesetzten WLAN-Komponenten (Access Points, WLAN-Clients, etc.) nachgehalten?

- Werden in der WLAN-Management-Lösung neben den vorgenommenen Konfigurationen auch deren Änderungen dokumentiert?
- Existiert eine Regelung zur Einbeziehung von bestehenden und neuen WLAN-Endgeräten zur Durchsetzung von Konfigurations- und Kontrollprozessen?
- Stehen durch das Management-System Alarmierungsmöglichkeiten und Fehlerbehandlungen zur Verfügung?
- Erfolgt eine regelmäßige Auswertung der durchgeführten Protokolldaten?
- Wird der Umfang der Protokollierung mit der Personalvertretung und dem Datenschutzbeauftragten abgestimmt?

# M 4.297 Sicherer Betrieb der WLAN-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

WLANs sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Alle WLAN-Komponenten müssen so konfiguriert sein, dass sie so gut wie möglich gegen Angriffe geschützt sind. Solange WLAN-Komponenten nicht entsprechend konfiguriert sind, dürfen sie nicht aktiviert bzw. mit der Produktivumgebung gekoppelt werden.

Abzusichernde WLAN-Komponenten sind unter anderem die Access Points, das Distribution System, die WLAN-Clients, die Betriebssysteme, auf denen die WLAN-Komponenten betrieben werden, und die verwendeten Protokolle. Insbesondere sind folgende Punkte zu beachten:

- Für die Administration der verschiedenen WLAN-Komponenten müssen Verantwortliche benannt werden.
- Nach der Installation und Inbetriebnahme von WLAN-Komponenten müssen alle erforderlichen Sicherheitsmechanismen aktiviert werden.
- Die Administration der WLAN-Komponenten darf nur über eine sichere Verbindung erfolgen, d. h. die Administration sollte an der Konsole direkt, nach starker Authentisierung (bei Zugriff aus dem LAN) oder über eine verschlüsselte Verbindung (bei Zugriff aus dem Internet) erfolgen.
- Es muss die Regel "Alles was nicht ausdrücklich erlaubt ist, ist verboten" realisiert sein. So darf z. B. kein Benutzer, der nicht in einer Access-Liste eingetragen ist, auf das WLAN zugreifen. Die Vergabe von Zugriffsrechten auf Verzeichnisse und Dateien sollte so restriktiv wie möglich erfolgen.
- Es ist darauf zu achten, dass die eingesetzte Software immer auf einem aktuellen Stand ist und etwaige sicherheitsrelevante Patches unverzüglich aufgespielt werden.
- Konfigurationsänderungen sollten durch das System so protokolliert werden, dass Manipulationen zeitnah nachvollzogen werden können. Die Protokolldaten selber müssen so abgesichert werden, dass Manipulationen an ihnen ausgeschlossen sind.
- Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. Dazu gehören z. B. Versuche von unberechtigten Zugriffen und Daten zur Netzauslastung und -überlastung. Die aufgezeichneten Protokolldaten müssen regelmäßig ausgewertet werden. Der Umfang der Protokollierung ist mit der Personalvertretung und dem Datenschutzbeauftragten abzustimmen.
- Die WLAN-Komponenten müssen in das Datensicherungskonzept einbezogen werden. Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren WLAN-Betrieb relevante Dateien wie Access-Listen, Passwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

Es sollte möglichst eine Standard-Konfiguration für die eingesetzten WLAN-Komponenten ausgearbeitet werden, die die Vorgaben aus der WLAN-Sicherheitsrichtlinie wiederspiegelt. Dies erleichtert bei einer Vielzahl zu betreuender Geräte außerdem das Einspielen von Änderungen. Ebenso lassen sich hierüber Abweichungen von der Soll-Konfiguration schneller feststellen.

Sinnvoll ist der Einsatz einer WLAN-Management-Lösung, die für eine effiziente Konfiguration der Access Points sorgt. Access Points und die aktiven

Komponenten des Distribution System sollten weiterhin in das Netz-Management-System eingebunden und überwacht werden können. Schließlich sollte auch die Verfügbarkeit der Authentisierungsserver über das Management-System geprüft werden können. Gegebenenfalls bietet sich die Erweiterung eines bereits genutzten Netz-Management-Systems um ein WLAN-Management-Modul an.

Der Anschluss von fremden Access Points oder Manipulationen an den Switches des Distribution Systems sollte durch das WLAN-Management-System erkannt werden. Der betroffene Netz-Port des Distribution Switch sollte in einem solchen Fall umgehend gesperrt werden.

Ebenso sollte die Konfiguration der Access Points und des Distribution Systems regelmäßig geprüft werden. Hierzu muss die aktuell vorgefundene Systemkonfiguration gegen eine dokumentierte und validierte Konfiguration geprüft werden. Bei nicht bestätigten Änderungen müssen die Systeme untersucht und gegebenenfalls sogar abgeschaltet und geprüft werden, ob ein Angriff vorliegt.

Für den sicheren Betrieb der WLAN-Komponenten ist sowohl die Grund-Konfiguration, die aufbauend auf der WLAN-Sicherheitsrichtlinie festgelegt wurde, als auch alle durchgeführten Änderungen sorgfältig zu dokumentieren, um diese jederzeit nachvollziehbar zu machen. Neben der Dokumentation der Sicherheitskonfigurationen gehört auch die Dokumentation der Firmware-Stände der Access Points und die Dokumentation von ortsspezifischen Konfigurationen.

Prüffragen:

- Erfolgt die Administration der WLAN-Komponenten ausschließlich über vertrauenswürdige Pfade?
- Sind die Zugriffsmöglichkeiten auf die WLAN-Komponenten auf das erforderliche Maß begrenzt?
- Sind die WLAN-Komponenten in das Datensicherungskonzept mit einbezogen?
- Ist sichergestellt, dass beim Wiedereinspielen von gesicherten Datenbeständen die aktuellste Version herangezogen wird?
- Wird die Verfügbarkeit des Authentisierungsservers über das Management-System geprüft?
- Wird der Anschluss fremder Access Points oder Manipulationen an den Switches des Distribution Systems durch das WLAN-Management-System erkannt?

# M 4.298 Regelmäßige Audits der WLAN-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei allen Komponenten der WLAN-Infrastruktur muss regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und ob diese korrekt konfiguriert sind. Neben den Access Points zählen hierzu die Komponenten des Distribution Systems, die Elemente der Sicherheitsinfrastruktur (inklusive der Authentisierungsserver) und die Elemente des WLAN-Management-Systems. Das WLAN-Management-System sollte je nach bereitgestelltem Funktionsumfang nicht nur die aktuelle Konfigurationen der Access Points, sondern auch die der Komponenten des Distribution Systems verwalten und über eine Historienverwaltung auch vorhergehende Konfigurationen führen (siehe M 4.296 *Einsatz einer geeigneten WLAN-Management-Lösung*). Ebenso sollten zentrale Sicherheitssysteme, wie der Authentisierungsserver oder das Koppelelement am Übergangspunkt zwischen Distribution System und LAN, regelmäßigen Sicherheitsüberprüfungen unterzogen werden.

Insbesondere für Installationen in öffentlich zugänglichen Bereichen sollte eine stichprobenartige Prüfung im Hinblick auf gewaltsame Öffnungsversuche oder Manipulationsversuche (speziell für Access Points) durchgeführt werden. Ein Indiz für eine Kompromittierung des WLAN ist zum Beispiel ein zwischen Access Point und Distribution Switch geschalteter Hub. Derartige zu Diagnosezwecken erfolgte Aufbauten dürfen nur autorisiertem Personal zugänglich sein und sind nach Ende der Messungen umgehend zu entfernen.

Weiterhin müssen die WLAN-Clients regelmäßig überprüft werden. Bei einer größeren Anzahl sollte dies zumindest stichprobenweise geschehen. Zu prüfen ist zunächst die Konfiguration von WLAN-Adapter und IEEE 802.1X Supplicant (bzw. VPN-Client, falls im WLAN genutzt). Weiterhin ist systemabhängig auch der Patch Level der Betriebssysteme, die Aktualität der Treibers für die WLAN-Adapter der Clients, die Regelbasis der Personal Firewalls, die Aktualität des verwendeten Virenschutzes sowie die Sicherheitseinstellungen der über das WLAN genutzten Anwendungen zu.

Falls Unregelmäßigkeiten oder Schwachstellen festgestellt werden, müssen diese dokumentiert werden, hierbei muss auch festgehalten werden, wie diese verfolgt werden.

Neben den regelmäßigen Audits der einzelnen WLAN-Komponenten sollte auch regelmäßig eine Revision der WLAN-Sicherheitsrichtlinie durchgeführt werden. Insbesondere sollte eine Bewertung erfolgen, ob die ergriffenen Maßnahmen zur Absicherung des WLANs noch dem Stand der Technik entsprechen und ob der zu Grunde gelegte Schutzbedarf nach wie vor gültig ist.

Außerdem sollte immer wieder hinterfragt werden, ob alle Benutzer über die erforderlichen WLAN-Sicherheitsmaßnahmen informiert sind und diese umsetzen.

Prüffragen:

- Existiert eine Regelung zur Historienverwaltung der einzelnen Konfigurationen von WLAN-Komponenten?
- Existiert eine Regelung zur Sichtprüfung der öffentlich zugänglichen WLAN-Komponenten?

- Wird der tatsächliche Software-Stand und die tatsächliche Konfiguration durch regelmäßige Audits der WLAN-Clients überprüft?
- Existiert eine Regelung Unregelmäßigkeiten und Schwachstellen im WLAN-Bereich zu dokumentieren und zu beheben?
- Erfolgt eine regelmäßige Revision der WLAN-Sicherheitsrichtlinie?
- Existiert eine Regelung zur kontinuierlichen Bewertung des Schutzbedarfs einzelner Komponenten und gekoppelter Netze der WLAN-Infrastruktur?
- Existiert eine Regelung zur kontinuierlichen Bewertung der eingesetzten Algorithmen und Verfahren zur Absicherung des WLAN nach dem Stand der Technik?

# M 4.299 Authentisierung bei Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Im normalen Büroalltag ist es oft einfach, Ausdrucke vertraulicher Dokumente direkt am Drucker einzusehen, da diese noch nicht abgeholt wurden. Daher müssen Maßnahmen ergriffen werden, die den Zugriff auf fremde Dokumente erschweren.

Generell sollten nur berechtigte Personen Zugriff auf die ausgedruckten oder kopierten Dokumente erhalten. Der Kreis der berechtigten Personen ist so klein wie möglich zu halten.

Kann der Zugang zu einem Netzdrucker nicht beschränkt werden, sollte überlegt werden, Geräte einzusetzen, die eine Authentisierungsfunktion für Benutzer bieten. Ist diese Funktion aktiviert, wird das Dokument erst ausgedruckt, nachdem sich der Benutzer, der den entsprechenden Druckauftrag abgesendet hat, am Gerät identifiziert und authentisiert hat. In der Praxis werden zur Authentisierung häufig Chipkarten oder PINs verwendet. Dabei können PINs je nach Gerätetyp benutzer- oder dokumentenspezifisch festgelegt werden. Bei letzterer Variante wird erst beim Absenden des Druckauftrags eine PIN festgelegt. Erst nachdem diese PIN am Gerät eingegeben wurde, wird das Dokument, das der PIN zugeordnet ist, ausgedruckt. Druckaufträge, die zwar abgesendet, aber nicht abgeholt wurden, müssen regelmäßig gelöscht werden. Die Drucker sollten möglichst so konfiguriert werden, dass bei mehrmaliger Eingabe einer falschen PIN der Druckauftrag automatisch gelöscht wird.

Ein weiterer Sicherheitsgewinn kann erzielt werden, wenn das zu druckende Dokument vom Arbeitsplatz-PC verschlüsselt zum Drucker übertragen und verschlüsselt zwischengespeichert wird. Erst nach einer erfolgreichen Authentisierung direkt am Drucker wird das Dokument entschlüsselt und ausgedruckt.

Es gibt auch Kopierer, die eine ähnliche Authentisierungsfunktion bieten, meist als optionale Erweiterung. Erst nachdem eine Chipkarte eingelesen oder eine PIN eingegeben wurde, können die Benutzer kopieren. Obwohl diese Authentisierungsfunktionen hauptsächlich für Kostenabrechnungen angeboten werden, erschweren diese Erweiterungen außerdem die Erstellung von Kopien durch Unbekannte.

Wenn an Netzdruckern oder Kopierern häufig hoch-vertrauliche Dokumente gedruckt beziehungsweise vervielfältigt werden müssen, sollte überlegt werden, hierfür Geräte mit Authentisierungsmöglichkeit einzusetzen.

Prüffragen:

- Wird verhindert, dass unberechtigte Personen Zugriff auf die Ausdrucke erhalten?
- Gibt es Kontrollmechanismen, um zu verhindern, dass Dokumente unberechtigt kopiert werden?

# M 4.300 Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Damit ein Ausdruck erstellt werden kann, müssen die erforderlichen Informationen vom Arbeitsplatzrechner zum Drucker übertragen werden. Bei Kopierern findet die Übertragung im Allgemeinen intern zwischen Scannereinheit und Speicher statt. Ein Angreifer könnte versuchen, auf den Speicher zuzugreifen oder die Informationen bei der Übertragung zum Drucker abzuhören.

Als Zwischenspeicher für die temporäre Ablage der zu druckenden Informationen werden bei größeren Geräten häufig Festplatten verwendet. Je nach Konfiguration werden die Informationen im Zwischenspeicher nicht nur temporär, sondern permanent gespeichert. Es sollte gewährleistet werden, dass die Informationen nach dem Ausdruck aus dem Zwischenspeicher gelöscht werden. Hierfür besitzen viele Kopierer eine Löschfunktion. Alle Benutzer müssen darauf hingewiesen werden, diese Funktion auch konsequent zu benutzen (siehe M 2.398 *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*).

Falls häufig Informationen mit einem höheren Schutzbedarf ausgedruckt oder kopiert werden, ist zu beachten, dass einfaches Löschen nicht ausreicht, um das Wiederherstellen der gelöschten Daten zu verhindern. Einige Geräte besitzen hierfür Mechanismen zum "sicheren Löschen". Hierbei handelt es sich um eine Löschfunktion mit zusätzlichem Überschreiben. Falls eine solche Funktion vorhanden ist, muss sie zu aktiviert werden. Anderenfalls müssen adäquate Alternativlösungen gefunden werden.

Wenn möglich, sollten Maßnahmen ergriffen werden, die einem Angreifer den physischen Zugriff auf den Speicher bzw. das Ausbauen der Festplatten erschweren. Um erkennen zu können, ob versucht wurde, den internen Speicher auszubauen oder zu manipulieren, sollten die Geräte versiegelt werden. Generell sollten Drucker und Kopierer so aufgestellt werden, dass sich niemand unbeobachtet an ihnen zu schaffen machen kann.

Als zusätzlicher Schutz wird empfohlen, die Informationen in den internen Speichern verschlüsselt zu speichern. Zahlreiche Drucker und Kopierer bieten diese Funktion an. Wenn das eingesetzte Gerät eine verschlüsselte Speicherung unterstützt, sollte diese Funktion aktiviert werden.

Die Kommunikation zwischen Arbeitsplatzrechnern, Druckservern und Netzdruckern erfolgt meist über ein Datennetz, für das die gleichen Gefährdungen wie bei anderen Datenverbindungen zu beachten sind. Damit diese Kommunikation nicht abgehört werden kann, sollten daher die Druckaufträge möglichst verschlüsselt übertragen werden.

Einige Druck-Protokolle, wie das besonders bei Unix-Systemen weit verbreitete LPR/LPD-Protokoll (Line Printer Remote / Line Printer Daemon), unterstützen keine Verschlüsselung. Ähnlich ist die Situation bei SMB/CIFS (Server Message Block / Common Internet File System) unter Windows.

Daher sollte ein Protokoll wie IPP (Internet Printing Protocol) gewählt werden, das eine Verschlüsselung unterstützt, beispielsweise TLS/SSL (Transport Layer Security / Secure Sockets Layer) in Verbindung mit IPP.

Unter Unix-Systemen sollte beispielsweise das Common Unix Printing System (CUPS) eingesetzt werden, das bei neueren Versionen in der Voreinstellung zur Kommunikation zwischen Client und Druckserver das Protokoll IPP verwendet. Durch eine entsprechende Konfiguration kann dabei TLS/SSL aktiviert werden.

Prüffragen:

- Unterstützen die Netzdrucker bzw. Kopierer das verschlüsselte Abspeichern von Informationen und wurden dieses aktiviert?
- Werden die Speicher von Druckern, Kopierern und Multifunktionsgeräten vom Benutzer beziehungsweise automatisch nach dem Ausdrucken gelöscht?
- Werden die Druckaufträge bei der Übertragung geschützt?
- Wurden Maßnahmen ergriffen, die den Ausbau der internen Speicherkomponenten von Druckern und Kopierern erschweren?

# M 4.301 Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um Angriffe auf Drucker, Kopierer und Multifunktionsgeräte zu erschweren, muss der Zugriff auf diese Geräte beschränkt werden. Im Folgenden werden einige Aspekte beschrieben, die für den sicheren Betrieb von Druckern und Kopierern berücksichtigt werden sollten:

- Beschränkung auf notwendige Zugriffsrechte
  Wenn möglich, sollten nur so wenig Administratoren wie nötig den vollständigen Zugriff erhalten. Dabei sollten immer nur die Zugriffsrechte vergeben werden, die für die Aufgabenwahrnehmung notwendig sind (siehe M 2.8 *Vergabe von Zugriffsrechten*).
- Absicherung der Administrationszugriffe:
  Auf administrative Bereiche und die Konfiguration sollten nur autorisierte Personen zugreifen dürfen. Der Zugriff sollte erst nach einer Authentikation, beispielsweise durch Eingabe eines Passwortes oder einer PIN, möglich sein. Falls Drucker, Kopierer oder Multifunktionsgeräte über ein Netz administriert werden, muss sichergestellt sein, dass sich die Administratoren hierfür ebenfalls authentisieren müssen. Wenn systemseitig keine Authentikation unterstützt wird, müssen geeignete Ersatzmaßnahmen ergriffen werden.
- Absicherung der Administration bei Fernzugriff:
  Alle Administrationszugriffe sollten möglichst nur über einen verschlüsselten Kanal stattfinden, damit keine Passwörter oder andere schutzbedürftige Informationen mitgehört werden können. Beispielsweise kann bei einigen Gerätetypen die Übertragung der Konfigurationsdaten über HTTPS oder SNMPv3 verschlüsselt werden. In diesem Fall sollte die unverschlüsselte Kommunikation unterbunden werden, indem beispielsweise die HTTP-Schnittstelle für die Konfiguration deaktiviert wird.
- Verzicht auf nicht benötigte Funktionen:
  Auch Drucker, Kopierer und Multifunktionsgeräte bieten im allgemeinen mehr Funktionen, als im normalen Betrieb benötigt werden. Dadurch können sich unnötige Risiken ergeben. Daher sollten alle nicht benötigten Funktionen deaktiviert bzw. deren Nutzung so weit wie möglich eingeschränkt werden.
- Paketfilter:
  In einigen Druckern sind Paketfilter integriert, über die Verbindungen anhand von IP-Adressen oder Portnummern gefiltert werden können. Alle Ports, die nicht für den Druckbetrieb und zur Konfiguration des Druckers benötigt werden, sind möglichst zu blockieren. Unterstützt das Gerät eine verschlüsselte Kommunikation, sollte die unverschlüsselte Kommunikation mit dem Gerät so weit wie möglich unterbunden werden, beispielsweise über die entsprechenden Portnummern.
  Werden Druckserver eingesetzt, ist darauf zu achten, dass nur von diesen Servern eine Verbindung zu den Druckern aufgebaut werden darf. Hierdurch wird der Verbindungsaufbau von unautorisierten IT-Systemen zu den Druckern erschwert. Eine Ausnahme bilden allerdings Systeme, von denen aus Drucker konfiguriert werden sollen. Diese Systeme müssen natürlich ebenfalls auf den Drucker zugreifen können.
  Die Paketfilter sind generell so restriktiv wie möglich zu konfigurieren. Dies gilt auch für den Verbindungsaufbau von den Netzdruckern zu anderen

IT-Systemen. Beispielsweise sollten die Paketfilter so konfiguriert werden, dass Netzdrucker keine Verbindungen zu einem IT-System außerhalb des LANs aufbauen können. Dies erschwert den ungewollten Datenaustausch mit externen IT-Systemen, beispielsweise mit Computern im Internet. Unabhängig von lokalen Paketfiltern muss am zentralen Sicherheitsgateway die Kommunikation zwischen den Druckern und externen Netzen blockiert werden.

- Netzsegmentierung:
  Oft ist es empfehlenswert, alle Drucker, Kopierer und Multifunktionsgeräte in einem logischen Netz zusammenzufassen. Dies erleichtert in vielen Fällen die Konfiguration und Administration. Wird dies konsequent umgesetzt, kann auf den zuständigen Routern und Gateways die Kommunikation zwischen den Druckern und anderen Netzsegmenten gezielt kontrolliert werden (sowohl Empfang als auch Versand von IP-Paketen).

Prüffragen:

- Wird der Zugriff auf die Konfiguration von Druckern, Kopierern und Multifunktionsgeräten geschützt?
- Wird die Fernkonfiguration von Druckern, Kopierern und Multifunktionsgeräten durch eine Authentisierung und eine verschlüsselte Verbindung geschützt?
- Wurden alle nicht benötigten Funktionen von Druckern, Kopierern und Multifunktionsgeräten abgeschaltet?

# M 4.302 Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Aktivitäten an Druckern, Kopierern und Multifunktionsgeräten sollten aus vielen Gründen überwacht und protokolliert werden. Zum Einen hilft eine aktivierte Protokollierung, potentielle Schwachstellen möglichst frühzeitig zu erkennen und zu beseitigen. Zum Anderen dient die Protokollierung dazu, Verstöße gegen die Sicherheitsrichtlinie zu erkennen (siehe M 2.398 *Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten*) oder Nachforschungen über einen Sicherheitsvorfall anzustellen. Außerdem kann die Überwachung meist auch genutzt werden, um frühzeitig zu erkennen, ob Verbrauchsmaterialien nachgefüllt werden müssen.

Folgende zentrale Fragen sollten im Rahmen der Protokollierung an Druckern, Kopierern und Multifunktionsgeräten mindestens beantwortet werden:

- Welche Informationen sollen protokolliert werden?
- Wie soll protokolliert werden?
- Wer ist berechtigt bzw. zuständig, die Protokolle auszuwerten?
- Wie und wann werden die Protokolle ausgewertet?
- Wer soll wie beim Eintreten bestimmter Ereignisse benachrichtigt werden?
- Wie lange müssen und dürfen die Protokolldaten aufbewahrt werden und wie erfolgt die Löschung?

Es muss sorgfältig ausgewählt werden, welche Informationen protokolliert werden sollen. Werden zu viele Informationen gespeichert, kann es passieren, dass bei der Auswertung wichtige Ereignisse übersehen werden. Wird zu wenig protokolliert, kann es passieren, dass wichtige Informationen nicht erfasst werden.

Aus Sicherheitssicht haben sich die folgenden Ereignisse als besonders relevant für die Protokollierung erwiesen, die Aufzählung ist dabei absteigend nach der Priorität sortiert:

- Änderungen der Konfigurationseinstellungen sind immer zu protokollieren.
- Es sollten fehlgeschlagene und bei einem höheren Schutzbedarf zusätzlich auch erfolgreiche Authentisierungsvorgänge protokolliert werden. Dies betrifft sowohl lokale Anmeldungen als auch Zugriffe über das Netz.
- Die Systemressourcen und Messwerte zur Betriebssicherheit sind immer auf kritische Werte hin zu überwachen. Hierzu gehören beispielsweise Informationen über die Temperatur, die Auslastung und den freien Speicherplatz.
- Um Engpässe bei der Versorgung zu vermeiden, sollten Informationen zum Verbrauch von Papier und Toner protokolliert und ausgewertet werden.
- Einträge, wer zu welcher Uhrzeit gedruckt oder das Gerät benutzt hat, können eventuell ebenfalls aufgezeichnet werden.

Je nach Gerät und Anwendungsfall kann es zweckmäßig sein, bei der Festlegung des Protokollierungsumfangs von diesen Ereignissen abzuweichen oder zusätzliche Ereignisse zu betrachten, beispielsweise das Einschalten und Ausschalten des Geräts. Der Protokollierungsumfang hängt in der Praxis

auch davon ab, inwieweit der jeweilige Gerätetyp die Protokollierung der unterschiedlichen Ereignisse technisch unterstützt.

Nachdem festgelegt wurde, welche Informationen protokolliert werden sollen, muss geklärt werden, wo die Protokolldaten abgelegt werden. Falls möglich, sollten hierfür zentrale Protokollierungsserver genutzt werden. Ansonsten müssen die Protokolldateien lokal auf den einzelnen Geräten gespeichert werden.

Für die Protokollierung bei vernetzten IT-Systemen sollte eine Zeitsynchronisation eingesetzt werden. Dies dient dazu, die Ereignisse zuverlässig mit den zu protokollierenden Informationen von anderen Systemen vergleichen zu können (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*).

Protokolldaten müssen nicht nur gespeichert, sondern auch systematisch ausgewertet werden. Auch hierfür muss festgelegt werden, wer zuständig ist und welche Vorgehensweise einzuhalten ist. Empfehlungen dazu finden sich unter anderem in M 2.64 *Kontrolle der Protokolldateien*.

Wenn unerwartete oder auffällige Ereignisse in den Protokollen auftreten, muss entsprechend hierauf reagiert werden. Eine Vielzahl fehlerhafter Authentisierungsversuche kann beispielsweise auf einen Angriff oder auf nicht ausreichend informierte Benutzer hindeuten. Aber auch normale Ereignisse können eine Reaktion erforderlich machen. Erreichen beispielsweise Verbrauchsmaterialien einen minimalen Füllstand, muss rechtzeitig für Ersatz gesorgt werden. Daher sollte der zuständige Administrator beziehungsweise Verantwortliche für die Verbrauchsmaterialen zeitnah informiert werden.

Sofern personenbezogene Daten archiviert werden, müssen die hierfür geltenden Gesetze und Vorschriften eingehalten werden. Dazu gehören vor allem das Bundesdatenschutzgesetz (BDSG) und die entsprechenden Gesetze der Länder. Weitere Informationen hierzu sind in M 2.110 *Datenschutzaspekte bei der Protokollierung* zu finden.

Prüffragen:

- Werden die Aktivitäten auf Druckern, Kopierern und Multifunktionsgeräten geeignet protokolliert?
- Werden bei der Auswertung Datenschutzaspekte berücksichtigt?
- Wird sichergestellt, dass alle Geräte eine korrekte Systemzeit haben?

# M 4.303 Einsatz von netzfähigen Dokumentenscannern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Über Dokumentenscanner können analoge Informationen digitalisiert werden, beispielsweise um ein Papierdokument auf IT-Systeme zu kopieren, zu archivieren oder weiter zu bearbeiten. Statt an jedem Arbeitsplatz-PC einen lokalen Scanner zu installieren, ist es besonders bei einer seltenen Nutzung solcher Geräte meist wirtschaftlicher, einen oder mehrere zentrale Scanner zur Verfügung zu stellen. Um geeignete Sicherheitsmaßnahmen auszuwählen, muss zwischen Scan-PCs und netzfähigen Dokumentenscannern unterschieden werden.

Ein Scan-PC ist ein Standard-PC, der im Allgemeinen an ein LAN angebunden ist und an den ein lokaler Scanner angeschlossen ist. Scan-PCs werden häufig in ähnlichen Räumlichkeiten wie Netzdrucker betrieben und können von diversen Benutzern bei Bedarf genutzt werden. Außerdem ist auf Scan-PCs üblicherweise auch die zur Nachbearbeitung der eingescannten Informationen erforderliche Software installiert, also beispielsweise OCR- oder Bildbearbeitungsprogramme.

Netzfähige Dokumentenscanner ("Büroscanner") sind Kompaktgeräte, an denen Papierdokumente und ähnliches ohne größeren Aufwand eingelesen und zur weiteren Bearbeitung über ein LAN an den Benutzer übertragen werden können, beispielsweise per E-Mail. Diese Funktion ist häufig auch in Faxgeräten integriert. Der Funktionsumfang von netzfähigen Dokumentenscannern ist meist deutlich geringer als bei Scan-PCs. Im Allgemeinen können nur einfache Papierdokumente in Standard-Formaten eingelesen werden, eine Nachbereitung direkt am Gerät ist meist nicht möglich.

### Scan-PC

Wird ein Standard-PC zum Scannen verwendet, so sind die Empfehlungen aus den zutreffenden Client-Bausteinen der Schicht 3 der IT-Grundschutz-Kataloge umzusetzen.

Scan-PCs können im Produktivnetz, in einem Testnetz oder auch als Stand-Alone-System ohne einen Netzanschluss betrieben werden. Sie sollten so konfiguriert sein, dass sich die Benutzer authentisieren müssen. Die eingescannten Daten können über das Netz oder über transportable Datenträger zu den Arbeitsplatz-PCs übertragen werden.

Die analogen Scan-Vorlagen (Papier, Folien etc.) sollten nicht unbeaufsichtigt beim Gerät verbleiben. Auch die digitalen Scan-Ergebnisse sollten nach der Übertragung auf das gewünschte Zielsystem, zum Beispiel auf den Arbeitsplatz-PC des jeweiligen Benutzers, aus allen allgemein zugreifbaren Verzeichnissen gelöscht werden.

### Netzfähige Dokumentenscanner

Mit diesen Kompaktgeräten können auch ohne einen angeschlossenen PC Dokumente gescannt werden. Dabei werden die Dokumente in Bild-Dateien mit gängigen Dateiformaten umgewandelt.

Zur weiteren Bearbeitung müssen die Geräte die eingescannten Dokumente an andere IT-Systeme im Netz versenden. Folgende Übertragungs- und Speicherverfahren werden in der Regel unterstützt:

- Ablage auf Netzlaufwerke.
  Die eingescannten Dokumente werden direkt über ein Netzprotokoll auf einen Datei-Server übertragen. Unterstützt werden in der Regel NFS- und SMB-Freigaben oder die Übertragung mittels FTP. Grundsätzlich muss sichergestellt werden, dass der Personenkreis, der Zugriff auf die Zielverzeichnisse mit den eingescannten Daten hat, so klein wie möglich ist. Bei erhöhtem Schutzbedarf ist es unter Umständen erforderlich, dass nur der Benutzer, der die Informationen eingescannt hat, auch auf die Scan-Ergebnisse zugreifen kann. Nicht alle Scanner ermöglichen es, die erzeugten Dateien in benutzerspezifischen Bereichen der Server zu speichern. Wenn hierfür nur ein allgemein zugreifbares Verzeichnis gewählt werden kann, müssen die Dokumente so schnell wie möglich aus diesen öffentlichen Verzeichnissen gelöscht werden. Die Benutzer müssen entsprechend angewiesen werden. Zusätzlich sollten diese Verzeichnisse einmal täglich automatisch gelöscht werden. Der Zeitpunkt der Löschung muss den Benutzern bekannt gegeben werden und ist so zu wählen, dass zu diesen Zeiten keine Benutzer mit den Scannern arbeiten.
- Scan-to-Mail:
  Hierbei hat der Benutzer beim Scannen die Möglichkeit, eine E-Mail-Adresse oder eine Benutzer-Kennung, der eine E-Mail-Adresse zugeordnet ist, anzugeben. An diese E-Mail-Adresse wird die erzeugte Datei über einen voreingestellten SMTP-Server übermittelt. Da auf diese Weise vertrauliche Informationen anonym das Netz verlassen könnten, sollte darauf geachtet werden, dass keine externen E-Mail-Adressen eingegeben werden können. Besser ist es, auch den SMTP-Server so zu konfigurieren, dass von den netzfähigen Dokumentenscannern keine E-Mails an externe E-Mail-Adressen versendet werden können.
- Scan-to-Print:
  Hier wird das Dokument direkt an einen Drucker gesendet, also die Scanner-Drucker-Kombination als digitaler Kopierer eingesetzt. Sind beide Geräte räumlich voneinander getrennt, besteht die Gefahr, dass während des Scannens die Dokumente unbefugt vom Drucker entfernt werden. Daher sollten die Systeme in diesem Fall möglichst so konfiguriert werden, dass der Ausdruck erst erfolgt, wenn alle Seiten des jeweiligen Dokuments vollständig eingescannt sind. Anderenfalls vergeht zwischen dem Scannen der ersten Seite und dem Abholen am Drucker unter Umständen zu viel Zeit.
- Scan-to-Fax:
  Das Verfahren Scan-to-Fax erlaubt es, eingescannte Dokumente direkt per Fax zu versenden. Hierfür wird beim Scannen eine Fax-Nummer angegeben. Das erzeugte Dokument wird dann entweder über ein integriertes Modem versendet, oder der Scanner baut über das LAN eine Verbindung zu einem Fax-Server auf.
  Beim Einsatz von Scannern, die über eingebaute Fax-, Modem- oder DFÜ-Schnittstellen verfügen, müssen besondere Sicherheitsvorkehrungen getroffen werden, damit über diese Schnittstellen keine unerwünschten Kommunikationsverbindungen mit externen Netzen aufgebaut werden. Entsprechende Empfehlungen sind in der Maßnahme M 5.146 *Netztrennung beim Einsatz von Multifunktionsgeräten* beschrieben.
  Wenn möglich, sollte ein zentraler Fax-Server als Schnittstelle zwischen Scanner und Telefonnetz agieren. In diesem Fall sind insbesondere die Maßnahmen-Empfehlungen, die im Baustein B 5.6 *Faxserver* aufgeführt sind, anzuwenden.

Wenn die eingesetzten Komponenten dies unterstützen, sollten die Kommunikationsverbindungen möglichst verschlüsselt werden, um das Abhören der übertragenen Informationen zu erschweren. Hinweise, wie die Übertragung geschützt werden kann, sind unter anderem auch in der Maßnahme M 4.300 *Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten* zu finden.

Scanner sollten auch vor Angriffen aus dem Netz geschützt werden. Hierfür sollte die Maßnahme M 4.301 *Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte* sinngemäß berücksichtigt werden.

Nach dem Scannen dürfen keine Restinformationen auf dem System verbleiben. Die Dokumentenspeicher des Geräts sollten möglichst automatisch gelöscht werden, wenn der Scan-Vorgang abgeschlossen ist. Ist dies nicht realisierbar, müssen die Benutzer darauf hingewiesen werden, dass sie die Dokumentenspeicher des Geräts nach der Benutzung manuell löschen müssen, damit nachfolgende Benutzer die eingescannten Informationen nicht einsehen können. Entsprechende Sicherheitsvorkehrungen müssen auch für sonstige Speicherbereiche getroffen werden, die im Rahmen des Scan-Vorgangs verwendet werden, beispielsweise für die dabei benutzten Netzlaufwerke.

Prüffragen:

- Können nur berechtigte Personen auf die digitalisierten Dokumente zugreifen?
- Ist sichergestellt, dass die gescannten Informationen sicher zum Arbeitsplatz-PC übertragen werden?
- Werden alle Speicherbereiche des Scanners nach der Benutzung gelöscht?

# M 4.304 Verwaltung von Druckern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Behörden und Unternehmen benötigen im Allgemeinen eine Vielzahl von Druckern und ähnlichen Geräten für die unterschiedlichen Einsatzzwecke. Hierfür müssen geeignete Drucksysteme ausgewählt und die Aufstellung der Hardware-Komponenten, wie Drucker und Kopierer, festgelegt werden.

Im Folgenden werden typische Drucksysteme, deren Bestandteile und Kommunikationsbeziehungen vorgestellt. Drucksysteme bestehen in der Regel aus Client- und Server-seitigen Software-Komponenten.

**Drucksysteme**

In den seltensten Fällen sendet eine Anwendung den Druckauftrag direkt an einen Drucker, sondern zwischen der Anwendung und dem Drucker wird ein Drucksystem betrieben. Hierbei ist es oft erforderlich, dass diese Drucksysteme netzfähig sind und mehrere Clients auf einen Drucker zugreifen können. Auch bei einer ausschließlich lokalen Installation wird ein Drucksystem benötigt. Hierbei sendet der Client intern den Druckauftrag an den Druckserver.

Ein Drucksystem kann unter anderem folgende Aufgaben erfüllen:

- Annahme des Druckauftrags von der Anwendung,
- Verwaltung der Druckaufträge in einer Warteliste (Spooling),
- Ergänzung um zusätzliche Informationen, wie Trennseiten,
- Anpassungen für das Papierformat oder andere Eigenschaften,
- Umwandlung in ein dem Drucker verständliches Datenformat, wie PostScript oder PCL,
- Verwaltung von logischen und physischen Druckern,
- Benutzerverwaltung und
- Protokollierung.

Es gibt mehrere Ansätze für Drucksysteme, wobei die verschiedenen Betriebssysteme unterschiedliche Ansätze favorisieren. Besonders bei heterogenen IT-Landschaften ist die Kompatibilität der Drucksysteme untereinander von entscheidendem Vorteil. Viele Systeme bieten Schnittstellen zu anderen Drucksystemen. Dadurch kann beispielsweise ein Unix-System auf einen Drucker zugreifen, der von einem Windows-System verwaltet wird.

Abhängig vom Betriebssystem sind folgende Drucksysteme am weitesten verbreitet:

- Berkeley Printing System,
- Common Unix Printing System (CUPS) und
- Druckerfreigaben auf der Basis von SMB unter Windows.

Bei heterogenen Netzlandschaften ist möglichst ein Drucksystem auszuwählen, das von allen Betriebssystemen unterstützt wird. Als Alternative kann es zweckmäßig sein, mehrere verschiedene Drucksysteme einzusetzen, die unter Umständen untereinander kommunizieren können. Die Entscheidung über die zu nutzenden Drucksysteme ist zu begründen und zu dokumentieren.

**Bestandteile**

Der Druckauftrag, der von einer Anwendung erstellt wurde und an einen Drucker ausgegeben werden soll, muss mehrere Zwischenschritte durchlau-

fen. Für diese Schritte sind jeweils einzelne Komponenten zuständig, die im folgenden vorgestellt werden.

- **Druckclient**
  Bei einem Druckclient handelt es sich um eine Softwarekomponente, die auf dem Arbeitsplatz-PC installiert ist. In der Regel empfängt der Druckclient eine entsprechende Anweisung von einer Anwendung und sendet den Druckauftrag an den Druckserver weiter.
  Mit der Auswahl eines Druckernamens kann in vielen Fällen der Zieldrucker ausgewählt werden. Eine Ausnahme ist der Ausdruck in Druckerpools, bei denen für jeden Druckauftrag ein anderer Drucker vom Druckserver bestimmt werden kann.
  Häufig können weitere Funktionen, wie Duplexdruck und Heften, durch den Druckclient festgelegt werden. Hierfür sendet der Druckclient die Druck-Daten an den Druckserver. Wie der Drucker angesteuert werden kann und welche Formate er beherrscht, wird in der Regel bei der Installation des Druckers dem Drucksystem bekannt gemacht.
- **Druckserver**
  Der Druckserver empfängt die Druckaufträge der Clients und verwaltet sie. Die Aufträge werden in eine Warteliste eingefügt und anschließend an den Drucker übertragen. Je nach Konfiguration wird bei mehreren Druckaufträgen das zuerst empfangene Dokument als erstes an den Drucker weitergeleitet oder durch eine entsprechende Priorität bevorzugt behandelt. In einigen Fällen können auch spezielle Zeiträume für die Ausführung der Druckaufträge festgelegt werden.
  Das Dokument wird in der Regel direkt auf dem Druckserver aufbereitet. Für die Aufbereitung benötigt das Drucksystem die gerätespezifischen Druckerinformationen und Filter. Beispielsweise können diese Druckerinformationen als PPD (PostScript Printer Description) definiert sein. Verallgemeinert handelt es sich dabei um eine Spezifikation, welche Formate und Funktionen vom Drucker beherrscht werden. Beispiele für die spezifizierten Parameter sind Papierformate, Rasterauflösungen, Schriftarten, Duplex, Heften, Lochen und Farbdruck. Anhand dieser Spezifikation kann die Druckanweisung, die an den Drucker übermittelt wird, generiert werden.
  Zur Aufbereitung des Druckauftrags gehört auch die Konvertierung in ein Datenformat, das vom jeweiligen Drucker unterstützt wird. Ist das Eingangsformat beispielsweise PostScript, muss das Dokument in ein für diesen Drucker verständliches Ausgangsformat konvertiert werden, wenn der Drucker nicht PostScript-fähig ist. Beispiele für Ausgangsformate sind PDF, PCL und PostScript.
- **Drucker**
  Der Drucker empfängt das vorbereitete Dokument vom Druckserver und gibt es aus. Es kann zwischen logischen und physischen Druckern unterschieden werden. Folgende Anschlussarten werden in der Praxis für physische Drucker eingesetzt:

  - Lokale Drucker: Diese Drucker verfügen über eine serielle, parallele oder USB-Schnittstelle und werden direkt an ein Client-System angeschlossen.
  - Netzdrucker: Der Drucker wird über ein Netz angesprochen.
  - Druckserver mit lokalen Druckern: Der Drucker wird lokal an einen Druckserver, der über einen Netzanschluss verfügt, angeschlossen. Dabei kann der Druckserver in Form einer Appliance oder als klassischer Server realisiert sein. Bei diesem Ansatz hat der Druckserver häufig die Funktion einer Konvertierung zwischen Netz und lokalem Anschluss, beispielsweise als USB-Ethernet-Bridge.

Logische Drucker können innerhalb des Drucksystems unterschiedliche Aufgaben haben. Die folgenden Szenarien sind in der Praxis häufig anzutreffen:

- Mehrere physische Drucker werden über einen logischen Drucker angesprochen. Neben dem Vorteil einer höheren Druckleistung (es kann parallel gedruckt werden), kann bei dem Ausfall eines Druckers ohne größeren Konfigurationsaufwand auf einen anderen Drucker zugegriffen werden. Es wird empfohlen, nur Geräte mit ähnlichen Eigenschaften in einer Klasse zusammenzufassen.
- Ein physischer Drucker wird von mehreren logischen Druckern, die jeweils auf unterschiedlichen Druckservern installiert sind, angesprochen. Dieser Fall bietet sich an, wenn mehrere Druckserver eingesetzt werden. Beim Ausfall eines Druckservers kann der Druckbetrieb durch den Wechsel auf einen anderen Druckserver ohne größeren Konfigurationsaufwand fortgesetzt werden.
- Im Weiterem können logische Drucker verwendet werden, um für einen physischen Drucker mit mehreren verschiedenen Einstellungen jeweils einen eigenen Druckernamen zuzuordnen. Beispielsweise können für einen physischen Drucker zwei logische Drucker definiert werden: einer für Simplex- und einer für Duplex-Druck. Alle logischen Drucker sind zu dokumentieren.

**Kommunikationsbeziehungen**

Wie in der folgenden Abbildung verdeutlicht, entstehen zwischen den einzelnen Komponenten eines Drucksystems unterschiedliche Kommunikationsverbindungen.

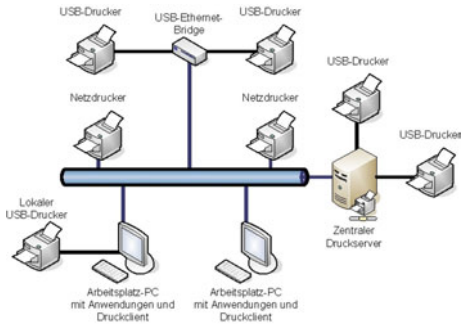



Abbildung: Druckerarchitektur mit Druckclients, Druckservern, lokalen und netzbasierten Druckern

- **Kommunikation zwischen Druckclient und Druckserver**
  Diese Kommunikationsverbindung kann zwischen einem Druckclient und dem Druckserver sowie zwischen verschiedenen Druckservern aufgebaut werden. Je nach Szenario werden die Druckinformationen über ein Netz oder lokal (Druckclient und Druckserver befinden sich auf einem Gerät) ausgetauscht.
  Je nach Drucksystem können folgende Protokolle eingesetzt werden:

  - HTTP (Hypertext Transfer Protocol),
  - IPP (Internet Printing Protocol),
  - LPR/LPD (Line Printer Remote / Line Printer Daemon),
  - SMB (Server Message Block) und
  - Appletalk beziehungsweise Bonjour.

  Abhängig von den eingesetzten Druckern und vom gewählten Drucksystem sind geeignete Protokolle auszuwählen. Innerhalb eines Netzes soll-

ten möglichst wenig unterschiedliche Druck-Protokolle eingesetzt werden. Die Entscheidung ist zu dokumentieren.
Auch für die Verwaltung müssen bei einigen Drucksystemen Informationen ausgetauscht werden. Die Clients müssen beispielsweise regelmäßig über die verfügbaren Drucker und deren Status informiert werden. Dabei können, je nach Drucksystem, folgende Strategie verfolgt werden:

- Broadcasting: In regelmäßigen Anständen sendet der Server unaufgefordert eine Nachricht an alle Clients in der Broadcast-Domäne.
- Polling: Der Druckclient fragt die Informationen vom Server ab.

Broadcasting vereinfacht die Administration, ist aber mit weiteren Problemen verbunden. Befinden sich die Clients und Server in verschiedenen Broadcast-Domänen, erreichen die Pakete nicht alle Clients. In der Praxis können auch Probleme auftreten, wenn der Druckserver mehrere Netzschnittstellen hat und die Broadcast-Pakete an die falschen Schnittstellen sendet. Für die Konfiguration ist ein Verfahren auszuwählen und zu dokumentieren.

- **Kommunikation zwischen Druckserver und Drucker**
  Für die Kommunikation mit den Druckern werden ebenfalls entsprechende Protokolle benötigt. Diese hängen von den Druckerspezifikationen und von der Anschlussart ab. Beispielsweise gibt es Protokolle für

  - die Kommunikation über die parallele Schnittstelle,
  - den Anschluss über USB,
  - den Betrieb über die serielle Schnittstelle und
  - die netzbasierte Kommunikation mit den Druckern, beispielsweise über das HP JetDirect Protokoll oder über IPP (Internet Printing Protocol).

  Einige Druckersysteme ermöglichen auch die Konfiguration der Drucker über den Druckserver. Neben proprietären Protokollen wird hier oft das Simple Network Management Protocol (SNMP) eingesetzt.
  Es müssen Protokolle ausgewählt werden, die für die Anforderungen der Institution und für die einzusetzenden Komponenten geeignet sind. Die Entscheidungen sind zu dokumentieren.

**Design der Druckerlandschaft**

Neben der Auswahl des Drucksystems spielt die Anordnung der einzelnen Bestandteile, wie Clients, Server und Drucker, eine wichtige Rolle. Grob können folgende Ansätze für die Druckerarchitektur unterschieden werden:

- Lokale Drucker: Sowohl die Anwendung, die den Druckauftrag generiert, als auch der Druckserver und der Druckclient werden gemeinsam auf einem IT-System betrieben. Der Drucker ist über die USB-, Parallele oder Serielle Schnittstelle an das IT-System angeschlossen.
- Arbeitsplatz-PC mit Netz-Drucker: Auf einem oder mehreren IT-Systemen befinden sich neben der sendenden Anwendung auch der Druckclient und der Druckserver. Die Druckserver der einzelnen IT-Systeme senden die Druckaufträge an einen netzfähigen Drucker.
- Zentraler Druckserver: Auf den Arbeitsplatzsystemen sind nur die Druckclients installiert. Diese nehmen den Druckauftrag an und leiten ihn über ein Netz an einen zentralen Druckserver weiter.
  Auf diesem Druckserver werden die Druckaufträge verwaltet. Der Druckserver sendet die Aufträge an lokale oder netzbasierte Drucker weiter, wo sie ausgegeben werden.
- Kombinationen: Es sind zahlreiche Kombinationen aus den oben genannten Anordnungen möglich. Ein Beispiel ist der Anschluss eines lokalen

Druckers am Arbeitsplatz-PC für kleinere Druckaufträge und der parallele Betrieb eines zentralen Druckservers für umfangreiche Ausdrucke.

Die getroffenen Entscheidungen zum Aufbau der Druckerlandschaft sind zu dokumentieren.

# M 4.305 Einsatz von Speicherbeschränkungen (Quotas)

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Auch wenn bei der Beschaffung eines IT-Systems darauf geachtet wurde, dass dieses genügend Speicherplatz bietet, wird in vielen Fällen bei längerer Nutzung der Speicherplatz früher oder später knapp. Auf IT-Systemen, die von verschiedenen Benutzern genutzt werden, müssen die vorhandenen Ressourcen daher so aufgeteilt werden, dass alle Benutzer möglichst optimal arbeiten können.

Häufig lässt sich das Phänomen beobachten, dass die Benutzer mehr Speicherplatz haben möchten, als ihnen zur Verfügung steht. Neben dem ständig wachsenden Speicherplatzbedarf von Anwendungen ist ein anderer Grund hierfür, dass sich viele Benutzer nur ungern von alten und unbenötigten Dateien trennen. Werden keine Regelungen zur Speicherplatz-Begrenzung und zur Archivierung getroffen, besteht die Gefahr, dass Speicherplatz für große Mengen an Altdaten verschwendet wird oder die Benutzerverzeichnisse überlaufen.

Eine einfache Lösung wäre es, bei steigender Nachfrage grundsätzlich immer mehr Speicherplatz als benötigt bereitzustellen. Dies ist allerdings in der Praxis nicht immer machbar.

Für Benutzer oder Benutzergruppen, aber auch für Anwendungen kann durch Disk Quotas ein Speichervolumen festgelegt werden, das nicht überschritten werden darf. Auf Servern und allen IT-Systemen, die von mehreren Benutzern bzw. Anwendungen konkurrierend benutzt werden, sollte daher der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen durch Disk Quotas beschränkt werden. Hierzu gehören Server (z. B. Datei-, Web- und Mailserver) und Clients mit mehreren Benutzerkonten. Für Clients, auf denen die Daten- von der Systempartition getrennt ist und die nur von einem Benutzer genutzt werden, kann auf eine Disk Quota verzichtet werden.

Dabei ist die Wahl des Quota-Volumens wichtig. Sollen alle Benutzer das gleiche Quota-Volumen erhalten, kann das erforderliche Volumen errechnet werden, indem der zu nutzende Speicherplatz durch die Anzahl der Benutzer dividiert wird. Zusätzlich sollte aber eine Speicherplatz-Reserve eingeplant werden. Problematisch ist die Wahl einer zu kleinen Disk Quota. Steht den Benutzern zu wenig Speicherplatz zur Verfügung, könnten sie versuchen, die Informationen außerhalb der vorgesehenen Verzeichnisse abzulegen, um die Restriktionen zu umgehen. Hierfür werden dann häufig Speicherorte verwendet, die dafür nicht geeignet sind, z. B. temporäre Verzeichnisse oder andere für alle Benutzer beschreibbare Verzeichnisse. Wenn der Speicherplatz auf Dateiservern zu knapp bemessen ist, weichen Benutzer oft auf lokale Festplatten aus. Dies verstößt in vielen Fällen gegen die Regelungen und kann beispielsweise dazu führen, dass die Dateien nicht in die zentrale Datensicherung (Backup) einbezogen werden.

Es sollte einerseits festgelegt werden, welche Informationen wo abgespeichert werden sollen und auch, wie viele Versionen einer Datei wie lange auf dem Produktivsystem gespeichert werden sollen.

Datenbestände aus abgeschlossenen Projekten sollten geordnet archiviert und nicht "für alle Fälle" auf den Produktivsystemen vorrätig gehalten werden. Andererseits sollte festgelegt werden, wie viel Speicherplatz den verschiedenen Benutzergruppen und Anwendungen zur Verfügung gestellt wird. Zusätzlich sollte eine Reserve eingeplant werden. Es muss auch festgelegt werden, wie den Benutzern bei Bedarf ein höheres Speichervolumen zugeteilt werden kann. Die festgesetzten Werte müssen dokumentiert werden. Außerdem müssen sie regelmäßig überprüft und aktualisiert werden.

Wurde die Größe der Disk Quota bestimmt, sollte überlegt werden, ob und wie auf einen höheren Bedarf an Speicherplatz reagiert werden soll. Diese Entscheidung wird durch die Auswahl eines Quota-Typs beeinflusst. Bei Hard Quotas werden feste Obergrenzen gesetzt, so dass die Benutzer nicht die Möglichkeit haben, mehr als das ihnen zugewiesene Speicherkontingent zu nutzen. Eine Soft Quota hingegen ermöglicht es den Benutzern, für eine festgelegte Zeitspanne und bis zu einer festgelegten Grenze die Disk Quota zu überschreiten. Wird die Disk Quota überschritten, muss mindestens der Benutzer hierüber informiert werden, beispielsweise per E-Mail. Es sollte überlegt werden, ebenfalls den Administrator zu benachrichtigen, damit er auf eventuell eintretende Probleme reagieren kann. Zusätzlich muss festgelegt werden, ob und wie einzelnen Benutzern zusätzlicher Speicherplatz zugeteilt werden kann. Dies sollte ein geregeltes und nachvollziehbares Verfahren sein. Disk Quotas sollten nicht "auf Zuruf" erhöht werden.

Bei vielen gängigen Betriebssystemen werden Hilfsmittel mitgeliefert, um Disk Quotas einzurichten. Es sollte aber geprüft werden, ob zusätzliche Software zur Einrichtung und Verwaltung einer Disk Quota benötigt wird.

Prüffragen:

- Existiert eine Regelung zur Speicherplatz-Begrenzung und zur Archivierung von Benutzer- und Anwendungsdaten?

# M 4.306 Umgang mit Passwort-Speicher-Tools

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, IT-Sicherheitsbeauftragter

Die meisten Menschen müssen sich sowohl im Arbeitsleben als auch privat eine Vielzahl von Passwörtern, PINs und anderen Authentikationsgeheimnissen merken. Dies führt immer wieder zu Problemen. Typische Beispiele dafür sind, dass Benutzer ihre Passwörter vergessen, so dass diese in aufwendigen Prozessen zurückgesetzt werden müssen, oder dass sie sie notieren und unsicher verwahren.

Um solche Probleme zu vermeiden, werden als technische Hilfsmittel Produkte angeboten, mit denen eine Vielzahl von Passwörtern, PINs und anderen Authentikationsgeheimnissen verwaltet werden können. Solche Passwort-Speicher-Tools, auch "Passwort-Safes" genannt, sind sowohl als reine Software-Lösungen als auch in Kombination mit eigenständiger Hardware erhältlich. Beim Einsatz von Passwort-Speicher-Tools sind diverse Aspekte zu beachten (siehe auch M 2.22 *Hinterlegen des Passwortes*):

Eine Hinterlegung oder Speicherung von Passwörtern ist immer mit organisatorischem Aufwand verbunden. Bei jeder Änderung eines der gespeicherten Passwörter ist dieses auch im Passwort-Speicher-Tool zu aktualisieren. Es darf kein Passwort dabei vergessen werden.

Bevor ein Passwort-Speicher-Tool eingesetzt wird, ist der Schutzbedarf der Passwörter abzuschätzen, die damit gespeichert werden sollen. Nicht alle Passwort-Tools eignen sich zur Speicherung hochschutzbedürftiger Passwörter. Andererseits unterstützen sie Benutzer darin, für jede Anwendung unterschiedliche und trotzdem möglichst komplexe Passwörter auszuwählen.

Wenn ein Tool zur Speicherung von Passwörtern benutzt werden soll, sind die im Folgenden beschriebenen Anforderungen an solche Werkzeuge zu beachten.

- Es darf nicht möglich sein, dass Unbefugte auf die gespeicherten Passwörter Zugriff nehmen. Jeder Zugriff auf das Passwort-Speicher-Tool sollte protokolliert werden.
- Ein Passwort-Speicher-Tool sollte einfach und intuitiv zu bedienen sein. Es sollte keine Einschränkungen bei der Länge und der Zeichenzusammensetzung der sicher hinterlegten Passwörter geben. Es sollte möglich sein, lange und komplexe Master-Passwörter zu benutzen, dies sollte möglichst auch technisch gefordert werden.
- Ein Passwort-Speicher-Tool darf auf keinen Fall die Möglichkeit bieten, dass Benutzer sich ohne Eingabe eines Master-Passwortes anmelden können oder dass das Master-Passwort vom Tool automatisch "vorgemerkt" werden kann.
- Nach einem vorgegebenen Inaktivitäts-Zeitraum sollte das Tool den angemeldeten Benutzer automatisch abmelden.
- Passwörter dürfen nur verschlüsselt gespeichert werden. Dafür muss ein anerkanntes Verschlüsselungsverfahren mit ausreichender Schlüssellänge gewählt worden sein.
- Vor der Beschaffung eines Passwort-Tools sollte in Fachzeitschriften und in Internet-Foren nachgeforscht werden, ob dort Erfahrungsberichte, Tests oder sogar Beschreibungen über erfolgreiche Angriffe auf die in Frage kommenden Tools zu finden sind. Ebenso sollte dort regelmäßig nachge-

prüft werden, dass bei den eingesetzten Tools keine Sicherheitslücken bekannt geworden sind.
- Leider gab und gibt es immer wieder Tools zur Passwort-Speicherung, bei denen schwerwiegende Sicherheitsmängel festgestellt wurden. Beispielsweise wurden Master-Passwörter im Klartext im Arbeitsspeicher abgelegt oder in der Zwischenablage gespeichert. Daher sollten möglichst nur sicherheitsüberprüfte Passwort-Tools eingesetzt werden (siehe M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*).
- Da der Zugriff auf Passwort-Speicher-Tools sehr gut abgesichert sein muss, kann es sinnvoll sein, Produkte mit spezieller Sicherheitshardware einzusetzen. Dies können z. B. Passwort-Tools auf USB-Token oder Chipkarte sein.
- Als Schutz vor Keyloggern kann es auch sinnvoll sein, ein Passwort-Tool einzusetzen, bei der die Passwörter über eine mausgesteuerten Bildschirm-Tastatur eingegeben werden. Diese sollte einerseits sowohl Zahlen, als auch Buchstaben und Sonderzeichen anbieten, damit möglichst vielfältige Passwörter ausgewählt werden können. Andererseits sollten die Zeichen dynamisch in der Bildschirmtastatur angezeigt werden, also die Zeichen nach jeder Eingabe an einer anderen Stelle angeordnet sein. Dies macht zwar für die Benutzer die Eingabe langsamer, erschwert aber, dass Schadsoftware anhand der Zeichenposition auf dem Bildschirm das Passwort mitlesen kann.
- Die Eingabe des Master-Passwortes sollte schnell und einfach möglich sein. Vor allem bei Passwort-Speicher-Tools mit integrierten Eingabetasten und bei der Nutzung von Bildschirm-Tastaturen sollte das Verfahren zur Eingabe des Master-Passwortes genau geprüft werden. Wenn hier die Eingabe zu lange dauert, beispielsweise weil einzelne Zeichen umständlich ausgewählt werden müssen, kann das Master-Passwort sehr leicht ausgespäht werden und die Akzeptanz seitens der Benutzer ist gefährdet.
- Sollte ein Passwort-Speicher-Tool mit einer externen Stromversorgung, z. B. über eine Batterie, verwendet werden, ist zu überprüfen, was nach einem Ausfall der Stromversorgung mit den Passwörtern geschieht. Eventuell sind dann zusätzliche Datensicherungen notwendig, die ebenfalls ausreichend geschützt werden müssen.

Außerdem sind beim Einsatz von Tools zur Speicherung von Passwörtern unter anderem folgende Rahmenbedingungen zu beachten:

- Der Zugriff auf Passwort-Speicher-Tools muss selbst wieder durch eine erfolgreiche Anmeldung freigegeben werden. Auch hierfür werden im Allgemeinen Passwörter oder PINs benutzt. An deren Qualität sollten natürlich höchste Ansprüche gelegt werden. Hierfür benutzte Master-Passwörter müssen lang und abwechslungsreich sein (siehe M 2.11 *Regelung des Passwortgebrauchs*).
- Erfolglose Anmeldeversuche sollten mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt werden. Insbesondere darf bei erfolglosen Anmeldeversuchen nicht erkennbar sein, ob der eingegebene Benutzername oder das eingegebene Passwort (oder beides) falsch ist. Nach drei aufeinander folgenden fehlerhaften Passworteingaben für dasselbe Benutzerkonto sollte das Authentisierungssystem den Zugang für das jeweilige Benutzerkonto sperren (für eine bestimmte Zeitspanne oder dauerhaft). Die Sperrung eines Benutzerkontos darf bei nachfolgenden erfolglosen Anmeldeversuchen ebenfalls nicht erkennbar sein, sondern sollte dem jeweiligen Benutzer auf separatem Weg mitgeteilt werden.
- Noch besser ist es, bei erfolglosen Anmeldeversuchen keine Fehlermeldung, sondern eine übliche Benutzeroberfläche anzuzeigen. Wenn dann im folgenden echt aussehende, aber nutzlose Ergebnisse angezeigt wer-

den, kann ein Angreifer nicht direkt erkennen, dass es sich bei dem angezeigten Passwort nicht um das korrekte handelt.
- Passwort-Tools sollten möglichst nur auf vertrauenswürdigen IT-Systemen benutzt werden, also solchen IT-Systemen, die unter der eigenen Aufsicht bzw. unter der Kontrolle der eigenen Institution stehen. Dies können beispielsweise Mobiltelefone, PDAs oder spezielle Authentisierungsserver sein.
- Externe webbasierte Dienstleistungen zur Passwort-Speicherung sollten nur dann benutzt werden, wenn die Zuverlässigkeit des Dienstleisters in einem angemessenen Verhältnis zum Schutzbedarf der Passwörter steht. In jedem Fall sollten hier nicht alle Kreditkartendaten inklusive PIN hinterlegt werden, da es schwierig ist, die Zuverlässigkeit und Sicherheit einer solchen Dienstleistung zu überprüfen.
- Es dürfen nur auf ihre Sicherheit überprüfte und in der Institution freigegebene Passwort-Tools eingesetzt werden.

In der Institution sollten alle Mitarbeiter darauf hingewiesen werden, ob Passwort-Speicher-Tools genutzt werden dürfen. Wenn dies der Fall ist, sind die hierfür freigegebenen Tools bekannt zu geben. Es sollte dann außerdem eine Regelung geben, in der beschrieben ist, welche Arten von Passwörtern damit gespeichert werden dürfen und welche Rahmenbedingungen dabei eingehalten werden müssen.

Prüffragen:

- Wird vor dem Einsatz eines Passwort-Speicher-Tools geprüft, ob sich der Einsatz mit dem Schutzbedarf der zu speichernden Passwörter vereinbaren lässt?
- Bietet das ausgewählte Passwort-Speicher-Tool eine ausreichende Zugriffskontrolle und eine verschlüsselte Speicherung?
- Falls der Einsatz von Passwort-Speicher-Tools in der Organisation genehmigt ist: Ist den Benutzern bekannt, welche Tools eingesetzt werden dürfen?
- Falls der Einsatz von Passwort-Speicher-Tools in der Organisation genehmigt ist: Ist geregelt, welche Arten von Passwörtern mit dem Tool gespeichert werden dürfen?

# M 4.307 Sichere Konfiguration von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem ein Verzeichnisdienst vollständig installiert ist (siehe M 4.308 *Sichere Installation von Verzeichnisdiensten*), sollte er sich in einem sicheren Zustand befinden, so dass in der anschließenden Konfigurationsphase nur berechtigte Administratoren auf den Verzeichnisdienst zugreifen können.

Die nachfolgende Konfiguration des Verzeichnisdienstes kann je nach Einsatzszenario um eine Vielzahl von Funktionen erweitert werden, die über einen reinen Verzeichnisdienst hinausgehen. Dabei ist die Sicherheit der verschiedenen Funktion durch geeignete Parameter bei der Konfiguration zu gewährleisten.

Typische Konfigurationsaufgaben bei Verzeichnisdiensten sind:

- Konfiguration der Verzeichnisbaumhierarchie,
- Konfiguration der Objekt-Zugriffsrechte,
- Konfiguration der Vererbungsfilter,
- Konfiguration der Administrationsrollen,
- Konfiguration der Delegation von Administrationsaufgaben,
- Konfiguration der Benutzer und der Benutzergruppen,
- Verteilung der Schlüssel-Objekte,
- Konfiguration des Client-Zugriffs auf den Verzeichnisdienst,
- Konfiguration der Partitionierung der Verzeichnisdatenbank,
- Konfiguration der Replikation des Verzeichnisdienstes,
- Konfiguration der Schnittstelle zur Synchronisation mit fremden Verzeichnisdiensten,
- Konfiguration der Systemüberwachung.

Dies alles betrifft originär die Verzeichnisdienst-Software. Es darf jedoch nicht vergessen werden, dass auch das zugrunde liegende Betriebssystem sicher konfiguriert werden muss, insbesondere was den Serverzugriff, die Netzanbindung und das Dateisystem betrifft.

Die Konfiguration von Verzeichnisdiensten kann um eine Vielzahl weiterer Module erweitert werden, deren Funktionen über einen reinen Verzeichnisdienst hinausgehen. Dazu gehören:

- Das LDAP-Servermodul, das einen Zugriff auf die Benutzerinformationen für LDAP-Clients erlaubt,
- das Tool, welches den administrativen Zugriff über einen Web-Browser gestattet,
- die Konsole (das Werkzeug) als Administrationsplattform des Verzeichnisdienstes,
- der Zertifikatsserver, der bei der Erstinstallation eines Verzeichnisdienst-Servers innerhalb eines Baums installiert wird und
- eventuell weitere eingesetzte Zusatzmodule.

Je nach Einsatzszenario und dem vom Verzeichnisdienst-Server angebotenen Funktionsumfang muss überprüft werden, welche Zusatzmodule für den Betrieb des Verzeichnisdienstes benötigt werden und genutzt werden sollen. Nicht genutzte Module sollten nicht installiert werden, da jedes installierte Modul bei Fehlkonfiguration Sicherheitsprobleme verursachen kann.

Für jedes aktivierte Modul muss eine entsprechende Sicherheitsplanung durchgeführt werden. Anschließend ist diese durch geeignete Konfigurationsparameter umzusetzen (siehe auch M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*).

Die Sicherheit eines Verzeichnisdienst-Systems hängt außerdem von der Sicherheit der zum Zugriff benutzten Clientsoftware ab. Daher müssen für die sichere Konfiguration eines Verzeichnisdienst-Systems auch die client-seitigen Rechner und Programme einbezogen werden. Besondere Schutzmaßnahmen sind für die administrativen Zugänge zum Verzeichnisdienst zu realisieren.

Die folgenden, generischen Hinweise sollten in jedem Fall beachtet werden:

- Zur Absicherung der jeweiligen Client-Installation sind die relevanten Bausteine der IT-Grundschutz-Kataloge für das jeweilige zugrunde liegende Betriebssystem anzuwenden.
- Soll die Clientsoftware zum Verzeichnisdienst eine mittels SSL geschützte LDAP-Verbindung aufbauen, muss der Client ein entsprechendes Wurzelzertifikat erhalten, anhand dessen er die Authentizität des SSL-Serverzertifikats überprüfen kann.
- Die Sicherheit der Verzeichnisdienst-Installation hängt auch von der Integrität der zur Administration verwendeten Clients ab. Die Absicherung dieser Clients ist daher besonders wichtig.

Es ist auch möglich, eigene Clientsoftware zu erstellen, die mit dem Verzeichnisdienst über die standardisierte LDAP-Schnittstelle (oder andere dafür vorgesehene Schnittstellen) kommuniziert.

Ein Verzeichnisdienst-System besteht in der Regel nicht nur aus einem Verzeichnisdienst-Server, sondern aus einem ganzen Serververbund (siehe auch M 2.403 *Planung des Einsatzes von Verzeichnisdiensten*). Die Verzeichnisdatenbank kann dabei in Form von einzelnen Partitionen auf verschiedene Server verteilt werden. Weiterhin können die einzelnen Server die Verzeichnisdatenbanken untereinander replizieren. Dadurch, dass mehrere Kopien einer Datenbank-Partition auf unterschiedlichen Servern vorliegen, kann eine Lastverteilung erreicht werden. Damit die Aktualität der Verzeichniskopien sichergestellt ist, müssen Veränderungen an den Daten zwischen den Servern ausgetauscht werden. Es muss daher ein Replikationskonzept erstellt werden. Unter anderem sind dabei folgende Aspekte zu berücksichtigen:

- Werden die Verzeichnisdienst-Server im Master-Slave-Modus betrieben oder ist eine Multi-Master-Replikation realisiert?
- Welche Replikationstypen werden konfiguriert?
- Auf welche Server soll der Verzeichnisdienst repliziert werden?
- Welche Informationen des Verzeichnisdienstes sollen repliziert werden (Definition von Filtern)?
- Sollen Änderungen an Replikaten des Verzeichnisdienstes erlaubt sein und sollen diese auf das Original übertragen werden (Definition als Typ Read/Write oder als Read-Only)?

Da ein System in der Regel ständig Veränderungen durch den laufenden Betrieb unterworfen ist, muss auch die Sicherheit permanent überprüft und neu konfiguriert werden. Hinweise dazu finden sich in M 4.311 *Sicherer Betrieb von Verzeichnisdiensten*.

Prüffragen:

- Sind alle Verzeichnisdienst-Server gemäß der ihnen zugedachten Rolle sicher konfiguriert?

- Wurden bei der Konfiguration auch die client-seitigen Rechner und Programme einbezogen?

# M 4.308 Sichere Installation von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem alle Rahmenbedingungen zum Einsatz eines Verzeichnisdienstes geplant wurden (siehe M 2.403 *Planung des Einsatzes von Verzeichnisdiensten*), müssen die Verzeichnisdienst-Komponenten auf den relevanten Servern und Clients installiert werden. Während der Installationsphase ist ein Verzeichnisdienst-Server nicht vollständig konfiguriert, so dass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Es empfiehlt sich daher, die erstmalige Konfiguration entweder in einer geschützten Umgebung durchzuführen oder alternativ eine vorbereitete Standardkonfiguration aufzuspielen. Es sollte allerdings nie die ausgelieferte Standardkonfiguration des Herstellers innerhalb eines Produktivnetzes in Betrieb genommen werden, da diese erfahrungsgemäß keine angemessene Betriebssicherheit bieten.

Gleiches gilt auch, wenn der Verzeichnisdienst aufgrund einer Migration (siehe M 2.408 *Planung der Migration von Verzeichnisdiensten*) aktualisiert oder neu installiert werden muss.

Bei der Installation eines Verzeichnisdienst-Servers in einen bereits bestehenden Verzeichnisbaum muss dessen genauer Kontext spezifiziert werden. Eine spätere Verschiebung des Servers innerhalb des Baums ist nur mit größerem Aufwand zu bewerkstelligen.

Während der Installation werden auch die lokalen Sicherheitseinstellungen erstmalig konfiguriert. Die wichtigsten Grundeinstellungen beziehen sich auf

- die Definition des Verzeichnisdienst-Baums,
- die Verzeichnisdienst-Zugriffsberechtigungen,
- die Verzeichnisdienst-Vererbungseinstellungen und
- die Sicherheitseinstellungen für den LDAP-Zugriff.

Während der Installation lassen sich diese Einstellungen zum Teil vorgeben, ein Teil wird jedoch zunächst mit Standardwerten initialisiert. Eventuell sind einige Einstellungen ohne verschlüsselten Zugang durchzuführen, bevor ein durch SSL geschützter LDAP-Zugriff verwendet werden kann. Je nachdem, welche Verzeichnisdienst-Module zum Einsatz kommen, ist für jedes Modul eine sichere Installationskonfiguration einzurichten, die den Zugriff verhindert, solange sich der Server in der erstmaligen Konfigurationsphase befindet und bis die festgelegten Sicherheitsrichtlinien umgesetzt worden sind. Weitere Empfehlungen hierzu finden sich in M 4.307 *Sichere Konfiguration von Verzeichnisdiensten*.

Generell ist bei der Installation aus Sicherheitssicht Folgendes zu beachten:

- Die Zugriffsrechte für Verzeichnisdienst-Objekte bei Systemen, die von Vorgängerversionen aktualisiert bzw. von anderen Verzeichnissystemen übernommen wurden, müssen aktualisiert werden.
- Upgrade-Mechanismen können die Standardeinstellungen verändern, z. B. durch die Einbeziehung eines anderen Verzeichnisdienstes in eine vorhandene Verzeichnisdienst-Struktur.
- Soll ein neuer Server in einen existierenden Verzeichnisdienst-Baum aufgenommen werden, so erlaubt es der implizite Vererbungsmechanismus, die erstmalige Konfiguration deutlich abzukürzen. Hierbei ist kritisch zu

prüfen, ob durch den Vererbungsmechanismus ungewollte Einstellungen vorgenommen wurden, die zu Sicherheitslecks führen.
- Bei der Installation der Verzeichnisdienst-Server ist besondere Sorgfalt erforderlich, da diese im späteren Betrieb schützenswerte Daten speichern.

Verzeichnisdienst-Server dürfen nur auf Servern installiert und betrieben werden, die sich in einer physikalisch sicheren Umgebung befinden, z. B. einem Serverraum oder einem Serverschrank. Dies gilt vor allem für Verzeichnisdienst-Server, auf denen besonders schützenswerte Daten abgelegt sind.

Prüffragen:

- Befinden sich die Verzeichnisdienst-Server in einer physikalisch geschützten Umgebung?
- Existiert ein Konzept, welche Administrations- und Zugriffsberechtigungen bei der Installation in den Sicherheitseinstellungen des Verzeichnisdienstes konfiguriert werden müssen?
- Sind die Zugriffsrechte für Verzeichnisdienst-Objekte bei Systemen, die von Vorgängerversionen aktualisiert beziehungsweise von anderen Verzeichnissystemen übernommen wurden, ebenfalls aktualisiert worden?

# M 4.309 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Verzeichnisdienst speichert in der Regel sehr viele schützenswerte Informationen einer Institution wie beispielsweise Benutzerdaten. Es ist deshalb unerlässlich, diese Informationen nur ausdrücklich autorisierten Applikationen, Benutzern und Administratoren zugänglich zu machen. Dazu ist es notwendig, eine zuvor erstellte Sicherheitsrichtlinie, die Regelungen für die Zugriffsberechtigungen enthalten muss (siehe M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*), konsequent und konsistent umzusetzen.

Die Rechtevergabe erfolgt in der Regel über Access Control Lists (ACLs). Zugriffsberechtigungen können dabei sowohl auf Objekt- als auch auf Attributsebene vergeben werden. Rechte können über ACLs grundsätzlich nur im positiven Sinne vergeben werden, d. h. der Zugriff wird explizit erlaubt. Ein ausdrücklicher Ausschluss eines Benutzers mittels einer Zugriffsliste kann nicht definiert werden.

Zugriffsberechtigungen werden explizit durch Zuweisung an den Rechte-Inhaber vergeben. Für ein Zielobjekt wird dabei eingetragen, welche weiteren Objekte darauf zugreifen dürfen. Umgekehrt kann daran auch abgelesen werden, auf welche Zielobjekte ein Objekt zugreifen darf.

Zugriffsberechtigungen vererben sich entsprechend der Baumhierarchie des Verzeichnisdienstes. Dies gilt allerdings zunächst nur für die Objektrechte, die Attributsrechte vererben sich nur, wenn dies explizit konfiguriert wird. Die automatische Vererbung von Zugriffsberechtigungen von Objekten auf deren Kindobjekte kann durch die Konfiguration so genannter Masken oder Filter reglementiert werden. Da über das "Self"-Recht eigene Attributswerte verändert werden können, ist es aus Sicherheitssicht kritisch und sollte ebenfalls mit Hilfe eines Filters kontrolliert werden.

Bei einer Partitionierung des Verzeichnisbaums entsteht zunächst eine Lücke in der Vererbungskette, welche allerdings automatisch durch das Anhängen einer inhärenten ACL geschlossen wird.

Wirksam bei einem Zugriffsversuch werden die so genannten effektiven Rechte, d. h. diejenigen Zugriffsberechtigungen, die sich gemäß der schon genannten Mechanismen zur Rechtevergabe als Endresultat ergeben. Diese effektiven Rechte werden bei jedem Zugriff dynamisch berechnet bzw. im Cache des Servers gehalten. Die Administratoren sollten über eine Managementkonsole die Möglichkeit haben, sich diese aktuell gültigen effektiven Rechte auf einzelne Objekte anzeigen zu lassen und sollten diese stichprobenartig kontrollieren.

Ein wichtiger Aspekt bei der Rechtevergabe im Verzeichnisdienst ist die Konfiguration der Benutzer- und der Gruppenkonten. Durch geeignete Definition der Benutzer- und Administratorgruppen lässt sich die Rechtevergabe transparenter und einfacher gestalten.

Dies ist zu empfehlen, da generell eine hohe Komplexität in der Administration die Gefahr durch Fehlkonfigurationen erhöht. Zur vereinfachten und konsistenten Konfiguration der Benutzer und Benutzergruppen sollten Templates (Vorlagen) verwendet werden.

Verzeichnisdienste erlauben eine rollen- und funktionsbasierte Administration. Falls diese administrativen Rollen nicht bereits definiert sind, erfordert dies eine Schema-Erweiterung des Verzeichnisdienstes. Administrative Aufgaben können delegiert werden, so dass sie von Mitgliedern einer zugewiesenen Benutzergruppe (Administratorengruppe) durchgeführt werden können. Auf diese Weise wird auch die Delegation von Administrationsaufgaben realisiert.

Bei einer eventuellen Zusammenführung zweier oder mehrerer Verzeichnisdienst-Bäume zu einem Gesamtbaum sind anschließend die resultierenden effektiven Rechte zu kontrollieren. Auch bei der Verschiebung von Partitionen innerhalb eines Verzeichnisdienst-Baums ist dies zu berücksichtigen. Ebenso müssen die Zugriffsberechtigungen kontrolliert und eventuell nachkonfiguriert werden, wenn z. B. eine Windows-Domäne in einen eDirectory-Baum durch Migration übernommen wurde.

Prüffragen:

- Wurden die Zugriffsrechte der Benutzer- und Administratorgruppen gemäß der erstellten Sicherheitsrichtlinie konfiguriert?
- Wurden die sich tatsächlich ergebenden effektiven Rechte auf die Zielobjekte stichprobenartig kontrolliert?
- Sind die Administratorrollen und die Delegation von Administrationsrechten konsistent konfiguriert?

# M 4.310 Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

LDAP (Lightweight Directory Access Protocol) ist ein Protokoll zum Zugriff auf Daten eines Verzeichnisdienstes. LDAP wurde ursprünglich als Alternative zu DAP (Directory Access Protocol) entwickelt, das im Rahmen des X.500-Directory-Standards definiert wurde. Das zugrunde liegende Datenmodell und die innerhalb des Protokolls möglichen Operationen wurden dabei im Wesentlichen vom X.500-Standard übernommen. Die aktuelle Version des Protokolls, LDAP Version 3, hat sich inzwischen zum dominierenden Standard für den Zugriff auf Verzeichnisdienste entwickelt.

Verzeichnisdienste verfügen nahezu alle über eine LDAP-Schnittstelle. Dies ermöglicht unter anderem die folgenden Einsatzszenarien:

- Der Verzeichnisdienst wird im Internet platziert, zum Beispiel als so genannte Zertifikatsdatenbank. Die Benutzer greifen über das Internet mit Hilfe eines geeigneten LDAP-fähigen Software-Clients darauf zu.
- Der Verzeichnisdienst wird im Intranet einer Institution zur Verwaltung von Benutzerkonten oder Ressourcen im Netz eingesetzt. Dann sind neben direkten Benutzerzugriffen über einen LDAP-Client auch Zugriffe von Netzapplikationen möglich.

In beiden Fällen ist der LDAP-Zugriff entsprechend der zuvor definierten Sicherheitsrichtlinie (siehe M M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*) zu konfigurieren.

Verzeichnisdienste erlauben prinzipiell eine anonyme Anmeldung von LDAP-Clients. In der Voreinstellung hat der LDAP-Client die Zugriffsrechte, die für das Objekt im Verzeichnisdienst eingetragen sind. Es handelt sich um ein virtuelles Objekt, das lediglich für die Rechtevergabe im Verzeichnisdienst genutzt wird. Jeder Zugriff auf Objekte im Verzeichnisbaum erfolgt automatisch mindestens mit den Rechten, die diesem "public" Objekt eingeräumt werden.

Sollen anonymen Benutzern auf einzelne Teilbereiche des Verzeichnisbaums weitergehende Zugriffe eingeräumt werden, so ist dafür ein gesondertes Benutzerkonto, ein sogenannter Proxy-User, für den anonymen LDAP-Zugriff einzurichten. Dieser anonyme Zugang setzt keine Authentisierung voraus, es ist nicht notwendig, diesem Konto ein Passwort zu vergeben. Es sollte darauf geachtet werden, dass dieses anonyme Benutzerkonto selbst auch kein Passwort einrichten kann, da der anonyme Zugang sonst durch einen Client blockiert werden könnte. Desweiteren sollten die Zugriffsrechte für diesen Proxy-User hinreichend restriktiv vergeben werden. Sie sollten wieder komplett entzogen werden, wenn der Account nicht mehr gebraucht wird.

Insbesondere bei einem anonymen Zugriff sollten die Suchmöglichkeiten über LDAP-Zugriffe eingeschränkt werden. Liefert der Server zum Beispiel nach Eingabe eines Namens die zugehörige E-Mail-Adresse oder für eine E-Mail-Adresse ein zugehöriges Zertifikat, so sollten Suchfilter nur eingeschränkt genutzt werden dürfen? Die E-Mail-Adresse und nur diese (nicht der zugehörige Distinguished Name) sollte nur nach Eingabe des vollständigen Namens oder eines ausreichend langen Namensteils an den Anfragenden zurückgegeben werden. Ein Zertifikat sollte nur bei Eingabe einer vollständigen E-Mail-Adresse zurück geliefert werden. Es sollte überlegt werden, Platzhalter (Wild-

cards) nicht zu erlauben, damit über solche Abfragen keine vollständige Liste aller E-Mail-Adressen der Institution erstellt werden können. Alternativ kann die Anzahl der ausgegebenen Ergebnisse mit einem niedrigen Limit ausgestattet werden. Empfohlen wird ein Limit zwischen 1 und 5. Andernfalls sind anonyme Benutzer in der Lage, den kompletten Verzeichnisdienst oder zumindest große Teile davon auszulesen und erhalten so wertvolle Informationen, die als Grundlage für Spam oder Social Engineering-Angriffe dienen können (siehe G 3.89 Fehlerhafte Konfiguration des LDAP-Zugriffs auf Verzeichnisdienste).

Bereits bei der Planung des Einsatzes eines Verzeichnisdienstes muss entschieden werden, welche Daten über eine anonyme Anmeldung zugänglich sein dürfen (siehe auch M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten*).

**Einsatz des Verzeichnisdienstes als LDAP-Server im Internet**

Wird der Verzeichnisdienst als LDAP-Server im Internet eingesetzt, so sind die entsprechenden Server durch ein Sicherheitsgateway zu schützen. Dies sollte so konfiguriert werden, dass nur die zum Betrieb der LDAP-Server notwendigen Datenpakete zu den LDAP-Servern weitergeleitet werden. Meist wird es sich dabei um TCP-Pakete an die Ports 389 und 636 handeln, die standardisierten Port-Nummern für LDAP bzw. LDAP über SSL.

Für Daten, auf die nicht anonym zugegriffen werden darf, ist eine Authentisierung des jeweiligen LDAP-Clients notwendig. Der jeweilige Client authentisiert sich also als im Verzeichnis eingetragener Benutzer.

Um zu verhindern, dass Kennwörter im Klartext über das Internet übertragen werden, sollten die entsprechenden Einstellungen gesetzt sein. Mit dieser Einstellung sind dennoch anonyme LDAP-Verbindungen ebenso möglich wie eine Benutzeranmeldung mit LDAP über SSL.

Grundsätzlich wird empfohlen, SSL für die Kommunikation und Übertragung einzusetzen. Hierbei werden die Optionen ein- sowie zweiseitige Authentisierung unterstützt. Zweiseitige Authentisierung bedeutet, dass auch der Client im Besitz eines gültigen Zertifikats sein muss und dass auf Basis des zugehörigen privaten Schlüssels ein Sitzungsschlüssel (Session Key) generiert wird. Dies ist die sicherste Konfiguration. Alternativ kann die Client-Authentisierung jedoch auch über ein Passwort erfolgen. Durch die Verwendung einer verschlüsselten SSL-Verbindung zum Server ist die Vertraulichkeit des Passworts bei der Übertragung gewährleistet. In jedem Fall müssen die Benutzer das CA-Wurzelzertifikat in ihren LDAP-Client, z. B. einen Browser, importieren, damit die eingerichteten Vertrauensbeziehungen auch lokal nachvollzogen werden können (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*).

Wird kein SSL verwendet, werden Benutzerpasswörter im Klartext über das Internet an den Verzeichnisdienst übertragen (siehe auch M 5.147 *Absicherung der Kommunikation mit Verzeichnisdiensten*). Dies sollte aber grundsätzlich vermieden werden.

Ein Verzeichnisdienst bietet die Möglichkeit, die innerhalb von LDAP verwendeten standardisierten Objektklassen auf andere im Verzeichnisdienst intern verwendete Objektklassen abzubilden. Diese Eigenschaft wird relevant, wenn LDAP-Clients bei der Suche standardisierte LDAP-Objektklassen verwenden, die entsprechenden Daten sich jedoch in Attributen von Verzeichnisdienst-Objektklassen mit anderen Namen befinden. Bei der erstmaligen Verwendung

von LDAP-Clients oder bei Änderungen des Verzeichnisdienst-Schemas sollte daher überprüft werden, ob die Abbildung der LDAP-Objektklassen auf Verzeichnisdienst-Objektklassen schlüssig ist und die verwendeten LDAP-Applikationen damit korrekt funktionieren.

Prüffragen:

- Sind alle Verzeichnisdienst-Server, die vom Internet aus über LDAP angesprochen werden können, durch ein Sicherheitsgateway geschützt?
- Falls ein Proxy-User für die LDAP-Gruppe konfiguriert wurde, sind die Zugriffsrechte für diesen Proxy-User hinreichend restriktiv vergeben?
- Wird die Kommunikation und Übertragung über LDAP ausreichend abgesichert?
- Wird die Suche über LDAP-Zugriffe eingeschränkt, um die unnötige Herausgabe sicherheitssensitiver Informationen zu verhindern?

# M 4.311 Sicherer Betrieb von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Sicherheit eines komplexen Systems muss im Betrieb permanent aufrecht erhalten werden, da sich im laufenden Betrieb notwendige Veränderungen ergeben. Es genügt daher nicht, eine sichere Anfangskonfiguration einzustellen (siehe M 4.308 *Sichere Installation von Verzeichnisdiensten* und M 4.307 *Sichere Konfiguration von Verzeichnisdiensten*).

Nach der Installation und erstmaligen Konfiguration gemäß den im Vorfeld festgelegten Verzeichnisdienst-Konzepten und Sicherheitsrichtlinien erfolgt der Betrieb von Verzeichnisdienst-Servern in der Regel im Netzverbund. Die Sicherheit eines solchen Netzes hängt dabei einerseits von der anfangs eingestellten Konfiguration ab. Sie wird jedoch auch maßgeblich durch die Art und Weise der Konfigurationsänderungen bestimmt, die im laufenden Betrieb erfolgen müssen. Dabei sind insbesondere auch Seiteneffekte zu berücksichtigen, die unter Umständen unbeabsichtigt zu Sicherheitslücken führen können.

Folgende Aspekte sind im laufenden Betrieb für ein Verzeichnisdienst-System aus Sicht der Informationssicherheit zu beachten:

- Ein wichtiger Aspekt der Systemsicherheit eines Verzeichnisdienst-Systems ist die konsistente Verwaltung von Benutzern und Berechtigungen. Das administrative Konzept hat dabei Auswirkungen auf die Komplexität der durchzuführenden Aufgaben. Da es bei komplexen Abläufen leicht zu Fehlern kommen kann, sollten die administrativen Aufgaben möglichst einfach gestaltet werden. Ein gruppenbasiertes Zugriffskonzept trägt zur Aufrechterhaltung eines sicheren Systemzustands bei. Die Verwaltung von Zugriffsrechten auf Datenbanken wird wesentlich vereinfacht und ist insgesamt weniger fehleranfällig. Insbesondere ist darauf zu achten, dass für normale Benutzer der Zugriff auf alle Administrationswerkzeuge unterbunden wird.
- Veränderungen in einem Verzeichnissystem ergeben sich insbesondere dann, wenn fremde LDAP-Verzeichnisse in einen bestehenden Verzeichnisdienst-Baum importiert werden. Diese neu importierten Verzeichnisse sind in der Regel noch nicht in die bestehenden Sicherheitsstrukturen eingebunden. Damit die definierte Sicherheitsrichtlinie auch weiterhin konsistent umgesetzt ist, muss die Konfiguration der Sicherheitseinstellungen umgehend nachgeholt werden. Die Berechtigungen zum Import neuer Verzeichnisse und zum Erzeugen von Verzeichnis-Replikationen müssen restriktiv vergeben werden.
- Kryptographische Zertifikate können eine wesentliche Rolle für die Zugriffskontrollmechanismen des Verzeichnisdienstes spielen. Wenn eine Zertifizierungsstelle auf einem Verzeichnisdienst-Server installiert ist, kann für jedes neue Objekt automatisch ein eigenes Schlüsselpaar generiert und im Verzeichnisdienst abgelegt werden. Der sichere Betrieb dieses Verzeichnisdienst-Server im Baum ist deshalb besonders wichtig. Zu schützen sind nicht nur die Daten, die sich auf diesem befinden, sondern vor allem auch dessen Verfügbarkeit, beispielsweise durch geeignete Replizierung.
- In Bezug auf den Virenschutz verlangt ein Verzeichnisdienst besondere Strategien, damit Replikationen nicht aufgrund von Zugriffen durch den

Virenscanner Änderungen registrieren und so zu unnötigem Datentransfer führen. Im schlimmsten Fall kann der Datenbestand im Verzeichnis dadurch inkonsistent werden und letztlich den Verzeichnisdienst unbrauchbar machen.

- Die Sicherheit eines IT-Systems basiert immer auch auf der physikalischen Sicherheit in der Umgebung der Server und Netzkomponenten. Daher muss ein Verzeichnisdienst-Server in einer sicheren Umgebung aufgestellt werden, siehe z. B. den Baustein B 2.4 *Serverraum*.
- Um den Sicherheitszustand eines Systems nachvollziehen zu können, ist es notwendig, dieses zu überwachen. Die Sicherheitseinstellungen und die Protokolldateien eines Servers sollten regelmäßig überprüft werden. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die potentiell zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept ist dabei auch als Teil des Sicherheitskonzeptes anzusehen. Komplexe Systeme wie Verzeichnisdienste können in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Überwachung muss automatisch durch entsprechende Systemkomponenten oder Produkte von Drittherstellern erfolgen. Dabei ist auch die Konfiguration der Systemüberwachung regelmäßig an das sich verändernde System anzupassen. Die Überprüfung von Protokolldateien und Sicherheitseinstellungen kann manuell oder werkzeuggestützt erfolgen. Die Empfehlungen zur Überwachung sind in M 4.312 *Überwachung von Verzeichnisdiensten* zusammengefasst.

Auch unter Sicherheitsgesichtspunkten ist es wichtig, dass alle den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse dokumentiert werden. Dazu sollten Betriebshandbücher erstellt und bei Systemänderungen aktualisiert werden. Da die Betriebshandbücher sicherheitsrelevante Informationen enthalten, sind sie so aufzubewahren, dass Unbefugte keinen Zugriff auf sie erlangen können. Befugte Administratoren sollten die Handbücher jedoch leicht einsehen können.

Die aufgeführten Empfehlungen können an dieser Stelle nur allgemeinen Charakter haben, da die Aufrechterhaltung der Systemsicherheit auch von lokalen Gegebenheiten abhängt. Daher müssen schon in der Planungsphase eines Verzeichnisbaums entsprechende Richtlinien zum sicheren Betrieb erstellt werden, die die lokalen Anforderungen berücksichtigen. Unter Umständen kann es auch vorkommen, dass bestimmte Mechanismen nicht optimal sicher konfiguriert werden können. Dies ist z. B. der Fall, wenn "alte" Applikationen weiter betrieben werden müssen, die nur auf schwache oder keine Authentisierung ausgelegt sind. Hier muss dann durch alternative Gegenmaßnahmen an anderer Stelle, z. B. auf organisatorischer Ebene, eine angemessene Sicherheit erreicht werden.

Potentielle Sicherheitslücken können nur von kompetenten Administratoren entdeckt bzw. vermieden werden. Daher ist die Schulung und Fortbildung der Systemverwalter eine wichtige Schutzmaßnahme (siehe auch M 3.62 *Schulung zur Administration von Verzeichnisdiensten*).

Daneben müssen auch die normalen Benutzer in Sicherheitsaspekten geschult werden (siehe auch M 3.63 *Schulung der Benutzer zur Authentisierung mit Hilfe von Verzeichnisdiensten*), damit potentielle Gefahren bekannt sind und die zur Verfügung stehenden Sicherheitsmechanismen richtig eingesetzt werden können.

Prüffragen:

- Sind alle Betriebsabläufe des Verzeichnisdienstes dokumentiert?
- Ist der Zugriff auf alle Administrationswerkzeuge für normale Benutzer unterbunden worden?

# M 4.312 Überwachung von Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT, Revisor

Um den Sicherheitszustand eines Systems nachvollziehen zu können, ist es notwendig, dieses kontinuierlich zu überwachen. Dafür sollten unter anderem die Sicherheitseinstellungen und die Protokolldateien eines Servers regelmäßig überprüft werden. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept ist dabei auch als Teil des Sicherheitskonzeptes anzusehen.

Komplexe Systeme wie Verzeichnisdienste können dabei in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Kontrolle muss automatisch durch entsprechende Systemkomponenten oder Produkte von Dritt-Herstellern erfolgen. Dabei ist auch die Konfiguration der Systemüberwachung regelmäßig an das sich verändernde System anzupassen.

Zur Systemüberwachung eines Verzeichnisdienstes sollten geeignete Werkzeuge eingesetzt werden. Wenn es sich um eine Client-Server-Verbindung handelt, müssen für den Zugriff auf die Werkzeuge geeignete Authentisierungsmechanismen vorhanden sein. Der Zugreifende darf nur nach erfolgreicher Authentisierung Zugriff auf die Daten erhalten, wobei die für ihn konfigurierten Rechte gelten. Der Zugriff auf alle Administrationswerkzeuge sollte für normale Benutzer unterbunden werden. Grundsätzlich sollten diese Zugriffe nur mit einer ausreichenden Verschlüsselung der Kommunikationsverbindung betrieben werden.

Je nach Verzeichnisdienst und den zur Verfügung stehenden Werkzeugen können sämtliche Verzeichnisdienst-Ereignisse in einer eigenen Protokolldatei gespeichert werden. Dadurch sind die Ereignisse gezielter zu erkennen und auszuwerten, wie wenn die Verzeichnisdienst-Ereignisse in der globalen Protokolldatei des Betriebssystems gespeichert werden.

Im Rahmen der Überwachung sind folgende Aspekte zu beachten:

- Der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat sollten frühzeitig in die Planung mit einbezogen werden, da bei einer System-Überwachung meist auch personenbezogene Daten erfasst werden.
- Neben den Verzeichnisdienst-spezifischen Ereignissen müssen auch Ereignisse des Betriebssystems beobachtet und protokolliert werden, um ein vollständigeres Bild über die Systemabläufe zu erhalten. Empfehlungen und Hinweise zur Protokollierung auf Betriebssystem-Ebene finden sich in den jeweiligen Bausteinen.
- Eine zentrale Sammelstelle für Protokolldateien mit entsprechend automatisierter Auswertung kann durch Produkte von Dritt-Herstellern aufgebaut werden. Wird ein Werkzeug zum Netz- und Systemmanagement eingesetzt (siehe Baustein B 4.2 *Netz- und Systemmanagement*), so können je nach Produkt, die Verzeichnisdienst-Protokolle direkt in dieses Werkzeug integriert werden.
- Durch die Überwachung fallen je nach Einstellung große Datenmengen an. Diese müssen nicht nur regelmäßig ausgewertet, sondern aus Platzgründen auch gelöscht oder auf andere Datenträgern ausgelagert werden. Zusätzlich kann eine intensive Überwachung zu Performanceverlu-

sten führen. Dadurch kann ein Server unter Umständen so überlastet werden, dass ein geregelter Betrieb nicht mehr möglich ist. Aus diesem Grund müssen die geeigneten Überwachungsparameter im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst werden. Anpassungen können auch Einfluss auf das gesamte Überwachungskonzept haben, da bestimmte Überwachungsaufgaben unter Umständen nicht mehr durchführbar sind. Dies gilt besonders, wenn zusätzliche Produkte eingesetzt werden, die hohe Voraussetzungen an die protokollierten Ereignisse stellen. Beispiele hierfür sind Programme, die eine automatische Analyse der Protokolldaten auf Verhaltensanomalien, etwa für die Erkennung von Angriffen, durchführen.

Im Rahmen der Überwachung der Systemfunktionen empfiehlt sich außerdem eine regelmäßige Kontrolle der Verzeichnisdienst-Replikation, durch die Konfigurationsänderungen weitergeleitet werden. Fehler in der Replikation haben meist zur Folge, dass Konfigurationsänderungen nicht überall durchgeführt werden und so z. B. einem Benutzer zu viele Rechte zugestanden werden.

Prüffragen:

- Wurde ein bedarfsgerechtes Überwachungskonzept zum Verzeichnisdienst entworfen und umgesetzt?
- Werden wichtige Systemereignisse des Verzeichnisdienstes protokolliert und regelmäßig ausgewertet?
- Werden die Überwachungsparameter des Verzeichnisdienstes im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst?

# M 4.313 Bereitstellung von sicheren Domänen-Controllern

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Da auf den Domänen-Controllern die Active-Directory-Infrastruktur gespeichert ist, müssen diese entsprechend sicher konfiguriert werden. Die folgenden Sicherheitsempfehlungen sollen dabei helfen, die Risiken bei der Bereitstellung von Domänen-Controllern auf ein Minimum zu reduzieren.

### Sicherer Betrieb von Domänen-Controllern

Grundsätzlich sollten Domänen-Controller in einer sicheren Umgebung, z. B. in einem Rechenzentrum oder in Räumlichkeiten, deren Zugang nur vertrauenswürdigem Personal möglich ist, aufgestellt werden. Darüber hinaus sollten sie durch eine gesicherte Infrastruktur, beispielsweise mit Routern, Switches etc. zusätzlich abgesichert werden.

Die Betriebssystem-Installation sollte unter Berücksichtigung der in den IT-Grundschutz-Katalogen enthaltenen Bausteine zu den einzelnen Windows-Server-Betriebssystemen in der Schicht 3 durchgeführt werden.

### Vorhersagbare und wiederholbare Bereitstellungen

Um mögliche Konfigurationsfehler zu vermeiden und einen einheitlichen Sicherheitsstand zu erhalten, sollte ausgehend von einer Referenzinstallation eine abbildbasierte Einrichtung der Domänen-Controller vorgenommen werden. Ferner sollten auch die Sicherheitseinstellungen in der Basiseinrichtung der Domänen-Controller einheitlich vorgenommen werden. Dies sollte durch die Implementierung eines vorhersagbaren und leicht zu wiederholenden Bereitstellungsvorgangs erreicht werden. Dies beinhaltet:

- Regelmäßiges Einspielen aktueller Hotfixes und Service Packs
  In regelmäßigen Abständen sollten aktuelle Hotfixes und Service Packs eingespielt werden. Die Auswirkungen sollten jedoch vorher an einem Abbild des Referenz-Domänen-Controllers ausführlich getestet werden.
- Vergabe von ausreichend starken Passwörtern
  Für die Benutzerkonten im Active Directory sind ausreichend starke Passwörter zu vergeben. Hierbei soll gewährleistet werden, dass unberechtigte Zugriffe nicht erschlichen werden können. Hinweise auf ausreichend starke Passwörter finden sich in Maßnahme M 2.11 *Regelung des Passwortgebrauchs*. Neben der Erstellung komplexer Passwörter ist sicherzustellen, dass die Weitergabe der Passwörter an die betroffenen Personen über vertrauensvolle Wege erfolgt. Auch sollten die Benutzerkonten insbesondere bei der Ersteinrichtung mit individuellen Passwörtern ausgestattet werden.
- Deaktivieren der automatischen Generierung von sogenannten 8.3-Dateinamen in NTFS.
  Die automatische Generierung von 8.3-Dateinamen (also solchen mit acht Zeichen für den Dateinamen, drei Zeichen für die Dateiendung) sollte deaktiviert werden, damit Viren und Angriffe, die speziell auf 8.3-kompatible Dateinamen zielen, vermieden werden können. Vor allem wenn keine 16-Bit-Anwendungen mehr verwendet werden, ist diese Funktion nicht mehr notwendig. Darüber hinaus wird dadurch die Performance beim Auflisten

von Verzeichnissen deutlich erhöht. Hierzu ist unter *HKLM\SYSTEM\CurrentControlSet\Control\FileSystem* folgender Eintrag festzulegen:
Eintragsname = *NtfsDisable8dot3NameCreation*
Datentyp = *REG_DWORD*
Wert = *1*
Änderungen der Registrierungsschlüssel sollten zunächst innerhalb einer Testumgebung hinsichtlich ihrer Kompatibilität und Auswirkungen getestet werden.

- Deaktivieren der Prä-Windows-2000-Kompatibilität:
  Befinden sich keine Server unter Windows NT 4.0 innerhalb oder außerhalb der Gesamtstruktur oder Server unter Windows 2000 in einer vertrauenden Domäne außerhalb der Gesamtstruktur, ist ein Verzicht auf die Prä-Windows-2000-Kompatibilität notwendig. Ansonsten würden Zugriffsberechtigungen erteilt, die einen anonymen Zugang zu Active-Directory-Informationen ermöglichen.
- Sicherstellen der Integrität der Installation
  Werden die Domänen-Controller an einem anderen Zielstandort bereitgestellt, sollten für deren Transport Signaturen verwendet werden, um auf diese Weise die Integrität der Installationen sicherzustellen

**Begrenzung auf erforderliche Dienste**

Um die sich bietende Angriffsfläche der Domänen-Controller möglichst gering zu halten, sollten die zur Verfügung gestellten Dienste auf das betrieblich notwendige Maß begrenzt werden.

**Berechtigung ausführbarer Dateien**

Um nach der Heraufstufung der Domänen-Controller die Stammordner der Datenträger vor Speicherplatzangriffen zu schützen, sollten die Berechtigungen für die Gruppe "Jeder" auf "Lesen und Ausführen" eingrenzt werden. Der "Vollzugriff" ist lediglich für die Administratoren zu erteilen.

**Systemstart von anderen Betriebssystemen verhindern**

Ein Systemstart von anderen Betriebssystemen auf den Domänen-Controllern kann die Zugangsrestriktionen von NTFS aushebeln und einen Zugriff auf kritische Daten ermöglichen. Neben der bereits erwähnten räumlichen Absicherung der Server sind daher ebenfalls organisatorische Vorkehrungen zu treffen.

Die Deaktivierung des Remote-Netzstarts und somit auch die Möglichkeit zur Remote-Netzinstallation, z. B. durch Remote Installation Services (RIS) oder Bootstrap Protocol (BOOTP), sollte wie auch die Verwendung eines BIOS-Kennwortes beim Systemstart vorgesehen werden.

**Neustart-Schutz mit SYSKEY**

Der Einsatz der Systemschlüssel (SYSKEY) schützt Sicherheitsinformationen unter Windows vor Offline-Angriffen. Die Kennwörter in der Active Directory-Datenbank und der lokalen Sicherheitsautorität (LSA) werden hierzu verschlüsselt auf dem Domänen-Controller hinterlegt. Bei einem Neustart des Domänen-Controllers ist nach Aktivierung des SYSKEY entweder das Kennwort oder der Datenträger mit dem Systemschlüssel erforderlich, andernfalls kann der Computer nicht gestartet werden. In jedem Fall ist es notwendig, den Datenträger mit dem Systemschlüssel nach Gebrauch wieder aus dem Domänen-Controller zu entfernen und an einem sicheren Ort zu hinterlegen. Es sollte außerdem sichergestellt sein, dass auch eine Arbeitskopie dieses Datenträgers vorhanden ist.

Prüffragen:

- Werden die Domänen-Controller in einer sicheren Umgebung betrieben?
- Ist bei allen Domänen-Controllern das grundlegende Windows-Server-Betriebssystem sicher installiert und konfiguriert?
- Wurde ein Abbild jedes Domänen-Controllers erstellt?
- Erfolgt eine Vergabe ausreichend starker Passwörter bei den Benutzerkonten?
- Wurde die Generierung der 8.3-Dateinamen deaktiviert?
- Wurde die prä-Windows-2000-Kompatibilität deaktiviert?
- Wurden die Berechtigungen für die Gruppe "Jeder" beschränkt?
- Sind die Domänen-Controller gegen unautorisierte Neustarts geschützt?

# M 4.314 Sichere Richtlinieneinstellungen für Domänen und Domänen-Controller

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Windows Server mit Active Directory enthält Standard-Sicherheitsrichtlinieneinstellungen für die Domäne und für die Domänen-Controller. Es werden jedoch Änderungen der Standard-Richtlinieneinstellungen zur Erhöhung der Sicherheit von Domäne und Domänen-Controllern durch die folgenden Punkte empfohlen:

- **Sichere Kennwortrichtlinien-Einstellungen**
  Der Zugriff auf Domänen-Controller muss mit starken Mechanismen abgesichert sein. Näheres zu den dafür notwendigen Einstellungen der Kennwortrichtlinien findet sich in den Microsoft-Server-spezifischen Bausteinen.
- **Konto-Sperrungsrichtlinien**
  Die Protokollierung der Anmeldeversuche (siehe hierzu auch M 4.316 *Überwachung der Active Directory Infrastruktur*) sollte so eingerichtet werden, dass Angriffe erkannt werden können. Beispielsweise könnte eine große Zahl nicht erfolgreicher Kennworteingaben während eines Anmeldeversuchs auf einen Brute-Force-Angriff hindeuten. Die eigentliche Kontosperrung ist über die Optionen Kontosperrdauer, Kontosperrungsschwelle und die Zurücksetzung des Kontosperrungszählers entsprechend der Beschreibung in Maßnahme M 2.231 *Planung der Gruppenrichtlinien unter Windows* zu definieren.
- **Kerberos-Richtlinien-Einstellungen**
  Der durch Kerberos zur Verfügung stehende Authentisierungsdienst teilt dem jeweiligen Client die erforderlichen Autorisierungsdaten für Ressourcenzugriffe zu. Hierbei wird der Zugriff auf Netzressourcen anhand von Sitzungstickets gewährt. Dazu stellt der Domänen-Controller im Vorfeld ein sogenanntes Ticket-Granting-Ticket (TGT) an den Client aus. Erfolgt ein Zugriffsversuch seitens der Clients auf eine Ressource, so übermittelt der Client das TGT zur Prüfung an den Domänen-Controller. Der Domänen-Controller wiederum generiert dem Client nach erfolgreicher Prüfung ein Sitzungsticket, mit dem ein zeitlich begrenzter Zugriff auf die Ressource ermöglicht wird.
  Durch eine Anpassung der Kerberos-Richtlinieneinstellung können für Domänen-Benutzerkonten die Kerberos-Tickets, z. B. die Gültigkeitsdauer, angepasst werden. Hinweise zur Anpassung der Kerberos-Richtlinien können den Hilfsmitteln zum IT-Grundschutz (siehe *Kerberos-Richtlinieneinstellungen für Domänen* in *Hilfsmittel zum Active Directory*) entnommen werden.

In Bezug auf sichere Richtlinieneinstellungen für Domänen-Controller werden des Weiteren nachfolgende Maßnahmen empfohlen:

Benutzerrechte sollten restriktiv vergeben werden, so dass die Benutzer in der Domäne oder auf dem Domänen-Controller die betrieblichen oder administrativen Aufgaben erledigen können. Die Zugriffsmöglichkeiten von Benutzern sollte dabei so eingeschränkt werden, dass sie die Sicherheit der Domänen-Controller nicht gefährden (siehe auch Maßnahme M 2.229 *Planung des Active Directory*).

Durch die Einrichtung von Richtlinieneinstellungen für die Domänen-Controller-Überwachung wird der Nachweis der Verantwortung für sensible Verzeichnisoperationen, z. B. Verwaltungs- oder Konfigurationsänderungen, ermöglicht. Es sollte eine Überwachung von Anmeldeversuchen, Kontoverwaltung, Active Directory-Zugriff, Objektzugriffsversuchen, Richtlinienänderungen, Rechteverwendung, Prozessverfolgung und Systemereignisse eingerichtet werden.

Wichtige Active Directory-Objekte, wie z. B. die Verzeichnispartitionen, sind mit geeigneten Richtlinieneinstellungen zu überwachen. Dazu muss die Überwachung der Verzeichnispartitionen (logische Bereiche der Active Directory-Datenbank) aktiviert werden. Die hiervon betroffenen Verzeichnispartitionen lauten "Schema", "Konfiguration" und "Domäne".

Die obigen Empfehlungen zur Einrichtung von Richtlinieneinstellungen führen dazu, dass die voreingestellte maximale Größe des Sicherheitsprotokolls angehoben werden muss, damit eine größere Anzahl überwachter Ereignisse aufgenommen werden kann. Die Protokolle müssen zeitnah ausgewertet werden. Außerdem muss es ein klar definiertes Vorgehen für die regelmäßige und rechtzeitige Archivierung sowie eine Sicherung der Sicherheits- und Systemereignisprotokolle geben, damit keine Ereignisse verloren gehen oder überschrieben werden.

Ist darüber hinaus die Zusammenarbeit zwischen Domänen in verschiedenen Gesamtstrukturen zu unterstützen, z. B. zur gemeinsamen Nutzung von Anwendungen oder zur begrenzten Zusammenarbeit zwischen verschiedenen Gesamtstrukturen in einer Institution, sollten externe Vertrauensstellungen eingerichtet werden. Durch externe Vertrauensstellungen entsteht jedoch ein potenzielles Sicherheitsrisiko, da Sicherheitsgrenzen überschritten werden. Daher sollten die Domänen-Controller in der vertrauenden Domäne Autorisierungsdaten der Benutzer filtern und Sicherheitskennungen (Security IDs, SIDs) entfernen, die sich nicht auf die Domäne des Benutzerkontos beziehen. Eine ausführliche Beschreibung hinsichtlich der Erschleichung umfassender Berechtigungen durch gefälschte SIDs und die Gegenmaßnahmen durch SID-Filterung ist in den Microsoft-Knowledge-Base-Artikeln 289243 und 289246 aufgeführt.

Die Richtlinieneinstellungen der Sicherheitsoptionen für Domänen-Controller beeinflussen die sicherheitsrelevanten Konfigurationseinstellungen der Windows Server Betriebssysteme und sollten daher gewissenhaft eingestellt werden. Dies gilt nicht nur für die Active Directory relevante Konfiguration, sondern auch für andere Komponenten des Windows Server Betriebssysteme (z. B. Sicherheitskonfigurationseinstellungen für Netz, Dateisystem und Benutzeranmeldung).

Prüffragen:

- Umfassen die Richtlinien für Domänen und Domänen-Controller sichere Einstellungen für Kennworte, Kontensperrung, Kerberos-Authentisierung, Benutzerrechte und Überwachung?
- Ist eine ausreichende Größe für das Sicherheitsprotokoll des Domänen-Controllers eingestellt?
- Bei externen Vertrauensstellungen zu anderen Domänen: Werden Autorisierungsdaten der Benutzer gefiltert und anonymisiert?

# M 4.315 Aufrechterhaltung der Betriebssicherheit von Active Directory

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die in der Produktivumgebung eingesetzten Domänen-Controller sind durch die Administratoren auf dem vorangegangen Sicherheitsniveau zu halten und bei erhöhten Anforderungen entsprechend anzupassen. Für Änderungen an den Systemen, welche sich unter anderem durch die regelmäßigen Wartungsarbeiten ergeben, sind im Vorfeld schriftlich niedergelegte Richtlinien zu entwickeln.

Eine regelmäßige Virenprüfung der Domänen-Controller ist für einen sicheren Betrieb unerlässlich und sollte entsprechend den jeweiligen Besonderheiten (siehe M 2.414 *Computer-Viren-Schutz für Domänen-Controller*, Abschnitt *Kritische Dateien auf Domänen-Controllern*) erfolgen.

### Laufende Aktualisierung mit Service Packs und Hotfixes

Die Domänen-Controller sollten in regelmäßigen Abständen durch entsprechende Maßnahmen, wie z. B. Windows Update, Service Packs und Hotfixes, gegen neue Gefährdungen geschützt werden. Auch wenn solche Updates sicherheitskritische Lücken schließen und zeitnah in die bestehende Struktur zu integrieren sind, müssen die Aktualisierungen im Vorfeld in einer Testumgebung geprüft werden, um mögliche negative Seiteneffekte innerhalb der Produktivumgebung rechtzeitig zu erkennen.

### Sicherheit der Dienste-Administratorkonten

Die Verantwortung zur Steuerung der Konfiguration und Funktionsweise des Verzeichnisdienstes ist nur zuverlässigen, vertrauenswürdigen Personen zu übertragen. Dieser Personenkreis muss mit den gültigen Sicherheitsrichtlinien der Institution vertraut sein und Bereitschaft demonstrieren, diese konsequent durchzusetzen.

Die Zugriffsrechte der Dienste-Administratoren sollten auf das für ihre Arbeiten notwendige Minimum reduziert und ausschließlich für Aufgaben genutzt werden, welche erhöhte Rechte voraussetzen. Um die berechtigte Notwendigkeit für Personen mit Dienste-Administratorrechten sicherzustellen, ist diese in regelmäßigen Abständen zu überprüfen und bei Bedarf entsprechend anzupassen. Auch ist die Mitgliederanzahl der Administratorenkonten auf einem notwendigen Minimum zu halten. Die Benutzung ausreichend starker Passwörter für die Konten der Administratorengruppen ist zwingend erforderlich. Es sollte überlegt werden, Verfahren zur starken Authentisierung zu verwenden, wie z. B. die zusätzliche Nutzung von Chipkarten zur Anmeldung am Betriebssystem.

### Gewährleistung der Aktualität von Basisinformationen

Unter dem Begriff "Basisinformationen" werden die wichtigsten Konfigurationsparameter des Active Directory zusammengefasst. Die Basisinformationen sollten mindestens folgende Punkte beinhalten:

- Überwachungsrichtlinien

- Gruppenrichtlinienobjekte und deren Zuweisung
- bestehende Vertrauensstellungen
- Organisationseinheit der Domänen-Controller und Dienst-Admins
- Inhaber der Betriebsmasterfunktionen
- Replikationstopologie
- Datenbankeigenschaften
- verwendete Service Packs und Hotfixes für Domänen-Controller und Administratorarbeitsstationen und deren aktueller Systemstatus
- aktuell vorhandene Sicherungsmedien
- Überprüfung der Sicherungsmedien
- Überprüfung der aktuell benötigten Dienste-Administratorenberechtigungen

Mit Hilfe dokumentierter Basisinformationen ist eine Nachverfolgung und Überprüfung der am Active Directory durchgeführten Änderungen möglich. Die Basisinformationen sollten für alle Domänen-Controller in einer Basisdatenbank zusammengefasst werden. Diese Basisdatenbank bietet zusätzlich einen Überblick der aktuell eingesetzten Komponenten. Die Zuständigkeiten für die Pflege der Basisinformationen muss geklärt werden.

Prüffragen:

- Werden regelmäßig Hotfixes und Service Packs auf dem Domänen-Controller eingespielt?
- Werden die Auswirkungen der Hotfixes und Service Packs auf den Domänen-Controller zunächst in einer Testumgebung getestet?
- Besitzen die Dienste-Administratoren auf dem Domänen-Controller nur die notwendigen Rechte?
- Werden die Rechte der Dienste-Administratoren in regelmäßigen Abständen überprüft?
- Werden alle notwendigen Parameter des Active Directory als Basisinformationen aktuell und nachvollziehbar festgehalten?

# M 4.316 Überwachung der Active Directory Infrastruktur

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Sicherheitsstatus der Active Directory Infrastruktur wird über die Protokollierung der systemeigenen Ereignisse überwacht und bewertet. Die Protokolltiefe ist den jeweiligen Anforderungen anzupassen und sollte kontinuierlich überwacht werden.

Die Protokolldaten sollten regelmäßig ausgewertet werden. Zur Kontrolle sollten sie des Weiteren zusätzlich mit einem Referenzwert verglichen werden, der sich beispielsweise aus früheren Daten ermitteln lässt.

**Active Directory**

Die Auswertung der bei der Überwachung erzeugten Protokolldaten, kann, in Abhängigkeit von deren Umfang, manuell oder mit der Hilfe spezieller Überwachungssoftware erfolgen. In großen Active Directory Strukturen kann normalerweise eine rein manuelle Auswertung der Überwachungsdaten nicht mehr realisiert werden.

Die Ergebnisse der Sicherheitsüberwachung sollten in regelmäßig erstellten Berichten zusammengefasst und ausgewertet werden, damit grundlegende Sicherheitsprobleme frühzeitig erkannt und behoben werden können.

Bei der Protokollierung können auch Sicherheitswarnungen auftreten, auf die sofort reagiert werden muss, so wie es im Notfallplan (siehe auch M 6.106 *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes*) des Unternehmens bzw. der Behörde vorgesehen ist.

Es können grundsätzlich zwei Methoden angewandt werden, um Änderungen an sicherheitsrelevanten Konfigurationsparametern des Domänen-Controllers bzw. des Active Directory zu erkennen. Zum einen ist dies die Ereignisbenachrichtigung, zum anderen sind das Trendanalysen.

Für die Ereignisbenachrichtigung werden so genannte Schwellen- oder Grenzwerte für Änderungen von Konfigurationsparametern im Active Directory oder am Domänen-Controller selbst definiert. Wird ein Konfigurationsparameter abgeändert und somit ein zuvor definierter Grenzwert überschritten, so wird dieses Ereignis vom Betriebssystem protokolliert.

Im Rahmen der Trendanalyse werden festgelegte Parameter über einen längeren Zeitraum in regelmäßigen Abständen erfasst. Werden bei der Auswertung dieser Daten extreme Änderungen bemerkt, so könnte das auf sicherheitsrelevante Vorfälle hindeuten. Wird beispielsweise der freie Festplattenspeicherplatz in regelmäßigen Abständen (z. B. alle 5 Minuten) erfasst und ein dramatischer Anstieg des Verbrauches von Festplattenspeicher bemerkt, so kann das auf einen Denial-of-Service-Angriff (DoS-Angriff) gegen den Domänen-Controller hinweisen.

**Änderungen des Domänen-Controller Status**

Änderungen an den Domänen-Controllern können die Sicherheit des Active Directory beeinflussen. Daher sollten mindestens die Bereiche Verfügbarkeit und Systemressourcen der Domänen-Controller überwacht werden:

Die Verfügbarkeit von Domänen-Controllern kann auf verschiedene Weise überwacht werden. Denkbar ist beispielsweise der Einsatz spezieller Überwachungssoftware. Alternativ können jedoch auch regelmäßige LDAP-Anfragen an die Domänen-Controller geschickt werden. Dabei kann mit dieser Methode nicht nur bestimmt werden, ob der entsprechende Domänen-Controller aktiv ist (der Test-Client erhält eine Antwort), sondern zusätzlich können aus der Antwortzeit auch Rückschlüsse auf die Systemauslastung des Domänen-Controllers gezogen werden.

Es ist außerdem sicherzustellen, dass Neustarts der Domänen-Controller erkannt werden, da ein nicht autorisierter Neustart von Domänen-Controllern auf einen Angriff hindeuten kann. Dementsprechend sind die Systemereignisprotokolle aller Domänen-Controller in einer Institution auf unautorisierte Systemneustarts zu untersuchen.

Zusätzlich zur direkten Verfügbarkeit von Domänen-Controllern sollten auch die Systemressourcen der Domänen-Controller überwacht werden. Eine Änderung der Systemressourcen muss nicht zwangsläufig auf einen Angriff hindeuten. Vielmehr kann die Ursache auch technischer Natur sein, z. B. Fehlkonfiguration oder Verwendung veralteter Hardware bei wachsenden Active-Directory-Strukturen.

Folgende Systemressourcen sollten auf allen Domänen-Controllern in einer Institution überwacht und bei Auffälligkeiten geeignete Gegenmaßnahmen ergriffen werden:

- Prozentuale Prozessorauslastung (oberer Grenzwert: 80%)
- Freier Speicherplatz auf dem Datenträger mit der Active-Directory-Datenbank in Prozent (unterer Grenzwert: 25%)
- Verfügbarer Arbeitsspeicher in Prozent (unterer Grenzwert: 10%)
- Bindungsdauer für LDAP-Verbindungen (Auffällig wäre eine ungewöhnlich starke Zunahme der Bindungsdauer.)
- Anzahl erfolgreicher LDAP-Verbindungen pro Sekunde (Auffällig wäre eine ungewöhnlich starke Zunahme der LDAP-Verbindungen. Der jeweilige Grenzwert hängt hierbei von dem Datenaufkommen von LDAP Verbindungen innerhalb der Organisation ab.)

**Änderungen im Active Directory**

Werden Änderungen auf Domänenebene durchgeführt, so wirken sich diese meist auf alle Domänen-Controller, Mitgliedsserver, Benutzer und Arbeitsstationen aus. Folgende Änderungen sind in diesem Zusammenhang denkbar:

- Ändern der domänenweiten Betriebsmasterfunktion
  Änderungen an den domänenweiten Betriebsmasterfunktionen wirken sich auf die gesamte Domäne aus. Zu den domänenweiten Betriebsmasterfunktionen gehört unter anderem der Emulationsmaster des Primären Domänen Controllers (PDC). Dies kann sich im Falle einer Fehlkonfiguration negativ auf das Gesamtkonstrukt der Domäne auswirken und zu weitreichenden Beeinträchtigungen innerhalb des Netzes führen. Eine im Vorfeld sorgfältig durchgeführte Planung hinsichtlich angedachter Änderungen an den Betriebsmasterfunktionen ist daher unabdingbar.
- Ändern der Vertrauensstellungen
  Zwischen unterschiedlichen Domänen einer Organisation oder Behörde können Vertrauensbeziehungen eingerichtet werden. Änderungen an Vertrauensbeziehungen müssen unbedingt überwacht werden, damit insbesondere das Hinzufügen von Vertrauensbeziehungen, und damit unter Umständen erweiterte Rechte der Domänen-Benutzer schnellstmöglich erkannt werden.

- Ändern des AdminSDHolder
  Das AdminSDHolder-Objekt wird vom Primären Domänen Controller (PDC) verwendet, um die Benutzer der Dienste-Administratorgruppen und die Dienste-Administratorengruppe selbst vor nicht autorisierten Veränderungen der Berechtigungen zu schützen. Dazu sollte vom PDC stündlich überprüft werden, ob die benutzerbestimmbaren Zugriffskontrolllisten (DACLs, Discretionary Access Control Lists) der zuvor genannten Benutzerkonten mit der DACL des AdminSDHolder-Objekt übereinstimmen. Weichen die DACLs voneinander ab, so müssen die DACLs der Benutzerkonten an die Einstellung des AdminSDHolder-Objekts angepasst werden.
- Änderungen an Gruppenrichtlinienobjekte und deren Zuweisung
  Änderungen an den Gruppenrichtlinien, wie z. B. Passwortrichtlinien für Domänenbenutzer, wirken sich auf die Domäne und damit auch auf alle Domänen-Controller der betroffenen Domäne aus und sind daher zu überwachen Darüber hinaus sind auch die Zuweisungen von Gruppenrichtlinienobjekten zu Domänen Containern sowie von Gruppenrichtlinienobjekten zur Organisationseinheit "Domänen-Controller" zu überwachen.
- Ändern der Mitgliedschaft vordefinierter Dienste-Administratorgruppen
  Das unautorisierte Hinzufügen oder Entfernen von Benutzern in vordefinierten Dienste-Administratorgruppen, wie z. B. Administratoren oder Sicherungs-Operatoren, kann auf einen Angriff hindeuten. Daher sind Änderungen an Mitgliedschaft von Diensteadministratorgruppen zu überwachen.
- Ändern der Überwachungsrichtlinien für eine Domäne
  Eine unautorisierte Änderung an den Überwachungsrichtlinien kann die Überwachung stören oder sogar komplett deaktivieren. Damit eine Deaktivierung der Überwachung erkannt werden kann, müssen die Überwachungsrichtlinien selbst auch überwacht werden.

Werden Änderungen durchgeführt, die sich auf die gesamte Active-Directory-Struktur, z. B. alle definierten Domänen, der Organisation oder der Behörde auswirken, so spricht man von Änderungen an der Gesamtstruktur. Änderungen an der Gesamtstruktur umfassen folgende Ereignisse:

- Änderungen an der Einstufung von Domänen-Controllern
  Wird ein Domänen-Controller herauf- oder herabgestuft, so wird von Änderungen an der Domänen-Controller-Einstufung gesprochen.
- Änderungen am Active-Directory-Schema
  Wird die Struktur der Verzeichnisdienstdatenbank verändert, z. B. bei Änderungen von Objektklassen oder Attributen innerhalb des Active Directory, so wird das Active-Directory-Schema geändert.
- Änderungen der LDAP-Richtlinien
  Mit Hilfe von LDAP-Richtlinien können LDAP-Anfragen und damit ebenfalls der Zugriff auf die Active-Directory-Daten per LDAP eingeschränkt werden.
- Änderungen an der Replikationstopologie zwischen Domänen-Controllern
  Unter Änderungen der Replikationstopologie wird das Erstellen, Löschen und Ändern von Active-Directory-Standorten, Standortverknüpfungen und Subnetzen verstanden.
- Ändern des dSHeuristic-Attribut
  Das dSHeuristic-Attribut steuert das Verhalten des Active Directory, hierüber kann z. B. die Auflistung von Objekten aktiviert oder deaktiviert werden.
- Änderungen der gesamtstrukturweiten Betriebsmasterfunktionen
  Die gesamtstrukturweiten Betriebsmasterfunktionen werden auch als Flexible Single Master Operations (FSMO) genannt. Zu den FSMO zählen die Schemamaster- und die Domänen-Master-Funktion.

Alle zuvor genannten Änderungsereignisse, sowohl auf Ebene einzelner Domänen, als auch in Bezug auf die Gesamtstruktur, sollten auf allen Domänen-Controllern einer Institution überwacht und ausgewertet werden. Wird bei der Auswertung der Sicherheitsüberwachungsprotokolle eines Domänen-Controller eine nicht autorisierte Änderung festgestellt, so sind entsprechende Notfallmaßnahmen einzuleiten (siehe auch M 6.106 *Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes*).

Bei einigen Ereignissen ist aus den Protokolldateien nicht ersichtlich welche Objekte oder Attribute geändert wurden. Daher ist das Schema des Active Directory zu dokumentieren, damit Änderungen später gegebenenfalls durch manuellen Abgleich identifiziert und behoben werden können.

Kann die vollständige Behebung unautorisierter Änderungen im Active Directory nicht sichergestellt werden, so ist die Wiederherstellung der Gesamtstruktur in Erwägung zu ziehen.

In der Gruppe "Dienst-Admins" ist die Erstellung, Löschung und Änderung von Benutzerkonten in der Dienste-Administratorgruppe zu überwachen. Darüber hinaus sollte ein Hinzufügen oder Löschen von Administratorarbeitsstationen in der Organisationseinheit "Dienst-Admins" überwacht werden.

Wenn der Speicherplatz auf dem Domänen-Controller für die Active-Directory-Datenbank erschöpft ist, können keine neuen Objekte im Active Directory mehr angelegt werden. Daher sollte der Speicherplatz, der von Active-Directory-Objekten verwendet wird, kontinuierlich überwacht werden.

Mit einer derartigen Überwachung kann nicht nur der zur Neige gehende Speicherplatz für die Active-Directory-Datenbank verfolgt werden, sondern es können auch Objektüberflutungsangriffe erkannt werden, bei denen der Speicherplatzbedarf in vergleichsweise kurzer Zeit dramatisch ansteigt.

Für ein schnelles Eingreifen bei einem Objektüberflutungsangriff kann auf den Domänen-Controllern eine Reservedatei beliebiger Größe angelegt werden. Im Fall eines Speicherplatzangriffs kann die Reservedatei auf den betroffenen Domänen-Controllern gelöscht werden, um kurzfristig freien Speicherplatz zu schaffen und so den normalen Betrieb zu sichern.

Im Nachgang müssen die unerwünschten Objekte des Angriffs im ActiveDirectory ermittelt und entfernt werden.

**Änderungen an kritischen Dateien**

Sowohl auf den Domänen-Controllern selbst, als auch an den Administrationsarbeitsplätzen sollte eine Überwachung eingerichtet werden, mit der eine Veränderung an kritischen Dateien erkannt werden kann. Dabei sollten mindestens die Dateien überwacht werden, die zur Konfiguration des Betriebssystems oder der installierten Anwendungen verwendet werden. Darüber hinaus sollten wichtige ausführbare Dateien, z. B. Administrationswerkzeuge auf den Administratorarbeitsplätzen, ebenfalls auf Änderungen überwacht werden.

Für die Überwachung der Systemkonfiguration muss zunächst eine geeignete Software ausgewählt werden. Anschließend sollte eine vertrauenswürdige Basiskonfiguration der zu überwachenden Betriebssysteme erstellt werden.

Mit Hilfe der Überwachungssoftware wird auf Basis dieser Konfiguration ein Referenzabbild erstellt, das als Grundlage für zukünftige Überprüfungen verwendet wird. In regelmäßigen Abständen ist zu überprüfen, ob sich die aktu-

elle Konfiguration der Domänen-Controller oder Administratoren-Arbeitsplätze im Vergleich zur Referenzkonfiguration geändert hat. Werden Änderungen festgestellt, so ist der ursprüngliche Systemzustand schnellstmöglich wieder herzustellen.

Prüffragen:

- Wird die Active Directory Infrastruktur anhand der systemeigenen Ereignisse überwacht und protokolliert?
- Werden die Ergebnisse der Sicherheitsüberwachung des Active Directory regelmäßig ausgewertet?
- Werden Verfügbarkeit und Systemressourcen der Domänen-Controller überwacht?
- Werden Änderungen auf Domänen-Ebene und an der Gesamtstruktur des Active Directory überwacht, protokolliert und ausgewertet?

# M 4.317 Sichere Migration von Windows Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Im Zuge verbesserter Funktionalitäten, erhöhter Sicherheit, größerer Kompatibilität und der Herstellerunterstützung ist eine Migration vorhandener Windows NT 4.0 Server-Strukturen auf Windows 2000 Server bzw. Windows Server 2003 (zusammenfassend im Folgenden Windows-Server genannt) ratsam. Mit Windows 2000 Server sind Leistungsmerkmale und Sicherheitsfunktionalitäten gegenüber Windows NT 4.0 Server erheblich verbessert worden. Daher sollte eine Migration in Erwägung gezogen werden. Im Vorfeld sind hierzu in einer Planungsphase zu klären,

- welche Server/Dienste konsolidiert werden können,
- ob die verwendete (Ziel-)Hardware ausreichend leistungsfähig ist und den erhöhten Systemanforderungen genügt,
- ob die innerhalb des Netzes erforderlichen Dienste mit der neueren Software kompatibel sind (Protokolle, Rechte etc.).

Unter Windows 2000 Server bereits verfügbare Funktionalitäten, z. B. DNS und Active Directory, werden durch die Migration auf Windows Server 2003 entsprechend erweitert. Generell sollte eine Migration zunächst in einer Testumgebung durchgeführt werden, um aufgrund der daraus resultierenden Ergebnisse eine möglichst optimale Migration des Produktiv-Systems gewährleisten zu können.

### Einsatz von DNS

Zu beachten ist, dass mit Einführung der Active-Directory-Funktionalität die Namensauflösung innerhalb des Netzes mittels DNS durchgeführt wird und damit die unter Windows NT 4.0 verwendete WINS (Windows Internet Name Service) NetBIOS Funktion abgelöst wird. Daraus ergibt sich die Anforderung, für das migrierte Netz den DNS-Dienst zur Verfügung zu stellen. Für weiterführende Informationen diesbezüglich empfiehlt sich der Herstellerartikel *Deploying Domain Name System* im Microsoft TechNet-Bereich (http://technet.microsoft.com).

### Gruppen-Richtlinien

Gegenüber den bei Windows NT 4.0 verwendeten System-Richtlinien steht unter Windows-Server eine Erweiterung mittels Gruppen-Richtlinien zur Verfügung, die eine umfangreichere Verwaltung der Objekte innerhalb der Active Directory Struktur ermöglicht. Aus diesem Grunde sind die unter Windows NT 4.0 verwendeten administrativen Vorlagen, welche nach der Migration weiterhin erforderlich sind, entsprechend in das Gruppen-Richtlinien-Konzept zu übernehmen und unter Umständen anzupassen.

### Migrationseinschränkungen

Während der Migrationsphase des Primären Domänen-Controllers (PDC) steht dieser nicht zur Verfügung, so dass clientseitig durchgeführte Anmeldungen und Ressourcenzugriffe über den Backup Domänen-Controller (BDC) laufen. Während der Migrationsdauer sind domänenspezifische Änderungen wie Passwort-Wechsel oder die Erstellung neuer Benutzerkonten nicht möglich. Nach erfolgter Migration des PDCs können sich die im Netz vorhandenen Windows-2000/XP-Clients nur noch an den vorhandenen Windows-Ser-

ver Domänen-Controllern anmelden, so dass eine zeitnahe Migration der verbleibenden Windows-NT-4.0-Domänen-Controller empfohlen wird. Des Weiteren sollte die sogenannte prä-Windows-2000-Kompatibilität aufgrund der erhöhten Funktionalität und der Vermeidung des anonymen Auslesens von Domäneninformationen deaktiviert werden, sobald innerhalb des Netzes keine entsprechende Abwärtskompatibilität diesbezüglich mehr erforderlich ist, zum Beispiel für Remote Access Services (RAS).

**Upgrade-Prüfung**

Im weiteren Installationsprozess wird das Active Directory eingerichtet und dabei die Objekte der Windows NT Security-Account-Manager-Datenbank (SAM-Datenbank) in die Active-Directory-Datenbank verschoben. Im Nachgang ist der Upgrade-Prozess hinsichtlich seiner erfolgreichen Durchführung zu testen und zu bewerten, bevor eine Abschaltung der bestehenden Windows NT 4.0-Struktur erfolgen kann. Eine detailgenaue Aufschlüsselung der zu prüfenden Komponenten hinsichtlich der korrekt umgesetzten Konfiguration und Funktion kann den Hilfsmitteln zum IT-Grundschutz (siehe *Prüfung der migrierten Verzeichnisdienst-Datenbank* in *Hilfsmittel zum Active Directory*) entnommen werden.

Nach erfolgter Migration des PDCs und ausführlicher Funktionstests sind die verbleibenden Windows-NT-4.0-Domänen-Controller ebenfalls zu migrieren. Auch hierbei ist im Vorfeld zu prüfen, ob diese den Systemanforderungen entsprechen. Aufgrund der Vorplanung werden an dieser Stelle die Serverrollen, wie z. B. Mitgliedsserver oder zusätzlicher Domänen-Controller, festgelegt, welche nach Einrichtung ebenfalls ausführlicher Tests zu unterziehen sind.

**Aktualisierung der Server-Umgebung**

Um den erweiterten Funktionsumfang insbesondere im Bereich der Active-Directory-Verwaltung von Windows-Server nutzen zu können, sollte in finaler Instanz eine Aktualisierung der Serverumgebung erfolgen. Hierbei ist jedoch zu beachten, dass ältere Versionen als die auf dem aktuellen System nach einer Systemaktualisierung nicht mehr unterstützt werden.

Prüffragen:

- Wird die Migration des Windows Verzeichnisdienstes geplant?
- Wird die Migration des Windows Verzeichnisdienstes zunächst in einer Testumgebung getestet?
- Wurden nach der Migration eine Aktualisierung der Serverumgebung vorgenommen?
- Wird nach der Migration getestet, ob alle Daten und Einstellungen korrekt übernommen wurden und funktionieren?

# M 4.318 Umsetzung sicherer Verwaltungsmethoden für Active Directory

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zur Administration einer Domäne werden Verantwortlichkeiten und Aufgabenfelder in weitere Untergruppen verteilt. Da die Benutzerkonten in den Verwaltungsgruppen "Dienste-Administratoren" (verantwortlich für das Ausführung der Aufgaben, die zur Bereitstellung des Verzeichnisdienstes erforderlich sind) und "Datenadministratoren" (verantwortlich für das Verwalten der Inhalte, welche in Active Directory gespeichert oder durch Active Directory geschützt werden) besonders weitreichende Zugriffsrechte haben, sind für deren Schutz entsprechende Vorkehrungen zu treffen:

**Dienste-Administratorkonten**

In jeder Domäne der Gesamtstruktur wird das Standardkonto "Administrator" bei der Installation angelegt. Als Standardkonto ist dieses Benutzerkonto im besonderen Maße Angriffen ausgesetzt. Da das Administrator-Konto nicht deaktiviert oder gelöscht werden kann, sollte es als Schutzmaßnahme umbenannt werden. Bei der Umbenennung ist darauf zu achten, dass auch die Beschreibung des Administrator-Kontos abgeändert wird. Nachdem das Konto umbenannt wurde, sollte anschließend ein unprivilegiertes Konto mit Namen "Administrator" eingerichtet werden, das im täglichen Betrieb nicht verwendet werden darf. Bei der Auswertung der Protokoll-Dateien kann so erkannt werden, ob es erfolgreiche oder nicht erfolgreiche Anmeldungen an dieses unprivilegierte Benutzerkonto gab. Dies würde auf einen Angriffsversuch hindeuten.

Die Anzahl der Dienste- und Datenadministratoren ist auf ein Minimum zu beschränken. Routinemäßige Administrations- und Verwaltungsaufgaben, z. B. Verwaltung der Domänen-Benutzer, die nicht die Konfiguration des Active Directory selbst betreffen, sollten nicht von Dienste-Administratoren durchgeführt werden, sondern an Datenadministratoren delegiert werden.

Die Administratorkonten sollten möglichst sparsam eingesetzt werden. Unnötige Anmeldung an der Domäne mit administrativen Rechten sollten vermieden werden. Daher sollten die Administratoren einer Institution für alltägliche, nichtadministrative Aufgaben, z. B. Informationsbeschaffung im Internet, unprivilegierte Benutzerkonten verwenden.

Die Verwaltung von Dienste-Administratorkonten darf ausschließlich von Mitgliedern der Dienste-Administratorgruppe durchgeführt werden. Insbesondere Benutzer mit weniger Privilegien, z. B. Datenadministratoren, dürfen keine Änderungen an Dienste-Administratorkonten vornehmen, da sich die weniger privilegierten Nutzer ansonsten erweiterte Rechte einräumen könnten.

Daher sollte zur Verwaltung der Dienste-Administratorkonten eine eigene Organisationseinheit, z. B. Dienst-Admins, in der Benutzerverwaltung des Active Directory angelegt werden. Die Berechtigungen für diese Unterstruktur müssen dabei wie folgt gewählt werden:

- Vererbung der Berechtigungen von übergeordneten Objekten deaktivieren

- Zugriffsberechtigungen auf die einzurichtende Organisationseinheit (inklusive untergeordnete Objekte)
  - Administratoren: Vollzugriff
  - Organisations-Admins: Vollzugriff
  - Domänen-Admins: Vollzugriff
- Prä-Windows-2000-kompatible Zugriffsberechtigungen für Benutzerobjekte, falls zutreffend
  - Inhalt auflisten
  - Alle Eigenschaften lesen
  - Berechtigungen lesen

Die Dienste-Administratorgruppen (Domänen-Admins, Organisations-Admins und Schema-Admins) werden anschließend in die neue Unterstruktur verschoben. Darüber hinaus sind die administrativen Benutzerkonten der Domänenadmins in die Organisationseinheit "Benutzer und Gruppen" und die Konten der Arbeitsstationen in die Organisationsstruktur "Administrator-Arbeitsstationen" der neuen Unterstruktur zu verschieben. Dabei ist zu beachten, dass Domänen-Controller-Konten nicht verschoben werden dürfen.

Zusätzlich sollten sowohl die Protokollierung von Änderungen, Löschungen und Einrichtung von Dienste-Administratorkonten und Arbeitsstationen sowie Änderungen an den Richtlinien überwacht werden.

Da einige der vordefinierten Dienste-Administratorkonten nicht in die neu erstellte Unterstruktur verschoben werden können, müssen diese Konten gesondert geschützt werden.

Im Active Directory werden die geschützten Dienste-Administratorkonten regelmäßig überprüft. Dabei werden die Sicherheitseinstellungen der geschützten Konten mit den Sicherheitsbeschreibungen des AdminSDHolder-Objekts (im Systemcontainer "CN=AdminSDHolder, CN=System, DC=Domänen-name") überschrieben. Der entsprechende Prozess, mit dessen Hilfe das Überschreiben angestoßen wird, startet nach fest vorgegebenen Intervallen (15 Minuten nach dem Systemstart und anschließend jede halbe Stunde).

Dieser Mechanismus gilt auf Windows-2000-Server-Systemen für die Benutzergruppen "Administratoren", "Domänen-Admins", "Organisations-Admins" und "Schema-Admins". In der Betriebssystemversion Windows Server 2003 wurde der Mechanismus auf die Gruppen "Serveroperatoren", "Kontenoperatoren", "Sicherungsoperatoren", "Druckoperatoren" und "Zertifikat-Herausgeber" erweitert.

Detaillierte Hinweise für die einzustellenden Berechtigungen auf das AdminSDHolder-Objekt können den Hilfsmitteln zum IT-Grundschutz (siehe *Berechtigungen auf AdminSDHolder-Objekt* in *Hilfsmittel zum Active Directory*) entnommen werden.

Die Personen der Dienste-Administratorengruppen müssen sowohl vertrauenswürdig sein, als auch über ausreichend sichere Kenntnisse hinsichtlich der Active-Directory-Administration verfügen. Damit eine geradlinige Umsetzung der Sicherheitsrichtlinien der Institution gewährleistet werden kann, müssen die Dienste-Administratoren mit den entsprechenden Richtlinien vertraut sein.

Die Mitgliederliste der Dienste-Administratorgruppen darf ausschließlich aus Benutzern der eigenen Active-Directory-Gesamtstruktur bestehen. Wird Dienste-Administratoren aus entfernten Domänen vertraut, so vertraut die Institution automatisch auch den Sicherheitsmaßnahmen der entfernten Institution.

Da diese Sicherheitsmaßnahmen in der Regel nicht beeinflusst werden können, ist für institutionsfremde Benutzer ein Benutzerkonto in der eigenen Gesamtstruktur einzurichten. Hierdurch können die Zugriffe auf die eigene Domäne besser reglementiert werden und es wird verhindert, dass Benutzer auf die Domäne zugreifen, deren Rechte aufgrund der automatischen Vertrauensregelung nicht bekannt sind.

Aufgrund der weitreichenden Berechtigungen sind Dienste-Administratorkonten bevorzugte Angriffsziele. Daher wird bei erhöhten Sicherheitsanforderungen empfohlen, die Zugehörigkeitsinformationen aller Dienste-Administratorgruppen für nicht privilegierte Benutzer zu unterbinden.

Dabei ist jedoch zu beachten, dass einige Serverapplikationen den lesenden Zugriff auf die Mitgliederliste der Dienste-Administratoren für einen störungsfreien Betrieb brauchen. Daher ist im ersten Schritt zu ermitteln, ob derartige Serveranwendungen in der Institution verwendet werden.

Die Benutzerkonten, unter denen die identifizierten Serverprozesse gestartet werden, sind in einer eigenen Gruppe, z. B. Serveranwendungen, zusammenzufassen. Anschließend werden folgende Berechtigungen in der ACL des AdminSDHolder Objekts für diese Gruppe vergeben:

- Inhalt auflisten
- Alle Eigenschaften lesen
- Berechtigungen lesen

Der Zugriff kann somit auf die authentisierten Benutzer eingegrenzt werden, die über einen lesenden Zugriff auf die Mitgliederliste verfügen müssen.

Da das Verbergen der Gruppenzugehörigkeit für Dienste-Administratorgruppen Auswirkungen auf den Betrieb haben kann, wird dringend empfohlen, die oben beschriebenen Änderungen am AdminSDHolder Objekt im Vorfeld auf mögliche Auswirkungen zu überprüfen.

Die Mitglieder der Active-Directory-Gruppe "Sicherungsoperatoren" sind als Dienstadministratoren anzusehen, da sie Systemdateien des Domänen-Controllers wiederherstellen können. Die Anzahl der Mitglieder dieser Benutzergruppen sollte möglichst klein gehalten werden. Daher sind Administratoren, die für die Sicherung und Wiederherstellung von Anwendungsservern innerhalb des ActiveDirectory verantwortlich sind, nicht in die Active-Directory-Gruppe "Sicherungsoperatoren" einzutragen. Vielmehr sind die entsprechenden Benutzerkonten in den lokalen Gruppen "Sicherungsoperatoren" der Anwendungsserver einzutragen.

Die Active-Directory-Gruppe "Kontenoperatoren" sollte nicht für die Datenverwaltung, z. B. Kontenverwaltung, verwendet werden, da Mitglieder die Möglichkeit haben, die eigenen Rechte auszuweiten. Aus Sicherheitsgründen sollten sich daher in der Gruppe "Kontenoperatoren" keine Mitglieder befinden.

Ähnliches gilt für die Active-Directory-Gruppe "Schema-Admins". Da Änderungen am Schema des ActiveDirectory normalerweise sehr selten sind, sollten vertrauenswürdige Administratoren nur solange zur Gruppe "Schema-Admins" hinzugefügt werden, wie die Berechtigungen auch tatsächlich benötigt werden. Sobald die Änderungen am Schema erfolgt sind, sollten die Mitglieder wieder aus der Gruppe entfernt werden.

Die Benutzerkonten der Gruppen "Organisations-Admins" und "Domänen-Admins" in der Stammdomäne der Active-Directory-Gesamtstruktur einer Institution sind aufgrund der weitreichenden Berechtigungen besonders zu schüt-

zen. Daher sollten jedem dieser Konten zwei Administratoren zugewiesen und das Passwort in zwei Hälften geteilt werden. Jedem der beiden Administratoren darf jeweils nur eine Hälfte des Passworts bekannt sein, damit innerhalb des Benutzerkontos nur unter Beachtung des Vier-Augen-Prinzips gearbeitet werden kann. So kann die unbemerkte Nutzung von Dienste-Administratorkonten der Stammdomäne in der Gesamtstruktur des Active Directory vermieden werden.

Alternative Methoden zur Durchsetzung des Vier-Augen-Prinzips, wie z. B. die Verwendung von Chipkarten, wobei PIN und Chipkarte voneinander getrennt werden, sind ebenfalls denkbar.

Neben der Absicherung der Dienste- und Datenadministratorkonten, sind ebenfalls die Arbeitsplätze der Administratoren wie folgt abzusichern:

- Die Benutzerkonten der Administratoren sollten so eingerichtet werden, dass die Konten nur von bestimmten Arbeitsplätzen aus verwendet werden können. Kompromittierte Administratorkonten können so nur noch von bestimmten Arbeitsstationen aus verwendet werden.
- Nach 5 Minuten Inaktivität durch den Benutzer ist die automatische Sperrung zu aktivieren. Dabei ist darauf zu achten, dass zur Aufhebung der Konsolensperrung keine zwischengespeicherten Daten verwendet werden dürfen, sondern zwingend eine erneute Authentisierung am Domänen-Controller erfolgen muss. Dazu muss der Wert des Registrierungsschlüssels *ForceUnlockLogon* im Verzeichnis *HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon* auf den Wert "*1*" gesetzt werden. Dieser Registrierungseintrag gilt für die Windows-Versionen 2000, XP und Vista.
- Auf den Arbeitsstationen der Administratoren müssen Viren-Schutzprogramme eingesetzt werden.
- Anwendungen sollten nicht im Kontext der Administratoren ausgeführt werden. Beim Hinzufügen einer neuen Arbeitstation zur Domäne ist daher darauf zu achten, dass die Domänen-Admins nicht automatisch zu der lokalen Gruppe der Administratoren der Arbeitsstation hinzugefügt werden.
- Prozesse sollten nicht mit den Berechtigungen der Domänen-Admins ausgeführt werden. Stattdessen sollte der Sicherheitskontext der lokalen Administratorgruppe der jeweiligen Arbeitsstation verwendet werden.
- Der Datenverkehr zwischen den Arbeitsstationen der Administratoren und den Domänen-Controllern ist entsprechend abzusichern. Hierzu sollten die LDAP-Paketsignaturen aktiviert werden (Dafür ist der Registrierungsschlüssel LDAPClientIntegrity in dem Windows-Registry-Pfad *HKLM\System\CurrentControlSet\Services\LDAP* auf den Wert "*2*" zu setzen). Dabei ist zu berücksichtigen, dass diese Option bei Windows 2000 Server erst ab ServicePack 3 zur Verfügung steht.

Für die Remoteadministration von Domänen-Controllern sollten ausschließlich Protokolle verwendet werden, die eine Verschlüsselung des Datenverkehrs ermöglichen.

**Datenadministratorkonten**

Grundsätzlich hängen die Strukturen und Berechtigungen der Datenadministratorenkonten stark von der Struktur der jeweiligen Institution ab. Für die im Folgenden aufgeführten Aspekte ist daher zu verifizieren, ob sie sich mit den Anforderungen der Organisation verbinden lassen.

Die Delegierung der Datenverwaltung erfolgt über Gruppen, denen die entsprechenden Benutzerrechte zugewiesen werden. Auf die Mitglieder dieser Gruppen werden die Gruppenrichtlinieneinstellungen angewendet. Nach die-

sen Schritten genügt es, für die Delegierung Benutzerkonten zu den erstellten Gruppen hinzuzufügen. Das gewährleistet größtmögliche Sicherheit und ermöglicht es den Administratoren, ihre übertragenen Aufgaben weiterhin zu erfüllen.

Der Zugriff auf die Gruppenrichtlinien ist auf vertrauenswürdige Personen einzuschränken. Benutzer, deren Konten die Erstellung und Änderung von Gruppenrichtlinieneinstellungen zulassen, können anderen Benutzerkonten über diese Richtlinien höhere Berechtigungen einräumen und müssen folglich vertrauenswürdig sein.

Datenadministratoren werden als Ersteller eines Objektes gleichzeitig auch dessen Besitzer. Im Zugriffssteuerungsmodell von Windows Server 2003 verfügt der Besitzer eines Objektes über Vollzugriff auf dieses Objekt. Dazu gehört auch die Möglichkeit, die ACL des Objektes zu ändern. Der Besitzer eines Objektes verfügt außerdem über Vollzugriff auf alle untergeordneten Objekte. Er hat des Weiteren die Möglichkeit, die ACL-Vererbung von übergeordneten Objekten zu sperren und den Zugriff von Dienste-Administratoren auf dieses Objekt zu blockieren.

Es ist sicherzustellen, dass die Gruppen "Administratoren" bzw. "Domänenadministratoren" in den einzelnen Domänen Besitzer des Domänenstammobjektes für die jeweilige Domänenpartition sind. Die Besitzer dieser Partitionsstammobjekte können über vererbliche Access Control Entries (ACEs) die Sicherheitseinstellungen aller anderen Objekte in dieser Partition ändern.

Es ist sicherzustellen, dass bei der Planung von Kontenverwaltungsaufgaben die Gruppenzugehörigkeit in einem delegierten Bereich von einem einzigen Datenadministrator geändert wird oder aber die Aufgabe unter Abstimmung weniger Datenadministratoren erfolgt. Falls im Rahmen der Replikation ein Konflikt zwischen zwei gleichzeitigen Änderungen der Gruppenzugehörigkeit durch verschiedene Domänen-Controller festgestellt wird, hat die aktuellste Änderung an einem Konto Vorrang. Bis zur Serverrepliktation ist die auf dem jeweiligen Server eingerichtete Änderung gültig.

Der Einsatz von domänenlokalen Gruppen für die Steuerung der Leseberechtigung für Objektattribute, die in den globalen Katalog repliziert werden, sollte vermieden werden, da hierbei fälschlicherweise der Objektzugriff verweigert oder gewährt werden könnte. Um dennoch Zugriffe auf die Daten des globalen Katalogs zu steuern, sollten stattdessen globale oder universelle Gruppen verwendet werden.

Prüffragen:

- Sind die Benutzerkonten der Dienste-Administratoren und der Datenadministratoren des Active Directory angemessen abgesichert?
- Ist die Anzahl der Dienste-Administratoren und der Datenadministratoren des Active Directory das notwendige Minimum vertrauenswürdiger Personen reduziert?
- Wurde das Standardkonto "Administrator" umbenannt und ein unprivilegiertes Konto mit dem Namen "Administrator" erstellt?
- Werden alltägliche, nichtadministrative Aufgaben mit unprivilegierten Benutzerkonten durchgeführt?
- Ist sichergestellt, dass die Verwaltung von Dienste-Administratorkonten ausschließlich von Mitgliedern der Dienste-Administratorgruppe erfolgt?
- Ist die Gruppe "Kontenoperatoren" leer?
- Werden Administratoren der Gruppe "Schema-Admins" nur temporär für den Zeitraum der Schema-Änderungen zugewiesen?

- Existiert für die Administration der Stammdomäne für die Gruppen "Organisations-Admins" und "Domänen-Admins" ein Vier-Augen-Prinzip?
- Sind die Arbeitsplätze zur Administration des Active Directory ausreichend abgesichert?
- Wird bei Remoteadministration der Domänen-Controller der Datenverkehr verschlüsselt?
- Wird sichergestellt, dass die Gruppen "Administratoren" bzw. "Domänenadministratoren" Besitzer des Domänenstammobjektes der jeweiligen Domäne sind?
- Wird der Einsatz von domänenlokalen Gruppen für die Steuerung der Leseberechtigung für Objektattribute vermieden?

# M 4.319 Sichere Installation von VPN-Endgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Mit dem Aufbau eines VPNs kann begonnen werden, sobald die erforderlichen Komponenten dafür beschafft worden sind (siehe M 2.419 *Geeignete Auswahl von VPN-Produkten*). Grundvoraussetzung für den sicheren VPN-Betrieb ist, dass die Installation und Konfiguration aller Komponenten gewissenhaft erfolgt und sich mit den gewählten VPN-Produkten auch tatsächlich die geforderten Sicherheitsfunktionen umsetzen lassen.

Zusätzlich muss die Sicherheit der IT-Systeme gewährleistet werden, auf denen die VPN-Komponenten eingesetzt werden. Dies betrifft besonders IT-Systeme, auf denen ein Standard-Betriebssystem installiert ist und das als VPN-Endpunkt betrieben wird (Beispiel: Linux-System mit VPN-Unterstützung). Daher sind zunächst die generellen Sicherheitsmaßnahmen für jedes dieser Betriebssysteme umzusetzen, wie sie in den jeweiligen Bausteinen der IT-Grundschutz-Kataloge beschrieben werden. Es gibt auch VPN-Komponenten, bei denen die Konfiguration der Plattform vom Hersteller vorgegeben ist und nicht geändert werden kann (VPN-Appliances). Der Einsatz solcher VPN-Geräte spart einerseits Zeit und es wird im Gegensatz zu einer individuellen Lösung weniger fachkundiges IT-Personal benötigt, z. B. für die Konfiguration des Betriebssystems. Andererseits muss beim Einsatz von Appliances den Vorgaben des Herstellers vertraut werden.

Im Rahmen der Installation eines VPNs sollten ebenfalls folgende Punkte betrachtet werden:

- Während der Installationsphase sollten weder Benutzer noch Dritte auf das VPN oder Teile davon zugreifen dürfen. Es dürfen in dieser Phase also keine Verbindungen zu anderen Netzen vorhanden sein.
- Es muss sichergestellt werden, dass die Installation aller VPN-Komponenten durch qualifiziertes Personal durchgeführt wird. Dies kann vor allem dann schwierig sein, wenn die zu vernetzenden Standorte geografisch weit voneinander entfernt sind. Beispielsweise muss geklärt werden, ob die nötigen Personalressourcen für eine VPN-Installation auch in anderen Ländern zur Verfügung stehen. Auch VPN-Endpunkte auf mobilen IT-Systemen, beispielsweise Laptops von Außendienstmitarbeitern, dürfen nur von qualifiziertem IT-Personal installiert werden.
- Die Installation und Konfiguration der VPN-Komponenten ist zu dokumentieren. Dies kann entweder durch eine separate Installationsdokumentation erfolgen oder aber durch eine Bestätigung, dass die Installation mit den Planungsvorgaben übereinstimmt. Abweichungen von der festgelegten Systemarchitektur (beispielsweise zusätzliche Verbindungen) müssen hierbei begründet und dokumentiert werden. Die Qualität der Dokumentation spielt im Hinblick auf die kontinuierliche Verbesserung des VPNs eine wesentliche Rolle.
- Die korrekte Funktion jeder einzelnen Komponente muss überprüft werden (z. B. durch Funktionsprüfungen bzw. Selbsttests oder Lasttests).
- Bei den eingesetzten Produkten müssen vor der Inbetriebnahme alle aktuellen sicherheitsrelevanten Patches bzw. Firmware-Updates eingespielt werden.
- Für jede sicherheitsrelevante Einstellung muss ein Funktionstest der Sicherheitsmechanismen durchgeführt werden. Beispielsweise sollten die

Verschlüsselung der Verbindung sowie die eingesetzten Authentisierungsfunktionen mittels eines Netzanalyse-Tools überprüft werden (siehe auch M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation*).
- Bevor das System in den Produktiveinsatz genommen wird, muss es in einer vom Produktivnetz getrennten Umgebung aufgebaut und entsprechend getestet werden. Ebenfalls ist es empfehlenswert, bereits in der Testumgebung Performance-Messungen und einen Testlauf der Schlüsselverteilung durchzuführen. Nach Abschluss der Installation ist die korrekte Funktion des Gesamtsystems zu überprüfen (Abnahme und Freigabe der Installation). Bei allen durchgeführten Tests ist darauf zu achten, dass nur die zum Test befugten Personen Zugriff auf das VPN erhalten.

Ist die grundlegende Installation erfolgt, so kann mit der in Maßnahme M 4.320 *Sichere Konfiguration eines VPNs* ausgeführten Konfiguration begonnen werden. Diese muss das System in einen sicheren Betriebszustand überführen, damit anschließend der laufende Betrieb aufgenommen werden kann. Für den reibungslosen Betrieb des VPNs sind die in Maßnahme M 4.321 *Sicherer Betrieb eines VPNs* erwähnten Handlungsweisen essenziell. Die dabei gewonnenen Erkenntnisse und Korrekturmaßnahmen müssen angemessen dokumentiert und in das Feinkonzept eingearbeitet werden.

**Beispiel:**

Nachfolgend werden die wesentlichen Punkte bei der Installation eines VPN-Systems beispielhaft dargestellt. Da die jeweiligen Konfigurationen von Hersteller zu Hersteller differieren, wird nur ein Grundgerüst vorgestellt, welches keinen Anspruch auf Vollständigkeit erhebt.

Für einen Remote Access-VPN-Client sollten während der Installation folgende Punkte beachtet werden:

- Die Server-Funktionen des VPN-Dienstes müssen deaktiviert werden. Dies erfolgt dadurch, dass auf allen Geräten, die für Remote Access verwendet werden können (z. B. Modem, ISDN-Karte, VPN-Adapter), nur ausgehende Anrufe erlaubt werden.
- Für den VPN-Client sind nur die für Remote Access zugelassenen Protokolle freizugeben.
- Die im VPN-Sicherheitskonzept festgelegten Parameter bezüglich Integrität, Authentizität und Vertraulichkeit müssen entsprechend konfiguriert werden.

Für einen Remote Access-VPN-Server sollten folgende Punkte beachtet werden:

- Die Client-Funktionen des VPN-Dienstes müssen deaktiviert werden. Dies erfolgt dadurch, dass auf allen Geräten, die für Remote Access verwendet werden können, nur eingehende Anrufe erlaubt werden.
- Für den VPN-Server sind nur die über Remote Access zugelassenen Protokolle freizugeben.
- Die im VPN-Sicherheitskonzept festgelegten Parameter bezüglich Integrität, Authentizität und Vertraulichkeit müssen entsprechend konfiguriert werden.
- Die Einwahl sollte nur berechtigten Benutzern gestattet werden.

Prüffragen:

- Falls keine Appliance eingesetzt wird: Ist das zugrunde liegende Betriebssystem der VPN-Plattform sicher konfiguriert?

- Steht für die Installation der VPN-Komponenten qualifiziertes Personal zur Verfügung?
- Wurden die Installation und Konfiguration der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben dokumentiert?
- Sind alle aktuellen Patches und Updates auf den VPN-Komponenten eingespielt?
- Wurden die Funktionen und Sicherheitsmechanismen der VPN-Komponenten getestet?

# M 4.320 Sichere Konfiguration eines VPNs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Alle VPN-Komponenten müssen sorgfältig konfiguriert werden, da es durch eine ungeeignete Konfiguration von VPN-Komponenten zu einem Verlust der Verfügbarkeit des Netzes oder Teilen davon kommen kann. Der Verlust der Vertraulichkeit von Informationen oder der Datenintegrität ist ebenfalls denkbar. Unabhängig davon, ob es sich bei VPN-Komponenten um dedizierte Hardware (Appliances) oder softwarebasierte Systeme handelt, spielt daher die korrekte Konfiguration der beteiligten Komponenten eine wesentliche Rolle. Da ein VPN aus mehreren Komponenten und deren Konfiguration besteht, ergibt sich eine erhöhte Komplexität der Gesamtkonfiguration. Das Ändern eines Konfigurationsparameters bei einer Komponente kann im Zusammenspiel mit den anderen Komponenten zu Sicherheitslücken, Fehlfunktionen und/oder Ausfällen führen.

Da die Konfiguration eines VPN-Systems in der Regel Veränderungen unterworfen ist (z. B. durch Personaländerungen, neue Nutzungsszenarien, Systemerweiterungen), kann nicht davon ausgegangen werden, dass es genau eine sichere (und statische) Konfiguration gibt, die einmal eingestellt und nie wieder verändert wird. Vielmehr wird die Konfiguration üblicherweise fortlaufend geändert. Es ist Aufgabe der für das VPN zuständigen Administratoren, dass jeweils nur sichere Versionen der Systemkonfiguration definiert werden und das System von einer sicheren Konfiguration in die nachfolgende sichere Konfiguration überführt wird. Alle Änderungen und die jeweils aktuelle Einstellungen müssen nachvollziehbar dokumentiert sein.

### Grundeinstellungen

Die Grundeinstellungen, die vom Hersteller oder Distributor einer VPN-Komponente vorgenommen werden, sind nicht unbedingt auf Sicherheit, sondern auf eine einfache Installation und Inbetriebnahme optimiert. Der erste Schritt bei der Grundkonfiguration muss daher sein, die Grundeinstellungen zu überprüfen und entsprechend den Vorgaben der Sicherheitsrichtlinie anzupassen. Standardpasswörter müssen durch eigene, ausreichend komplexe Passwörter ersetzt werden.

### Server-Konfiguration

Die sichere Konfiguration der VPN-Server-Software erfordert, dass die durch die Software angebotenen und im vorliegenden Einsatzszenario sinnvollen Sicherheitseinstellungen auch aktiviert sind und genutzt werden können. Die Nutzung von bestimmten Sicherheitseinstellungen setzt voraus, dass auch andere Komponenten des VPNs entsprechende Funktionen besitzen bzw. entsprechend konfiguriert werden können. So ist z. B. bei der Nutzung der Rufnummernübertragung (Calling Line Identification Protocol - CLIP) sicherzustellen, dass diese für den gewählten Anschluss auch aktiviert ist. Damit die Benutzer-Identifikation beispielsweise beim Zugriff über das Internet über X.509-Zertifikate erfolgen kann, muss dem VPN der Speicherort der Benutzerzertifikate bekannt sein.

Dazu muss die VPN-Software entweder externe Authentisierungsserver unterstützen oder eine eigene Zertifikatsverwaltung anbieten.

Daher sollte vorab überprüft werden, ob alle angebotenen Sicherheitsmechanismen auch genutzt werden können oder ob hierzu andere bzw. zusätzliche Hard- oder Software benötigt wird. Im laufenden Betrieb muss dann regelmäßig die Korrektheit der Einstellungen überprüft werden.

**Client-Konfiguration**

Für die sichere Konfiguration der VPN-Client-Software gelten ähnliche Anforderungen wie für die Server-Software. Damit Client und Server in sicherer Art und Weise kommunizieren können, ist auf eine konsistente Konfiguration der beteiligten Komponenten zu achten (z. B. beim benutzten Verfahren zur Kommunikationsabsicherung).

Zusätzlich ist darauf zu achten, dass zum VPN-Zugang benötigte Passwörter nicht durch die Software gespeichert werden, auch wenn dies vielfach angeboten wird. Kann die Speicherung technisch nicht verhindert werden, muss sie allen Benutzern untersagt werden. Die Benutzer sollten über die Sicherheitsproblematik gespeicherter Passwörter aufgeklärt werden.

**Einrichten von standardisierten IT-Systemen**

Die sichere und konsistente Konfiguration von Client und Server kann dadurch unterstützt werden, dass eine Standardkonfiguration für VPN-Clients (Hard- und Software) durch das VPN-Konzept festgelegt und durch organisatorische Maßnahmen durchgesetzt wird. Dadurch wird erreicht, dass nur eine feste Anzahl unterschiedlicher Client-Konfigurationen im Einsatz ist.

**Einrichtung von Zugangsnetzen**

Neben der Konfiguration des VPNs kann auch die Aufteilung der angebundenen Netze in Teilnetze der Zugriffssteuerung dienen. Aus Gründen der Informationssicherheit kann es daher zweckmäßig sein, so genannte Zugangsnetze (Access-Networks) einzurichten (siehe auch M 5.77 *Bildung von Teilnetzen*).

**Routing-Einstellungen**

Über die Routing-Einstellungen der für das VPN-System verwendeten Netzkoppelelemente sollte der Netz-Verkehrsfluss restriktiv gesteuert werden. Moderne Netzkoppelelemente lassen das selektive Weiterleiten von Paketen innerhalb erlaubter Netzverbindungen (Paketfilter-Funktion) zu. Auf diese Weise kann z. B. erreicht werden, dass ausschließlich Verbindungsanfragen an den HTTP-Dienst eines Servers weitergeleitet werden.

Auf VPN-Clients sollten nur autorisierte Benutzern zugreifen können. Besonderes bei mobilen Rechnern ist es wichtig, dass der Zugang zum VPN eingeschränkt wird. Wird der mobile Rechner gestohlen, könnten sich ansonsten Unberechtigte in das VPN einwählen. Die Benutzer müssen sich daher strikt an die festgelegten Regelungen halten (z. B. sichere Authentisierung und Diebstahlschutz, siehe auch Baustein B 3.203 *Laptop*).

Mobile VPN-Clients sollten so konfiguriert werden, dass bei gestarteter VPN-Client-Software der gesamte Datenverkehr nur über die VPN-Verbindung geleitet wird.

Datenverbindungen an der VPN-Verbindung vorbei in andere Netze sollten unterbunden werden. Viele VPN-Client-Produkte bieten diese Einstellungsmöglichkeit als Funktionalität an.

**Zugriffsberechtigungen**

Es muss darauf geachtet werden, dass eventuell vorhandene Testzugänge und Benutzerkennungen (beispielsweise von Testläufen bei der Installation) wieder entfernt werden. Weiterhin müssen die erteilten Zugriffsrechte regelmäßig überprüft werden, damit einerseits alle benötigten Funktionalitäten genutzt und andererseits fälschlich vergebene Zugriffsrechte nicht missbraucht werden können.

**Remote-Zugriff**

Aktive Netzkomponenten bieten aus Wartungsgründen in der Regel die Möglichkeit eines Remote-Zugriffs. Remote-Zugriffe für die Administration dürfen nur erlaubt werden, wenn gewährleistet ist, dass Benutzername und Passwort nicht im Klartext übertragen werden (wie beispielsweise bei Telnet). Besteht die Möglichkeit einer lokalen Konfiguration, so sollte diese vorgezogen und der Remote-Zugriff deaktiviert werden.

**Login-Banner**

Bei der Anmeldung an VPN-Komponenten wird oft eine relativ ausführliche Anmelde-Nachricht angezeigt. In dieser Login-Nachricht können Informationen (beispielsweise Modell- oder Versionsnummer und Software-Version) enthalten sein, die einem potentiellen Angreifer von Nutzen sein können. Sofern möglich muss die Standard-Login-Nachricht durch eine angepasste Version ersetzt werden, die diese Informationen nicht mehr enthält. Die Modell- und Versionsnummer des Geräts und die Version des Betriebssystems sollte aus Sicherheitsgründen unter keinen Umständen vom Login-Banner verraten werden.

**Schnittstellen**

Nicht genutzte Schnittstellen von VPN-Komponenten sind häufig standardmäßig nicht deaktiviert. Im Zuge der Erstinstallation und Konfiguration müssen diese daher deaktiviert werden, um die gebotene Angriffsfläche zu verkleinern.

**Protokollierung**

VPN-Komponenten bieten in der Regel Möglichkeiten der Protokollierung, welche auf jeden Fall aktiviert und sorgfältig eingerichtet werden müssen. Die Auswertung dieser Informationen ermöglicht es, die korrekte Funktion des Geräts zu beurteilen und Angriffsversuche zu erkennen. Mit Hilfe der Protokollierungsinformationen kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden. Die Protokollfunktionen müssen sorgfältig konfiguriert werden, da nur bei einer sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert werden können.

Neben einer geeigneten Speicherung der Informationen muss für eine möglichst zeitnahe Auswertung der gewonnenen Daten gesorgt werden (siehe M 4.321 *Sicherer Betrieb eines VPNs*). Entsprechende Bestimmungen des Datenschutzes sind zu beachten.

**Dokumentation**

Es sollte dokumentiert werden, welche Einstellungen der VPN-Komponenten im Rahmen der Grundkonfiguration überprüft, sowie ob und gegebenenfalls wie sie geändert wurden. Die Dokumentation muss so beschaffen sein, dass im Notfall auch eine andere Person als der eigentliche Administrator ohne vor-

herige Kenntnis des Systems nachvollziehen kann, was getan wurde. Bei einem Ausfall sollte es möglich sein, alleine mit Hilfe der Dokumentation das System wiederherzustellen. Hierbei sollte auch die in M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen* erläuterte Vorgehensweise beachtet werden.

**Standortbasierte Authentisierung**

Eine Authentisierung für ein Site-to-Site- oder End-to-Site-VPN kann nicht nur nutzer-, sondern auch standortbasiert erfolgen. Eine eindeutige Identifizierung der jeweiligen Gegenstelle muss dabei gewährleistet werden können. Dies setzt voraus, dass bereits behörden- bzw. unternehmensweit eine zentrale Standortverwaltung existiert. Das VPN baut lediglich auf dieser auf. Für Remote-Access-Zugänge in das interne Netz einer Institution sei hierbei auf die Maßnahme M 4.113 *Nutzung eines Authentisierungsservers bei Remote-Access-VPNs* hingewiesen.

**Änderungsmanagement**

Änderungen an der VPN-Systemkonfiguration sollten einem organisatorischen Prozess unterliegen, der sicherstellt, dass das VPN nur mit geprüften Konfigurationen aktiviert wird. Alle Änderungen sollten dokumentiert und genehmigt sein.

Hinweis: Das Hinzufügen oder Löschen von VPN-Benutzerkennungen erfordert in der Regel keine Änderung der VPN-Systemkonfiguration, da diese Änderungen oft durch die Benutzerverwaltung des Betriebssystems oder eines Authentisierungsservers (z. B. RADIUS, TACACS+) erfolgen.

**Regelmäßige Prüfung der VPN-Konfiguration**

Die Konfiguration aller VPN-Komponenten sollte regelmäßig überprüft werden. Dabei ist sicherzustellen, dass alle Vorgaben der VPN-Sicherheitsrichtlinie umgesetzt sind und die Einstellungen keine Schwachstellen aufweisen.

Bei der VPN-Konfiguration handelt es sich um die eigentliche Realisierung der VPN-Sicherheitsrichtline. Es müssen alle dort festgelegten Sicherheitsanforderungen an das VPN entsprechend umgesetzt werden. Die hier angeführten Themenbereiche sind im Rahmen der VPN-Systemplanung und des VPN-Betriebes zu konkretisieren, zu erweitern und anzupassen. Grundsätzlich ist die Konfiguration der beteiligten Komponenten jedoch immer von lokalen Gegebenheiten oder Anforderungen abhängig. Eine allgemein gültige Anleitung kann nicht gegeben werden, da die beteiligten Komponenten im unternehmensspezifischen Kontext betrachtet werden müssen.

Prüffragen:

- Wurden die Grundeinstellungen aller VPN-Komponenten überprüft und entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst?
- Wurden die Standardpasswörter aller VPN-Komponenten durch eigene, ausreichend komplexe Passwörter ersetzt?
- Werden die Sicherheitsmechanismen, die vom VPN-Server angeboten werden und im vorliegenden Einsatzszenario sinnvoll sind, auch aktiviert und genutzt?
- Wird die Korrektheit der Sicherheitseinstellungen für den VPN-Server regelmäßig überprüft?
- Ist sichergestellt, dass VPN-Server und VPN-Clients konsistent konfiguriert werden?

- Ist technisch oder organisatorisch sichergestellt, dass Benutzer-Passwörter für den VPN-Zugang nicht gespeichert werden?
- Sind die Routing-Einstellungen der Netzkoppelelemente, die für das VPN verwendet werden, restriktiv konfiguriert?
- Sind alle mobilen VPN-Clients so konfiguriert, dass der gesamte Datenverkehr nur über die VPN-Verbindung transportiert wird?
- Sind alle eventuell vorhandenen Testzugänge und -konten auf den VPN-Komponenten entfernt?
- Falls für die Administration ein Fernzugriff erforderlich ist: Ist sichergestellt, dass Benutzername und Passwort nicht im Klartext übertragen werden?
- Falls die Login-Meldung angepasst werden kann: Ist die Login-Meldung so definiert, dass die Modell- und Versionsnummer des Gerätes sowie die Version des Betriebssystems nicht angezeigt werden?
- Sind alle nicht genutzten Schnittstellen der VPN-Komponenten deaktiviert?
- Ist die Protokollierung im VPN aktiviert und geeignet konfiguriert?
- Ist das VPN-System so dokumentiert, dass notfalls auch fachkundige Dritte das System neu aufbauen können?
- Werden alle Änderungen an der VPN-Konfiguration genehmigt, geprüft und dokumentiert?

# M 4.321 Sicherer Betrieb eines VPNs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

VPNs sind aufgrund der übertragenen Daten attraktive Ziele für Angreifer und müssen daher sicher betrieben werden. Voraussetzungen hierfür sind die sichere Installation (M 4.319 *Sichere Installation von VPN-Endgeräten*) und Konfiguration der beteiligten Hard- und Softwarekomponenten (M 4.320 *Sichere Konfiguration eines VPNs*). Zusätzlich müssen alle organisatorischen Abläufe definiert und umgesetzt worden sein (z. B. Meldewege und Zuständigkeiten). Hierfür sind die in Maßnahme M 2.418 *Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung* gegebenen Empfehlungen zu beachten.

Immer häufiger ist es erforderlich, dass die VPN-Verbindungen von Institutionen kontinuierlich stabil betriebsbereit sind. In vielen Institutionen müssen sie sogar rund um die Uhr verfügbar sein (24/7-Betrieb). Für den reibungslosen Ablauf des VPN-Betriebs muss daher ein Betriebskonzept erstellt und auch ein entsprechendes Notfallkonzept ausgearbeitet werden (siehe M 6.109 *Notfallplan für den Ausfall eines VPNs*). Bei der Erstellung eines Betriebskonzepts müssen insbesondere die folgenden Aspekte beachtet werden.

**Monitoring**

Hierbei wird Monitoring im Sinne von Qualitätsmangement verstanden. So muss die Dienstequalität eines VPNs laufend gemessen werden. Die gewonnenen Daten sollten zu Managementreports zusammengefasst und regelmäßig (beispielsweise monatlich oder quartalsweise) dem IT-Management vorgelegt werden. Die gemessenen Kennwerte dienen der laufenden Feinabstimmung von Dienstgüte und Bandbreitenverteilung im VPN. Auf diese Weise können Engpässe sowie Soft- oder Hardwareprobleme frühzeitig erkannt werden. Hierbei muss auch überlegt werden, ob die VPN-Verfügbarkeit durch entsprechende SLAs (Service Level Agreements) oder OLAs (Operational Level Agreements) abgesichert werden muss. Unabhängig von den regelmäßigen Berichten müssen plötzlich auftretende Auffälligkeiten umgehend gemeldet werden, damit Probleme zeitnah behoben werden kann.

**Überwachungskonzept**

Im Gegensatz zum erwähnten Monitoring der Dienstequalität steht beim Überwachungskonzept die Sicherheit des VPNs im Vordergrund. Die gewonnenen Protokolldaten müssen gemäß der Sicherheitsrichtlinie (z. B. Zugriffsbeschränkungen) überprüft, ausgewertet und gegebenenfalls aus rechtlichen Gründen archiviert werden.

Die im Rahmen der Überwachung gewonnenen Informationen sollten regelmäßig durch einen sachkundigen Administrator überprüft werden. Durch den zusätzlichen Einsatz von spezieller Software zur Auswertung der Protokolldaten kann das bestmögliche Ergebnis erzielt werden. Wichtig ist, dass die Bestimmungen des Datenschutzes eingehalten werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

**Alarmierung**

Ein Alarmierungskonzept muss dafür sorgen, dass bei Entdeckung einer kritischen Situation die verantwortlichen Personen unverzüglich informiert werden. Dabei müssen vorher festgelegte Maßnahmen ergriffen und die Vorfälle entsprechend dokumentiert werden (siehe Baustein B 1.8 *Behandlung von*

*Sicherheitsvorfällen*). Zur Behebung von Ausfällen kann anschließend das mit Hilfe von M 6.109 *Notfallplan für den Ausfall eines VPNs* erstellte Notfallkonzept angewandt werden.

**Wartung**

Wartungsarbeiten an einem VPN sollten möglichst nicht im Echtbetrieb durchgeführt werden, also solange Benutzer darauf zugreifen können. Bei der Durchführung von Wartungsarbeiten muss immer sorgfältig vorgegangen werden. Für die Durchführung von Wartungsarbeiten oder Änderungen an den Systemen müssen die entsprechenden Verantwortlichkeiten im Vorhinein festgelegt werden.

Für Wartungen und Änderungen müssen Wartungsfenster definiert und in den Arbeitsablauf eingeplant werden. Art, Umfang, Zeitpunkt und Dauer von Wartungsarbeiten müssen rechtzeitig angekündigt werden, ebenso welche Dienste und Services betroffen sind. Im Anschluss an jede Wartung oder Änderung müssen die vorgenommenen Modifikationen dokumentiert und kontrolliert werden.

**Autorisierung bei Remote Access-VPNs**

Remote-Access-VPNs zeichnen sich oft dadurch aus, dass sich nicht nur wenige, sondern viele VPN-Gegenstellen im VPN einwählen müssen. In der Regel sind dies Benutzer, deren Passwörter sich regelmäßig ändern können.

Damit eine geregelte Benutzer-Authentisierung (z. B. via RADIUS, TACACS, TACACS+) beim Fernzugriff möglich ist, muss die Konsistenz der Authentisierungsdaten sichergestellt sein. Dies kann durch zentrale Verwaltung der Daten (Authentisierungsserver) oder durch periodischen Abgleich geschehen.

**Einwahl über Wählverbindungen bei Remote Access-VPNs**

Je nachdem, welche VPN-Varianten eingesetzt werden, kann die Einwahl auch über Datennetze oder Wählverbindungen, wie ISDN oder GSM, erfolgen. Bei Wählverbindungen sind besondere Vorkehrungen zu ergreifen:

- Für jede Verbindungsaufnahme ist immer eine Benutzer-Authentisierung über den gewählten Mechanismus durchzuführen. Insbesondere ist die alleinige Nutzung des CLIP-Mechanismus (Rufnummernübertragung) zur Authentisierung nicht ausreichend.
- Für jede Verbindung sollte die Absicherung der Kommunikation durch eines der im VPN-Sicherheitskonzept erlaubten Verfahren erzwungen werden, damit die übertragenen Daten ausreichend geschützt sind.
- Die durch die Zugangstechnik zur Verfügung gestellten zusätzlichen Sicherheitsmechanismen (Nutzung der Rufnummernübertragung, Rückruf einer voreingestellten Telefonnummer für nicht mobile oder über Mobiltelefon angebundene VPN-Clients) sollten genutzt werden.
- Die Anbindung eines tragbaren IT-Systems an ein LAN kann über ein Mobilfunk-Netz wie GSM realisiert werden (siehe auch M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Bei der Nutzung von VPN über Mobiltelefon-Netze ist zu beachten, dass sich der CLIP-Mechanismus (Rufnummernübertragung) in der Regel nur als *zusätzliches* Authentisierungsmerkmal eignet, da das über die Rufnummer identifizierte Mobiltelefon sehr leicht entwendet werden kann.
- Bei der Einwahl über ein WLAN müssen zusätzlich die Empfehlungen aus dem Baustein B 4.6 *WLAN* berücksichtigt werden.

**Schulung und Sensibilisierung**

Den Benutzern eines VPNs müssen in die Benutzung von Sicherheitsmechanismen des VPNs eingewiesen werden. Dazu sollte ihnen zunächst ein Überblick über typische VPN-Gefährdungen und erforderliche Schutzmaßnahmen gegeben werden. Aber auch die Administratoren und Mitglieder des Störungsbearbeitungsteams müssen angemessen in die Benutzung von Sicherheitslösungen der VPNs eingeführt werden. Generelle Hinweise hierfür finden sich in M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit*.

**Clients für Remote-Access-VPNs**

Sehr oft wird gewünscht, dass sich einzelne Benutzer über unsichere Netze in das LAN eines Unternehmens oder einer Behörde einwählen können. Beispiele hierfür sind Telearbeiter oder Benutzer, die sich über ein öffentliches WLAN oder von einem mobilen Telefon einwählen. Hierbei werden typischerweise Standard-IT-Systeme benutzt, auf denen eine Applikation für die Einwahl in ein Remote-Access-VPN installiert wird.

Da VPN-Clients für den Fernzugriff oft in nicht vollständig kontrollierten Umgebungen betrieben werden, müssen für diesen Fall spezielle Mechanismen, Verfahren und Maßnahmen zum Einsatz kommen, die den Schutz des Clients gewährleisten können. Insbesondere mobile VPN-Clients sind hier einer besonderen Gefahr ausgesetzt, da diese physikalisch besonders leicht anzugreifen sind (z. B. Diebstahl, Manipulation). Ist ein VPN-Client kompromittiert, besteht die Gefahr, dass dadurch auch die Sicherheit des LANs beeinträchtigt wird.

Für den sicheren Betrieb von mobilen VPN-Clients sind daher neben den Empfehlungen der Maßnahme M 5.122 *Sicherer Anschluss von Laptops an lokale Netze* folgende Aspekte zu berücksichtigen:

- Die Grundsicherheit des mobilen IT-Systems muss gewährleistet werden (siehe auch Bausteine B 3.203 *Laptop*, B 4.3 *Modem*, B 3.404 *Mobiltelefon* und B 5.8 *Telearbeit*).
- Da mobile VPN-Clients größeren Risiken ausgesetzt sind als stationäre, sollten diese durch zusätzliche Maßnahmen gesichert werden. Hierzu bietet sich eine Festplattenverschlüsselung an, um sicherzustellen, dass von abhanden gekommenen Geräten weder Daten ausgelesen noch unbefugt eine VPN-Verbindung aufgebaut werden kann.
- Insbesondere beim VPN-Zugriff über Internetverbindungen ist die Installation von Computer-Viren-Schutzprogrammen auf allen RAS-Clients notwendig (siehe auch Baustein B 1.6 *Schutz vor Schadprogrammen*).
- Auch mobile VPN-Clients sollten in das Systemmanagement einbezogen werden, soweit dies möglich ist. Dies erlaubt einerseits die Überwachung der Clients im Rahmen der Aufrechterhaltung des laufenden Betriebes. Andererseits können so einfach Software-Updates (Viren-Datenbanken, Anwendungsprogramme) auf geregeltem Weg eingespielt werden. Entfernte Rechner stellen jedoch erhöhte Anforderungen an das Systemmanagement, da diese nicht permanent mit dem Netz verbunden sind, so dass die Rechner regelmäßig auf (unzulässige) Konfigurationsveränderungen untersucht werden müssen.
  Es ist dabei zu beachten, dass diese Erfassung der Informationen den VPN-Client belastet und die Daten über die VPN-Verbindung übertragen werden müssen. Bei VPN-Verbindungen mit geringer Bandbreite (z. B. über Mobiltelefon) kann dies zu nicht akzeptablen Antwortzeiten für den Benutzer führen.

**Kommunikationsverbindungen**

Für den sicheren Betrieb eines VPNs ist eine Verschlüsselung für alle übertragenen Daten erforderlich. Des Weiteren muss die Authentizität und Integrität der übertragenen Daten zweifelsfrei sichergestellt werden können. Dies kann beispielsweise durch die in Maßnahme M 5.148 *Sichere Anbindung eines externen Netzes mit OpenVPN* oder die in Maßnahme M 5.149 *Sichere Anbindung eines externen Netzes mit IPSec* beschriebenen Verfahren gewährleistet werden.

**Trusted VPNs**

Nur selten werden VPNs über Netzinfrastrukturen betrieben, die unter der eigenen Kontrolle stehen. Häufig werden VPNs genutzt, um eine sichere Verbindung über fremde Netze, wie dem Internet oder einer exklusiv genutzten Leitung von einem Fremdanbieter, zu realisieren. Besonders im letzteren Fall muss die Anbindung im Allgemeinen, die Qualität der Anbindung und die Einhaltung der Sicherheitsaspekte, die bei der Auswahl festgelegt wurden (siehe M 2.420 *Auswahl eines Trusted-VPN-Dienstleisters*), beobachtet werden.

Prüffragen:

- Für Hochverfügbarkeit: Existiert ein Betriebskonzept zur Sicherstellung des VPN-Betriebs?
- Ist sichergestellt, dass Qualitätsmängel der VPN-Verbindungen (durch Monitoring) frühzeitig erkannt werden?
- Werden die anfallenden Protokolldaten regelmäßig überprüft und durch fachkundiges Personal ausgewertet?
- Werden bei der Überwachung des VPN die Bestimmungen des Datenschutzes eingehalten?
- Sind systematische Vorgehensweisen für Wartung, Änderungen und Revisionen von VPN-Komponenten festgelegt?
- Ist festgelegt, wie mit Fehlern und Störungen des VPN umgegangen wird?
- Ist sichergestellt, dass bei kritischen Situationen bei der VPN-Nutzung unverzüglich die zuständigen Personen informiert werden?
- Sind die VPN-Benutzer und -Administratoren hinreichend geschult und für die relevanten VPN-Sicherheitsaspekte sensibilisiert?

# M 4.322 Sperrung nicht mehr benötigter VPN-Zugänge

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

VPN-Zugänge müssen so abgesichert werden, dass nur berechtigte Benutzer oder IT-Systeme hierüber zugreifen können. Dafür müssen an den VPN-Endpunkten Zugriffskontrollverfahren eingesetzt werden, die überprüfen, ob ein Sender zur Kommunikation mit dem Empfänger berechtigt ist. Die ordnungsgemäße Funktion und Konfiguration dieser Verfahren ist in regelmäßigen Zeitabständen zu überprüfen. In Vergessenheit geratene Zugänge oder Benutzerkennungen bereits ausgeschiedener Mitarbeiter oder ausgesonderter IT-Systeme stellen gefährliche Sicherheitslücken dar und sind schnellstmöglich zu sperren. Auch nicht mehr benötigte VPN-Zugänge von Zulieferern, Partner und Kunden müssen zeitnah deaktiviert werden. Nachdem ein Zugang gelöscht wurde, ist zu prüfen, ob hierüber auch tatsächlich nicht mehr auf das Netz zugegriffen werden kann.

Ist absehbar, dass einzelne Benutzer des VPNs längere Zeit abwesend sind oder dieses aus anderen Gründen nicht nutzen (z. B. durch Urlaub, Krankheit oder andere Aufgaben), sollte überlegt werden, deren Benutzerkennung für diese Zeit am VPN-Server zu sperren, so dass das Arbeiten unter ihrer Nutzerkennung für diese Zeit nicht mehr möglich ist. Wenn möglich, sollte hierfür jeder Nutzer dem Netzadministrator längere Abwesenheitszeiten rechtzeitig mitteilen. Wenn Externe wie Kunden oder Lieferanten nur zu bestimmten Zeiten VPN-Zugriff benötigen, sollten die Zugriffsberechtigungen auf diese Phasen beschränkt werden.

Eine effiziente Verwaltung der zugriffsberechtigten Benutzer und IT-Systeme, beispielsweise auf Grundlage von Zertifikaten, sollte eingeführt und in regelmäßigen Abständen überprüft und angepasst werden. Die Zugangsdaten und die zugeordneten Dienste müssen vor unberechtigtem Zugriff geschützt werden.

Prüffragen:

- Wird regelmäßig überprüft, ob nur berechtigte IT-Systeme und Personen auf das VPN zugreifen können?
- Ist sichergestellt, dass nicht mehr benötigte VPN-Zugänge umgehend deaktiviert werden?
- Wird der VPN-Zugriff für Externe auf die Zeiten beschränkt, in denen er benötigt wird?
- Werden neue und nicht erreichbare IT-Systeme für die Sicherstellung der Patch- und Änderungsverteilung berücksichtigt?
- Werden alle Phasen des Prozesses auch für die nicht erreichbaren Systeme im Zuge der Synchronisation umgesetzt?
- Wird auf Veränderungen an der IT-Infrastruktur auch im Patch- und Änderungsmanagementprozess reagiert?

# M 4.323 Synchronisierung innerhalb des Patch- und Änderungsmanagements

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Änderungsmanager

In den meisten Behörden und Unternehmen werden häufig Änderungen an der IT-Infrastruktur vorgenommen. Auf diese Änderungen muss der Patch- und Änderungsmanagementprozess reagieren. Dabei muss gewährleistet werden, dass die jeweiligen Patches und Änderungen zeitnah und möglichst gleichzeitig auf alle betroffenen IT-Systeme aufgespielt werden.

Bei mobilen Endgeräten oder auch bei Überlastung der verwendeten Netztechnologie kann es vorkommen, dass IT-Systeme bei der Verteilung von Hard- oder Software-Änderungen nicht erreichbar sind. Für solche Fälle müssen geeignete Mechanismen etabliert werden, die sicher stellen, das sich Systeme erst dann wieder am Netz anmelden können, wenn sie mit geeigneten Updates versorgt wurden. Es gibt verschiedene Werkzeuge, die vor einem Zugriff auf das Produktivnetz überprüfen, ob Sicherheitsprogramme und Sicherheitspatches auf dem aktuellsten Stand sind, und bei Sicherheitsmängeln den Zugriff auf das interne Netz abweisen. In der Regel werden solche Tools dazu benutzt, den Softwarestand der Systeme zunächst festzustellen und dann die Software zur Aktualisierung zusammen zu stellen. Je nach Art des Patch- und Änderungsprozesses können diese dann automatisch oder nach vorheriger Freigabe für diese Systeme verteilt und installiert werden. Änderungen die einen Systemneustart erfordern, sollten als letztes installiert werden, oder erst beim Herunterfahren des IT-Systems. Je nach technischer Unterstützung und Umsetzung des Prozesses können die Aktualisierungen auch installiert werden und der danach nötige Neustart kann gesondert freigegeben werden.

Prüffragen:

- Wird auf Veränderungen an der IT-Infrastruktur auch im Patch- und Änderungsmanagementprozess reagiert?

# M 4.324 Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement

**Verantwortlich für Initiierung:** Änderungsmanager
**Verantwortlich für Umsetzung:** Administrator

Viele Produkte verfügen über automatische Update-Mechanismen (Autoupdate), die die Anwender darüber informieren, wenn Patches oder Updates vorhanden sind. Häufig bieten diese auch die Option, die Updates sofort über das Internet herunterzuladen und zu installieren. In der Regel enthalten heute alle Betriebssysteme und verfügbaren Standardsoftwarepakete solche Mechanismen. Die Funktionsweise des Update-Mechanismus ist je nach Version, Installationsmodus und Hersteller unterschiedlich ausgeprägt.

Üblicherweise suchen IT-Produkte mit Autoupdate bei jedem Start des Systems oder bei jeder Einwahl in das Internet auf einem öffentlichen Updateserver nach neuen Versionen oder Softwarepaketen. Produkte bieten verschiedene Möglichkeiten, den Autoupdate-Mechanismus zu konfigurieren. Wenn neue IT-Komponenten in Betrieb genommen werden, sollte immer auch überprüft werden, ob und welche Update-Mechanismen diese haben und wie diese konfiguriert werden können. Dabei sollten auch kontrolliert werden, welche Daten vom Autoupdate-Mechanismus zum Hersteller übertragen werden. Es sollte zunächst grundsätzlich geklärt werden, wie mit diesen Mechanismen umgegangen wird. Danach sollte festgelegt werden, wie die Update-Funktionen konkret in den verschiedenen Produkten konfiguriert werden. Im folgenden wird ein Überblick über verschiedene Varianten dieser Mechanismen gegeben.

Das komplette Deaktivieren wird nicht von jeder Software angeboten. Falls die Institution die unkontrollierte Kommunikation von IT-Komponenten mit der Außenwelt unterbinden will, müssen hierfür Paketfilter eingesetzt werden.

Wird eine Abfrage von einem öffentlichen Update-Server nicht gewünscht, lassen sich viele Softwareprodukte auf andere Internet-Adressen als die des Herstellers, beispielsweise interne, umlenken.

Einige Hersteller bieten Software für den Eigenbetrieb von Update-Servern oder Update-Spiegelservern an, dabei wird der Update-Server in der Institution lokal installiert (z. B. Windows Server Update Services WSUS). Der Update-Server kommuniziert dann direkt mit dem Hersteller und lädt die gewünschten Aktualisierungen direkt vom Hersteller. Der Vorteil dieser Lösung ist, dass die von der Aktualisierung betroffenen IT-Systeme einer Institution nicht selber mit dem Update-Server des Herstellers kommunizieren müssen, sondern nur mit dem lokal installierten. Dadurch kann der Datenverkehr nach Außen auf ein Mindestmaß reduziert werden. Bei vielen Produkten für Update-Servern lassen sich die gewünschten Einstellungen komfortabel über eine grafische Benutzeroberfläche (GUI) vornehmen. Allerdings gibt es auch Produkte, bei denen die notwendigen Einstellungen, um lokale Update-Server zu verwenden oder die Abfrage von einem öffentlichen Updateserver zu unterbinden, verborgen oder nur per Paketfilter bzw. Firewall zu unterbinden sind.

Falls öffentliche Update-Server genutzt werden sollen, so ist zunächst die Authentizität des Update-Servers zu prüfen, siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*. Außerdem sollte untersucht werden, ob Zeitintervalle oder Ereignisse zur Steuerung der Update-Abfrage-

aktion eingestellt werden können. Die Einstellungen müssen dann entsprechend der festgelegten Änderungsstrategie vorgenommen werden.

Es sollte geprüft werden, wie die Kommunikation mit Update-Servern auf das geringst mögliche Maß beschränkt werden kann. Außerdem muss entschieden werden, ob die direkte Kommunikation mit dem Hersteller als einzige Alternative oder parallel zur internen Kommunikation (Parallelkonfiguration) betrieben werden soll.

Eine Parallelkonfiguration ist häufig sinnvoll für mobile Nutzer, welche nicht immer innerhalb des Behörden- oder Unternehmensnetzes kommunizieren. Bei mobilen IT-Systemen kann es beispielsweise wichtiger sein, unterwegs einen aktuellen Patch einzuspielen, wenn dieser eine gefährliche Sicherheitslücke schließt, als auf die Freigabe vom Änderungsmanagement zu warten. Es kann jedoch auch gewünscht werden, dass sämtliche Software-Änderungen ausschließlich durch die interne freigegebene Softwareverteilung erfolgen.

Bei Autoupdate-Mechanismen ist unter anderem noch zu beachten, ob die Änderungen vom Hersteller nur auf ein internes IT-System geladen werden und die Installation der Änderung danach dem Benutzer überlassen wird, oder ob diese nach dem Herunterladen sofort automatisch installiert werden.

Außerdem muss festgelegt werden, wie mit eventuell benötigten Neustarts von IT-Systemen nach der Installation von Änderungen umgegangen wird, also ob diese direkt oder z. B. erst beim Herunterfahren des Systems erfolgen.

Prüffragen:

- Wurden bei der Festlegung der Patch- und Änderungsmanagementstrategie für die Institution auch Vorgaben zu Autoupdate-Mechanismen getroffen?
- Werden neue Komponenten daraufhin überprüft, ob und welche Autoupdate-Mechanismen diese haben?
- Wurde festgelegt, wie Autoupdate-Mechanismen abgesichert werden?

# M 4.325 Löschen von Auslagerungsdateien

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Heutige Betriebssysteme unterstützen virtuelle Speicher. Damit Benutzern (virtuell) mehr Hauptspeicher zur Verfügung steht, als in dem Computer eingebaut ist, wird jeweils der gerade nicht verwendete Teil des Arbeitsspeichers auf Festplatte ausgelagert (Swap-Bereich).

In diesen Auslagerungsdateien finden sich auch Teile der Informationen wieder, die die Benutzer während ihrer Arbeit verwendet haben. Dazu können auch sensible Daten wie Passwörter oder kryptographische Schlüssel gehören. Die Dateien werden nicht gelöscht, wenn sich der Benutzer abmeldet bzw. das System ausgeschaltet wird. Daher könnten Auslagerungsdateien von einem Angreifer genutzt werden, um vertrauliche Daten auszulesen.

Um das Auslesen von Auslagerungsdateien zu verhindern, sollte der Auslagerungsbereich entweder temporär bzw. dauerhaft deaktiviert oder vor jedem Ausschalten sicher gelöscht werden.

Aktuelle Windows-Betriebssysteme können so konfiguriert werden, dass beim Booten oder Herunterfahren des Rechners die Auslagerungsdatei überschrieben wird. Die Auslagerungsdatei (Windows Paging File, pagefile.sys) wird ebenso wie die Datei für den Ruhezustand (Hibernation File, hiberfil.sys) beim Herunterfahren des Systems mit Nullen überschrieben, wenn "Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen" gesetzt ist. Das Überschreiben der Auslagerungsdatei kann allerdings je nach Größe längere Zeit in Anspruch nehmen. Dennoch sollte diese Option bei Clients, insbesondere bei Laptops, gesetzt werden. Bei Servern mit sehr großen Auslagerungsdateien sollte bei normalen Schutzbedarf abgewogen werden, ob dies dort erforderlich ist. Bei höherem Schutzbedarf sollte die Auslagerungsdatei auf jedem Fall automatisch gelöscht werden. Ab Windows Vista gibt es die Möglichkeit, dass die Auslagerungsdatei bei einem Systemstart per EFS verschlüsselt wird. Das ist deutlich effizienter und in allen Fällen empfehlenswert, in denen die Auslagerungsdatei nicht bereits durch eine vollständige Festplattenverschlüsselung wie BitLocker Drive Encryption verschlüsselt wird.

Bei höherem Schutzbedarf sollten weitere Maßnahmen gegen das Auslesen von Auslagerungsdateien ergriffen werden. Dazu können z. B. Werkzeuge, die den Auslagerungsbereich vor jedem Ausschalten sicher löschen, eingesetzt werden. Um die Problematik als solche aber zu vermeiden, können auch kryptographische Dateisysteme eingesetzt werden, mit denen der gesamte Inhalt der Festplatte verschlüsselt wird. Somit ist auch kein Zugriff auf die Auslagerungsdatei mehr möglich.

Das Abschalten oder Löschen des Auslagerungsbereichs ist für ad hoc-Lösungen brauchbar, aber keine dauerhafte Alternative. Die vollständige Verschlüsselung der Festplatten ist bei höherem Schutzbedarf die bessere Lösung.

Bei Unix-Systemen werden die Auslagerungsdateien im Swap-Dateisystem abgelegt. Hierbei handelt es sich um eine eigenständige Partition, die verschlüsselt werden kann. Es muss vor der Verschlüsselung der Swap-Partion geprüft werden, ob hierfür ausreichend Rechenleistung verfügbar ist. Eine sichere Maßnahme zum Schutz vor einer unerwünschten Auswertung des Aus-

lagerungsbereichs ist die Verschlüsselung des gesamten Datenträgers und wird daher, wenn möglich, empfohlen.

Prüffragen:

- Wird zuverlässig verhindert, dass auf den Auslagerungsbereich von IT-Systemen zugegriffen werden kann?

# M 4.326 Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Windows-Dateisysteme unterscheiden sich teilweise stark von Unix-Dateisystemen. Werden Dateisystemobjekte über Systemgrenzen hinweg kopiert oder verschoben (beispielsweise von einem Windows XP System auf eine Dateifreigabe eines Samba-Servers) können unter Umständen Informationen verloren gehen, wenn sich Administratoren solcher Effekte nicht bewusst sind und Samba falsch konfiguriert ist. Konkret geht es dabei um Informationen, die in New Technology File System (NTFS) Access Control Lists (ACLs) oder NTFS Alternate Data Streams (ADS) abgelegt sein können.

### 1. NTFS Access Control Lists

Samba 3 bildet NTFS ACLs über Portable Operating System Interface (POSIX) ACLs ab. Dieser Mechanismus ist standardmäßig aktiv, wenn:

- das Dateisystem der Samba-Freigabe POSIX ACLs unterstützt,
- Samba mit ACL-Unterstützung kompiliert wurde (Parameter *-with-acl-support* des *configure* Skripts) und
- der Konfigurationsparameter "*nt acl support"* in der Konfigurationsdatei smb.conf nicht auf "no" gesetzt wurde.

Dabei handelt es sich um keine direkte Abbildung der NTFS ACLs auf POSIX ACLs. In M 4.332 *Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server* ist näher beschrieben in welcher Art und Weise und mit welchen Einschränkungen Samba NTFS ACLs im darunterliegenden Dateisystem abbildet.

Bevor Dateisystemobjekte über Systemgrenzen hinweg verschoben werden, muss sichergestellt werden, dass diesen keine NTFS ACLs zugewiesen sind, die Samba nicht abbilden kann. Dieser Umstand sollte bereits beim Entwurf des organisationsweiten Zugriffsberechtigungskonzepts für Dateisysteme beachtet werden. Es sollte darauf verzichtet werden, Kombinationen von NTFS ACL-Einträgen zu verwenden, die Samba nicht direkt abbilden kann.

### 2. NTFS Alternate Data Streams

Samba 3.0.x bietet keine Möglichkeit NTFS ADS abzubilden. Samba 3.2.x und höher kann NTFS ADS direkt über POSIX Extended Attributes (xattr) abbilden.

Kommt eine Version von Samba zum Einsatz, die NTFS ADS nicht abbilden kann, muss sichergestellt werden, dass Dateisystemobjekte keine ADS mit wichtigen Informationen enthalten, bevor diese über Systemgrenzen hinweg kopiert oder verschoben werden.

### 3. Weitere Unterschiede zwischen Windows- und Unix-Dateisystemen

Es gibt einige weitere Unterschiede zwischen Windows- und Unix-Dateisystemen, wie beispielsweise die Beachtung der Groß- und Kleinschreibung bei Unix oder das Trennzeichen für Verzeichnisse. Die Unterschiede kann Samba in transparenter Art und Weise ausgleichen, so dass durch diese kein Informationsverlust droht.

Prüffragen:

- Kennen die Administratoren die Unterschiede zwischen der Unix- und Windows-Dateisystemtechnologie?
- Wird sichergestellt, dass Dateisystemobjekten keine NTFS ACL zugewiesen sind, die Samba nicht abbilden kann, bevor diese Objekte über Systemgrenzen hinweg verschoben werden?
- Wird sichergestellt, dass Dateisystemobjekte keine ADS mit wichtigen Informationen enthalten, welche die eingesetzte Version von Samba nicht abbilden kann, bevor diese Objekte über Systemgrenzen hinweg verschoben werden?

# M 4.327 Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem bei der Planung des Einsatzes von Samba (siehe M 2.437 *Planung des Einsatzes eines Samba-Servers*) entschieden wurde, ob Samba aus einem Quelltext- oder Binärpaket installiert wird, muss dessen Authentizität überprüft werden (siehe auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*). Die Herkunft der zu installierenden Software sollte ebenso wie der Prozess der Integritätsprüfung der Software dokumentiert werden.

**1. Installation aus einem Quelltextpaket**

Die Entwickler von Samba verwenden mit dem Programm GnuPG erstellte digitale Signaturen zur Absicherung der Quelltextpakete (siehe auch M 5.63 *Einsatz von GnuPG oder PGP*. Die digitale Signatur befindet sich stets in einer gesonderten Datei, die den gleichen Namen trägt, wie das Paket selbst, jedoch ergänzt durch das Suffix ".asc". Beispielsweise wird die digitale Signatur des Pakets samba-3.0.28a.tar.gz in der Datei samba-3.0.28a.tar.asc zur Verfügung gestellt.

Der öffentliche Schlüssel, den die Samba-Entwickler zum Signieren nutzen, hat die Benutzer-ID "Samba Distribution Verification Key <samba-bugs@samba.org>". In der Regel ist der Schlüssel mit einem Ablaufdatum von ein bis zwei Jahren versehen. Danach kommt ein neuer Schlüssel, mit einem neuen Fingerabdruck (englisch: Fingerprint) zum Einsatz. Der öffentliche Schlüssel kann beispielsweise über folgende Quellen bezogen werden:

- Über den Webserver des Samba Projekts. Die Datei http://www.samba.org/samba/ftp/samba-pubkey.asc enthält der von den Samba-Entwicklern zum Signieren von Quellcode benutzte öffentlichen GPG-Schlüssel.
- Über einen Keyserver.

Bevor das Quelltextpaket überprüft werden kann, muss es mit gzip -d samba-<version>.tar.gz dekomprimiert werden.

**2. Installation aus Binärpaketen der Distribution**

Wird Samba aus den offiziellen Installationsquellen der verwendeten Distribution über einen entsprechenden Paketmanager (zum Beispiel yum oder rpm) installiert, so stellt in der Regel der Paketmanager die Authentizität und Integrität der Pakete sicher.

**3. Installation aus Binärpaketen fremder Quellen**

Werden Binärpakete aus Installationsquellen, die nicht Teil der eingesetzten Distribution sind, bezogen, so muss sichergestellt werden, dass es sich um einen vertrauenswürdigen Anbieter handelt. Die Überprüfung der Authentizität der Binärpakete erfolgt in weiterer Folge entweder wie im Abschnitt "Installation aus einem Quelltextpaket" oder Abschnitt "Installation aus Binärpaketen der Distribution" beschrieben.

Prüffragen:

- Wurde eine Authentizitäts- und Integritätsprüfung der Installationspakete vorgenommen?
- Sind die Herkunft der Installationspakete und die vorgenommene Integritätsprüfung dokumentiert?

# M 4.328 Sichere Grundkonfiguration eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem der Samba-Server installiert wurde, muss eine sichere Grundkonfiguration des Dienstes hergestellt werden. Dies betrifft unter anderem die Einstellungen für die Zugriffskontrollen, aber auch Einstellungen, die auf die Performance des Servers Einfluss haben.

Die zentrale Konfigurationsdatei von Samba ist die Datei smb.conf. Normalerweise befindet sich diese im Verzeichnis /etc/samba/. In dieser Konfigurationsdatei wird zwischen einem globalen und mehreren freigabespezifischen Konfigurationsabschnitten unterschieden. Freigabespezifische Konfigurationsabschnitte sind daran erkennbar, dass diese Abschnitte mit einer Markierung beginnen, die nicht "[global]" lautet. Parameter, die im globalen Abschnitt stehen, sind allgemein gültig. Parameter in freigabespezifischen Abschnitten sind hingegen immer nur für die Freigabe gültig, auf die sie sich beziehen. In der Dokumentation, beziehungsweise Manpage, zu smb.conf sind alle Konfigurationsparameter beschrieben.

Im Folgenden werden die wichtigsten Konfigurationseinstellungen beschrieben:

**Security Modes**

Wesentlich für die Authentisierung von Benutzern ist der Parameter "security". Das Server Message Block (SMB)-Protokoll unterscheidet zwischen zwei Sicherheitsstufen (Security Levels):

- user-level
- share-level

In der Sicherheitsstufe *share-level* wird die Zugriffssteuerung auf Freigabeebene geregelt. Eine Freigabe wird bei dieser Sicherheitsstufe nur durch ein Passwort geschützt. Jeder beliebige Benutzer kann, wenn er das Passwort kennt, auf die Freigabe zugreifen. Die Sicherheitsstufe *user-level* regelt die Zugriffssteuerung hingegen auf Benutzerebene. Das bedeutet, das für jeden Benutzer individuell bestimmt werden kann, welche Rechte er für eine Freigabe erhält. Bevor der Benutzer die Freigabe nutzen darf, muss er sich authentisieren. Samba setzt diese beiden Sicherheitsstufen auf fünf verschiedene Arten um, die Security Modes (Sicherheitsmodi) genannt werden. Die Sicherheitsstufe *user-level* ist auf vier verschiedene Arten (user, server, domain und ads Sicherheitsmodus) implementiert, die Sicherheitsstufe share-level nur auf eine Art (share Security Mode). Der Sicherheitsmodus share ist der einzige, bei dem die Zugriffssteuerung auf Freigabeebene geregelt ist. Alle anderen Sicherheitsmodi regeln die Zugriffssteuerung auf Benutzerebene.

Im Folgenden werden die einzelnen Sicherheitsmodi genauer beschrieben:

- share:
  Dieser Sicherheitsmodus sollte nicht verwendet werden, weil sich einzelne Benutzer nicht unterscheiden lassen. Jeder Freigabe wird ein Passwort zugewiesen.
- server:
  Dieser Sicherheitsmodus wurde durch den Sicherheitsmodus domain ersetzt und sollte möglichst nicht mehr verwendet werden. Samba delegiert

bei diesem Sicherheitsmodus die Authentisierung an ein externes IT-System in einer Art und Weise weiter, wie dies ein IT-System mit installierten Windows 95 oder Windows 98 tun würde. Das bringt viele Nachteile mit sich, beispielsweise:

- Winbind kann nicht eingesetzt und
- Accounts können unbeabsichtigt gesperrt werden,
- Samba kann die Identität des Servers, an den die Authentisierung delegiert wird, nicht verifizieren.

Erst im domain Sicherheitsmodus delegiert Samba die Authentisierung an einen DC weiter, wie es ein Windows NT Server tun würde.

- user:
  Dies ist die Standardeinstellung von Samba. Mit dieser Einstellung werden Benutzer und Passwörter zur Authentisierung genutzt.
- domain:
  Samba gibt bei diesem Sicherheitsmodus die Authentisierung an ein externes System weiter. Dieser Sicherheitsmodus bewegt Samba dazu, die Authentisierung mit Windows NT-konformen Mitteln an einen DC zu delegieren. Zur Authentisierung wird das NT LAN-Manager (NTLM)-Verfahren in seinen unterschiedlichen Ausprägungen bis hin zu NTLMv2, das Samba auch unterstützt, eingesetzt. Die Benutzerverwaltung erfolgt über so genannte Remote Procedure Calls (RPCs).
- ads:
  Mit Windows 2000 hat Microsoft Active Directory eingeführt. Dieses setzt zur Authentisierung bevorzugt Kerberos ein und bietet zur Benutzerverwaltung ein Lightweight Directory Access Protocol (LDAP)-Verzeichnis an. Samba delegiert beim Sicherheitsmodus "ads" die Authentisierung an ein externes System. Dieser Sicherheitsmodus ist in vielerlei Hinsicht äquivalent zum domain Sicherheitsmodus, nur dass Samba dem Client ausschließlich Kerberos als Authentisierungsmethode anbietet.

Die Sicherheitsmodi domain und ads sind sich sehr ähnlich. Folgende Aspekte sollten bei der Entscheidung für einen der beiden Sicherheitsmodi beachtet werden.

Jedes Active Directory kann Samba-Dienste im domain Sicherheitsmodus als Mitglieder aufnehmen. Dies gilt nicht nur für Domänen im sogenannten Mixed Mode, auch Domänen im Windows-2003-Infrastrukur-Modus sind in der Lage, NT-kompatible Mitglieder aufzunehmen. Der Unterschied ist, dass Domänen im Windows-2003-Infrastrukur-Modus die Aufnahme eines NT4-Backup Domain Controller (BDC)s nicht erlauben. Da Samba aber kein solcher BDC werden kann (siehe M 2.437 *Planung des Einsatzes eines Samba-Servers*), ist dieser Aspekt irrelevant.

Die Sicherheitsrichtlinien des Informationsverbundes können die Benutzung von Kerberos erfordern. Kerberos gilt allgemein als deutlich sicherer als NTLM (NT LAN Manager), wobei NTLMv2 ebenfalls einen durchaus akzeptablen Sicherheitsstandard vorzuweisen hat.

Standardmäßig benutzt Samba zur Authentisierung das NTLM oder NTLMv2 Verfahren. Damit Samba nur NTLMv2 einsetzt, muss der Parameter "*ntlm auth = no"* in der Konfigurationsdatei smb.conf gesetzt werden.

Ein Vorteil von Kerberos gegenüber NTLM ist die geringere Beanspruchung der DC und die niedrigere Netzlast. Bei einer NT-Domäne muss ein Mitgliedsserver für jede Benutzeranmeldung beim DC nachfragen. Hingegen ist ein Kerberosticket für eine gewisse Zeit gültig und steht für sich alleine. Kann sich

ein Benutzer mit einem gültigen Ticket gegenüber dem Samba-Dienst authentisieren, ist eine zusätzliche Authentisierung beim DC nicht nötig. Eine geringere Beanspruchung der Domänencontroller und eine niedrigere Netzlast kann auch durch die Verwendung von Winbind erreicht werden (siehe M 4.333 *Sichere Konfiguration von Winbind unter Samba*).

Windows 2003 listet bei Verwendung der NT-kompatiblen RPCs nur die ersten 100 Benutzer auf. Bei der Nutzung von LDAP werden dagegen alle Benutzer angezeigt. Das Auflisten von Benutzern ist eine Operation, die man vermeiden sollte, denn bei großen Domänen kann dieser Vorgang ausgesprochen lange dauern. Ist man jedoch auf das Auflisten der Benutzer angewiesen, so muss der Sicherheitsmodus ads gewählt werden.

Im Active Directory existiert das Konzept der sogenannten Standorte (Sites). Jeder DC und jeder Mitgliedsrechner ist einem Standort zugeordnet. Will sich ein Mitgliedsrechner mit einem DC verbinden, dann sollte dies nur innerhalb des vorgesehenen Standortes geschehen. Die entsprechenden Mechanismen bietet Samba nur im ads Security Mode.

Der Security Mode ads ist sehr kritisch bezüglich der Zeitsynchronisation und eines korrekt funktionierenden Domain Name System (DNS). Wenn Samba einen DC sucht, geschieht dies im ads Security Mode über das DNS und nicht über die Network Basic Input/Output System (NetBIOS)-Namensauflösung. Die Authentisierung erfolgt per Kerberos. Die Sicherheit von Kerberos beruht zum Teil darauf, dass die Uhrzeiten auf allen Rechnern im Netz synchron sind. Ist dies nicht der Fall, so schlägt die Authentisierung über Kerberos fehl. Wird der Security Mode ads eingesetzt so sollte überlegt werden, einen Windows-DNS-Server als Nameserver und für den Samba-Dienst als Zeitserver zu verwenden. Dies kann am Samba-Dienst mit einem entsprechenden Eintrag in der Datei /etc/resolv.conf und /etc/ntp.conf realisiert werden.

Älteren Kerberos Bibliotheken bereiten die im Active Directory verwendeten kryptographischen Algorithmen häufig schwerwiegende Probleme. Entweder unterstützen sie das benötigte Hash-Verfahren HMAC-MD5 gar nicht, oder die Implementierungen sind fehlerhaft. Dies kann mitunter zu, durch Kerberos verursachten, Abstürzen des Rechners führen. Insbesondere Hersteller proprietärer Unix-Betriebssysteme liefern teilweise noch zu alte Kerberos Bibliotheken aus.

Der Sicherheitsmodus ads ist im Vergleich zum Sicherheitsmodus domain deutlich fortschrittlicher. Auf Grund der eventuell höheren Komplexität der Installation und Konfiguration von Samba im Security Mode ads wird in kleinen Domänen mit nur einem Standort beziehungsweise LAN die Verwendung des Security Mode domain empfohlen. Soll Winbind mit dem ID-Mapping-Backend ads eingesetzt werden (M 4.333 *Sichere Konfiguration von Winbind unter Samba*), so muss Samba im Security Mode ads betrieben werden.

**Benutzerbasierter Schutz**

Generell sollte nur ausgewählten Benutzern und Benutzergruppen erlaubt werden, sich mit dem Samba-Dienst verbinden zu dürfen. Der Zugriff sollte daher in der Konfigurationsdatei smb.conf mit der Option "valid users" beschränkt werden. Wichtig dabei ist, dass diese Option im Abschnitt [global] der Konfigurationsdatei smb.conf gesetzt wird. Der Parameter kann auch in einem freigabespezifischen Abschnitt der Konfigurationsdatei verwendet werden, dann beschränkt er nur den Zugriff auf diese Freigabe. Ein Beispiel könnte sein:

valid users = @smbusers Administrator

Das oben angeführte Beispiel beschränkt sämtlichen Zugriff auf den Server auf Benutzer der Gruppe "smbusers" und den Benutzer "Administrator". Standardmäßig ist diese Option nicht gesetzt. In diesem Fall kann sich jeder Benutzer, der einen gültigen Account besitzt, am Server anmelden.

Ist ein Benutzer in beiden Listen, valid users und invalid users, eingetragen, so wird dem Benutzer die Anmeldung verwehrt.

Die Sonderzeichen in den Gruppennamen werden folgendermaßen interpretiert:

- @ Der Name wird zuerst als Network Information Service (NIS) Netgroup interpretiert. Wird keine NIS Netgroup gefunden, wird angenommen, dass es sich um eine Unix-Gruppe handelt.
- + Der Name wird als Unix Gruppe interpretiert.
- & Der Name wird als NIS Gruppe interpretiert.

Die Sonderzeichen + und & können in beliebiger Weise kombiniert werden, um die jeweils erwünschte Reihenfolge bei der Namensauflösung zu erzwingen.

**Hostbasierter Schutz**

Standardmäßig akzeptiert Samba Verbindungen von jedem Host. Daher sollte Samba so konfiguriert werden, dass Verbindungen nur von als sicher geltenden Hosts und Netzen entgegengenommen werden. Samba bietet hierzu eine eigene "tcpwrapper"- Implementierung. Um diese zu nutzen, gibt es für die Konfigurationsdatei smb.conf die Optionen "hosts allow" und "hosts deny". Ein Beispiel könnte sein:

*hosts allow = 127.0.0.1 192.168.2.0/24*
*hosts deny = 0.0.0.0/0*

Das oben angeführte Beispiel erlaubt Verbindungen nur von localhost (127.0.0.1) und von den IT-Systemen mit einer Internet Protocol (IP)-Adresse zwischen 192.168.2.1 und 192.168.2.255. Alle anderen Verbindungsversuche weist der Samba-Dienst mit der Nachricht "not listening on called name" zurück.

Die Netzadresse 127.0.0.1 muss erlaubt werden, damit folgende Applikationen von Samba ordnungsgemäß funktionieren:

- smbpasswd:
  smbpasswd verbindet sich als SMB-Client standardmäßig mit der Adresse 127.0.0.1 um das Passwort eines Benutzers zu wechseln.
- swat:
  Die Statusseite des Samba-Webkonfigurationsprogramms swat verbindet sich mit nmbd und smbd auf der Adresse 127.0.0.1 um festzustellen, ob diese laufen. Kann swat diese Prozesse nicht erreichen, so wird deren Status nicht korrekt angezeigt und Samba kann nicht zuverlässig gestartet, gestoppt und neugestartet werden.

**Netzschnittstellen**

Standardmäßig bindet sich Samba an alle verfügbaren Netzadressen des Systems. Samba sollte so konfiguriert werden, dass es sich nur an als sicher geltende Netzadressen bindet. Unerwünschte Pakete werden dann nicht an Samba Prozesse weitergeleitet.

Hierzu gibt es für die Konfigurationsdatei smb.conf die Optionen "interfaces" und "bind interfaces only". Ein Beispiel könnte sein:

*interfaces = lo eth0*
*bind interfaces only = yes*

Im oben genannten Beispiel bindet sich Samba nur an die Adressen der Netzschnittstellen lo und eth0. Versucht sich jemand beispielsweise über das Netzgerät ppp0 mit dem Samba-Dienst zu verbinden, lehnt bereits das Betriebssystem den Aufbau einer Transmission Control Protocol (TCP)-Verbindung ab. Dabei erhält der Client die Meldung, dass der Aufbau einer TCP-Verbindung abgelehnt wurde. Diese Information kann einem Angreifer unter Umständen nützlich sein. Zusätzlich sollte daher die in M 4.331 *Sichere Konfiguration des Betriebssystems für einen Samba-Server* beschriebene Maßnahme zur Konfiguration eines lokalen Paketfilters umgesetzt werden.

Über einen Paketfilter kann erreicht werden, dass eingehende unerwünschte Pakete einfach ignoriert werden.

Pakete von Adresse 127.0.0.1 (Interface lo) sollten erlauben werden, damit Programme der Samba-Umgebung ordnungsgemäß funktionieren. Weitere Informationen hierzu sind im Abschnitt hostbasierter Schutz zu finden.

**Freigaben**

Der Parameter "follow symlinks" steuert, ob Samba einem symbolischen Link im Unix-Dateisystem folgt oder ob der Benutzer eine Fehlermeldung erhält. Standardmäßig ist dieser Parameter auf "yes" gesetzt. Die Standardeinstellung des Parameters sollte beibehalten werden, auch wenn smbd beim Auflisten von Verzeichnissen geringfügig langsamer arbeitet.

Der Parameter "wide links" steuert, ob der Benutzer symbolischen Links im Unix-Dateisystem folgen kann, deren Ziel außerhalb des freigegebenen Verzeichnisbaums liegt. Dazu gehören Dateien und Verzeichnisse am anderen Ende der Links, solange die Berechtigungen des Dateisystems dafür vorliegen. Die Standardeinstellung für diesen Parameter ist "yes". Dieser Parameter wird ignoriert, falls "follow symlinks = no" gesetzt ist. Bei "wide links = no", kann es sein, dass smbd merklich langsamer arbeitet, da jeder Link überprüft werden muss. Wird dieser Parameter auf "yes" gesetzt, kann verhindert werden, dass ein Benutzer beispielsweise über einen symbolischen Link auf Informationen im Ordner /etc/ zugreifen kann. Schreiben die Sicherheitsrichtlinien vor, dass Benutzer keinen Zugriff auf Informationen außerhalb der Freigaben haben dürfen, so wird empfohlen "wide links = no" zu setzen.

Falls hohe Anforderungen an die Performance gestellt werden und trotzdem verhindert werden muss, dass auf Dateien außerhalb der Freigaben zugegriffen werden kann, bietet Samba noch eine zusätzliche Möglichkeit, wenn auch mit erhöhten Administrationsaufwand.

Der Parameter "root directory" gibt an, in welches Verzeichnis Samba nach der Initialisierung wechselt. Dazu wird der chroot() Systemaufruf verwendet. Standardmäßig gilt "root directory = /". Wird dieser Parameter beispielsweise auf "root directory = /var/fileserver/" gesetzt, so kann keiner der von Samba gestarteten Prozesse in Zukunft auf Dateien außerhalb von "/var/fileserver/" zugreifen. Davon betroffen sind auch einige Dateien, die für eine ordnungsgemäße Ausführung von Samba benötigt werden. In diesem Fall muss sichergestellt werden, dass folgende Dateien für Samba unter /var/fileserver/ zur Verfügung stehen:

- Die Datei etc/passwd

- Falls auf die Druckfunktionen von Samba zurückgegriffen wird, jegliche Binärdateien oder Konfigurationsdateien die für die Druckfunktion benötigt werden.

Außerdem kann es sein, dass noch weitere Dateien für Samba unter /var/fileserver/ zur Verfügung gestellt werden müssen. Dies hängt vom eingesetzten Betriebssystem ab.

**[netlogon] Freigabe**

Über die [netlogon] Freigabe kann Samba für Clients beispielsweise Windows-NT kompatible Richtlinien oder Anmeldeskripte bereitstellen. Wird eine [netlogon] Freigabe konfiguriert, so muss sichergestellt werden, dass unberechtigte Benutzer keinesfalls Dateien in dieser Freigabe modifizieren können. Dies kann beispielsweise durch den freigabespezifischen Parameter "read only = yes" erreicht werden.

**Benutzerdatenbanken**

Samba kann Benutzer nicht mit Hilfe der Mechanismen des darunter liegenden Unix-Betriebssystems authentisieren. Samba muss die in der Windows-Welt verwenden Hash-Werte (LAN Manager (LM) und/oder NTLM-Hashes) der Benutzerpasswörter separat speichern. Zur Abspeicherung der Hash-Werte verwendet Samba sogenannte Backends. Zusätzlich zu den Hash-Werten kann Samba, je nach verwendetem Backend, weitere Informationen über die Benutzer speichern.

Als Backend kann eine einfache Textdatei, eine Datenbank, oder ein LDAP-Verzeichnisdienst, das beispielsweise von OpenLDAP bereitgestellt wird, verwendet werden. In Samba 3.0.0 bis 3.0.23 konnten mehrere Backends gleichzeitig verwendet werden. Frühere sowie spätere Versionen von Samba unterstützen diese Funktion nicht. Backends sind:

- smbpasswd:
  Bei diesem Backend werden die Kontoinformationen in einer einfachen Textdatei abgespeichert. Im Gegensatz zu den Backends tdbsam und ldapsam kann dieses Backend keine der Microsoft Windows NT/200x SAM (Security Account Manager) Informationen abspeichern. Bei Neuinstallationen wird von der Verwendung dieses Backends daher abgeraten.
- tdbsam:
  Es wird empfohlen dieses Backend anstatt des Backends smbpasswd zu verwenden, auch wenn dies noch nicht die Standardeinstellung ist. Die Kontoinformationen werden in einer Trivial Database (TDB)-Datei abgelegt.
- ldapsam:
  Bei diesem Backend werden die Kontoinformationen in einem LDAP-Verzeichnis abgelegt. Dieses Backend bietet sich vor allem in großen Netzen an und vor allem dann, wenn ein Samba Primary Domain Controller/BDC-Setup eingesetzt wird.

Es muss sichergestellt werden, dass ein Benutzer keine Hash-Werte aus dem Backend auslesen kann. Bei den Backends smbpasswd und tdbsam sollte daher nur der Benutzer "root" Lese- und Schreibzugriff auf die Datei haben, in denen die Benutzerinformationen abgelegt werden. Alle anderen Benutzer sollten keinerlei Zugriffsrechte auf diese Datei besitzen. Wird das ldapsam Backend eingesetzt, sollten die Zugriffsrechte in äquivalenter Form mittels Access Control Lists (ACLs) umgesetzt werden.

Da unter Windows die Hash-Werte gleichbedeutend mit Klartextpasswörtern sind, sollten die Benutzer keinen Zugriff darauf bekommen. Um die Konse-

quenzen dieser Aussage zu verdeutlichen, wird im Folgenden kurz das NTLM- und NTLMv2- Authentisierungsverfahren von Windows erläutert. Das Prozedere, mit dem Windows-Rechner verschlüsselte Authentisierung ausüben, ist eine Anwendung eines symmetrischen Verschlüsselungsalgorithmus und wird durch ein ein Challenge-Response-Verfahren realisiert. Grob skizziert läuft das Verfahren folgendermaßen ab:

- Bevor ein SMB-Client eine Verbindung zu einem Server aufbaut, muss der Benutzer seinen Benutzernamen und sein Passwort eingeben. Anschließend wendet der Client eine Hash-Funktion auf das eingegebene Passwort an und speichert den daraus resultierenden Hash-Wert.
- Der Client baut eine Verbindung mit dem Server auf und erhält als Antwort eine Zufallszahl, auch Herausforderung (Challenge) genannt.
- Der Client verschlüsselt mit einem symmetrischen Verschlüsselungsalgorithmus die Herausforderung und benutzt dabei den Hash-Wert des Benutzerpassworts als Schlüssel.
- Der Client schickt den Benutzernamen und die verschlüsselte Herausforderung an den Server (Response).
- Der Server liest aus seiner Benutzerdatenbank den Hash-Wert aus dem Passwortfeld des Benutzers aus. Unter Windows werden in der Benutzerdatenbank nicht die Klartextpasswörter der Benutzer, sondern nur die Hash-Werte der Passwörter abgespeichert. Anschließend verwendet der Server den ausgelesenen Hash-Wert um die vom Client erhaltene Antwort (Response) zu entschlüsseln. Stimmt das Ergebnis mit der Zufallszahl überein, die der Server in Schritt 2 an den Client übermittelt hat, so ist die Authentisierung erfolgreich. Andernfalls schlägt eine Authentisierung fehl.

Falls ein Angreifer Zugriff auf den Benutzernamen und den Hash-Wert von dessen Passwort erhält, könnte er folgendermaßen verfahren: Werden einem SMB-Client der Benutzername und der Hash-Wert eines Benutzerpassworts als Passwort übergeben, wendet der SMB-Client normalerweise noch einmal eine Hash-Funktion auf das eingegebene Passwort an, bevor er die Antwort an den Server schickt. Eine Authentisierung würde in diesem Fall fehlschlagen. Verwendet ein Angreifer aber einen SMB-Client (zum Beispiel eine modifizierte Version von smbclient), der ohne vorhergehende Anwendung einer Hash-Funktion auf das eingegebene Passwort den Benutzernamen und das Passwort zum Server schickt, so kann er sich erfolgreich authentisieren. Daher sind die Hash-Werte der Klartextpasswörter unter Windows gleichbedeutend mit den Klartextpasswörtern.

Prüffragen:

- Werden Schreibzugriffe auf die Freigabe [netlogon] unterbunden?
- Ist sichergestellt, dass der Sicherheitsmodus share nicht verwendet wird?
- Ist sichergestellt, dass der Sicherheitsmodus server nicht verwendet wird?
- Verwendet Samba ausschließlich Kerberos zur Authentisierung, falls die Sicherheitsrichtlinien des Informationsverbundes dies erfordern?
- Setzt Samba ausschließlich die Version 2 des NTLM-Verfahrens (NTLMv2) zur Authentisierung ein?
- Wird Samba im Sicherheitsmodus ads betrieben, falls der Informationsverbund das Konzept von Standorten benutzt?
- Können nur ausgewählte Benutzer und Benutzergruppen auf den Samba-Dienst zugreifen?
- Ist Samba so konfiguriert, dass es Verbindungen nur von als sicher geltenden Hosts und Netzen entgegennimmt?
- Ist Samba so konfiguriert, dass es sich nur an als sicher geltende Netzadressen bindet?

- Wird verhindert, dass Benutzer Zugriff auf Informationen außerhalb der Freigaben haben, falls die Sicherheitsrichtlinien des Informationsverbundes dies erfordern?
- Wird von der Verwendung des smbpasswd-Backends abgesehen?
- Ist sichergestellt, dass Benutzer keine Hash-Werte der Benutzerpasswörter unberechtigt aus dem verwendeten Backend auslesen können?

# M 4.329 Sicherer Einsatz von Kommunikationsprotokollen beim Einsatz eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Durch Fehlkonfiguration der Kommunikationsprotokolleinstellungen kann die Verfügbarkeit und die Sicherheit der Dienste, die von einem Samba-Server zur Verfügung gestellt werden, beeinträchtigt werden. Um den sicheren Einsatz der verwendeten Kommunikationsprotokolle sicherzustellen, werden daher die folgenden Maßnahmen empfohlen.

### NetBIOS

Samba ist ausschließlich in der Lage, Network Basic Input/Output System (NetBIOS) über Transmission Control Protocol (TCP)/Internet Protocol (IP) zu benutzen. Für ein zuverlässig funktionierendes Netz ist es sehr wichtig, dass auf den Windows-Clients nur die Protokolle genutzt werden, die wirklich benötigt werden. Wenn Windows beispielsweise NetBEUI (NetBIOS Extended User Interface) zusätzlich zu TCP/IP nutzt, ist nicht eindeutig, ob die Windows-Netzwerkumgebung NetBEUI oder TCP/IP nutzt. Normalerweise ist heute ausschließlich TCP/IP notwendig. Internetwork Packet Exchange (IPX) kann noch benötigt werden, wenn Netware-Systeme auf den Samba-Server zugreifen müssen.

### Verschlüsselung

Das Server Message Block (SMB)-Protokoll unterstützt keine Verschlüsselung der Datenpakete. Durch die in M 4.334 *SMB Message Signing und Samba* beschriebene Maßnahme kann nur die Integrität der übertragenen Datenpakete geschützt werden. Bei einem erhöhten Schutzbedarf der übertragenen Informationen sollte daher die Verschlüsselung der übertragenen Informationen durch zusätzliche Maßnahmen sichergestellt werden. Eine gute Möglichkeit ist der Einsatz von Internet Protocol Security (IPSec).

Durch IPSec können alle IP-basierten Kommunikationsverbindungen von und zu einem Client abgesichert werden. Dabei ist es möglich, die Endpunkte der Kommunikation zu authentisieren und die Datenpakete signiert und verschlüsselt zu übertragen, so dass die Integrität und Vertraulichkeit der Daten bei erhöhten Anforderungen an die Sicherheit gewährleistet werden kann. Das Teilkonzept für eine IPSec-Infrastruktur sollte den erhöhten Administrationsaufwand berücksichtigen und setzt eine Verträglichkeitsprüfung mit den beteiligten Systemen in einer Testumgebung voraus. Generell darf der erhöhte Rechenaufwand und der mögliche Einfluss auf das Lastverhalten des Servers durch IPSec nicht vernachlässigt werden.

Prüffragen:

- Werden auf den Windows-Clients nur die wirklich benötigten Protokolle genutzt?
- Wird bei einem erhöhten Schutzbedarf der im Netz übertragenen Informationen eine Verschlüsselung dieser Informationen durch zusätzliche Maßnahmen sichergestellt?

# M 4.330 Sichere Installation eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Installation eines Samba-Servers sind verschiedene Aspekte zu berücksichtigen, die direkten Einfluss auf die Sicherheit haben.

Das Betriebssystem, auf dem der Samba-Dienst betrieben wird, muss unter Berücksichtigung vieler Sicherheitsaspekte installiert und konfiguriert werden. Dazu müssen die entsprechenden IT-Grundschutz-Bausteine umgesetzt werden. Darüber hinaus gibt M 4.331 *Sichere Konfiguration des Betriebssystems für einen Samba-Server* Hinweise, welche zusätzlichen Schritte auf dem Server durchgeführt werden müssen, der den Samba-Dienst ausführt.

Ein wichtiger Aspekt bei der Installation des Samba-Dienstes ist die Integrität der zu installierenden Software (siehe M 4.327 *Überprüfung der Integrität und Authentizität der Samba-Pakete und -Quellen*).

Die mit dem Samba-Dienst mitgelieferte Dokumentation ist sehr detailliert und beschreibt ausführlich die für eine Installation notwendigen Schritte. Die Grundschutz-Maßnahme kann die mitgelieferte Dokumentation nicht ersetzen, sondern lediglich Hinweise auf besonders zu beachtende Punkte geben. Sie bezieht sich auf die Installation eines Samba-Servers aus dem kompilierten Quelltext. Binärpakete von Betriebssystemherstellern oder Distributoren können davon abweichen.

**Kompilierung und Installation aus dem Quelltext**

Nachdem die Integrität und Authentizität des Quelltextpakets anhand der Pretty Good Privacy (PGP)-Signatur überprüft wurde, sollte das Paket unter einem unprivilegierten Benutzeraccount entpackt, konfiguriert (mit Hilfe des Skripts "configure") und übersetzt (Programm "make") werden. Erst der letzte Schritt, die eigentliche Installation des übersetzten Programms ("make install") muss gegebenenfalls mit höheren Privilegien erfolgen. Hat der unprivilegierte Benutzeraccount Schreibberechtigungen in sämtlichen Zielverzeichnissen der Installation, so kann selbst dieser letzte Schritt ohne "root" Berechtigungen durchgeführt werden. Von einer unkontrollierten Installation von Samba mittels "make install" in das Wurzeldateisystem des Servers ist abzuraten. Andernfalls kann eine restlose Deinstallation des Samba-Dienstes unter Umständen nur mit erheblichem manuellem Aufwand bewerkstelligt werden. Denkbar ist, beim letzten Schritt der Installation, (Aufruf von "make install") auf Hilfsmittel wie "CheckInstall" zurückzugreifen. Bei "CheckInstall" handelt es sich um ein Programm, dass aus dem übersetzten Quelltext automatisch Pakete für unterschiedliche Paketmanagementsysteme erstellt (beispielsweise RPM Package Manager (RPM) oder Debian). Die erstellten Pakete können anschließend über die Paketmanagementsysteme des verwendeten Betriebssystems installiert und bei Bedarf vollständig deinstalliert werden. Hat der Administrator bereits Erfahrung im Paketbau für das eingesetzte Paketmanagementsystem, ist es empfehlenswert, für die Samba-Version eigene Pakete zu erstellen.

Wird der Samba-Server aus dem Quelltext übersetzt, müssen die gewählten Parameter genau dokumentiert werden. Es ist wichtig, dass der Kompilationsvorgang anhand dieser Dokumentation jederzeit nachvollziehbar und reproduzierbar ist. Es empfiehlt sich zudem, ein Protokoll der Ausgaben des Konfi-

gurations- und Übersetzungslaufs (beispielsweise durch Umleiten der Ausgaben in eine Datei) anzufertigen und aufzubewahren.

Alle Schritte, die bei der Installation gemacht werden, sollten dokumentiert werden, damit sich die Konfiguration im Notfall schnell reproduzieren lässt. Dies betrifft neben den Einstellungen beim Kompilieren auch Installationspfade, Berechtigungen, Änderungen an der Konfigurationsdatei smb.conf und ähnliche Informationen.

Der Start des Samba-Servers sollte im Allgemeinen aus den Startup-Skripts des Betriebssystems erfolgen. So steht der Samba-Server auch nach einem Neustart des Servers direkt zur Verfügung.

Prüffragen:

- Wurde die Integrität der Software vor der Installation überprüft?
- Ist die Installation und Konfiguration ausreichend dokumentiert?
- Wurde das Quelltextpaket unter einem unprivilegierten Benutzeraccount entpackt, konfiguriert und übersetzt?
- Wurde Samba in kontrollierter Art und Weise in das Wurzeldateisystem des Servers installiert?
- Wurde dokumentiert, mit welchen Parametern der Kompilationsvorgang gestartet wurde?
- Wurde ein Protokoll der Ausgaben des Konfigurations- und Kompilationsvorgangs angefertigt?

# M 4.331 Sichere Konfiguration des Betriebssystems für einen Samba-Server

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Das Betriebssystem des Samba-Servers sollte für einen sicheren Betrieb in folgender Weise konfiguriert werden:

### ReiserFS und Datenbanken im TDB-Format

Samba legt in mehreren Verzeichnissen Datenbanken im Trivial Database (TDB)-Format ab. Die Verzeichnisse, in denen Samba diese Datenbanken ablegt, werden im Abschnitt "TDB-Dateien (Konfigurationsdaten und Statusinformationen" in M 6.135 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers* beschrieben.

Die Dateien in diesen Verzeichnissen sind für das einwandfreie Funktionieren von Samba sehr wichtig. Sämtliche Datenbanken im TDB-Format sollten auf einer Partition gespeichert werden, die nicht ReiserFS als Dateisystem verwendet (siehe G 4.72 *Inkonsistenzen von Datenbanken im Trivial Database Format unter Samba*).

### Einbinden von Dateisystemen

Einige der notwendigen Maßnahmen in B 5.17 *Samba* setzen voraus, dass das Dateisystem, auf dem Samba Freigaben anbietet, Access Control Lists (ACLs) unterstützt. Der Kernel des Servers, auf dem Samba ausgeführt wird, muss daher ACLs in Verbindung mit dem eingesetzten Dateisystem unterstützen. Zusätzlich muss sichergestellt werden, dass das Dateisystem mit den passenden Parametern eingebunden wird ("acl" Parameter des "mount"-Programms), damit die Unterstützung von ACLs auch aktiviert wird. Dasselbe gilt für Extended Attributes (xattr), falls diese in Verbindung mit Samba eingesetzt werden.

### Paketfilter

Samba benutzt die im Folgenden aufgelisteten Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) Ports:

- Port 137/UDP (benutzt vom Prozess nmbd): Network Basic Input/Output System (NetBIOS) Name Service
- Port 138/UDP (benutzt vom Prozess nmbd): NetBIOS Datagram Service
- Port 139/TCP (benutzt vom Prozess smbd): NetBIOS Session Service. Datei- und Druckdienste, falls Server Message Block (SMB) über NetBIOS eingesetzt wird.
- Port 445/TCP (benutzt vom Prozess smbd): Datei- und Druckdienste falls SMB über TCP/IP eingesetzt wird.

Zusätzlich zu den in M 4.328 *Sichere Grundkonfiguration eines Samba-Servers* beschriebenen Maßnahmen zu den Konfigurationsparametern "interfaces" und "bind interfaces only", sollten alle nicht angeführten Ports an einem lokalen Paketfilter auf den Interfaces und Internet Protocol (IP)-Adressen geblockt werden, über die Samba nicht erreichbar sein soll (siehe M 4.238 *Einsatz eines lokalen Paketfilters*).

Prüffragen:

- Sind am lokalen Paketfilter nur die TCP und UDP Ports frei geschaltet, die für den Betrieb des Samba-Servers nötig sind?
- Werden Datenbanken im TDB-Format ausschließlich auf Partitionen gespeichert, die nicht ReiserFS als Dateisystem verwenden?
- Unterstützt der Kernel des Betriebssystems, auf dem Samba ausgeführt wird, ACLs in Verbindung mit dem eingesetzten Dateisystem?
- Wird das Dateisystem mit den erforderlichen Parametern eingehängt?
- Falls nötig: unterstützt der Kernel des Betriebssystems, auf dem Samba ausgeführt wird, xattr in Verbindung mit dem eingesetzten Dateisystem?

# M 4.332 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Samba überlässt die Zugriffskontrolle im Dateisystem dem Kernel des Betriebssystems. Aus diesem Grund müssen für jeden Benutzer auf dem Samba-Server sowohl ein Windows- als auch ein Unix-Benutzerkonto vorhanden sein. Das heißt, dass jeder Domänenbenutzer mit allen Gruppenmitgliedschaften im Unix-Betriebssystem existieren muss.

Die Komplexität der Zugriffssteuerung beim Einsatz von Samba hat zwei Gründe. Samba kann erstens das Windows-Rechtemodell nicht direkt auf das von Unix abbilden und zweitens wertet Samba bei einem Zugriff auf das Dateisystem folgende Schichten aus:

- Unix-Dateiberechtigungen
- Samba Share Definitions
- Samba Share Access Control Lists (ACLs)

**Unix-Dateiberechtigungen**

Wenn ein Benutzer auf eine Freigabe eines Samba-Servers zugreifen will, muss sich der Benutzer zuerst am Samba-Dienst anmelden. Samba prüft anschließend, ob der angemeldete Benutzer im Unix-Dateisystem die nötigen Rechte für den Zugriff besitzt.

Samba bildet das Windows-Rechtemodell folgendermaßen im Unix-Dateisystem ab: Aus dem Standard Unix-Triplet "Benutzer" / "Gruppe" / "Andere Benutzer" ("user" / "group" / "others") wird eine NT ACL mit drei Elementen gebildet. Die Unix-Rechtebits werden dabei nach der folgenden Tabelle auf die NT-Berechtigungen abgebildet. Die Rechtebits für "Andere Benutzer" werden von Samba auf die Gruppe "Jeder" abgebildet. ACL-Einträge, die einem Benutzer bestimmte NT-Berechtigungen verweigern, können nicht gesetzt werden.

| NT Berechtigung | File Attribute Flag |
|---|---|
| Vollzugriff | # |
| Ordner durchsuchen / Datei ausführen | x |
| Ordner auflisten / Daten lesen | r |
| Attribute lesen | r |
| Erweiterte Attribute lesen | r |
| Dateien erstellen / Daten schreiben | w |
| Ordner erstellen / Daten anhängen | w |
| Attribute schreiben | w |
| Erweiterte Attribute schreiben | w |
| Unterordner und Dateien löschen | w |
| Löschen | # |
| Berechtigungen lesen | siehe Text |
| Berechtigungen ändern | # |

| NT Berechtigung | File Attribute Flag |
|---|---|
| Besitzrechte übernehmen | # |

Tabelle: Abbildung des Rechtemodells auf Unix-Dateisysteme

Das Zeichen "#" bedeutet, dass diese Berechtigung nur unter zwei Bedingungen für eine Datei oder ein Verzeichnis gesetzt wird. Entweder, wenn ein Windows-Administrator die Berechtigung "Vollzugriff" aktiviert, oder wenn der Benutzer oder dessen Gruppe im Unix-Dateisystem über die Berechtigungen für "lesen", "schreiben" und "ausführen" für diese Datei verfügen. Die NT Berechtigung "Berechtigungen lesen" wird einem Benutzer immer erlaubt, sobald diesem Benutzer mindestens eine weitere NT Berechtigung eingeräumt wird.

Wenn Windows NT4 Berechtigungen setzt, die nicht in dieser Tabelle aufgeführt sind, werden diese von Samba ignoriert. Eventuell vorhandene Portable Operating System Interface (POSIX) ACL-Einträge werden in derselben Art und Weise von Samba auf das NT-Rechtemodell umgesetzt. POSIX ACLs werden von Samba nur benutzt, um Berechtigungen für Benutzer und Gruppen zu setzen, wenn diese nicht die Besitzer der Datei oder des Verzeichnisses sind.

Samba kennt mehrere Möglichkeiten, um DOS-Attribute abzubilden. Diese Attribute sind Eigenschaften von Dateien, die es in dieser Form unter Unix nicht gibt. Viele Applikationen, die auf ein Netzlaufwerk zugreifen, setzen jedoch funktionierende DOS-Attribute voraus. Insgesamt kennt DOS vier verschiedene Attribute, die für Dateien vergeben werden können:

- Read-Only (Schreibschutz):
  Der Inhalt dieser Datei kann nur gelesen, aber nicht geschrieben werden. Die Datei kann nicht gelöscht werden. Da unter DOS die DOS-Attribute aber von jedem Benutzer frei gesetzt werden können, setzt dieses Attribut keinen effektiven Schreibschutz um. Das Schreibschutzbit ist nur als Hilfestellung gegen Fehlbedienungen zu verstehen.
- System (System):
  Diese Datei ist für spezielle Betriebssystemzwecke vorgesehen.
- Hidden (Versteckt):
  Diese Datei wird dem Benutzer nicht angezeigt (beispielsweise wenn er den Windows Explorer oder den Befehl "dir" auf der Kommandozeile benutzt.).
- Archive (Archiv):
  Das Archivbit wird bei jedem Schreibzugriff gesetzt. Sicherungsprogrammen ist es freigestellt, dieses Bit zurückzusetzen. Damit kann eine inkrementelle Sicherung ermöglicht werden.

Samba bildet DOS-Attribute standardmäßig auf Unix-Bits ab:

| Attribut | Unix-Recht | Maske | Parameter | Standard-wert |
|---|---|---|---|---|
| Schreibschutz | w Besitzer | 200 | map read only | yes |
| Archiv | x Besitzer | 100 | map archive | yes |
| System | x Gruppe | 010 | map system | no |
| Versteckt | x Andere | 001 | map hidden | no |

Tabelle: Abbildung der DOS-Attribute auf Unix-Dateisysteme

Da das Recht "Ausführen" unter DOS nicht existiert, kann das entsprechende Bit verwendet werden, um die DOS-Attribute im Unix-Dateisystem abzubilden. Das Schreibschutzbit unter DOS hat mit dem Schreibrecht des Dateibesitzers unter Unix ein ungefähr passendes Gegenstück.

Samba muss für den Eigenschafts-Dialog von Windows aus den Unix-Rechten die passenden Attribute für die Dateien erzeugen. Zudem muss Samba neu erstellten Dateien Unix-Rechte zuordnen. Wird eine Datei neu erstellt, übergibt der Client dem Server die gewünschten DOS-Attribute. Aus diesem Wunsch des Clients formt Samba einen Satz von Unix-Zugriffsrechten. Diese Rechte werden vom Parameter "create mask" eingeschränkt. Die Standardvorgabe für "create mask" ist 744, was der Maske rwxr--r-- entspricht. Der Dateieigentümer hat Schreib- und Leserecht, alle anderen haben reines Leserecht.

Samba schränkt die Rechte ein, indem der gewünschte Satz an Rechten mit einer logischen UND-Operation mit der create mask verknüpft wird. Nur die Rechte, die in "create mask" gesetzt sind, können möglicherweise in der neu erzeugten Datei auftauchen. In einem weiteren Schritt setzt Samba explizit gewünschte Zugriffsrechte anhand des Parameters "force create mode", dessen Standardwert auf 000 steht. Dies geschieht durch eine ODER-Verknüpfung mit diesem Wert.

Wenn auf neu erstellte Dateien nur der Dateibesitzer und die Gruppe Leserecht haben sollen und der Rest der die Dateien nicht lesen darf, wird die create mask = 740 gesetzt. Das maskiert das Leserecht für den Rest der Welt aus. Soll darüber hinaus die besitzende Gruppe ein Schreibrecht eingeräumt bekommen, lässt sich das durch "force create mode = 020" erreichen. Die Tabelle zeigt den Vorgang:

| **Gruppe erhält Schreibrecht** | | | |
|---|---|---|---|
| Aufgabenstellung | | | rw-r--r-- |
| create mask | 740 | UND | rw-r----- |
| | | | rw-r----- |
| force create mode | 020 | ODER | ----w---- |
| Ergebnis | | | rw-rw---- |

Bei "map read only = yes" in der smb.conf verhält sich Samba folgendermaßen: Wird das DOS-Attribut "Schreibschutz" gesetzt, so setzt Samba die "w"-Bits von Besitzer / Gruppe / Andere des Dateisystemobjekts auf "0". Die "w"-Bits in ACLs werden von Samba ignoriert. Wird hingegen das DOS-Attribut "Schreibschutz" entfernt, so setzt Samba lediglich das "w"-Bit des Besitzers des Dateisystemobjekts auf "1". Die "w"-Bits für Gruppe / Andere bleiben auf "0". Außerdem gibt es noch den Parameter "map read only = Permissions". Informationen zu diesem Parameter sind in der Manpage von smb.conf zu finden.

Zu beachten ist, dass die Samba Parameter "create mask" und "directory mask" das Setzen der Unix-Rechtebits verhindern können und die DOS-Attribute somit nicht übernommen werden. Die Spalte "Maske" gibt die mindestens notwendigen Werte für die Parameter "create mask" und "directory mask" an, die nötig sind, damit Samba alle nötigen Unix-Rechtebits setzen kann.

Unter bestimmten Bedingungen kann es zu Konflikten zwischen den Unix-Berechtigungen, die sich aus den DOS-Attributen ableiten und Unix-Berechtigungen, die sich aus einer Windows-ACL ableiten, kommen.

Diese von Samba standardmäßig verwendeten Parameter zum Abbilden von DOS-Attributen auf das Unix-Dateisystem sollten nicht verwendet werden. Stattdessen sollte Samba so konfiguriert werden, dass es DOS-Attribute in "Extended Attributes" speichert. Dazu sind in der Konfigurationsdatei smb.conf folgende Einstellungen notwendig:

*store dos attributes = yes*
*map archive = no*
*map read only = no*

**Samba Share Definitions**

Der Administrator kann durch eine Vielzahl von Konfigurationsparametern in der Konfigurationsdatei smb.conf die Zugriffssteuerung auf Freigaben und das Verhalten, wann Benutzer mit der Freigabe interagieren, beeinflussen.

Die benutzer- und gruppenbezogenen Konfigurationsparameter überschreiben die im Unix-Dateisystem gültigen Zugriffsberechtigungen für Benutzer oder Gruppen. Folgende Konfigurationsparameter stehen zur Verfügung:

- admin users
- force group
- force user
- guest ok
- invalid users
- only user
- read list
- username
- valid users
- write list

Die folgenden Konfigurationsparameter kontrollieren das Verhalten von Freigaben bei Operationen mit Dateien und Ordnern. Bevor einer dieser Parameter geändert wird, sollte die Manpage der Konfigurationsdatei smb.conf betrachtet werden:

- create mask
- directory mask
- dos filemode
- force create mode
- force directory mode
- force directory security mode
- force security mode
- hide unreadable
- hide unwriteable files
- nt acl support
- security mask

Des Weiteren gibt es noch diverse Einstellungen, die das Verhalten von Freigaben in unterschiedlicher Weise beeinflussen. Bevor einer dieser Parameter geändert wird, sollte die Manpage der Konfigurationsdatei smb.conf berücksichtigt werden:

- case sensitive, default case und short preserve case
- csc policy
- dont descend

- dos filetime resolution
- dos filetimes
- fake oplocks
- hide dot files, hide files und veto files
- read only und dessen invertierte Synonyme writeable und writable
- veto files

Für eine ausführliche Beschreibung aller Konfigurationsparameter sei auf die Manpage der Konfigurationsdatei smb.conf verwiesen ("man smb.conf").

**Samba Share ACLs**

Mit Samba kann, genauso wie mit Windows, für jede Freigabe eine ACL erstellt werden. Standardmäßig sind keine Einschränkungen aktiv. Das bedeutet, der Benutzer "Jeder" hat die Berechtigung "volle Kontrolle".

Samba speichert die ACLs für Freigaben in der Datei share_info.tdb. Samba stellt aber kein Programm zum Administrieren dieser ACLs zur Verfügung. Der Administrator ist daher auf Windows angewiesen. Unter Windows bieten sich dem Administrator folgende Möglichkeiten:

- Unter Windows NT4 kann der NT Server Manager zum Administrieren der ACLs der Freigaben eingesetzt werden.
- Unter Windows 2000 gibt es zwei Möglichkeiten. Es kann der Windows Dateimanager oder das Computer Management Snap-In für die Microsoft Management Console (MMC) benutzt werden.
    - Im geöffneten Dateimanager von Windows muss folgendermaßen vorgegangen werden: Rechtsklick auf den freigegebenen Ordner. Eigenschaften | Sicherheit. In diesem Fenster können die ACL-Einträge der Freigabe administriert werden.
    - Um das Computer Management Snap-In für die MMC zu benutzen muss folgendermaßen vorgegangen werden: Zuerst wird die MMC mit dem Computer Management Snap-In geladen: Systemsteuerung / Verwaltung / Computerverwaltung. Danach Aktion | Verbindung mit anderem Computer herstellen. Hostname des Samba-Servers eingeben. Damit eine Verbindung mit dem Computer aufgenommen werden kann, benötigt der Benutzer administrative Privilegien in der Domäne. Nachdem zum Samba-Server erfolgreich eine Verbindung hergestellt wurde, können folgende Schritte vollzogen werden: Auswählen von System | Freigegebene Ordner | Freigaben. Anschließend im rechten Fenster - Rechtsklick auf die Freigabe die administriert werden soll | auswählen der Registerkarte "Sicherheit" - In diesem Fenster kann die ACL der Freigabe administriert werden.

Werden dem Benutzer "Jeder" sämtliche Rechte entzogen, ohne ihn aus der ACL der Freigabe komplett zu löschen, so hat kein Benutzer mehr Zugriff auf die Freigabe. Der Grund hierfür ist, dass ACL-Einträge, die die Rechte eines Benutzers verringern, Vorrang haben vor ACL-Einträgen, die die Rechte eines Benutzers ausweiten.

Prüffragen:

- Werden zur Abbildung der DOS-Attribute im Unix-Dateisystem Extended Attributes verwendet?
- Sind die Administratoren damit vertraut, wie Samba das Windows-Rechtemodell im Unix-Dateisystem abbildet?
- Wissen die Administratoren, wie die Unix-Rechte für neu erstellte Dateien zu Stande kommen?

- Ist den Administratoren klar, wie sich das Entfernen des DOS-Attibuts "Schreibschutz" auf die UNIX-Rechte auswirkt?
- Wissen die Administratoren, dass die benutzer- und gruppenbezogenen Konfigurationsparameter die im Unix-Dateisystem gültigen Zugriffsberechtigungen für Benutzer oder Gruppen überschreiben?

# M 4.333 Sichere Konfiguration von Winbind unter Samba

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wird Samba im "domain"- oder "ads"- Security-Mode eingesetzt (siehe M 4.328 *Sichere Grundkonfiguration eines Samba-Servers*), spielt die sichere Konfiguration von Winbind eine wichtige Rolle. In diesem Fall sind eine ganze Reihe von Empfehlungen zu berücksichtigen.

Mit dem Beitreten einer Domäne ist smbd in der Lage, Benutzer beim Domain Controller (DC) zu authentisieren. Je nach Security Mode und Client geschieht dies durch Auswertung des Kerberos-Tickets oder durch Nachfragen beim DC. Insbesondere letzteres ist aufwändig, da sich smbd einen DC suchen und sich dort anmelden muss, bevor er die Benutzerauthentisierung durchführen kann. Dies generiert mindestens 30 Netzpakete, von denen nur zwei für die eigentliche Authentisierung relevant sind.

Windows arbeitet anders. Die Local Security Authority (LSA) baut beim Start des Domänenmitglieds einmal eine Verbindung zum DC auf und authentisiert sich als Maschine. Sämtliche Benutzerauthentisierungen laufen danach nur noch über diese Verbindung. Dieses Konzept mit smbd allein umzusetzen funktioniert nicht, da es für jeden Client einen eigenen smbd-Prozess gibt und sich Netzverbindungen nicht einfach von mehreren Prozessen gleichzeitig nutzen lassen.

Daher kann als Proxy für die Verbindung zum DC winbindd eingesetzt werden. Er hat eine, mit der LSA unter Windows vergleichbare, Funktion. Insbesondere hält er eine Verbindung zum DC offen und bietet seine Dienste für alle Prozesse im System über einen Unix Domain Socket unter /tmp/winbindd/pipe an. Die smbd-Prozesse versuchen sich bei einer Authentisierung zunächst mit diesem Socket zu verbinden. Erst wenn dies fehlschlägt, initiieren die Prozesse selbst eine Verbindung mit einem DC.

Neben der erfolgreichen Authentisierung benötigt Samba weitere Informationen über einen Benutzer. Es ist erforderlich, dass für jeden Benutzer ein Windows- und ein Unix-Benutzerkonto auf dem Samba-Server vorhanden sind. Das Unix-Benutzerkonto wird unter anderem benötigt, damit Samba die Zugriffskontrolle im Dateisystem dem Kernel überlassen kann (siehe auch M 4.332 *Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server*).

Das heißt, dass jeder Domänenbenutzer mit allen Gruppenmitgliedschaften im Unix-Betriebssystem existieren muss. Theoretisch ist es möglich, alle Domänenbenutzer von Hand unter Unix nachzupflegen. Von dieser Vorgehensweise sollte aber abgesehen und stattdessen Winbind eingesetzt werden.

Winbind ist in der Lage, dynamisch zu Windows-Benutzern und -Gruppen passende Unix-Benutzer und -Gruppen zu erzeugen, falls diese unter Unix noch nicht existieren. Dabei kommt das "nss_winbind"-Modul zum Einsatz., es kann durch einen Eintrag in /etc/nsswitch.conf eingebunden werden. Dies könnte beispielsweise folgendermaßen aussehen:

*passwd: files winbind*
*group: files winbind*

Mit diesen Einstellungen sucht das Betriebssystem Benutzernamen erst in der Datei /etc/passwd. Findet es dort keinen passenden Benutzer, kontaktiert es winbindd. Damit winbindd in der Lage ist, zu einem Benutzernamen dynamisch alle erforderlichen Unix-Benutzerattribute (beispielsweise Benutzer-ID, Heimatverzeichnis oder Login-Shell) zu erzeugen, muss der Daemon zwei Schritte durchführen. Zuerst erfragt Winbind beim DC den Security Identifier (SID) des Benutzernames. Danach muss Winbind, da der DC normalerweise die Unix-Benutzer-ID für einen Benutzer nicht kennt, selbst eine passende Unix-Benutzer-ID zur SID finden. Je nach konfiguriertem ID-Mapping-Backend geht Winbind anders vor:

- tdb:
  Dabei handelt es sich um die Standardeinstellung. Meldet sich ein Benutzer, dem noch keine Unix-Benutzer-ID zugeordnet ist, an, so weist Winbind dem Benutzer aus einem vorgegebenen Bereich die nächste freie Unix-Benutzer-ID zu und speichert das ID-Mapping lokal in einer tdb-Datei. Die ID-Mappings werden in der Datei winbindd_idmap.tdb abgelegt.
  Ein Verlust dieser Datei führt zum Verlust sämtlicher Rechtezuordnungen im Dateisystem. Dies kann zu schwerwiegenden Sicherheitslücken führen. Folgendes Beispiel verdeutlicht dies:
  Der Benutzer "Benutzer1" meldet sich mit seinem Windows-Benutzernamen BERLIN\benutzer1 zum ersten Mal am Samba-Server an. Der Benutzer BERLIN\benutzer1 hat in der Windows-Domäne die SID S-1-5-12-7623811015-3361044348-030300820-1013. Windbind reserviert eine freie Unix-Benutzer-ID und ordnet der SID die Unix-Benutzer-ID 2000 zu. Dieses Mapping wird in der Datei winbindd_idmap.tdb abgelegt.
  Nach einer erfolgreichen Anmeldung legt der Benutzer BERLIN\benutzer1 einige Dateien auf dem Samba-Server ab. Diese werden unter der Unix-Benutzer-ID 2000 abgespeichert. Nach einer falsch durchgeführten Sicherung der Datei winbindd_idmap.tdb gehen einige der darin gespeicherten Mappings verloren. Kurze Zeit später meldet sich der Benutzer "Benutzer2" mit seinem Windows-Benutzernamen BERLIN\benutzer2 am Samba-Server an. Der Benutzer BERLIN\benutzer2 hat in der Windows-Domäne die SID S-1-5-12-7623811015-3361044348-030300820-1017. Da die Zuordnung der Unix-Benutzer-ID 2000 durch den Datenverlust verloren gegangen ist, ordnet Winbind diese der SID von Benutzer2 zu.
  Der Benutzer "Benutzer2" kann nun auf alle Dateien zugreifen, die der Benutzer Benutzer1 ursprünglich unter der Unix-Benutzer-ID 2000 abgelegt hat.
  Es muss daher eine regelmäßige Sicherung der Datei winbindd_idmap.tdb durchgeführt werden. Zusätzlich zu den in M 6.135 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers* angeführten Erläuterungen und Empfehlungen kann das ID-Mapping auch auf folgende Weise gesichert werden. Der Befehl "net idmap dump" führt zu einer Klartextdatei, die sich im Bedarfsfall mit "net idmap restore" wiederherstellen lässt.
- rid:
  Dieses Backend verwendet den Relative Identifier (RID), die Zeichen hinter dem letzten Bindestrich des Windows-SID, um die Unix-Benutzer-ID algorithmisch zu berechnen. Bei diesem Backend wird keine Datenbank benötigt, da das Mapping deterministisch erfolgt.
- ad:
  Dieses Backend lässt sich verwenden, wenn im Active Directory die Erweiterungen für die Services For Unix (SFU) implementiert sind und Samba im "ads" Security Mode betrieben wird. Im Rahmen dieser Erweiterung kann der Administrator im Active Directory explizit Unix-Benutzer-IDs ver-

geben. Winbind liest bei diesem Backend die ID-Mappings nur aus. Ergänzungen oder Änderungen an ID-Mappings werden von Winbind nicht vorgenommen.
Außerdem handelt es sich bei diesem Backend um das Einzige, das Winbind nutzen kann, um noch weitere Unix-Benutzerattribute zu beziehen (zum Beispiel das Heimatverzeichnis oder die Login-Shell eines Benutzers). Bei allen anderen Backends müssen hierfür andere Mechanismen eingesetzt werden, beispielsweise die Konfigurationsparameter "template shell" und "template homedir" in der Konfigurationsdatei smb.conf.

- ldap:
  Dieses Backend speichert selbst gewählte ID-Mappings in einem Lightweight Directory Access Protocol (LDAP)-Verzeichnis.
- nss:
  Dieses Backend nimmt kein Mapping anhand von SIDs vor, sondern setzt voraus, dass Domänencontroller und Domänenmitglied die /etc/passwd Informationen mit anderen Mitteln, etwa per nss_ldap, synchronisieren. Fragt ein System Winbind dennoch nach einem Mapping, liefert er dieses namensbasiert zurück. Das heißt, er konvertiert einen SID zunächst in den zugehörigen Benutzernamen und schlägt den Namen in /etc/passwd nach. Dieses Backend löst den Winbind Parameter "winbind trusted domains only" ab.

Weitere Informationen über die unterschiedlichen Backends für das ID-Mapping finden sich in deren Manpages. Diese sind nach dem Schema "idmap_<name des backends>" benannt. Die Eingabe "man idmap_nss" liefert weitere Informationen zum nss-Backend. Jedes der ID-Mapping-Backends hat individuelle Konfigurationsparameter. Zur Fehleranalyse sollte das Programm "wbinfo" benutzt werden.

Neben der Unix-Benutzer-ID muss Winbind in der Regel jedem Benutzer weitere Unix-Benutzerattribute zuordnen, beispielsweise ein Heimatverzeichnis. Dies lässt sich über Parameter wie "template homedir" oder "template shell" steuern. Nur beim ID-Mapping-Backend "ad" steht, wie bereits angeführt, zusätzlich ein anderer Mechanismus zur Verfügung.

Wenn es nur einen Samba-Server als Domänenmitglied gibt und die Unix-Benutzer-IDs serverübergreifend nicht synchronisiert werden müssen, kann das ID-Mapping-Backend tdb benutzt werden.

Gibt es mehrere Samba-Server als Domänenmitglieder und müssen daher die Unix-Benutzer-IDs serverübergreifend synchronisiert werden, dann muss auf eines der anderen ID-Mapping-Backends zurückgegriffen werden.

Falls eine Vertrauensstellung zwischen Domänen im Informationsverbund existiert, so muss die folgende Empfehlung im Abschnitt Vertrauensstellungen zwischen Domänen umgesetzt werden.

**Vertrauensstellungen zwischen Domänen**

Eine Vertrauensstellung ist eine Beziehung zwischen Domänen, durch die Benutzer einer Domäne von einem DC authentifiziert werden können, der sich in einer anderen Domäne befindet.

Auch wenn momentan noch keine Vertrauensstellungen zwischen Domänen im Informationsverbund existieren, ist es sinnvoll, in Hinblick auf die Zukunft, die Maßnahmen in diesem Abschnitt umzusetzen.

**Unix-Benutzer-IDs**

Windows weist jedem Benutzer und jeder Gruppe eine eindeutige ID zu, den SID (Security Identifier). Der SID enthält einen 96 Bit großen Domänenanteil und einen, innerhalb der Domäne eindeutigen, RID (Relative Identifier). Solange nur eine Domäne im Informationsverbund existiert, kann Unix den RID verwenden um eine eindeutige Unix-Benutzer-ID zu berechnen. Existieren im Informationsverbund mehrere Domänen, die sich gegenseitig vertrauen, funktioniert diese Vorgehensweise nicht mehr. Vertraut die Domäne, in der der Samba-Server Mitglied ist, einer anderen Domäne, ist der RID nicht mehr eindeutig. Der RID "500" bezeichnet grundsätzlich den Administrator, der RID "513" ist der Gruppe der Domänenbenutzer zugeordnet und ab 1000 aufsteigend vergibt jede Domäne fortlaufend RIDs.

Seit Samba Version 3.0.25 gibt es den Parameter "idmap domains". Dieser Parameter ermöglicht es das ID-Mapping, abhängig vom Namen der Domäne, zu konfigurieren.

*[global]*
*idmap domains = BONN BERLIN*
*idmap config BONN:backend = rid*
*idmap config BONN:range = 10000 - 49999*
*idmap config BERLIN:backend = rid*
*idmap config BERLIN:range = 50000 - 99999*

Im oben angeführten Beispiel würde dem Benutzer BONN\Administrator die Unix-Benutzer-ID 10500 zugewiesen, während der Benutzer BERLIN\Administrator die Unix-Benutzer-ID 50500 von Winbind erhalten würde.

Existieren Vertrauensstellungen zwischen Domänen im Informationsverbund, so muss eines der folgenden ID-Mapping-Backends verwendet werden:

- Backend rid mit idmap domains Konfiguration.
- Backend ldap mit idmap domains Konfiguration.
- Backend ad.
- Backend nss.

**Unix Heimatverzeichnis**

Die Domäne des Benutzers sollte in den Pfad seines Heimatverzeichnisses aufgenommen werden. Diese Maßnahme verhindert Namenskollisionen bei Vertrauensstellungen. Der Benutzer "benutzer1" in der Domäne BERLIN muss ein anderes Heimatverzeichnis bekommen als der Benutzer "benutzer1" in der Domäne BONN. Dies kann mit folgendem Eintrag in der smb.conf Konfigurationsdatei realisiert werden:

*template homedir = /home/%D/%u*

Alternativ kann man die Heimatverzeichnisse der Benutzer auch im Active Directory (AD) pflegen, wenn Winbind das ID-Mapping-Backend "ad" einsetzt. Im oben angeführten Beispiel würde der Benutzer BERLIN\benutzer1 das Unix Heimatverzeichnis /home/BERLIN/benutzer1 zugewiesen bekommen.

Die Heimatverzeichnisse werden von Winbind nicht automatisch erzeugt. Dies ist, wenn der Samba-Server beispielsweise als Dateiserver eingesetzt wird, auch nicht wünschenswert.

**Unix-Benutzername**

Um die Eindeutigkeit der Benutzernamen zu gewährleisten, müssen Windows-Benutzernamen auf folgende Art und Weise in Unix-Benutzernamen umgesetzt werden. Der Unix-Benutzername des Windows-Benutzers BONN \benutzer1 lautet BONN<winbind seperator>benutzer1. Standardmäßig ist der Parameter "winbind seperator" auf das Zeichen '\' voreingestellt. Bereitet das voreingestellte Zeichen auf Unix-Systemen Probleme, beispielsweise hat das Zeichen '\' für Unix Eingabeaufforderungen eine Sonderbedeutung, so kann in der Konfigurationsdatei smb.conf ein anderes Zeichen spezifiziert werden.

Beim Ändern des Parameters "winbind seperator" muss vorher geprüft werden an welchen Stellen Domänenbenutzer und -gruppen angegeben sind (beispielsweise in der Konfigurationsdatei smb.conf). Alle diese Stellen müssen nach Ändern des Parameters angepasst werden.

Prüffragen:

- Wurde Winbind so konfiguriert, dass es zu keinen Kollisionen bei Unix-Benutzer-IDs kommt?
- Wurde Winbind so konfiguriert, dass es zu keinen Kollisionen bei Benutzerverzeichnissen in Domänen mit Vertrauensstellungen kommt?
- Setzt Winbind Windows-Benutzernamen in eindeutige Unix-Benutzernamen um?
- Wird regelmäßig eine Sicherung des ID-Mappings erstellt?

# M 4.334 SMB Message Signing und Samba

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Samba unterstützt in der Version 3 Server Message Block (SMB) Message Signing. Beim SMB Message Signing wird jedem Paket eine Signatur hinzugefügt. So weiß der Client, dass das Paket vom richtigen Server stammt und der Server, dass ein Paket vom richtigen Client stammt. Ohne SMB Message Signing ist das SMB-Protokoll anfällig für Man-in-the-Middle-Angriffe. Microsoft unterstützt SMB Message Signing seit Microsoft Windows NT 4.0 Service Pack 3 (SP3) and Microsoft Windows 98.

Der Konfigurationsparameter "client signing" ist auf "auto" voreingestellt, während "server signing" auf "disabled" voreingestellt ist. Diese Voreinstellungen in smb.conf decken sich weitestgehend mit denen der Microsoft Betriebssysteme (nachzulesen im Microsoft Knowledge Base Article #887429). Folgende Unterschiede sind zu beachten:

- Windows 2000 in der Rolle als Domain Controller (DC) aktiviert SMB Message Signing für den Server Service.
- Windows 2003 in der Rolle als Domänencontroller setzt SMB Message Signing für den Server Service voraus.

Microsoft hat SMB Message Signing standardmäßig nur auf Domänencontrollern aktiviert, da SMB Message Signing einen deutlichen negativen Einfluss auf die Performance hat. Beim Übertragen kleiner Datenmengen können die Performanceeinbußen in der Regel vernachlässigt werden. Werden große Datenmengen übertragen, kann sich die Performance in manchen Situationen bis um die Hälfte reduzieren.

Es wird empfohlen, den Vorgaben von Microsoft zu folgen, sofern dies nicht im Widerspruch zu den existierenden Sicherheitsrichtlinien im Informationsverbund steht. Wird Samba als Domänencontroller eingesetzt, so sollte "server signing = yes" in der Konfigurationsdatei smb.conf gesetzt werden. Wird Samba hingegen exklusiv als Dateiserver eingesetzt, so sollte die Standardeinstellung beibehalten werden.

Prüffragen:

- Ist SMB Message Signing bei Samba in Abstimmung mit den geltenden Sicherheitsrichtlinien des Informationsverbundes umgesetzt?
- Wird SMB Message Signing verwendet, falls Samba in der Rolle als Domänencontroller eingesetzt wird?

# M 4.335 Sicherer Betrieb eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Sicherheit eines Samba-Servers auch im Betrieb aufrecht zu erhalten, genügt es nicht, eine sichere Anfangskonfiguration zu erzeugen. Vielmehr müssen regelmäßig eine Reihe von Maßnahmen durchgeführt werden, um eventuelle Probleme rechtzeitig zu entdecken. Beim Betrieb eines Samba-Servers sollten insbesondere folgende Aspekte berücksichtigt werden:

- Änderungen an der Konfiguration müssen sorgfältig dokumentiert werden, so dass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat. Für die Änderungen an den Konfigurationsdateien wird empfohlen, ein Revisionskontrollprogramm (beispielsweise git, mercurial oder RCS) einzusetzen. So kann jederzeit ein früherer Stand der Konfiguration wiederhergestellt werden und es bleibt nachvollziehbar, wer welche Änderungen aus welchem Grund durchgeführt hat.
- Nach jeder Änderung an der Datei smb.conf muss zunächst mit dem Programm testparm geprüft werden, ob die Syntax der Konfigurationsdatei korrekt ist. Syntaxfehler in der Konfigurationsdatei können sonst dazu führen, dass der Server nicht neu startet oder Sicherheitslücken entstehen.
- Die Zugriffsberechtigungen der Samba Freigaben sollten regelmäßig überprüft werden (siehe M 4.332 *Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server*). Insbesondere sollte dies nach Software-Updates oder Konfigurationsänderungen geschehen. Für die Dateien des Servers selbst (beispielsweise das Serverprogramm smbd oder die Konfigurationsdatei smb.conf) sollten Prüfsummen angelegt und regelmäßig überprüft werden.
- Die Administratoren müssen sich über aktuelle Sicherheitslücken in der eingesetzten Software frühzeitig informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Informationen über neu entdeckte Sicherheitslücken veröffentlicht das Samba Team stets auf der samba-announceMailing-Liste (http://lists.samba.org/archive/samba-announce/). Eine Übersicht über alle bis dato veröffentlichten sicherheitsrelevanten Patches wird außerdem auf http://www.samba.org/samba/security/ gepflegt.
- Die in M 2.64 *Kontrolle der Protokolldateien* beschriebenen Maßnahmen müssen auch in Verbindung mit Samba umgesetzt werden. In der Regel speichern die Applikationen nmbd, smbd und winbind ihre Protokolldaten im Verzeichnis /var/log/samba/.
- Zum sicheren Betrieb gehören auch regelmäßig durchzuführende Maßnahmen zur Datensicherung und zur Notfallvorsorge (siehe M 6.135 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers*).

Prüffragen:

- Werden Änderungen an der Konfiguration sorgfältig dokumentiert, so dass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat?
- Wird nach jeder Änderung an der Konfigurationsdatei smb.conf mit Hilfe des Programms testparm überprüft, ob die Syntax noch korrekt ist?
- Werden die effektiven Zugriffsberechtigungen auf die Freigaben des Samba-Servers regelmäßig überprüft?

- Informieren sich die Administratoren regelmäßig, ob neue Sicherheitslücken in Samba entdeckt wurden?
- Werden die Protokolldateien des Samba-Servers regelmäßig überprüft?
- Werden Maßnahmen der Datensicherung und Notfallvorsorge regelmäßig durchgeführt?

# M 4.336 Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für ein arbeitsfähiges Windows-System müssen ab Windows Vista oder Windows Server 2008 das Betriebssystem installiert und im Anschluss eine Lizenz aktiviert werden. Ein nur installiertes und nicht aktiviertes Windows Vista ist nach Ablauf einer definierten Kulanzfrist (Grace Period) von 30 Tagen nicht mehr arbeitsfähig. Der Vista Client fällt dann zwangsweise in den so genannten RFM (Reduced Functionality Mode, Modus mit reduzierter Funktionalität). Ab Windows Vista Service Pack 1, Windows 7 und Windows Server 2008 hat der Hersteller den RFM zurückgenommen. Anstelle des RFM zeigen die Systeme nun entsprechende Warnmeldungen an.

Lizenzen für Windows Vista Enterprise,Windows 7 Enterprise und Windows 8 Enterprise können nur im Rahmen eines Volumenlizenzvertrags erworben werden. Weitere Voraussetzung ist, dass der Kunde zusätzlich auch einen so genannten "Software-Assurance-Vertrag" mit Microsoft schließt. Volumenlizenzverträge können analog auch für die Server-Betriebssysteme abgeschlossen werden. Eine Volumenlizenz ist ein Produkt-Schlüssel, mit dem eine Institution für eine bestimmte Anzahl von Clients die Nutzung einer bestimmten Software aktivieren kann.

Die Aktivierung von Windows-Lizenzen aus einem Volumenlizenzvertrag erfolgt durch das Tool "Volume Activation Management Tool" (VAMT). Es handelt sich dabei um eine eigenständige Anwendung, welche die Aktivierungsanforderungen mehrerer Computer zusammenträgt und gebündelt an Microsoft versendet.

### Wahl der geeigneten Aktivierungsform

Bei einer Aktivierung aus einem Volumenlizenzvertrag gibt es die Aktivierungsformen

- MAK-Proxyaktivierung (Multi Activation Key, Mehrfachaktivierungsschlüssel),
- MAK-unabhängige Aktivierung und
- KMS-Aktivierung (Key Management Service, Schlüsselverwaltungsdienst).

Zusätzlich zur Aktivierung mittels MAK und KMS ist unter Windows 8 und Windows Server 2012 noch die folgenden Aktivierungsmethode hinzugekommen:

- Aktivierung mit Active Directory "Activation Objects" über die Rolle Volumenaktivierungsdienste.

Innerhalb dieser Aktivierungsformen gibt es weitere Unterscheidungen, die durch die Kommunikationswege zum Austausch der Lizenzinformationen mit Microsoft begründet sind. Unterstützt werden Internet und Telefon. Teil der Lizenzinformationen ist das Schlüsselmaterial, das auf den zu aktivierenden Systemen oder beteiligten Hilfsprogrammen im Zuge der Aktivierung automatisch oder manuell eingespielt wird.

Es muss die geeignete Aktivierungsform ausgewählt werden. Zu den Kriterien für die Auswahl zählen die Anzahl der zu aktivierenden Systeme sowie der Verbindungsstatus der Systeme zu einem LAN und zum Internet. Nachfolgend werden die möglichen Kriterien zu einer geeigneten Aktivierungsform und wichtige Eigenschaften jeder Aktivierungsform genannt.

**Auswahlkriterien für eine geeignete Aktivierungsform**

Die Aktivierung aus einem Volumenlizenzvertrag ist ein sehr komplexer Vorgang, der im Rahmen des vorliegenden Textes nur zur ersten Orientierung vorgestellt werden kann. Weitere Informationen liefert die Dokumentation des Herstellers.

Die nachfolgende Tabelle führt Kriterien auf, die für die Wahl der geeigneten Aktivierungsform relevant sind.

| Zielsysteme | Aktivierungsmethode | Beschreibung |
|---|---|---|
| Windows Server 2012 oder Windows 8, mindestens einmal alle 180 Tage mit Netzverbindung zum Active Directory | Aktivierung über Active Directory | Wenn ein Standort mit einer sicheren Verbindung mit dem Kernnetzwerk vorhanden ist, kann für Systeme unter Windows Server 2012 oder Windows 8 die Aktivierung über Active Directory verwendet werden. |
| Windows-Versionen vor Windows Server 2012 und Windows 8, mindestens einmal alle 180 Tage mit Netzverbindung zum Netz, KMS-Aktivierungsschwellwert wird überschritten. | KMS | Wenn ein Standort mit einer sicheren Verbindung mit dem Netz vorhanden ist, kann KMS zum Aktivieren über das Netz verwendet werden. |
| Computer ohne Netzanbindung oder in isolierten Netzen, oder Windows-Versionen vor Windows Server 2012 und Windows 8, bei denen der KMS-Aktivierungsschwellwert nicht erreicht wird. | MAK | Unabhängige MAK-Aktivierung per Telefon oder über das Internet für Computer, auf denen selten oder nie eine Verbindung mit dem Kernnetzwerk hergestellt wird. |

Die einzelnen Aktivierungsmethoden können je nach der Konnektivität der betrachteten Systeme unterschiedlich ausgeprägt sein. Dafür kommen die in der folgenden Tabelle dargestellten Fälle in Betracht:

| **Aktivierungsmethode** | **Konnektivität** | | | **Szenario** |
|---|---|---|---|---|
| | Direkte Internetanbindung | Internet-Zugang über Proxy möglich | Zugang zu zentralem Server möglich | |
| Active Directory | | X | X | Fall 1: Online-Aktivierung mit VAMT |
| | | | X | Fall 1: Proy-Aktivierung mit VAMT |
| MAK | | X | X | Fall 2: MAK-Proxyaktivierung |
| | X | | | Fall 2: MAK-unabhängige Aktivierung über Internet |
| | | | | Fall 3: MAK-unabhängige Aktivierung über Telefon |
| KMS | | X | X | Fall 4: KMS-Aktivierung über LAN / Internet |
| | | | X | Fall 4: KMS-Aktivierung über LAN / Telefon |

**Ausgewählte Eigenschaften der Aktivierungsformen**

Fall 1: Aktivierung über Active Directory - Active Directory Based Activation

- In Windows Server 2012 wurden so genannte Activation Objects eingeführt, um die zentrale Aktivierung über Active Directory - Active Directory Based Activation (ADBA) - zu ermöglichen. Der Vorteil dieser Aktivierungsmethode besteht darin, dass kein zusätzlicher KMS-Host erforderlich ist. ADBA funktioniert allerdings momentan nur mit Windows Server 2012 und Windows 8 und setzt ein Windows-Server-2012-Schema im Active Directory voraus. ADBA erfordert die Installation der Serverrolle "Volume Activation Services".
- Für die Aktivierung über Active Directory werden die Produktschlüssel verwendet, die auch von KMS verwendet werden.
- Die Aktivierung der Systeme bleibt nur so lange bestehen, wie diese Mitglied der Domäne sind. Eine weitere Voraussetzung ist ebenfalls das Vorhandensein eines Generic Volume License Keys (GVLK). Die Aktivierungsanforderungen werden jeweils während des Computerstarts verarbeitet, direkt nach dem Start des "Licensing Service". Dabei kontaktiert der

Computer automatisch den Domänencontroller und empfängt das "Activation Object", alles ohne Benutzeraktion.
- Für isolierte Arbeitsgruppen ohne Internetzugang ist die Aktivierung über einen Proxy zusätzlich zur direkten Online-Aktivierung möglich.
- ADBA besitzt keine Obergrenzen mehr, wie dies für KMS der Fall ist. Die Produkte werden aktiviert, sobald der Client mit der Domäne verbunden ist. Das Produkt bleibt nach der Aktivierung 180 Tage aktiv und wird automatisch erneuert, vorausgesetzt, das Produkt ist weiterhin mit der Domäne verbunden.

Fall 2, MAK-Proxyaktivierung, über LAN und Internet

- Der Administrator installiert einmalig das VAMT (Volume Activation Management Tool) auf einem IT-System im LAN. Das VAMT dient als MAK-Proxy und zur Verwaltung der Volumenlizenzen. Das VAMT unterstützt das Client-Betriebssystem Windows Vista, die Windows-7-Editionen Business und Enterprise, Windows 8 Professional und Enterprise und die Server-Betriebssysteme ab Windows Server 2008 ab SP2.
- Zum Austausch von Lizenzinformationen kommuniziert jedes System mit dem MAK-Proxy im LAN. Der MAK-Proxy kommuniziert mit Microsoft über das Internet.
- Auf jedem System werden die notwendigen Lizenzinformationen (MAK-Lizenzschlüssel) automatisch installiert.
- Die Aktivierung muss nicht erneuert werden.
- Zu Beginn des Aktivierungsvorgangs muss die Anzahl der möglichen Aktivierungen festgelegt werden. Bei Bedarf können Lizenzen nachgekauft werden.

Fall 3, MAK-unabhängige Aktivierung

- Jedes System muss einzeln durch den Administrator aktiviert werden.
- Zum Austausch von Lizenzinformationen kommuniziert jedes System einzeln mit Microsoft über das Internet. Ist keine Internet-Verbindung möglich, kann der Austausch auch durch die Administratoren per Telefon erfolgen.
- Der MAK-Lizenzschlüssel wird auf jedem System automatisch installiert oder muss bei telefonischer Aktivierung eingegeben werden.
- Die Aktivierung muss nicht erneuert werden.
- Zu Beginn des Aktivierungsvorhangs muss die Anzahl der möglichen Aktivierung festgelegt werden. Bei Bedarf können Lizenzen nachgekauft werden.

Fall 4, KMS-Aktivierung

- Der Administrator installiert einmalig den KMS auf einem IT-System im LAN und aktiviert diesen online oder per Telefon bei Microsoft. Der KMS unterstützt die Client-Betriebssysteme ab Windows Vista und die Server-Betriebssysteme ab Windows Server 2003.
- Für die erste Aktivierung der Systeme im LAN kommunizieren diese mit dem KMS über das LAN der Institution. Die Aktivierung erfolgt für einen Client erst, wenn beim KMS innerhalb von 30 Tagen von mindestens 25 Systemen eine Aktivierung angefordert wurde (''Aktivierungsschwellwert''). Für Server erfolgt die Aktivierung bereits ab fünf anfordernden Systemen. Virtuelle Systeme können ebenfalls über den KMS aktiviert werden, zählen beim Aktivierungsschwellwert aber nicht mit.
- Die Systeme müssen spätestens nach 210 Tagen (180 Tage Frist plus 30 Tage Kulanzfrist) oder nach einer Hardware-Änderung erneut aktiviert werden. Hierzu müssen die Systeme eine Verbindung über das LAN der Institution mit dem KMS aufnehmen. Auch zu diesem Zeitpunkt muss der "Aktivierungsschwellwert" erfüllt sein.

- Der KMS-Host verbindet sich alle 180 Tage zu Microsoft, um die Gültigkeit der Lizenz zu überprüfen.

Hinweise

- Die Aktivierungsformen können je nach Anforderung und Eigenschaften des Netzes beliebig kombiniert werden.
- Zur Installation von Windows-Systemen aus einem Volumenlizenzvertrag werden keine Lizenzinformationen benötigt, sondern erst zur späteren Aktivierung innerhalb eines Kulanzzeitraums von 30 Tagen.
- Zur MAK-Aktivierung (Fall 2 und 3) werden administrative Rechte benötigt. Optional kann über einen Registry-Schlüssel die Aktivierung auch für Standardbenutzer ermöglicht werden.
- Unter Windows Server 2012 und Windows wird zunächst versucht, die Aktivierung mittels ADBA durchzuführen, und falls dies nicht gelingt, wird auf die Aktivierung mittels KMS ausgewichen. Die Aktivierung mittels MAK ist ebenfalls möglich.
- Werden noch andere Windows-Versionen neben Windows 8 eingesetzt, sollte auch noch ein KMS-Host bereitgestellt werden.
- Zur Aktivierung von Windows 8 und Windows Server 2012 mittels Key Management Service benötigt der KMS-Server ein Update, da Version 6 des KMS-Protokolls verwendet wird.

Das Tool VAMT bietet die Möglichkeit der Verwaltung des Aktivierungsprozesses für Volumen- und Einzelhandelsversionen von Windows und Office mittels der Aktivierungsmethoden MAK und KMS.

Prüffragen:

- Ist die geeignete Aktivierungsform gewählt worden?
- Sind die technischen Voraussetzungen für die Aktivierung erfüllt?

# M 4.337 Einsatz von BitLocker Drive Encryption

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, IT-Sicherheitsbeauftragter, Leiter IT

Die Laufwerksverschlüsselung BitLocker (engl. BitLocker Drive Encryption, BDE) bietet die Verschlüsselung von kompletten Laufwerken. Zusätzlich können bei vorhandenem TPM (Trusted Platform Module) der Systemzustand erfasst und eine Entschlüsselung der Festplatte bei fehlerhaftem Messwert verweigert werden.

BitLocker ist serverseitig ab Windows Server 2008 und clientseitig ab Windows Vista (ausschließlich in den Betriebssystemversionen Enterprise und Ultimate) enthalten. Unter Windows 8 ist BitLocker in den Versionen Pro und Enterprise verfügbar. Ab Windows 7 wurde ebenfalls noch BitLocker To Go hinzugefügt, mit dem externe portable Datenträger verschlüsselt werden, sodass auch der Zugriff auf verschlüsselte Daten von einem anderen Windows-System erfolgen kann.

Das primäre Sicherheitsziel von BitLocker ist die Vertraulichkeit der Daten bei ausgeschaltetem System. Während des Startvorgangs von Windows lädt BitLocker die Schlüssel für die verschlüsselten Festplattenpartitionen und hält sie für die gesamte Dauer, in der der Client eingeschaltet ist, vor. Im laufenden Betrieb bietet BitLocker daher keinen Schutz der Vertraulichkeit.

BDE kann eingesetzt werden, um die Vertraulichkeit der Daten eines Windows-Clients zu schützen. Dies gilt insbesondere für mobile Clients, die dem Risiko von Verlust und Diebstahl ausgesetzt sind, und wenn deren Hardware keine vergleichbare Laufwerksverschlüsselung und Authentisierung anbietet. Der Schutzbedarf hinsichtlich der Vertraulichkeit und Verfügbarkeit des kryptographischen Schlüsselmaterials ist mindestens so hoch einzustufen wie der Schutzbedarf der verschlüsselten Daten selbst. Für den Einsatz von BitLocker auf mehreren Systemen muss daher vorab das Schlüsselmanagement geplant werden, was bei BitLocker zum Beispiel mittels Active Directory realisiert werden kann.

Für den Einsatz von BitLocker auf mehreren Systemen sollte auch B 1.7 *Kryptokonzept* angewendet werden.

### Vorbereitung des Einsatzes von BitLocker

Ist auf der Plattform ein Trusted Platform Module (TPM) vorhanden, so kann BitLocker dieses nutzen. Das TPM ist ein manipulationsgeschützter Hardware-Baustein auf der Hauptplatine des Systems, der dem Benutzer geschützte Funktionalitäten und einen isolierten Speicher bereitstellt. BitLocker nutzt das TPM zur Aufbewahrung kryptographischer Schlüssel und um die Systemintegrität während des Bootprozesses zu bestimmen. Ein TPM ist für BitLocker nicht zwingend erforderlich, in diesem Fall wird ein USB-Speichermedium als Schlüsselspeicher genutzt. Der zusätzliche Integritätsschutz ist in dieser Konfiguration nicht gegeben.

Die BitLocker-Laufwerksverschlüsselung verschlüsselt Partitionen auf Datenträgern. Die Begriffe Volume und Partition werden von Microsoft synonym verwendet.

Für BitLocker müssen mindestens zwei Partitionen eingerichtet werden:

- Eine Partition für das Betriebssystem (in der Regel Laufwerk *C:*). Diese muss mit dem NTFS-Dateisystem formatiert sein. BitLocker verschlüsselt die Betriebssystem-Partition vollständig mit Ausnahme des Bootsektors und eines Bereichs mit BitLocker-Metadaten.
- Eine Partition, die unverschlüsselt bleiben muss, damit Windows gestartet werden kann. Die Start-Partition (Systempartition) muss mit dem NTFS-Dateisystem formatiert sein. Ab Windows 7 wird sie standardmäßig bei der Installation angelegt. Die Start-Partition muss unter Vista mindestens 1,5 GB groß sein, ab Windows 7 und Server 2008 mindestens 100 MB. Für Computer, die systemseitig mit UEFI starten, sind mindestens eine 350 MB umfassende FAT32-Partition für das Systemlaufwerk und eine NTFS-Partition für das Betriebssystemlaufwerk erforderlich.

Wenn ein Windows-System noch keine separate Start-Partition besitzt, wird sie ab Windows 7 automatisch bei der Installation oder bei der Aktivierung von BitLocker erstellt. Unter Vista muss sie manuell mit dem Bitlocker-Laufwerkvorbereitungstool erstellt werden (unter *Start* | *Alle Programme* | *Zubehör* | *Systemprogramme* | *BitLocker*). Die Aktivierung von BitLocker und der im Hintergrund ablaufende Verschlüsselungsvorgang können zu Unverträglichkeiten mit bereits installierter Software führen. Um dies rechtzeitig zu erkennen, ist BitLocker nach der Installation von Windows und vor der Installation weiterer Software zu aktivieren. Wird die Start-Partition erst später erstellt, sollte vorher ein Backup des aktuellen Gesamtsystems angelegt werden.

Die Aktivierung von BitLocker kann mit Hilfe der BitLocker-Kommandozeilen-Tools automatisiert werden. Die Automatisierungsskripte dürfen dafür keine Wiederherstellungskennwörter enthalten. Stattdessen sollte vorab das zentrale Schlüsselmanagement für BitLocker geplant und aktiviert werden, was sich beispielsweise über Active Directory realisieren lässt.

Es sollte überlegt werden, den Schreibzugriff durch die Standardbenutzer auf die unverschlüsselte Startpartition zu unterbinden. Dies lässt sich durch die entsprechenden NTFS-Berechtigungen erreichen. Dadurch werden die Systemintegrität und die Sicherheit des Startvorgangs erhöht. Für Standardbenutzer wird verhindert, dass sie irrtümlich die Vertraulichkeit ihrer Daten durch die BDE geschützt glauben, obwohl sie ihre Daten versehentlich in die unverschlüsselte Startpartition geschrieben haben.

Weitere Partitionen, wie eine Datenpartition, sollten insbesondere bei einem höheren Schutzbedarf ebenfalls verschlüsselt werden, sofern nicht die Unverträglichkeit mit bestimmten Anwendungen dagegen spricht. Es sollten ausschließlich NTFS-Partitionen verwendet werden. BitLocker unter Windows Vista ohne Service Pack 1 unterstützt nur die Verschlüsselung der Betriebssystempartition.

Ab Windows 8 und Windows Server 2012 kann bei der Aktivierung von BitLocker angegeben werden, ob das gesamte Laufwerk oder nur der verwendete Speicherplatz auf dem Laufwerk verschlüsselt werden soll. Die Dauer für die Verschlüsselung des nur belegten Speicherplatzes nimmt deutlich weniger Zeit in Anspruch als eine Komplettverschlüsselung, gibt dafür aber Informationen über den belegten Speicherplatz preis. Sobald Daten gespeichert werden, verschlüsselt BitLocker diese automatisch und stellt sicher, dass keine Daten unverschlüsselt bleiben. Unter Windows 8 und Windows 2012 kann bereits vor der Installation von Windows festgelegt werden, ob die Festplatte mittels BitLocker verschlüsselt werden soll, wodurch die zu formatierende Partition schon vor der Installation verschlüsselt werden kann.

**Planen der Gruppenrichtlinien**

Wenn BitLocker auf mehreren Systemen eingesetzt wird, sollten ab Windows Vista mit Service Pack 1 Gruppenrichtlinien verwendet werden, um die Verschlüsselungseinstellungen zu steuern und deren Einhaltung sicherzustellen. Falls das zentrale Schlüsselmanagement mittels Active Directory verwendet wird, ist die Planung der Gruppenrichtlinien zwingend erforderlich.

In den folgenden Abschnitten werden die wichtigsten Einstellungen der Windows-Gruppenrichtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *BitLocker Laufwerksverschlüsselung* beschrieben.

**Auswahl einer sicheren Authentisierungsmethode für den Systemstart**

Für den erfolgreichen Start von BitLocker während des Startvorgangs von Windows kann der Administrator unterschiedliche Verfahren sowie Kombinationen daraus zur Authentisierung konfigurieren.

- TPM-Nutzung ohne Benutzer-Authentisierung (setzt ein Trusted Platform Modul [TPM] voraus): BitLocker startet ohne Interaktion durch den Benutzer.
- Authentisierung mittels eines Schlüssels auf einem USB-Stick
  Diese Variante ist sowohl mit als auch ohne TPM Client möglich. Ohne TPM wird das zur Entschlüsselung notwendige BitLocker-Schlüsselmaterial gemeinsam mit einem Authentisierungsschlüssel auf dem USB-Stick gespeichert. Mit TPM wird dieses Schlüsselmaterial auf das TPM und den USB-Stick verteilt.
- Authentisierung mittels PIN, also "Wissen"
  Dies setzt ein TPM auf dem Windows-System voraus. Das TPM prüft die eingegebene PIN.
- Multifaktorauthentisierung mittels USB-Stick und PIN
  Dies setzt ein TPM auf dem Windows-System voraus. Das TPM dient als Speicher eines Teils des Schlüsselmaterials und zur Prüfung der PIN.

Es muss eine geeignete Form der Authentisierung des Benutzers gegenüber BitLocker gewählt werden. Hierbei sind folgende Gesichtspunkte zu berücksichtigen und gegeneinander abzuwägen:

- "TPM-Nutzung ohne Benutzer-Authentisierung" kann geeignet sein, wenn die Benutzer neben der lokalen Anmeldung am Client oder an der Domäne keine weitere Anmeldung und die damit verbundenen Authentisierungsmittel wie PIN und/oder USB-Stick akzeptieren würden. Da dies den geringsten Schutz bietet, sollte diese Einstellung nur im Ausnahmefall verwendet werden.
- "TPM-Nutzung ohne Benutzer-Authentisierung" begünstigt bekannte Angriffsvektoren, bei denen Unbefugte Zugang zum Schlüsselmaterial erlangen, wenn sie physischen Zugang zum System haben, Bei "Keine Authentisierung" wird während des Boot-Vorgangs automatisch das BitLocker-Schlüsselmaterial aus dem TPM in den Arbeitsspeicher (RAM, Random Access Memory) des Systems geladen. Dies geschieht vor der Anmeldung eines Benutzers. Allerdings erfordern diese Angriffsvektoren spezielle Werkzeuge und eine hohe Qualifikation seitens des Angreifers. Gegen diese Angriffsvektoren wird der Einsatz der Authentisierungsmittel PIN und/oder USB-Stick empfohlen.
- Das Authentisierungsmittel PIN ist im Gegensatz zur Authentisierung mit einem USB-Stick durch mögliche Keylogger gefährdet. Keylogger gibt es als Software- und als Hardware-Ausführung. Keylogger zeichnen unbemerkt die Tastatureingaben eines Benutzers auf, so dass diese von unbefugten Dritten missbraucht werden können. Ein Software-basierter Key-

logger müsste die Sicherheitsmechanismen von Windows zum Schutz der Systemintegrität überwinden. Eine weitere PIN-spezifische Gefährdung liegt vor, wenn zur PIN-Eingabe eine drahtlose Tastatur eingesetzt wird. Deren Übertragung kann abgehört werden. Die PIN-Eingabe sollte daher nicht über eine drahtlose Tastatur erfolgen, wenn keine oder nur eine schwache Verschlüsselung für die drahtlose Datenübertragung eingesetzt wird.
- Das Authentisierungsmittel USB-Stick empfiehlt sich nicht in Verbindung mit einem mobilen Client, da ein USB-Stick häufig direkt mit diesem (etwa in der Laptop-Tasche) aufbewahrt wird.
- Das Authentisierungsmittel USB-Stick *und* PIN empfiehlt sich bei erhöhten Sicherheitsanforderungen. Diese Form der Multi-Faktor-Authentisierung ist erst ab Windows Vista Service Pack 1 und Server 2008 (nur mittels Kommandozeile zu konfigurieren) sowie unter Windows 7 und Server 2008 R2 (mittels Gruppenrichtlinie) möglich.

Alle vier vorgestellten Authentisierungsformen können auch im Pool-Betrieb eingesetzt werden, wenn ein mobiler Client mehreren Benutzern zur Verfügung steht. Alle Benutzer müssen dann über dieselbe PIN und/oder über dasselbe Schlüsselmaterial auf einem USB-Stick verfügen. Alternativ kann in Verbindung mit einem TPM ein individueller Authentisierungsschlüssel auf jedem USB-Stick verwendet werden (nur mittels Kommandozeile möglich).

Ab Windows 7 sollte die Gruppenrichtlinie für komplexe PINs aktiviert werden (*Betriebssystemlaufwerke* | *Erweiterte Systemstart-PINs*). Bestimmte Hardware- und Boot-Konfigurationen, zum Beispiel ältere PXE-Boot-Umgebungen, unterstützen dies nicht und sollten nicht verwendet werden.

Unter Windows 8 wurde die Möglichkeit eingeführt, dass Standardbenutzer ihre BitLocker-PIN oder das Kennwort für das Betriebssystemvolume oder das BitLocker-Kennwort für feste Datenpartitionen selbst ändern können. Das heißt, Benutzer können ihre PINs und Kennwörter entsprechend einer eigenen Gedächtnishilfe festlegen, anstatt sich einen zufällig generierten Zeichensatz merken zu müssen. Hierdurch wird die Verwendung derselben initialen PIN- bzw. Kennworteinstellungen für alle Computerimages ermöglicht.

Die Einstellung *Standardbenutzern das Ändern von PINs nicht gestatten* kann unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *BitLocker-Laufwerkverschlüsselung* | *Betriebssystemlaufwerke* des Editors für lokale Gruppenrichtlinien deaktiviert werden.

Seit Windows Server 2013 wird für Betriebssystempartitionen die Netzentsperrung unterstützt. Sie ermöglicht, dass Clients und Server mit aktiver BitLocker-Verschlüsselung in einer Domänenumgebung automatisch entsperrt werden, wenn eine Verbindung zu einem vertrauenswürdigen kabelgebundenen Unternehmensnetz besteht. Diese Funktion erfordert allerdings eine UEFI-Firmware mit DHCP-Treibern.

**Wiederherstellung verschlüsselter Windows-Systeme im Notfall**

Wiederherstellungskennwörter und -schlüssel ermöglichen einem Administrator das Wiederherstellen verschlüsselter Daten, falls das TPM defekt ist oder der Benutzer die Start-PIN oder den USB-Stick verloren hat. Weiterhin ermöglichen sie die Fortführung des Startvorgangs von Windows, falls BitLocker eine Manipulation am BIOS oder anderen von BitLocker geschützten Boot-Komponenten festgestellt hat. Für den Start des abgesicherten Modus von Windows, zum Beispiel zur Wartung oder Fehlerbehebung, wird ebenfalls das Wieder-

herstellungskennwort beziehungsweise der Wiederherstellungsschlüssel benötigt.

Der Administrator muss beim Verschlüsseln von Festplattenpartitionen ein 48-stelliges Wiederherstellungskennwort setzen. Hierfür wird standardmäßig ein Zufallskennwort erzeugt. Es sollte übernommen und kann ausgedruckt oder als Textdatei gespeichert werden. Gemäß M 2.22 *Hinterlegen des Passwortes* sollte genau dokumentiert werden, wie das Wiederherstellungskennwort abgelegt wird. Es muss genauso vertraulich und sorgsam behandelt werden wie die Start-PIN, der USB-Stick oder die Smartcard. Zusätzlich kann in einer Domänenumgebung per Gruppenrichtlinie festgelegt werden, dass für alle durch BitLocker geschützten Laufwerke die Wiederherstellungskennwörter generiert und diese in Active-Directory-Domänendiensten gespeichert werden.

Es muss gemäß M 4.86 *Sichere Rollenteilung und Konfiguration der Kryptomodule* geregelt werden, ob und wie Wiederherstellungskennwörter und -schlüssel zentral abgelegt werden sollen und wer zwecks Wiederherstellung darauf zugreifen darf. Um die Vertraulichkeit dieser Informationen besser zu schützen und die Wiederherstellung im Notfall zu beschleunigen, ist es empfehlenswert, dass diese Informationen unabhängig vom Benutzereingriff automatisch im Active Directory hinterlegt werden, und dass ansonsten das System die BitLocker-Aktivierung verweigert (Gruppenrichtlinie *Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können*). Bei dezentralem Schlüsselmanagement sollte überlegt werden, Sicherheitskopien des Wiederherstellungskennworts und -schlüssels zu erstellen und an einer geeigneten Stelle separat aufzubewahren. In jedem Fall sollten die Schritte, Personen und Ressourcen genau dokumentiert werden, die zur Wiederherstellung benötigt werden (gemäß den Vorgaben von B 1.7 *Kryptokonzept*).

Wenn das Wiederherstellungskennwort manuell gewählt oder nachträglich geändert wird, müssen triviale Formen vermieden werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Besteht der Verdacht, dass PIN, USB-Stick, Wiederherstellungskennwort oder Wiederherstellungsschlüssel kompromittiert wurden, muss der entsprechende Schlüssel neu gesetzt werden. Dies kann mit dem Kommandozeilenwerkzeug *manage-bde.wsf* (Vista, Server 2008) oder *manage-bde.exe* (ab Windows 7, Server 2008 R2) in Verbindung mit dem Wiederherstellungskennwort oder dem Wiederherstellungsschlüssel erfolgen. Auf diese Weise können auch verlorene oder defekte USB-Sticks und/oder PINs gesperrt und neu angelegt werden.

Weiterhin kann mittels Gruppenrichtlinie festgelegt werden, dass für jeden verschlüsselten Datenträger ein 256-Bit-Wiederherstellungsschlüssel erzeugt wird. Auf diese Weise kann auf den Datenträger zugegriffen werden, wenn die ursprünglichen Authentisierungsmittel nicht mehr zur Verfügung stehen. Der Wiederherstellungsschlüssel ist nicht druckbar und kann nicht mündlich, zum Beispiel am Telefon, weitergegeben werden. Dies erhöht den Schutz der Vertraulichkeit der Daten, verzögert andererseits aber im Notfall die Datenwiederherstellung. Diese Wiederherstellungsschlüssel können nur auf USB-Sticks, als Dateien oder im Active Directory gespeichert werden. Auf Systemen, mit denen Daten mit sehr hoher Vertraulichkeitsanforderung verarbeitet werden, sollten nur Wiederherstellungsschlüssel, aber keine -kennwörter zugelassen werden.

Zusätzlich kann ab Windows 7 und Server 2008 R2 vom Administrator ein Datenwiederherstellungsagent installiert werden (*Gruppenrichtlinien-Snap-in*

| *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für öffentliche Schlüssel* | *BitLocker*). Das ist der öffentliche Teil eines universellen Wiederherstellungsschlüssels, er wird einheitlich auf allen BitLocker-Clients installiert. Der dazu passende private Schlüssel kann die verschlüsselten Datenträger entschlüsseln. Er sollte nicht im Besitz des Administrators sein. Datenwiederherstellungsagenten erfordern prinzipiell einen besonders hohen Schutz gegen Missbrauch. Ihr Austausch ist im Falle einer Kompromittierung sehr aufwendig. Sie sind daher kein Ersatz für Wiederherstellungskennwörter oder -schlüssel, sondern nur ein zusätzlicher Schutz vor Datenverlust für Benutzer, die nicht am zentralen Schlüsselmanagement teilnehmen.

**Vernichtung des Schlüsselmaterials**

Sobald ein verschlüsselter Datenträger ausgesondert wird oder verloren gegangen ist, müssen alle Schlüssel und Kennwörter in Verbindung mit diesem Datenträger unverzüglich vernichtet werden. Bei zentral gespeicherten Schlüsseln sollte über die Vernichtung ein revisionssicheres Protokoll geführt werden, sofern die verschlüsselten Daten einen höheren Schutzbedarf bezüglich der Vertraulichkeit aufweisen.

**Überwachen des BitLocker-Wartungsmodus**

Die BitLocker-Verschlüsselung muss für Wartungszwecke, beispielsweise für ein BIOS-Update, vom Administrator vorübergehend deaktiviert werden. In diesem Wartungsmodus kann das interne BitLocker-Schlüsselmaterial leicht von Angreifern und Schadprogrammen ausgespäht werden. Daher sollte die System-Ereignisanzeige lückenlos auf Meldungen von *BitLocker-Driver* hin überwacht werden. Falls unerwartete oder sehr lange Wartungsphasen oder unerwartete Ver-/Entschlüsselungsereignisse protokolliert wurden, oder die Ereignisanzeige lückenhaft ist, dann sollte dies dem IT-Sicherheitsbeauftragten gemeldet werden. Handelt es sich um einen Sicherheitsvorfall, dann muss der betroffene Client vollständig neu verschlüsselt werden. Das Ändern der Schlüssel und Wiederherstellungskennwörter alleine genügt in einem solchen Fall nicht (siehe G 3.97 *Vertraulichkeitsverletzung trotz BitLocker-Laufwerksverschlüsselung ab Windows Vista*).

**Schulung der Benutzer**

Die Benutzer müssen grundsätzlich im Umgang mit BitLocker geschult und darüber informiert werden, welche Festplattenpartitionen durch BitLocker verschlüsselt werden und welche nicht.

Weiterhin müssen Benutzer darin unterrichtet werden, welche Schritte oder Ansprechpartner bei Verlust der Start-PIN, des USB-Schlüssels oder der Smartcard für sie gelten.

**BitLocker in Verbindung mit Energiesparmodi**

Die Benutzer müssen darüber informiert werden, wie sie mit den möglichen Energiesparmodi unter dem Gesichtspunkt der Wirksamkeit der BitLocker-Verschlüsselung umgehen sollten.

Ein Windows-Client, der aktuell nicht benutzt wird und auch nicht ausgeschaltet ist, kann sich im Energiesparmodus befinden. Bei Windows-Systemen gibt es die Energiesparmodi *Standby-Modus* (ab Windows 7 "Energie sparen" genannt), *Ruhezustand* (auch Hibernate-Modus genannt) und *Hybrider Energiesparmodus*.

Der Standby-Modus ist ein typisches Merkmal von mobilen Clients, um Energie zu sparen. Im Standby-Modus verbleibt das BitLocker-Schlüsselmaterial im Arbeitsspeicher (RAM) des Windows-Clients. Dadurch ist die Vertraulichkeit der BitLocker-verschlüsselten Daten durch den *Angriffsvektor gegen BitLocker-Schlüssel im RAM* gefährdet (siehe Abschnitt oben). Gegen diesen Angriffsvektor wird empfohlen, einen Windows-Client nicht unbeaufsichtigt im Standby-Modus zu belassen. Alternativen sind der Ruhezustand und das vollständige Ausschalten des Systems.

Der Ruhezustand ist durch den geschilderten *Angriffsvektor gegen BitLocker-Schlüssel im RAM* nicht gefährdet, sofern für die BitLocker-Authentisierung nicht ausschließlich das TPM genutzt wird. Der Grund dafür ist, dass das Schlüsselmaterial nicht im Arbeitsspeicher verbleibt, sondern verschlüsselt auf die Festplatte geschrieben und nach dem "Aufwachen" erst nach einer erfolgreichen Benutzerauthentisierung wieder in den Arbeitsspeicher geladen wird.

Der hybride Energiesparmodus ist eine Neuerung ab Windows Vista. Dieser Modus kombiniert den Standby-Modus mit dem Ruhezustand. Analog dem Standby-Modus ist der hybride Energiesparmodus durch den *Angriffsvektor gegen BitLocker-Schlüssel im RAM* gefährdet. Der hybride Energiesparmodus sollte deshalb nicht eingesetzt werden, wenn hohe Anforderungen an den Schutz der Vertraulichkeit durch BitLocker gestellt werden und der Windows-Client zumindest zeitweise unbeaufsichtigt ist.

Bei Verwendung von Standby-Modus, Ruhezustand oder dem hybriden Energiesparmodus sollte das IT-System nur nach erneuter Kennworteingabe entsperrt werden können. Diese Empfehlung gilt unabhängig von BitLocker. Hierzu ist im entsprechenden Gruppenrichtlinienobjekt unter *Benutzerkonfiguration* | *Administrative Vorlagen* | *System* | *Energieverwaltung* die Richtlinie *Kennworteingabe bei der Wiederaufnahme aus dem Ruhezustand bzw. Energiesparmodus* zu aktivieren.

**BitLocker für sehr hohe Sicherheitsanforderungen**

Es sollte die Gruppenrichtlinie *Schreibzugriff auf Festplattenlaufwerke verweigern, die nicht durch BitLocker geschützt sind* gesetzt werden (unter *BitLocker Laufwerksverschlüsselung* | *Festplattenlaufwerke*). Dies verhindert grundsätzlich, dass auf nachträglich erstellte Datenpartitionen und auf jede zusätzlich eingehängte interne Festplatte geschrieben werden kann. Alle regulären Datenpartitionen müssen dann jedoch verschlüsselt werden.

Unter Windows 8 besteht zusätzlich noch die Möglichkeit, den Schreibzugriff auf Wechseldatenträger zu verweigern, sofern diese nicht durch BitLocker geschützt sind. Die Einstellung *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind* ist unter der Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *BitLocker-Laufwerkverschlüsselung* | *Wechseldatenträger* zu finden.

Die Verschlüsselungsstärke kann von 128-Bit AES Diffuser auf 256-Bit AES Diffuser erhöht werden (Gruppenrichtlinie *Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen*). Der Verschlüsselungsvorgang erzeugt dadurch erheblich höhere CPU-Last und sollte vor allem auf schwächeren Notebooks vor dem Produktiveinsatz erst getestet werden.

In der Gruppenrichtlinie *TPM-Plattformvalidierungsprofil konfigurieren* können zusätzliche Hardware-Integritätsprüfungen aktiviert werden, um den Schutz gegen Manipulation und Rootkits zu erhöhen. Diese Einstellungen erhöhen

allerdings erheblich die in *Verlust von BitLocker-verschlüsselten Daten* beschriebenen Gefahren.

Das Verschlüsseln virtueller Datenträger mit BitLocker To Go auf Festplatten, die bereits mit BitLocker verschlüsselt sind (doppelte Verschlüsselung), ist grundsätzlich möglich, aber nutzlos, da immer derselbe Verschlüsselungsalgorithmus eingesetzt wird und somit kein höherer Schutz gegen Entschlüsselungssoftware erreicht wird. Gleichzeitig steigt die Komplexität und Fehleranfälligkeit des Schlüsselmanagements und die Systemgeschwindigkeit wird reduziert. Daher sollte die doppelte Verschlüsselung mit BitLocker vermieden werden.

**BitLocker-Werkzeuge**

Microsoft stellt Werkzeuge zur Verfügung, um BitLocker vorbereiten, konfigurieren und administrieren zu können:

- Das *TCG BIOS DOS Test Tool* (*tcgbios.exe*) dient der Prüfung einer BIOS-Funktion, die BitLocker benötigt (siehe Microsoft Developer Network - MSDN).
- Nur Windows Vista: BitLocker benötigt eine separate Startpartition, die nachträglich mit dem *BitLocker-Laufwerkvorbereitungstool (Drive Preparation Tool)* erstellt werden kann (siehe Knowledge-Base-Artikel 930063).
- Die Kommandozeilentools *manage-bde.wsf* (Vista/Server 2008) und *manage-bde.exe* (ab Windows 7 / Server 2008 R2) dienen der Verwaltung von BitLocker. Ein TPM ist nicht notwendig.
- Nur Windows Vista: Die graphische Bedienoberfläche *BitLocker Control Panel GUI* dient der Verwaltung von BitLocker. Voraussetzung hierfür ist ein TPM.
- Ab Windows 7 / Server 2008 R2 steht eine graphische Verwaltung der verschlüsselten Datenträger und des TPM unter *Systemsteuerung* | *BitLocker-Laufwerksverschlüsselung* zur Verfügung.
- Der *Recovery Password Viewer* dient zur Verwaltung von Wiederherstellungsschlüsseln im Active Directory (siehe Knowledge-Base-Artikel 928202 bzw. 958830).
- Das Kommandozeilentool *repair-bde.exe* dient der Sicherung von Daten aus beschädigten Volumes, die durch BitLocker verschlüsselt worden sind (für Vista ist das Tool unter dem Knowledge-Base-Artikel 928201 erhältlich).

**Abgrenzung der Einsatzbereiche von BitLocker**

Soll neben Windows ab der Version Vista ein anderes Betriebssystem gestartet werden können (Multiboot-System), dann empfiehlt sich der Einsatz eines Programms zur Festplattenverschlüsselung, das Betriebssystempartitionen für jedes Betriebssystem einzeln und unabhängig voneinander entschlüsseln kann. BDE ist für Multiboot-Systeme in der Praxis ungeeignet.

Alternativ zu BitLocker kann auch EFS (Encrypting File System - verschlüsselndes Dateisystem) eingesetzt werden, das statt Partitionen einzelne Dateien verschlüsselt (siehe M 4.147 *Sichere Nutzung von EFS unter Windows*).

Der Einsatz des EFS empfiehlt sich auch, wenn die zu schützenden Daten auf einem mobilen Client auch dann verschlüsselt vorliegen sollen, wenn der mobile Client unter Windows eingeschaltet ist. Im eingeschalteten Zustand bietet die BitLocker-Verschlüsselung keinen wirksamen Schutz der Vertraulichkeit.

Um diese Konfiguration auch ohne den Einsatz von EFS zu realisieren, können virtuelle Laufwerke ab Windows 7 und Windows Server 2008 R2 mit Bit-

Locker To Go verschlüsselt werden. Virtuelle Laufwerke sind Abbilddateien von Datenträgern und können im laufenden Betrieb eingebunden und wieder getrennt werden. Nutzer ohne administrative Berechtigungen können mit Software von Drittanbietern virtuelle Laufwerke im regulären Betrieb erstellen und, vergleichbar mit USB-Sticks, temporär einbinden.

**Weiterführende Informationen zu BitLocker**

Die Herstellerdokumentation befindet sich in Microsoft Technet unter dem Titel *Schrittweise Anleitung zur BitLocker-Laufwerkverschlüsselung*. Weiterführende Informationen zu BitLocker sind im Anwenderleitfaden "BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz" auf den Webseiten des BSI zu finden. Der Leitfaden ist das Ergebnis einer gemeinsamen Sicherheitsanalyse des BSI und des Fraunhofer-Instituts für sichere Informationstechnologie unter Einbeziehung der für die Entwicklung von BDE verantwortlichen Produktgruppe von Microsoft.

Prüffragen:

- Ist eine geeignete Form der Authentisierung des Benutzers gegenüber BitLocker beim Systemstart ausgewählt worden?
- Ist sichergestellt, dass Wiederherstellungskennwort und -schlüssel von BitLocker vertraulich und sorgsam behandelt werden?
- Kann auf Wiederherstellungskennwörter und -schlüssel von BitLocker im Bedarfsfall schnell zugegriffen werden?
- Ist den Benutzern bekannt, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben?
- Ist ein Schreibzugriff der Standardbenutzer auf die Startpartition unterbunden?
- Wird nach der Rückkehr aus dem Standby-Modus, dem Ruhezustand oder dem hybriden Energiesparmodus ein Kennwort vom Benutzer verlangt?
- Enthält das Bereitstellungskonzept für Windows die Vorbereitung des BitLocker-Einsatzes?
- Werden alle Schlüssel und Kennwörter vernichtet, wenn Datenträger verloren gehen oder ausgesondert werden?

# M 4.338 Einsatz von File und Registry Virtualization bei Clients ab Windows Vista

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Windows-Altanwendungen, kurz Altanwendungen (legacy applications), bezeichnet Anwendungen, die ursprünglich für ältere Windows-Versionen entwickelt wurden, nun aber auch unter einer aktuellen Windows-Version, wie Windows Vista, Windows 7 und Windows 8, betrieben werden sollen. Häufig zeichnen sich Altanwendungen, die für Standardbenutzer entwickelt worden sind, durch eine bestimmte Sicherheitsschwäche aus: Altanwendungen erfordern Schreibrechte in kritische Datei-Ordner oder Registry-Schlüssel. Zu kritischen Datei-Ordnern gehören beispielsweise die Ordner *%ProgramFiles%* (in einer Standardinstallation *C:\Programme*) oder *%SystemRoot%* (in einer Standardinstallation). Ein kritischer Registry-Bereich ist *HKLM\Software.* Schreiboperationen in diese kritischen Bereiche erfordern administrative Privilegien. In der Folge muss sich der Standardbenutzer mit einem Administratorkonto anmelden, um eine Altanwendung des beschriebenen Typs nutzen zu können. Dies gefährdet die Integrität des Windows-Systems durch mögliche Schadprogramme, die mit den Privilegien des angemeldeten Kontos, hier einem Administratorkonto, laufen.

Windows-Versionen ab Windows Vista nutzen für den sicheren Einsatz von Altanwendungen die Techniken *File Virtualization* und *Registry Virtualization*. Die damit verbundenen Mechanismen erlauben den Betrieb der Altanwendung unter dem Konto eines Standardbenutzers, das heißt ohne administrative Privilegien. Dadurch wird die beschriebene Gefährdung der Integrität des eigentlichen, nicht "virtualisierten" Windows-Systems unterbunden. Bei *File Virtualization* und *Registry Virtualization* leiten Windows-Versionen ab Windows Vista alle Schreibzugriffe und im Bedarfsfall auch Lesezugriffe einer Anwendung um, die als Ziel kritische Verzeichnis- oder Registry-Bereiche haben, zu denen die Anwendung nicht berechtigt ist. Diese Umleitung erfolgt in spezielle Bereiche, die nur für den angemeldeten Benutzer gelten. Für Operationen in Verzeichnisse erfolgt der umgeleitete Zugriff auf den Bereich *%UserProfile%\AppData\Local\VirtualStore,* für Operationen in Registry-Bereiche erfolgt die Umleitung nach *HKEY_CURRENT_USER\Software\Classes\VirtualStore.* Die Schädigung der Integrität dieser Bereiche gefährdet nicht die Integrität des eigentlichen Windows-Systems, die Integrität des für den betreffenden Benutzer sichtbaren, "virtualisierten" Systems bleibt jedoch ungeschützt.

Grundsätzlich sollten Altanwendungen für Standardbenutzer, die vor Windows Vista nur mit administrativen Privilegien liefen, nicht eingesetzt werden. Möglicherweise ist der Betrieb einer solchen Altanwendung aber für die Erledigung einer Aufgabenstellung in einem Fachverfahren oder einem Geschäftsprozess unerlässlich. In solchen Einzelfällen kann der Betrieb der Altanwendung nach einer Abwägung der Sicherheitsrisiken ab Windows Vista erwogen werden.

In den Windows-Client-Versionen ab Windows Vista beinhaltet das Kommandozeilenwerkzeug *reg.exe* eine Erweiterung um den Befehl *FLAGS*. Mit diesem kann ein Administrator für Registry-Schlüssel unterhalb von *\HKLM\Software* steuern, ob eine *Registry Virtualization* unterstützt werden soll oder nicht.

Es sollte kritisch geprüft werden, ob der Betrieb von Altanwendungen des beschriebenen Typs notwendig ist. Es empfiehlt sich, die Menge der Registry-Schlüssel, die eine *Registry Virtualization* unterstützen sollen, im Hinblick auf die Erfordernisse der Altanwendungen zu minimieren.

Langfristig muss in Betracht gezogen werden, die Altanwendungen des beschriebenen Gefährdungstyps durch sichere Anwendungen zu ersetzen. Sichere Anwendungen erfordern als Anwendung für Standardbenutzer keine Schreiboperationen in kritische Verzeichnis- und/oder Registry-Bereiche. Der Umstieg auf sichere Anwendungen empfiehlt sich auch deshalb, weil Microsoft selbst die Techniken der *File Virtualization* und *Registry Virtualization* nur als Übergangslösungen für bisher unsichere Altanwendungen betrachtet. Eine Einschränkung der File und Registry Virtualization ist, dass sie keine 64-Bit-Anwendungen unterstützt und auch nicht bei der Ausführung einer Anwendung mit Administrationsrechten funktioniert.

Prüffragen:

- Ist die Notwendigkeit des Betriebs von Altanwendungen unter einer Windows-Client-Version ab Windows Vista einer kritischen Prüfung unterzogen worden?
- Ist die Registry Virtualization auf die notwendigen Schlüssel beschränkt?
- Gibt es eine Strategie zum Umstieg auf sichere Anwendungen als Alternative zu Altanwendungen unter Windows-Client-Versionen ab Windows Vista?

# M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows-Clients ab Windows Vista

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Unter Windows können sämtliche Wechseldatenträger (zum Beispiel: CD, DVD, USB-Stick, SD Karte, etc.) automatisch erkannt und bearbeitet werden. Als Folge lassen sich auf dem Datenträger gespeicherte Programme automatisch auf dem Windows-System ausführen. Die automatische Wechselmedien-Erkennung sollte daher permanent unterbunden werden.

Windows-Clients ab Windows Vista stellen Mechanismen bereit, um den Zugriff auf Wechselmedien zu kontrollieren. Beispiele für Wechselmedien sind Speicherkarten, USB-Sticks, mobile Festplatten, Digitalkameras, Disketten, CDs oder DVDs. Sie dienen der mobilen Speicherung von Daten und des Datenaustauschs zwischen IT-Systemen. Daten können von einem Client-System ab Windows Vista aus einem Wechselmedium gelesen und auf ein Wechselmedium gespeichert werden, Applikationen können von Wechselmedien gestartet werden. Zur Nutzung von Wechselmedien zählen auch die Installation oder Aktualisierung notwendiger Treiber.Seit Windows Vista können Vorgaben zur Installation und zur Nutzung von Wechselmedien über Gruppenrichtlinien konfiguriert werden.

**Ermittlung der Vorgaben zur Nutzung von Wechselmedien**

Die Vorgaben zur Nutzung von Wechselmedien müssen ermittelt werden. Hierfür können die fachlichen Aufgaben betrachtet werden, zu deren Erfüllung ausgewählte Benutzer Wechselmedien einsetzen müssen. Daraus lassen sich die zu erlaubenden und/oder die zu unterbindenden Wechselmedien und ihre Nutzungsmöglichkeiten ableiten.

Für Windows-Clients ab Windows Vista bietet Microsoft die Funktionen AutoRun und AutoPlay. AutoRun wird verwendet, um Programme oder erweiterte Inhalte, wie etwa Mediadateien, automatisch zu starten, wenn ein Datenträger eingelegt oder angeschlossen wird. AutoPlay ist eine Funktion mit der festgelegt wird, welches Programm genutzt werden soll, um ein bestimmtes Medium zu starten. So können beispielsweise Audio-CDs direkt mit dem MediaPlayer verknüpft werden. Dieser wird dann nach dem Einlegen einer Audio-CD automatisch gestartet. Es wird dringend empfohlen, die Funktion AutoPlay als auch die Funktion AutoRun zu deaktivieren, da diese unberechtigterweise Schadsoftware, die sich auf einem Wechselmedium befindet, starten könnte.

Zu Vorgaben, deren Durchsetzung überlegt werden sollte, zählen:

- Deaktivierung der AutoRun-Funktion für Wechselmedien
  Zugehöriges Gruppenrichtlinienobjekt:
  *AutoAusführen-Standardverhalten* unter Richtlinie *Computerkonfiguration | Administrative Vorlagen | Windows Komponenten | Richtlinien für die automatische Wiedergabe*
- Deaktivierung der AutoPlay-Funktion für CD- und Wechselmedienlaufwerke
  Zugehöriges Gruppenrichtlinienobjekt:

*AutoPlay deaktivieren* unter Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Windows Komponenten* | *Richtlinien für die automatische Wiedergabe*

- Nutzung von Wechselmedien auf lokale Benutzer beschränken
  Zugehörige Gruppenrichtlinienobjekte:
  *Zugriff auf CD-Laufwerke auf lokal angemeldete Benutzer beschränken* unter Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien / Sicherheitsoptionen* | *Geräte*
  *Alle Wechselmedien: Jeglichen direkten Zugriff in Remotesitzungen verweigern* unter Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Wechselmedienzugriff*

Insbesondere USB-Sticks sind zu berücksichtigen, da diese auch als Authentisierungsmittel beispielsweise gegenüber einer Festplattenverschlüsselung eingesetzt werden können. Entsprechend notwendige Lese- und Schreibzugriffe müssen dann zugelassen werden.

Auf Clients ab Unter Windows Vista kann die automatische Wiedergabe (AutoPlay) auch über *Systemsteuerung* | *Hardware und Sound* | *Automatische Wiedergabe* unterbunden werden. Hier lässt sich auch spezifisches Verhalten je nach Medientyp oder generelles Verhalten bei Wechselmedien einstellen. Es sollte die Einstellung *Automatische Wiedergabe für alle Medien und Geräte verwenden* deaktiviert werden.

**Geräte verbieten oder einschränken**

Standardmäßig installiert Windows sämtliche Geräte, für die Gerätetreiber vorhanden sind. Seit Windows Vista ist über Gruppenrichtlinien steuerbar, welche Geräte installierbar sind oder nicht. Hier kann zwischen speziellen Geräten oder auch ganzen Geräteklassen (z. B. Wechseldatenträger oder Drucker) unterschieden werden, die anhand einer Positivliste freigegeben oder anhand einer Negativliste verboten sind. Für die Identifizierung von Geräteklassen stellt Microsoft eine Liste sämtlicher vorhandener Gerätesetupklassen zur Verfügung. Eine weitere, restriktivere Einschränkung ist die Freigabe eines Gerätes anhand seiner Hardware-ID, die somit nur ein bestimmtes Gerät umfasst. Bei Geräten oder Geräteklassen, die in einer Negativliste aufgeführt sind, wird die Installation unterbunden. Sofern allerdings ein Gerät bereits verwendet worden ist, muss davon ausgegangen werden, dass die benötigten Treiber für das Gerät bereits installiert worden sind. In diesem Fall sind die Treiber für das Gerät zunächst zu deinstallieren.

**Einschränkungen für die Geäteinstallation definieren**

Wenn die folgende Richtlinieneinstellung aktiviert ist, kann ein Gerät, das nicht in den Richtlinieneinstellungen beschrieben ist, nicht installiert und dessen Treiber nicht aktualisiert werden:

*Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind unter Richtlinie Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Geräteinstallation* | *Einschränkungen bei der Geräteinstallation*

Sobald versucht wird, ein neues Gerät zu installieren, wird die Installation abgebrochen. Eine Ausnahme lässt sich für Administratoren durch Aktivieren der folgenden Richtlinie erlauben:

*Administratoren das Außerkraftsetzen der Richtlinien* unter *Einschränkungen bei der Geräteinstallation erlauben*

Dadurch ist die Installation nur mittels administrativer Rechte möglich. Die Treiberinstallationseinschränkungen sind lediglich nur pro Computer und nicht auf Benutzerebene anwendbar.

**Durchsetzung der Nutzungsanforderungen von Wechselmedien**

Die ermittelten Nutzungsanforderungen von Wechselmedien müssen umgesetzt werden. Vorrangig sollte dies auf technischer Ebene über Gruppenrichtlinien erfolgen. Sofern die Nutzung von Wechselmedien für den Datenaustausch im Unternehmen freigegeben ist, sollte die Speicherung von Daten auf diesen verschlüsselt erfolgen.

Als Ausweichmöglichkeit oder Ergänzung bieten sich auch organisatorische Vorgaben an.

Die Konfigurationseinstellungen von Gruppenrichtlinien sollten auf ihre Korrektheit hin getestet werden, bevor sie in den Regelbetrieb übernommen werden.

Die Benutzer müssen über die sie betreffenden Vorgaben zur Nutzung von Wechselmedien informiert werden.

Prüffragen:

- Wurden Vorgaben zur Nutzung von Wechselmedien definiert und umgesetzt?
- Wurde die Korrektheit der technischen Umsetzung getestet?
- Sind die Benutzer über die sie betreffenden Vorgaben zur Nutzung von Wechselmedien informiert?

# M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Benutzerkontensteuerung (UAC, User Account Control) ist ein Sicherheitsmechanismus in Windows, der clientseitig ab Vista und serverseitig ab Server 2008 verfügbar ist. Die UAC realisiert das Prinzip des *Least-Privileged User Account*, um die Missbrauchsmöglichkeiten administrativer Berechtigungen zu begrenzen. Sie unterstützt insbesondere die Umsetzung der Maßnahme M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung* für normale Benutzer und Administratoren.

Bei aktiver Benutzerkontensteuerung arbeiten alle Benutzer grundsätzlich als Standardbenutzer. Auch Administratoren führen ihre Tätigkeiten zunächst als Standardbenutzer aus. Die UAC erkennt, wenn eine Aktivität erhöhte Rechte benötigt und gibt diese frei oder verweigert sie, je nachdem wie sie konfiguriert wurde. Die UAC wirkt sich ausschließlich auf lokale Benutzersitzungen aus (auch Remotedesktop-Sitzungen). Auf Anmeldungen von Benutzern über das Netz, ausgehend von anderen Rechnern (z. B. Zugriff auf Dateifreigaben), hat sie keine Auswirkung, wenn Domänen-Konten verwendet werden.

Lokale Konten sind bei aktivierter UAC nicht mit allen netzbasierten Verwaltungsdiensten, zum Beispiel beim Zugriff auf die WMI-Schnittstelle (Windows Management Interface) des IT-Systems über das Netz, kompatibel. Verwaltungsdienste und -tätigkeiten sollten daher immer mit Domänenkonten ausgeführt werden.

Bestimmte Aktivitäten erfordern erhöhte Rechte innerhalb der lokalen Sitzung, die Standardbenutzer nicht besitzen. Zu diesen Aktivitäten zählen beispielsweise die Installation von Anwendungen, schreibender Zugriff auf Systemverzeichnisse, ältere Fachapplikationen oder die Ausführung bestimmter Betriebssystemprogramme und administrative Skripte. Doch auch Schadprogramme bedienen sich fast immer erhöhter Rechte. Wenn auf dem IT-System Konten mit Administratorberechtigungen verwendet werden, sollte die UAC immer aktiviert sein. Unter Windows Vista und Windows Server 2008 ist dies standardmäßig der Fall.

Unter Windows 7 und Windows Server 2008 R2 ist die UAC in einer abgeschwächten Form voreingestellt. Administrative Konten können mit uneingeschränkten Berechtigungen weiterarbeiten, ohne dass der Desktop abgeblendet wird. Damit die Schutzfunktionen der UAC gegen Angreifer und Schadprogramme wirksam sind, müssen sie auf *Immer benachrichtigen* konfiguriert werden (*Systemsteuerung* | *Benutzerkonten* | *Einstellungen der Benutzerkontensteuerung ändern*).

**Einfluss auf die Benutzerumgebung**

Bevor ein normaler Benutzer eine Aktivität ausführen kann, die erhöhte Rechte erfordert, erscheint ein geschütztes Benutzeranmeldefenster zur Eingabe der Authentisierungsdaten eines Administrators. Dies kann den normalen Benutzer verunsichern oder ihn zu Fehlhandlungen anstiften. Zum anderen kann es zu einer Art "Über-die-Schulter"-Situation kommen, bei der Service-Mitarbeiter mehrfach im Beisein des Benutzers ein Kennwort eingeben müssen. Dadurch

kann das Kennwort versehentlich kompromittiert werden. Es ist zu empfehlen, die lokale Sicherheitsoption *Benutzerkontensteuerung: Verhalten der Anhebungsaufforderung für Standardbenutzer* auf die Einstellung *Anforderungen für erhöhte Rechte automatisch ablehnen* zu konfigurieren (unter *gpedit.msc* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*). Seit Windows 7 / Windows Server 2008 R2 heißt diese Sicherheitsoption: *Benutzerkontensteuerung : Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer.* In der Folge erhalten Standardbenutzer nur noch eine normale Fehlermeldung. Administratoren können weiterhin die Befehle *runas* und *Ausführen als ...* verwenden, wenn sie erhöhte Rechte für eine Tätigkeit benötigen. Werden die Rechner in Umgebungen mit hohen oder sehr hohen Sicherheitsanforderungen eingesetzt, sollte diese Option immer gesetzt sein.

Bevor ein Mitglied der Gruppe *Administratoren* eine Aktivität mit erhöhten Rechten ausführen kann, erscheint ein einfaches Bestätigungsfenster der UAC. Andere Authentisierungsdaten müssen und können hier nicht eingegeben werden.

Eine Ausnahme bildet unter Windows Server 2008 das vordefinierte Konto "Administrator", das durch die Benutzerkontensteuerung generell nicht eingeschränkt wird (bei Vista ist eine Anmeldung mit dem Konto "Administrator" nicht möglich).

Das Bestätigungsfenster selbst kann die Anzahl der Schritte, die ein Administrator bei seinen regelmäßigen Aufgaben durchführen muss, unangemessen erhöhen. Werden häufig administrative Konsolen benötigt, sollten diese in einer MMC-Konsole (*mmc.exe*, *Microsoft Management Console*) gebündelt werden, um mehrfache störende Abfragen zu vermeiden. Andere Möglichkeiten der Bündelung administrativer Vorgänge sind die Aufgabenplanung, Verwaltungs-Tools von Drittanbietern sowie die Kommandozeilenfenster (Powershell mit erhöhten Rechten, "DOS-Box" usw.).

Es empfiehlt sich, die Auswirkungen der zusätzlichen Schritte und die Möglichkeiten der Bündelung gemeinsam mit den betroffenen Administratoren zu beurteilen. Bei einer zu starken Beeinträchtigung der Arbeitseffizienz der Administratoren kann das Bestätigungsfenster abgeschaltet werden. Dies geschieht, indem der GPO-Richtlinie *Benutzerkontensteuerung: Verhalten der Benutzeraufforderung mit erhöhten Rechten für Administratoren im Administratorbestätigungsmodus* die Einstellung *Keine Aufforderung* zugewiesen wird. In der Folge erhöht die UAC die Rechte für den Administrator im Hintergrund, das heißt ohne Interaktion mit dem Administrator. Die beschriebene Einstellung erfordert ein Abwägen von Bedienbarkeit und Sicherheitsniveau und muss dokumentiert werden.

Das häufigste Beispiel für diese Einstellung sind Arbeitsplatzrechner, an denen in einer eingeschränkten Benutzerumgebung gearbeitet wird. Muss ein Administrator Wartungsarbeiten an diesen Rechnern durchführen, dann meldet er sich nur für einen kurzen Zeitraum darauf an und schließt die Wartung schnellstmöglich ab. Er verwendet normale Benutzerapplikationen entweder gar nicht oder nur in sehr geringem Maße.

Ein Gegenbeispiel, bei dem die oben genannte Einstellung nicht verwendet werden darf, sind administrative Konten für normale Benutzer, unter Umständen auch Zweitkonten, die regelmäßig zum Einsatz kommen oder auf mobilen Rechnern zur Verfügung gestellt werden.

Für Arbeitsstationen von Administratoren sollte in einer Richtlinie (M 2.325 *Planung der Sicherheitsrichtlinien für Windows-Clients ab Windows XP*) festge-

legt werden, ob Teile der Administration in einer eingeschränkten Benutzerumgebung stattfinden müssen. Dies sollte hauptsächlich von den Aufgaben, von der Verwaltungssoftware und vom erforderlichen Sicherheitsniveau abhängen. Ist eine eingeschränkte Benutzerumgebung vorgesehen, dann sollten im Rahmen dieser Richtlinie der sichere Desktop und die Bestätigungsmeldungen nicht deaktiviert werden.

Ist keine eingeschränkte Benutzerumgebung für den jeweiligen Administrationsbereich vorgesehen, empfiehlt es sich, die UAC ganz abzuschalten. Eine UAC mit abgeschwächten Einstellungen würde kaum eine Schutzwirkung erzielen. Andererseits bleiben jedoch die Kompatibilitätsprobleme der UAC erhalten, zum Beispiel mit WMI-Skripten.

Die unter Windows 8 eingeführten Windows Apps, die aus dem Windows Store bezogen werden können, erfordern allerdings, dass die Benutzerkontensteuerung aktiviert ist. Sobald die Benutzerkontensteuerung deaktiviert wird, kann dies dazu führen, dass Apps nicht mehr ordnungsgemäß funktionieren. Aufgrund der Abhängigkeit der neuen Metro-Apps von der Benutzerkontensteuerung kann diese nicht mehr komplett über die Systemsteuerung deaktiviert werden. Ist es erforderlich, die Benutzerkontensteuerung komplett zu deaktivieren, dann muss dies über die Veränderung des entsprechende Eintrags in der Registry unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System* für den Eintrag *EnableLUA* erfolgen.

Unabhängig von der Konfiguration der UAC sollten alle Konten mit Administratorenrechten dokumentiert sein. Vergebene Administratorrechte sollten regelmäßig auf ihre Notwendigkeit überprüft und entsprechend angepasst (das heißt auch wieder entzogen) werden, siehe M 2.8 *Vergabe von Zugriffsrechten*.

**Sicherer Desktop**

Die Bestätigungsmeldung der UAC oder das zusätzliche Anmeldefenster sind gegen Angreifer und Schadprogramme geschützt, solange sie im sogenannten *sicheren Desktop* angezeigt werden. Die oben genannte Gruppenrichtlinie enthält eine Reihe weiterer Einstellungen, die den sicheren Desktop umgehen oder deaktivieren. Der sichere Desktop darf jedoch nicht umgangen oder deaktiviert werden.

**Geschützter Modus im Internet Explorer**

Zur Nutzung des *Geschützten Modus* des Internet Explorer 7 muss die Benutzerkontensteuerung aktiviert sein, wie es in der Standardkonfiguration ab Windows Vista der Fall ist. Wird die Benutzerkontensteuerung deaktiviert, verliert der Internet Explorer 7 unmittelbar (und ohne Warnmeldung durch das Betriebssystem) den Status des *Geschützten Modus*. Unter Internet Explorer 11, der mit Windows 8 ausgeliefert wird, ist die Benutzerkontensteuerung für den geschützten Modus nicht erforderlich.

Prüffragen:

- Ist die Benutzerkontensteuerung (UAC, User Account Control) aktiviert?
- Ist die GPO-Richtlinie Benutzerkontensteuerung: Verhalten der Anhebungsaufforderung für Standardbenutzer mit der Einstellung Anforderungen für erhöhte Rechte automatisch ablehnen konfiguriert?
- Ist für Administratoren die GPO-Richtlinie Benutzerkontensteuerung: Verhalten der Benutzeraufforderung mit erhöhten Rechten für Administratoren im Administratorbestätigungsmodus gemäß einer

Abwägung von Bedienbarkeit und Sicherheitsniveau konfiguriert und diese Entscheidung dokumentiert?
- Sind alle Konten mit Administratorrechten dokumentiert?
- Werden vergebene Administratorrechte regelmäßig auf ihre Notwendigkeit überprüft, entsprechend angepasst und gegebenenfalls wieder entzogen?

# M 4.341 Integritätsschutz ab Windows Vista

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Mit Windows Vista hat Microsoft verschiedene Sicherheitsmechanismen zum Schutz der Integrität kritischer Systemressourcen und zum Schutz der Integrität von Benutzerdaten neu eingeführt. Zu diesen Sicherheitsmechanismen zählen der Windows Integrity Mechanism (WIM), Integritätsebenen (Integrity Level - IL), der *Geschützte Modus* des Internet Explorers, die Windows Ressource Protection (WRP), der Trusted Installer und die Windows-Ressourcenprüfung (*sfc.exe*). Welche Sicherheitsmechanismen zum Integritätsschutz eingesetzt werden sollen, ist in Abhängigkeit von den Schutzanforderungen festzulegen.

**Windows Integrity Mechanism (WIM) und Integritätsebenen**

WIM dient in Verbindung mit der Benutzerkontensteuerung (UAC) dem Schutz der Systemintegrität und dem Schutz der Benutzerdaten gegen unbemerkte Integritätsverletzungen durch Schadsoftware. WIM basiert technisch auf so genannten Integritätsebenen (Integrity Level, IL), die bestimmten Betriebssystemobjekten, so genannten *Securable Objects*, zugeordnet sind. Beispiele für Securable Objects sind Benutzerkonten, Gruppenkonten, Dateien, Ordner, Prozesse und Registry-Schlüssel.

Es gibt folgende Integritätsebenen für Betriebssystemobjekte (hier in absteigender Bedeutung für die Integrität des Gesamtsystems geordnet):

- *System*
- *High*
- *Medium*
- *Low*
- *Untrusted*

Für die Interaktion zwischen Betriebssystemobjekten auf unterschiedlichen Integritätsstufen können drei Regeln festgelegt werden:

- *No write up (nw)*
  Ein Betriebssystemobjekt kann andere Objekte auf einer höheren Integritätsebene nicht modifizieren, auch dann nicht, wenn es zum Beispiel nach Access Control Lists (ACL) erlaubt wäre.
- *No read up (nr)*
  Ein Betriebssystemobjekt kann auf Daten anderer Objekte auf einer höheren Integritätsebene nicht lesend zugreifen (zum Beispiel auf ein Passwort, das von einem Prozess im Speicher gehalten wird).
- *No execute up (nx)*
  Ein Betriebssystemobjekt (zum Beispiel ein Prozess) kann keinen neuen Prozess auf einer höheren Integritätsebene starten.

Standardmäßig ist nur die *nw*-Regel aktiviert, die *nr*-Regel und die *nx*-Regel sind deaktiviert.

Die höchste Integritätsebene für Prozesse, die von einem Standardbenutzer gestartet werden, und für Objekte, die von einem Standardbenutzer erstellt werden, ist *Medium*. Für Administratoren gilt für entsprechende Aktionen *High* als höchstmögliche Integritätsebene. Systemdiensten schließlich ist die Integritätsebene *System* zugeordnet. Ist einem Objekt nicht explizit eine Integri-

tätsebene zugeordnet, dann gilt als Standardebene *Medium*. Integritätsebenen vererben sich analog den Einträgen einer ACL.

Durch *nw*-, *nr*- oder *nx*-Regeln festgelegte Beschränkungen für die Interaktion zwischen Betriebssystemobjekten werden unabhängig von der ACL der beteiligten Objekte vom Betriebssystem durchgesetzt. So arbeitet beispielsweise ein Administrator bei aktivierter Benutzerkontensteuerung und noch nicht erfolgter Rechteerhöhung als Standardbenutzer auf der Integritätsebene *Medium*. Gemäß der *nw*-Regel kann daher der Administrator selbst dann nicht auf Objekte auf der Integritätsebene *High* schreibend zugreifen, wenn ihm gemäß ACL als Eigentümer Vollzugriff auf das Objekt zusteht. Für den schreibenden Zugriff auf ein Objekt auf der Integritätsebene *High* benötigt der Administrator (als hier handelndes Betriebssystemobjekt) die Integritätsebene *High*. Diese Ebene wird dem Administrator erst nach einer Rechteerhöhung durch die Benutzerkontensteuerung zugewiesen. In der Standardkonfiguration erfordert diese Rechteerhöhung die explizite Zustimmung des Administrators. Schreibende Zugriffe des Administrators auf Systemprozesse sind jedoch auch dann noch nicht möglich, da diese auf einer noch höheren Integritätsebene als *High* laufen, nämlich auf der Ebene *System*.

**Geschützter Modus und Internet Explorer**

Unter dem *Geschützten Modus* (Protected Mode) versteht Microsoft im Wesentlichen die Zuweisung der Integritätsebene *Low* anstelle von *Medium* an Prozesse. Der Internet Explorer (IE) ab Version 7 (IE7) läuft ab Windows Vista / Server 2008 standardmäßig im Geschützten Modus, das heißt auf der Integritätsebene *Low*. Ältere Versionen des Internet Explorers (vor IE7) oder der IE7 unter Windows-Versionen vor Windows Vista / Server 2008 (z. B. unter Windows XP) unterstützen den Geschützten Modus nicht.

Für den Geschützten Modus des IE muss die Benutzerkontensteuerung aktiviert sein, wie es in der Standardkonfiguration ab Windows Vista / Server 2008 der Fall ist. Bei einer Deaktivierung der Benutzerkontensteuerung verliert der IE unmittelbar (und ohne Warnmeldung durch das Betriebssystem) seinen Geschützten Modus.

Vom IE herunter geladene Daten, wie ausführbarer Programmcode, können nur in Verzeichnisse auf der Integritätsebene *Low* geschrieben werden, da für den IE die Integritätsebene *Low* gilt. Diese Daten befinden sich dann selbst auf der Ebene *Low*. Aufgrund der *nw*-Regel kann der herunter geladene Programmcode nicht unbemerkt schreibend auf Daten des Benutzers (in der Regel auf der Integritätsebene *Medium*) oder des Betriebssystems (auf der Ebene *High* oder *System*) zugreifen. Der *Geschütze Modus* erschwert somit das unbemerkte Herunterladen und Ausführen von Programmcode durch den IE.

Der IE unterstützt aber bei Bedarf auch das Herunterladen und Speichern von Daten auf die Integritätsebene *Medium*. Dies ist beispielsweise dann erforderlich, wenn es sich um eine Anwendung handelt, mit der der Benutzer anschließend seine Daten (auf der Ebene *Medium*) bearbeiten möchte. Hierfür läuft parallel zum Prozess des Internet Explorers ein so genannter User Broker Prozess (IEUser.exe). Die Nutzung dieses Prozesses um Daten mit der Integritätsebene *Medium* zu speichern, kann nur nach der expliziten Zustimmung des Benutzers erfolgen. Um zu verhindern, dass unabsichtlich Schadsoftware auf dem IT-System eingeschleppt wird, sind die Benutzer im Umgang mit dem Geschützten Modus zu schulen.

Es gibt Erweiterungen des Internet Explorers (auch Extensions oder Add-ons genannt), die nicht kompatibel zum *Geschützten Modus* sind, da sie herunter

geladene Daten in Bereiche des Dateisystems oder der Registry auf der Integritätsebene *Medium* schreiben müssen. Der IE nutzt eine Virtualisierung des Dateisystems und der Registry, um diese Erweiterungen zu unterstützen. Virtualisierung bedeutet in diesem Zusammenhang, dass der IE die Schreibzugriffe dieser Erweiterungen in Kopien der benötigten Bereiche umleitet. Diese duplizierten (beziehungsweise virtualisierten) Bereiche liegen auf der Integritätsebene *Low*. So wird die Integrität der nicht virtualisierten Benutzerdaten nicht gefährdet. Die gleiche Technik setzt Windows ab Vista / Server 2008 zur geschützten Ausführung unsicherer Alt-Applikationen ein (siehe M 4.338 *Einsatz von File und Registry Virtualization bei Clients ab Windows Vista*).

Im IE kann der Geschützte Modus gesondert für jede der vier Sicherheitszonen von einem Standardbenutzer aktiviert oder deaktiviert werden. Zu beachten ist, dass in der Standardkonfiguration der Geschützte Modus für die Sicherheitszone *Vertrauenswürdige Sites* deaktiviert ist. Nur für die anderen drei Sicherheitszonen *Internet*, *Lokales Intranet* und *Eingeschränkte Sites* ist der Geschützte Modus aktiviert.

Für die drei Sicherheitszonen *Internet*, *Lokales Intranet* und *Eingeschränkte Sites* sollte ein Standardbenutzer den Geschützten Modus nicht deaktivieren können. Hierzu muss für jede der drei Sicherheitszonen für das Gruppenrichtlinienobjekt *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Internet Explorer* | *Internetsystemsteuerung* | *Sicherheitsseite* | *Sperrung für* <Name der Zone> die Richtlinie *Geschützten Modus aktivieren* aktiviert werden.

Wenn eine nachweislich vertrauenswürdige Web-Seite inkompatibel mit dem Geschützten Modus ist, dann sollte sie der Sicherheitszone *Vertrauenswürdige Sites* zugewiesen werden. Für diese Sicherheitszone sollte der Geschützte Modus deaktiviert bleiben. Das damit verbundene erhöhte Risiko des unbemerkten Herunterladens und Ausführens von Programmcode durch den IE ist gegen die Anforderungen zur Verfügbarkeit der betreffenden Web-Seite abzuwägen.

Mit dem Internet Explorer 11 hat Microsoft den *Enhanced Protected Mode* eingeführt, der in den Schutzfunktionen deutlich weiter geht. Nähere Informationen hierzu finden sich in den Hilfsmitteln zum Baustein *Client unter Windows 8*.

**Windows Resource Protection und Trusted Installer**

Neben WIM, Integritätsebenen und Geschütztem Modus ist die Windows Ressource Protection (WRP) ein weiterer Sicherheitsmechanismus ab Windows Vista / Server 2008 zum Integritätsschutz kritischer Systemressourcen. WRP ist die neue Bezeichnung für den in früheren Windows-Versionen als Windows File Protection (WFP) bezeichneten Sicherheitsmechanismus.

Zu den kritischen Systemressourcen zählen dabei bestimmte Registry-Schlüssel, Verzeichnisse und Dateien. Die Dateien sind alle Dateien des Typs *.dll, .exe, .ocx,* und *.sys* sowie ausgewählte kritische Dateien (insgesamt ca. 90) einer Windows-Installation.

Trusted Installer ist eine zentrale Komponente der WRP Trusted Installer bezeichnet einen Systemdienst zur ordnungsgemäßen Modifikation der kritischen Systemressourcen und eine Benutzergruppe, deren Mitglieder die Eigentümer der kritischen Systemressourcen sind.

Die vollen Zugriffsrechte auf die kritischen Systemressourcen sind auf den Eigentümer des Trusted Installers beschränkt. Die Konten *System* und *Admi-*

*nistrator* haben auf kritische Systemressourcen nur eingeschränkte Zugriffsrechte, insbesondere keine Schreibrechte. Dadurch werden versehentliche Integritätsverletzungen kritischer Systemressourcen, beispielsweise durch einen Administrator, unterbunden. Allerdings kann sich ein Administrator als Eigentümer einsetzen und selbst volle Zugriffsrechte zuweisen. Vorsätzliche Integritätsverletzungen werden also nur erschwert und nicht grundsätzlich verhindert.

Modifikationen an kritischen Systemressourcen, wie das Einspielen von Service Packs oder Hotfixes, sollten ausschließlich über WRP und den Trusted Installer (in Form des Systemdiensts *TrustedInstaller*) erfolgen.

Für die manuelle Überprüfung der Integrität von kritischen Systemdateien steht dem Administrator als Kommandozeilenwerkzeug die Windows-Ressourcenprüfung *sfc.exe* zur Verfügung. Damit lassen sich im Fall festgestellter Integritätsverletzungen die betroffenen Dateien manuell gegen die unversehrten Versionen austauschen.

**App-Container Mechanismus und AppLocker ab Windows 8**

Mit Windows 8 gibt es eine neue Kategorie von Programmen, die sogenannten Windows-Apps (auch Modern UI Apps). Ein Windows-App kann ohne Administrator-Rechte installiert werden. Um die Sicherheit der Systemintegrität zu gewährleisten, läuft jede Windows-App innerhalb einer Sandbox (AppContainer) mit eingeschränktem Zugriff auf die Betriebssystem-Ressourcen. Jede Windows-App muss anzeigen, welche Verwendungsberechtigungen (Capabilities) sie benötigt. Verwendungsberechtigungen, welche die Privatsphäre des Benutzers beinträchtigen können, müssen beim ersten Start der Windows-App bestätigt werden (z. B. Zugriff auf Mikrofon, Kamera, Ortung).

Mittels AppLocker ist es zudem möglich, die Installation bestimmter Windows-Apps grundsätzlich zu verbieten. Wird AppLocker mit Regeln eingesetzt, die auf einem Dateihash oder einer Signatur basieren, besteht hierdurch auch ein Schutz vor Veränderungen der installierten Apps. Nähere Informationen hierzu finden sich in M 4.419 *Anwendungssteuerung ab Windows 7 mit AppLocker*.

Prüffragen:

- Wurde definiert, welche Sicherheitsmechanismen für den Integritätsschutz ab Windows Vista/Server 2008 umgesetzt werden sollen?
- Ist sichergestellt, dass Standardbenutzer den Geschützten Modus für die drei Sicherheitszonen Internet, Lokales Intranet und Eingeschränkte Sites nicht deaktivieren können?
- Wurden die Benutzer für den Umgang mit dem Geschützten Modus geschult, so dass sie nicht ohne hinreichende Prüfung herunter geladene Dateien bzw. Programme autorisieren?
- Wird der Geschützte Modus für die gewünschten Zonen in den Internetsicherheitseinstellungen erzwungen?

# M 4.342 Aktivierung des Last Access Zeitstempels ab Windows Vista

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Das Dateisystem NTFS verwaltet drei Zeitstempel, um Änderungen am Dateisystem nachvollziehen zu können. Diese Zeitstempel werden auch MAC-Zeitstempel genannt. Der Begriff MAC-Time steht unter Windows für die Modification-, Access- und Creation-Time einer Datei im NTFS-Dateisystem.

- Die Modification Time (Zeitpunkt der letzten Modifikation) ist der Zeitpunkt, zu dem zum letzten Mal schreibend auf eine Datei zugegriffen wurde. Dieser Zeitstempel wird aktualisiert, wenn sich der Inhalt der Datei verändert.
- Last Access Time (Zeitpunkt des letzten Zugriffs) ist der Zeitpunkt, zu dem eine Datei das letzte Mal gelesen oder ausgeführt wurde. Dieser Zeitstempel wird aktualisiert, wenn Metadaten oder Dateiinhalte angezeigt werden. Hierbei ist es unerheblich, ob die Datei gespeichert oder anderweitig verändert wurde. Wird die Datei geöffnet, aufgerufen oder durch andere Mittel betrachtet, findet sich dies im Zeitstempel wieder.
- Creation Time (Zeitpunkt der Erstellung) ist der Zeitpunkt, zu dem eine Datei neu oder durch Kopieren erstellt wurde.

Muss während der Untersuchung eines Sicherheitsvorfalls (siehe B 1.8 *Behandlung von Sicherheitsvorfällen*) ein Datenträger mit NTFS analysiert werden, hilft eine Analyse der MAC-Times, um herauszufinden, welche Dateien während des vermutlichen Missbrauchs gelesen, geschrieben, ausgeführt oder verändert wurden. Dies gibt Hinweise darauf, welche Konfigurationsdateien beziehungsweise welche Systemdateien verändert wurden, um zum Beispiel eine Hintertür in das System zu installieren. Zusätzlich kann man die während des angenommenen Angriffszeitpunkts veränderten Dateien analysieren und unter Umständen erfahren, welche Methode zum Systemeinbruch angewandt wurde. Durch die Erstellung von so genannten Timelines kann recht genau bestimmt werden, zu welchem Zeitpunkt eine Datei auf ein System kopiert wurde, und ob sie in der Folge betrachtet beziehungsweise aufgerufen wurde.

Unter Windows Vista, Windows 7 und Windows Server 2008 ist das Aktualisieren des Last-Access-Zeitstempels in der Registry standardmäßig deaktiviert, da bei einer ungünstigen Dateisystemstruktur Leistungseinbußen möglich wären. Im Rahmen der Erstellung eines Sicherheitskonzeptes für ein solches System sollte geprüft werden, ob der Last-Access-Zeitstempel geschrieben werden soll, um die Analyse eines Systemmissbrauchs zu erleichtern. Performanceaspekte sind in die Bewertung einzubeziehen. Gibt es andere angemessene Verfahren zur Missbrauchsanalyse, kann auf die Aktivierung der Funktion verzichtet werden.

Zum Aktivieren des Last-Access-Zeitstempels ist der Registry-Key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate* auf den Wert "0" zu setzen.

Prüffragen:

- Wurde bei der Erstellung des Sicherheitskonzeptes für Systeme mit Windows Vista, Windows 7 oder Windows Server 2008 geprüft, ob man auf den Last-Access-Zeitstempel verzichten kann?
- Wurden bei dieser Prüfung auch Performanceaspekte von Windows Vista und Windows 7 in die Bewertungen einbezogen?

# M 4.343 Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, IT-Sicherheitsbeauftragter, Leiter IT

Für einen arbeitsfähigen Client ab Windows Vista oder einen Server ab Windows 2008 müssen das Betriebssystem installiert und eine Lizenz aktiviert worden sein (siehe M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

An den Vorgang der Aktivierung einer Lizenz sind bestimmte Vorgaben geknüpft. Wenn gegen diese verstoßen wird, fällt der Windows Vista Client automatisch in den so genannten RFM (Modus mit reduzierter Funktionalität, Reduced Functionality Mode). Im RFM ist der Vista Client solange nicht mehr arbeitsfähig, bis erfolgreich eine Windows Vista Lizenz für den Client reaktiviert wurde. Mit dem Erscheinen des Windows Vista Service Pack 1 und ab Windows 7 sowie Windows Server 2008 hat Microsoft den RFM zurückgenommen. Anstelle des RFM zeigen Windows-Systeme nun entsprechende Warnmeldungen an. Auch diese behindern den Regelbetrieb des Systems. In beiden Fällen ist eine Reaktivierung des betroffenen Systems erforderlich, um in den unbehinderten Regelbetrieb zurückzukehren.

Insbesondere vor Hardwaremodifikationen (z. B. Wechsel der Festplatte oder Erweiterung des Arbeitsspeichers) sollte der Microsoft-Support kontaktiert werden, um Aussagen zu einer möglicherweise erforderlichen Reaktivierung zu erhalten. Es sollte auch überlegt werden, in einer Testumgebung vorab auf eine möglicherweise erforderliche Reaktivierung zu testen.

**Speziell für KMS-Aktivierung**

Systeme, die im Rahmen eines Volumenlizenzvertrags mit dem Key Management Service (KMS) aktiviert wurden, müssen spätestens nach 180 Tagen plus eines Kulanzzeitraums von 30 Tagen reaktiviert werden. Dazu müssen sie mit dem KMS kommunizieren können. Zur Sicherstellung der Verfügbarkeit sollten jedoch die Verbindungen von den betroffenen Systemen zum KMS in wesentlich kürzeren Zeitabständen regelmäßig erfolgen. Dies mindert die Gefahr der Überschreitung der maximal zulässigen Frist von 210 Tagen.

Für die initiale Aktivierung der Systeme im LAN kommunizieren diese mit dem KMS über das LAN der Institution. Clients werden erst aktiviert, wenn innerhalb von 30 Tagen mindestens 25 Systeme beim KMS angefragt haben ("Activation Threshold"). Server werden bereits ab fünf anfordernden Systemen aktiviert.

Für den Zeitraum einer angestrebten Reaktivierung muss ein KMS verfügbar sein, eventuell kann überlegt werden, einen zweiten KMS zu betreiben.

**Speziell für Active Directory-based Activation (ADBA)**

Auch für die ab Windows 8 eingeführte Aktivierungsmethode Active Directory-based Activation, das Institutionen das Aktivieren von Windows 8, Windows Server 2012 und Office 2013 im internen Netz über eine Verbindung mit der Domäne ermöglicht, ist eine Reaktivierung spätestens nach 180 Ta-

gen notwendig. Befindet sich das System in einem isolierten Netz, ist ebenfalls sicherzustellen, dass eine Verbindung innerhalb von 180 Tagen zum Domänen-Controller erfolgen kann. Ist dies nicht möglich, kann der Austausch der Aktivierungsdaten auch über einen Wechseldatenträger erfolgen. Microsoft beschreibt hierzu die einzelnen Schritte ausführlich.

Prüffragen:

- Ist speziell für die KMS-Reaktivierung sichergestellt, dass die Windows-Systeme innerhalb von 210 Tagen nach der letzten Aktivierung mit dem KMS kommunizieren können?
- Ist speziell für die KMS-Reaktivierung sichergestellt, dass der KMS bei Clients von insgesamt mindestens 25 Windows-Systemen und bei Servern von mindestens 5 Windows-Systemen aktiv genutzt wird?
- Ist speziell für die KMS-Reaktivierung sichergestellt, dass ein KMS im Zeitraum einer angestrebten Reaktivierung verfügbar ist?
- Ist für die Active Directory-based Activation sichergestellt, dass die Windows-Systeme sich innerhalb von 180 Tagen mit dem Domänen-Controller im Hauptnetz verbinden können, oder wurden andere Aktivierungsmethoden, wie z. B. die Aktivierung über Wechseldatenträger, berücksichtigt?

# M 4.344 Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Revisor

Rechnersysteme sollten überwacht werden, um die Systemsicherheit und Systemintegrität aufrecht zu erhalten. Nur so können mögliche Sicherheitslücken, Verstöße gegen die geltenden Sicherheitsrichtlinien oder gar Angriffe durch Außen- und Innentäter entdeckt und geeignete Gegenmaßnahmen eingeleitet werden.

Die Überwachung von Clients ab Windows Vista und Servern ab Windows Server 2008 müssen schon in der Planungsphase berücksichtigt und relevante Parameter in einem Überwachungskonzept festgehalten werden. Damit auf Windows-Clients eine Überwachung erfolgen kann, muss diese zunächst über Gruppenrichtlinien oder lokale Einstellungen aktiviert werden. Dies gilt insbesondere für die Datei- und Registry-Überwachung.

Windows-Systeme unterscheiden in der Ereignisanzeige zwischen "Windows-Protokollen" und "Anwendungs- und Dienstprotokollen".

In den Windows-Protokollen werden folgende Ereignisse überwacht:

- Anwendungsprotokoll: enthält Ereignisse, die von den Anwendungen gemeldet werden. Welche Ereignisse protokolliert werden können, legen die Anwendungsentwickler fest. Dieses Protokoll trägt bei Clients ab Windows 7 den Namen: Anwendung.
- Sicherheitsprotokoll: enthält von Microsoft als sicherheitsrelevant eingestufte Ereignisse. Durch die Konfiguration der Überwachungsrichtlinien kann ein Administrator festlegen, was protokolliert werden soll.
- Setupprotokoll oder Einrichtungsprotokoll: enthält Ereignisse, die während der Installation von Anwendungen auftreten. Dieses Protokoll trägt bei Clients ab Windows 7 den Namen: Installation.
- Systemprotokoll: enthält Ereignisse, die von Microsoft Windows Systemkomponenten ausgehen. Dieses Protokoll trägt bei Clients ab Windows 7 den Namen: System.
- Weitergeleitete Ereignisse: nur wenn ein Client explizit zum Sammeln von Ereignissen auf entfernten Computern (Remote Clients) konfiguriert wurde, werden auf dem Client "Weitergeleitete Ereignisse" angezeigt. Es handelt sich dabei um Ereignisse der zuvor genannten Protokolle. Die Remote Clients müssen ebenfalls konfiguriert werden, um den Zugriff auf ihre Ereignisanzeige zuzulassen.

Es ist zu überlegen, einen Sammel-Client zur zentralen Kontrolle der Ereignisprotokolle einzurichten, ähnlich eines Syslog-Servers. Diese Funktion kann auch von Server-Produkten von Microsoft oder von Tools anderer Hersteller, wie Virenschutz-Software für den professionellen Einsatz, übernommen werden.

Anwendungs- und Dienstprotokolle wurden mit Microsoft Windows Vista eingeführt. In diesen Protokollen werden keine systemweiten Ereignisse gespeichert, sondern Ereignisse, die einzelne Anwendungen oder Komponenten betreffen.

In den folgenden Tabellen werden Empfehlungen zu Einstellungen der Anzeige von Ereignissen in der *Ereignisanzeige* gegeben. Die Ereignisse erzeugen entsprechende Nachrichten im Sicherheitsprotokoll.

Die Überschriften der folgenden Tabellen geben die Pfade in den Gruppenrichtlinien (Group Policy Objects, GPOs) an. Diese können lokal (lokale XP Gruppenrichtlinie) oder im Active Directory konfiguriert werden (siehe M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*).

**Pfad "Computerkonfiguration | Windows-Einstellungen | Sicherheitseinstellungen | Lokale Richtlinien | Überwachungsrichtlinie"**

| Parameter | Empfehlung |
|---|---|
| Prozessnachverfolgung überwachen | Die Prozessverfolgung ist im Allgemeinen nicht sinnvoll und sollte nur für Debugging-Zwecke aktiviert werden. |
| Rechteverwendung überwachen | Fehlgeschlagene Zugriffsversuche sollten überwacht werden. (Fehler) |
| Richtlinienänderungen überwachen | Das Verändern von Richtlinieneinstellungen (GPOs) ist eine sicherheitskritische Operation und sollte überwacht werden. (Erfolg) |
| Systemereignisse überwachen | Systemereignisse sollten überwacht werden. (Erfolg) |
| Anmeldereignisse überwachen | Die Protokollierung der Anmeldeereignisse auf dem lokalen Rechner (z. B. Arbeitsplatzrechner) sollte aktiviert sein. (Erfolg). Auf Domänencontrollern oder Systemen mit hohem Schutzbedarf sollten auch fehlgeschlagene Ereignisse überwacht werden. (Erfolg und Fehler) |
| Kontenverwaltung überwachen | Änderungen in den Konteneinstellungen sind sicherheitskritische Ereignisse und sollten überwacht werden. (Erfolg und Fehler) |
| Objektzugriff überwachen | Fehlgeschlagene Objektzugriffe sollten nur auf Systemen mit hohem Schutzbedarf oder zur Fehlerbehebung überwacht werden. Bedingt durch die Menge der Events sollten erfolgreiche Objektzugriffe nur für eine geringe Anzahl wichtiger Objekte aktiviert werden. |
| Verzeichnisdienstzugriff überwachen | Die Verzeichnisdienstzugriffe sollten überwacht werden. Dabei sollte mindestens die Erfassung von Fehlern bei den Zugriffen aufgezeichnet werden. (Fehler) |

Bei Clients ab Windows Vista und Servern ab Windows Server 2008 sind zu den oben genannten noch weitere Einstellungen zur Überwachung möglich.

Die folgenden Tabellen geben Empfehlungen zu Konfigurationseinstellungen zu den Themen:

- "Zuweisen von Benutzerrechten auf die Ereignisanzeige",
- "Einstellungen für das Ereignisprotokoll" Teil 1,
- "Einstellungen für das Ereignisprotokoll" Teil 2 und
- "Sicherheitsoptionen"

für die Überwachung von Clients ab Windows Vista und Servern ab Windows Server 2008-Systemen wieder.

**Pfad "Computerkonfiguration | Windows-Einstellungen | Sicherheitseinstellungen | Lokale Richtlinien | Zuweisen von Benutzerrechten"**

| Parameter | Empfehlung |
|---|---|
| Verwalten von Überwachungs- und Sicherheitsprotokollen | Dieses Recht ermöglicht:<br>- die Konfiguration der Audit-Einstellungen für die einzelnen Objekte (Dateien, Registry, Active Directory),<br>- das Ansehen bzw. Löschen des Sicherheitsprotokolls.<br><br>Welcher Benutzergruppe (bzw. -gruppen) dieses Recht eingeräumt wird, hängt vom Überwachungskonzept ab. Prinzipiell sollte dieses Recht restriktiv vergeben werden, zum Beispiel an die Gruppe der Administratoren. Es sollte dabei jedoch beachtet werden, dass:<br><br>- auch zur Diagnose und Behebung von nicht sicherheitsrelevanten Problemen der Zugriff auf das Sicherheitsprotokoll notwendig sein kann<br>- Administratoren sich dieses Benutzerrecht auch selbst einräumen können, wenn es ihnen entzogen wird. Es empfiehlt sich daher, diesen Vorgang zu protokollieren (Option Computer Richtlinien / Lokale Richtlinien / Überwachungsrichtlinien \| Rechteverwendung überwachen). |

**Pfad "Computerkonfiguration | Administrative Vorlagen | Windows-Komponenten | Ereignisprotokolldienst | <Protokoll>"**

| Parameter | Empfehlung |
|---|---|
| - Maximale Protokollgröße (Anwendungsprotokoll)<br>- Maximale Protokollgröße (Setupprotokoll)<br>- Maximale Protokollgröße (Sicherheitsprotokoll) | Die Größe muss so gewählt werden, dass je nach Aufbewahrungsmethode auch bei überdurchschnittlicher Systemaktivität genügend Platz zur Verfügung steht. Dies ist besonders wichtig für das Sicherheitspro- |

| Parameter | Empfehlung |
|---|---|
| - Maximale Protokollgröße (Systemprotokoll) | tokoll, da sonst eine zeitliche Lücke in der Sicherheitsüberwachung des Systems entstehen kann. Vorschläge für die hier vorzunehmenden Einstellungen finden sich in M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* beziehungsweise M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*. Diese müssen jedoch den realen Bedingungen (Tests im Probebetrieb) angepasst werden. |
| Alte Ereignisse beibehalten | Wenn diese Richtlinie deaktiviert ist und die Protokolldatei ihre maximale Größe erreicht hat, werden die Einträge zu älteren Ereignissen in der Protokolldatei mit Einträgen zu neuen Ereignissen überschrieben. Die Informationen zu diesen älteren Ereignissen stehen dann nicht mehr zur Verfügung. Wenn diese Richtlinie aktiviert ist und die Protokolldatei ihre maximale Größe erreicht hat, werden keine Einträge zu den neuen Ereignissen in der Protokolldatei protokolliert. Die Informationen zu den neuen Ereignissen gehen verloren. Es wird empfohlen, die Richtlinie "Alte Ereignisse beibehalten" zu aktivieren. Wenn die Richtlinie "Volles Protokoll automatisch sichern" (siehe weiter unten) genutzt werden soll, um Protokolle automatisch zu archivieren, muss die Richtlinie "Alte Ereignisse beibehalten" aktiviert werden. |
| Volles Protokoll automatisch sichern | Wenn diese Richtlinie und die Richtlinie "Alte Ereignisse beibehalten" aktiviert sind, wird die Protokolldatei automatisch geschlossen und umbenannt, wenn sie ihre maximale Größe erreicht hat. Diese Richtlinie sollte aktiviert werden. |

Die Einstellungen der folgenden Tabelle können nur im Active Directory und nicht über lokale Gruppenrichtlinien konfiguriert werden.

**Pfad "Computerkonfiguration | Windows-Einstellungen | Sicherheitseinstellungen | Ereignisprotokoll"**

| Parameter | Empfehlung |
|---|---|
| - Aufbewahrungsmethode des Anwendungsprotokolls<br>- Aufbewahrungsmethode des Sicherheitsprotokolls | Je nach Protokollierungskonzept kann gewählt werden zwischen:<br>- Ereignisse auf Tagen basierend überschreiben, |

| Parameter | Empfehlung |
|---|---|
| - Aufbewahrungsmethode für das Setupprotokoll<br>- Aufbewahrungsmethode des Sysytemprotokolls | - Ereignisse bei Bedarf überschreiben und<br>- Ereignisse nicht überschreiben (Protokoll manuell aufräumen).<br><br>Wenn keine Protokollierung erfolgen soll oder die Protokolle nicht ausgewertet werden sollen, kann die Option "Ereignisse bei Bedarf überschreiben" gewählt werden. Sonst können die Optionen "Ereignisse auf Tagen basierend überschreiben" oder "Ereignisse nicht überschreiben (Protokoll manuell aufräumen)" konfiguriert werden. Dabei ist darauf zu achten, dass bei der Wahl von "Ereignisse auf Tagen basierend überschreiben" die Richtlinie "<Protokollname> aufbewahren" mit einer entsprechenden Anzahl von Tagen konfiguriert werden muss. Siehe dazu auch die nächste Konfigurationseinstellung. Wird die Option "Ereignisse nicht überschreiben (Protokoll manuell aufräumen)" gewählt, muss sichergestellt werden, dass die Protokolle manuell gelöscht werden. Wenn diese Löschung nicht erfolgt, werden neue Ereignisse nicht mehr protokolliert, sobald die maximale Protokollgröße erreicht ist. |
| - Anwendungsprotokoll-Aufbewahrung<br>- Sicherheitsprotokoll-Aufbewahrung<br>- Setupprotokoll-Aufbewahrung<br>- Systemprotokoll-Aufbewahrung | Mit dieser Richtlinie kann die Zeit konfiguriert werden, für die ein Protokoll aufbewahrt wird. Diese Einstellung ist wichtig, wenn die Aufbewahrungsmethode eines Protokolls auf "Ereignisse auf Tagen basierend überschreiben" gesetzt wurde. Die konfigurierte Anzahl von Tagen hängt von der jeweiligen Systemumgebung ab und muss groß genug sein, um eine Sicherung der Protokolldaten zu ermöglichen. Weiterhin muss die "Maximale Protokollgröße" der Protokolle so groß gewählt werden, dass diese nicht überschrieben werden. Siehe dazu auch Tabelle "Einstellungen für das Ereignisprotokoll Teil 1". Um die Protokolle archivieren zu können, muss ein Administrator oder Benutzer über das Privileg "Verwalten von Überwachungs- und Sicherheitsprotokollen" verfügen. Siehe dazu auch in der Ta- |

| Parameter | Empfehlung |
|---|---|
| | belle "Zuweisen von Benutzerrechten auf Ereignisanzeige". |
| - Lokalen Gastkontozugriff auf das Setupprotokoll verhindern<br>- Lokalen Gastkontozugriff auf Anwendungsprotokoll verhindern<br>- Lokalen Gastkontozugriff auf Sicherheitsprotokoll verhindern<br>- Lokalen Gastkontozugriff auf Systemprotokoll verhindern | Die Zugriffsbeschränkung für das Gastkonto sollte aktiviert werden. |

**Pfad "Computerkonfiguration | Windows-Einstellungen | Sicherheitseinstellungen | Lokale Richtlinien | Sicherheitsoptionen"**

| Parameter | Empfehlung |
|---|---|
| Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können | Zur Gewährleistung der Verfügbarkeit sollte diese Option deaktiviert werden. Lediglich bei hohem Schutzbedarf ist diese Option zu aktivieren, da dort Nachweisführung vor Verfügbarkeit geht. Bei Aktivierung sind weitere Maßnahmen zur Aufrechterhaltung des Betriebs erforderlich. |

Lokal können in der Ereignisanzeige für jedes Protokoll einzeln die Protokollgröße und das Verhalten bei Erreichen der maximalen Ereignisprotokollgröße konfiguriert werden.

Bei Einsatz von *DirectAccess* ab Windows 7 sollte auf dem Client eine Protokollierung der Verbindungsaktivitäten des Tunnels eingerichtet werden (siehe M 5.123 *Absicherung der Netzkommunikation unter Windows*). Hierfür müssen unter anderem Leistungsindikatoren von *perfmon.exe* abgefragt und Sammlungssätze erstellt werden. Als Speicherort der Sammlungssätze sollte ein sicheres Systemverzeichnis, wie *%systemdrive% \perflogs \System \Diagnostics* verwendet werden. Die optimale Größe der Log-Dateien muss durch regelmäßige Überprüfung an die aktuellen Bedingungen des Informationsverbundes angepasst werden. Die Verbindungsinformationen sollten mindestens eine Woche lang rückwirkend nachvollziehbar sein, um Fehlfunktionen und mögliche Angriffsmuster identifizieren zu können.

Mit Clients ab Windows 8 und Servern ab Windows Server 2012 besteht die Möglichkeit, den Zugriff auf Wechselmedien nachzuverfolgen. In früheren Versionen von Windows war es nur möglich, den Zugriff auf Wechselmedien einzuschränken oder zu verweigern. Wenn diese Richtlinieneinstellung aktiviert ist, so wird jedesmal ein Überwachungsereignis generiert, sobald ein Nutzer auf ein Wechselmedium zugreift.

Die Überwachungsrichtlinie wird unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Erweiterte Überwachungsrichtlinienkonfiguration* | *Systemüberwachungsrichtlinien* | *Objektzugriff* konfiguriert. Erfolgsüberwachungen zeichnen erfolgreiche Versuche auf, auf ein Wechselmedium zu schreiben oder davon zu lesen. Fehlerüberwachungen zeichnen erfolglose Versuche auf, auf Wechselmedienobjekte zuzugreifen. Für die Protokollierung von Wechselmedien-Fehlerereignissen muss die Einstellung *Handleänderung überwachen* ebenfalls konfiguriert werden.

Im Rahmen der Überwachung sind allgemein auch folgende Aspekte zu berücksichtigen:

- Der Datenschutzbeauftragte und der Personal- oder Betriebsrat sollten frühzeitig in die Planung der Überwachung mit einbezogen werden. Bei einer Überwachung werden meist auch personenbezogene Daten erfasst, um im Falle einer Sicherheitsverletzung den Verursacher zuverlässig feststellen zu können.
- Damit die Überwachungskomponenten Protokolleinträge generieren, muss die Überwachung über die relevanten Gruppenrichtlinieneinstellungen aktiviert werden.
- Clients ab Windows Vista und Server ab Windows Server 2008 stellen zur Überwachung zusätzlich die Protokoll-Funktionalität "Anwendungs- und Dienstprotokolle" zur Verfügung. Die bereits in älteren Microsoft Windows Versionen vorhandenen Windows-Protokolle sind um "Einrichtung" und "Weitergeleitete Ereignisse" ergänzt worden. Lokal kann für alle Protokolle die Protokollierung aktiviert oder deaktiviert werden. Weiterhin sind die Protokollgröße und das Verhalten bei Erreichen der maximalen Protokollgröße konfigurierbar.
- Der Aufbau einer zentralen Sammelstelle von Protokolldateien mit entsprechend automatisierter Auswertung kann durch Produkte von Microsoft oder von Drittherstellern erreicht werden. Wird ein Werkzeug zum Netz- und Systemmanagement eingesetzt (siehe auch B 4.2 *Netz- und Systemmanagement*), so ist es je nach Produkt möglich, die Windows Protokolldaten direkt in dieses Werkzeug zu importieren. Microsoft Windows ab Version Vista ermöglicht es, auf einem weiteren Windows-System ab Version Vista Ereignisse anderer Windows-Systeme abzurufen.
- Sollte eine zentrale Sammelstelle von Protokolldateien auf Windows Vista oder folgenden Versionen eingesetzt werden, so sind sogenannte *Abonnements* zu konfigurieren. Vor der Erstellung von *Abonnements* müssen jedoch sowohl der *Sammlungscomputer* als auch der *Quellcomputer* für das Senden und Empfangen von Ereignissen entsprechend konfiguriert sein. Die Ereignisse der konfigurierten Abonnements werden auf dem *Sammlungscomputer* unter "Weitergeleitete Ereignisse" angezeigt. Das Abonnement ist eine neue Funktionalität ab Windows Vista.
  In einem Abonnement wird konfiguriert, welche Ereignisse gesammelt werden sollen. In einer Standardinstallation werden die Daten der weitergeleiteten Ereignisse über HTTP übertragen. Der Datentransport per HTTPS ist ebenfalls möglich und sollte gewählt werden.
  Die Client-Systeme ab Windows Vista und Server-Systeme ab Windows Server 2008- müssen konfiguriert werden, damit sie den Fernzugriff auf die entsprechenden Daten ermöglichen. Das kann mit Hilfe des Werkzeugs *winrm* erfolgen. Es sorgt dafür, dass entsprechende Ports in der Windows Firewall geöffnet werden.
  Auf dem System, auf dem die Auswertung durchgeführt wird, müssen Abonnements eingerichtet werden. Das kann unter *Weitergeleitete Ereignisse* | *Eigenschaften* | *Abonnements* konfiguriert werden.
- Einzelne Überwachungsrichtlinien können unter Microsoft Windows ab Version Vista über Gruppenrichtlinien konfiguriert werden. Eine feinere Konfiguration der Überwachung als Ergänzung zu den Gruppenrichtlinien ist mit dem Werkzeug *auditpol.exe* möglich.
- Durch die Überwachung fallen je nach Einstellung große Datenmengen an. Zusätzlich führt eine intensive Überwachung zu Leistungsverlusten. Dadurch kann im Extremfall ein System so überlastet werden, dass ein geregelter Betrieb nicht mehr möglich ist. Aus diesem Grund müssen die geeigneten Überwachungsparameter im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst werden. Es ist zu beachten, dass

die Anpassung auch Einfluss auf das gesamte Überwachungskonzept haben kann, da bestimmte Überwachungsaufgaben nicht mehr durchführbar sind. Dies gilt insbesondere dann, wenn zusätzliche Produkte eingesetzt werden, die hohe Anforderungen an die protokollierten Ereignisse stellen. Dies sind zum Beispiel Programme, die eine automatische Analyse der Protokolldaten auf Verhaltensanomalien, etwa für die Erkennung von Angriffen, durchführen.

Im Rahmen der Überwachung von Systemfunktionen empfiehlt sich auch die regelmäßige Kontrolle der AD-Replikation, mit der Konfigurationsänderungen an die Domänencontroller einer Domäne verteilt werden. Dazu können sowohl AD-Werkzeuge als auch das ADS-Log (Active Directory Service) und das FRS-Log (File Replication Service) auf Fehlermeldungen hin überprüft werden. Fehler in der Replikation haben meist zur Folge, dass Konfigurationsänderungen nicht überall durchgeführt werden. Dadurch besteht die Gefahr, dass einem Benutzer ungeeignete oder zu viele Rechte zugestanden werden.

Die Systemzeit spielt eine wichtige Rolle bei der Systemüberwachung und der Auswertung protokollierter Daten. Insbesondere wenn mehrere Systeme überwacht werden, sollte die Systemzeit auf allen Rechnern synchronisiert werden. Der Dienst *Windows-Zeitgeber* ist für die Zeitsynchronisierung verantwortlich und darf daher nicht deaktiviert werden.

In einer Active Directory-Umgebung kann ein Domänencontroller als Zeitgeber für die Domänenmitglieder genutzt werden. Ein hierarchischer Aufbau des Zeitdienstes von Windows ist möglich.

Die Domänencontroller nutzen den Primären Domänencontroller (PDC) Betriebsmaster oder einen Domänencontroller der übergeordneten Domäne als Zeitquelle. Die PDC-Betriebsmaster nutzen den PDC-Betriebsmaster der übergeordneten Domäne als Zeitquelle. Der PDC der Stammdomäne ist der autorisierende Zeitgeber. Ein Domänencontroller kann mit dem Kommando

*net time /setsntp:<Zeitquelle>*

so konfiguriert werden, dass er eine externe Zeitquelle zum Synchronisieren verwendet. Die Zeitquelle kann sich innerhalb oder außerhalb des eigenen Netzes befinden, wobei eine interne Zeitquelle bevorzugt eingesetzt werden sollte. Wird eine Zeitquelle außerhalb des eigenen Netzes verwendet, muss ihre Vertrauenswürdigkeit sichergestellt sein.

Client-Rechner, die keine Domänenmitglieder sind, benutzen standardmäßig den Microsoft Zeitserver *time.windows.com*. Sie können aber auch mit dem Kommando *net time* konfiguriert werden, dass sie eine andere Zeitquelle verwenden.

Prüffragen:

- Wird die Synchronisierung der Systemzeit mittels einer zuverlässigen Zeitquelle sichergestellt?
- Wurde ein bedarfsgerechtes Überwachungskonzept für IT-Systeme entworfen und umgesetzt?
- Ist die Überwachung in den Gruppenrichtlinien bzw. den lokalen Einstellungen aktiviert worden?
- Wurden Überwachungseinstellungen für wichtige Systemdateien und Registry-Einträge konfiguriert?
- Werden wichtige Systemereignisse protokolliert?
- Werden die Protokolldateien bei Erreichen der Maximalgröße gesichert?

# M 4.345 Schutz vor unerwünschten Informationsabflüssen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Vertrauliche Informationen sollten nicht in die falschen Hände geraten. Um dies zu verhindern, können eine Vielzahl organisatorischer oder technischer Maßnahmen ergriffen werden. Viele davon haben den Nachteil, dass sie die Arbeitsabläufe stark beeinträchtigen oder dass sie zwar einige Schnittstellen nach außen absichern, aber nicht alle.

Eine Lösung, um den Abfluss vertraulicher Informationen besser steuern zu können, sind Tools, die den Datenfluss im Netz und/oder auf Endgeräten kontrollieren. Sie sollen erkennen oder sogar einschreiten, wenn vertrauliche Informationen über unsichere Wege übertragen werden oder in falsche Hände geraten. Solche Tools überprüfen beispielsweise, ob per E-Mail, Datenaustausch oder bei der Internet-Nutzung bestimmte Informationen übermittelt werden sollen oder ob diese auf CD gebrannt oder auf einen USB-Stick kopiert werden sollen. Als Bezeichnungen für solche Tools werden die Begriffe *Data Loss Prevention* (DLP), *Information Leakage Prevention* (ILP) oder auch *Extrusion Prevention* verwendet, die Ziele und Mechanismen sind jedoch vergleichbar.

Solche Systeme unterscheiden zwischen vertraulichen und unkritischen Informationen. Während der Versand unkritischer Dateien per E-Mail erlaubt werden kann, könnte bei vertraulichen Dateien der E-Mail-Versand und das Kopieren auf mobile Datenträger wie USB-Sticks blockiert werden. Einige DLP-Tools können sogar verhindern, dass einzelne Inhalte einer Datei in eine andere Datei kopiert werden.

Derzeit gibt es zwei verschiedene technische Ansätze für DLP-Tools. Die einen versuchen, mit einem Gerät oder einer Appliance im Netz vertrauliche Inhalte im Datenstrom zu erkennen und darauf zu reagieren. Die anderen benötigen auf allen beteiligten Endgeräten einen Agenten, der Bewegungen und die Verarbeitung sensibler Dateien kontrolliert. Analog zum Intrusion-Detection-Bereich spricht man auch bei DLP von netzbasierten und hostbasierten Ansätzen.

### Netzbasierter Ansatz

Bei einem netzbasierten DLP-Tool werden an bestimmten Stellen im Netz Sensoren oder Agenten platziert. Da nur an wenigen Stellen zusätzliche Software installiert werden muss, ist die Einrichtung und der Betrieb einfacher als bei Produkten, die auf jedem beteiligten Endgerät installiert werden müssen. Hierbei werden allerdings nur Datenabflüsse kontrolliert, die über diese Sensoren bzw. Agenten im Netz laufen, nicht aber diejenigen, die über dezentrale Schnittstellen oder mobile Datenträger erfolgen, z. B. über USB-Sticks. Ein weiteres Problem kann die Kontrolle verschlüsselter Informationen sein.

### Hostbasierter Ansatz

Bei hostbasierten DLP-Tools müssen Agenten oder Sensoren auf jedem IT-System installiert werden, das in die Datenfluss-Kontrolle mit einbezogen werden soll. Dies zieht einen höheren Aufwand bei Installation und Betrieb nach sich. Der Vorteil ist dafür, dass das DLP-Tool alle Benutzer-Aktivitäten, die zu Datenabflüssen führen könnten, überwachen kann.

**Konzeptionelles Vorgehen**

Ein ganzheitlicher Schutz vor unerwünschten Informationsabflüssen kann nur erreicht werden, wenn die technischen Maßnahmen mit organisatorischen und personellen Maßnahmen Hand in Hand gehen und diese in den Sicherheitsmanagement-Prozess eingebettet sind. Eine wichtige Grundlage für DLP-Prozesse ist die Klassifizierung aller geschäftsrelevanten Informationen gemäß ihres Schutzbedarfs (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*). Hierauf aufbauend muss geklärt werden, wer diese Informationen unter welchen Rahmenbedingungen bearbeiten, speichern und weitersenden darf und wie diese dabei zu schützen sind.

Für den Einsatz von DLP-Tools muss nicht jede einzelne Datei einzeln klassifiziert sein. Die Tools können typischerweise so konfiguriert werden, dass der Schutzbedarf einer Datei aus ihrem Speicherort (kontextbasiert), bestimmten Strukturmerkmalen oder über deren Inhalte, also über die Suche nach vordefinierten Schlüsselwörtern, abgeleitet wird. Beim kontextbasierten Ansatz ist eine strukturierte Datenhaltung erforderlich, bei der konsequent Dateien mit höherem Schutzbedarf von weniger vertraulichen getrennt werden, z. B. über Verzeichnisstrukturen (siehe M 2.138 *Strukturierte Datenhaltung*).

Vor der Beschaffung eines DLP-Tools sollte der Einsatzzweck genau definiert werden. Bevor ein DLP-Tool in Betrieb genommen wird, muss eine Richtlinie zu dessen Nutzung erstellt werden sowie der Regelsatz festgelegt werden, den das Tool überprüfen soll. Der Einsatz und das Regelwerk sollten sorgfältig geplant und auf die Institution abgestimmt werden. Dabei sollten die Arbeitnehmervertretung und der Datenschutzbeauftragte einbezogen werden. Es empfiehlt sich, die getroffenen Regelungen in einer Betriebsvereinbarung zu fixieren.

Wichtig ist es, nicht überzureagieren. Nach ersten Tests mit DLP-Tools sind die Verantwortlichen meist entsetzt über die vielen potentiellen Schwachstellen, die damit aufgezeigt werden. Die Regeln sollten allerdings nicht zu eng aufgesetzt werden, damit ein vernünftiges Arbeiten noch möglich bleibt.

Die Mitarbeiter sollten darüber informiert werden, dass DLP-Tools eingesetzt werden, was diese Tools prüfen und welche Reaktionen auf Verstöße gegen das Regelwerk vorgesehen sind. Bei Verstößen gegen die definierten Regeln bieten DLP-Tools abgestufte Reaktionsmöglichkeiten, dazu gehören beispielsweise:

- Anzeige eines Hinweis für den Benutzer, dass die geplante Transaktion gegen das Regelwerk verstoßen würde
- Abfrage einer expliziten Zustimmung des Benutzers
- Blockade der Aktion
- Protokollierung
- Information Dritter, z. B. eines Administrators oder Vorgesetzten

Die Erfahrung zeigt, dass die Anzeige von Warnhinweisen sehr wirkungsvoll ist, um die Mitarbeiter für den verantwortungsbewussten Umgang mit vertraulichen Informationen zu sensibilisieren. Zu starke Einschränkungen oder Kontrollen über DLP-Tools können sich negativ auf die Motivation der Mitarbeiter auswirken.

Die Konfiguration des DLP-Tools muss regelmäßig überprüft und optimiert werden und an Änderungen in der Institution, den Geschäftsprozessen und der IT angepasst werden.

Prüffragen:

- Sind die Maßnahmen zum Schutz vor unerwünschten Informationsabflüssen in den Sicherheitsmanagement-Prozess integriert?
- Sind die Maßnahmen zum Schutz vor unerwünschten Informationsabflüssen mit der Arbeitnehmervertretung und dem Datenschutzbeauftragten abgestimmt?
- Ist sichergestellt, dass die Maßnahmen zum Schutz vor unerwünschten Informationsabflüssen mit den Arbeitsabläufen der Mitarbeiter vereinbar sind?
- Sind die Mitarbeiter über den Einsatz, die Regelungen und die möglichen Sanktionen in Bezug auf den Schutz vor unerwünschten Informationsabflüssen informiert?

# M 4.346 Sichere Konfiguration virtueller IT-Systeme

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Virtuelle IT-Systeme (gelegentlich auch als virtuelle Maschinen bezeichnet) sind in erster Linie IT-Systeme. Sie sind daher wie in M 2.392 *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen* beschrieben genauso zu behandeln und zu modellieren wie physische IT-Systeme.

Allerdings gelten für virtuelle IT-Systeme einige Besonderheiten, die beachtet werden müssen.

Virtuellen IT-Systemen muss oft der Zugang zu Geräten, die an den Virtualisierungsserver angeschlossen sind, wie beispielsweise CD- oder DVD-Laufwerke, USB-Dongles, Bandlaufwerke (SCSII) und andere Peripheriegeräte, ermöglicht werden. Dabei können Geräte, die der Virtualisierungsserver den virtuellen IT-Systemen zur Verfügung stellt, häufig über Gastwerkzeuge aus der virtuellen Maschine heraus gesteuert werden. So kann beispielsweise die Netzwerkkarte deaktiviert oder es können Datenträger über das physische in das virtuelle CD-/DVD-Laufwerk oder Diskettenlaufwerk geladen werden.

Bei einigen Virtualisierungssystemen besteht des Weiteren die Möglichkeit, Hauptspeicher oder Festplattenplatz zu überbuchen. Es wird von einer "Überbuchung" von Ressourcen gesprochen, wenn den virtuellen IT-Systemen in Summe mehr Ressourcen zugewiesen werden können, als tatsächlich physisch vorhanden sind. Um Ressourcenengpässen vorzubeugen, können durch die Gastwerkzeuge in virtuellen IT-Systemen Funktionen bereitgestellt werden, um diese Überbuchungsfunktionen zu steuern. Die Gastwerkzeuge des Herstellers VMware (VMware Tools) besitzen beispielsweise eine Funktion, um Hauptspeicher zu belegen, der anderen virtuellen IT-Systemen zur Verfügung gestellt werden kann (Balooning). Diese Werkzeuge können auch eine virtuelle Festplatte für eine Verkleinerung des Dateicontainers, in dem sie enthalten ist, vorbereiten. Hierzu werden alle belegten Blöcke einer virtuellen Festplatte an den Anfang des Containers verschoben und die frei gewordenen Blöcke mit Nullen überschrieben, damit sie von der Virtualisierungsschicht als frei erkannt werden können.

Daher sind bei der Inbetriebnahme von virtuellen IT-Systemen neben den aus dem physischen Serverbetrieb schon bekannten Maßnahmen noch die folgenden Aspekte zu beachten:

- Veränderungen der Binärdateien von Kernel, Anwendungen und Systembibliotheken wirken sich bei der Betriebssystemvirtualisierung im Gegensatz zur Servervirtualisierung auf alle virtuellen IT-Systeme, die auf dem Virtualisierungsserver betrieben werden, sowie auf den Virtualisierungsserver selbst aus. Diese Daten sind auf Veränderungen hin zu überwachen, vor allem, da beispielsweise durch eine Kompromittierung solcher Dateien ein sehr hohes Schadenspotenzial entsteht. Siehe hierzu auch M 4.93 *Regelmäßige Integritätsprüfung*.
- Die Gastwerkzeuge können es Benutzern der virtuellen IT-Systeme ermöglichen, auf Datenträger in Disketten- oder CD-/DVD-Laufwerken des Virtualisierungsservers zuzugreifen. Auch mechanische Vorgänge wie das Öffnen und Schließen der Laufwerksschublade eines physischen Laufwerkes können hierüber gesteuert werden. Es besteht daher die Möglichkeit, dass unberechtigt auf Datenträger in physischen Laufwerken zugegriffen

wird, oder der Datenträger einem virtuellen IT-System entzogen wird, indem das Laufwerk von einem anderen virtuellen System aus geöffnet wird. Die virtuellen IT-Systeme und der Virtualisierungsserver müssen so konfiguriert sein, dass dies weitgehend ausgeschlossen ist. Am einfachsten kann dies geschehen, wenn den virtuellen IT-Systemen diese Geräte nur dann exklusiv zugeordnet werden, wenn sie aktuell benötigt werden. Werden sie nicht gebraucht, sollte die Verbindung zu diesen Geräten getrennt werden. Besteht die Möglichkeit, CD- oder DVD-Datenträger als Imagedateien (ISO-Images) statt über physische Laufwerke bereitzustellen, sollte sie genutzt werden.

- Funktionen, die die Überbuchung von Hauptspeicher oder Festplattenplatz ermöglichen, sind bei den virtuellen IT-Systemen zu deaktivieren, bei denen hohe Performanceanforderungen bestehen oder deren Datenintegrität besonders wichtig ist. Ressourcenengpässe bei einer Überbuchung von Hauptspeicher auf einem Virtualisierungsserver führen in der Regel zu starken Performanceeinbußen der davon betroffenen virtuellen IT-Systeme. Wird Festplattenplatz überbucht und reicht der physisch vorhandene Platz nicht mehr aus, werden durch den Virtualisierungsserver in der Regel keine weiteren Schreibzugriffe auf den überbuchten Speicherplatz zugelassen. Hierdurch treten in den virtuellen IT-Systemen Festplattenfehler auf, die zu Inkonsistenzen der abgespeicherten Daten führen können.
- Die Vorbereitung von virtuellen Festplatten auf eine Verkleinerung ihres physischen Containers bedeutet eine starke Belastung der Massenspeicher der Virtualisierungsserver. Dies kann zu Einschränkungen der Performance aller virtuellen IT-Systeme führen, die auf dem Virtualisierungsserver ausgeführt werden. Greifen mehrere Virtualisierungsserver auf ein Speichernetz zu, können unter Umständen alle Virtualisierungsserver davon betroffen sein. Daher sollte diese Funktion deaktiviert werden, wenn sie nicht benötigt wird.
- Die Deaktivierung von Geräten wie Netzwerkkarten über Gastwerkzeuge bildet ein virtuelles Äquivalent zur Entfernung des Netzwerkkabels eines physischen IT-Systems. Da dies in virtualisierten Umgebungen auch oft ohne Zutritt zu diesem System möglich ist, sollte diese Funktion deaktiviert werden. Sie sollte nur dann zeitweise aktiviert werden, wenn sie zwingend benötigt wird.

Einige der oben beschriebenen Funktionen werden über Gastwerkzeuge, die in den virtuellen IT-Systemen installiert werden können, gesteuert oder ermöglicht. Es sind daher verbindliche Regelungen zur Konfiguration und zum Einsatz dieser Gastwerkzeuge in virtuellen IT-Systemen zu erstellen.

Prüffragen:

- Ist bei Umgebungen mit Betriebssystemvirtualisierungen die Integrität von Daten des Betriebssystemkerns, der Systembibliotheken und gemeinsam genutzten Anwendungen gewährleistet?
- Sind verbindliche Regelungen zum Einsatz von Gastwerkzeugen in virtuellen IT-Systemen getroffen und umgesetzt worden?
- Werden Geräte wie CD-Laufwerke nur dann mit einem virtuellen IT-Systemen exklusiv verbunden, wenn sie im betreffenden IT-System benötigt werden?
- Sind für virtuelle IT-Systeme bei denen hohe Performanceanforderungen bestehen oder ein hoher Schutzbedarf bezüglich Integrität festgestellt worden ist, Überbuchungsfunktionen für Hauptspeicher oder Festplattenplatz deaktiviert?

- Ist die Funktion, mit der Geräte wie Netzwerkkarten oder CD-/DVD-Laufwerke über die Gastwerkzeuge aktiviert oder deaktiviert werden können, standardmäßig ausgeschaltet?

# M 4.347 Deaktivierung von Snapshots virtueller IT-Systeme

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Die Möglichkeit, den Zustand virtueller IT-Systeme zu einem bestimmten Zeitpunkt im laufenden Betrieb einzufrieren und diesen Zustand beliebig lang zu konservieren, in dem er beispielsweise auf auf eine Festplatte abgespeichert wird, ist eine technische Besonderheit virtueller IT-Systeme. Kann ein solcher Zustand abgespeichert und das System danach weiter fortgesetzt werden, besteht auch die Möglichkeit, das System wieder auf den abgespeicherten Zustand zurückzusetzen. Ein solcher Zustand wird bei den meisten Virtualisierungsprodukten "Snapshot" genannt. Dieses Verfahren kann für vielfältige Administrationstätigkeiten eingesetzt werden. So kann zum Beispiel nach einem fehlgeschlagenen *Update* auf einfache Weise ein *Downgrade* auf die vorherige Version durchgeführt werden. Auch elementare Funktionen einer virtuellen Infrastruktur, wie die Migration von Gastsystemen zwischen Virtualisierungsservern über *LiveMigration*, *vMotion* oder *XenMotion*, basieren auf der Fähigkeit, Snapshots zu erzeugen. Dies betrifft in der Folge auch die daran gekoppelten Hochverfügbarkeitsmechanismen.

Daher sind beim Einsatz solcher Snapshots die folgenden Aspekte zu beachten:

**Schutz der Vertraulichkeit und Integrität bei gefährdeten Gästen**

In einer virtuellen Infrastruktur können bestimmte IT-Systeme einem hohen oder sehr hohen Schutzbedarf in Bezug auf die Vertraulichkeit oder Datenintegrität unterliegen. Daten eines Prozesses werden häufig in voneinander abgeschotteten Hauptspeicherbereichen verarbeitet, so dass andere Prozesse auf einem IT-System nicht darauf zugreifen und die Daten lesen oder verändern können. Hierdurch bleibt die Vertraulichkeit und Integrität dieser Daten während der Verarbeitung im Hauptspeicher eines (virtuellen) IT-Systems gewahrt. Wird nun ein beliebiger Zustand des virtuellen IT-Systems eingefroren, um das System zu einem späteren Zeitpunkt wieder in diesen Zustand zu versetzen, werden die Arbeitsspeicherdaten auf einen Massenspeicher des Virtualisierungsservers geschrieben. Der Zugriffsschutz, den das Betriebssystem des virtuellen IT-Systems für die Daten der einzelnen Prozesse gewährt, kann nun durch einen Angreifer umgangen werden, indem er die Datei analysiert, in der die Arbeitsspeicherdaten enthalten sind.

Das folgende Beispiel soll dies verdeutlichen: Ein virtuelles IT-System ist mit einer Festplattenverschlüsselung ausgestattet, um die Vertraulichkeit und Integrität der gespeicherten Daten zu gewährleisten. Da der Hauptspeicherinhalt der virtuellen Maschine beim Erzeugen des Snapshots ausgelesen und auf einer Festplatte des Virtualisierungsservers gespeichert wird, können dabei die kryptographischen Schlüssel der Festplattenverschlüsselungssoftware in unverschlüsselter Form auf die Festplatte geschrieben werden. Das gleiche passiert im Übrigen, wenn das System über die Virtualisierungssoftware nur angehalten und der Zustand für eine spätere Fortsetzung des Betriebs auf die Festplatte geschrieben wird. Aus der Datei mit dem abgespeicherten Hauptspeicherinhalt lässt sich dann möglicherweise der Schlüssel zur Entschlüsselung des Festplatteninhaltes herauslesen.

Dies zeigt, dass Maßnahmen zur Sicherung der Vertraulichkeit und Integrität von physischen IT-Systemen bei virtuellen IT-Systemen häufig nur noch eine eingeschränkte Wirksamkeit haben. Sie können möglicherweise mit Mitteln der Virtualisierungsserver umgangen werden. Um die Offline-Analyse eines Snapshots eines virtuellen IT-Systems mit hohem Schutzbedarf zu erschweren, sollte daher überlegt werden, für solche Systeme die Möglichkeit, Snapshots zu erzeugen oder das System einzufrieren, zu deaktivieren. In diesem Fall ist zu prüfen, ob die eventuell eingesetzten Snapshot-basierten Datensicherungsverfahren weiterhin funktionieren.

**Beständigkeit von Datenveränderungen**

Snapshots eines virtuellen IT-Systems enthalten den kompletten Zustand des IT-Systems inklusive aller abgelegten Daten zum Zeitpunkt seiner Erzeugung. Wenn ein virtuelles IT-System mittels eines Snapshots auf einen früheren Stand zurückgesetzt wird, können hierdurch Veränderungen an Daten zurückgenommen werden. Beispiele hierfür sind der Datenbestand eines Dateiservers oder Struktur und Inhalt eines Verzeichnisdienstes wie Active Directory.

Für ein virtuelles IT-System, das auf keinen Fall auf einen früheren Stand zurückgesetzt werden darf, muss ebenfalls die Option, Snapshots zu erzeugen, deaktiviert werden.

Falls auf die Funktionalität von Snapshots nicht verzichtet werden kann, sollte der Umfang des Snapshots eingegrenzt werden, in dem beispielsweise nur bestimmte Laufwerke vom Snapshot erfasst werden, oder die Arbeitsschritte jeweils bevor und nachdem ein Snapshot erzeugt oder zurückgespielt wurde, spezifiziert werden. Wird beispielsweise ein Active Directory Domaincontroller auf einen Snapshot zurückgesetzt, sind Maßnahmen zur Wiederherstellung seiner Active Directory-Datenbank durchzuführen, da diese sonst inkonsistente Daten enthält.

Der Umfang der eingegrenzten Snapshots und die notwendigen Arbeitsschritte sind zu dokumentieren.

Prüffragen:

- Ist gewährleistet, dass für alle virtuellen IT-Systeme mit nicht deaktivierter Snapshot-Funktionalität die Umfänge der Snapshots sowie die darüber hinaus für den Umgang mit Snapshots notwendigen Arbeitsschritte evaluiert und dokumentiert sind?
- Ist die Möglichkeit, Snapshots zu erzeugen oder das System einzufrieren, für virtuelle IT-Systeme deaktiviert worden, bei denen Gefährdungen der Integrität oder Vertraulichkeit besonderes schwerwiegende Konsequenzen haben?

# M 4.348 Zeitsynchronisation in virtuellen IT-Systemen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Viele Anwendungen benötigen eine korrekte Systemzeit, um einwandfrei zu funktionieren. Dies beginnt schon bei Dateiservern damit, dass die auf ihm gespeicherten Dateien mit einem Zeitstempel versehen werden. Andere Systeme verwenden die Systemzeit auf unterschiedliche Weise. Bestimmte Authentisierungssysteme wie Kerberos oder auch tokenbasierte Systeme benötigen eine korrekte Systemzeit, um störungsfrei zu arbeiten. Monitoringsysteme wie beispielsweise *mrtg* nutzen die Systemzeit üblicherweise als Index für ihre in einer Datenbank abgelegten Aufzeichnungen.

Aus diesen Gründen muss darauf geachtet werden, dass auch die Systemzeit eines virtuellen IT-Systems stets korrekt voranschreitet. Bei Virtualisierungsprodukten, die auf einer vollständigen Servervirtualisierung beruhen, ist dies häufig nicht ohne Weiteres gewährleistet.

**Die Berechnung der Systemzeit durch Taktzählung**

Moderne Betriebssysteme ermitteln die Systemzeit nicht, indem die Systemuhr ständig ausgelesen wird, sondern indem Prozessorzyklen gezählt und diese Zyklen mit einer externen Zeitquelle verglichen werden. Diese externe Zeitquelle kann ein Zeitserver oder auch eine Hardware-Uhr sein. Der Grund für diese auf den ersten Blick umständliche Zeitermittlungsmethode ist, dass für moderne Prozessoren eine Zeitquelle benötigt wird, die eine höhere Auflösung als die meisten Uhren besitzt. Diese Auflösung muss im Bereich des Taktes eines modernen Prozessors liegen. Durch ständigen Vergleich der Prozessorzyklen mit der verlässlichen Zeitquelle wird ein Umrechungsfaktor gebildet, der es erlaubt, die Prozessorzyklen in die Zeit umzuwandeln. In bestimmten Zeitabständen wird dieser Umrechnungsfaktor durch Vergleich der vergangenen Zyklen mit der Zeitquelle korrigiert, um eine etwaige Ungenauigkeit in der Berechnung auszugleichen.

Die meisten Produkte für eine Servervirtualisierung ordnen den virtuellen IT-Systemen und damit den virtuellen Prozessoren abhängig von deren Last dynamisch Prozessorzyklen zu. Daher läuft der Zähler für die Prozessorzyklen aus Sicht der virtuellen Maschine mit unterschiedlichen Geschwindigkeiten. Der Algorithmus zur Zeitbestimmung und -korrektur ermittelt damit bei jedem Durchlauf andere Werte, was dazu führt, dass auch die Systemzeit in einem virtuellen IT-System scheinbar mit unterschiedlichen Geschwindigkeiten voranschreitet. Dadurch kann es in virtuellen IT-Systemen durchaus zu Abweichungen von mehreren Minuten kommen, sodass in Extremfällen die Zähler überkorrigiert werden und die Systemzeit des virtuellen IT-Systems zum Teil scheinbar rückwärts läuft.

Normalerweise läuft die Systemuhr in virtuellen IT-Systemen, die eine gleichmäßige Prozessorauslastung haben, mit ausreichender Genauigkeit. Hierbei ist es belanglos, ob die Auslastung hoch oder niedrig ist, entscheidend ist die Gleichmäßigkeit. Bei Systemen mit zeitweise hoher und zeitweise niedriger Auslastung kommt es zu den bereits beschriebenen Effekten. Hierbei verhalten sich die Betriebssysteme abhängig von ihrer Konfiguration sehr unterschiedlich.

**Korrekturmethoden und deren Grenzen**

Die meisten Virtualisierungsprodukte besitzen einen Mechanismus, um die Systemzeit in den virtuellen IT-Systemen zu korrigieren. Dies wird häufig über eine Funktion der Gastwerkzeuge realisiert. Die Produkte der Hersteller Citrix und VMware beispielsweise beinhalten eine Funktion zur Synchronisierung der Systemzeit der virtuellen IT-Systeme mit der Systemzeit des Virtualisierungsservers.

Diese Mechanismen sind allerdings nicht immer für die in einem virtuellen IT-System betriebenen Anwendungen ausreichend, da sie in der Regel nicht auf alle Timer eines Betriebssystems wirken, sondern nur auf die so genannte Time of Day Clock. Zudem erfolgt die Synchronisierung nicht ständig, sondern in bestimmten Abständen. Diese Abstände liegen meist im Bereich von einigen wenigen Bruchteilen von Sekunden, sind aber für eine genaue Zeitanpassung häufig zu groß.

Dieser Aspekt ist beim Betrieb von Anwendungen in virtuellen IT-Systemen zu beachten. Die Anwendungen müssen entweder mit einer ungleichmäßig laufenden Systemuhr auskommen können oder es müssen Konfigurationsänderungen am Virtualisierungsserver oder dem virtuellen IT-System vorgenommen werden, die die Genauigkeit der Systemuhr der virtuellen IT-Systeme steigern.

Solche Konfigurationsänderungen bestehen darin, die Abfrage einer externen Zeitquelle häufiger durchzuführen, als dies standardmäßig der Fall ist. Dies kann über die Gastwerkzeuge geschehen, wenn diese eine entsprechende Konfigurationsmöglichkeit besitzen. Es ist aber auch möglich, dass betreffende virtuelle IT-System so einzurichten, dass es beispielsweise öfter einen NTP-Server abfragt und dadurch seine Systemuhr korrigiert. Hierdurch werden die Intervalle kleiner, in denen die Uhr mit einer falschen Geschwindigkeit läuft und der Umrechnungsfaktor für die Prozessorzyklen wird schneller angepasst. In der Regel ist es nicht sinnvoll, diese beiden Möglichkeiten miteinander zu kombinieren, da ansonsten mit geringen Performanceverlusten gerechnet werden muss. Für Unix-Betriebssysteme müssen häufig auf die Virtualisierung abgestimmte Kernel verwendet werden. Hier sind in Abhängigkeit von den eingesetzten Unix-Derivaten z. B. im Bootloader entsprechende Parameter zu setzen. Unter Umständen muss ein solcher Kernel auch dediziert erzeugt (selbst kompiliert) werden.

Prinzipiell sollte ein Vorgehen etabliert werden, welches sicherstellt, dass Probleme mit der Synchronizität der Systemzeit erkannt und beseitigt werden können, bevor die virtuellen Systeme ausgerollt werden. Während des Pilotbetriebs eines neuen virtuellen IT-Systems ist die Systemzeit des Systems verstärkt zu überwachen. Dabei ist zu ermitteln, ob die interne Uhr des virtuellen IT-Systems von der tatsächlichen Zeit abweicht. In diesem Fall muss geprüft werden, ob sich dies nachteilig auf die im virtuellen IT-System betriebene Applikation auswirkt, gegebenenfalls sind Korrekturmaßnahmen durchzuführen. Der Erfolg der Korrekturmaßnahmen ist im weiteren Pilotbetrieb und auch nach der Überführung in den Produktivbetrieb zu prüfen.

Prüffragen:

- Sind die Einflüsse der Virtualisierung auf die Systemzeit bei der Virtualisierung eines bestimmten IT-Systems oder einer bestimmten Anwendung hinreichend bedacht worden?

- Wurden die Anwendungen der virtuellen IT-Systeme auf Probleme mit unregelmäßig laufender Systemzeit geprüft?
- Ist ein allgemeines Konzept entwickelt worden, wie eine ausreichende Synchronizität der Systemzeit in den virtuellen IT-Systemen gewährleistet wird?

# M 4.349 Sicherer Betrieb von virtuellen Infrastrukturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auf Virtualisierungsservern werden in der Regel mehrere virtuelle IT-Systeme betrieben. Da die einzelnen virtuellen IT-Systeme allesamt von dieser Infrastruktur abhängen, kann ein Fehler auf einem Infrastruktursystem wie einem Virtualisierungsserver Auswirkungen auf sämtliche auf diesem System betriebenen virtuellen IT-Systeme haben.

Im Folgenden werden einige Hinweise gegeben, die für den sicheren Betrieb der Virtualisierungsserver bzw. der virtuellen Infrastruktur beachtet werden sollten. Empfehlungen bezüglich des Virtualisierungsservers selbst, die nicht den Aspekt der Virtualisierung betreffen und zu den Grundsätzen des Serverbetriebs gehören, sind in den Maßnahmen des Bausteins B 3.101 *Allgemeiner Server* beschrieben.

**Administrationszugänge**

Virtualisierungsserver besitzen Funktionen, um die auf ihnen betriebenen virtuellen IT-Systeme zu steuern, warten und überwachen. Diese Verwaltungsfunktionen können in der Regel entweder lokal auf dem Virtualisierungsserver selbst oder über das Netz von der Arbeitsstation eines Administrators aus genutzt werden. Dazu werden entweder webbasierte Administrationsoberflächen auf dem Virtualisierungsserver oder eine spezielle Administrationssoftware wie z. B. *VMware vSphere Client* bereitgestellt.

Weiterhin besteht bei einigen Virtualisierungslösungen die Möglichkeit, mehrere Virtualisierungsserver sowie alle darauf betriebenen virtuellen IT-Systeme von einem zentralen System aus zu verwalten (z. B. *Citrix XenCenter, Microsoft System Center Virtual Machine Manager, SUN Management Center, VMware vCenter*).

Die entsprechenden Netzschnittstellen der Virtualisierungsserver bzw. des zentralen Verwaltungssystems ermöglichen einen vollständigen Zugriff auf die Virtualisierungsserver und die virtuellen IT-Systeme. Aus diesem Grund müssen die Administrationsschnittstellen abgesichert werden. Hierzu ist auch die Maßnahme M 5.154 *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen* zu berücksichtigen.

**Überwachung des Betriebszustands**

Die Administratoren der virtuellen Infrastruktur sollten in regelmäßigen Abständen entsprechend der Sicherheitsrichtlinien (siehe M 2.477 *Planung einer virtuellen Infrastruktur*) Überwachungstätigkeiten ausführen. Hierzu gehört:

- das Anlegen, Löschen von Snapshots.
- die Überwachung des Betriebszustandes der Virtualisierungsserver und der virtuellen IT-Systeme.
- die Prüfung der Auslastung von Ressourcen.
- die Prüfung, ob ausreichend Prozessorressourcen zur Verfügung stehen, um die Performance-Anforderungen der virtuellen IT-Systeme zu befriedigen.
- die Prüfung, ob Hauptspeicherengpässe bestehen, die die Verfügbarkeit der virtuellen IT-Systeme gefährden.

- die Prüfung, ob ausreichend Massenspeicher (Festplattenplatz bzw. zugeordnete und Gesamtkapazität im Speichernetz) zur Verfügung steht.
- die Prüfung, ob es Engpässe bei der Netzbandbreite gibt.
- die Prüfung der Verbindungen zu den physikalischen Netzen.
- der Integritätscheck der Konfiguration der Virtualisierungsserver und der virtuellen IT-Systeme (siehe auch M 2.449 *Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme*, M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*)

Insbesondere dann, wenn die von einigen Virtualisierungsprodukten gebotene Möglichkeit zur Überbuchung von Hauptspeicher und Festplattenplatz genutzt wird, muss ein ständiger Prozess zur Überwachung dieser Ressourcen etabliert werden. Geschieht dies nicht, drohen im Fall von zu stark überbuchtem Hauptspeicher massive Performanceverluste. Wenn ein Engpass bezüglich des Festplattenplatzes entsteht, können alle davon betroffenen IT-Systeme gleichzeitig ausfallen. Wenn Snapshots verwendet werden, sollte die Auslastung des Massenspeichers ebenfalls sorgfältig beobachtet werden, da Snapshotdateien in der Regel dynamisch wachsen.

Die in regelmäßigen Abständen durchzuführenden Überwachungsaufgaben können in vielen Fällen automatisiert werden (z. B. E-Mail-Benachrichtigung etc.).

**Tests von Konfigurationsänderungen**

Von Konfigurationsänderungen auf den Virtualisierungsservern können viele IT-Systeme betroffen sein. Fehler hierbei können dazu führen, dass alle IT-Systeme auf diesen Virtualisierungsservern nicht mehr starten können oder die Verbindung zu von ihr benötigten Ressourcen verliert. Wird die Konfiguration auf Virtualisierungsservern geändert, so muss diese Änderung auf technische Korrektheit überprüft werden, bevor sie aktiviert wird. Dies kann z. B. in einer Testumgebung oder mittels Vier-Augen-Prinzip erfolgen.

Prüffragen:

- Besteht ein abgesicherter Zugang zu den administrativen Schnittstellen der virtuellen Infrastruktur?
- Werden regelmäßige Überwachungsaufgaben bezüglich der virtuellen Infrastruktur durchgeführt?
- Werden Konfigurationsänderungen an der Virtualisierungsinfrastruktur vor der Umsetzung geprüft?

# M 4.350 Sichere Grundkonfiguration eines DNS-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

DNS-Server stellen attraktive Ziele für Angreifer dar. Durch die Manipulation von DNS-Servern können alle Dienste beeinflusst werden, die DNS verwenden. Zum Beispiel können durch die Manipulation von Domain-Informationen Webserver, E-Mail-Server, Remote-Administrationsanwendungen oder Ähnliches beeinflusst werden. Aus diesem Grund ist eine sorgfältige Konfiguration der DNS-Server unerlässlich.

### Rechteeinschränkung

Ein DNS-Server-Prozess sollte nur mit den minimal notwendigen Rechten ausgestattet werden, um die potenziellen Auswirkungen im Fall eines erfolgreichen Angriffs auf den Prozess gering zu halten. Falls es technisch möglich ist, sollten für den DNS-Server-Prozess ein eigener Benutzer und eine eigene Gruppe angelegt werden. Der Benutzer erhält nur Rechte auf die benötigten Dateien. Wird der DNS-Server automatisch beim Systemstart mitgestartet, muss der automatisierte Aufruf so gestaltet werden, dass der DNS-Server-Prozess mit dem für ihn vorgesehenen Benutzer und der vorgesehenen Gruppe startet.

### DNS-Server-Version

Die Version des verwendeten DNS-Server-Produktes kann einem Angreifer wertvolle Informationen liefern. Unter http://www.isc.org/sw/bind/bind-security.php können beispielsweise alle bisher publizierten Schwachstellen im DNS-Server-Produkt BIND nachgelesen werden. Aus diesem Grund sollte die Versionsnummer verborgen werden, beispielsweise indem sie durch "unknown" ersetzt wird. Diese Maßnahme erhöht zwar nicht direkt das Sicherheitsniveau eines DNS-Servers, erschwert einem Angreifer aber die Informationsbeschaffung.

### Anfragen

Eine erhöhte Gefahr durch Cache-Poisoning-Angriffe besteht dann, wenn DNS-Server Anfragen bedingungslos akzeptieren. Daher ist es wichtig einzuschränken, welche Anfragen akzeptiert werden.

Resolving DNS-Server sind für Anfragen von Resolvern aus dem Netz der Institution zuständig, in der Regel handelt es sich dabei um rekursive Anfragen. Das bedeutet, dass Resolving DNS-Server rekursive Anfragen aus dem internen Netz akzeptieren müssen. Anfragen mit Ursprung aus dem Internet sollten nicht akzeptiert werden, da hierfür der Advertising DNS-Server zuständig ist.

Anfragen mit Ursprung aus dem Internet sollten immer iterativ behandelt werden, dadurch liefert der Advertising DNS-Server nur Informationen über seine verwalteten Zonen und kann keine gefälschten Antworten versenden.

Um das Sicherheitsniveau von Resolving DNS-Servern zu erhöhen, sollte ein weiterer Mechanismus eingesetzt werden. Wie bereits erwähnt, müssen Resolving DNS-Server rekursive Anfragen von institutionsinternen IT-Systemen akzeptieren. Resolving DNS-Server werden also zwangsläufig Namen auflösen müssen, für die sie nicht autoritativ sind. Ein Angreifer könnte hier ge-

fälschte Antworten einschleusen. Die Zuordnung von Antworten zu Anfragen erfolgt über:

- IP-Adresse
- ID der Anfrage (Zufallszahl)
- Source Port der Anfrage

Da IP-Adresse und ID zu wenig Schutz bieten, sollten zusätzlich zufällige Source Ports beim Versenden von Anfragen verwendet werden. Aktuell wird auch dazu übergegangen, mehrere IP-Adressen für Resolving DNS-Server zu konfigurieren und diese zu randomisieren.

**Zonentransfers**

Grund und Ziel von Zonentransfers ist die Synchronisation zwischen dem Primary DNS-Server und dem oder den Secondary DNS-Servern. Der Primary DNS-Server liest die Domain-Informationen aus den Zonendateien aus, über einen Zonentransfer gelangen diese auf den oder die Secondary DNS-Server und werden somit synchron gehalten. Zonentransfers sollten nur zwischen dem Primary DNS-Server und den Secondary DNS-Servern einer Domain möglich sein, siehe dazu M 4.351 *Absicherung von Zonentransfers*.

**Ausschließen bestimmter DNS-Server**

Sind DNS-Server bekannt, die falsche Domain-Informationen liefern, muss man seine Resolving DNS-Server daran hindern, Anfragen an diese DNS-Server zu senden.

Werden private IP-Netze wie 10/8, 172.16/12 und 192.168/16 in der Institution nicht genutzt, sollten aus Sicherheitsgründen Anfragen aus diesen Netzen ignoriert werden.

Prüffragen:

- Sind die Rechte des DNS-Server Prozesses auf das notwendige Minimum beschränkt?
- Dürfen nur berechtigte Hosts rekursive DNS-Anfragen stellen?
- Sind Zonentransfers nur zwischen Primary und Secondary DNS-Server möglich?

# M 4.351 Absicherung von Zonentransfers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Zonentransfer synchronisiert die Domain-Informationen zwischen einem Primary DNS-Server und einem oder mehreren Secondary DNS-Servern. Der Primary DNS-Server liest die Domain-Informationen aus den Master Files aus und über Zonentransfers gelangen diese auf den oder die Secondary DNS-Server. Bei einem Zonentransfer sollten zwei Sicherheitsaspekte beachtet werden:

- Es muss sicher gestellt werden, dass der Zonentransfer zwischen dem Primary und dem Secondary DNS-Server auch wirklich funktioniert, und
- Es dürfen keine unerlaubten Zonentransfers möglich sein.

Um die Funktionsfähigkeit eines Zonentransfers zu gewährleisten, sollte nach jeder Änderung an den Einstellungen für den Zonentransfer die einwandfreie Funktionalität überprüft werden. Dazu kann beispielsweise ein Zonentransfer durchgeführt werden. Danach wird in den Logdateien überprüft, ob Fehler aufgetreten sind. Bei nicht allzu umfangreichen Zonen besteht die Möglichkeit, die vom Primary DNS-Server verwalteten Domain-Informationen händisch mit denen des Secondary DNS-Servers zu vergleichen.

Um zu verhindern, dass unberechtigte Personen einen Zonentransfer starten und somit die gesamten Domain-Informationen einer Zone erhalten, müssen Zonentransfers so konfiguriert werden, dass diese nur zwischen Primary und Secondary DNS-Servern möglich sind. Dies muss zumindest über die Beschränkung auf die IP-Adressen der DNS-Server erfolgen, noch sicherer ist es Transaction Signatures (TSIG) zu verwenden. Die Einschränkungen über IP-Adressen sehen wie folgt aus: Am Primary DNS-Server muss für jede Zone konfiguriert werden, welches die dazu gehörenden Secondary DNS-Server sind. Dies erfolgt über die Angabe von einer oder mehreren IP-Adresse(n). Auf dem oder den Secondary DNS-Server(n) für eine Zone muss konfiguriert werden, welcher der dafür zuständige Primary DNS-Server ist.

Die Absicherung von Zonentransfers über TSIG bietet ein höheres Sicherheitsniveau. Bei TSIG werden auf dem Primary DNS-Server und dem oder den Secondary DNS-Server(n) symmetrische Schlüssel definiert. Wird ein Zonentransfer gestartet, erzeugt TSIG aus den Binärdaten der Anfrage mithilfe des symmetrischen Schlüssels und einer Hashfunktion einen Hash Message Authentication Code (HMAC). Der HMAC wird der Anfrage beigefügt. Der Secondary DNS-Server, der den Schlüssel ebenfalls kennt, berechnet den HMAC eigenständig. Stimmen erhaltener und berechneter HMAC überein, wird der Zonentransfer durchgeführt, ansonsten wird dieser abgelehnt. Diese Methode schützt im Gegensatz zur IP-Adressen-basierten Absicherung auch gegen IP-Spoofing. Bei TSIG ist jedoch zu beachten, dass nicht jedes DNS-Server-Produkt diese Funktionalität zur Verfügung stellt oder möglicherweise vom Standard abweichend implementiert hat.

Prüffragen:

- Sind DNS-Zonentransfers funktionstüchtig?
- Sind DNS-Zonentransfers nur zwischen dem Primary und dem oder den Secondary DNS-Server(n) einer Zone erlaubt?

# M 4.352 Absicherung von dynamischen DNS-Updates

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um dynamische Updates sicher nutzen zu können, muss gewährleistet sein, dass nur legitimierte IT-Systeme Änderungen an Domain-Informationen vornehmen können. Des Weiteren muss festgelegt werden, welche Domain-Informationen die einzelnen IT-Systeme ändern dürfen. Um sicherzustellen, dass Domain-Informationen nicht von unautorisierten IT-Systemen mit Hilfe von dynamischen Updates manipuliert werden, stehen zwei Möglichkeiten zur Verfügung:

- Beschränkung der berechtigten Hosts durch IP-Adressen
- Beschränkung der berechtigten Hosts mit Hilfe von TSIG

Bei der Beschränkung mittels IP-Adresse wird über die IP-Adresse die Quelle des dynamischen Updates identifiziert. Bei TSIG wird symmetrische Verschlüsselung benutzt, um die Quelle des dynamischen Updates zu identifizieren, siehe hierzu M 4.351 *Absicherung von Zonentransfers*.

Neben der Anfälligkeit für IP-Spoofing gibt es bei der Verwendung von IP-Adressen ein weiteres Problem. Secondary DNS-Server können als Forwarder für dynamische Updates eingerichtet und der Primary DNS-Server so konfiguriert werden, dass er nur Updates von den Secondary DNS-Servern akzeptiert. Weil nur auf den Secondary DNS-Servern konfiguriert wird, von welchen IT-Systemen Updates akzeptieren werden, bleibt es dem Primary DNS-Server verborgen, woher die Updates stammen. Somit ist es nicht möglich, aufgrund der originalen Quelle einzuschränken, welche Hosts dynamische DNS-Updates vornehmen dürfen.

Neben der Identifikation der Quelle muss konfiguriert werden, welche Domain-Informationen verändert werden dürfen. Die Regeln sollten so konfiguriert werden , dass ein reibungsloser Einsatz von dynamischen Updates möglich ist. Ein DHCP-Server benötigt beispielsweise die Berechtigung, die Zuordnung von Domainnamen und IP-Adressen zu ändern, jedoch besteht kein Grund einem DHCP-Server zu erlauben, den zuständigen DNS-Server für eine Zone zu ändern.

Prüffragen:

- Wurden dynamische DNS-Updates auf berechtige Hosts eingeschränkt?
- Wurde festgelegt, welche Domain-Informationen die berechtigten Hosts im Einzelnen ändern dürfen?

# M 4.353 Einsatz von DNSSEC

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

DNS Security Extensions (DNSSEC) ist noch nicht weit verbreitet, trotz konzeptioneller Schwachstellen im DNS-Protokoll und Schwächen in der DNS-Software. Dies wurde beispielsweise durch die im Sommer 2008 aufgezeigte Designschwäche im DNS-Protokoll wieder deutlich. Dieser Designfehler bewirkt, dass Cache-Poisoning Angriffe (und dadurch weitere Angriffsmethoden) erheblich erleichtert werden. Kurzfristig kann diese Designschwäche umgangen werden, indem bei Anfragen kryptografisch starke Zufallszahlen als ID und ein zufälliger Source Port verwendet werden. Auf lange Sicht lassen sich Probleme und Krisen wie diese nur durch DNSSEC bewältigen. DNSSEC wurde speziell entwickelt, um DNS gegen eine Großzahl von Angriffen zu schützen, darunter auch Cache-Poisoning Angriffe.

Realisiert wird dies durch asymmetrische Kryptografie, daher muss im Zusammenhang mit dieser Maßnahme auch die Maßnahme M 2.46 *Geeignetes Schlüsselmanagement* realisiert werden.

Bei DNSSEC werden die gesamten Zoneninformationen mit einem privaten Schlüssel signiert. Diese Signaturen können mithilfe des zugehörigen öffentlichen Schlüssels geprüft werden. Das Schlüsselpaar wird als Zone-Signing-Key (ZSK) bezeichnet. Stellt ein DNSSEC unterstützender Resolver eine Anfrage an einen DNS-Server, auf dem DNSSEC konfiguriert ist, sendet der Server als Antwort die Domain-Informationen mit den Signaturen zurück. Der Resolver kann die Richtigkeit der Domain-Informationen mithilfe der Signatur und dem öffentlichen Schlüssel überprüfen.

Um die Authentizität des ZSK sicher zustellen, wird dieser mit Hilfe von Key-Signing-Keys (KSK) signiert. Ein Hashwert des öffentlichen Teils des KSK wird der übergeordneten Domain übermittelt. Die übergeordnete Domain signiert mithilfe ihrer Schlüssel den Hashwert und bestätigt die Authentizität des Hashwertes. Somit entsteht eine Vertrauenskette ("Chain-of-Trust"). Setzt die übergeordnete Domain DNSSEC nicht ein, besitzt diese keine Schlüssel und kann keine Signatur erstellen, um die Authentizität der KSK zu bestätigen. Man kann jedoch seine DNS-Server anweisen, den eigenen Schlüsseln zu vertrauen, somit entstehen Vertrauensinseln ("Island-of-Trust"). Mit höherem Verbreitungsgrad von DNSSEC werden diese Vertrauensinseln größer und somit das Sicherheitsniveau höher. DNSSEC bietet folgende Sicherheitsmechanismen:

- Die Quelle der DNS-Informationen wird authentisiert.
- Die Integrität der Domain-Informationen wird sichergestellt, somit können Domain-Informationen nicht mehr manipuliert werden, da die Signatur diese Manipulation sichtbar macht. Kunden können beispielsweise sicher sein, mit dem richtigen Webserver, Mailserver, etc. zu kommunizieren.
- Existiert ein Domainname nicht, wird eine authentisierte Fehlermeldung gesendet.

Die Schlüssel ZSK und KSK müssen wie in Maßnahme M 2.46 *Geeignetes Schlüsselmanagement* beschrieben sorgfältig verwaltet und regelmäßig getauscht werden. Da mit den ZSK mehr Datenmaterial signiert wird, sind diese öfter zu tauschen. Je nach Größe der signierten Zonen stellt ein Wechsel im Zeitrahmen von ein bis drei Monaten ein geeignetes Sicherheitsniveau dar. Bei den KSK sollte spätestens nach einem Jahr ein Wechsel erfolgen. Gelan-

gen die KSK und ZSK an die Öffentlichkeit, müssen die Schlüssel umgehend getauscht werden.

Durch den Einsatz von DNSSEC und die dadurch nötigen kryptografischen Operationen ist es notwendig, die Leistungskapazität von DNS-Servern zu anzupassen, insbesondere die Rechenleistung muss gegebenenfalls erhöht werden. Es muss sichergestellt werden, dass auch bei Lastspitzen die Antwortzeit gering gehalten wird.

Prüffragen:

- Ist sichergestellt, dass die Schlüssel KSK und ZSK für DNSSEC regelmäßig gewechselt werden?
- Ist die Leistungskapazität der DNS-Server im Vergleich zu DNS-Servern ohne DNSSEC erhöht worden?

# M 4.354 Überwachung eines DNS-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Sicherheit eines DNS-Servers auch im Betrieb aufrecht zu erhalten, reicht es nicht aus, sich alleine auf eine sorgfältige Planung und Anfangskonfiguration zu verlassen. Es müssen eine Reihe von Maßnahmen durchgeführt werden, um eventuelle Probleme und sicherheitskritische Lücken aufzudecken.

Die Kapazitätsanforderungen müssen bereits in der Planung festgelegt werden. Aufgrund der Tatsache, dass die Kapazitätsanforderungen von der

- Größe der Zone(n),
- Anzahl der Anfragen,
- Anzahl der rekursiven Anfragen,
- Anzahl der Zonentransfers,
- Anzahl der dynamischen Updates, etc.

abhängen, ist es schwierig die benötigten Kapazitäten zu planen. Daher muss ein DNS-Server regelmäßig bezüglich der Auslastung überwacht werden, um gegebenenfalls die Leistungskapazität der Hardware anzupassen. Des Weiteren kann eine erhöhte Auslastung ein Indikator für einen laufenden Angriff sein.

Änderungen an der Konfiguration müssen sorgfältig dokumentiert werden, sodass zu jeder Zeit nachvollziehbar ist, wer etwas geändert hat und aus welchem Grund. Für die Änderungen an den Konfigurationsdateien kann ein Revisionskontrollprogramm eingesetzt werden, um die Dokumentation zu erleichtern und um zu früheren Konfigurationseinstellungen zurückkehren zu können (siehe M 2.25 *Dokumentation der Systemkonfiguration*).

Des Weiteren müssen die Zugriffsberechtigungen des DNS-Servers im Dateisystem regelmäßig überprüft werden. Insbesondere sollte dies nach Software-Updates oder Konfigurationsänderungen geschehen.

Die Administratoren müssen sich über aktuelle Sicherheitslücken in der eingesetzten Software frühzeitig informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Die Logdateien des DNS-Servers sowie des unterliegenden Betriebssystems sollten regelmäßig überprüft und ausgewertet werden. Unregelmäßigkeiten in den Logdateien, die Hinweise auf mögliche Probleme sein können, sind beispielsweise:

- Eine Häufung von Anfragen von bestimmten Quellen
- Eine Häufung von (fehlgeschlagenen) Zonentransfers
- Eine Häufung von Anfragen bezüglicher bestimmter Domain-Namen
- Eine Häufung von Anfragen bezüglich Domain-Namen, die nicht existieren
- Eine Häufung von unerlaubten rekursiven Anfragen

Unregelmäßigkeiten müssen aber nicht unbedingt Hinweise auf eine Kompromittierung des Servers sein. Oft treten Unregelmäßigkeiten aufgrund fehlerhafter Einstellungen auf.

Zu einem sicheren Betrieb gehören weitere regelmäßig durchzuführende Maßnahmen der Notfallvorsorge (siehe auch M 6.139 *Erstellen eines Notfallplans für DNS-Server*).

Prüffragen:

- Wird die Auslastung der DNS-Server regelmäßig überprüft?
- Werden Konfigurationsänderungen des DNS-Servers (automatisch) dokumentiert?
- Werden die Zugriffsberechtigungen des DNS-Servers regelmäßig überprüft?
- Sind die Administratoren über aktuelle Sicherheitslücken bezüglich der DNS-Server Software informiert?
- Werden die Protokolldateien des DNS-Servers regelmäßig ausgewertet?

# M 4.355 Berechtigungsverwaltung für Groupware-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Sicherheit der in einem Groupware-System verarbeiteten Geschäftsdaten wird stark durch die eingestellten Berechtigungen für Benutzer und Administratoren bestimmt. Diese legen fest, welche Daten eingesehen bzw. verändert werden können. Daher sind die konfigurierten Berechtigungen und deren Verwaltung ein sehr wichtiger Bestandteil der Systemsicherheit. Die vergebenen Berechtigungen, vor allem die privilegierten Berechtigungen, müssen regelmäßig gegenüber dem Berechtigungskonzept überprüft und bei Aufgabenänderungen zeitnah angepasst werden. Das Berechtigungskonzept muss dem Schutzbedarf angemessen sein und alle betriebenen Groupware-Komponenten umfassen.

Für die Verwaltung von Berechtigungen sollten die folgenden Empfehlungen berücksichtigt werden. Die Liste ist an die lokalen Bedürfnisse und Anforderungen anzupassen und zu erweitern.

### Rechtevergabe

Berechtigungen sollten grundsätzlich möglichst restriktiv vergeben werden. Dies gilt vor allem in Bezug auf die Groupware-Administratoren: Jeder Administrator sollte nur diejenigen Rechte erhalten, die zur Wahrnehmung seiner Aufgaben notwendig sind. Alle Rechtezuordnungen sind zu dokumentieren.

Es wird empfohlen, administrative Tätigkeiten auf Betriebssystemebene und Groupware-Anwendungsebene soweit wie möglich zu trennen. Es sollte jedoch beachtet werden, dass dies nicht uneingeschränkt möglich ist. Für einige Aufgaben benötigen Groupware-Administratoren auch lokale Administratorrechte (so z. B. zum Starten und Stoppen von Diensten).

### Schulung

Administratoren, die für die Verwaltung von Benutzerkennungen, Rollen, Profilen oder Berechtigungen verantwortlich sind, müssen zwingend Schulungen zum Berechtigungskonzept und zur Berechtigungsverwaltung (Vorgehen, Werkzeuge, richtige Verwendung) erhalten oder die entsprechenden Kenntnisse nachweisen. Nur so wird erreicht, dass die Berechtigungsverwaltung versiert durchgeführt werden kann (siehe auch M 3.74 *Schulung zur Systemarchitektur und Sicherheit von Groupware-Systemen für Administratoren*).

### Rollentrennung bei der Administration

Das Verwaltungskonzept muss so ausgelegt sein, dass die Verantwortlichkeiten möglichst getrennt werden. Folgendes sollte dabei beachtet werden:

- Es sollte ein Benutzeradministrator vorgesehen werden. Dieser sollte Benutzerkennungen anlegen, verändern und Rollen zuordnen können. Das Anlegen oder Verändern von Rollen oder Profilen darf dem System-Administrator nicht erlaubt sein.
- Es sollte ein Profiladministrator vorgesehen werden. Dieser darf für vorhandene Rollen Profile generieren, die keine privilegierten System-Berechtigungen enthalten.

Durch die Trennung (sofern technisch richtig umgesetzt) wird erreicht, dass sich die Administratoren nicht selbst Berechtigungen zuordnen können und für sie auf diese Weise nur die ihnen zugeordneten Aufgaben ausführbar sind.

In kleineren Unternehmen oder Behörden kann es aufgrund eingeschränkter Personalverfügbarkeit vorkommen, dass keine Trennung vorgenommen werden kann und alle Aufgaben durch eine Person ausgeführt werden. Alle Daten im Groupware-System können dann durch den Administrator unbemerkt eingesehen und verändert werden. Generell ist dies als sicherheitskritisch zu bewerten, so dass zusätzliche Kontrollen notwendig sind. Gleiches gilt allgemein auch im Kontext bei der Verarbeitung personenbezogener Daten, wo beispielsweise eine entsprechende Funktionstrennung vorhanden sein muss. Kann diese nicht erreicht werden, müssen geeignete Kontrollen auf organisatorischer Ebene definiert und deren Durchführung sichergestellt werden. Die von der Groupware-Software vorgegebenen und ausgelieferten Rollen sind sorgfältig gegen die eigenen Anforderungen zu prüfen und anzupassen.

Prüffragen:

- Ist ein angemessenes Berechtigungskonzept für die betriebenen Groupware-Komponenten vorhanden?
- Wurden die Groupware-Administratoren in der Anwendung der Berechtigungsverwaltung geschult?

# M 4.356 Sichere Installation von Groupware-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für die Installation eines Groupware-Systems sind die nachfolgend beschriebenen Aspekte zu berücksichtigen, denn schon in der Installationsphase werden wichtige Weichen für dessen Sicherheit gestellt.

**Verwendete Betriebssysteme absichern**

Die Komponenten eines Groupware-Systems werden als Applikationen auf IT-Systemen wie Server und Clients installiert und in Form von Prozessen ausgeführt. Damit ist die Sicherheit des jeweils genutzten Betriebssystems auch wichtig für die Sicherheit des Groupware-Systems. Die Bausteine der IT-Grundschutz-Kataloge, die für die genutzten IT-Systeme relevant sind, müssen daher in die Modellierung einbezogen und umgesetzt werden.

Ein Groupware-System besteht potentiell aus vielen Komponenten unterschiedlichster Ausprägung. Ungenutzte Komponenten jeglicher Art bergen jedoch Sicherheitsrisiken, da diese oftmals vergessen werden und daher ohne angepasste Konfiguration sind. Daher müssen ungenutzte Komponenten, soweit es geht, von der Installation ausgeschlossen oder später deaktiviert werden.

Schon während der Installation müssen wichtige Authentisierungsdaten eingestellt werden. Dies sind beispielsweise Passwörter für Dienste-Benutzer, die von den Groupware-Systemkomponenten zur Authentisierung bei internen Kommunikationsverbindungen genutzt werden.

Es ist darauf zu achten, dass dabei sichere Passwörter gewählt werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs*). Die Passwörter sollten sich an den internen Passwortvorgaben orientieren. Es ist auch dann ein neues Passwort einzugeben, falls die Installationsroutine bereits ein Passwort vorgibt.

Im Rahmen der Risikobetrachtung für das Groupware-System ist zu bedenken, dass der Administrator, der das Groupware-System installiert und die Passwörter festlegt, dadurch die Möglichkeit besitzt, die Sicherheitsmechanismen des Groupware-Systems zu unterwandern. Die technischen Benutzer, für die Passwörter anzugeben sind, besitzen in der Regel hohe Privilegien. Daher müssen die Passwörter nach der Installation durch vertrauenswürdige Administratoren verändert werden. Dies sollte technisch erzwungen werden. Bei Administrator-Zugängen, bei denen keine Rollentrennung möglich ist, sollte überlegt werden, das Passwort aufzuteilen, so dass die Passworteingabe im Vier-Augen-Prinzip erfolgt, wobei je einer von zwei Administratoren die Hälfte des Passwortes eingibt.

In der Regel werden Groupware-Systeme nicht direkt von den ausgelieferten Datenträgern installiert. Vielmehr wird eine Verzeichnisstruktur lokal oder im Netz genutzt, um für die jeweiligen IT-Systeme die Daten anzubieten, die dort zur Installation benötigt werden. Es wird empfohlen, die Daten nicht lokal auf dem Rechner zu halten, auf dem die jeweiligen Groupware-Komponenten installiert werden, sondern auf einem separaten Installationsrechner im LAN. In großen Behörden und Unternehmen kann dieses Verzeichnis genutzt werden, um zusätzliche Groupware-Systeme zu installieren. Werden die Systeme nicht

in einem separaten und abgeschirmten Netzsegment installiert, so sollte der Installationsrechner vom Netz genommen werden, solange er nicht benötigt wird. Zumindest sollte die Freigabe des Servers deaktiviert werden.

Der Zugriff auf die Installationsquellen ist mit Mitteln des Betriebssystems so abzusichern, dass nur berechtigte Administratoren darauf zugreifen können. Unberechtigte Benutzer dürfen insbesondere keine schreibenden Rechte auf die Installationsquellen besitzen, damit die enthaltenen Daten nicht verändert werden können. Werden die Installationsquellen lokal auf Rechnern des Groupware-Systems vorgehalten, so sollten diese nach Abschluss der Installation gelöscht werden.

**Sichere Installation und Konfiguration der Systemlandschaft**

Entsprechend der Planung der Systemlandschaft müssen die für den Betrieb des Groupware-Systems benötigten Komponenten (z. B. auch die Sicherheitsgateways) installiert und konfiguriert werden.

Prüffragen:

- Wurden alle für den Betrieb des Groupware-Systems benötigten Komponenten sicher installiert und konfiguriert?
- Sind alle Passwörter während der Groupware-Installation sicher gewählt worden?
- Wurden die Groupware-Installationsquellen gegen unbefugten Zugriff gesichert?

# M 4.357 Sicherer Betrieb von Groupware-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Revisor

Nach der Installation und Konfiguration der eingesetzten Groupware-Komponenten müssen Maßnahmen zur Gewährleistung des sicheren Betriebs ergriffen werden. Dabei ist die Umsetzung der Sicherheitsrichtlinien der betreffenden Institution zu prüfen.

Folgende sicherheitsrelevante Aspekte sind dabei zu berücksichtigen:

**Software- und Systempflege**

Eine wichtige Voraussetzung für den sicheren Betrieb von IT-Systemen ist, dass alle sicherheitsrelevanten Service Packs, Updates und Patches für das Softwareprodukt eingespielt werden. Es ist daher erforderlich, dass sich die Administratoren regelmäßig über neu bekannt gewordene Schwachstellen der eingesetzten Groupware und der genutzten Betriebssysteme informieren und geeignete Maßnahmen zu deren Beseitigung zeitnah umsetzen. Vor dem Einspielen eines Service Packs, Updates oder Patches in das Produktivsystem sollte dies jedoch zunächst in einer Testumgebung geschehen. So kann überprüft werden, ob unerwünschte Seiteneffekte zu erwarten sind. Darüber hinaus sollten die Konfigurationseinstellungen des Gesamtsystems regelmäßig daraufhin überprüft werden, ob sie den Vorgaben entsprechen und den Sicherheitsanforderungen genügen.

**Schutz vor Denial-of-Service-Attacken (DoS)**

Als Schutz vor DoS-Attacken wird empfohlen, Einschränkungen der maximal möglichen Nachrichten- bzw. Speichergrößen einzuführen. Dies gilt vor allem für eingehende Verbindungen. Über die Begrenzungen müssen die Benutzer informiert sein. Es ist außerdem festzulegen und zu kommunizieren, wie mit zu großen eingehenden Nachrichten umgegangen wird, also z. B., ob Empfänger oder Absender darüber informiert werden, dass sie nicht zugestellt wurden.

Ein weiterer Mechanismus ist die Filterung von Nachrichten. Damit können zwar keine großangelegten Spam-Angriffe abgewehrt werden, jedoch kann dieser Mechanismus für die Filterung einzelner Absender sinnvoll eingesetzt werden.

**Kontrolle von Verteilerlisten**

Um die Adressierung von E-Mails zu vereinfachen, werden häufig Alias-Dateien oder Verteilerlisten geführt. Werden sowohl auf den Mailservern als auch auf den Mail-Clients Alias-Dateien geführt, ist zunächst zu klären, welche Einträge Priorität haben, d. h. ob bei gleicher Wahl eines Alias der vom Mailserver oder der vom Mail-Client akzeptiert wird. Beim Empfang von E-Mails sollte die Alias-Umsetzung des Mailservers ausschlaggebend sein, beim Versand die des Mail-Clients. Die Benutzer müssen darüber informiert sein, welche Aliase auf dem Mailserver aufgelöst werden, damit sie dies bei der Weitergabe von E-Mail-Adressen berücksichtigen können.

Damit die Benutzer die Alias-Dateien auf dem Mailserver verwenden können, müssen sie lesend darauf zugreifen können. Schreibrecht darauf sollte aber nur der Mail-Administrator haben.

Um zu verhindern, dass E-Mails aufgrund fehlerhafter, nicht aktueller oder manipulierter Verteilerlisten an falsche Empfänger übertragen werden, müssen die Verteilerlisten regelmäßig auf Korrektheit und Aktualität überprüft werden.

**Datensicherung**

Als Grundlage für die schnelle Wiederherstellung der Daten, z. B. nach einem Systemausfall, muss regelmäßig eine Datensicherung des Groupware-Systems angelegt werden (siehe M 6.90 Datensicherung und Archivierung bei Groupware und von E-Mails). Es sollte sporadisch überprüft werden, ob die erstellten Datensicherungen sich wiedereinspielen lassen und alle erforderlichen Bereiche umfassen.

**Ausfallsicherheit**

Als Vorsorge sollte schließlich eine praktikable Notfallplanung vorliegen (siehe M 6.140 *Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen*).

**Regelmäßige Sicherheitsprüfungen**

Die Sicherheit eines Groupware-Systems muss regelmäßig überprüft werden. Auf diese Weise können Fehlkonfigurationen und Schwachstellen aufgedeckt und behoben werden. Sicherheitsprüfungen sollten in regelmäßigen Abständen durch unterschiedliche Personen erfolgen. So sollten beispielsweise Administratoren in relativ kurzen Abständen (etwa monatlich) Kurzprüfungen durchführen. Es empfiehlt sich dabei, eine Prüfliste aufzubauen, damit ein definierter Prüfumfang gewährleistet ist. Festgestellte kleinere Probleme können meist sofort durch die Administratoren korrigiert werden, größere Probleme sind entsprechend der Prozessvorgaben weiterzumelden. In mittleren Zeitabständen (mehrere Monate) sollten Sicherheitsprüfungen durch andere, interne Rollen (z. B. Informationssicherheit, IT-Revision) erfolgen. In längeren Zeitabständen können dann auch Prüfungen durch externe Prüfer sinnvoll sein.

Prüffragen:

- Wurden geeignete Maßnahmen zur Gewährleistung des sicheren Betriebs der Groupware-Systeme ergriffen?
- Werden alle Aspekte aus der Sicherheitsrichtlinie zum sicheren Betrieb der Groupware-Systeme umgesetzt?
- Wird das Groupware-System regelmäßig einer Sicherheitsprüfung unterzogen?
- Werden die sicherheitsrelevanten Groupware-Protokolle regelmäßig ausgewertet?

# M 4.358 Protokollierung von Groupware-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Damit die Systemfunktionen und die Systemsicherheit eines Groupware-Systems überwacht werden können, müssen sicherheitsrelevante Ereignisse protokolliert werden. Generell ist bei der Protokollierung Folgendes zu beachten:

### Protokollierungskonzept

Es muss ein Protokollierungskonzept erstellt werden. Im Konzept ist festzulegen, welche Protokolldaten im Groupware-System gesammelt und ausgewertet werden sollen. Da bei der Protokollierung auch personenbezogene Daten anfallen können, sind der Datenschutzbeauftragte und der Personal- oder Betriebsrat in die Planung einzubeziehen.

### Sicherheit der Protokolldaten

Die protokollierten Daten können wichtige Systeminformationen und personenbezogene Daten enthalten. Der Zugriff auf die Protokolldaten muss daher eingeschränkt werden. Dies kann Einstellungen sowohl innerhalb als auch außerhalb des Groupware-Systems (z. B. auf Dateiebene) notwendig machen.

### Wichtige Systemereignisse auswerten

Wichtige Systemereignisse wie Änderungen, Fehler und Störungen an Hardware, Betriebssystem, Treibern, Diensten und sonstiger Software sind zu protokollieren und regelmäßig auszuwerten.

Beim Betrieb mehrerer Groupware-Systeme empfiehlt es sich, eine zentrale Protokollierung einzusetzen, so dass die Auswertung auf einem System erfolgen kann.

### Zugriff auf die Monitoring-Werkzeuge einschränken

Der Zugriff auf die durch das Groupware-System angebotenen Monitoring-Werkzeuge ist auf die berechtigten Administratoren einzuschränken.

Prüffragen:

- Wurde ein angemessenes Protokollierungskonzept für Groupware erstellt?
- Werden die Groupware-Protokolle regelmäßig ausgewertet?

# M 4.359 Überblick über Komponenten eines Webservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um ein Web-Angebot zur Verfügung stellen zu können, werden sowohl Hardware- als auch Software-Komponenten benötigt. Abhängig von der Funktionalität der Web-Anwendung werden dabei unterschiedliche Server-Typen benötigt. Die Basis-Komponenten stellen der Webserver und der Web-Anwendungsserver dar. In der Regel sind die Dienste für den Webserver und für den Web-Anwendungsserver auf verschiedenen IT-Systemen installiert. Für eine persistente Datenhaltung der Inhalte kommen meist Datenbank-Server zum Einsatz. Daneben kommen für einfache Operationen häufig auch Verzeichnis-Server zum Einsatz, auf deren Daten Clients meist nur lesend zugreifen können. Derartige Verzeichnisse werden beispielsweise zur Ablage von Benutzerdaten verwendet.

**Webserver**

Ein Webserver ist eine Software-Komponente, mit der Web-Angebote über HTTP und HTTPS bereitgestellt werden können. Damit wird ein Framework zur Verfügung gestellt, dessen Funktionen von der Web-Anwendung genutzt werden können. Häufig wird auch die Hardware, auf dem eine Webserver-Software installiert ist, als Webserver bezeichnet.

Der Webserver ist die Kern-Komponente jedes Web-Angebotes. Er nimmt die Anfragen der Benutzer entgegen und liefert, sofern möglich, selbst die entsprechende Antwort zurück. Dies ist beispielsweise bei statischen Web-Anwendungen der Fall. Angefragte Inhalte werden dabei sofort ohne Aufruf dynamischer Funktionen durch den Webserver zurückgeliefert. Bei dynamischen Web-Anwendungen leitet der Webserver die Anfrage meist an den Web-Anwendungsserver weiter. Dort werden dynamische Funktionen durchgeführt, wie beispielsweise der Aufbau einer Web-Seite auf Grund von Datenbank-Inhalten, und das Ergebnis wieder an den Webserver gesandt. Manche Webserver haben den Web-Anwendungsserver für einige Programmiersprachen integriert (z. B. unterstützt der Apache-Webserver die Skriptsprache PHP (Akronym für "PHP: Hypertext Preprocessor"). In diesem Fall wird die Anwendung auf dem Server lokal ausgeführt und muss nicht an einen Web-Anwendungsserver weitergeleitet werden.

Da der Webserver direkt von Benutzern angesprochen wird, bietet er auch die exponierteste Angriffsfläche für einen Angreifer. Der Webserver muss sicherstellen, dass nur legitime Anfragen an Hintergrundsysteme weitergeleitet werden, dass Benutzer nur auf die Inhalte Zugriff bekommen, für die sie autorisiert sind, und dass der Webserver nicht durch die Ausnutzung von Software-Schwachstellen kompromittiert werden kann.

Ein Web-Angebot stellt Benutzern Informationen und Funktionen zur Verfügung. Die Benutzer greifen mittels eines Browser darauf zu. Um Web-Angebote betreiben zu können, welche dynamische Funktionen zur Verfügung stellen, bieten sich die folgenden Architekturen an:

- Realisierung der dynamischen Funktion über externe Programme, die über Schnittstellen aufgerufen werden. Beispiele hierfür sind CGI (Common Gateway Interface) und SSI (Server Side Includes). Beim Aufruf eines Web-Angebotes werden Programme direkt auf dem Webserver auf-

gerufen. Die Ergebnisse des Programmaufrufs werden in jenes Ergebnis eingebettet, das an den Browser des Benutzers zurückgeliefert wird.
- Realisierung der dynamischen Funktion in Form von Funktionen oder Modulen, die im Webserver integriert sind. Ein Beispiel dazu ist PHP als Modul in Apache. Der wesentliche Unterschied zum ersten Punkt besteht darin, dass keine externen Programme aufgerufen werden. Die dynamische Funktion wird direkt in die anzuzeigenden Web-Seiten, beispielsweise in Form von Skriptcode, eingebettet. Vor Auslieferung der Web-Seite an den Browser wird der Skriptcode interpretiert und das Ergebnis in die Antwort des Servers eingeschlossen.
- Realisierung der dynamischen Funktion auf einem eigenständigen Web-Anwendungsserver wie JBoss, Weblogic oder WebSphere. Bei dieser Architekturform werden Anfragen zunächst vom Webserver entgegengenommen und verarbeitet. Jene Teile der Anfrage, welche den Aufruf von dynamischen Funktionen erfordern, werden an einen Web-Anwendungsserver weitergeleitet. Dieser führt die benötigten Funktionen und die eventuelle Kommunikation mit Hintergrundsystemen durch und liefert das Ergebnis an den Webserver zurück. Der Webserver bettet das Ergebnis des Web-Anwendungsservers anschließend in jene Antwort ein, die an den Browser des Clients gesandt wird.

**Web-Anwendungsserver**

Zahlreiche Web-Angebote benötigen zusätzlich zum Webserver weitere Systeme. Beispielsweise werden eigene Web-Anwendungsserver benötigt, wenn Web-Angebote mit Hilfe von Java oder .NET bereitgestellt werden. Programmiersprachen wie PHP, ASP oder Perl funktionieren größtenteils ohne zusätzlichen Web-Anwendungsserver, da die benötigten Funktionen meist direkt im Webserver integriert sind.

Ein Web-Anwendungsserver wird verwendet, um dynamische Web-Angebote zur Verfügung stellen zu können. Dabei werden Anfragen vom Webserver mit entsprechenden Parametern an den Web-Anwendungsserver weitergereicht. Dieser ruft in weiterer Folge die für die Verarbeitung der Anfrage erforderlichen Skripte, Methoden oder Funktionen auf. Je nach Art des Aufrufs führt der Anwendungsserver auch Anfragen an Hintergrundsysteme, beispielsweise an Datenbank- oder Verzeichnis-Server, durch. Das Ergebnis des Web-Anwendungsservers wird dann wieder an den Webserver zurückgegeben.

In einem Web-Anwendungsserver sind einige wichtige Funktionen und Frameworks, welche häufig zum Betrieb von Web-Angeboten benötigt werden, vereinigt. Durch die Kapselung und Abstraktion von Schnittstellen zu anderen Systemen (z. B. Hintergrundsysteme) kann eine saubere Trennung zwischen Anwendung und Datenhaltung erfolgen. Frameworks, die auf Web-Anwendungsservern bereitgestellt werden können, umfassen eine Vielzahl an Funktionen zur Kommunikation mit Hintergrundsystemen. Beispielsweise werden abstrakte Funktionen zum Auslesen und zur Manipulation von Datenbankinhalten geboten, welche nur geringe Kenntnisse über die tatsächlich eingesetzte Datenbank erfordern. Darüber hinaus sind in Frameworks verschiedenste Sicherheitsfunktionen bereits implementiert (z. B. Prepared Statements für SQL-Anfragen, welche die Ausnutzung von SQL-Injection-Schwachstellen verhindern). Durch Hinzufügen weiterer Web-Anwendungsserver zu einem Cluster ist eine Skalierung möglich, ohne dass hierfür die Anwendung modifiziert werden muss.

**Datenbank-Server**

Um Daten dauerhaft zu speichern, kommen im Zusammenhang mit Web-Angeboten meist Datenbanken zum Einsatz. Diese werden gemeinsam mit den zugehörigen Datenbank-Management-Systemen (DBMS) meist auf dedizierten Datenbank-Servern betrieben. Grundsätzlich werden folgende Formen von Datenbanken unterschieden:

- Hierarchische Datenbanken stellen Datenobjekte in einer Eltern-Kind-Beziehung dar.
- Netz-basierte Datenbanken können Datenobjekte über Netze miteinander verknüpfen.
- Relationale Datenbanken bilden Datenobjekte in Tabellen ab. Diese Tabellen können untereinander in Beziehung stehen.
- Objektorientierte Datenbanken legen Datenobjekte als Objekte im Sinne der objektorientierten Programmierung ab. Dies bedeutet, dass Objekte in einer objektorientierten Datenbank die gleichen Eigenschaften aufweisen wie Objekte in der Programmierung.

Datenbank-Server müssen speziell geschützt werden (siehe dazu B 5.7 *Datenbanken*). So darf der Zugriff auf die darauf befindlichen DBMS nur durch autorisierte Ressourcen erfolgen. Darüber hinaus muss im Sinne des Minimalprinzips auch der Zugriff auf Datenobjekt-Ebene klar definiert und gewartet werden. Wie jede andere Software können auch DBMS Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können, um Zugriff zu vertraulichen Daten zu erhalten. Neben der Einschränkung des Zugriffs müssen daher Maßnahmen umgesetzt werden, um bekannte Schwachstellen zu beseitigen. Speziell für Datenbank-Systeme müssen im Web-Angebot Maßnahmen zum Schutz vor SQL-Injection getroffen werden, da Angreifer sonst möglicherweise Inhalte der Datenbank unberechtigterweise auslesen oder verändern können.

Besonders vertrauliche Inhalte einer Datenbank (z. B. Passwörter) sollten verschlüsselt werden, um sie vor unbefugtem Zugriff zu schützen. Dies erfordert ein geeignetes Schlüsselmanagement und verhindert das Auslesen vertraulicher Daten im Klartext.

**Verzeichnisdienst**

Mit Hilfe eines Verzeichnisdienstes kann eine zentrale Verwaltung der Benutzerdaten sowie von Rechten erfolgen. Diese Daten werden meist in einer hierarchischen Datenbank abgelegt. Der Zugriff auf einen Verzeichnisdienst erfolgt in der Regel über LDAP (Lightweight Directory Access Protocol). Dieses setzt auf TCP/IP auf und erlaubt die Abfrage und Modifikation von Informationen auf dem Verzeichnisdienst-Server.

Da in Verzeichnisdiensten häufig sensible Daten gespeichert werden, sind auch sicherheitsrelevante Faktoren zu berücksichtigen (siehe B 5.15 *Allgemeiner Verzeichnisdienst*). Zum einen sollten sensible Daten (z. B. Passwörter) durch Anwendung geeigneter kryptografischer Verfahren vor unbefugtem Zugriff geschützt werden. Zum anderen besteht bei LDAP, ähnlich wie bei SQL, die Möglichkeit, Anfragen zu manipulieren. Es sind daher geeignete Maßnahmen umzusetzen, um sogenannte LDAP-Injections zu verhindern.

**Reverse Proxy**

Proxies kommen meist auf der Client-Seite zur Nutzung von Web-Angeboten zum Einsatz. Daneben besteht jedoch auch die Möglichkeit, diese auf der Server-Seite einzusetzen, um Zugriffe zu optimieren (Caching) bzw. eine Filterung durchzuführen. Befindet sich der Proxy auf der Server-Seite, spricht man von

einem "Reverse Proxy" (siehe auch M 4.223 *Integration von Proxy-Servern in das Sicherheitsgateway*). Alle Anfragen, die an den zugehörigen Webserver gerichtet sind, werden zuerst vom Proxy angenommen. Dieser entscheidet anhand eines konfigurierbaren Regelwerks, ob er die Anfrage selbst beantworten kann (Caching), ob er die Anfrage an den Webserver bzw. einen der Webserver im Cluster weiterleitet oder ob er die Abfrage aus Sicherheitsgründen abweist. Im folgenden werden die wichtigsten Funktionen eines Reverse Proxys kurz erläutert:

- Caching
  Statische Inhalte wie Bilder oder statischer HTML-Text können auf einem Reverse Proxy zwischengespeichert werden. Werden diese Inhalte angefragt, können diese direkt vom Reverse Proxy beantwortet werden. Durch dieses Caching können Antwortzeiten verkürzt und die Auslastung der Webserver reduziert werden.
  Caching kann jedoch auch zu sicherheitskritischen Problemen führen. Werden beispielsweise Inhalte auf dem Reverse Proxy zwischengespeichert, für die im Normalfall eine Autorisierung auf dem Webserver erforderlich ist, muss sichergestellt werden, dass diese Inhalte auch nur an autorisierte Benutzer ausgeliefert werden.
- Lastverteilung
  Kann ein Reverse Proxy eine Anfrage selbst beantworten, weil die erforderlichen Daten im Cache verfügbar sind, ist es nicht erforderlich, die Anfrage an den dahinter liegenden Webserver weiterzuleiten. Auf diese Weise kann die Last auf den Webservern verringert werden. Da alle Anfragen zunächst an den Reverse Proxy gerichtet werden, kann dieser auch Anfragen auf mehrere Server verteilen. Somit kann eine Load-Balancer-Funktion realisiert werden.
- Authentisierung
  Ein Reverse Proxy erlaubt es, die Authentisierung aus dem Webserver auszulagern. Dadurch wird eine Art Einmal-Anmeldung (in der Fachliteratur auch als Single Sign On bezeichnet) möglich, wenn der Reverse Proxy die Authentisierung von Benutzern für mehrere Webserver übernimmt. Hat sich der Benutzer einmal am Reverse Proxy angemeldet, steht ihm die Benutzung mehrerer Server zur Verfügung, ohne sich erneut anmelden zu müssen. Zusätzlich kann die Weiterleitung von Anfragen von einer Authentisierung am Reverse Proxy abhängig gemacht werden.
- Verschlüsselung
  Die Terminierung einer Ende-zu-Ende-Verschlüsselung (z. B. bei der Verwendung von HTTPS über TLS oder SSL) kann am Reverse Proxy erfolgen. Nur wenn die Entschlüsselung bereits am Reverse Proxy durchgeführt wird, ist es möglich, diesen für die Filterung von Anfragen zu verwenden. Zudem entlastet eine Terminierung der Verschlüsselung am Reverse Proxy den dahinter liegenden Webserver, da dieser keine zusätzlichen Ressourcen für die Entschlüsselung aufwenden muss. Ein weiterer Vorteil dieser Variante ist die Unabhängigkeit des Verschlüsselungskanals von dem tatsächlich verwendeten Webserver. Auf diese Weise können aufeinanderfolgende Anfragen auch von unterschiedlichen Servern bearbeitet werden, ohne dass der Verschlüsselungskanal geändert werden muss. Erfolgt eine Terminierung der Verschlüsselung und Filterung der Daten auf einem Proxy, sind jedoch auch entsprechende datenschutzrechtliche Aspekte zu beachten. Beispielsweise könnten IP-Adressen jedes Clients, Zeitpunkte von Anmeldungen und die aufgerufenen Seiten mitprotokolliert werden.
- Einschränkung der Kommunikationsverbindungen
  Alle Anfragen, die aus dem nicht-vertrauenswürdigen Netz stammen, können über den Reverse Proxy geleitet werden. Unerwünschte Verbindungs-

anfragen können hier abgewiesen werden, die Administration des Sicherheitsgateways wird erleichtert und die Wahrscheinlichkeit von Fehlkonfigurationen verringert. Der IP-Stack des Webservers wird vom nicht-vertrauenswürdigen Netz getrennt.

- Verschleierung
  Es ist nicht nötig, die IP-Adressen der eigentlichen Webserver zu veröffentlichen, da diese ausschließlich mit dem Reverse Proxy und nicht mit den Clients kommunizieren. Der direkte und oft unerwünschte Verbindungsaufbau zum Webserver wird erschwert, da die hierfür benötigten Informationen erst ermittelt werden müssen. Reverse Proxies sorgen dafür, dass Informationen über den internen Netzaufbau nicht an die Clients übermittelt werden. Auch Fehlermeldungen, die auf die eingesetzte Webserver-Applikation schließen lassen und Hinweise zur Kompromittierung geben können, können zentral abgefangen werden. Es wird aber empfohlen, dass die eigentlichen Webserver diese Informationen nicht übermitteln, Reverse Proxies können aber als "zweite Verteidigungslinie" genutzt werden.

# M 4.360 Sichere Konfiguration eines Webservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem ein Webserver-Dienst auf einem Webserver installiert wurde, muss eine sichere Grundkonfiguration vorgenommen werden. Dies betrifft beispielsweise, wie zusätzliche Module eingebunden werden können und wie auf Verzeichnisse innerhalb und außerhalb des Dateisystembereichs mit den veröffentlichten Informationen zugegriffen werden kann, aber auch Einstellungen, die auf die Performance des Servers Einfluss haben.

### Zuordnung zu einem unprivilegierten Benutzer

Wird eine Webserver-Anwendung gestartet, erhält sie in der Regel die gleichen Zugriffsrechte wie der Benutzer, der die Anwendung aufgerufen hat. Startet beispielsweise ein Administrator, der alle Informationen im Dateisystem des IT-Systems lesen und schreiben darf, die Anwendung, kann der Webserver-Prozess auf diese Informationen ebenfalls lesend und schreibend zugreifen. Daher sollte der Webserver-Prozess einem unprivilegierten Benutzerkonto zugewiesen werden. Die Zugriffsrechte im Dateisystem des IT-Systems sollten restriktiv vergeben werden, so dass dieses Benutzerkonto und somit der Webserver-Prozess nur auf benötigte Informationen zugreifen darf.

Dennoch ist es oft nötig, den Webserver-Dienst als privilegierten Benutzer ("root") zu starten. In diesem Fall sollte, wenn möglich, der Prozess nachträglich einem unprivilegierten Benutzer zugeordnet werden. Beim Apache-Webserver kann beispielsweise mit einer User-Direktive in der Konfigurationsdatei eine Benutzerkennung angegeben werden, unter der der Serverprozess als unprivilegierter Benutzer ausgeführt wird.

### Server-Verzeichnisse

Je nach eingesetzter Webserver-Anwendung müssen die Dateisystempfade angegeben werden, auf die der Webserver zugreifen darf. Dazu gehört beispielsweise der Dateisystempfad zu dem Verzeichnis mit den Informationen, die der Webserver den Clients zur Verfügung stellen soll ("WWW-Wurzelverzeichnis") und der Pfad zu den Protokollierungsdateien.

Wird das WWW-Wurzelverzeichnis festgelegt, ist darauf zu achten, dass sich innerhalb des Verzeichnisses nur Informationen befinden, die allen potentiellen Benutzern zur Verfügung gestellt werden sollen. Der Zugriffsbereich für Benutzer des Webservers sollte nicht zu groß gewählt werden. Beispielsweise sollten Benutzer keinen Zugriff auf das Root-Verzeichnis ("/") eines Unix-Systems oder die System-Partition eines Windows-Systems erhalten. Das Verzeichnis, in dem die abrufbaren Dateien gespeichert sind, sollte sich auf einer eigenen Partition oder Slice einer Festplatte befinden, um eine leichtere Wiederherstellung nach einem Festplattenschaden zu ermöglichen.

Der Webserver-Dienst sollte generell nur auf Informationen zugreifen dürfen, die sich innerhalb des WWW-Wurzelverzeichnisses befinden. Der lesende und insbesondere schreibende Zugriff auf Informationen außerhalb des WWW-Wurzelverzeichnisses sollte verhindert werden. Daher sollte auf Dateisystemverweise ("Links") auf Bereiche außerhalb des WWW-Wurzelverzeichnisses verzichtet werden. Wenn möglich, sollte der Webserver-Dienst so konfiguriert werden, dass nicht auf Informationen außerhalb des WWW-Wurzel-

verzeichnisses zugegriffen werden kann, beispielsweise durch einen Limit-Abschnitt beim Apache-Webserver.

**Schreibrechte**

Der Prozess des ausgeführten Webserver-Dienstes sollte nur über jene Rechte verfügen, die für den Betrieb erforderlich sind. Die Zugriffsrechte eines Webserver-Prozesses werden in der Regel von den Zugriffsrechten des Benutzers, der den Webserver-Prozess gestartet hat, abgeleitet. Normalerweise benötigt ein Webserver-Prozess keine Schreibrechte im Betriebssystem und sollte deshalb diese auch nicht besitzen. Werden Protokollierungsdateien an einen dedizierten Protokollierungsserver übermittelt, sind hierfür in dem Dateisystem des IT-Systems, auf dem der Webserver aufgerufen wurde, keine lokalen Schreibrechte notwendig (Ausnahme: Informationen müssen zwischengespeichert werden, wenn der Protokollierungsserver nicht erreichbar ist). Alle Dateien, die nicht mehr verändert werden sollen, wie beispielsweise statische HTML-Seiten, sollten mit einem Schreibschutz versehen werden. Falls der Webserver-Dienst automatische Verzeichnislisten generieren kann, sollte diese Funktion deaktiviert werden.

**Einschränken der Prozesse**

Ein Webserver-Dienst sollte in einer einer eingeschränkten Prozessumgebung betrieben werden, z. B. mittels "chroot" bei Unix-Systemen. Bei einer chroot-Umgebungen handelt es sich um einen abgeschotteten Bereich innerhalb des Computersystems, wie eine sogenannte Sandbox, die es einem Angreifer erschwert, nach der Kompromittierung des Webservers-Dienstes Zugriff auf das gesamte System zu erlangen. Vertiefende Informationen hierzu sind in M 4.198 *Installation einer Applikation in einem chroot Käfig* zu finden.

**Informationen über den Server**

Standard-Fehlermeldungen bergen oft die Gefahr in sich, zu viel Information preiszugeben. Aus den HTTP-Header-Zeilen von Antworten auf Anfragen oder von Fehlermeldungen können Angreifer oft Informationen über die Version der eingesetzten Server-Software und andere Details gewinnen. Diese Informationen können dann eventuell dazu genutzt werden, um bestimmte Angriffsmethoden auszuwählen und so schneller den Server zu kompromittieren. Daher sollten auf diesen "Seitenkanälen" so wenig Informationen wie möglich geliefert werden, indem eigene Fehlermeldungen konfiguriert werden, die die Benutzer über einen aufgetretenen Fehler informieren, aber keine Details dazu preisgeben.

**Authentisierung**

Um Zugriffsbeschränkungen auf Webservern oder für einzelne Bereiche des Webangebots einzurichten, gibt es verschiedene Möglichkeiten, die teilweise bereits im Webserver-Dienst selbst implementiert sind oder über Erweiterungsmodule eingebunden werden können. Oft wird der Zugriff gesteuert, indem der Zugriff auf bestimmte IP-Adressbereiche oder Domains (beispielsweise im Intranet) beschränkt wird oder indem sich Benutzer vor dem Zugriff auf bestimmte Ressourcen authentisieren müssen, z. B. über Benutzernamen und Passwort (siehe auch M 4.176 *Auswahl einer Authentisierungsmethode für Webangebote*).

In Abhängigkeit der Anwender (z. B. nur eigene Mitarbeiter, Kunden oder Benutzer, die sich vorher zwar registrieren müssen, aber ansonsten unbekannt sind), die auf den Webserver zugreifen dürfen und des Schutzbedarfs der bereitgestellten Informationen, sollten die Zugriffsrechte auf ein Minimum be-

schränkt werden. Generell sollten die Benutzer nur auf die erforderlichen Informationen zugreifen dürfen. Eine Ausnahme sind öffentliche Webserver, auf dessen WWW-Inhalte oft jeder interessierte Anwender zugreifen darf, wie beispielsweise ein öffentlicher Webserver im Internet.

**Verschlüsselung der Datenübertragung**

In der Regel werden die Informationen zwischen einem Webserver-Dienst und den Clients über HTTP übertragen. Bei HTTP handelt es sich um ein Klartextprotokoll, bei dem alle übertragenen Daten, wie Passwörter und Webinhalte, von einem möglichen Angreifer mitgelesen werden können. Daher wird dringend empfohlen, die Integrität und Vertraulichkeit von sensiblen Informationen zwischen Webserver-Dienst und Client zu schützen, beispielsweise indem Verschlüsselungsprotokolle wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) verwendet werden. Vertiefende Informationen sind unter M 5.66 *Clientseitige Verwendung von SSL/TLS* zu finden.

**Administration**

Webserver-Dienste werden oft mittels Konfigurationsdateien oder über graphische Oberflächen administriert, lokal oder über eine Netzverbindung. Wird das IT-System mit dem Webserver-Dienst über eine Netzverbindung administriert, ist der Netzzugang und der Informationsaustausch zwischen dem Webserver und dem IT-System, von dem aus der Webserver administriert wird, zu schützen. Dazu gehört, dass der Administrationszugang beschränkt werden sollte, beispielsweise indem durch Paketfilter alle Verbindungsanfragen außer von definierten IT-Systemen der Administratoren auf die Portnummer des Fernadministrationsdienstes abgewiesen werden (siehe M 4.238 *Einsatz eines lokalen Paketfilters*). Damit der Informationsaustausch nicht abgehört oder geändert werden kann, muss dieser verschlüsselt werden, beispielsweise über SSH (siehe M 5.64 *Secure Shell*).

Werden Applikationen oder Weboberflächen eingesetzt, die die Konfiguration erleichtern, sind diese ebenfalls vor dem Zugriff von unberechtigten Personen zu schützen.

**Deaktivierung von unnötigen Diensten**

Die Standardinstallation eines Webservers-Dienstes kann eine Reihe von Netzdiensten umfassen, die nicht immer benötigt werden und die gerade deswegen eine Quelle von Sicherheitslücken sein können. Ein Beispiel ist eine Weboberfläche zur Webserver-Konfiguration, die nicht benötigt wird, wenn der Webserver-Dienst über andere Mechanismen konfiguriert wird. Daher sollte überprüft werden, welche Netzdienste auf dem IT-System mit dem Webserver-Dienst installiert und aktiviert sind. Nicht benötigte Netzdienste sollten deaktiviert oder ganz deinstalliert werden.

**Beschränkung der Konnektivität**

Obwohl es sich in der Regel bei Webservern um IT-Systeme handelt, auf die viele Benutzer zugreifen dürfen, sollte dennoch die Kommunikation nur so restriktiv wie möglich erlaubt werden. Werden Netzdienste auf dem Server betrieben, die nur von ausgewählten IT-Systemen mit festen IP-Adressbereichen genutzt werden sollen, empfiehlt es sich, den Zugriff auf bestimmte IP-Adressen mit Paketfiltern zu beschränken. Der Zugriff auf Administrationszugänge sollte generell durch Paketfilter auf die IT-Systeme der Administratoren beschränkt werden. Werden Datenbanken oder Applikationsserver eingesetzt, ist diese Kommunikation ebenfalls zu beschränken. Vertiefende Informationen

zu Paketfiltern sind unter M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* und M 4.238 *Einsatz eines lokalen Paketfilters* zu finden.

Sollen die Webserver nur von internen Mitarbeiter genutzt werden dürfen, sollten die Webserver in einem Netzsegment betrieben werden, auf das nur aus dem LAN zugegriffen werden kann. Sollen auch externe, beziehungsweise fremde Benutzer Informationen vom Webserver abrufen können, empfiehlt es sich, den Webserver in einer demilitarisierten Zone zu betreiben.

**Protokollierung**

Zugriffe auf den Webserver-Dienst und das IT-System, auf dem der Webserver-Dienst installiert ist, sollten in dem Umfang protokolliert werden, wie es nötig ist, um Angriffe, Angriffsversuche und Sicherheitsverletzungen zeitnah erkennen und gegebenenfalls verfolgen zu können. Daher ist zu entscheiden, welche Informationen protokolliert werden sollen, wie und zu welchen Zeitpunkten die Protokolldaten auszuwerten sind und wann diese zu löschen sind. Der Webserver-Dienst und das IT-System sind entsprechend zu konfigurieren. Personenbezogene Daten dürfen nur in dem Umfang mitprotokolliert werden, in dem dies gesetzlich zulässig ist. Um abzuklären, was hier zulässig ist, sollte daher der Datenschutzbeauftragte beteiligt werden.

**Löschen von Beispieldokumenten**

Oft werden bei der Installation von Webservern Beispieldokumente mit installiert. So kann beispielsweise der Administrator direkt nach der Installation mit einem Browser auf den Webserver zugreifen, ohne vorher eigene Webinhalte entworfen zu haben. Wird eine vorhandene Beispiel-Index-Datei angezeigt, kann der Administrator auf den ersten Blick sehen, ob der Webserver korrekt installiert wurde. Oft beinhaltet die Beispiel-Index-Datei auch Informationen zu dem eingesetzten Webserver, wie die Versionsnummer.

Oft gibt es auch serverseitige Programme (CGI-, Perl- oder PHP-Skripte), die ebenfalls mit installiert werden. Aktiviert der Administrator die entsprechenden Module, die es ermöglichen, diese Skripte auszuführen, kann er direkt überprüfen, ob das Modul einwandfrei funktioniert.

Alle Beispiel-Dokumente und -Skripte sollten nach der Installation entfernt werden.

**Erweiterung mit Modulen**

Der Funktionsumfang von einigen Webserver-Diensten kann durch sogenannte Module erweitert werden. Funktionen, die von den Entwicklern der Webserver-Dienste nicht vorgesehen wurden, können so nachträglich hinzugefügt werden. Beispielsweise können über Erweiterungsmodule Applikationen direkt auf dem Webserver ausgeführt werden und so Seiteninhalte dynamisch erzeugt werden. Beispiele hierfür sind PHP und Perl, bei denen im Gegensatz zu "Aktiven Inhalten" die Applikationen nicht auf den Client des Benutzers ausgeführt werden (siehe auch M 5.69 *Schutz vor aktiven Inhalten*).

Wird die Funktionalität des Webserver-Dienstes mit Hilfe von Modulen erweitert, so müssen diese denselben Anforderungen wie der Webserver-Dienst selbst genügen. Zudem müssen Module nach dem Minimalprinzip ausgewählt werden. Module, die als Beispiele vom Webserver mit installiert werden und nicht benötigt werden, sollten gelöscht werden.

Sowohl Webserverdienste als auch die Module werden in der Regel permanent weiterentwickelt und als eigene Versionen veröffentlicht. Eine Ver-

sion eines Moduls, das vorher auf einer konkreten Version eines Webserver-Dienstes fehlerfrei ausgeführt werden konnte, kann unter einer späteren Version des Webserver-Dienstes zu Problemen führen. Auch eine aktuellere Version eines Moduls kann anderes als eine ältere Version auf einem Webserver-Dienst reagieren. Daher muss neben der Version des Serverdienstes, die eingesetzt werden soll, auch die konkrete Version des Moduls getestet werden.

Für manche Webserver-Dienste gibt es spezielle Sicherheitsrahmenwerke (z. B. mod_security für Apache), mit denen verschiedene Sicherheitsfunktionen implementiert werden können, um beispielsweise Eingaben zu filtern. Einzelne Sicherheitsfunktionen lassen sich zum Teil auch mit anderen Erweiterungen für Webserver-Diensten realisieren. So kann beispielsweise mit dem Modul mod_rewrite Anfragen regelbasiert weitergeleitet und somit gefiltert werden. Es ist zu entscheiden, ob und welche Sicherheitsrahmenwerke eingesetzt werden sollen.

**Aktive Inhalte**

Interaktive Funktionen in Web-Angeboten können auch durch Aktive Inhalte umgesetzt werden, die auf dem Client-System ausgeführt werden. Soweit es möglich ist, sollten diese Funktionalitäten mit dynamischen oder statischen Inhalten bereitgestellt werden.

Die verschiedenen Techniken, die unter dem Oberbegriff "Aktive Inhalte" zusammengefasst werden, unterscheiden sich unter anderem durch die Art, wie sie in eine HTML-Seite integriert werden. Code von Skriptsprachen wie JavaScript, JScript oder VBScript wird im Textformat direkt in den HTML-Code eingefügt oder in einer aus dem HTML-Code aufgerufenen Datei abgelegt. Als weitere Möglichkeit kann ausführbarer Code in eine HTML-Seite integriert werden, indem er im HTML-Code referenziert und über vorkompilierte Programm-Module wie Java-Applets oder Active-X-Controls aufgerufen wird.

Eine neue Technik im Bereich der Aktiven Inhalte ist AJAX (Asynchronous JavaScript and XML), das auf JavaScript und XML-basiert. Häufig wird auch Flash zu den Aktiven Inhalten gezählt, da in den neueren Versionen der Funktionsumfang von Flash über die Darstellung reiner Animationen hinausgeht und es damit nicht mehr nur als Plug-In betrachtet werden kann.

Aktive Inhalte bringen dadurch, dass auf dem Client-System "fremder" Code ausgeführt wird, eine Reihe von Sicherheitsproblemen mit sich. Browser-Hersteller und Anbieter von Plug-Ins versuchen zwar, diese Probleme durch Maßnahmen wie eingeschränkte Rechte für Java-Applets, Active-X Controls oder andere Plug-Ins zu begrenzen, trotzdem zählen Bedrohungen im Zusammenhang mit Aktiven Inhalten derzeit zu den häufigsten. Diese Bedrohungen sollten ein Webseiten-Anbieter im Blick behalten, wenn er in seinem Angebot Aktive Inhalte benutzt.

**Betriebssystem**

Eine sichere Konfiguration des Betriebssystems, auf dem der Webserver-Dienst installiert wurde, ist eine Grundvoraussetzung, um Informationen auf Webservern sicher bereitstellen zu können. Grundsätzlich sollten auf einem IT-System nur jene Dienste und Applikationen installiert sein, die für den Betrieb erforderlich sind. Dies bedeutet, dass eine Vielzahl nicht benötigter Applikationen (wie beispielsweise Compiler oder Editoren) entfernt werden sollten. Nach außen sollten auch nur die Dienste sichtbar sein, die für den Betrieb

unbedingt benötigt werden (siehe M 5.95 *Sicherer E-Commerce bei der Nutzung von Internet-PCs*).

Um möglichst wenig Information über das Betriebssystem und die darauf befindlichen Dienste preiszugeben, kann Banner-Spoofing verwendet werden. Dabei liefern die auf dem Server betriebenen Dienste nicht ihre korrekte Programmbezeichnung und Versionsnummer zurück, sondern ersetzen diese durch Falschinformationen. Dadurch ist es für einen Angreifer schwieriger, Rückschlüsse auf die tatsächlich vom System verwendeten Programme zu ziehen. Auch müssen alle Standard-Benutzerkonten entfernt beziehungsweise umbenannt werden. Ein Beispiel dafür ist das unter Windows-Betriebssystemen oftmals vorhandene Gastkonto. Privilegierte Benutzerkonten, wie "Administrator" oder "root", sollten deaktiviert und stattdessen eigene Benutzer mit den notwendigen administrativen Rechten angelegt werden.

Prüffragen:

- Wurde auf dem Webserver eine sichere Grundkonfiguration hergestellt?
- Kann der Webserver nur auf Informationen zugreifen, die sich innerhalb des WWW-Wurzelverzeichnisses befinden?
- Kann der Webserver nur lesend auf die abgelegten Informationen zugreifen?
- Werden die Administrationszugänge zum Webserver geschützt, so dass nur berechtige Administratoren hierauf zugreifen können?
- Wurde überprüft, welche Netzdienste, Applikationen und Webservermodule auf dem Webserver installiert und aktiviert sind und wurden alle nicht benötigten Dienste, Applikationen und Module deaktiviert oder ganz deinstalliert?
- Wird in Abhängigkeit der berechtigten Anwender und des Schutzbedarfs der Informationen der Zugriff auf ein Minimum beschränkt?
- Wird die Integrität und Vertraulichkeit der zwischen Webserver und Client übertragenen Informationen geschützt?

# M 4.361 Sichere Konfiguration von Webanwendungen

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen und durch den Baustein B 5.21 *Webanwendungen* ersetzt worden.

# M 4.362 Sichere Konfiguration von Bluetooth

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte Konfiguration zu überprüfen und wenn möglich zu ändern, da diese oft unsicher ist:

- Häufig sind bei Bluetooth-Geräten im Auslieferungszustand viele Dienste aktiviert, damit alle Möglichkeiten der Kommunikation mit anderen Geräten genutzt werden können. Nicht benötigte Dienste sollten stets deaktiviert werden. Sporadisch benötigte Dienste sollten nur bei Bedarf gezielt aktiviert und danach wieder deaktiviert werden.
- Die Bluetooth-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.
- Bluetooth-Geräte sollten möglichst wenig "offen" konfiguriert werden. Es sind nach Möglichkeit die Betriebsmodi non-discoverable, non-connectable und non-pairable bzw. non-bondable einzustellen.
- Die Bluetooth-Reichweite sollte auf die dafür vorgesehenen Bereiche beschränkt werden. Dafür sollte die Sendeleistung von Bluetooth-Geräten so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich gewählt werden. So sollte an z. B. an einem Notebook ein Bluetooth-Gerät Klasse 3 eingesetzt werden, wenn dieses hierüber an ein Mobiltelefon gekoppelt wird, das sich nur wenige Meter entfernt befindet.
- Falls möglich, sollten voreingestellte PINs sofort geändert werden.
- PINs sollten möglichst lang und zufällig gewählt sein.
- Authentisierung und Verschlüsselung sind dem Schutzbedarf angemessen zu wählen.
- Für die Nutzung in Umgebungen mit normalem Schutzbedarf sind die von Bluetooth bereitgestellten kryptographischen Verfahren, insbesondere für die Verschlüsselung, angemessen. Dies gilt auch unter Berücksichtigung der bisher bekannt gewordenen Schwachstellen. Wird höherer Schutzbedarf gefordert, sind zusätzliche Maßnahmen, die über die Möglichkeiten von Bluetooth hinausgehen, zu treffen.
- Für starke Verschlüsselung muss die Schlüssellänge mindestens 64 Bit betragen, und als Verschlüsselungsmodus darf nur Punkt-zu-Punkt-Verschlüsselung akzeptiert werden. Die Schlüssellänge sollte so groß wie möglich gewählt werden. Da sich die Länge des Verschlüsselungsschlüssels vom Benutzer nicht vorgeben lässt, sind nach Möglichkeit nur solche Geräte einzusetzen, die den genannten Anforderungen genügen.

Darüber hinaus ist es empfehlenswert, Bluetooth-Geräte regelmäßig mit entsprechenden Hilfsmitteln nach versteckten Diensten bzw. offenen Ports zu untersuchen.

Von den Geräteherstellern bereitgestellte Sicherheitspatches bzw. aktuellere Versionen der Firmware sollten nach Test und bei entsprechendem Sicherheitsbedarf eingespielt werden.

Damit Bluetooth-Komponenten sicher betrieben werden können, müssen alle damit gekoppelten Geräte sicher konfiguriert sein. Geeignete Sicherheitsempfehlungen für Clients sind in den entsprechenden Bausteinen der Schicht 3 beschrieben.

Prüffragen:

- Wurden alle Bluetooth-Komponenten ausreichend sicher konfiguriert?
- Wurden voreingestellte PINs, insofern möglich, geändert?

# M 4.363 Sicherer Betrieb von Bluetooth-Geräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Bluetooth-Geräte müssen in geeigneter Weise abgesichert werden. Im Folgenden wird beschrieben, welche Maßnahmen ergriffen werden sollten.

### Stationäre Geräte

Stationäre Geräte, bei denen Bluetooth als Kabelersatz verwendet wird, zum Beispiel zur Verbindung mit immer den gleichen Peripheriegeräten, sollten mit Authentisierung betrieben werden. Dabei sind Lösungen mit semipermanenten Verbindungsschlüsseln zu bevorzugen. Grundsätzlich sollte Verschlüsselung aktiviert werden.

### Mobile Geräte

Bluetooth-Geräte, die mobil verwendet werden und mit fremden Geräten (d. h. Geräten mit unbekanntem Sicherheitsniveau) kommunizieren, müssen besonders geschützt werden:

- Die Paarung zweier Geräte sollte immer in abhörsicherer Umgebung durchgeführt werden. Eine Umgebung kann als abhörsicher angesehen werden, wenn es keine Möglichkeit gibt, unbeobachtet per Bluetooth von außen einzudringen. Die Reichweite der eigenen Bluetooth-Geräte alleine ist nicht entscheidend.
- Lösungen mit semipermanenten Verbindungsschlüsseln sind zu bevorzugen.
- Die Paarung sollte nur mit vertrauenswürdigen Geräten erfolgen.

Bei Verlust oder Diebstahl eines mobilen (bzw. stationären) Geräts müssen alle zugehörigen Verbindungsschlüssel in den verbliebenen Geräten gelöscht werden. Dies geschieht im Allgemeinen durch Löschen des entsprechenden Eintrages in der Bluetooth-Geräteliste der verbliebenen Geräte.

### Verwendung von Secure Simple Pairing

Wenn beide zu paarende Geräte mindestens der Bluetooth-Spezifikation 2.1 + EDR entsprechen, sollte Secure Simple Pairing mit dem Sicherheitsmodus 4 mit dem Attribut authenticated verwendet werden (siehe M 3.79 *Einführung in Grundbegriffe und Funktionsweisen von Bluetooth*). Dienste, bei denen dies nicht unterstützt wird, sollten nicht genutzt werden.

### Hinweise zur Wahl von PINs bei Bluetooth ohne SSP

PINs sollten eine möglichst zufällige Folge aus den verwendbaren Zeichen sein, triviale PINs wie "0000" oder "1234" sind unbedingt zu vermeiden. Für eine ausreichende Sicherheit bei der Paarung zweier Bluetooth-Geräte ist eine ausreichend lange PIN notwendig. PINs sollten mindestens 6 Stellen lang sein. Die PIN ist im Normalfall nur bei der ersten Verbindungsaufnahme zwischen Geräten einzugeben (semipermanente Verbindungsschlüssel). Wird bei einem solchen Geräte-Paar zu einem unerwarteten Zeitpunkt vom Benutzer eine PIN-Eingabe verlangt, sollte dieser nach Möglichkeit darauf verzichten, bis er sich in abhörsicherer Umgebung befindet. Eine entsprechende Nutzereinweisung oder -schulung wird empfohlen.

**Weitere Schutzmaßnahmen**

Solange Bluetooth nicht benutzt wird, sollten die Bluetooth-Schnittstellen der Geräte deaktiviert bleiben. Ob dies tatsächlich der Fall ist, sollte sporadisch geprüft werden. Darüber hinaus sollten auf Bluetooth-Geräten weitere lokale Schutzmaßnahmen installiert bzw. aktiviert werden, soweit dies technisch möglich ist. Dazu zählen:

- Zugriffsschutz (z. B. Diebstahlsicherungen)
- Benutzerauthentisierung
- Schutz vor Schadprogrammen (z. B. Virenschutz)
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- Verschlüsselung des Endgeräts

Es sollte regelmäßig überprüft werden, dass alle getroffenen Sicherheitseinstellungen noch aktuell sind und ob diese Einstellungen auch greifen.

Weitere Informationen hierzu finden sich in den Bausteinen zur Endgeräte-Sicherheit. Im Zweifel sollten sich Anwender am Baustein B 3.208 *Internet-PC* orientieren und die zugehörigen Maßnahmen sinngemäß anwenden.

Prüffragen:

- Werden die Bluetooth-Schnittstellen aller Geräte deaktiviert, solange keine Bluetooth-Kommunikation erfolgt?
- Wird zum Verbinden mit anderen Bluetooth-Geräten Secure Simple Pairing verwendet?

# M 4.364 Regelungen für die Aussonderung von Bluetooth-Geräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wenn Bluetooth-Geräte außer Betrieb genommen werden, müssen alle sensiblen Informationen gelöscht werden. Hierbei müssen insbesondere die Authentikationsinformationen für den Zugang zu Bluetooth-Netzen und anderer erreichbarer Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Dies bedeutet, dass beispielsweise kryptographische Schlüssel sicher gelöscht und Zertifikate für digitale Signaturen gesperrt werden müssen.

Als Bluetooth-Geräte findet eine Vielzahl verschiedener Geräte Verwendung. Hierzu zählen unter anderem:

- Laptops
- PDAs, Smartphones und ähnliche Geräte mit Bluetooth-Unterstützung
- Bluetooth-fähige Telefone, Drucker und Kameras
- Bluetooth-fähige Peripheriegeräte wie beispielsweise Headsets, Mäuse, Tastaturen usw.

Die Bluetooth-Funktionalität ist typischerweise eine neben diversen anderen Funktionen bei diesen Endgeräten. Bei der Außerbetriebnahme dieser Endgeräte ist daher zu berücksichtigen, ob solche Geräte sicherheitskritische Bluetooth-Informationen beinhalten, die zu löschen, zu übertragen bzw. zu archivieren sind, z. B.:

- Informationen über den Benutzer des Endgerätes
- Zertifikate bzw. zugehörige private Schlüssel (für Benutzer oder Geräte)
- Informationen über verbundene Endgeräte (Pairing-Informationen)
- Schlüsselmaterial von Authentikationsverfahren wie z. B. Schlüssel für das Pairing zwischen Bluetooth-Endgeräten

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung der sicherheitsrelevanten Informationen zu nutzen. Bei Zertifikaten ist beispielsweise ein Eintrag in die entsprechende Zertifikatsrückruflisten (Certificate Revocation List, CRL) vorzunehmen, um das Zertifikat zu widerrufen.

Falls ein Bluetooth-Gerät gestohlen wird, sind mindestens alle oben aufgeführten Informationen zu berücksichtigen, und es ist dafür zu sorgen, dass diese Endgeräte keinen Zugriff mehr auf noch vorhandene Bluetooth-Geräte oder Netzstrukturen haben. Dies wird am Besten erreicht, indem die Pairing-Informationen zu den gestohlenen Endgeräten auf den noch vorhandenen Endgeräten gelöscht werden.

Prüffragen:

- Wird bei der Außerbetriebnahme von Bluetooth-fähigen Endgeräten darauf geachtet, dass die sicherheitskritischen Bluetooth-Informationen gelöscht werden?
- Sind geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung von sicherheitsrelevanten Informationen von Bluetooth-Geräten vorhanden?

# M 4.365 Nutzung eines Terminalservers als grafische Firewall

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Prinzipiell stellen Zugangsmöglichkeiten in ein unsicheres Netz und der Schutz der Grundwerte in einer sicheren IT-Infrastruktur einen Zielkonflikt dar.

Zum einen müssen beispielsweise Internetdienste mit aktiven Inhalten genutzt werden. Zum anderen erfolgt der Zugriff durch Anwendungen, die jeweils auf das unsichere Netz zugreifen müssen. In klassischen Client-Server Netzen werden diese Applikationen geschützt hinter Port,- Paket- oder Applikationsfiltern auf dem Client und im Kontext des Benutzers ausgeführt. Eine Kompromittierung der Client-Software bedroht Sicherheit des Clients, sowie die des internen Netzes. Terminalserver bieten hier, durch die Kapselung der Anwendungen auf einem separaten IT-System, ein zusätzliches Maß an Sicherheit, indem über den Terminalserver auf das unsichere Netz zugegriffen wird. Ein Terminalserver, der anstelle des Clients auf das unsichere Netz zugreift, wird als grafische Firewall bezeichnet.

Viren, Würmer oder andere Schadsoftware können bei konsequenter Planung und Umsetzung einer grafischen Firewall zu keiner Zeit auf dem Client des Benutzers ausgeführt werden, da lediglich Bildinformationen, sowie Ein- und Ausgabedaten zwischen dem Terminalserver und dem Terminal übertragen werden.

Bei der Konzeption einer grafischen Firewall spielen im Wesentlichen zwei, gegebenenfalls ergänzende anzustrebende Zielsetzungen, eine Rolle.

- Der Schutz der internen IT-Systeme vor dem unsicheren äußeren Netz.
- Die Verhinderung, dass keine vertraulichen Daten in das externe Netz durch technische Mängel, Schadsoftware oder durch Sabotage entweichen können. Die hierzu erforderliche strikte Unterbindung jeglichen Informationsaustauschs zwischen dem internen und dem externen Netz, etwa über den Dateitransfer oder die Zwischenablage, schränkt jedoch den praktischen Nutzen erheblich ein.

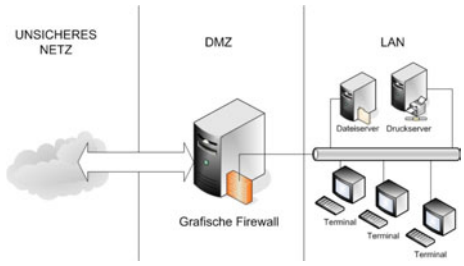



Abbildung: Grafische Firewall in einer separierten Zone

In beiden Fällen ist aber für die Wirksamkeit der Maßnahme wichtig, dass die Kommunikation in das unsichere Netz ausschließlich über die grafische Firewall erfolgt. Zudem sollte der Terminalserver, wie in der obigen Abbildung zu sehen, in einer von schutzbedürftigen Bereichen getrennten Zone (DMZ, demilitarisierte Zone des Sicherheitsgateways) untergebracht werden, um im Falle einer Kompromittierung das interne Netz nicht zu gefährden.

Hierbei ist es sinnvoll, auf der Route zwischen den beiden Netzsegmenten nur das Transportprotokoll und die Ports des Terminalserver-Dienstes zuzulas-

sen, um die Zahl der Angriffsvektoren in das sichere Netz zu minimieren. Eine Auflistung der Standardeinstellungen einiger Terminalserver-Dienste enthält die folgende Tabelle.

| Dienst | Protokoll | Server-Port | Server-Zone |
|---|---|---|---|
| Windows Terminalserver | RDP | 3389 | DMZ |
| Citrix Presentation Server | ICA | 1494 | DMZ |
| X-Window | X11 | 6000 | LAN |
| X-Window mit SSH | X11+SSH | 22 | DMZ |
| VNC | VNC | 5900 | DMZ |

Tabelle: Protokolle und Portnummern verschiedener Terminalserver-Lösungen

Gegebenenfalls ist es notwendig, weitere Ports zu öffnen, um z. B. den Zugriff auf den Dateiserver oder Druckdienste im LAN zu gewähren. Um dies zu vermeiden, kann bei manchen Lösungen der Datenverkehr für diverse Dienste direkt im Datenstrom des Terminalserver-Protokolls übermittelt werden. Protokolle, die diese Option mittels virtueller Kanäle bieten, sind unter anderem das Protokoll RDP des Windows Terminalserver oder ICA unter Citrix Metaframe, Presentation Server oder XenApp. Darüber hinaus besteht die Möglichkeit, Tunnelverbindungen mittels SSH z. B. für das X-Window System zu nutzen, das dazu von Haus aus nicht in der Lage ist.

Ferner sind bei der Verwendung von X-Window die technischen Besonderheiten des X11 Protokolls zu berücksichtigen. Während sich bei den sonst gängigen Verfahren das Terminal die Ausgabe vom Terminalserver holt, senden bei X-Window die Anwendungen und damit in diesem Fall die grafische Firewall, ihre Bildschirmausgaben aktiv an den X-Server, der auf dem Client des Benutzers ausgeführt wird. Als Konsequenz ist im Router der Port 6000 von der DMZ in das LAN durchzuleiten. Für jeden weiteren Client im LAN, der über den Terminalserver kommuniziert, ist ein weiterer Port oberhalb der Portnummer 6000 zu öffnen. Dies führt in diesem Szenario zu einer großen Anzahl von Zugängen in das interne Netz und sollte vermieden werden. Stattdessen empfiehlt sich der Aufbau der Verbindung über einen SSH-Tunnel oder ein VPN.

Aufgrund der besonderen Gefährdung der grafischen Firewall, ist der Einsatz eines Virenscanners, gemäß M 4.3 *Einsatz von Viren-Schutzprogrammen*, obligatorisch. Die Maßnahme M 5.163 *Restriktive Rechtevergabe auf Terminalservern* und M 4.368 *Regelmäßige Audits der Terminalserver-Umgebung* sorgen dafür, dass das Prinzip der geringsten Berechtigung herrscht.

Prüffragen:

- Erfolgt die Kommunikation in das unsichere Netz ausschließlich über die grafische Firewall?
- Ist der Terminalserver, der als grafische Firewall eingesetzt wird, in einer von schutzbedürftigen Bereichen getrennten Zone (DMZ) untergebracht?

# M 4.366 Sichere Konfiguration von beweglichen Benutzerprofilen in Terminalserver-Umgebungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um Anwendungen für eine größere Anzahl an Benutzern bereitzustellen, werden häufig mehrere Terminalserver in einem Verbund eingesetzt. Dieser wird auch als Terminalserver-Farm bezeichnet.

Bei dem hier genannten Szenario entstehen einige spezifische Sicherheitsanforderungen an die Benutzerprofile. In Benutzerprofilen werden individuelle Benutzereinstellungen, Endgerätekonfigurationen (beispielsweise für Drucker) und gegebenenfalls auch selbst erstellte Dateien für jeden Anwender gespeichert.

In Verbünden von Terminalservern ist zumeist durch die Benutzer nicht vorherzusehen, mit welchen Terminalservern sie eine Sitzung aufbauen. Die Verwaltungsdienste der jeweiligen Terminalserver-Lösungen regeln dies automatisch, zumeist unter Berücksichtigung der Auslastung der einzelnen Server in der Farm.

Meldet sich der Anwender an, wird sein individuelles Profil von diesem Server geladen. Wurden keine entsprechenden Vorkehrungen getroffen, ist dies das lokal auf dem Server abgespeicherte Profil. Meldet sich der Benutzer nun ab und ein weiteres Mal an, kommt sehr wahrscheinlich eine Verbindung mit einem anderen Terminalserver zustande und es wird damit auch ein neues lokales Benutzerprofil erzeugt. Die auf dem ersten Terminalserver hinterlegten Einstellungen und Dateien sind erst dann wieder für den Nutzer erreichbar, wenn er sich zufällig mit genau diesem Server verbindet.

An dieser Stelle wird deutlich, dass eine zentrale Ablage der Dateien auf einem Dateiserver bei dem Einsatz von Terminalserver-Farmen notwendig ist, sollen Änderungen des Benutzers innerhalb seines Profils erhalten bleiben. Diese Methode zur Speicherung der Profildaten wird auch als "*bewegliches Profil"* bezeichnet.

Es ist hierbei jedoch zu beachten, dass in Anwendungsszenarien, in denen direkt auf einzelne Anwendungen anstatt eine vollständige Benutzeroberfläche (Desktop) zugegriffen wird, dies gegebenenfalls nicht erforderlich oder gewünscht ist.

Bei dem Einsatz von Windows Servern hat die Auswahl von beweglichen Benutzerprofilen, dort auch als "*roaming profile"* bezeichnet, einige Nachteile. So hat der Anwender, wie beabsichtigt, zahlreiche Möglichkeiten zur Änderung des Aussehens und Verhaltens seiner Benutzersitzung. Allerdings kann so auch sehr leicht durch einen Fehler des Benutzers das Sitzungsprofil unbenutzbar werden. Zudem wächst ein derart konfiguriertes Profil sehr schnell in seiner Größe an. Es benötigt dann lange Zeit um vom Dateiserver bei jeder Anmeldung geladen zu werden und erhöht so außerdem die Netz- und Serverlast.

Daher empfiehlt es sich, auf sogenannte "*mandatory profiles"* zurückzugreifen, die die Geschwindigkeit der Terminalserver erhöhen und die verhindern, dass Anwender sich versehentlich von der Nutzung ausschließen.

Dieser Profiltyp kann ebenfalls auf einem entfernten Server abgelegt werden, angelegte Dateien und Änderungen an Einstellungen werden jedoch nur für die Dauer der Sitzung gespeichert. Durch entsprechend erstellte Stapelverarbeitungsprogramme (Scripts) können vor dem endgültigen Schließen gezielt bestimmte Bestandteile des Profils (z. B. neu angelegte Dokumente) auf dem Dateiserver gesichert werden.

Es sollte zudem eine Begrenzung der Größe des Profils administrativ vorgegeben werden, um ein Anwachsen über ein tolerables Maß hinaus zu unterbinden.

Prüffragen:

- Wurde ein Verfahren definiert und umgesetzt um die Dateien von Benutzern, die innerhalb einer Terminalserver-Sitzung erstellt wurden, auf allen Terminalservern einer Terminalserver-Farm synchron verfügbar zu halten.
- Wurde eine maximale Obergrenze für die Speichernutzung des Benutzerprofils auf den Terminalservern festgelegt?
- Falls ja, wurde die Obergrenze der Benutzerprofile auf Terminalservern dokumentiert und die Benutzer darüber informiert?

# M 4.367 Sichere Verwendung von Client-Applikationen für Terminalserver

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Terminalserver-Dienste werden oft über Client-Systeme mit einem eigenständigen Betriebssystem (Fat Client) bereitgestellt. Dem Benutzer stehen in einer solchen Umgebung oft potentiell Möglichkeiten zur Verfügung, die Konfiguration oder die Client-Software abzuändern. Dieser kann dann etwa die Sicherheit seiner eigenen Verbindung herabsetzen oder Details über den internen Aufbau des Informationsverbunds an unberechtigte Dritte offenbaren.

Um dies zu verhindern sollten, wenn möglich alle Verbindungsparameter, wie die Verschlüsselungstiefe und das Verfahren administrativ auf der Serverseite vorgegeben werden. Auch Informationskanäle, wie die Einbindung von lokalen Laufwerken, Druckern, Schnittstellen oder die Zwischenablage sollten so gesteuert werden. Aber nicht immer ist dies innerhalb der eingesetzten Terminalserver-Lösung zentral, benutzerbezogen sowie für alle Einstellungen erzielbar und zudem können die Anforderungen der Anwender variieren.

In Terminalserver-Umgebungen mit normalem Schutzbedarf ist in den Benutzerrichtlinien vorzusehen, dass der Anwender in keinem Fall Konfigurationsdaten, etwa aus .ICA- oder .RDP-Dateien, an unberechtigte Personen versenden darf. Zudem dürfen keine vorgegebenen Einstellungen verändert oder Zugänge zu abweichenden Serveradressen ausprobiert werden. Weitere Hinweise zur Gestaltung angemessener Richtlinien können der Maßnahme M 2.464 *Erstellung einer Sicherheitsrichtlinie zur Terminalserver-Nutzung* entnommen werden. In Informationsverbünden mit hohem und sehr hohem Schutzbedarf genügen diese organisatorischen Festlegungen allein nicht.

Eine mögliche Alternative stellt hier die Nutzung von nicht konfigurierbaren Client-Programmen, wie die so genannte Gray Version des Citrix Program Neighborhood, dar. Voraussetzung ist in diesem Fall, dass der Client, auf der die Terminalsoftware bereitgestellt wird, unter der vollen Kontrolle der IT-Administration steht. Zudem muss ein Schreibzugriff auf die Dateien der Client-Software wirksam unterbunden werden.

Nicht geeignet für dieses Verfahren sind jedoch Entwicklersysteme, bei denen, z. B. mittels Softwareanalysewerkzeugen (Debugger) oder Netzwerkmonitoren (Sniffer) der Verbindungsaufbau überwacht oder manipuliert werden kann. Insbesondere eine automatische Authentisierung (Pass-Through-Authentication) kann so leicht gebrochen werden.

Wird auf die lokale Installation der Terminalsoftware und deren Konfiguration auf den Rechnern der Anwender verzichtet, können die oben genannten Sicherheitsmängel vermieden werden. Realisierbar wird dies durch den Einsatz von Portallösungen, wie beispielsweise:

- Microsoft Terminalserver Web-Access
- Citrix Access Gateway
- NX-Builder für X-Window Systeme

Für eine Benutzerauthentisierung gegenüber einer Porttallösung über ein unsicheres Netz wird empfohlen, auf eine Zwei-Faktor-Authentisierung zurückzugreifen.

Auch bei der Auslieferung von Client-Software für Terminalserver über Webserver, sind restriktive Vorgaben zur Konfigurierbarkeit des Clients üblicherweise nicht Standard. Sie müssen daher vor der Inbetriebnahme der Terminalserver-Umgebung administrativ festgelegt werden. Überdies sind für das Portal die korrespondierenden Maßnahmen aus dem Baustein B 5.4 *Webserver* zu berücksichtigen.

Prüffragen:

- Wurden alle Verbindungsparameter, wie die Verschlüsselungstiefe und das Verfahren, administrativ beim Terminalserver vorgegeben?
- Sind die Anwender der Terminalserver über Ihre Pflichten zum Schutz der Vertraulichkeit von Konfigurationsdaten informiert?
- Ist bei Systemen mit hohem oder sehr hohem Schutzbedarf spezielle Client-Software für die Nutzung des Terminalservers vorgesehen oder werden Portallösungen genutzt?

# M 4.368 Regelmäßige Audits der Terminalserver-Umgebung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Revisor

Bei allen Komponenten der Terminalserver-Infrastruktur muss regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Neben den Terminalservern selbst, zählen hierzu die Verwaltungsdienste wie Sitzungsdatenbanken und Lizenzserver, aber auch Elemente der Sicherheitsinfrastruktur.

Insbesondere sollten Authentisierungsserver und Sicherheitsgateways an den Übergangspunkten zwischen zwei Netzen, zu denen die Terminalserver-Umgebung Verbindungen hat, regelmäßig geprüft werden. Dies betrifft auch Router, Firewalls und VLAN bildende Switches. Dabei sind auch Webportale (siehe B 5.4 *Webserver*) zu berücksichtigen, die als Zwischenglied Applikationen bereitstellen können.

Protokolldaten der einzelnen Komponenten können dabei wichtige Hinweise zu kritischen Vorkommnissen geben. Bei der Protokollierung fallen zumeist sehr viele Einträge an, so dass diese nur mit Hilfe eines Werkzeugs sinnvoll ausgewertet werden können.

Bei der Untersuchung auf eventuelle Sicherheitsereignisse sollten Einträge über An- und Abmeldevorgänge sowie Nutzungszeiträume von Benutzern analysiert werden. Überdies ist auf nicht autorisierte Sitzungsspiegelungen zu achten.

Ein bedeutender Aspekt in Bezug auf die Verfügbarkeit der Terminalserver-Umgebung ist die Auslastung von Ressourcen wie Speicher, Prozessor und Festplattenplatz, aber auch die genutzte Bandbreite im Netz oder die Anzahl der aktiven Sitzungen. Um hier Entwicklungen korrekt beurteilen zu können, müssen im Vorfeld entsprechende Analysen vorgenommen werden (siehe M 2.465 *Analyse der erforderlichen Systemressourcen von Terminalservern* und M 5.162 *Planung der Leitungskapazitäten beim Einsatz von Terminalservern*). Nur so sind verlässliche Rückschlüsse auf Engpässe in der individuellen Terminalserver-Umgebung möglich.

Neben den Informationen, die sich aus Protokolldaten entnehmen lassen, ist es unabdingbar, die sichere Grundkonfiguration der Terminalserver zu kontrollieren. Hier sollten zumindest stichprobenartig die durchführten Maßnahmen zur Härtung der Terminalserver-Systeme, deren Dateisysteme und der nachgelagerten Dienste inspiziert werden.

Ein besonderes Augenmerk sollte auf vergessene temporäre Dateien gelegt werden, die bei der automatischen Installation anfallen können, denn darin befinden sich oft kritische Informationen, wie z. B. unverschlüsselte Anmeldedaten.

Weiterhin müssen die Client-Systeme, über die auf Terminalserver zugegriffen wird, regelmäßig überprüft werden. Bei einer größeren Anzahl sollte dies zumindest stichprobenartig geschehen. Zu kontrollieren ist zunächst die Konfiguration von gegebenenfalls lokal installierter Client-Software auf nicht autorisierte Veränderungen. Werden auf den Terminalserver-Betrieb spezialisierte Druckertreiber eingesetzt, sollten auch diese in die Untersuchung eingebunden werden. Weiterhin ist bei Clients mit einem eigenständigen Betriebssy-

stem (Fat Clients) auch der Versionsstand des Betriebssystems sowie Aktualität und Integrität der Client-Software und des Virenschutzes zu beachten.

Neben den vorgenannten technischen Mitteln zur Analyse der Sicherheit, können Interviews der Anwender Probleme in der Verlässlichkeit oder Sicherheitsvorfälle aufdecken.

Falls Unregelmäßigkeiten oder Schwachstellen festgestellt werden, müssen diese dokumentiert werden, und festgehalten werden, wie sie zu verfolgen sind.

Neben den Audits der einzelnen Terminalserver-Komponenten sollte auch zyklisch eine Revision der Richtlinie zur sicheren Terminalserver-Nutzung durchgeführt werden. Es sollte hierbei eine Bewertung erfolgen, ob die ergriffenen Maßnahmen zur Absicherung der Terminalserver-Umgebung noch dem Stand der Technik entsprechen und ob der zu Grunde gelegte Schutzbedarf nach wie vor gültig ist.

Außerdem sollte immer wieder hinterfragt werden, ob alle Benutzer über die erforderlichen und auf den Terminalserver-Betrieb bezogenen, Sicherheitsmaßnahmen informiert sind und diese umsetzen.

Es muss weiterhin festgelegt werden, wer die Protokolle und Audit-Daten inspiziert. Hierbei muss eine angemessene Trennung zwischen Ereignisverursacher und -auswerter (z. B. Administrator und Auditor) vorgenommen werden. Für alle erhobenen Daten sind insbesondere die gesetzlichen Anforderungen des Datenschutzes zu beachten.

Prüffragen:

- Werden regelmäßig Sicherheitsaudits bei den Terminalservern durchgeführt?
- Werden festgestellte Unregelmäßigkeiten bei den Terminalservern dokumentiert und verfolgt?

# M 4.369 Sicherer Betrieb eines Anrufbeantworters

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Administrator

Anrufbeantworter können zusätzlich zum Telefon an das interne Telefonnetz angeschlossen werden und können eingehende Gespräche oder Nachrichten in gesprochener Form aufzeichnen, wenn der Angerufene nicht erreichbar ist. Eine weitere Möglichkeit ist auch, nur eine Mitteilung über die Abwesenheit abzuspielen, das Hinterlassen einer Nachricht durch den Anrufer jedoch nicht zuzulassen. Anrufbeantworter können entweder als externes Gerät (Stand-Alone) zusätzlich zum Telefon an das interne Telefonnetz angeschlossen werden oder sind bereits im Telefon (integrierter Anrufbeantworter) oder in der TK-Anlage enthalten. Wird VoIP eingesetzt, können bei vielen VoIP-Anlagen die Sprachnachrichten dem Empfänger per E-Mail zugeschickt werden (Voice-Mail).

Technisch gesehen lassen sich Anrufbeantworter in zwei Klassen einteilen: analoge oder digitale Speichermöglichkeit. Bei analogen Geräten werden die Nachrichten auf Audiokassetten (oft Mini- bzw. Microkassetten) aufgenommen. Inzwischen werden solche Geräte allerdings nicht mehr hergestellt. Bei digitalen Anrufbeantwortern, die mittlerweile häufig direkt im Telefon oder in der Telefonanlage integriert sind, werden die Nachrichten auf einem Speichermodul im Gerät oder auf einem Massenspeicher, wie einer Festplatte, aufgezeichnet. Bei einigen älteren digitalen Anrufbeantwortern mit Speichermodulen können die gespeicherten Informationen (Ansagetexte und Nachrichten) bei einem Stromausfall verloren gehen. Daher sollten bei diesen vorhandene (Puffer)-Batterien regelmäßig ausgewechselt werden.

Generell sollten keine schutzbedürftigen Informationen auf dem Anrufbeantworter hinterlassen werden. Beim Ansagetext sollte darauf geachtet werden, dass die Anrufer keine Informationen erhalten, die für Social Engineering (siehe G 5.42 *Social Engineering*) ausgenutzt werden können. Hierzu gehören beispielsweise der momentane Aufenthaltsort oder die (längerfristige) Dauer der Abwesenheit des Angerufenen. Im Ansagetext sollte darauf hingewiesen werden, keine vertraulichen Informationen auf dem Anrufbeantworter zu hinterlassen.

Telefone mit eingebautem Anrufbeantworter verfügen neben der Anrufaufzeichnung und dem Abhören der eingegangenen Nachrichten oft noch über weitere Leistungsmerkmale wie Fernabfrage, Umleitung eines Anrufes, Raumüberwachung oder Fernwirkung auf angeschlossene elektrische Geräte. Diese Funktionen lassen sich bei manchen Telefonen während eines Anrufes, der vom Anrufbeantworter angenommen wird, fernsteuern. Da die Fernabfrage- und Fernsteuerungsmöglichkeit ein erhebliches Gefährdungspotenzial darstellt, sollte sie nach Möglichkeit deaktivierbar sein und im Falle einer Nutzung durch einen Sicherungscode (Geheimzahl, PIN) geschützt werden. Dieser sollte zumindest drei- bis vierstellig und frei wählbar sein. Alle werksseitig eingestellten Codes sollten vor Inbetriebnahme verändert werden. Der Sicherungscode ist wie ein Passwort zu hinterlegen (siehe hierzu M 2.22 *Hinterlegen des Passwortes*) und regelmäßig zu ändern.

Es sollte darauf geachtet werden, dass sich bei der Eingabe der Codes keine Fremden in der Nähe aufhalten, die diesen beobachten oder erlauschen könn-

ten. Ein zusätzlicher Schutz gegen das Abhören der Nachrichten durch Unbefugte oder den Missbrauch von anderen Leistungsmerkmalen ist eine Sperrschaltung, die den Anrufbeantworter nach drei vergeblichen Versuchen die Verbindung unterbrechen lässt. Besser noch sind Geräte, bei denen die Fernabfragefunktionen nach drei vergeblichen Versuchen vollkommen gesperrt werden und nur noch am Gerät selbst wieder aktivierbar sind. Auch Sperrzeiten, die nach jedem Fehlversuch verlängert werden, sind sinnvoll. Neben der vom Benutzer initiierten Fernabfrage sind einige Geräte in der Lage, den Benutzer über neu eingegangene Nachrichten via Anruf auf eine vorher angegebene Rufnummer oder per SMS auf das Mobiltelefon zu informieren.

Unabhängig davon, wie die eingegangenen Nachrichten abgehört werden, sollten die gespeicherten Gespräche regelmäßig abgehört werden. Nicht mehr benötige Aufzeichnungen sollten regelmäßig gelöscht werden, damit das Speichermedium (digitaler Speicher oder Audiokassette) des Anrufbeantworters nicht erschöpft und eine Aufzeichnung der Gespräche unmöglich macht oder alte Nachrichten überschrieben werden. Aus diesem Grund sollte auch die maximale Sprechdauer pro Anruf begrenzt werden, da ein Angreifer den begrenzten Speicher des Anrufbeantworters ansonsten mit unsinnigen Informationen füllen könnte und damit weitere Nachrichten verhindert. Ist das Löschen bei analog aufzeichnenden Geräten nicht möglich, sollte das Magnetband regelmäßig an den Anfang zurückgespult werden, damit die Aufzeichnung neuer Gespräche gespeicherte alte Nachrichten überschreibt.

Jeder Anwender, der einen Anrufbeantworter in seinem Bereich einsetzt, sollte sich mit der Bedienung vertraut machen und so Möglichkeiten und Grenzen des Gerätes kennen lernen. Hierfür sollten entsprechende Bedienungsanleitungen oder Benutzungshinweise zur Verfügung gestellt werden.

Prüffragen:

- Wird die Fernabfrage der Anrufbeantworter zugelassen und in diesem Fall durch eine PIN geschützt?
- Wird im Ansagetext des Anrufbeantworters darauf hingewiesen, dass keine vertraulichen Informationen auf den Anrufbeantworter gesprochen werden sollen?
- Werden die neu eingegangenen Nachrichten auf dem Anrufbeantworter regelmäßig abgehört und nicht mehr benötigte Nachrichten gelöscht?
- Wurde die Nachrichtendauer auf dem Anrufbeantworter zeitlich beschränkt?

# M 4.370 Einsatz von Anoubis unter Unix

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Angriffe auf IT-Systeme basieren oft auf dem Missbrauch von Zugriffsrechten. Je großzügiger solche Rechte vergeben werden, desto einfacher werden erfolgreiche Angriffe. Im schlimmsten Fall kann z. B. ein Fehler im Browser oder eine unvorsichtige Einstellung in dessen Konfiguration einem Angreifer vollen Zugriff auf alle Daten eines Anwenders ermöglichen.

Da ein Browser in der Regel mit den Rechten des Benutzers ausgeführt wird, ist der Zugriff auf Daten und Verzeichnisse, auf die er Schreibrechte hat, nicht weiter beschränkt. Hier liegt das Grundproblem: Die Rechtevergabe unter Unix erfolgt oft benutzerbasiert, d. h. sie weist Benutzern individuelle Zugriffsrechte zu. Ein Prozess, der mit den Rechten eines Benutzers ausgeführt wird, besitzt dessen gesamte Rechte. Dadurch hat eine ausgeführte Anwendung wesentlich mehr Rechte, als sie für ihren eigentlichen Zweck benötigt. Ein Benutzer hat in der Regel praktisch keine Kontrolle über die Zugriffsrechte der von ihm ausgeführten Anwendungen. Im Falle von Fehlern in Applikationen sind die Vertraulichkeit, Integrität und Verfügbarkeit der Benutzerdaten unmittelbar bedroht.

Anoubis ist eine freie Software, um Applikationen zu kontrollieren und Anforderungen an die Datenintegrität bei Unix-Systemen durchzusetzen. Dazu werden Anwendungen und Dateien sowie zugehörige Prüfsummen berechnet und digital signiert. Die Verwaltung und Überprüfung der hinterlegten Prüfsummen sollte mit Hilfe der grafischen Benutzeroberfläche von Anoubis durchgeführt werden.

**Einsatz von Anoubis**

Da es sich bei Anoubis um eine individuell konfigurierbare Lösung mit zahlreichen Komponenten wie Application Level Firewall, Sandbox, Playground und einem sicheren Dateisystem handelt, sollten sich die zuständigen Administratoren mit den Möglichkeiten der Lösung vertraut machen. Nach der Installation schützt Anoubis alle Unix-Rechner, auf denen es installiert ist, zunächst durch eine Standardkonfiguration. Diese sollte mit Hilfe von Richtlinien, die von Anoubis als Policies bezeichnet werden, bedarfsgerecht an unterschiedliche Anwendergruppen oder Anwendungsszenarien angepasst werden. Policies werden unter Anoubis zentral vom Systemadministrator vorgegeben und können von den Benutzern nicht aufgehoben oder umgangen, sondern nur weiter eingeschränkt werden. Vertiefende Informationen zu Policies sind im Installations- und Konfigurationshandbuch von Anoubis zu finden. Um auf unterschiedliche, aber typische Einsatzumgebungen besser reagieren zu können, können auf Basis geeigneter Policies vorgefertigte Profile erstellt werden. Vorgefertigte Profile erleichtern es den Benutzern, das für die jeweilige Einsatzumgebung passende Profil auszuwählen, ohne Policies anfassen zu müssen. Die Administratoren sollten daher geeignete Profile erstellen und die Benutzer in deren korrekte Anwendung einweisen.

Profile können zum Beispiel bei Laptops genutzt werden, die an unterschiedlichen Orten in unterschiedlichen Netzen eingesetzt werden. So sind in Abhängigkeit von der Umgebung und je nach Anforderungen speziell angepasste Policies für folgende Umgebungen denkbar:

- Büro

Für die Arbeit im Büro braucht das Profil auf dem Laptop nicht besonders streng zu sein, wenn das lokale Netz durch Sicherheitsgateways geschützt ist und der Benutzer ohne große Einschränkung die internen Dienste nutzen können soll. Zugriffe auf alle möglichen internen und ausgewählten externen Dienste sind in diesem Fall oft erlaubt. Müssen ausgewählte Netzdienste auf dem Client bereitgestellt werden, um beispielsweise den Laptop zu konfigurieren, könnte das Profil so eingestellt werden, dass nur in dieser sicheren Umgebung andere IT-Systeme auf den Laptop zugreifen dürfen.

- Zu Hause
  Hier gibt es oft kein externes Sicherheitsgateway, das den Laptop schützen könnte. Deshalb könnte hier ein Profil Zugriffe von außen verbieten und nur bestimmten Applikationen Verbindungen ins Internet erlauben. Beispielsweise könnte ein Profil vorsehen, dass nur der Browser HTTP-Verbindungen öffnen, der VPN-Client eine Verbindung ins interne Netz herstellen und der Virenscanner Updates ziehen darf.
- Fremdes Netz
  Will der Benutzer in öffentlichen Umgebungen, wie z. B. auf einem Flughafen über ein WLAN arbeiten, muss das eingesetzte Profil sehr restriktiv sein. Nur der Browser sollte sich über HTTP in das Internet verbinden dürfen, der E-Mail-Client nur über verschlüsselte Kanäle (POP3s und IMAPs) zum Mail-Hoster, und der VPN-Tunnel sollte nur zur Gegenstelle in der Firma aufgebaut werden dürfen. Alle anderen Verbindungen sollten geblockt werden.

Der Benutzer braucht lediglich das geeignete Sicherheitsprofil in der Benutzeroberfläche auszuwählen und kann dann in jeder Umgebung die vorher festgelegten Vorgaben erfüllen. Eine Einweisung der Benutzer wird empfohlen, um eine korrekte Profil-Auswahl zu gewährleisten.

**Kontrolle der Applikationen**

Soll für bestimmte Applikationen der Zugriff auf das Netz oder das Dateisystem eingeschränkt werden, so können in Anoubis für diese Applikationen entsprechende Regeln erzeugt werden. Soll der PDF-Reader z. B. keine Updates selbstständig herunterladen oder sollen keine Dateien außerhalb eines vorgegebenen Dateiordners geschrieben werden können, so kann eine entsprechende Regel für eine Application Level Firewall und eine Sandbox angelegt werden, die diese Einschränkungen durchsetzen.

Um sicherzustellen, dass keine gefälschten oder durch ein Schadprogramm eingeschleusten Applikationen ausgeführt werden, sollten solche Dateien mit einer digital signierten Prüfsumme versehen werden. Darüber hinaus müssen in Anoubis SFS-(Sicheres File System)-Regeln eingerichtet werden, die den lesenden Zugriff und die Ausführung von veränderten Dateien, sowie die Ausführung unsignierter Dateien verbietet. Dadurch kann die Applikation nicht mehr ausgeführt bzw. keine gefälschte Konfigurationen mehr eingelesen werden. Je nach Konfiguration von Anoubis können Benutzer bei Verstößen gewarnt werden.

**Definition und Nachvollziehbarkeit von Regelsätzen**

Anoubis kann über eine grafische Benutzeroberfläche konfiguriert werden. Mit einem Regeleditor können Regelsätze erstellt und geändert werden. Darüber hinaus können Regelsätze für einzelne Anwendungen mit Hilfe eines Regel-Wizards erzeugt werden. Dieser ermöglicht auch unerfahrenen Benutzern, Regelsätze zu erstellen.

Ein Prozessbrowser zeigt erstellte Regelsätze bzw. die Standardkonfiguration für die jeweilig ausgewählte Applikation an.

**Abgesicherte Bereiche zum Schutz des Dateisystems**

Um zu verhindern, dass Prozesse in das Dateisystem schreiben können, sollten Anwendungen in dafür vorgesehenen abgesicherten Bereichen ("Playgrounds") ausgeführt werden. Wird z. B. ein Browser in einem Playground verwendet, hinterlässt er, nachdem der Playground gelöscht wurde, keinerlei Spuren im Dateisystem.

Sollen einzelne Dateien aus einem abgesicherten Bereich ins Dateisystem übertragen werden, dann muss der Benutzer diesen Transfer willentlich in der Benutzeroberfläche durchführen Dabei sollte ein Datentransfer in das Produktivsystem je nach Bedarf durch einen Virenscanner abgesichert werden. Hierfür müssen geeignete Virenscanner installiert und konfiguriert werden. Darüber hinaus kann der Benutzer am Ende einer Session entscheiden, ob Daten innerhalb des abgesicherten Bereichs behalten oder gelöscht werden.

Prüffragen:

- Hat sich der Administrator mit allen Möglichkeiten von Anoubis vertraut gemacht?
- Wurden für unterschiedliche Anwendergruppen oder Anwendungsszenarien geeignete Anoubis-Policies erstellt?
- Wurden die Benutzer in die Anwendung der Anoubis-Profile eingewiesen?
- Sind die relevanten Anwendungen und Dateien, die mit Anoubis geschützt werden sollen, mit einer signierten Prüfsumme versehen?
- Wurden unter Anoubis SFS-Regeln konfiguriert, die den Zugriff auf sensible Dateien oder Anwendungen verhindern, die keine gültige Prüfsumme haben?
- Sind unter Anoubis für die Benutzung des Playgrounds geeignete Virenscanner installiert und konfiguriert?

# M 4.371 Konfiguration von Mac OS X Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach der Installation von Mac OS X auf den Clients erfolgt deren Konfiguration. Die jeweils vorzunehmenden Einstellungen hängen wesentlich vom Verwendungszweck ab. In dieser Maßnahme wird auf die sichere Client-Konfiguration eingegangen.

Folgende Punkte sind für die sichere Grundkonfiguration eines Mac OS X Systems zu beachten:

### Aktualisierung des Betriebssystems

Grundsätzlich sollte ein Betriebssystem nach der Installation sofort aktualisiert werden, um bekannte Fehler in Softwarekomponenten zu beheben. Weiterhin sollte regelmäßig überprüft werden, ob Programmaktualisierungen vorliegen. Unter Mac OS X kann dies in den Systemsteinstellungen unter "Softwareaktualisierung" konfiguriert werden.

Um den Update-Server *swupdate.apple.com* zu verwenden, kann folgender Kommandozeilen-Befehl genutzt werden:

sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL http://swupdate.apple.com:8088/index-leopard-snowleopard.merged-1.sucatalog

Um das Betriebssystem per Kommandozeilen-Befehl zu aktualisieren, kann im Terminal der Befehl "*softwareupdate --download --all --install*" ausgeführt werden. Zur Installation von Updates werden zwingend Administratorrechte benötigt. Existiert ein interner Update-Server im lokalen Netz, sollte dieser benutzt werden.

### Internen Apple-Update-Server festlegen

Um das Betriebssystem Mac OS X auf dem neuesten Stand zu halten, kann die integrierte Update-Funktion benutzt werden. Es empfiehlt sich, einen eigenen internen Update-Server zu nutzen. Damit können interne Netzverbindungen genutzt und höhere Transferraten erreicht werden. Es ist weniger Datenaustausch mit dem Internet nötig und die Updates müssen nur einmal auf Viren oder Veränderungen geprüft werden. Ein weiterer Grund für einen internen Update-Server ist, dass eine hinreichende Kompatibilitätsprüfung zwischen Update und bestehenden Softwarekomponenten durchgeführt werden kann, bevor ein Update im gesamten Netz verteilt wird.

### Den Gültigkeitszeitraum des sudo-Befehls herabsetzen

Wurde der *sudo*-Befehl genutzt, um ein Programm mit root-Privilegien auszuführen und das entsprechende Passwort eingegeben, so bleibt das Passwort fünf Minuten gespeichert. Selbst wenn der Konsolen-Prozess geschlossen und ein neues Konsolenfenster geöffnet wird, erscheint keine erneute Aufforderung zur Passworteingabe und jegliche Programme können mit root-Privilegien ausgeführt werden. Daher sollte die Datei */etc/sudours* wie folgt geändert werden:

Defaults timestamp_timeout=0

Defaults tty_tickets

Damit wird erreicht, dass nur ein Befehl mit root-Privilegien pro Authentisierung ausgeführt werden kann und die Authentisierungsinformationen an den jeweiligen Terminalprozess gebunden sind, in dem die Authentisierung stattgefunden hat.

**Liste der zuletzt verwendeten Objekte reduzieren**

Mac OS X speichert eine Liste der zuletzt verwendeten Anwendungen, Dokumente und Serververbindungen. In erster Linie erleichtern diese Informationen das Arbeiten, jedoch sind damit auch Rückschlüsse auf vertrauliche Informationen möglich, wie zum Beispiel mit welchen Dokumenten kürzlich gearbeitet wurde oder die Adressen der zuletzt benutzten Server. Um diese Informationen auf ein Minimum zu beschränken, kann in den Systemeinstellungen unter Erscheinungsbild die Einstellung "*Benutzte Objekte merken*" auf "Keine" geändert werden. Alternativ kann dies per Kommandozeilen-Befehl erfolgen:

defaults write com.apple.recentitems Applications -dict MaxAmount 0

**Automatisches Öffnen "sicherer Dateien" in *Safari* deaktivieren**

Der mitgelieferte Browser *Safari* von Apple bietet die Möglichkeit, Dateien direkt nach einem Download mit dem damit verknüpften Programm zu öffnen. Diese Einstellung ermöglicht es auch, Dateien automatisch und ohne Nachfrage auszuführen, die Schadcode enthalten könnten. Wird zum Beispiel aus einer unsicheren Quelle, wie einer manipulierten Webseite im Internet, eine präparierte PDF-Datei heruntergeladen und automatisch geöffnet, könnte angehängter Schadcode ausgeführt werden, was zu Datenverlusten oder anderen Problemen führen kann. Um das automatische Öffnen zu deaktivieren, muss in den Safari-Einstellungen unter "Allgemein" der Punkt *"Sichere Dateien nach dem Laden öffnen*" deaktiviert werden.

**Installation eines Viren-Schutzprogramms**

Auf jedem Mac OS X Client muss ein Viren-Schutzprogramm installiert sein. Dabei muss darauf geachtet werden, dass dessen Signaturen regelmäßig aktualisiert werden. Das Viren-Schutzprogramm sollte im Hintergrund laufen und mindestens beim Zugriff auf eine Datei eine Virenüberprüfung durchführen. Weitere Informationen sind in der Maßnahme M 4.3 *Einsatz von Viren-Schutzprogrammen* zu finden. Dabei sollte beachtet werden, dass das Viren-Schutzprogramm auch Schadsoftware für Windows-Systeme erkennt, damit gefahrlos mit Windows-Systemen kommuniziert werden kann.

**Datensicherung**

Um bei einem Störfall möglichst wenige Informationen zu verlieren und schnell normal weiterarbeiten zu können, sollte eine regelmäßige Datensicherung durchgeführt werden. Ausführliche Informationen sind in der Maßnahme M 6.146 *Datensicherung und Wiederherstellung von Mac OS X Clients* finden.

**Zeitzone und Zeitsynchronisation anpassen**

Auf jedem IT-System sollten Uhrzeit und Datum korrekt eingestellt sein. Ist der Zeitunterschied zwischen zwei IT-Systemen zu groß, können Fehler beim Authentisieren eintreten. Zum Beispiel erfordert das Kerberos-Protokoll eine korrekte Uhrzeit und Datum. In den Systemeinstellungen unter "Datum und

Uhrzeit" können die aktuell eingestellte Uhrzeit und das Datum eingesehen und geändert werden. Es wird empfohlen, einen eigenen, vorzugsweise internen Zeitserver zu verwenden. Besteht diese Möglichkeit nicht, kann ein externer Zeitserver verwendet werden, zum Beispiel der Zeitserver ptbtime1.ptb.de der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*).

**Sicheres Entleeren des Papierkorbes aktivieren**

Um zu verhindern, dass gelöscht geglaubte Dateien aus dem Papierkorb unter Mac OS X wiederhergestellt werden können, sollte der Papierkorb regelmäßig entleert werden. Mac OS X bietet zudem die Einstellung "Sicheres Entleeren" an, bei der das Betriebssystem die Dateien nach dem Entleeren des Papierkorbs mit einem Bitmuster überschreibt. Um diese Einstellung zu aktivieren, muss der Finder geöffnet und im Abschnitt "Erweitert" der Haken bei "Papierkorb sicher entleeren" gesetzt werden.

**Autostart-Funktion deaktivieren**

Die Funktion Autostart ermöglicht es, Programme von externen Datenträgern sofort auszuführen, wenn diese, wie zum Beispiel CDs, DVDs oder externe Festplatten, mit dem Computer verbunden werden. Da die hierdurch automatisch ausgeführten Programme auch Schadsoftware enthalten könnten, sollte diese Funktion für jeden Benutzer deaktiviert werden. In den Systemeinstellungen unter CDs & DVDs muss bei allen aufgeführten Parametern die Option "Keine Aktion" festgelegt werden.

Bemerkung: Die Funktion Autostart greift nur, wenn das eingelegte Medium als leere CD/DVD, "Musik-CD", "Bilder-CD" oder "Video-CD" von Mac OS X erkannt wird.

Diese Einstellungen können auch über die Konsole festgelegt werden:

```
# Disable blank CD automatic action:

defaults write /Library/Preferences/com.apple.digihub

com.apple.digihub.blank.cd.appeared -dict action 1

# Disable music CD automatic action:

defaults write /Library/Preferences/com.apple.digihub

com.apple.digihub.cd.music.appeared -dict action 1

# Disable picture CD automatic action:

defaults write /Library/Preferences/com.apple.digihub

com.apple.digihub.cd.picture.appeared -dict action 1

# Disable blank DVD automatic action:

defaults write /Library/Preferences/com.apple.digihub

com.apple.digihub.blank.dvd.appeared -dict action 1

# Disable video DVD automatic action:

defaults write /Library/Preferences/com.apple.digihub
```

com.apple.digihub.dvd.video.appeared -dict action 1

**Entfernen nicht benötigter Programme**

Mit Mac OS X werden standardmäßig einige Programme installiert, die entfernt werden sollten, um die mögliche Angriffsfläche zu minimieren. Zu diesen Programmen zählen beispielsweise Spiele oder diverse Multimedia-Anwendungen. Jedoch muss abhängig von den lokalen Gegebenheiten beurteilt werden, welche Programme notwendig sind und welche entfernt werden sollten. Auf produktiven Systemen dürfen nur die zum Arbeiten notwendigen Programme installiert sein. Wurden Standardprogramme entfernt, müssen diese Veränderungen dokumentiert werden.

Folgende Programme sollten mindestens entfernt werden:

- AppleScript-Ordner samt Inhalt
- Automator
- Chess
- Front Row
- iTunes
- iChat
- Photo Booth
- QuickTime
- Dashboard

Die Programme sind im Finder, nach Auswahl des Startlaufwerks, im Verzeichnis "Programme" zu finden. Einige dieser Programme sind ebenfalls im Mac OS X Dock hinterlegt. Diese Verweise müssen ebenfalls entfernt werden.

Das Dashboard kann alternativ mit folgendem Kommandozeilen-Befehl deaktiviert werden:

defaults write com.apple.dashboard mcx-disabled -boolean yes

In jedem Fall sollten alle Minianwendungen ("Widgets") aus dem Verzeichnis Finder | Festplatte | Library | Widgets gelöscht werden. Zusätzlich installierte Widgets können sich in den Benutzerverzeichnissen jeweils unter Library | Widgets befinden. Alternativ kann eine Suche nach "*.wdgt" ausgeführt werden, um alle Widgets auf dem System zu finden und zu entfernen.

**"Sicheren virtuellen Speicher" aktivieren**

Sofern nicht genügend freier Arbeitsspeicher zur Verfügung steht, sieht das Speicherverhalten von Mac OS X vor, Teilinhalte des Arbeitsspeichers auf der lokalen Festplatte zu speichern. Diese Daten werden in einer "Swap"-Datei unverschlüsselt abgelegt und können mitunter sensitive Informationen beinhalten. Wenn das IT-System ausgeschaltet wird, werden alle Daten im Arbeitsspeicher verworfen. Die Daten in der gespeicherten "Swap"-Datei bleiben jedoch auch nach einem Neustart erhalten, bis sie überschrieben werden. Wird das System in den Schlafmodus (Hibernation Mode) versetzt, wird zusätzlich in der bereits vorhandenen "Swap"-Datei der gesamte Inhalt des Arbeitsspeichers unverschlüsselt in ein sogenanntes "sleepimage" gesichert. Wenn die Verwendung des sicheren virtuellen Speichers aktiviert ist, werden die Daten in der "Swap"- und der in der "sleepimage"-Datei nur noch verschlüsselt auf der lokalen Festplatte gespeichert. Aktiviert werden kann der sichere virtuelle Speicher unter "Systemeinstellungen | Sicherheit | Allgemein | Sicheren virtuellen Speicher verwenden". Alternativ kann diese Einstellung auch in der Anwendung "Terminal" mit folgendem Befehl konfiguriert werden:

defaults write /Library/Preferences/com.apple.virtualMemory UseEncryptedSwap -bool YES

**Ortungsdienste deaktivieren**

Unter Verwendung der Daten aus WLAN-Netzen ist es möglich, den ungefähren Aufenthaltsort eines Mac OS X Clients zu ermitteln. Diese Standortinformationen können dazu verwendet werden, Systemdienste wie die Zeitzone für das aktuelle Datum und die Uhrzeit automatisch einzustellen. Jedoch können auch Webseiten mit Lokalisierungsfunktion diese Informationen nutzen, um den Standort des Webseiten-Besuchers zu bestimmen. Dies kann nützlich, aber auch aus Datenschutz- und Sicherheitssicht problematisch sein. Beispielsweise kann mithilfe der Ortungsdienste der Standort des nächsten Bankautomaten oder Postamtes angezeigt werden. Möchte eine Webseite den Standort lokalisieren, erscheint normalerweise ein Dialogfenster, um die Erlaubnis des Benutzers dazu einzuholen. Dennoch sollten die Ortungsdienste in den Systemeinstellungen unter "Sicherheit | Allgemein" generell deaktiviert werden.

**Automatische Anmeldung deaktivieren**

Das automatische Anmelden am System muss deaktiviert werden. Ist es möglich, sich an einem Mac OS X System ohne Passwortabfrage anzumelden, werden viele Sicherheitsfunktionen übergangen. Die Option "Automatisches Anmelden deaktivieren" ist in den Systemeinstellungen unter Sicherheit im Menüreiter "Allgemein" zu finden und muss aktiviert werden.

**Aktivierung der Bildschirmsperre**

Wird der Bildschirmschoner oder der Ruhezustand beendet, muss zwingend eine erneute Kennwortabfrage für den aktuell angemeldeten Benutzer erfolgen. Die Option "Kennwort erforderlich":

- sofort
- 5 Sekunden
- 1 Minute
- 5 Minuten
- 15 Minuten
- 1 Stunde
- 4 Stunden

nach Beginn des Ruhezustandes oder Bildschirmschoners" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden und muss aktiviert werden. Dieser Wert muss möglichst niedrig gewählt werden. Es empfiehlt sich eine Einstellung von höchstens 15 Minuten (siehe auch M 4.2 *Bildschirmsperre*).

**Abmelden nach X Minuten Inaktivität**

Befindet sich das IT-System längere Zeit im Leerlauf, kann eine automatische Abmeldung des Benutzers sinnvoll sein. Die Option "Abmelden nach X Minuten Inaktivität" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden und kann aktiviert werden. Dieser Wert sollte möglichst niedrig gewählt werden. Wenn das System den Benutzer nach einer bestimmten Zeit automatisch abmelden soll, empfiehlt sich eine Einstellung von 15 Minuten.

**Aktivieren des Firmware-Kennworts**

Um Änderungen an der System-Firmware zu unterbinden, sollte das Firmware-Kennwort aktiviert werden. Sofern dieses aktiviert ist, können ohne Authentisierung keine Änderungen an den Einstellungen, wie den Bootoptionen, durchgeführt werden. Auf der Installations-DVD von Mac OS X ist eine Applikation mit dem Namen "Open Firmware Password Utility" zu finden, mit der das Firmware-Passwort gesetzt und zurückgesetzt werden kann.

Zusätzlich zum Kennwortschutz der Firmware kann mithilfe des systemeigenen Tools NVRAM zwischen drei verschiedenen Sicherheitsmodi gewählt werden. Die Auswahl erfolgt über Terminalbefehle innerhalb des Betriebssystems:

- None: Diese Einstellung bietet keinen Schutz des Extensible Firmware Interfaces (EFI) eines Mac OS X-Systems und der Standardwert ist:
  $ sudo nvram security-mode = none
- Command: Diese Einstellung bietet einen Kennwortschutz gegen Änderungen an der Firmware und gegen das Booten von einem anderen Medium oder Datenträger als der Systempartition.
  $ sudo nvram security-mode = command
- Full: Diese Sicherheitsrichtlinie bietet aufbauend auf der "Command"-Einstellung ein übergreifendes Systempasswort beim Starten und Neustarten des Rechners.
  $ sudo nvram security-mode = full

Der Standardwert sollte von "none" auf mindestens "command" angehoben werden.

Bemerkung: Das NVRAM-Tool benötigt Administratoren- oder root-Berechtigungen, um die Sicherheitsempfehlung umzusetzen. Des Weiteren muss beachtet werden, dass das Firmware-Kennwort nicht verschlüsselt im NVRAM abgelegt wird, sondern im Klartext in hexadezimaler Schreibweise. Es ist jedem System-Administrator möglich, dieses Kennwort auszulesen.

**Sicherheit des Schlüsselbundes erhöhen**

Das Passwort des Schlüsselbundes sollte geändert werden, sodass es nicht mehr mit dem Passwort des aktuell angemeldeten Benutzers übereinstimmt. Damit wird verhindert, dass eine Person, die unberechtigten Zugang zum Computer erlangt, auch Zugang zu allen Informationen im Schlüsselbund erhält. Um das Passwort zu ändern, muss unter den Dienstprogrammen die Applikation "Schlüsselbund" aufgerufen und unter dem Menüpunkt "Bearbeiten" die Option "Kennwort für Schlüsselbund "Anmeldung" ändern" gewählt werden. Dadurch wird die Synchronisation zwischen Benutzeraccount-Passwort und Schlüsselbund-Passwort aufgehoben. Zusätzlich sollte die Option "Einstellungen für den Schlüsselbund "Anmeldung" ändern" aufgerufen werden, um die Optionen "Nach X Minuten Inaktivität schützen" und "Bei Wechsel in Ruhezustand schützen" zu aktivieren. Bei der ersten Option empfiehlt es sich, 15 Minuten einzustellen.

**Verwenden der Passwortabfrage für jede Systemeinstellung**

Es sollte die "Kennwortabfrage für die Freigabe jeder geschützten Systemeinstellung" aktiviert werden, damit nur Administratoren die Systemeinstellungen ändern können. Weiterhin sorgt diese Einstellung dafür, dass bei einem unbefugten Zugriff nur freigeschaltete Systemeinstellungen verändert werden können. Die Option "Kennwortabfrage für die Freigabe jeder geschützten Systemeinstellung" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden.

**Gast-Benutzer-Account deaktivieren**

Der Gast-Benutzer-Account unter Mac OS X ist standardmäßig aktiviert und muss zusammen mit dem Zugriff für Gäste auf freigegebene Ordner deaktiviert werden. Unter "Systemeinstellungen | Benutzer | Andere Accounts | Gast-Account" muss die Option "Gästen den Zugriff auf freigegebene Ordner erlauben" deaktiviert werden.

**Manuelle Anpassung von Konfigurationsdateien**

Um unter Mac OS X die Systemkonfiguration zu verändern, können die Konfigurationsdateien mit einem Texteditor, per Kommandozeilenaufruf oder über die grafische Benutzeroberfläche angepasst werden. Werden verschiedene Methoden eingesetzt, um Änderungen am System vorzunehmen, können Inkonsistenzen entstehen, da die Anpassungen oft in unterschiedlichen Konfigurationsdateien gespeichert werden und zwischen diesen nicht synchronisiert wird. Weiterhin können sich Sicherheitseinstellungen gegenseitig aufheben oder die Verwaltung des Clients unter Mac OS X komplizieren.

Wird zum Beispiel mit einem Texteditor in der SSH-Konfigurationsdatei "sshd_conf" ein Benutzer freigeschaltet und ein anderer Benutzer über die grafische Benutzeroberfläche in den Systemeinstellungen für die "Entfernte Anmeldung" freigegeben, so wird sich keiner dieser Benutzer per SSH am System anmelden können.

Daher sollte festgelegt werden, welche Methode zur Anpassung von Konfigurationsdateien unter Mac OS X verwendet wird. Alle Administratoren müssen über diese Vorgehensweise informiert werden.

Prüffragen:

- Gibt es Regelungen, wie Mac OS X zu konfigurieren ist?
- Ist sichergestellt, dass nach der Installation eine Aktualisierung des Betriebssystems und der Anwendungsprogramme vorgenommen wird?
- Wurde das automatische Öffnen "sicherer Dateien" durch Safari unter Mac OS X deaktiviert?
- Wurden der Gast-Benutzer-Account und die Autostart-Funktion von Mac OS X deaktiviert?
- Wurde ein Firmware-Kennwort für Mac OS X gesetzt?
- Wurde das Gültigkeitszeitfenster des sudo-Befehls herabgesetzt?

# M 4.372 Einsatz von FileVault unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Seit der Mac OS X-Version "Panther" (10.3) können Benutzerordner mit FileVault mit dem Algorithmus AES-128 verschlüsselt werden. Das Haupt-FileVault-Kennwort wird jedoch mit RSA-1024 verschlüsselt, was zu einem effektiven Verschlüsselungsschutz von 112 Bit führt. FileVault ist direkt in das Betriebssystem integriert, es wird keine zusätzliche Software benötigt, um den Benutzerordner zu verschlüsseln.

Weil FileVault sehr einfach zu benutzen ist, wird empfohlen, die Benutzerverzeichnisse generell zu verschlüsseln. Das gilt besonders für sensible Informationen auf mobilen Rechnern, die einem erhöhten Diebstahlsrisiko ausgesetzt sind. FileVault kann hierfür eine Alternative sein.

FileVault schützt die Informationen nur, wenn der Client ordnungsgemäß heruntergefahren wurde oder der Benutzer noch nicht angemeldet ist. Nachdem sich der Benutzer erfolgreich angemeldet hat, wird das von FileVault verschlüsselte Disk-Image in das System als Benutzerverzeichnis ("*home*") eingebunden und steht zur Verfügung. Zu keinem Zeitpunkt wird das gesamte Disk-Image entschlüsselt, es werden nur die gerade benötigten Teile in den Arbeitsspeicher geladen. Die Verschlüsselung der Datei erfolgt wieder, sobald sie sich nicht mehr im Arbeitsspeicher befindet. Meldet sich der Benutzer ab, wird das von FileVault verschlüsselte Disk-Image aus dem Dateisystem ausgehängt und die Dateien sind geschützt.

Können sich die Benutzer ohne Authentisierung am Client anmelden ("Automatische Anmeldung"), werden die mit FileVault geschützten Informationen ohne Passwortabfrage entschlüsselt. Für wirksamen Schutz der Informationen durch FileVault muss die automatische Anmeldung deaktiviert und ein ausreichend sicheres Passwort gewählt werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).

**Vorbereitung des Einsatzes von FileVault**

Mit FileVault können nur Benutzerverzeichnisse geschützt werden, die auf "Mac OS Extended"-Dateisystemen abgelegt sind und bei denen der Zusatz "Case sensitive" bzw. "Groß- und Kleinschreibung" nicht aktiviert wurde. Soll FileVault eingesetzt werden, empfiehlt es sich, das Dateisystem "Mac OS Extended (Journaled)" für die Partition mit den Benutzerverzeichnissen zu verwenden.

Generell wird empfohlen, die Benutzerverzeichnisse auf einer separaten Partition zu installieren. Bei der Planung der Größe der Partitionen und des benötigten Festplattenspeichers ist zu beachten, dass während der Verschlüsselung zusätzlich Festplattenspeicher in der Größe des zu verschlüsselnden Benutzerordners benötigt wird. Diese Anforderung liegt an der Arbeitsweise von FileVault. Wird FileVault für einen Benutzer aktiviert, so erstellt Mac OS X ein verschlüsseltes Disk-Image, kopiert alle Daten aus dem bestehenden Benutzerordner in das Disk-Image und löscht danach den originalen Benutzerordner. Es sollte verhindert werden, dass die gelöschten, unverschlüsselten Benutzerordner wieder hergestellt werden können. Das lässt sich durch die Auswahl der Einstellung "*sicheres Löschen verwenden*" gewährleisten.

**FileVault aktivieren**

Damit FileVault genutzt werden kann, muss es aktiviert werden. FileVault kann bereits beim Erstellen eines neuen Benutzers aktiviert werden, indem die Einstellung "*FileVault-Schutz aktivieren*" in den Benutzereigenschaften angewählt wird.

Um FileVault nachträglich für den angemeldeten Benutzer zu aktivieren, muss unter "*Systemeinstellungen* | *Sicherheit* | *FileVault"* die Schaltfläche "*FileVault aktivieren*" angewählt werden. In beiden Fällen sollte aufgrund der oben beschriebenen Arbeitsweise von FileVault zusätzlich unbedingt die Einstellung "*sicheres Löschen verwenden*" gewählt werden. Die Einstellung "*sicheren virtuellen Speicher verwenden*" sollte ebenfalls aktiviert werden, da sonst Informationen oder gar das Passwort unverschlüsselt in */var/vm* abgelegt werden.

**Datenwiederherstellung**

Der Administrator muss ein Hauptkennwort für die jeweiligen Computer festlegen, um alle FileVault-verschlüsselten Benutzerordner auf den Computern wiederherstellen zu können, falls ein FileVault-Benutzerpasswort verloren geht. Das Wiederherstellungskennwort sollte ausreichend komplex sein (siehe M 2.11 *Regelung des Passwortgebrauchs*). Wenn das Wiederherstellungskennwort aus Effizienzgründen für verschiedene Clients identisch gewählt wird, dann muss unbedingt ein ausreichend komplexes Passwort genutzt werden.

Besteht der Verdacht, dass das Hauptkennwort publik wurde, weil es zum Beispiel an einem ungesicherten Ort aufbewahrt worden ist, muss es sofort geändert werden, da sonst der Zugriff auf alle auf dem Computer befindlichen verschlüsselten Daten möglich ist.

Das Hauptkennwort sollte an einer geeigneten Stelle aufbewahrt werden, damit die Daten in einem Störfall schnell und personalunabhängig durch einen Administrator wiederhergestellt werden können (siehe M 2.22 *Hinterlegen des Passwortes*).

**FileVault in Verbindung mit Energiesparmodi**

Ein Client unter Mac OS X, der aktuell nicht benutzt wird und auch nicht ausgeschaltet ist, kann sich in einem Energiesparmodus befinden. Hierzu zählt unter anderem der sogenannte Ruhezustand. Bei Mac OS X wird damit sowohl ein Zustand beschrieben, in dem der Computer den Inhalt des RAM auf der Festplatte speichert, als auch ein Zustand, in dem nur der aktuelle Inhalt des Arbeitsspeichers eingefroren wird.

Unter Mac OS X verbleiben im Ruhezustand die Informationen zum FileVault-Passwort im Arbeitsspeicher (RAM) oder auf der Festplatte des Clients. Dadurch ist die Vertraulichkeit der FileVault-verschlüsselten Daten gefährdet. Bei einem höheren Schutzbedarf wird empfohlen, einen Client unter Mac OS X nicht unbeaufsichtigt im Ruhezustand zu belassen. Alternativ muss der Benutzer sich abmelden und den Client ausschalten. Die Bildschirmsperre stellt, wie der Ruhezustand, eine Gefahr für die Vertraulichkeit dar, weil auch hier die Passwortinformationen im RAM vorhanden sind und ausgelesen werden könnten.

**Sensibilisierung der Benutzer**

Die Benutzer müssen darüber informiert werden, dass FileVault nur den eigenen Benutzerordner verschlüsselt und dies auch nur, wenn der Client unter

Mac OS X ordnungsgemäß heruntergefahren wurde. Im Weiterem müssen die Benutzer darüber informiert werden, wie sie mit den Energiesparmodi in Verbindung mit FileVault-Verschlüsselung umgehen sollten und dass der Administrator die Daten beim Verlust des Passworts mit dem Hauptkennwort wiederherstellen kann. Weiterführende Informationen zum Thema sichere Datenablage und Datentransport sind in M 4.379 *Sichere Datenhaltung und sicherer Transport unter Mac OS X* beschrieben.

**Abgrenzung der Eignung von FileVault**

FileVault bietet keine Einstellungsmöglichkeit, welche Dateien verschlüsselt werden. Es wird ausschließlich der Benutzerordner verschlüsselt. Potentiell können aber auch Daten in anderen Verzeichnissen schützenswerte Informationen enthalten. So beinhalten die Verzeichnisse */Library/Logs* und */var/log* diverse Log-Dateien mit detaillierten Systeminformationen, die Verzeichnisse */Library/Caches* und */tmp* beinhalten temporäre Dateien bzw. Cache-Dateien von einigen Datensicherungsprogrammen und in */Library/Preferences* befinden sich systemweite Einstellungsdateien. Somit sollten bei einem höheren Schutzbedarf statt FileVault andere Verschlüsselungsprogramme eingesetzt werden, die die gesamte Festplatte verschlüsseln können.

Prüffragen:

- Wird das "Mac OS Extended (Journaled)"-Dateisystem für die Partitionen benutzt, die mit FileVault verschlüsselt werden sollen und ist dort der Zusatz "Case sensitive" bzw. "Groß- und Kleinschreibung" abgewählt?
- Sind beim Einsatz von FileVault ein ausreichend starkes Benutzerkennwort für Mac OS X gesetzt und die automatische Anmeldung deaktiviert worden?
- Ist ein ausreichend starkes Haupt-FileVault-Kennwort für Mac OS X gesetzt und sicher hinterlegt?
- Ist den Mac OS X Benutzern bekannt, dass mit FileVault nur der persönliche Benutzerordner verschlüsselt wird?
- Wissen die Mac OS X Benutzer, dass sie mithilfe des Haupt-FileVault-Kennworts ihre Daten im Fall des Verlusts des Benutzerkennworts wiederherstellen können?

# M 4.373 Deaktivierung nicht benötigter Hardware unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Alle nicht unter Mac OS X benötigten Geräte und Schnittstellen sollten deaktiviert werden. Sind beispielsweise in einem Unternehmen oder einer Behörde Webcams oder Mikrofone nicht erlaubt, so kann die entsprechende Kernel-Extension (kext) gelöscht werden, um einen Zugriff auf die Hardware und ein mögliches Abhören zu erschweren.

Die kexts befinden sich in folgendem Verzeichnis:

/System/Library/Extensions

Nun müssen die entsprechenden kexts ausgewählt und sicher gelöscht werden.

| **WLANDateiname der Kernel-Extension** | **Funktion der Kernel-Extension** |
|---|---|
| WLANIOBluetoothFamily.kextBluetoothAppleAirPort2.kextAppleAirPort.kext | |
| IOBluetoothHIDDRiver.kextAppleAirPortBluetooth.kext | Bluetooth |
| AppleIRController.kext | Infrarotempfänger |
| AppleOnboardAudio.kext | Audio |
| AppleUSDAudio.kext | Audio |
| AudioDeviceTreeUpdater.kext | Audio |
| IOAudioFamily.kext | Audio |
| VirtualAudioDriver.kext | Audio |
| Apple_iSight.kext | Video |
| AppleUSBVideoSupport.kextDiese Datei befindet sich innerhalb von IOUSBFamily.kext im Verzeichnis */Contents/PlugIns* | Video |
| IOUSBMassStorageClass.kext | USB Massenspeicher |
| IOFireWireSerialBusProtocolTransport.kext | Firewire |

Anschließend muss folgender Befehl ausgeführt werden, um das Änderungsdatum des Ordners zu aktualisieren. Dadurch wird der Extension-Cache gelöscht und neu geladen.

sudo touch /System/Library/Extensions

Bevor die Kernel-Extensions sicher aus dem Papierkorb gelöscht werden, um ein einfaches Wiederherstellen zu unterbinden, sollten die Daten gesichert werden, beispielsweise auf ein Netzlaufwerk. Diese Kopie sollte an einem gesicherten Ort abgelegt werden und nur Administratoren zugänglich sein.

Auch wenn eine kext entfernt wurde, um den Zugriff auf die entsprechende Hardware zu verhindern, kann die Software, zum Beispiel nach einem Apple Softwareupdate, durch eine neuere Version ersetzt worden sein. Daher sollte nach einer Systemaktualisierung kontrolliert werden, ob die kexts nach wie vor

gelöscht sind. Alle Änderungen an Mac OS X, die die kexts betreffen, sind an geeigneter Stelle zu dokumentieren.

Wird ein Entfernen der Kernel-Extension nicht als ausreichend sicher betrachtet, besteht die Möglichkeit, die entsprechenden Hardwarekomponenten physikalisch zu entfernen.

Prüffragen:

- Wurden alle Geräte und Schnittstellen, die nicht unter Mac OS X benötigt werden, deaktiviert?
- Wird nach einer Systemaktualisierung von Mac OS X überprüft, ob die Kernel-Extensions nach wie vor gelöscht sind?
- Wurden die originalen kext-Dateien von Mac OS X an einem sicheren Ort zur eventuellen Wiederherstellung abgelegt?
- Wurden die Änderungen an Mac OS X in die Dokumentation aufgenommen?

# M 4.374 Zugriffschutz der Benutzerkonten unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auf einem Client unter Mac OS X müssen die Einstellungen der Benutzerkonten angepasst werden, um die System-Sicherheit zu erhöhen. Zum Beispiel könnte die Merkhilfe für Passwörter von Unbefugten genutzt werden, um Hinweise auf das Passwort zu erhalten. Diese Anpassungen lassen sich in den Systemeinstellungen unter "Benutzer" vornehmen.

Die Sicherheit eines Benutzerkontos vor unbefugtem Zugriff ist im hohen Maße von dem verwendeten Passwort abhängig, daher muss ein starkes Passwort verwendet werden. Hierzu müssen die Empfehlungen aus M 4.376 *Festlegung von Passwortrichtlinien unter Mac OS X* umgesetzt werden. Eine weitere wichtige Bedingung für ein sicheres Benutzerkonto ist das Deaktivieren von Merkhilfen des Passwortes, durch die ein Angreifer wichtige Hinweise auf das Passwort erhalten kann. Da die Informationen in der Merkhilfe im schlimmsten Fall dem eigentlichen Passwort entsprechen, sollte diese Funktion deaktiviert werden. Wird eine Passwort-Merkhilfe dennoch eingesetzt, müssen unbedingt alle Benutzer für diese mögliche Gefahr sensibilisiert werden. Ebenfalls sollte das Anmeldefenster nicht in Form einer Liste aller Benutzer angezeigt werden, da ein Angreifer damit alle Informationen über auf dem System existierende Benutzer erhält. Er benötigt dann nur noch die entsprechenden Passwörter, um unerlaubten Zugriff auf das System zu erhalten. Ohnehin sollte die Anmeldung am System grundsätzlich nicht automatisch erfolgen sondern nur mit Benutzername und Passwort möglich sein.

Alternativ können diese Restriktionen per Befehlszeile für den aktuell angemeldeten Benutzer umgesetzt werden:

```
# Keine Merkhilfe für Passwörter

defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint -int 0

# Abfrage von Name und Passwort im Anmeldefenster, keine Anzeige von Namensliste

defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -bool yes

# Deaktivieren von Neustart, Ruhezustand und Herunterfahren

defaults write /Library/Preferences/com.apple.loginwindow PowerOffDisable -bool yes
```

Die oben vorgenommenen Einstellungen sollten nach jeder Systemaktualisierung überprüft werden.

Prüffragen:

- Ist die automatische Anmeldung unter Mac OS X deaktiviert?
- Wurde ein komplexes Benutzerkonten-Passwort unter Mac OS X gewählt?

- Wurden die Passwort-Merkhilfen unter Mac OS X für das Benutzerkonto deaktiviert oder die Benutzer diesbezüglich sensibilisiert?

# M 4.375 Einsatz der Sandbox-Funktion unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Betriebssystem Mac OS X ist mit einer Sandbox-Funktion ausgestattet. Eine Sandbox-Funktion ermöglicht es, einen Prozess in einer eigenen, eingeschränkten Umgebung auszuführen, in der er vom Rest des IT-Systems vollständig abgeschirmt ist. Es ist somit zum Beispiel möglich, der in einer Sandbox eingesperrten Applikation den Netz- oder Dateizugriff zu entziehen, um den möglichen Schadensumfang bei einer Fehlfunktion des Prozesses zu minimieren. Die Sandbox-Funktion ist eine weiterführende Einschränkung und setzt keine tiefer liegenden Limitierungen wie Access-Control-Listen außer Kraft. Somit kann eine Sandbox nichts ermöglichen, was durch andere Techniken beschränkt wurde, es handelt sich vielmehr um eine sehr feingliedrige Möglichkeit, um die Auswirkungen von Programmen zu testen und deren Auswirkungen gezielt einzuschränken.

Es ist empfehlenswert, neue Programme oder Dienste, die an einer Netzkommunikation teilnehmen, vor dem produktiven Einsatz in einer Sandbox zu testen. Wird ein neuer Kindprozess in der Sandbox gestartet, erbt er die Einschränkungen der Sandbox. Wenn beispielsweise Safari in einer Sandbox läuft und durch den Browser eine mit Schadsoftware präparierte PDF-Datei heruntergeladen und automatisch geöffnet wird, dann werden die eingeschränkten Rechte der Sandbox für die Ausführung der PDF-Datei übernommen und der mögliche Schadensumfang erheblich eingeschränkt.

Wenn Benutzer den Browser nur in einer Sandbox nutzen können, kann auf diese Weise auch das Installieren von nicht freigegebenen Plug-Ins verhindert werden, da der Browser nach jedem Neustart wieder im ursprünglichen Zustand ist. Welche Anwendungen innerhalb einer Sandbox ausgeführt werden sollen, ist durch den Administrator festzulegen und zu konfigurieren.

Folgender Befehl startet *Safari* in einer Sandbox ohne Dateizugriffsrechte:

sandbox-exec -p "(version 1) (allow default) (deny file-write*)" /Applications/Safari.app/Contents/MacOS/Safari

Wird der Befehl um den Parameter (debug all) ergänzt, können alle Aktionen in der *Console.app* angesehen werden.

Weiterhin ist es möglich, ein Sandbox-Profil anzulegen, um alle Konfigurationsparameter dorthin auszulagern. Im Verzeichnis */usr/share/sandbox* befinden sich mehrere Profilvorgaben für eine Sandbox, die für bestimmte Systemdienste definiert wurden. Ist ein entsprechendes Profil vorhanden und an die lokalen Richtlinien angepasst, so kann der Befehl zum Aufruf einer Anwendung wie folgt aussehen:

sandbox-exec -f /usr/share/sandbox/safari.sb /Applications/Safari.app/Contents/MacOS/Safari &

Prüffragen:

- Sind die Anwendungen, die innerhalb einer Sandbox laufen sollen, durch den Administrator festgelegt worden?

# M 4.376 Festlegung von Passwortrichtlinien unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für alle Clients unter Mac OS X müssen Richtlinien für Passwörter definiert werden, um sie mit einem angemessenen starken Passwort zu versehen. Die beschriebenen Maßnahmen in M 2.11 *Regelung des Passwortgebrauchs* sollten unter Mac OS X umgesetzt werden. Dazu kann das Kommandozeilen-Programm "*pwpolicy*" benutzt werden. Mit diesem Programm lassen sich beispielsweise eine minimal erforderliche Anzahl von Buchstaben und Zahlen, eine Mindestzeichenlänge oder eine maximale Anzahl fehlgeschlagener Login-Versuche definieren. Es wird eine minimale Passwortlänge von 8 Zeichen vorgeschrieben, wenn für das Passwort alphanumerische Zeichen genutzt werden. Außerdem ist das Passwort in regelmäßigen Abständen zu wechseln.

Der folgende Befehl legt eine Richtlinien für Passwörter fest, die eine Minimallänge des Passwortes von 8 Zeichen fordert und 8 fehlgeschlagene Anmeldeversuche zulässt, bevor das Konto deaktiviert wird.

pwpolicy -n /Local/Default -setglobalpolicy "minChars=8 maxFailedLoginAttempts=8"

Weitere mögliche Passwortrichtlinien sind:

| **Variable** | **Funktion** |
|---|---|
| usingHistory | 0 = Benutzer kann das aktuelle Passwort nochmals verwenden 1 = Benutzer darf das aktuelle Passwort nicht nochmals verwenden 2-15= Benutzer darf die letzten n Passwörter nicht nochmals verwenden. |
| usingExpirationDate | Ist der Wert 1, wird der Benutzer zur in expirationDateGMT hinterlegten Zeit zur Passwortänderung aufgefordert. |
| usingHardExpirationDate | Ist der Wert 1, so wird das Konto zur in hardExpireDateGMT hinterlegten Zeit deaktiviert. |
| requiresAlpha | Ist der Wert 1, so wird mindestens ein Buchstabe im Passwort erwartet. |
| requiresNumeric | Ist der Wert 1, so wird mindestens eine Zahl im Passwort erwartet. |
| expirationDateGMT | Datum, an dem das Passwort geändert werden muss. Format: mm/dd/yy |
| hardExpireDateGMT | Datum, an dem das Konto deaktiviert wird. Format: mm/dd/yy |
| maxMinutesUntilChangePassword | Der Benutzer muss sein Passwort in dem hier angegebenen Intervall ändern. |
| maxMinutesUntilDisabled | Das Konto wird in den hier angegebenen Minuten deaktiviert. |

| Variable | Funktion |
|---|---|
| maxMinutesOfNonUse | Bei Nichtbenutzung für die hier angegebenen Minuten wird das Konto deaktiviert. |
| maxFailedLoginAttempts | Das Konto wird deaktiviert, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche die hier hinterlegte Anzahl überschreitet. |
| minChars | Das Passwort muss mindestens den hier angegebenen Wert an Zeichenlänge besitzen. |
| maxChars | Das Passwort darf den hier angegebenen Wert an Zeichenlänge nicht überschreiten. |

In den man(ual)-Pages unter Mac OS X lassen sich weitere Parameter zur Richtliniendefinition hinsichtlich Passwörtern einsehen.

Prüffragen:

- Gibt es geeignete globale Passwortrichtlinien unter Mac OS X?
- Werden unter Mac OS X Passwörter von mindestens 8 Zeichen erzwungen?

# M 4.377 Überprüfung der Signaturen von Mac OS X Anwendungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Seit Mac OS X 10.5 ist jede ausführbare Betriebssystemkomponente von Apple digital signiert. Dritthersteller sind ebenfalls dazu aufgefordert, ihre eigenen Programme zu signieren. Wird ein signiertes Programm in irgendeiner Form verändert, zum Beispiel durch Schadsoftware, so wird die Signatur ungültig. Wird ein neues Programm eingesetzt, muss daher dessen Signatur überprüft werden. Liegen keine Signaturinformationen vor, sollte das Programm zumindest mit einem Viren-Schutzprogramm überprüft werden. Um die Gültigkeit einer Signatur zu überprüfen, wird von Apple eine Public-Key-Infrastruktur verwendet, ähnlich wie bei HTTPS-Webseiten. Die Administratoren sollten im Umgang mit dem Befehl "*codesign*" geschult werden, um jedes neue Programm einer einmaligen Signaturprüfung unterziehen zu können.

Ob ein Programm eine gültige Signatur hat, kann mit folgendem Kommandozeilen-Befehl überprüft werden:

codesign --verify --verbose /Pfad/zur_Datei/Dateiname.app

Handelt es sich um eine gültige Signatur, so entspricht die Datei dem vom Hersteller vertriebenen Original und wurde nicht verändert. Somit kann mit einer Signaturprüfung eine mögliche Manipulation auf dem Übertragungsweg ausgeschlossen werden.

Signaturen werden ebenfalls genutzt, um Programme eindeutig wiederzuerkennen. So ist sichergestellt, dass für diese Programme die entsprechenden Einstellungen in der "Eltern-Kontrolle", der Firewall und dem Schlüsselbund gelten.

Prüffragen:

- Werden die digitalen Signaturen von Mac OS X Anwendungen vor der Installation überprüft?

# M 4.378 Einschränkung der Programmzugriffe unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um unter Mac OS X den Zugriff auf bestimmte Funktionen des Computers einzuschränken, können die "Parental Controls" eingesetzt werden. Obwohl diese Funktion als "Parental Controls" oder Kindersicherung bezeichnet wird, kann deren Nutzung auch in Behörden oder Unternehmen sinnvoll sein. Durch diese Kindersicherung, zu finden in den Systemeinstellungen, können Benutzerkonten weiter eingeschränkt werden. Auch die Programmzugriffe lassen sich mit der Kindersicherung weiter einschränken, nachdem alle nicht benötigten Programme entfernt wurden, wie in M 4.371 *Konfiguration von Mac OS X Clients* im Abschnitt "Entfernen nicht benötigter Programme" beschrieben. Unter Umständen können Einschränkungen hierdurch präziser eingestellt werden.

So kann zum Beispiel für die Benutzer der Zugriff auf bestimmte Anwendungsprogramme, Webseiten oder Computerkomponenten beschränkt werden. Dieses Vorgehen ist auch geeignet, um das Verzeichnis "*Dienstprogramme*" zu sperren, da hier Programme zur Administration des Computers liegen, die tiefere Einblicke in das System ermöglichen. Soll nur der Zugriff auf bestimmte Webseiten bzw. Domänen erlaubt sein, kann unter dem Menüpunkt "Inhalt" beziehungsweise "Content" der Zugriff auf eine Domäne wie "*.bund.de" erlaubt werden. Weiterhin ist es möglich, die E-Mail-Kommunikation nur zwischen vorher festgelegten Partnern zu erlauben.

Unter dem Menüpunkt "Mail & iChat" kann eine Liste von freigegebenen E-Mail- sowie iChat-Kommunikationspartnern erstellt werden. Durch diese Einstellung lässt sich das Abfließen von Informationen über die Programme *Mail* und *iChat* vermeiden. Es muss jedoch beachtet werden, dass weiterhin HTTP-Webmailer benutzt werden können, um E-Mails an nicht autorisierte Personen zu versenden. Jedoch ist es zurzeit nicht möglich, die Liste der erlaubten Kommunikationspartner mittels regulären Ausdrücken anzupassen. Die Anmeldezeiten für Benutzerkonten lassen sich unter dem Menüpunkt "Time Limits" anpassen. Wird zum Beispiel davon ausgegangen, dass die Hauptarbeitszeit zwischen 7 und 17 Uhr liegt, sollten die erlaubten Benutzeranmeldezeiten diesen Zeiten ungefähr entsprechen.

Weitere verfügbare Einstellungsmöglichkeiten, wie zum Beispiel der Zugriff auf CD-/DVD-Laufwerke, sollten möglichst restriktiv gehalten werden. Jedoch muss beachtet werden, dass eine zu starke Einschränkung hinderlich und demotivierend sein kann. Daher sollte im Vorfeld durch den Leiter der IT und den IT-Sicherheitsbeauftragten geklärt werden, welche Restriktionen an welchen Clients umgesetzt werden sollen. Dies sollte dokumentiert werden.

Eine zentrale Steuerung der Client-Computer ist ebenfalls möglich. Wird in den "Systemeinstellungen" unter "Kindersicherung" die Option "*Kindersicherung von einem anderen Computer aus verwalten*" aktiviert, können Benutzerkonten auf entfernten Computern mittels Kindersicherung eingeschränkt werden. Hierfür wird der Benutzername und das Passwort eines Administrators auf dem zu steuernden IT-System benötigt. Mit diesen Zugangsdaten können

die Benutzerrechte auf dem zu steuernden IT-System vom administrierenden IT-System aus, so wie oben beschrieben, eingeschränkt werden.

Prüffragen:

- Sind die Programmzugriffe mithilfe entsprechender Maßnahmen entsprechend der Sicherheitsrichtlinien so weit wie möglich eingeschränkt worden?

# M 4.379 Sichere Datenhaltung und sicherer Transport unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Unter Mac OS X können Disk-Images erstellt werden. Disk-Images stellen sich wie Dateien dar, enthalten jedoch intern ein eigenes Dateisystem, das per Doppelklick als virtuelles Laufwerk in das System eingebunden werden kann. Disk-Images können komprimiert und verschlüsselt werden. Jedes Mac OS X System kann die so erzeugten Disk-Images problemlos lesen. Auf anderen Plattformen ist dafür zusätzliche Software notwendig. Grundsätzlich sollte darauf geachtet werden, dass vertrauliche Informationen unter Mac OS X nur in einem verschlüsselten Disk-Image oder mittels einer anderen geeigneten Verschlüsselungsmethode transportiert und gelagert werden. Die Benutzer müssen im Umgang mit Disk-Images geschult sein.

Wird ein Disk-Image von einem vorhandenen Verzeichnis erstellt, so werden zwei Einstellungsmöglichkeiten angeboten. Einmal kann das Image-Format ausgewählt werden, zum Beispiel "Komprimiert", "Nur lesen" oder "Lesen/Schreiben". Für genaue Abbilder von CDs/DVDs ist das Image-Format "DVD/CD-Master" geeignet. Zum anderen wird eine Verschlüsselung angeboten. Befinden sich vertrauliche Informationen im Disk-Image, sollte es verschlüsselt werden. Hierfür sollte eine 256-Bit-AES-Verschlüsselung sowie ein komplexes Passwort gewählt und triviale Passwörter vermieden werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Soll ein neues, leeres Disk-Image erstellt werden, stehen im Gegensatz zu einem Image aus einem vorhandenen Ordner weitere Einstellungsmöglichkeiten zur Verfügung. Die wichtigsten Optionen sind das Einstellen der maximalen Größe des Disk-Images sowie die Wahl des Image-Formats. Wird ein "Mitwachsendes Bundle-Image" gewählt, so wird Festplattenspeicher nur dann belegt, wenn er benötigt wird. Das Image wächst mit den hinzugefügten Daten. Das "Mitwachsende Bundle-Image" schrumpft jedoch nicht, wenn Daten wieder daraus entfernt werden. Belegter Speicher lässt sich jedoch mit dem Befehl "*hdiutil compact namedesimages*" freigeben. Dieser Befehl funktioniert nur auf Computern, die sich nicht im Batterie-Betrieb befinden. Eine weitere Einstellung bei einem neu erstellen Disk-Image ist die Wahl zwischen den gängigen Dateisystemen von Apple und Microsoft.

Das Kennwort für das Disk-Image kann ebenfalls wie andere vertrauliche Informationen im Schlüsselbund als "sichere Notiz" abgelegt werden. Dann sind jedoch die Maßnahmen in M 4.371 *Konfiguration von Mac OS X Clients* umzusetzen. Arbeiten mehrere Personen mit einem Disk-Image, muss ein zentraler, sicherer Ablageort gewählt werden, damit das aktuelle Passwort jedem autorisierten Mitarbeiter zur Verfügung steht.

Prüffragen:

- Werden Daten unter Mac OS X sicher vorgehalten und transportiert?
- Ist jeder Benutzer von Mac OS X im Umgang mit Disk-Images geschult?
- Wird ein starkes Passwort zum Schutz der Mac OS X Disk-Images verwendet?
- Wird das Passwort von Mac OS X Disk-Images an einem geeigneten Ort aufbewahrt?

# M 4.380 Einsatz von Apple-Software-Restore unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Unter Mac OS X können Dateisysteme mit der Applikation Apple-Software-Restore (ASR) dupliziert und geklont werden. ASR bietet nicht nur die Möglichkeit, Partitionen zu klonen, sondern auch ein Disk-Image im Netz bereitzustellen und dieses über das Netz auf Clients zu verteilen.

Wurde ein Client unter Mac OS X nach den Vorgaben des Unternehmens oder der Behörde installiert und entspricht den Sicherheitsrichtlinien, so kann dieses System geklont und für eine Netz-Installation für weitere Clients genutzt werden. Damit wird es ermöglicht, dass alle Clients unter Mac OS X eine gleiche Grundkonfiguration erhalten, die den Sicherheitsvorgaben der Institution entspricht.

Als Erstes muss dafür ein Disk-Image vom Standard-System erstellt werden. Hierzu sind folgende Schritte zu durchlaufen:

- Die Installations-DVD muss eingelegt werden.
- Nach Auswahl der Menüsprache muss das Festplatten-Dienstprogramm gestartet werden.
- Nun muss die zu klonende Partition ausgewählt und mit einem Rechtsklick deaktiviert werden.
- Anschließend muss mit dem Menüpunkt "Ablage | Neu | Image von DiskXYZ" ein Disk-Image von der Partition erstellt werden, die auf weitere Client-Rechner geklont werden soll. Dieser Vorgang kann je nach Größe des zu kopierenden Laufwerks einige Minuten in Anspruch nehmen.
- Ist der Vorgang abgeschlossen, ist das erzeugte Disk-Image auf Fehler zu überprüfen. Hierzu muss der Computer neu gestartet und folgender Befehl im Terminal ausgeführt werden:

```
sudo asr --source /Pfad_zum/Image.dmg --imagescan
```

Nach erfolgreicher Prüfung des Disk-Images muss eine Property-List (Plist) erstellt werden. Der Inhalt dieser Plist ist die Variable "Data Rate" vom Typ "Number". Entsprechend dem vorhandenen Netz und der gewünschten Streaming-Bandbreite, muss in diese Variable ein Wert in der Einheit "Bytes pro Sekunde", ohne Kommata oder Punkte zur Abgrenzung eingetragen werden. Zum Beispiel würde "1000000" bedeuten, dass ein Durchsatz von 1 Megabit pro Sekunde (Mbit/s) erwünscht ist. In die Variable mit dem von Apple festgelegten Namen "Multicast Address" wird die Adresse des Servers, der das Disk-Image zur Verfügung stellt, eingetragen. Die Variable ist vom Typ "String", ein möglicher Inhalt ist zum Beispiel "239.255.0.1".

Um eine Plist zu erstellen, bietet sich das Programm "Property List Editor" im Verzeichnis /Developer/Applications/Utilities an. Dieses Programm ist nach einer Installation der Developer-Tools von der Installations-DVD verfügbar.

Um das Disk-Image im Netz bereitzustellen, muss ASR mit folgendem Befehl als Server gestartet werden:

```
sudo asr server --source /Pfad_zum/Image.dmg --config /Pfad/zur/server.plist
```

Der letzte Schritt ist der Start des Kopiervorgangs über das Netz. Dazu wird am Client die Installations-DVD eingelegt und in den Dienstprogrammen das Terminal aufgerufen. Folgender Befehl startet den Kopiervorgang:

asr restore --source asr://IP-Adresse-des-Servers --target /Volumes/Zielvolume --erase

Dabei muss beachtet werden, dass der Client eine funktionierende Netzverbindung aufbauen kann.

Prüffragen:

- Entspricht das erzeugte Mac OS X-Image den Sicherheitsvorgaben der Institution?
- Wurde das Mac OS X-Image nach Fertigstellung auf Fehler überprüft?

# M 4.381 Verschlüsselung von Exchange-System-Datenbanken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Microsoft Exchange Informationsspeicher sind Datenbanken, die Benutzer-Postfächer und weitere relevante Daten zentral auf Serverseite verwalten. Microsoft Outlook verwendet sogenannte Personal Store (PST) Container-Dateien, die Datenbank-ähnlich strukturiert sind, und die lokal ein nutzerbezogenes Abbild der Informationsspeicher auf dem Client ablegen. Der Speicherort einer PST-Datei auf dem Server oder lokal beim Client hat einen entscheidenden Einfluss auf die Verschlüsselungsmöglichkeiten.

Für Informationsspeicher-Dateien des Exchange Servers ist eine Verschlüsselung auf Dateiebene, zum Beispiel mit Encrypted File System (EFS), nicht empfohlen; der Aufwand einer derartigen Online-Verschlüsselung ist für die Ausführung eines Microsoft Exchange-Servers nicht geeignet.

Folgende Aspekte sind für lokale PST-Dateien in Microsoft Outlook zu berücksichtigen:

- Die PST-Datei stellt einen Speicher von Benutzerdaten dar: Ordner, E-Mails, deren Anhänge, Kontaktdaten und Kalender. Für PST-Dateien stehen eigene Verschlüsselungsfunktionen zur Verfügung.
- Der Verschlüsselungsgrad kann in drei Stufen eingestellt werden:
  - "keine Verschlüsselung"
  - "komprimierbare Verschlüsselung": Es wird ein Outlook-eigenes Verfahren angewandt.
  - "hohe Verschlüsselung": Es wird ein Outlook-eigenes Verfahren eingesetzt.
- Keine der Optionen bietet ausreichenden Schutz für vertrauliche Daten.
  - Es empfiehlt sich, EFS (Encrypting File System), Windows BitLocker-Laufwerkverschlüsselung oder ähnliche Mechanismen zum Absichern der Daten in einer PST-Datei zu verwenden.
- Dateien, die mit dem Verschlüsselungsgrad "hohe Verschlüsselung" verschlüsselt wurden, können nur eingeschränkt komprimiert vorgehalten werden.
- Die Daten zwischen Server und Client werden bei der Datei-Verschlüsselung unverschlüsselt übertragen. Gegen Abhören müssen sie also zusätzlich geschützt werden (siehe dazu auch M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*).

In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln. Die Randbedingungen hierbei sollten geregelt werden, z. B. in der Sicherheitsrichtlinie für Microsoft Exchange-Systeme (siehe M 2.248 *Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000*). Die Benutzer müssen über die Funktionsweise und Schutzmechanismen bei der Verschlüsselung von PST-Dateien informiert sein.

Die Anforderungen aus dieser Maßnahme können für die Version 2010 wie folgt konkret umgesetzt werden:

- Die Verschlüsselung der Exchange-Datenbanken ist mit der Windows BitLocker-Laufwerksverschlüsselung durchzuführen. Hierbei können sowohl die Datenbanken als auch die Transaktions-Logs berücksichtigt werden, ohne signifikante Performance-Einbußen zu verzeichnen. Die BitLocker Verschlüsselung ist erst ab Windows Server 2008 für die Verwendung mit Microsoft Exchange Server 2010 zugelassen. Nähere Informationen bietet das Dokument "Microsoft-Supportrichtlinie für die Exchange 2007-Datenbankverschlüsselung: Exchange 2007-Hilfe" im Microsoft Technet.
- Es empfiehlt sich, EFS (Encrypting File System) oder Windows BitLocker-Laufwerkverschlüsselung zum Absichern der lokalen Daten in einer PST-Datei bzw. OST-Datei zu verwenden.

Prüffragen:

- Existiert ein Konzept für die Verschlüsselung von PST-Dateien und Informationsspeicher-Dateien?
- Sind die Benutzer über die Funktionsweise und Schutzmechanismen bei der Verschlüsselung von PST-Dateien informiert?

# M 4.382 Auswahl und Prüfung der OpenLDAP-Installationspakete

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In Abhängigkeit von der verwendeten Infrastruktur ist zu entscheiden, ob OpenLDAP aus einem Quelltext- oder Binärpaket installiert wird. Wird eine Betriebssystemdistribution eingesetzt, ist darin oft auch OpenLDAP als Binärpaket enthalten. Dies bietet den Vorteil, dass Abhängigkeiten zu anderen Softwarepaketen meist automatisch aufgelöst und zusätzlich benötigte Pakete nachinstalliert werden. In jedem Fall muss eine geeignete aktuelle Version ausgewählt, beschafft und deren Authentizität überprüft werden (siehe auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*). Die Auswahl und Herkunft der zu installierenden Software sollte ebenso wie der Prozess der Integritätsprüfung der Software dokumentiert werden.

### Grundsätzliches zur Auswahl der Version

Die Entwickler von OpenLDAP stellen den aktuellen Quelltext und Zwischenversionen der Software regelmäßig über eine Versionsverwaltung zur Verfügung. Aus dieser Versionsverwaltung kann jederzeit die aktuellste Version aller Dateien bezogen werden (Head-Branch).

In unregelmäßigen Abständen wird ein erreichter Entwicklungsstand von der weiteren Entwicklung separiert, das heißt, diesem werden bewusst keine neuen Funktionen mehr hinzugefügt (Feature Freeze). Dieser Software-Stand wird bereinigt, getestet und als Release (Veröffentlichung) veröffentlicht. Ein Release erhält eine Versionsnummer in der Form [Software-Generation].[Hauptversion].[Release-Nr.], wie beispielsweise 2.4.23.

OpenLDAP ist als Open Source Software für zahlreiche Betriebssysteme und in zahlreichen Umgebungen nutzbar. Es ist nicht möglich, dass ein Release von den Entwicklern von OpenLDAP in allen möglichen Konstellationen und für alle möglichen Einsatzzwecke getestet wird. Allerdings werten die Entwickler von OpenLDAP die Rückmeldungen von Anwendern und professionellen Distributoren zu einem Release sorgfältig aus. Werden Probleme aufgedeckt, wird in der Regel ein neues Release bereitgestellt. Wird ein Release über einen hinreichend langen Zeitraum von erfahrenen Anwendern und Distributoren verwendet und treten dabei keine Probleme auf, so wird das Release von den OpenLDAP-Entwicklern zum Stable Release (stabile Veröffentlichung) erklärt. Über Releases informieren die OpenLDAP-Entwickler mit der Mailingliste "openldap-announce" (http://www.openldap.org/lists/openldap-announce). Die Liste sollte zur Überwachung der OpenLDAP-Entwicklung abonniert und die erhaltenen Nachrichten archiviert werden.

### Installation aus einem Quelltextpaket

Auf der Internetseite von OpenLDAP wird auf mehrere weltweit verteilte Server verwiesen, von denen die aktuelle Release und Stable Release Versionen heruntergeladen werden können. Über einen FTP-Server werden auch ältere Software-Versionen zum Download bereitgestellt. Durch das Versionsverwaltungssystem sind zudem der aktuelle Entwicklungsstand und Zwischenversionen, die keinem Release entsprechen, verfügbar. In Produktionsumgebungen dürfen ausschließlich Releases oder Stable Releases eingesetzt werden. Es wird empfohlen, den aktuellsten Stable Release zu verwenden. Keinesfalls

dürfen der aktuelle Entwicklungsstand oder eine andere, nicht für den Betrieb empfohlene Version eingesetzt werden.

Die Entwickler von OpenLDAP verwenden **keine** digitalen Signaturen, um die Quelltextpakete abzusichern. Allerdings werden von der komprimierten Version des Quelltextes eines Releases (Datei mit der Endung "tgz") die Hashwerte mit den Verfahren MD5 und SHA1 berechnet und in der zugehörigen Nachricht zum Release über die Mailingliste openldap-announce mitgeteilt. Vor der Installation eines Paketes sollten möglichst beide Hashwerte erstellt und mit den erwarteten Werten abgeglichen werden. Wird nur ein Hashwert berechnet, ist SHA1 zu bevorzugen, da das Verfahren sicherer ist. Die Software und die Information über den Hashwert dürfen nicht zeitgleich vom gleichen Server heruntergeladen werden. Statt dessen sind die Hashwerte aus der Mailingliste openldap-announce zur Prüfung zu verwenden.

**Installation aus Binärpaketen der Distribution**

Wird OpenLDAP aus den offiziellen Installationsquellen der verwendeten Distribution installiert, so ergibt sich die einzusetzende Version in der Regel aus dem Angebot des Distributors. Wird ein Paketmanager (zum Beispiel yum oder rpm) eingesetzt, so stellt dieser auch die Authentizität und Integrität der Pakete sicher.

**Installation aus Binärpaketen fremder Quellen**

Werden Binärpakete aus Installationsquellen bezogen, die nicht Teil der eingesetzten Distribution sind, so muss sichergestellt werden, dass es sich um einen vertrauenswürdigen Anbieter handelt. Bei OpenLDAP gilt dies insbesondere für Windows-Installationspakete, die von Software-Portalen zum Download angeboten werden, aber nicht von den Entwicklern von OpenLDAP erstellt wurden. Die Auswahl der Version sowie die Überprüfung der Authentizität der Binärpakete erfolgen sukzessive, wie im Abschnitt "Installation aus einem Quelltextpaket" oder im Abschnitt "Installation aus Binärpaketen der Distribution" beschrieben.

Prüffragen:

- Wird die Herkunft der OpenLDAP-Installationspakete dokumentiert und eine Integritätsprüfung vorgenommen?
- Ist sichergestellt, dass in Produktionsumgebungen ausschließlich Releases oder Stable Releases eingesetzt werden?

# M 4.383 Sichere Installation von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Installation von OpenLDAP sind verschiedene Aspekte zu berücksichtigen, die direkten Einfluss auf die Sicherheit haben. Diese Maßnahme kann lediglich Hinweise auf besonders zu beachtende Punkte geben. Sie bezieht sich auf die Installation von OpenLDAP aus dem Quelltext. Binärpakete von Betriebssystemherstellern oder Distributoren können davon abweichen, so lösen diese in der Regel die Abhängigkeiten zu anderen Anwendungen selbstständig auf. Die mit OpenLDAP gelieferte Dokumentation, insbesondere die Manpages und die "help"-Ausgabe des Skripts "configure" liefern weitere Informationen.

### Absicherung des Servers

Auch der Server, auf dem OpenLDAP betrieben wird, sollte nach IT-Grundschutz abgesichert werden. Die mit OpenLDAP verarbeiteten Verzeichnisdienstinhalte müssen auf einem lokalen Speichermedium unter Kontrolle des Serverbetriebssystems gespeichert werden, denn auf einem verteilten Dateisystem wie NFS (Network File System) stehen einige, für OpenLDAP notwendige Funktionen nicht zur Verfügung. Auf dem Server muss der Port 389 erreichbar sein. Wird "ldaps://" verwendet (siehe M 5.170 *Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP*), muss der Port 636 ebenfalls geöffnet werden. Andere Dienste sollten auf dem Server nicht betrieben werden (siehe auch M 4.97 *Ein Dienst pro Server*).

### Weitere Software-Produkte

Bei der Installation von OpenLDAP ist zu überprüfen, ob alle im Rahmen der Planung (siehe M 2.484 *Planung von OpenLDAP*) identifizierten weiteren Anwendungen in einer kompatiblen Version installiert sind. Dies gilt insbesondere für die BerkeleyDB. Ist diese bereits installiert, kann die Version am Eintrag DB_VERSION_STRING der Datei "db.h" abgelesen werden. Der Speicherort dieser Datei hängt von der Installation der BerkeleyDB ab, üblich sind auf einem Unix- oder Linux-System /usr/include/db.h, /usr/local/include/db.h und /usr/local/BerkeleyDB/include/db.h. Wird eine Betriebssystem-Distribution verwendet, kann die Version auch im Paketmanager abgefragt werden.

Sind noch weitere Anwendungen zu installieren, kann die Reihenfolge der Installationen wichtig sein, damit für eine Anwendung jeweils alle benötigten Header-Informationen gefunden werden. Eine sinnvolle Installationsreihenfolge ist beispielsweise:

1. OpenSSL oder GnuTLS
2. BerkeleyDB
3. Heimdal Kerberos oder MIT Kerberos
4. Cyrus-SASL
5. OpenLDAP
6. Heimdal Kerberos (sofern schon in Schritt 3 verwendet)

7. Cyrus-SASL

Die zweifache Installation von Heimdal Kerberos (nicht MIT Kerberos) und Cyrus-SASL vor und nach OpenLDAP kann sinnvoll sein, da diese Programme dann wiederum in OpenLDAP Benutzerdaten hinterlegen können.

**Übersetzung und Installation von OpenLDAP**

Die Version der Software muss vor der Installation sorgfältig ausgewählt und deren Integrität überprüft werden (siehe M 4.382 *Auswahl und Prüfung der OpenLDAP-Installationspakete*).

Ein Quelltextpaket sollte unter einem unprivilegierten Benutzeraccount entpackt und mit Hilfe des Skripts "configure" konfiguriert werden. Nicht genutzte Backends und Overlays müssen durch Konfigurationsparameter von der Installation ausgeschlossen werden, da sie wie jede installierte Software die Gefahr von Schwachstellen und Fehlkonfigurationen bergen. Zu beachten ist weiter, dass die Parameter bei der Installation bzw. beim configure-Skript Auswirkungen auf die zu verwendende Konfiguration haben. Beispielsweise können Backends und Overlays fest einkompiliert oder als Module dynamisch geladen werden. Wird das dynamische Laden aktiviert, kann OpenLDAP nicht ohne Weiteres mit einer Konfiguration eingesetzt werden, die fest einkompilierte Backends und Overlays erwartet.

Nachdem das Paket konfiguriert wurde, sind mit dem Programmaufruf "make depend" Abhängigkeiten zu den oben vorbereiteten Anwendungen einzufügen, bevor OpenLDAP mit dem Programmaufruf "make" übersetzt wird. Die übersetzte Software sollte wegen der beschriebenen Abhängigkeiten mittels "make test" geprüft werden. Erst der letzte Schritt, die eigentliche Installation des übersetzten Programms mit "make install", muss gegebenenfalls mit höheren Privilegien erfolgen. Hat der unprivilegierte Benutzeraccount Schreibberechtigungen für sämtliche Zielverzeichnisse der Installation, so kann selbst dieser letzte Schritt ohne root-Berechtigungen durchgeführt werden. Dadurch wird die Sicherheit bei der Installation erhöht, da ein gegebenenfalls fehlerhaftes oder manipuliertes Programm auf diese Weise nur eingeschränkte Rechte erhält.

Wird OpenLDAP aus dem Quelltext übersetzt, müssen die gewählten Parameter genau dokumentiert werden. Zudem empfiehlt es sich, ein Protokoll der Ausgaben des Konfigurations- und Übersetzungslaufs (beispielsweise, indem Ausgaben in eine Datei umgeleitet werden) anzufertigen und aufzubewahren. Alle Installationsschritte sollten dokumentiert werden, damit sie sich im Notfall schnell reproduzieren lassen. Dies betrifft neben den Einstellungen beim Übersetzen auch Installationspfade, Berechtigungen, Änderungen an der Konfiguration und ähnliche Informationen.

Der Start des slapd-Servers sollte im Allgemeinen aus den Startup-Skripten des Betriebssystems erfolgen. So ist der slapd-Server nach einem Neustart des Servers sofort verfügbar und es ist sichergestellt, dass beispielsweise keine Parameter beim Starten des Servers vergessen werden.

Prüffragen:

- Sind die für den slapd-Server nötigen Ports freigegeben, wenn ein lokaler Paketfilter eingesetzt wird?
- Wird die Installation von OpenLDAP nachvollziehbar dokumentiert?
- Werden nur Backends und Overlays für OpenLDAP übersetzt, die auch verwendet werden?

- Wird überprüft, ob Anwendungen, von denen OpenLDAP abhängig ist, in einer kompatiblen Version installiert sind?

# M 4.384 Sichere Konfiguration von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In dieser Maßnahme wird beschrieben, wie der slapd-Server korrekt konfiguriert wird, damit er die ihm zugedachten Aufgaben sicher erfüllt. Um die Sicherheit der Daten eines Verzeichnisdienstes zu gewährleisten, sind auch die verwendeten Client-Anwendungen sicher zu konfigurieren. Dies können, müssen aber nicht, die ldap*-Werkzeuge von OpenLDAP sein. Auf die Vielfalt der verfügbaren Werkzeuge kann in den IT-Grundschutz-Katalogen nicht eingegangen werden. Umso wichtiger ist es, den slapd-Server sicher zu konfigurieren, um sich nicht auf die Sicherheitseinstellungen der verwendeten Clients verlassen zu müssen.

### Verschiedene Konfigurationswege

Bei OpenLDAP bestehen seit der Version 2.3 zwei verschiedene Wege, um den slapd-Server zu konfigurieren. Der klassische Weg ist, alle Einstellungen in die Datei "slapd.conf" einzutragen. Die Datei wird von OpenLDAP auf Unix- und Linux-Systemen unter usr/local/etc/openldap/slapd.conf abgelegt, kann sich aber auch an anderen Orten befinden, beispielsweise wenn distributionsspezifische Installationspakete verwendet werden. In OpenLDAP 2.3 ist zusätzlich das "slapd-config" Format eingeführt worden. Hierbei handelt es sich um eine hierarchische Datenbank, die unterhalb von /usr/local/etc/openldap/slapd.d bzw. an einem distributionsspezifischen Ort in Form von LDIF-Dateien gespeichert wird.

Der wesentliche Vorteil von "slapd-config" gegenüber "slapd.conf" ist die Möglichkeit, die Konfiguration zur Laufzeit zu verändern, während der slapd-Server bei jeder Änderung in der slapd.conf neu gestartet werden muss. Im Zusammenhang mit der Datenbank "slapd-config" wird deshalb auch von der Online-Konfiguration oder seltener von der RunTimeConfiguration (RTC) gesprochen. Die Online-Konfiguration ist mit dem fest eingestellten Suffix "CN=config" Teil des Verzeichnisbaums im slapd-Server. Bei der Planung ist der Konfigurationsweg auszuwählen und dann beizubehalten. Es ist ferner zu beachten, dass die in der Datei "slapd.conf" sichtbaren Einstellungen nicht gültig sind, wenn die Datenbank "slapd-config" verwendet wird.

### Benutzerrechte auf Betriebssystemebene

Während Änderungen der "slapd.conf" umgesetzt werden, indem die Datei editiert wird, sind Änderungen der Online-Konfiguration über Änderungsbefehle im Rahmen des Protokolls LDAP zu initiieren. Daraus folgt, dass ein Administrator bei der Konfiguration via "slapd.conf" Zugriff auf das Dateisystem des IT-Systems benötigt, auf dem der slapd-Server betrieben wird. Dem Systembenutzer, in dessen Kontext der slapd-Server läuft, sollten dagegen nur Leserechte auf die Datei gewährt werden. Für die Konfiguration mittels der Datenbank "slapd-config" ist ein Benutzeraccount im Verzeichnisdienst ausreichend, allerdings muss der Systembenutzer, in dessen Kontext der slapd-Server ausgeführt wird, für das Datenbankverzeichnis schreibberechtigt sein. Wurde OpenLDAP mit root-Berechtigungen installiert und eingerichtet, sind anschließend die Berechtigungen auf das Verzeichnis oftmals falsch gesetzt. Dies kann zur falschen Einschätzung führen, dass der Betrieb des slapd-Servers root-Berechtigungen erfordern würde.

**Aufbau der Konfiguration**

Die Konfigurationseinstellungen werden in OpenLDAP als Direktiven bezeichnet. Es gibt globale Direktiven, Backend-Direktiven und Datenbank-Direktiven. Die globalen Direktiven werden in Abgrenzung zu den Backends und Datenbanken gelegentlich auch als Frontend-Direktiven bezeichnet. Die Direktiven bauen hierarchisch aufeinander auf: Globale bzw. Frontend-Direktiven können von Backend-Direktiven verdrängt werden und diese wiederum von Datenbank-Direktiven. Direktiven haben teilweise Sub-Direktiven, in denen weitere Einstellungen zur jeweiligen Direktive vorgenommen werden. Dies ist insbesondere bei Backends und Overlays der Fall, die durch eine Direktive aufgerufen und durch Sub-Direktiven konfiguriert werden.

**Umwandlung von slapd.conf in slapd-config**

Zwischen den Direktiven beider Konfigurationswege besteht eine eindeutige Beziehung, wobei dem jeweiligen Attribut in der Datenbank "slapd-config" in der Regel die Buchstaben "olc" vorangestellt sind (für Online Configuration). So entspricht "backend" in der "slapd.conf" dem Ausdruck "olcBackend" in der Datenbank "slapd-config". Jedes slap*-Werkzeug von OpenLDAP ist in der Lage, eine klassische Konfiguration in eine Online-Konfiguration umzuwandeln, indem mit dem Parameter "-f" die Position von "slapd.conf" angegeben wird und mit dem Parameter "-F" das Zielverzeichnis von der Datenbank "slapd-config". Ein Beispiel ist: slaptest -f /usr/local/etc/openldap/slapd.conf -F /usr/local/etc/openldap/slapd.d.

Unabhängig von der gewählten Konfigurationsmethode muss jede neue oder geänderte Konfiguration mit dem Werkzeug slaptest darauf geprüft werden, ob sie syntaktisch korrekt ist. Dies ist zu tun, bevor der slapd-Server mit der neuen Konfiguration gestartet wird. Bei Änderungen am laufenden System im Rahmen der Online-Konfiguration weist der slapd-Server unzulässige Konfigurationsänderungen ab. Wichtig ist, alle Konfigurationseinstellungen zu dokumentieren, damit sie sich im Notfall schnell reproduzieren lassen.

**slapd.conf**

Die Datei "slapd.conf" entspricht in ihrer Syntax dem in RFC 2849 definierten LDAP Data Interchange Format (LDIF), das die Administratoren kennen sollten. Die Konfigurationsdatei "slapd.conf" beginnt mit globalen Direktiven. Die globalen Direktiven enthalten die Schema-Spezifikationen. Da die Einbindung von Schemas in die slapd.conf sehr umfangreich werden kann, wird empfohlen, für ein Schema eine eigene lokale Datei zu erstellen und diese mit "include" in der Konfigurationsdatei "slapd.conf" aufzurufen. Auf die globalen Direktiven folgen gegebenenfalls Backend-Direktiven, sofern diese verwendet werden. Sie werden mit der Direktive "backend <typ>" eingeleitet, wobei <typ> das Backend angibt, d. h. dessen Typbezeichnung ohne das Suffix "back-". Ein Beispiel ist "backend hdb". Die dann folgenden Direktiven gelten nicht mehr global, sondern nur für alle Datenbanken dieses Typs. Datenbank-Direktiven werden mit der Direktive "database <typ>" eingeleitet, wobei <typ> analog zu den Backends den Datenbanktyp festlegt. Die folgenden Direktiven gelten dann nur für diese Datenbank. Zu beachten ist, dass der Typ einer bestehenden Datenbank nicht einfach geändert werden darf, indem der Datenbank-Aufruf angepasst wird. Dies hat keinen Einfluss auf die bestehenden Datenstrukturen, die für verschiedene Datenbanktypen unterschiedlich sein können.

**slapd-config**

Im Konfigurations-Teilbaum der Datenbank "slapd-config" werden globale Direktiven als Werte im Bereich "CN=config" oder in der speziellen Dummy-Datenbank "olcDatabase=frontend, CN=config" eingetragen. Schemas sind Kindelemente des Teilbaums "CN=schema, CN=config". Backends und Datenbanken sind wiederum Kindelemente von "CN=config". Die initiale Konfiguration kann erzeugt werden, indem eine bestehende Konfigurationsdatei "slapd.conf" umgewandelt wird oder indem das Suffix "CN=config" mit seinen Elementen im Format LDIF erstellt und mittels "slapadd" in den Verzeichnisdienst importiert wird. Zu beachten ist, dass die "slap-config"-Konfiguration nicht geändert werden darf, indem die LDIF-Dateien im Datenbank-Verzeichnis "slapd.d" angepasst werden. Dabei werden die als operationelle Attribute geführten Zeitstempel nicht aktualisiert. Der slapd-Server bemerkt diese Änderungen deshalb nicht und setzt sie nicht um.

**Overlays**

Overlays werden in der Konfigurationsdatei "slapd.conf" entweder bei den globalen Direktiven aufgerufen oder in einem Datenbank-Abschnitt. Overlays sollten erst nach allen anderen datenbankspezifischen Direktiven aufgerufen werden, um Fehlkonfigurationen zu vermeiden, bei denen Datenbank-Direktiven als Sub-Direktiven des Overlays interpretiert werden. In der Datenbank "slapd-config" sind Overlays Kindelemente von "CN=config" (für globale Overlays) oder des Datenbank-Elements (für datenbankspezifische Overlays). Da die genaue Wirkung von Overlays von der Reihenfolge ihres Aufrufs abhängen kann, sind Overlays sorgfältig in die Konfiguration einzufügen. In der Konfigurationsdatei "slapd.conf" werden die Overlays in umgekehrter Reihenfolge der Nennung innerhalb der Datei aufgerufen.

Im Folgenden werden einige grundlegende und sicherheitsspezifische Direktiven aufgeführt, deren Vorgabewerte bei der Konfiguration kontrolliert und gegebenenfalls angepasst werden sollten. Weitere Direktiven befinden sich im OpenLDAP Administrator's Guide sowie den Manpages.

- suffix bzw. olcSuffix (Datenbank-Direktive)

Dies ist die wichtigste Sub-Direktive eines Datenbank-Aufrufs. Mit ihr wird festgelegt, welcher Teil des Verzeichnisses in der jeweiligen Datenbank abzulegen ist, z. B. "DC=bsi, DC=bund, DC=de". Soll eine Datenbank einen untergeordneten Teilbaum aufnehmen, so muss diese Datenbank vor der übergeordneten Datenbank aufgerufen werden. Zum Beispiel muss "DC=grundschutz, DC=bsi, DC=bund, DC=de" vor "DC=bsi, DC=bund, DC=de" definiert werden, da sonst immer die übergeordnete Datenbank selektiert wird.

- include (nur slapd.conf)

In dieser Direktive kann auf Dateien außerhalb der Konfigurationsdatei "slapd.conf" verwiesen werden, deren Inhalt dann bei der Auswertung der "slapd.conf" an die Stelle der Direktive tritt. Die Direktive wird empfohlen, um beispielsweise Schema-Definitionen und Zugriffskontrolllisten separat zu verwalten. Die Direktive kann auch in diesen externen Dateien verwendet werden. Der slapd-Server erkennt allerdings keine Ringverweise, was zum Einlesen einer scheinbar unendlich großen Konfiguration führen kann ("slapd.conf" enthält "include ACL1.conf", "ACL1.conf" enthält "include ACL2.conf", "ACL2.conf" enthält "include ACL1.conf"). In einem solchen Fall ist der slapd-Server nicht nutzbar, gegebenenfalls wird der Betrieb des kompletten IT-Systems durch den Ressourcenbedarf des slapd-Servers gestört. Es ist ebenfalls darauf zu achten, dass die für den Betrieb des slapd-Ser-

vers verwendete Benutzerkennung ein Leserecht auf die externen Dateien eingeräumt bekommt. Wenn eine "slapd.conf"-Konfiguration in eine "slapd-config"-Konfiguration umgewandelt wird, werden die über "include" eingefügten Dateien einbezogen.

- idleTimeout bzw. olcIdleTimeout (globale Direktive)

Über diese Direktive wird ein Wert in Sekunden festgelegt, nachdem für eine ungenutzte Verbindung zu einem Client ein "unbind" erzwungen wird. Diese Direktive ist in der Voreinstellung mit 0 belegt und dadurch deaktiviert. Es wird empfohlen, hier einen Wert größer Null zu setzen, damit ungenutzte Verbindungen zu nicht ordnungsgemäß heruntergefahrenen Clients oder zu verlassenen Workstations nicht für Angriffe verwendet werden können. Der Wert sollte sorgsam festgelegt werden und die in der Institution übliche Nutzung nicht behindern. Sinnvoll ist z. B. ein Wert kleiner 900, damit ungenutzte Verbindungen nach spätestens 15 Minuten Inaktivität getrennt werden.

- referral bzw. olcReferral (globale Direktive)

Diese Direktive benennt einen LDAP-Server, den der slapd-Server an einen anfragenden Client zurückmeldet, wenn der slapd-Server die vom Client gewünschte Operation nicht selbst durchführen kann. Die Direktive sollte mit einem übergeordneten LDAP-Server belegt werden, sofern ein solcher vorhanden ist, um die Verfügbarkeit zu verbessern. Es ist darauf zu achten, keine Ringverweise zwischen gleichberechtigten Servern einzurichten, da dies von einigen Client-Anwendungen nicht bemerkt wird.

- readonly bzw. olcReadonly (Datenbank-Direktive)

Mit dieser Direktive wird eine Datenbank in einen Nur-Lese-Zustand versetzt.

- rootDN bzw. olcRootDN und rootPW bzw. olcRootPW (Datenbank-Direktiven)

Über diese beiden Direktiven werden eine administrative Benutzerkennung für die jeweilige Datenbank und das zugehörige Passwort festgelegt. Limits oder Zugriffsbeschränkungen (siehe M 4.387 *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*) haben auf diese Benutzerkennung keine Auswirkungen. Die sichere Ablage eines Passwortes, wie in der Maßnahme M 4.388 *Sichere Authentisierung gegenüber OpenLDAP*beschrieben, ist auch für das Passwort des "rootDN" durchzuführen.

- sizeLimit bzw. olcSizeLimit (globale Direktive)

Die Direktive schränkt die Anzahl von Ergebnissen für Suchoperationen ein. Der Vorgabewert für die Direktive beträgt 500. Der Wert ist zu prüfen und gegebenenfalls anzupassen, er sollte aber nicht auf "unlimited" gesetzt werden, um Denial-of-Service-Attacken auf den Verzeichnisdienst zu erschweren und vollständige Kopien der Datenbank durch unberechtigte Benutzer zu verhindern.

- timeLimit bzw. olcTimeLimit (globale Direktive)

Mit dieser Direktive wird die Zeit in Sekunden angegeben, bevor eine Suche abgebrochen wird. Der Vorgabewert für die Direktive beträgt 3600. Der Wert ist zu prüfen und gegebenenfalls anzupassen, er sollte aber nicht auf "unlimited" gesetzt werden, weil er sonst Denial-of-Service-Attacken auf den Verzeichnisdienst erleichtert.

- limits bzw. olcLimits (Datenbank-Direktive)

Diese Direktive erlaubt Einschränkungen analog zu sizeLimit und timeLimit auf Datenbankebene. In diesem Fall werden globale Limits nicht beachtet. Hier sind auch Limits pro Benutzer möglich. Die Benutzerangabe erfolgt dabei analog zur Benutzerangabe im Rahmen von Zugriffskontrolllisten (siehe

M 4.387 *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*). Es wird empfohlen, benutzerspezifische Limits zu setzen, um beispielsweise nicht authentisierte Benutzer von der Erkundung der Verzeichnisstruktur abzuhalten oder Einschränkungen zu lockern, wenn sie die Replikation behindern.

Weitere Direktiven werden in anderen Maßnahmen zu OpenLDAP angesprochen, insbesondere in der Maßnahme M 4.385 *Konfiguration der durch OpenLDAP verwendeten Datenbank*.

Prüffragen:

- Sind für die Konfiguration von OpenLDAP via slapd.conf die korrekten Berechtigungen auf Betriebssystemebene gesetzt?
- Werden die Vorgabewerte aller relevanten Konfigurationsdirektiven von OpenLDAP geprüft und gegebenenfalls angepasst?
- Werden die Sub-Direktiven von Backends und Overlays von OpenLDAP in die Konfiguration einbezogen?
- Werden angemessene Zeit- und Größenbeschränkungen für die Suche innerhalb von OpenLDAP festgelegt?
- Wird die Konfiguration des slapd-Servers nach jeder Änderung mit dem Werkzeug slaptest geprüft und nachvollziehbar dokumentiert?

# M 4.385 Konfiguration der durch OpenLDAP verwendeten Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In OpenLDAP können durch die Konfigurationsdirektiven Einstellungen für das tatsächlich verwendete Datenbankmanagementsystem (DBMS) vorgenommen werden. Die Einstellungen sind nur für die BerkeleyDB über die Backends "back-bdb" oder "back-hdb" möglich. Sie haben keinen unmittelbaren Einfluss auf die Funktion und Bedienung von OpenLDAP, haben aber große Auswirkungen auf die Performance des Verzeichnisdienstes. Im Folgenden werden nur sicherheitsrelevante Einstellungen und häufige Fehlerquellen aufgeführt. Für weitere Einstellungen sollte gegebenenfalls ein Datenbankspezialist zurate gezogen werden. Beispielsweise ergeben sich aus den Einstellungen zur Zwischenspeicherung und Transaktionsprotokollen Geschwindigkeitsvorteile zu Lasten einer optimalen Integrität, die sorgsam im Einzelfall abzuwägen sind.

- dbDirectory bzw. olcDbDirectory
  Über die Direktive kann der Speicherort für Datenbankdateien im IT-System festgelegt werden, auf dem der slapd-Server betrieben wird. Die Benutzerkennung, in deren Kontext OpenLDAP ausgeführt wird," muss Schreibrechte auf das angegebene Verzeichnis haben.
- dbConfig bzw. olcDbConfig
  Die in dieser Direktive vorgenommenen Einstellungen sind datenbankspezifisch und werden in die Datei "DB_CONFIG" des DBMS eingetragen. Wenn eine solche Datei noch nicht existiert, wird sie durch die Nutzung dieser Direktive erstellt. Es ist zu beachten, dass spätere Änderungen in der Zieldatei selbst, beispielsweise mit einem Texteditor, die hier gewählten Einstellungen überschreiben. Deshalb muss festgelegt sein, wie und durch wen an welcher Stelle Einstellungen vorgenommen werden. Änderungen der Direktive erzwingen immer einen Neustart des DBMS, jedoch nicht des slapd-Servers. Dies kann je nach Umfang und Einstellungen der Datenbank eine längere Zeit in Anspruch nehmen, währenddessen der Verzeichnisdienst nicht verfügbar ist. Änderungen der Datenbank-Konfiguration sollten deshalb sorgfältig geplant und möglichst in Wartungsfenstern z. B. nachts oder am Wochenende umgesetzt werden.
- dbIndex bzw. olcDbIndex
  Mit dieser Direktive können Attribute von Verzeichnisdienstobjekten festgelegt werden, für die ein Index erstellt werden soll. Ohne einen Index müssen bei einer Suche sämtliche Objekte aufgerufen und geprüft werden. Um die Verfügbarkeit zu verbessern, sollten deshalb häufige Suchen durch einen Index unterstützt werden. Fehlende aber wünschenswerte Indizes können aus den OpenLDAP-Protokollen (siehe M 4.407 *Protokollierung beim Einsatz von OpenLDAP*) erkannt werden. Erscheint dort häufig der Hinweis, dass der Zugriff auf einen bestimmten Attributsindex fehlschlug, sollte ein entsprechender Index eingerichtet werden. Die in der Direktive angegebenen Indizes werden vom slapd-Server automatisch erzeugt. Sollte der slapd-Server während des Indizierungsvorgangs gestoppt werden, so wird die Indizierung nicht automatisch fortgesetzt. In diesem Fall ist sie mit dem Werkzeug slapindex manuell durchzuführen.
- dbMode bzw. olcDbMode
  Über diese Direktive werden die Benutzerrechte festgelegt, die für neu angelegte Datenbankdateien gelten. Die Voreinstellung 0600 bzw. -rw-------

gewährt lediglich der Benutzerkennung Zugriff, in deren Kontext der slapd-Server betrieben wird. Diese Voreinstellung ist sinnvoll und sollte nicht geändert werden.

Prüffragen:

- Werden Zugriffsrechte für neu angelegte Datenbankdateien auf die Benutzerkennung beschränkt, in deren Kontext der slapd-Server betrieben wird?

# M 4.386 Einschränkung von Attributen bei OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der slapd-Server kann durch Overlays in die Lage versetzt werden, Restriktionen umzusetzen, ohne dass dafür Schemas angepasst oder erstellt werden müssen. Derartige Einschränkungen sind sinnvoll, um die Qualität und Integrität der Verzeichnisdienstinhalte zu verbessern. Folgende Overlays können verwendet werden:

- constraint
  Das Overlay "constraint" (Constraints) ermöglicht, dass Werte einem bestimmten regulären Ausdruck entsprechen müssen. So kann beispielsweise erzwungen werden, dass das Attribut "mail" lediglich mit Mailadressen der eigenen Institution belegt werden kann.
- unique
  Das Overlay "unique" (Attribute Uniqueness) ermöglicht, dass ein ausgesuchter Wert lediglich einmal im Verzeichnisbaum vorhanden sein darf. So kann beispielsweise verhindert werden, dass eine Personalnummer zwei verschiedenen Benutzern zugewiesen wird.
- refint
  Das Overlay "refint" (Referential Integrity) wahrt die referenzielle Integrität von Referenz-Attributen. Werden zum Beispiel Distinguished Names (DNs) als Gruppenmitglieder eingetragen oder der DN eines Vorgesetzten in einem Attribut beim Mitarbeiter hinterlegt, so ändert das Overlay "refint" diese Referenzen, wenn der jeweilige DN verändert wird. Dafür führt "refint" bei der Änderung jedes DNs eine Suche durch, ob der DN in solche Attribute eingetragen ist. Änderungen setzt das Overlay "refint" im Attribut um, im Fall der Löschung entfernt es den DN.
  Achtung: Entfernt das Overlay das letzte Mitglied aus einer Gruppe, so wird stattdessen der in der Sub-Direktive "refint_nothing" definierte DN eingefügt, da leere Gruppen das Gruppenschema verletzen können. Hier ist darauf zu achten, einen geeigneten DN, wie einen fachlichen Administrator, vorzugeben, damit kein DN mit geringeren Rechten durch die Gruppe unangemessene Rechte erhalten würde.

Bei derartigen Beschränkungen ist zu beachten, dass diese nur für neue oder geänderte Attribute und Objekte gelten. Bestehen Verstöße gegen die festgelegten Regeln, bevor die Overlays aktiviert werden oder werden unpassende Datensätze durch einen direkten Zugriff auf die verwendete Datenbank eingefügt, so wirken die genannten Overlays nicht.

Solche Restriktionen dürfen ausschließlich auf Nutzerdaten angewendet werden. Werden die Beschränkungen zum Beispiel verwendet, um operationelle Attribute vorzugeben oder werden sie innerhalb der "slapd-config"-Konfiguration erzwungen, kann dies zu unvorhersehbarem Verhalten bis hin zur Unbrauchbarkeit des slapd-Servers führen.

Prüffragen:

- Werden die Einschränkungen von Attributen von OpenLDAP ausschließlich auf Nutzerdaten und nicht auf operationelle Attribute angewendet?

# M 4.387 Sichere Vergabe von Zugriffsrechten auf OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die richtige Vergabe und korrekte Umsetzung von Zugriffsrechten sind elementare Voraussetzungen, um die Informationssicherheit zu gewährleisten. Wann immer ein Benutzer eine Operation gegen ein Objekt im Verzeichnisdienst richtet, muss entschieden werden, ob es zulässig ist, diese Operation auszuführen. Das Berechtigungskonzept ist im Rahmen der Maßnahme M 2.405 *Erstellung einer Sicherheitsrichtlinie für den Einsatz von Verzeichnisdiensten* festzulegen. Die dort getroffenen Regelungen müssen in OpenLDAP technisch umgesetzt werden. Allgemeine Informationen zu diesem Thema finden sich auch in der Maßnahme M 4.309 *Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste*. Der LDAP-Standard bestimmt lediglich, dass eine Zugriffskontrolle stattfinden soll und definiert im Rahmen des Standards Server-Antworten für den Fall, dass Operationen wegen unzureichender Berechtigungen abgewiesen werden. Wie eine Zugriffskontrolle jedoch konkret umzusetzen ist, wird im LDAP-Standard nicht spezifiziert und ist in hohem Maße vom eingesetzten Verzeichnisdienst abhängig. Auf die Vergabe von Zugriffsrechten in OpenLDAP wird deshalb in dieser Maßnahme umfassend eingegangen.

### Zugriffskontrolllisten in OpenLDAP

In OpenLDAP werden Zugriffskontrolllisten (Access Control Lists, ACLs) in Form von Direktiven in der Konfiguration geführt. Bei jeder von einem Benutzer ausgelösten Operation wird ermittelt, ob diese durch eine Direktive gedeckt ist.

Eine Zugriffsdirektive hat folgende Syntax:

access to [Zielobjekt]

by [Benutzer] [Berechtigungsumfang]

by [Benutzer] [Berechtigungsumfang]

...

Als Zielobjekt können dabei unter anderem Suffixe, Objekte oder Attribute bestimmt werden. Sogar das Ergebnis einer LDAP-Suche oder bestimmte Attributbelegungen können hier vorgegeben werden. Dabei sind fast beliebige Detailtiefen und Kombinationen möglich, auf die hier nicht eingegangen werden kann. Besonders zu nennen ist jedoch das Zielobjekt *, das alle möglichen Zielobjekte des Verzeichnisdienstes umfasst.

### Benutzer

Als Benutzer sieht OpenLDAP unter anderem folgende Eintragungen vor:

- ***** für alle Benutzer des Verzeichnisdienstes, einschließlich nicht authentisierter Benutzer
- **anonymus** für nicht authentisierte Benutzer
- **users** für authentisierte Benutzer (für die Unterscheidung von authentisierten und nicht authentisierten Benutzern siehe M 4.388 *Sichere Authentisierung gegenüber OpenLDAP*)

- **self** für Benutzer, die einen "bind" mit der Identität des Zielobjektes vollzogen haben
- **Distinguished Names** (DNs) für voll qualifizierte Benutzer oder reguläre Ausdrücke
- **Attributsfilter**, um den Zugriff auf ein Objekt zu gewähren, bei dem der Benutzer in ein Attribut eingetragen ist, beispielsweise als Vorgesetzter einer Person
- **Gruppenattribute**, um Zugriffsrechte über statische oder dynamische Gruppenmitgliedschaften zu steuern
- **IP-Einträge** für alle Benutzer, deren Client aus einem vorgegeben IP-Adressraum oder mit einer vorgegebenen Domäne verbunden ist

Obwohl von OpenLDAP akzeptiert, sollte die Zugriffssteuerung in keinem Fall anhand der IP-Adressen vorgenommen werden, da IP-Adressen einfach gefälscht werden können.

**Berechtigungsumfang**

Als Berechtigungsumfang kennt OpenLDAP folgende Werte:

- **none**: keine Zugriffsberechtigung
- **disclose**: Existenzprüfung zur Fehlerverfolgung
- **auth**: Möglichkeit, einen "bind" als Zielobjekt durchzuführen
- **compare**: Durchführung von Vergleichen
- **search**: Anwendung von Suchfiltern auf das Zielobjekt
- **read**: Lesender Zugriff auf das Zielobjekt
- **write**: Schreibender Zugriff auf das Zielobjekt (ändern, umbenennen, löschen)
- **manage**: Vollzugriff einschließlich der benötigten Rechte, um auf operationelle Attribute zuzugreifen

Daneben existieren noch spezielle Berechtigungen wie "selfwrite". Diese ermöglicht es, lediglich den eigenen DN zu schreiben, beispielsweise um eigene Gruppenmitgliedschaften zu pflegen. Jeder Berechtigungsumfang enthält automatisch alle jeweils vorgenannten. So gibt eine read-Berechtigung auch die Rechte zu "disclose", "auth", "compare" und "search"-Aktionen. Dies ist in der Regel sinnvoll und die Verwendung der "access levels" ist meist ausreichend. Andernfalls können Berechtigungen über privilege-Operatoren detaillierter vergeben werden.

**Mehrere "by"-Klauseln**

Innerhalb einer Zugriffsdirektive können beliebig viele "by"-Klauseln aufeinander folgen. Die Auswertung innerhalb einer Direktive wird gestoppt, sobald eine zutreffende "by"-Klausel gefunden wird. Dies ist der Fall, sobald ein in der "by"-Klausel genannter Benutzer dem anfragenden Benutzer entspricht oder diesen beinhaltet. Eine klassische Zugriffsdirektive ist z. B.

access to *

by self write

by anonymus auth

by group.exact="CN=admin, ou=groups, DC=bsi, DC=bund, DC=de" write

by users read

Durch diese Direktive kann jeder Benutzer seinen eigenen Eintrag verändern, ein anonymer Benutzer kann jeden Eintrag benutzen, um sich zu authentisie-

ren, Mitglieder der Administratorengruppe können Einträge verändern und ein authentisierter Benutzer kann alle Einträge lesen. Die letzte "by"-Klausel könnte auch "by * read" lauten und hätte den selben Effekt. Da für nicht authentisierte Benutzer bereits die zweite "by"-Klausel zutrifft, wird die vierte Klausel immer nur für authentisierte Benutzer (users) geprüft, die keine Administratoren sind. Wären die erste und vierte "by"-Klausel vertauscht, würden keine Schreibrechte auf Einträge bestehen, da die hinter der "users"-Klausel folgende "group"-Klausel sowie die "self"-Klausel nicht mehr verarbeitet würden. Trifft keine Benutzerangabe in einer Direktive auf einen anfragenden Benutzer zu, wird diesem auch keine Berechtigung gewährt. Bei der Auswertung wird jede Direktive behandelt, als würde sie mit der Klausel "by * none" abschließen, auch wenn diese nicht dort steht.

**Mehrere Zugriffsdirektiven**

Es können beliebig viele Zugriffsdirektiven aufeinanderfolgen. Die Direktiven werden der Reihe nach abgearbeitet. Eine ACL wird nicht weiter ausgewertet, sobald eine zutreffende Direktive gefunden wird. Eine Direktive gilt als zutreffend, wenn das angefragte Zielobjekt dem aus der Direktive entspricht oder in diesem enthalten ist. Zum Beispiel führen die Direktiven

access to dn.subtree="DC=grundschutz, DC=bsi, DC=bund, DC=de"

by users write

access to dn.subtree="DC=bsi, DC=bund, DC=de"

by users read

dazu, dass authentisierte Benutzer alle Inhalte des fiktiven Teilverzeichnisses bsi.bund.de lesen können und auf Inhalte von grundschutz.bsi.bund.de schreibend zugreifen dürfen. Wären die Direktiven in umgekehrter Reihenfolge angegeben, würde das Schreibrecht entfallen, da eine Operation mit dem Zielobjekt "DC=grundschutz" bereits eine Teilmenge von "DC=bsi, DC=bund, DC=de" ist. Trifft keine Zielobjektangabe irgendeiner Direktive auf ein angefragtes Zielobjekt zu, so wird auf das Zielobjekt auch keine Berechtigung gewährt. Jede Zugriffskontrollliste wird bei der Auswertung behandelt, als würde sie der Direktive "access to * by * none" abschließen, auch wenn diese nicht dort steht.

**Reihenfolge und Control Flags**

Aus diesen Beispielen wird ersichtlich, dass die Reihenfolge von ACL-Einträgen von großer Bedeutung ist. Es gilt grundsätzlich, dass spezielle Rechte zuerst und allgemeine Rechte zuletzt definiert werden müssen.

Sollte dennoch der Bedarf bestehen, die Berechtigungen weiter auszuwerten, nachdem eine zutreffende Regel gefunden wurde, kann dies durch die Steuerungsschalter ("Control Flags") "continue" (für die Prüfung weiterer "by"-Klauseln innerhalb einer Direktive) und break (für die Prüfung weiterer Direktiven) erreicht werden. Die Control Flags sollten äußerst sparsam eingesetzt werden, da sie eine Zugriffskontrollliste unübersichtlich machen. Es muss beachtet werden, dass eine weitere zutreffende Regel die schon gewährten Rechte ersetzt. Das Control Flag "continue" kann durch eine korrekte Planung der ACL eigentlich immer vermieden werden. Es wird nur benötigt, wenn die "privilege"-Operatoren eingesetzt werden.

Das Control Flag "break" ist dazu geeignet, eine umfassende Berechtigung für spezielle Benutzer an den Anfang einer ACL zu stellen. Zum Beispiel gewährt

die folgende Direktive einem für Replikationszwecke eingesetzten Benutzer Leserechte auf das gesamte Verzeichnis, während die Direktive für alle anderen Benutzer "überlesen" wird:

access to *

by dn.exact="[DN des Replikations-Benutzers]" read

by * break

ACL in der slapd-config

Die bisher beschriebene Syntax gilt für die Konfiguration mittels der Konfigurationsdatei "slapd.conf". Wird die Datenbank "slapd-config" verwendet, gilt entsprechend:

olcAccess: {n}to [Zielobjekt]

by [Benutzer] [Berechtigungsumfang]

by [Benutzer] [Berechtigungsumfang]

...

Der optionale Index {n} steuert die Reihenfolge der Einträge, die sich im Gegensatz zur Konfigurationsdatei "slapd.conf" nicht aus deren Positionen in der Datei ergeben kann, da die Verzeichnisdienstobjekte olcAccess auf der gleichen Ebene stehen. Ohne einen Index ist die konfigurationsinterne Reihenfolge und damit die Wirksamkeit der Einträge nicht vorhersehbar.

**ACLs global und datenbankspezifisch**

Zugriffskontrolllisten lassen sich global und auf Datenbankebene festlegen. Die Zusammenhänge müssen bei der Umsetzung von OpenLDAP korrekt berücksichtigt werden. Datenbank-Direktiven haben Vorrang vor globalen Direktiven. Dabei wird die globale Zugriffskontrollliste an die datenbankspezifische angehängt und die Gesamtliste für die Auswertung durch die Direktive "access to * by * none" abgeschlossen, auch wenn diese nicht eingetragen wurde. Spezielle Direktiven zu Beginn einer globalen ACL werden deshalb bei Kombination mit einer datenbankspezifischen Zugriffskontrollliste oft nicht wie gewünscht umgesetzt.

**Zugriffsrechte über Gruppenmitgliedschaften**

Die Vergabe von Berechtigungen über Gruppenmitgliedschaften ermöglicht es, die Zugriffsrechteverwaltung und die technische Wartung des slapd-Servers organisatorisch zu trennen. Um Zugriffsrechte zu verwalten, müssen nur noch Gruppenobjekte geändert werden, ein Zugriff auf die Konfiguration selbst ist nicht mehr notwendig.

Werden Zugriffsrechte über Gruppenmitgliedschaften verwaltet, so sind folgende Punkte zu beachten:

- OpenLDAP löst in der Version 2.4 keine Zugriffsrechte auf, wenn sich Gruppen innerhalb von Gruppen befinden. Als Lösungsansatz bietet OpenLDAP das "Set"-Konzept an. Solange "Sets" in der Version 2.4 als experimentell eingestuft werden, sollten sie in produktiven Umgebungen nicht eingesetzt werden.
- Es wird empfohlen, das Overlay "memberof" (Member of) einzusetzen. Wenn ein DN einem Gruppenobjekt zugeordnet wird, sorgt das Overlay

"memberof" dafür, dass die entsprechende Eigenschaft auch beim DN als operationelles Attribut vermerkt wird. Dadurch werden aufwändige Suchoperationen im Rahmen der Zugriffskontrolle vermieden.

In OpenLDAP besteht für eine ebenfalls von der Konfiguration losgelöste Verwaltung von Zugriffsrechten die Möglichkeit, über den Mechanismus "Access Control Information" (ACI) Zugriffsrechte beim jeweiligen Benutzer zu hinterlegen. ACI ist jedoch sehr aufwändig in der Konfiguration, da jeder Benutzer einzeln einzurichten ist. Zudem ist die Syntax des Mechanismus noch nicht standardisiert, der Mechanismus hat in der Version 2.4 zudem nur einen experimentellen Status. Solange ACI einen experimentellen Status hat, sollte es nicht verwendet werden.

**Testen von Zugriffsberechtigungen**

Jede Änderung der Zugriffskontrollliste sollte anschließend durch das Werkzeug slapacl überprüft werden. Über das Werkzeug werden ein Benutzer und eine Operation angegeben und slapacl ermittelt, ob diese Operation vom angegebenen Benutzer erfolgreich durchgeführt werden könnte, ohne die Operation tatsächlich durchzuführen. Diese Prüfung sollte insbesondere dann durchgeführt werden, wenn der Zugriff abgelehnt werden soll. Das Tool slapacl prüft gegen die Konfigurationsdatei "slapd.conf". Wirksam ist die geänderte Zugriffskontrollliste aber erst nach einem Start oder Neustart des slapd-Servers. Darum sollte der slapd-Server beim Einsatz der slap*-Werkzeuge immer gestoppt sein. Selbst wenn der Einsatz der slap*-Werkzeuge keine technischen Auswirkungen hat, können Ergebnisse bei laufendem slapd-Server zu falschen Schlussfolgerungen führen.

Es wird empfohlen, aus dem Berechtigungskonzept Testfälle abzuleiten und diese mit dem Werkzeug slapacl zu testen,

- wenn die Zugriffskontrolllisten wesentlich verändert wurden,
- wenn neue Backends, Datenbanken oder Suffixe definiert wurden oder
- wenn OpenLDAP aktualisiert wurde.

**Keine Einschränkung des rootDN**

Die ACLs gelten grundsätzlich nicht für den rootDN einer Datenbank. Wird er dennoch in Zugriffskontrolllisten einbezogen, so führt dies lediglich zu erhöhtem Administrationsaufwand und einem Performanceverlust. Andererseits ist zu beachten, dass der Verzicht auf Zugriffskontrolllisten nicht dazu führt, dass lediglich der "rootDN"-Zugriff auf den Verzeichnisdienst unter OpenLDAP hat. Ohne Zugriffskontrolllisten greift eine Voreinstellung, die allen, auch anonymen Benutzern, Leserecht auf alle Inhalte des Verzeichnisdienstes gewährt. Auf ACLs darf keinesfalls verzichtet werden.

**Komplexität der Zugriffsberechtigungen**

Zugriffskontrolllisten können in zahlreichen Einzelaspekten gesteuert werden und fast beliebig komplex sein. Administratoren sollten sich mit den umfangreichen Beispielkonfigurationen im frei verfügbaren OpenLDAP Administrator's Guide vertraut machen. Es wird jedoch darauf hingewiesen, dass sich die in dieser Maßnahme zusammengestellten "access levels" bewährt haben und für die Abbildung von Zugriffsrechten in der Regel ausreichend sind. Insbesondere mit regulären Ausdrücken und Suchfiltern ist vorsichtig zu verfahren, da diese sehr leicht zu umfangreich definiert werden und so ungewollt Zugriffsrechte gewähren. Darüber hinaus schränken sie die Verarbeitungsgeschwindigkeit bei Zugriffen deutlich ein, da ihre Prüfung Ressourcen verbraucht. Je umfangreicher die Zugriffsrechte in der slapd-Server-Konfiguration wird, desto wichtiger sind umfangreiche Tests mittels slapacl. Kommt es hierbei immer

wieder zu Fehlern, sollte das Design der Zugriffsrechte grundsätzlich überarbeitet werden.

Prüffragen:

- Wird ein Berechtigungskonzept für den Zugriff auf Objekte in OpenLDAP technisch umgesetzt?
- Werden die Zusammenhänge von globalen und datenbankspezifischen ACLs bei der Umsetzung von OpenLDAP korrekt berücksichtigt?

# M 4.388 Sichere Authentisierung gegenüber OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um OpenLDAP zu nutzen, ist es in der Regel notwendig, dass der Verzeichnisdienst einer Sitzung die Identität eines Benutzers zuordnen kann. Nur dann kann der Verzeichnisdienst sinnvoll eingesetzt werden, um z. B. Betriebssystemressourcen zu verwalten und nur dann greifen die festgelegten Zugriffsrechte (siehe M 4.387 *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*). Im Rahmen des "binds" am slapd-Server wird deshalb die Identität des Benutzers angegeben. Geschieht dies nicht, wird von einem anonymen Zugriff (anonymus) gesprochen. Wird die Identität im Rahmen des "binds" angegeben, so sollte der Benutzer nachweisen, dass er tatsächlich die Identität hat, die er vorgibt. Ist ein solcher Nachweis nicht notwendig, kann sich jeder Benutzer mit einer beliebigen Identität anmelden, es handelt sich dann um eine nicht authentisierte Nutzung (unauthenticated).

### Anonyme Benutzer

Wenn nicht im Rahmen der Planung von OpenLDAP (siehe M 2.484 *Planung von OpenLDAP*) entschieden wurde, dass der Verzeichnisdienst anonym genutzt werden darf, muss die anonyme Nutzung durch die Konfigurationsdirektive "disallow bind_anon" unterbunden werden.

Wenn der Verzeichnisdienst zwischen verschiedenen Benutzern unterscheiden soll, muss auch eine Authentisierung stattfinden. Eine Anmeldung ohne Identitätsnachweis sollte außerhalb von Teststellungen nicht zugelassen werden. Die Authentisierung ist mit der Konfigurationsdirektive "require authc" zu erzwingen.

### Authentisierung mittels Passwort

Die grundsätzliche Methode, die OpenLDAP zur Authentisierung eines Benutzers vorsieht, ist die Kombination einer Benutzerkennung und eines Passwortes, sie wird als "simple bind" bezeichnet. Diese Authentisierungsmethode gilt dann als sicher, wenn das verwendete Passwort nur dem zugehörigen Benutzer bekannt ist.

### Übertragung des Passworts

Nach den Spezifikationen des Standards LDAPv3 wird das Passwort zur Authentisierung im Klartext an den Server übertragen. Daher muss die Kommunikationsverbindung zwischen Client und Server verschlüsselt werden (siehe M 5.170 *Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP*), damit das Passwort nicht von einem Angreifer abgehört werden kann.

Es wird dringend empfohlen, die mögliche Verschlüsselung der Kommunikationsverbindung durch den slapd-Server nicht nur anzubieten, sondern als Voraussetzung für eine "bind"-Operation zu erzwingen. Andernfalls hängt die Sicherheit einer Verbindung von der Entscheidung und der Fachkenntnis des Benutzers sowie den Fähigkeiten der eingesetzten Client-Software ab. Über die Direktive "security" können global oder datenbankspezifisch Anforderungen an die bestehende Verbindungssicherheit über die Verschlüsselungsstärke für verschiedene Operationen festgelegt werden, beispielsweise durch "security simple_bind=XYZ". Die Angabe XYZ ist durch einen Security Strength

Factor (SSF) zu ersetzen. Der SSF ist eine Zahl, die für das Verschlüsselungsverfahren und die verwendete Schlüssellänge steht, die zur Verschlüsselung der eigentlichen Nachrichten mit einer symmetrischen Chiffre verwendetet wird, wie beispielsweise 56 für DES, 112 für Triple DES und 128, 192, oder 256 für AES. Sie sollte mindestens auf 112 festgelegt werden. Gegebenenfalls sind aktuelle Forschungsergebnisse und die Empfehlungen des BSI zu berücksichtigen. In der Direktive aufgeführte Operationen werden bei einer niedrigeren Verbindungssicherheit abgewiesen.

**Ablage des Passworts**

Ist sichergestellt, dass das Passwort nur gesichert übertragen wird, kann das Passwort immer noch auf Seiten des Servers gefährdet sein. Wird ein Server kompromittiert oder gelingt beispielsweise ein Zugriff auf eine Datensicherung der Verzeichnisdienstobjekte, könnte ein Angreifer Kenntnis von Passwörtern der Benutzer erlangen. Deshalb sind lediglich die Prüfsummen (Hashwerte) von Passwörtern zu speichern. Dem steht entgegen, dass der LDAP-Standard keine gehashten Passwörter unterstützt. OpenLDAP realisiert serverseitig eine Ablage der gehashten Passwörter und unterstützt verschiedene Hashing-Algorithmen. Es sollte ein Algorithmus aus der Gruppe Secure Hash Algorithm (SHA) in der Variante SSHA, das heißt "gesalzen" verwendet werden. Gesalzen bedeutet, dass das Passwort vor Bildung des Hashwertes um einen weiteren Wert ergänzt wird, um Wörterbuchattacken auf das Passwort zu erschweren. Keinesfalls sollte als Hashing-Algorithmus CRYPT ausgewählt werden. CRYPT wird betriebssystemspezifisch implementiert, weshalb die Authentisierung gegenüber OpenLDAP nach einer Migration auf ein anderes Betriebssystem gegebenenfalls nicht mehr funktioniert.

Der slapd-Server wird über die Direktive "password-hash {Algorithmus}" angewiesen, nur den, mit dem angegebenen Algorithmus erzeugten Hashwert eines Passworts, im Verzeichnis abzulegen. Die geschweiften Klammern sind dabei Teil der Syntax, so wird SSHA mittels "password-hash {SSHA}" festgelegt. Die Direktive gilt immer dann, wenn Passwörter über den slapd-Server eingerichtet oder geändert werden, das heißt mittels der Applikation "ldappasswd" oder über eine andere Client-Anwendung.

Werden LDIF-Dateien erzeugt und importiert, so müssen in der Datei angegebene Inhalte des Feldes "userPassword" bereits als Hashwerte vorliegen, wenn ein Hashwert genutzt werden soll. Das gleiche gilt für die Angabe des rootDN-Passworts in der Konfiguration (siehe M 4.384 *Sichere Konfiguration von OpenLDAP*). Um Hashwerte von Passwörtern zu erzeugen, ist das slap*-Werkzeug slappasswd zu benutzen. Über den Parameter "-h" wird der zu verwendende Hashing-Algorithmus angegeben, der empfohlene Wert SSHA entspricht der Voreinstellung. Hinter dem Parameter "-s" wird das Passwort im Klartext angegeben. Die Ausgabe des Werkzeugs ist dann mit einem vorangestellten {SSHA} in die LDIF- oder Konfigurationsdatei zu übernehmen. Wird das Werkzeug in der Kommandozeile verwendet, ist die in der Regel eingerichtete Eingabe-Historie vorher abzuschalten, weil das Passwort sonst im Klartext darin gespeichert wird.

**Qualität des Passworts**

Selbst wenn Passwörter verschlüsselt übertragen und als Hash-Wert abgelegt werden, besteht immer noch die Gefahr, dass Benutzer zu schwache Passwörter verwenden. Sie können beispielsweise durch Wörterbuchattacken leicht ermittelt werden. Es sollte organisatorische Vorgaben geben, damit Benutzer keine schwachen Passwörter wählen (siehe M 2.11 *Regelung des Passwortgebrauchs*). OpenLDAP unterstützt derartige Vorgaben technisch

durch das Overlay "ppolicy" (Password Policy). Das Overlay setzt Regeln wie eine minimale Länge eines Passwortes oder ein minimales und maximales Alter bis zur möglichen bzw. nötigen Änderung eines Passworts um. Außerdem kann es diverse Qualitätsprüfungen von Passwörtern vornehmen und führt pro Benutzer eine Liste früherer Passwörter, um zu verhindern, dass diese erneut verwendet werden. Über Passwortregeln hinaus sperrt das Overlay "ppolicy" das Passwort-Attribut nach mehrmals fehlgeschlagener Authentisierung für einen vorgegebenen Zeitraum für jeglichen Zugriff, um eine Brute-Force-Attacke auf das Passwort zu verhindern. Die jeweiligen Vorgaben, zum Beispiel wie lang ein Passwort sein muss oder nach wie vielen Fehleingaben eine Sperrung erfolgt, können in Richtlinien (policies) detailliert festgelegt werden. Richtlinien lassen sich benutzerspezifisch oder für das gesamte Verzeichnis sowie für Teilbäume zuordnen. Der rootDN ist wird nicht durch das Overlay "ppolicy" eingeschränkt.

**Weitere Authentisierungsmechanismen**

OpenLDAP ist in der Lage, für die Authentisierung von Benutzern auf Funktionen anderer Anwendungen zurückzugreifen. So können auch Authentisierungsmechanismen verwendet werden, deren Sicherheit über diejenige von Benutzerkennung und Passwort hinausgeht (strong bind). Notwendig ist dafür die Abstraktionsschicht Simple Authentication and Security Layer (SASL). SASL unterstützt über sogenannte Mechs verschiedene Authentisierungs- und Verschlüsselungsmechanismen und kann selbst wiederum auf externe Verfahren zurückgreifen. So können Benutzer unter anderem über SSL/TLS-Zertifikate (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*) oder durch das Kerberos-Verfahren authentisiert werden. Die Authentisierung wird von OpenLDAP an SASL delegiert. Besteht für den Informationsverbund ein hoher oder sehr hoher Schutzbedarf oder existiert bereits eine Authentisierungsinfrastruktur außerhalb von OpenLDAP, sollte die Anbindung via SASL erfolgen.

Prüffragen:

- Ist sichergestellt, dass die Authentisierung am OpenLDAP-Verzeichnisdienst ausschließlich über verschlüsselte Verbindungen erfolgt?
- Werden OpenLDAP Passwörter lediglich als Hashwerte gespeichert und wird dafür ein geeigneter Hashing-Algorithmus verwendet?

# M 4.389 Partitionierung und Replikation bei OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Aufteilung von Teilbäumen eines Verzeichnisdienstes auf verschiedene Server (Partitionierung) ist eine effektive Möglichkeit, um durch Lastverteilung eine höhere Verfügbarkeit zu erreichen. Damit die Aktualität der Verzeichniskopien sichergestellt ist, müssen Veränderungen an den Daten durch Replikation zwischen den Servern ausgetauscht werden. Welcher Replikationsmodus angemessen ist, muss in Anhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen gewählt werden.

In dieser Maßnahme ist die mögliche Umsetzung dieser Konzepte mit OpenLDAP beschreiben, für die generelle Planung von Partitionierung und Replikation siehe Maßnahme M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst*.

**Partitionierung**

Die Partitionierung von Verzeichnisdiensten unter OpenLDAP ist sehr einfach zu konfigurieren. Wird ein Teil des Verzeichnisses ausgelagert oder soll ein Server wissen, welcher andere Server gewisse Teilbäume vorhält, so ist in der globalen Konfiguration dieses Servers der entsprechende Suffix als ein Objekt der Objektklasse "referral" anzulegen. Die Referenzadresse des Servers mit dem ausgelagerten Teilbaum wird dem Attribut "ref" zugeordnet. Operationen von Clients, die diesen Teil des Verzeichnisdienstes betreffen, beantwortet der Server mit einem Verweis auf diese Adresse. Die Zuordnung wird als "Subordinate Knowledge Information" bezeichnet. Der Server "weiß", welcher Teil des Verzeichnisbaumes auf welchem Server zu finden ist. Soll sichergestellt werden, dass der Server bei Suchanfragen ausgelagerte Teilbäume selbst durchsucht, ist die jeweilige Datenbank mit der Direktive "subordinate" bzw. "olcSubordinate" mit der Datenbank des Servers zu verbinden. Dieser Vorgang wird als Gluing (leimen) bezeichnet.

Ein untergeordneter Server wird im Gegenzug nicht mit der genauen Information darüber versorgt, von welchen anderen Servern welche Teilbäume oberhalb oder gleichberechtigt mit seinem gespeichert werden. Wann immer eine Operation nicht zu einem Suffix des Servers passt, wird diese mit einem globalen "Referral" (Verweis) beantwortet, das heißt, der anfragende Client wird an einen Server verwiesen, der die Antwort liefern könnte. Bei Partitionen wird hier der übergeordnete Verzeichnisdienst eingetragen. Das Referral wird in diesem Zusammenhang auch als "Superior Knowledge Information" bezeichnet, obwohl die Direktive auch unabhängig von Partitionierungen verwendet werden kann. Die über die Adressen in den Referrals identifizierten Verzeichnisdienste müssen nicht mit OpenLDAP betrieben werden.

Durch das Overlay "chain" (Chaining) kann der Server Referrals auch selbst verfolgen. Der Client bemerkt dadurch nichts von einer Partitionierung und bekommt eine abschließende Antwort immer vom ursprünglich angefragten Server. Dies funktioniert unabhängig von den Fähigkeiten des Clients, der gegebenenfalls selbst keine Referrals verarbeiten kann.

**Replikation**

Bei OpenLDAP wird die Replikation über den "LDAP Sync Replication Engine" (syncrepl) Mechanismus umgesetzt. Der Mechanismus ist auf die BerkeleyDB abgestimmt und wird nur von den Backends "back-bdb" und "back-hdb" unterstützt. Das bedeutet, OpenLDAP kann nicht ohne Weiteres als Agent eingesetzt werden, um Verzeichnisdienste zu replizieren, für die der slapd-Server lediglich einen Proxy darstellt.

Vor der Entwicklung des "syncrepl"-Mechanismus wurde der "stand-alone LDAP update replication daemon" (slurpd) zur Replikation verwendet. Hierbei handelte es sich um ein Programm, das wie der slapd-Server als Dienst ausgeführt wurde und Kopien der Verzeichnisdienstinhalte pflegte. Dieser Dienst hat nicht zuverlässig funktioniert und wurde mit der Version 2.4 offiziell aus OpenLDAP entfernt. Hinweise auf "slurpd" in veralteten Dokumentationen sind als historisch anzusehen. Der "slurpd" darf keinesfalls verwendet werden.

**Master und Slave, Provider und Consumer**

Traditionell werden die an der Replikation beteiligten Server als Master und Slave bezeichnet. Der Master ist der eigentliche Verzeichnisdienst, über diesen Server kann schreibend auf Verzeichnisdienstinhalte zugegriffen werden. Der Slave übernimmt nur alle Informationen vom Verzeichnisdienst und gewährt auf diese Kopie lesenden Zugriff. Diese strikte Trennung gilt in OpenLDAP seit der Version 2.3 nicht mehr. Bei der Replikation in OpenLDAP übernimmt ein sogenannter Consumer-Dienst Daten von einem Provider -Dienst. Es wichtig zu verstehen, dass ein Consumer gegenüber dem Provider als Client auftritt, obwohl der Consumer seine Replik selbst als Server für andere Clients zur Verfügung stellt. Die Einstellungen zur Serversicherheit des Consumers gelten für die Verbindung zum Provider nicht. Stattdessen gilt die Client-Konfiguration, diese ist auf einem Consumer sorgfältig vorzunehmen, obwohl sie für Server eigentlich nicht benötigt wird. Es ist insbesondere zu berücksichtigen, dass der Consumer ein "bind" beim Provider vornehmen muss und etwaige Zugriffsbeschränkungen und Suchlimits des verwendeten Benutzers die Replikation behindern können.

**refreshOnly und refreshAndPersist**

Die Replikation kann in einem pull- oder einem push-Mode betrieben werden. Beim pull-Mode, der in OpenLDAP als "refreshOnly" bezeichnet wird, fragt der Consumer in festgelegten Abständen den Provider auf Änderungen ab. Dabei sendet der Consumer in Form eines "Sync Cookies" die Aktualität der von ihm gehaltenen Daten. Aufgrund dieser Information wird beim Provider eine Suche gestartet, die alle Änderungen seit dem vom Consumer gemeldeten Zeitpunkt umfasst. Der Provider "kennt" in diesem Fall den Consumer nicht, er beantwortet lediglich Suchabfragen. Damit diese Suchen korrekte Ergebnisse bringen, ist es besonders wichtig, dass die Uhren von Provider und Consumer möglichst synchron laufen (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation* und M 4.348 *Zeitsynchronisation in virtuellen IT-Systemen*). Beim "push-Mode", der in OpenLDAP als "refreshAndPersist" bezeichnet wird, bleibt die Verbindung zwischen Provider und Consumer bestehen und der Provider sendet alle Änderungen immer an den Consumer. Bei der Auswahl der geeigneten Replikationsmethode gilt als Faustregel, dass "refreshOnly" umso sinnvoller ist, je größer die zu replizierenden Datenmengen sind und "refreshAndPersist" umso eher eingesetzt werden sollte, je wichtiger eine zeitnahe Aktualisierung des Providers ist.

**Einrichtung einer Replikation**

Um die Replikation eines Verzeichnisdienstes mit OpenLDAP einzurichten, sind mehrere Schritte nötig:

- Der Consumer muss installiert (siehe M 4.383 *Sichere Installation von OpenLDAP*) und konfiguriert (siehe M 4.384 *Sichere Konfiguration von OpenLDAP*) werden. Dies kann und sollte nach Möglichkeit durchgeführt werden, indem Kopien der Provider-Konfiguration auf den Provider übertragen werden. Bei der Consumer-Konfiguration ist besonders wichtig, dass auf dem Consumer die gleichen Schemas eingerichtet werden, wie auf dem Provider.
- Auf dem Consumer muss für die zu replizierende Datenbank die Datenbank-Direktive "syncrepl" eingerichtet werden. Mit den Sub-Direktiven "searchbase", "filter", "scope" und "attrs" lässt sich bestimmen, was repliziert werden soll. So können neben dem gesamten Verzeichnisdienst zum Beispiel nur Teilbäume repliziert werden oder auch nur bestimmte Attribute von Objekten. Bei der Einrichtung ist besonders zu beachten, dass im Fall der Online-Konfiguration auch der Konfigurationssuffix "CN=config" repliziert werden kann. Weitere Sub-Direktiven bestimmen die Adresse des Providers, replikationsspezifische Einstellungen zur Sicherung der Kommunikation zwischen Consumer und Provider, die Replikationsmethode und die Wiederaufnahme der Verbindung zum Provider, wenn diese abbricht (refreshAndPersist) oder der Provider nicht erreicht werden kann (refreshOnly).
- Besonders wird außerdem auf die Sub-Direktive "schemachecking" hingewiesen. Ist "schemachecking" deaktiviert (was dem Vorgabewert entspricht), können durch die Replikation auch solche Daten eingefügt werden, die nach den Schemas eigentlich unzulässig sind. Dies kann sinnvoll sein (insbesondere bei Teilrepliken), aber die Integrität der Repliken einschränken.
- Obwohl die Einstellungen zur Replikation hauptsächlich auf dem Consumer vorzunehmen sind, muss auch der Provider für eine korrekte Replikation konfiguriert werden. Damit er Suchanfragen des Consumers in Abhängigkeit von einem Änderungszeitpunkt beantworten kann, muss sich der Provider selbst vorgenommene Änderungen merken beziehungsweise eine Übersicht aktueller Zeitstempel, sogenannter "context change sequence numbers" (contextCSNs) führen. Dies wird durch den Aufruf des Overlay "syncprov" (Sync Provider) erreicht.
- Um die Consumer-Datenbank erstmals zu befüllen, wird empfohlen, nur die benötigten Datensätze aus einer Datensicherung des Providers einzuspielen (siehe M 6.150 *Datensicherung beim Einsatz von OpenLDAP*), da eine vollständige Übertragung aller Verzeichnisdienstinhalte über das Netz unnötig Zeit und Ressourcen beansprucht. Weil syncrepl über Mechanismen zum Datenabgleich verfügt, ist es nicht notwendig, dass die verwendete Datensicherung aktuell ist. Wird eine Datensicherung eingespielt, die noch keine contextCSNs enthält, ist der Parameter "-w" anzugeben, wenn die Datenbank mit slapadd befüllt wird, damit contextCSNs erzeugt werden. Dies wird insbesondere bei einer ersten Replikation der Fall sein, da der Provider üblicherweise noch nicht auf einen solchen Betrieb vorbereitet war und das Overlay "syncprov" noch nicht aufgerufen wurde.

**Delta-Replikation**

Grundsätzlich sendet der Provider alle Attribute von Einträgen, die geändert wurden, als Suchergebnis oder im Rahmen der Replikation. Er tut dies selbst dann, wenn im Eintrag nur eines der Attribute verändert wurde. In Verbindung mit dem Overlay "accesslog" (siehe auch M 4.407 *Protokollierung beim Ein-*

*satz von OpenLDAP*) ist es auch möglich, die Veränderungen von Attributen detailliert aufzuzeichnen und dann mit dem "syncrepl"-Mechanismus lediglich die Änderungen zu übermitteln. Dies setzt eine umfangreichere Konfiguration voraus. Bei häufigen Änderungen von kleinen Attributen an relativ großen Objekten sollte diese Möglichkeit geprüft werden, bei wenigen Objekten oder geringen Anzahlen ist die Delta-Replikation nicht notwendig.

**Multi-Master- und Mirror-Mode-Betrieb**

Es ist auch möglich, einen Multi-Master-Betrieb einzurichten. Bei einem Multi-Master-Betrieb gibt es mehr als einen Server, auf den schreibend zugegriffen werden kann, und die Master sind untereinander sowohl Provider als auch Consumer. Der Sinn dieser Betriebsvariante besteht darin, dass beim Ausfall eines Servers immer noch schreibender Zugriff auf den Verzeichnisdienst besteht, ohne dass (wie bei einem Slave/nur-Consumer) erst die Konfiguration angepasst werden muss. Dieser Betrieb ist nicht unumstritten und wird von einigen Mitgliedern des OpenLDAP-Teams als nicht sinnvoll angesehen, da er die Konsistenz eines Verzeichnisses bedrohen kann. Dies geschieht, wenn auf den beiden Mastern zeitgleich konkurrierende Änderungen vorgenommen werden. Ein Multi-Master-Betrieb ist für eine OpenLDAP-Installation in einem Informationsverbund mit normalem Schutzbedarf nicht notwendig. Sollten hohe oder sehr hohe Anforderungen an die Verfügbarkeit bestehen, kann eine Multi-Master-Konfiguration geprüft werden. Als Faustregel kann gelten, je wichtiger die unterbrechungsfreie Verfügbarkeit ist, desto eher ist ein Multi-Master-Betrieb sinnvoll, je wichtiger die Integrität der Daten zu jedem Zeitpunkt ist, desto weniger sinnvoll ist der Multi-Master-Betrieb.

Als Alternative zwischen dem Single-Master- und Multi-Master-Betrieb besteht die Möglichkeit eines Mirror-Mode-Betriebs. Bei dieser Betriebsvariante bestehen ebenfalls mehrere Server, über die schreibend auf den Verzeichnisdienst zugegriffen werden kann. Allerdings legt eine externe Monitoring-Komponente immer einen aktiven Server fest, der Änderungen durchführt. Fällt ein Server aus, bestimmt die Monitoring-Komponente automatisch den anderen Server zum aktiven Server. Die Delta-Replikation wird in dieser Betriebsart noch nicht unterstützt. Nachteilig ist auch, dass beim Ausfall der Monitoring-Komponente der eigentlich redundant ausgelegte Verzeichnisdienst nicht mehr verfügbar ist.

Prüffragen:

- Werden bei OpenLDAP auf Provider und Consumer hinreichend genaue Zeitdienste betrieben?
- Wird in Abhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen über den angemessenen Replikationsmodus von OpenLDAP entschieden?
- Sind bei der Consumer-Konfiguration von OpenLDAP die gleichen Schemas eingerichtet worden, wie auf dem Provider?

# M 4.390 Sichere Aktualisierung von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

OpenCMR wird ständig von den Entwicklern von OpenLDAP weiterentwickelt. Es ist deshalb sinnvoll, im Fall von Schwachstellen der Software sogar notwendig, die bestehende OpenLDAP-Installation durch eine neuere Version zu ersetzen.

### Überwachung neuer Versionen

Die OpenLDAP-Entwickler informieren über die Mailingliste openldap-announce (http://www.openldap.org/lists/openldap-announce) über alle neuen Releases und Änderungen des Stable Release (Release Notes). Diese Mailingliste sollte von Administratoren abonniert und die Nachrichten sorgfältig gelesen. Sofern nicht über Sicherheitslücken berichtet wird oder ein neues Release eine für den Anwender wertvolle Funktion einführt, besteht kein Bedarf, neu veröffentlichte Releases zeitnah zu installieren. Wird eine neuere als die eingesetzte Version zum Stable Release erklärt, wird empfohlen, eine Aktualisierung von OpenLDAP für das nächste Wartungsfenster zu planen. Bei sicherheitsrelevanten Änderungen, wie behobenen Schwachstellen, muss OpenLDAP so schnell wie möglich aktualisiert werden.

Soll die bestehende OpenLDAP-Installation aktualisiert werden, sind alle relevanten Release Notes zu prüfen, um Änderungen zur bestehenden OpenLDAP-Installation zu identifizieren. Hierbei sind neben der unmittelbar zur geplanten Version gehörenden Nachricht alle Release Notes von Versionen relevant, die zwischen der eingesetzten und der geplanten Version veröffentlicht wurden. Insbesondere ist darauf zu achten, ob Änderungen eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten betreffen. Ist dies der Fall, so ist die Planung von OpenLDAP zu aktualisieren (siehe M 2.484 *Planung von OpenLDAP*).

### Durchführung der Aktualisierung

Im Rahmen der Vorbereitung sind die Installationspakete für die geplante OpenLDAP-Version herunterzuladen und zu überprüfen (siehe M 4.382 *Auswahl und Prüfung der OpenLDAP-Installationspakete*). Werden Binärpakete eines Distributors verwendet, stellt er gegebenenfalls auch spezielle Aktualisierungspakete bereit. Vor der Aktualisierung ist der slapd-Server anzuhalten und es ist eine aktuelle Datensicherung des bestehenden Verzeichnisses durchzuführen (siehe M 6.150 *Datensicherung beim Einsatz von OpenLDAP*). Anschließend ist die neue Version von OpenLDAP zu installieren (siehe M 4.383 *Sichere Installation von OpenLDAP*). Die Installation kann in ein neues Zielverzeichnis erfolgen, um zur bisher verwendeten Version zurückkehren zu können. Die neu installierte Software ist zu konfigurieren, dies geschieht in der Regel durch die Übernahme der vorigen Konfiguration aus der Datensicherung. Anschließend müssen die Konfiguration mittels "slaptest" und die Zugriffsrechte mittels slapacl getestet werden, bevor der slapd-Server neu gestartet wird.

Folgende Punkte sind im Rahmen der Aktualisierung von OpenLDAP besonders zu beachten:

- Oftmals setzen Administratoren eigene Skripte ein, um Aufgaben im Zusammenhang mit OpenLDAP zu automatisieren. Wird OpenLDAP aktualisiert, müssen derartige Skripte überprüft werden, ob sie mit der aktualisierten Version von OpenLDAP problemlos zusammenarbeiten.
- Insbesondere, wenn verschiedene Versionen von OpenLDAP parallel auf einem IT-System installiert sind, ist es von großer Bedeutung, dass immer die slap*-Werkzeuge der jeweiligen Version eingesetzt werden. Tests von Konfiguration und Zugriffsrechten müssen mit den "neuen" Versionen von slaptest und slapacl durchgeführt werden und die Datensicherung muss mit dem "neuen" slapadd eingespielt werden.

Prüffragen:

- Werden sicherheitsrelevante Aktualisierungen von OpenLDAP schnellstmöglich installiert?
- Werden bei OpenLDAP veränderte Anforderungen an eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten bei der Aktualisierung geprüft und beachtet?
- Werden gegebenenfalls eingesetzte eigene Skripte überprüft, ob sie mit der aktualisierten Version von OpenLDAP zusammenarbeiten?
- Werden bei OpenLDAP die Konfiguration und die Zugriffsrechte nach einer Aktualisierung mit den korrekten, das heißt den "neuen" Werkzeugen, sorgfältig geprüft?

# M 4.391 Sicherer Betrieb von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Sicherheit von OpenLDAP auch im Betrieb aufrecht zu erhalten, müssen regelmäßig eine Reihe von Schritten durchgeführt werden, um eventuelle Probleme rechtzeitig zu entdecken.

Beim Betrieb von OpenLDAP sollten insbesondere folgende Aspekte berücksichtigt werden:

- Es ist darauf zu achten, dass der slapd-Server mit der beabsichtigten Konfiguration gestartet wird. Mit dem Parameter "-f [Pfad/Dateiname]" wird eine zu verwendende slapd.conf festgelegt, mit dem Parameter "-F [Pfad]" ein zu verwendendes slapd-config-Verzeichnis. Wichtig ist, dass sich die Konfigurationen nicht ergänzen, wenn gleichzeitig beide Parameter verwendet werden, sondern dass die slap-config-Konfiguration durch die slapd.conf-Konfiguration überschrieben wird.
- Der slapd-Server sollte beim Start mit dem Parameter "-h [Protokolle]" auf die benötigten Protokolle eingeschränkt werden, beispielsweise "-h ldaps://".
- Der slapd-Server ist durch den Parameter "-r [Verzeichnis]" auf ein Laufzeitverzeichnis einzuschränken (chroot-Mechanismus). Dieses Verzeichnis muss alle Konfigurationsdateien und Datenbanken beinhalten.
- Vor einem geplanten Anhalten des slapd-Servers sollte geprüft werden, ob dieser noch Operationen durchführt oder Verbindungen zu Clients bestehen (siehe M 4.407 *Protokollierung beim Einsatz von OpenLDAP*). Dies gilt insbesondere für Operationen, die bei einem Neustart nicht fortgeführt werden wie der Indizierung). Der slapd-Server verfügt über keinen stop-Befehl, zum Anhalten ist der zugehörige Prozess zu beenden, zum Beispiel durch "kill -INT 'cat /usr/local/var/slapd.pid'".
- Änderungen an der Konfiguration müssen sorgfältig dokumentiert werden, so dass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund welche Änderungen vorgenommen hat. Für die Änderungen an den Konfigurationsdateien wird empfohlen, ein Revisionskontrollprogramm (beispielsweise git, mercurial oder RCS) einzusetzen. So kann jederzeit ein früherer Stand der Konfiguration wiederhergestellt werden und es bleibt nachvollziehbar, wer welche Änderungen aus welchem Grund durchgeführt hat.
- Nach jeder Änderung der Konfiguration muss zunächst mit dem Programm slaptest geprüft werden, ob die Syntax der Konfigurationsdatei korrekt ist. Syntaxfehler in der Konfigurationsdatei können sonst dazu führen, dass der slapd-Server nicht startet oder Sicherheitslücken entstehen.
- Nach jeder Änderung von Zugriffsberechtigungen ist mit dem Programm slapacl zu prüfen, ob die gerade durchgeführte Änderung wirksam ist.
- Die Administratoren müssen sich über aktuelle Sicherheitslücken in der eingesetzten Software frühzeitig informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Informationen über neu entdeckte Sicherheitslücken veröffentlichen die Entwickler von OpenLDAP im "Issue Tracking System" unter http://www.openldap.org/its.
- Die in M 2.64 *Kontrolle der Protokolldateien* beschriebenen Maßnahmen müssen auch für OpenLDAP umgesetzt werden. Speicherort und Umfang der Protokolle hängen von M 4.407 *Protokollierung beim Einsatz von OpenLDAP* ab.
- Zum sicheren Betrieb gehören auch regelmäßig durchzuführende Maßnahmen zur Notfallvorsorge und zur Datensicherung (siehe M 6.136 *Er-*

*stellen eines Notfallplans für den Ausfall eines Samba-Servers* und M 6.150 *Datensicherung beim Einsatz von OpenLDAP*).

Prüffragen:

- Wird der slapd-Server auf ein Laufzeitverzeichnis eingeschränkt?
- Wird nach Änderungen der Konfiguration und der Zugriffsrechte von OpenLDAP geprüft, ob die Syntax korrekt ist und die neuen Zugriffsrechte wirksam sind?
- Ist sichergestellt, dass die Administratoren zeitnah von neuen Sicherheitslücken bei OpenLDAP erfahren?

# M 4.392 Authentisierung bei Webanwendungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Soll eine Webanwendung oder Teile davon ausschließlich von einem eingeschränkten Benutzerkreis genutzt werden können, so muss sich der Benutzer gegenüber der Anwendung authentisieren. Für die Authentisierung können unterschiedliche Methoden verwendet werden, die in den Maßnahmen M 4.176 *Auswahl einer Authentisierungsmethode für Webangebote* und M 5.160 *Authentisierung gegenüber Webservern* beschrieben sind.

Bei der Umsetzung von Authentisierungsmechanismen für Webanwendungen sind folgende Punkte zu berücksichtigen.

**Anforderungen an die Authentisierungskomponente**

Die Authentisierungslogik sollte nur an einer Stelle und nicht mehrfach im Programmcode realisiert werden. Treten während der Authentisierung Fehler auf, sollte die angeforderte Aktion abgebrochen und die Anfrage zurückgewiesen werden.

Die Authentisierungskomponente sollte das Erzwingen sicherer Passwörter gemäß einer Passwort-Richtlinie unterstützen. Anforderungen an sichere Passwörter können der Maßnahme M 2.11 *Regelung des Passwortgebrauchs* entnommen werden.

Darüber hinaus wird empfohlen, die geschätzte Stärke des eingegebenen Passworts einzublenden (z. B. schwach, mittel, sicher). Dadurch wird der Benutzer dabei unterstützt, sichere Passwörter zu wählen.

Um Fehler bei der Entwicklung der Authentisierungskomponente zu vermeiden, wird empfohlen die Authentisierungskomponente auf Basis etablierter Standardkomponenten (Bibliotheken oder Frameworks) umzusetzen (z. B. Enterprise Security API der OWASP).

Besteht ein erhöhter Schutzbedarf der Webanwendung, sollte eine Zwei-Faktor-Authentisierung eingesetzt werden.

Damit ein Benutzer den Missbrauch seines Benutzerkontos erkennen kann, kann die Webanwendung das Datum und die Uhrzeit der letzten erfolglosen und erfolgreichen Anmeldeversuche nach der Anmeldung eines Benutzers als Warnhinweis anzeigen.

**Remember-Me-Funktion**

Zur Steigerung der Benutzerfreundlichkeit werden die Authentisierungsdaten von Webanwendungen teilweise dauerhaft auf dem Client der Benutzer gespeichert (z. B. innerhalb eines Cookies im Web-Browser). Diese Möglichkeit wird häufig als Remember-Me-Funktion bezeichnet. Wurden Authentisierungsdaten im Rahmen der Remember-Me-Funktion auf dem Client gespeichert, werden diese bei einer späteren Nutzung der Webanwendung automatisch übertragen. Der Benutzer muss somit keine Zugangsdaten mehr eingeben.

Erhält ein Angreifer Zugriff auf den Web-Browser oder wird Schadcode auf dem Client ausgeführt, können diese gespeicherten Authentisierungsdaten

ausgelesen werden. Aus diesem Grund sollte die Verwendung dieser Funktion vermieden werden. Kann auf die Remember-Me-Funktion nicht verzichtet werden, so sollte der Benutzer explizit einer Aktivierung zustimmen müssen (Opt-In). Darüber hinaus sollte der Benutzer auf die Risiken der Funktion hingewiesen werden.

Neben Authentisierungsdaten in Cookies können aktuelle Browser häufig Formularfelder (z. B. Benutzername/Passwort oder Adressdaten) für eine spätere Wiederverwendung speichern. Wird ein Web-Formular, für das die eingegebenen Daten zuvor gespeichert wurden, erneut aufgerufen, so werden die Daten automatisch vom Browser in die Felder eingetragen. Daher sollte die Option "autocomplete=off" für alle Formularfelder mit vertraulichen Daten gesetzt werden. Dadurch werden die Browser angewiesen, die Daten der entsprechenden Formularfelder nicht zu speichern.

**Zusätzliche Authentisierung bei kritischen Funktionen**

Hat sich ein Benutzer erfolgreich authentisiert, so wird ihm von der Webanwendung üblicherweise eine eindeutige Sitzung (mittels SessionID) zugewiesen. Die Webanwendung kann mithilfe dieser SessionID die eintreffenden Requests den angemeldeten Benutzern zuordnen. Somit kann die SessionID als eine Art temporäres Anmeldedatum betrachtet werden, mit dessen Hilfe auf die Sitzungen angemeldeter Benutzer zugegriffen werden kann (siehe auch M 4.394 *Session-Management bei Webanwendungen und Web-Services*).

Da viele Angriffe gegen die SessionID bekannt sind (siehe G 5.169 *Unzureichendes Session-Management von Webanwendungen und Web-Services*), kann eine Übernahme von gültigen Sitzungen nicht vollständig ausgeschlossen werden. Daher sollte bei sicherheitskritischen Aktionen (z. B. Änderung des Passworts oder Löschung des kompletten Datenbestandes) eine erneute Authentisierung des Benutzers (z. B. durch Eingabe des alten Passworts bei einem Passwortwechsel) erfolgen.

**Grenzwerte für gescheiterte Anmeldeversuche**

Versucht ein Benutzer sich mehrfach in kurzen Zeitabständen an der Webanwendung anzumelden, so sollten diese Authentisierungsversuche als Angriff gewertet werden. Wenn die Zahl der fehlgeschlagenen Versuche einen festgelegten Wert überschreitet (z. B. fünf Fehlversuche), sollte das Benutzerkonto für ein definiertes Zeitintervall (z. B. 10 Sekunden) gesperrt werden. Darüber hinaus können die Zeitintervalle zur Sperrung des Benutzerkontos mit der Anzahl der Fehlversuche progressiv ansteigen. Hierdurch soll verhindert werden, dass Benutzer unbefugt Kennwörter anderer Benutzer erraten.

Bei der Wahl des Grenzwerts und der Zeitintervalle sollte beachtet werden, dass dieser Mechanismus für Denial-of-Service-Angriffe missbraucht werden kann. Ein Angreifer kann bewusst das Sperren vieler Benutzerkonten provozieren und somit diese Benutzer von der Nutzung der Webanwendung ausschließen.

**Automatisiertes Zurücksetzen von Authentisierungsdaten**

Da Webanwendungen oftmals von einem großen Benutzerkreis genutzt werden, bieten sie häufig Funktionen zum automatisierten Zurücksetzen der Authentisierungsinformationen (Passwort-Reset) an. So soll der administrative Aufwand möglichst gering gehalten werden, wenn z. B. ein Benutzer sein Passwort vergessen hat. Können die Authentisierungsdaten unbefugt zurückgesetzt werden, kann auf diese Weise der Authentisierungsmechanismus umgangen werden. Deshalb ist darauf zu achten, dass alle Funktionen einer We-

banwendung zur Änderung der Authentisierungsdaten mindestens genauso abgesichert sind wie die primäre Authentisierung der Webanwendung.

Wird beispielsweise im Prozess zum Zurücksetzen des Passworts die Authentisierung des Benutzers über eine geheime Frage mit entsprechender Antwort sichergestellt, so sollten die Merkmale vom Benutzer formuliert werden können. Er sollte darauf hingewiesen werden, dass sie keine Daten beinhalten sollten, die öffentlich verfügbar oder leicht zu erraten sind. Zur Erhöhung des Schutzniveaus können mehrere Fragen und Antworten bei der Registrierung aufgenommen werden (z. B. fünf, von denen mindestens drei Fragen für eine erfolgreiche Authentisierung richtig beantwortet werden müssen).

Zusätzlich kann noch ein weiteres Sicherheitsmerkmal verwendet werden, indem nach der korrekten Beantwortung der Fragen ein Link an eine zuvor vom Benutzer spezifizierte E-Mail-Adresse versendet wird oder ein weiteres Sicherheitstoken (z. B. eine PIN) per SMS an eine hinterlegte Rufnummer gesendet wird. Erst nach Klicken auf den Link bzw. Eingabe der PIN kann sich der Benutzer dann anmelden.

Da das Authentisierungsverfahren beim Zurücksetzen von Anmeldeinformationen in der Regel nur schwer auf das gleiche Sicherheitsniveau der primären Authentisierung zu bringen ist, sollte nach Möglichkeit auf ein automatisiertes Zurücksetzen durch die Webanwendung verzichtet werden. Bei eingeschränkten Nutzerkreisen der Webanwendung (z. B. bei einer Webanwendung im Intranet) kann stattdessen das Passwort manuell beispielsweise über eine Hotline mit sicheren Authentisierungsmerkmalen und entsprechendem Freigabeverfahren zurückgesetzt werden. Insbesondere bei einem hohen Schutzbedarf sollte eine manuelle Zurücksetzungsfunktion umgesetzt werden.

Prüffragen:

- Verwendet die Webanwendung eine zentrale Authentisierungskomponente?
- Erzwingt die Webanwendung die Verwendung sicherer Passwörter?
- Setzen die Webanwendungen eine explizite Zustimmung des Benutzers bei der Verwendung der Remember-Me-Funktion voraus (Opt-In)?
- Werden kritische Funktionen der Webanwendung durch eine zusätzliche Authentisierung geschützt?
- Definiert die Webanwendung Grenzwerte für fehlgeschlagene Anmeldeversuche, die Brute-Force-Angriffe erschweren?
- Erfüllen alle angebotenen Authentisierungsverfahren der Webanwendung (beispielsweise auch Funktionen zum automatisierten Zurücksetzen des Passworts) das gleiche Sicherheitsniveau?
- Wird der Benutzer einer Webanwendung umgehend über die Nutzung der angebotenen Passwort-Zurücksetzungsfunktion informiert?

# M 4.393 Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Alle an eine Webanwendung oder einen Web-Service übergebenen Daten, unabhängig von Kodierung oder Form der Übermittlung, müssen als potenziell gefährlich behandelt und entsprechend gefiltert werden. Durch eine zuverlässige und gründliche Filterung der Ein- und Ausgabedaten mittels einer Validierungskomponente kann ein wirksamer Schutz vor gängigen Angriffen erreicht werden. Hierbei sollten sowohl die Eingabedaten von Benutzern an die Webanwendung als auch die Ausgabedaten der Webanwendung an die Clients oder an nachgelagerte Systeme wie zum Beispiel Datenbanken gefiltert und transformiert (output encoding) werden. Entsprechendes gilt für die Aufrufparameter und Rückgabewerte von Web-Services. Dadurch wird sichergestellt, dass nur erwartete und keine schadhaften Daten verarbeitet oder ausgegeben werden.

Ist es für einzelne Funktionen notwendig, den Datenfilter weniger restriktiv zu setzen, muss dies explizit beim Zugriff auf die Daten definiert und dokumentiert werden. Zusätzlich ist es möglich, kontextsensitive Filter in der Geschäftslogik der Anwendung oder in den Hintergrundsystemen zu nutzen.

Für eine sichere Verarbeitung der Daten sollten folgende Punkte bei der Umsetzung und der Konfiguration der Validierungskomponente berücksichtigt werden:

**Identifizierung der Daten**

Damit die Ein- und Ausgabedaten umfassend validiert werden können, müssen zunächst alle zu verarbeitenden Datenstrukturen (zum Beispiel E-Mail-Adresse) und die darin zulässigen Werte identifiziert werden. Für jede Datenstruktur sollte eine entsprechende Validierungsroutine umgesetzt werden. Neben der Datenstruktur sollte auch die Art und Weise der Datenverarbeitung erfasst werden (zum Beispiel Weiterleitung an einen Interpreter, Rückgabe an den Client, Speicherung in einer Datenbank).

**Berücksichtigung aller Daten und Datenformate**

Die Validierungskomponente sollte alle zu verarbeitenden Datenformate und verwendeten Interpreter berücksichtigen. Typische Datenformate bei Webanwendungen sind zum Beispiel personenbezogene Daten (Name, Telefonnummer, Postleitzahl), Bilder, PDF-Dateien und formatierte Texte. Typische Interpreter für Daten, die von Webanwendungen und Web-Services verarbeitet oder ausgegeben werden, sind zum Beispiel HTML-Renderer, SQL-, XML-, JSON-, LDAP-Interpreter und das Betriebssystem.

Daten können durch unterschiedliche Techniken auf ihre Gültigkeit geprüft werden. So kann die Validierungskomponente den Wertebereich der Eingaben überprüfen oder es können beispielsweise reguläre Ausdrücke verwendet werden, um erlaubte Zeichen und die Länge der erwarteten Daten zu validieren. Die Gültigkeit von XML-Daten kann unter anderem mithilfe des entsprechenden XML-Schemas überprüft werden. Darüber hinaus stellen Fra-

meworks und Bibliotheken für gängige Datenformate entsprechende Validierungsfunktionen bereit.

Die folgenden Zeichen werden gewöhnlich von in Webanwendungen oder Web-Services eingesetzten Programmen interpretiert und können daher für das Einschleusen von schadhaftem Code genutzt werden. Aus diesem Grund sollten sie bei der Filterung berücksichtigt werden:

Nullwert, Zeilenvorschub, Wagenrücklauf, Hochkommata, Kommas, Schrägstriche, Leerzeichen, Tabulator-Zeichen, größer als und kleiner als, XML- und HTML-Tags.

Diese Aufzählung erhebt keinen Anspruch auf Vollständigkeit. Zudem können die Interpreter-Zeichensätze (zum Beispiel SQL-Syntax) bei unterschiedlichen Produkten variieren. Beispiele für kritische Zeichen werden im Abschnitt Potenziell gefährliche Zeichen für Interpreter in Hilfsmittel zum Baustein Webanwendungen aufgeführt.

Neben den eigentlichen Nutzdaten (zum Beispiel Formular-Parameter in GET- oder POST-Variablen) sind auch Daten anderer Herkunft (Sekundärdaten) zu validieren. Dazu zählen beispielsweise:

- Namen von Form-Variablen (Sie können ebenso wie der Wert der Form-Variablen beliebig manipuliert werden),
- HTTP-Header-Felder (Header-Felder in HTTP-Requests und -Responses sollten ausschließlich ASCII-Zeichen enthalten und zum Beispiel keine Zeilenvorschubzeichen wie \r\n),
- Session-IDs (zum Beispiel aus Cookies).

Automatisierte Aufrufe durch den Client zum Beispiel durch Ajax- beziehungsweise Flash-Skripte oder JSON-Requests sind ebenfalls zu prüfen.

Bei den Hintergrundsystemen ist eine (gegebenenfalls erneute) Validierung der Daten vorzunehmen. Dies gilt auch dann, wenn Daten beispielsweise nach einem erfolgten Schreibvorgang in die Datenbank wieder ausgelesen werden, da die Daten auch in der Datenbank zwischenzeitlich geändert worden sein können.

Schadhafter Code kann aber auch über einen Weg übermittelt werden, der nicht von der Webanwendung oder dem Web-Service kontrolliert werden kann (zum Beispiel FTP, NFS). Kann ein Angreifer über diese Dienste Dateien ändern oder erzeugen, die von der Webanwendung oder dem Web-Service integriert werden, so kann Schadcode über diesen Umweg eingebettet werden. Bei dem sogenannten Cross-Channel-Scripting wird auf diese Weise JavaScript-Code eingefügt, der ähnlich wie bei persistentem Cross-Site-Scripting vom Browser ausgeführt wird. Daher sollten unabhängig von der Quelle immer alle Daten vor der Ausgabe an die Benutzer oder der Weiterverarbeitung durch die Anwendung validiert werden.

**Serverseitige Validierung**

Üblicherweise greifen die Benutzer mit generischen Clients (zum Beispiel Web-Browser) auf die Webanwendung zu. Diese Clients befinden sich nicht im Sicherheitskontext der Webanwendung, sondern stehen unter der Kontrolle der Benutzer. In gleicher Weise kann sich auch ein Web-Service nicht darauf verlassen, dass die aufrufende Anwendung die Daten überprüft hat. Die Datenvalidierung ist daher als serverseitiger Sicherheitsmechanismus auf einem vertrauenswürdigen IT-System umzusetzen.

Werden Daten zusätzlich durch Code von der Webanwendung clientseitig verarbeitet (zum Beispiel JavaScript-Code), so sollten diese Daten auch auf dem Client validiert werden. Die ausgelieferten Skripte der Webanwendung sollten hierbei die entsprechenden Validierungsroutinen mitliefern. Werden die Daten im nachgelagerten Verarbeitungsprozess an den Server gesendet, so ist zu beachten, dass die clientseitige Prüfung die serverseitige Validierung nicht ersetzen kann.

**Validierungsansatz**

Bei der Datenvalidierung wird zwischen dem White-List- und dem Black-List-Ansatz unterschieden.

Bei dem White-List-Ansatz werden ausschließlich solche Daten zugelassen, die in der Liste enthalten sind. Dabei werden, ausgehend von einer möglichst kleinen Zeichenmenge, Regeln erstellt, die Daten in einem festgelegten Zeichenraum zulassen und Daten zurückweisen, die abweichende Zeichen enthalten. Hierbei sollten komplexe Regeln durch die sequenzielle Verwendung einfacher Regeln abgebildet werden.

Dagegen werden bei einem Black-List-Ansatz solche Daten als unzulässig eingestuft und abgewiesen, die in der Liste enthalten sind. Alle Daten, die nicht explizit verboten sind, werden bei diesem Ansatz akzeptiert.

Bei dem Black-List-Ansatz besteht jedoch die Gefahr, dass nicht alle Variationen unzulässiger Daten berücksichtigt und somit erkannt werden. Daher sollte der White-List-Ansatz dem Black-List-Ansatz vorgezogen werden.

**Kanonisierung vor der Validierung**

Daten können in verschiedenen Kodierungen (zum Beispiel UTF-8, ISO 8859-1) und Notationen (zum Beispiel bei UTF-8 ist "." = "2E" = "C0 AE") vorliegen. Abhängig vom angewendeten Kodierungsschema kann der gleiche Wert demnach unterschiedlich interpretiert werden. Findet eine Validierung der Daten ohne Berücksichtigung der Kodierung und der Notation statt, so werden gegebenenfalls schadhafte Daten nicht erkannt und gefiltert. Daher sollten alle Daten vor der Validierung in eine einheitliche, normalisierte Form überführt werden. Dieser Vorgang wird als Kanonisierung der Daten bezeichnet. Die so dargestellten Daten werden dann weiterverarbeitet. Bei der Verwendung von AJAX sollte zudem für das Nachladen die Eigenschaft textContent anstatt von innerHTML genutzt werden, da textContent automatisch eine Enkodierung vornimmt.

Darüber hinaus sollte das Kodierungsschema bei der Auslieferung von Daten durch die Webanwendung explizit gesetzt werden (zum Beispiel über den Content-Type-Header: charset=ISO-8859-1). Auch bei Web-Services sollten die verwendeten Kodierungen den Client-Systemen mitgeteilt werden, beispielsweise in den entsprechenden XML-Tags.

**Kontextsensitive Maskierung der Daten**

Falls potenziell schadhafte Daten von einer Webanwendung oder einem Web-Service verarbeitet werden müssen (zum Beispiel Zeichen mit einer Bedeutung für verwendete Interpreter) und somit eine Filterung nicht durchgeführt werden kann, müssen diese Daten maskiert und so in eine andere Darstellungsform überführt werden. In dieser maskierten Form werden die Daten nicht mehr als ausführbarer Code interpretiert. Da die Maskierung Interpreter-spezifisch ist, müssen alle verwendeten Interpreter berücksichtigt werden (zum

Beispiel SQL, LDAP). Die Maskierung muss demnach kontextsensitiv für das erwartete Ein- und Ausgabeformat und die Interpretersprache durchgeführt werden. Aufgrund der Komplexität und der spezifischen Anforderungen unterschiedlicher Interpretersprachen wird empfohlen, für die Maskierung spezialisierte Bibliotheken einzusetzen.

Es sollte eine Maskierung aller Zeichen vorgenommen werden, die als unsicher für den beabsichtigten Interpreter eingestuft werden. Dazu zählen zum Beispiel:

- unerwartetes JavaScript und HTML zur Auslieferung an den Client (zum Beispiel den Web-Browser),
- unerlaubt eingefügte SQL-Statements an die Datenbank (zum Beispiel aus Eingaben in Formularfeldern),
- Befehle an das Betriebssystem (zum Beispiel in manipulierten HTTP-Variablen).

Eine Maskierung kann durch eine Überführung der betroffenen Daten beziehungsweise Metazeichen der jeweiligen Interpretersprache in sogenannte Zeichenreferenzen erfolgen. Das folgende Beispiel zeigt ausgewählte HTML-Zeichen mit den entsprechenden Zeichenreferenzen (engl. HTML-Entities):

- & => &
- < => <
- > => >
- " => "
- ' => '

Hier ist darauf zu achten, dass &-Zeichen im ersten Durchlauf ersetzt werden und dass keine Mehrfach-Maskierung erfolgt, da dieses Zeichen in anderen Zeichenreferenzen als Metazeichen wiederverwendet wird.

**Verwendung eines eigenen Markups zur Filterung von HTML-Tags**

Falls die Webanwendung HTML-Formatierungstags in Benutzereingaben erfordert (zum Beispiel zur Formatierung von Benutzer-Beiträgen), sollten erlaubte HTML-Tags von problematischen Tags unterschieden und gefiltert werden (siehe auch Abschnitt Kontextsensitive Maskierung der Daten).

Bei diesem Ansatz besteht das hohe Risiko, problematische Tags (beispielsweise <script>) zu übersehen. Auch scheinbar harmlose Tags lassen sich teilweise über Attribute wie "onMouseOver" zur Ausführung von Code missbrauchen. Daher sollte der alternative Ansatz, für das Markup des Benutzers eigene Markup-Tags zu definieren (zum Beispiel BBCode), vorgezogen werden. Diese Markup-Tags werden dann von der Anwendung in die zugehörigen HTML-Tags übersetzt. Herkömmliche Tags beziehungsweise problematische Zeichen werden nach wie vor gefiltert.

Ein mögliches Verfahren, wenn ein einfaches Markup zugelassen werden soll, ist die Verwendung von { und } statt < und >. Fett würde dann als {F}**Dies ist fett**{/F} geschrieben und ein Bild könnte auf diese Weise platziert werden: {img src=/images/img.gif width=1 height=1 img}.

Hierbei darf die Umwandlung in HTML nicht einfach geschweifte Klammern durch spitze Klammern ersetzen, sondern muss jedes Tag als Ganzes ansehen:

- {img nach <img,
- img} nach >,
- src=Datei nach src="Datei" (wobei Datei zusätzlich zu filtern ist).

Wenn HTML-Tags zugelassen sind, ist grundsätzlich darauf zu achten, dass mindestens die folgenden Tags nicht erlaubt sind:

- applet
- base
- iframe
- link
- object
- script
- style

Mithilfe dieser Tags können beliebige Inhalte in die Webseite eingefügt werden. Diese dürfen daher nicht genutzt werden können.

**Abwehr von Code-Injection in SOAP-Nachrichten**

Allgemein sollten nie Eingaben ohne vorherige Prüfung weitergegeben werden. Um Injection-Angriffe zu vermeiden, ist es notwendig, Eingabeparameter aus der Schnittstellenbeschreibung (WSDL-Datei) heraus auf schädlichen Code zu filtern und zum Beispiel über eine Whitelist nur systemkonforme Strings zuzulassen. Empfohlen wird außerdem, Strings als Eingabetyp möglichst komplett zu vermeiden und zudem Integer-Werte auf deren Länge zu überprüfen.

**Behandlung von Fehleingaben (Sanitizing)**

Anstatt Daten aufgrund eines unerwarteten Datenformats oder Zeichens abzulehnen, können Fehleingaben korrigiert und automatisch transformiert werden (engl. sanitize). Dadurch soll eine benutzerfreundliche Eingabe der Daten in unterschiedlichen Schreibweisen ermöglicht werden. Für eine Weiterverarbeitung lassen sich die Daten von unerwarteten Zeichen säubern (zum Beispiel die Telefonnummer (0049)-201-12345678 kann in das nur aus Zahlen bestehende Format 004920112345678 überführt werden).

Eine Säuberung kann darin bestehen, Zeichen zu löschen, zu ersetzen oder zu maskieren (siehe auch Abschnitt Kontextsensitive Maskierung der Daten).

Beim Sanitizing besteht die Gefahr, dass Änderungen an den Daten zu einer neuen Komplexität, neuen Angriffsvektoren oder einer Missinterpretation führen. Daher sollte Sanitizing nach Möglichkeit vermieden und nur in Fällen angewendet werden, in denen ein Missbrauch des Sanitizing ausgeschlossen werden kann.

Falls die Webanwendung oder der Web-Service fehlerhafte Daten erkannt hat, sollten Fehler, die auf eine bewusste Manipulation hindeuten (zum Beispiel eine veränderte Session-ID) nicht automatisch korrigiert, sondern abgelehnt werden. Darüber hinaus sollten Eingabedaten, die mit bestimmungsgemäßer Browser- beziehungsweise Client-Bedienung nicht eintreten können, grundsätzlich abgelehnt werden. Dazu zählen zum Beispiel:

- Zusätzliche oder fehlende Formular-Parameter,
- Session-Cookies mit unerwarteten Zeichen oder ungültiger Länge,
- Unerwartete Werte bei der Übertragung von Formular-Parametern aus vordefinierten HIDDEN-, SELECT- oder CHECKBOX-Feldern,
- Abweichender oder unerwünschter Übertragungsweg der Parameter (zum Beispiel GET, POST, Cookie).

Bei einer Säuberung der Daten sollte die geschachtelte Eingabe von Angriffsvektoren berücksichtigt werden. Problematisch ist zum Beispiel der auf den ersten Blick vernünftig erscheinende Filter s/<script>//g; (hier in Perl RegEx-Syn-

tax geschrieben), um <script>-Tags im Eingabestrom zu löschen. Dieser kann jedoch mit einer geschachtelten Eingabe (zum Beispiel <sc<script>ript>) umgangen werden. Es ist daher rekursiv zu filtern. Im Zweifelsfall sind die Eingabedaten abzulehnen.

Grundsätzlich sollte bei einer Ablehnung der Daten die angeforderte Aktion ebenfalls abgebrochen und eine neutrale Fehlermeldung ausgegeben werden (siehe auch M 4.400 *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*). Bei Webanwendungen oder Web-Services mit hohem Schutzbedarf sollte zusätzlich die Sitzung invalidiert (abgebrochen) werden.

Prüffragen:

- Werden alle Daten (Ein- und Ausgabedaten) und Datenströme der Webanwendung oder des Web-Service (zum Beispiel zwischen Benutzer, Webanwendung, Clientsystemen und Hintergrundsystemen) bei der Validierung berücksichtigt?
- Werden auch Sekundärdaten (wie beispielsweise Session-IDs) bei der Validierung berücksichtigt?
- Führt die Webanwendung oder der Web-Service eine serverseitige Validierung der Daten auf einem vertrauenswürdigen IT-System durch?
- Führt die Webanwendung oder der Web-Service vor der Validierung eine Kanonisierung der Daten durch?
- Findet in der Webanwendung oder dem Web-Service eine kontextsensitive Validierung der Daten unter Berücksichtigung des erwarteten Interpreters der Daten statt?
- Bei Webanwendungen/Web-Services mit automatischer Behandlung von Fehleingaben (engl. Sanitizing): Wird die Behandlung von Fehleingaben sicher umgesetzt?
- Wird die Art der Eingabedaten geprüft?
- Sind bestimmte Eingabetypen ausgeschlossen?

# M 4.394 Session-Management bei Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Webanwendungen und Web-Services verwenden in der Regel das zustandslose Protokoll HTTP zur Übertragung der Daten. Es unterstützt keine Zuordnung zusammengehörender Anfragen zu einem Benutzer wie zum Beispiel einzelne Seitenaufrufe zur Füllung eines virtuellen Warenkorbs. Um zusammengehörende Anfragen eines Benutzers zu erkennen und einer Sitzung zuzuordnen, wird eine Session-ID (zum Beispiel nach erfolgreicher Anmeldung) vergeben, die anschließend bei jedem Seitenaufruf, oder bei jeder Interaktion mit dem Web-Service, übertragen wird. Die Session-ID wird typischerweise von der Webanwendung oder dem Web-Service selbst erzeugt. Verwendet ein Web-Service den Standard WS-SecureConversation, kann der Security Context, und damit auch der Identifikator für die Sitzung, auch von einem dedizierten Security Token Service erzeugt werden.

Wenn sich der Benutzer bei der Webanwendung oder dem Web-Service angemeldet hat, ist die Session-ID vergleichbar mit seinen Zugangsdaten. Die Webanwendung identifiziert mit ihr bei jedem Seiten- oder Dienstaufruf den Benutzer und ordnet ihn einer (gegebenenfalls privilegierten) Sitzung zu. Nutzen Unbefugte die Session-ID, werden sie als legitime Benutzer identifiziert und können die Anwendung oder den Dienst im Namen des Opfers verwenden.

Das Session-Management einer Webanwendung oder eines Web-Service hat zur Aufgabe, die Sitzungen zu verwalten und neue Session-IDs zu vergeben. Dabei sollten die folgenden Anforderungen und Aspekte berücksichtigt werden.

**Anforderungen an die Session-ID**

Es ist zu beachten, dass die Gültigkeitsdauer einer Session-ID (siehe auch Abschnitt *Beschränkte Sitzungsdauer*) deutlich kleiner sein sollte als die Zeit, die ein Angreifer zum Erraten einer Session-ID benötigt. Dies kann mit einer Formel für eine Webanwendung oder einen Web-Service individuell bewertet werden (siehe *Formel zur Berechnung der Bewertungsgrundlage für Session-IDs in Hilfsmittel zum Baustein Webanwendung*).

Die Session-ID sollte mindestens folgende Anforderungen erfüllen:

- Die Session-ID muss mithilfe kryptografischer Zufallszahlengeneratoren zufällig erzeugt werden und sollte eine Entropie von mindestens 64 Bit haben, damit sie von einem potentiellen Angreifer nicht erraten werden kann. Um die Entropie der Session-ID zu erhöhen, kann beispielsweise die Länge erhöht (zum Beispiel 128 Bit) und der Zeichenraum der Session-ID (zum Beispiel alphanumerische Zeichen und Sonderzeichen) vergrößert werden. Als Richtwert sollte hierbei die Länge der Session-ID mindestens die doppelte Anzahl an Bits haben wie die Anzahl an Entropie-Bits der Session-ID. Demzufolge sollte die Session-ID mindestens 128 Bit lang sein. Unter der Annahme, dass ein Zeichen durch 8 Bit dargestellt wird, bestünde eine solche Session-ID aus mindestens 16 Zeichen (128 Bit / 8 = 16 Byte).

- Es sollten keine extern bekannten oder erratbaren Daten (zum Beispiel RFC-Adresse, Uhrzeit) in die Berechnung der Session-ID einfließen, sofern dies die Entropie nicht tolerierbar verringert.
- Unterstützt das der Webanwendung zugrunde liegende Framework die Generierung von Session-IDs, sollte vorzugsweise die Funktion des Frameworks verwendet werden. Die Funktionalität von führenden Frameworks ist in der Regel getestet und unterstützt die sichere Erzeugung von Session-IDs. Eine fehleranfällige Neuentwicklung sollte daher vermieden werden.
- Wird ein Framework zur Verwaltung und Erzeugung der Session-IDs verwendet, so ist auf eine sichere Konfiguration des Frameworks zu achten, sodass die zuvor genanten Anforderungen an die Session-ID erfüllt sind.

**Schutz vor unbefugtem Zugriff auf die Session-ID**

Die Session-ID kann sowohl in der URL eines Requests (GET-Methode), im Rumpf des Requests (POST-Methode) oder als Cookie im Header des Requests übertragen werden. Wird bei Web-Services der Standard WS-SecureConversation eingesetzt, so ist die Session-ID Teil des XML-Elements wsc:SecurityContextToken, welches innerhalb der SOAP-Header übertragen wird.

Wenn Daten mithilfe der GET-Methode übermittelt werden, können sie von beteiligten IT-Systemen gespeichert und dadurch von Dritten eingesehen werden (zum Beispiel im Browser-Verlauf, auf Bildschirmfotos, Seitenkopien oder Ausdrucken). Daher sollte die Session-ID nicht über die GET-Methode (also in der URL) übertragen werden. Für Webanwendungen oder Web-Services mit hohem Schutzbedarf ist dies nicht erlaubt. Stattdessen sollte die Session-ID vorzugsweise in Cookies übertragen werden.

Erfordert die Anwendung die GET-Methode (zum Beispiel aus Gründen der Kompatibilität mit Clients, die keine Cookies verarbeiten können), sind folgende Punkte zu beachten:

- Benutzer sollten auf die genannten Gefahren hingewiesen werden und beim Verlassen des Rechners die Sitzung beenden oder den Rechner sperren.
- Die Benutzer sollten angewiesen werden, keine gespeicherten Seiten oder Bildschirmfotos von Seiten der Webanwendung zu versenden, bei der die Session-ID in der URL sichtbar ist.
- Bei Nutzung der Webanwendung über einen öffentlichen Rechner sollte eine Meldung darauf hinweisen, dass der Browser-Verlauf nach Beenden der Sitzung gelöscht werden sollte.
- Durch sehr lange Session-IDs kann das Abschreiben und das zufällige Mitlesen erschwert werden.
- Bei der Verlinkung auf externe Seiten darf die Session-ID nicht übertragen werden. Dies gilt sowohl für die Übertragung in der URL als auch für das Referrer-Feld. Daher sollte bei Verlinkungen auf externe Seiten eine erzwungene Weiterleitung erfolgen, welche das Referrer-Feld bereinigt.

Zum Schutz vor unbefugtem Mitlesen der Session-ID sollte nach einer erfolgreichen Anmeldung die Kommunikation über eine sichere Verbindung stattfinden. Dies kann über eine Transportsicherung, beispielsweise mittels SSL/TLS(siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*) oder mittels WS-SecureConversation realisiert werden. Die Session-ID kann über eine ungesicherte Verbindung übertragen werden, wenn mit der bestehenden Sitzung keine zugriffsgeschützten Bereiche der Webanwendung verwendet werden können. Gewöhnlich ist der Benutzer in diesem Fall noch nicht authentisiert.

Der Zugriff auf die Session-ID als Authentisierungsmerkmal sollte streng reglementiert werden. Wird die Session-ID in einem Cookie übertragen, sollte der clientseitige Zugriff auf diesen Cookie nach Möglichkeit durch das Setzen folgender Flags eingeschränkt werden (für eine detaillierte Beschreibung der Cookie-Flags siehe M 4.401 *Schutz vertraulicher Daten bei Webanwendungen*):

- Path (zum Beispiel /webapp/),
- Secure und
- HttpOnly.

**Beschränkte Sitzungsdauer**

Eine Webanwendung oder ein Web-Service muss Benutzern die Möglichkeit geben, eine bestehende Sitzung nach ihrer Nutzung explizit zu beenden. Daher muss auf allen Webseiten, für deren Abruf eine Authentisierung des Benutzers notwendig ist, eine deutlich sichtbare Abmeldemöglichkeit bestehen. Bei der Verwendung von WS-SecureConversation sollte der Security Context einer Sitzung nach der Nutzung des Dienstes explizit durch das Senden einer Nachricht "WS-Trust Cancel" invalidiert werden. Nach erfolgter Abmeldung sollte die Sitzung vollständig beendet werden und die Session-ID ihre Gültigkeit verlieren. Darüber hinaus sollte der Benutzer bei der Verwendung von Webanwendungen und Web-Services für folgende Verhaltensweisen sensibilisiert werden:

- Ist der Benutzer angemeldet, sollte er sich nach Abschluss der Tätigkeiten von der Webanwendung ordnungsgemäß abmelden.
- Falls beim letzten Besuch keine Abmeldung erfolgt ist, sollte der Benutzer bei dem nächsten Anmeldevorgang an der Webanwendung darauf hingewiesen werden, sich zukünftig abzumelden.

Ungenutzte, bestehende Sitzungen bieten eine Angriffsfläche für Brute-Force-Angriffe auf die Session-ID. Daher sollten Sitzungen nach einem Zeitintervall der Inaktivität ihre Gültigkeit verlieren (Idletime). Darüber hinaus sollte eine maximale Gültigkeits-Lebensdauer vergeben werden (Timeout), sodass auch die Session-IDs von aktiven Sitzungen eine begrenzte Gültigkeit haben. Diese sollte für die Sitzungen so gering wie möglich gewählt werden, sodass Brute-Force-Angriffe erschwert werden, wobei die Benutzbarkeit der Webanwendung hierbei nicht unnötig eingeschränkt werden sollte. Die Formel aus dem Abschnitt *Anforderungen an die Session-ID* kann für die Ermittlung einer angemessenen Gültigkeitsdauer herangezogen werden.

Treten bei der Nutzung der Webanwendung oder des Web-Service schwerwiegende Fehler auf, sollten angeforderte Aktionen abgebrochen und zusätzlich die Sitzung beendet werden. Schwerwiegende Fehler sind zum Beispiel auftretende Ausnahmefehler (Exceptions) und erkannte Angriffsversuche. Bei einem hohen Schutzbedarf sollten noch engere Kriterien in Erwägung gezogen werden, die zur Invalidierung der Sitzung führen (zum Beispiel ungültige Eingaben, Aufruf fehlender Seiten).

Bei der Invalidierung sollten die Sitzungsdaten server- und clientseitig vollständig gelöscht werden, sodass die Sitzung serverseitig nicht weiter akzeptiert wird und clientseitig keine Informationen über zuvor aufgebaute Sitzungen verbleiben. Dies kann zum Beispiel durch Löschen des Cookies mit der Session-ID erfolgen.

Darüber hinaus können mehrere parallele Sitzungen unter dem gleichen Benutzerkonto verhindert werden. Eine bestehende Sitzung kann bei erneuter Anmeldung invalidiert werden, sodass nur die neue Sitzung gültig bleibt. Al-

ternativ ist es beispielsweise möglich, die erste Sitzung über einen begrenzten Zeitraum (zum Beispiel 15 Minuten) aufrechtzuerhalten, bevor sie invalidiert wird. Dabei sollte dem Benutzer bei der Anmeldung über eine parallele, zweite Sitzung eine Meldung über die ablaufende, erste Sitzung eingeblendet werden. Auf diese Weise können noch bestehende, aber nicht mehr verwendete Sitzungen nach erneuter Anmeldung nicht oder nur eingeschränkt unbefugt von Dritten genutzt werden.

Zum Schutz vor Session-Fixation-Angriffen sollte nach erfolgter Anmeldung eine bereits bestehende Session-ID durch eine neue ersetzt werden.

Ebenso sollte nach einem Wechsel von einem ungesicherten Kommunikationskanal (HTTP) auf einen gesicherten Kommunikationskanal (HTTPS) eine neue Session-ID vergeben werden, da die Session-ID bei der Übertragung über einen ungesicherten Kanal mitgelesen worden sein könnte.

**Schutz der Sitzungsdaten**

Zum Schutz der Vertraulichkeit sollten die anfallenden Sitzungsdaten (zum Beispiel Warenkorb) ausschließlich serverseitig auf einem vertrauenswürdigen IT-System gespeichert werden. Darüber hinaus sollten die Daten vor unbefugtem Zugriff von anderen Benutzern durch eine Zugriffskontrolle geschützt werden. Falls die Webanwendung oder der Web-Service eine clientseitige Speicherung der Sitzungsdaten erfordert, sollte ebenfalls M 4.401 *Schutz vertraulicher Daten bei Webanwendungen* für die Speicherung von Daten auf dem Client beachtet werden.

**Zuordnung einer Sitzung anhand zusätzlicher Attribute**

Neben der Session-ID können weitere Merkmale zur Zuordnung zwischen Benutzer und Sitzung verwendet werden (zum Beispiel die IP-Adresse). Hierdurch kann die unbefugte Nutzung bestehender Sitzungen erschwert werden, da ein Angreifer für eine erfolgreiche Übernahme der Sitzung neben einer gültigen Session-ID die zusätzlichen Merkmale kennen muss. Die Verwendung von zusätzlichen Attributen zur Zuordnung einer Sitzung ist zumindest bei Webanwendungen mit hohem Schutzbedarf zu berücksichtigen.

Wird die IP-Adresse als zusätzliches Merkmal für die Sitzungszuordnung verwendet, so ist diese serverseitig zu speichern und zu prüfen. Wechselt die IP-Adresse im Laufe einer Sitzung, so sollte dies bei Anwendungen mit hohem Schutzbedarf als Angriffsversuch gewertet und demzufolge die Sitzung invalidiert werden. Dabei ist jedoch zu berücksichtigen, dass die IP-Adresse nicht immer einem Benutzer eindeutig zugeordnet werden kann. Erfolgt die Verbindung einiger Benutzer der Webanwendung über einen Proxy mit gleicher (zum Beispiel Reverse-Proxy) oder wechselnder IP-Adresse (zum Beispiel wechselnde, ausgehende Proxys), besteht die Gefahr, dass die IP-Adressen dieser Benutzer nicht eindeutig einer Sitzung zugeordnet werden können. Es sollte somit bedacht werden, dass einige Benutzer die Webanwendung möglicherweise nur eingeschränkt oder gar nicht nutzen können.

Wenn der Referrer als Identitätsmerkmal verwendet wird, kann auf einen festen Teil des Referrer-Pfades geprüft werden, der für alle Zugriffe identisch bleibt (zum Beispiel die Domäne der Webanwendung). Die Benutzer müssen demnach eine Webseite der Webanwendung im Referrer vorweisen. Hierbei ist zu berücksichtigen, dass einige Browser eine Deaktivierung oder benutzerseitige Manipulation der Referrer-Übermittlung erlauben und Content-Filter dieses Feld gegebenenfalls filtern.

Die Identitätsmerkmale können zum Schutz vor unbefugter Nutzung der Sitzung auf mehrere Eigenschaften des HTTP-Headers verteilt werden. Denkbar sind zum Beispiel HTTP-Header-Informationen wie

- die Browsertypenbezeichnung (User-Agent-Header),
- unterstützte Formate und Sprachen des Clients (Accept- und Accept-Language-Header) und
- der Referrer (Referrer-Header).

Aufgrund der teilweise geringen Variationsbreite der genannten Merkmale des HTTP-Headers ist der zusätzlich erreichte Schutz begrenzt. Dagegen erhöht sich der Umsetzungsaufwand und unter Umständen die Komplexität bei der Fehlersuche. Aus diesem Grund sollte im Einzelfall abgewogen werden, ob der zusätzlich erreichte Schutz den Umsetzungsaufwand rechtfertigt.

**Eigenimplementierungen vermeiden**

Kann für die Sitzungsverwaltung einer Web-Anwendung oder eines Web-Service auf eine erprobte Implementierung in einem Framework oder einen verbreiteten Standard (wie WS-SecureConversation) zurückgegriffen werden, so ist dies gegenüber einer Eigenimplementierung in jedem Fall zu bevorzugen, da sich Eigenimplementierungen dieser sicherheitskritischen, komplexen Funktion sehr häufig als angreifbar erweisen.

Prüffragen:

- Hat die Session-ID der Webanwendung beziehungsweise des Web-Service eine ausreichende Entropie, um dem Erraten der Session-ID (zum Beispiel durch einen Brute-Force-Angriff) standzuhalten?
- Wird die Vertraulichkeit der Session-ID bei der Übertragung und clientseitigen Speicherung ausreichend geschützt?
- Hat die Sitzung eine begrenzte Gültigkeit (Timeout) und ist diese gemessen an den Anforderungen zur Nutzung der Webanwendung oder des Web-Service möglichst kurz gewählt worden?
- Erfolgt ein Wechsel der Session-ID nach erfolgreicher Authentisierung?
- Werden alle Sitzungsdaten (sowohl server- als auch clientseitig) nach der Invalidierung der Sitzung ungültig und gelöscht?
- Kommt für die Sitzungsverwaltung eine erprobte Implementierung oder ein verbreiteter Standard zum Einsatz?

# M 4.395 Fehlerbehandlung durch Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Tritt während des Betriebs einer Webanwendung oder eines Web-Services ein Fehler auf, sollte dieser so behandelt werden, dass ein konsistenter Zustand der Webanwendung gewährleistet ist und somit etwa der Schutz der Daten aufrechterhalten wird.

Eine Webanwendung oder ein Web-Service ist in einem inkonsistenten Zustand, wenn sie aufgrund eines Fehlers in einen unerwarteten Zustand überführt wird und dadurch Daten unkontrolliert verarbeitet werden (zum Beispiel keine Fehlermeldung bei erfolgloser Speicherung von Daten).

Der konsistente Zustand einer Webanwendung oder eines Web-Service kann unter anderem durch folgende Ereignisse gefährdet werden:

- Absturz der Anwendung
- unvollständig durchgeführte Transaktionen auf Anwendungsebene
- Durchführung einer Aktion trotz Fehler (zum Beispiel bei unvollständigen Prüfungen durch Sicherheitskomponenten)
- Verhinderung von Diensten (Denial-of-Service)
- Rechteausweitung (privilege escalation)
- Ausführen von Schadcode (code execution)

Folgende Punkte sollten bei der Fehlerbehandlung berücksichtigt werden:

### Vermeidung vertraulicher Informationen in Fehlermeldungen

Die Webanwendung muss dem Benutzer im Falle eines Fehlers neutrale, angepasste Fehlerseiten ausgeben, die keine vertraulichen Informationen beinhalten. Auch die Rückmeldungen von Web-Services sollten im Fehlerfall keine vertraulichen Informationen, wie etwa interne Pfade oder die Versionsnummern von verwendeten Softwarekomponenten, enthalten. Siehe hierzu auch M 4.400 *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*.

### Protokollierung der Fehler

Für eine vollständige Nachvollziehbarkeit aufgetretener Fehler müssen diese als Ereignis gemäß M 4.397 *Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services* protokolliert werden.

### Abbruch des Vorgangs nach Auftreten eines Fehlers

Treten Fehler im Zusammenhang mit Sicherheitskomponenten der Webanwendung oder des Web-Service auf (zum Beispiel während der Autorisierung oder Authentisierung), muss die veranlasste Aktion abgebrochen und der Zugriff auf die angeforderte Ressource oder Funktion abgewiesen werden. Es muss gewährleistet sein, dass durch provozierte Fehler keine Sicherheitsmechanismen umgangen werden können.

Für Webanwendungen oder Web-Services mit einem hohen Schutzbedarf sollte zusätzlich die Invalidierung einer gegebenenfalls bestehenden Sitzung

in Betracht gezogen werden (siehe auch M 4.394 *Session-Management bei Webanwendungen und Web-Services*).

**Freigabe von reservierten Ressourcen**

Im laufenden Betrieb belegen Webanwendungen und Web-Services Ressourcen wie zum Beispiel Netz- oder Datei-Streams, um auf Hintergrundsysteme, zwischengespeicherte Zustände oder sonstige Daten zuzugreifen. Solange die Webanwendung oder der Web-Service auf diese Ressourcen zugreift, sind diese in der Regel für deren exklusiven Zugriff reserviert und können von anderen Prozessen nicht verwendet werden.

Tritt ein Fehler auf, sollten zuvor reservierte Ressourcen (zum Beispiel ein Datei-Handle auf eine temporäre Datei) im Rahmen der Fehlerbehandlung freigegeben werden. Darüber hinaus sind zwischengespeicherte Daten bei der Fehlerbehandlung zu löschen.

**Unmittelbare Behandlung von Fehlern**

Interne Fehler sollten von der Webanwendung oder dem Web-Service selbst behandelt werden. Die Weiterleitung eines unbehandelten Fehlers an andere Komponenten (zum Beispiel Applikationsserver oder nachgelagerte Web-Services) kann zu einem Verlust von Informationen führen, die zur Behandlung des Fehlers notwendig sind (zum Beispiel zur Freigabe von gebundenen Ressourcen). Daher sollten unbehandelte Fehler nicht weitergeleitet werden.

**Vermeidung einer zu hohen Fehlertoleranz**

Sind Ursachen von Fehlerzuständen nicht vollständig geklärt, sollte der Fehler nicht zum Beispiel aufgrund der Bedienungsfreundlichkeit toleriert, sondern die Aktion im Zweifelsfall abgebrochen werden. Schwerwiegende Fehler sollten immer zum Abbruch der Aktion führen.

Das Ziel sind robuste und fehlertolerante Webanwendungen und Web-Services, die bestimmungsgemäße Bedienung durch den Anwender von offensichtlichen Missbrauchsversuchen und schwerwiegenden Fehlern unterscheiden und dann angemessen reagieren können.

Prüffragen:

- Werden von der Webanwendung oder dem Web-Service ausschließlich Fehlermeldungen ausgegeben, die keine vertraulichen Informationen beinhalten?
- Ist eine Protokollierung von Fehlern vorgesehen?
- Wird eine veranlasste Aktion im Fehlerfall abgebrochen und in der Folge der Zugriff auf die angeforderte Ressource oder Funktion abgewiesen?
- Sieht die Fehlerbehandlung eine Freigabe gebundener Ressourcen vor?
- Werden Fehler möglichst von der gleichen Komponente behandelt, in der der Fehler aufgetreten ist?

# M 4.396 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Eine Webanwendung wird gewöhnlich von Menschen genutzt und erfordert somit keine automatisierte Nutzung (z. B. durch Skripte). Brute-Force-Angriffe (z. B. Erraten von Zugangsdaten) und Enumeration-Angriffe (z. B. automatisiertes Ermitteln von gültigen Login-Namen) beruhen hingegen auf der automatisierten Steuerung einer Webanwendung (Automation). Bei diesen Angriffen wird zumeist versucht, vertrauliche Daten durch wiederholende, leicht variierende Abfragen (z. B. geänderte Benutzernamen) zu sammeln.

Zur Verhinderung von Automation und der Abwehr damit einhergehender Angriffe muss die Webanwendung automatisierte von manuellen Zugriffen unterscheiden können. Automatisierte Angriffe zeichnen sich durch eine hohe Zahl an Zugriffsversuchen innerhalb einer kurzen Zeitspanne aus, die das übliche Maß deutlich übersteigt.

Daher kann eine Toleranzschwelle für wiederholt abgerufene Ressourcen derartige Angriffe erschweren (Teergrube). Werden Grenzwerte gegen automatisierte Anfragen festgelegt, ist darauf zu achten, dass legitime Benutzer in der Funktionalität und der Bedienung der Webanwendung möglichst wenig eingeschränkt werden. Falls Grenzwerte für elementare Funktionen der Webanwendung zu eng bemessen sind, können Angreifer dies auf Webanwendungs-Ebene für Denial-of-Service-Angriffe missbrauchen. Werden beispielsweise Benutzerkonten nach einer festgelegten Anzahl an erfolglosen Anmeldeversuchen für ein gewisses Zeitintervall gesperrt, können gezielte Falscheingaben zu einer längerfristigen Sperrung vieler Benutzerkonten führen. Demzufolge können sich legitime Benutzer in diesem Zeitraum nicht mehr an der Webanwendung anmelden.

Darüber hinaus ist die Effizienz automatisierter Angriffe in der Regel stark abhängig vom Detailgrad der Informationen in den Rückantworten der Webanwendung (siehe M 4.400 *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*).

Folgende Beispiele geben Hinweise auf mögliche Schutzmechanismen:

- Eine künstliche Verzögerung zwischen der Eingabe der Zugangsdaten bei der Benutzer-Authentisierung und der Meldung über einen fehlgeschlagenen Anmeldeversuch kann Brute-Force-Angriffe aufgrund des erhöhten Zeitbedarfs erschweren. Die Wirksamkeit dieser Methode kann durch ein progressives Ansteigen der Verzögerung nach jedem gescheiterten Versuch erhöht werden.
- Werden Eingaben zurückgewiesen, sollten Informationen über die Ursache generisch verfasst sein. Einem Angreifer darf es beispielsweise nicht möglich sein aufgrund von Meldungen, wie "Passwort ungültig" anstelle von "Zugangsdaten ungültig", auf ein gültiges Benutzerkonto zu schließen (siehe auch M 4.395 *Fehlerbehandlung durch Webanwendungen und Web-Services*).
- Angriffsversuche sind häufig gekennzeichnet durch vielfache Fehlversuche bei der Durchführung einer Aktion. Daher sollte eine vorhandene Sitzung beendet werden, wenn eine ungewöhnlich hohe Anzahl von Fehlver-

suchen identifiziert wird, und anschließend eine Neuanmeldung erforderlich sein.
- Automatisierte Angriffe können durch eine temporäre Sperrung der IP-Adresse bei Verdacht auf einen Angriff abgewehrt werden. Es sollte hierbei bedacht werden, dass durch diese Maßnahme gegebenenfalls Unbeteiligte ebenfalls von der Sperrung betroffen sind (z. B. wenn mehrere Benutzer denselben Proxy verwenden).
- Häufig werden sogenannte CAPTCHAs (Completely Automated Public Turing Test To Tell Computers and Humans Apart) zur Unterscheidung automatisierter und manueller Zugriffe eingesetzt. Hierbei müssen vom Benutzer der Webanwendung Aufgaben gelöst werden (z. B. die Zeichen in einem Bild müssen erkannt und abgetippt oder Rätselfragen beantwortet werden), was für ein Computerprogramm nicht ohne Weiteres möglich ist. Abhängig von der verwendeten Technik und Aufgabenstellung ist die Webanwendung dadurch gegebenenfalls nur eingeschränkt für Menschen mit Behinderung nutzbar. So sollte z. B. alternativ zum Einblenden der Aufgabe, diese auch akustisch zur Verfügung gestellt werden, um Menschen mit Sehbehinderung die Nutzung der Webanwendung zu ermöglichen. Es ist zu beachten, dass der Einsatz von CAPTCHAs aus Gründen der Diskriminierung in vielen Ländern gesetzlich geregelt oder verboten ist. In Deutschland ist die Bundesverwaltung verpflichtet ihre öffentlich zugänglichen Internet- und Intranet-Angebote nach der Barrierefreien Informationstechnik-Verordnung (BITV) zu gestalten.

Prüffragen:

- Erkennt die Webanwendung automatisierte Zugriffe und werden geeignete Maßnahmen getroffen, die eine automatisierte Nutzung erschweren oder unterbinden?
- Werden bei der Festlegung von Grenzwerten bei Webanwendungen mögliche Auswirkungen berücksichtigt (z. B. Anfälligkeit für Denial-of-Service-Angriffe)?
- Wird eine restriktive Informationspolitik von der Webanwendung umgesetzt?
- Werden die rechtlichen Rahmenbedingungen vor dem Einsatz von Schutzmaßnahmen geprüft, die die Nutzung der Webanwendung auf bestimmte Anwenderkreise einschränken und somit diskriminieren könnten (z. B. CAPTCHA)?

# M 4.397 Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Sicherheitsrelevante Ereignisse (zum Beispiel Zugriffe auf Ressourcen, Authentisierungsversuche) müssen nachvollziehbar protokolliert werden, damit im Stör- oder Fehlerfall oder nach Angriffsversuchen die Protokolldaten zur Ursachenfindung herangezogen werden können.

Neben den Empfehlungen in den Maßnahmen M 5.9 *Protokollierung am Server* und M 2.110 *Datenschutzaspekte bei der Protokollierung* sollten zusätzlich die folgenden Punkte bei der Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services beachtet werden.

### Zu protokollierende Ereignisse bei Web-Anwendungen und Web-Services

Zusätzlich zur Protokollierung auf den Server- und Hintergrundsystemen (zum Beispiel Betriebssystem, Web- und Applikationsserver, Datenbank) sollte auch die Anwendung sicherheitsrelevante Ereignisse protokollieren. Mindestens folgende Ereignisse sollten auf Anwendungsebene erfasst werden:

- erfolgreiche und erfolglose Anmeldeversuche an der Webanwendung oder dem Web-Service,
- fehlgeschlagene Autorisierungsversuche beim Zugriff auf Ressourcen (zum Beispiel Datenbankzugriffe) und Funktionen der Webanwendung oder des Web-Service,
- fehlgeschlagene Validierung von Ein- und Ausgabedaten,
- fehlgeschlagene XML-Schema-Validierungen,
- XML-Parser-Fehler,
- aufgetretene Fehler (zum Beispiel Exceptions),
- Änderungen von Berechtigungen für Benutzer oder Benutzergruppen der Webanwendung oder des Web-Service (zum Beispiel Zugriffsrechte, Änderung an der Web-Service-Policy),
- Änderungen an Benutzerkonten (zum Beispiel Passwortänderung),
- Löschvorgänge der Webanwendung (zum Beispiel Beiträge),
- erkannte Manipulationsversuche und unerwartete Änderungen (zum Beispiel Anmeldeversuche mit ungültigen oder abgelaufenen Session-IDs),
- administrative Funktionsaufrufe und Änderungen an der Konfiguration (zum Beispiel Abruf von Benutzerdaten, Aktivierung und Deaktivierung der Protokollierung),
- Starten und Stoppen von Diensten,
- Produktionsübernahme (Deployment) neuer oder bestehender Web-Services.

### Zu protokollierende Merkmale von Ereignissen

Um sicherheitsrelevante Vorgänge anhand von Protokolldaten nachvollziehen zu können, müssen grundlegende Merkmale der Ereignisse verfügbar sein. Daher sollten mindestens die folgenden Merkmale protokolliert werden:

- Datum,
- Uhrzeit mit Zeitzone,

- assoziierter Benutzername,
- betroffenes Objekt (zum Beispiel Benutzerkonto, Datei, Datenquelle),
- Status der Aktion (zum Beispiel fehlgeschlagen, erfolgreich),
- Ort des Auftretens (zum Beispiel Komponente),
- Aktion (zum Beispiel Authentisierung, Autorisierung),
- Schweregrad (zum Beispiel Information, Warnung, Fehler).

Darüber hinaus kann es auch hilfreich sein, folgende Merkmale zu protokollieren:

- Source-IP-Adresse,
- Referenzen auf die SessionID (nicht die SessionID selbst),
- IT-System, an dem der Fehler aufgetreten ist,
- Softwarestand (Version) der Webanwendung.

Vertrauliche und sicherheitsrelevante Daten (zum Beispiel SessionID, Zugangsdaten) sollten nicht protokolliert werden.

**Geeignete Datenformate und Mechanismen**

Die protokollierten Daten sollten in einem einheitlichen Format gespeichert werden, damit eine effiziente Auswertung möglich ist. Die Protokollierungskomponente der Webanwendung oder des Web-Service sollte aus diesem Grund ein Datenformat verwenden, das in bestehende Lösungen integriert werden kann. Wird beispielsweise eine zentrale Komponente für die Auswertung der Protokolldaten verwendet, so sollten Datenformate gewählt werden, die diese Komponente unterstützt.

**Serverseitige Protokollierung durch eine zentrale Komponente**

Die Protokollierung der Webanwendung oder des Web-Service ist ausschließlich serverseitig durchzuführen, da nur auf diese Weise die Protokolldaten zentral ausgewertet werden können. Die Protokolldaten sollten von einer einzigen, zentralen Protokollierungskomponente der Webanwendung oder des Web-Service und nicht von unterschiedlichen Protokollierungskomponenten erhoben werden.

Eine fehleranfällige Neuentwicklung der Protokollierungskomponente sollte vermieden werden. Stattdessen sollte auf die Funktionalität etablierter Frameworks zurückgegriffen werden, die in der Regel einen zentralisierten Protokollierungsansatz und die Protokollierung in verbreiteten Protokolldatenformaten unterstützen (siehe Abschnitt *Geeignete Datenformate und Mechanismen*).

**Schutz vor unbefugtem Zugriff und der Manipulation von Protokolldaten**

Da die Protokolldaten vertrauliche Informationen (zum Beispiel über das Benutzerverhalten und den Aufbau beziehungsweise die Konfiguration der Webanwendung oder des Web-Service) enthalten können, muss der Zugriff auf die Protokolldaten reglementiert und nur befugten Benutzern ermöglicht werden. Der Zugriff auf Protokolldaten sollte nicht über öffentliche Schnittstellen möglich sein. Protokolldaten sollten daher in dedizierten Logverzeichnissen (zum Beispiel außerhalb des Web-Root-Verzeichnisses des Web-Servers) gespeichert werden.

Werden die Protokolldaten in einer Datenbank abgelegt, so sollten die Protokolldaten von den eigentlichen Nutzdaten getrennt werden. Diese Trennung kann mittels einer separaten Datenbanktabelle erreicht werden. Darüber hinaus kann ein eigener Datenbankbenutzer für die Protokollierung den Schutz

der Protokolldaten erhöhen. In diesem Fall darf der Datenbankbenutzer für die Nutzdaten keine Zugriffsrechte auf die Protokolldaten haben.

Alternativ können die Protokollierungsdaten mit hohem Schutzbedarf auch in einer separaten Datenbankinstanz gespeichert werden.

**Sichere Protokollauswertung**

Ein Angreifer kann bewusst Protokoll-Einträge provozieren (zum Beispiel wenn Eingabefelder protokolliert werden), die schadhaften Programmcode beinhalten. Daher sollte bei der Auswertung der Protokolldaten sichergestellt werden, dass Schadcode in Protokoll-Einträgen vom Auswertungsprogramm nicht interpretiert wird (zum Beispiel durch die Ansicht in einem Browser und der Interpretation von JavaScript-Code in den Protokolldaten).

Da bei der Protokollauswertung keine Änderungen an den Protokolldaten vorgenommen werden dürfen, sind die Protokolldaten ausschließlich in einem schreibgeschützten Modus zu analysieren.

**Zeitsynchronisation**

Die Protokolldaten verschiedener Komponenten einer Webanwendung oder eines Web-Service (zum Beispiel Applikationsserver, Webserver, Datenbankserver) müssen in der Regel korreliert werden, um komponentenübergreifende Vorgänge vollständig nachvollziehen zu können. Dazu sollte die Zeit auf den Systemen synchronisiert sein, um anhand der Uhrzeiten Vorgänge in den Protokollen konsistent nachverfolgen zu können. Hierzu sollte M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation* beachtet werden.

Prüffragen:

- Werden sicherheitsrelevante Ereignisse mit den erforderlichen Merkmalen von der Webanwendung oder dem Web-Service protokolliert?
- Werden keine vertraulichen Daten (zum Beispiel Zugangsdaten) protokolliert?
- Wird die Protokollierung ausschließlich serverseitig von einer zentralen Komponente der Webanwendung oder des Web-Service durchgeführt?
- Ist der Zugriff auf die Protokolldaten nur befugten Benutzern ermöglicht?
- Wird der Zugriff auf die Protokolldaten über die öffentliche Schnittstelle unterbunden?
- Verwendet die Webanwendung oder der Web-Service Datenformate und Mechanismen zur Protokollierung, die eine Integration in bestehende Lösungen ermöglicht?
- Wird eine Zeitsynchronisation für die Komponenten der Webanwendung oder des Web-Service umgesetzt?
- Wird das Ausführen von Schadcode bei der Protokollauswertung verhindert?

# M 4.398 Sichere Konfiguration von Webanwendungen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Ist eine Webanwendung unzureichend konfiguriert, so kann ein Angreifer möglicherweise bestehende Sicherheitsmechanismen überwinden. Daher muss sichergestellt werden, dass die Webanwendung so konfiguriert wird, dass Zugriffe ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade möglich sind. Der Zugriff auf nicht benötigte Ressourcen und Funktionen ist daher einzuschränken.

Folgende Punkte sollten bei der Konfiguration der Webanwendung berücksichtigt werden:

**Deaktivierung nicht benötigter HTTP-Methoden**

Auf eine Webanwendung kann gemäß HTTP-Standard mit unterschiedlichen HTTP-Methoden (z. B. GET, POST, PUT, DELETE oder TRACE) zugegriffen werden. Üblicherweise benötigt eine Webanwendung jedoch nur eine sehr eingeschränkte Menge dieser HTTP-Methoden (z. B. GET und POST).

Darüber hinaus kann eine Webanwendung in Abhängigkeit der verwendeten HTTP-Methode unterschiedlich auf einen Request reagieren. Wird beispielsweise die Eingabedatenfilterung nur bei einem GET- oder POST-Request durchgeführt, so kann diese Sicherheitsfunktion durch den Aufruf einer nicht vorgesehenen HTTP-Methode gegebenenfalls umgangen werden.

Einige HTTP-Methoden (z. B. PUT) bieten Zugriff auf sicherheitskritische Funktionalität (z. B. Hochladen beliebiger Dateien) und ermöglichen auf diese Weise Restriktionen der Webanwendung zu umgehen (z. B. die Dateitypenprüfung bei einer Upload-Funktion).

Aus diesen Gründen sollten nicht benötigte HTTP-Methoden deaktiviert und von der Webanwendung nicht bearbeitet werden. Dies gilt auch für fiktive HTTP-Methoden, die nicht im entsprechenden Standard RFC 2616 definiert werden. Auch wenn die HTTP-Methoden bereits in der Konfiguration des Webservers deaktiviert wurden, sollte auch die Webanwendung nicht benötigte HTTP-Requests nicht bearbeiten.

**Erzwingen der HTTP-POST-Methode**

Bei der Bedienung einer Webanwendung werden üblicherweise Daten (z. B. Formulardaten oder die SessionID) an die Webanwendung übermittelt. Diese Daten können als Parameter in der URL (GET-Methode) und im Rumpf des HTTP-Requests (POST-Methode) übertragen werden.

Bei der Verwendung der GET-Methode sind vertrauliche Daten wie Formulardaten in der URL sichtbar (z. B. im Browser-Verlauf) und können von zwischengelagerten Systemen protokolliert und gespeichert werden.

Daher sollten schützenswerte Daten ausschließlich über die POST-Methode übertragen werden. Hierbei ist zu berücksichtigen, dass Frameworks häufig die HTTP-Request-Methode abstrahieren. Eine falsche Konfiguration des Frameworks kann dazu führen, dass trotz erzwungener Eingrenzung auf die POST-Methode durch die Webanwendung weiterhin beide Methoden zuläs-

sig sind (z. B. über eine Weiterleitung eines HTTP-GET-Requests auf einen HTTP-POST-Request durch das Framework).

**Sicherer Umgang mit SSL/TLS**

Zum Schutz der übertragenen Daten zwischen Webanwendung und Client des Benutzers kann der Transportkanal durch kryptographische Verfahren (z. B. SSL/TLS) geschützt werden. Vertrauliche Daten sollten immer über einen verschlüsselten Transportkanal übertragen werden (siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS*).

Darüber hinaus ist darauf zu achten, dass bei Fehlern während des SSL/TLS-Verbindungsaufbaus oder bei der Übertragung von Daten über einen verschlüsselten Kanal nicht zu einer unverschlüsselten Verbindung gewechselt wird. Stattdessen sollte der Verbindungsaufbau erneut erfolgen oder abgelehnt werden. Es muss verhindert werden, dass vertrauliche Daten über eine ungesicherte Verbindung übertragen werden (z. B. durch setzen des Secure-Flags für Cookies; siehe M 4.401 *Schutz vertraulicher Daten bei Webanwendungen*).

**Zeichenkodierungskonfiguration**

Die übermittelten Daten zwischen dem Client des Benutzers und der Webanwendung können in verschiedenen Kodierungen vorliegen. Abhängig von der erwarteten Kodierung werden die Daten von Clients, von der Webanwendung oder von den Hintergrundsystemen unterschiedlich interpretiert. Damit Clients Daten an die Webanwendung in der gewünschten Kodierung senden, sollte die Webanwendung bei der Auslieferung von Webseiten in den Header-Feldern der HTTP-Response das Zeichenkodierungsschema (z. B. UTF-8) mit angeben.

Falls die Webanwendung international verwendet wird, sollte darauf geachtet werden, dass alle internationalen Zeichensätze auf allen logischen Ebenen der Webanwendung und von den angebundenen Hintergrundsystemen unterstützt werden.

**Speicherung von Konfigurationsdateien außerhalb von Web-Root**

Konfigurationsdateien der Webanwendung enthalten häufig schützenswerte Informationen wie z. B. Zugangsdaten. Daher dürfen Benutzer der Webanwendung keine Zugriffsmöglichkeiten auf die Konfigurationsdateien haben.

Aus diesem Grund sollten Konfigurationsdateien ausschließlich außerhalb des Webserver-Root-Verzeichnisses gespeichert werden. Außerhalb dieses Verzeichnisses werden in der Regel keine Daten von der Webanwendung ausgeliefert.

Grundsätzlich müssen Konfigurationsdaten außerhalb des Quelltextes in separaten Konfigurationsdateien gespeichert werden. Konfigurationseinstellungen, die vertrauliche Daten beinhalten, sollten zudem verschlüsselt werden.

**Festlegung von Grenzwerten**

Einige Schutzmechanismen sehen den Einsatz von Grenzwerten vor (siehe z. B. M 4.396 *Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen*. Wird ein Grenzwert überschritten, erfolgt häufig die zeitweise Sperrung einer betroffenen Funktion oder Ressource. So können wiederholt fehlgeschlagene Anmeldeversuche die Sperrung des Benutzer-Kontos zur Folge haben (z. B. zur Abwehr von Brute-Force-Angriffen).

Auf diese Weise eingeleitete Maßnahmen können die Bedienung der Webanwendung beeinflussen und somit ebenfalls unbeteiligte Benutzer betreffen. Diese Benutzer können sich beispielsweise nicht mehr an der Webanwendung anmelden, falls ihr Benutzer-Konto gesperrt wurde.

Diese Auswirkungen sollten daher auch bei der Festlegung von Grenzwerten berücksichtigt werden.

**Restriktive Dateisystemberechtigungen**

Webanwendungen bieten Benutzern häufig direkt oder indirekt Zugriff auf das darunterliegende Dateisystem (z. B. über abrufbare Dateien oder eine Upload-Funktion). Damit ein Angreifer nicht unbefugt schützenswerte Dateien lesen oder manipulieren kann, sollten diese zusätzlich zu Zugriffsbeschränkungen auf Webanwendungsebene durch restriktive Dateisystemberechtigungen geschützt werden. Der Server, auf dem die Webanwendung läuft, muss mit eingeschränkten Rechten gestartet werden und nicht als Administrator (root).

**Administration einer Webanwendung**

Die Webanwendung sollte vorrangig über ein von der Anwendung entkoppeltes System administriert werden. Im Fall einer E-Commerce-Anwendung kann beispielsweise die Artikelpflege über ein getrenntes System mit Zugriff auf die Datenbank der Webanwendung erfolgen. Das System sollte idealerweise alleine für diesen Zweck bestimmt sein und keine direkte Verbindung zu der Webanwendung haben. Dementsprechend sollte die Webanwendung die Artikeldaten ausschließlich von der Datenbank abrufen.

Häufig bieten Webanwendungen zur Administration eine Web-Oberfläche auf demselben Server an. Diese Funktion sollte gemieden und stattdessen die Administration über ein separates System durchgeführt werden. Falls die Administration auf demselben Server erforderlich ist, sollte die Administrationsoberfläche ausschließlich aus dem Administrationsnetz heraus erreichbar und der Zugriff durch gewöhnliche Benutzer der Webanwendung nicht möglich sein. Möglichkeiten zur Administration der Webanwendung, die nicht genutzt werden (z. B. Konsole), sollten nicht nutzbar sein.

Prüffragen:

- Werden bei der Webanwendung ausschließlich die HTTP-Methoden zugelassen, die erforderlich sind?
- Wird zur Übertragung vertraulicher Daten (z. B. Formulardaten) vorzugsweise die HTTP-POST-Methode verwendet?
- Werden vertrauliche Daten ausschließlich über einen verschlüsselten Transportkanal übertragen?
- Wird verhindert, dass im Fall von Verbindungsfehlern bei einem verschlüsselten Kanal nicht auf eine unverschlüsselte Verbindung gewechselt wird?
- Werden Konfigurationsdateien der Webanwendung außerhalb des Web-Root-Verzeichnisses gespeichert?
- Wird für die Administration der Webanwendung ein separates System verwendet oder ist die Administrationsoberfläche der Webanwendung nur aus dem Administrationsnetzwerk heraus erreichbar?

# M 4.399 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Eine Webanwendung erstellt zur Laufzeit Webseiten, deren Inhalte sich aus unterschiedlichen Quellen zusammensetzen können. Diese Inhalte werden z. B. in Form von Dateien dynamisch bei der Erstellung der Webseite eingebunden oder von der Webanwendung generiert. Da dem Benutzer die fertige Webseite ausgeliefert wird, ist für ihn häufig nicht ersichtlich, aus welcher Quelle die angezeigten Inhalte stammen. Daher muss die Webanwendung sicherstellen, dass ausschließlich vorgesehene Daten und Inhalte eingebunden und an den Benutzer ausgeliefert werden.

Die Inhalte können mittels unterschiedlicher Techniken eingebunden werden. Daher werden in den folgenden Abschnitten Hinweise zur sicheren Verwendung üblicher Techniken zusammengefasst.

**Einbinden von Dateien (File Inclusion)**

Häufig werden bei der Generierung von Webseiten durch die Webanwendung Teile der ausgelieferten Internet-Seite aus unterschiedlichen Dateien dynamisch eingebunden (z. B. eine Navigationsleiste). Hierdurch verringert sich der Wartungsaufwand bei Änderungen an der Webseite (z. B. ein neuer Navigations-Eintrag). Dabei sollten der Inhalt und der Pfad der einzubindenden Dateien ausschließlich vom Administrator oder von privilegierten Benutzern der Webanwendung geändert werden können. Gewöhnlichen Benutzern sollte es dagegen nicht möglich sein, die Dateien zur Einbindung frei zu wählen oder zu modifizieren (z. B. über veränderte Parameter). Aus diesem Grund sollte die Verarbeitung von Benutzer-Eingaben zur Einbindung von Dateien grundsätzlich vermieden werden.

Erfordert die Webanwendung Benutzer-Eingaben als Quelle zur Einbindung von Dateien, sollten die vorgesehenen Pfadangaben zu den Quell-Dateien nicht frei wählbar sein. Benutzer sollten nicht in der Lage sein, den gesamten Pfad vorzugeben, sondern stattdessen sollten Benutzer-Eingaben in vordefinierte Pfadangaben gekapselt werden.

Angriffe, wie Path Traversal, versuchen durch relative Bezüge den Pfad auf schützenswerte Dateien umzusetzen (z. B. */../../../etc/passwd*) und so aus den vorgegebenen Pfadangaben auszubrechen. Zur Verhinderung derartiger Angriffe sollten daher die Benutzereingaben auf unerwünschte Zeichen zur Manipulation des Pfades (z. B. "/.." und "\..") gefiltert werden (siehe auch M 4.393 *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*).

Bei der Auswahl der Quell-Dateien können Indizes anstelle von Dateinamen verwendet werden, denen serverseitig hinterlegte Dateinamen zugeordnet werden. Somit hat ein Angreifer keinen direkten Einfluss auf den Dateinamen und kann durch Manipulation des Index keine beliebigen Inhalte direkt einbinden.

Webanwendungen können, neben Dateien auf dem Serversystem, auch entfernt gespeicherte Ressourcen über die Netzwerkverbindung mittels URL ein-

binden (Remote File Inclusion). Nach Möglichkeit sollte das Einbinden entfernter Inhalte komplett unterbunden werden. Kann auf die Einbindung externer Inhalte nicht verzichtet werden, so muss die vertrauenswürdige Herkunft dieser Dateien unbedingt sichergestellt werden (z. B. auf Basis einer Whitelist mit der Limitierung auf einen Server oder eine Auflistung von absoluten URLs).

**Verwendung von Datei-Uploads**

Bei vielen Webanwendungen kann der Benutzer Inhalte mittels einer Upload-Funktion übermitteln. Ein typischer Anwendungsfall ist der Upload eines Profilfotos. Die hochgeladenen Daten sind auf die benötigten Dateiformate zu beschränken (z. B. sollten für das Profilfoto ausschließlich Bilddateien zugelassen werden). Hierbei sollte neben der Prüfung der Dateiendung ebenfalls der Inhalt der Datei, z. B. durch eine Auswertung des Dateiheaders, geprüft werden.

Hochgeladene Dateien sollten nach Möglichkeit in einem Verzeichnis gespeichert werden, welches nicht über die Web-Schnittstelle erreichbar ist (z. B. außerhalb des Wurzelverzeichnisses des Webservers). So wird verhindert, dass ein Benutzer auf seine hochgeladenen Dateien direkt zugreifen kann (z. B. auf schadhafte Skripte). Werden die hochgeladenen Dateien zunächst in einem temporären Verzeichnis gespeichert, so ist sicherzustellen, dass andere Benutzer nicht unerlaubt auf die Datei zugreifen dürfen.

Stellt eine Webanwendung dem Benutzer eine Upload-Funktion von Dateien zur Verfügung, so sind folgende Punkte zu beachten:

- Die Funktionalität sollte möglichst nur angemeldeten Benutzern zur Verfügung stehen.
- Hochgeladene Dateien dürfen nicht im Wurzelverzeichnis des Webserver-Dienstes gespeichert werden. Es sollten entweder feste Verzeichnisstrukturen vorgegeben werden, in denen Ordner und Dateien angelegt werden können oder die Speicherung in einem anderen Kontext (wie z. B. in einer Datenbank oder einem fest vorgegebenen Pfad) erfolgen. Ein Angreifer sollte nicht aus dem vorgegebenen Kontext ausbrechen können.
- Der vorgegebene Pfad zur Speicherung der hochgeladenen Dateien darf nicht von den Benutzern geändert werden können.
- Zum Schutz vor Denial-of-Service-Angriffen sollte die Dateigröße begrenzt werden.
- Die Berechtigungen hochgeladener Dateien sollten restriktiv gesetzt sein, um einen unberechtigten Zugriff zu verhindern. Auf diese Weise soll unterbunden werden, dass hochgeladene Dateien eines Angreifers ausgeführt werden.
- Ein Virenschutzprogramm sollte die hochgeladenen Dateien auf Schadsoftware untersuchen.
- Die Wahl des Dateinamens sollte wie folgt eingeschränkt werden:
- Der Dateiname mit der Dateiendung sollte auf eine feste Anzahl von Zeichen begrenzt werden (z. B. 200 Zeichen).
- Alle nicht sichtbaren Zeichen (z. B. Steuerzeichen) und alle kodierten Varianten dieser Zeichen sollten vom Dateinamen entfernt werden (z. B. Unicode).
- Alle Zeichen mit einer spezifischen Bedeutung für Interpreter sollten entfernt werden (z. B. ; : > < / \ . * % $).
- Falls möglich sollten ausschließlich alphanumerische Zeichen und der Punkt für die Dateiendung erlaubt sein.

**Einbinden von Inhalten aus übergebenen Parametern**

Webanwendungen nehmen häufig Eingaben in Form von Parametern (z. B. aus Formularen) entgegen, verarbeiten diese und stellen sie erneut in der Rückantwort dar (z. B. der Suchbegriff bei einer Websuche). Ein Angreifer kann dies ausnutzen, um über ausgewählte Eingaben die Darstellung der Webseite zu manipulieren. Daher müssen alle von der Webanwendung zur Darstellung von Webseiten verwendeten Parameter gemäß M 4.393 *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services* validiert werden.

**Sicheres Weiterleiten von Requests (Redirect)**

Die Weiterleitungsfunktion einer Webanwendung sollte nicht beliebige Webseiten als Weiterleitungsziel zulassen, sodass Benutzer ausschließlich auf vertrauenswürdige, vorgesehene Webseiten weitergeleitet werden. So sollte vermieden werden, dass Benutzer beispielsweise über einen präparierten Link auf die Weiterleitungsfunktion der Webanwendung auf eine Phishing-Seite geführt werden.

Die folgenden Punkte geben Hinweise zu Einschränkungsmöglichkeiten von Weiterleitungszielen.

- Beschränkung auf lokale Seiten
  Wenn keine Weiterleitung auf externe Webseiten erfolgen muss, kann das Weiterleitungsziel auf externe Adressen geprüft und nur lokale Seiten zugelassen werden. Hierbei sollten ausschließlich relative Pfadangaben auf Ziele innerhalb der Webanwendung als Eingabe zugelassen und der notwendige Host-Teil nachträglich statisch hinzugefügt werden.
- Vordefinierte Weiterleitungsziele
  Ist eine Weiterleitung ausschließlich auf bekannte, statische Ziele vorgesehen, sollten diese serverseitig in einer vordefinierten Liste mit Indizes hinterlegt werden. Den Zielen werden somit statische Index-Werte zugeordnet. Anstelle der Zieladresse übergibt der Client einen Index-Wert (z. B. aus einer Auswahlliste eines Formulars), der serverseitig einer Zieladresse aus der Liste zugeordnet wird.
- Manuelle Bestätigung
  Der Benutzer muss vor der Weiterleitung die Zieladresse und somit die Vertrauenswürdigkeit des Weiterleitungsziels prüfen und bestätigen (z. B. über eine eingeblendete Weiterleitungsseite). Hiermit wird der Benutzer vor dem Verlassen der Webanwendung und damit des Sicherheitskontextes gewarnt.
- Referrer-Test
  Das Refferer-Feld des HTTP-Requests kann von der Weiterleitungsfunktion als zusätzliches Merkmal für die bestimmungsgemäße Nutzung geprüft werden. Eine Weiterleitung sollte nur dann erfolgen, wenn das Referrer-Feld die Adresse zu einer Webseite der Webanwendung mit einem Verweis auf das Weiterleitungsziel enthält.

**Einbindung von Inhalten Dritter**

Von Partnern eingebundene Daten und Inhalte (z. B. Werbeeinblendungen) sollten grundsätzlich als weniger vertrauenswürdig eingestuft werden. Es wird daher eine starke Kontrolle dieser Inhalte empfohlen, da die Gefahr besteht, dass Schadcode oder nicht vertrauenswürdige Inhalte eingebettet werden.

Prüffragen:

- Wird durch die Webanwendung eine Manipulation einzubindender Ressourcen verhindert (z. B. File Inclusion und Remote File Inclusion)?
- Wird das Hochladen von Dateien über eine mögliche Upload-Funktion der Webanwendung eingeschränkt (z. B. auf notwendige Dateitypen) und werden die Zugriffs- und Ausführrechte restriktiv gesetzt?
- Wird ein Ausbruch aus dem vorgegebenen Pfad zur Speicherung von Dateien unterbunden (z. B. durch Path Traversal)?
- Werden die Ziele der Weiterleitungsfunktionen einer Webanwendung ausreichend eingeschränkt (z. B. nur lokale Seiten) und der Benutzer beim Verlassen der Vertrauensdomäne informiert?

# M 4.400 Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** Fachverantwortliche, Verantwortliche der einzelnen Anwendungen
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Webseiten und Rückantworten von Webanwendungen und Web-Services können sicherheitsrelevante Informationen beinhalten, mit deren Hilfe Angreifer Sicherheitsmechanismen umgehen und Schwachstellen ausnutzen können. Daher dürfen keine sicherheitsrelevanten Informationen angezeigt werden, die nicht zwingend für den Betrieb und die Nutzung der Webanwendung oder des Web-Service notwendig sind.

Die folgenden Beispiele verdeutlichen, welche Informationen sicherheitsrelevante Hinweise enthalten können und wie verhindert werden kann, dass diese offengelegt werden.

**Keine sicherheitsrelevanten Informationen in Fehlermeldungen**

Tritt bei der Bedienung der Webanwendung oder des Web-Service ein Fehler auf (zum Beispiel Zugriffsfehler), sollten dem Benutzer neutrale Fehlermeldungen übermittelt werden. Die Fehlermeldungen dürfen keine direkten Rückschlüsse auf eingesetzte Techniken, Sicherheitsmechanismen und Zustände der Webanwendung ermöglichen.

Die folgenden Beispiele zeigen Informationen, die nicht in Fehlermeldungen enthalten sein sollten:

- Stacktraces und Debugging-Informationen,
- Meldungen wie "Benutzername ungültig" oder "Passwort ungültig" (anstelle von allgemeinen Fehlermeldungen wie "Benutzername oder Passwort ungültig"),
- von Hintergrundsystemen weitergereichte Fehlermeldungen wie zum Beispiel SQL-Fehlermeldungen einer Datenbank statt einer Meldung "Fehler bei der Überprüfung der Zugangsdaten",
- Fehlercodes statt zum Beispiel der Meldung "Ein Fehler ist aufgetreten".

Im Fall einer fehlgeschlagenen Authentisierung sollte beispielsweise unabhängig von der Gültigkeit des Benutzernamens stets eine allgemeingültige Meldung wie "Falsche oder ungültige Zugangsdaten" ausgegeben werden, damit ein Angreifer nicht auf die Existenz von Benutzerkonten rückschließen kann (user enumeration).

Grundsätzlich kann unterschiedlicher HTML-Code zur gleichen Ausgabe im Webbrowser führen. Beispielsweise werden zwei HTML-Seiten mit einer unterschiedlichen Anzahl von Leerzeichen im Browser gleich dargestellt, obwohl sie sich im HTML-Code unterscheiden. Es ist daher darauf zu achten, dass die Fehlermeldungen nicht nur in der Darstellung im Browser, sondern auch im HTML-Code identisch sind. Hiermit soll verhindert werden, dass ein Angreifer aufgrund eines veränderten HTML-Codes auf die Gültigkeit von Teil-Eingaben (zum Beispiel gültiger Benutzername bei falschem Passwort) schließen kann.

Weitere Informationen zur Fehlerbehandlung finden sich in M 4.395 *Fehlerbehandlung durch Webanwendungen und Web-Services*.

**Verhinderung von "WS-Interface Probing"**

Wenn Web-Services-Description-Language-(WSDL)-Dateien generiert werden, ist darauf zu achten, dass die verwendeten Tools oder Frameworks keine zusätzlichen und womöglich sicherheitskritischen Informationen in die Dateien schreiben. Deswegen sind die Dateien, bevor sie veröffentlicht werden, zunächst entsprechend zu prüfen. Bei Bedarf müssen die Tools bzw. Frameworks dann so umkonfiguriert werden, dass sie keine sicherheitskritischen Informationen mehr in die WSDL-Dateien schreiben oder die Dateien müssen nachträglich bereinigt werden.

XML-Transportcontainer sollten generell keine Fehlermeldungen mit detaillierten Informationen an Benutzer (potenzielle Angreifer) weitergeben. Die Meldungen sollten so allgemein bzw. generisch gestaltet sein, dass sie keine Informationen über eingesetzte Anwendungen, Frameworks und Versionsnummern enthalten und auch keinen Rückschluss auf diese zulassen.

Sollen Dienste nur von bestimmten, dem Service-Provider bekannten Benutzern gesucht und aufgerufen werden können, bietet es sich an, die WSDL-Dateien bzw. deren Repositories mittels einer vorherigen Nutzerauthentisierung vor direktem und unberechtigtem Zugriff zu schützen.

**Vermeidung von sicherheitsrelevanten Kommentaren in ausgelieferten Webseiten oder Web-Service-Antworten**

Bei der Entwicklung von Webanwendungen werden möglicherweise Kommentare in den HTML-Code geschrieben. Diese Kommentare können sicherheitsrelevante Informationen (zum Beispiel Todo-Listen, Versionsnummern, Zugangsdaten oder uninterpretierter Quellcode) enthalten, die als HTML-Kommentare in der Webseite vom Benutzer leicht eingesehen werden können. Auch die Rückantworten von Web-Services können Kommentare mit sicherheitsrelevanten Informationen enthalten, beispielsweise Kommentare in XML-Antworten eines SOAP-Dienstes. Aus diesem Grund ist darauf zu achten, dass in den Kommentaren keine sicherheitsrelevanten Informationen enthalten sind. Idealerweise sollten in in den ausgelieferten Webseiten oder Rückantworten einer produktiven Webanwendung oder eines Web-Service keine Kommentare verwendet werden.

**Eingeschränkter Zugriff auf Dokumentation**

Informationen in der Dokumentation einer Webanwendung oder eines Web-Service (zum Beispiel Dokumente zur Administration der Webanwendung) können einem Angreifer auf potentielle Schwachstellen (zum Beispiel Standardbenutzer nach der Installation) hinweisen und missbraucht werden, um Angriffe vorzubereiten. Daher sollte verzichtbare Dokumentation zur Webanwendung oder zum Web-Service und den zugehörigen Komponenten (zum Beispiel Datenbank) gelöscht werden. Ist die Dokumentation online verfügbar, so sollte ausschließlich der entsprechende Adressatenkreis darauf zugreifen können. Beispielsweise sollte die Dokumentation zur Administration einer Webanwendung oder eines Web-Service nicht aus dem Internet heraus erreichbar sein.

**Löschen nicht benötigter Dateien**

Im laufenden Betrieb einer Webanwendung oder eines Web-Service fallen häufig Dateien an, die nicht für den produktiven Betrieb benötigt werden (zum Beispiel temporäre Dateien, oder Backup-Dateien). Diese Dateien können sicherheitskritische Informationen beinhalten (zum Beispiel Test-Ergebnisse) oder Funktionen anbieten (zum Beispiel Testwerkzeuge zur Ermittlung von Versionsnummern der eingesetzten Bibliotheken), die für Angriffe auf die Webanwendung genutzt werden können.

Darüber hinaus ist zu beachten, dass insbesondere bei temporären Dateien oder Backup-Dateien häufig andere Dateiendungen (zum Beispiel *.bak-Dateien als Sicherheitskopien eines Editors) verwendet werden. Werden diese Dateien vom Webserver abgerufen, wäre es möglich, dass die Dateien aufgrund der unbekannten Dateiendung nicht mehr interpretiert werden und stattdessen der Quelltext der Webanwendung ausgeliefert wird.

Versionsverwaltungssysteme legen zumeist Dateien oder Ordnerstrukturen für die von ihnen verwalteten Objekte an (zum Beispiel Ordner wie .svn oder .git). Diese Dateien oder Ordner enthalten häufig detaillierte Informationen zu den verwalteten Projekten und ermöglichen unter Umständen einen kompletten Zugriff auf den Quellcode. Aus diesem Grund sollten Anwendungen oder Anwendungskomponenten grundsätzlich nicht über die Versionsverwaltung auf Produktivsysteme aufgespielt werden. Zumindest sollte der Zugriff auf von der Versionsverwaltungssoftware angelegte Dateien und Ordner blockiert werden.

Aus den genannten Gründen sind alle Dateien zu löschen, die für den produktiven Betrieb nicht benötigt werden. Darüber hinaus sollte regelmäßig kontrolliert werden, ob neue Dateien angefallen sind und ob diese gelöscht werden können. Ist dies nicht möglich, kann der Zugriff auf diese Dateien gesperrt werden.

**Sichere Erfassung durch externe Suchmaschinen**

Suchmaschinen setzen sogenannte Agenten (auch Robots oder Crawler genannt) ein, um neue oder geänderte Inhalte im Netz zu indizieren. Diese Agenten können durch die Datei robots.txt im Wurzelverzeichnis der Webanwendung instruiert werden, ausgewiesene Ressourcen (zum Beispiel Pfade) der Webanwendung zu ignorieren. Auf diese Weise können schützenswerte Informationen von der Indizierung in der Suchmaschine ausgenommen werden. Die vertraulichen Ressourcen (zum Beispiel Verzeichnis-Pfade) sollten in der Datei robots.txt unter der Direktive "Disallow" aufgeführt werden. So werden die Agenten veranlasst, die gelisteten Ressourcen nicht zu indizieren.

Damit die Einträge in der Datei robots.txt einem Angreifer keine Hinweise auf sicherheitskritische Ressourcen der Webanwendung geben, sollten alle zu schützenden Verzeichnisse nach Möglichkeit in einem gesonderten Verzeichnis der Webanwendung zusammengefasst werden. Ausschließlich dieses Verzeichnis sollte in die Datei robots.txt eingetragen werden, sodass diese keine internen Verzeichnisstrukturen mit sicherheitsrelevanten Informationen enthält.

**Schutz vor Directory-Traversal-Angriffen**

Ein Zugriff auf Ressourcen darf nur mit den dafür benötigten Rechten und nach einer vorausgegangenen Authentisierung erfolgen. Demzufolge sind geeignete Authentisierungsmechanismen zu implementieren sowie strikte Zu-

griffsregeln (Policies) zu definieren und umzusetzen. Zusätzlich kann ein Intrusion-Detection-System eingesetzt werden, das Directory-Traversal-Angriffe erkennt.

**Vermeidung von Produkt- und Versionsangaben**

Häufig enthalten Antworten und Ausgaben der einzelnen Komponenten der Webanwendung Angaben zu Produktnamen und Versionsnummern. Diese Informationen können zum Beispiel in HTTP-Headern oder in Kommentaren im HTML-Quelltext der ausgelieferten Webseiten, aber auch in XML- oder JSON-Antworten von Web-Services enthalten sein. Auf der Grundlage dieser Angaben kann ein Angreifer gezielt nach bekannten Schwachstellen des Produkts suchen und über diese die Webanwendung oder den Web-Service angreifen. Daher sollten Angaben zu verwendeten Produkten und Versionen vermieden werden (zum Beispiel Applikationsframework, Webserver).

**Verzicht auf absolute Pfadangaben**

Absolute Pfadangaben ermöglichen oft Rückschlüsse auf die interne Struktur und den Aufbau der Webanwendung. So kann beispielsweise der Speicherort schützenswerter Informationen ermittelt werden. Daher sollten nach Möglichkeit keine absoluten Pfadangaben der Webanwendung oder des Web-Service veröffentlicht werden.

Prüffragen:

- Werden ausschließlich Informationen veröffentlicht, die für den Betrieb oder die Nutzung der Webanwendung oder des Web-Service erforderlich sind?
- Werden von der Webanwendung oder dem Web-Service ausschließlich neutrale Fehlermeldungen ausgegeben und sind diese im Quelltext identisch?
- Werden sicherheitsrelevante Informationen in Webseiten (zum Beispiel in Kommentaren) oder Web-Service Antworten vor der Auslieferung an die Benutzer gelöscht?
- Ist nur dem entsprechenden Adressatenkreis der Zugriff auf sicherheitsrelevante Dokumentation der Webanwendung oder des Web-Service möglich?
- Werden vor der produktiven Inbetriebnahme alle Dateien gelöscht, die nicht für den Betrieb der Webanwendung oder des Web-Service notwendig sind, und wird eine entsprechende Prüfung auf nicht benötigte Dateien regelmäßig durchgeführt?
- Enthält die Datei robots.txt ausschließlich URLs, die keine sicherheitsrelevanten Informationen enthalten?
- Sind die WSDL-Dateien/Repositories mittels geeigneter Authentisierungsmechanismen geschützt?
- Sind für den Zugriff auf Ressourcen geeignete Authentisierungsmechanismen implementiert und strikte Zugriffsregeln festgelegt?

# M 4.401 Schutz vertraulicher Daten bei Webanwendungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Bei Webanwendungen werden Daten sowohl auf dem Server (z. B. in einer Webanwendung) als auch auf den Clients (z. B. im Browser) gespeichert und dabei über Netze übertragen. Hierbei kann es sich um vertrauliche Bankdaten, wie Kreditkarteninformationen oder Überweisungen, handeln. Daher müssen Maßnahmen getroffen werden, damit diese Daten nicht unbefugt eingesehen oder manipuliert werden können.

**Allgemeine Aspekte**

Werden vertrauliche Daten durch die Webanwendung verarbeitet, übertragen oder gespeichert (server- wie auch clientseitig), sollten sie durch kryptographische Verfahren geschützt werden. Auch wenn die Webanwendung kompromittiert ist, sollten die eingesetzten kryptographischen Verfahren diese Daten weiterhin schützen.

Vertrauliche Daten einer Webanwendung sind z. B.:

- Zugangsdaten (z. B. Benutzer, Passwort),
- Authentisierungsdaten (z. B. SessionID),
- kritische Daten, die von der Webanwendung verarbeitet werden (z. B. Zahlungsinformationen oder Gesundheitsdaten).

Kryptographische Verfahren können bei der Verarbeitung, Übertragung und Speicherung dieser Daten durch die Webanwendung und den Clients verwendet werden. Sie können dabei z. B. wie folgt eingesetzt werden:

- Verschlüsselung von Daten,
- Sichere Speicherung von Zugangsdaten,
- Schutz des Transportkanals.

Es ist darauf zu achten, kryptographische Algorithmen für den jeweiligen Einsatzzweck auszuwählen, die dem Stand der Technik entsprechen und keine bekannten Schwachstellen aufweisen (siehe hierzu M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Die kryptographischen Algorithmen sollten serverseitig umgesetzt sein.

Eine besondere Bedeutung bei der Kryptographie kommt den verwendeten Schlüsseln zu. Diese müssen je nach Einsatzgebiet über eine gewisse Mindestlänge verfügen und verschiedenen mathematischen Anforderungen (z. B. Komplexität) genügen. Zudem muss für einen entsprechend sicheren Transport beziehungsweise Austausch von Schlüsseln gesorgt werden. Gleiches gilt auch für deren Speicherung. Bei der Gestaltung einer Webanwendung sollten diese Punkte geregelt und in einem Kryptokonzept zusammengefasst werden (siehe B 1.7 *Kryptokonzept*).

Für Webanwendungen mit hohem Schutzbedarf kann zusätzlich eine Absicherung der Nutzdaten erforderlich sein. Werden beispielsweise Sozialdaten mit hohen Anforderungen an die Vertraulichkeit von der Webanwendung verarbeitet, können diese Daten von der Webanwendung vor der Speicherung verschlüsselt werden. So kann sichergestellt werden, dass auch bei einem di-

rekten Zugriff auf die Datenbank (z. B. durch Datenbankadministratoren) keine verwertbaren Daten ausgelesen werden können.

Werden vertrauliche Daten übertragen, können sie durch einen sicheren Transportkanal vor dem unbefugten Einsehen oder der Manipulation geschützt werden. Bevor vertrauliche Daten übertragen werden, sollte daher zu einer gesicherten Verbindung gewechselt werden. Auch nach der Anmeldung eines Benutzers sollten die übertragenen Daten weiterhin durch eine gesicherte Verbindung geschützt werden. Der Transportkanal wird hierzu üblicherweise durch den Einsatz von SSL/TLS abgesichert (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*L).

**Schutz clientseitig gespeicherter Daten**

Die zwischen dem Client und der Webanwendung ausgetauschten Daten können vom Client im lokalen Browsercache zwischengespeichert werden. Wenn der Browser die Daten über die Sitzungsdauer des Webanwendungsbenutzers hinaus im Cache speichert, können diese von Personen mit Zugriff auf den Rechner des Benutzers und von Skripten und Browser-Plugins ohne zusätzliche Zugriffskontrolle aus dem Cache abgerufen werden.

Das clientseitige Zwischenspeichern (Cachen) von vertraulichen Daten der Webanwendung kann durch folgende Direktiven in den HTTP-Headern der Webanwendung unterbunden werden:

- *Cache-Control: no-cache, no-store*
- *Pragma: no-cache*
- Expires: -1

Da der Web-Browser üblicherweise nicht unter der Kontrolle des Betreibers der Webanwendung steht, kann somit nicht vollständig ausgeschlossen werden, dass Daten trotzdem zwischengespeichert werden. Daher kann es für Webanwendungen mit hohem Schutzbedarf zusätzlich erforderlich sein, dass der Benutzer den Browsercache während der Bedienung der Webanwendung deaktiviert oder ihn löscht, sobald er seine Tätigkeiten an der Webanwendung beendet hat. In diesem Fall kann dem Benutzer beispielsweise nach erfolgter Abmeldung ein Hinweis für das Löschen des Browsercaches angezeigt werden. Dies betrifft insbesondere Webanwendungen, die von öffentlichen IT-Systemen aus genutzt werden. Alternativ kann der Benutzer auf die Verwendung des Private Modes des Browsers hingewiesen werden, bei dem keine Daten über die Sitzung zwischengespeichert werden.

Häufig werden bei der Bedienung einer Webanwendung Daten in Cookies auf dem Client gespeichert. Bei jedem Zugriff auf die Webanwendung werden diese Cookies transparent für den Benutzer an die Webanwendung übermittelt. Dabei kann es sich auch um schützenswerte Daten wie die SessionID handeln. Der Zugriff auf Cookies mit vertraulichen Daten sollte daher so weit wie möglich eingegrenzt werden. Wenn Cookies durch die Webanwendung erstellt werden, sollten folgende Cookie-Flags gesetzt sein:

- *Domain*
  Das Cookie-Flag sollte nicht gesetzt werden, denn dann werden per Default nur Anfragen der Domain beantwortet, die das Cookie gesetzt hat. Sollte es notwendig sein, dies auch anderen (Sub-)Domains zu ermöglichen, dann sollte die Domäne so weit wie möglich eingeschränkt werden, ohne die Funktionalität der Webanwendung einzuschränken (z. B. webapp.domain.tld anstatt domain.tld).
- *Path*

Das Path-Attribut beschränkt die Gültigkeit des Cookies auf einen festgelegten Pfad der Webanwendung. Auch das Path-Attribut sollte so weit wie möglich eingeschränkt werden, ohne die Funktionalität der Webanwendung einzuschränken (z. B. /webapp/ anstelle von /).

- *Secure*
  Ist die Direktive Secure gesetzt, so wird das Cookie ausschließlich über verschlüsselte Kommunikationskanäle übertragen, wie z. B. über SSL/ TLS.
- *HttpOnly*
  Diese Direktive verhindert, dass clientseitige Skripte auf das Cookie zugreifen (z. B. JavaScript). Es ist zu beachten, dass dieses Attribut nicht von allen Browsern unterstützt wird.

Das folgende Beispiel zeigt die Anweisung zur Erstellung eines Cookies unter Verwendung genannter Direktiven:

Set-Cookie: SESSIONID=sl342kdfjslaal39skdj; path=/webapp; secure; HttpOnly

Bei der Authentisierung des Benutzers gegenüber einer Webanwendung wird gewöhnlich ein HTML-Formular verwendet, in das der Benutzername und das Passwort eingegeben werden. Wenn der Benutzer sein Passwort in das Passwortfeld eintippt, sollte es nicht im Klartext wiedergegeben, sondern durch sogenannte Wildcards ersetzt werden (z. B. Sterne oder Punkte). Hierfür muss in der Formulardefinition der Passwort-Feld-Typ ausgewählt werden (*type="password"*).

Darüber hinaus kann der Web-Browser angewiesen werden, vertrauliche Formulardaten (z. B. den Benutzernamen und das Passwort) nicht zwischenzuspeichern und beim nächsten Aufruf des Formulars als Auswahl vorschlagen. Die Option *autocomplete="Off"* sollte hierfür bei der Definition des Formulars im Formularkopf gesetzt werden.

Während der Sitzung eines Benutzers an einer Webanwendung müssen in der Regel benutzerspezifische Daten gespeichert werden (z. B. die Artikel im Warenkorb). Diese Daten können dabei nicht nur serverseitig, sondern auch clientseitig in einem Cookie oder im Web-Storage des Browsers gespeichert werden. Grundsätzlich sollte vermieden werden, vertrauliche Daten an den Client zu übertragen oder auf dem Client zu speichern, da die Webanwendung keinen Einfluss auf den Schutz von clientseitig hinterlegten Daten hat. So können vom Browser auf dem Client umgesetzte Sicherheitsmechanismen zum Schutz der Daten häufig umgangen werden (z. B. durch direkten Zugriff auf das Dateisystem durch lokale Benutzer oder durch Cross-Site Scripting). Stattdessen sollten vertrauliche Daten grundsätzlich serverseitig gespeichert werden und ausschließlich das Identifikationsmerkmal des Benutzers (z. B. die SessionID) clientseitig hinterlegt sein.

Falls nicht vermieden werden kann, dass Sitzungsdaten clientseitig gespeichert werden, sollten diese Daten verschlüsselt und vor der Verarbeitung durch die Webanwendung auf Integrität geprüft werden. Damit wird sichergestellt, dass die Daten während der Übertragung nicht unbefugt eingesehen oder unbemerkt manipuliert werden können.

Darüber hinaus sollten die Daten vorzugsweise nur über den Zeitraum der Sitzung und nicht persistent gespeichert werden. Beim Web-Storage-Mechanismus sollte daher das sessionStorage-Objekt vor dem localStorage-Objekt bevorzugt werden.

**Schutz serverseitig hinterlegter Daten**

Sollen sich Benutzer an der Webanwendung anmelden können, müssen Zugangsdaten auf der Webanwendung gespeichert werden. Damit auch nach einer möglichen Kompromittierung der Webanwendung durch einen Angreifer die Zugangsdaten geschützt sind, dürfen sie nicht im Klartext gespeichert werden. Stattdessen sollten sie mithilfe von zeitgemäßen kryptographischen Algorithmen als salted Hashes hinterlegt werden, bei denen eine zufällige Zeichenfolge an den Klartext angehängt wird. Hierbei sollte für jedes Passwort ein unterschiedlicher, zufälliger Salt verwendet werden.

Darüber hinaus sollten die Zugangsdaten serverseitig auf einem vertrauenswürdigen IT-System (z. B. auf dem der Webanwendung) und in einem geschützten Bereich (z. B. außerhalb des Web-Root-Verzeichnisses oder in separaten Datenbanktabellen) hinterlegt sein. Die Zugangsdaten sollen nicht im Quelltext der Webanwendung (Hardcoded Passwords) gespeichert werden.

Darüber hinaus sollte ausschließlich die Webanwendung mit Schreibrechten auf die Zugangsdaten zugreifen können. Die Zugangsdaten sollten nur durch den Benutzer und über die vorgesehenen Schnittstellen und Funktionen der Webanwendung geändert werden können, sodass es Benutzern nicht möglich ist, Zugangsdaten unbefugt über z. B. den direkten Zugriff auf das Dateisystem zu lesen, zu ändern oder zu löschen.

Ruft ein Benutzer eine Webseite von der Webanwendung auf, so wird die Seite in der Regel von der Anwendung zur Laufzeit erstellt. Die aufgerufene Datei enthält Code, der von der Webanwendung vor der Auslieferung interpretiert wird und eine Webseite zurückliefert. Diese Webseite wird an den Benutzer übermittelt.

Üblicherweise werden anhand der Datei-Endung diese Dateitypen einem Interpreter oder Parser zugeordnet. Ändert sich die Datei-Endung, werden diese möglicherweise an den Benutzer übertragen, ohne vorher interpretiert zu werden. Werden derartige Dateien abgerufen, erhält der Benutzer Einsicht in die Programmlogik und vertrauliche Informationen, die gegebenenfalls im Code gespeichert sind. Dies kann beliebige Dateien betreffen, deren Datei-Endung nicht einem Interpreter oder Parser zugeordnet ist. Beispiele für anfällige Dateien sind:

- temporäre Dateien (z. B. temp.tmp),
- Backup Daten (z. B. backup.bak),
- Konfigurationsdateien (z. B. config.conf),
- Einzubindende Dateien (z. B. include.inc).

Die Dateien können vertrauliche Informationen, wie Zugangsdaten, enthalten, die hierüber bei unzureichender Zugriffsbeschränkung abgerufen werden können.

Daher sollten Dateien, die nicht für die Interpretation und den direkten Abruf durch den Benutzer vorgesehen sind, von der Webanwendung nicht ausgeliefert werden. Zusätzlich sollten die Dateisystemberechtigungen auf diese Dateien restriktiv gesetzt sein. Nicht mehr benötigte Dateien sollten zeitnah gelöscht werden (siehe auch M 4.400 *Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services*, Absatz *Löschen nicht benötigter Dateien).*

Prüffragen:

- Verwendet die Webanwendung sichere, kryptographische Algorithmen zum Schutz der Daten und werden diese serverseitig auf einem vertrauenswürdigen IT-System umgesetzt?
- Übermittelt die Webanwendung vertrauliche Daten über einen geschützten Transportkanal (z. B. SSL/TLS)?
- Sind Direktiven in den HTTP-Headern der Webanwendung vorgesehen, die ein clientseitiges Zwischenspeichern vertraulicher Daten verhindern?
- Setzt die Webanwendung Cookie-Flags zum Schutz der Cookies vor unbefugter Einsicht?
- Sind Formularfelder der Webanwendung so konfiguriert, dass vertrauliche Formulardaten (z. B. das Passwort) nicht im Klartext angezeigt oder vom Browser gespeichert werden?
- Werden Zugangsdaten der Webanwendung serverseitig mithilfe von kryptographischen Algorithmen vor unbefugtem Zugriff geschützt (Salted Hash)?
- Wird der Abruf von Dateien unterbunden, die Quelltexte der Webanwendung enthalten?

# M 4.402 Zugriffskontrolle bei Webanwendungen

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter Fachabteilung
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Die Autorisierungskomponente einer Webanwendung muss sicherstellen, dass Benutzer nur solche Aktionen durchführen können, für die sie über ausreichende Berechtigungen verfügen. Die Zuweisung von Rechten kann dabei auf der Grundlage von Benutzer-Rollen erfolgen.

Die Autorisierungskomponente sollte alle verwalteten Ressourcen einer Webanwendung berücksichtigen. Dazu zählen z. B.

- URLs,
- Dateien,
- Objektreferenzen,
- Geschäftsfunktionen,
- Anwendungsdaten,
- Konfigurationsdaten und
- Protokolldaten.

Eine Zugriffskontrolle ist möglichst auf allen Ebenen einer Webanwendung (z. B. durch die Webanwendung, den Applikationsserver, den Webserver und das Betriebssystem) umzusetzen. Demzufolge sollten neben einem Zugriffsschutz auf Webanwendungs-Ebene die Maßnahmen M 4.94 *Schutz der Webserver-Dateien* als auch M 5.168 *Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services* für den Zugriffsschutz von Daten auf dem Webserver und in Hintergrundsystemen berücksichtigt werden.

Folgende Punkte sollten für eine sichere Zugriffskontrolle auf Webanwendungs-Ebene berücksichtigt werden:

### Generelle Aspekte

Berechtigungen sollten restriktiv und nach dem Minimalprinzip vergeben werden. Die Benutzer der Webanwendung sollten daher nur über solche Rechte verfügen, die sie zur Bewältigung ihrer Aufgaben unbedingt benötigen.

Jeder Zugriff auf geschützte Inhalte und Funktionen sollte kontrolliert werden, bevor er ausgeführt wird. Dies gilt auch dann, wenn beispielsweise der gleiche Benutzer auf eine geschützte Ressource wiederholt zugreift. Auch automatisierte Client-Requests durch Web-Technologien (z. B. Ajax) sollten als unabhängige Requests behandelt und entsprechend kontrolliert werden.

### Anforderungen an die Autorisierungskomponente

Die Nutzung von Webanwendungen erfolgt gewöhnlich über einen generischen Client, der nicht unter der Kontrolle der Webanwendung steht. Damit kann ein Angreifer die Anfrage grundsätzlich beliebig manipulieren und clientseitig umgesetzte Sicherheitsmechanismen umgehen. Aus diesem Grund muss die Autorisierung serverseitig auf einem vertrauenswürdigen IT-System umgesetzt werden.

Die Routinen zur Autorisierung sollten zentral an einer Stelle und nicht verteilt im Programmcode der Webanwendung umgesetzt werden. Auf diese Weise wird der Code der Autorisierungskomponente von der Geschäftslogik der

Webanwendung getrennt und eine redundante und fehleranfällige Umsetzung vermieden. Bei der Entwicklung der Autorisierungskomponente sollte nach Möglichkeit auf Funktionen aus bereits existierenden Frameworks zurückgegriffen werden.

Kommt es zu Fehlern während der Zugriffskontrolle (z. B. weil unzureichende Informationen für die Autorisierung verwendet werden), müssen Zugriffe abgelehnt werden. Im Fehlerfall dürfen keine angeforderten Ressourcen übermittelt oder Funktionen unkontrolliert ausgeführt werden.

**Kontrolle aller beteiligten Ressourcen an einer Aktion**

Es darf einem Benutzer nicht möglich sein, eine Aktion auf eine Ressource durchzuführen, für die er keine ausreichenden Rechte hat. Falls z. B. ein authentisierter Benutzer einen URL-Parameter für die Zuordnung zu einem Bankkonto ändert, darf dieser dadurch keinen Zugriff auf ein fremdes Bankkonto erlangen. Werden die Rechte zur Durchführung einer Aktion geprüft, sollten daher ebenso alle an der Aktion beteiligten Ressourcen bei der Prüfung mit eingeschlossen werden.

Dies betrifft ebenfalls die Umsetzung und Konfiguration der Suchfunktion einer Webanwendung. Es sollte darauf geachtet werden, dass zugriffsgeschützte Ressourcen einem unbefugten Benutzer nicht als Suchergebnis präsentiert werden. Vor der Ausgabe der Suchergebnisse sollte daher beispielsweise geprüft werden, ob der Benutzer über ausreichende Rechte verfügt, um diese zu betrachten.

**Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen**

Webseiten und andere Ressourcen der Webanwendung werden gewöhnlich über die URL identifiziert und abgerufen. Dabei ruft ein Benutzer Webseiten oder Funktionen der Webanwendung in der Regel über die angezeigten Verlinkungen auf einer bereits dargestellten Webseite der Anwendung auf.

Wenn Ressourcen der Webanwendung geschützt werden sollen, ist es nicht ausreichend, den Link auf die Ressource aus den angezeigten Webseiten zu entfernen (z. B. ein Link auf die Administrationsseite), sondern es muss auch der direkte Aufruf der Ressource über die URL geschützt werden.

Die Seiten von Webanwendungen werden häufig dynamisch anhand von Referenzen auf Objekte (z. B. die ID eines Datenbankeintrags) erstellt. Werden diese Referenzen durch die Benutzer der Webanwendung übergeben (z. B. als Parameter in der URL), kann der Parameter und somit die Referenz von einem Benutzer beliebig geändert werden.

Da es sich hierbei nicht um direkte Referenzen (z. B. auf Dateien), sondern um indirekte Referenzen (Verweise auf Objekte) handelt, sollte eine Zugriffskontrolle anhand der Referenzwerte (z. B. IDs) erfolgen. Des Weiteren sollte nach Möglichkeit eine zusätzliche Zugriffskontrolle für die angeforderten Objekte in den Hintergrundsystemen durchgeführt werden. Dies kann beispielsweise durch das Durchreichen der Benutzerauthentisierung an die Hintergrundsysteme realisiert werden (siehe auch M 5.168 *Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services*).

**Restriktive Dateisystemberechtigungen bei der Upload-Funktion**

Grundsätzlich sollte der Zugriff auf Dateien durch die Benutzer der Webanwendung durch restriktive Dateisystemberechtigungen beschränkt werden (siehe M 4.398 *Sichere Konfiguration von Webanwendungen*).

Stellt die Webanwendung eine Funktionalität zum Hochladen von Dateien bereit, sollte nach dem erfolgten Hochladevorgang ausschließlich der Besitzer die Dateisystemberechtigung für den Zugriff auf die erstellten Dateien haben. In einem weiteren Schritt kann der Zugriff auf die Dateien explizit für andere Benutzer freigegeben werden. Generell ist darauf zu achten, dass hochgeladenen Dateien die Rechte für das Ausführen entzogen werden, sodass ein Angreifer hierüber keinen Schadcode zur Ausführung bringen kann (siehe auch M 4.399 *Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen*).

**Schutz temporärer Dateien**

Bei dynamisch erstellten Webseiten werden häufig temporäre Daten (z. B. Auswertungsgrafiken, Berichte) erzeugt. Handelt es sich dabei um schützenswerte Daten, so sollten diese nach Möglichkeit nicht im Dateisystem zwischengespeichert werden. Stattdessen sollten die Daten direkt an den Benutzer ausgeliefert werden. Falls eine Speicherung zu schützender Daten in temporären Dateien notwendig ist, sollten folgende Punkte berücksichtigt werden:

- Die Zugriffsberechtigungen im Dateisystem sind restriktiv zu setzen, sodass der Zugriff nur befugten Benutzern und Diensten möglich ist.
- Dateinamen sollten sich aus Zufallswerten zusammensetzen (z. B. einem Globally Unique Identifier (GUID)), sodass sie nicht leicht erraten werden können.
- Sobald die Daten nicht mehr benötigt werden, sollten sie zeitnah gelöscht werden.
- Es wird empfohlen, die Dateien in einem Verzeichnis zu speichern, welches nicht über den Webserver erreichbar ist (z. B. außerhalb des Wurzelverzeichnisses des Webservers).
- Der Zugriff auf die Dateien sollte ausschließlich über solche Schnittstellen der Webanwendung möglich sein, die ausreichende Sicherheitsmechanismen bei der Zugriffskontrolle und Protokollierung umsetzen.

Prüffragen:

- Findet eine Zugriffskontrolle bei der Webanwendung auf der Grundlage von Benutzerrollen und -rechte statt?
- Werden alle von der Webanwendung verwalteten Ressourcen von der Autorisierungskomponente berücksichtigt?
- Erfolgt die Autorisierung bei der Webanwendung serverseitig und zentral auf einem vertrauenswürdigen IT-System?
- Führen Fehler während der Zugriffskontrolle bei der Webanwendung zur Ablehnung des Zugriffs?
- Werden Zugriffsberechtigungen für direkte URL-Aufrufe und Objekt-Referenzen von der Autorisierungskomponente der Webanwendung berücksichtigt?
- Werden Dateisystemberechtigungen bei der Webanwendung (insbesondere beim Hochladen von Dateien) restriktiv vergeben?
- Ist ein sicherer Umgang mit temporären Dateien von der Webanwendung vorgesehen (z. B. restriktive Vergabe von Berechtigungen und zeitnahes Löschen nicht mehr benötigter Dateien)?

# M 4.403 Verhinderung von Cross-Site Request Forgery (CSRF, XSRF, Session Riding)

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Bei einem CSRF-Angriff (Cross-Site Request Forgery) wird einem Benutzer ein Befehl für eine Webanwendung (z. B. in Form eines Links in einem Gästebuch) von einem Angreifer übermittelt. Folgt der Benutzer diesem Link, wird der Befehl an die Webanwendung gesendet und im Kontext dieses Benutzers ausgeführt. Ist der Benutzer an der Webanwendung angemeldet, so wird die Vertrauensstellung des Benutzers gegenüber der Webanwendung ausgenutzt und der Befehl mit den Rechten des Benutzers ausgeführt.

Um derartige Angriffe zu erschweren, sollte die Webanwendung Sicherheitsmechanismen unterstützen, die es ermöglichen, beabsichtigte Seitenaufrufe des Benutzers von unbeabsichtigt weitergeleiteten Befehlen Dritter zu unterscheiden. Mit den folgenden Sicherheitsmaßnahmen soll verhindert werden, dass kritische Aktionen durch CSRF-Angriffe unbeabsichtigt ausgeführt werden.

**Verwendung eines zusätzlichen Tokens**

Bei einem CSRF-Angriff muss ein gültiger HTTP-Request nachgestellt und an das Opfer übermittelt werden. Ein solcher HTTP-Request kann z. B. durch eine URL auf die Webanwendung abgebildet werden (z. B. http://webapp.tld/addUser?name=benutzer). Hierfür muss der Angreifer die benötigten Request-Parameter, wie z. B. GET- und POST-Variablen, für den Aufruf kennen. Diese Parameter sind im Allgemeinen leicht zu ermitteln.

Als Schutz gegen einen CSRF-Angriff kann ein geheimes Token eingeführt werden, das nur schwer vom Angreifer erraten werden kann. Bei jedem Seitenaufruf der Webanwendung wird dieses Token als Parameter in URLs oder als verstecktes Element (Hidden-Field) in Formularen mit übertragen (Double Submit Cookies). Die Webanwendung prüft bei jedem Client-Request, ob das übertragene Token mit dem zur Sitzung hinterlegten Wert übereinstimmt. Im Fehlerfall wird der angeforderte Aufruf abgelehnt. Ohne Kenntnis dieses Tokens kann ein Angreifer keinen gültigen HTTP-Request nachstellen.

Obwohl die SessionID ein vertrauliches Datum ist und daher als Token zum Schutz gegen CSRF-Angriffe eingesetzt werden könnte, sollte vorzugsweise ein separates Token erzeugt werden. Für das Token sollten dabei ähnliche Anforderungen gelten, die auch an die SessionID gestellt werden.

Wird ein CSRF-Schutz implementiert, so wird empfohlen die Funktion aus bereits verwendeten Frameworks einzusetzen, falls diese eine entsprechende Implementierungen anbieten.

Bei Webanwendungen mit hohem Schutzbedarf sollte in Betracht gezogen werden, das Token für jeden Request derart zu erzeugen, dass bei jedem Aufruf der Webanwendung ein neues Token an den Client gesendet wird, das dann im darauffolgenden Request verwendet werden muss.

Bevor kritische Aktionen ausgeführt werden (z. B. zustandsändernde Anfragen wie eine Änderung des Passworts), sollte der Benutzer erneut von der Webanwendung authentisiert werden. Hierdurch können diese Funktionen nicht unbemerkt ausgeführt werden, sondern es ist eine Interaktion mit dem Benutzer erforderlich. Webanwendungen mit hohem Schutzbedarf sollten ein Authentisierungsverfahren mit mehreren Authentisierungsfaktoren (z. B. TAN, Chipkarte) verwenden.

Alternativ kann der Benutzer beim Aufruf von kritischen Aktionen auf eine Seite umgeleitet werden, die eine Benutzerinteraktion erfordert, bevor die Aktion ausgeführt wird (z. B. die Eingabe einer zufälligen Zeichenkette). Erst nachdem der Benutzer die Interaktion ausgeführt hat (z. B. richtige Zeichenkette eingegeben), wird er weitergeleitet und die ursprüngliche Anfrage bearbeitet. Anstelle der Zeichenkette können auch andere Mechanismen eingesetzt werden, die eine Benutzerinteraktion verlangen (z. B. CAPTCHAs oder Rätselfragen, siehe auch M 4.405 *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*).

Das Referrer-Feld im HTTP-Request (die URL der Webseite, von der der Benutzer zur aktuellen Seite gekommen ist) kann als ein weiteres Sicherheitsmerkmal genutzt werden. Ein Request eines Benutzers der Webanwendung ist häufig nur dann gültig, wenn das Referrer-Feld eine URL der eigenen Webanwendung enthält. So kann davon ausgegangen werden, dass der Request durch den Klick auf einen Link der Webanwendung erzeugt wurde.

Dabei ist zu berücksichtigen, dass das Referrer-Feld deaktiviert oder gefiltert werden kann (z. B. aus Gründen des Datenschutzes) und die Maßnahme daher nicht für alle Webanwendungen umgesetzt werden kann.

**Umgehung von Schutzmechanismen**

Sicherheitsmechanismen zum Schutz vor CSRF-Angriffen, die auf das Referrer-Feld oder zusätzliche Tokens (siehe Abschnitt *Verwendung eines zusätzlichen Tokens*) basieren, können durch Cross-Site-Scripting-Angriffe umgangen werden. Die korrekte Filterung von Benutzerdaten (siehe M 4.393 *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services*) ist daher entscheidend für die Wirksamkeit der Sicherheitsmaßnahmen zum Schutz vor CSRF-Angriffen.

Mindestens eine der ersten beiden Prüffragen sollte zum Schutz vor CSRF-Angriffen umgesetzt sein:

Prüffragen:

- Wird neben der SessionID ein geheimes Token für den Zugriff auf geschützte Ressourcen und Funktionen der Webanwendung benötigt?
- Wird bei Webanwendungen das Referrer-Feld im HTTP-Request als zusätzliches Merkmal zur Erkennung eines beabsichtigten Aufrufs durch einen Benutzer geprüft?
- Werden bei Webanwendungen kritische Aktionen nur nach einer erneuten Authentisierung oder einer manuellen Interaktion ausgeführt?

# M 4.404 Sicherer Entwurf der Logik von Webanwendungen

**Verantwortlich für Initiierung:** Fachabteilung, IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen
**Verantwortlich für Umsetzung:** Entwickler, Tester

Webanwendungen bilden komplexe Geschäftsprozesse ab, die über das bloße Anzeigen von einzelnen Webseiten hinausgehen. Beim technischen Entwurf dieser Prozesse muss darauf geachtet werden, dass die umgesetzte Anwendungslogik nicht missbräuchlich verwendet werden kann. So soll beispielsweise nicht aus einem vorgesehenen Prozess der Webanwendung ausgebrochen und somit der Ablauf des Prozesses von außen gesteuert werden können.

Die Anforderungen an die abgebildete Geschäftslogik müssen exakt erfasst und korrekt umgesetzt sein, sodass ausschließlich beabsichtigte und vorgesehene Aktionen durchgeführt werden können. Ein abweichendes Verhalten muss zurückgewiesen werden. Ist beispielsweise eine Empfehlungsfunktion der Webanwendung ausschließlich zum Versand von Artikelempfehlungen gedacht, sollte berücksichtigt werden, dass diese Funktion auch missbraucht werden kann, um SPAM-E-Mails zu versenden. Wird in diesem Beispiel der Empfehlungstext fest vorgegeben, so ist der Versand von SPAM über diese Funktion nicht möglich. Des weiteren ist auch zu prüfen, ob Fehler in der Geschäftslogik durch zwei gleichzeitige Sessions (concurrent sessions) auftreten können (race conditions).

Bei der Konzeption der Webanwendung sollten daher alle Funktionen anhand von Anwendungsfällen (Use Cases) dokumentiert werden. Dabei sollte erfasst werden, für welche Zwecke die Funktionen verwendet werden sollen und wie eine missbräuchliche Nutzung vermieden werden kann.

Wird die Webanwendung aus irgendeinem Grund abgebrochen, so muss die Logik sicherstellen, dass die Webanwendung wieder in einen konsistenten Zustand kommt (roll back).

Interaktive Funktionen in Web-Angeboten können auch durch aktive Inhalte umgesetzt werden, die auf dem Client-System ausgeführt werden (z. B. per JavaScript). Oft ist es auch möglich, diese Funktionalitäten mit dynamischen oder statischen Inhalten bereitzustellen. Da die Nutzung von aktiven Inhalten aus Sicherheitsgründen auf den Client-Systemen häufig deaktiviert ist, wird empfohlen, bei der Konzeption der Webanwendung auf die Verwendung aktiver Inhalte zu verzichten und die Anwendungslogik rein serverseitig zu realisieren.

Interaktive Funktionen in Webanwendungen können auf unterschiedliche Weise realisiert werden: Server-seitig oder Client-seitig. Da der Client nicht unter der Kontrolle der Webanwendung steht, kann nicht ausgeschlossen werden, dass dieser missbräuchlich benutzt wird. Gerade aktive Inhalte wie JavaScript oder ActiveX wurden und werden immer wieder ausgenutzt, Webanwendungen und die von ihnen verwalteten Informationen anzugreifen. Aus Sicherheitsüberlegungen empfiehlt es sich deshalb, aktive Inhalte Server-seitig umzusetzen oder, wo dies möglich ist, auf sie zu verzichten.

Ist die Nutzung aktiver Inhalte erforderlich, sind folgende Punkte zu beachten:

- Es sollte sichergestellt sein, dass die Webanwendung auch dann verwendet werden kann, wenn die Ausführung aktiver Inhalte im Browser deaktiviert ist.
- Für aktive Inhalte sollte nach Möglichkeit nachvollziehbar sein, aus welcher Quelle sie stammen, damit eine wirksame Prüfung im Client vorgenommen werden kann. Dies kann beispielsweise durch die Signatur von ActiveX-Komponenten erreicht werden.
- Ist die Serialisierung und die dynamische Erzeugung von XML-Daten bei der Verwendung von Ajax nicht zu vermeiden, sollte nach Möglichkeit auf Frameworks zurückgegriffen werden.
- Bei der Verwendung von JavaScript sollte auf den Funktionsaufruf eval() verzichtet werden.
- Benutzt die Webanwendung JSON für den Datenaustausch, so sind ausschließlich Objekte als Top-Level-Elemente zu verwenden.

Beispiele:

- Eine Webanwendung authentisiert die Benutzer in mehreren, aufeinanderfolgenden Schritten. Die Benutzer müssen im ersten Schritt Benutzername und Passwort und im zweiten Schritt ein Authentisierungstoken eingeben. Dabei sollte der erste Schritt nicht übersprungen werden können, damit sichergestellt ist, dass alle Authentisierungsmerkmale eingegeben werden. Im letzten Schritt für die endgültige Authentisierung muss dann eine erneute Prüfung aller Authentisierungsmerkmale durchgeführt werden.
- Bereits in der Konzeptionsphase einer Banking-Anwendung muss bedacht werden, dass ein Benutzer auch negative Beträge in ein Überweisungsformular eintragen kann. Die Webanwendung muss dabei sicherstellen, dass hierdurch nicht die Logik des Überweisungsformulars umgekehrt und keine unvorgesehene Gutschrift ausgelöst wird.

Prüffragen:

- Sind für die Funktionen der Webanwendung Anwendungsfälle (Use Cases) dokumentiert?
- Berücksichtigen die dokumentierten Anwendungsfälle der Webanwendung die missbräuchliche Nutzung der Funktionen?
- Wurde geprüft, ob auf die Verwendung von aktiven Inhalten bei Webanwendungen verzichtet werden kann?
- Wurde der Einsatz von aktiven Inhalten auf das Notwendige beschränkt?

# M 4.405 Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Webanwendungen und Web-Services bieten häufig ressourcenintensive Funktionen an, die zum Beispiel komplexe Datenbankabfragen oder Datenübermittlungen auslösen. Werden diese rechenintensiven Operationen bewusst gehäuft aufgerufen oder die Webanwendungen und Web-Services mit Anfragen überflutet, können hierdurch Ressourcen im Übermaß belegt und der Betrieb bis zur Unerreichbarkeit eingeschränkt werden. Dieses Vorgehen wird als Denial-of-Service-Angriff (DoS) bezeichnet.

DoS-Angriffe beruhen in den meisten Fällen ebenso wie Brute-Force- und Enumeration-Angriffe auf Automation (siehe M 4.396 *Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen*). Daher sollten zur Vorbeugung gegen DoS-Angriffe ähnliche Schutzmechanismen umgesetzt werden. Dazu zählen beispielsweise folgende Maßnahmen:

- Grenzwerte festlegen (zum Beispiel die vorübergehende Blockierung einer Ressource oder des Benutzerkontos nach wiederholten Fehlzugriffen),
- die Zeitspanne zwischen Anfrage und Verarbeitung durch die Webanwendung künstlich verzögern (zum Beispiel bei wiederholt erfolgloser Anmeldung),
- die aufrufende IP-Adresse bei Verdacht auf einen Angriff temporär sperren,
- CAPTCHAs verwenden,
- Eingaben bei Eingabefeldern verifizieren, bevor rechenintensive Operationen angestoßen werden,
- XML-Filtermechanismen und XML-Validitätsprüfungen einsetzen.

Zusätzlich geben die folgenden Beispiele Hinweise auf spezifische Schutzmaßnahmen, um Denial-of-Service-Angriffe bei Webanwendungen und Web-Services zu erschweren:

- Ressourcenintensive Operationen sind besonders anfällig für DoS-Angriffe. Daher kann die Ressourcennutzung pro Benutzer auf ein Maximum eingeschränkt werden. Darüber hinaus können bestimmte Operationen nur angemeldeten Benutzern zugänglich gemacht werden (zum Beispiel komplexe Datenbankaufrufe).
- Pro Benutzer sollte nur eine Anfrage zur gleichen Zeit bearbeitet werden. Mehrere Anfragen desselben Benutzers sollten sequenziell bearbeitet werden.
- Die Last durch DoS-Anfragen kann teilweise durch Zwischenspeichern (cachen) der Webseitenaufrufe deutlich verringert werden. Somit wird die angeforderte, rechenintensive Operation nicht bei jedem Aufruf ausgeführt, sondern lediglich das zwischengespeicherte Resultat zurückgegeben. Stark Ressourcen belastende Anfragen können auch in lastarmen Zeiten vorberechnet werden (Voraggregation).
- Die Architektur und Flusskontrolle der Webanwendung sollten darauf ausgelegt sein, rechenintensive Operationen zu vermeiden (zum Beispiel bei der Erstellung der Session-ID oder anderen kryptographischen Mechanismen sollten ressourcenintensive Operationen gemieden werden). Zur

Erkennung rechenintensiver Operationen können Lasttests durchgeführt werden.
- Ein Überlauf von Speicherplatz, zum Beispiel im Rahmen der Protokollierung, kann dazu führen, dass keine Schreibzugriffe mehr auf den Datenträger möglich sind. Werden Speichervorgänge von der Webanwendung oder dem Web-Service durchgeführt, kann dies den Betrieb gefährden. Daher sollte der Zugriff auf Datenspeicher begrenzt und die Kapazität der Datenspeicher regelmäßig geprüft werden. Ebenso sollte auch der Verbrauch von Arbeitsspeicher (RAM) pro Thread begrenzt werden.
- SOAP-Nachrichten müssen gemäß dem entsprechenden XML-Schema validiert werden. Ist die Validierung nicht erfolgreich, da sie zum Beispiel eine undefinierte Zahl an Elementen enthält, darf die SOAP-Nachricht nicht weiter verarbeitet werden, da diese ansonsten zu Problemen bei der Verarbeitung durch den XML-Parser führen kann.
- Ebenso sollten Webanwendungen und Web-Services vor SOAP-Flooding-Attacken geschützt werden. Diese sind vergleichbar mit herkömmlichen Flooding-Angriffen (z. B. SYN-Flooding) und können deswegen auch mit ähnlichen Schutzmaßnahmen bekämpft werden. So lassen sich mit einem Intrusion-Detection-System wiederholt gesendete Nachrichten erkennen und direkt blockieren, z. B. durch Anwendung von Heuristiken.

Bei Web-Anwendungen und Web-Services, bei denen aufgrund ihrer Natur mit gezielten, zum Beispiel politisch motivierten DoS-Angriffen aus dem Internet zu rechnen ist, kann auch die Zusammenarbeit mit einem Dienstleister sinnvoll sein, der sich auf die Abwehr von DoS-Angriffen spezialisiert hat. Solche Dienstleister leiten den IP-Verkehr im Angriffsfall über eigene Systeme, die Zugriffe filtern und/oder die Zielsysteme durch andere Maßnahmen wie zum Beispiel Zwischenspeicher (Caching) entlasten. Dabei ist im Vorfeld abzuwägen, ob durch die Umleitung der Datenströme über die Systeme Dritter zusätzliche Gefährdungen oder Anforderungen entstehen. Eine beliebte Angriffsmethode für zwischengespeicherte Web-Seiten ist beispielsweise, dass der Angreifer nicht vorhandene Unterseiten aufruft. Wenn dies der Dienstleister nicht abfängt und die Anfrage nach der vermeintlich neuen Unterseite an die ursprüngliche Seite weiterleitet, kommt es zu einem unbeabsichtigten DoS-Angriff des Dienstleisters. Solchen neuen Angriffsvektoren muss bei der Auswahl des Anti-DoS-Dienstleisters begegnet werden.

In serviceorientierten Architekturen (SOA) müssen zudem die Einträge in der Service-Registry von SOA-Diensten vor Manipulationen geschützt werden. Deshalb ist in der WS-Policy festzulegen, wer schreibenden Zugriff auf die Service-Registry hat. Das sind üblicherweise Service-Provider der eigenen technischen Domäne und Administratoren. SOAP-Nachrichten, die von Providern an die Service-Registry zwecks Registrierung übersandt werden, sind zusätzlich über das Provider-Zertifikat abzusichern, z. B. im Label der SOAP-Nachricht. Anhand der Zertifikate kann die Service-Registry überprüfen, ob der Eintrag echt ist. Ebenso muss sich ein Quality-of-Service-(QoS)-Agent mit einem Zertifikat gegenüber der Service-Registry ausweisen, wenn er QoS-Parameter an einen SOA-Dienst übermittelt. Zum Schutz der in der Regel periodisch erfolgenden Synchronisation zwischen verteilten Service-Registries sind die SOAP-Nachrichten, die die Synchronisationsinformation beinhalten, mittels des Zertifikats der absendenden Service-Registry abzusichern, z. B. im Label der SOAP-Nachricht.

Prüffragen:

- Werden der Einsatz und die Nutzung ressourcenintensiver Operationen bei Webanwendungen und Web-Services gemieden, und werden diese besonders geschützt?

- Wird ein möglicher Überlauf von Protokolldaten bei Webanwendungen und Web-Services überwacht und verhindert?
- Werden SOAP-Nachrichten anhand eines entsprechenden XML-Schemas validiert?
- Wurde bei kritischen Diensten und Anwendungen die Zusammenarbeit mit einem Anti-DoS-Dienstleister geprüft?
- Sind in serviceorientierten Architekturen die Einträge in der Service-Registry von SOA-Diensten vor Manipulationen geschützt?

# M 4.406 Verhinderung von Clickjacking

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Wird die Webanwendung Ziel eines Clickjacking-Angriffs, so werden Inhalte der Webanwendung in einem nicht sichtbaren Frame eingebunden. Besucht ein Benutzer eine Webseite, in der dieser Frame eingebunden ist, so werden Klicks auf sichtbare Inhalte unwissentlich vom unsichtbaren Frame abgefangen. Ist der Benutzer an der Webanwendung angemeldet, so können auf diese Weise zugriffsgeschützte Aktionen in der Webanwendung unbefugt ausgeführt werden. Um dies zu vermeiden, muss die Webanwendung sicherstellen, dass die Inhalte der eigenen Webanwendung nicht in Frames verwendet werden.

Daher sollten folgende Gegenmaßnahmen zur Verhinderung von Clickjacking umgesetzt werden:

- Eingebetteter Code (z. B. JavaScript) in den Webseiten sollte auf dem Client prüfen und sicherstellen, dass die Inhalte der Webanwendung auf der obersten Ebene des Browser-Fensters eingeblendet werden. Dies soll verhindern, dass keine anderen Ebenen über dem ursprünglichen Inhalt der Webseite gelagert werden können. Ist dies nicht möglich, so sollte die Anzeige der Webanwendung unterbunden werden (siehe *Skript zur Vermeidung von Clickjacking* in *Hilfsmittel zum Baustein Webanwendung*).
- Bei der Auslieferung der Webseiten durch die Webanwendung sollte zusätzlich in den HTTP-Response-Headern die Direktive X-FRAME-OPTIONS gesetzt sein. X-FRAME-OPTIONS DENY verhindert, dass Inhalte der Webseite in einem Frame angezeigt werden. Alternativ kann diese Einschränkung auf Seiten begrenzt werden, die nicht von derselben Domäne stammen (X-FRAME-OPTIONS SAMEORIGIN).

Prüffragen:

- Wird auf allen Webseiten der Webanwendung sichergestellt, dass die Inhalte ausschließlich auf der obersten Ebene des Browser-Fensters angezeigt werden?
- Ist in den HTTP-Response-Headern der Webanwendung die Direktive X-FRAME-OPTIONS gesetzt?

# M 4.407 Protokollierung beim Einsatz von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Da OpenLDAP in der Regel eine zentrale Komponente eines Netzes darstellt, sind Aktivitäten in OpenLDAP zu protokollieren und zu überwachen, um beispielsweise technische Probleme oder Angriffsversuche frühzeitig zu bemerken. Für OpenLDAP bestehen mehrere Möglichkeiten, Protokolle von Ereignissen anzulegen und den aktuellen Zustand des Systems zu überwachen.

Die Protokolldaten müssen unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Bei der Protokollierung und Überwachung eines zur Benutzerverwaltung eingesetzten Verzeichnisdienstes fallen zwangsläufig personenbezogene Daten an, die zur Leistungs- oder Verhaltenskontrolle geeignet sind. Wenn Protokollierung und Überwachung eingerichtet werden, sollten deshalb der Datenschutzbeauftragte (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*) und die zuständige Mitarbeitervertretung beteiligt werden. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei deren Auftreten ein Administrator zu benachrichtigen ist.

**Debug und Syslog**

Der slapd-Server verfügt über eine Debug-Funktion, um insbesondere technische Fehler zu identifizieren. Diese Funktion wird verwendet, wenn der slapd-Server mit dem Parameter "-d" gestartet wird:

slapd -d [Loglevel] -d [Loglevel] ....

Beim Start des slapd-Servers mit dem Parameter "-d" wird der slapd-Server im Gegensatz zum Aufruf ohne Debug-Funktion nicht vom aufrufenden Terminal getrennt und weiter im Vordergrund ausgeführt. Die Debug-Meldungen werden über die Standard-Ausgabe ausgegeben, in der Regel ist dies das aufrufende Terminal.

Der slapd-Server ist auch in der Lage, die Debug-Ausgaben an den Systemdienst Syslog zu leiten, der auch anderen zentralen Überwachungswerkzeugen als Basis dient. Statt des Parameters "-d" ist dafür der Parameter "-s" beim Aufruf zu verwenden, die Zahlen und Aliase der Loglevel bleiben gleich. Das gleiche Ergebnis wird durch die Angabe der Loglevel in der globalen Direktive "logLevel" (slapd.conf) bzw. "olcLogLevel" (slapd-config) erreicht. Syslog oder andere zentrale Werkzeuge werden insbesondere für große Strukturen empfohlen, da eine manuelle Kontrolle von Ereignissen dort kaum noch darstellbar ist. Bei akuten technischen Problemen ist die Debug-Funktion in der Konsole allerdings hilfreicher, da Syslog bei steigender Belastung oft nur zeitverzögert aktuelle Ereignisse ausgibt oder bei zu zahlreichen Nachrichten einige nicht verarbeitet.

Neben der Suche nach einem akuten technischen Fehler sind die technischen Protokolle geeignet, Unzulänglichkeiten der Konfiguration aufzudecken, die bisher nicht bemerkt wurden. Ist zum Beispiel aus den Protokollen ersichtlich, dass häufig nach einem bestimmten Attribut gesucht wird, für das kein Index

existiert (index_param failed), so sollte ein entsprechender Index erzeugt werden, um aufwändige Suchläufe zu vermeiden.

Die Debug-Funktion ist nicht dazu geeignet, die fachliche Nutzung des Verzeichnisdienstes zu protokollieren. Die Ausgaben sollten deshalb regelmäßig gelöscht werden, nachdem sie analysiert wurden.

**Protokollierung durch auditlog**

Über das Overlay "auditlog" (Audit Logging) können alle Veränderungen an einer Datenbank in eine Datei im Format LDIF geschrieben werden. Das Overlay kann nur Veränderungen aufzeichnen und ist schlecht anpassbar. Der Funktionsumfang ist wesentlich geringer als der des neueren Overlays "accesslog". Das Overlay "auditlog" wird gelegentlich eingesetzt, wenn keine Notwendigkeit besteht, erfolgte Zugriffe zu erfassen und dies zum Beispiel aus Datenschutzgründen sicher vermieden werden soll.

**Protokollierung durch accesslog**

Mit dem Overlay "accesslog" (Access Logging) können alle Zugriffe auf eine Datenbank erfasst werden. Das Overlay wird auch im Rahmen der Delta-Replikation verwendet. Es wird benötigt, um die geänderten Attribute aufzuzeichnen, damit nur diese im Rahmen der Replikation an den Consumer übermittelt werden müssen (siehe M 4.389 *Partitionierung und Replikation bei OpenLDAP*).

Das Overlay zeichnet sich durch folgende Eigenschaften aus:

- Es ist möglich, die Protokollierung durch die Sub-Direktive "logops" auf bestimmte Operationen wie ausschließlich Schreibzugriffe zu beschränken.
- Es können auch nicht erfolgreiche Zugriffe aufgezeichnet werden (Sub-Direktive "logsuccess FALSE"). Treten erfolglose Zugriffsversuche gehäuft auf, sollte dies näher untersucht werden. Mögliche Gründe dafür sind:
    - Zugriffsrechte wurden fehlerhaft vergeben.
    - Anwender wurden unzureichend geschult.
    - Ein Angreifer versucht, unzulässige Operationen im Verzeichnisdienst durchzuführen.
    - Die Protokolldaten werden in einer anderen Datenbank abgelegt, die über die Sub-Direktive "logdb" festgelegt wird. Durch eine geschickte Rechtevergabe beziehungsweise Replikation der Datenbank besteht die Möglichkeit, die Aufzeichnungen von Zugriffen dem Einflussbereich der Administratoren zu entziehen.
    - Durch die Ablage der Zugriffe in einer LDAP-Datenbank sind die Einträge selbst via LDAP zugänglich. Entsprechend stehen komfortablere Auswertungsmöglichkeiten zur Verfügung, als dies bei einem normalen Protokoll in Form einer Textdatei der Fall ist.
    - Das Overlay kann über die Sub-Direktive "logpurge" angewiesen werden, Inhalte der Datenbank in bestimmten Intervallen zu löschen, zum Beispiel täglich alle Inhalte, die älter als zwei Wochen sind. So können unter anderem Vorgaben des Datenschutzes technisch unterstützt werden.

Das Overlay "accesslog" stellt die beste Möglichkeit dar, Protokolle über die fachliche Nutzung des Verzeichnisdienstes anzulegen. Dies ist insbesondere sinnvoll, um zum Beispiel regulatorische Anforderungen wie die Eingabekontrolle des Bundesdatenschutzgesetzes (BDSG) zu erfüllen.

**Monitoring via back-monitor**

In jedem Fall werden bei der Durchsicht von Protokollen relevante Ereignisse wie Sicherheitsvorfälle lediglich im Nachhinein betrachtet. Bei einer zentralen Software, wie dem Verzeichnisdienst einer Institution, ist der laufende Betrieb zu überwachen (Monitoring). OpenLDAP stellt dafür benötigte Funktionen über das Backend "back-monitor" zur Verfügung. Aufgrund der schützenswerten Daten des Monitorings sollte eine restriktive eigene ACL für das Backend in Betracht gezogen werden (siehe M 4.387 *Sichere Vergabe von Zugriffsrechten auf OpenLDAP*).

Das Suffix ist im Gegensatz zu den meisten anderen Datenbanken in OpenLDAP fest vorgegeben. Es ist immer "CN=monitor". "back-monitor" gehört zur Klasse der dynamischen Backends, das heißt, eine Suche mittels ldapsearch oder ähnlichen Tools greift nicht auf einen geschriebenen Datenbestand zu, sondern generiert die Daten bei Anfrage. Für den Benutzer geschieht dies allerdings transparent, so dass das Backend "back-monitor" mit dem Werkzeug ldapsearch von OpenLDAP ebenso wie mit grafischen Oberflächen oder speziellen Anwendungen für Überwachungszwecke abgefragt werden kann.

Die durch das Backend "back-monitor" verfügbaren Informationen sind sehr umfangreich und wachsen proportional mit dem eingerichteten Funktionsumfang von OpenLDAP. Es wird deshalb empfohlen, eine Dokumentation anzulegen, welche Werte anzuschauen sind. Sinnvolle Objekte für das Monitoring sind beispielsweise:

CN=Backends, CN=Monitor

Dieses Suffix liefert Informationen über vorhandene Backends. Die Kindelemente enthalten Informationen zum jeweiligen Backend, seinem Status und unterstützten Funktionen.

CN=Databases, CN=Monitor

"Databases" gibt Informationen über eingerichtete Datenbanken aus. Die Kindelemente enthalten Informationen zur jeweiligen Datenbank.

CN=Overlays, CN=Monitor

Dieser Teilbaum liefert Informationen über genutzte Overlays. Die Kindelemente enthalten Informationen zur jeweiligen Datenbank.

CN=Connections, CN=Monitor

"Connections" enthält Informationen über bestehende Verbindungen. Die Kindelemente enthalten jeweils Details zu einer Verbindung. Daneben gibt es zwei besondere Kindelemente, die die Anzahl von allen (CN=Total, CN=Connections, CN=Monitor) sowie der bestehenden Verbindungen (CN=Current, CN=Connections, CN=Monitor) angeben. Die bestehenden Verbindungen sollten unter anderem vor dem Anhalten des Verzeichnisdienstes geprüft werden.

CN=Listener, CN=Monitor

Dieses Suffix enthält Angaben über IP-Adressen und Ports, an denen der slapd-Server auf Verbindungen wartet. Hier sollte regelmäßig überprüft werden, dass nur bewusst eingerichtete Verbindungsmöglichkeiten aktiv sind.

CN=Operations, CN=Monitor

"Operations" liefert Informationen über initiierte und abgeschlossene Operationen. Die mögliche Ausgabe ist sehr umfangreich. Sie sollte nur anlassbezogen erfolgen und dann nach den entsprechenden Operationen wie "bind", "add", "delete" gefiltert werden. Die aktuell durchgeführten Operationen sollten zum Beispiel vor dem Anhalten des Verzeichnisdienstes geprüft werden.

CN=Statistics, CN=Monitor

Der Teilbaum liefert statistische Angaben über die vom Server übermittelten Daten. Für die Ausgaben sollte eine Historie von Erfahrungswerten geführt werden, um dann regelmäßig auf Anomalien prüfen zu können.

Die Überwachung von OpenLDAP sollte mit einer Überwachung des IT-Systems, auf dem OpenLDAP betrieben wird, einhergehen. Die Funktionsfähigkeit von OpenLDAP hängt auch wesentlich von der verfügbaren Prozessorleistung und dem Speicherplatz für die Datenbank ab. Diese Größen werden jedoch nicht von den Überwachungsfunktionen von OpenLDAP abgedeckt.

Prüffragen:

- Erfolgt eine Protokollierung der Aktivitäten von OpenLDAP?
- Werden die Debug-Ausgaben von OpenLDAP lediglich zur technischen Problembehebung eingesetzt und regelmäßig gelöscht?
- Wird der laufende Betrieb des slapd-Servers mit geeigneten Werkzeugen wie back-monitor überwacht?
- Werden die OpenLDAP-Protokolle unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet?
- Ist die Überwachung des IT-Systems, auf dem OpenLDAP eingesetzt wird, gewährleistet?

# M 4.408 Übersicht über neue, sicherheitsrelevante Funktionen in Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Einführung von Windows Server 2008 brachte durch die minimale Standard-Installation des Betriebssystems eine erhebliche Verbesserung der grundlegenden Sicherheit, da nach erfolgter Basisinstallation nur die wirklich erforderlichen Dienste aktiviert und konfiguriert werden müssen. Darüber hinaus wurden weitere sicherheitsrelevante Werkzeuge und Funktionen mit Windows Server 2008 entwickelt oder freigegeben.

Die folgende Übersicht zeigt die wesentlichen, sicherheitsrelevanten Neuerungen von Windows Server 2008 auf und verweist auf Maßnahmen mit näheren Einzelheiten.

### Server-Manager

Der *Server-Manager* stellt das zentrale Verwaltungstool eines Windows Server 2008 dar. Über ihn lassen sich Rollen oder Features konfigurieren, die Firewall administrieren und Dienste verwalten. Teilweise sind die aufgeführten Konfigurationen auch über den *Sicherheitskonfigurations-Assistenten* (SCW) möglich, der seit Windows Server 2008 integraler Bestandteil des Systems ist.

### Server Core Installation

Der Server Core stellt ein minimales, weitestgehend ohne grafische Oberfläche auskommendes System dar. Die Vorteile eines Server Core sind:

- Die notwendige Softwarewartung wird reduziert.
- Der notwendige Verwaltungsaufwand wird reduziert.
- Es existiert nur noch eine reduzierte Angriffsfläche des Systems.

Weitere Informationen zu den Besonderheiten des Server Core finden sich in M 4.416 *Einsatz von Windows Server Core*.

### Autorisierungs-Manager

Der *Autorisierungs-Manager* bietet eine rollenbasierte Sicherheitsarchitektur für Windows-Systeme und -Applikationen und wurde unter Windows Server 2008 weiter entwickelt. Er bekommt insbesondere bei der Verwaltung des Hyper-V eine besondere Bedeutung, da dort gegebenenfalls eine auf Rollen aufsetzende Trennung der Administration von Host- und Gastsystemen erfolgt (siehe M 2.490 *Planung des Einsatzes von Virtualisierung mit Hyper-V*).

### BitLocker-Laufwerkverschlüsselung

Die mit Windows Vista eingeführte BitLocker-Laufwerkverschlüsselung ist nun auch unter Windows Server 2008 einsetzbar (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*).

### Verschlüsselndes Dateisystem

Ab Windows Server 2008 wurden folgende Neuerungen für die Nutzung von EFS eingeführt:

- Speicherung des Verschlüsselungszertifikats auf einer Chipkarte

- Verschlüsselung von Dateien auf Benutzerbasis im clientseitigen Cache
- Weitere Gruppenrichtlinienoptionen

Weitere Informationen zu EFS finden sich in M 4.147 *Sichere Nutzung von EFS unter Windows*.

**Benutzerkontensteuerung**

Die Benutzerkontensteuerung ist seit Windows Server 2008 auch auf Server-Systemen einsetzbar (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*).

**AppLocker**

Mit der Einführung von Windows Server 2008 R2 wurden die zuvor eingesetzten *Softwareeinschränkungsrichtlinien* durch *AppLocker* ersetzt. Damit lassen sich Zugriffe auf Dateien steuern, die Ausführung von bestimmten Dateitypen wie *.exe* oder *.bat* unterbinden und der Aufruf von DLLs verhindern (siehe M 4.419 *Anwendungssteuerung ab Windows 7 mit AppLocker*).

**Active Directory**

Innerhalb des Active Directory wurden zahlreiche Neuerungen eingeführt. Zu den wichtigsten gehören:

- Active Directory-Dienste sind als dedizierte Rolle installierbar. Eine minimale Installation des Active Directory oder die Verteilung einzelner Rollen des AD auf eigenständige Systeme ist somit möglich.
- Read-Only Domain Controller (*RODC*), der als System mit nur lesendem Zugriff auf das Active Directory eingeführt wurde.
- Verwaltete Dienstkonten zur zentralen Verwaltung von Diensten und Passwörtern über das Active Directory, oder durch die Nutzung von *Verwalteten lokalen Konten sind hinzugekommen*.
- Die Kennwort- und Kontosperrungsrichtlinien lassen sich granular konfigurieren, um Passwortrichtlinien innerhalb einer Domäne besser anzupassen.

Weitere Details hierzu sind in den Maßnahmen M 4.414 *Überblick über Neuerungen für Active Directory ab Windows Server 2008* und M 4.284 *Umgang mit Diensten ab Windows Server 2003* beschrieben.

**Windows-Firewall mit erweiterter Sicherheit**

Die sogenannte Hostfirewall eines Windows Server 2008 ist nach erfolgter Installation per Standard aktiviert und blockiert eingehende und gegebenenfalls ausgehende Verbindungen.

Sie arbeitet zustandsorientiert und filtert alle IPv4- und IPv6-Verbindungen. Anwendungen mit Netzkommunikation können durch die Administratoren einzeln freigegeben oder blockiert werden.

Bei Rollenänderungen des Servers oder der Aktivierung von Features werden die erforderlichen Ports oder Protokolle automatisch in den Regelwerken freigeschaltet.

**DirectAccess**

Die in M 4.411 *Sichere Nutzung von DirectAccess unter Windows* ausführlich dargestellte VPN-Technologie bietet eine integrierte Lösung, um sicher auf freigegebene Ressourcen innerhalb einer Windows Server 2008-R2-Umgebung zuzugreifen.

Es ist zu beachten, dass nur die beiden Versionen *Enterprise* und *Ultimate* von Windows 7 in der Lage sind, auf Ressourcen zuzugreifen, die durch einen DirectAccess-Server unter Windows Server 2008 R2 freigegeben wurden.

**Netzwerkzugriffsschutz**

Der Netzwerkzugriffsschutz ist eine neue Technik, die mit Windows Server 2008 und Windows Vista eingeführt wurde. Über den Netzwerkzugriffsschutz lassen sich zentrale Regelwerke definieren, mit denen sich der Zugriff auf das Netz absichern lässt.

Weitere Informationen zu NAP finden sich in M 4.410 *Einsatz von Netzwerkzugriffsschutz unter Windows*.

**Neues in der Windows-Sicherheitsüberwachung**

Mit Einführung des Windows Server 2008 und Windows Vista wurden grundlegende Veränderungen an der Sicherheitsüberwachung vorgenommen.

Wesentliche Veränderungen sind in M 2.489 *Planung der Systemüberwachung unter Windows Server 2008* ausführlich dargestellt:

- Änderung des Protokollformats in ein XML-basiertes Format,
- Einführung einer neuen Nummerierung der Ereignis-IDs,
- die Möglichkeit zum Sammeln von Ereignissen auf einem zentralen Windows System.

Darüber hinaus wurden mit der Einführung von Windows Server 2008 R2 und Windows 7 weitere Ergänzungen vorgenommen, die nur auf diesen beiden Versionen nutzbar sind:

- Globale Objektzugriffsüberwachung
  Über sogenannte Systemzugriff-Steuerungslisten (*System Access Control Lists, SACLs*) können die Zugriffe auf besonders schützenswerte Dateien oder Ordner überwacht werden. Dies ist hilfreich bei der Überprüfung, ob alle kritischen Daten eines Systems durch adäquate Rechte geschützt sind.
- Darstellung von Zugriffssteuerungseinträgen
  Über Listen mit Zugriffssteuerungseinträgen (*Access Control Entries, ACEs*) können die effektiven Rechte *Zulassen* oder *Verweigern* für ein Objekt dargestellt werden. Dadurch können beispielsweise die effektiven Gruppenmitgliedschaften und Zugriffsrechte eines überwachten Objektes angezeigt werden.
- Erweiterte Einstellungsmöglichkeiten für die Überwachungsrichtlinien
  Die mit Windows Server 2008 und Windows Vista eingeführten 53 neuen Kategorien erweitern die neun grundlegenden Überwachungseinstellungen in den Lokalen Richtlinien bzw. Überwachungsrichtlinien. Mit Windows Server 2008 R2 und Windows 7 können diese über die Überwachungsfunktionen in den Gruppenrichtlinien verwaltet werden. Die Nutzung eigener Skripte oder des Tools *Auditpol.exe* ist nicht mehr notwendig.

**Neues in den Gruppenrichtlinien**

Aufgrund des Zusammenspiels und der nahen Verwandtschaft von Windows Server 2008 (R2), Windows Vista und Windows 7 gelten die in Maßnahme M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP* ausführlich aufgeführten Neuerungen auch für Windows-Server-Systeme ab Version 2008. Es folgt eine kurze Übersicht der wesentlichen Neuerungen ab Windows Server 2008:

- Einführung neuer Kategorien für die Richtlinienverwaltung

- Neues Format und neue Funktionalität von administrativen Vorlagendateien (*ADMX,* siehe auch Maßnahme M 2.368 *Umgang mit administrativen Vorlagen unter Windows ab Server 2003*)
- Neue Starter-Gruppenrichtlinienobjekte (*GPOs*, siehe M 2.491 *Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008*)
- Möglichkeit zur Nutzung von Kommentaren für GPOs und die Richtlinieneinstellungen

Darüber hinaus wurde mit Windows Server 2008 R2 folgendes eingeführt:

- Nutzung der Windows PowerShell Commandlets für Gruppenrichtlinien,
- Verbesserung der vorhandenen Starter-Gruppenrichtlinienobjekte,
- Neue Benutzeroberfläche und zusätzliche Richtlinieneinstellungen zur Verwaltung der administrativen Vorlagen.

# M 4.409 Beschaffung von Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Beschaffungsstelle

Für Windows Server 2008 ist vor der Hard- als auch vor der Softwarebeschaffung die exakte Planung des Einsatzzweckes notwendig. Mit Einführung von Windows Server 2008 R2 wurde die Unterstützung der 32-Bit Prozessor-Architektur eingestellt. Neben der notwendigen Planung für die einzusetzende Hardware müssen auch die zu installierenden Applikationen auf 64-Bit Kompatibilität überprüft werden.

Darüber hinaus existieren sieben Editionen des Windows Server 2008 R2. Die drei vermutlich am häufigsten eingesetzten Systeme *Standard, Enterprise und Datacenter* wurden bis einschließlich Windows Server 2008 noch in Versionen mit und ohne Hyper-V unterschieden. Seit Windows Server 2008 R2 wird diese Unterscheidung von Microsoft nicht mehr vorgenommen. Die Installation des Hyper-V erfolgt durch die jeweilige Auswahl der Rolle und ist zum Beispiel auf den Editionen *Itanium, Web oder Foundation* nicht verfügbar.

Daher muss vor Beschaffung der jeweiligen Software-Lizenz des Servers der gewünschte Einsatzzweck des Systems festgelegt sein. Nur so können unnötige Kosten bei der Beschaffung der Windows Server 2008 Edition vermieden werden.

Dies gilt ebenso für die Anzahl der benötigten CPUs und die Größe des Arbeitsspeichers (RAM). Auch hier existieren erhebliche Unterschiede zwischen den einzelnen Editionen: Die Standard-Edition kann statt der 64 CPUs der Datacenter-Edition zum Beispiel nur 4 CPUs nutzen.

| **Editionen von Windows Server 2008 R2** | **Zusammenfassung** |
|---|---|
| Windows Server 2008 R2 Foundation | Einstiegsserver für kleinere Unternehmen |
| Windows Server 2008 R2 Standard | Standardplattform für die meisten Anforderungszwecke |
| Windows Server 2008 R2 Enterprise | - Bietet Failover Clusterknoten- Hot-Add Memory |
| Windows Server 2008 R2 Datacenter | Zusätzlich zu den Funktionen der Enterprise-Edition:- Hot-Add Processors- Hot-Replace Memory- Hot-Replace Processors |
| Windows Web Server 2008 R2 | Diese Edition dient ausschließlich als Plattform des IIS |
| Windows Server 2008 R2 für Itanium-basierte Systeme | Betriebssystem ausschließlich für Itanium-basierte CPU |
| Windows HPC Server 2008 R2 | Betriebssystem für High-Performance Computing |

Neben den Restriktionen bezüglich der nutzbaren Hardware weisen die jeweiligen Editionen erhebliche Unterschiede bei der möglichen Nutzung von Rollen auf. So erfordert die Web-Server-Edition neben der Installation des IIS auch

einen DNS-Server, weitere Rollen sind nicht verfügbar. Microsoft bietet als Entscheidungshilfe zur Auswahl der benötigten Edition detaillierte Übersichten wie zum Beispiel Tabellen der Editionen mit ihren unterstützten Serverrollen. Diese Dokumente sollten vor Beschaffung der jeweiligen Edition unbedingt berücksichtigt werden.

Weitere Details zu den installierbaren Server-Rollen finden sich in M 4.418 *Planung des Einsatzes von Windows Server 2008*.

Bei der Beschaffung aus einem Volumenlizenzvertrag ist auch die notwendige Infrastruktur für die Aktivierung der Systeme zu berücksichtigen (siehe M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*).

Prüffragen:

- Wird vor der Beschaffung von neuen Windows-Servern geprüft, welchen Einsatzzweck das System haben soll?

# M 4.410 Einsatz von Netzwerkzugriffsschutz unter Windows

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Unter dem Stichwort *Netzwerkzugriffsschutz* (englisch: Network Access Protection) werden bei Microsoft Betriebssystemen mehrere Schutztechniken zusammengefasst. Sie steuern den Zugang von einzelnen IT-Systemen zu einem Netz in Abhängigkeit des auf dem jeweiligen IT-System realisierten Sicherheitsniveaus. Auf diese Weise werden die im Netz erreichbaren sensiblen Systeme vor Bedrohungen durch andere Systeme mit mangelnden Sicherheitsvorkehrungen wie veralteten Virensignaturen geschützt.

Microsoft hat unter dem Namen "Network Access Protection" (NAP) einen Mechanismus zum Zugriffsschutz auf Netze in einige Produkte integriert. Die Nutzung von NAP ist optional, sie erfordert mindestens einen Windows Server 2008 sowie Clients mit Windows Vista, Windows 7 oder Windows XP mit Service Pack 3. Dabei steuern Komponenten auf dem Windows-Server den Zugriff durch die Clients. Diese senden beim Anmeldevorgang Informationen über ihr Sicherheitsniveau wie eingespielte Updates oder die Aktualität der Virensignaturen an den Server. Anhand von hinterlegten Sicherheitsregeln ("Policies") entscheidet der Server, ob die Clients auf das Netz zugreifen dürfen, oder ob der Zugriff verweigert oder auf wenige Server begrenzt wird. Diese Server enthalten in der Regel Dienste, die der Client zur Wiederherstellung des gewünschten Zustands benötigt. Das kann ein Update-Mechanismus für Virensignaturen oder Windows-Updates sein.

Der Zugriff zum zu schützenden Netz kann auf verschiedenen Ebenen kontrolliert werden:

- **VPN-Zugang**: In diesem Szenario steuert der Windows-Server den Zugriff von über ein VPN angebundenen Computern auf das interne Netz.
- **IPSec**: Auch beim Aufbau verschlüsselter Kommunikationskanäle via IPSec kann ein Windows-Server den Sicherheitsstatus des Clients in die Überprüfung einbeziehen.
- **IEEE 802.1X**: Hierbei handelt es sich um einen Standard, der die Authentisierung von IT-Systemen in einem Netz als Basis für die Zugriffssteuerung vorsieht. Die Authentisierung erfolgt dabei direkt zwischen Endgerät und einem sogenannten LAN Service Access Point, typischerweise einem Netz-Switch mit entsprechender Funktionalität. In Verbindung mit Windows Server 2008 können IEEE 802.1X-fähige Switches während des Authentisierungsvorgangs auch eine Prüfung des Client-Sicherheitsniveaus anfordern und die Konformität mit den Sicherheitsanforderungen des Netzes prüfen.
- **DHCP**: Bei diesem Ansatz wird dem Client in Abhängigkeit von der Prüfung seines Sicherheitsstatus eine DHCP-Konfiguration übermittelt, die entweder den Netzzugriff ermöglicht oder entsprechend beschränkt. Diese Variante ist allerdings durch einen Angreifer leicht auszuhebeln und nicht empfehlenswert.
- **Terminalserver-Access**: Auch beim Zugriff von Clients auf einen Windows Terminalserver via RDP kann am Terminalserver-Gateway eine Sicherheitsprüfung via NAP in den Authentisierungsvorgang einbezogen werden.

Je nach Szenario sind die technischen Abläufe und die eingesetzten Komponenten unterschiedlich. In jedem Fall benötigen die Clients eine lokal laufende Komponente namens Systemintegritätsagent (System Health Agent, SHA), der in sogenannten Systemintegritätsprüfungen (System Health Validators, SHVs) die lokalen Parameter der Sicherheitskonfiguration ermittelt und an die Gegenstelle sendet. In Clients mit Windows XP Service Pack 3, Windows Vista und Windows 7 ist ein entsprechender SHA im Betriebssystem integriert, für Clients mit Mac OS X oder Linux sind ebenfalls Implementierungen verfügbar.

Der in Windows verfügbare Client kann die folgenden Zustände prüfen:

- Auf dem Clientcomputer ist eine Firewall-Software installiert und aktiviert.
- Auf dem Clientcomputer ist eine Anti-Viren-Software installiert und wird ausgeführt.
- Auf dem Clientcomputer sind aktuelle Anti-Viren-Updates installiert.
- Auf dem Clientcomputer ist eine Anti-Spyware-Software installiert und wird ausgeführt.
- Auf dem Clientcomputer sind Anti-Spyware-Updates installiert.
- Die Microsoft Update-Dienste sind auf dem Clientcomputer aktiviert.

Die bei der Prüfung beteiligten Serverkomponenten umfassen je nach ausgewähltem Schutzmechanismus eine Integritätsregistrierungsstelle (Health Registration Authority, HRA) zur Ausstellung von Zertifikaten für geprüfte Clients, einen Server zur Übermittlung und Verwaltung von Netz-Richtlinien (Network Policy Server, NPS), der die übermittelten Konfigurationen mit dem Regelwerk abgleicht, sowie sogenannte Erzwingungsserver (Enforcement Server, ES) zur Durchsetzung des Ergebnisses der NAP-Prüfung.

Cisco bietet auf Netzebene unter dem Namen "Network Admission Control" eine eigene Umsetzung eines Netzzugriffsschutz-Konzeptes an. Beide Technologien lassen sich auch kombiniert einsetzen. Dazu integrieren die Cisco-Netzkomponenten eine Abfrage bei einem Windows Network Policy Server in die Prüfung der Clients.

NAP ist ein empfehlenswertes Mittel, um sensible Systeme in einem Netz zusätzlich abzusichern. Der Sicherheitsgewinn darf jedoch nicht überbewertet werden: Da die Agenten zur Ermittlung des Sicherheitsniveaus zwangsläufig auf den Clients selbst laufen, kann ein Angreifer den Client mit administrativem Zugang prinzipiell soweit manipulieren, dass er sich mit falschen Angaben Zugriff zum Netz verschaffen kann. NAP schützt nicht vor zielgerichteten Angriffen ("targeted Attacks"), sondern eignet sich insbesondere zur Schadensbegrenzung bei ungerichteten Angriffen wie Virusinfektionen.

Bei der Planung des Einsatzes von NAP müssen die folgenden Aspekte beachtet werden:

- **Definition der mit NAP verfolgten Schutzziele**: Welche Informationswerte sollen mit NAP geschützt werden und gegen welche Gefährdungen sollen diese mit NAP geschützt werden?
- **Planung der NAP-Architektur**: Auf der Grundlage welcher technischen Umsetzungsvariante wird NAP eingesetzt? Welche Serverkomponenten kommen zum Einsatz und auf welchen Servern werden diese betrieben?
- **Planung der NAP-Regelwerke**: Welche Systeme und Netze sollen durch NAP geschützt werden? Welche Anforderungen bestehen an IT-Systeme, die auf die geschützten Bereiche zugreifen wollen? Welche Dienste müssen für ein abgewiesenes System erreichbar sein, um den gewünschten Zustand wiederherzustellen?

- **Planung der NAP-Administration**: Wer hat administrativen Zugriff auf die NAP-Systeme und -Regelwerke? Wer ist verantwortlich für die Aktualität und Pflege der Regelwerke?

Prüffragen:

- Wurden bei der Planung des Einsatzes von NAP die verfolgten Schutzziele, die NAP-Architektur und die NAP-Administration beachtet?
- Werden die Ergebnisse der Planung von NAP einschließlich der Regelwerke dokumentiert?

# M 4.411 Sichere Nutzung von DirectAccess unter Windows

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Seit Windows 7 und Server 2008 R2 ist mit DirectAccess eine VPN-Technologie in das Betriebssystem integriert. Sie soll den Fernzugriff auf Ressourcen im lokalen Netz vereinfachen und Benutzer ermöglichen, ihre Clients überall so zu verwenden, als wären sie direkt mit dem LAN verbunden.

Um das zu erreichen, baut DirectAccess ohne Zutun der Benutzer und bereits vor der Anmeldung am Betriebssystem einen IPSec-Tunnel zu einer Gegenstelle auf Basis von Windows Server 2008 R2 im LAN auf. Es ist zu beachten, dass nur die beiden Versionen *Enterprise* und *Ultimate* von Windows 7 in der Lage sind, auf Ressourcen zuzugreifen, die durch einen DirectAccess-Server unter Windows Server 2008 R2 freigegeben wurden.

Über diese Gegenstelle sind zentrale Infrastrukturkomponenten wie Active Directory und DNS erreichbar ("Infrastructure Tunnel"). Für diesen ersten Tunnel wird nur das Computerkonto des Client-Rechners zur Authentisierung verwendet, das heißt, dieserTunnel steht einem Angreifer, der sich unbefugten Zugang zum Client-System verschafft, prinzipiell offen.

Nach erfolgter Benutzeranmeldung wird ein zweiter IPSec-Tunnel aufgebaut, über den der Zugriff auf weitere interne Ressourcen erfolgt ("Intranet Tunnel").

Bei der Einrichtung des DirectAccess-Zugriffs gibt es verschiedene Konfigurationsmöglichkeiten:

- Voller Intranetzugriff: In diesem Szenario haben über DirectAccess angebundene Systeme uneingeschränkten Zugriff auf alle Ressourcen im Intranet.
- Ausgewählte Server: Über DirectAccess angebundene Systeme haben nur Zugriff auf ausgewählte Server im Intranet.
- Ende-zu-Ende: Soll das über DirectAccess angebundene System auf einen Server im Intranet zugreifen, zum Beispiel für eine bestimmte interne Anwendung, so kann der per IPSec verschlüsselte Kanal vom Client bis zum Zielserver geführt werden. Auf diese Weise ist nicht nur der Zugriff von außen, sondern auch der Transport durch das LAN abgesichert.

Dabei ist zu beachten, dass die Rechner im internen Netz bei DirectAccess ausschließlich über IPv6 angesprochen werden können. Systeme, die im internen Netz nur per IPv4 erreichbar sind, sind mit DirectAccess nicht zugänglich. Die Beschränkung kann mit NAT64 oder Proxies umgangen werden, was jedoch zu Problemen mit Anwendungen führen kann.

Für die Kommunikation zwischen externem DirectAccess-Client und Gateway besteht diese Beschränkung nicht. Hier sind zahlreiche Möglichkeiten implementiert, um die erforderliche IPv6-Verbindung auch über eine vorhandene IPv4-Anbindung zu realisieren, so dass an die Anbindung des Clients keine erhöhten Anforderungen bestehen. Der DirectAccess-Client prüft die vorhandenen Verbindungsmöglichkeiten und wählt selbstständig ein passendes Protokoll aus.

Die Konfiguration von DirectAccess kann entweder über die dafür bereitgestellte *DirectAccess Management Console* erfolgen, oder über das Kommandozeilentool *Network Shell* und Gruppenrichtlinienobjekte.

Insbesondere im Einsatzszenario mit vollem Intranetzugriff stellt DirectAccess einen kritischen Zugang zum internen Netz dar. Dieser Zugang erfordert besondere Sicherheitsmaßnahmen. Es ist möglich, für den DirectAccess-Zugang ein bestimmtes Sicherheitsniveau bei der Authentisierung einzufordern, beispielsweise auf der Grundlage einer Chipkarte mit PIN (Zwei-Faktor-Authentisierung). Von dieser Beschränkungsmöglichkeit sollte beim Einsatz von DirectAccess Gebrauch gemacht werden.

Weiterhin ist es wichtig, dass der Tunnel ins interne Netz nur aufgebaut wird, wenn sich das angebundene System im Besitz eines rechtmäßigen Benutzers befindet. Deshalb sollten solche Systeme mit einer Festplattenverschlüsselung versehen werden (zum Beispiel gemäß M 4.337 *Einsatz von BitLocker Drive Encryption*) und über eine automatische Sperrung bei Inaktivität des Benutzers verfügen (siehe M 4.2 *Bildschirmsperre*).

Beim Zugriff auf das interne Netz von mobilen Systemen aus besteht stets ein erhöhtes Risiko von Schadsoftware-Infektionen, da die mobilen Systeme unter Umständen infiziert sein könnten. Um zumindest grundlegende Sicherheitseigenschaften des Endgeräts zu prüfen, bevor eine Verbindung per DirectAccess zugelassen wird, kann der DirectAccess-Zugang mit einer Netzzugriffsschutz-Prüfung versehen werden (siehe M 4.410 *Einsatz von Netzwerkzugriffsschutz unter Windows*).

Der DirectAccess-Server muss für die Clients von außen erreichbar sein und stellt daher einen möglichen Angriffspunkt auf das interne IT-Netz dar. Für seine Einbindung in das Netz ist M 4.224 *Integration von VPN-Komponenten in ein Sicherheitsgateway* zu beachten. Dabei ist zu berücksichtigen, dass der DirectAccess-Server Mitglied der Windows-Domäne sein muss.

In der Standardeinstellung teilen DirectAccess-Clients ihren Datenverkehr zum Intranet und ihren Datenverkehr zum Internet auf. Während Verbindungen zu Ressourcen im Intranet automatisch durch den DirectAccess-Tunnel geführt werden, baut das Client-System Verbindungen ins Internet direkt und außerhalb des Tunnels auf. Diese Verhaltensweise soll das interne Netz und den Tunnel von Datenverkehr entlasten.

In diesem Szenario kann jedoch der DirectAccess-Client auch einen Netzübergangspunkt darstellen, den ein Angreifer benutzt, um sich vom Internet über den Client Zugriff auf das interne Netz zu verschaffen. Gleichzeitig sind die vom Client direkt aufgebauten Internet-Verbindungen nicht durch eventuell vorhandene zentrale Sicherheitseinrichtungen geschützt, wie Proxy-Server mit Content-Filterung.

Aus den genannten Gründen sollte abweichend von der Voreinstellung aller Datenverkehr vom Client durch den DirectAccess-Tunnel geleitet werden ("Force Tunneling"). So wird ein kontrollierter und sicherer Internetzugriff über die vorhandenen Sicherheitseinrichtungen realisiert und "Hintereingänge" ins interne Netz werden verhindert.

Prüffragen:

- Ist zum Verbindungsaufbau per DirectAccess Zwei-Faktor-Authentisierung erforderlich?

- Ist auf allen DirectAccess-Clients eine Festplattenverschlüsselung aktiviert?
- Ist der DirectAccess-Server auf geeignete Art in einem Sicherheitsgateway integriert?
- Wird Datenverkehr vom Client in das Internet als auch in das Intranet durch den DirectAccess-Tunnel geleitet ("Force Tunneling")?

# M 4.412 Sichere Migration von Windows Server 2003 auf Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Die Migration von Windows Server 2003 auf Server 2008 erfordert zunächst eine sorgfältige Planung. Dazu ist zuerst die Migrationsstrategie festzulegen:

- Bei einer *Neuinstallation* werden die Daten des alten IT-Systems gesichert, ein neues (aktuelles) IT-System auf der gleichen Hardware installiert und die Dienste unter Nutzung der gesicherten Datenbestände neu aufgesetzt. Diese Variante ist mit Ausfallzeiten während der Migration verbunden und erfordert hohe Planungsaufwände. Es besteht das Risiko eines verlängerten Ausfalls bei unvorhergesehenen Problemen.
- Bei einem sogenannten *In-Place-Update* wird aus dem laufenden System heraus ein Update der Systemsoftware initiiert. Diese Variante birgt verschiedene Risiken, unter anderem die Übernahme von "Altlasten" in der Konfiguration, Produktivitätsausfälle während des Updates und das Risiko eines gescheiterten Updates.
- Bei einer "echten" Migration wird das neue System auf neuer Hardware parallel zum Altsystem installiert und anschließend werden die produktiven Dienste vom Altsystem auf das Neusystem umgezogen.

Das dritte Szenario bietet den besten Schutz gegen Produktions- oder Datenverluste, erfordert aber die Verfügbarkeit von zusätzlicher Hardware, um das neue IT-System parallel aufzusetzen. Insbesondere wegen der besseren Testmöglichkeiten sollte dieses Migrationsszenario vorrangig ausgewählt werden.

**Migrationsplanung**

Für die Planung müssen die mindestens die folgenden Punkte betrachtet werden:

- Die benötigte Zeitspannung der Migration unter Berücksichtigung der Auswirkungen auf produktive Dienste auf dem migrierten System oder davon abhängigen weiteren Systemen muss berücksichtigt werden.
- Es ist festzulegen, wer die Migration durchführt.
- Die Vorgehensweise für die Migration ist auszuwählen.
- Testschritte im Migrationsprozess, inklusive Abbruchkriterien.
- Notfallpläne und Handlungsoptionen sind zu diskutieren und festzulegen.
- Die betroffenen Nutzer sowie die Verantwortlichen abhängiger IT-Systeme sind über die sie betreffenden Schritte der Migration zu informieren.

Die Ergebnisse sollten in einem Migrationskonzept dokumentiert werden. Nähere Hinweise zum Migrationskonzept und seinen Inhalten finden sich in M 2.319 *Migration eines Servers*.

Sind in der Windows-Domäne bislang noch keine Server 2008 Systeme vorhanden, so muss in die Planung auch die Migration des Domänen-Controllers (siehe M 4.317 *Sichere Migration von Windows Verzeichnisdiensten*) oder zumindest die Anhebung der Active Directory-Funktionsebene einbezogen werden. Dabei ist vorher zu testen, ob sich durch die Veränderungen im Active Directory Probleme mit vorhandenen Anwendungen ergeben (siehe G 2.156 *Kompatibilitätsprobleme beim Anheben der Active Directory-Funktionsebene*).

Befinden sich Daten des Quellsystems auf einem externen Datenspeicher wie einem SAN/NAS oder einer externen Festplatte, so muss festgelegt werden,

ob die Dateien bei der Migration kopiert werden, oder ob der neue Server auf die Daten auf dem vorhandenen Speichersystem zugreifen soll. Die zweite Variante ist einfacher, weil der Kopiervorgang entfällt, unterliegt jedoch bestimmten Einschränkungen. So können dabei die Berechtigungen lokaler Benutzerkonten verloren gehen, wenn gleich bezeichnete lokale Konten auf dem Zielsystem eine andere SSID besitzen und die Migration von BitLocker- oder EFS-verschlüsselten Daten auf diesem Weg ist nicht möglich.

Werden Daten in bestehende Verzeichnisse auf dem Zielsystem kopiert, ist dagegen zu beachten, dass sich die Vererbung von Zugriffsrechten auf dem Zielverzeichnis mit untergeordneten Dateien dann auf die bestehenden Rechte im Zielverzeichnis und nicht mehr auf die ursprünglichen Rechte im Quellverzeichnis bezieht (siehe G 2.116 *Datenverlust beim Kopieren oder Verschieben von Daten ab Windows Server 2003*) Die Berechtigungen für Quell- und Zielverzeichnis müssen daher vorab angeglichen werden.

**Hilfsmittel**

Für die Migration von Systemen zu einem Windows 2008 Server stellt Microsoft umfangreiche Hilfsmittel bereit. Dies umfasst zum einen Migrationshandbücher für die Serverrollen, in denen die einzelnen Schritte zur Vorbereitung des Ziel- und des Quellsystems, zur Durchführung der Migration und zu den abschließenden Schritten ausführlich beschrieben sind. Erfüllt das zu migrierende System mehrere Rollen, so sollte vorab aus den Migrationshandbüchern für die beteiligten Rollen ein eigenes Migrationshandbuch konsolidiert werden.

In den Anhängen zu den Migrationshandbüchern finden sich Arbeitsblätter, die dabei helfen, relevante Konfigurationseinstellungen für die Migration im Altsystem zu erheben und gesammelt zu dokumentieren. Die hier abgefragten Informationen sollten jedoch auch Bestandteil einer guten Systemdokumentation sein (siehe M 2.25 *Dokumentation der Systemkonfiguration*).

Für die einzelnen Serverrollen werden dabei zum Teil spezielle Windows-Server-Migrationstools genutzt, die auf dem Quell- und dem Zielsystem installiert werden und für eine automatisierte Übertragung der Dienstekonfiguration sorgen. Unter Windows Server 2008 R2 können die Migrationstools als Feature nachinstalliert werden, auf dem Quellsystem ist eine separate Installation erforderlich. Die Migrationstools unterstützen auch die Migration von Servern auf eine Zielplattform, die als Server Core betrieben wird (siehe M 4.416 *Einsatz von Windows Server Core*), sowie die Migration von physischen auf virtuelle Maschinen. Die Migrationstools erfordern die vorherige Installation des .NET-Frameworks 2.0 sowie der Windows PowerShell und ausreichend verfügbaren Speicherplatz für die Installation. Quell- und Zielsystem müssen in der gleichen Sprache installiert sein.

Da auch die Installation der Migrationstools einen Server-Neustart erfordern kann, sollte sie bereits in die Migrationsplanung einbezogen werden.

**Migrationsvorbereitung**

Für die Vorbereitung der Migration sind verschiedene Schritte durchzuführen oder zu prüfen:

Für die Migration wird ein Administrationsaccount auf dem Quell- und auf dem Zielsystem benötigt.

Der Zielserver muss ausreichend Speicherplatz für die Übernahme der Daten bereithalten. Dabei ist auch eine möglicherweise aktive Kontingentverwaltung auf dem Zielsystem zu berücksichtigen.

Das Quellsystem sollte vor der Migration komplett gesichert werden, um im Fall von Problemen, die nicht im für die Migration vorgesehenen Zeitfenster gelöst werden können, einen definierten Rückfallpunkt zu haben.

Auf dem Quell- und auf dem Zielsystem sollten alle aktuellen Patches eingespielt sein, um sicherzustellen, dass alle bekannten Fehler in der Systemsoftware behoben sind.

Die Systemzeit auf Quell- und Zielsystem muss synchronisiert sein, beispielsweise über eine gemeinsame externe Zeitquelle.

Je nach Serverrolle müssen die entsprechenden Migrationstools auf dem Quellsystem und auf dem Zielsystem installiert werden.

Für die Kommunikation benötigen die Migrationstools von Microsoft die Ports udp/7000 und tcp/7000. Sie müssen auf den lokalen Firewalls der beiden Systeme und im Netz dazwischen freigeschaltet sein.

Schließlich müssen alle betroffenen Benutzer und Administratoren abhängiger Systeme und Anwendungen rechtzeitig über die Durchführung der Migration und die sich daraus ergebenden Einschränkungen informiert werden.

**Durchführung der Migration**

Um die Konsistenz des Zielsystems nicht zu gefährden, muss ausgeschlossen werden, dass während des Migrationsvorgangs Zugriffe von Dritten auf das Zielsystem erfolgen. Ebenso dürfen nach Beginn der Migration keine Arbeiten mehr auf dem Quellsystem erfolgen, die eine Veränderung der Konfiguration oder des Datenbestands bewirken. Entsprechende Zugriffe können organisatorisch oder besser technisch zum Beispiel auf Netzebene verhindert werden.

Nach Abschluss der Migration sollten alle relevanten Funktionen des Servers ausführlich getestet werden, um mögliche Migrationsfehler zu erkennen und Auswirkungen auf den produktiven Betrieb zu vermeiden.

Um keine unnötige Angriffsfläche auf dem Zielsystem zu bieten, sollten die Migrationstools nach Abschluss der Migration wieder vom System entfernt und die dafür eingerichteten UDP- und TCP-Ports in der lokalen Firewall und auf weiteren Sicherheitsgateways im Netz wieder geschlossen werden.

Prüffragen:

- Wurde eine bedarfsgerechte Migrationsplanung von Windows Server 2008 durchgeführt?
- Sind alle Werkzeuge, die im Rahmen der Migration auf Windows Server 2008 benötigt werden, bekannt und getestet?
- Ist sichergestellt, dass die weitreichenden Berechtigungen des Migrationsteams nach Abschluss der Migration auf Windows Server 2008 wieder zurückgesetzt werden?
- Ist eine IT-Sicherheitskonzeption für die Migrationsphase von Windows Server 2008 erarbeitet worden?
- Ist sichergestellt, dass alle Ausnahmeregelungen, die während der Migration auf Windows Server 2008 notwendig sind, nach der Migration aufgehoben werden?

- Sind alle Betroffenen ausreichend auf die Migration auf Windows Server 2008 vorbereitet worden?

# M 4.413 Sicherer Einsatz von Virtualisierung mit Hyper-V

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Leiter IT

Die Grundlage für den sicheren Einsatz von Virtualisierung mit Hyper-V bilden die Umsetzung der Planungsmaßnahmen (siehe M 2.490 *Planung des Einsatzes von Virtualisierung mit Hyper-V*) und des Bausteins B 3.40Y *Virtualisierung*, hier insbesondere der Maßnahmen M 4.v7 *Sicherer Betrieb von virtuellen Infrastrukturen* und M 5.154 *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen* Die vorliegende Maßnahme zeigt die darauf aufsetzenden Hyper-V-spezifischen Punkte auf. Das Schwergewicht liegt auf den folgenden Punkten:

- Wirksame Umsetzung der geplanten Berechtigungskonzepte
- Härtung der Management-Instanz

Die Gäste selbst benötigen nur wenige Hyper-V-spezifische Anpassungen.

Für die Absicherung der Management-Instanz und der Konfiguration sowie für die Umsetzung der Berechtigungen bietet Microsoft mit dem Hyper-V Security Guide und den dort referenzierten Online-Ressourcen eine ausführliche Dokumentation an, die unbedingt genutzt werden sollte.

**Management-Instanz**

Die Grundlage für eine Härtung der Management-Instanz bildet die Reduzierung der Angriffsfläche durch eine Basis mit reduzierter Funktionalität (siehe M 2.490 *Planung des Einsatzes von Virtualisierung mit Hyper-V*). Dazu eignen sich insbesondere Server Core (siehe M 4.416 *Einsatz von Windows Server Core*), beziehungsweise der Stand-alone Hyper-V-Server.

Ohne eine solche Basis sollte zumindest der Einsatz der SSLF-Baseline (Specialized Security Limited Functionality) erfolgen. Sie kann auch zusätzlich angewandt werden.

Die SSLF-Baseline muss vor der Installation der Hyper-V-Rolle angewendet werden, sonst sind nach dem Einsatz der SSLF-Baseline Korrekturen notwendig, die in Microsofts *Hyper-V Security Guide* beschrieben sind.

Für die Management-Instanz gilt der Grundsatz: Es dürfen keine weiteren Dienste und Anwendungen betrieben werden. Ausnahmen gelten prinzipiell für Sicherheitssoftware wie Anti-Virus-Scanner, Host-IDS und standardmäßig genutzte Infrastrukturdienste (Zeitsynchronisierung), Remote-Management- und Softwarepflege-Werkzeuge. Nach Möglichkeit sollte auch auf diese Ausnahmen verzichtet werden.

Wird ein Anti-Virus-Scanner mit Echtzeit-Prüfung verwendet, sollten unbedingt alle Hyper-V-Ressourcen vom Scan ausgenommen werden, um Fehlalarme (Ausfälle von Gästen) und Performance-Einbußen zu vermeiden. Ein Virenschutz dieser Ressourcen muss durch Anti-Virus-Scanner in den Gastsystemen realisiert werden.

Für die Dekommissionierung von Gastsystemen sollten Tools zur sicheren Löschung der VHD-Dateien vorgehalten werden (siehe M 2.433 *Überblick über Methoden zur Löschung und Vernichtung von Daten*).

**Hyper-V-Konfiguration**

Standardmäßig gibt es keine Limits für die CPU-Nutzung der Gäste, die sich denselben Kern teilen. Ohne Limits auf die CPU-Nutzung können einzelne Gäste Störungen anderer Dienste verursachen, indem sie die insgesamt verfügbare Rechenkapazität vollständig ausnutzen. Da die CPU-Anforderungen nicht immer vollständig im Voraus bekannt sind, sollte die CPU-Last der Gäste einem durchgängigen Monitoring unterliegen.

Mit Hyper-V lassen sich für die CPU-Nutzung Limits setzen (feste Grenze) oder Prioritäten einteilen (relative Gewichtung). Beide Möglichkeiten können nicht das "Aushungern" eines Systems vermeiden; dies ist nur durch das Setzen einer absoluten Reserve (*Virtual Machine Reserve*) möglich. Für kritische Services sollte diese Option genutzt werden.

Bei Host-Systemen mit vielen CPUs/Kernen ist diese Problematik weniger ausgeprägt, da eine implizite Einschränkung über die Zahl der virtuellen CPUs pro VM existiert.

Um eine ausreichende Trennung der Gäste sicherzustellen, muss bei der Konfiguration darauf geachtet werden, keine Überschneidungen im Zugriff für physische Ressourcen zuzulassen. Es darf keinen gemeinsamen Zugriff auf virtuelle Speichermedien (Virtual Hard Disks/VHDs) oder physische Devices des Hosts (USB-Stick, DVD-Laufwerk) geben.

Bei einer Serversicherung über den Hyper-V VSS Writer wird die Konfiguration des virtuellen Netzes und der virtuellen Netzkomponenten nicht mitgesichert. Die Netz-Konfiguration sollte daher so dokumentiert werden, dass im Notfall eine Wiederherstellung aus der Dokumentation möglich ist.

**Berechtigungen**

Häufig sollen die Administratoren der Gastsysteme ihre IT-Systeme selbstständig herunter- und hochfahren und auf die Konsole zugreifen können, ohne dabei Einfluss auf andere Systeme und Netze zu haben (siehe M 2.446 *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*).

Um dies umzusetzen, dürfen für Hyper-V im Autorisierungs-Manager nur Berechtigungen für folgende Vorgänge vergeben werden:

- Keine Berechtigungen für Hyper-V-Service- und Netzwerk-Vorgänge außer "Read"-Vorgänge
- Für VM-Operationen keine Berechtigungen außer:

Alle weiteren Berechtigungen können die Trennung zwischen den Systemen beeinträchtigen und benötigen eine auf die spezifische Umgebung angepasste Sicherheitsbetrachtung.

**Gastsystemkonfiguration**

Die Maßnahme M 4.348 *Zeitsynchronisation in virtuellen IT-Systemen* fordert die Zeitsynchronisation der Gäste, um die durch die Virtualisierung erzeugte lastabhängige Drift auszugleichen. Ohne eine Zeitsynchronisation sind die Gastsysteme auf die Timer-Interrupts der virtuellen CPU angewiesen. Damit laufen die Uhren der VM mit steigender Last anderer Systeme ungenauer. Für Hyper-V kommt die Problematik des Supports verschiedener Zeitzonen in Gästen (Windows erwartet, dass die RTC mit lokaler Zeit läuft) sowie von Suspend- und Resume-Events hinzu. Werden Snapshots reaktiviert, zum Beispiel nach dem Bewegen einer VM auf einen anderen Server, läuft das Gastsystem

mit einer falschen Uhrzeit und benötigt mitunter lange, um sich aus einer externen Quelle neu zu synchronisieren. Um die Synchronisation zu ermöglichen, bietet Microsoft einen Synchronisierungsservice als Teil der "Hyper-V Integration Services" an, der im Gastsystem installiert werden muss. Über diesen Dienst wird die Systemzeit des Gastes mit der Uhr des Host-Systems abgeglichen; außerdem werden bei virtualisierungsbedingten Zeitsprüngen (Suspend/Resume) die Uhren sofort korrigiert. Das Hostsystem sollte sich dabei mit einer zuverlässigen Netzzeit synchronisieren (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*).

Probleme können auftreten, wenn Hostsysteme oder Gäste Mitglieder von Domänen oder gar von unterschiedlichen Domänen sind. Dann werden die Uhren gleichzeitig über das Netz und lokal korrigiert. Dies führt zu häufigen geringen Abweichungen. Insbesondere bei Active Directory-Servern als Gastsystem kann dies zu Problemen mit der Replikation führen. In diesem Fall sollte die Synchronisation mit dem Host deaktiviert werden. Dabei geht allerdings die Fähigkeit verloren, nach einem Wiederanlauf der virtuellen Maschine schnell die ursprüngliche Zeit wiederherzustellen.

Es ist möglich, auf einem Windows-Gast die Synchronisierung bei installierten "Integration Services" mit dem Host nur teilweise zu deaktivieren, ohne das Setzen der Zeit nach dem Boot und bei Suspend-/Resume-Ereignissen zu beeinflussen. Dazu dient das Kommando

reg add HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\VMICTimeProvider /v Enabled /t reg_dword /d 0

Anschließend muss im Gast eine externe Zeitquelle konfiguriert werden.

Wann immer mit einer externen Zeitquelle synchronisiert wird, sollte ein relativ kurzes Synchronisierungsintervall gewählt werden (alle 10-20 Minuten), um die situationsbedingt hohe Drift kompensieren zu können.

Prüffragen:

- Ist die Management-Instanz des Hyper-V-Servers als minimales System ausgelegt (durch den Einsatz von Server Core) bzw. mit einer SSLF-Baseline gehärtet?
- Werden keine weiteren Dienste durch die Hyper-V-Management-Instanz angeboten?
- Sind Hyper-V-Ressourcen vom Virenscan ausgenommen?
- Sind die CPU-Anforderungen von kritischen Diensten in Hyper-V-Systemen in ausreichende CPU-Reservierungen umgesetzt worden?
- Wird die virtuelle Netzwerk-Konfiguration von Hyper-V separat gesichert und dokumentiert?
- Sind physische Speichermedien (für den direkten Zugriff) jeweils nur einer einzigen VM unter Hyper-V zugeordnet?

# M 4.414 Überblick über Neuerungen für Active Directory ab Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

### Grundsätzliches

Das mit Windows 2000 Server eingeführte Active Directory stellt unter Windows Server 2008 und Windows 7 die elementare Basis der Benutzer- und Objektverwaltung dar. Trotz der teilweise erheblichen Neuerungen, die ein Domänen-Controller unter Windows Server 2008 bietet, bleiben wesentliche Anforderungen an die Planung und Konfiguration des Active Directory erhalten (siehe M 2.230 *Planung der Active Directory-Administration* und M 2.231 *Planung der Gruppenrichtlinien unter Windows*). Bedingt durch die grundsätzlichen Möglichkeiten, die verschiedenen Rollen des Active Directory zu trennen oder einen sogenannten *Read-Only Domain Controllers* (RDOC) einzusetzen, kommt der Planungsphase unter Windows Server 2008 und seinem Active Directory jedoch eine verstärkte Bedeutung zu.

### Neuerungen ab Windows Server 2008

Neben dem zentralen Dienst des Active Directory, den sogenannten Active Directory-Domänendiensten (*Active Directory Domain Services, AD DS*), sind vier weitere Active Directory-Dienste als Rolle installierbar:

- Active Directory-Zertifikatsdienste (*Active Directory Certificate Services, AD CS*). In diesem Einsatzszenario dient das Active Directory der Veröffentlichung von Zertifikaten im Rahmen einer Public-Key-Infrastruktur (PKI). Die Zertifikatsdienste waren bereits in früheren Windows-Server-Versionen vorhanden, allerdings ohne den Namenszusatz *Active Directory.*
- Active Directory-Verbunddienste (*Active Directory Federation Services, AD FS*). Dieser Dienst wurde mit Windows Server 2008 R2 eingeführt. Er sorgt für die Authentisierung von Benutzern, die nicht Mitglied des Active Directory sind. Ein gängiger Anwendungsfall ist die Authentisierung von Benutzern von Webanwendungen.
- Active Directory Lightweight Directory Services (*AD LDS*), frühere Bezeichnung: Active Directory-Anwendungsmodus (*Active Directory Application Mode, ADAM*). Dieser Dienst stellt einen LDAP-Server als Daten-Repository für verzeichnisdienstfähige Anwendungen bereit. Dabei entfällt gegenüber den anderen Szenarien der Verwaltungsaufwand für Domänen und Gesamtstrukturen. Für jede AD LDS-Instanz wird ein eigenes Schema verwaltet.
- Active Directory-Rechteverwaltungsdienste (*Active Directory Rights Management Services, AD RMS*). Der AD-RMS-Dienst bietet Schutz von Daten und Dateien über eine zentral gesteuerte Verschlüsselung.

Diese Dienste sind jeweils als einzelne Rolle auswählbar und können auf einem dedizierten System installiert werden.

### Weitere grundsätzliche Neuerungen

Eine der wesentlichen Neuerungen des Windows Server 2008 ist die Einführung des sogenannten Read-Only Domain Controllers (*RODC*). Dieses Server-System stellt einen Domänen-Controller dar, der ausschließlich Lesezu-

griff auf den Verzeichnisdienst gewährt. Geeignet ist der RODC für Systeme, auf die der physische Zugriff durch große Benutzerkreise nicht verhindert werden kann, zum Beispiel weil die Aufstellung des Systems in einer gesicherten RZ-Umgebung nicht möglich ist. Unterschiede zum normalen Domain Controller sind:

- Manipulationen an exponierten RODC werden nicht repliziert (unidirektionale Replikation), zum Beispiel sind dies:
  - Änderungen am AD-Schema
  - Änderungen an der DNS-Datenbank
  - Die Administration des Servers ist trennbar von Domänenadministrationsrechten.
- Allerdings birgt der Betrieb eines RODC auch potenzielle Nachteile, die beachtet werden müssen:
- Es entsteht eine hohe Abhängigkeit von einem vollwertigen Domänen-Controller, da nur durch diesen neue Objekte im Active Directory angelegt werden können.
- Gegebenenfalls treten bei der AD-Integration von Drittprodukten mit einem RDOC Kompatibilitätsprobleme auf. Es entsteht ein erhöhter Testaufwand.
- Es muss eine angemessene Strategie zur lokalen Zwischenspeicherung von Benutzer-Passwörtern entwickelt werden, da grundsätzlich alle zwischengespeicherten Passwörter bei einem Verlust des Systems ausgelesen werden können. Insbesondere für die Konten von Domänen-Administratoren gilt es zu überlegen, ob die Zwischenspeicherung unterbunden wird. In diesem Fall muss für die Anmeldung dieser Gruppe an einem RODC die Verbindung zu einem vollwertigen Domänen-Controller zur Verfügung stehen.

Neu sind auch die sogenannten *Verwalteten Dienstkonten*, die mit Windows Server 2008 R2 eingeführt wurden. Damit ist eine zentrale Verwaltung von Dienstkonten über das Active Directory möglich (siehe M 4.284 *Umgang mit Diensten ab Windows Server 2003*).

Mit den *granularen Kennwort- und Kontosperrungsrichtlinien* besteht nun die Möglichkeit, abgestufte Passwort-Richtlinien innerhalb einer Domäne zu nutzen (siehe M 4.48 *Passwortschutz unter Windows-Systemen*).

Weitere grundlegende Neuerungen des Active Directory ab Windows Server 2008 R2 sind:

- Active Directory-Papierkorb: Versehentlich gelöschte Objekte innerhalb des Active Directory können durch die Funktion des Papierkorbs wiederhergestellt werden.
- Active Directory-Verwaltungscenter: Zentrales, auf der PowerShell basierendes Management-Tool mit erweiterten Optionen zur Verwaltung des Active Directory. Es ist zu beachten, dass das Active Directory-Verwaltungscenter keinen vollständigen Ersatz des Management-Tools *Active Directory-Benutzer und -Computer* darstellt, da teilweise unterschiedliche Funktionen implementiert sind.
- Active Directory Best Practice Analyzer: Tool zur Analyse der effektiven Active Directory-Einstellungen. Die Ergebnisse des Best Practice Analyzers können als Basis zur Fehlerbehebung verwendet werden.
- Active Directory-Webdienste: Dieser neu eingeführte Dienst stellt eine Webdienst-Schnittstelle für Active Directory-Domänen dar. Er wird in der Regel von Anwendungen genutzt, die einen Zugriff auf das Active Directory über HTTP(S) ermöglichen.

- Offline-Domänenbeitritt: Systeme können ohne Verbindung zur Domäne vorab aufgenommen werden. Die jeweiligen Computer werden dann beim ersten Starten der Domäne zugefügt.
- Active Directory Management Pack: Dient zur Zustands-Überwachung der zentralen AD-Dienste (*Active Directory Domain Services, AD DS*).

# M 4.415 Sicherer Betrieb der biometrischen Authentisierung unter Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ab Windows Server 2008 R2 und Windows 7 unterstützt Windows standardmäßig eine biometrische Authentisierung mit Fingerabdrücken. Dafür wurde das Windows Biometric Framework (WBF) entwickelt und in das Betriebssystem integriert. Mit dem WBF können die Hersteller von Biometrie-Lösungen ihre Sensoren und Algorithmen in das Betriebssystem einbinden und biometrisch erfasste Daten sicher hinterlegen. Mit dem WBF wird die Systemsteuerung entsprechend um ein Element Biometrische Geräte erweitert, sofern Windows einen Fingerabdruckleser am System erkennt.

Zunächst unterstützt Windows dabei die Nutzung von Fingerabdrucklesern für die folgenden Zwecke:

- Biometrische Authentisierung für den Zugang zum Betriebssystem oder zur Domäne (Windows-Anmeldung)
- Biometrische Authentisierung zur Rechteerhöhung für die Benutzerkontensteuerung (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*)
- Zugriff auf biometrische Funktionen aus Anwendungen heraus durch Bereitstellung einer einheitlichen Schnittstelle

Ob die Domänenanmeldung mit biometrischer Authentisierung zugelassen wird, kann über ein Gruppenrichtlinienobjekt vorgegeben werden. Dieses sollte nach Möglichkeit genutzt werden, um eine einheitliche, sichere Konfiguration für alle Geräte in der Domäne durchzusetzen. Die Nutzung der biometrischen Authentisierung für Gast-Konten oder das vordefinierte Konto "Administrator" ist nicht möglich.

Die Motivation für den Einsatz von Fingerabdrucklesern besteht oft vorrangig in der einfacheren Authentisierung für die Benutzer. Die üblicherweise in Laptops verbauten Fingerabdruckleser haben sich dabei in Tests immer wieder als nur eingeschränkt zuverlässig erwiesen. Je nach Modell ist ein "Kopieren" von fremden Fingerabdrücken mit mehr oder weniger technischem Aufwand machbar. Für Systeme mit erhöhtem Schutzbedarf ist deshalb sorgfältig zu prüfen, ob das Sicherheitsniveau der konkret verwendeten Geräte ausreichend ist, wenn die Authentisierung ausschließlich über Fingerabdruck-Erkennung erfolgen soll. Beim Einsatz anderer biometrischer Verfahren sollte die Zuverlässigkeit der Erkennung vorab bewertet und dem Schutzbedarf der betroffenen Systeme und Anwendungen gegenübergestellt werden. Für Systeme mit hohem und sehr hohem Schutzbedarf ist heute in der Regel eine Authentisierung, die auf Chipkarten oder Token basiert, den verfügbaren biometrischen Verfahren überlegen.

Wichtig bei der Planung des Einsatzes ist auch, Möglichkeiten zum Systemzugang vorzusehen, falls der biometrisch erfasste Fingerabdruck nicht zur Verfügung steht, beispielsweise durch eine Verletzung am Finger. Windows erlaubt hier die Erfassung mehrerer Finger, die alternativ genutzt werden können. Zusätzlich sollte ein Zugang mit einem sicheren zentral hinterlegten Passwort als Rückfalllösung eingerichtet werden.

Prüffragen:

- Wurde der Einsatz der biometrischen Authentisierung anhand des Schutzbedarfs der betroffenen Systeme und Anwendungen abgewogen?
- Wird die Zulässigkeit der biometrischen Authentisierung über Gruppenrichtlinien gesteuert?
- Sind Ersatzverfahren für den Systemzugang verfügbar, wenn keine biometrische Authentisierung erfolgen kann?

# M 4.416 Einsatz von Windows Server Core

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Ab Windows Server 2008 kann das Betriebssystem als "Server Core" installiert werden. Der Server Core stellt ein minimales, weitgehend ohne graphische Oberfläche auskommendes System dar. Konfigurationen am System selbst sind ausschließlich über die Kommandozeile oder unter Windows Server 2008 R2 mit der PowerShell möglich, soweit dieses Feature installiert ist.

Die Vorteile eines Server Core sind:

- Die Angriffsfläche des Systems wird erheblich reduziert (weniger Software bedeutet weniger relevante Schwachstellen).
- Es müssen weniger Patches eingespielt werden. Dadurch entstehen geringere Ausfallzeiten durch die Softwarewartung.

In bestimmten Fällen wie beim Einsatz als Hyper-V ist auch der geringere Ressourcenverbrauch vorteilhaft.

Eine Server Core-Installation sollte für alle Serverdienste in Betracht gezogen werden, wenn wohldefinierte und zentrale Infrastrukturdienste aufgesetzt werden oder wenn ein höherer Schutzbedarf absehbar ist.

Da keine direkte Migration zwischen einer Vollinstallation und Server Core möglich ist, muss bereits in der Planungsphase geklärt werden, ob Server Core eingesetzt werden soll und ob bestimmte Features benötigt werden. Besonderes Augenmerk sollte auch auf die Art der Administration gelegt werden.

Die Administratoren eines Server Core müssen ausreichend geschult sein, um den Server über die verfügbaren Werkzeuge auf der Kommandozeile zu administrieren.

Die fehlenden interaktiven lokalen Administrationsoptionen werden meist durch die generischen Remote-Administrationsmöglichkeiten (Server-Manager, MMC) oder anwendungsspezifische Remote-Management-Möglichkeiten aufgewogen. Die Anwendbarkeit bestehender Administrationstools sollte vorab geprüft werden.

Auf einem Server Core sind nicht alle Rollen oder Features installierbar, es werden nur spezifische Rollen unterstützt. Die in der Praxis größte Einschränkung liegt in der fehlenden Unterstützung von .NET (kein "Managed Code") in der Standard-Installation.

Das Hauptaugenmerk bei den unterstützten Server-Rollen liegt daher bei "einfachen" Diensten wie

- Active Directory Certificate Services,
- Active Directory Domänendienste,
- Active Directory Lightweight Directory Services (AD-LDS),
- DHCP-Server, DNS-Server,
- Dateidienste, Druckdienste,
- Hyper-V,
- Streaming-Media-Dienste und
- Web-Server.

Da sich nicht jede Software auf dem Server Core nutzen lässt, ist ein ausreichender Test der einzusetzenden Software auf dieser Konfiguration unerlässlich.

Prüffragen:

- Wurde für den Betrieb von Infrastrukturdiensten oder für Server mit erhöhtem Schutzbedarf geprüft, ob der Server als Server Core betrieben werden kann?
- Ist das Administrationspersonal für die kommandozeilenbasierte Administration ausreichend geschult?
- Sind alle auf dem Windows Server Core benötigten Software-Komponenten ausreichend in dieser Umgebung getestet worden?

# M 4.417 Patch-Management mit WSUS ab Windows Server 2008

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die *Windows Server Update Services* (WSUS) sind ein Dienst, der von Microsoft bereitgestellte Patches, Updates und Service-Packs über das Internet bezieht und weiteren Systemen in der Domäne zur Verfügung stellt. Durch den gebündelten Download wird einerseits die Netzanbindung der Institution entlastet, andererseits lässt sich das Patch-Management für Microsoft-Betriebssysteme bedarfsgerecht automatisieren. Die zeitnahe Verteilung wichtiger Sicherheitspatches wird dadurch deutlich erleichtert. Angesichts laufend neuer bekannt gewordener Software-Schwachstellen stellt das Patch-Management eine der wichtigsten technischen Sicherheitsmaßnahmen dar (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Alle Windows-Systeme im Informationsverbund sollten daher an einen entsprechenden Update-Service angeschlossen sein.

Während WSUS bei Windows Server 2003 und 2008 nur als Zusatzmodul verfügbar waren, sind sie ab Windows Server 2008 R2 als Server-Rolle enthalten. WSUS setzt dabei das Vorhandensein eines Internet Information Servers (Server-Rolle Web-Server) auf dem Server voraus. Zusätzlich müssen ausreichend Festplattenplatz für das Zwischenspeichern der Updates sowie eine Datenbank für die Verwaltungsinformationen vorhanden sein. Falls kein geeigneter MS-SQL-Server zur Verfügung steht, kann als Datenbank auch eine Instanz der Windows Internal Database auf dem Serversystem gewählt werden. Für die Auswertung und Überwachung der WSUS-Aktivitäten muss zusätzlich das Paket *Report Viewer Redistributable* installiert werden.

In komplexeren Informationsverbünden ist es möglich, mehrere WSUS-Server parallel oder "in Reihe" zu betreiben, um beispielsweise verschiedene Standorte zu versorgen. Jeder WSUS-Server lädt dabei in definierbaren Abständen relevante Updates von seiner Quelle (entweder von Microsoft oder einem anderen vorgeschalteten WSUS-Server) herunter. Der in der Hierarchie ganz oben stehende WSUS-Server benötigt dazu eine Verbindung mit dem Internet, die jedoch auch über einen WWW-Proxy mit oder ohne Authentisierung realisiert werden kann.

Jedes Update muss nach dem Herunterladen für die Installation freigegeben werden. Das kann entweder manuell durch einen Administrator erfolgen, oder durch eine Regel definiert sein. Regeln sollten für sogenannte *WSUS-Computergruppen* unterschiedlich definiert sein, so dass beispielsweise kritische Sicherheits-Updates auf Clients automatisch installiert werden, Server-Systeme mit kritischen Anwendungen hingegen eine manuelle Administrator-Freigabe benötigen. Für jede definierte Gruppe ist eine Abwägung zwischen der schnellen Wirksamkeit von automatisch eingespielten Sicherheits-Patches und der Gefährdung der Systemstabilität durch fehlende Tests zu treffen.

Die übrigen Systeme in der Domäne werden über Gruppenrichtlinien für den Zugriff auf den WSUS-Server konfiguriert. Dabei können den Systemen nicht nur der "zuständige" WSUS-Server bekannt gemacht, sondern auch weitere Konfigurationseinstellungen wie die Intervalle zur Prüfung auf vorliegende Updates vorgenommen werden. Die so konfigurierten Systeme fragen dann bei ihrem WSUS-Server regelmäßig an, ob relevante Updates zur Installation vorliegen (*Pull-Mechanismus*). Der WSUS-Server ermittelt aus der Anfrage das

auf dem jeweiligen System vorhandene Windows-Betriebssystem und identifiziert die dazu vorliegenden Aktualisierungen und ihren jeweiligen Genehmigungsstatus.

WSUS wird über eine Verwaltungskonsole konfiguriert, die nicht auf dem WSUS-Server selbst laufen muss, sie kann auch von einem Administrations-PC aus aufgerufen werden. In jedem Fall sollte der Zugriff auf die Verwaltungskonsole des WSUS-Servers auf einen kleinen Kreis berechtigter Administratoren beschränkt werden.

Mit dem Paket *Report Viewer Redistributable* stehen in der Verwaltungskonsole unter *Berichte* verschiedene Auswertungen zum Patch-Status der angeschlossenen Systeme zur Verfügung. Hier kann unter anderem ermittelt werden, wann sich die einzelnen Systeme das letzte mal über den WSUS-Server aktualisiert haben und welche Updates und Patches jeweils schon eingespielt sind. Gerade bei besonders kritischen Schwachstellen lässt sich so das Ausrollen der entsprechenden Patches nachhalten und verfolgen.

Prüffragen:

- Ist für alle Windows-Systeme im Informationsverbund ein WSUS-Server konfiguriert?
- Hat der WSUS-Server Zugriff auf das Internet oder einen anderen WSUS-Server als Quelle für Updates?
- Ist der Zugriff auf die Verwaltungskonsole des WSUS-Servers auf einen kleinen Kreis berechtigter Administratoren beschränkt?
- Verfügt der WSUS-Server über genügend Speicherplatz zum Zwischenspeichern der anstehenden Updates?
- Sind geeignete WSUS-Computergruppen und Richtlinien für die Freigabe von Patches, Updates und Service Packs definiert?
- Wird eine Abwägung zwischen der schnellen Wirksamkeit von automatisch eingespielten Sicherheits-Patches und der Gefährdung der Systemstabilität durch fehlende Tests getroffen?

# M 4.418 Planung des Einsatzes von Windows Server 2008

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Durch die verstärkte Unterscheidung von Rollen während der Installationsphase kommt der Planungsphase vor dem Einsatz eines Windows Server 2008 eine noch höhere Bedeutung zu, als dies bei früheren Windows-Versionen der Fall war. Beispielsweise kann die Rolle des Server Core nur während der Installation ausgewählt werden, eine nachträgliche Änderung ist für diese Rolle nicht möglich. Daher müssen die ausgewählten Rollen und Features genau an die Anforderungen des geplanten Einsatzes des Windows Server 2008-Systems angepasst werden.

Aufbauend auf M 2.315 *Planung des Servereinsatzes* und M 4.409 *Beschaffung von Windows Server 2008* beschreibt die folgende Maßnahme die wesentlichen zu beachtenden Aspekte der Planungsphase vor dem Einsatz eines Windows Server 2008.

**Erstellung eines Grobkonzept**

Die Planung eines Windows Server 2008 erfolgt in mehreren Schritten.

Die konkrete Planung kann nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifischen Teilkonzepten festgelegt. Im Grobkonzept werden beispielsweise folgende typische Fragestellungen behandelt:

- Wird ein neues Netz aufgebaut oder wird ein bestehendes Netz migriert?
- Soll ein existierendes Windows-Netz beispielsweise basierend auf Windows 2000 Server oder Windows Server 2003 vollständig oder nur teilweise nach Windows Server 2008 migriert werden? Eine Migration von Windows NT-Systemen auf Windows Server 2008-Systeme ist nicht direkt möglich.
- Handelt es sich um einen zusätzlichen einzuführenden Server oder um das Upgrade eines existierenden Servers?
- Welche Komponenten wie Dateiserver, Druckserver oder DNS-Server werden ersetzt, welche bleiben erhalten?
- Müssen existierende Verfahren oder Komponenten, wie ein bestehendes Kerberos-System oder auch eine bestehende PKI in Windows Server 2008 integriert werden? Hier sind unter anderem die Interoperabilität mit anderen IT-Systemen sowie der angebotene Funktionsumfang zu berücksichtigen.
- Wird die geplante Konfiguration des Servers der zu erwartenden Datenmenge und Spitzenlast gerecht?
- Ist das Lizenzierungsmodell ausreichend und geeignet für das Bereitstellungskonzept und das Notfallkonzept?
- Ist ein Mischbetrieb von Windows Server 2008 und anderen Betriebssystemen, wie Windows 2000 oder 2003, Novell oder Unix notwendig? Das kann Einfluss auf die im System verwendeten Authentisierungsverfahren haben, die abhängig von den eingesetzten Betriebssystemen auch Schwachstellen aufweisen können und damit die Sicherheit der Windows Server 2008-Umgebung insgesamt herabsetzen. Die notwendigen Sicherheitsvorgaben für eine solche Mischumgebung sollten in einer Sicherheitsrichtlinie festgelegt sein.

**Auswahl der Rollen und Features**

Mit Windows Server 2003 R2 hat Microsoft die sogenannten Server-Rollen eingeführt.

Es handelt sich um Anwendungen, die entweder nachinstalliert werden können, oder, wie der Server Core, bei der Installation festgelegt werden müssen. Bis Windows Server 2003 wurden Anwendungen wie der Internet Information Services (IIS) oder andere Basisdienste wie Druck- oder Dateidienste als Standard mitinstalliert.

Ein neu installierter Windows Server 2008 hingegen besitzt nach erfolgter Installation noch keine zu erfüllende Rolle oder Funktion. Diese müssen explizit durch den Administrator pro System zugewiesen und konfiguriert werden.

Neben den Rollen existieren noch sogenannte *Features.* Sie stellen in der Regel eine Erweiterung einer bestehenden Rolle dar, können aber auch, wie der WINS-Dienst, eine vollständig eigene Funktionen darstellen.

Das Zusammenspiel aus einer minimalen Basisinstallation und gezielt ausgewählten Rollen und Features stellt eine erhebliche Verbesserung der Sicherheit dar, weil damit auf allen Systemen die Möglichkeit besteht, nur die tatsächlich benötigten Funktionen zu installieren. Die Notwendigkeit, vorhandene, nicht benötigte Funktionen oder Dienste wieder zu deinstallieren, entfällt.

Installation und Konfiguration der Server-Rollen oder der Features erfolgt üblicherweise über den *Server-Manager*. Dieser stellt das zentrale Management-Tool eines Windows Server 2008 dar (siehe M 1.1 *Einhaltung einschlägiger Normen und Vorschriften*).

Auf einem Windows Server 2008 R2 stehen siebzehn verschiedene Rollen zur Auswahl bereit. Die folgende Tabelle zeigt eine Übersicht dieser Rollen und die Verfügbarkeit der jeweiligen Rolle pro Edition.

| **Serverrolle** | **Enterprise** | **Datacenter** | **Standard** | **Web** | **Itanium** | **Foundation** |
|---|---|---|---|---|---|---|
| Active Directory-Zertifikatdienste | Ja | Ja | Begrenzt | Nein | Nein | Begrenzt |
| Active Directory-Domänendienste | Ja | Ja | Ja | Nein | Nein | Ja |
| Active Directory Federation Services | Ja | Ja | Ja | Nein | Nein | Nein |
| Active Directory Lightweight Di- | Ja | Ja | Ja | Nein | Nein | Ja |

| Server-rolle | Enterprise | Datacenter | Standard | Web | Itanium | Foundation |
|---|---|---|---|---|---|---|
| rectory Services | | | | | | |
| Active Directory-Rechteverwaltungs-dienste | Ja | Ja | Ja | Nein | Nein | Ja |
| Anwendungsserver | Ja | Ja | Ja | Nein | Ja | Ja |
| DHCP-Server | Ja | Ja | Ja | Nein | Nein | Ja |
| DNS-Server | Ja | Ja | Ja | Ja | Nein | Ja |
| Faxserver | Ja | Ja | Ja | Nein | Nein | Ja |
| Dateidienste | Ja | Ja | Begrenzt | Nein | Nein | Begrenzt |
| Hyper-V | Ja | Ja | Ja | Nein | Nein | Nein |
| Netzwerkrichtlinien- und Zugriffsdienste | Ja | Ja | Begrenzt | Nein | Nein | Begrenzt |
| Druck- und Dokumentdienste | Ja | Ja | Ja | Nein | Nein | Ja |
| Remotedesktop-dienste | Ja | Ja | Begrenzt | Nein | Nein | Begrenzt |
| Webdienste (IIS) | Ja | Ja | Ja | Ja | Ja | Ja |
| Windows-Bereitstellungs-dienste | Ja | Ja | Ja | Nein | Nein | Ja |
| Windows Server Update Services (WSUS) | Ja | Ja | Ja | Nein | Nein | Ja |

**Abhängigkeiten zwischen Server und Client**

**Zusammenspiel von Windows Server 2008 (R2), Windows Vista und Windows 7**

Grundsätzlich können alle Kombinationen der von Microsoft freigegebenen und unterstützten Server- und Client-Systeme innerhalb einer Windows-Domäne eingesetzt werden.

Allerdings ist zu beachten, dass die vollständige Nutzung aller Funktionen, insbesondere für neu eingeführte Gruppenrichtlinienobjekte, nur im Zusammenspiel mit dem jeweiligen korrespondierenden Client-System möglich ist. Als korrespondierende Server-Client-Kombinationen können zum Beispiel Windows Server 2008 und Windows Vista oder Windows Server 2008 R2 und Windows 7 genannt werden.

Beispiele für nutzbaren Funktionen, die ausschließlich in der Kombination Windows Server 2008 R2 und Windows 7 zur Verfügung stehen, sind unter anderem:

- DirectAccess: Der Aufbau der VPN-Verbindungen mit DirectAccess ist nur über die Kombination Windows Server 2008 R2 und Windows 7 möglich. Gleiches gilt für die sogenannte Funktion des *VPN-Reconnect*.
- BranchCache: Diese Windows 7-Client-Funktion ermöglichst es, den WAN-Verkehr in Außenstellen zu minimieren.
- Remotedesktopdienste: Die neuen Funktionen der ehemals als Terminaldienste bekannten Serverrolle eines Windows Server 2008 R2 können nur durch Windows 7-Client-Systeme vollständig genutzt werden.

Es kann davon ausgegangen werden, dass mit der Einführung weiterer Releases oder Service-Packs neue Funktionen hinzukommen. Dies gilt erst recht für die Einführung neuer Server- oder Client-Systeme.

Prüffragen:

- Wurde die Konfiguration des Windows Server 2008-Systems unter Berücksichtigung aller relevanten Rahmenbedingungen sorgfältig geplant?
- Entsprechen die ausgewählten Rollen und Features den Anforderungen an den geplanten Einsatz des Windows-Server-2008-Systems?
- Wurden die Restriktionen vorhandener, älterer Systeme oder die Besonderheiten eines Mischbetriebs in den Planungen für einen Windows Server 2008 ausreichend berücksichtigt?

# M 4.419 Anwendungssteuerung ab Windows 7 mit AppLocker

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

### Softwarekonfiguration und Installation

Die Softwarekonfiguration eines Clients weicht in manchen Fällen bereits kurz nach der Bereitstellung von der vorgegebenen Standardkonfiguration ab, sofern dies nicht technisch verhindert wird. Diese Abweichungen nehmen in der Regel zu, je länger der Client in Betrieb ist. Die Ursache dafür sind Installationen durch die Endbenutzer, die nicht den Standard-Änderungsmanagementprozess durchlaufen. Dabei kann es sich um nützliche Werkzeuge für die tägliche Arbeit handeln. Es wird aber auch oft Software installiert, die nichts mit dem Regelbetrieb zu tun hat. In beiden Fällen sollte jedoch der definierte Änderungsmanagementprozess durchlaufen werden.

Durch die Installation dieser zusätzlichen Software verliert ein Administrator schnell den Überblick über die aktuelle Softwarekonfiguration auf den Clients. Dies kann dazu führen, dass eventuell auftretende Fehler für einen Administrator nicht mehr nachvollziehbar sind. Gravierender ist jedoch die Tatsache, dass die zusätzlich installierte Software nicht durch das Patch- und Änderungsmanagement abgedeckt wird (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). So können Sicherheitslücken in der Software von Angreifern ausgenutzt werden, um beispielsweise Schadcode auf den Clients einzuschleusen und auszuführen.

Auch auf Server-Systemen darf Software nicht unkontrolliert installiert werden. Wenn beispielsweise ein Backup-Administrator bestimmte Tools einsetzen will, sollte er diese nicht einfach installieren, sondern über den Änderungsmanagementprozess einbringen. So wird die Installation dokumentiert und die Tools werden in das Patch-Management einbezogen.

### AppLocker

Das mit Windows 7 (nur Versionen Enterprise und Ultimate) und Windows Server 2008 R2 eingeführte Feature AppLocker hilft dem Administrator, die Kontrolle über die Systeme zu behalten, indem es die unautorisierte Installation und Ausführung von Software durch andere Benutzer technisch verhindert. Unter Windows 7 Professional kann AppLocker die gestarteten Anwendungen protokollieren, nicht jedoch Ausführungsregeln erzwingen.

AppLocker sollte zum Schutz der Systemintegrität eingesetzt werden.

AppLocker ist die Weiterentwicklung der Softwareeinschränkungsrichtlinien (Software Restriction Policies, SRP), die in den Betriebssystemen Microsoft Windows XP, Vista und Server 2003 eingesetzt werden (siehe M 4.286 *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003*). Bei der Konfiguration dieser Richtlinien muss der Administrator jedoch für jede Software und jede notwendige Aktualisierung eine eigene Regel erstellen. Dies kann zu einem hohen Verwaltungsaufwand führen.

AppLocker bietet Administratoren im Gegensatz zu den Softwareeinschränkungsrichtlinien flexiblere Möglichkeiten, Richtlinien für die Softwaresteuerung zu definieren, die den Anforderungen der Institution gerecht werden. Beispiele hierfür sind die enthaltenen Assistenten und Regelerstellungstools, mit deren

Hilfe Regeln automatisch erstellt werden können. Sie sollten benutzt werden, um beispielsweise die Standardregeln, die die Ausführung von wichtigen Systemdateien erlauben, zu definieren. Die schrittweisen Anleitungen und die integrierte Hilfe unterstützen den Administrator zusätzlich bei der Konfiguration benutzerdefinierter Regeln. Ergänzend zu den Standardregeln sollten Richtlinien für ausführbare Dateien, Installationsprogramme, Skripte und DLLs definiert werden. Die Richtlinien sind separat konfigurierbar und bieten einen besseren Schutz der Systeme, da sie nicht ausschließlich auf ausführbare Dateien beschränkt sind.

**Regeln**

Es gibt drei Regeltypen: Zulassen, Verweigern und Ausnahme. Damit können Regeln definiert werden, die die Ausführung der in der Institution definierten Standardsoftware erlauben (Positivliste), oder die Ausführung bekannter Schadprogramme verweigern (Negativliste). Es sollte der Ansatz gewählt werden, alle Anwendungen zu verbieten, und nur die Installation und Ausführung von Software aus der Positivliste zu erlauben. So wird verhindert, dass Software, die noch nicht in die Negativliste aufgenommen wurde, installiert und ausgeführt werden kann.

Die Standardregeln werten den Datei- oder Ordnerpfad oder einen Hashwert über die ausführbare Datei ("Dateihash") der Software aus. Zusätzlich sind Regeln auf der Grundlage von Anwendungssignaturen möglich. Folgende Aspekte sind hierbei zu beachten:

**Regeln, die auf dem Datei- oder Ordnerpfad basieren**

Wird beispielsweise eine Regel definiert, die die Ausführung aller Software unter *C:\Programme* erlaubt, kann der Schutz umgangen werden, indem eine ausführbare Datei einer gesperrten Software in diesen Ordner verschoben wird. Voraussetzung hierfür sind lokale Administrationsrechte der Endbenutzer. Dies sollte durch entsprechende Maßnahmen verhindert werden (siehe M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*).

**Regeln, die auf dem Dateihash basieren**

Ein Dateihash kann als ein kryptographischer Fingerabdruck einer Datei bezeichnet werden. Dieser Regeltyp kann eingesetzt werden, wenn eine ausführbare Datei nicht digital signiert ist. Nach jeder Softwareaktualisierung müssen der Hash erneut gebildet und die Regeln angepasst werden. Dies kann zu einem hohen Verwaltungsaufwand führen. Aus diesem Grund sind die Regeltypen, die entweder auf dem Datei- oder Ordnerpfad oder der digitalen Anwendungssignatur basieren, diesem Regeltyp vorzuziehen.

**Regeln, die auf Anwendungssignaturen basieren**

Ist die Datei elektronisch signiert, sollten Herausgeberregeln definiert werden, die auf den digitalen Anwendungssignaturen basieren. Bei dieser Methode muss sichergestellt sein, dass der Anwendungsidentitätsdienst (AppIDSvc) auf dem Client ausgeführt wird.

Bei der Nutzung von Anwendungssignaturen sollte nicht die Sicherheitsstufe "Beliebiger Herausgeber" gewählt, sondern mindestens der jeweilige Herausgeber definiert werden. Durch die zusätzliche Angabe von Attributen wie der Versionsnummer, kann die Regel weiter eingeschränkt werden. So ist zum Beispiel die Ausführung einer Anwendung ab einer bestimmten Version mög-

lich, solange sie vom Herausgeber signiert wurde. Ältere Versionen werden nicht ausgeführt, neuere Versionen hingegen automatisch zugelassen.

Verantwortlich für die Erstellung der Positiv- und Negativliste sind der Informationssicherheitsbeauftragte und der Leiter IT. Sie sollten in Gesprächen mit den Abteilungsleitern und den Endbenutzern deren jeweilige Anforderungen aufnehmen, auf Vollständigkeit prüfen und die Listen in regelmäßigen Abständen kontrollieren. Gegebenenfalls müssen Anpassungen vorgenommen werden.

**Gruppenrichtlinienverwaltung**

Die Umsetzung der Anwendungssteuerung sollte durch einen Administrator erfolgen. In einem Domänennetzwerk sollten die Regeln zentral über die Gruppenrichtlinienverwaltung konfiguriert werden. Voraussetzung ist mindestens die Domänenfunktionsebene Windows Server 2008 R2. In einer Domäne mit der Funktionsebene Windows Server 2008 R2 kann die Anwendungssteuerung mit entsprechenden Client-Verwaltungstools (beispielsweise den Remoteserver-Verwaltungstools für Windows 7 und Windows 8) konfiguriert werden.

Mit Hilfe von Gruppenrichtlinienobjekten (Group Policy Objects, GPOs) sollten verschiedene Regelsätze definiert und im Anschluss bestimmten Benutzern oder Gruppen zugeordnet werden. So kann beispielsweise festgelegt werden, dass das Verwaltungstool für die zentrale Datenbank nur von der Entwicklungsabteilung ausgeführt werden darf. Die Office Suite von Microsoft darf hingegen von allen Mitarbeitern der Institution in ihrem vollen Funktionsumfang genutzt werden.

Die nötigen Einstellungen sind im Gruppenrichtlinienverwaltungs-Editor unter *Computerkonfiguration* | *Richtlinien* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Anwendungssteuerungsrichtlinien* | *AppLocker* zu finden.

**AppLocker für Windows-Apps**

Die ab Windows 8 eingeführten Windows-Apps (Modern UI Apps) können mit AppLocker getrennt von Desktopanwendungen administriert werden. Die nötigen Einstellungen sind im Gruppenrichtlinienverwaltungs-Editor unter *Computerkonfiguration* | *Richtlinien* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Anwendungssteuerungsrichtlinien* | *AppLocker*| *App-Paketregeln* zu finden.

Eine Paketregel besteht aus den folgenden 3 Informationen:

- Herausgeber des Pakets
- Name des Pakets
- Version des Pakets

Durch das neue Design mit einer isolierten Sandbox (AppContainer) für jede Windows-App haben alle Bestandteile der Windows-App die selbe Identität und so können mit einer Regel Installation und Ausführung administriert werden.

**Protokollierung**

Versucht ein Benutzer, eine Anwendung entgegen den in AppLocker definierten Regeln zu starten, so unterbindet AppLocker die Programmausführung und dokumentiert den Vorgang durch einen Eintrag im Systemprotokoll. Um Manipulationsversuche zu erkennen und aufzuklären, muss das Systemprotokoll auch im Hinblick auf die AppLocker-Einträge regelmäßig ausgewertet

werden. Idealerweise werden die Systemprotokolle dazu auf einem zentralen Log-Server zusammengeführt und automatisiert ausgewertet.

Wenn AppLocker auf einem produktiven System neu eingeführt wird, kann es übergangsweise auch im *Überwachungsmodus* betrieben werden. In diesem Modus wird bei einer Regelverletzung die Programmausführung nicht verhindert, aber dennoch ein Protokolleintrag geschrieben. Durch die Auswertung der Protokolle können Programme identifiziert werden, die durch das Regelwerk noch nicht geeignet erfasst werden.

Prüffragen:

- Wird AppLocker zur Verhinderung der unautorisierten Installation und Ausführung von Software und Windows-Apps (ab Windows 8) auf den Clients genutzt?
- Wird bei der Nutzung von AppLocker der Ansatz der Positivliste ("Es ist alles verboten, was nicht explizit erlaubt ist") genutzt?
- Werden unter AppLocker bevorzugt Regeln auf der Grundlage von Anwendungssignaturen definierter Herausgeber eingesetzt?
- Erfolgt die Verwaltung der AppLocker-Regelsätze in einem domänenbasierten Netz mittels Gruppenrichtlinienobjekten je Benutzer/ Benutzergruppe?
- Werden die Protokolleinträge, die AppLocker bei versuchten Regelverstößen generiert, bei der Protokollauswertung der Systeme berücksichtigt?
- Werden die AppLocker-Regeln vor dem Einsatz auf einem produktiven System zunächst auf einem Testsystem oder durch den Betrieb im Überwachungsmodus erprobt?

# M 4.420 Sicherer Einsatz des Wartungscenters unter Windows 7

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Das Wartungscenter unter Windows 7 ist eine Weiterentwicklung des Sicherheitscenters. Das Sicherheitscenter wird bereits seit Windows Vista von Microsoft eingesetzt. Das Wartungscenter steht ohne Unterschied im Funktionsumfang in allen Windows 7 Editionen zur Verfügung.

Im Wartungscenter können die Sicherheitseinstellungen, Wartungseinstellungen sowie die Problembehandlung zentral überwacht und konfiguriert werden. Das Wartungscenter ist von folgenden Windows-Diensten abhängig, die bewirken, dass Probleme automatisch diagnostiziert und dem Benutzer über das Wartungscenter gemeldet werden:

- Diagnoserichtliniendienst (Diagnostic Policy Service, DPS):
  Dieser Windows-Dienst ermöglicht die Problemerkennung und Problembehebung unter Windows. Die Probleme können verschiedene Ursachen haben, zum Beispiel Speicher-, Festplatten- oder Netzprobleme. Der Dienst diagnostiziert Probleme und meldet diese anschließend dem Benutzer über das Wartungscenter.
- Diagnosediensthost (Diagnostic Service Host, WDiSvcHost):
  Dieser Windows-Dienst wird für Analysen benötigt, die als lokaler Dienst laufen müssen. Der Dienst ist direkt vom Diagnoserichtliniendienst abhängig.
- Diagnosesystemhost (Diagnostic System Host, WDiSystemHost):
  Dieser Windows-Dienst diagnostiziert, behandelt und löst Probleme, die direkt mit Windowskomponenten verbunden sind. Der Dienst ist direkt vom Diagnoserichtliniendienst abhängig.
- Windows-Fehlerberichterstattungsdienst (Windows Error Reporting Service, WerSvc):
  Der Fehlerberichterstattungsdienst sammelt Informationen zu bestehenden Problemen und stellt bereits existierende Lösungsvorschläge bereit. Des Weiteren generiert er Problemberichte, die bei Bedarf an Microsoft gesendet werden können, um weitere Lösungsmöglichkeiten zu erhalten.

Die "Problembehandlung" ist eine Sammlung von Applikationen und sammelt Informationen und Lösungsansätze zu bestehenden Problemen, die bei Windows 7 basierenden IT-Systemen auftreten können. Es wird eine Internetverbindung benötigt, um Lösungsvorschläge von Microsoft abzufragen. Weiter werden regelmäßig neue Lösungsansätze und Komponenten auf Microsoft Servern gesucht und diese heruntergeladen. Um keine institutions- oder computerspezifischen Konfigurationen an Microsoft zu senden, sollte diese Einstellung deaktiviert werden.

Beim Auftreten eines konkreten Problems werden zum Erhalt spezifischer Lösungsvorschläge auf dem Windows-Client Daten erhoben und an Microsoft gesendet. Welche Daten das im Einzelfall sind, kann den Details des Problemberichts entnommen werden. Der Problembericht enthält immer Informationen zum Betriebssystem sowie der Hard- und Software des IT-Systems. Es können auch personenbezogene Daten enthalten sein. Wurde ein Problem erkannt, kann die Problembehandlung versuchen, es selbstständig zu lösen. Dazu nimmt sie Konfigurationsänderungen am System vor.

Für den sicheren Einsatz des Wartungscenters und dessen Funktionen sollten nachfolgende Aspekte umgesetzt werden:

Da die Windows-Dienste Wechselwirkungen mit anderen Diensten aufweisen, sollten die Standardstarteinstellungen der Windows-Dienste auf jeden Fall beibehalten werden. Sonst wäre es möglich, dass wichtige Windowsdienste nicht korrekt arbeiten.

| **Windowsdienst** | **Standard-Starttyp** |
|---|---|
| Diagnoserichtliniendienst (DPS) | Automatisch |
| Diagnosediensthost (WDiSvcHost) | Manuell |
| Diagnosesystemhost (WDiSystem-Host) | Manuell |
| Windows-Fehlerberichterstattungs-dienst (WerSvc) | Automatisch |

Weiterführend sollten folgende Einstellungen per Gruppenrichtlinie für jedes Windows 7 basierte IT-System umgesetzt werden:

- Einstellung: Neueste Problembehandlungen vom Windows-Onlinedienst für Problembehandlung abrufen
- Pfad in der Systemsteuerung: Systemsteuerung | Alle Systemsteuerungselemente | Problembehandlung
- Gruppenrichtlinienpfade:
- Computerkonfiguration | Richtlinien | Administrative Vorlagen | System | Problembehandlung und Diagnose | Microsoft Support-Diagnosetool | Tooldownload einschränken
- Computerkonfiguration | Richtlinien | Administrative Vorlagen | System | Problembehandlung und Diagnose | Microsoft Support-Diagnosetool | Ausführungsebene konfigurieren
- Empfehlung: Einstellungen deaktivieren
- Begründung: Verhindert, dass Daten für die Problembehandlung mit dem Microsoft Support ohne Kenntnis und Einverständnis des Benutzers über das Internet ausgetauscht werden
- Einstellung: Problemberichte senden
- Pfad in der Systemsteuerung: nicht existent
- Gruppenrichtlinienpfade:
- Computerkonfiguration | Richtlinien | Administrative Vorlagen | Windows-Komponenten | Windows-Fehlerberichterstattung | Fehlerberichterstattung konfigurieren.
- Computerkonfiguration | Richtlinien | Administrative Vorlagen | System | Internetkommunikationsverwaltung | Internetkommunikationseinstellungen | Fehlerberichterstattung deaktivieren
- Empfehlung: Einstellungen deaktivieren
- Begründung: Diese Einstellungen sollten deaktiviert werden, um nicht institutions- oder computerspezifische Konfigurationen an Microsoft zu senden.
- Einstellung: Regelmäßig Daten über Computerkonfiguration an Microsoft senden
- Pfad in der Systemsteuerung: nicht existent
- Gruppenrichtlinienpfad:
- Computerkonfiguration | Administrative Vorlagen | Windows-Komponenten | Anwendungskompatibilität | Programmbestand deaktivieren
- Empfehlung: Einstellungen deaktivieren

- Begründung: Wenn diese Einstellung nicht durch Gruppenrichtlinien unterbunden wird, ist es möglich, dass Daten über installierte Softwareprodukte an Microsoft gesendet werden, ohne dass der Benutzer dies beauftragt hat oder darüber Kenntnis erlangt.

Um weitere sicherheitsgefährdende Funktionen zu unterbinden, sollten folgende Einstellungen konfiguriert werden:

- Einstellung: Windows-Sicherung
- Pfad in der Systemsteuerung:
- Systemsteuerung | Alle Systemsteuerungselemente | Wartungscenter | Wartungscentereinstellungen ändern
- Empfehlung: Einstellung deaktivieren
- Begründung: Die Meldung könnte Benutzer mit lokalen Rechten auf dem IT-System veranlassen, eine Sicherung der Daten aus Unwissenheit auf einem lokalen Datenträger zu erstellen. Dies kann von der IT-Abteilung nicht nachvollzogen werden, womit weitere Sicherheitsrisiken entstehen.
- Einstellung: Programm zur Benutzerfreundlichkeit
- Pfad in der Systemsteuerung:
- Systemsteuerung | Alle Systemsteuerungselemente | Wartungscenter | Wartungscentereinstellungen ändern | Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit
- Empfehlung: Einstellung deaktivieren
- Begründung: Die Einstellung verhindert, dass Daten über das Nutzerverhalten an Microsoft übertragen werden.
- Einstellung: Computerwartung
- Pfad in der Systemsteuerung:
- Systemsteuerung | Alle Systemsteuerungselemente | Problembehandlung | Einstellungen ändern
- Empfehlung: Einstellung aktivieren
- Begründung: Diese Einstellung sollte aktiviert werden, sodass der Computer nach Problemen durchsucht und der Benutzer über gefundene Probleme in Kenntnis gesetzt wird.
- Einstellung: Problembehandlung andere Einstellungen
- Pfad in der Systemsteuerung:
- Systemsteuerung | Alle Systemsteuerungselemente | Problembehandlung | Einstellungen ändern
- Empfehlung: Einstellungen deaktivieren
- Begründung: Diese Einstellungen sollten deaktiviert werden, sodass weder neue Problemlösungen von Microsoft heruntergeladen sowie gesendet werden oder Probleme automatisch gelöst werden. Diese Einstellung ist deshalb nicht zu empfehlen, da Konfigurationen am IT-System nicht automatisch verändert werden sollten.

Für den Umgang mit dem Wartungscenter und den nach Umsetzung der Einstellungen noch für den Nutzer potenziell angezeigten Dialogen sollte eine verbindliche Regelung definiert werden, wie der Benutzer zu verfahren hat. Die Regelung sollte weiterhin enthalten, ob und wann der Nutzer die Wartungscenterkomponente manuell starten darf (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*). Im Normalfall sollten Probleme, die während des Betriebes eines IT-Systems auftreten, an die dafür vorgesehenen Personen eskaliert werden (siehe M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen*).

Prüffragen:

- Wurde eine verbindliche Regelung für den Umgang durch die Benutzer mit dem Wartungscenter unter Windows ab Version 7 definiert?

- Werden die Standardstarteinstellungen der Windows-Dienste DPS, WDiSvcHost, und WerSvc genutzt?
- Wurden die Einstellungen für "Neueste Problembehandlungen vom Windows-Onlinedienst für Problembehandlung abrufen", "Problemberichte senden", "Regelmäßig Daten über Computerkonfiguration an Microsoft senden", "Windows-Sicherung", "Programm zur Benutzerfreundlichkeit" und "Problembehandlung - andere Einstellungen" unter Windows ab Version 7 deaktiviert?
- Wurde unter Windows ab Version 7 die Einstellung für "Computerwartung" aktiviert?

# M 4.421 Absicherung der Windows PowerShell

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Windows PowerShell (WPS) ist eine .NET-basierte Skriptumgebung für die interaktive Systemadministration mittels so genannter Cmdlets. WPS kann auch administrative Skripte ausführen. Skripte sind eine Auflistung von einzelnen Kommandos, die in einer Textdatei gespeichert und in der Kommandozeile aufgerufen werden.

Wenn die WPS nicht benötigt wird, sollte sie deinstalliert werden.

Ab Windows 7 lässt sich die PowerShell-Skriptumgebung nur noch entfernen, indem das .NET-Framework deinstalliert wird. Ist dieses für andere Applikationen notwendig, müssen für die PowerShell-Umgebung folgende Sicherheitsaspekte beachtet werden:

Auf 64-Bit-Systemen existieren parallel eine 32-Bit-PowerShell und eine 64-Bit-PowerShell. Die 32-Bit-Umgebung verwendet die 32-Bit-Emulationsschicht *SysWOW64* für den Zugriff auf das Dateisystem und die Registrierung. SysWOW64 kann zu Fehlfunktionen beim Zugriff auf Systembereiche führen. Außerdem können 32-Bit-Skripte Unverträglichkeiten mit der 64-Bit-Umgebung aufweisen und umgekehrt. Daher sollte auf 64-Bit-Systemen nur die 64-Bit-PowerShell verwendet werden. Skripte, die auf einem 32-Bit-System erstellt und getestet wurden, sollten nicht auf einem 64-Bit-System verwendet werden.

Mit Veröffentlichung der Version 3.0 wurde der Funktionsumfang der PowerShell durch die Einführung neuer Cmdlets erhöht. Eine weitere neu eingeführte Funktion ist der PowerShell Web Access, mit dem sich die PowerShell auch über einen Webbrowser nutzen lässt und somit auch auf Geräten angewendet werden kann, die nicht kompatibel mit der aktuellen PowerShell-Version sind (z. B. mobile Geräte). Zur Nutzung auf einem anderen Server ist die Aktivierung der PowerShell-Remote-Unterstützung notwendig und die Einrichtung eines PowerShell Web Access Gateways erforderlich. Die auf dem System installierte Version der PowerShell kann mit dem Befehl *get-host* ermittelt werden.

### Schutz vor ungewollten Änderungen

Sofern die PowerShell mit aktivierten Administratorrechten ausgeführt wird, besitzt diese vollen Zugriff auf den Computer. Fehleingaben könnten somit zu Schäden führen, oder ungewollt ausgeführte Skripte (Schadsoftware) können weitreichende Zugriffe auf das System vornehmen. Aus diesem Grund wird empfohlen, die PowerShell nicht unter uneingeschränkten Administratorrechten auszuführen. Grundsätzlich sollten nur jene Befehle mit Administratorrechten ausgeführt werden, für die dies erforderlich ist und mit deren Funktionsweise der aufrufende Administrator vertraut ist. Sofern die Benutzerkontensteuerung auf dem System aktiv ist, verfügt die normale PowerShell-Konsole über keine Administratorrechte.

### Absicherung auf Dateiebene

Nur Administratoren sollten die Programmdateien *C:\Windows\System32\WindowsPowerShell\powershell.exe* und *powershell_ise.exe*

aufrufen dürfen. Aus diesem Grund sollte in den Sicherheitseinstellungen dieser Dateien nur die Gruppe der Administratoren das *Ausführen*-Recht erhalten. Auf 64-Bit-Systemen befinden sich die 32-Bit-Versionen im Ordner *C:\Windows\SysWOW64\WindowsPowerShell* und müssen ebenfalls abgesichert werden.

Es sollte überlegt werden, den Zugriff auf bestimmte Administratorkonten zu beschränken, beispielsweise wenn die automatische Ausführung von Skripten oder die Ausführung von Skripten über das Netz vorgesehen ist. Hierzu bietet es sich an, eine eigene Sicherheitsgruppe lokal oder in einer Domäne zu definieren und ihr die notwendigen Berechtigungen auf die Programmdateien zu geben.

Hinweis: Bei Programmen, die Berechtigungen auf die Ausführung von WPS besitzen, dürfen die Sicherheitsgruppen *System* und *TrustedInstaller* nicht entfernt werden!

**Absicherung des PowerShell-Profils**

Das benutzerspezifische PowerShell-Profil, das beim Aufruf von WPS geladen wird, sollte abgesichert werden. In der WPS kann mit dem Befehl *$profile* ermittelt werden, welche Datei das Profil für den aktuell angemeldeten Benutzer enthält. Das Profil liegt normalerweise in einem Ordner innerhalb des Windows-Benutzerprofils, auf den nur der Benutzer selbst sowie Administratoren Zugriff haben. Das PowerShell-Profil ist eine Konfigurationsdatei, über die das Aussehen der Shell konfiguriert werden kann, und über die auch eigene Aliase und Funktionen definiert werden können. Über die Profildatei kann auch die Einbindung von Cmdlets von Drittherstellern erfolgen. Um unberechtigte Zugriffsversuche auszuschließen, sollte die Objektüberwachung für die Profil-Dateien aktiviert werden (Näheres siehe M 4.344 *Überwachung von Windows-Systemen ab Windows Vista und Windows Server 2008*). Insbesondere ist bei den Profildateien jede Gruppe, die generelle Änderungsrechte besitzt, auch als SACL (System Access Control List) hinzuzufügen (Eigenschaften | Sicherheit | Erweitert | Überwachung). Die Überwachungsereignisse sollten stichprobenartig in der Ereignisanzeige ausgewertet werden.

**Absicherung der Skript-Ausführung**

Ebenso ist die Absicherung der ausgeführten Skripte notwendig. Besondere Bedeutung kommt dem PowerShell-Profil zu, da es benutzerspezifisch beim Aufruf von WPS gestartet wird. Die Ausführung von Skripten kann, auch ohne dass ein administrativer Zugriff auf Betriebssystemkomponenten erfolgt, für die Stabilität und Integrität des Betriebssystems und der Applikationen kritisch sein. Aus diesem Grund sollten die folgenden ausführbaren Skript-Dateien und Hilfsdateien auf Dateisystemebene mit entsprechend eingeschränkten Berechtigungen versehen werden:

- *.ps1*-Dateien: Windows PowerShell Shell-Skript
- *.ps1xml*-Dateien: Windows PowerShell Format- und Typdefinitionen
- *.psc1*-Dateien: Windows PowerShell Konsolendatei (exportierte Shell-Konfiguration)
- *.psd1*-Dateien: Windows PowerShell Datendatei
- *.psm1*-Dateien: Windows PowerShell Moduldatei

Die *Ändern*-Berechtigung an den Skripten sollte auf bestimmte Gruppen eingeschränkt werden, um die Integrität der Skripte zu gewährleisten.

Die Ausführung von PowerShell-Skripten sollte außerdem mit dem Befehl *Set-ExecutionPolicy* eingeschränkt werden. Hierbei wird festgelegt, welche Bedin-

gungen Skripte erfüllen müssen, um ausgeführt zu werden. Folgende Optionen sind möglich:

- *Restricted:* Die Ausführung von Skripten ist gänzlich unterbunden (Standard-Einstellung).
- *AllSigned*: *.Ps1* und *.Ps1xml*-Dateien müssen digital signiert sein, um ausgeführt werden zu können.
- *RemoteSigned*: Skripte, die lokal erstellt wurden, können ohne Signatur ausgeführt werden.
- *Unrestricted:* Alle Skripte können ohne Einschränkungen ausgeführt werden.

Die Ausführung von PowerShell-Skripten sollte auf signierte Skripte eingeschränkt werden. Hierzu wird in der PowerShell-Umgebung folgender Befehl ausgeführt:

*Set-ExecutionPolicy AllSigned*

Die Ausführung von Skripten kann auch zentral über Gruppenrichtlinien gesteuert werden:

*Skriptausführung aktivieren* unter *Richtlinie Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows PowerShell*

**Signieren von PowerShell-Skripten**

Das Signieren von Skripten erfordert ein Authenticode-Codesignaturzertifikat der Klasse 3, das auf dreierlei Weise bezogen werden kann.

Institutionen, die über eine interne Public Key Infrastruktur (PKI) verfügen, können das notwendige Zertifikat selbst erzeugen, wenn die zugehörige interne Zertifizierungsstelle von allen IT-Systemen im an die PKI angeschlossenen Informationsverbund als vertrauenswürdig eingestuft wird.

Die zweite Möglichkeit besteht darin, eine externe Zertifizierungsstelle (Certification Authority*, CA*) zu verwenden. Clients ab Windows Vista sind bereits so konfiguriert, dass sie den Zertifikaten der führenden externen CAs vertrauen.

Die dritte Möglichkeit besteht darin, ein selbst signiertes Zertifikat mithilfe des Tools *Makecert.exe* zu erstellen. Dieses kostenlose Tool wird mit dem Windows Plattform-SDK geliefert und in einigen Editionen von Microsoft Office automatisch installiert. Der Nachteil besteht darin, dass ein Zertifikat immer nur auf dem IT-System eingesetzt werden kann, auf dem es erzeugt wurde. Für die Ausführung von PowerShell-Skripten über das Netz, beispielsweise als Anmeldeskript (siehe M 2.326 *Planung der Gruppenrichtlinien für Clients ab Windows XP*), ist eine interne oder externe Zertifizierungsstelle zu empfehlen.

Prüffragen:

- Ist in der Windows PowerShell die Ausführbarkeit der Dateien von WPS auf Dateiebene den Gruppen der Administratoren, lokal und Domäne vorbehalten?
- Ist eine Protokollierung von Schreib- und Lesezugriffen auf das Windows PowerShell-Profil eingerichtet, und werden die Protokolle regelmäßig ausgewertet?
- Ist die Ausführung von Windows PowerShell-Skripten mit dem Befehl Set-ExecutionPolicy AllSigned oder durch eine Gruppenrichtlinie eingeschränkt worden?

# M 4.422 Nutzung von BitLocker To Go ab Windows 7

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer, IT-Sicherheitsbeauftragter

Mit BitLocker To Go können Benutzer mit den Windows 7 Versionen Enterprise und Ultimate Partitionen auf Wechseldatenträgern wie USB-Sticks, externen Festplattenlaufwerken oder virtuellen Laufwerken (Virtual Hard Drives, VHD) verschlüsseln. Falls ein verschlüsselter Datenträger verloren geht oder gestohlen wird, sind die Daten darauf geschützt, da die Entschlüsselung nur mithilfe eines Passwortes, einer Smartcard oder den Wiederherstellungsinformationen möglich ist. Über das Kontextmenü des jeweiligen Laufwerkssymbols wird BitLocker To Go über die Option "*BitLocker aktivieren...*" eingeschaltet. Dazu sind keine administrativen Benutzerrechte erforderlich. Die Verwaltung von verschlüsselten Wechseldatenträgern erfolgt in der Systemsteuerung unter *Bitlocker-Laufwerksverschlüsselung*.

Vor dem Einsatz von BitLocker To Go wird empfohlen, B 1.7 *Kryptokonzept* anzuwenden. Weiterhin sollte in den Sicherheitsrichtlinien gemäß M 2.401 *Umgang mit mobilen Datenträgern und Geräten* und M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung* ergänzt werden, in welchen Szenarien welche Personengruppen Verschlüsselung einsetzen müssen, dürfen oder nicht dürfen. Zu beachten ist, dass mit BitLocker To Go keine einzelnen Dateien verschlüsselt werden können, sondern nur eine Partition eines Datenträgers.

Die größte Herausforderung besteht im sorgsamen Umgang mit dem kryptographischen Schlüsselmaterial durch die Benutzer (M 2.46 *Geeignetes Schlüsselmanagement*). Gelangt es in unbefugte Hände, ist die Vertraulichkeit der Daten nicht mehr gewährleistet. Der Schutzbedarf hinsichtlich Vertraulichkeit und Verfügbarkeit der Schlüssel ist mindestens so hoch einzustufen, wie der der unverschlüsselten Daten selbst. Sobald mehrere Benutzer BitLocker To Go verwenden, sollte ein zentral gesteuertes Schlüsselmanagement, zum Beispiel mittels Active Directory, verwendet werden.

BitLocker To Go ist standardmäßig aktiviert. Falls der Einsatz von BitLocker To Go jedoch nicht ausdrücklich vorgesehen ist (siehe M 2.325 *Planung der Sicherheitsrichtlinien für Windows XP, Windows Vista und Windows 7*), sollte es per Gruppenrichtlinie deaktiviert werden, da es sonst zu Gefahren wie in G 3.98 *Verlust von BitLocker-verschlüsselten Daten* und G 3.97 *Vertraulichkeitsverletzung trotz BitLocker Drive Encryption* kommen kann.

Die im Folgenden beschriebenen Einstellungen für BitLocker To Go befinden sich in der Gruppenrichtlinie:

*Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *BitLocker Laufwerksverschlüsselung* | *Wechseldatenträger*.

### Art des Schlüssels

Nach Aufruf des Befehls "*Bitlocker aktivieren...*" hat der Benutzer die Möglichkeit, ein Verschlüsselungskennwort zu vergeben oder eine Smartcard mit Verschlüsselungszertifikat einzulegen. Der öffentliche Teil dieses Zertifikats wird unverschlüsselt auf dem mobilen Datenträger abgelegt und könnte bei Verlust des Datenträgers Informationen über die genutzte Zertifikatsinfrastruktur (PKI)

preisgeben. Ist der Schutzbedarf der PKI hinsichtlich der Vertraulichkeit hoch, sollte überlegt werden, den Datenträger nur mittels Kennwort zu verschlüsseln oder gesonderte Zertifikate zu verwenden. Bei hohem Schutzbedarf hinsichtlich der Vertraulichkeit der zu verschlüsselnden Daten ist die einfache Kennwort-Authentisierung nicht ausreichend. Hierfür sollten Smartcard-Systeme mit einer eigenen Multifaktor-Authentisierungslösung verwendet werden.

Die Länge des Verschlüsselungskennnworts ist gemäß M 2.11 *Regelung des Passwortgebrauchs* festzulegen. Die Einstellung *Kennwortkomplexität anfordern* sollte ebenfalls gesetzt sein (erfordert M 4.48 *Passwortschutz unter NT-basierten Windows-Systemen*).

**Verschlüsselungsstärke**

Bei sehr hohem Schutzbedarf hinsichtlich der Vertraulichkeit der Daten sollte die Verschlüsselungsstärke von 128-Bit AES mit Diffuser auf 256-Bit AES mit Diffuser erhöht werden (Gruppenrichtlinie *Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen*). Der Verschlüsselungsvorgang kostet dadurch jedoch erheblich mehr Rechenzeit und kann auf einem langsamen Rechner möglicherweise nicht stabil betrieben werden.

**Verschlüsselte Datenträger ohne BitLocker To Go öffnen**

Verschlüsselte Datenträger können mit Hilfe des Tools *Bitlockertogo.exe* auch von Windows Versionen ab Windows XP ohne BitLocker gelesen werden, sofern sie mit dem FAT-Dateisystem formatiert sind. Ein Schreibzugriff auf das Medium ist nicht möglich. Für alternative Betriebssysteme wie Mac OS oder Linux existiert kein Programm zum Lesen von mit BitLocker To Go verschlüsselten Datenträgern.

Per Gruppenrichtlinie kann festgelegt werden, dass *Bitlockertogo.exe* automatisch auf jedem neu verschlüsselten FAT-Datenträger unverschlüsselt gespeichert werden soll. Die Applikation unterstützt keine Zugriffsberechtigungen und keine Smartcard-Authentisierung und ist daher in der Regel für den internen Gebrauch ungeeignet. In einer Sicherheitsrichtlinie für den verschlüsselten Datenaustausch mit Dritten sollte festgelegt werden, welche Personen zur Datenweitergabe autorisiert sind und auf welchen IT-Systemen verschlüsselte FAT-Datenträger erstellt werden dürfen.

**Unverschlüsseltes Schreiben unterbinden**

Es ist anhand des Kryptokonzepts zu entscheiden, ob und für welche IT-Systeme das Schreiben auf externe unverschlüsselte Datenträger per Gruppenrichtlinie verboten wird. Die entsprechende GPO lautet: *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind*. Mit dieser Einstellung lässt sich sicherstellen, dass Daten auf externen Datenträgern immer verschlüsselt sind.

Wird diese Einstellung genutzt, müssen in der Praxis in den meisten Fällen Ausnahmen konfiguriert und den Benutzern bekannt gegeben werden, sodass auch bei schwierigen Anwendungsfällen eine regelkonforme und nachvollziehbare Verschlüsselungsstrategie umgesetzt werden kann.

Die häufigsten Gründe dafür sind Präsentationsgeräte, die einen USB-Stift lesen sollen sowie die gezielte Weitergabe von externen Datenträgern an externe Stellen. Eine Möglichkeit besteht darin, einige USB-Sticks gut sichtbar als "öffentlich" zu kennzeichnen und sie von der Verschlüsselung auszuschließen. Unverschlüsselte Datenträger sollten nur von dazu autorisierten Personen herausgegeben und verwendet werden. Restriktivere organisatorische

Maßnahmen, zum Beispiel Protokollierung der Herausgabe von USB-Sticks, sind je nach Schutzbedarf hinsichtlich der Vertraulichkeit der Daten in Betracht zu ziehen. Alle benötigten Ausnahmen müssen in der Sicherheitsrichtlinie für den Datenaustausch beziehungsweise im Kryptokonzept geregelt werden. Auf technischer Ebene lässt die oben genannte Gruppenrichtlinie Ausnahmen für bestimmte Datenträger zu, denen vorher eine ID gegeben wurde. Genaue Anweisungen für das Konfigurieren der IDs sind direkt in der Gruppenrichtlinie zu finden. Die Anwender müssen im Umgang mit verschlüsselten und unverschlüsselten Datenträgern geschult werden.

**Wiederherstellung verschlüsselter Wechseldatenträger im Notfall**

Wiederherstellungskennwörter und -schlüssel ermöglichen einem Administrator oder Benutzer das Wiederherstellen verschlüsselter Daten, falls der Benutzer das Verschlüsselungskennwort oder die Smartcard verloren hat. Beim ersten Verschlüsseln des Datenträgers generiert der Assistent ein 48-stelliges Zufallskennwort für die Wiederherstellung. Es sollte übernommen und kann ausgedruckt oder als Textdatei gespeichert werden. Es sollten gemäß M 2.22 *Hinterlegen des Passwortes* genaue Anweisungen für Benutzer erstellt werden, wie mit Wiederherstellungskennwörtern zu verfahren ist. Sie müssen genauso vertraulich und sorgsam behandelt werden wie das Verschlüsselungskennwort oder die Smartcard.

So muss gemäß M 4.86 *Sichere Rollenteilung und Konfiguration der Kryptomodule* geregelt werden, ob und wie Wiederherstellungskennwörter und -schlüssel zentral abgelegt werden sollen und wer auf diese zwecks Wiederherstellung der Daten zugreifen darf. Um die Vertraulichkeit der Wiederherstellungsinformationen besser zu schützen und die Wiederherstellung im Notfall zu beschleunigen, ist es empfehlenswert, dass diese Informationen ohne Benutzereingriff automatisch im Active Directory hinterlegt werden. In jedem Fall ist der geeignete Umgang mit Wiederherstellungskennwörtern und -schlüsseln sicherzustellen. Hierzu dient die Gruppenrichtlinie *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können*. Zusätzlich sind die Schritte, Personen und Ressourcen, die zur Wiederherstellung benötigt werden, genau zu definieren.

Wenn das Wiederherstellungskennwort manuell gewählt oder nachträglich geändert wird, müssen triviale Formen vermieden werden (entsprechend M 2.11 *Regelung des Passwortgebrauchs*). Wenn das Wiederherstellungskennwort aus Effizienzgründen für verschiedene Datenträger gleich gewählt wird, dann gilt die Vermeidung trivialer Formen umso dringender.

Besteht der Verdacht, dass ein Kennwort, eine Smartcard oder ein Schlüssel kompromittiert worden ist, muss der entsprechende Schlüssel neu gesetzt werden. Dies erfolgt in Verbindung mit dem Wiederherstellungskennwort oder dem Wiederherstellungsschlüssel.

Mittels Gruppenrichtlinie kann für jeden verschlüsselten Datenträger ein 256-Bit-Wiederherstellungsschlüssel erzeugt werden. Dieser ermöglicht den Zugriff auf den Datenträger, wenn die ursprünglichen Authentisierungsmittel nicht mehr zur Verfügung stehen. Er ist nicht druckbar und es ist nicht möglich, ihn mündlich, zum Beispiel am Telefon, weiterzugeben. Dies erhöht den Schutz der Vertraulichkeit der Daten, verzögert andererseits im Notfall die Datenwiederherstellung. Diese Wiederherstellungsschlüssel können nur auf einem zusätzlichen USB-Stick oder im Active Directory gespeichert werden. Auf Systemen, mit denen Daten mit sehr hoher Vertraulichkeitsanforderung verschlüs-

selt werden, sollten nur Wiederherstellungsschlüssel, aber keine Kennwörter zugelassen werden.

Zusätzlich kann vom Administrator ein Datenwiederherstellungsagent installiert werden (*Gruppenrichtlinien-Snap-in* | *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für öffentliche Schlüssel* | *BitLocker*). Er ist der öffentliche Teil eines universellen Wiederherstellungsschlüssels und wird einheitlich auf allen BitLocker-Clients installiert. Der dazu passende private Schlüssel kann die verschlüsselten Datenträger entschlüsseln und sollte sich nicht im Besitz des Administrators befinden. Datenwiederherstellungsagenten erfordern prinzipiell einen besonders hohen Schutz gegen Missbrauch und ihr Austausch ist im Falle einer Kompromittierung sehr aufwendig. Der Datenwiederherstellungsagent ist kein Ersatz für Wiederherstellungskennwörter oder -schlüssel, sondern nur ein zusätzlicher Schutz vor Datenverlust für Benutzer, die nicht am zentralen Schlüsselmanagement teilnehmen. Vor- und Nachteile des Datenwiederherstellungsagenten müssen vor dem Einsatz abgewogen werden.

**Vernichtung des Schlüsselmaterials**

Sobald ein verschlüsselter Datenträger ausgesondert wird oder verloren gegangen ist, müssen alle Schlüssel und Kennwörter in Verbindung mit diesem Datenträger unverzüglich vernichtet werden. Bei zentral gespeicherten Schlüsseln sollte über die Vernichtung ein revisionssicheres Protokoll geführt werden, sofern die verschlüsselten Daten noch als vertraulich eingestuft sind.

**Schulung der Benutzer**

Durch die einfache Bedienung und starke Präsenz der BitLocker To Go-Verschlüsselungsfunktion für den Benutzer entsteht oft das in G 3.44 *Sorglosigkeit im Umgang mit Informationen* beschriebene Fehlverhalten.

Benutzer müssen darin unterrichtet werden, wie die Ablage der Wiederherstellungskennwörter und -schlüssel zu erfolgen hat und welche Schritte und Ansprechpartner bei Verlust von Kennwörtern, sonstigen Schlüsseln und verschlüsselten Datenträgern für sie gelten.

Benutzer, die BitLocker To Go ohne zentrales Schlüsselmanagement verwenden, sind häufig Führungspersonen oder Geheimnisträger innerhalb des Informationsverbunds. Sie sollten in regelmäßigen Gesprächen für die Gefahren sensibilisiert werden. Dazu gehört auch, sie für die Regelungen zum Erstellen und Aufbewahren von Datenträgern und Schlüsseln sowie zur Vorgehensweise bei Verlust und Aussonderung zu schulen.

**Abgrenzung der Eignung von BitLocker To Go**

Die Verschlüsselung mit BitLocker To Go schützt Daten auf mobilen oder virtuellen Datenträgern nur bei Verlust oder Diebstahl. Der Schutz ist nicht wirksam, während der Datenträger mit dem System verbunden ist und sich der Nutzer erfolgreich authentisiert hat. BitLocker To Go bietet keinen Schutz gegen unerlaubtes Kopieren von Daten oder Einschleusen von Schadsoftware während des Betriebs.

Prinzipbedingt sind bei tragbaren Medien, bei denen Sicherheitsmechanismen direkt in die Hardware integriert sind, die Verschlüsselungs- und Authentisierungsvorgänge weniger anfällig für Manipulation des Betriebssystems. Sie sind für Anwendungen mit besonders hohem Schutzbedarf hinsichtlich der Vertraulichkeit zu empfehlen.

**BitLocker-Werkzeuge**

- Der *Recovery Password Viewer* dient zur Verwaltung von Wieder-herstellungsschlüsseln im Active Directory (siehe Knowledge-Base-Artikel 958830).
- Das Kommandozeilentool *repair-bde.exe* dient der Datensicherung aus beschädigten Volumes, die durch BitLocker verschlüsselt worden sind.
- Das Tool *Bitlockertogo.exe* wird je nach Konfiguration automatisch auf einen mit BitLocker To Go verschlüsselten Datenträger kopiert. Das Tool erlaubt lesenden Zugriff auf verschlüsselte Datenträger unter Windows XP und Windows Vista, wenn der Datenträger das Dateisystem FAT nutzt.

Prüffragen:

- Verwenden Benutzer unter Windows 7 ein geeignetes Verschlüsselungskennwort oder -zertifikat?
- Ist sichergestellt, dass nur Befugte Zugriff auf das Wiederherstellungskennwort oder den Wiederherstellungsschlüssel von Windows BitLocker To Go haben?
- Ist die Nutzung von BitLocker To Go in der Sicherheitsrichtlinie für den Einsatz von Windows geregelt?
- Werden Benutzer, die ihre Wechseldatenträger ohne zentrales Schlüsselmanagement verschlüsseln, regelmäßig bezüglich Windows BitLocker To Go geschult?
- Ist der Einsatz von BitLocker und BitLocker To Go im Kryptokonzept berücksichtigt?
- Wird das Schlüsselmaterial von Windows BitLocker To Go vernichtet, wenn Datenträger verloren gehen oder ausgesondert werden?

# M 4.423 Verwendung der Heimnetzgruppen-Funktion ab Windows 7

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

In Windows 7 wurde die neue Funktion *Heimnetzgruppe* (englisch *Homegroup*) eingeführt. Sie ermöglicht den einfachen Zugriff auf Dateien (Bilder, Musik, Videos und Dokumente) und Drucker anderer IT-Systeme im lokalen Netz. Der Zugriff auf die Daten erfolgt gruppiert über die Bibliotheksfunktion (Zusammenfassung von Dateien in unterschiedlichen Ordnern des gleichen Typs, beispielsweise Musikdateien, Dokumente, Bilderdateien oder Videodateien) von Windows 7.

Es kann mit allen Windows-7-Versionen auf eine bestehende Heimnetzgruppe zugegriffen werden. Die Erstellung einer neuen Heimnetzgruppe ist ab der Version Home Premium möglich. Unter Windows 8 gibt es keine Beschränkungen. Wenn der Computer bereits einer Domäne angehört, kann zwar einer Heimnetzgruppe beigetreten werden, eine solchen Gruppe kann allerdings nicht erstellt werden.

Während des Anlegens einer Heimnetzgruppe wird ein Passwort generiert, dass auf allen IT-Systemen eingegeben werden muss, die der Heimnetzgruppe angehören sollen. Danach kann auf die vorhandenen Freigaben zugegriffen werden. Das Passwort der Heimnetzgruppe kann nachträglich geändert werden. Während des Passwortänderungsvorgangs müssen alle IT-Systeme der Heimnetzgruppe eingeschaltet sein. Im Anschluss muss an jedem dieser IT-Systeme das neue Passwort eingetragen werden. Alternativ kann die Authentisierung über bestehende Benutzerkonten eines IT-Systems erfolgen.

Die Heimnetzgruppe wird auf Basis von IPv6 über das Microsoft Peer Name Resolution Protocol (PNRP), sowie der Verwendung der Freigabe-Funktionen und der Benutzerverwaltung des Betriebssystems realisiert.

Jedes IT-System kann auf die freigegebenen Daten der anderen Heimnetzgruppen-Systeme zugreifen und selbst Daten freigeben. Voraussetzung für die Funktion Heimnetzgruppe ist die Einstellung "Heimnetzwerk" als Standorttyps des Netzes. Auf den IT-Systemen einer Heimnetzgruppe wird standardmäßig eine neue Benutzergruppe namens *HomeUsers* (deutsch: *Heimnetzgruppe*, sie enthält alle lokalen Benutzer des Computers) und der Benutzer *HomeGroupUser$* eingerichtet.

**IT-Systeme, die mit einer Domäne verbunden sind**

Ist ein IT-System (beispielsweise ein Laptop) Teil einer Domäne, kann durch dieses IT-System keine Heimnetzgruppe erstellt werden. Solche IT-Systeme können vorhandenen Heimnetzgruppen beitreten, jedoch werden keinerlei Daten von diesem IT-System im Heimnetz freigegeben. Dadurch wird sichergestellt, dass durch die Verwendung der Heimnetzgruppe keine vertraulichen Informationen durch Unbefugte eingesehen oder verändert werden können. Wenn die Verwendung von dienstlich zur Verfügung gestellter IT in Heim-Umgebungen per Anweisung generell untersagt ist, dann sollte die Heimnetzgruppen-Funktionalität des IT-Systems per Gruppenrichtlinie deaktiviert werden.

**Einsatz der Heimnetzgruppe in einer Institution**

Vor dem Einsatz der Heimnetzgruppen-Funktionalität in einer Institution ist zu prüfen, ob die Funktionalität zur Erreichung der Institutionsziele benötigt wird und der damit verbundene Nutzen die Risiken überwiegt. Unter Umständen kann der Datenzugriff auch über andere technische Mittel (beispielsweise über Fileserver mit angeschlossenem Verzeichnisdienst) erreicht werden.

Die Entscheidung zur Nutzung oder Nicht-Nutzung dieser Funktionalität sollte in einer Richtlinie festgelegt werden. Hierbei ist festzulegen, ob die Datei- und Druckerfreigabe via Peer-to-Peer-Funktionalität (vgl. M 5.152 *Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste*) erlaubt sein soll.

Im Gruppenrichtlinienobjekt-Editor ist der Beitritt zu einer Heimnetzgruppe im Bereich *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Heimnetzgruppe* konfigurierbar. In der Gruppenrichtlinie *Beitritt des Computers zu einer Heimnetzgruppe verhindern* können drei Zustände eingestellt werden: *Nicht konfiguriert*, *Deaktiviert* und *Aktiviert*. Bei den ersten beiden Zuständen ist der Beitritt zur Heimnetzgruppe möglich.

Sollte der Einsatz der Heimnetzgruppe durch die Richtlinie erlaubt sein, dann muss dessen Einsatz sorgfältig geplant und danach sicher betrieben werden.

Zudem sind für betroffene mobile IT-Systeme M 2.442 *Einsatz von Windows-Clients ab Windows Vista auf mobilen Systemen* und B 3.3 *Laptop* anzuwenden.

Da beim Zugriff auf freigegebene Daten Schadsoftware auf das IT-System gelangen kann, ist dafür zu sorgen, dass die Maßnahmen des Bausteins B 1.6 *Schutz vor Schadprogrammen* institutionsweit und speziell für den in der Heimnetzgruppe befindlichen Computer umgesetzt sind.

Auch müssen die Benutzer im Umgang mit den Freigaben geschult werden, so dass sie zum Beispiel keine vertraulichen Daten ihres Laptops in die freigegebenen Ordner einstellen.

Wenn die Verwendung der Heimnetzgruppe wieder aufgehoben werden soll, muss die Heimnetzgruppe verlassen werden. Dazu ist die *Systemsteuerung* zu öffnen, im Suchfeld *Heimnetzgruppe* einzutragen und auf diesen Begriff zu klicken. Im Dialog-Fenster *Heimnetzgruppe* wählt man anschließend den Link *Heimnetzgruppe verlassen* und im nächsten Fenster erneut *Heimnetzgruppe verlassen* und klickt auf *Fertig stellen*.

Windows setzt dann die entsprechenden Rechte wie vor dem Beitritt zur Heimnetzgruppe und löscht den Benutzer *HomeGroupUser$* und die Benutzergruppe *HomeUsers*.

**Schulung der Benutzer im Umgang mit der Heimnetzgruppen-Funktion**

Entscheidet sich die Institution für den Einsatz der Heimnetzgruppe, so sind in jedem Fall die Benutzer über die möglichen Gefahren bei der Nutzung dieser Funktion aufzuklären und der sichere Umgang zu schulen (siehe M 3.28 *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*).

Prüffragen:

- Existiert eine Richtlinie für die Nutzung der Heimnetzgruppen-Funktionalität?
- Wurde die Gruppenrichtlinie Beitritt des Computers zu einer Heimnetzgruppe verhindern entsprechend der Richtlinie konfiguriert?
- Wurden die Benutzer im Umgang mit den Freigaben der Heimnetzgruppe geschult?

# M 4.424 Sicherer Einsatz älterer Software ab Windows 7

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Nicht jede Software, die für Windows-Systeme geschrieben wurde, ist mit Clients ab Windows 7 kompatibel. Um sie dennoch nutzen zu können, stehen drei Werkzeuge zur Verfügung:

- Kompatibilitätsmodus für einzelne ausführbare Dateien
- Application Compatibility Toolkit (ACT)
- Windows XP-Modus (nur für Windows 7 und seit dem 8. April 2014 nicht mehr vom Support abgedeckt)

Soll zur aktuellen Windows-Versioninkompatible Software eingesetzt werden, ist es sehr wichtig, dass nicht zugunsten der Lauffähigkeit der Software die Sicherheit des gesamten Systems gelockert wird. Es sollten deshalb nur diejenigen Einstellungen angepasst werden, die tatsächlich benötigt werden, damit die ältere Software lauffähig ist. Um die notwendigen Einstellungen herauszufinden und zu dokumentieren, ist eine isolierte Testumgebung zu verwenden. Die Testumgebung muss mindestens aus einem -Client-System für jede einzusetzende Windows-Version bestehen. Die damit betraute Person sollte in der Anpassung und Bereitstellung von Windows-Clients geschult sein.

Vorab sollten jedoch die Supportvereinbarungen des Herstellers der Software geprüft werden. Wenn der Support der Software für die eingesetzte Windows-Version verweigert wird, selbst wenn sie im Kompatibilitätsmodus von Windows 7 lauffähig wäre, kann die Software gegebenenfalls auch in einer Virtualisierungs-Umgebung mit lizensierter Windows-XP-Installation ausgeführt werden.

Unter Windows 7 kann hierfür die Software im *VirtualPC XP-Modus* (nachfolgend XP-Modus genannt) getestet werden. Der XP-Modus ist für Windows 7 ab Version Professional als kostenloses Zusatzpaket erhältlich und stellt eine virtuelle Maschine mit Windows-XP zur Verfügung. Dabei ist zu beachten, dass Microsoft für Windows XP seit April 2014 keinen Support und damit auch keine Sicherheitsupdates mehr liefert. Dies gilt entsprechend auch für den XP-Modus in Windows 7, weshalb ein Einsatz möglichst vermieden werden sollte. Ist der Einsatz aus betrieblichen Gründung unverzichtbar, müssen flankierende Maßnahmen zum Schutz des Systems ergriffen werden.

Der XP-Modus ist nicht Bestandteil von Windows 8. Stattdessen gibt es in der Pro-Version die Virtualisierungstechnik Hyper-V. Eine alternative Virtualisierungsumgebung kann ebenfalls genutzt werden.

Eine virtuelle Maschine kann auch dann benutzt werden, wenn die Software trotz der weiter unten beschriebenen Anpassungen nicht unter der eingesetzten Windows-Version lauffähig ist. Wenn möglich, sollte die Software jedoch direkt auf den Clients mit der üblichen Windows-Umgebung betrieben werden. Die Virtualisierungs-Software ermöglicht neue Angriffsvektoren, und der XP-Modus enthält keine Werkzeuge zu Verwaltung, Schutz und Überwachung. Die vorgefertigte Windows-XP-Installation erfordert eine eigene Risikobetrachtung im Zusammenhang mit dem fehlenden Hersteller-Support und der verwendeten Software sowie die entsprechende Umsetzung von B 3.209 *Client unter Windows XP*.

In der Testumgebung ist zu ermitteln, ob die Software innerhalb einer Benutzersitzung ohne Administratorberechtigung und mit aktivierter Benutzerkontensteuerung (siehe M 4.340 *Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista*) lauffähig ist. Soll ältere Hardware weiterverwendet werden, müssen deren Treiber getestet werden. Die Tests sollten die Lauffähigkeit der Software und Treiber, die Installationsmöglichkeiten und, falls vorhanden, die Aktualisierungsmechanismen umfassen.

**Programmkompatibilitäts-Assistent (PCA)**

Wenn ältere Software auf dem Windows-Client ausgeführt werden soll, ist als Erstes der Programmkompatibilitäts-Assistent (*PCA*) zu starten (unter *Systemsteuerung* | *Alle Systemsteuerungselemente* | *Problembehandlung* | *Programme*). Dieser Assistent bezieht Informationen und sogenannte Kompatibilitätsfixes aus der *System Compatibility Database* und wendet individuelle Kompatibilitätsmodi auf Programmdateien an, die der System Compatibility Database bereits bekannt sind. Unbekannte Programmdateien kann der Administrator analysieren lassen und danach einem der zur Auswahl stehenden vordefinierten Kompatibilitätsmodi zuordnen. Die System Compatibility Database wird durch die Windows Update-Funktion mit neuen Informationen und Fixes versorgt. Die Aktualisierung der Informationen und Kompatibilitätsfixes kann sicherheitsrelevant sein und sollte daher immer mit durchgeführt werden.

Damit die Analyse und die Fixes des PCA funktionieren, müssen die PCA-Funktionen zugelassen sein. Dies ist standardmäßig der Fall und kann in den administrativen Vorlagen im Gruppenrichtlinien-Snap-in eingestellt werden: *Computerkonfiguration* | *Windows-Komponenten* | *Anwendungskompatibilität*. Speziell für die Analyse wird folgende Einstellung benötigt: *Computerkonfiguration* | *System* | *Problembehandlung und Diagnose* | *Szenarioausführungsebene konfigurieren* | *Erkennung, Problembehandlung*.

**Application Compatibility Toolkit (ACT)**

Falls der PCA nicht ausreicht, muss die Software zusammen mit dem *Application Compatibility Toolkit (ACT)* auf dem Windows XP-Testrechner installiert werden. Das ACT ist bei vorhandener Windows-Lizenz als kostenloses Zusatzpaket erhältlich und enthält Assistenten und Werkzeuge. Mit den Assistenten kann der Administrator das System analysieren lassen, während die Software gestartet ist. Neben den Assistenten sollte auch das Tool *Standard User Analyser* genutzt werden. Es erlaubt die interaktive Analyse mittels einer grafischen Oberfläche.

Die Analyseergebnisse der getesteten Software zeigen an, welche Systemzugriffe zu Fehlern führen würden. Zur Fehlerbehebung gibt es nun zwei Vorgehensweisen:

- Die passenden Einstellungen können auf Basis der Analyseergebnisse auf dem Test-Client vorgenommen werden oder
- die System Compatibility Database des Test-Clients wird mit Hilfe des Kommandozeilenbefehls *sdbinst* und des Tools *Compatibility Administrator* aus dem ACT erweitert.

Viele Fehler lassen sich durch die zuerst genannte Vorgehensweise beheben. Beispielsweise können Berechtigungen gesetzt, Installationspfade und Arbeitsverzeichnisse geändert, UAC-Manifeste erstellt, Systemprivilegien und Systemberechtigungen angepasst und zusätzliche Benutzerkonten mit erhöhten Berechtigungen verwendet werden.

Berechtigungen an Systemordnern und Systemschlüsseln in der Registrierdatenbank dürfen keinesfalls geändert werden. Berechtigungen im Programmordner sollten nur sehr gezielt geändert und müssen auf Verträglichkeit mit dem Windows Ressourcen-Schutz (WRP) und den Sicherheitszonen getestet werden. Des Weiteren sollten keine Berechtigungen an den Ordnern und Registrierschlüsseln geändert werden, die von der UAC-Virtualisierung betroffen sind (siehe M 4.338 *Einsatz von File und Registry Virtualization bei Clients ab Windows Vista*) oder die vom *WoW64*-Emulationsmodus umgeleitet werden (betrifft nur die 64 Bit-Versionen von Windows).

Für die zweite Vorgehensweise ist der *Compatibility Administrator* notwendig. Dieses Werkzeug enthält eine Reihe mitgelieferter Kompatibilitätsfixes. Die genaue Vorgehensweise ist der Herstellerdokumentation zu entnehmen, zum Beispiel unter *http://technet.microsoft.com/de-de/library/dd835539.aspx.* Aktualisierte Kompatibilitätsfixes werden von Microsoft zur Verfügung gestellt oder können auch individuell programmiert werden.

Falls bestimmte manuelle Anpassungen der Sicherheitsrichtlinie für Windows-Clients widersprechen, sollten der Einsatz des Compatibility Administrator-Tools beziehungsweise des VirtualPC XP-Modus getestet werden. Im Zweifelsfall müssen Ausnahmeregelungen überlegt und dokumentiert oder andere Möglichkeiten der Isolierung der inkompatiblen Software betrachtet werden.

Die Kompatibilitätsanpassungen müssen für jede Software dokumentiert werden. Folgende Tabelle zeigt ein Beispiel:

| **analysierter Fehler** | **Schweregrad** | **Anpassung** | **Kompat.-Fix** |
|---|---|---|---|
| verweigerter Start wegen falscher Windows-Version | hoch | - | Kompatibilitäts-modus des PCA |
| .ini Datei kann nicht geschrieben werden | hoch | Anpassung der UAC-Virtualisierung durch den PCA | - |
| Programm-Modul "Faktura" startet nicht | wird nicht gebraucht | - | - |

Der VirtualPC XP-Modus ist nicht mehr Bestandteil von Windows 8. Weiterhin wurde der Support für Windows XP und den XP-Modus von Microsoft eingestellt. Sollte sich der Einsatz von Windows-XP in einer virtualisierten Umgebung nicht vermeiden lassen, so sollten diese möglichst vom restlichen System abgeschottet werden und ein Netzwerkzugriff vermieden werden.

**VirtualPC XP-Modus**

Falls PCA und ACT nicht ausreichen, kann der XP-Modus auf dem Windows 7-Testrechner installiert werden. Anschließend wird die inkompatible Software innerhalb des virtuellen Windows XP-Systems installiert. Im Windows 7-Startmenü erscheint unter *Microsoft VirtualPC* | *Windows XP Mode Anwendungen* automatisch ein Startsymbol für die Software, wenn sie im XP-Modus für alle Nutzer installiert wurde. Wird die Software gestartet, führt der XP-Modus das Programm in einer virtuellen Windows XP-Umgebung im Hintergrund aus und blendet das Programmfenster in die Windows 7-Oberfläche ein. Alternativ

kann der Benutzer auch ein komplettes Windows XP-Fenster anzeigen lassen, indem er *Windows XP-Mode* auswählt. Einmal gestartet, bleibt die virtuelle Windows XP-Umgebung geladen, bis Windows 7 heruntergefahren wird. Die Verbindung zum virtuellen System wird durch den Remotedesktop-Dienst hergestellt, der auch die Zwischenablage, Soundausgabe, Druckertreiber, Smartcards etc. verbindet. Die Netzkommunikation und der Zugriff auf Datenträger und Anschlüsse erfolgen durch die Software *VirtualPC* im Hintergrund. Geräte ohne USB oder seriellen Anschluss können nicht verwendet werden.

In der Testumgebung sollten Software und Treiber auf ihre Verträglichkeit hinsichtlich der Netzkommunikation, Hardwareunterstützung, des Datenträgerzugriffs und der Remotedesktop-Unterstützung geprüft werden. Installations- und Aktualisierungsmechanismen sind ebenfalls zu prüfen. Weiterhin ist die Startzeit und Ausführungsgeschwindigkeit der Software zu testen sowie die Verfügbarkeit der sonstigen Windows-Anwendungen. Besonderes sorgfältig ist eine geeignete Ausschalt-Methode für den XP-Modus zu wählen und zu testen. Durch unsauberes Herunterfahren des XP-Modus können die Software-Installation oder die Daten der laufenden Sitzung beschädigt werden.

Falls eine Datensicherungslösung für den Windows 7-Client eingesetzt wird, muss diese Lösung mit VirtualPC getestet werden und Änderungen an der virtuellen Instanz sichern können.

Nachdem der XP-Modus auf dem Rechner installiert ist, können die Einstellungen für die virtuelle Umgebung aufgerufen werden unter *Startmenü* | *Microsoft VirtualPC* | Symbol für *Windows Virtual PC* | im Kontextmenü von *Windows XP-Mode* den Eintrag *Einstellungen* auswählen.

**Einschränkungen für den XP-Modus**

Beim Einsatz von *VirtualPC* sind die Bausteine B 3.304 *Virtualisierung* und B 3.209 *Client unter Windows XP* anzuwenden. Darüber hinaus gelten weiterhin die Maßnahmen für Clients der eingesetzten Windows-Version, sofern zutreffend, zum Beispiel die Verwendung komplexer Kennwörter, das Absichern der Netzkommunikation oder der Einsatz von BitLocker.

Der XP-Modus muss so weit wie möglich vom übergeordneten Windows-System isoliert werden. Hierzu sind folgende Grundsätze zu beachten:

- Der XP-Modus sollte im produktiven Betrieb nicht als alternatives Desktopsystem verwendet werden. Benutzer sollten keine Komponenten oder Software des XP-Systems verwenden, die nicht zum Anwendungsszenario der älteren Software gehören.
- Datenisolation: Keine Nutzerdaten im virtuellen Windows XP-System halten.
- Netzisolation: Keine uneingeschränkte Netzkommunikation des virtuellen Windows XP-Systems zulassen.

Für den ersten Punkt sollte ein Nutzungsverbot für nicht freigegebene virtualisierte Software ausgesprochen werden und gegebenenfalls M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung* für das virtuelle Windows XP-System in Betracht gezogen werden.

Um Nutzerdaten zu speichern, sollten die in VirtualPC eingebundenen Laufwerke des Host-Rechners benutzt werden. Die Laufwerke des virtuellen Betriebssystems sollten nicht benutzt werden. Falls die Software schützenswerte Sitzungsdaten und Protokolldateien erzeugt, müssen diese täglich außerhalb des virtuellen Windows XP-Systems gesichert werden, zum Beispiel durch ein

Shutdown-Skript im Windows XP-System oder mit Hilfe einer VirtualPC-kompatiblen Datensicherungssoftware.

Aufgrund der Netzisolation darf kein Direktzugriff auf die Netzadapter des Rechners eingestellt werden (unter *Windows XP-Mode* | *Einstellungen* | *Netzwerk*). Nur die Zugriffsarten *Nicht verbunden*, *Internes Netzwerk* und *Gemeinsam genutztes Netzwerk (NAT)* sind zulässig. Weiterhin sollten in der Windows-Firewall eine eingehende und eine ausgehende Regel für die Programmdatei *%SystemRoot%\System32\vpc.exe* erstellt werden, die den Netzwerkverkehr blockieren. Zu den Regeln sind Ausnahmen zu konfigurieren, um die Kommunikation für die benötigten Anwendungen innerhalb des virtuellen XP-Systems gezielt freizuschalten.

**Bereitstellen der Kompatibilitätseinstellungen auf produktiven Clients**

Die Testergebnisse sollten dokumentiert und in ein Bereitstellungskonzept für den Einsatz älterer Software überführt werden. (siehe auch M 2.324 *Einführung von Windows auf Clients ab Windows XP planen* ).

**Verwenden der Herstellerdokumentation**

Die Herstellerdokumentation zu PCA und ACT ist über die Microsoft Technet-Distribution oder im Internet verfügbar unter:

http://technet.microsoft.com/de-de/library/dd835539.aspx

In der Dokumentation der Testergebnisse sollten die entsprechenden Teile der Herstellerdokumentation enthalten sein.

Prüffragen:

- Wurden Gewährleistung und Herstellersupport für den Einsatz von Altanwendungen auf Clients ab Windows 7 geklärt?
- Wurden die vorgenommenen Kompatibilitätsanpassungen von Altanwendungen an Clients ab Windows 7 vollständig dokumentiert?
- Wird bei der Verwendung des XP-Modus unter Windows 7 das virtualisierte Windows XP vom übergeordneten Client-System isoliert? Sind geeignete Maßnahmen getroffen, um das Windows-XP-System trotz fehlender Sicherheitsupdates des Herstellers vor Angriffen zu schützen?
- Werden unter Clients ab Windows 7 die Daten der im XP-Modus bzw. in der Virtualisierungssoftware laufenden Anwendung außerhalb der virtuellen Umgebung gesichert?

# M 4.425 Verwendung der Tresor- und Cardspace-Funktion auf Clients ab Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Windows bietet für Clients ab Windows 7 verschiedene Netzfunktionen an, die sich vornehmlich an Privatanwender richten und deren Verwendung standardmäßig aktiviert ist. So können seit Windows 7 Zugangsdaten (*Anmeldeinformationsverwaltung*) für verschiedene Ressourcen, beispielsweise auf externe Computersysteme und Webseiten, und persönliche Informationen (*Windows Cardspace*) für die Registrierung und Anmeldung bei Webseiten und Online-Diensten verwaltet werden. Windows Cardspace ist mit Einführung von Windows 8 nicht mehr Bestandteil des Betriebssystems und wurde vollständig entfernt.

Damit durch die Verwendung dieser Funktionalitäten innerhalb einer Institution keine Schwachstellen entstehen, müssen für deren Einsatz zunächst die Risiken gegenüber dem Nutzen abgewogen werden. Bei einer positiven Entscheidung hinsichtlich des Einsatzes ist die Verwendung der Funktionen sorgfältig zu planen und umzusetzen.

**Anmeldeinformationsverwaltung (Tresor)**

Seit der Version 7 verfügt das Windows-Betriebssystem über eine zentrale Speicherstelle für Zugangsdaten für verschiedene Netzressourcen, beispielsweise für andere Windows-Systeme, Online-Dienste und Webseiten. Die gespeicherten Zugangsdaten werden nach Windows-Anmeldeinformation, zertifikatbasierte Anmeldeinformationen und generischen Anmeldeinformationen unterschieden und auf dem Computer in einem besonderen Ordner gespeichert, der auch die Bezeichnung Tresor trägt. Unter Windows 8 verfügt die Anmeldeinformationsverwaltung neben der Verwaltung von *Windows-Anmeldeinformationen* auch über die Funktion der Verwaltung von *Webanmeldeinformationen*, durch welche die Speicherung von Passwörtern von Webseiten erfolgt.

Die *Anmeldeinformationsverwaltung* ist in der Systemsteuerung unter dem Pfad *Benutzerkonten und Family Safety* zu finden

Diese zentrale Speicherung von Anmeldeinformationen birgt unter anderem das Risiko, dass sich unbefugte Dritte Zugang zum Zugangsdatenspeicher verschaffen können, beispielsweise wenn der Bildschirm nicht gesperrt wurde. Über die Funktion *Tresor sichern* könnte ein Unbefugter, ohne sich als der aktuelle Benutzer authentisieren zu müssen und mit einem selbst gewählten Passwort, alle Anmeldeinformationen beispielsweise auf einem externen Datenträger sichern. Anschließend kann er die Zugangsdaten auf einem anderen System in seinen Tresor mit Hilfe der Funktion *Tresor wiederherstellen* überspielen.

Es muss daher abgewogen werden, ob der Nutzen und die Zeitersparnis nicht jedes Mal die Zugangsdaten eingeben zu müssen, das beschriebene Risiko überwiegt.

In einer Richtlinie sollte festgehalten werden, ob in der Institution die Speicherung der Zugangsdaten im sogenannten Tresor erlaubt oder verboten wird.

Ein Verbot lässt sich technisch über eine Gruppenrichtlinie durchsetzen. Dazu ist im Gruppenrichtlinienobjekt-Editor im Bereich *Computerkonfiguration* | *Richtlinien* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | Systemdienste der Dienst A*nmeldeinformationsverwaltung* zu deaktivieren. Ohne diesen gestarteten Dienst ist die zentrale Speicherung von Zugangsdaten im Tresor nicht mehr möglich.

**Windows Cardspace (nur Windows 7)**

Im Tresor können nur die benötigten Informationen für eine Anmeldung an einem Dienst gespeichert werden (Benutzername, Passwort oder Zertifikat). Dagegen wird über Windows Cardspace unter Windows 7 eine Möglichkeit bereitgestellt, Informationen, die für eine Registrierung oder Anmeldung bei Webseiten und Online-Diensten verwendet werden, zentral mittels sogenannter Karten zu speichern. Wenn Zugangsdaten in Windows Cardspace gespeichert werden sollen, muss dafür eine Richtlinie existieren.

Es können zwei Arten von Karten verwendet werden: persönliche und verwaltete Karten.

Persönliche Karten können von den Benutzern selbst erstellt und mit persönlichen Informationen wie Vorname, Name und E-Mail-Adresse ergänzt werden.

Verwaltete Karten können nur von einer Institution erstellt werden und enthalten validierte Informationen, beispielsweise zu einer Person und deren Kontonummer. Der Benutzer installiert die verwaltete Karte. Die durch die Karte referenzierten Daten bleiben lokal auf dem IT-System in der Institution gespeichert und werden von ihr an den Diensteanbieter, beispielsweise einen Online-Buchhändler, auf Betreiben des Benutzers hin übermittelt. Auf Seiten der Diensteanbieter werden Mechanismen für die Verarbeitung der CardSpace-Informationen beispielsweise über das .NET-Framework bereitgestellt.

Jede Karte kann bei den unterschiedlichsten Online-Diensten und Webseiten verwendet werden. Zu jeder Karte werden der Verlauf der Verwendung und der Gültigkeitszeitraum der Karte gespeichert.

Die Karten werden verschlüsselt auf dem IT-System des Benutzers abgespeichert. Sie können auch verschlüsselt auf externe Datenträger übertragen werden. Zum einen ist dadurch eine Möglichkeit zum Backup der Karten gegeben und zum anderen können die Karten auf einem anderen Windows-System entschlüsselt und verwendet werden.

Um einen unbefugten Zugriff auf die Karten zu unterbinden, sollte von der Institution, beziehungsweise vom Benutzer, eine PIN für jede Karte und ein Passwort für die Kartensicherung festgelegt werden. Gehen diese Informationen verloren, ist kein Zugriff auf die Karten mehr möglich und die Karten müssen neu erstellt oder neu von der kartenausgebenden Institution angefordert werden.

Auch hier muss die Möglichkeit betrachtet werden, dass sich Unbefugte Zugriff auf diese Karten verschaffen und diese missbräuchlich einsetzen. Beispielsweise könnten die dazugehörenden PINs per Keylogger oder Social Engineering abgefangen werden. Daher ist der Einsatz von Windows Cardspace im Vorfeld abzuwägen.

In Institutionen, in denen es keinen Verwendungszweck für Windows Cardspace gibt, oder wo die Nutzung von Windows Cardspace durch die Windows 7 Richtlinie verboten wird, sollte dieser Dienst deaktiviert werden.

Eine Deaktivierung von Windows Cardspace ist im Gruppenrichtlinienobjekt-Editor im Bereich *Computerkonfiguration* | *Richtlinien* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Systemdienste* möglich.

**Schulung der Benutzer im Umgang mit den Windows-Funktionen**

Entschließt sich die Institution für den Einsatz einer der beiden hier beschriebenen Funktionen, sind in jedem Fall auch die Benutzer über die möglichen Gefahren bei der Nutzung dieser Funktionen aufzuklären und im sicheren Umgang zu schulen (siehe M 3.28 *Schulung zu Sicherheitsmechanismen für Benutzer bei Windows Client-Betriebssystemen*).

Prüffragen:

- Existiert für Windows-Clients ab Windows 7 eine Richtlinie zur Speicherung der Zugangsdaten im sogenannten Tresor?
- Wurde für Windows-Clients ab Windows 7 die Gruppenrichtlinie für das Verhalten des Dienstes Anmeldeinformationsverwaltung entsprechend der Richtlinie konfiguriert?
- Existiert eine Richtlinie für den Einsatz von Windows Cardspace unter Windows 7?
- Wurde die Gruppenrichtlinie für das Verhalten des Dienstes Windows Cardspace unter Windows 7 entsprechend der Richtlinie konfiguriert?

# M 4.426 Archivierung für die Lotus Notes/Domino-Umgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Dienste der Lotus Notes/Domino-Umgebung können eine Vielzahl von Geschäftsprozessen unterstützen. Aus diesen Geschäftsprozessen können fachliche Anforderungen an die Archivierung der elektronisch verarbeiteten, ausgetauschten oder gespeicherten Information bestehen. Diese sind in das in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* genannte Archivierungskonzept für Lotus Notes/Domino einzubringen.

Die bestehenden gesetzlichen Anforderungen und Anforderungen von Regulierungs- und Prüfungsbehörden müssen in den fachlichen Anforderungen berücksichtigt werden.

Die Umsetzung des Archivierungskonzeptes ist im Betrieb der Lotus Notes/Domino-Umgebung zu realisieren. Der Baustein B 1.12 *Archivierung* ist dabei anzuwenden.

Folgende Aspekte der Archivierung sind im Betrieb der Lotus Notes/Domino-Umgebung vor allem zu berücksichtigen:

- Die Archivierung muss konform zu den Bestimmungen des Datenschutzes erfolgen. Personenbezogene Daten sind, im Rahmen der technischen Möglichkeiten, nach den definierten Fristen zu löschen. Je nach Art der Daten müssen auch andere gesetzliche oder vertragliche Regelungen eingehalten werden.
- Die Gültigkeit elektronischer Signaturen (in Bezug zur vorgesehenen Archivierungsfrist) ist bei der Umsetzung der Archivierungsprozesse zu berücksichtigen. Das Archivierungsverfahren muss eine mögliche Erneuerung der Signatur vorsehen.
- Der Schutzbedarf der Archive im Hinblick auf Vertraulichkeit und Integrität kann durch Kumulationseffekte sogar höher sein als der der entsprechenden Produktivdatenbestände. Die Sicherheitsmaßnahmen für die Archive müssen dies abbilden.
- Lotus Notes/Domino Daten werden in proprietären Formaten archiviert. Die Nutzung des Archivs erfordert das Vorhalten alter Versionen von Lotus Notes/Domino oder die periodische Migration der bei der Archivierung genutzten ODS-Formate. In jedem Fall sind gültige Lizenzen erforderlich, was bei Nutzung von zeitlich begrenzten Lizenzen (siehe M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*) problematisch sein kann. Es ist sicherzustellen, dass für die in den Archivierungsanforderungen definierten Fristen der Zugriff auf die Archive auch technisch und lizenzrechtlich möglich ist.

Wenn bereits für andere elektronisch vorgehaltene Dokumente bzw. Daten Archivsysteme genutzt werden, kann eine Anbindung von Lotus Notes/Domino (bzw. der entsprechenden Domino-Anwendungen oder Dienste) an diese Archivsysteme sinnvoll sein.

Die Funktionen von Lotus Notes/Domino zur server- und clientseitigen Archivierung wie auch die konfigurierbare Administrator-Richtlinie zur E-Mail-Archivierung stellen Hilfsmittel dar, mit denen sich eine den meisten Anforderungen genügende Archivierung realisieren lässt. Hier ist jedoch im Detail zu prüfen,

ob die mit diesen Funktionen realisierbaren Lösungen den gesetzlichen und fachlichen Anforderungen (z. B. an E-Mail-Archivierung) genügen.

Wird DAOS (*Domino Attachment and Object Service*, verfügbar ab Version 8.5) genutzt, sind das bestehende Archivierungskonzept und die dazugehörigen Verfahren zu überprüfen und bei Bedarf anzupassen, da die zu archivierenden Daten nicht mehr redundant vorgehalten werden.

Prüffragen:

- Sind die gesetzlichen Anforderungen an die Archivierung elektronischer Daten und E-Mails bekannt und im Archivierungskonzept für Lotus Notes/ Domino berücksichtigt?
- Setzen die Verfahren zur Archivierung im Betrieb das Archivierungskonzept angemessen um?
- Wurde das Archivierungskonzept bei Nutzung von DAOS (Domino Attachment and Object Service) überarbeitet und die Verfahren entsprechend angepasst?

# M 4.427 Sicherheitsrelevante Protokollierung und Auswertung für Lotus Notes/Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Administrator, IT-Sicherheitsbeauftragter, Personalrat/ Betriebsrat

Zur Abbildung des Schutzbedarfs der Anwendungen und Dienste, die auf der Lotus Notes/Domino-Plattform betrieben werden, ist es erforderlich, sicherheitsrelevante Vorkommnisse zu protokollieren und periodisch oder ereignisgesteuert auszuwerten. Dies kann für die Lotus Notes/Domino-Umgebung über die Funktionen der Administration bzw. Sicherheitsadministration erfolgen.

Da Protokolle sicherheitsrelevanter Daten bzw. deren Auswertungen sowohl personenbezogene Daten als auch Daten mit Aussagekraft zu Mitarbeiterverhalten und Mitarbeiterproduktivität beinhalten können, ist hier die diesbezügliche Gesetzgebung zu berücksichtigen. Es ist erforderlich, den Datenschutzbeauftragten und den Personalrat/Betriebsrat sowohl bei der Erstellung des in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* beschriebenen Protokollierungs- und Auswertungskonzeptes für Lotus Notes/Domino wie auch bei den betrieblichen Maßnahmen zur Umsetzung dieses Konzeptes einzubinden.

Wird die private Nutzung von Diensten der Lotus Notes/Domino-Umgebung (z. B. E-Mail, Internet-Zugang der Mitarbeiter) explizit zugelassen oder toleriert, ist vor allem auf die dann anfallenden Beschränkungen und die notwendigen Vereinbarungen zwischen Institution und Mitarbeitern mit Bezug zu Protokollierung und Auswertung zu achten.

Möglich für die Auswertung von Protokolldaten ist die Nutzung sogenannter SIEM-Tools (Security Information Event Management) oder Log Analyzer. Auch diese setzen jedoch eine angemessene Konfiguration der Protokollierung in den angebundenen Plattformen voraus.

Prüffragen:

- Ist ein Protokollierungs- und Auswertungskonzept für die Lotus Notes/ Domino-Umgebung vorhanden und umgesetzt?
- Bestehen Regelungen zum Umgang mit der privaten Nutzung?

# M 4.428 Audit der Lotus Notes/Domino-Umgebung

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Datenschutzbeauftragter, Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter, Revisor

Um festzustellen, ob der tatsächliche Status der Sicherheit der Lotus Notes/Domino-Umgebung den Anforderungen entspricht, und eventuelle Schwachstellen zu identifizieren, ist es erforderlich, periodisch Audits und Sicherheitsüberprüfungen der Lotus Notes/Domino-Umgebung durchzuführen.

Unterschieden wird dabei zwischen intern initiierten und extern initiierten Audits und Sicherheitsüberprüfungen. Erstere werden in der Regel im Rahmen des Informationssicherheitsmanagement-Prozesses oder im Rahmen von Revisionstätigkeiten initiiert und abgearbeitet, während letztere häufig Bestandteil externer Prüfungen, z. B. durch Aufsichtsbehörden, Wirtschaftsprüfer oder auch Lizenzgeber (siehe dazu die Maßnahme M 2.493 *Lizenzmanagement und Lizenzierungsaspekte in der Beschaffung für Lotus Notes/Domino*) sind.

Externe Audits haben in der Regel als Ziel, die Einhaltung gesetzlicher und regulatorischer Vorgaben oder vertraglicher Regelungen zu überprüfen. Sie können auch als Voraussetzung für die Teilnahme an elektronischem Datenaustausch, Zahlungsverfahren, Handelssystemen, zur Gewährung besonderer Konditionen oder zum Abschluss IT-bezogener Versicherungen sein.

Die besondere Stellung des Datenschutzes rechtfertigt häufig auf Datenschutz bezogene Schwerpunkt-Audits. Diese können auch ein Datenschutz-Audit der Lotus Notes/Domino-Umgebung beinhalten, da vielfach mit Lotus Notes/Domino personenbezogene Daten verarbeitet und gespeichert werden.

Audits sind nach Möglichkeit mit entsprechendem Vorlauf zu planen. Rechtliche Aspekte der Audits sind im Vorfeld zu klären und zu bewerten. Eine Abstimmung mit dem Datenschutzbeauftragten und der Personalvertretung kann bei bestimmten Audits erforderlich sein.

Audits (insbesondere externe) sind grundsätzlich durch das Informationssicherheitsmanagement zu begleiten. Umfang und inhaltliche Gestaltung dieser Begleitung sind innerhalb des Informationssicherheitsmanagements vorab zu definieren und zu dokumentieren (beispielsweise für die Begleitung von Lizenzierungsaudits, Zertifizierungsaudits und Audits im Rahmen von Prüfungen durch die zuständigen Prüfungsstellen).

Es ist sicherzustellen, dass die Ergebnisse durchgeführter Audits in die Optimierung des Informationssicherheitsmanagement-Prozesses einfließen. Durch das Audit erkannte Schwachstellen und die mit diesen assoziierten IT-Risiken müssen den Verantwortlichen (Institutionsleitung, Leiter IT, IT-Sicherheitsbeauftragter, Fachverantwortliche) unverzüglich gemeldet werden.

Audits sind transparent und nachvollziehbar durchzuführen. Audits und Sicherheitsüberprüfungen, deren Durchführung gegebenenfalls Risiken für den IT-Betrieb oder für die Informationswerte der Institution beinhalten kann, wie z. B. Penetrationstests, müssen unter Berücksichtigung der Rechtslage und der im Vorfeld durchgeführten Risikobewertung geplant und durchgeführt werden.

Audits der Lotus Notes/Domino-Umgebung können einen ganzheitlichen Ansatz verfolgen oder punktuell besonders sicherheitssensitive Bereiche prüfen. Der ganzheitliche Ansatz kann z. B., ausgehend von den durch Notes/Domino unterstützten Geschäftsprozessen, eine Bewertung des Sicherheitsmanagements im Umfeld von Lotus Notes/Domino auf Prozessebene und auf technischer Ebene vornehmen. Punktuelle Audits können im Detail Konfigurationen und Verfahren im Umfeld besonders sicherheitssensitiver Komponenten oder Dienste prüfen (z. B. die Zertifikatsverwaltung oder die Konfiguration der Lotus Notes/Domino-Sicherheitsmechanismen).

Prüffragen:

- Existiert eine dokumentierte Planung zur Auditierung der Lotus Notes/ Domino-Umgebung?
- Ist die Zuständigkeit für die Begleitung externer Audits definiert?
- Ist inhaltlich festgelegt, wie externe Audits begleitet werden?

# M 4.429 Sichere Konfiguration von Lotus Notes/Domino

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Unmittelbar nach der Installation, Anpassung oder Migration ist die Konfiguration der installierten bzw. angepassten oder migrierten Komponenten vorzunehmen. Nur so kann gewährleistet werden, dass in der Zeitspanne zwischen Installation und Konfiguration keine Schwachstellen der Standardkonfiguration für Angriffe genutzt werden.

**Sichere Grundkonfiguration**

Die sichere Grundkonfiguration des Lotus Domino Servers beinhaltet die Korrektur voreingestellter, unsicherer Systemparameter:

- Standardmäßig ist der anonyme Zugriff auf Domino-Server zu verweigern. Werden keine xACLs genutzt (in diesem Fall wird bei der Einrichtung der xACLs der anonyme Zugriff unterbunden), ist bei der Domino-Installation die Gruppe ANONYMOUS standardmäßig auf NO ACCESS zu setzen. Zugriffe von Lotus Notes-Benutzern, deren Zertifikate von unbekannten Zertifizierungsinstanzen ausgestellt wurden und für die kein Cross-Zertifikat existiert, werden von Domino als anonyme Zugriffe behandelt. Sollen für einzelne Datenbanken anonyme Zugriffe erlaubt werden, ist dies auf Datenbankebene explizit freizuschalten. Ist anonymer Zugriff auf dedizierte Server gewünscht, sind diese in der Gesamtarchitektur entsprechend zu planen und über andere Sicherheitsmaßnahmen abzusichern. Insbesondere sollten diese Server keine Dienste mit hohem Schutzbedarf bereitstellen.
- Für die Hashwerte der HTTP-Passwörter ist das sicherere Hash-Format mit Salt-Wert zu wählen (verfügbar seit Notes 4.6). Dies geschieht über *Actions -> Edit Directory Profile* und Auswahl von *Yes* bei der Checkbox *Use more secure Internet password format*. Siehe dazu auch die Technote 1244808 des Herstellers.

Weiterhin sind im Rahmen der sicheren Grundkonfiguration die Einstellungen zur Zugriffssicherheit vorzunehmen, die auf Ebene des Lotus Notes/Domino-Servers (und nicht auf der Ebene der Domino-Dienste) greifen:

- Der Abgleich des öffentlichen Schlüssels der Notes-ID des Benutzers bei der Anmeldung mit der im Namens- und Adressbuch gespeicherten Kopie des öffentlichen Schlüssels ist standardmäßig zu aktivieren.
- Der Zugriff auf den Server ist auf Benutzer einzuschränken, die im Namens- und Adressbuch des Servers stehen.
- Die serverseitige Überprüfung des Passwortes der Notes-ID über Hashwert ist zu aktivieren. Dies birgt das Risiko, dass bei Kopie der ID und Kompromittierung des Notes-Passwortes durch einen Angreifer nach einer Passwortänderung durch den Angreifer nur noch die ID des Angreifers als legitime ID akzeptiert wird.
- Access/Deny-Listen sind sowohl für Server wie auch für Benutzer einzurichten und zu pflegen. Dadurch können unerwünschte Verbindungen bereits beim Zugriff auf den Server zurückgewiesen werden (z. B. für IDs ausgeschiedener Mitarbeiter oder bei zeitlich beschränktem Zugriff nach Ablauf der vorgesehenen Zeitspanne).
- Der Einsatz von Vermittlungsservern (*Pass-Through*) ist zu vermeiden, möglichst über eine sicherheitsorientierte Architektur und Netztopologie der eingesetzten Lotus Notes/Domino-Plattform und die Einschränkung

des Pass-Through-Zugriffes auf definierte Benutzergruppen. Eine generelle Vermittlung für alle anfragenden Server (*Routing über Server* = *) ist unbedingt zu vermeiden.
- Bestimmte Server-Operationen können auf eine Liste von Benutzern oder Gruppen eingeschränkt werden. Beispiele für solche Operationen sind das Anlegen von Datenbanken, das Erzeugen von Repliken, die Nutzung von Monitoren, die Administration über die Web-Schnittstelle und das Ausführen von Agenten und Skripten. Je nach Option kommen verschiedene Vorgaben zum Einsatz, wenn keine explizite Liste angegeben wird. Beispielsweise dürfen standardmäßig alle Benutzer neue Datenbanken anlegen.
- Die Zugriffsrechte auf das Namens- und Adressbuch (Abkürzung: NAB, Datei *names.nsf*) sind möglichst restriktiv zu vergeben, auch wenn dies Kompromisse bei der Nutzung verschiedener Funktionen durch die Benutzer zur Folge hat.
- Administrative Zugriffsrechte sind unter Verwendung der administrativen Rollen *[GroupCreator]*, *[GroupModifier]*, *[ServerCreator]*, *[ServerModifier]*, *[UserCreator]*, *[UserModifier]*, *[NetCreator]* und *[NetModifier]* entsprechend dem Administrationskonzept für Lotus Notes/Domino zu vergeben.

**Sichere Konfiguration serverseitiger Einstellungen für die Kommunikation**

Angemessene Kommunikationssicherheit kann über eine SSL-verschlüsselte Verbindung mit einem durch ein Zertifikat authentisierten Kommunikationspartner gewährleistet werden.

Ein Domino-Server kann über die Einrichtung der Serverzertifikatsadministration (certsrv.nsf) für die Nutzung von SSL konfiguriert werden. Voraussetzung ist die Umsetzung des Konzepts zur Domänen- und Zertifikatshierarchie aus M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino*. Anschließend kann auf Protokoll-Ebene (z. B. E-Mail-Protokolle IMAP, POP3, SMTP) individuell konfiguriert werden, für welche Protokolle SSL zu aktivieren ist. Dies sollte in Abhängigkeit des Schutzbedarfs der genutzten Dienste erfolgen.

Das Erzwingen von SSL-Verbindungen kann für Web-Zugriffe auch auf Datenbankebene eingestellt werden (*Web: SSL-Verbindung anfordern*). Die SSL-Anschlusskonfiguration sollte möglichst nicht auf *Nur-Server-Authentifizierung*, sondern auf *Clientzertifikatsauthentifizierung* als Authentifizierungsverfahren konfiguriert werden (nicht alle Protokolle unterstützen die Clientzertifikatsauthentifizierung).

Folgende serverseitigen Parameter sind konform zu den Verschlüsselungsrichtlinien der Institution zu konfigurieren:

- Version des SSL-Protokolls (möglichst nur SSL3.0, da Verschlüsselungsverfahren für SSL 2.0 in Domino nicht einstellbar),
- SSL-Site-Zertifikate annehmen (Einstellung *NEIN*, um den Zugriff auf Internet-Server ohne gemeinsame Zertifikate zu unterbinden),
- Abgelaufene SSL-Zertifikate annehmen (Einstellung in der Regel *JA*, um Probleme mit abgelaufenen Clientzertifikaten zu vermeiden, NEIN bei hohem und sehr hohem Schutzbedarf),
- SSL-Verschlüsselungscodes (gemäß dem institutionseigenen Verschlüsselungskonzept, grundsätzliches Vermeiden der *no encryyption with MD5 MAC*, *no encryption with SHA-1 MAC* und der 40-Bit RC4 wie auch der 56-Bit-DES-Verschlüsselung).

**Sichere Dienstekonfiguration**

Domino bietet unter anderem folgende Dienste an:

- E-Mail-Dienste (Notes Mail, POP3-Mail, SMTP-Mail, IMAP-Mail)
- Web-Dienste (Webserver, Instant Messaging und Presence, News (NNTP), Web Services konform zum W3C-Standard SOAP 1.1, WebDAV)
- Datenbank-Dienste (inklusive Datenbankreplizierung und DB2-Anbindung)
- DAOS (Domino Attachment and Object Service)
- Groupware-Dienste
- Directory- und CA-Dienste (Dienste der Zertifikatshierarchie) inklusive LDAP-Schnittstelle

Eine sichere Dienstekonfiguration muss sowohl die üblichen Standards zur sicheren Parametrisierung der Dienste berücksichtigen wie auch den Kontext im Rahmen der Sicherheitsarchitektur, in dem dieser Dienst betrieben wird. So kann sich die Konfiguration eines E-Mail- oder Instant-Messaging-Dienstes, der nur unternehmensintern genutzt wird und auf einem Domino-Server ohne Außenanbindung betrieben wird, erheblich von der Konfiguration des gleichen Dienstes unterscheiden, der auf einem Server in der DMZ zur Abwicklung des E-Mail-Verkehrs und zur Instant-Messaging-Anbindung an das Internet betrieben wird.

Es ist daher erforderlich, für jeden Dienst eine Sicherheitsbetrachtung vorzunehmen, die nicht nur den Schutzbedarf des Dienstes, sondern auch den Schutzbedarf des Domino-Servers (und damit der weiteren Dienste, die auf demselben Domino-Server laufen) berücksichtigt. Dazu sind die in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* beschriebenen Empfehlungen, vor allem die dort enthaltene Konzeption zur Absicherung der genutzten Domino-Dienste, umzusetzen.

Für jeden Dienst ist in dem entsprechenden Konzept zur Absicherung sowohl ein Berechtigungskonzept für den Zugriff auf den Dienst (Zugriffskonzept) zu erstellen, als auch die dienstspezifischen Parameter sicher zu konfigurieren. Hierbei sind insbesondere unsichere Voreinstellungen der Software zu bereinigen. Die Umsetzung dieses Konzeptes hat für jeden Domino-Dienst direkt nach der Installation des Dienstes zu erfolgen.

Nicht benötigte Dienste sollten, wenn möglich, nicht installiert werden, indem bereits eine passende Grundinstallation ausgewählt wird. Ist dies nicht möglich, sind die entsprechenden Server Tasks zu deaktivieren.

**Sichere Client-Konfiguration**

Für die Lotus Notes/Domino-Plattform können unterschiedliche Clients eingesetzt werden. Dabei ist nach Einsatzzweck zwischen folgenden Arten zu unterscheiden:

- administrative Clients
- Entwickler-Clients
- Clients für Endnutzer

Aus technologischer Sicht ist zu unterscheiden zwischen:

- proprietären Notes Clients
- Eclipse-basierten Clients (ab Notes 8)
- Browsern als Clients
- proprietären Clients auf PDAs und Smartphones

- fremden E-Mail-Clients, die über IMAP und POP3 auf den Domino-Server zugreifen

Grundsätzlich sind alle eingesetzten Client-Typen gemäß dem institutionsspezifischen, in M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* erwähnten Härtungskonzept und Konfigurationsvorgaben abzusichern. Für Clients, die in Zusammenhang mit Push-Diensten betrieben werden, sind bei der Konfiguration auch die clientseitigen Parameter des Konzeptes zur Nutzung von Push-Diensten aus M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* zu berücksichtigen.

Bereits bei der Architekturplanung ist festzulegen, welche Client-Typen zum Einsatz kommen sollen. Dabei ist zu berücksichtigen, dass abhängig vom Einsatzzweck und dem Schutzbedarf der Clients eine unterschiedliche Konfiguration erforderlich sein kann. Grundsätzlich sind administrative und andere hoch schutzbedürftige Clients restriktiver abzusichern.

In der Client-Konfiguration sind Schwachstellen, die durch unsichere Voreinstellungen entstehen, zu beheben. Weiterhin sind die Parameter zum Aufbau einer sicheren Verbindung, Replikationsparameter und die Parameter zur Notes-basierten Verschlüsselung aller clientseitiger Daten zu berücksichtigen. Hier sind die Vorgaben der Planung der Kommunikationssicherheit aus M 2.206 *Planung des Einsatzes von Lotus Notes/Domino*, des Konzeptes zur Absicherung der Domino-Dienste aus M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* und des Konzeptes zur Nutzung der Notes/Domino-eigenen Sicherheitsmechanismen aus M 2.207 *Sicherheitskonzeption für Lotus Notes/Domino* (u. a. für die Verschlüsselung der clientseitigen Daten) zu beachten.

Wird erstmalig der Full Client genutzt, so ist der bislang nicht vorhandenen Komplexität Rechnung zu tragen und eine detaillierte Konfigurationsvorgabe (idealerweise mit einem entsprechenden Schulungsangebot für die Benutzer) für den Rollout vorzubereiten.

Prüffragen:

- Sind für alle genutzten Dienste Konfigurationsvorgaben vorhanden und umgesetzt, die die entsprechenden Konzepte zur Diensteabsicherung abbilden?
- Sind für alle genutzten Clients Konfigurationsvorgaben vorhanden?
- Wenn auf Clients besonders schützenswerte Informationen (Schutzbedarf "sehr hoch") vorgehalten werden (z. B.. über Replikation), sind diese angemessenen zu verschlüsseln?

# M 4.430 Analyse von Protokolldaten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In einem Informationsverbund wird in der Regel eine große Menge an Protokolldateien generiert.

Bevor die Protokollierungseinträge ausgewertet werden können, muss eine Normalisierung der Daten durchgeführt werden. Durch eine Normalisierung werden die unterschiedlichen Datenformate der protokollerzeugenden Systeme in ein einheitliches Format überführt. Vor der Auswertung ist es zudem wichtig, dass die relevanten Daten eingegrenzt werden, um die Masse der Protokolldaten zu reduzieren. Dies wird mit Hilfe von Filtermöglichkeiten, Aggregation und Korrelation der Daten bewirkt (siehe M 4.431 *Auswahl und Verarbeitung relevanter Informationen für die Protokollierung*). Besonders wichtig sind diese Maßnahmen, wenn an zentraler Stelle protokolliert wird.

Ein weiterer wichtiger Punkt bei der Analyse der Protokolldaten ist die Zeitsynchronisation. Um Angriffe oder Fehlfunktionen über mehrere IT-Systeme und Anwendungen hinweg erkennen zu können, sollte auf jedem System eine identische Uhrzeit eingestellt sein. Damit auch in einem großen Informationsverbund alle Systeme zeitsynchron sind, kann auf zentrale Zeitserver zurückgegriffen werden (siehe auch M 5.172 *Sichere Zeitsynchronisation bei der zentralen Protokollierung*). Diese stellen die Systemzeit zum Beispiel über das Network Time Protokoll (NTP) zur Verfügung (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*). Alle weiteren Systeme im Informationsverbund können damit synchronisiert werden.

Für eine Alarmierungsfunktion müssen die protokollierten Informationen zeitnah ausgewertet werden. Bei der Auswertung werden sicherheitskritische Ereignisse ohne Zeitverzögerung betrachtet. Zusätzlich werden auch relevante Daten aus bereits bestehenden Protokolldateien extrahiert und für die Analyse verwendet. Besonders Abweichungen vom Normalverhalten, Konfigurationsfehler und Fehlermeldungen müssen bei der Analyse berücksichtigt werden, um eine Übersicht über alle relevanten Ereignisse innerhalb eines Informationsverbundes zu erhalten.

Um einen relevanten Protokollierungseintrag zeitnah identifizieren zu können, ist es möglich, geeignete Algorithmen und Analysetechniken wie Signaturerkennung und Schwellwertanalyse einzusetzen. Diese Techniken werden häufig von IT-Frühwarnsystemen genutzt. Sobald ein Angriff erkannt wird, sollte ein Alarm ausgelöst werden, sodass ein unmittelbares Eingreifen gegen die Bedrohung möglich ist.

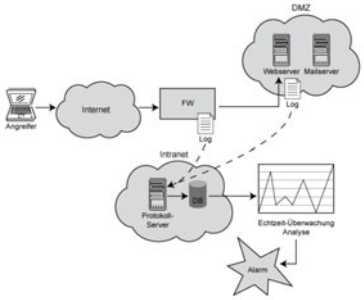



Abbildung: Grundlegender Ablauf bei einem IT-Frühwarnsystem

Um die Ereignisse und die Protokollierungseinträge für eine mögliche Beweissicherung nachvollziehen zu können, sollte nach der Auswertung ein Bericht erstellt werden. Viele Protokollierungsapplikationen bieten eine Web-Schnittstelle an, um das Ergebnis der Analyse auch grafisch darstellen zu können. Dadurch können mögliche Trends besser erkannt werden. Über die Web-Schnittstelle können auch beliebige Auswertungsansichten ("Views") und Filter definiert werden.

Werden die Protokolldaten zentral analysiert, ist es möglich, komplexe Zusammenhänge im Informationsverbund zu erkennen und nach Betriebs- oder Sicherheitsvorfällen innerhalb eines Informationsverbundes zu suchen. Daher sollten die Protokolldaten für zukünftige Auswertungen archiviert werden. Neben den eigenen Anforderungen an die Aufbewahrungsdauer muss im Vorfeld auch überprüft werden, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokolldateien gelten. Um die Nachvollziehbarkeit von Aktionen zu gewährleisten, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch eine Löschungspflicht geben (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Prüffragen:

- Werden die Daten vor der Auswertung normalisiert?
- Wird der Informationsverbund zeitsynchron betrieben?
- Wird nach der Auswertung der Protokolldaten ein Bericht erstellt?
- Werden die Protokolldaten für zukünftige Auswertungen archiviert?
- Werden bei der Archivierung der Protokolldaten gesetzliche Regelungen berücksichtigt?

# M 4.431 Auswahl und Verarbeitung relevanter Informationen für die Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Protokolldaten müssen aussagekräftige Informationen enthalten. Dabei spielt es keine Rolle, ob sie lokal oder zentral erfasst oder ob sie für ein IT-Frühwarnsystem bereitgestellt werden. Welche Ereignisse protokolliert werden, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab und muss in der Institution vorab abgestimmt und festgelegt werden (siehe M 2.500 *Protokollierung von IT-Systemen*). Unter anderem sind die folgenden Ereignisse besonders zu beachten:

- falsche Passworteingabe für eine Benutzer-Kennung,
- Sperrung einer Benutzer-Kennung,
- Versuche von unberechtigten Zugriffen,
- Ausfall oder Störungen der Hardware,
- Daten zur Netzauslastung und -überlastung sowie
- Informations- oder Warnmeldungen von Intrusion Detection Systemen.

Ein IT-Frühwarnsystem kann aus all diesen Ereignissen Meldungen extrahieren, sie qualifizieren und übersichtlich aufbereiten. Dazu werden die Protokolldaten vorab gefiltert, normalisiert, aggregiert und kategorisiert.

### Filterung

Beim Filtern der gesammelten Protokolldaten werden unnötige Protokollmeldungen aussortiert. Dies ist notwendig, da die Menge der anfallenden Protokolldaten zu groß ist, um alle Informationen verarbeiten zu können. Die Filtereinstellungen können meist am zentralen Protokollierungsserver beziehungsweise am IT-Frühwarnsystem geregelt werden. Die Einstellungen müssen an die Gegebenheiten des Informationsverbundes angepasst und sollten nur von gut geschulten Administratoren durchgeführt werden. Es dürfen nicht zu viele, aber auch nicht zu wenig Protokollereignisse aussortiert werden. Des Weiteren sollten die Filtereinstellungen regelmäßig überprüft und aktualisiert werden, zum Beispiel, wenn neue Server zum zentralen Protokollserver beziehungsweise zum IT-Frühwarnsystem hinzugefügt oder alte Server außer Betrieb genommen werden.

### Normalisierung

Um die Daten weiterverarbeiten und beispielsweise in einer Datenbank speichern zu können, müssen alle anfallenden Protokollmeldungen in ein einheitliches Datenformat konvertiert werden. Dieser Vorgang wird Normalisierung genannt. Die Meldungen unterscheiden sich von Hersteller zu Hersteller. Allerdings bestehen auch große Unterschiede zwischen Protokolldaten von Betriebssystemen und Applikationen.

### Aggregation

Um die Daten weiter zu verarbeiten, folgt die Aggregation. Hier werden Protokollmeldungen mit identischem Inhalt zu einem Datensatz zusammengefasst. Oft werden vom gleichen System mehrmals hintereinander identische Protokollmeldungen erzeugt, was einen geringeren Informationswert für die nachfolgenden Meldungen bedeutet. Aus diesem Grund wird nur die erste Protokolldatei weiterverarbeitet. Allerdings ist es wichtig, die erste Protokollmeldung

um die Anzahl der aufgetretenen redundanten Ereignisse zu ergänzen, um feststellen zu können, wie häufig die identischen Protokollmeldungen aufgetreten sind.

**Kategorisierung und Priorisierung**

Nachdem die Daten gefiltert, normalisiert und aggregiert wurden, sollten diese kategorisiert und priorisiert werden. Dadurch lässt sich der Informationsgehalt der Meldung erhöhen. So können beispielsweise Meldungen durch Zoneninformationen wie DMZ oder Hochsicherheitsbereich priorisiert und bei der Auswertung bevorzugt berücksichtigt werden. Zusätzlich lassen sich die Meldungen in einen System-Typ, wie Sicherheitsgateway, Betriebssystem oder Applikationen einordnen.

**Korrelation der Daten**

Eine wesentliche Anforderung des Protokollservers beziehungsweise des IT-Frühwarnsystems ist die Korrelation der Protokollmeldungen aus Protokolldatenquellen, bei der unterschiedliche Ereignisse miteinander verknüpft werden. Innerhalb eines Informationsverbundes haben die separaten Sicherheitskomponenten, wie Sicherheitsgateways, Intrusion-Detection-/-Prevention-Systeme und Antiviren-Gateways nur eine beschränkte Sicht auf ihre jeweilige Funktion. Deshalb sollten die entsprechenden Protokolldaten korreliert werden. Ein Beispiel für korrelierte Protokolleinträge wäre die Verbindung von Sicherheitsgateway- und Router-Protokolldaten mit Accounting-Informationen von einem kompromittierten System.

Korrelation kann auf verschiedenen Ebenen stattfinden:

- Korrelierung innerhalb der gleichen Geräteklasse (z. B. Sicherheitsgateways): Hierbei wird analysiert, ob Auslastungen und abnormes Verhalten innerhalb der Geräteklasse auftreten. Daraus werden beispielsweise Trendreports erzeugt.
- Eine Korrelation über Geräteklassen mit ähnlichen Datenfeldern (z. B. Sicherheitsgateways und Router): Hier lässt sich der Ablauf eines Angriffs erweitert analysieren.
- Eine Korrelation über verschiedene Geräteklassen: Erst dies ermöglicht einen umfassenden Einblick auf Transport- und Applikationsebene. Beispielsweise meldet der Virenscanner eines Arbeitsplatzrechners einen Wurm und dessen Quarantäne. Danach meldet das IDS einen Anstieg von Netzwerkverkehr auf einem dedizierten Port, ausgehend vom System mit dem Malware-Befall. Ohne Korrelation könnten diese beiden Einzelmeldungen als irrelevant eingestuft werden oder in der Menge an Protokollmeldungen untergehen.

Prüffragen:

- Werden alle sicherheitsrelevanten Ereignisse nach den Vorgaben der Institution protokolliert?
- Werden die Filtereinstellungen nur durch ausreichend geschulte Administratoren an die Gegebenheiten des Informationsverbundes angepasst?
- Findet eine regelmäßige Überprüfung und Aktualisierung der Filtereinstellungen statt?

# M 4.432 Sichere Konfiguration von Serverdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nachdem das Betriebssystem des Servers installiert (siehe M 2.318 *Sichere Installation eines IT-Systems*) und konfiguriert wurde, muss der eigentliche Serverdienst eingerichtet werden. Bei Serverdiensten handelt es sich um ausgeführte Prozesse, die den Clients bestimmte Funktionen zur Verfügung stellen. Beispiele hierfür sind Web-, E-Mail- und Verzeichnisdienste.

Serverdienste können in zwei unterschiedlichen Kategorien aufgeteilt werden. Serverdienste der ersten Kategorie stellen ihre Funktion frei im Netz zur Verfügung, ohne dass sich die Benutzer hierfür authentisieren müssen. Beispiele hierfür sind DNS-, DHCP- oder NTP-Server. Die zweite Kategorie erfordert hingegen eine Authentisierung der Benutzer vor der Benutzung des Dienstes, z. B. um vertrauliche Informationen vor unbefugtem Zugriff zu schützen. Beispiele hierfür sind Datei-, E-Mail-, SSH- oder RDP-Server. Ob und welche Form der Authentisierung für die Nutzung eines Serverdienstes erforderlich ist, hängt von der Art des Dienstes, der Konfiguration des jeweiligen Dienstes und dem Schutzbedarf der Daten ab.

Generell sollten alle vorhandenen, aber nicht benötigten Serverdienste deinstalliert werden, der Server sollte nur die zwingend benötigten Dienste zur Verfügung stellen. Neben dem eigentlichen Serverdienst wird in der Regel zusätzlich ein Serverdienst zur Administration auf dem IT-System benötigt. Vertiefende Informationen hierzu sind in M 4.97 *Ein Dienst pro Server* zu finden.

Bevor der neue Serverdienst z. B. aus der Paketverwaltung oder aus anderen Quellen installiert wird, sollte dessen Dokumentation gesichtet werden, falls dies noch nicht geschehen ist. Hierbei sollte unter anderem ermittelt werden, welche Dateien für den Betrieb des Dienstes benötigt und welche Prozesse gestartet werden. Erst hiernach sollte mit der Konfiguration des eigentlichen Serverdienstes begonnen werden.

**Restriktive Vergabe von Rechten**

Damit ein Server den Clients bestimmte Informationen oder Funktionen bereitstellen kann, benötigt der Serverdienst in der Regel zahlreiche Informationen, die im Dateisystem des Servers abgelegt werden müssen. Hierzu gehören:

- ausführbare Dateien, mit denen der Serverdienst gestartet oder verwaltet werden kann, sowie diverse Hilfsapplikationen, die für den Betrieb des Servers hilfreich sein können,
- Konfigurationsdateien oder -Einträge, die das Verhalten des Serverdienstes steuern,
- Protokolldateien, in denen der Serverdienst bestimmte Ereignisse, die eingetreten sind, ablegt, und
- Nutzdaten mit den eigentlichen Informationen, die der Serverdienst bereitstellt.

Die Rechte auf diese Informationen müssen so restriktiv wie möglich vergeben werden. Nur Prozesse und Benutzer, die auf diese Informationen zugreifen müssen, sollten hierauf auch zugreifen können. Der Zugriff sollte auf ein Mindestmaß beschränkt werden. Um Zugriffsrechte ressourcenschonend an eine Vielzahl von Benutzern zu vergeben, empfiehlt sich die Einrichtung von Gruppen oder Rollen. Rechte können jedoch auch an einzelne Benutzerkon-

ten oder auf Grundlage vordefinierter IP-Adressen oder -Adressbereiche zur Authentisierung vergeben werden.

Damit ein Serverdienst Funktionen anbieten kann, muss ein Prozess, der auf die benötigten Informationen und anderen Ressourcen zugreifen kann, gestartet werden. Die Zugriffsrechte des Prozesses werden in der Regel von den Zugriffsrechten des Benutzers, der den Prozess gestartet hat, abgeleitet. Normalerweise benötigt ein Prozess keine Schreibrechte auf Betriebssystem-Verzeichnisse und sollte deshalb diese auch nicht besitzen. Oft ist es aber so, dass ein privilegierter Benutzer mit Schreibrechten in Betriebssystem-Verzeichnissen den Prozess starten muss, um beispielsweise TCP- oder UDP-Ports zu öffnen. Wenn möglich, ist in diesem Fall dafür zu sorgen, dass der Prozess nach dem Start an einen unprivilegierten Benutzer übergeben wird.

Kann nur ein privilegierter Benutzer den Prozess und somit den Serverdienst starten, sollte der Prozess nach Möglichkeit in eine chroot-Umgebung, Sandbox oder ähnliche Umgebung "eingesperrt" werden. Bei einer chroot-Umgebung handelt es sich um einen abgeschotteten Bereich innerhalb des Computersystems, die es einem Angreifer erschwert, nach der Kompromittierung des Serverdienstes Zugriff auf das gesamte System zu erlangen. Eine chroot-Umgebung erfordert allerdings, dass alle vom Serverdienst benötigten Dateien ebenfalls im Verzeichnis des Serverdienstes und somit im abgeschotteten Bereich abgelegt werden. Vertiefende Informationen hierzu sind in M 4.198 *Installation einer Applikation in einem chroot Käfig* zu finden.

**Abhängigkeiten zu Bibliotheken, Betriebssystemaufrufe und externe Ressourcen**

In den Installationspaketen von Serverdiensten sind zahlreiche Dateien integriert, die bei der Installation auf das Zielsystem kopiert werden. Darüber hinaus werden in der Regel oft weitere Dateien benötigt, um den Serverdienst ausführen zu können. Hierzu gehören beispielsweise Applikationen und Bibliotheken von Drittentwicklern oder aus dem Betriebssystem. Obwohl in der Regel schon bei der Installation des Serverdienstes automatisch geprüft wird, ob alle benötigten Dateien vorhanden sind, sollte vorab zusätzlich manuell überprüft werden, ob diese wirklich vorhanden sind.

Wird beispielsweise ein vorhandener Serverdienst durch eine aktuellere Version ersetzt, ist darauf zu achten, dass weiterhin alle Dateien, die zu dessen Nutzung benötigt werden, vorhanden sind. Durch eine Aktualisierung kann es auch passieren, dass der Serverdienst Zugriff auf zusätzliche Dateien benötigt, die vor der Aktualisierung noch nicht erforderlich waren. Eine Aktualisierung kann auch dazu führen, dass neuere Versionen einer Bibliothek zwingend benötigt werden. Im Allgemeinen sollte im Zuge einer Aktualisierung nicht nur der Serverdienst, sondern alle zugehörigen Applikationen und Bibliotheken aktualisiert werden. Nutzt beispielsweise der Serverdienst eine Bibliothek, von der Schwachstellen bekannt sind, kann hierdurch ebenfalls der Serverdienst anfällig für Angriffe sein.

Betriebssystemaufrufe durch den Serverdienst sollten so weit wie möglich vermieden werden. Wenn sie nötig sind, ist darauf zu achten, dass z. B. durch Command-Injection-Angriffe keine kompromittierenden Anweisungen auf dem Server ausgeführt werden. Diese Anweisungen sollten so restriktiv wie möglich gefiltert werden.

Oft werden Serverdienste nicht autark eingesetzt, sondern sind auf externe Ressourcen angewiesen. Hierzu gehören beispielsweise

- Serverdienste, die von Authentisierungsservern, Webservern oder Web-Anwendungsservern, abhängig sind,
- Web-Anwendungsserver, die von Datenbankservern abhängig sind, oder
- Fileserver, die von Speichernetzen abhängig sind.

Bei einem Ausfall solcher Serverdienste oder der Anbindung hieran kann unter Umständen auch der darauf zugreifende Serverdienst ausfallen. Besonders bei einem höheren Schutzbedarf bei Verfügbarkeit kann eine redundante Anbindung oder eine redundante Auslegung der nachgelagerten Serverdienste nötig sein.

**Einschränkung der Erreichbarkeit**

Viele Serverdienste, die Informationen in einem Netz bereitstellen, können so konfiguriert werden, dass sie nur an einer oder wenigen Netzschnittstellen lauschen, beziehungsweise dass sie hieran "gebunden" werden. Netzschnittstellen können physische Netzkarten oder logische Verknüpfungen, wie virtuelle Netzkarten oder loopback-Schnittstellen, sein. Verfügt ein IT-System über mehrere Schnittstellen und wird der Netz-Serverdienst nur an eine gebunden, nimmt der Netz-Serverdienst keine Verbindungsanfragen an einer anderen Netzschnittstelle an, solange keine Portweiterleitungen oder Ähnliches erfolgen. Dadurch kann der Zugriff auf Netz-Serverdienste so eingeschränkt werden, dass nur Benutzer aus bestimmten Netzbereichen zugreifen können. Daher sollte generell ein Netz-Serverdienst nur an so wenige Netzschnittstellen wie möglich gebunden werden. Soll ein Netz-Serverdienst nur innerhalb des lokalen IT-Systems genutzt werden, darf dieser Dienst nur an der loopback-Schnittstelle gebunden werden. Beispiele für lokale Netzdienste können Super- (wie inetd), X-, Druck- oder Zeitserver sein.

Der Zugriff auf einen Netzdienst kann auch über Paketfilter beschränkt werden. Generell sollten nur berechtige IT-Systeme auf einen Netzdienst zugreifen dürfen. Soll das IT-System, auf dem der Netzdienst betrieben wird, nur Verbindungsanfragen von bestimmten IT-Systemen über festgelegte Portnummern annehmen dürfen, kann mit Paketfiltern der Verbindungsaufbau reguliert werden. Der Zugriff auf einen Backendserver kann beispielsweise so mit Paketfilterregeln beschränkt werden, dass nur der zugehörige Applikationsserver hierauf zugreifen kann. Paketfilter können in der Regel auch so konfiguriert werden, dass sie alle oder ausgewählte Verbindungsanfragen protokollieren. Vertiefende Informationen zu Paketfiltern sind in M 2.74 *Geeignete Auswahl eines Paketfilters* und M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* auf Minimum beschränken zu finden.

**Verschlüsselung der Authentisierung und Nutzdaten**

Je nach Serverdienst und bereitgestellten Ressourcen kann unterschieden werden, ob diese allen Benutzern oder nur einen ausgewählten Benutzerkreis zur Verfügung gestellt werden sollen. Abhängig vom Schutzbedarf müssen hierfür geeignete Authentisierungsverfahren ausgewählt werden. Typische Authentisierungsverfahren sind unter anderem (fälschbare) IP-Adressen, Benutzername und Passwort oder Zertifikate. Generell sollten alle Informationen, die für eine Authentisierung gegenüber dem Serverdienst benötigt werden, verschlüsselt übertragen werden.

Werden Nutzdaten über unsichere Netze übertragen, sollte geprüft werden, ob diese ebenfalls verschlüsselt übertragen werden sollen. In der Regel werden z. B. DNS-, Routing- oder NTP-Informationen nicht verschlüsselt übertragen,

hingegen HTTP- oder IMAP/POP3-Informationen öfter, um deren Vertraulichkeit zu schützen. Es ist daher zu entscheiden, welche Nutzdaten verschlüsselt werden sollen. Generell wird empfohlen, immer zu verschlüsseln, wenn dies möglich ist, da der Aufwand oft nur unwesentlich höher ist.

Vertiefende Informationen zur Verschlüsselung sind unter anderem in M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation* zu finden.

**Einschränken der Versionsinformationen**

Standard-Fehlermeldungen bergen oft die Gefahr in sich, zu viel Information preiszugeben. Beispielsweise könnte ein Angreifer mit Hilfe von ausgegebenen Versionsinformationen nach Serverdiensten mit Schwachstellen suchen und diese ausnutzen.

Aus diesem Grund sollten, wenn möglich, alle Systemmeldungen so konfiguriert werden, dass sie keine Rückschlüsse auf die eingesetzte Softwareversion oder Konfiguration zulassen. Auch selbst erstellte Fehlermeldungen sollten die Benutzer über aufgetretene Fehler informieren, aber keine Details dazu preisgeben.

**Datensicherung**

Alle Informationen, die für eine Datenwiederherstellung benötigt werden, müssen regelmäßig gesichert werden, damit z. B. bei einem Hardwaredefekt oder einem unbeabsichtigten Löschen von Steuerdateien der Serverdienst zeitnah wieder in Betrieb genommen werden kann. Hierzu gehören mindestens

- Konfigurationsdateien,
- Nutzdaten und
- Protokolldaten.

Bei vielen Arten von Serverdiensten spielt die Verfügbarkeit der Nutzdaten eine besondere Rolle. Bei Datei-, E-Mail- oder Webservern sind dies Informationen, die im Gegensatz zu Konfigurationsdateien nicht ohne Weiteres neu erstellt werden können.

Bei einigen Serverdiensten ist es nicht ausreichend, die zu sichernden Dateien nur zu kopieren. Insbesondere wenn die zu sichernden Informationen in Datenbanken abgelegt werden, müssen alternative Sicherungsverfahren genutzt werden. Ein Beispiel hierfür sind TDB-Dateien unter Samba, deren Inhalte vom Serverdienst oft für längere Zeit zwischengespeichert und nicht immer auf der Festplatte zur Laufzeit aktualisiert werden (siehe auch M 6.135 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers*). Daher muss die Dokumentation des Serverdienstes für die korrekte Datensicherung konsolidiert werden.

**Updates**

Der eingesetzte Serverdienst sollte immer auf dem aktuellen Stand sein. Wurden Schwachstellen der eingesetzten Software entdeckt und diese mit einer neueren Version behoben, sollte zeitnah auf die fehlerbereinigte Version gewechselt werden. Bevor eine neue Version ausgerollt wird, sollte diese getestet werden. Nicht nur der eigentliche Serverdienst, auch nachgelagerte Serverdienste, das Betriebssystem und alle weiteren installierten Applikationen, sollten regelmäßig aktualisiert werden. Vertiefende Informationen sind in M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* zu finden.

**Protokollierung**

Sicherheitsrelevante Aktivitäten an Serverdiensten sollten aus vielen Gründen protokolliert werden. Zum einen hilft eine aktivierte Protokollierung, potentielle Schwachstellen frühzeitig erkennen und damit beseitigen zu können. Zum anderen kann Protokollierung dabei helfen, Verstöße gegen Sicherheitsvorgaben zeitnah zu erkennen oder Nachforschungen über einen Sicherheitsvorfall vorzunehmen.

Die Protokollierung des Serverdienstes sollte im Protokollierungskonzept integriert werden (siehe M 2.500 *Protokollierung von IT-Systemen*).

Je nach Serverdienst sollten mindestens folgende Ereignisse aufgezeichnet werden:

- Fehlgeschlagene Anmeldeversuche
- Fehlgeschlagene Zugriffe auf Ressourcen aufgrund von:
- - mangelnder Berechtigungen
  - nicht vorhandener Ressourcen
  - Server-Fehlern
  - Hardware-Engpässe und -Ausfälle
  - Sonstige Fehlermeldungen

Prüffragen:

- Wurden die Zugriffsrechte, die für den Betrieb eines Serverdienstes auf ausführbare Dateien, Konfigurations- und Protokolldateien sowie Nutzdaten benötigt werden, restriktiv vergeben?
- Sind alle Ressourcen, die für den Betrieb eines Serverdienstes benötigt werden, in einer aktuellen Version vorhanden?
- Kann der Netz-Serverdienst nur Verbindungen über notwendige Netzschnittstellen beantworten?
- Werden Authentisierungsinformationen für Serverdienste immer verschlüsselt übertragen?
- Werden alle für einen Serverdienst relevanten Informationen regelmäßig gesichert?
- Werden die sicherheitsrelevanten Ereignisse des Serverdienstes protokolliert?

# M 4.433 Einsatz von Datenträgerverschlüsselung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Vertrauliche Informationen auf wiederbeschreibbaren Datenträgern können auf verschiedene Weise verschlüsselt und damit vor unbefugter Kenntnisnahme geschützt werden. So kann beispielsweise der komplette Datenträger, eine einzelne Partition oder nur einzelne Dateien verschlüsselt werden. Aus Sicherheitssicht ist es besser, den kompletten Datenträger zu verschlüsseln, da dann weniger Benutzereingriffe erforderlich sind und alle Daten vor unbefugtem Zugriff geschützt sind. Die Verschlüsselung eines gesamten Datenträgers oder einer kompletten Partition ist für die Benutzer nahezu transparent. Lediglich beim Booten oder dem ersten Zugriff auf die Partition müssen sich die Benutzer authentisieren. Werden nur einzelne Dateien oder Dateicontainer verschlüsselt, besteht die Gefahr, dass versehentlich schützenswerte Daten in unverschlüsselten Bereichen der Festplatte abgelegt werden. Zudem muss hierfür ein Verschlüsselungsprogramm explizit von den Benutzern gestartet werden.

Auch wenn einzelne Partitionen komplett verschlüsselt werden, kann dies dazu führen, dass aus verschiedenen Gründen vertrauliche Informationen auf unverschlüsselten Partitionen landen. Daher ist eine vollständige Verschlüsselung von Datenträgern die beste und effizienteste Methode, um vertrauliche Daten zuverlässig vor unbefugtem Zugriff zu schützen.

Datenträgerverschlüsselung lässt sich mit Software, aber auch mit Hardware-Unterstützung umsetzen. Software-Lösungen sind z. B. BitLocker von Microsoft (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*) oder das vom BSI für die Verarbeitung von Daten bis zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH zugelassene TrustedDisk.

Mobile Datenträgern wie USB-Sticks und Laptops sollten möglichst immer vollständig verschlüsselt werden, auch wenn sie nur gelegentlich für vertrauliche Informationen eingesetzt werden. Bei stationären IT-Systemen sollten die Datenträger bei hohem Schutzbedarf bezüglich Vertraulichkeit komplett verschlüsselt werden. Bei der Verschlüsselung von Server-Festplatten sollte geprüft werden, ob die gewählte Variante der Verschlüsselung ausreichend leistungsfähig für die Anzahl der Benutzerzugriffe ist.

Neben dem Verschlüsselungsprogramm selbst sind für die Datenträgerverschlüsselung noch die kryptographischen Schlüssel nötig. Die kryptographischen Schlüssel sollten gemäß der Maßnahme M 2.46 *Geeignetes Schlüsselmanagement* sicher erzeugt und getrennt vom verschlüsselten Datenträger aufbewahrt werden. Hierfür können beispielsweise Chipkarten oder USB-Token eingesetzt werden. Eine solche Trennung ist bei der Verschlüsselung von USB-Sticks in der Regel nicht möglich, was bei der Sicherheitsanalyse berücksichtigt werden sollte.

Natürlich müssen auch die auf den verschlüsselten Datenträgern gespeicherten Daten regelmäßig gesichert werden (siehe M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*).

Einige Programme zur Datenträger- oder Partitionsverschlüsselung oder für den Einsatz von verschlüsselten Dateicontainern bieten die Möglichkeit, die verschlüsselten Bereiche zu "verstecken". Da solche Funktionen schwierig

anzuwenden sind und Fehlbedienung zu vollständigem Datenverlust führen kann, sollten sie nicht angewendet werden.

Prüffragen:

- Wurde eine geeignete Lösung zur Datenträgerverschlüsselung für alle mobilen Clients und mobilen Datenträger ausgewählt und installiert?
- Wurde eine geeignete Lösung zur Datenträgerverschlüsselung für alle stationären IT-Systeme ausgewählt und installiert, die Informationen mit einem mindestens hohen Schutzbedarf in der Kategorie Vertraulichkeit verarbeiten?

# M 4.434 Sicherer Einsatz von Appliances

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Als Appliance werden Geräte bezeichnet, die speziell für einen Einsatzzweck konstruiert worden sind, z. B. zum Einsatz als Firewall, Router, Paketfilter, NAS- oder VoIP-System. Dies bietet den Vorteil, dass Hard- und Software optimal aufeinander abgestimmt sind und sich die teilweise komplexen Abläufe für die Anwender einfach darstellen. Auch die Konfiguration wird meist weitgehend bereits durch die Hersteller vorgenommen. Sie werden häufig betriebsfertig ausgeliefert und können nach einigen elementaren Eingaben in Betrieb genommen werden. Appliances sind daher oft einfach zu installieren und zu bedienen. Umgekehrt ist bei einer Appliance allerdings auch die Konfiguration weniger flexibel und bietet dadurch weniger Möglichkeiten zur Anpassung an individuelle Bedürfnisse als eine Lösung, die (in Eigenregie oder durch einen Dienstleister) individuell aus IT-Komponenten zusammengestellt wurde.

Selbst zusammengestellte Geräte wie beispielsweise eine Firewall können oft auf handelsüblicher Hardware mit Standardbetriebssystemen und passenden Software-Komponenten installiert werden. Daher bieten sie eine hohe Flexibilität und sind für viele Anwendungsfälle gut geeignet. Die Installation und Integration der benötigten Komponenten kann jedoch fehlerträchtig sein. Ein weiterer Nachteil ist, dass bei Support-Anfragen meist unterschiedliche Ansprechpartner für die einzelnen Komponenten (z. B. Hardware, Betriebssystem, Software) kontaktiert werden müssen.

Im Folgenden werden einige Vor- und Nachteile von Appliances gegenübergestellt:

| **Vorteile** | **Nachteile** |
|---|---|
| - Einfache Installation, geringer Zeitaufwand nötig bis zur Inbetriebnahme<br>- Niedriger Aufwand zur Konfiguration, geringe Komplexität<br>- Wenig Aufbau von spezifischen Wissen zum Betrieb notwendig<br>- Vereinfachte Konfiguration, da Appliances oft Administrationsoberflächen anbieten<br>- Appliances unterstützen oft automatische Updates der bereitgestellten Funktionen<br>- Im Vergleich zu Lösungen auf Basis für den Einsatzzweck zusammengestellten IT-Komponenten geringere Ausfallwahrscheinlichkeit, da Appliances oft weniger "bewegliche Teile" enthalten (z. B. Festplatte oder Lüfter) als normale Rechner | - Geringe Erweiterungsmöglichkeiten der proprietären Hard- und Software<br>- bei Defekten muss unter Umständen das komplette System ausgetauscht werden<br>- Lange Ausfallzeiten, falls das Gerät im Fehlerfalle zum Hersteller gesandt werden muss. Gegebenenfalls muss deshalb ein Ersatzgerät beschafft werden, das als "Cold Standby" vorgehalten wird<br>- Wie gut die Sicherheitsmechanismen in den Geräten implementiert sind, ist schwer überprüfbar<br>- Wenig Informationen zur sicheren Konfiguration und zum sicheren Betrieb zu speziellen Produkten erhältlich (über die Informationen des Herstellers hinaus). Dies ist besonders dann problematisch, wenn der Hersteller den Support einstellt<br>- Einige Appliances besitzen nur eine geringe Verbreitung. In diesem Fall existieren evtl. wenig Berater |

| Vorteile | Nachteile |
|---|---|
| | bzw. Dienstleister zur Administration |

Die Gründe für die Entscheidung, Appliances einzusetzen, sowie für die Auswahl bestimmter Geräte sollten dokumentiert werden.

**Installation, Konfiguration und Datensicherung**

Appliances werden oft mit vorinstalliertem Betriebssystem, der sogenannten Firmware, ausgeliefert. Diese befindet sich in der Regel auf einem fest verbauten Flashspeicher, bei einigen Appliances auch auf Festplatten oder austauschbaren Speicherkarten. Da die vorinstallierte Firmware schon bei der Herstellung der Appliances auf das Gerät kopiert wurde und da zwischen Herstellung und Inbetriebnahme oft sehr viel Zeit vergehen kann, ist die vorinstallierte Firmware bei der Inbetriebnahme in der Regel veraltet und neue Firmware-Versionen sind verfügbar. Daher sollte anhand der Hersteller-Anleitung vor der Inbetriebnahme der Appliance ein Firmware-Update durchgeführt werden. Die zu installierende Firmware-Version muss hierbei aus einer vertrauenswürdigen Quelle stammen, siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*.

In der Regel werden Appliances über Webschnittstellen, per Telnet/SSH, SNMP oder proprietäre Protokolle konfiguriert. Je nach Produkt und Hersteller werden Konfigurationswerkzeuge angeboten, die auf einem anderen IT-System installiert werden können, um darüber eine oder mehrere Appliances zu konfigurieren. Bei jeder dieser Konfigurationsmöglichkeiten sollte darauf geachtet werden, dass bei einer Konfiguration über das Netz die Kommunikation nicht durch Dritte mitgelesen oder verändert werden kann. Daher sollte die Konfiguration ausschließlich über abgesicherte Verbindungen erfolgen, also beispielweise verschlüsselt oder über ein separates Konfigurationsnetz.

Appliances werden in der Regel mit voreingestellten Passwörtern ausgeliefert. Diese sollten sofort geändert (M 4.7 *Änderung voreingestellter Passwörter*) und geeignet hinterlegt (M 2.22 *Hinterlegen des Passwortes*) werden.

Nachdem die Konfiguration abgeschlossen wurde, sollten die Konfigurationseinstellungen gesichert werden, damit bei einem Ausfall zeitnah ein baugleiches Gerät in Betrieb genommen werden kann. Wird die Konfiguration der Appliances im laufenden Betrieb geändert, sollten die Konfigurationseinstellungen ebenfalls gesichert und die Änderungen dokumentiert werden.

**Protokollierung**

Auf Appliances treten oft Ereignisse auf, die protokolliert werden müssen. Oft verfügen Appliances nicht über genügend Speicherplatz, um Protokolldateien abzuspeichern, oder die Speicherart ist nicht für permanente Schreibvorgänge geeignet. Daher wird empfohlen, die Ereignisse auf einem dedizierten IT-System, in der Regel einem separaten Protokollierungsserver, abzulegen. Weitere Informationen sind in B 5.22 *Protokollierung* zu finden.

**Sichere Außerbetriebnahme**

Sollen Appliances außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden. Je nach Einsatzzweck können dies beispielsweise

- Konfigurationsdateien, aus denen Informationen über die Netzstruktur der Institution entnommen werden können,
- Passwortdateien,
- Protokolldateien, die sicherheitsrelevante Informationen oder personenbezogene Daten enthalten,
- Zertifikate und kryptographische Schlüssel (etwa für den Zugang auf andere IT-Systeme)

sein. Das Löschen solcher Informationen kann sich bei Appliances schwieriger gestalten als bei normalen IT-Systemen. Bei Appliances hängt die Vorgehensweise davon ab, wo und wie die Daten gespeichert werden, also beispielsweise auf einer eingebauten Festplatte oder in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Sind auf dem Gerät besonders sicherheitskritische Informationen gespeichert und kann nicht mit hinreichender Sicherheit gewährleistet werden, dass die Daten wirklich gelöscht sind, so kann es erforderlich sein, die Speicherbausteine oder Festplatten physisch zu zerstören bzw. unbrauchbar zu machen.

Oft sind Appliances von außen mit IP-Adressen, Hostnamen oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Prüffragen:

- Sind die Gründe für die Auswahl einer Appliance dokumentiert?
- Werden alle Appliances vor Inbetriebnahme aktualisiert und die voreingestellten Passwörter geändert?
- Werden die Appliances ausschließlich über geschützte Verbindungen (oder direkt am Gerät) konfiguriert?
- Werden die Konfigurationseinstellungen der Appliances regelmäßig gesichert?
- Werden Appliances sicher außer Betrieb genommen und alle vertraulichen Informationen gelöscht?

# M 4.435 Selbstverschlüsselnde Festplatten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Um zu verhindern, dass Unbefugte an vertrauliche Daten auf Festplatten gelangen können, sollten diese nach Möglichkeit komplett verschlüsselt werden (siehe auch M 4.433 *Einsatz von Datenträgerverschlüsselung*). Es gibt Hard- und Software-basierte Verfahren zur Verschlüsselung. In dieser Maßnahme wird die hardware-basierte Verschlüsselung in Form von selbstverschlüsselnden Festplatten (englisch: "Self-Encrypting Device", SED) behandelt. SEDs greifen für die Verschlüsselung auf einen speziellen Hardware-Kryptocontroller zu und sind dadurch sehr performant. Die eingesetzten Verschlüsselungslösungen sehen nur die Nutzung durch einen Benutzer vor, Mehr-Benutzer-Lösungen sind im Allgemeinen nicht vorgesehen.

Bei Nutzung einer selbstverschlüsselnden Festplatte kann das IT-System unter Umständen nicht mehr in den Arbeitsspeicher suspendiert werden, da beim Abschalten der Festplatte alle Daten verschlüsselt werden und ein im RAM gespeicherter Schlüssel ein Sicherheitsrisiko wäre. Dies ist vor dem Einsatz zu bedenken.

Selbstverschlüsselnde Festplatten sollten nicht mit einem TPM-Modul kombiniert werden, da es bei einer solchen Kombination in der Regel keine Möglichkeit gibt, die Festplatte in einem anderen IT-System mit einem Master-Key zu entschlüsseln. Wird in so einem Fall das IT-System beschädigt, lassen sich die Daten auf der Festplatte nicht mehr entschlüsseln, da die Festplatte durch das TPM-Modul fest mit dem IT-System verwoben ist.

Bei selbstverschlüsselnden Festplatten wird in der Regel AES mit Schlüssellängen von 128 bis 256 Bit eingesetzt. Der Schlüssel, mit dem die Informationen verschlüsselt werden, ist der sogenannte "Data Encryption Key" (DEK). Der DEK befindet sich im Kryptocontroller, der vor Manipulationen besonders geschützt ist. Er wird auf Basis zufälliger Hardware-Ereignisse generiert. Dieser DEK wird mit einem "Authentication Key" (AK) verschlüsselt. Der AK wird typischerweise vom Benutzer durch die Wahl eines Passwortes erzeugt. Bei einigen selbstverschlüsselnden Festplatten kann auch der AK auf einem Token, beispielsweise einer Chipkarte oder einem USB-Stick, gespeichert und zusätzlich mit einem Passwort verschlüsselt werden. Dies ermöglicht die Umsetzung einer Zwei-Faktor-Authentisierung.

Zusätzlich zum DEK und AK gibt es in der Regel auch noch einen Master-Key, der es erlaubt, die Daten zu entschlüsseln, auch wenn das Passwort oder der Token verloren wurde. Ein solcher Schlüssel muss bei der Installation erzeugt und für den Fall, dass das Passwort bzw. der Token verloren geht, sicher aufbewahrt werden. Es muss geregelt werden, wie organisatorisch vorgegangen wird, wenn ein Benutzer das Passwort zu einer verschlüsselten Festplatte vergisst. In diesem Fall muss mit dem Master-Key das Passwort zurückgesetzt werden und der Benutzer ein neues Passwort setzen.

Wenn sich der Benutzer erfolgreich authentisiert hat, wird der DEK entschlüsselt. Mit dem DEK werden alle auf der Festplatte befindlichen Daten ent- und verschlüsselt, ohne dass der Benutzer im Betrieb etwas davon bemerkt. Fährt der Rechner herunter oder wird die Laufwerkseinbindung des SEDs gelöst, werden alle Daten mit dem DEK und der DEK mit dem AK verschlüsselt.

Generell sollte die verwendete Schlüssellänge des von der Festplatte verwendeten Verschlüsselungsverfahrens hinreichend lang sein. Nähere Details zu angemessenen Schlüssellängen kryptographischer Verfahren sind in M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* zu finden.

Bevor selbstverschlüsselnde Festplatten beschafft werden, sollte geprüft werden, ob die Festplatten mit der übrigen Hardware des IT-Systems kompatibel sind. Ferner sollte geprüft werden, ob die Schreib- und Leserate der ausgesuchten Festplatte angemessen ist. Überdies sollte geprüft werden, ob weitere Randbedingungen für den Einsatz beim IT-System erfüllt werden müssen. Zum Beispiel lassen sich nur sehr wenige Modelle von selbstverschlüsselnden Festplatten in einer bestehenden "Single-Sign-On"-Architektur integrieren. Auch sollte überprüft werden, ob und wie IT-Systeme mit normalen Festplatten zu selbstverschlüsselnden Festplatten migriert werden können (z. B. mit einem mitgelieferten Programm oder über eine Neuinstallation).

Die Installation einer selbstverschlüsselnden Festplatte sollte in Institutionen durch geschulte Administratoren durchgeführt werden. Dafür müssen diese zunächst einen neuen DEK erzeugen und ein Passwort vergeben sowie einen Master-Key erstellen, der sicher aufbewahrt werden muss (siehe M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren* und M 2.22 *Hinterlegen des Passwortes*). Das DEK-Startpasswort muss der Benutzer des Clients als Erstes in ein sicheres Passwort ändern (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Wird eine selbstverschlüsselnde Festplatte repariert oder soll sie verkauft bzw. entsorgt werden, so muss sichergestellt sein, dass sich von ihr keine schützenswerten Informationen entnehmen lassen. Dazu sollte vor Reparatur, Verkauf oder Entsorgung der DEK neu generiert oder ein Löschbefehl "ATA Secure Erase" ausgeführt werden.

Prüffragen:

- Wurde bei der Installation von selbstverschlüsselnden Festplatten der DEK neu generiert und ein Master-Key erstellt sowie sicher hinterlegt?
- Wird vor Reparatur, Verkauf oder Entsorgung einer selbstverschlüsselnden Festplatten der DEK gelöscht bzw. ein ATA Secure Erase ausgeführt?

# M 4.436 Planung der Ressourcen für Cloud-Dienste

**Verantwortlich für Initiierung:** Fachabteilung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche

Bei der Planung einer Cloud-Infrastruktur müssen eine Reihe von Rahmenbedingungen berücksichtigt werden.

Neben den Fragen nach der zu verwendenden Virtualisierungstechnik und den hierzu einzusetzenden Produkten ist die Eignung der Cloud-Elemente (Hardware, Software und Netzanbindung) und die damit zu realisierende Netzstruktur und Speicheranbindung zu planen. Bei der Planung der Cloud-Infrastruktur muss darüber hinaus die Kompatibilität von IT-Systemen und (Verwaltungs-) Softwarelösungen von verschiedenen Anbietern geprüft werden.

Ergebnisse der Planung müssen somit Auswahlentscheidungen für Hardware und Software sowie für Netzstruktur und Speicheranbindung sein. Die Planung sollte die Eigenschaften (Dimensionierung, Durchsatz usw.) der Hardware, Software und Anbindungen dokumentieren, anhand oder aufgrund derer die Auswahl getroffen wurde. Dies sollte insbesondere Betrachtungen zur Kompatibilität der Bestandteile untereinander einschließen.

### Auswahl der Hardware

Bei der Auswahl der Hardware für eine Cloud-Infrastruktur ist darauf zu achten, dass sie für die geplante virtuelle Ressourcenschicht über eine geeignete Leistungsfähigkeit verfügt. Um der Skalierbarkeit und der Elastizität der Cloud-Infrastruktur Rechnung zu tragen, müssen die eingesetzten IT-Systeme und Netzkomponenten geeignet und ausreichend dimensioniert und gegebenenfalls einfach erweiterbar sein, um für alle virtualisierten Cloud-Infrastrukturen, Plattformen und Anwendungen genügend Kapazitäten bereitzustellen.

### Planung der Netzanbindung

Es muss geplant werden, mit welcher Technik virtuelle IT-Systeme mit dem Netz des Rechenzentrums verbunden werden sollen. Diese Anbindung kann zum Beispiel über virtuelle Switches erfolgen. Zusätzlich müssen Speichernetze und deren Anbindung (z. B. SAN-Anbindung über Lichtwellenleiter) geplant werden. Hierbei ist insbesondere die Maßnahme M 2.351 *Planung von Speicherlösungen* zu berücksichtigen. In diesem Zuge muss die Netzplanung für die Cloud-Infrastruktur auch die vorhandene Segmentierung des Netzes berücksichtigen, wobei die Maßnahmen M 2.141 *Entwicklung eines Netzkonzeptes*, M 5.61 *Geeignete physische Segmentierung* sowie M 5.62 *Geeignete logische Segmentierung* umzusetzen sind.

### Planung von Infrastrukturdiensten

Es müssen mandantenübergreifende Cloud-Infrastrukturdienste geplant und konzipiert werden. Cloud-Dienste benötigen in ihrer technischen Einsatzumgebung:

- schnelle und erweiterbare Anbindungen an CPU-, Arbeitsspeicher- und Speicherressourcen.
- Verbindungen in Speichernetze für den Zugriff auf Massenspeicherkomponenten.
- Anbindungen an Infrastruktursysteme wie DNS-, DHCP- und Verzeichnisdienst-Server.

- Anbindungen an Infrastrukturdienste wie Update-Server für Schadprogramm-Signaturen.

**Einsatzplanung für einen Cloud-Verwaltungsserver**

Bei der Einsatzplanung für einen Cloud-Verwaltungsserver ist auf Besonderheiten zu achten, die insbesondere dadurch entstehen, dass auf dem Verwaltungsserver in der Regel mehrere virtuelle IT-Systeme betrieben werden sollen. Es muss daher ermittelt werden, wie viel Prozessorleistung, Hauptspeicher und Festplattenplatz für den Betrieb der virtuellen IT-Systeme benötigt wird. Weiterhin muss festgelegt werden, welche Netzverbindungen für die Virtualisierungsserver und die virtuellen IT-Systeme benötigt werden. Es ist eine detaillierte Analyse im Rahmen des Anforderungsmanagements zu erstellen. Insbesondere ist die Ausfallsicherheit des Verwaltungsservers hinreichend zu konzipieren, da die verschiedenen virtuellen Maschinen auf dem Cloud-Verwaltungsserver die Element Manager und die Cloud-Verwaltungssoftware beinhalten.

Zudem ist im Rahmen der Planung der Cloud-Infrastruktur die Protokollierung und Analyse der Protokolldateien zu berücksichtigen (Maßnahmen M 4.443 *Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur* und M 4.430 *Analyse von Protokolldaten*). Im Rahmen eines Kapazitätsmanagements muss die erforderliche Verfügbarkeit aufrechterhalten werden. Dazu muss es möglich sein, die Auslastung der Ressourcen zu überwachen und je nach Anforderung entsprechende Kapazitäten für Speicher, CPU und weitere virtuelle Ressourcen bereitzustellen.

Bei der Auswahl einer Verwaltungslösung für das Cloud Management muss bei Einzellösungen wie auch für Komplett-Pakete von Herstellern, welche zugleich Element Manager und Virtualisierungslösungen anbieten, analysiert werden, ob die Anforderungen des Cloud-Diensteanbieters und dessen Cloud-Anwendern hinreichend durch die Komplettlösung abgedeckt sind. Insbesondere muss hier beachtet werden, dass bereits vorhandene Produkte und IT-Komponenten des Cloud-Diensteanbieters mit den Bestandteilen der ausgewählten Komplettlösung für die Cloud-Infrastruktur kompatibel sind.

Prüffragen:

- Wurde bei der Auswahl der Hardware für eine Cloud-Infrastruktur darauf geachtet, dass sie über eine geeignete Leistungsfähigkeit verfügt?
- Wurde bei der Planung der Anbindung an das Netz des Rechenzentrums die vorhandene Segmentierung des Netzes berücksichtigt?
- Wurden bei der Planung von Infrastrukturdiensten alle Anforderungen an die Anbindung erforderlicher Ressourcen berücksichtigt?
- Wurde ermittelt, wie viel Prozessorleistung, Hauptspeicher und Festplattenplatz für den Betrieb der virtuellen IT-Systeme auf dem Verwaltungsserver benötigt wird?
- Wurde festgelegt, welche Netzverbindungen für die Virtualisierungsserver und die virtuellen IT-Systeme benötigt werden?
- Wurde festgelegt, wie die Auslastung der Ressourcen überwacht wird, um anforderungs- und bedarfsgerecht Kapazitäten für Speicher, CPU und weitere virtuelle Ressourcen bereitzustellen?
- Wurde analysiert, ob die Anforderungen des Cloud-Diensteanbieters und der Cloud-Anwender hinreichend durch die Verwaltungslösung für das Cloud Management abgedeckt sind?

# M 4.437 Planung von Cloud-Diensteprofilen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Aufgrund der hohen Komplexität ist eine detaillierte Planung für die Bereitstellung von Cloud-Diensten unerlässlich. Bereits in einer konzeptionellen Betrachtung und im Vorfeld einer Projektierung ist deshalb eine Analyse der notwendigen Rahmenbedingungen durchzuführen.

Cloud-Diensteprofile werden durch einen Satz von Informationen definiert, der die Cloud-Ressourcen und deren Konfiguration beschreibt. Cloud-Ressourcen sind CPU, Arbeitsspeicher, Netze oder Speichersysteme/Speichernetze (Storage). Die Cloud-Diensteprofile müssen eine fehlerfreie automatische Reproduktion von Cloud-Diensten ermöglichen.

### Anforderungen aufnehmen

Zuerst müssen die Anforderungen an Cloud-Dienste aufgenommen werden. Für die Cloud-Diensteprofile sind, wie bei Anwendungen und IT-Systemen, die notwendigen Komponenten (Software, Datenbanken, Betriebssysteme, Netze, Infrastrukturdienste wie DNS) sowie deren Konfiguration zu planen. Zudem müssen messbare Qualitätsindikatoren für die Cloud-Dienste festgelegt werden.

### Automatisierung planen

Es muss geplant werden, wie die Bereitstellung des Cloud-Dienstes automatisiert werden kann. Hierbei sind auch Sicherheitsmaßnahmen zur Mandantentrennung zu berücksichtigen. Abhängig von den Sicherheitsanforderungen an die Mandantentrennung muss der Cloud-Diensteanbieter gegebenenfalls unterschiedliche Netze, Virtualisierungshosts oder Speichersysteme vorsehen und die damit verbundenen Konfigurationen vorbereiten.

### Bei Konfiguration durch Cloud-Anwender: Eingaben validieren

Cloud-Dienste können zum Teil auch direkt über Eingaben der Cloud-Anwender in ihrer Ausprägung definiert und anschließend (teil-)automatisiert bereitgestellt werden. Die Eingaben der Cloud-Anwender können über Administrationsschnittstellen oder Webportale (sogenannte Self-Service-Portale) erfolgen.

Wenn Cloud-Anwender in dieser Weise Cloud-Dienste konfigurieren können, muss der Cloud-Diensteanbieter Prozesse planen, um diese Eingaben zu überprüfen: In der Schnittstellenlogik oder in den Webportalen müssen Parameter vordefiniert und Wertegrenzen festgelegt werden, um die Eingaben der Cloud-Anwender zu validieren.

### Authentisierung und Verschlüsselung (Zugriffsweg) planen

Unabhängig von der Ausprägung des Cloud-Dienstes oder dem Bereitstellungsmodell muss der Cloud-Diensteanbieter die Authentisierung und den Zugriffsweg für die Cloud-Dienste planen. Hierzu gehört die Vorkonfiguration des Secure Sockets Layer (SSL/TLS) für die Verschlüsselung des Zugriffsweges.

**Verwaltung von Schlüsseln, Authentisierungsdaten, Rollen und Rechten planen**

Es muss die sichere Ablage von Schlüsselmaterial und Authentisierungsdaten für den kontrollierten Zugriff auf den Cloud-Dienst konzipiert werden. In diesem Rahmen ist die sichere Anbindung an ein zentrales Identitätenmanagementsystem, z. B. über Standards wie SAML (Security Assertion Markup Language), für die Cloud-Dienste vorzubereiten. Die Anlage vorbereiteter Rollen- und Rechteprofile ist ebenfalls im Rahmen der Cloud-Diensteprofile zu planen und für die Vervielfältigung des Cloud-Dienstes für verschiedene Mandanten vorzubereiten.

**Zentrale Überwachung (Monitoring) vorbereiten**

Für eine zukünftige Überwachung und Abrechnung von Cloud-Diensten muss in den Cloud-Diensteprofilen hinterlegt werden, wie eine zentrale Überwachung angebunden wird.

**Mehrschichtige Sicherheitsarchitektur planen**

Es müssen Einstellungen für eine mehrschichtige Sicherheitsarchitektur (engl.: *layered security*) geplant werden. Dementsprechend sind Einstellungen für virtuelle Netze, für virtuelle Firewalls, VLANs und sichere Transportkanäle vorzubereiten.

**Ergänzend: Sichere Software-Entwicklung und sichere Betriebsumgebung berücksichtigen**

Es sind je nach Konfiguration des Cloud-Diensteprofils Sicherheitsaspekte aus der sicheren Software Entwicklung zu berücksichtigen. Insbesondere ist bei der Entwicklung von Cloud-Angeboten für SaaS der Baustein B 5.21 *Webanwendungen* heranzuziehen. Je nach Ausprägung der Cloud-Dienste kann es notwendig sein, die Vorbereitung von gekapselten Laufzeitumgebungen (engl.: *Sandboxing*) zu planen.

Prüffragen:

- Sind die Sicherheitsanforderungen an die Cloud-Dienste aufgenommen und in die Planung der Cloud-Dienste einbezogen?
- Sind Rollen und Berechtigungen für die Cloud-Diensteprofile klar vordefiniert?
- Sind Eingabevalidierungen und Grenzwerte für die Bereitstellung von Cloud-Diensten definiert?
- Sind eine Authentisierung und eine Verschlüsselung des Zugriffswegs für die Cloud-Dienste geplant und genügen sie den anerkannten Regeln der Technik?
- Ist eine Überwachung der Cloud-Dienste in der Planung berücksichtigt worden?
- Sind Einstellungen zur netzbasierten Mandantentrennung über virtuelle Netze, virtuelle Firewalls, VLANs bei der Planung der Cloud-Diensteprofile berücksichtigt worden?

# M 4.438 Auswahl von Cloud-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In Abhängigkeit vom gewählten Bereitstellungsmodell (IaaS, PaaS, SaaS) ergeben sich Anforderungen an die Hardware- und Virtualisierungslösungen (siehe M 4.436 *Planung der Ressourcen für Cloud-Dienste*). Hieraus entstehen individuelle Anforderungen an die zugrunde liegende Hardware-Architektur bzw. die Ausstattung des Verwaltungsservers für die Cloud-Infrastruktur mit Hardwarekomponenten und dessen Anbindungen an die Speichernetze oder Massenspeicher.

Diese Anforderungen müssen bei der Beschaffung von Serversystemen berücksichtigt werden, wenn diese als Cloud-Verwaltungsserver eingesetzt werden sollen.

Anforderungen an Virtualisierungsserver, die zumeist wesentlicher Bestandteil einer Cloud Lösung sind, sind in der Maßnahme M 2.445 *Auswahl geeigneter Hardware für Virtualisierungsumgebungen* definiert.

Folgende Aspekte sollten bei der Auswahl von Cloud-Komponenten beachtet werden:

- Bei der Auswahl der **Hardware** für die Cloud-Infrastruktur muss beachtet werden, dass Cloud-Dienste stark skalieren können, daher müssen modular erweiterbare Hardwarelösungen ausgewählt werden. Auch die Vernetzung der Hardware mit neuen und erweiterten Hardwareblöcken muss hierbei berücksichtigt werden.
- **Hard- und Software** für die Cloud-Dienste müssen so ausgelegt sein, dass die Anforderungen an die *Verfügbarkeit* des Servers und die *Integrität* der Cloud-Anwenderdaten erfüllt werden können. Hierbei müssen realistische Annahmen für die Datenmengen getroffen werden.
- Die **Anbindung** an vorhandene oder zu beschaffende Speichernetze und die Schnittstelle zur Verwaltung der Speichernetze oder Massenspeicher muss konzipiert und die erforderlichen Komponenten beschafft werden. Oft ist eine untereinander kompatible Auswahl von Produkten und Lösungen *eines* Herstellers die geeignetste Lösung. Für die Anbindung und die Auswahl von Speichersystemen und Speichernetzen ist die Maßnahme M 2.362 *Auswahl einer geeigneten Speicherlösung* umzusetzen.
- Für die **Administration** und **Verwaltung** der Cloud-Infrastruktur bestehen Anforderungen an sichere Zugriffe (vgl. Maßnahme M 5.174 *Absicherung der Kommunikation zum Cloud-Zugriff*). Die ausgewählten Softwareprodukte für die Cloud-Verwaltung müssen daher Protokolle mit für die Anforderungen der Cloud-Anwender hinreichend sicherer Verschlüsselung (siehe Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*) und starker Authentisierung berücksichtigen.
- Es muss eine **Verwaltungslösung** für die Cloud-Komponenten entwickelt werden, die eine notwendige zeitnahe Verteilung von Ressourcen ermöglicht, daher sollten Virtualisierungswerkzeuge eingesetzt werden. Zudem muss der Verwaltungsserver physische Verbindungen in alle Netze für die Cloud-Infrastruktur haben.
- Die zu wählende Lösung zur Verwaltung der Cloud muss vorsehen, dass eine Mandantenfähigkeit sowohl in der Administration als auch bei der Provisionierung und De-Provisionierung hierüber umgesetzt werden kann.

- Die **Software und Virtualisierungslösungen** müssen die Umsetzung eines Rollen- und Rechtekonzeptes ermöglichen (Anforderung der Mandantenfähigkeit). Es muss möglich sein, die Befugnisse der Cloud Administratoren zu beschränken und gegebenenfalls auch auf der Administrationsoberfläche eine mandantenbezogene Rollentrennung zwischen Administratoren zu ermöglichen.
- Für SaaS: Viele Cloud-Anwender erwarten Interoperabilität und Portabilität der Cloud-Daten. Dieses kann durch standardisierte und offengelegte Schnittstellen und Formate erreicht werden. Dementsprechend sollten die **Cloud-Anwendungen**, welche entwickelt oder ausgewählt werden, standardisierte Schnittstellen bereitstellen und Exporte in verbreiteten Datenformaten (API, Protokolle) ermöglichen. Dadurch wird für den Cloud-Anwender eine Plattformunabhängigkeit ermöglicht.
- Es gibt Kompatibilitätsanforderungen an die **Kommunikation** zwischen Verwaltungsserver und virtuellen und physischen Ressourcenkontrollschichten. Daher muss bereits bei der Auswahl der Hard- und der Softwarekomponenten (insbesondere Netzmanagement, Virtualisierungsserver, Steuerung der Speichersysteme) darauf geachtet werden, dass Cloud Element Manager und Orchestrierungsserver korrekt miteinander kommunizieren können, sodass die geforderte Verfügbarkeit der Cloud-Dienste sichergestellt werden kann.

Prüffragen:

- Wird bei der Auswahl der Hardware für die Cloud-Infrastruktur eine modular erweiterbare Hardware-Lösung ausgewählt, um Cloud-Dienste in erforderlichem Umfang skalieren zu können?
- Sind Speichernetze und die Schnittstelle zur Verwaltung der Speichernetze so konzipiert, dass sie an vorhandene oder zu beschaffende Komponenten angebunden werden können?
- Bieten die Protokolle der ausgewählten Softwareprodukte für die Cloud-Verwaltung eine hinreichend sichere Verschlüsselung und starke Authentisierung für den administrativen Zugriff?
- Ermöglicht die eingesetzte Verwaltungslösung für die Cloud-Komponenten eine zeitnahe Verteilung von Ressourcen?
- Kann mit der eingesetzten Verwaltungslösung für die Cloud-Komponenten eine Mandantenfähigkeit sowohl in der Administration als auch bei der Provisionierung und De-Provisionierung umgesetzt werden?
- Ermöglicht die eingesetzte Software und Virtualisierungslösung die Umsetzung eines Rollen- und Rechtekonzeptes?
- Für SaaS: Werden standardisierte und offengelegte Schnittstellen und Formate so eingesetzt, dass die Erwartungen von Cloud-Anwendern an Interoperabilität und Portabilität der Cloud-Daten erfüllt werden können?

# M 4.439 Virtuelle Sicherheitsgateways (Firewalls) in Clouds

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

In einer Cloud-Infrastruktur werden Cloud-Dienste betrieben, auf die Cloud-Benutzer zugreifen. Für jeden Cloud-Anwender entsteht dabei ein System aus den verschiedenen Cloud-Diensten, die er nutzt. Dieses System läuft auf einer oder mehreren virtuellen Maschinen. Es wird nachstehend als Anwendersystem bezeichnet.

Zum Schutz der Cloud-Lösungen sollten auf den virtuellen Maschinen Sicherheitsgateways (Firewalls) eingesetzt werden, um die Kommunikation zwischen Anwendersystemen und den Verwaltungsservern abzusichern. Zudem sollten, soweit technisch möglich, auch die einzelnen Mandanten voneinander getrennt und gegeneinander abgeschottet werden.

Es gibt unterschiedliche Umsetzungsmöglichkeiten, z. B. als Installation einer virtuellen Anwendung auf dem Host oder als Kernel-Modul der zentralen Komponente des Virtualisierungsservers (Hypervisor) für die virtuellen IT-Systeme. Die Sicherheitsgateways (Firewalls) steuern die IP-Dienste, die zwischen Anwender-, Verwaltungs- und externen Systemen genutzt werden können. Die Firewalls müssen dabei eine Segmentierung von Diensten durch die Einrichtung von Vertrauenszonen sicherstellen und hierbei so restriktiv wie möglich eingestellt werden. Den Anwendersystemen sollte kein Zugriff auf die Verwaltungsserver erlaubt werden. Dabei gilt der Grundsatz: *Alles, was nicht ausdrücklich erlaubt ist, ist verboten.*

Die eingesetzte Firewall-Lösung muss über Firewall-Richtlinien gewährleisten, dass der Netzverkehr zwischen den virtuellen Maschinen überwacht und gesteuert wird, insbesondere wenn diese auf einen anderen virtuellen Host umziehen oder wenn virtuelle Profile für neue Cloud-Mandanten vervielfacht werden. Die Filterregeln der Firewalls sollten nach der erstmaligen Konfiguration daraufhin getestet werden, ob die erlaubten Ereignisse zugelassen und unerlaubte Ereignisse unterbunden werden.

Die Kommunikation der virtuellen IT-Systeme mit anderen virtuellen oder physischen IT-Systemen sollte detailliert geplant werden. Hierbei müssen bestehende Sicherheitsrichtlinien beachtet werden. Im Netz existierende Sicherheitsgateways oder Monitoring-Systeme dürfen nicht mit den Mitteln der Virtualisierung umgangen werden können. Dies betrifft insbesondere Virtualisierungsprodukte, bei denen der Netzverkehr zwischen virtualisierten IT-Systemen nicht zwingend über physische Netze geführt wird.

Müssen virtuelle IT-Systeme mit mehreren Netzen verbunden werden, muss geeignet sichergestellt werden, dass über diese keine unerwünschten Netzverbindungen aufgebaut werden können. Es dürfen insbesondere keine Verbindungen zwischen Verwaltungsnetzen der Virtualisierungsserver und den Netzen der produktiven virtuellen IT-Systeme ermöglicht werden, um einer Kompromittierung der Virtualisierungsserver vorzubeugen. Dieses muss entweder durch eine physische oder durch eine logische Trennung (z. B. über VLANs) sichergestellt werden.

Prüffragen:

- Sind die Verwaltungsnetze der Virtualisierungsserver durch Firewall-Richtlinien von den Produktivnetzen mit den Anwendersystemen getrennt?
- Sind die Systeme der verschiedenen Cloud-Mandanten durch Firewall-Richtlinien voneinander getrennt?

# M 4.440 Verschlüsselte Speicherung von Cloud-Anwenderdaten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Neben der verschlüsselten Übertragung über öffentliche Netze kann auch die verschlüsselte Speicherung von Cloud-Anwenderdaten notwendig sein, um zu verhindern, dass Administratoren oder andere Mitarbeiter des Cloud-Diensteanbieters auf gespeicherte Informationen zugreifen können.

Die Verschlüsselung von Cloud-Datenbeständen kann so ausgestaltet sein, dass der Cloud-Diensteanbieter die Verschlüsselungsmittel bereitstellt und einsetzt, also Verfahren und Schlüssel bei ihm liegen. Alternativ kann der Cloud-Anwender über den Schlüssel verfügen, während der Cloud-Diensteanbieter lediglich die Verschlüsselung bereitstellt. Letzteres ist zu bevorzugen, falls dies die technischen Möglichkeiten des genutzten Cloud-Service-Modells zulassen.

Eine Verschlüsselung von Cloud-Datenbeständen muss mit einem geeigneten Verschlüsselungsalgorithmus und in einer Weise erfolgen, dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch des Vorgangs) systemseitig abgefangen wird.

Die Auswahl eines geeigneten Verschlüsselungsalgorithmus sollte gemäß Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* erfolgen.

Die Umsetzung einer verschlüsselten Speicherung hängt stark von dem Servicemodell (PaaS, IaaS, SaaS) und von der bereitgestellten Architektur ab:

**Beispiel: PaaS / Datenbank**

Eine Verschlüsselung kann auf Datenbank-Ebene erfolgen, z. B. über feldbasierte Ver- und Entschlüsselung (vgl. M 4.72 *Datenbank-Verschlüsselung*). Bei der Datenbankverschlüsselung sind besonders die Export- und Import-Funktionen zu berücksichtigen, die unter Umständen Daten unverschlüsselt übertragen. Einige Datenbankmanagementsysteme bieten eine zusätzliche Berechtigungsumgebung an, mit deren Hilfe den Datenbankadministratoren der lesende Zugriff auf Feldebene der Datenbank entzogen werden kann, indem z. B. der *Select*-Befehl für den Datenbankadministrator gesperrt wird. In diesem Fall können die Datenbankadministratoren zwar Tabellen einfügen oder löschen und Backup-Operationen durchführen, den Inhalt der Tabellen aber nicht einsehen.

Diese Art der "Datenunterdrückung" erfordert ein zusätzliches Berechtigungskonzept und ein Vier-Augen-Prinzip für diejenigen, die die Berechtigungen für die Datenbankadministratoren vergeben. Die Informationen des Cloud-Anwenders in den Datenbanken können aber auf diese Weise effizient vor unberechtigter Einsichtnahme durch die Administratoren geschützt werden.

**Beispiel: IaaS / Festplattenverschlüsselung**

Es kann bei IaaS der Fall sein, dass die virtuelle Festplatte verschlüsselt wird. Je nach eingesetzter Lösung der Festplattenverschlüsselung kann die Systemintegrität während des Bootprozesses geprüft werden.

Eine Entschlüsselung kann dann nur durch den Cloud-Anwender erfolgen. Im Allgemeinen erfolgt dies nach anfänglicher Eingabe eines Passworts oder einer PIN automatisch, wenn Cloud-Benutzer auf Daten des verschlüsselten Bestandes zugreifen wollen.

Die Anwenderdaten sind in diesem Fall durch den Administrator des Cloud-Diensteanbieters nicht einsehbar.

Bei Festplattenverschlüsselung muss zusätzlich darauf geachtet werden, dass die Backup-Methode ebenfalls Verschlüsselung unterstützt. Wenn die Datensicherung unverschlüsselt erfolgt, könnten unter Umständen über diesen Weg Informationen ausgespäht werden.

**Beispiel: IaaS oder PaaS / Bereitstellung von Hilfsmitteln zur Verschlüsselung**

Bei diesem Szenario stellt der Cloud-Diensteanbieter dem Cloud-Anwender Software zur eigenständigen Verschlüsselung bereit, z. B. Container-Lösungen, welche der Cloud-Anwender mit einem Passwort zur Verschlüsselung der darin abgelegten Daten verwenden kann. Verantwortung für Schlüsselmanagement und verschlüsselte Ablage liegen hier beim Cloud-Anwender.

**Beispiel: SaaS / Verschlüsselung über die Anwendungslogik**

Der Cloud-Diensteanbieter, hier als Software-Anbieter, bindet in die Cloud-Anwendung (SaaS) eine proprietäre Verschlüsselung ein, welche die Daten anwendungsseitig verschlüsselt ablegt. Die Verantwortung für Einsatz und Verwaltung der Verschlüsselung liegt hier beim Cloud-Diensteanbieter / Software-Anbieter.

Prüffragen:

- Werden vertrauliche Cloud-Anwenderdaten derart verschlüsselt, dass der Cloud-Administrator keinen Zugriff auf die Informationen hat?

# M 4.441 Multifaktor-Authentisierung für den Cloud-Benutzerzugriff

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein kontrollierter Zugriff auf die Ressourcen und Daten unterschiedlicher Cloud-Anwender stellt einen wesentlichen Aspekt bei der Realisierung einer mandantenfähigen Cloud-Lösung mit einer heterogenen Anwenderstruktur dar. Hierzu können unterschiedliche Authentisierungsverfahren eingesetzt werden.

Eine sichere Lösung stellt hierbei eine Multifaktor-Authentisierung dar. Dabei sind mindestens zwei Faktoren für eine erfolgreiche Authentisierung erforderlich. Häufig werden dabei *Wissen* (ein Passwort, eine PIN oder Ähnliches) und *Besitz* (eine Chipkarte, ein USB-Stick oder Ähnliches) kombiniert. Eine Zwei-Faktor-Authentisierung kann z. B. über eine hardwarebasierte Authentisierung mit Chipkarten oder USB-Sticks oder über Einmal-Passwörter, die von Hardwarekomponenten generiert werden, realisiert werden.

Bei der Umsetzung einer Cloud-Lösung sind im Bezug auf die Authentisierung folgende Punkte zu beachten:

- Der Zugriff auf alle IT-Systeme oder Cloud-Dienste muss in jedem Fall durch eine Authentisierung der zugreifenden Benutzer oder IT-Systeme abgesichert werden, auch wenn dies nur durch ein Passwort erfolgt.
- Für sicherheitskritische Anwendungsbereiche sollte eine starke Authentisierung, also mindestens eine Zwei-Faktor-Authentisierung, verwendet werden, wenn der Zugang zum genutzten Cloud-Dienst direkt über das Internet erfolgt.
- Eine Multifaktor-Authentisierung ist insbesondere für die Anmeldung von privilegierten Cloud-Benutzern zur Verwaltung von Cloud-Diensten zu empfehlen. Darüber hinaus muss der Cloud-Anwender risikobasiert entscheiden, ob dieses sichere Authentisierungsverfahren auf weitere Benutzer seiner Cloud-Dienste auszuweiten ist.
- Es wird empfohlen, eine Multifaktor-Authentisierung für Self-Service-Portale einzurichten. Dort können die Cloud-Benutzer ihre Cloud-Dienste verwalten und über eine Anwendung direkt die geänderten Cloud-Anforderungen und damit verbundenen Cloud-Ressourcen an die automatisierte Orchestrierung des Cloud-Diensteanbieters übergeben, die dieser entsprechend in Rechnung stellen kann. Für Sicherheitsempfehlungen bzgl. der weiterführenden Absicherung für ein Self-Service-Portal wird auf den Baustein B 5.21 *Webanwendungen* verwiesen, da die Portale zumeist als Webanwendung bereitgestellt werden.
- Es gibt auch Szenarien, in denen ein Benutzer schon vor Anmeldung an Cloud-Dienste eine Multifaktor-Authentisierung durchläuft. Dies kann z. B. bei der Benutzeranmeldung an das Kundennetz des Cloud-Anwenders oder beim Aufbau einer VPN-Verbindung aus dem Kundennetz zur Cloud der Fall sein. Dann kann eine nochmalige Multifaktor-Authentisierung bei der Anmeldung an die Cloud entfallen.

Prüffragen:

- Wird für sicherheitskritische Anwendungsbereiche (z. B. Verwaltung, Self-Service-Portal, oder Schutzbedarf höher als "normal") eine Multifaktor-Authentisierung eingesetzt, wenn der Zugang zum genutzten Cloud-Dienst direkt über das Internet erfolgt?

- Wird Multifaktor-Authentisierung für die Anmeldung von privilegierten Cloud-Benutzern eingesetzt?

# M 4.442 Zentraler Schutz vor Schadprogrammen in der Cloud-Infrastruktur

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Aufgrund der hohen Konzentration von Daten und Anwendungen in einer Cloud-Infrastruktur ist zusätzlich zum lokalen Schutz vor Schadprogrammen eine zentrale Komponente zur Abwehr von Schadprogrammen zu betreiben.

Dieser zentrale Schutz vor Schadprogrammen ("Virenschutz") muss an den zentralen Zugangspunkten zum Netz des Cloud-Diensteanbieters eingerichtet werden. Dies sollte unter Verwendung eines Application-Level-Gateways (ALG) erfolgen. Hierzu ist die Maßnahme M 4.226 *Integration von Virenscannern in ein Sicherheitsgateway* heranzuziehen und umzusetzen.

Empfehlenswert ist es, für den zentralen Schutz vor Schadprogrammen ein Schutzprogramm eines anderen Anbieters als für den lokalen Schutz auszuwählen, um die Erkennungsrate von Schadprogrammen zu maximieren.

Prüffragen:

- Wird zusätzlich zu lokalen Komponenten ein zentraler Schutz vor Schadprogrammen eingesetzt, entsprechend den anerkannten Regeln der Technik?

# M 4.443 Protokollierung und Monitoring von Ereignissen in der Cloud-Infrastruktur

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In einer Cloud-Infrastruktur muss für eine angemessene Protokollierung gesorgt werden, um technische Probleme und potenzielle Angriffe erkennen und darauf reagieren zu können. Da die Cloud-Infrastruktur hoch-integriert ist und über ein zentrales Cloud Management verfügt, muss eine zentrale Protokollierung eingeführt und der Baustein B 5.22 *Protokollierung* umgesetzt werden. Das Monitoring zielt in erster Linie darauf ab, den Betrieb zu steuern und die erhobenen Daten dienen dem Reporting an den Cloud-Anwender (siehe M 2.522 *Berichtswesen und Kommunikation zu den Cloud-Anwendern*).

Für eine angemessene Protokollierung und ausreichendes Monitoring sind folgende Aspekte zu berücksichtigen:

- Im Rahmen des Cloud Managements müssen die genutzten Cloud-Ressourcen überwacht werden, um stetig die in der Planung definierten Ressourcen gegenüber der aktuellen Benutzung und Nachfrage zu kontrollieren.
- Cloud-Dienste sollten je nach Servicemodell und Dienstgütevereinbarung bzgl. der Verfügbarkeit und anderer messbarer Größen, die Gegenstand der Vereinbarung sind, angemessen überwacht werden.
- Bei Public- und Private-Cloud-Angeboten muss eine Überwachung rund um die Uhr (24/7) erfolgen und Personal für zeitnahe Reaktionen bei Angriffen bzw. Sicherheitsvorfällen vorgehalten werden. Die Reaktionszeiten werden in der Dienstgütevereinbarung festgeschrieben. Bei Private-Cloud-Angeboten kann eine manuelle Interaktion als Reaktion auf Vorfälle zu Geschäftszeiten angemessen sein, sofern dieses mit den Service Level Agreements der Cloud-Dienste vereinbar ist.
- Der Cloud-Diensteanbieter verantwortet die Protokollierungs- und Monitoring-Möglichkeiten, die je nach Servicemodell unterschiedlich ausgeprägt sind. Wird z. B. Infrastructure as a Service angeboten, liegt die entsprechende Verantwortung für die Protokollierung und das Monitoring auf Plattform- und Anwendungsebene beim Cloud-Anwender. Hier kann der Cloud-Diensteanbieter die Anbindung an seine Monitoring-Systeme als zusätzliche Dienstleistung den Cloud-Anwendern anbieten. In diesem Fall muss der Cloud-Diensteanbieter dementsprechend die Maßnahmen zur Protokollauswertung umsetzen (siehe M 4.430 *Analyse von Protokolldaten*).
- Grundsätzlich muss technisch die Protokollierung auf allen vorhandenen Ebenen der Cloud-Infrastruktur eingerichtet sein (Applikationen/Dienste, Plattformen, Infrastruktur). Zu den entsprechenden Einrichtungen auf den unterschiedlichen Ebenen sind die Protokollierungsmaßnahmen aus den zu modellierenden Bausteinen aus den IT-Grundschutz-Katalogen heranzuziehen (z. B. auf der Schicht IT-Systeme die Maßnahme M 5.9 *Protokollierung am Server*).
- Bestehen seitens des Cloud-Diensteanbieters oder seitens der Cloud-Anwender Anforderungen an Computer-Forensik oder rechtliche Anforderungen hinsichtlich revisionssicherer Protokollierung, so muss der Cloud-Diensteanbieter integritätssichernde Mechanismen für die Logdateien einrichten. Beispielsweise können Protokolldateien digital signiert oder mit Checksummen versehen werden, um die Integrität nachzuweisen. In je-

dem Fall dürfen Zugriffsrechte auf Protokolle nur sehr restriktiv vergeben werden.
- Die Zugriffsrechte auf die Protokolldateien müssen regelmäßig (z. B. zweimal pro Jahr) evaluiert werden.
- Zur Nachvollziehbarkeit der Administration müssen alle kritischen administrativen Handlungen protokolliert werden (z. B. Starten von Diensten und Ändern von Log-Dateien). So kann der Cloud-Diensteanbieter gegenüber seinem Kunden nachvollziehbar darstellen, wer wann welche Änderungen an den bereitgestellten Diensten und ggf. Daten vorgenommen hat.
- Folgende Aspekte müssen aus Sicht des Cloud Managements mindestens protokolliert werden und müssen in der Umsetzung der Maßnahme M 2.499 *Planung der Protokollierung* berücksichtigt werden:
  - Netzlast und Verbindungsunterbrechungen,
  - Verbindungszeiten (Cloud-Management-Prozess SLA),
  - Ab- und Anmeldungen der Cloud-Benutzer, insbesondere fehlerhafte Anmeldeversuche,
  - Änderungen an Rollen und Berechtigungen,
  - kritische Transaktionen der Cloud-Administratoren und ggf. der privilegierten Benutzer des Cloud-Anwenders (Protokollierung privilegierter Benutzer auf Anwendungsebene obliegt bei SaaS dem Cloud-Diensteanbieter, bei IaaS- oder PaaS-Systemen den Cloud-Anwendern),
  - Aufzeichnung der Konfigurationsänderungen an Cloud-Dienstepro-filen, um eine Fehleranalyse zu vereinfachen,
  - Auslastung der Cloud-Ressourcen (CPU, Netz, Speicher),
  - Angriffsversuche,
  - Versuch von unberechtigten Zugriffen oder Manipulationsversuche.
- Eine Mandantentrennung sollte auch für den Zugriff auf die Protokolldaten durchgeführt werden, damit diese den Cloud-Anwendern zur Verfügung gestellt werden können, ohne die Vertraulichkeit der Protokolldaten der anderen Mandanten zu verletzen, und um die Benutzung in Gerichtsverfahren zu ermöglichen.

Prüffragen:

- Werden Ereignisse in der Cloud-Infrastruktur wie gefordert protokolliert?
- Werden Aktionen von Benutzern (nicht privilegierten und privilegierten) wie gefordert protokolliert?
- Enthalten die Aufzeichnungen der Protokollierung die geforderten Angaben?
- Erfolgt Protokollierung auf allen erforderlichen Ebenen?
- Gibt es eine Mandantentrennung beim Zugriff auf die Protokolldaten?
- Kann die Protokollierung effektiv ausgewertet werden?
- Ist der Zugriff auf Aufzeichnungen beschränkt?

# M 4.444 Patchmanagement für Cloud-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Änderungsmanager

Alle Cloud-Komponenten müssen in das Patch- und Änderungsmanagement integriert sein (siehe Baustein B 1.14 *Patch- und Änderungsmanagement*).

Beim Patchmanagement und bei der Installation des Patchens für Cloud-Komponenten müssen die Verantwortlichkeiten gemäß Maßnahme M 2.423 *Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement* beachtet werden.

Mit steigender Komplexität von Cloud-Infrastrukturen ist es üblich, dass die Mitarbeiter verschiedener Bereiche eines Cloud-Diensteanbieters unterschiedliche Verantwortlichkeiten bezüglich des Patchens besitzen. So kann es beispielsweise unterschiedliche Zuständigkeiten geben für

- Netze (Infrastrukturkomponenten, Router, Switches etc.)
- Betriebssysteme
- Virtualisierungs-Komponenten
- Applikationen
- Sicherheitskomponenten (z. B. Sicherheitsgateway, Schutz vor Schadprogrammen, Intrusion Detection).

Es ist nötig, sich bei den Software-Herstellern und Herausgebern von Patches regelmäßig über neue Patches zu informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Das Patchmanagement bildet den Rahmenprozess zur Kontrolle eines durchgängig angemessenen Sicherheitsniveaus durch aktuelle Patch-Stände. Detaillierte Vorgaben, wie beim Patchen einer Anwendung vorzugehen ist, enthält Maßnahme M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*.

Das Patchmanagement in Clouds umfasst verschiedene Teilaufgaben (siehe M 4.446 *Einführung in das Cloud Management*):

- Patchen von Cloud-Diensten (PaaS oder SaaS)
- Patchen von unterliegender Cloud-Infrastruktur (IaaS, PaaS und SaaS) einschließlich Zugangskomponenten wie Self-Service-Portal
- Patchen des Cloud-Verwaltungsservers und der Cloud-Verwaltungssoftware
- Patchen von Cloud-Ressourcen und Element-Managern

Beim Patchen von Cloud-Diensten wird empfohlen, nach Maßnahme M 2.422 *Umgang mit Änderungsanforderungen* vorzugehen. Hinsichtlich der Aspekte "Beurteilung der Auswirkungen" und Zeitplan ("geplantes Datum für die Umsetzung der Änderung") ist beim Cloud Management zu beachten:

- Das Patch- und Änderungsmanagement sollte in den Verträgen/Dienstgüte-Vereinbarungen (SLAs) mit Cloud-Anwendern geregelt sein.
- Diese Vereinbarungen zum Patch- und Änderungsmanagement können die Regelung von Standard-Änderungen (vergleiche Maßnahme M 3.66 *Grundbegriffe des Patch- und Änderungsmanagements*) einschließen.

- Während des Patchens können Cloud-Dienste zeitweise nicht oder mit verringerter Funktion bzw. reduzierter Leistung zur Verfügung stehen, mit Auswirkungen auf die Arbeitsfähigkeit der Cloud-Anwender.
- Auch bei bestmöglicher Vorbereitung sind unvorhergesehene Auswirkungen möglich, sodass die Funktion oder Verfügbarkeit von Cloud-Diensten nach dem Patchen beeinträchtigt sind. Eventuell muss eine Änderung sogar wieder rückgängig gemacht werden.
- Wegen dieser möglichen Auswirkungen sollten die betroffenen Cloud-Anwender vorher über anstehende Patches, den Zeitplan dafür und mögliche Auswirkungen informiert werden.
- Die Pflicht zur Information über anstehende Patches und die Abstimmung darüber mit dem Cloud-Anwender muss vertraglich festgelegt sein (SLA).

Die unterschiedlichen Service-Modelle legen die Einflussbereiche und somit die Verantwortung des Cloud-Diensteanbieters und des Cloud-Anwenders fest. Im Falle von IaaS sind die Patch-Möglichkeiten für den Cloud-Diensteanbieter eingeschränkt. Die Verantwortung für das Patch- und Änderungsmanagement auf Betriebssystemebene, Plattformebene und Anwendungsebene hat hier der Cloud-Anwender. Diese Verantwortungsbereiche sollten in den SLAs klar definiert sein.

Die durchgängige Virtualisierung beim Cloud Computing bietet für das Patch- und Änderungsmanagement Vorteile. Die Lastverteilung und die Beweglichkeit der virtuellen Ressourcen ermöglichen neue Strategien für das Patchen. So kann z. B. das Betriebssystem unter einem SaaS-Angebot gepatcht werden, ohne die Verfügbarkeit des Cloud-Dienstes zu stören. Ferner erlaubt die Cloud-Verwaltungslösung den Einsatz von Patch-Strategien, bei denen die Durchführung von Änderungen weitgehend automatisiert wird. Grundsätzlich wird eine Automatisierung zum Ausrollen von aktuellen Patch-Ständen z. B. über Cloud-Diensteprofile empfohlen. Es muss jedoch sichergestellt werden, dass die Konfigurationen der Cloud-Ressourcen nicht durch neue Patches beeinträchtigt werden. Alle Änderungen sollten entsprechend Maßnahme M 2.221 *Änderungsmanagement* oder Maßnahme M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* geplant, getestet, genehmigt und dokumentiert werden. Wenn vollständige Tests auf speziellen Test-Systemen nicht möglich sind, müssen zumindest die Konfigurationen vorab auf mögliche Auswirkungen von Patches überprüft werden.

Beim Ausrollen einer Anwendung für einen neuen Mandanten sollte die für diesen Mandanten genutzte Software auf den aktuellen Patch-Stand gebracht werden, bevor von außen auf die Anwendung zugegriffen werden kann.

In der Praxis sollte der Patch-Stand von den in der Cloud angebotenen Betriebssystemen und Anwendungen über einen sogenannten Update Manager des Cloud- oder Virtualisierungsproduktes verwaltet werden. Dafür muss konfiguriert werden, welche Updates auf Betriebssysteme und Anwendungen auf den Virtualisierungs-Hosts und virtuellen Maschinen durchgeführt werden sollen.

Prüffragen:

- Sind Patch-Verantwortliche für die Cloud-Dienste benannt?
- Werden beim Ausrollen neuer Mandanten alle Softwarestände auf den aktuellen Patch-Stand gebracht, bevor von außen auf die Anwendung zugegriffen werden kann?
- Ist die Verantwortung für das Patchen der Cloud-Systeme in den SLA vereinbart?

# M 4.445 Durchgängige Mandantentrennung von Cloud-Diensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine Mandantentrennung muss eingerichtet werden, damit ein Mandant (Cloud-Anwender) nicht unberechtigt Informationen von anderen Mandanten (Cloud-Anwendern) einsehen kann. Auch muss gewährleistet werden, dass kein Mandant auf die Ressourcen eines anderen Mandanten zugreifen kann, beispielsweise auf virtuelle Maschinen, Netze oder Cloud Storage.

**Allgemeine Prinzipien zur Mandantentrennung**

Die technische Umsetzung einer Mandantentrennung erfolgt an verschiedenen Komponenten der Cloud-Infrastruktur. Für die einzelnen Komponenten sieht der IT-Grundschutz eigene Bausteine vor, die die zu ergreifenden Maßnahmen zur Mandantentrennung beschreiben (siehe, je nach Komponente, insbesondere die Bausteine B 3.302 *Router und Switches*, B 3.303 *Speicherlösungen / Cloud Storage*, B 3.301 *Sicherheitsgateway (Firewall)* und B 4.1 *Lokale Netze*. Das Cloud Management stellt eine durchgängige Mandantentrennung über alle relevanten Ebenen der Cloud-Dienste und der Cloud-Infrastruktur sicher. Eine Mandantentrennung an einzelnen Komponenten der Cloud-Infrastruktur wird von den Administratoren dieser Komponenten eingerichtet. Die Anforderung einer durchgängigen Mandantentrennung für Cloud-Dienste verlangt eine Kontrolle der Trennmaßnahmen durch die Verantwortlichen für das Cloud Management (z. B. durch den Cloud-Administrator). Der Cloud-Diensteanbieter muss überprüfen, ob Maßnahmen zur Mandantentrennung sowohl in der Anwendung als auch in der Servervirtualisierung, im Netz und im Netz-Speicher (Storage) umgesetzt und wirksam sind. Das Cloud Management bildet hierbei den Rahmen um alle betroffenen IT-Grundschutz-Schichten, wohingegen die konkrete technische oder organisatorische Umsetzung in den anderen für Cloud Computing zu modellierenden Bausteinen verbleibt (siehe M 2.524 *Modellierung von Cloud Management*).

Eine technische Isolation der Cloud-Anwender und deren Daten kann durch Firewalls, Zugriffslisten, Tagging, VLANs, Virtualisierung, Maßnahmen im Speichernetz (z. B. LUN Masking) und physische Trennung erreicht werden.

**Mandantentrennung prüfen**

Um eine Kontrolle der Mandantentrennung in den einzelnen Cloud-Komponenten vorzunehmen, muss der Cloud-Diensteanbieter Prüfungen einrichten. Er muss die Rückmeldungen der Cloud-Komponenten für die Umsetzung von Maßnahmen zur Mandantentrennung nachvollziehen.

Die Umsetzung von Maßnahmen zur Mandantentrennung kann nachvollzogen werden über:

- Test- und Freigabeverfahren der Cloud-Diensteprofile,
- Auswertung der Protokolldateien der Cloud-Verwaltung,
- manuelle Prüfung der Konfigurationsdateien an den Cloud-Elementen oder
- Durchführung von Penetrationstests zur Validierung der Mandantentrennung.

**Mandantentrennung auf Anwendungs-Ebene**

Die sichere Isolierung von Anwendungen und Cloud-Daten kann über abgeschottete Bereiche (*Sandboxes*), virtuelle getrennte Speicherbereiche oder Kennzeichnung von Daten mittels *Tagging* erfolgen. Die Umsetzungsverantwortung dieser Maßnahmen liegt nicht im Cloud Management, sondern bei den Verantwortlichen in der Anwendungsentwicklung, die eine vom Cloud-Diensteanbieter spezifizierte Mandantentrennung zu implementieren haben. Bei webbasierten Cloud-Diensten sind die Empfehlungen des Bausteins B 5.21 *Webanwendungen* umzusetzen.

**Für PaaS: Mandantentrennung auf Plattform-Ebene**

Im Falle von PaaS-Angeboten können Datenbanken als Cloud-Dienste angeboten werden. In diesem Fall muss der Cloud-Diensteanbieter eine Mandantentrennung in der Datenbank einrichten. Diese Mandantentrennung kann über verschiedene Wege erfolgen:

- über eine separate Datenbank pro Cloud-Anwender (z. B. eine virtualisierte Datenbank pro Mandant)
- über eine Trennung der Mandantendaten durch Tagging-Methoden (d. h. Auszeichnung des Datenbestandes mit zusätzlichen Informationen) oder
- über die Anlage von getrennten Tabellen für jeden Mandanten.

Genaueres hierzu definiert der Baustein B 5.7 *Datenbanken*.

**Mandantentrennung auf Speicher-Ebene**

Auch auf Speicherebene sind Mechanismen zur Trennung von Speicher-Bereichen für unterschiedliche Mandanten zu ergreifen. Es kann eine logische Trennung von Speicherressourcen über LUNs mit mandantenbezogener Quell- und Ziel-Adresse erfolgen. Die Segmentierung eines SANs erfolgt durch Einteilung in Zonen (Zoning). Die Umsetzung von Trennmechanismen im SAN beschreibt M 5.130 *Absicherung des SANs durch Segmentierung*. Detaillierte Umsetzungsanweisungen gibt der Baustein B 3.303 *Speicherlösungen / Cloud Storage*.

**Mandantentrennung auf Netz-Ebene**

Eine durchgängige Mandantentrennung setzt eine Trennung auf Netz-Ebene zwingend voraus. Hierbei muss das Cloud Management insbesondere bei der Provisionierung von Cloud-Diensten auf Basis von Cloud-Diensteprofilen automatisiert getrennte Netze einrichten. Entsprechend müssen die Verwaltungssysteme für die Netzkomponenten Netztrennungskonfigurationen aus der Cloud-Verwaltungssoftware umsetzen.

Eine Mandantentrennung erfolgt über eine Trennung von VLANs, durch entsprechende Routing-Einstellungen (u. a. über Zugriffskontrolllisten) oder durch virtuelle Firewalls. Es sind entsprechende Maßnahmen aus der Schicht Netze für die konkreten Maßnahmen heranzuziehen:

- M 5.154 *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen*
- M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*

Im Cloud Management muss für die Einrichtung der Netze sichergestellt werden, dass das Management-Netz des Cloud-Diensteanbieters vom Datennetz der Cloud-Dienste isoliert ist. Hierbei kann eine Netztrennung auch über die vorgenannten Netztrennmechanismen erfolgen, die zur Mandantentrennung genutzt werden, wobei eine physische Trennung des Management-Netzes vorzuziehen ist.

**Mandantentrennung in der Verwaltungssoftware bei "virtual" bzw. "managed" Private-Cloud-Diensten**

"Virtual" bzw."managed" Private-Cloud-Dienste können auch als "DataCenter as a Service" bezeichnet werden. Hierunter versteht man komplexe IT-Infrastrukturen (virtuelle Maschinen, Netze inklusive Netzkoppelelemente und Speicher), die vom Cloud-Diensteanbieter angeboten werden. Hier kann sich auf Anforderung des Cloud-Anwenders die Mandantentrennung auch auf die Administration des Cloud-Diensteanbieters ausdehnen. In diesem Fall muss der Cloud-Diensteanbieter sicherstellen, dass ein dedizierter Cloud-Administrator die privaten Cloud-Dienste eines Cloud-Anwenders betreibt. Dieses muss über ein geregeltes Berechtigungs- und Rollenkonzept umgesetzt werden, welches die Zugriffe auf die Verwaltungsfunktionen der privaten Cloud über personenbeziehbare Konten auf autorisierte Cloud-Administratoren beschränkt. Diese Anforderungen sind bei der Auswahl einer Cloud-Verwaltungslösung zu berücksichtigen (siehe M 4.438 *Auswahl von Cloud-Komponenten* ).

Prüffragen:

- Ist die Mandantentrennung durchgängig an den relevanten Cloud-Komponenten umgesetzt?
- Werden Trennmechanismen bei der Vervielfältigung von Cloud-Diensten durchgängig eingehalten?
- Werden Prüfungen für eine durchgängige Trennung durchgeführt?
- Bestehen Rückmeldungen der Cloud-Komponenten, dass eine Mandantentrennung umgesetzt wurde?
- Wurden die Konfigurationen für die Mandantentrennung in den Cloud-Diensteprofilen überprüft?

# M 4.446 Einführung in das Cloud Management

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die nachfolgenden Eigenschaften zeichnen einen Cloud-Dienst aus:

- Die Provisionierung der Cloud-Ressourcen (z. B. Rechenleistung, Arbeitsspeicher, Netze, Speichernetze) läuft automatisch und ohne oder mit minimaler Interaktion, mit dem Cloud-Diensteanbieter ab (über sogenannte Self-Service-Portale).
- Die Cloud-Dienste sind über Standard-Schnittstellen (wie z. B. HTTP) über das Netz verfügbar und können so von unterschiedlichen Clients genutzt werden.
- Die Ressourcen des Cloud-Diensteanbieters liegen in einem Pool vor, welcher von vielen Cloud-Anwendern gemeinsam benutzt wird (Mandantenfähigkeit).
- Die Cloud-Dienste können schnell und elastisch zur Verfügung gestellt werden. Die Bereitstellung erfolgt hochgradig automatisch.
- Die Ressourcennutzung kann gemessen und überwacht werden und die Auswertung hierüber den Cloud-Anwendern zur Verfügung gestellt werden.

**Definitionen für Cloud Computing**

**Cloud Computing** bezeichnet das dynamisch an den Bedarf angepasste *Anbieten*, *Nutzen* und *Abrechnen* von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über *definierte technische Schnittstellen und Protokolle*. In den IT-Grundschutz-Katalogen wird der Begriff Cloud Computing nach vorgenannter Definition verwendet. Eine einfache Webanwendung ist in der Regel kein Cloud Computing.

Es gibt verschiedene Bereitstellungsmodelle für Cloud Computing. Die unterschiedlichen Bereitstellungsmodelle werden wie folgt definiert:

- In einer **Private Cloud** wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und kann dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen.
- Von einer **Public Cloud** wird gesprochen, wenn Cloud-Dienste von der Allgemeinheit oder einer großen Gruppe, wie beispielsweise einer ganzen Industriebranche, genutzt werden können und die Dienste von einem Anbieter zur Verfügung gestellt werden.
- In einer **Community Cloud** wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben. Eine solche Cloud kann von einer dieser Institutionen oder einem Dritten betrieben werden.
- Werden mehrere Cloud-Infrastrukturen, die für sich selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam genutzt, wird dies **Hybrid Cloud** genannt.

Die Bereitstellungsmodelle haben also damit zu tun, wie viele Anwender in welcher Konstellation eine Cloud nutzen.

Neben den Bereitstellungsmodellen gibt es auch verschiedene **Servicemodelle**. Die Servicemodelle richten sich nach Art und Umfang der bereitgestellten Cloud-Dienste:

- **Infrastructure as a Service (IaaS):** Bei IaaS werden IT-Ressourcen wie Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Cloud-Kunde kauft diese virtualisierten und in hohem Maß standardisierten Grund-Dienste und baut darauf eigene Dienste zum internen oder externen Gebrauch auf. So kann ein Cloud-Anwender z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.
- **Platform as a Service (PaaS):** Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf dieser Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe etc. zur Verfügung stellen. Der Kunde hat keine Verantwortung für die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der Cloud-Diensteanbieter in der Regel eigene Werkzeuge anbietet. PaaS erweitert die Grund-Dienste von IaaS um Plattformdienste wie Datenbank, Zugriffskontrollen oder Webserver.
- **Software as a Service (SaaS):** Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computing entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. SaaS-Angebote setzen auf die Grund-Dienste von IaaS und auf die Plattformdienste von PaaS mit vorkonfigurierten Anwendungen auf und bieten den Cloud-Anwendern ein ohne weiteres nutzbares Angebotspaket. Beispiele hierfür sind Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen.

**Rollen und Verantwortliche beim Cloud Computing**

Der Cloud-Diensteanbieter (CSP) bietet den Cloud-Dienst in unterschiedlichen Ausprägungen (SaaS, PaaS, IaaS) an. Die natürliche Person, die den Cloud-Dienst letztendlich in Anspruch nimmt, wird Cloud-Benutzer genannt. Ermöglicht eine Institution ihren Mitarbeitern die Nutzung von Cloud-Diensten, indem die Institution einen Vertrag mit dem Cloud-Diensteanbieter schließt, so tritt die Institution als Cloud-Anwender auf. Im Fall der privaten Nutzung eines Cloud-Dienstes sind Cloud-Anwender und Cloud-Benutzer identisch.

**Verwaltungskomponenten im Cloud Computing**

Für die Steuerung und die Verwaltung der *virtuellen* Infrastruktur der Cloud wird eine **Virtualisierungssoftware** eingesetzt.

Zur Verwaltung der Cloud selbst und ihrer *logischen* Infrastruktur wird üblicherweise ebenfalls eine Software benötigt. Diese wird als **Cloud-Verwaltungssoftware** bezeichnet.

Die Virtualisierungssoftware und die Cloud-Verwaltungssoftware können auf einem gemeinsamen oder auf getrennten physischen oder virtuellen IT-Systemen installiert sein.

Der Server für die Bereitstellung der Virtualisierungssoftware wird **Virtualisierungsserver** genannt.

Der Server für die Bereitstellung der Cloud-Verwaltungssoftware wird **Cloud-Verwaltungsserver** genannt.

Wenn Virtualisierungs- und Cloud-Verwaltungssoftware gemeinsam auf einem IT-System laufen, dient der Virtualisierungsserver somit gleichzeitig als Cloud-Verwaltungsserver.

**Referenzmodell für Cloud Computing**

Um die Betriebsprozesse des Cloud Managements zu beschreiben, wird ein Cloud-Referenzmodell genutzt, in dem die wesentlichen Aspekte abgedeckt sind. Dem Baustein B 5.23 *Cloud Management* liegt das Referenzmodell der Internet Engineering Task Force (IETF) zugrunde (Cloud Reference Framework, liegt als sogenannter Internet-Draft vor). Die IETF hat darin Bestandteile einer Cloud-Umgebung, deren Schnittstellen und die Steuerung von Cloud-Diensten definiert.

Das Referenzmodell ist in **Schichten** für Cloud-Dienste, Virtualisierung (virtuelle Maschinen, in denen die Cloud-Dienste laufen) und physische Komponenten (als Träger der virtuellen Maschinen) aufgebaut und beschreibt deren Zusammenwirken. Diese Schichten werden als "horizontale Schichten" bezeichnet. Diese Schichten sind:

- **Anwendungsschicht**: Hier werden die Servicemodelle (SaaS, PaaS, IaaS) verwaltet und Cloud-Dienste konfiguriert. Diese Schicht definiert die Anforderungen an die Cloud-Dienste und stellt diese den Cloud-Benutzern bereit.
- **Ressourcen-Kontroll-Schicht**: Diese Schicht verwaltet die virtuellen Ressourcen der Cloud-Infrastruktur für eine effiziente, verlässliche und sichere Bereitstellung. Die Ressourcen-Kontroll-Schicht stellt über Authentisierungskontrollen sicher, dass die verwalteten Cloud-Ressourcen den richtigen Cloud-Diensten und damit auch den korrekten Cloud-Benutzern bereitgestellt werden. Genauso wird über die Ressourcen-Kontroll-Schicht dafür gesorgt, dass die virtuellen Cloud-Ressourcen effizient auf die Hardware-Komponenten der Cloud-Infrastruktur verteilt werden.
- **Virtualisierungsschicht**: Physische Hardware-Komponenten sind schwierig auf unterschiedliche Mandanten aufzuteilen. Hingegen können virtuelle Ressourcen bedarfsorientiert allokiert und freigegeben werden. Daher werden über die Virtualisierungsschicht die physischen Cloud-Ressourcen in virtuelle Cloud-Ressourcen konvertiert. Die virtuellen Ressourcen werden in einem Ressourcen-Pool verwaltet und nach Bedarf den Cloud-Anwendern bereitgestellt oder entzogen.
- **Schicht der physischen Ressourcen**: Die Schicht zur Verwaltung von physischen Cloud-Ressourcen übernimmt die Einbindung und Bereitstellung von Hardware-Komponenten für die Cloud. Zu den Hardware-Komponenten zählen: Rechenleistung (CPU), Arbeitsspeicher, Speichernetze und deren Anbindung, Netzkarten (oft *Netzwerkkarten* genannt) und Netzverbindungen, Netz-Bandbreite und Netz-Ports.

Übergreifend zu diesen Schichten führt das Referenzmodell das Cloud Management als *vertikale* Schicht ein, die alle horizontalen Schichten betrifft und querschnittlich auf die zu verwaltenden Ressourcen (SaaS, PaaS, IaaS) wirkt. Hier wird unter anderem hervorgehoben, dass das Sicherheitsmanagement und die Sicherheitsmaßnahmen einen Querschnitt in alle horizontalen Cloud-Schichten haben. In der vertikalen Schicht des Cloud Managements sieht die IETF eine Reihe von Aufgaben und Funktionen vor:

- Konfigurationsmanagement,
- Provisionierungs- und Registrierungsdienste,
- Monitoring und Berichtswesen,
- Management der Dienstgüte-Vereinbarungen (SLAs),
- Sicherheit.

Zu den typischen Aufgaben eines Cloud-Diensteanbieters im Cloud Management zählen:

- die Bereitstellung eines Dienste-Katalogs mit der Beschreibung der angebotenen Cloud-Dienste;
- die Cloud-Konfiguration zur Provisionierung (Bereitstellung) bzw. De-Provisionierung von Cloud-Ressourcen (hierzu zählen: virtuelle Maschinen, virtuelle Datenspeicher, virtuelle Netze) und Cloud-Diensteprofilen (definierte Konfigurationen für Cloud-Ressourcen, mit deren Hilfe die angebotenen Dienste bereitgestellt werden);
- die Zuweisung der physischen und virtuellen Ressourcen zu den Cloud-Anwendern und die Konfiguration dieser Ressourcen;
- das Zugangs- und Zugriffsmanagement für die Cloud-Ressourcen und die Authentisierung von Zugang und Zugriff;
- die Überwachung der bereitgestellten Cloud-Dienste und -Ressourcen, um die garantierte Dienstgüte einzuhalten;
- die für den Kunden nachvollziehbare Abrechnung der in Anspruch genommenen Cloud-Dienste (anhand des Dienste-Katalogs).

Die nachstehende Abbildung zeigt das für den IT-Grundschutz verwendete Referenzmodell für Cloud Computing:

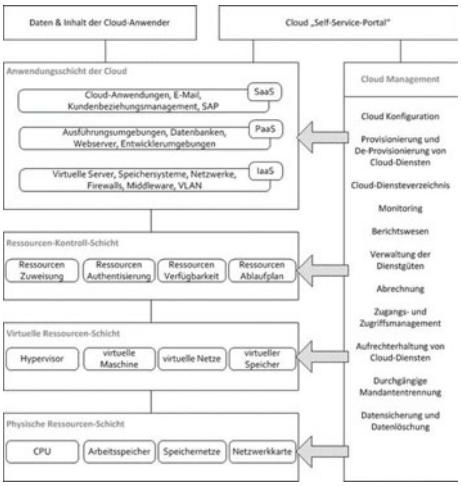



Abbildung: Referenzmodell für Cloud Computing (Überblick)

# M 4.447 Sicherstellung der Integrität der SAN-Fabric

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Integrität der SAN-Fabric bedeutet in dieser Maßnahme, dass lediglich die geplanten und vom Betreiber vorgesehenen Komponenten in einer SAN-Fabric in Betrieb sind und nicht ein unachtsamer Mitarbeiter oder vorsätzlich handelnder Angreifer Komponenten in die SAN-Fabric einbringt und dadurch die SAN-Fabric im Betrieb stört oder einen Datenabfluss ermöglicht. Um die Integrität der SAN-Fabric sicherzustellen, sollten Protokolle mit zusätzlichen Sicherheitsmerkmalen eingesetzt werden, die in dieser Maßnahme beschrieben werden.

Das American National Standards Institute (ANSI) hat in diesem Zusammenhang einen Standard entwickelt, der verschiedene Protokolle zur Erhöhung der Sicherheit in Fibre-Channel-Netzen beschreibt.

**Fibre Channel Secure Protocol (FC-SP)**

FC-SP beschreibt mögliche Architekturen für die sichere Authentisierung zwischen zwei Switches, Endgerät und Switch sowie zwischen zwei Endgeräten. Mithilfe der in FC-SPP beschriebenen Protokolle kann ein Switch neue Endgeräte am SAN entweder lokal authentisieren oder über einen zentral installierten Server, indem häufig auf eine bereits vorhandene Authentisierungsinfrastruktur zurückgegriffen wird.

Dem Anwender stehen drei verschiedene Protokolle zur Verfügung, mit deren Hilfe sich Authentisierungsmechanismen in einem Fibre-Channel-SAN umsetzen lassen:

- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP): DH-CHAP bietet die bidirektionale, passwortbasierte Authentisierung (CHAP) zusätzlich gesichert per Diffie-Hellmann-Verfahren zum Schlüsselaustausch.
- Fibre Channel Authentication Protocol (FCAP):
  FCAP realisiert die beiderseitige Authentisierung von FC-Komponenten auf der Basis digitaler Zertifikate.
- Fibre Channel Password Authentication Protocol (FCPAP):
  FCPAP stellt ein passwortbasiertes Verfahren dar, das sich das Secure Remote Password (SRP) zunutze macht.

Die Möglichkeiten dieser Protokolle sollten zur gegenseitigen Authentisierung der Komponenten genutzt werden. Durch den Einsatz dieser Protokolle kann sichergestellt werden, dass keine Komponenten der FC-Fabric beitreten können, ohne über die entsprechenden Zertifikate oder Passwörter zu verfügen. Die Konfiguration der Fabric kann damit weder gelesen noch manipuliert werden.

Selbst bei erfolgreichem physischen Anschluss fremder Komponenten an die SAN-Fabric besteht in der Folge kein Zugang, der beispielsweise das Mitlesen des Datenverkehrs ermöglichen würde. WWN-Spoofing bleibt auf diesem Weg erfolglos.

Prüffragen:

- Wird die Sicherstellung der Integrität der SAN-Fabric durch den Einsatz von Protokollen mit zusätzlichen Sicherheitsmerkmalen unterstützt?
- Werden beim Einsatz der Protokolle DH-CHAP, FCAP und FCPAP die Sicherheitseigenschaften dieser Protokolle berücksichtigt und entsprechende Konfigurationen verwendet?

# M 4.448 Einsatz von Verschlüsselung für Speicherlösungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für Informationen, die in einer Speicherlösung einen hohen Schutzbedarf bezüglich Vertraulichkeit aufweisen, sollten Möglichkeiten zum Einsatz von Verschlüsselung geprüft werden.

Werden Daten in Speicherlösungen verschlüsselt, müssen Institutionen weiterhin die Maßnahmen M 2.46 *Geeignetes Schlüsselmanagement* sowie M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation* beachten und die notwendigen Vorgaben umsetzen.

Es ist zwischen der Verschlüsselung der Daten auf dem Transportweg (Data-in-Motion) oder der Daten direkt auf der Speichereinheit (Data-at-Rest) zu unterscheiden. Die Verschlüsselung auf dem Transportweg ist auch bei Replikationen und Backup-Traffic relevant, während erstellte Backup- oder Archivdaten at Rest zu verschlüsseln sind.

Die Verschlüsselung von Daten mit hohem oder sehr hohem Schutzbedarf bezüglich Vertraulichkeit sollte vorrangig durch die Anwendung sichergestellt werden, die auch für die Verarbeitung der Daten zuständig ist.

Hierbei kann die Verschlüsselungstechnik entweder direkt in die Komponenten einer Speicherlösung integriert sein oder die Verschlüsselung mithilfe eines zusätzlichen Produkts gewährleistet werden. Eine einfach umzusetzende Lösung bietet zum heutigen Stand der Einsatz von selbst verschlüsselnden Festplatten innerhalb eines Speichersystems.

Der Transport von Fibre-Channel-Frames sollte auch dann über eine verschlüsselte Verbindung erfolgen, wenn die Daten das Rechenzentrum nicht verlassen.

Die Sicherung einer SAN-Verbindung über IP erfordert die Umsetzung zusätzlicher Schutzmaßnahmen, da eine IP-Verbindung wesentlich leichter zu kompromittieren ist als eine dedizierte Fibre-Channel-Verbindung. Stellt die Anwendung die Verschlüsselung der Verbindung nicht zur Verfügung, muss eine verschlüsselte Verbindung auf anderem Weg (beispielsweise über Funktionen des Betriebssystems oder des Transportnetzes) herbeigeführt und genutzt werden, um die Vertraulichkeit der Daten aufrechtzuerhalten.

Prüffragen:

- Erfolgt eine Verschlüsselung von Informationen mit hohem Schutzbedarf?
- Ist festgelegt, auf welchen Ebenen (Data-in-Motion und Data-in-Rest) die Verschlüsselung erfolgen soll?
- Werden zusätzliche Schutzmaßnahmen zur Absicherung einer SAN-Verbindung über IP umgesetzt?

# M 4.449 Einführung eines Zonenkonzeptes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Oft werden in Institutionen in der Regel große, aber einfache Netze aufgebaut, die ohne zusätzliche Sicherheitszonen auskommen. Dabei werden alle IT-Systeme einem einheitlichen Netz zugeordnet, an dessen Schnittstelle zum Internet eine zentrale Sicherheitsgateway-Lösung (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) für die Informationssicherheit zuständig ist. Eine solche einfache Sicherheitsarchitektur bietet jedoch gegen Angreifer oder Schadsoftware häufig ein zu geringes Maß an Sicherheit, da nach Überwindung des Sicherheitsgateways das gesamte Netz mit allen Komponenten und Daten offen steht.

Institutionen sollten angesichts dieser Gefährdung Maßnahmen ergreifen, um ihr Netz und damit die angeschlossenen IT-Systeme wie beispielsweise Server, Clients, Netz (IP und FC) und Speicherkomponenten abzusichern. Als eine mögliche Lösung bietet sich dabei die Bildung von Zonen an. Dazu wird das Netz in separate Bereiche untergliedert, die jeweils beispielsweise durch ein eigenes Sicherheitsgateway oder einen Paketfilter abgesichert werden.

Ein Zonenkonzept unterscheidet in der Folge verschiedene Sicherheitszonen mit unterschiedlichen Sicherheitseigenschaften. Die Einführung eines solchen Zonenkonzeptes basiert auf der Feststellung des unterschiedlichen Schutzbedarfs vorgehaltener Daten und bedarf zunächst sorgfältiger Planung.

Neben einer Schutzbedarfsanalyse sind alle derzeit im Netz vorhandenen Kommunikationsbeziehungen zu ermitteln und mit den tatsächlich notwendigen Verbindungen abzugleichen. Dieses Vorgehen dient der Reduktion des Netzverkehrs auf ein sinnvolles und notwendiges Maß und der Minimierung der Abhängigkeiten zwischen IT-Systemen. Die ermittelten Daten bilden die Basis für die Einteilung in Sicherheitszonen.

Sicherheitszonen unterscheiden sich dabei in der Regel durch:

- den Eigentümer der Prozesse und Daten,
- die Klassifizierung und den Schutzbedarf der zu verarbeitenden Informationsobjekte,
- die Benutzergruppen und Komponenten, die auf diese Informationsobjekte zugreifen dürfen,
- die Bedrohungen und die umgesetzten Sicherheitsmaßnahmen.

Alle eingesetzten IT-Systeme einer Institution werden genau einer Zone des Zonenkonzeptes zugeordnet. Eine Sicherheitszone stellt für dieses System eine Umgebung mit definierten Sicherheitseigenschaften bezüglich des Schutzes der Kommunikationsbeziehungen zu anderen Zonen dar. Im Zusammenspiel mit der Umsetzung eines Rechte- und Rollenkonzeptes, durch das Zugriffe auf IT-Systeme in jeweils angrenzende Zonen erlaubt oder unterbunden werden, können Daten mit einem höheren Schutzbedarf nach außen hin abgesichert werden.

Das Prinzip des Verbots zonenübergreifender Zugriffe sorgt dabei zusätzlich für die Erhöhung des Sicherheitsniveaus, da es verhindert, dass Angreifer ein kompromittiertes System mit weniger starken Sicherheitsmaßnahmen als "Sprungbrett" für das ganze Netz nutzen können. Wird ein IT-System kompromittiert, dann können lediglich die IT-Systeme aus der selben Zone angegrif-

fen werden. IT-Systeme anderer Zonen außerhalb der betroffenen Zone sind durch die Maßnahmen zur Trennung der Zonen abgesichert.

Das Zonenkonzept formuliert das Sicherheitsniveau von Einsatzumgebungen, das durch eine konkrete Netz-, Anwendungs- und Sicherheitsarchitektur realisiert werden muss. In Abhängigkeit vom Schutzbedarf der IT-Systeme sind unterschiedliche Ausprägungen möglich, die ein niedrigeres, mittleres oder höheres Schutzniveau gewährleisten.

Prüffragen:

- Ist eine Analyse der bestehenden Kommunikationsbeziehungen innerhalb des Netzes der Institution erfolgt?
- Wurde jedes IT-System einer einzigen Sicherheitszone zugeordnet?
- Existiert eine Sicherheitsarchitektur, die Anforderungen an die notwendigen Sicherheitsdienste und deren Schnittstellen für die einzelnen Sicherheitszonen beschreibt?

# M 4.450 Absicherung der Kommunikation bei Web-Services

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Da die Kommunikation mit Web-Services nicht immer zwingend intern, sondern auch extern über fremde Netze und weitere beteiligte Stellen ablaufen kann, muss sichergestellt werden, dass die Daten über einen sicheren Kanal übertragen werden. Ziel dabei ist es, die Vertraulichkeit und die Integrität der übertragenen Daten zu gewährleisten. Zur Absicherung der Kommunikation bei Web-Services können unterschiedliche Methoden und Standards angewendet werden, die sich in zwei grundlegende Strategien gliedern lassen:

- Transportbasierte Verschlüsselung und
- Nachrichtenbasierte Verschlüsselung.

**Transport-basierte Verschlüsselung mittels SSL/TLS**

Durch die Anwendung des SSL/TLS-Protokolls können die Kommunikationswege von Web-Services auf Transportebene abgesichert werden. Durch die Verschlüsselung des Datenstroms zwischen zwei Endpunkten ist sichergestellt, dass die Daten während der Übertragung geschützt sind und nicht mitgelesen werden können. Durch die Verschlüsselung wird ebenfalls sichergestellt, dass die Nachrichtenintegrität bewahrt wird. Zusätzlich zur Verschlüsselung birgt die Nutzung von SSL/TLS den Vorteil, dass dadurch mehrere Formen der Authentisierung relativ problemlos umgesetzt werden können:

- Serverauthentisierung: Der Server authentisiert sich gegenüber dem Web-Service-Client auf der Grundlage eines kryptographischen Zertifikats.
- Clientauthentisierung: Zusätzlich zum Server authentisiert sich auch der Client gegenüber dem Server anhand eines maschinenspezifischen Zertifikats.
- Benutzerauthentisierung: Die client-seitige Authentisierung kann auch mit benutzerbezogenen Zertifikaten erfolgen und so gleichzeitig zur Authentisierung des jeweiligen Benutzers verwendet werden.

Der Vorteil einer Verschlüsselung mit SSL/TLS besteht insbesondere darin, dass die Umsetzung weitgehend unabhängig von der Realisierung der Web-Services selbst erfolgen kann, im einfachen Fall durch entsprechende Konfiguration der Web- oder Applikationsserver.

Der Nachteil in der Verwendung von SSL/TLS liegt darin, dass nur die Verbindung zwischen zwei direkten Endpunkten verschlüsselt wird. Komplexere Szenarien, in denen zum Beispiel eine Nachricht über mehrere Zwischenstationen gesendet werden muss und der jeweilige Empfänger nur einen bestimmten Teil einer Nachricht lesen darf, lassen sich nicht abbilden.

Bei einer Verschlüsselung mittels SSL/TLS sind die Daten nur bei der Übertragung selbst verschlüsselt. Während sich die Daten zum Beispiel noch in der Warteschlange für die Nachrichtenverarbeitung auf dem Server befinden, liegen diese unverschlüsselt auf dem System vor. Der Einsatz von SSL/TLS muss daher vor dem Hintergrund des konkreten Anwendungsszenarios geprüft werden. Weitere Informationen zur Nutzung von SSL/TLS finden sich in M 5.66 *Clientseitige Verwendung von SSL/TLS* und M 5.177 *Serverseitige Verwendung von SSL/TLS*.

**Nachrichten-basierte Verschlüsselung mittels WS-Standards**

Da bei Web-Services Nachrichten über mehrere Intermediäre gehen können und eine Direktverbindung nicht immer möglich ist, erhält der Intermediär eventuell Informationen, die gar nicht für ihn bestimmt sind. Um die Sicherheit der Nachrichten gewährleisten zu können, müssen Nachrichten so behandelt werden können, dass Teilnachrichten nur von den rechtmäßigen Empfängern gelesen werden können, weshalb in diesem Fall auf eine nachrichtenbasierte Verschlüsselung, zum Beispiel auf XML-Ebene, zurückzugreifen ist. Dafür stehen verschiedene Standards zur Verfügung:

- XML-Encryption (XMLEnc)
- XML-Signaturen (XMLSig)
- WS-Security
- WS-SecureConversation

Eine nähere Beschreibung dieser Standards und ihrer Einsatzmöglichkeiten findet sich in der W-Maßnahme M 4.451 *Aktuelle Web-Service Standards*.

Für die Implementierung von kryptographischen Mechanismen sollte auf eine etablierte Softwarebibliothek (Framework) und bestehende Kryptobibliotheken (zum Beispiel für Java die Krypto-Bibliotheken IAIK-JCE oder Bouncy Castle, Letztere ist auch für C#/Microsoft .NET verfügbar) zurückgegriffen werden, da eine eigenständige Kryptoimplementierung sehr fehlerträchtig ist und erfahrungsgemäß Schwachstellen beinhaltet.

**Integrität**

Um die Kommunikation bei Web-Services abzusichern, sollte validiert werden, ob die XML-Strukturen der empfangenen Nachrichten dem vorgegebenen XML-Schema entsprechen. Wenn eine Nachricht nicht dem gewünschten Format entspricht, ist sie abzuweisen.

Zudem können XML-Signaturen eingesetzt werden, sodass Nachrichten erkannt werden, die auf der Kommunikationsstrecke manipuliert wurden. Eine Signatur sollte möglichst auf die komplette Nachricht angewendet werden, sodass ein Angriff auf die Integrität von vornherein nicht durchführbar ist. Können jedoch, z. B. aufgrund erheblicher Performance-Vorteile bei großen Nachrichten, nur bestimmte Elemente signiert werden, muss neben dem referenzierten Namen, die korrekte Position von signierten Inhalten mittels einer kontextabhängigen Semantik überprüft werden. Das bedeutet, es wird der absolute Pfad des signierten Elements geprüft. Weicht dieser von den Erwartungen ab, muss die Nachricht abgelehnt werden.

**Verfügbarkeit**

Da durch Web-Services ermöglicht wird, dass Geschäftsprozesse organisationsübergreifend realisiert werden, ist hierbei auch ein besonderes Augenmerk auf die Verfügbarkeit zu legen. Ein Ausfall einer Komponente kann zu einem Ausfall des gesamten Geschäftsprozesses führen, was sich auf mehrere Parteien auswirken kann. Aus diesem Grund müssen im Hinblick auf die Verfügbarkeit der Systeme Maßnahmen wie eine Lastverteilung oder Redundanzen der eingesetzten Applikationsserver mit betrachtet werden, um eine ausreichend hohe Verfügbarkeit erzielen zu können. Das Ziel muss dabei sein, den Verlust der Verfügbarkeit durch Ausfall einer einzigen Komponente (engl. Single Point of Failure) zu vermeiden. Abhängig von der Menge der durch das System verarbeiteten Nachrichten muss das System so skalierbar sein, dass dieses auch mit einem vermehrten Aufkommen von Anfragen umgehen kann.

Zusätzlich müssen Sicherheitsmaßnahmen getroffen werden, um das Risiko eines Ausfalls eines Web-Service durch gezielte Angriffe (Denial of Service) zu minimieren. Weitere Informationen hierzu finden sich in der Maßnahme M 4.405 *Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services*.

Prüffragen:

- Wird ein geeignetes Transport-basiertes oder Nachrichten-basiertes Verschlüsselungsverfahren eingesetzt, um den Nachrichtenaustausch abzusichern?
- Wurde für die Implementierung kryptographischer Funktionen auf eine etablierte Softwarebibliothek zurückgegriffen?
- Wurden für die Kommunikationsschnittstellen des Web-Service die Verfügbarkeitsanforderungen berücksichtigt und entsprechend umgesetzt?
- Werden XML-Signaturen eingesetzt und wird die korrekte Position des signierten Inhalts bei jeder Verwendung überprüft?

# M 4.451 Aktuelle Web-Service Standards

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Web-Services sind Softwareanwendungen, die über ein Netz bereitgestellt werden. Sie stellen vielfältige IT-basierte Dienste zur Verwendung durch nahezu beliebige Clients bereit.

Im Zusammenspiel komplexer IT-Landschaften spielen Web-Services zunehmend eine bedeutende Rolle. Dabei sind Sicherheitsaspekte in der Verwendung solcher Dienste von großer Relevanz.

Um eine reibungslose Integration von Web-Services in eine Service-Orientierte Architektur (SOA) zu gewährleisten, wurden verschiedene Standards entwickelt, die die unterschiedlichen Aspekte von Web-Services betrachten. Vor allem die *Organization for the Advancement of Structured Information Standards* (OASIS) und das *World Wide Web Consortium* (WC3) bieten eine Vielzahl von sich ergänzenden und aufeinander aufbauenden Standards zum Thema.

Basierend auf bewährten Internet-Transportprotokollen werden neben technischen und organisatorischen Themen auch Sicherheitsaspekte in Standards abstrahiert, um den komplexen Anforderungen der Geschäftsprozessmodellierung gerecht zu werden.

Die wichtigsten Standards mit Sicherheitsbezug sind in der folgenden Grafik visualisiert und werden in den nächsten Abschnitten kurz vorgestellt. Aufgrund der Komplexität des Themas und der beständigen Weiterentwicklung der Standards kann dies nur eine Auswahl darstellen, die keinen Anspruch auf Vollständigkeit erhebt.

**XML-Encryption**

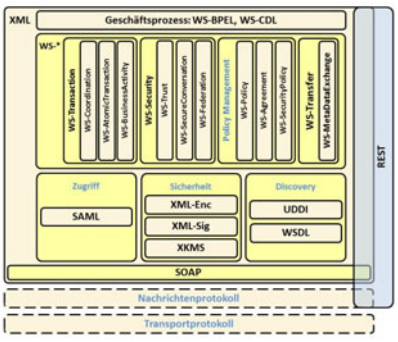



Abbildung: XML-Encryption ist eine Spezifikation zur Verschlüsselung von XML-Dokumenten. Sie wird vom WC3 verwaltet.

Die XML-Encryption-Spezifikation definiert verschiedene Möglichkeiten der Verschlüsselung. Es können ganze XML-Dokumente verschlüsselt werden, einzelne Elemente mit ihren Unterelementen oder der Inhalt einzelner XML-Elemente. Damit ist eine fein granulierte Verschlüsselung der XML-Daten möglich. Die verschlüsselten Daten sind wiederum XML-Dokumente oder Teile davon.

Durch die Verschlüsselung einzelner Elemente eignet sich XML-Encryption insbesondere dann, wenn mehrere nicht vertrauenswürdige Instanzen an der Nachrichtenübermittlung beteiligt sind, diese aber keine Kenntnis über die Nachrichten der anderen Empfänger haben dürfen. Das folgende Beispiel illustriert die Verschlüsselung von Kreditkartendaten innerhalb einer Nachricht:

*<?xml version='1.0'?>*

*<PaymentInfo xmlns='http://example.org/paymentv2'>*

*<Name>John Smith</Name>*

*<EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'*

*xmlns='http://www.w3.org/2001/04/xmlenc#'>*

*<CipherData>*

*<CipherValue>A23B45C56</CipherValue>*

*</CipherData>*

*</EncryptedData>*

*</PaymentInfo>*

Zu verschlüsselnde Daten werden durch die Anwendung von XML-Encryption immer durch das übergeordnete Element *EncyptedData* ersetzt.

Neben den verschlüsselten Daten können auch Informationen zum verwendeten Verschlüsselungsalgorithmus, dem Schlüssel und zum beabsichtigten Empfänger mit eingebettet werden. Damit ist auch eine Verschlüsselung für mehrere Empfänger möglich (zum Beispiel mit asymmetrischer Verschlüsselung im Rahmen einer Public-Key-Infrastruktur).

Die Verschlüsselung kann sowohl mit symmetrischen als auch asymmetrischen Verfahren realisiert werden. Zu beachten bei der Nutzung von XML-Encryption ist, dass sichere kryptographische Algorithmen eingesetzt werden müssen. Weitere Hinweise zu kryptografischen Algorithmen und Schlüssellängen sind in der Technischen Richtlinie des BSI *Kryptografische Verfahren: Empfehlungen und Schlüssellängen - Teil 2 Verwendung von TLS (TR-02102-2)* und M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* enthalten.

**XMLSignature**

*XML-Signature* definiert eine XML-Syntax für elektronische Signaturen. Funktionell ähnelt XML Signature dem Krypto-Standard PKCS#7, ist aber leichter erweiterbar und speziell auf XML-Dokumente zugeschnitten.

Mit XML-Signaturen können beliebige Ressourcen signiert werden. Typischerweise sind das XML-Dokumente oder Teile davon, aber es ist auch möglich, beliebige Daten zu signieren, die über eine URL adressierbar sind.

Wird eine XML-Signatur verwendet, um eine Ressource außerhalb des umgebenden XML-Dokuments zu signieren, wird sie als *detached signature* bezeichnet, werden Teile des umgebenden Dokuments signiert, ist das eine *enveloped signature*, sind die signierten Daten in der XML-Signatur enthalten, eine *enveloping signature*.

Da eine logische XML-Struktur je nach Umgebung unterschiedliche, gleichermaßen gültige Darstellungsformen haben kann, muss für eine zuverlässige Signierung eine standardisierte Transformation in eine kanonische Darstellung erfolgen (*Canonical XML*).

Beim Einsatz von XML-Signature ist wie auch bei der Anwendung von XML-Encryption auf die Auswahl starker kryptographischer Verfahren zu achten.

**XML Key Management Specification**

Die *XML Key Management Specification* (XKMS) basiert auf SOAP, XML-Signature und XML-Encryption und erlaubt es, asymmetrische kryptografische Schlüssel auf Basis von XML über Web-Services zu validieren und zu verwalten. Damit wird eine einfache Einbindung einer PKI (*Public-Key-Infrastruktur*) in die SOA ermöglicht.

Mittels *XML Key Registration Service Specification* (X-KRSS) werden der Lebenszyklus von Schlüsseln (Registrierung, Widerruf, Neuauflage) sowie die Wiedergewinnung von zugehörigen privaten Schlüsseln beschrieben.

*XML Key Information Service Specification* (X-KISS) definiert den Zugriff auf die Verifizierung von öffentlichen Schlüsseln und zugehörigen Zertifikaten.

Eine vertrauenswürdige Zwischeninstanz (*TrustPoint*, ebenfalls ein Web-Service) verarbeitet die Anfragen der Clients und bildet die Schnittstelle zu bestehenden Public-Key-Infrastrukturen. Dabei kann ein zentrales *Trust Management* realisiert werden, um die jeweiligen Anforderungen an Zugriffsschutz, Teilnehmerkreis und Vertrauenswürdigkeit umzusetzen.

**SAML**

Die *Security Assertion Markup Language* (kurz SAML) ist ein XML-basiertes Datenformat zum Austausch von Authentisierungs- und Autorisierungsinformationen. Damit können sicherheitsrelevante Informationen beschrieben und transferiert werden.

Die Entwicklung erfolgte durch das OASIS-Konsortium in Hinsicht auf Sicherheitsanforderungen in verteilten IT-Umgebungen. Neben der Nutzung verschiedener Anwendungen auf der Basis einer einmaligen Benutzeranmeldung (*Single Sign-On*) können auch verteilte Transaktionen mit mehreren Beteiligten und Autorisierungsdienste abgebildet werden.

Eine *SAML Assertion* enthält eine gekapselte Sicherheitsinformation, die grob vereinfacht folgendes besagt: "Zusicherung *A* wurde geprüft zur Zeit *t* von Prüfer *R* bezüglich Subjekt *S* unter der Bedingung *C*." Damit können neben Authentisierungsinformationen auch Zusicherungen über Eigenschaften von Objekten übertragen werden, die bei der Prüfung von Zugriffsrechten und dem Ablauf von Transaktionen eine Rolle spielen.

**SOAP**

SOAP (*Simple Object Access Protocol*) ist ein Netzprotokoll zum Austausch strukturierter Daten zwischen Systemen und zur Interprozesskommunikation. Es baut auf bekannte Internet-Protokolle wie zum Beispiel HTTP oder SMTP auf und basiert auf der W3C-Spezifikation *XML Information Set* zur Repräsentation der Daten. Es ist ein industrieller Standard des *World Wide Web Consortium* (W3C).

SOAP stellt ein Rahmenwerk dar, das die Struktur von Nachrichten beschreibt und festlegt, wie Daten in Nachrichten einzubetten und auszulesen sind. Da keine Vorgaben für eine Semantik der Nutzdaten definiert sind, können beliebige applikationsspezifische Inhalte übertragen werden. Somit können neben XML auch andere Datenformate (wie zum Beispiel CSV) Verwendung finden.

Zwar kann mittels SOAP über beliebige Transportprotokolle kommuniziert werden, aber in der Praxis wird aufgrund der Kompatibilität mit üblichen Netzarchitekturen meist auf die Nutzung von HTTP und HTTPS zurückgegriffen.

**REST**

*Representational State Transfer* (REST) beschreibt ein Entwurfsparadigma für Web-Anwendungen und kann im Großen und Ganzen auf Web-Services angewendet werden. REST basiert auf einfachen Prinzipien, die beim Entwurf und der Umsetzung einer REST-konformen Web-Anwendung berücksichtigt werden müssen.

Ursprünglich wurde REST in Hinsicht auf das HTTP-Protokoll entworfen, legt jedoch keine Details für die Implementierung fest. Es werden also auch keine Protokolle oder Standards vorgeschrieben. REST kann gut mit HTTP- beziehungsweise SOAP-basierten Web-Services umgesetzt werden.

Im Zentrum der Betrachtung steht bei REST neben den Ressourcen, die eine Web-Anwendung bereitstellt, die Uniformität der Kommunikationsschnittstelle. Daneben wird eine simplifizierte Struktur der Netzkommunikation entworfen, um die Unabhängigkeit, Skalierbarkeit und Vernetzbarkeit der Komponenten zu erhöhen.

Im Einzelnen gelten folgende Prinzipien:

- *Client-Server*: Die Zuständigkeiten zwischen Server und Client werden klar aufgeteilt (*Separation of Concerns*). Dies gilt insbesondere für die Datenhaltung.
- *Zustandslosigkeit*: Die Kommunikation ist zustandslos. Jede REST-Anfrage enthält alle Informationen, die der Server benötigt, um die Anfrage ordnungsgemäß zu verarbeiten. Der Server muss keine Client-bezogenen Informationen aus Kommunikationsvorgängen speichern, um zukünftige Anfragen zu bearbeiten.
- *Cachefähigkeit*: Ressourcen können vom Server als cachefähig gekennzeichnet werden. Damit können alle Stationen der Netzkommunikation bis hin zum Client die Serverantwort zwischenspeichern und für Interaktionen wiederverwenden.
- *Einheitliche Schnittstelle*: Auf die Schnittstelle zwischen Client und Server wird das aus der Softwareentwicklung bekannte Prinzips der Generalisierung angewendet. Dadurch wird die Standardisierung von Adressierung, Kommunikation, Datenstrukturen und Transaktionen verpflichtend für eine REST-konforme Web-Anwendung.
- *Mehrschichtigkeit*: Durch die Einführung einer geschichteten Web-Architektur wird die Skalierbarkeit und Flexibilität weiter erhöht. Dabei kennt jede Komponente nur ihre unmittelbaren Kommunikationspartner und hat keine Informationen über die weitere Struktur des Gesamtsystems. Zudem können durch Zwischenschichten und Proxys auch Dienste gekapselt, Altsysteme eingebunden, Sicherheitsanforderungen umgesetzt und Aufgaben und Lasten verteilt werden.
- *Code on Demand*: Dem Server wird ermöglicht, den Clients Softwarebestandteile zur Verfügung zu stellen, mit denen die clientseitige Funktiona-

lität erweitert werden kann. Damit werden dem Client serverunabhängige Aktivitäten auf der Basis der übermittelten Daten ermöglicht.

Das für die Standardisierung der Schnittstelle relevante Prinzip der einheitlichen Schnittstelle enthält folgende Vorgaben:

- *Adressierung*: Bereitgestellte Ressourcen müssen eindeutig identifizierbar sein. Dafür bieten sich URIs (*Uniform Resource Identifier*) oder URLs (*Uniform Resource Locator*) an.
- *Manipulation von Ressourcen über Repräsentationen*: Aktionen über Ressourcen (Anlegen, Abrufen, Ändern, Löschen) werden durch den Austausch von Repräsentationen der Ressourcen durchgeführt. Dabei können die gewünschten Daten in verschiedenen Darstellungsformen (*Media Type*) transferiert werden (zum Beispiel HTML, XML, JSON, PDF). Die gewünschte Aktion wird über Operationen wie zum Beispiel POST (Erzeugen von Ressourcen), GET (Abrufen von Ressourcen), PUT (Aktualisieren von Ressourcen), DELETE (Löschen von Ressourcen) festgelegt. Weitere Operationen zu Status, Zugriffsrechten, Historie der Ressource oder anderen Funktionen sind möglich.
- *Selbstbeschreibende Nachrichten*: Jede Anfrage eines Clients und jede Serverantwort ist eine Nachricht und muss selbstbeschreibend sein, das heißt die Nachricht enthält alle Informationen, die der Empfänger benötigt, um seine Aufgabe ordnungsgemäß durchzuführen.
- *Verwendung von Hypermedia*: Hypermedia ist der Antrieb einer Web-Anwendung. Jede Manipulation des Anwendungszustandes und jeder Ressourcenabruf erfolgt über Hypermedia. Hypermedia bedeutet in diesem Zusammenhang, dass alle für den Client relevanten Web-Service-internen Verweise auf andere Repräsentationen der Ressourcen sowie alle angebotenen Aktivitäten durch den Web-Service selbst zur Verfügung gestellt werden müssen, der Client also keine umfassende Kenntnis der Web-Service-Struktur benötigt, um diesen nutzen zu können. Die Bereitstellung dieser Informationen kann zum Beispiel als in eine XML-Struktur eingebundene URL erfolgen.

Folgende Vorteile ergeben sich aus der Anwendung von REST für Web-Services:

Durch die strikte Aufgabenteilung können Client und Server leichtgewichtig ausgelegt sein, ein hoher Grad an Interoperabilität wird ermöglicht, und alle Komponenten können unabhängig voneinander weiterentwickelt oder sogar ausgetauscht werden. Die Zustandslosigkeit der Kommunikation vereinfacht die beidseitige Datenhaltung. Hypermedia ermöglicht die Nutzung von Web-Services ohne genaue Kenntnis der zugrunde liegenden Implementierung und erleichtert die Orchestrierung einer SOA-Landschaft. Die Einheitlichkeit der Schnittstellen erfordert ein hohes Maß an Standardisierung, die Voraussetzung für eine systemübergreifende SOA-Integration ist. Die Mehrschichtigkeit erlaubt eine transparente Kommunikation auch in komplexen Systemlandschaften mit hohen Anforderungen an Verfügbarkeit.

**Web Services Description Language (WSDL)**

*WSDL* ist eine XML-basierte Metasprache zur Beschreibung von XML-basierten Webservices. Eine WSDL-Datei stellt eine maschinenlesbare Beschreibung der Aufrufe, Parameter, Datenstrukturen und Rückgabewerte eines Web-Service dar. Es sind neben der Schnittstellenbeschreibung und den Zugangsprotokollen alle notwendigen Informationen für den Zugriff auf den Web-Service enthalten.

WSDL wird häufig mit *SOAP* und *XML Schema* eingesetzt, um XML-basierte Web-Services in einer verteilten IT-Landschaft zu orchestrieren. Ein Client kann aus der WSDL-Datei ermitteln, welche Funktionen auf dem Server verfügbar sind. Aus der WSDL-Spezifikation des Dienstes kann automatisiert Quellcode für die Verwendung des Web-Service mittels SOAP-Nachrichten generiert werden.

**UDDI (Universal Description, Discovery and Integration)**

UDDI bezeichnet im SOA-Umfeld einen standardisierten Verzeichnisdienst für Web-Services. Er spielt eine zentrale Rolle bei der dynamischen Bindung von Clientanforderungen an Web-Services.

Die benötigten Informationen werden in drei Katalogen angeboten. In den *White Pages* werden die Basisinformationen vorgehalten, sie beschreiben die Identität des Serviceanbieters. Die *Yellow Pages* kategorisieren die angebotenen Dienste nach einer standardisierten Taxonomie. Dabei können international anerkannte Standards zum Einsatz kommen (zum Beispiel UNSPSC - *United Nations Standard Products and Services Code*). Die *Green Pages* schließlich halten die Schnittstellenbeschreibungen der Web-Services vor.

Die technischen Aspekte des Dienstes werden strukturiert im sogenannten *tModel* abgelegt. Um eine Anforderung einem konkreten Dienst zuzuordnen, werden die tModel-Beschreibungen (*tModel-Keys*) von Client und Web-Service miteinander abgeglichen. Die Binding-Informationen (*bindingTemplate*) werden dann dem Client dynamisch hinzugefügt.

**WS-***

Eine eigene Gruppe industrieller Standards sind die WS-*-Spezifikationen. Sie werden überwiegend vom W3C und OASIS betreut und schließen die Lücke zwischen den eher technisch ausgerichteten Web-Service-Standards und den hohen Anforderungen der Geschäftsprozess-Ebene. Sie richten sich an jeweils genau ein Anwendungsgebiet, bauen teilweise aufeinander auf, und können kombiniert werden, um komplexe Anforderungen abzubilden. Dazu gehören neben Adressierung, Kontext, Koordination, Zuverlässigkeit, Metadaten und Transaktion insbesondere auch Vertraulichkeit, Integrität und Verfügbarkeit, aber auch Zugriffssteuerung und Rechtemanagement.

Die Standardisierung ermöglicht die plattformunabhängige und systemübergreifende Abbildung komplexer Geschäftsprozesse auf der Basis von SOAP und WSDL. Es folgt eine Auswahl von WS-*-Spezifikationen mit besonderer Relevanz für die Sicherheit von Web-Services.

**WS-Policy**

WS-Policy ist ein Standard, der es Web-Services erlaubt, Auskunft über ihre Richtlinien bezüglich Sicherheit, Qualität oder andere Anforderungen zu geben. Es ist die grundlegende Spezifikation für ein Rahmenwerk, das die Definition erforderlicher und optionaler Richtlinien für Dienste und Dienstnutzer ermöglicht.

Mittels *WS-PolicyAssertions* wird eine Menge an Standardzusicherungen beschrieben, die innerhalb einer Policy verwendet werden können. Eine Policy Assertion beschreibt eine Verhaltenseigenschaft, eine Pflicht oder eine Möglichkeit. Eine Menge dieser Richtlinien kann in der WSDL einer Web-Service-Entität (Operation, Nachricht, Endpunkt) zugeschrieben werden. In der WS-Policy-Spezifikation wird nicht festgelegt, welche Richtlinien existieren,

das geschieht in speziellen Domänen-spezifischen Spezifikationen (Sicherheit, Transaktion und andere).

*WS-PolicyAttachment* standardisiert das Verknüpfen von Policies mit WSDL und UDDI, wahlweise innerhalb der Beschreibungselemente oder extern und referenzierbar.

**WS-Security**

Die *Web Services Security Language* (WS-Security, WSS) basiert auf XML-Signature und XML-Encryption. Ziel vom WS-Security ist es, den sicheren Austausch von SOAP-Nachichten zu gewährleisten und somit die Vertraulichkeit und Integrität von Nachrichten sicherzustellen. Als Erweiterung für SOAP schreibt sie genau vor, auf welche Weise Verschlüsselungsinformationen, Signaturen und Authentisierungstoken in Nachrichten eingebettet werden. Dabei werden verschiedene Modelle von Authentisierungstoken unterstützt, unter anderem X.509-Zertifikate, Kerberos-Tickets, Benutzername/Password-Kombinationen und SAML-Assertions. Die Nachricht ist somit durchgehend geschützt, wenn die Übertragung durch mehrere Instanzen erfolgt.

Ein einfaches Authentisierungstoken für eine Authentisierung mit Benutzername und Passwort sieht bei WS-Security zum Beispiel so aus:

*<wsse:UsernameToken>*

*<wsse:Username>manfred.testheimer</wsse:Username>*

*<wsse:Password Type="wsse:PasswordDigest">*

*59xi0qBCwKxwgmMxU38nOouyqDA=*

*</wsse:Password>*

*<wsse:Nonce>Sd7rTLv5W/mLa9eX2a0+rk==</wsse:Nonce>*

*<wsu:Created xmlns:wsu=*

*"http://schemas.xmlsoap.org/ws/2002/07/utility">*

*2013-07-12T14:12:45Z*

*</wsu:Created>*

*</wsse:UsernameToken>*

Die Zufallszahl (Nonce) und der Generierungszeitpunkt, die beide in den Password-Hash eingehen, sind optional. Von diesen Möglichkeiten sollte Gebrauch gemacht werden, da damit die Robustheit gegen Angriffe erhöht wird.

Ein Kerberos-Ticket sieht in WS-Security dagegen zum Beispiel so aus:

*<wsse:BinarySecurityToken*

*ValueType="wsse:Kerberosv5ST"*

*EncodingType="wsse:Base64Binary">*

*SGllciBrb2VubnRIIElocmUgV2VyYnVuZyBzdGVoZW4hCg==*

*</wsse:BinarySecurityToken>*

**WS-Transfer**

WS-Transfer ist die Spezifikation eines SOAP-basierten Protokolls für den Austausch von XML-basierten Repräsentationen von Entitäten über eine Web-Service-Infrastruktur. Entitäten sind dabei:

- Ressourcen, die über einen Web-Service adressierbar sind und eine XML-Repräsentation haben
- Web-Services, die entsprechend einer XML-Repräsentation neue Ressourcen generieren (*Resource Factories*)

Dabei werden Anfrage und Antwort zu einer Transaktion jeweils als XML-Dokumente übertragen. Eine direkte Einbettung der XML-Repräsentation ist möglich.

Als Operationen für Ressourcen sind *GET* (verpflichtend) sowie *PUT* und *DELETE* (jeweils optional) vorgeschrieben. Für *Resource Factories* ist die Operation *CREATE* (optional) vorgesehen.

**WS-MetaDataExchange**

Web-Services benutzen Metadaten, um zu beschreiben, auf welche Art andere Endpunkte auf sie zugreifen können, und was dabei zu beachten ist. Dazu werden vor allem *XML-Schema*, *WSDL*, *WS-Policy* und *WS-PolicyAttachment* verwendet. Um den automatisierten Zugriff auf diese Metadaten zu erleichtern, definiert WS-MetaDataExchange *Metadata Resources*, die Consumern erlauben, die für eine korrekte Nutzung der Web-Services erforderlichen Metadaten abrufen zu können. Dafür werden Ressourcen nach dem WS-Transfer-Standard verwendet, die die entsprechenden Informationen in XML verpackt enthalten.

**WS-Agreement**

In einer SOA-Landschaft sind Aussagen über Verfügbarkeit, Qualität und andere Eigenschaften von Web-Services von entscheidender Bedeutung für die Konsumenten. WS-Agreement beschreibt Protokolle und Datenstrukturen zur Repräsentation von *Service Level Agreements* für Web-Services.

Unter anderem können Übereinkünfte angeboten, akzeptiert, abgelehnt oder terminiert werden, und der Status einer Übereinkunft kann abgefragt werden.

Großer Wert wurde auf Flexibilität und Erweiterbarkeit gelegt, um die domänenspezifischen Anforderungen in unterschiedlichen Umgebungen abbilden zu können.

**WS-ReliableMessaging**

WS-ReliableMessaging widmet sich der zuverlässigen Nachrichtenübermittlung. Damit kann sichergestellt werden, dass Nachrichten auch im Falle eines Versagens einzelner Komponenten verlässlich den Empfänger erreichen. Damit kann die Anwendung einerseits auf Fehler oder Probleme in der Kommunikation reagieren, andererseits kann für die übermittelten Nachrichten nachgewiesen werden, dass sie den Empfänger erreicht haben (Schutzziel der Nichtabstreitbarkeit).

Das wird erreicht, indem zwischen Sender und Empfänger eine Vermittlerschicht eingezogen wird, die von den Kommunikationsteilnehmern praktisch transparent genutzt wird. Die Nachricht wird über die *Reliable Messaging Source* an die Zwischenschicht übergeben, durch entsprechende Mechanismen abgesichert zugestellt und von der *Reliable Messaging Destination* dem

eigentlichen Empfänger übergeben. Die Kommunikation basiert auf SOAP und WSDL. An die Übermittlung können unterschiedliche Anforderungen gestellt werden: *AtLeastOnce* (mindestens einmal), *AtMostOnce* (höchstens einmal), *ExactlyOnce* (genau einmal) sowie, kombinierbar mit jedem der anderen, *In-Order* (in der ursprünglichen Reihenfolge). Wenn die geforderte Übermittlung nicht möglich ist, wird dem Absender ein Fehler gemeldet.

Zu WS-ReliableMessaging gehört auch *WS-Reliable Messaging Policy Assertion*, womit sich Richtlinien rund um die verlässliche Nachrichtenübermittlung beschreiben lassen, die in *WS-Policy* eingebunden werden können.

**WS-Transaction**

WS-Transaction ist ein Standard, der das aus der Datenbankwelt bekannte Konzept der *Transaktion* für Web-Services bereitstellt. Ziel ist, bei Operationen in komplexen Umgebungen gemeinsame Aktivitäten zu koordinieren und ein transparentes und konsistentes Verhalten aller beteiligten Dienste zu gewährleisten.

Dafür werden drei Unterspezifikationen bereitgestellt: *WS-Coordination* zur Koordinierung von Aktivitäten, *WS-AtomicTransaction* für kurz laufende Transaktionen und *WS-BusinessActivity* für länger laufende Transaktionen.

**WS-Coordination**

WS-Coordination bietet einen erweiterbaren Rahmen, der Protokolle beschreibt, die die Koordinierung von Web-Service-Aktivitäten in verteilten Systemen erlauben. Damit kann zwischen mehreren Beteiligten eine Übereinkunft hergestellt werden, wie das Ergebnis ihrer aus einzelnen Aktivitäten bestehenden Transaktion aussehen soll. Es stellt auch eine Abstraktionsmöglichkeit für bestehende Koordinationssysteme wie zum Beispiel Arbeitsabläufe (*Workflows*) dar.

Eine zentrale Stelle (*Coordination Service*) übernimmt die Koordination und erlaubt die Registrierung der Teilnehmer innerhalb eines Koordinationskontextes.

**WS-AtomicTransaction**

WS-AtomicTransaction basiert auf WS-Coordination und spezifiziert nur noch die Protokolle für kurz laufende Transaktionen, für die die *ACID*-Eigenschaften wichtig sind: *Atomicity* (Abgeschlossenheit), *Consistency* (Konsistenzerhaltung), *Isolation* (Isolation), *Durability* (Dauerhaftigkeit).

Dafür werden folgende Protokolle vorgesehen: *Completion* (für den Initiator der Transaktion), *Volatile Two-Phase Commit* (für Teilnehmer mit flüchtigen Ressourcen wie zum Beispiel Caches) und *Durable Two-Phase Commit* (für Teilnehmer mit nicht flüchtigen Ressourcen wie zum Beispiel Datenbanken).

Eine *Atomic Transaction* kann nur erfolgreich beendet werden, wenn alle Teilaufgaben erfolgreich beendet wurden. Da vorausgesetzt wird, dass sich alle Teilnehmer kooperativ verhalten, sollten *Atomic Transactions* nur in einem vertrauenswürdigen Umfeld eingesetzt werden.

**WS-BusinessActivity**

WS-BusinessActivity basiert ebenfalls auf WS-Coordination und definiert den Koordinationstyp *Business Activity*. Dieser Koordinationstyp ist für den Einsatz

bei langlebigen Aktivitäten mit Teilnehmern unterschiedlicher Vertrauenswürdigkeit (*Trust Domains*) gedacht.

Eine *Business Activity* erlaubt den Teilnehmern die wechselseitige Übereinkunft bezüglich verteilt auszuführender Operationen. Ein wesentliches Merkmal ist, dass Operationen beliebig verschachtelt werden können (*Nested Scopes*). Dabei kann auch auf *Atomic Transactions* zurückgegriffen werden.

Im Unterschied zur *Atomic Transaction* kann eine *Business Activity* auch dann erfolgreich beendet werden, wenn einzelne, untergeordnete Aktivitäten scheitern. Die Entscheidung darüber ist vom Initiator der Aktivität zu treffen. Damit sind auch komplexe Geschäftsprozesse und Entscheidungsabläufe abbildbar, und es können Teilnehmer unterschiedlicher Kooperationsfähigkeit eingebunden werden.

**WS-Trust**

WS-Trust ist eine Erweiterung von WS-Security und ermöglicht den Austausch von zugesicherten Eigenschaften bestimmter Subjekte innerhalb und zwischen Domänen (Trust Domänen). Dabei geht es um das Herausgeben, Erneuern und Validieren von *Security Tokens* sowie die Vermittlung, den Aufbau und die Bewertung eines sicheren Nachrichtenaustauschs.

WS-Trust umfasst die Beschreibung eines Web-Service, der mit WS-Security kompatible Security Tokens herausgibt (*Security Token Services*, STS). Zudem wird das Format von Nachrichten festgelegt, die für die Kommunikation rund um Security Tokens Verwendung finden, sowie Mechanismen zum Austausch kryptografischer Schlüssel.

**WS-SecureConversation**

WS-SecureConversation verfolgt den Ansatz einer sitzungsbasierten Sicherheit. Somit unterstützt WS-SecureConversation einen Sicherheitskontext, der nach der ersten Authentisierung generiert wird. Der Sicherheitskontext erlaubt eine fortdauernde abgesicherte Kommunikation über mehrere Nachrichten oder Transaktionen hinweg und senkt damit den Aufwand für die Absicherung der Kommunikation. Dieser Standard sollte insbesondere dann angewendet werden, wenn eine hohe Anzahl an Nachrichten zwischen Web-Services ausgetauscht werden muss.

Der durch WS-Secure-Conversation generierte Sicherheitskontext besteht aus einem gemeinsamen Sitzungsschlüssel, der auch als *SecurityContextToken-Element* bezeichnet wird. Der Austausch des Tokens zwischen den Parteien erfolgt durch das Diffie-Hellmann-Verfahren und wird dann für die Ver- und Entschlüsselung verwendet. Zur Generierung des Sicherheitskontextes stehen die folgenden Möglichkeiten bereit:

- Nutzung eines Security Token Services (STS) mit WS-Trust: Die Kommunikationspartner vertrauen einem externen Dienst, der für das Erzeugen der Token verantwortlich ist.
- Erzeugung und Verteilung durch einen Kommunikationspartner: Ein Kommunikationspartner ist für das Erzeugen und Verteilen des Tokens verantwortlich. Das setzt voraus, dass alle Beteiligten dem Aussteller vertrauen.
- Erzeugung mit einem Challenge/Response-Verfahren.

Zusätzlich existieren Mechanismen, um einen Sicherheitskontext zu erneuern, abzuändern, zu erweitern oder aufzukündigen.

**WS-Federation**

WS-Federation steht in engem Zusammenhang mit WS-Security und beschreibt eine flexible Infrastruktur für föderierte Identitäten. Bei diesem Konzept werden Identitäten nicht von einer zentralen Instanz verwaltet, sondern von verteilten Instanzen, die jeweils für eine bestimmte Gruppe von Identitäten zuständig sind (zum Beispiel Für die Mitarbeiter einer Institution). Die einzelnen Instanzen zur Identitätsverwaltung sind miteinander verbunden und vertrauen sich gegenseitig. WS-Federation erlaubt die Vermittlung von Identitäten, Attributen und Authentisierungsvorgängen zwischen unterschiedlichen Sicherheitskontexten. Dabei wird auf WS-Trust und WS-MetadataExchange zurückgegriffen.

**WS-SecurityPolicy**

*Web Service Security Policy Language* (WS-SecurityPolicy) beschreibt sicherheitsbasierte *Policy Assertions*. Damit sind spezielle Zusicherungen gemeint, die Web-Services erfüllen müssen, damit sicherheitsrelevante Aspekte erfüllt sind.

Die Spezifikation erweitert die fundamentalen Sicherheitsprotokolle, die in WS-Security, WS-Trust und WS-SecureConversation spezifiziert sind, indem Mechanismen angeboten werden, die Anforderungen und Fähigkeiten von Web-Services als Zusicherungen (Policies) darzustellen.

**Web Single Sign-On**

*Web Single Sign-On Interoperability Profile* und *Web Single Sign-On Metadata Exchange Protocol* sind Spezifikationen zum Identitätsmanagement, die die Interoperabilität mit Protokollen der *WS-Federation* und der *Liberty Alliance* sicherstellen sollen. Sie basieren unter anderem auf SAML und WS-MetadataExchange.

Ziel ist es, das Identitätsmanagement bestehender Lösungen in Web-Services zu integrieren und den Zugriff auf Eigenschaften der hinterlegten Identitäten zu ermöglichen. Damit ist eine plattformübergreifende, zentralisierte Identitätsverwaltung möglich, die eine Zugriffssteuerung für Web-Services mit einbezieht.

**WS-BPEL**

Die *Web Services Business Process Execution Language* (WS-BPEL) ist eine Sprachdefinition zur Spezifizierung von Web-Service-Aktivitäten innerhalb von Geschäftsprozessen. Sie wird zur Beschreibung der Orchestrierung von Webservices verwendet und basiert auf WSDL. Die Beschreibung selbst wird wiederum als Web-Service bereitgestellt.

Neben *Basic Activities* (grundlegende Aktivitäten) und *Structured Activities* (komplexe Abläufe von Aktivitäten) sind auch *Scopes* (gebündelte Aktivitäten) vorgesehen, die auch eine Fehlerbehandlung, eine Ereignisbehandlung, eine Terminationsbehandlung sowie eine Kompensationsbehandlung erlauben. Damit werden auch langandauernde Transaktionen ermöglicht.

Durch funktionale Aufspaltung und die Komposition von Web-Services ist ein hohes Maß an Flexibilität gewährleistet.

Mit den Erweiterungen *WS-BPEL4People* und *WS-HumanTask* lässt sich auch menschliche Interaktion in Geschäftsprozessen adressieren.

**WS-CDL**

*Web Services Choreography Description Language* (WS-CDL oder auch WS-Choreography) wird zur Choreografie von Web-Services eingesetzt. Die XML-basierte Sprache beschreibt die unmittelbare Kommunikation zwischen Web-Service-Akteuren aus der Beobachterperspektive, indem das Verhalten der Akteure definiert wird.

Dabei werden mit der Kommunikationsstruktur die nicht-funktionalen Eigenschaften eines Web-Service beschrieben. Das Ziel ist, ein globales Szenario zu beschreiben, dem die Akteure in ihrem Verhalten folgen, das aber keine zentrale Kontrollinstanz kennt.

Eine Choreografie definiert wiederverwendbare allgemeine Regeln, die den Nachrichtenaustausch zwischen Akteuren steuern, und die möglichen Muster kollaborativen Verhaltens, die zwischen zwei oder mehr zusammenwirkenden Teilnehmern vereinbart sind. Die Wiederverwendbarkeit der Vorschriften erlaubt die vereinfachte Komposition auch komplexer Choreografien.

**OSCI**

Online Services Computer Interface (OSCI) ist eine Protokollspezifikation für die öffentliche Verwaltung in Deutschland. Sie basiert auf bereits bestehenden Standards wie zum Beispiel den Sicherheitsstandards für XML (XML-Encryption und XML Signature), SOAP, SAML und einigen WS-*-Standards. Für die Anforderungen der öffentlichen Verwaltung wurden spezielle Erweiterungen definiert. Ziel ist die sichere, vertrauliche und rechtsverbindliche Übertragung elektronischer Daten über das Internet. Das Protokoll wird vom Bundesministerium des Inneren als obligatorischer Standard für elektronische Transaktionen mit der Bundesverwaltung gesetzt und ist die Basis für viele weitere Spezifikationen für *XML in der öffentlichen Verwaltung* (XÖV), zum Beispiel zur elektronischen Datenübermittlung im Meldewesen.

Außerhalb von E-Government-Anwendungen der öffentlichen Verwaltung hat OSCI praktisch keine Bedeutung.

Als wesentliche Anforderungen an die Kommunikation wurden fünf Sicherheitsaspekte identifiziert und umgesetzt: Authentizität, Integrität und Vertraulichkeit sowie Nichtabstreitbarkeit und Zurechenbarkeit. Dabei wurden auch Erfordernisse nach dem Signaturgesetz berücksichtigt. So ist es möglich, zwischen fortgeschrittener und qualifizierter elektronischer Signatur mit und ohne Anbieterakkreditierung gemäß Signaturgesetz zu wählen.

Mit der Version 2 des Standards wurde besonderes Gewicht auf die Anforderungen bei der Verwendung mit Web-Services gelegt. Die Erweiterung berücksichtigte dementsprechend vor allem international anerkannte WS-Standards.

# M 4.452 Überwachung eines Web-Service

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um den Sicherheitszustand eines Web-Service nachvollziehen zu können, ist es notwendig, diesen kontinuierlich zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die zu Sicherheitslücken führen können, zu erkennen.

Als Bestandteil des Sicherheitskonzeptes für einen Web-Service muss deshalb ein Überwachungskonzept entwickelt werden.

Komplexe Systeme wie Web-Services können in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Kontrolle muss automatisch durch entsprechende Systemkomponenten oder Produkte erfolgen. Die Überwachung eines Web-Service muss bei Veränderungen entsprechend angepasst werden.

Des Weiteren müssen in der Planung zur Überwachung eines Web-Service grundsätzlich alle relevanten Komponenten berücksichtigt werden. Daher sollten im Überwachungskonzept beispielsweise auch Datenbanken und Verzeichnisdienste, abhängige und genutzte Web-Services sowie die relevanten IT-Systeme enthalten sein. Dies ist von besonderer Bedeutung, wenn unterschiedliche Services über einen Enterprise Service Bus (ESB) miteinander verbunden sind.

**Überwachung von Verfügbarkeit und Leistung**

Wenn Dienste ausfallen, ihre Schnittstellen ändern oder ihr Antwortzeitverhalten verschlechtern, kann das weitreichende Folgen auf eine Vielzahl von abhängigen Systemen haben. Die Verfügbarkeit und Leistung von Web-Services müssen daher geeignet überwacht werden.

Neben der generellen Erreichbarkeit und Aktivität des Web-Service sowie der relevanten Schnittstellen-Dienste und Abhängigkeiten sollten daher auch Leistungsparameter überwacht werden. Hierzu gehören beispielsweise:

- Antwortzeiten von Anfragen,
- Anzahl der Anfragen beziehungsweise Anforderungen,
- Größe von Anforderungen und Antworten oder
- Füllstände von Speichern (zum Beispiel Speicher der JVM, Message-Queues).

Dadurch können zum einen Fehlkonfigurationen oder technisch bedingte Engpässe sowie zum anderen Denial-of-Service-Angriffe frühzeitig erkannt und zeitnah behandelt werden.

Insbesondere bei höheren Anforderungen an die Verfügbarkeit und bei der Verteilung eines Web-Service über mehrere Systeme sollte die Lastverteilung überwacht werden.

**Meldungen**

Des Weiteren sollten die Protokolldateien und Systemmeldungen (Notifications) hinsichtlich relevanter Meldungen kontinuierlich ausgewertet werden. Hierzu sollte ein am Schutzbedarf ausgerichtetes Log-Level im jeweiligen Web-Service konfiguriert werden (siehe auch M 4.397 *Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services*). Für die Überwachung können beispielsweise die folgenden Meldungen relevant sein:

- Fehler- oder Warnmeldungen,
- Meldungen zu Berechtigungsverstößen oder -änderungen (zum Beispiel Vergabe von Administratorberechtigungen),
- Meldungen zur Änderung von sicherheitsrelevanten Einstellungen,
- Meldungen zu ungültigen XML-Nachrichten oder
- Fehlermeldungen zur Inkonformität von Schnittstellen.

Meldungen mit einer höheren Kritikalität müssen zu einer Alarmierung eines verantwortlichen Mitarbeiters führen, um eine Reaktion in einem angemessenen Zeitraum sicherzustellen. Hierfür empfiehlt sich der Einsatz eines Alarmierungssystems.

**Überwachung von Policies**

In diesem Zusammenhang sollten auch die unterschiedlichen Meldungen zu Verstößen gegen die eingesetzten Policies (zum Beispiel WS-Policies, WS-SecurityPolicies) berücksichtigt werden. Diese könnten beispielsweise beinhalten:

- Verstöße gegen die vordefinierte Nachrichtengröße,
- Verstoß gegen die Verschlüsselungsanforderung an Nachrichten,
- Fehler in der Ver- oder Entschlüsselung von Nachrichteninhalten,
- Fehler in der Signatur von Nachrichteninhalten oder
- fehlerhafte Authentisierung.

**Überwachung der Verschlüsselung des Service**

Werden aufgrund höherer Vertraulichkeitsanforderungen Verschlüsselungsmaßnahmen eingesetzt (zum Beispiel TLS), sollten diese hinsichtlich ihrer Funktionalität überwacht werden. Gerade durch die automatisierte Funktion eines Web-Service besteht die Gefahr, dass Fehler in der Verschlüsselung nicht rechtzeitig bemerkt werden.

Ansatzpunkte für eine Überwachung der Verschlüsselung sind beispielsweise:

- Aktualität und Gültigkeit des Zertifikats des Web-Service,
- Aktualität und Gültigkeit der Zertifikate von anfragenden Diensten,
- Fehler- oder Warnmeldungen beim Aufbau von verschlüsselten Verbindungen (zum Beispiel Warnmeldungen bei veralteten SSL-Versionen)

**Auswertung durch Schwellwerte und Trends**

Um Bedrohungen und Schwachstellen rechtzeitig erkennen zu können, ist es erforderlich, Schwellwerte zu definieren sowie Trends aus den überwachten Werten abzuleiten, zum Beispiel für den belegten Speicherplatz, die Systemauslastung oder die genutzte Bandbreite. Anhand der Schwellwerte und jeweils kritischen Trendrichtungen sollten im Rahmen des Überwachungskonzepts Handlungsanweisungen definiert werden.

Prüffragen:

- Existiert ein Überwachungskonzept für Web-Services?
- Existiert eine angemessene Verfügbarkeits- und Leistungs-Überwachung?
- Werden Meldungen der Betriebssysteme und Dienste angemessen überwacht? Ist eine zeitnahe Reaktion auf kritische Meldungen sichergestellt?
- Werden die eingesetzten Policies hinsichtlich ihrer Einhaltung überwacht?
- Werden die Verschlüsselungsfunktionen angemessen überwacht?
- Wurden Schwellwerte und Trends definiert und mit Handlungsanweisungen untersetzt?

# M 4.453 Einsatz eines Security Token Service (STS)

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Security Token Service (STS) ist ein Web-Service, über den Identitäts- und Berechtigungsinformationen angefordert, erneuert und überprüft werden können. Das Prinzip ist das eines Claims-based (deutsch etwa *anspruchsbasierten*) Identitätsmodells, wobei ein Anspruch (*Claim*) eine Aussage einer Entität über eine andere Entität oder sich selbst bedeutet, etwa über einen Benutzernamen oder ein bestimmtes Recht. Ein STS kann genutzt werden, um die Authentisierung und Autorisierung auszulagern oder, wenn mehrere Anwendungen oder Dienste den STS nutzen, einen Single Sign-on zu realisieren. Grundsätzlich wird eine Entkopplung von Diensten und ihren Aufrufern vorgenommen, nach der ein Dienst nicht mehr jedem einzelnen Aufrufer hinsichtlich der übermittelten Identitätsinformationen direkt vertrauen muss, sondern lediglich einem STS. Der Aufrufer kann dabei ebenfalls ein Web-Service sein (Web-Service-Authentisierung), aber auch eine Client-Anwendung oder ein Browser (*passiver Client*), wobei in letzterem Fall der STS als Webanwendung auftritt (Web-SSO).

Eine Vereinfachung entsteht dadurch, dass nicht mehr jede Anwendung oder jeder Dienst die Authentisierung von Benutzern, die Verwaltung von Benutzerkonten und Kennwörtern, die Anbindung an Verzeichnisdienste und die Integration in weitere Identitäts- und Zugriffskontrollsysteme der Institution beherrschen muss. Naturgemäß hat dieser Architekturwechsel jedoch bedeutende Auswirkungen auf Sicherheitsfragen.

Da der STS selbst auch einen Web-Service darstellt, sind für ihn die Maßnahmen des Bausteins B 5.24 *Web-Services* ebenfalls umzusetzen. Diese Maßnahme umfasst im Folgenden zusätzlich die Aspekte der Nutzung eines STS durch einen anderen Web-Service, gegebenenfalls auch aus einer anderen Institution heraus.

In der Praxis ist häufig ein STS bereits gegeben. Wird ein nicht selbst betriebener STS genutzt, handelt es sich um ein Outsourcing von Authentisierungsfunktionen. Es sind daher auch die Maßgaben des Bausteins B 1.11 *Outsourcing* und gegebenenfalls des Bausteins B 1.17 *Cloud-Nutzung* zu beachten. Bei einer Individualvereinbarung mit dem STS-Anbieter sind vertragliche Regelungen derart zu treffen, dass der Schutz der durch die Zugriffskontrolle gesicherten Daten gewährleistet ist. Andernfalls sind die Vertragsbedingungen des Anbieters genau daraufhin zu prüfen, ob diese dem Schutzbedarf gerecht werden. Ob ein bestimmter STS für eine Anwendung verwendet werden darf, hängt vom Schutzbedarf der Anwendung und der Möglichkeit weiterer Maßnahmen ab, den Schutz der Zugriffskontrolle eventuell noch zu verstärken, zum Beispiel durch eine Zwei-Faktor-Authentisierung. Hier ist das Vertrauen in den Anbieter durch klare Kriterien und die Stichhaltigkeit ihrer Einhaltung zu begründen.

Aber auch, wenn der STS innerhalb der eigenen Institution betrieben wird, findet durch die Auslagerung der Authentisierung eine Vererbung des Schutzbedarfs auf den STS statt, der mit Kumulationseffekten einhergeht, wenn mehrere Anwendungen oder Dienste als Konsumenten auftreten.

Es ist davon auszugehen, dass ein STS seinen Schutzbedarf bezüglich Vertraulichkeit und Integrität nach dem Maximumprinzip von den Daten erbt, auf die durch seine Verwendung zugegriffen werden kann. Bezüglich der Verfügbarkeit ist das ebenfalls der Fall, wenn die Nutzung des STS die einzige effektiv nutzbare Möglichkeit der Authentisierung darstellt. Zusätzlich sind Kumulationseffekte zu berücksichtigen, falls der STS die Authentisierung für eine hohe Anzahl von Diensten oder institutionen übernimmt.

Hinzu kommt, dass am STS nicht nur die Information vorliegen muss, welcher Benutzer welche Ansprüche hat, sondern durch die Anfragen nach Tokens auch Daten anfallen, welcher Benutzer welchen Dienst wie oft und in welchem Kontext nutzt. Bei menschlichen Benutzern ist hier die Privatsphäre zu betrachten (etwa durch Beachtung von Baustein B 1.5 *Datenschutz*), bei maschinellen die Vertraulichkeit der Metadaten.

Die Realisierung eines STS ist mittels verschiedener Techniken (zum Beispiel REST) möglich, praktisch werden STS allerdings häufig mittels SOAP implementiert. Hierbei kommen im Allgemeinen Standards aus der WS-*-Familie zum Einsatz, um die Funktionalität und Interoperabilität zu gewährleisten.

Der Begriff des Security Tokens ist im Standard WS-Security definiert als jegliches Datenobjekt, das einen oder mehrere Claims, also verbürgte Aussagen über eine Entität, enthält und einer SOAP-Nachricht hinzugefügt werden kann. Häufig werden Security Tokens digital signiert, um die Aussagekraft kryptographisch nachzuweisen.

WS-Security unterstützt verschiedene Typen von Security Tokens, etwa das UsernameToken für die Authentisierung mittels Benutzername und Passwort. Das Passwort wird dabei als Hashwert übertragen, in dessen Berechnung eine Nonce (Zufallswert) und ein Zeitstempel einfließen, um Replay-Angriffe zu verhindern. Ein anderer vorgesehener Tokentyp ist das BinarySecurityToken für nicht XML-basierte Formate wie etwa X.509-Zertifikate. Weitere Tokentypen sind über einen Erweiterungsmechanismus vorgesehen.

Die meisten STS nutzen heute Token, die in der *Security Assertion Markup Language* (SAML) beschrieben werden. Dabei handelt es sich um einen verbreiteten Standard zur Beschreibung von Claims. Ein SAML Security Token (genauer eine *SAML Assertion*; die Spezifikation enthält außerdem noch weitere Elemente, die jedoch vor allem für Web-SSO benötigt werden) ist eine Beschreibung von Identitätsinformationen, Attributen, Authentisierungs- und Autorisierungsentscheidungen in XML, welche für eigene Zwecke erweiterbar ist.

Der SAML-Standard hat sich von Version 1.1 zu Version 2.0 bedeutend erweitert und umfasst nun weitere Protokolle und Einsatzszenarien (*Profiles*), welche sich vor allem um Web-SSO drehen. In jedem Fall ist eine grundlegende Entscheidung für einen in ausgereiften und in interoperablen Implementationen vorliegenden Satz von Standards zu treffen, die miteinander und mit den geplanten Kommunikationspartnern kompatibel sind und den jeweiligen Sicherheitsanforderungen gerecht werden.

In der Spezifikation WS-Trust, welche auf WS-Security aufbaut, wird der STS selbst mit seinen Aktionen definiert. Wenn ein Server eine Authentisierung verlangt, schickt der Client einen *Request for Security Token* (RST), zum Beispiel mit seinem Benutzernamen und Passwort in Form eines UsernameToken, an den STS. Hierin kann spezifiziert werden, welcher Tokentyp benötigt wird, welche Claims im Token enthalten sein sollen und wie das auszustel-

lende Token zu sichern ist. Der STS liefert eine *Request for Security Token Response* (RSTR) zurück, die das Security Token enthält, welches der Client nun dem Server präsentieren kann. Dieser kann es je nach Szenario entweder anhand der Signatur selbst überprüfen oder wiederum dem STS zur Überprüfung vorlegen.

Damit Sicherheitstoken als vertrauenswürdig gelten können, sollten sie entweder verifizierbar signiert sein, oder die Übertragung muss auf anderem Weg durchgängig abgesichert sein, etwa auf Transportebene. Da die Signatur eines STS allerdings auch der Bestätigung der Claims in einem Security Token dient, müsste ihr Fehlen durch andere Maßnahmen wie etwa eine sichere Authentisierung während des Austauschs ausgeglichen werden.

Vertrauliche Daten wie etwa Passwörter dürfen nie ungesichert zu einem STS oder von diesem zum Konsumenten übertragen werden. Hier ist immer ein sicheres Hash-Verfahren mit Zufallskomponente (Salt, zum Beispiel mit Nonce) einzusetzen. Zusätzlich sind Replay-Angriffe durch geeignete Methoden, etwa den Einsatz von Zeitstempeln, zu verhindern, falls der Transportkanal diese nicht schon zuverlässig unterbindet.

Wenn das Security Token nicht den direkten, verschlüsselten Weg vom STS zum Server nimmt, muss auch dessen Inhalt durch Verschlüsselung geschützt werden, um zu verhindern, dass unbefugte Dritte das Token zur Authentisierung einsetzen können. Hierfür reicht es, den kryptographischen Teil, also die Signatur des STS, zu verschlüsseln. Enthält die Assertion jedoch weitere vertrauliche Daten, sind auch diese zu schützen. Grundsätzlich ist aber die benötigte Vertraulichkeit durch das Prinzip der Datensparsamkeit zu minimieren, indem immer nach möglichst allgemeinen Claims (zum Beispiel "Benutzer ist volljährig") gefragt wird.

Als weitere Schutzmaßnahme ist eine kurzfristige Lebensdauer für Token je nach Schutzbedarf anzusetzen, um den Schaden bei missbräuchlicher Verwendung zu verringern. Die meisten Frameworks geben hier Standards vor, die nach Möglichkeit verkürzt werden sollten.

Durch die vielen ineinander spielenden Standards samt ihrer verschiedenen Versionen und Standardisierungsgrade haben in der Vergangenheit Implementierungen häufig Schwachstellen aufgewiesen, die die Sicherheit erheblich beeinträchtigt oder sogar ausgehebelt haben. Da es sich bei den zugrundeliegenden Sicherheitsfunktionen um XML-Encryption, XML-Signaturen sowie häufig TLS/SSL handelt, spielen entsprechende Angriffe auch hier eine Rolle, was umso schwerer wiegt, je mehr kritische Autorisierungsentscheidungen von dem STS getroffen werden.

Angriffe wie XML Signature Wrapping, also die böswillige Änderung einer Nachricht, ohne dass die Signatur ungültig wird, werden vor allem dadurch möglich, dass die Erzeugung und Prüfung von Signaturen nicht aufeinander abgestimmt sind. Hier sollten entweder dieselbe Softwarebasis zum Einsatz kommen, oder, wenn dies nicht möglich ist (zum Beispiel externe STS, XML-Gateways), ausgiebige Tests der Schnittstellen nach jeder Anpassung stattfinden. Grundsätzlich sind etablierte, gut getestete Bibliotheken und Frameworks zur Realisierung der STS-Funktionalität auszuwählen, zu denen Informationen über Schwachstellen und Sicherheitspatches zeitnah bereitstehen und eingespielt werden müssen. Bei der Absicherung der Kommunikationswege ist Maßnahme M 4.450 *Absicherung der Kommunikation bei Web-Services* zu beachten.

In jedem Fall ist bei der Komplexität der Materie unbedingt Sachverstand bezüglich des sicheren Einsatzes eines STS bereits während der Konzeptionsphase hinzuzuziehen.

Prüffragen:

- Wurde auch der STS selbst als Web-Service modelliert und entsprechend angemessene Maßnahmen aus dem Baustein B 5.24 *Web-Services* umgesetzt?
- Wurden bei Nutzung eines fremden STS die Maßnahmen des Bausteins B 1.11 *Outsourcing* und B 1.17 *Cloud-Nutzung* beachtet?
- Wurde die SSL/TLS Konfiguration vor der Freigabe zur Nutzung auf Fehler geprüft und wird der Status in periodischen Abständen validiert?
- Entsprechen die vertraglichen Regelungen mit dem STS-Betreiber dem Schutzbedarf der über den STS zugänglichen Daten und Anwendungen?
- Wurde die Vertraulichkeit der am STS anfallenden Daten betrachtet?
- Wird die Datensparsamkeit durch möglichst allgemeine Claims konsequent durchgesetzt?
- Wurden ausgereifte Bibliotheken und Frameworks für die Nutzung der STS-Funktionalität ausgewählt, für die auch aktuelle Informationen über Schwachstellen und Sicherheitspatches verfügbar sind?
- Werden entweder Token signiert oder der Transportkanal durchgängig verschlüsselt und authentisiert?
- Werden alle Passwörter nur als Hashwert übertragen mit Schutz gegen Brute-Force- und gegen Replay-Angriffe?
- Wurde die Lebensdauer für Security Token möglichst niedrig gewählt?

# M 4.454 Schutz vor unerlaubter Nutzung von Web-Services

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Um zu gewährleisten, dass Web-Services nur von berechtigten Parteien genutzt werden dürfen, ist es erforderlich, konkrete Anforderungen an die Authentisierung und Autorisierung einzelner Benutzer oder Clients zu stellen. Diese Anforderungen müssen im Rahmen eines sorgfältig gewählten Authentisierungs- und Autorisierungsmodells durch einen oder eine Kombination mehrerer verfügbarer WS-Standards realisiert werden. Dies gewährleistet die Einschränkung und Kontrolle einzelner Zugriffe auf den Web-Service. Welche Web-Service-Standards für die Umsetzung einer geeigneten Authentisierung und Autorisierung eingesetzt werden können, ist näher in den Maßnahmen M 4.456 *Authentisierung bei Web-Services* und M 4.455 *Autorisierung bei Web-Services* beschrieben.

Um Angriffe auf einen Web-Service zu erschweren, die im schlimmsten Fall zu einer Umgehung des Berechtigungssystems führen und somit unberechtigten Zugriff auf vertrauliche Daten oder schützenswerte Funktionen ermöglichen, sollten zusätzliche Maßnahmen gegen Brute-Force-Angriffe oder andere automatisierte Angriffe auf Web-Services ergriffen werden. Automatisierte Angriffe zeichnen sich durch eine hohe Zahl an Zugriffsversuchen innerhalb einer kurzen Zeitspanne aus. Hoch frequentierte Anfragen (zum Beispiel zum Erraten von Passwörtern) sollten durch festgelegte Schwellwerte erkannt werden und zu geeigneten Reaktionen führen (Alarmierung von Verantwortlichen, Sperrung des Zugangs). Solche Schwellwerte können sich zum Beispiel auf die Anzahl der Zugriffe, Fehlanmeldungen, die übertragene Datenmenge oder die Größe der übertragenen XML-Nachrichten beziehen. Im Falle eines erkannten Angriffsversuches kann eine temporäre Sperrung des Zugangs erfolgen. Eine Alternative zur Sperrung des Zugangs ist die inkrementelle Verzögerung von Antworten (das heißt eine bei jedem Fehlversuch ansteigende Wartezeit), die automatisierte Angriffe effektiv ausbremst.

Bei der Festlegung von Schwellwerten ist darauf zu achten, dass legitime Dienstnutzer (Clients und ihre Benutzer, andere Web-Services) nicht in der Funktionalität und der Bedienung des Web-Service eingeschränkt werden.

Grundsätzlich sollte immer sichergestellt werden, dass nur berechtigte Systeme oder Benutzer auf den Web-Service zugreifen dürfen. Durch eine Firewall kann sichergestellt werden, dass nur berechtigte IP-Adressen oder IP-Adressblöcke auf den Web-Service zugreifen können. In geschlossenen Umgebungen bietet sich dieser Whitelisting-Ansatz an. Wird ein Web-Service betrieben, der aus dem Internet erreichbar sein soll (zum Beispiel APIs zur freien Nutzung durch Dritte), empfiehlt sich ein Blacklisting-Ansatz. Durch die Sperrung bekannter IP-Adressen, die zum Beispiel Spam-Servern zugeordnet werden können, kann sichergestellt werden, dass Zugriffe von Systemen ausgeschlossen werden, die als bösartig angesehen werden müssen. Auch unberechtigte Zugriffe aus bestimmten Regionen oder Ländern können durch solche Sperrlisten verhindert werden. Alternativ kann die Sperrung von IP-Adressblöcken auch direkt beim Provider veranlasst werden. Durch eine entsprechende Konfiguration der Firewall kann auch sichergestellt werden, dass auffällig häufige Aufrufe aus einem IP-Adressbereich oder von einer einzelnen IP-Adresse be-

grenzt werden, um so einem potenziellen Denial-of-Service-Angriff entgegenzuwirken.

Eine weitere Möglichkeit, den Zugriff auf einen Web-Service nur für berechtigte Benutzer einzuschränken, bietet der Einsatz eines VPNs. Durch ein Standort-zu-Standort-VPN kann beispielsweise sichergestellt werden, dass nur ein ausgewählter Kreis von Geschäftspartnern unter Wahrung der Vertraulichkeit und Integrität auf den Web-Service zugreifen darf. Weitere Hinweise zum Einsatz eines VPNs finden sich im Baustein B 4.4 *VPN*. Ein VPN trägt zum Schutz des Web-Service bei, da keine externen Brute-Force-Angriffe auf den Web-Service durchführbar sind, wenn dieser nur aus einem internen Netz erreichbar und somit nicht im Internet exponiert ist.

Web-Services sind oft darauf ausgelegt, dass diese sowohl intern als auch extern (zum Beispiel durch Geschäftspartner) aufgerufen werden können, wobei jeweils ein Zugriff auf unterschiedliche Funktionen erfolgen kann. Externe Benutzer dürfen zum Beispiel nur in der Lage sein, eine Bestellung aufzugeben, während die internen Benutzer auch die Möglichkeit haben sollten, die eingegangenen Bestellungen zu verwalten und zu bearbeiten. Oft werden diese unterschiedlichen Funktionen über ein und denselben Web-Service-Endpunkt angeboten. Dadurch, dass allerdings alle Funktionen über den selben Endpunkt aufrufbar sind, kann ein externer Angreifer durch Auslesen der WSDL-Datei oder andere Verfahren der Informationsgewinnung Aufrufpunkte der internen Funktionen ermitteln, um Daten zu manipulieren oder auszulesen. Aus diesem Grund sollte bei der Realisierung des Web-Service darauf geachtet werden, dass die Bereitstellung von Funktionen für interne und externe Aufrufer nicht auf dem selben Endpunkt erfolgt. Idealerweise befinden sich die unterschiedlichen Web-Service-Endpunkte auf unterschiedlichen Systemen. Durch die Trennung der zugehörigen URLs kann dann auch eine feingranulare Kontrolle auf den Web-Service durch eine Firewall erzielt werden, da der Web-Service durch unterschiedliche URLs und Ports, oder sogar nur aus bestimmten Netzen aufrufbar ist.

Sofern nicht gewollt ist, dass auf bestimmte Operationen zugegriffen werden kann, kann auch die Beschreibung der XML-Struktur (Schema) für den Dienstaufruf derart modifiziert werden, dass die unerwünschten Operationen entfernt werden. Sofern eine Anfrage gestellt wird, die eine aus dem Schema entfernte Operation enthält, wird diese im Rahmen der Validierung der XML-Anfrage gegen das Schema als nicht valide identifiziert und entsprechend abgelehnt.

Die Zugriffsbeschränkung auf einen Web-Service über Authentisierung und Autorisierung der Dienstnutzer kann sich als wirkungslos erweisen, wenn der Angriff seinen Effekt zeigt, bevor die Mechanismen der Zugriffskontrolle zur Geltung kommen. Aus diesem Grund muss im Vorfeld eine adäquate Validierung der gesamten Nachricht erfolgen, bevor der Web-Service diese weiter verarbeiten darf. Dieser Prozess wird auch als Schemavalidierung bezeichnet. Durch die Schemavalidierung wird sichergestellt, dass Nachrichten und Angriffe abgewehrt werden, die vom definierten Schema abweichen. Dies bedeutet, dass das Schema so restriktiv wie möglich zu gestalten ist, das heißt nur eine begrenzte Menge an XML-Formaten zur Nutzung des Dienstes verfügbar sein darf. Bei der Schemavalidierung ist es daher notwendig, das Schema so einzuschränken, dass Nachrichten mit bekannten Angriffsmustern ausgeschlossen werden. Zusätzlich ist es notwendig, die Nachricht auf bestimmte Zeichenfolgen zu untersuchen, die eventuell für Injection-Angriffe genutzt werden können (siehe G 5.174 *Injection-Angriffe*).

Weiter müssen die Schemata eines Web-Service so angepasst werden, dass nur Nachrichten bis zu einer bestimmten Größe verarbeitet werden können. Die Verarbeitung einer übergroßen Nachricht kann die Ressourcen des verarbeitenden Systems auslasten und somit zu Leistungseinbußen oder Ausfällen führen. Bei der Beschränkung der Nachrichtengröße ist darauf zu achten, dass keine unbeschränkten Nachrichtenteile verarbeitet werden dürfen, die folgende Merkmale besitzen:

- xsd:any,
- xsd:anyType,
- xsd:anySimpleType,
- rekursive Definition von Elementen oder Typen,
- unbeschränkte Listen.

Die Validierung eines Schemas kann entweder bereits an einem XML-Gateway oder direkt auf dem System erfolgen, welches den Web-Service bereitstellt. Die Entscheidung, an welcher Stelle die Validierung erfolgen soll, ist bereits während der Planungsphase zu treffen, da dies auch Auswirkungen auf die Gesamtarchitektur haben kann.

Prüffragen:

- Wurden geeignete Standards für die Authentisierung und Autorisierung gewählt und umgesetzt?
- Sind Maßnahmen umgesetzt, die automatisierte Angriffe erkennen und abwehren können, zum Beispiel durch die Überwachung von Schwellwerten für Anfragen?
- Ist darüber hinaus sichergestellt, dass nur berechtigte Teilnehmer auf den Web-Service zugreifen dürfen?
- Erfolgt eine Trennung zwischen internen und externen Operationen und ist sichergestellt, dass nur die jeweiligen Benutzer die für sie benötigten Operationen aufrufen dürfen?
- Wurde das XML-Schema entsprechend restriktiv aufgebaut, und wird die Einhaltung des Schemas überprüft?

# M 4.455 Autorisierung bei Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

### Autorisierung

Während Authentisierung das Ziel hat, eine behauptete Identität zu verifizieren, bezweckt die Autorisierung die Überprüfung, ob eine zuvor authentisierte Entität befugt ist, auf bestimmte Ressourcen zuzugreifen. Beide Begriffe ergänzen sich also zu den Bestandteilen von Identitäts- und Zugriffsmanagement (englisch Identity and Access Management, IAM), und vor jeder Autorisierung muss entsprechend eine Authentisierung erfolgt sein. Das wichtigste Prinzip der Autorisierung ist, dass bei jedem Zugriff auf eine Ressource geprüft werden muss, ob die Berechtigungen der anfragenden Entität diesen erlauben - und zwar bei jeder Aktion, sprich im Fall von Web-Services jeder einzelnen Anfrage.

### Rollen und Rechte

**Rollen-und- Rechte-Modell**

Die Zuordnung und Verwaltung von Einzelberechtigungen zu jedem einzelnen Benutzer ist bei komplexeren Anwendungen nicht sinnvoll umsetzbar. Daher muss ein geeignetes Rollenmodell entwickelt werden, bei dem den Benutzern jeweils ihren Aufgaben entsprechende Rollen zugewiesen werden können, über die sie die erforderlichen Berechtigungen erhalten.

### Besondere Herausforderungen bei Web-Services

Bei Web-Services und insbesondere bei Serviceorientierten Architekturen (SOA) gibt es im Gegensatz zu monolithischen Anwendungen nicht nur einen, sondern mehrere Punkte, an denen diese Überprüfung stattfinden muss, denn die Durchsetzung von Zugriffsregeln (Policies) hat am Zugriffspunkt zu jedem Dienst stattzufinden. Diese Überprüfungspunkte werden auch als Policy Enforcement Points (PEP) bezeichnet. Sowohl die Planung als auch die praktische Administration solcher Regelwerke ist eine komplexe Herausforderung und sollte in einem zentralen Tool durchführbar sein.

Die Autorisierungsprüfinstanz muss in der Lage sein, Web-Service-Nachrichten zu lesen. Oft werden solche Prüfungsinstanzen auch selbst als Web-Service realisiert und nutzen Web-Service-Standards für die Abbildung von Rollen und Rechten.

### Organisationsübergänge

Besondere Herausforderungen stellen sich, wenn die Web-Service-Nutzung Organisationsgrenzen überschreitet. Dann müssen Konzepte gefunden und Regelungen getroffen werden, wie mit Autorisierungsentscheidungen bei Anfragen aus und an andere Organisationen umgegangen wird. Entsprechende Vertrauensbeziehungen sollten immer durch formale Regelungen und Rechtemodelle konkretisiert werden.

### Schichten

Da moderne Anwendungen und damit auch Web-Services typischerweise in mehreren Schichten (mindestens zwei, besser drei, etwa Präsentation, Geschäftslogik und Datenhaltung) aufgebaut sind, stellt sich die Frage nach der

Autorisierung nicht nur einmal, beim Zugriff auf die Präsentationsschicht, sondern darüber hinaus auch beim Zugriff jeder Schicht auf die jeweils darunter liegende.

Eine weitere, darüber liegende Schicht können in einer SOA Verzeichnisse (*Repositories*) bilden, also Datenbanken, die Informationen über Dienste etwa nach dem Standard UDDI bereitstellen.

**Minimale Rechte**

Grundsätzlich ist auf jeder Schicht das Prinzip *Zugriff nur soweit erforderlich* (englisch *Least Privilege*) einzuhalten: Es dürfen immer nur so viele Rechte vergeben werden, wie im aktuellen Kontext zur Durchführung der fachlichen Aufgabe benötigt werden. Dies impliziert insbesondere, dass administrative Rechte nur von besonderen Benutzern und nur zum Zweck der Administration ausgeübt werden dürfen. Das Prinzip der minimalen Berechtigungen gilt auch für den Zugriff auf Repositories, falls diese nicht komplett öffentlich sind.

Der Grundsatz der minimalen Berechtigungen gilt ebenso für die Systemberechtigungen, mit denen die Prozesse von Applikationsserver, Datenbank, XML-Firewall und anderen Komponenten laufen.

**Öffentlich zugängliche Web-Services**

Insbesondere wenn Web-Services großen, möglicherweise anonymen Benutzerschichten angeboten werden (etwa als Dienst im Internet), ist mit zufälligen und systematischen Angriffen auf die Autorisierung auf allen Schichten zu rechnen. Hier sind besondere architektonische Maßnahmen zu treffen.

Von außen erreichbare Schnittstellen sollten dabei in ein isoliertes Grenznetz (DMZ) verlagert und von internen Diensten und Datenbeständen getrennt werden. Ebenfalls in der DMZ angesiedelt werden kann ein ergänzender Security-Service, der alle Anfragen an den Web-Service zuerst überprüft. Dabei kann er auch die Authentisierung und Autorisierung der Anfragen übernehmen, etwa mithilfe des Zugriffs auf einen Verzeichnisdienst im internen Netz. Die eigentlichen Daten befinden sich auf einem Anwendungsserver, ebenfalls im internen Netz, zu welchem der Web-Service nur bestimmte Anfragen erlaubt.

**Sicherheitsgateways**

Da Web-Service-Kommunikation sich häufig zwischen verschiedenen Netzbereichen vollzieht, spielen klassische Firewallkonzepte zur sicheren Trennung der Netze eine große Rolle. Hier kommt allerdings die Tatsache hinzu, dass innerhalb von SOAP-Nachrichten beliebige Daten, Befehle und Dateien (als Anhänge) verschickt werden können, auf die eine Firewall, die lediglich auf Adress- und Portebene filtert, nicht gezielt reagieren kann.

Dem Zweck angemessene Web-Service-Firewalls müssen als Application Level Gateways (ALG) ausgeführt sein. Sie werden in diesem Fall häufig auch als XML-Firewall oder XML-Security-Gateway bezeichnet. Solche Systeme können XML filtern, parsen, auf Schadsoftware prüfen und SOAP-Nachrichten untersuchen, um beispielsweise bestimmte Aktionen oder Akteure zu blockieren.

Auch für die Autorisierung kann eine XML-Firewall genutzt werden. In diesem Fall trifft sie die Entscheidung, ob ein authentisierter Benutzer berechtigt ist, eine bestimmte Aktion auszuführen, indem das in der Nachricht enthaltene Security Token untersucht, ausgewertet und kryptographisch überprüft wird.

**Standards**

Bestehende IT-Systeme verfügen häufig über proprietäre Zugriffsmechanismen. Informationen über Entitäten und Attribute werden in der Regel in Zugriffslisten (Access Control Lists, ACL) gespeichert, die sehr unterschiedlich aussehen können. Dadurch werden ein Austausch und eine gemeinsame Nutzung über verschiedene Systeme hinweg unnötig erschwert. Im Bereich der Web-Services, wo bereits Schnittstellen, Datenmodelle und Authentisierungsmethoden homogenisiert sind, sollten deshalb einschlägige Standards auch für die Zugriffskontrolle umgesetzt werden.

Im Gegensatz zu anderen spezifischen Themen ist Autorisierung allerdings bisher nicht in einen dedizierten Standard der WS-*-Familie gemündet: Der Standard WS-Authorization wurde bis Anfang 2014 nicht veröffentlicht. Stattdessen gibt es verschiedene XML-Standards, die sich teilweise überschneiden, teilweise ergänzen und jeweils das Thema Autorisierung mit einem bestimmten Fokus in Angriff nehmen.

In SAML (Security Assertion Markup Language), einem standardisierten XML-Framework für die Beschreibung und Abfrage von Authentisierungs-, Autorisierungs- und Attributinformationen einer Entität, zum Beispiel über SOAP, lassen sich in sogenannten Assertions (Zusicherungen) unter anderem Autorisierungsentscheidungen kodieren und austauschen.

XACML (eXtensible Access Control Markup Language) auf der anderen Seite stellt eine Sprache dar, die XML-basiert beschreibt, wie Regeln und dazugehörige Anfragen und Antworten zu gestalten sind, um eine kontext- oder attributbasierte Autorisierung der Zugriffskontrolle auf Ressourcen zu ermöglichen. Neben dem einfachen Gewähren oder Verwehren von Aktionen gibt es hier die Möglichkeit, vor oder nach der Autorisierungsentscheidung bestimmte weitere Aktionen zu erzwingen. XACML hat seine Stärken vor allem in der feingranularen Beschreibung und Übertragung von Zugriffsrechten.

XACML und SAML überschneiden sich zwar teilweise als Standards für Authentisierung und Autorisierung, ergänzen sich aber aufgrund des unterschiedlichen Fokus auch und werden daher häufig in Kombination eingesetzt. Während SAML allgemein die Authentisierung sowie die Übertragung von Authentisierungs- und Autorisierungsentscheidungen zwischen Entitäten ermöglicht, deckt XACML vor allem die Autorisierungsentscheidungen selbst ab, also wie diese im PEP verarbeitet werden.

**Gestaffelte Verteidigung**

Insbesondere, wenn Daten oder Operationen höheren Schutzbedarf tragen, sollte die Autorisierung nicht nur an einer Stelle geprüft werden, sondern eine gestaffelte Verteidigung (Defense in Depth) stattfinden. So kann ein Sicherheits-Gateway bereits die Autorisierung einer Anfrage überprüfen und der Dienst selbst vor der Ausführung noch einmal, um mögliche Fehlkonfigurationen oder Software-Schwachstellen des Gateways abzufangen.

Schließlich sollte im Fehlerfall immer auf eine sichere Entscheidung zurückgefallen werden (Fail Securely): Geht es um Vertraulichkeit oder Integrität, muss bei fehlgeschlagener Autorisierung der Zugriff verweigert werden. Nur im Fall, dass die Verfügbarkeitsanforderungen die übrigen Sicherheitsanforderungen deutlich überwiegen, darf im Fehlerfall eine Erlaubnis des Zugriffs erfolgen. Eine solche Entscheidung muss jedoch in jedem Fall in einer Risikoanalyse dokumentiert werden.

Prüffragen:

- Wurde ein geeignetes Rollen-und-Rechte-Modell entwickelt?
- Werden bei jedem einzelnen Zugriff auf jede Ressource immer wieder die Zugriffsrechte überprüft?
- Existiert bei einer SOA ein zentrales Tool für die Verwaltung von Rollen und Rechten?
- Wird das Prinzip der minimalen Berechtigungen konsequent durchgehalten, insbesondere auch für administrative Zugriffe und die Dienstkonten der beteiligten Software?
- Kommt bei öffentlich erreichbaren Web-Services eine sichere Architektur zum Einsatz, zum Beispiel in Form einer DMZ mit Security-Service oder XML-Security-Gateway?
- Fällt bei fehlgeschlagener Autorisierung das System auf einen sicheren Zustand entsprechend des Schutzbedarfs zurück?

# M 4.456 Authentisierung bei Web-Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Um den Zugriff auf einen Web-Service auf einen berechtigten Personenkreis einzugrenzen oder unterschiedliche Berechtigungen innerhalb eines Web-Service zu realisieren (vergleiche M 4.455 *Autorisierung bei Web-Services*) ist es notwendig, die Benutzer, die auf den Dienst zugreifen, eindeutig zu identifizieren und zu authentisieren. Umgekehrt muss der Benutzer eines Web-Service sicherstellen können, dass er tatsächlich mit dem gewünschten Dienst kommuniziert.

Die Authentisierung muss dabei erfolgen, bevor schützenswerte Informationen übertragen werden. Dies bedeutet, dass der Benutzer eines Web-Service sicherstellen muss, dass er tatsächlich mit dem gewünschten Web-Service kommuniziert, bevor er eine Anfrage mit vertraulichen Informationen an den Dienst sendet. Umgekehrt muss ein Web-Service die Identität des anfragenden Benutzers oder Web-Services prüfen, bevor er vertrauliche Informationen an diesen zurücksendet oder dem Benutzer Berechtigungen zum Aufruf von Funktionen erteilt (siehe M 4.455 *Autorisierung bei Web-Services*).

Die Authentisierung von Kommunikationspartnern kann auf unterschiedlichen Ebenen umgesetzt werden. Eine Möglichkeit ist etwa die Authentisierung auf Transportebene mittels SSL-/TLS. Dies wird häufig auch als *Transport Layer Authentication* bezeichnet. Eine andere Möglichkeit ist die Authentisierung auf Nachrichtenebene, zum Beispiel mittels der Mechanismen aus den WS-Security-Standards. Sollen nicht nur einzelne Nachrichten, sondern ein komplexerer Nachrichtenaustausch authentisiert werden, so empfiehlt es sich, ein entsprechendes Session-Management einzuführen (vergleiche M 4.394 *Session-Management bei Webanwendungen und Web-Services*).

**Identitätsmanagement**

Um die Benutzer von Web-Services zu authentisieren, ist es notwendig, Benutzerdaten zu erfassen und die zugehörigen Identifikationsmerkmale zu hinterlegen. Diese Vorgänge sind Teil des sogenannten Identitätsmanagements (engl. *Identity Management*).

Der klassische Anwendungsfall ist dabei, dass jeder Anbieter eines Web-Service seine eigene Benutzerverwaltung betreibt und die Authentisierung selbst vornimmt. Hierbei spricht man von isoliertem Identitätsmanagement. Bei diesem Modell kommuniziert der Benutzer ausschließlich mit dem gewünschten Web-Service. Bei der Nutzung weiterer Web-Services muss seine Identität dort jeweils eigenständig verwaltet werden.

Kommen Web-Services in service-orientierten Architekturen (SOA) zum Einsatz, so handelt es sich zumeist um komplexe Systeme, die oft nicht mehr der Kontrolle einer einzelnen Institution unterliegen. Es ist dann meistens nicht mehr möglich, die Identitäten durch die Betreiber der einzelnen Dienste verwalten zu lassen. Diese Aufgabe wird stattdessen von spezialisierten Organisationen oder Organisationseinheiten, den Identitätsanbietern (engl. *Identity Providers*) übernommen.

Beim zentralisierten Identitätsmanagement existiert ein solcher Identitätsanbieter, der das Identitätsmanagement für eine Vielzahl an Dienstanbietern übernimmt. Beispiele für diese Art von Identitätsmanagement sind Dienste von Anbietern wie Microsoft, Facebook oder Google, oder aber der Einsatz eines zentralen Authentisierungssystems innerhalb eines Unternehmens. Zentralisierte Identitätsmanagementsysteme bieten oftmals Single-Sign-On-Funktionalität: Der Benutzer muss sich lediglich gegenüber einem Identitätsanbieter authentisieren, um die Dienste verschiedener Dienstanbieter in Anspruch zu nehmen.

Die dritte Variante des Identitätsmanagements ist das föderierte Identitätsmanagement (engl. *Federated Identity Management*). In dieser Variante existieren mehrere Identitätsanbieter. Die Authentisierung der Benutzer erfolgt über standardisierte Schnittstellen und Protokolle. Für Web-Services ist hier vor allem die Spezifikation *WS-Federation* von Bedeutung. Konkrete Technologien, die zur Umsetzung dieser Spezifikation verwendet werden können, sind die *Security Assertion Markup Language* (SAML) und *OpenID*.

**Art der eingesetzten Indikatoren**

Die Authentisierung der Teilnehmer an einer Web-Service-Kommunikation erfolgt über den Nachweis von eindeutig einer Identität zuzuordnenden Merkmalen, sogenannten Identifikatoren. Übliche Identifikatoren sind dabei Benutzernamen mit Passwörtern, Zertifikate und Signaturen, sowie kryptographisch gesicherte Datensätze (Token) eines Identitätsanbieters oder eines Security-Token-Services, wie er im Rahmen von *WS-Trust* spezifiziert ist (vergleiche M 4.453 *Einsatz eines Security Token Service (STS)*). Verschiedene Authentisierungsverfahren sind im Folgenden dargestellt. Für den Web-Service muss hier ein Verfahren ausgewählt werden, dessen Sicherheit dem Schutzbedarf gerecht wird.

Ein Beispiel für eine sehr einfache Authentisierung mit Hilfe von Benutzernamen und Passwörtern ist der Einsatz von HTTP Basic Authentication. Diese lässt sich sowohl für Web-Services auf Basis von REST als auch für SOAP-basierte Web-Services verwenden, bietet allerdings nur ein geringes Maß an Schutz der Authentisierungsdaten und muss daher durch zusätzliche Sicherheitsmaßnahmen wie etwa eine Transportverschlüsselung ergänzt werden. Ein weiteres Beispiel ist die Verwendung eines *Username Tokens* beim Einsatz von WS-Security.

Besseren Schutz bieten verschiedene Möglichkeiten, um Web-Service-Nachrichten mittels Zertifikaten und Signaturen zu authentisieren. Zumeist kommen XML-Signaturen gemäß der XMLDSIG-Spezifikation zum Einsatz. Einer der Vorteile des Einsatzes von Signaturen zur Authentisierung ist, dass die Authentisierung auf Nachrichtenebene stattfindet. Dadurch kann gegebenenfalls auf eine Sitzungsverwaltung (Session Management) verzichtet werden, da jede Nachricht einzeln durch eine Signatur authentisiert werden kann. Der Nachteil dieser Vorgehensweise sind Leistungseinbußen durch die Erzeugung, Übertragung und Verifikation einer Signatur für jede einzelne Nachricht. Darüber hinaus erfordert der Einsatz von Signaturen die Nutzung einer Public Key Infrastruktur (PKI).

Bei XML-Signaturen muss sichergestellt werden, dass sich die Signatur tatsächlich auf die vom Dienst zu verarbeitenden Daten bezieht. Ist dies nicht der Fall, werden so genannte *XML Signature Wrapping*-Angriffe möglich (siehe G 5.183 *Angriffe auf XML*). Bei diesem Angriff werden gültige, signierte XML-Daten in ein von einem Angreifer manipuliertes XML-Dokument eingebettet.

Wenn nun die Funktionen zur Verifikation der Signatur und die eigentliche Anwendungslogik die XML-Daten auf unterschiedliche Art und Weise verarbeiten, kann eine Situation entstehen, bei der die Signatur für die ursprünglichen eingebetteten Daten überprüft wird, auf Anwendungsebene aber die manipulierten Daten verarbeitet werden.

Eine weitere Möglichkeit zur Authentisierung der Teilnehmer einer Web-Service-Kommunikation ist die Authentisierung mittels Token, die von vertrauenswürdigen Dritten ausgestellt wurden. Als Token wird hierbei eine Datenstruktur bezeichnet, die die Identität des Tokeninhabers bestätigt. Die Integrität und Authentizität des Tokens selbst muss wiederum durch kryptografische Maßnahmen sichergestellt werden. Beispiele für häufig im Rahmen von Web-Service-Kommunikation eingesetzte Token sind SAML oder OAuth-Token.

Beim Zugriff von Benutzern auf Web-Services mit erhöhtem Schutzbedarf kann es erforderlich sein, eine starke Authentisierung unter Verwendung mehrerer Authentisierungsmerkmale (zum Beispiel der Besitz einer Chipkarte und die Kenntnis der dazugehörigen PIN) zu realisieren. Werden für eine solche Mehrfaktorauthentisierung voneinander unabhängige Authentisierungsmerkmale verwendet, so wird die Wahrscheinlichkeit, dass ein Angreifer alle erforderlichen Merkmale unter seine Kontrolle bekommt, stark verringert.

Werden kryptografische Algorithmen zur Authentisierung eingesetzt, beispielsweise für Hashing-Verfahren oder Signaturen, muss sichergestellt werden, dass diese dem Stand der Technik entsprechen. Hierzu sollten die entsprechenden Maßnahmen des Bausteins B 1.7 *Kryptokonzept* umgesetzt werden.

**Gesicherte Übertragung von Authentisierungsdaten**

Die Übertragung von Identifikatoren muss auf angemessene Art und Weise geschützt werden, sodass ein Angreifer die Identifikatoren nicht nutzen kann, um sich als legitimier Benutzer oder Anbieter eines Web-Service auszugeben. Die notwendigen Schutzmechanismen hängen von der Art des genutzten Identifikators ab. Bei der Übertragung von Benutzernamen und Passwörtern muss die Vertraulichkeit gewährleistet werden, beispielsweise durch eine Transportverschlüsselung oder eine Verschlüsselung der einzelnen Web-Service-Nachrichten.

Darüber hinaus müssen die Authentisierungsdaten vor Wiedereinspielung (Replay-Angriffe) und Weiterleitung (Relay-Angriffe) geschützt werden. Dies erfolgt üblicherweise durch Zeitstempel in der Nachricht, beispielsweise über ein *wsu:Timestamp*- Element beim Einsatz von WS-Security, oder durch die Verwendung von Einmal-Zufallszahlen (*Nonce)*, beispielsweise in Form eines *wsse:Nonce*- Elements. Bei der Verwendung von Noncen muss sichergestellt werden, dass die Zufallszahlen keinesfalls mehrfach verwendet werden. Ein Schutz vor Relay-Angriffen kann durch explizite, vor Manipulationen geschützte Angabe des Empfängers einer Nachricht realisiert werden.

Prüffragen:

- Erfolgt in der Kommunikation zwischen Web-Service und Web-Service-Nutzer eine gegenseitige Authentisierung, bevor der Gegenseite vertrauliche Informationen übermittelt oder Zugriffe auf Funktionen gewährt werden?
- Werden ausreichend starke Verfahren zur Authentisierung eingesetzt?
- Werden Passwörter ausschließlich verschlüsselt übertragen?

- Wird beim Einsatz von XML-Signaturen sichergestellt, dass sich die Signatur tatsächlich auf die auf der Anwendungsebene verarbeiteten Daten bezieht, um XML Signature Wrapping-Angriffe zu verhindern?
- Sind für die Authentisierung genutzte kryptographische Verfahren im Kryptokonzept der Institution berücksichtigt?
- Sind Schutzmaßnahmen gegen die Wiedereinspielung und Weiterleitung von Identifikatoren umgesetzt?

# M 4.457 Sichere Mandantentrennung bei Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Wird ein Web-Service von mehreren, voneinander unabhängigen Anwendern ("Mandanten") gemeinsam genutzt, so müssen Maßnahmen umgesetzt werden, die verhindern, dass ein Anwender versehentlich oder missbräuchlich auf die Daten eines anderen Mandanten zugreift (siehe G 4.94 *Unbefugter Zugriff auf Daten eines anderen Mandanten bei Webanwendungen und Web-Services*).

Zur Trennung der Datenbestände sind verschiedene Verfahren möglich, die einzeln oder kombiniert zum Einsatz kommen können:

**Applikationsseitige Trennung**

Der Programmcode der Anwendung entscheidet bei der Ausführung einer Programmfunktion, welche Daten für welchen Benutzer zugänglich sind, indem zum Beispiel ausschließlich vom Benutzer selbst angelegte Datensätze angezeigt werden oder die Datensätze ein bestimmtes Mandantenkennzeichen enthalten, das von der Anwendung ausgewertet wird. Hier ist die Gefahr eines ungewollten Zugriffs auf Daten anderer Mandanten besonders hoch, da bereits ein Implementierungsfehler im Code oder eine fehlende Prüfung beim Direktaufruf von Funktionen entsprechende Daten offenlegen kann.

**Trennung in der Datenhaltung**

Bei dieser Realisierungsvariante werden die Daten verschiedener Mandanten in den eingesetzten Datenspeichersystemen getrennt vorzuhalten (zum Beispiel in verschiedenen logischen Datenbanken, verschiedenen Tabellen oder unterschiedlichen Zweigen im Verzeichnisdienstschema). Durch die Nutzung entsprechender mandantenspezifischer Accounts für den Datenzugriff und ein passendes Berechtigungskonzept kann dabei sichergestellt werden, dass jeweils nur mandanteneigene Daten gelesen oder verändert werden können. In diesem Szenario sind Zuordnungsfehler nur noch dann möglich, wenn der Fehler auch zu einer falschen Zuordnung des eingesetzten Datenbank-/Verzeichnisdienstaccounts führt.

**Trennung der Umgebungen**

Die Dienste verschiedener Mandanten werden auf verschiedenen virtuellen oder physischen Systemen angeboten. Beim Zugriff eines Anwenders wird sichergestellt, dass nur Dienste auf den Systemen des eigenen Mandanten erreichbar sind. Dies kann zum Beispiel durch ein entsprechendes Authentisierungsverfahren erreicht werden oder durch netzseitige Maßnahmen, die die verschiedenen Systeme nur aus dem Netz des jeweiligen Mandanten heraus erreichbar machen.

**Mandantenspezifische Verschlüsselung**

Zusätzlicher Schutz von unbefugten Zugriffen kann durch die verschlüsselte Ablage von Daten realisiert werden. Die Verschlüsselung kann dabei gan-

ze Datenbankinhalte, alternativ aber auch nur einzelne sensible Datenfelder umfassen. Durch die Erzeugung, Nutzung und Vorhaltung der erforderlichen kryptographischen Schlüssel in den Systemen der Anwender wird ein Zugriff Dritter auf die jeweils eigenen Daten ausgeschlossen. Dieses Verfahren gewährleistet auch einen Schutz gegen die unbefugte Einsicht in Daten durch Administratoren des Diensteanbieters, erfordert aber entsprechend geeignete Strategien für das Schlüsselmanagement, insbesondere beim Verlust oder Wechsel von Schlüsseln. Weiterhin schränken Verschlüsselungsmaßnahmen auch die serverseitige Verarbeitung der Daten stark ein, so ist zum Beispiel ein Suchen oder Sortieren mit Mitteln des Datenbank-Managementsystems nicht mehr möglich.

Um eine Mandantentrennung sicher und wirksam umzusetzen, müssen die folgenden Punkte beachtet werden:

- Die Trennung der Datenbestände verschiedener Mandanten darf nicht nur rein applikationsseitig umgesetzt werden, sondern muss nach Möglichkeit durch eine logisch getrennte Datenhaltung mit separaten Datenbank-Accounts für den Zugriff und entsprechend eingeschränkten Berechtigungen unterstützt werden.
- Bei erhöhtem Schutzbedarf sind ergänzend Möglichkeiten zur mandantenspezifischen Verschlüsselung zu prüfen und nach Bedarf umzusetzen. Dabei muss sichergestellt werden, dass der Zugriff auf die erforderlichen kryptografischen Schlüssel nur den jeweils Berechtigten möglich ist (clientseitige Kryptierung). Eine solche Lösung ist insbesondere erforderlich, wenn ein Zugriff auf Datenbestände durch Administratoren des Diensteanbieters sicher ausgeschlossen werden muss.
- Die Zuordnung von Benutzern zu ihrem Mandanten muss manipulationssicher realisiert werden (durch eine entsprechende, nach Mandanten getrennte Benutzerverwaltung oder geeignete Kriterien für die automatisierte Zuordnung von Benutzern zu Mandanten, zum Beispiel auf der Grundlage von Zertifikaten).
- Die Mandantentrennung muss durchgängig umgesetzt werden. Dies betrifft externe Schnittstellen, aber auch Verfahren zur Datensicherung (Möglichkeit zur getrennten Rücksicherung der Mandantendaten). Auch die Protokollierungsmechanismen müssen so gestaltet sein, dass eine mandantenspezifische Auswertung oder Bereitstellung von Logdateien möglich ist.
- Das gewählte Konzept zur Mandantentrennung muss in der Dokumentation nachvollziehbar beschrieben sein. Im Rahmen von regelmäßigen Audits und Penetrationstests muss die Wirksamkeit der Mandantentrennung im Prüfumfang berücksichtigt werden.

Prüffragen:

- Sieht das Konzept Maßnahmen vor, die über eine rein applikationsseitig realisierte Mandantenzuordnung hinausgehen, um auszuschließen, dass einfache Softwarefehler zu einem Zugriff auf Daten anderer Mandanten führen?
- Erfolgt die Zuordnung von Dienstnutzern zu Mandanten mit einem zuverlässigen und manipulationssicheren Verfahren?
- Berücksichtigt das Konzept zur Mandantentrennung alle relevanten Aspekte (Dienstnutzung, Schnittstellen, Datensicherung, Protokollierung)?
- Ist das umgesetzte Konzept zur Trennung von Daten verschiedener Mandanten nachvollziehbar dokumentiert? Entspricht die Umsetzung der Dokumentation?
- Wird die Wirksamkeit der Mandantentrennung regelmäßig im Rahmen von Sicherheitsaudits oder Penetrationstests überprüft?

# M 4.458 Planung des Einsatzes von Web-Services

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Vor dem Einsatz eines Web-Service ist der genaue Zweck zu bestimmen, den der Web-Service erfüllen soll. Denn Web-Services stellen nur eine Art der Kommunikation zwischen Maschinen dar und bringen spezifische Vor- und Nachteile gegenüber anderen Formen der Integration von Anwendungen und Diensten mit sich. Nicht jede Anwendung eignet sich für eine Ausführung als Web-Service. Auch Kosten-Nutzen-Überlegungen spielen hier eine Rolle. So wird der Datendurchsatz, gerade beim durchgängigen Einsatz von Web-Service-Sicherheitsstandards, regelmäßig deutlich schlechter sein als bei klassischen Massendaten-Übertragungsverfahren. Dem gegenüber stehen Vorteile in der Wiederverwendbarkeit von Diensten und Funktionen und in der Skalierbarkeit von Anwendungen durch Verteilung der Aufgaben auf unterschiedliche Dienste.

Am Anfang steht eine gründliche Analyse der Anforderungen, die auch dokumentiert werden sollten. Hierbei empfiehlt es sich, mit einer Abbildung der betroffenen Prozesse auf einer hohen Abstraktionsebene zu beginnen, daraufhin die Arbeitsabläufe im Ist und Soll zu skizzieren und darauf aufbauend einen Entwurf mit Eingaben, Ausgaben, Schnittstellen und Daten zu detaillieren. Ebenso zu identifizieren sind Anbieter, Konsumenten, Kommunikationsverbindungen und erforderliche Service-Verzeichnisse. Zu letzteren ist zu entscheiden, ob und welche Web-Services darin veröffentlicht werden sollen.

Eine grundlegende Entscheidung ist die für einen REST- oder einen SOAP-basierten Web-Service. Während SOAP bei internen betrieblichen Anwendungen wesentlich weiter verbreitet ist und auf eine Vielzahl von Werkzeugen und Standards aufbaut, ist REST hauptsächlich im agilen Web-Umfeld anzutreffen. Letztlich wird die Entscheidung im Wesentlichen von den anderen Diensten und Anwendungen abhängen, die bereits vorhanden sind, noch entstehen oder angebunden werden sollen. In jedem Fall sind die Folgen der grundlegenden Architekturentscheidung am Anfang zu berücksichtigen und durchzuspielen.

Dies ist insbesondere dann relevant, wenn eine serviceorientierte Architektur (SOA) entstehen oder ein Dienst in eine bestehende SOA integriert werden soll. Hierbei sind Fragen des SOA-Betriebsmodells zu klären: Wer ist innerhalb der Institution für die fachliche Funktionalität und für die verarbeiteten Informationen verantwortlich? Rollen und Verantwortlichkeiten sind spätestens jetzt festzulegen und zu dokumentieren.

Ob eine Architektur in Richtung Serviceorientierung umgeformt werden soll, ist eine strategische Entscheidung, die mit der Strategie zur Nutzung von Web-Services und der Plattformstrategie Hand in Hand gehen sollte. Sollen viele Web-Services auf unterschiedliche, möglicherweise wechselnde Art und Weise miteinander interagieren können - man spricht von Orchestrierung -, so können Modellierungs- und Beschreibungssprachen wie BPMN oder BPEL eingesetzt werden, um die Interaktion der Geschäftsprozesse zu steuern. Dies ergibt jedoch frühestens dann Sinn, wenn eine ausreichend große Zahl von Web-Services vorhanden ist, welche auf verschiedene Art verknüpft werden sollen, um neue Dienste zu kreieren.

Besonders gut geeignet für die Ausführung als Web-Service sind Dienste, die von mehreren Anwendungen oder anderen Diensten benötigt werden. Hier sollte auch berücksichtigt werden, dass die Dienste nicht nur intern genutzt werden könnten. Werden diese weiteren Institutionen zur Verfügung gestellt werden, ist unbedingt zu klären, wer über die Bereitstellung von Diensten und Daten an Dritte entscheidet. Außerdem sind die Absicherung der Netzübergänge und Kommunikationsschnittstellen zu betrachten, damit die Web-Services im erforderlichen Maß von außen angesprochen werden können, ohne die Sicherheit interner Netze unnötig zu gefährden. Dabei werden häufig Unternehmensdaten über Netzsegmente hinweg und auf freigeschalteten Ports wie 80 (HTTP) oder 443 (HTTPS) durch Firewalls hindurch transportiert. Auch Schadsoftware kann auf diesem Weg in die Institution hinein gelangen, etwa als eingebettete Datei. Hier sind Schutzkonzepte und technische Sicherheitsmaßnahmen wie Application Level Gateways (ALG) zu überprüfen und gegebenenfalls anzupassen.

Um den Web-Service gegen Angriffe abzusichern, müssen auch bei der Implementierung geeignete Sicherheitsmaßnahmen vorgesehen werden, zum Beispiel eine durchgängige Validierung von Ein- und Ausgabedaten und Konformitätsprüfungen der verarbeiteten XML-Daten. Auch hierzu sollten entsprechende Vorgaben in der Planungsphase erarbeitet und dokumentiert werden.

Um über die Einführung von Web-Services, die damit verbundenen Risiken und die notwendige Absicherung informiert entscheiden zu können, ist es wichtig, die komplette Funktionalität des Web-Service zu dokumentieren und diese Dokumentation aktuell zu halten. Dies geschieht am besten für alle Web-Services an einer zentralen Stelle. Bei Nutzung des Web-Service durch mehrere Parteien sollten alle Seiten Zugriff auf diese Informationen haben.

Auch auf den Lebenszyklus eines Web-Service hat die Mehrfachnutzung Einfluss: Es muss geklärt und beschrieben werden, wie Änderungen eines Web-Service, der von mehreren Anwendungen oder Organisationen genutzt wird, durchgeführt werden können. Entsprechendes gilt für die Abschaltung am Ende des Lebenszyklus.

Für die Realisierung der Web-Service-Funktionalität empfiehlt es sich, bewährte und gut getestete Komponenten heranzuziehen, da die Materie komplex ist und Programmierfehler bei Eigenentwicklungen häufig vorkommen. Sowohl beim Applikationsserver wie bei Web-Service-Bibliotheken oder -Frameworks sollten Produkte ausgewählt werden, die aktiv weiter gepflegt werden, und bei denen Informationen über Schwachstellen und Patches zeitnah bereitstehen.

Kommen komplexere Standards wie etwa WS-Security, WS-Trust oder WS-Federation zum Einsatz, ist die gegenseitige Abhängigkeit und Beeinflussung der verschiedenen Sicherheitsfunktionen genau zu planen und zu testen. Für die Aufrechterhaltung der Sicherheit in einer kompletten SOA ist schließlich ein Zusammenspiel von Standards, Konzepten und Mechanismen notwendig, das über die Absicherung einer reinen Client-Server-Beziehung hinausgeht. Hier ist besonderes Fachwissen gefragt.

Neben anderen Sicherheitszielen, die je nach Einsatzzweck eine Rolle spielen können, ist fast immer die Absicherung der Kommunikation zwischen Dienstnutzer und Dienstanbieter entscheidend. Dies kann entweder auf Transportebene erfolgen, wenn der Transportweg der Nachrichten dies erlaubt (etwa durch SSL-/TLS bei HTTP), oder aber auf Nachrichtenebene. Letzteres erlaubt neben der Ende-zu-Ende-Absicherung auch, die Sicherheitsparameter

in einer feineren Granularität auszuwählen und auszuwerten, zum Beispiel die Signatur oder Verschlüsselung lediglich für bestimmte Teile einer Nachricht. Dabei ist tiefliegendes Wissen über die verwendeten Mechanismen notwendig, um nicht durch Schwachstellen in Protokollen oder in der Implementierung angreifbar zu werden, beispielsweise durch *XML Signature Wrapping* (siehe G 5.183 *Angriffe auf XML*). Außerdem erschwert eine Ende-zu-Ende-Verschlüsselung die Filterung bösartiger Nachrichten. Hier kann es helfen, die Verschlüsselung am Application-Level-Gateway zu terminieren.

Um die Vorteile von Web-Services, insbesondere ihre Wiederverwendbarkeit und Skalierbarkeit, voll ausnutzen zu können, ist es entscheidend, das Identitäts- und Zugriffsmanagement nicht in jedem Dienst einzeln neu zu realisieren. Die Planung der Web-Service-Landschaft umfasst deshalb auch die Planung der übergreifenden Verwaltung der Benutzer und Rechte. Näheres hierzu findet sich in den Maßnahmen M 4.456 *Authentisierung bei Web-Services* und M 4.455 *Autorisierung bei Web-Services*.

Die vorgenannten, für die Planung eines Web-Service erforderlichen Aspekte gelten in ähnlicher Form auch für klassische IT-Anwendungen. Durch die mögliche Mehrfach-Nutzung und Orchestrierung zu übergreifenden Aufgaben und durch die technische Komplexität der Standards und Protokolle ist der Einfluss von Planungsmängeln auf den Projekterfolg jedoch gegenüber anderen Technologien erhöht.

Prüffragen:

- Ist der Einsatzzweck des Web-Service beschrieben und sind die Anforderungen der Consumer analysiert und dokumentiert?
- Ist dokumentiert, wer für die fachliche Funktionalität und die verarbeiteten Informationen verantwortlich ist?
- Wurden Konzepte und Maßnahmen zur Absicherung der Netzübergänge im Hinblick auf den Einsatz von Web-Services angepasst?
- Besteht ein Schutz vor Schadsoftware in Web-Service-Nachrichten, und sind Sicherheitsmaßnahmen wie eine Eingabe- und Ausgabevalidierung für die Software-Implementierung vorgegeben?
- Wurden bewährte, gut getestete Komponenten, Bibliotheken und Frameworks für die Realisierung des Web-Service ausgewählt?
- Ist die Kommunikation zwischen Consumer und Dienstanbieter entweder auf Transport- oder auf Nachrichtenebene auf eine dem Schutzbedarf angemessene Weise abgesichert?

# M 4.459 Einsatz von Verschlüsselung bei Cloud-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Grundsätzlich ist bei Cloud-Nutzung hinsichtlich der Verschlüsselung von Daten auf dem Transportweg (engl.: *data in motion*) und der Verschlüsselung von Daten an deren Ablageort (engl.: *data at rest*) zu unterscheiden.

Die Verschlüsselung auf dem Transportweg wird dabei im Zusammenhang mit der Nutzung von Cloud Services immer gefordert, außer es handelt sich um einen Cloud-Dienst einer Private Cloud, der über das abgesicherte lokale Netz genutzt wird. Die Anmeldung an einem Cloud Service muss in jedem Fall verschlüsselt erfolgen, auch im Falle der Nutzung einer Private Cloud. Vorgaben beziehungsweise Empfehlungen hierzu finden sich daher in den Maßnahmen zur Service-Definition (siehe M 2.536 *Service-Definition für Cloud-Dienste durch den Anwender*) und zur Vertragsgestaltung mit dem Cloud-Diensteanbieter (siehe M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*). Deshalb wird in dieser Maßnahme nicht näher auf die Möglichkeiten zur Umsetzung einer Verschlüsselung in Motion eingegangen und auf M 5.66 *Clientseitige Verwendung von SSL/TLS* bzw. M 5.177 *Serverseitige Verwendung von SSL/TLS* verwiesen.

Bei der Verschlüsselung der Daten an ihrem Speicher- beziehungsweise Verarbeitungsort sind zwei Varianten zu unterscheiden. Zum einen kann die Verschlüsselung im Vorfeld einer Datenübertragung an den Cloud-Diensteanbieter direkt durch die nutzende Institution vorgenommen werden. Bei der zweiten Variante erfolgt die Verschlüsselung der übertragenen Daten erst auf den Systemen des Cloud-Diensteanbieters.

Sofern die Verschlüsselung durch den Cloud-Diensteanbieter vorgenommen wird, sind hierzu entsprechende vertragliche Regelungen zu treffen, die unter anderem Vorgaben zur Auswahl sicherer Verschlüsselungsmechanismen und zum Einsatz geeigneter Schlüssellängen beinhalten. Darüber hinaus sollte vereinbart werden, dass der Cloud-Anwender bei Bedarf die Neuvergabe von Schlüsseln anstoßen kann und er Einfluss auf die Lebenszyklen der Schlüssel nehmen kann. Es ist zu beachten, dass bei der Verschlüsselung durch den Cloud-Diensteanbieter die Verantwortung für das Schlüsselmanagement auch bei ihm liegt. Mitarbeiter des Cloud-Diensteanbieters, die Kenntnis von den entsprechenden Schlüsseln haben, können so auf die Daten der Institution zugreifen.

Alternativ zur Verschlüsselung der Daten durch den Cloud-Diensteanbieter kann, abhängig vom Cloud Service, für die Institution die Möglichkeit bestehen, eigene Verschlüsselungsmechanismen einzusetzen. Das sichere Schlüsselmanagement liegt dann in ihrer Hand. In diesem Zusammenhang hat sich der Einsatz sogenannter Hardware-Security-Module (HSM) zur Unterstützung einer sicheren Erzeugung und Speicherung der Schlüssel als hilfreich erwiesen. Beim Einsatz eines HSM ist es in der Folge unerheblich, wo die Verschlüsselung stattfindet, in der Cloud oder auf den Systemen der Institution, der Cloud-Diensteanbieter kann nicht auf die Schlüssel zugreifen.

Es gilt zu beachten, dass eine Verschlüsselung durch die Institution nicht in jedem Fall realisierbar ist. Als eine Besonderheit im Zusammenhang mit der Nutzung von Cloud-Diensten ist hier die Abhängigkeit vom genutzten Service-Mo-

dell zu berücksichtigen. So ist beispielsweise bei der Nutzung von Software as a Service eine eigene Verschlüsselung in Verbindung mit der Nutzung von Anwendungen über eine API (zum Beispiel CRM-Datenbankverschlüsselung) in vielen Fällen nicht möglich. Sollte aber eine Verschlüsselung gefordert werden und der Cloud-Diensteanbieter kann diese nicht bereitstellen, so kann man, je nach Cloud Service, auch auf Drittanbieter zurückgreifen, die eine solche Verschlüsselung anbieten. Sofern eine Institution den Einsatz eigener Verschlüsselungsmechanismen plant oder einen Drittanbieter nutzt, empfiehlt sich eine enge Abstimmung mit dem Cloud-Diensteanbieter, um mögliche Probleme im laufenden Betrieb möglichst frühzeitig ausschließen zu können.

Bei der Umsetzung dieser Maßnahme ist zusätzlich der Baustein B 1.7 *Kryptokonzept* zu berücksichtigen.

Prüffragen:

- Existieren bei Verschlüsselung durch den Cloud-Diensteanbieter vertragliche Regelungen, die diesem Vorgaben zur Auswahl sicherer Verschlüsselungsmechanismen und zum Einsatz geeigneter Schlüssellängen machen?
- Wird beim Einsatz eigener Verschlüsselungsmechanismen die Umsetzung eines geeigneten Schlüsselmanagements sichergestellt?
- Werden Besonderheiten der Cloud-Nutzung hinsichtlich des gewählten Service-Modells bei der Umsetzung von Verschlüsselung berücksichtigt?

# M 4.460 Einsatz von Federation Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter

Wesentliches Merkmal von Federation Services ("Verbunddiensten") ist die Trennung zwischen Authentisierung und Autorisierung. Für Federation Services spielen der sogenannte Identity Provider und der Service Provider eine wesentliche Rolle. Der Identity Provider übernimmt die Authentisierung des Benutzers, beim Service Provider erfolgt die Autorisierung. Zwischen Identity Provider und Service Provider muss eine explizite Vertrauensstellung eingerichtet werden.

Der Einsatz von Federation Services bietet eine Möglichkeit zur Absicherung der Cloud-Nutzung durch gesicherte Übertragung von Claims-Token (verifizierte, zentral ausgestellte Aussagen zur Identität eines Benutzers), häufig auch Authentisierungstoken genannt. Dabei können die Benutzerinformationen (zum Beispiel Benutzername) oder andere Informationen zur Identifizierung eines Mitarbeiters auch über Unternehmensgrenzen hinweg sicher übertragen werden.

Nur durch die beschriebene Vertrauensstellung kann gewährleistet werden, dass der Service Provider die vom Identity Provider ausgestellten Claims-Token akzeptiert. Sollen Federation Services zum Einsatz kommen, übernimmt die Institution als Cloud-Anwender dabei die Rolle des Identity Providers.

Mitarbeiter, die einen Cloud Service in Anspruch nehmen wollen, melden sich dazu zunächst am zentralen Verzeichnisdienst an und erhalten in der Folge ein Ticket (zum Beispiel Kerberos-Ticket), mit dessen Hilfe sie sich für festgelegte Dienste authentisieren können. Die Anforderung zur Nutzung eines bestimmten Cloud-Dienstes wird in der Folge vom Federation Server der nutzenden Institution in ein sogenanntes SAML-Ticket umgewandelt.

SAML steht dabei für Security Assertion Markup Language und stellt einen Standard für die Gestaltung von Tokens dar. Das auf diesem Weg erzeugte Token wird an den Federation Server des Cloud-Diensteanbieters übertragen. Dieser entpackt das SAML-Ticket, verifiziert die Unterschrift vom Federation Server des Cloud-Anwenders und leitet die Inhalte an die Anwendung weiter. Bei Nutzung von Federation Services sollte SAML ab Version 2.0 eingesetzt werden.

Da die Institution wie beschrieben als Identity Provider agiert, geht die Verantwortung für die ordnungsgemäße Authentisierung der Benutzer auf diese über. Die Verantwortlichen innerhalb der nutzenden Institution müssen sicherstellen, dass lediglich berechtigten Benutzern ein SAML-Ticket ausgestellt wird. Auch die weitergehenden Berechtigungen, die nach erfolgreicher Authentisierung an die Anwendung übergeben werden, sollten sorgfältig definiert und regelmäßig überprüft werden. Benutzern sollten nur Berechtigungen zugewiesen werden, die diese auch tatsächlich zur Erfüllung ihrer Aufgaben benötigen.

Die Übernahme der Verantwortung für die Authentisierung ihrer Benutzer bei der Nutzung von Cloud Services bringt gleichzeitig eine Reihe von Vorteilen für die nutzende Institution mit sich. So ist beispielsweise die Umsetzung einer institutionsweiten Passwortrichtlinie unabhängig von möglicherweise abweichenden Vorgaben des Cloud-Diensteanbieters möglich. Außerdem liegt

die Hoheit über die Berechtigungsvergabe allein bei der nutzenden Institution. Bei sorgfältiger Konfiguration des zentralen Verzeichnisdienstes können unberechtigte Zugriffe, beispielsweise durch ehemalige Mitarbeiter, wirksam ausgeschlossen werden, ohne dabei auf die Mitwirkung des Cloud-Diensteanbieters angewiesen zu sein.

Aufgrund dieser Vorteile für die nutzende institution und die Möglichkeit zur einfacheren Bereitstellung von Services durch den Cloud-Diensteanbieter werden Federation Services daher bereits in großem Umfang von Cloud Services unterstützt.

Sollen bei einem Cloud-Nutzungs-Vorhaben Federation Services zum Einsatz kommen, ist dies im Rahmen der Vertragsverhandlungen mit dem Cloud-Diensteanbieter zu berücksichtigen (siehe hierzu Maßnahme M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*). In der Regel stellt der Cloud-Diensteanbieter der nutzenden Institution zusätzlich Informationen bezüglich notwendiger Konfigurationsparameter für deren Federation Server zur Verfügung. Bei der Festlegung der Konfigurationsparameter und der im SAML-Ticket zu übertragenden Informationen sollte die Institution darauf achten, dass nach Möglichkeit nur die erforderlichen Informationen an den Cloud-Diensteanbieter übertragen werden. Eine umfassende Replikation weitreichender und nicht erforderlicher Informationen aus dem Verzeichnisdienst, wie zum Beispiel Telefonnummern, sollte vermieden werden.

Prüffragen:

- Ist sichergestellt, dass nur die erforderlichen Informationen in dem sogenannten SAML-Ticket an den Cloud-Diensteanbieter übertragen werden?
- Werden die Benutzerberechtigungen regelmäßig geprüft und wird sichergestellt, dass lediglich berechtigten Benutzern ein SAML-Ticket ausgestellt wird?

# M 4.461 Portabilität von Cloud Services

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter

Grundsätzlich ist bei Cloud-Nutzung der Wechsel von einem Diensteanbieter zu einem anderen einfacher möglich, als dies beispielsweise bei klassischen Outsourcing-Vorhaben der Fall ist. In der Praxis hat sich jedoch gezeigt, dass auch bei Cloud Services häufig Probleme auftreten, wenn diese zu einem anderen Cloud-Diensteanbieter übertragen oder zurück in die eigene Institution geholt werden sollen.

Institutionen, die sich zur Nutzung von Cloud Services entscheiden und dabei erhöhte Anforderungen hinsichtlich der benötigten Flexibilität haben, sollten daher zusätzliche Maßnahmen zur Aufrechterhaltung der Portabilität von Cloud Services umsetzen.

Die Notwendigkeit zur Portabilität von Cloud Services ergibt sich zum einen durch einen angestrebten Wechsel des Cloud-Diensteanbieters und zum anderen durch die Möglichkeit, Cloud Services wieder durch die IT der eigenen Institution erbringen zu lassen. Beim Wechsel des Cloud-Diensteanbieters kann der Cloud Service direkt von einem Dienstleister zum anderen übertragen werden. In Fällen, in denen dies nicht möglich oder gewünscht ist, wird der Cloud Service zunächst an die beauftragende Institution übergeben und im Anschluss zum neuen Cloud-Diensteanbieter migriert.

In beiden Fällen sind durch die Institution alle wichtigen Anforderungen (zum Beispiel hinsichtlich einzusetzender Datenformate) zu definieren, die einen einfachen Wechsel des Dienstleisters oder eine Rückholung in die eigene Infrastruktur ermöglichen.

Insbesondere bei der Nutzung von Software as a Service sollte ein besonderes Augenmerk auf die eingesetzten Datenformate gelegt werden. Hier treten in der Praxis häufig Probleme beim Import der Daten in einen neuen Service auf, da der Cloud-Diensteanbieter ein eigenes, nicht standardisiertes Format zum Einsatz bringt. Die Durchführung von Portabilitätstests kann hier erheblich zur Sicherstellung der Portabilität von Cloud Services beitragen.

Sofern die nutzende Institution auf den flexiblen Wechsel des Cloud-Diensteanbieters angewiesen ist, empfiehlt es sich, die Portabilität vertraglich zu regeln. In diesem Fall sind die inhaltlichen Vorgaben der Maßnahme zur Vertragsgestaltung (siehe hierzu M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*) um den entsprechenden Aspekt zu ergänzen.

Prüffragen:

- Wurden alle wichtigen Anforderungen für den Wechsel des Cloud-Diensteanbieters oder die Rückholung in die eigene IT definiert?
- Ist die Durchführung von Portabilitätstests vorgesehen?
- Sind Vorgaben zur Realisierung der Portabilität in die Vertragsgestaltung mit dem Cloud-Diensteanbieter eingeflossen?

# M 4.462 Einführung in die Cloud-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Im Sinne der IT-Grundschutz-Vorgehensweise umfasst Cloud-Nutzung alle Themengebiete, die zur Nutzung einer Cloud-Umgebung erforderlich sind. Damit schließt Cloud-Nutzung insbesondere folgende Aspekte ein:

- Anwendung des Cloud Services durch Mitarbeiter der nutzenden Institution
- Administration des Cloud Services durch Mitarbeiter der nutzenden Institution

**Definitionen und Grundbegriffe zur Cloud-Nutzung**

Ein Cloud Service wird in der Regel durch die nachfolgend aufgeführten Eigenschaften charakterisiert (gemäß Cloud Security Alliance - CSA). Die Beschreibung ist dabei nicht starr definiert, sondern kann immer noch interpretiert, ergänzt oder auch reduziert werden.

**On-demand Self-Service**

Die Provisionierung, also die Bereitstellung der IT-Ressourcen, wie beispielsweise Rechnerleistung oder Speicherkapazitäten, läuft automatisch ohne Interaktion mit dem Cloud-Diensteanbieter (engl. *Cloud Service Provider*, kurz CSP) ab.

**Broad Network Access**

Cloud Services werden über ein Netz bereitgestellt und sind über Standard-Mechanismen beziehungsweise Standard-Protokolle zugänglich.

**Resource Pooling**

Die IT-Ressourcen des Cloud-Diensteanbieters sind in sogenannten Pools organisiert. Basierend auf einem mandantenfähigen Modell ist es dem Cloud-Diensteanbieter somit möglich, den Anforderungen einer Vielzahl von Anwendern bedarfsgerecht zu entsprechen.

Bei der Nutzung von Cloud Services ist dem Auftraggeber der genaue Ort der IT-Ressourcen des Cloud-Diensteanbieters in der Regel nicht bekannt. Beispiele für solche Ressourcen können Speichersysteme, Prozessorleistung, Arbeitsspeicher oder auch Anwendungssoftware sein.

**Rapid Elasticity**

Cloud Services lassen sich (automatisiert), schnell und flexibel anpassen, um auf sich rasch ändernden Bedarf aufseiten der nutzenden Institution reagieren zu können.

**Measured Services**

Cloud Services verwenden häufig Werkzeuge, die die Ressourcennutzung in Abhängigkeit des genutzten Services (zum Beispiel Speicherlösungen, Prozessorleistung oder aktive Benutzerkonten) automatisch überwachen und optimieren können.

Um Transparenz sowohl aufseiten der nutzenden Institution als auch aufseiten des Providers zu schaffen kann die Ressourcennutzung gemessen und die Ergebnisse gegenüber dem Anwender kommuniziert werden.

**Pay per Use**

Die Abrechnung erfolgt bei Cloud-Nutzung in der Regel auf Basis der Leistungen beziehungsweise Ressourcen, die auch tatsächlich vom Anwender in Anspruch genommen wurden.

**Definition des BSI**

Um für alle Arbeiten rund um Cloud Computing eine einheitliche Grundlage zu haben, hat das BSI folgende Definition für den Begriff "Cloud Computing" festgelegt:

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (zum Beispiel Rechenleistung, Speicherplatz), Plattformen und Software.

In diesem Dokument wird der Begriff "Cloud Computing" entsprechend benutzt, wobei die oben genannten Charakteristika stets im Hinterkopf zu behalten sind. So ist eine einfache Webanwendung in der Regel kein Cloud Computing, obwohl dies von den Marketingabteilungen der Hersteller oft so bezeichnet wird.

**Cloud-Nutzung mittels unterschiedlicher Cloud-Service-Modelle**

Bei Cloud-Nutzung können grundsätzlich drei unterschiedliche Kategorien von Service-Modellen unterschieden werden. Zum besseren Verständnis sind diese nachfolgend näher beschrieben.

**Infrastructure as a Service (IaaS)**

Bei IaaS werden IT-Ressourcen wie zum Beispiel Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Cloud-Anwender kauft diese virtualisierten und in hohem Maße standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Anwender zum Beispiel Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

Die Verwaltung der IT-Ressourcen obliegt der nutzenden Institution und wird in der Regel durch den Cloud Service Administrator auf Kundenseite (engl. *Customer Cloud Service Administrator*) vorgenommen.

**Platform as a Service (PaaS)**

Ein PaaS-Anbieter stellt eine komplette Infrastruktur bereit und bietet dem Anwender auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform zum Beispiel Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe etc. als Service zur Verfügung stellen. Die nutzende Institution hat keinen Zugriff auf die darunter liegenden Schichten (Betriebssystem, Hardware), sie kann aber auf

der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der Cloud-Diensteanbieter in der Regel eigene Werkzeuge anbietet.

**Software as a Service (SaaS)**

Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computings entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

Die Mitarbeiter der Institution nutzen Software-Anwendungen direkt über das Internet. Eine Installation auf dem eigenen PC beziehungsweise im Rechenzentrum der Institution ist häufig nicht erforderlich.

Teilweise werden jedoch auch Architekturen eingesetzt, bei denen der Einsatz spezieller Clientsoftware erforderlich oder möglich ist (Nutzung über Browser und/oder Clientsoftware).

**Cloud-Nutzung mittels unterschiedlicher Cloud-Bereitstellungsmodelle**

Institutionen, die sich für die Nutzung von Cloud Services entscheiden, haben in der Regel die Wahl zwischen folgenden Bereitstellungsmodellen:

**Public Cloud**

Bereitstellung von Cloud Services für beliebige Anwender über das Internet.

**Private Cloud**

Bereitstellung von Cloud Services ausschließlich für die eigene Institution. Bei einer Private Cloud ist eine weitere Unterscheidung möglich:

- On-Premise: Die Cloud-Infrastruktur wird in einem Rechenzentrum der Institution betrieben.
- Off-Premise: Die Cloud-Infrastruktur wird in einem fremden Rechenzentrum betrieben.

Hinweis zur Problematik bei der Zuordnung zu einem Bereitstellungsmodell:

In Konzernen mit mehreren Konzerngesellschaften wird aus Sicht der IT-Tochter eine Private Cloud für den Konzern betrieben. Eine nutzende Konzerngesellschaft teilt diese Sicht jedoch unter Umständen nicht, da sie sich diese Cloud in ihren Augen mit "Fremden" teilt. Daher betrachtet die Konzerngesellschaft die Cloud als "public".

**Hybrid Cloud**

Eine Hybrid Cloud stellt in der Regel eine Mischform aus Public Cloud und Private Cloud dar.

Teile des Services werden dabei durch On-Premise-Systeme abgebildet, während andere Teile des Services durch (Public)-Cloud-Systeme bei einem Cloud-Diensteanbieter abgebildet werden. Die Services, die durch den Cloud-Diensteanbieter abgebildet werden, können auch Private-Cloud-Off-Premise- oder Community-Cloud-Lösungen sein.

Die Hybrid Cloud bietet die Möglichkeit zur Aufteilung eines Services zwischen Public Cloud und Private Cloud.

**Beispiel:**
- Für die Inanspruchnahme eines Office-Services werden die E-Mail-Konten in der Private Cloud der Institution verwaltet, für die Nutzung von Webkonferenzen und Dateifreigaben wird jedoch auf die Public-Cloud-Infrastruktur des Dienste-Anbieters zurückgegriffen.

Eine **Virtual Private Cloud** wird durch einen Cloud-Diensteanbieter in seinem Rechenzentrum für dedizierte Kunden betrieben. Aus Kundensicht sieht die Cloud wie eine Private Cloud aus, der Dienstleister stellt diese aber in der Regel auf einer mandantenfähigen, geteilten Infrastruktur bereit.

Bei der **Managed Private Cloud** kann die Cloud-Infrastruktur hingegen auch im eigenen Rechenzentrum untergebracht sein. Betrieben und gemanagt wird diese allerdings von einem externen Dienstleister.

**Community Cloud**

In einer Community Cloud schließen sich Institutionen der gleichen Branche oder mit gleichen Interessen zusammen und nutzen gemeinsam eine Cloud-Umgebung, die vom Cloud-Diensteanbieter speziell für diese "Community" bereitgestellt wird.

Community Clouds finden sich auch im Bereich der öffentlichen Verwaltung. Hier stellt ein Cloud-Diensteanbieter einer Benutzergruppe eine Anwendung dediziert als Cloud Service zur Verfügung - Beispiel: Personalverwaltung oder E-Mail-Service.

# M 4.463 Sichere Installation einer Anwendung

**Verantwortlich für Initiierung:** Fachverantwortliche, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nach erfolgreichem Abschluss der Tests und der Freigabe der Anwendung ist der Roll-Out bzw. die Installation der Anwendung zu planen. Hierbei ist es zweckmäßig, eine Installationsanweisung zu erstellen (siehe M 2.84 *Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware*). Bevor die Software installiert wird, ist die Vollständigkeit und Korrektheit der Software-Lieferung zu überprüfen (siehe M 2.90 *Überprüfung der Lieferung*) und die Integrität der eingesetzten Software sicherzustellen (siehe M 2.86 *Sicherstellen der Integrität von Standardsoftware*, diese Maßnahme ist auch bei Individualsoftware anwendbar). Bei der Installation ist M 2.87 *Installation und Konfiguration von Standardsoftware*, die auch für Individualsoftware anwendbar ist, umzusetzen.

Um später im laufenden Betrieb überprüfen zu können, ob die Anwendung korrekt konfiguriert wurde und um eine Neuinstallation der Anwendung zu vereinfachen, sollte die Installation einer Anwendung mit allen ihren Schritten dokumentiert werden. Dies kann beispielsweise in Form von aufeinanderfolgenden Screenshots der Installationsbildschirme erfolgen, in denen jeweils die relevanten Einstellungen vorgenommen werden.

Bei der Durchführung späterer Änderungen der Konfiguration oder bei Updates der Anwendung ist darauf zu achten, dass diese Dokumentation aktualisiert wird. Eine ausschließliche Dokumentation von späteren Konfigurationsänderungen in einem Ticketsystem oder Change-Tool führt in der Regel dazu, dass die Soll-Konfiguration nicht ohne erheblichen Aufwand nachvollziehbar ist. Damit ist die Konfiguration der Anwendung später nicht ohne Weiteres prüfbar (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Prüffragen:

- Wurde die Installation der Anwendungen so dokumentiert, dass ein mit der ursprünglichen Installation nicht vertrauter Administrator diese erfolgreich anhand der Dokumentation durchführen kann?

# M 4.464 Aufrechterhaltung der Sicherheit im laufenden Anwendungsbetrieb

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, Leiter IT

Während des Betriebes einer Anwendung oder eines Fachverfahrens sollte sichergestellt sein, dass die Benutzer ausreichend bei Fragen und Problemen unterstützt werden. Dies kann beispielsweise über den IT-Betrieb, etwa über das Bereitstellen eines IT-Ansprechpartners oder einen sogenannten Service- oder User-Help-Desk (SD / UHD), erfolgen.

Darüber hinaus sollten die Benutzer auch bezogen auf fachliche Aspekte geeignet unterstützt werden. Dies kann etwa durch einen Key-User oder eine so genannte fachliche Leitstelle erfolgen. Diese organisieren die Einführung und Schulung neuer Benutzer, unterstützen bei der korrekten Bedienung der Anwendung und nehmen Anforderungen für kommende Versionen der Anwendung auf.

Ein wichtiger Aspekt der Sicherheit einer Anwendung im laufenden Betrieb ist die geeignete Vergabe von Zugriffsrechten (siehe M 2.8 *Vergabe von Zugriffsrechten*) und die stets aktuelle Dokumentation von zugelassenen Benutzern und Rechteprofilen (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*). Die Korrektheit der vergebenen Berechtigungen sollte regelmäßig überprüft werden.

Es ist darauf zu achten, dass die Protokolldaten der Anwendung regelmäßig ausgewertet werden (siehe M 2.64 *Kontrolle der Protokolldateien*). Hierbei sind die jeweils geltenden spezifischen gesetzlichen und vertraglichen Vorgaben zu Speicherfristen für Protokolldateien, deren Zugreifbarkeit durch Dritte (z. B. Aufsichtsbehörden) und Vorgaben zur Auswertung zu beachten.

Typischerweise ergibt sich im laufenden Anwendungsbetrieb die Notwendigkeit, die Anwendung funktional anzupassen, Fehler zu beheben oder Sicherheitslücken zu schließen. Bei der Durchführung des Patch- und Änderungsmanagements sind die Vorgaben des Bausteins B 1.14 *Patch- und Änderungsmanagement* zu berücksichtigen. Insbesondere ist darauf zu achten, dass

- sicherheitskritische Patchs und Updates zeitnah eingespielt werden (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*),
- Konfigurationsänderungen einschließlich Patchs und Updates vorher geeignet getestet, freigegeben (siehe M 2.556 *Planung und Umsetzung von Test und Freigabe von Anwendungen*) und sorgfältig durchgeführt (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*) werden, und
- Konfigurationsänderungen geeignet dokumentiert werden (siehe M 4.463 *Sichere Installation einer Anwendung*).

Ferner ist sicherzustellen, dass Datensicherungen wie vorgesehen (siehe M 6.33 *Entwicklung eines Datensicherungskonzepts*) durchgeführt werden und eine Wiederherstellung der Anwendung aus den vorhandenen Datensicherungen erfolgreich möglich ist (siehe M 6.41 *Übungen zur Datenrekonstruktion*). Hierzu sind Art und Umfang der Datensicherungen festzulegen, da-

bei kann es für die verschiedenen Komponenten unterschiedliche Vorgehensweisen zur Datensicherung geben, beispielsweise für Quellcode, Konfigurationsdaten, Protokolldaten und Inhaltsdaten.

Bei von Dritten entwickelten Anwendungen ist unter Umständen, um Urheberrechtsverstößen vorzubeugen, eine Lizenzverwaltung erforderlich. Ebenso ist es zur Sicherstellung des störungsfreien Betriebes sinnvoll, dass auf allen Arbeitsplätzen einer Institution einheitliche Versionen der Anwendungen eingesetzt werden (siehe M 2.88 *Lizenzverwaltung und Versionskontrolle von Standardsoftware*).

Prüffragen:

- Werden die Benutzer im laufenden Anwendungsbetrieb ausreichend unterstützt?
- Finden bei Anwendungen regelmäßige Protokollauswertungen und Überprüfungen der vergebenen Berechtigungen statt?
- Ist sichergestellt, dass Sicherheitslücken in Anwendungen zeitnah geschlossen werden?

# M 4.465 Aussonderung von Mobiltelefonen, Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter IT

Immer wieder werden auf gebrauchten Mobiltelefonen, Smartphones, Tablets und PDAs vertrauliche Daten der Vorbesitzer entdeckt und so die Informationssicherheit der Institution, die das Gerät verkauft oder ungenügend ausgesondert hat, verletzt. Auch für gezielte Angriffe werden Endgeräte von Institutionen aufgekauft und auf sensitive Daten hin untersucht.

Auf ausgesonderten Mobiltelefonen, Smartphones, Tablets und PDAs müssen alle schützenswerten Informationen auf geeignete Weise vernichtet werden. Dazu sollten der Gerätespeicher und die gegebenenfalls vorhandene Speicherkarte mit einer speziellen Software gelöscht werden. Das Gerät ist auf den Werkszustand zurückzusetzen. Außerdem muss überprüft werden, ob alle Daten auch wirklich gelöscht wurden, dazu kann der Verantwortliche spezielle Computer-Forensik-Software und Geräte einsetzen. Werden mittels forensischem Ansatz dennoch entsprechend kritische Daten gefunden und es existiert für das spezielle Mobiltelefon keine Methode zum sicheren Löschen, wird empfohlen, das Gerät zu vernichten. Wird nur die externe Speicherkarte ausgesondert oder entsorgt, sollte M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* beachtet werden.

Soll ein Smartphone, Tablet oder PDA verkauft werden, bei dem durch Maßnahmen zur Informationssicherheit der Betriebssystemkern oder das Betriebssystem verändert wurde, so sollte berücksichtigt werden, dass durch diese Maßnahme in der Regel die Garantie bzw. der Support durch den Hersteller erlischt. Daher ist zu überlegen, ob diese Maßnahmen vor einem Verkauf rückgängig gemacht werden müssen.

Mobiltelefone, Smartphones, Tablets und PDAs dürfen in der Regel nicht über den Hausmüll entsorgt werden. Entsprechende Regelungen zur Entsorgung müssen beachtet und kontrolliert werden.

Prüffragen:

- Ist organisatorisch sichergestellt, dass mobile Geräte ausschließlich kontrolliert ausgesondert werden?
- Werden Hilfsmittel vorgehalten, um Daten sicher zu löschen und das Ergebnis zu kontrollieren?

# M 4.466 Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Virenschutzprogramme für Smartphones, Tablets und PDAs haben in der Regel eine andere Schutzfunktion als ihre Pendants auf anderen Clients (siehe G 5.193 *Unzureichender Schutz vor Schadprogrammen auf Smartphones, Tablets und PDAs*).

Schutzprogramme gegen Schadsoftware müssen entsprechend dem Schutzbedürfnis der Institution und unter Berücksichtigung der Anforderungen an den Schutz vor Verlust und Diebstahl des Endgerätes (siehe M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*) ausgesucht werden. Sie sollten zentral installiert und eingerichtet werden.

Die Programme sollten täglich die Signaturdatenbank aktualisieren und mindestens einmal wöchentlich einen kompletten Scan durchführen. Da ein solcher Scan die Prozessor-Ressourcen des Endgerätes für eine gewisse Zeit stark beanspruchen kann, sollte er nur zu Zeiten stattfinden, in denen das Endgerät wenig oder gar nicht benutzt wird. Das Schutzprogramm sollte dabei alle Dateitypen untersuchen und infizierte Dateien zur späteren Analyse in den Quarantäneordner verschieben. Wenn es keine Quarantänefunktion gibt oder eine weitergehende Analyse der Schadsoftware aus anderen Gründen nicht möglich ist, sollte das Programm so eingestellt werden, dass es die infizierten Dateien sofort löscht. In jedem Fall ist über ein solches Ereignis der IT-Support beziehungsweise das Informationssicherheitsmanagement zu informieren. Das befallene Endgerät sollte so schnell wie möglich durch den IT-Betrieb genauer auf weitere Schadprogramme untersucht werden.

Wird ein Smartphone, Tablet oder PDA an einen PC angeschlossen und werden Daten auf dem mobilen Endgerät gespeichert, so sollte das Schutzprogramm die neuen Daten so schnell wie möglich untersuchen. Zudem sollte es auch neu installierte Anwendungen sofort auf Schadsoftware überprüfen und bei einem Virenfund diese deinstallieren.

Es sollte ein Virenschutzprogramm ausgesucht werden, das den Netzverkehr beim Surfen im Internet lokal auf Schadprogramme testet. Die Benutzer müssen darauf hingewiesen werden, dass sie nur mit diesem Schutz im Internet surfen dürfen. Sind die Endgeräte über VPN mit dem Netz der Institution verbunden und wird in der Institution bereits der gesamte Netzverkehr auf Schadprogramme untersucht, muss nicht zusätzlich lokal der Netzverkehr untersucht werden.

Prüffragen:

- Wurde auf dem Endgerät ein Viren-Schutzprogramm installiert, das mindestens wöchentlich alle Nutzerdaten auf Schadsoftware untersucht und täglich seine Viren-Datenbank aktualisiert?
- Ist das Viren-Schutzprogramm so konfiguriert, dass es den Webverkehr auf Schadsoftware untersucht und Infektionen abwehrt?
- Ist das Viren-Schutzprogramm so konfiguriert, dass neue Dateien und Anwendungen umgehend auf Schadsoftware untersucht und bei einem Virenfund gelöscht beziehungsweise deinstalliert werden?

# M 4.467 Auswahl von Applikationen für Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Applikationen (kurz Apps) für Smartphones, Tablets und PDAs werden in der Regel durch Online-Shops der Endgeräte- oder Betriebssystemhersteller vertrieben. In den regulären Shops werden Applikationen sowohl von großen Unternehmen als auch von einzelnen Entwicklern angeboten. Die Preise für die Applikationen sind sehr unterschiedlich und reichen von kostenlos bis in den mehrstelligen Bereich. Es stehen in der Regel für einen dienstlichen Verwendungszweck sehr viele Applikationen zu Verfügung.

Daneben gibt es noch einige Online-Shops, auf die in der Regel nur über Umwege zugegriffen werden kann, indem entweder ein "Jailbreak" (bei iPhone und iPad) durchgeführt wird oder bei Android in den Einstellungen die Installation aus unbekannten Quellen zugelassen wird. Ein Jailbreak sollte in keinem Fall ausgeführt werden und die Installation aus unbekannten Quellen sollte nur nach eingehender Prüfung der Quelle für einzelne Anwendungen ermöglicht werden.

Applikationen für Smartphones, Tablets und PDAs müssen entsprechend dem Einsatzzweck dieser Endgeräte und dem Schutzbedürfnis der Informationen auf dem Endgerät ausgewählt und vor dem Einsatz getestet werden. Deshalb sollte der IT-Betrieb vor der Installation eine Liste mit gewünschten Funktionen und Eigenschaften erstellen. Zudem sind Kriterien zu definieren, die Applikationen auf keinen Fall besitzen dürfen. Hierunter fällt beispielsweise das unbefugte Versenden des Adressbuches an Adresshändler. Anhand der Vorgaben sollten die infrage kommenden Applikationen auf Nutzerkommentare und Tests durch andere Stellen hin untersucht werden, um festzustellen, ob sie zuverlässig arbeiten und ob Sicherheitsupdates zeitnah zur Verfügung stehen. Danach sollten die jeweiligen Applikationen durch den IT-Betrieb getestet und überprüft werden und erst dann an die Benutzer ausgerollt werden. Es sollte überlegt werden, einen internen Shop für Anwendungen bereitzustellen, über den die Applikationen bezogen werden können.

Wenn es keine Applikationen gibt, die den Qualitäts- oder Sicherheitsanforderungen genügen, müssen die Anwendungen selbst entwickelt werden. Hierfür ist der Baustein B 5.25 *Allgemeine Anwendungen* zu berücksichtigen. Je nach Lizenz einer Anwendung ist es auch möglich, diese den eigenen Bedürfnissen anzupassen und beispielsweise kritische Programmaufrufe, wie etwa zu Werbeservern, Versenden des Adressbuches, grundlose GPS-Lokalisierung auszuschalten. Dies kann eine preiswerte Alternative zur Eigenentwicklung sein.

Wenn die Benutzer weitere Applikationen wünschen, die nicht oder nicht nur dienstlichen Zwecken dienen, sollte es auch dafür einheitliche Regeln geben. Wenn diese Programme, z. B. Kartenspiele oder Sudoku, die Informationssicherheit nicht gefährden und vom Mitarbeiter selbst bezahlt werden, kann die Applikation in der Regel erlaubt werden. Sollte dies nicht der Fall sein, ist dem Mitarbeiter die Entscheidung plausibel zu erklären, damit sie nicht umgangen wird.

Prüffragen:

- Werden Applikationen für die Endgeräte gezielt ausgesucht, angepasst und vor dem Einsatz getestet?

# M 4.468 Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter IT

Werden Smartphones, Tablets oder PDAs dienstlich und privat benutzt, sollten beide Bereiche strikt getrennt werden. Dies ist auf verschiedene Arten möglich:

- Im einfachsten Fall wird auf den Geräten eine Applikation installiert, die einen Datencontainer mit allen dienstlichen Daten und Zugängen verwaltet. Diese Applikation muss für sämtliche dienstliche Tätigkeiten, wie E-Mail, Termine, Kontakte, Aufgaben, ausgelegt sein, einen eigenen Browser beinhalten und selbsttätig eine verschlüsselte Verbindung zur Institution aufbauen. Die Trennung zwischen den verschiedenen Applikationen erfolgt allerdings ausschließlich durch das Betriebssystem. Daher ist die Wirksamkeit dieser Trennung vom eingesetzten Betriebssystem und dessen Zugriffskontrollmöglichkeiten (Mandatory Access Control, MAC) abhängig und somit von System zu System unterschiedlich.
  Für die Datencontainer-Variante muss in der Regel nicht in das Betriebssystem selbst eingegriffen werden. Sie ist für verschiedene Betriebssysteme erhältlich. Unabhängig von welchem Hersteller eine Applikation für die Trennung zwischen privaten und dienstlichen Daten eingesetzt wird, sollte diese die dienstlichen Daten im Container verschlüsseln und so bei privater Nutzung des Endgerätes den Zugriff auf die Daten durch andere, gegebenenfalls bösartige Applikationen verhindern.
  Es kann zudem sinnvoll sein, dass der IT-Betrieb zusammen mit dem Sicherheitsmanagement eine Ausschlussliste ("Blacklist") von Anwendungen erstellt, die Funktionen oder Rechte besitzen, durch die die Informationssicherheit der dienstlichen Anwendungen gefährdet werden könnte.
  Zusätzlich sollten sich Benutzer vor einem Zugriff auf den Container erfolgreich authentisieren müssen. Verbindungen zum Netz der Institution müssen kryptografisch abgesichert werden. Lösungen, die dies nicht unterstützen, bieten keinen hinreichenden Schutz und sollten daher nicht eingesetzt werden.
- Eine andere Möglichkeit, private und dienstliche Bereiche auf Endgeräten zu trennen, ist, die Informationen auch bei der Verarbeitung auf den Servern der Institution zu belassen. In diesem Fall wird auf dem Client lediglich eine Oberfläche bereitgestellt, mit der über eine abgesicherte Netzverbindung die Anwendung auf einem Server der Institution bedient wird. Das entsprechende Programm auf dem Endgerät muss dabei so konfiguriert werden, dass die Daten nicht lokal gespeichert werden können. Solche Thin-Clients oder serverbasierten Lösungen sind auch im Desktop-Bereich seit Längerem im Einsatz. Damit eine serverbasierte Lösung funktionieren kann, muss jedoch zu jedem Nutzungszeitpunkt eine ausreichend dimensionierte Internetverbindung verfügbar sein. Ferner muss der Dienst auf die Randbedingungen eines Smartphones oder Tablets, zum Beispiel berührungsempfindlicher Touch-Screen statt Maus und Tastatur, angepasst sein.
- Eine weitere Option, besteht darin, die beiden Bereiche als unterschiedliche virtuelle Maschinen auf einem Gerät zu betreiben. Im Gegensatz zur Datencontainer-Variante wird bei der Virtualisierung der private und dienstliche Bereich nicht auf Anwendungsebene, sondern auf Betriebssystemebene getrennt. Dadurch werden die Schnittstellen entfernt, die sonst

zwischen den Anwendungen durch das Betriebssystem mit seinen vorhandenen Zugriffskontroll-Mechanismen bereitgestellt werden. Ein Datenaustausch zwischen beiden virtuellen Maschinen ist nur über die tiefer liegende Virtualisierungsschicht in Form des Hypervisors (auch Virtual Machine Monitor, VMM) möglich. Zudem können in den einzelnen virtuellen Bereichen jeweils eigene Anwendungen installiert und getrennt voneinander betrieben werden. So kann auch dem Bedürfnis der Benutzer Rechnung getragen werden, eigene Apps zu installieren und zu benutzen. Eine Ausschlussliste für Anwendungen ist in diesem Fall in der Regel nicht nötig, da die Anwendungen nur in einer virtuellen Maschine arbeiten und somit Anwendungen im privaten Bereich nicht auf die Daten und Anwendungen im dienstlichen Bereich zugreifen können.

Jede Institution muss prüfen, welche der dargestellten Lösungen dem Schutzbedarf der verarbeiteten Informationen entspricht und der Sicherheitsstrategie der Institution angemessen ist. Generell sollten noch folgende Vor- bzw. Nachteile in die Entscheidungsfindung einfließen:

- Eine Virtualisierungslösung bietet bei entsprechender Qualität des Hypervisors ein höheres Maß an Sicherheit als eine Container-Lösung.
- Bei einer Virtualisierungslösung muss sehr tief in das Betriebssystem eingegriffen werden oder es muss sogar ausgetauscht werden. Viele Gerätehersteller verbieten das und unterbinden es mit technischen Maßnahmen. Auch erlischt in der Regel mit einem solchen Eingriff in das Betriebssystem die Garantie auf das Endgerät.
- Eine Virtualisierungslösung erhöht oft den Stromverbrauch deutlich, sodass der Akku im Vergleich zu einem Gerät ohne Virtualisierung schneller entlädt.
- Eine Virtualisierungslösung ist nicht auf allen Endgeräten realisierbar, da einige Gerätetreiber nicht zur Verfügung stehen.
- Eine Container-Lösung bietet zwar ein geringeres Maß an Sicherheit als die Virtualisierung, aber im Gegenzug wird nicht so tief in das Betriebssystem eingegriffen, sodass die Gewährleistung für das Endgerät in der Regel nicht erlischt.
- Sowohl bei der Container- als auch bei der Virtualisierungslösung können bei Datensicherungen durch die Institution unbeabsichtigt private Daten mit einbezogen werden. Daher muss für die Umsetzung dieser Maßnahme in der Regel auch der Datenschutzbeauftragte hinzugezogen werden. Bei der Virtualisierungslösung ist das unbeabsichtigte Erheben personenbezogener Daten deutlich unwahrscheinlicher, da hier die Trennung zwischen privaten und dienstlichen Bereich strikter umgesetzt ist. Bei der Thin-Client-Lösung ist dies hingegen ausgeschlossen, da keine dienstlichen Daten auf dem Endgerät gespeichert und daher auch nicht gesichert werden müssen.
- Eine Thin-Client-Lösung setzt eine durchgehend verfügbare und ausreichend dimensionierte Internetverbindung voraus. Dies ist in Deutschland nicht flächendeckend gewährleistet, und im Ausland entstehen durch Daten-Roaming in der Regel hohe Kosten. Kurzzeitige Verbindungsausfälle können die Anwendungen auf dem Server beeinträchtigen und gegebenenfalls werden sogar Daten zerstört. Zudem steigt durch die dauerhafte Datenverbindung der Stromverbrauch erheblich an, wodurch die Betriebsdauer bis zum nächsten Aufladen verkürzt wird.

Prüffragen:

- Werden auf den mobilen Endgeräten dienstliche und private Daten durch einen geschützten Container oder durch eine Virtualisierungslösung voneinander getrennt?

- Wird der Datenschutzbeauftragte in die Umsetzung der Maßnahmen zur Trennung von dienstlichen und privaten Daten einbezogen?

# M 4.469 Abwehr von eingeschleusten GSM-Codes auf Endgeräten mit Telefonfunktion

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter IT

Die Menge an GSM-Codes und ihre Funktion ist herstellerspezifisch für jedes Endgerät anders. In der Regel lassen sich GSM-Codes aber nicht generell abschalten. Damit nicht unbefugt GSM-Codes auf Endgeräten mit Telefonfunktion eingeschleust werden, müssen die folgenden Empfehlungen umgesetzt werden.

Um zu verhindern, dass ein Angreifer GSM-Codes direkt auf dem Endgerät eingibt, sollte das Endgerät nie unbeaufsichtigt sein. Außerdem muss die Code-Sperre aktiv sein.

Um zu verhindern, dass GSM-Codes von Webseiten im Internet auf dem Endgerät ausgeführt werden, müssen Programme installiert sein, die lokal die besuchten Internetseiten durchsuchen und entsprechende GSM-Codes herausfiltern. Dafür gibt es am Markt entsprechende Anwendungen. Diese Filterfunktion ist häufig auch in Virenschutzprogrammen für Smartphones, Tablets und PDAs integriert.

Um zu verhindern, dass GSM-Codes über die Near-Field-Communication-(NFC)-Schnittstelle oder über QR-Code eingeschleust werden, müssen die Applikationen auf dem Endgerät so konfiguriert sein, dass sie die über NFC oder aus QR-Code empfangenen Daten nicht sofort interpretieren und ausführen, sondern erst den Benutzer über den Inhalt der empfangenen Daten informieren und die Ausführung durch ihn bestätigen lassen. Die Benutzer müssen dahingehend sensibilisiert werden, dass sie jede Anfrage auch wirklich prüfen und GSM-Codes immer ablehnen. Dafür muss ihnen vermittelt werden, dass ein GSM-Code mit tel: beginnt und eine URL mit HTTP:// oder HTTPS://.

Prüffragen:

- Ist auf dem Endgerät eine Code-Sperre eingerichtet?
- Verfügt das Endgerät über eine Anwendung, die den Webverkehr auf GSM-Codes hin untersucht und diese Codes herausfiltert?
- Sind auf dem Endgerät nur solche Programme für NFC oder QR-Codes installiert, die den Nutzer über den Inhalt der empfangenen Daten informieren und eine Bestätigung für die Ausführung verlangen?

# M 4.470 Grundlagenwissen zu Windows 8

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Client-Betriebssystem Windows 8 von Microsoft stellt grundsätzlich eine Weiterentwicklung von Windows 7 dar. Darüber hinaus ist es jedoch das erste Betriebssystem der Windows-Familie, das für den Einsatz sowohl auf klassischen PC-Systemen als auch auf Tablet-PCs entwickelt wurde.

Auf der einen Seite wurden erhebliche Teile der Codebasis von Windows Vista und Windows 7 übernommen, sodass Anwendungen grundsätzlich weiter verwendet werden können. Gleichzeitig kam aber eine weitere Schicht des Betriebssystems hinzu, deren Oberfläche "Modern UI" (früher "Metro" genannt) für Touch-Geräte optimiert ist, sich eine Codebasis mit dem ebenfalls neuen Windows Phone 8 teilt und nicht binärkompatibel zum "klassischen" Teil von Windows ist.

Die Ausgabe "Windows RT" enthält nur den "Modern"-Teil und ist bis einschließlich der Version 8.1 ausschließlich auf günstigen ARM-Prozessoren ausführbar. Das eigentliche Windows 8 ist im Gegensatz dazu auf Intel- oder AMD-Prozessoren (x86/x64) eigenständig installierbar und kann darüber hinaus sowohl klassische als auch Modern-UI-Anwendungen ("Apps") ausführen. Zum Teil liegen Anwendungen gleichzeitig in beiden Versionen vor (etwa der Internet Explorer).

Die Besonderheiten des Systemaufbaus führen dazu, dass viele Gefährdungen und Maßnahmen aus bereits existierenden Bausteinen der Baustein-Schicht 3 der IT-Grundschutz-Kataloge übernommen werden und, wo erforderlich, entsprechend ergänzt werden können. Hier sind insbesondere die Bausteine zu Windows XP, Vista und Windows 7 sowie Allgemeiner Client zu nennen.

Darüber hinaus gibt es neue Aspekte zu beachten, die bisherige Windows-Versionen nicht betrafen. Als Beispiel sei u. a. die "Cloud-Anbindung" erwähnt, also die zum Teil in der Grundeinstellung aktivierte oder dem Benutzer nicht bewusste Integration von Cloud-Diensten in das Betriebssystem.

Wie schon bei früheren Windows-Versionen wurden mit Windows 8 einige neue Sicherheitsfunktionen eingeführt, die neu zu betrachten und zu bewerten sind (siehe M 4.471 *Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8*).

Die von Microsoft als "Windows 8.1" herausgebrachten Aktualisierungen von Windows 8 sind im entsprechenden IT-Grundschutz-Baustein berücksichtigt.

### Editionen und deren Unterschiede

Neben der Hauptunterscheidung von Windows 8 in die ARM-basierten RT-Versionen und die klassischen PC-Versionen lassen sich die letztgenannten noch in sogenannte Editionen unterteilen (siehe M 2.559 *Beschaffung von Windows 8*). Die für den Institutionsseinsatz in Frage kommenden Editionen *Pro* und *Enterprise* unterscheiden sich untereinander wie in der nachfolgenden Tabelle aufgeführt. Keine dieser Funktionen sind in der Standard-Version von Windows 8 enthalten.

Eine wesentliche Neuerung, die nur in der Enterprise-Edition enthalten ist, ist die Funktion *Windows-To-Go*. Diese ermöglicht es, Windows 8 auf einem portablen Datenträger, z. B. einem USB-Stick, zu installieren.

| **Funktionen** | **Windows 8 Pro** | **Windows 8 Enterprise** |
|---|---|---|
| BitLocker und BitLocker To Go | x | x |
| Booten von virtueller Festplatte (VHD) | x | x |
| Hyper-V Virtualisierung | x | x |
| Domänenbeitritt | x | x |
| Gruppenrichtlinien | x | x |
| Encrypting File System (EFS) | x | x |
| Remote Desktop (Host) | x | x |
| Windows To Go | | x |
| DirectAccess | | x |
| BranchCache | | x |
| AppLocker | | x |
| VDI (Virtuelle Desktop Infrastruktur) Verbesserung, z. B. 3D-Grafik | | x |

Die Enterprise-Edition kann nur über eine Volumenlizenz oder eine Microsoft-Windows-Intune-Lizenz bezogen werden.

**Unterschiede zwischen Windows 8 und Windows 8 RT**

Obwohl beide Versionen erhebliche Gemeinsamkeiten und Übereinstimmungen aufzeigen, z. B. die Modern-UI Oberfläche, Funktionen wie Safeboot, in Teilen identischen Quellcode und Kernel, handelt es sich trotzdem um zwei eigenständige Systeme der Windows-Betriebssystem-Familie.

Im Gegensatz zu den 32-Bit- und 64-Bit-Versionen von Windows 8 für Desktops können auf den Windows-RT-Geräten ausschließlich Windows-Store-Apps installiert werden. Des Weiteren können klassische x86- oder x64-Anwendungen, die auf die Win32-API aufsetzen, nicht ausgeführt werden. Ausnahmen dieser Regel sind jedoch die vorinstallierten Versionen Office Home und Student 2013 RT.

Weitere, wesentliche Unterschiede sind:

- Windows 8 RT wird mit aktivierter Geräteverschlüsselung, aktiviertem Windows Update und Windows Defender ausgeliefert.
- Einer Domäne kann nicht beigetreten werden.
- Die Windows-RT-Version wird nur als vorinstalliertes Betriebssystem ausgeliefert, der direkte Bezug durch Endanwender ist nicht möglich.

**Modern-UI und klassische Benutzeroberfläche**

Die sichtbarste Neuerung von Windows 8 ist die sogenannte *Modern-UI* als neue Benutzeroberfläche. Sie ist für die Tablet-PC-spezifische Bedienung mit den Fingern ausgelegt, kann aber auch über die Tastatur oder Maus bedient werden.

Das Design orientiert sich an der aus Windows Phone bekannten Oberfläche.

Anwender können zwischen der *Modern-UI* und der klassischen Oberfläche wechseln. Ursprünglich wurde nach erfolgtem Systemstart die *Modern-UI* automatisch gestartet. Durch Installation eines Updates für Windows 8.1 wurde die klassische Benutzeroberfläche wieder als Standard festgelegt.

**Sicherheitsaspekte von Windows 8**

Wesentliche Sicherheitsfunktionen von Windows 8 wie BitLocker, AppLocker oder DirectAcces wurden mit Vista oder Windows 7 eingeführt und der Funktionsumfang unter Windows 8 erweitert.

Darüber hinaus wurden mit Windows 8 aber auch gänzlich neue Sicherheitsfunktionen wie die Unterstützung für *Secure Boot* oder *Smart Screen* eingeführt.

Teilweise sind bei diesen Neuerungen datenschutzrechtliche Aspekte zu berücksichtigen (siehe Maßnahme M 4.472 *Datensparsamkeit bei Windows 8*).

Weitere Informationen zu sicherheitsrelevanten Neuerungen von Windows 8 finden sich in der Maßnahme M 4.471 *Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8*.

**Entfernte Funktionen**

Über die Neuerungen von Windows 8 hinaus wurden Funktionen entfernt.

Dies betrifft einerseits die vollständige Entfernung von Programmen, andererseits die Entfernung von Optionen oder Funktionen weiterhin verfügbarer Programme. Folgende Programme und Funktionen sind in Windows 8 nicht mehr enthalten:

Sicherheitsfunktionen:

- CardSpace
- Windows-Defender: Veränderungen der Scan-Optionen

Benutzeroberfläche:

- Der "klassische" Startbutton wurde aus der Taskleiste entfernt.
- "*Zuletzt verwendete Dokumente"* sind als Folge des nicht mehr vorhandenen Startmenüs nicht mehr zentral verfügbar.
- Die Windows Desktop Gadgets sind nicht mehr verfügbar.
- Das Aero-Design ist nicht mehr verfügbar.

Multimedia:

- Der Windows DVD-Maker ist nicht mehr Bestandteil der Betriebssysteminstallation.
- Das Windows Media Center kann nur noch in ausgewählten Editionen hinzugefügt werden. Es kann darüber hinaus nicht mehr als Standard-Benutzeroberfläche verwendet werden.

Netz:

- Verschiedene Einstellungen oder Übersichten zu WLAN und Bluetooth wurden entfernt.

Windows Explorer:

- Die Funktion des Aktenkoffers ist nicht mehr verfügbar.

Spiele:

- Alle bei Windows 7 installierten Spiele wurden entfernt. Verknüpfungen zum Spiele-Explorer wurden ebenfalls entfernt.

# M 4.471 Übersicht über neue, sicherheitsrelevante Funktionen in Windows 8

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Windows 8 stellt aus sicherheitstechnischer Sicht einerseits eine konsequente Weiterentwicklung der Windows-Vista- und Windows-7-Betriebssysteme-Systeme dar, darüber hinaus wurden aber auch gänzlich neue Sicherheitsfunktionen eingeführt. Dies ist teilweise durch den Aufbau des Systems bedingt: So können die neuen Apps nur über den App-Store installiert werden, eine Absicherung des Boot-Prozesses für x86-Prozessoren auf UEFI-Systemen erfolgt über Secure Boot. Teilweise haben jedoch auch vollständig neue Funktionen in das System Einzug gehalten (z. B. Windows To Go mit seinen sicherheitsrelevanten Konfigurationsmöglichkeiten).

Die folgende Übersicht zeigt die wesentlichen, sicherheitsrelevanten Neuerungen von Windows 8 auf und verweist jeweils auf Maßnahmen mit näheren Einzelheiten. Die zwischenzeitlich von Microsoft als "Windows 8.1" herausgebrachten Aktualisierungen von Windows 8 sind entsprechend berücksichtigt.

**Schutz der Pre-Boot- und Bootphase**

Eine der wichtigsten Neuerungen des Windows-8-Betriebssystems ist die Absicherung des Start-Vorgangs des Systems. Die Absicherung erfolgt in verschiedenen Phasen des Systemstarts. Für die Absicherung des Boot-Prozesses ist UEFI (Unified Extensible Firmware Interface) anstelle des bisher üblichen BIOS Voraussetzung (siehe M 2.559 *Beschaffung von Windows 8*). Folgende Funktionen sichern den Systemstart ab:

Secure Boot unter Windows 8

Secure Boot wurde im Rahmen der Version 2.3.1 des Unified Extensible Firmware Interface (UEFI) definiert. Es soll unterbinden, dass nicht erwünschte Software (z. B. Schadsoftware) ausgeführt wird. Im Secure-Boot-Modus lädt die Firmware des Systems ausschließlich UEFI-Bootloader, deren digitale Signatur oder Hash vorab gespeichert worden ist. Das Betriebssystem darf dafür allerdings nicht im BIOS-Modus installiert worden sein.

ELAM (Early Launch Antimalware)

Der ELAM-Treiber (Early Launch Anti Malware) ist der erste Treiber, der nach dem Windows-Kernel initialisiert wird. Dadurch können alle weiteren Treiber auf Rootkits überprüft werden. Die Überwachung erfolgt allerdings auf der Basis von Hash-Werten bekannter Rootkits oder Bootkits. Neue und unbekannte Rootkits können somit nicht erkannt werden.

Measured Boot

Measured Boot protokolliert alle geladenen Software-Komponenten (Firmware und Treiber) beim Start des Systems. Das entstandene Protokoll kann dann von einer weiteren Software, z. B. einer Antivirus-Software, oder von einem Netzdienst zur Überprüfung des Systemzustands verwendet werden.

**Schutz vor Schadsoftware und weitere Sicherheitsfunktionen**

Windows Defender als vollständige *Security-Suite* ist nun integraler Bestandteil des Windows-8-Systems.

Trotz der integrierten Sicherheitsfunktion sollte in einer Institution die Notwendigkeit einer dedizierten *Security-Suite* über Windows Defender hinaus geprüft werden.

Weitere neue Sicherheitsfunktionen sind:

- Malicious Software Removal Tool
- SmartScreen: Diese Funktion zur Überwachung von Programmaufrufen ist nun systemweit vorhanden. Beim Einsatz von SmartScreen sollten Datenschutzaspekte berücksichtigt werden (siehe Maßnahme M 4.472 *Datensparsamkeit bei Windows 8 Gewährleistung des Datenschutzes*).
- Möglichkeit des Einsatzes der Funktion "Family Safety" für Arbeitsplätze mit beschränkten Rechten (z. B. Kiosk-Modus). Diese Funktion ermöglicht die Einschränkung durch Nutzung eines Web-Filters oder Ausführungseinschränkung von Anwendungen

**Windows To Go**

Mobile Benutzer einer Institution können über die neu geschaffene Windows-To-Go-Installation ihre persönliche Umgebung auf einem USB-Stick installieren.

Aus Sicherheitsgründen ist unter Windows To Go standardmäßig der Zugriff auf USB-Sticks oder Festplatten deaktiviert. Dadurch wird das Risiko, sich durch externe Peripheriegeräte mit Schadsoftware zu infizieren, erheblich reduziert.

Dateien oder Anwendungen sind jedoch für den Benutzer verfügbar.

**Neues in den Gruppenrichtlinien**

Mit der Einführung von Windows 8 und dem korrespondierenden Windows 2012 Server wurden neue Gruppenrichtlinienobjekte (GPO) geschaffen, bzw. bestehende wesentlich erweitert.

Es gilt zu beachten, dass die neuen GPOs in der Regel nur in Verbindung mit einem Active Directory auf einem Windows 2012 Server anwendbar sind.

Wichtige neue GPOs für Windows 8 sind unter anderem Möglichkeiten zur Nutzung oder Sperrung der Optionen "PIN Logon" und "Picture Password" als Login-Methoden. Darüber hinaus wurde die biometrische Sicherheit (Windows Biometric Framework) erweitert.

Über die Dynamic Access Control (DAC) können Daten automatisch oder manuell klassifiziert werden.

Dies ermöglicht die Überwachung von Zugriffen. Beispielsweise kann der Zugriff auf vertrauliche Informationen nachvollzogen werden.

**Neues in der Sicherheitsüberwachung**

Als Folge der neuen Sicherheitsfunktion *Dynamische Zugriffssteuerung* (englisch DAC - *Dynamic Access Control)* kann ein Benutzer über unterschiedliche Berechtigungen verfügen, abhängig davon, ob er von einem Desktop oder von einem Laptop über ein VPN-Netz auf die Ressourcen der Institution zugreift.

Für die Überwachung dieser neuen Funktion stehen in Windows 8 und Windows Server 2012 folgende neue oder erweiterte Überwachungsoptionen zur Verfügung:

Dateizugriffsüberwachung

Beim Einsatz der Dateizugriffsüberwachung werden nun auch Informationen zu den Attributen der Datei, auf die zugegriffen wurde, protokolliert.

Erweiterte Benutzeranmeldungsüberwachung

Windows-Server- und Windows-Client-Systeme bieten die Möglichkeit, Benutzeranmeldungen zu überwachen. Sobald sich ein Anwender lokal oder über ein Netz anmeldet, generiert das Windows-Betriebssystem ein Überwachungsereignis.

Ab Windows Server 2012 und Windows 8 werden erweiterte Informationen durch eine neue Ereignis-ID zusätzlich zum Anmeldeereignis erfasst. So werden z. B. bei einem Dateizugriff die Attribute der Datei, auf die zugegriffen wird, protokolliert.

Ausdrucksbasierte Überwachungsrichtlinien

Für eine Datei oder einen Ordner können nun auch ausdrucksbasierte Überwachungsrichtlinien erstellt werden. Hierfür können verschiedene Ereignisse ausgewählt und zusammengefasst werden, bei deren Eintreten ein entsprechender Eintrag im Protokoll erzeugt wird.

Ein Beispiel einer solchen ausdrucksbasierten Überwachungsrichtlinie ist die Protokollierung der Dateizugriffe durch Externe auf Daten, für die keine Berechtigungen bestehen.

Überwachen von Wechselmedien

Beim Zugriff auf ein Wechselmedium wird nun ein Überwachungsereignis generiert.

**DirectAccess**

Bisher war für den Einsatz von DirectAccess für den VPN-Zugriff im internen Netz zwingend der Einsatz von IPv6 erforderlich. Ab Windows 8 ist nun auch der Einsatz von DirectAccess in Verbindung mit IPv4 im internen Netz möglich.

**Virtuelle Smartcards**

Mit Windows 8 können nun virtuelle Smartcards eingesetzt werden. Diese emulieren die Funktionalität physikalischer Smartcards, nutzen jedoch den TPM-Chip des Systems.

# M 4.472 Datensparsamkeit bei Windows 8

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die neu eingeführten Funktionen von Windows 8 bringen zum Teil einen umfangreichen Zugriff auf System- oder Benutzerdaten mit sich. Beispiele hierfür sind die direkte Speicherung von Daten in der Cloud durch Apps und die mit Windows 8 erweiterte Sicherheitsfunktion SmartScreen (siehe G 2.203 *Integrierte Cloud-Funktionalität*).

Die vom Betriebssystem oder von Anwendungen und Apps benötigten Informationen werden häufig automatisiert während der Nutzung erfasst, ohne dass die Benutzer dies wahrnehmen. Es ist darüber hinaus für die Benutzer oft nicht möglich, den Umfang und die Synchronisationsintervalle zu übermittelnder Daten festzulegen.

Um einer angemessenen Vertraulichkeit und datenschutzrechtlichen Anforderungen gerecht zu werden, sollte daher im Vorfeld des Einsatzes überprüft werden, ob die genutzten Funktionen von Windows 8 sowie die eingesetzten Anwendungen und Apps im Einklang mit gesetzlichen und organisationsspezifischen Vorgaben stehen.

Einige Beispiele solcher Anwendungen oder Systemfunktionen, deren Konformität zum Datenschutz zu verifizieren sind, sind im Folgenden dargestellt.

**Systemanmeldung mit einem Microsoft-Konto**

Neben der klassischen Anmeldung an einem System über ein lokales oder Active-Directory-basiertes Konto ist unter Windows 8 die Anmeldung am System auch über ein sogenanntes Microsoft-Konto möglich. Bei dieser Variante meldet Windows den Benutzer bei der Nutzung von Apps und dazugehörigen Webseiten automatisch an.

Ein solches Konto ist erforderlich, um Apps zu installieren und auf den Windows Store von Microsoft zuzugreifen. Die Einrichtung eines Kontos erfordert jedoch nicht zwingend, dass auch die Anmeldung an Windows auf das Microsoft-Konto-Verfahren umgestellt wird. Im betrieblichen Umfeld sollte daher die Anmeldung über das Microsoft-Konto nicht verwendet werden.

Sofern ein Microsoft-Konto angelegt werden muss, um bestimmte Apps zu nutzen, sollten die dabei bei Microsoft hinterlegten Angaben zum Benutzer auf das notwendige Minimum beschränkt werden.

**SmartScreen**

Zur Absicherung des Internet-Explorers hat Microsoft den SmartScreen-Filter entwickelt, der aufgerufene Webseiten blockiert, wenn sie als Plattform für Phishing-Angriffe oder als Verteiler von Schadsoftware bekannt sind. Diese Funktion wurde in Windows 8 erweitert. Neben der Überwachung des Internet Explorers warnt der Filter nun gegebenenfalls auch bei der Ausführung von Programmen, die sich bei der Darstellung von Webinhalten auf das Betriebssystem abstützen (z. B. Apps oder Darstellung von HTML-Inhalten in Office/Outlook), oder die von einem externen Laufwerk ausgeführt werden. Voraussetzung für die Nutzung des Filters ist jedoch eine bestehende Inter-

net-Verbindung, da wesentliche Information zu Programmen und möglichem Schadcode in zentralen Datenbanken vorgehalten wird. Dadurch nutzt der Smartscreen stets aktuelle Informationen über als schädlich erkannte Webseiten.

Diese Funktion bedeutet jedoch auch, dass erhebliche Informationen über das genutzte IT-System an zentrale Dienste übermittelt und zumindest zeitweise auf den Servern von Microsoft gespeichert werden. Beispiele dafür sind Name und Version sowie kryptographische Prüfsummen (Hashwerte) von auf dem PC ausgeführten Programmen sowie die IP-Adresse des Quell-Systems.

Die SmartScreen-Funktion kann unter *Systemsteuerung* | *System und Sicherheit* | *Wartungscenter* | *Windows Smartscreen-Einstellungen ändern* vollständig deaktiviert werden. Dies sollte erfolgen, wenn der Schutz der anfallenden Nutzungsdaten vor Missbrauch die Gefahr einer Infektion beim Web-Zugriff überwiegt.

**Apps und (un)bewusste Cloud-Nutzung**

Wenn ein Microsoft-Konto erstellt wird, wird diesem automatisch kostenloser Speicherplatz in der Cloud zugewiesen.

Die zugrundeliegende Cloud von Microsoft hieß bis Februar 2014 SkyDrive und wurde dann in OneDrive umbenannt.

| **Alter Name** | **Neuer Name** |
|---|---|
| SkyDrive | OneDrive |
| SkyDrive Pro | OneDrive for Business |

Bei Anmeldung über das Microsoft-Konto werden mindestens die folgenden Daten in OneDrive gespeichert:

- Fotos, die mit dem PC aufgenommen wurden,
- Dokumente (OneDrive wird als Standardspeicherort beim Speichern ausgewählt),
- Sicherungskopien der PC-Einstellungen.

Falls die Anmeldung am PC nicht über das Microsoft-Konto erfolgt, kann die Synchronisation nur über die sogenannte OneDrive-App erfolgen, diese ist aber seit Windows 8.1 integraler Bestandteil des Systems.

Darüber hinaus speichern auch verschiedene Apps Daten in Cloud-Diensten. Teilweise ist dabei es dabei nicht möglich, den Umfang oder die Dauer der Speicherung zu beeinflussen.

**"Nach-Hause-Telefonieren" von Apps**

Die Installation von Apps birgt die Gefahr der sogenannten "Nach-Hause-Telefonieren"-Funktion (englisch "Phone home"). Dies bedeutet, dass Apps automatisch Kontakt zu den Servern des Herstellers aufnehmen. In der Regel ist dies eine gewünschte und elementare Funktion einer App, z. B. indem jeweils aktuelle Nachrichten heruntergeladen und angezeigt werden. Allerdings ist es häufig nicht möglich, eine genaue Aussage über Art und Umfang der dabei zum Anbieter übermittelten Daten zu treffen.

Neben dem Risiko ungewollter Datenverbindungen und den damit verbundenen Kosten besteht die Möglichkeit, dass Apps auf personenbezogene Daten des Systems zugreifen und diese Informationen an den Hersteller übertragen.

**Prüfung von Anwendungen und Apps**

Bevor eine Anwendung oder App zur Nutzung innerhalb der Institution freigegeben wird, sollte daher eine sorgfältige Prüfung darüber erfolgen:

- welche Daten an externe Cloud-Anbieter übertragen werden,
- wie Daten vom Hersteller der App synchronisiert werden, und welche Daten dabei an den Hersteller übertragen werden.

Diese Aspekte sollten insbesondere bei der Auswahl alternativer Anwendungen oder Apps für einen Einsatzzweck berücksichtigt werden. Auf den Einsatz von Apps mit unerwünschter oder unnötig umfangreicher Datenübertragung an Dritte sollte nach Möglichkeit verzichtet werden.

Prüffragen:

- Erfolgt die Anmeldung am Windows-System über ein lokales oder Active-Directory-basiertes Konto und nicht mit einem Microsoft-Konto?
- Wurden Microsoft-Konten für die Nutzer nicht oder nur mit den unbedingt erforderlichen Angaben zu den Personen angelegt?
- Wurde die Verträglichkeit der SmartScreen Funktion zu internen oder externen Datenschutzvorgaben überprüft und bewertet?
- Wurde bei der Auswahl von Anwendungen und Apps die Minimierung der Datenübertragung an Dritte als Kriterium berücksichtigt?
- Sind die notwendigen Kommunikationsbeziehungen und übermittelten Daten der Anwendungen bekannt und dokumentiert? Wurden die Anwendungen so konfiguriert, dass nur ein notwendiges Minimum an Daten übertragen wird?

# M 4.473 Schutz vor Abhören von XML-Transportcontainern in einer SOA

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT, Benutzer

Wenn innerhalb einer serviceorientierten Architektur (SOA) vertrauliche Daten übertragen werden, müssen zu ihrem Schutz geeignete Verschlüsselungsmethoden eingesetzt werden. Diese verschlüsseln nach Bedarf entweder die gesamte Nachricht oder nur bestimmte Elemente, zum Beispiel mit XML-Encryption (XMLENC nach W3C).

Es ist sicherzustellen, dass die Art der eingesetzten Verschlüsselung (z. B. Verschlüsselung der ganzen Nachricht, eines Unterelements oder des Inhalts eines XML-Elements) auch dem gewünschten Vertraulichkeitsschutz entspricht.

Zudem ist darauf zu achten, dass generierte Nachrichten nur so viele Metainformationen wie nötig enthalten, sodass einem potenziellen Angreifer keine Angriffspunkte angeboten werden.

Prüffragen:

- Wird XML verschlüsselt?
- Wird mit der verwendeten Verschlüsselung (ganze Nachricht oder bestimmte Elemente) der gewünschte Vertraulichkeitsschutz erreicht?

# M 4.474 Schutz vor Schwachstellen in Backend-Anwendungen einer SOA

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Durch vorgeschaltete Authentisierungs- und Autorisierungsmechanismen sollten zunächst die Angriffschancen auf die Backend-Anwendungen einer serviceorientierten Architektur (SOA) eingeschränkt werden. Außerdem ist zu gewährleisten, dass bereits authentisierte und autorisierte Nutzer keine Angriffe auf diese Systeme durchführen können.

Die Backend-Anwendungen sind durch regelmäßige Updates abzusichern. Zudem können XML-Nachrichten gefiltert werden, um zu unterbinden, dass schädlicher Code übermittelt wird bzw. kritische Kommandos ausgeführt werden.

Bei der Auswahl des XML-Transportcontainers ist deshalb darauf zu achten, dass die Sicherungsmittel in einer Weise verwendet werden können, die eine Manipulation des Inhaltes unterbinden.

Prüffragen:

- Werden die Backend-Anwendungen durch regelmäßige Updates abgesichert?
- Werden XML-Nachrichten bezüglich Schadcode und kritischen Kommandos gefiltert?

# M 4.475 Schutz vor Spoofing-Angriffen auf Identitätsdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Um Spoofing-Angriffe auf Identitätsdienste zu verhindern, sollte ein Benutzer nur die Dienste aufrufen, denen er vertrauen kann. Dies kann für ihn beispielsweise am gültigen Zertifikat für den jeweiligen Dienst erkennbar sein bzw. durch den automatischen Nachweis einer vorgegebenen Identität sichergestellt werden (*Service Authentication*). Der Benutzer sollte bei jedem Dienstzugriff die bereitgestellten Vertrauensmerkmale kritisch prüfen.

Prüffragen:

- Ist sichergestellt, dass nur Identitätsdienste mit gültigem Zertifikat genutzt werden?

# M 4.476 Schutz einer WS-Notification-Subscription im Broker

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein *NotificationConsumer* kann eine *Subscription* bei einem *NotificationBroker* entweder für sich selbst oder für einen Dritten vornehmen. Standardmäßig informiert ein Broker einen dritten Consumer auch nicht über eine für ihn vorgenommene Subscription.

Damit ein Angreifer diesen Mechanismus nicht missbrauchen kann, muss sich der platzierende Consumer gegenüber dem Broker authentisieren. Geschieht dies nicht, sollte der Broker die Subscription prinzipiell ablehnen.

Bei einer erfolgreichen Subscription muss der Broker außerdem entweder eine URI (Uniform Resource Identifier) oder über WS-Resource eine Nachricht über die vorgenommene Platzierung zurückliefern. Mit dieser Information kann der Consumer den Status seiner Subscription überprüfen. Auch diese Antwort ist in jedem Fall zu authentisieren.

Eine *Subscription* wird von einem *NotificationConsumer* einmalig platziert und dauert normalerweise so lange, bis derselbe Consumer diese beim *NotificationBroker* wieder löscht. In einer bestehenden Subscription wird der Consumer vom Broker nicht darüber informiert, ob eine ehemals platzierte Subscription noch weiterhin existiert. Für den Consumer ist daher nicht erkenntlich, ob ein Broker nur deshalb nicht mehr reagiert, weil keine Daten für Nachrichten (*Notification*) vorliegen oder weil keine Subscription mehr vorhanden ist.

Prüffragen:

- Ist sichergestellt, dass sich NotificationConsumer und NotificationBroker gegenseitig authentisieren?

# M 4.477 Schutz einer WS-Notification

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein *NotificationBroker* ist dafür zuständig, eine Nachricht (*Notification*) zuzustellen. Er wertet zu diesem Zweck lediglich das Thema (*Topic*) der Nachricht aus. Am eigentlichen Inhalt ist der Broker nicht interessiert. Deswegen kann der Inhalt einer Nachricht beispielsweise komplett verschlüsselt werden, ohne dass dies für den Broker ein Problem darstellt.

Um Nachrichten vor Manipulationen zu schützen, sind diese mindestens zu signieren. Das muss über alle Inhalte und im Falle eines XML-Labels auch für das Label-Attribut im Protokoll-Header hinweg geschehen.

Bei Bedarf können zum Schutz der Vertraulichkeit zusätzlich Elemente im Body-Bereich der Nachricht (*SOAP body*) seitens des Absenders verschlüsselt werden.

Prüffragen:

- Werden SOAP-Nachrichten (gegebenenfalls inklusive Label-Attribut) signiert?
- Werden SOAP-Nachrichten bei höherem Schutzbedarf verschlüsselt?

# M 4.478 Schlüsselmittelverwaltung bei SOA

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In einer serviceorientierten Architektur (SOA) müssen sich Dienste in gleicher Weise identifizieren können wie Nutzer oder Rollen. Dies bedingt, dass der zugehörige Identitätsschutz mit einem automatisch generierten asymmetrischen Schlüsselpaar und der nachfolgenden automatischen Zertifikatsgenerierung und -publizierung verbunden ist.

Um Angriffe auf den damit verbundenen Zertifizierungsprozess zu erschweren, sind die Zertifikatsprozesse in einem abgeschotteten "Trusted Key Store" unterzubringen. Der private Schlüssel (Private Key) des SOA-Dienstes darf den "Trusted Key Store" nicht verlassen. Zur Verwaltung der Zertifizierungsprozesse wird jeweils dem SOA-Dienst ein Key-Management-Service zugeordnet (*XML Key Management Service, XKMS*). SOA-Dienst und XKMS kommunizieren lokal und reduzieren damit die Angriffsmöglichkeit auf die verwendeten Schlüsselelemente. Als lokale Zertifizierungsstelle muss der XKMS den öffentlichen Schlüssel (Public Key) des SOA-Dienstes signieren und ihn als gültig in der eigenen Informationsdomäne publizieren.

Prüffragen:

- Wird eine lokale Schlüsselmittelverwaltung genutzt, um die Schlüsselmittel besser gegen Angriffe zu schützen?
- Werden die veröffentlichten Schlüssel signiert?
- Bleibt der private Schlüssel des SOA-Dienstes sicher im eigenen System gespeichert?

# M 4.479 Schutz von Richtlinien in einer SOA

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In serviceorientierten Architekturen (SOA) werden Dienstzugriffe und Berechtigungen über verschiedene SOA-Plattformen hinweg mit Hilfe von Richtlinien (Policies) organisiert. Sie müssen bereits vorhanden sein, bevor ein Dienstnutzer in einer SOA-Umgebung agiert oder ein Service-Provider Informationen bzw. Dienste auf einer SOA-Plattform verfügbar macht. In einer Informationsdomäne kann nur eine Richtlinie implementiert sein. Anders ausgedrückt: eine Informationsdomäne definiert sich durch ihre Policy. Wird eine Richtlinie auf allen SOA-Plattformen einer Informationsdomäne umgesetzt, erzwingt dies, dass ein lokaler Policy-Enforcement-Point (PEP) pro SOA-Plattform verwendet wird.

Die Richtlinien müssen für alle SOA-Plattformen einer Informationsdomäne zentral verfügbar sein, z. B. in einem Service-Repository. Sie werden in der Regel in einem Web-Services-Description-Language-(WSDL)-Statement festgelegt und bereitgestellt. Durch Modifikation einer solchen WSDL-Datei auf der Provider- oder Consumer-Seite kann auf eine falsche Richtlinie geschlossen werden. Damit die Policy-Einstellungen nicht manipuliert werden können, muss ein Signaturwert "hart" an die WSDL-Datei gebunden werden, z. B. über *XML Strong Binding*.

Mehrere Informationsdomänen lassen sich so miteinander koppeln, sodass ein Dienstnutzer der Domäne A auf einen Service-Provider der Domäne B zugreifen kann. Hierbei sind zwischen den Administratoren der einzelnen Domänen die Richtlinien so abzustimmen, dass ein Dienstnutzer durch mehrere aufeinanderfolgende Zutritte zu Domänen nicht unberechtigterweise Rechte akkumuliert. Die Vorgehensweise und die daraus entstandenen Richtlinien sollten nachvollziehbar festgehalten werden.

Prüffragen:

- Werden die Policy-Einstellungen bzw. Regelungen in einer SOA gegen Manipulationen geschützt?
- Wird die SOA-Richtlinie mit nachvollziehbaren Regeln erzeugt?

# M 4.480 Schutz von WS-Resource in SOA-Umgebungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Mithilfe des OASIS-Standards "Web Services Resource" (WS-Resource) lassen sich Dienste zusätzlich schützen. So legt der Standard verschiedene Parameter fest, die angeben, ob ein Dienst nutzbar ist oder falls erforderlich gesperrt wird.

Für die Herkunft der Parameterwerte für WS-Resource gibt es zwei Möglichkeiten.

- Parameterwerte werden direkt in Verbindung mit dem dazugehörigen Dienst festgelegt, z. B. ein Dienst darf mit der Klassifikation offen, Stufe 1 oder vergleichbar benutzt werden.
- Parameterwerte werden aus anderen, außerhalb der SOA-Umgebung befindlichen Ressourcen abgeleitet, z. B. Übertragungsgeschwindigkeit eines Kommunikations-Ports. Werden im SOA-System Ressourcen verwendet, die mit einem geringeren Klassifikationsgrad als das SOA-System selbst definiert sind, ist ein Übergang von "Klassifikationsstufe 1" nach "Klassifikationsstufe 2" gegeben. Dabei werden auch Daten der Klassifikationsstufe 1 in eine Umgebung der Klassifikationsstufe 2 importiert.

Es sollte überlegt werden, die WS-Resource-Informationen durch die in Maßnahme M 4.478 *Schlüsselmittelverwaltung bei SOA* beschriebenen Empfehlungen zu schützen.

Im Falle des Überganges von "Klassifikationsstufe 1" nach "Klassifikationsstufe 2" sind zusätzliche Plausibilitätskontrollen zu integrieren, abhängig vom Normalverhalten der niedriger klassifizierten Ressource.

Prüffragen:

- Sind Maßnahmen festgelegt, die den Informationsübergang für Informationen aus WS-Resource von einem Bereich der Klassifikationsstufe 1 in einen Bereich der Klassifikationsstufe 2 schützen?
- Gibt es eine Plausibilitätskontrolle für Daten aus WS-Resource beim Übergang von einem Bereich der Klassifikationsstufe 1 in einen Bereich der Klassifikationsstufe 2?

# M 4.481 Sichere Nutzung verbindungsloser SOAP-Kommunikation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Protokollprofil SOAP über UDP wird vornehmlich aufgrund der Multicast-Adressierung verwendet. Auch schont es die Ressourcen schmalbandiger Kommunikationsmittel. SOAP-Nachrichten werden hierbei an eine anonyme Multicast-Adresse geschickt, ein Provider weiß daher in der Regel nicht, wer die Empfänger sind.

Um zu verhindern, dass Nachrichten an unberechtigte Empfänger verschickt werden, ist der entsprechende Schutz in den SOAP-Nachrichten selbst umzusetzen. Der Provider kann dies durch eine geeignete Inhaltsverschlüsselung erreichen, sodass ausschließlich berechtigte Empfänger die SOAP-Nachrichten lesen können.

Um Replay-Attacken vorzubeugen, sollten zudem Sequenzzähler im verschlüsselten Bereich der Nachricht verwendet werden.

Prüffragen:

- Sind Maßnahmen festgelegt, die verhindern, dass SOAP-Nachrichten an unberechtigte Empfänger weitergeleitet werden?
- Sind Maßnahmen festgelegt, die bei SOAP-Nachrichten eine Replay-Attacke verhindern?

# M 4.482 Hardware-Realisierung von Funktionen eingebetteter Systeme

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Planer, Entwickler, Beschaffer

Wird ein eingebettetes System entworfen, wird festgelegt, welche Funktionen auf einem programmierbaren Prozessor ablaufen sollen und welche unmittelbar in Hardware implementiert werden sollen. Die potenzielle Bandbreite bei der Hardware-Software-Partitionierung ist groß. Am einen Ende der Skala stehen universell programmierbare Mehrzweck-Prozessoren (General Purpose Processor, GPP), wie sie auch im Bereich der Arbeitsplatzrechner eingesetzt werden. Am anderen stehen hochspezialisierte digitale Hardware-Systeme welche nur ein Programm ausführen (Single Purpose Processor, SPP). Einen Mittelweg zwischen voll programmierbaren Prozessoren und reinen Hardware-Implementierungen stellen programmierbare Prozessorkerne mit anwendungsspezifischem Befehlssatz (Application Specific Instruction set Processor, ASIP) dar. Es sind Prozessoren, deren Befehlssatz für bestimmte Anwendungsarten, z. B. digitale Signalverarbeitung oder Steuerungsfunktionen optimiert wurde.

Auch bei den Hardware-Implementierungen gibt es verschiedene Abstufungen. Bei den Optionen um integrierte Schaltkreise zu implementieren, reicht die Bandbreite von Chips, die individuell für bestimmte Kunden entworfen und hergestellt werden ("Application Specific Integrated Circuit", ASIC) bis zu Chips, die zwar für spezielle Aufgaben entwickelt werden, aber so allgemein gehalten sind, dass sie in einer Vielzahl unterschiedlicher Produkte eingesetzt werden können ("Application Specific Standard Product", ASSP). Dazu kommen einige Mischformen wie z. B. Chips die auf Kundenwunsch hin vom Hersteller angepasst werden ("Customer Specific Standard Product", CSSP), Chips mit einigen vorimplementierten Elementen (englisch: "structured ASIC") und Chips mit einem vordefinierten Bereich und einem für Kundenkonfigurationen freien Bereich (englisch: "platform ASIC").

Weit verbreitet, insbesondere zur Prototypenentwicklung sind programmierbare ASICs. Die wichtigsten Vertreter dieser Technologie sind Field Programmable Gate Array (FPGA) und Complex Programmable Logic Device (CPLD). Beides sind integrierte Schaltkreise in die eine logische Schaltung programmiert werden kann, wobei damit gemeint ist, dass die Funktionsstruktur des Schaltkreises definiert wird und nicht, dass zeitliche Abläufe festgelegt werden. CPLDs weisen im Vergleich zu FPGAs eine wesentlich einfachere Struktur auf. Sie besitzen kein feinmaschiges Array von Logikblöcken und Flip-Flops, sondern nur eine konfigurierbare Schaltmatrix, die verschiedene Eingangssignale zu verschiedenen Ausgangssignalen verbinden kann. Ein CPLD ist sofort nach dem Einschalten betriebsbereit, ebenso wie ein nur einmal programmierbares FPGA. Rekonfigurierbare FPGA mit static random-access memory (SRAM)-basierenden Zellen benötigen erst einen Ladezyklus für die Konfiguration. FPGA Bausteine sind größer als CPLD Bausteine und haben einen höheren Stromverbrauch.

Programmierbare Logik-Bausteine können außerhalb des Zielsystems oder, falls die entsprechenden Schnittstellen vorhanden sind, auch innerhalb des Zielsystems programmiert werden. Sie werden oft verwendet, um einen Pro-

totypen zu entwickeln. Im produktiven System werden sie meist durch ASICs ersetzt. Eine Weiterentwicklung stellen rekonfigurierbare ASICs dar, welche sich während der Laufzeit umprogrammieren und so an aktuelle Erfordernisse anpassen können.

Die unterschiedlichen Sicherheitseigenschaften der Realisierungen in Software oder Hardware sind beim Entwurf eines eingebetteten Systems zu berücksichtigen und mit den jeweiligen Sicherheitsanforderungen in Einklang zu bringen. Festverdrahtete Algorithmen, z. B. als ASIC oder FPGA, stellen einerseits einer Manipulation der Funktionalität höhere Hürden entgegen als typische softwarebasierte Implementationen, andererseits sind sie weniger flexibel und erlauben im allgemeinen keine nachträgliche Integration zusätzlicher Sicherheitsmechanismen. Werden die Sicherheitsmechanismen allerdings von Anfang an beim Entwickeln der Hardware einbezogen, lassen sie sich effizient realisieren. Auch parallele Prozesse können sehr gut in Hardware realisiert werden, z. B. kann die virtuelle Maschine für Java nicht als Software, sondern durch einen Java-Prozessor als Hardware realisiert werden.

Wird entschieden die Funktionen in Hardware zu realisieren, ist zu beachten, dass ASICs und FPGAs unterschiedliche Stärken und Schwächen hinsichtlich der IT-Sicherheit aufweisen. Bei ASICs gibt es Risiken im Entwurf und der Fertigung. Um zu verhindern, dass ein Angreifer nicht gewollte Funktionen oder Hintertüren einbaut oder vertrauliche Informationen ausspäht, sollten die Chips entsprechend getestet werden und die Entwicklungs- und Herstellungskette sollte vertraulich sein (siehe M 2.563 *Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie eines qualifizierten Herstellers für eingebettete Systeme*). Bei FPGAs wird die Schaltung zunächst in einer Hardwarebeschreibungssprache formuliert, wobei auch fremdes geistiges Eigentum einfließen kann. Mittels spezieller Entwurfswerkzeuge wird die Schaltung synthetisiert und implementiert. Anschließend werden die Konfigurationsdaten auf das FPGA übertragen. Es ist darauf zu achten, dass eventuell verwendetes fremdes geistiges Eigentum vertrauenswürdig ist, die Entwurfstools nicht manipuliert sind und die Daten in einer gesicherten Umgebung auf das FPGA übertragen werden. Falls erforderlich, ist die Übertragung zu verschlüsseln.

Bei den Logik-Bausteinen gibt es auch Unterschiede in der elektromagnetischen Verträglichkeit. FPGAs sind empfindlicher gegenüber Teilchenstrahlung und elektromagnetischen Wellen als ASICs.

Wird ein eingebettetes System nicht selbst entwickelt, sondern als ganzes oder in Komponenten beschafft, gelten die genannten Empfehlungen entsprechend.

Prüffragen:

- Wurden bei der Designentscheidung zur Hardware- und Software-Realisierung Sicherheitsaspekte berücksichtigt?
- Wurden bei der der Designentscheidung zur Implementierung mit einer bestimmten Hardware-Technologie Sicherheitsaspekte berücksichtigt?

# M 4.483 Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Beschaffer, Planer

Bei eingebetteten Systemen kann ein zusätzlicher Mikrocontroller verwendet werden, um kryptographische Algorithmen und Protokolle abzuarbeiten, z. B. um Hash-Funktionen und Signaturverifikation zu beschleunigen. Dieser kommuniziert mit dem System-Mikrocontroller über die Gültigkeit der Firmware-Authentifizierung.

Ab einem hohen Schutzbedarf der Vertraulichkeit oder der Integrität ist diese Kommunikation gegen Hardwareattacken widerstandsfähig zu machen, indem

- die Leiterbahnen auf den inneren Lagen der Leiterplatte verlaufen,
- dynamische Signale (Impulse) verwendet werden, um dem Haupt-Mikrocontroller einen erfolgreichen Bootvorgang zu signalisieren und
- nach Möglichkeit mehrere Pins mit unterschiedlichen dynamischen Signalen verwendet werden.

Das Prinzip von Trusted Computing wird durch die Trusted Computing Group (TCG) anhand einer Reihe von Ankern für Vertrauen in einem System definiert. Wichtige Anker im Zusammenhang mit eingebetteten Systemen sind die Root of Trust for Measurement (RTM), die Root of Trust for Storage (RTS), sowie die Root of Trust for Reporting (RTR). Die Aufgabe der RTM ist es, als Anker für die Erhebung der Konfiguration einer Plattform zu dienen. Sie wird noch initialisiert, bevor das Betriebssystem gestartet wird. Beim Starten des RTM misst diese die Konfiguration der Hardware-Plattform während diese initialisiert wird, sowie die erste gestartete Software-Komponente. Danach ist sie beendet und führt keine weiteren Aktionen mehr durch. Es lassen sich also alle Änderungen an der Plattform oder der zuerst gestarteten Software-Komponente, etwa dem Bootloader, erkennen. Veränderungen an danach gestarteten Software-Komponenten, wie dem Betriebssystem oder Applikationen, werden damit nicht erkannt. Der Mechanismus für diesen Zweck verlangt, dass jede Software-Komponente die jeweils als nächstes zu startende Software-Komponente misst und die Korrektheit feststellt. Somit entsteht eine sogenannte "Trusted Chain of Measurement". Die RTM stell hierbei den Beginn der Kette dar. Die Messwerte werden mittels kryptografischer Funktionen zu Hashwerten reduziert und in gesicherten Speicherbereichen als Referenzwerte abgelegt. Die Root of Trust for Storage dient dazu, Daten sicher zu speichern und die Root of Trust for Reporting dazu sicherheitsrelevante Informationen korrekt wiederzugeben.

Eingebettete Systeme sind zwar spezialisierte Geräte aber im Gegensatz zur reinen Hardwareimplementierung (ASIC) universelle Rechner. Deshalb ist es auch bei eingebetteten Systemen sinnvoll und nötig, Gerätekonfiguration, Software und Daten genauer zu prüfen, ob sie verändert wurden. Die Informationen in Systemen mit hohen Anforderungen an die Integrität sollten durch den Einsatz kryptographischer Prozessoren oder Hardware-Sicherheitsmodule (Trusted Platform Module) durch das verarbeitende System authentisiert

werden. Bei eingebetteten Systemen mit Kommunikationsfunktionen sollte es möglich sein, Geräte sicher zu identifizieren und mit diesen Geräten vertrauenswürdig zu kommunizieren. Darüber hinaus sollen verlässlich Zustandsinformationen über ein Gerät eingeholt werden können. Insbesondere darf es dabei nicht möglich sein, dass ein Gerät die Identität eines anderen Gerätes duplizieren kann oder dass ein Gerät Statusinformationen eines anderen Gerätes anstelle seiner selbst ausliefert.

Vertrauensanker und darauf basierende Überprüfungen können bei eingebetteten Systemen meist einfacher realisiert werden als bei einem Standard-Rechner, beispielsweise wenn Firmware zusammen mit dem Read-Only Dateisystem squashfs genutzt wird und Konfiguration und Zustand getrennt von der Software gespeichert werden. Ein RTM kann dann die komplette Firmware messen, bevor sie gestartet wird, und es muss keine komplexe Vertrauenskette aufgebaut werden. Betriebssysteme müssen dadurch nicht angepasst werden und das Laufzeitverhalten ändert sich nicht. Auch ist es nicht nötig, jede Software-Komponente einzeln zu messen. Es kann das gesamte Firmware-Image gemessen und gegen einen Referenzwert abgeglichen werden.

Prüffragen:

- Falls ein zusätzlicher Mikrocontroller für die kryptographischen Berechnungen verwendet wird, ist dessen Kommunikation mit dem System-Mikrocontroller ausreichend abgesichert?
- Sind für das eingebettete System die nötigen Vertrauensanker realisiert?
- Ist für das eingebettete System eine Chain of Trust realisiert?

# M 4.484 Speicherschutz bei eingebetteten Systemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Beschaffer, Planer

Wenn in einem eingebetteten System mehrere Softwarekomponenten ablaufen, kann es sinnvoll sein, diese zu separieren. Soll nicht für jede Komponente ein eigener Mikrocontroller verwendet werden, kann dies auch durch Speicherschutztechnologien erreicht werden. Ziel des Speicherschutzes ist es, Arbeitsspeicher so zu strukturieren und Bereiche so zu separieren, dass ein Programmierfehler oder Absturz eines einzelnen Programms nicht die Stabilität anderer Programme oder des Gesamtsystems beeinträchtigt. Programme sollen daran gehindert werden, auf den Speicherbereich anderer Programme zuzugreifen.

Um Daten auf dem eingebetteten System mit erhöhten Anforderungen an die Integrität und Verfügbarkeit besser abzusichern, sollen Speicherschutzmechanismen bereits im Entwurf des Systems berücksichtigt werden. Es ist eine Realisierungsform zu wählen, die das benötigte Sicherheitsniveau gewährleistet und den Einsatzerfordernissen des eingebetteten Systems nicht entgegensteht. Die beiden grundsätzlichen Realisierungen sind Hardware-Speicherschutz und Software-Speicherschutz.

Hardwareseitig kann eine Speicherverwaltungseinheit ("Memory Management Unit", MMU) oder eine einfachere Speicherschutzeinheit ("Memory Protection Unit", MPU) den Speicherschutz unterstützen. Mit einer MMU ist es möglich, mehrere virtuelle Prozessoren auf einem physikalischen Prozessor zu vereinen, der durch das Betriebssystem verwaltet wird. Jedes Programm kann seinen eigenen virtuellen Mikrocontroller erhalten, und die Ressourcen des physikalischen Mikrocontrollers lassen sich flexibel zuordnen. MMU sind standardmäßig Bestandteil von Servern, PCs und modernen Smartphones, in kleinen eingebetteten Systemen sind sie normalerweise nicht vorhanden.

Bei einer MPU nutzen alle Programme den gemeinsamen Adressraum des physikalischen Speichers. Die MPU überwacht, auf welchen Speicherbereich ein Programm zugreift. Ist ein Zugriff nicht erlaubt, so kann das Betriebssystem den Speicherzugriff abfangen, bevor die Daten im Speicher verändert werden. Theoretisch könnte jedes Programm einen separaten, sogenannten Schutzraum bekommen. Aufgrund der meist knappen Ressourcen bei eingebetteten Systemen sollten aber nur so viele Schutzräume etabliert werden wie nötig, z. B. zwei, um die Ausführung von vertrauenswürdigen Programmen gegenüber der von nicht-vertrauenswürdigen zu trennen.

Bei hardwarebasiertem Speicherschutz werden die Speicherzugriffe durch die Hardware überwacht. Dieser Ansatz funktioniert auch, wenn die nicht vertrauenswürdige Softwarekomponente direkt in einer Maschinensprache programmiert wurde. Die überwachten Speicherzugriffe umfassen nicht nur die Lade- und Speicherbefehle sondern auch Maschinenbefehle, die vor ihrer Ausführung geladen werden. Schlägt die Überprüfung beim Speicherzugriff fehl, so unterbricht die Hardware den Ablauf des aktuellen Maschinenprogramms und wechselt zu einer Unterbrechungsbehandlung in die Systemsoftware. Welche Rechte für welchen Speicherbereich gelten, wird durch spezielle, zugriffsgeschützte Register beschrieben. Eine für hardwarebasierten Speicherschutz

geeignete CPU benötigt eine Hardware, die einen privilegierten und einen unprivilegierten Betriebsmodus unterstützt.

Beim softwarebasierten Speicherschutz werden die Speicherzugriffe nicht implizit durch die Hardware überprüft, sondern vorab explizit durch die Software. Die Überprüfung kann dabei zum Teil zum Übersetzungszeitpunkt stattfinden oder auch zur Laufzeit, zum Beispiel durch automatisch generierte Überprüfungen.

Prüffragen:

- Verfügt das eingebettete System über Vorkehrungen zum Speicherschutz?
- Sind die Art des Speicherschutzes und Anzahl und Größe der Schutzräume für das System und den Einsatzzweck angemessen und ausreichend?

# M 4.485 Sicheres Betriebssystem für eingebettete Systeme

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Planer, Beschaffer, Entwickler

Für eingebettete Systeme gibt es sehr viele verschiedene Betriebssysteme. Einige hochspezialisierte Systeme benötigen gar kein Betriebssystem, andere sind eingebettete Betriebssysteme, die aus Mehrzweckbetriebssystemen heraus entwickelt wurden, z. B. Embedded Linux Varianten oder Windows CE. Dazwischen existieren zahlreiche unter verschiedensten Aspekten für eingebettete Systeme spezialisierte (Echtzeit) Betriebssysteme, wie z. B. RTOS oder VxWorks.

Auf der einen Seite wird von den Merkmalen eines Mehrzweckbetriebssystems in der Regel nur ein Teil benötigt, z. B.

- sind Adressraumdeskriptoren nur notwendig im Falle von Systemen, die eine Adressraumisolation erfordern,
- spielen Dateisystem und Dateienverwaltung bei einigen Einsatzbereichen keine Rolle,
- benötigen ROM-basierte Systeme auf denen lediglich automatisiert ein einziges Programm abläuft keine prozessbezogene Benutzerrechteverwaltung,
- kann auf eine aufwändige Verwaltung von Prozesszuständen verzichtet werden wenn der Ablaufplan für die Prozesse vorab festgelegt wird und sich nicht mehr ändert,
- wird eine Ereignisverwaltung nur bei ereignisgesteuerten und/oder präemptiven Systemen benötigt.

Auf der anderen Seite können für eingebettete Systeme Anforderungen vorliegen, die mit Mehrzweckbetriebssystemen nicht oder schwierig umzusetzen sind, z. B.

- harte Echtzeit-Zusicherungen,
- weitergehende Mechanismen zur Fehlererkennung und -behandlung,
- Zwang, ressourcenschonend zu arbeiten.

Wird ein eingebettetes System konzipiert oder beschafft, ist daher darauf zu achten, dass das Betriebssystem und seine Konfiguration für den vorgesehenen Betrieb unter den vorgegebenen Bedingungen, einschließlich der Sicherheitsanforderungen, geeignet sind. Das Betriebssystem ist gemäß den spezifischen Sicherheitsanforderungen des Gesamtsystems zu konfigurieren. Die Sicherheitsanforderungen sollten in der Sicherheitsrichtlinie und im Software-Entwicklungsprozess dokumentiert sein. Grundsätzlich sollte das Betriebssystem nur die für die vorgesehene Aufgabe notwendigen Dienste, Funktionen und Eigenschaften aufweisen. Es dürfen nur Treiber genutzter Schnittstellen eingebunden werden.

Sicherheitsaspekte eines Betriebssystems sollten in unterschiedlichen Bereichen und Betriebsphasen berücksichtigt werden. Das System sollte in einem sicheren planvollen Prozess entwickelt werden. Die Systemarchitektur sollte den Kernel von Paketen wie Middleware, Netz-Protokollen und Applikationen trennen. Es sollte möglich sein, diese Komponenten zu ergänzen und zu verändern, ohne dass der Kernel geändert werden muss. Das kann mit einem sogenannten Mikrokern erreicht werden. Ein Mikrokern (englisch: Microkernel) verfügt im Gegensatz zu einem monolithischen Kernel nur über grundlegen-

de Funktionen zur Speicher- und Prozessverwaltung und zur Synchronisation und Kommunikation. Er ist somit weniger angreifbar und auch absturzsicherer.

Wie in M 4.489 *Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen* und M 4.483 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen* sowie M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen* und M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen* empfohlen, muss das Betriebssystem Mechanismen zum sicheren Booten und zur sicheren Programmausführung bereitstellen. Dazu muss es in der Lage sein, ein Trusted Plattform Module (TPM) zu integrieren und zu nutzen.

Während des laufenden Betriebs sollte das System Angriffe abwehren können. Dies kann auch dadurch erreicht werden, dass zusätzliche Sicherheitsprodukte installiert und genutzt werden. Im Ruhezustand darf es für einen Angreifer nicht möglich sein auf Daten zuzugreifen.

Ein Chipkartenbetriebssystem sollte insbesondere folgende Mechanismen und Dienste bereitstellen:

- Benutzeridentifizierung und Authentikation mittels PIN, PUK oder biometrischen Verfahren
- Zugriffskontrolle mit Rechteverwaltung
- Gegenseitige Authentisierung von Chipkarten und anderen Rechnern
- Sichere Datenübertragung ("Secure Messaging") gegen Ausforschung und Manipulation
- Bereitstellung von Signier- und Verschlüsselungsfunktionen im gesicherten Zusammenwirken mit Kryptoterminals
- I/O-Kontrolle aller Schnittstellen durch das Betriebssystem gegen unerlaubte Zugriffe
- Gewährleistung der Interferenzfreiheit einzelner Anwendungen: verschiedene Anwendungen dürfen sich nicht gegenseitig beeinflussen
- Möglichkeit die Chipkarte zu deaktivieren

Für Systeme mit hohem oder sehr hohem Schutzbedarf ist zu prüfen, ob es erforderlich ist das Betriebssystem zu evaluieren, z. B. nach ISO 15408. Statt ein ganzes Betriebssystem komplett zu evaluieren, ist es ratsam, das BSI-Schutzprofil "Operating System Protection Profile (OSPP)" zu beachten.

Prüffragen:

- Wurden bei der Konzeption oder zur Beschaffungsplanung des eingebetteten Systems die Anforderungen an das Betriebssystem analysiert?
- Ist die Funktionalität des Betriebssystems auch im Hinblick auf Sicherheitsmechanismen für die vorgesehene Aufgabe ausreichend?
- Sind nur die benötigten Dienste und Funktionen vorhanden bzw. aktiviert?
- Unterstützt es das Betriebssystem, ein Trusted Plattform Module zu nutzen?
- Ist das Betriebssystem hinsichtlich eines anerkannten Standards auf einer angemessenen Stufe evaluiert?

# M 4.486 Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Beschaffer

Durch einen oder mehrere der nachfolgend beschriebenen Mechanismen ist das eingebettete System entsprechend seinem Schutzbedarf gegenüber Seitenkanalangriffen zu härten. Diese Maßnahme beschreibt die möglichen Angriffsformen und Gegenmaßnahmen zu deren Abwehr.

### Arten von Seitenkanalangriffen

Wenn IT-Systeme Kryptografie einsetzen, findet dies nicht in einem abstrakten mathematischen System statt, sondern wird durch programmierte integrierte Schaltkreise geleistet. Diese interagieren gemäß den Naturgesetzen mit ihrer Umgebung und geben dadurch Informationen über die verarbeiteten Daten preis. Ein Seitenkanalangriff ist eine kryptoanalytische Vorgehensweise um Kryptovariablen zu kompromittieren, in dem die physische Implementierung eines Kryptosystems in einem Gerät oder in einer Software ausgenutzt wird. Seitenkanalangriffe sind zeitaufwändig. Sie erfordern den vollständigen Zugang zum Gerät, der häufig nur in ausgebautem Zustand gegeben ist.

Seitenkanalangriffe lassen sich grundsätzlich in nicht-invasive und invasive Angriffe unterteilen.

### Nicht-invasive Angriffe

Nicht-invasive oder passive Angriffe beobachten physikalische Parameter wie z. B. Stromverbrauch, Laufzeiten und Speichernutzung während relevante kryptografische Codeanteile ablaufen und schließen daraus auf geschützte Daten, wie Schlüssel und Passwörter.

### Analyse des Energieverbrauchs

Simple Power Analysis ist eine Methode, bei der der Energieverbrauch eines Mikroprozessors während kryptologischer Berechnungen direkt aufgezeichnet wird. Der Energieverbrauch variiert abhängig von den jeweils ausgeführten Mikroprozessorbefehlen. Er gibt somit Aufschluss über die ausgeführten Operationen sowie über den Schlüssel. Durch den Vergleich von Energieverbrauchsmessungen einer kryptologischen Operation können Muster wie etwa DES-Runden oder RSA-Operationen entdeckt werden und Rückschlüsse auf den geheimen Schlüssel gezogen werden.

Die Differential Power Analysis (DPA) setzt zusätzlich statistische Methoden ein. Damit kann ein Angreifer auch bei komplexeren Verarbeitungsarten wie Parallelität oder Speicherdirektzugriff (Direct Memory Access, DMA) an sein Ziel kommen.

### Analyse des Zeitverhaltens

Rechenzeitangriffe nutzen den Umstand, dass Kryptosysteme in Abhängigkeit vom Schlüssel für unterschiedliche Klartexte oder Chiffrate leicht unterschiedliche Ausführzeiten benötigen. Wenn ein Angreifer Zugriff auf das System hat, kann er durch Ausprobieren von verschiedenen Eingaben mittels Laufzeitanalyse den Schlüssel nach und nach rekonstruieren. Rechenzeitan-

griffe sind sowohl gegen Chipkarten als auch gegen Software-Implementierungen veröffentlicht worden.

**Mikroarchitekturelle Angriffe (z.B. Cache-Angriffe, Instruktions-Cache-Angriffe)**

Die Angriffe richten sich gegen software-implementierte Kryptosysteme. Die Idee des Angriffs basiert darauf, dass beim Ausführen kryptologischer Software Daten und Routinen schlüsselabhängig in den Cache bzw. Instruktionscache geladen werden. Ziel ist es; die mikroarchitekturellen Prozessoreigenschaften/-funktionen auszunutzen und so an den Schlüssel zu gelangen.

Weitere Ansatzpunkte für nicht-invasive Seitenkanalangriffe sind Rechenfehler in fehlerhaften Mikroprozessoren, elektromagnetische Abstrahlung und Schallemissionen. Unterschiedliche Seitenkanalangriffsarten können auch kombiniert werden.

**(Semi-) Invasive Angriffe**

Als invasiv oder aktiv werden Angriffe bezeichnet, bei denen in ein Gerät physisch eingegriffen wird. Nach dem eine kurzfristigen Fehlfunktion der entscheidenden Sicherheitsfunktionen erzeugt wurde, können die fehlerhaften Ergebnisse untereinander und / oder mit dem korrektem Ergebnis verglichen werden. Dies ist für einen Angreifer besonders interessant, wenn kryptografische Algorithmen ablaufen, z. B. bei der Signaturerzeugung. Aus den gewonnen Daten kann auf den geheimen Schlüssel geschlossen werden. Die Fehlfunktion kann im Moment der Ausführung des kritischen Codes hervorgerufen werden, z. B. können Spannungsschwankungen wie Spikes (Impulsspitzen) oder Glitches (Störimpulse) erzeugt werden. Das System kann auch elektromagnetischer Strahlung oder extremen Temperaturen ausgesetzt werden. Diese Attacken werden in der Fachliteratur auch als "semi-invasiv" bezeichnet, da zwar physikalisch eingegriffen, der Chip aber nicht zerstört oder dauerhaft beschädigt bzw. manipuliert wird. Fault Attacken, die kurzfristige Fehlfunktion auslösen, haben in den letzten Jahren erheblich an Bedeutung gewonnen.

Weitere Verfahren für Seitenkanalangriffe sind Gegenstand der aktuellen Forschung, z. B. photonische Seitenkanalangriffe durch photonische Emissionsanalyse oder photonische Fehlerinduktion.

**Abwehrmöglichkeiten gegenüber Seitenkanalangriffen**

Da jedes physikalische System mit seiner Umgebung interagiert, ist ein hundertprozentiger Schutz gegen Seitenkanalangriffe nicht möglich. Ziel ist es daher deren Erfolgswahrscheinlichkeit herabzusetzen. Widerstandsfähigkeit gegen Seitenkanalangriffe bedeutet also nicht, dass diese bzw. deren Erfolg absolut unmöglich gemacht wird, sondern dass sie erschwert werden. Das wesentliche Konzept dazu besteht darin, die erforderliche Anzahl von Messungen für den Erfolg einer Attacke so zu erhöhen, dass ein Restrisiko getragen oder anderweitig abgefangen werden kann.

**Maskieren der Daten**

Ziel ist es den Zusammenhang zwischen den tatsächlichen geheimen Daten und der vom Angreifer gemessenen Seitenkanalinformation zu verwischen. Die Zwischenergebnisse werden mit einem geheimen Maskenwert randomisiert. Dadurch wird der Zusammenhang zwischen den tatsächlichen Daten und der gemessenen Seitenkanalinformation gebrochen. Die Maskierung kann sowohl auf Algorithmusebene als auch auf der Gatterebene erfolgen.

Bei der softwaretechnischen Lösung werden nach einem Maskierungsschemas Masken spezifiziert und durch den Algorithmus auf alle Zwischenresultate angewendet. Auf der Gatterebene können spezielle Logikstile, wie z. B. mC-MOS, MDPL oder iMDPL, verwendet werden, die ein einheitliches Stromprofil während des Verschlüsselungs- und Entschlüsselungsvorganges herstellen sollen. Das Thema ist noch Gegenstand aktueller Forschungen. Weit verbreitete Hardware basierend auf CMOS Logik erfüllt diese Bedingungen nicht und ihre Stromaufnahme hängt stark von den verarbeiteten Daten ab.

**Verrauschen oder Filtern des Stromverbrauchs**

Ziel ist es im Rauschen das Signal zu verstecken, welches die Seitenkanalinformation beinhaltet. Typische Ansätze sind das vorhandene Rauschen durch den Einsatz von Rauschgeneratoren zu verstärken oder die Amplitude des Signals, welches die Seitenkanalinformation trägt zu verringern. Letzteres kann durch einen möglichst konstanten, datenunabhängigen Stromverbrauch des zu schützenden Geräts weitgehend erreicht werden. Es können auch künstliche Stromrauschquellen hinzugefügt und willkürlich Strom verbraucht werden.

**Härten gegen Laufzeitattacken**

Ziel ist es das zeitliche Verhalten des Systems zu verschleiern, während es sensible Daten verarbeitet. Dazu können Dummy-Operationen oder zufällige Wartezyklen in den Programmablauf eingefügt werden, z. B. bei einem kryptographischen Algorithmus.

Ein wirkungsvoller Schutz gegen verschiedene Laufzeitattacken und Power-Analysen ist mit Randomisierungstechniken, dem sogenannten Blinding zu erreichen. Dabei wird zu Zwischenwerten ein Zufallswert addiert oder multipliziert. Abhängig davon, mit welchen Größen in einem kryptografischen Algorithmus dies geschieht, wird von Basis-Blinding, Modulus-Blinding oder Exponenten-Blinding gesprochen. Sie verhindern, dass einem Angreifer Zwischenwerte des modularen Exponentiationsalgorithmus zur Kenntnis kommen, welcher bei kryptografischen Verfahren eingesetzt wird.

**Härten gegen (Semi-) Invasive Angriffe**

Angriffe durch differentielle Fehleranalyse können erkannt bzw. qualifiziert vermutet werden, wenn Berechnungsschritte redundant durchgeführt werden und die Ergebnisse nicht übereinstimmen. Filter können eingebaut werden um Unregelmäßigkeiten in der Spannungsversorgung auszugleichen bzw. die Toleranz gegenüber gestörten Taktsignalen zu erhöhen. Optische Eingriffe mit Lasern können mittels Lichtdetektoren und speziellen Schutzschichten erkannt bzw. erschwert werden. Eingebettete Systeme können auch mit Speicherelementen ausgestattet werden, deren Inhalt sich im Normalbetrieb nicht ändert. Wird eine Änderung erkannt, liegt der Verdacht auf einen Angriff mittels differentieller Fehleranalyse nahe. Dafür wird zusätzlicher Speicherplatz bzw. zusätzliche Rechenzeit benötigt.

Prüffragen:

- Sind dem Schutzbedarf und der Bedrohungslage angemessene Vorkehrungen gegen nicht invasive Seitenkanalangriffe getroffen?
- Sind dem Schutzbedarf und der Bedrohungslage angemessene Vorkehrungen gegen (semi-)invasive Seitenkanalangriffe getroffen?

# M 4.487 Tamper-Schutz (Erkennung, Verhinderung, Abwehr) bei eingebetteten Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Administrator, Planer

Für eingebettete Systeme ist ab einem hohen Schutzbedarf für die Vertraulichkeit oder Integrität ein Tamper-Schutz-Konzept zu planen und umzusetzen.

Ein umfassender Tamper-Schutz besteht aus den drei Funktionsbereichen "Verhinderung", "Erkennung und Nachweis" und "Reaktion und Abwehr". In der Fachliteratur werden dafür meist die englischen Begriffe "tamper resistance", "tamper evidence" und "tamper response" verwendet. Tamper-Schutz kann Infrastrukturelemente, Hardware und Software betreffen. Bei letzterem kommen kryptografische Mechanismen zum Einsatz (siehe M 4.483 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*, M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*).

Um Tamper-Angriffe auf Infrastrukturelemente und Hardware zu verhindern, ist es notwendig, ein einbruchssicheres ("tamper resistant") System herzustellen, das auf Grund seiner Konstruktion nicht unautorisiert verändert werden kann. Für den Fall, dass ein Angreifer frei über ein System verfügen kann, ist ein vollkommener Schutz nicht möglich. Allerdings können durch bauliche und technische Vorkehrungen die für ihn zu überwindenden Hürden sehr hoch gesetzt werden. Ein solches System zu realisieren kann aufwändig sein und das Resultat ist möglicherweise ein kompliziertes, wenig flexibles System. Bevor dieser Weg eingeschlagen wird, sollte daher analysiert und bewertet werden, welcher Aufwand aufgrund des Schutzbedarfs des Systems erforderlich und sinnvoll ist. Verschiedene Konstruktionselemente können dazu beitragen, die Einbruchsicherheit zu erhöhen. Beispiele sind spezielle Schrauben wie Torx-TR mit einem Stift in der Profilmitte, der verhindert, dass diese Schraube mit einem normalen Torx- oder Schlitz-Schraubendreher zu drehen ist, oder Ummantelungen, Schutzschichten und passive oder aktive Metallleitungen. Eingebettete Systeme können auch bautechnisch so mit einer Umgebung verbunden werden, dass sie nur sehr schwer herausgelöst werden können und zusammen mit der Umgebung nicht transportabel wären, z. B. durch Metall oder Beton.

Deutlich aufwändiger ist es Vorkehrungen zu treffen, die Einbrüche erkennen und dokumentieren ("tamper evidence"). Diese erlauben es, Modifikationen an einem System automatisiert zu erkennen oder durch externe Prüfer die Korrektheit eines Systems zu bestätigen. Beispiele für derartige Mechanismen sind Plomben und Siegel, aktiv getriebene Metallleitungen mit Sensoren, die auf Licht, Druck oder Widerstands- und Kapazitätsänderungen reagieren.

Als Reaktion auf einen Tamper-Angriff ("tamper response") kann ein Alarm an eine übergeordnete Managementeinheit abgesendet werden. Zudem sollten sensitive Daten des Systems möglichst automatisch gelöscht werden. Abhängig vom Schutzbedarf der Daten sollten verschiedene Optionen betrachtet werden. Einfach zu realisieren ist die Energieversorgung des RAM zu unterbrechen, allerdings könnte ein Angreifer mit entsprechender Ausrüstung und Expertise die Daten rekonstruieren. Außerdem betrifft dies nur einen Teil der Daten eines eingebetteten Systems. Eine verbreitete Methode besteht darin,

das RAM mehrfach zu überschreiben. Häufig wird dabei zuerst mehrfach mit "0", dann mehrfach mit "1" überschrieben. Der Nachteil dieser Methode liegt darin, dass nicht garantiert werden kann, dass dieser Vorgang auch tatsächlich stattfindet, wenn das Gerät oder seine Energieversorgung beeinträchtigt ist. Am sichersten ist es, das Gerät physikalisch zu zerstören. Dies kann z. B. durch eine Thermitreaktion hervorgerufen werden.

Prüffragen:

- Existiert ein Tamper-Schutz-Konzept?
- Sind dem Schutzbedarf angemessene Mechanismen etabliert, die Tamper-Angriffe verhindern?
- Sind dem Schutzbedarf angemessene Mechanismen zum Erkennen und Aufzeichnen eines Tamper-Angriffes etabliert?
- Sind dem Schutzbedarf angemessene Mechanismen zur Reaktion auf einen Tamper-Angriff etabliert?

# M 4.488 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Eingebettete Systeme sind häufig mit einer Vielzahl unterschiedlicher Schnittstellen ausgerüstet. Neben einfachen Ein-/Ausgängen zur Sensorik- und Aktuatorikanbindung finden sich Netzkommunikations-, Bedien- und Anzeigeschnittstellen unterschiedlicher Komplexität.

**Physikalische Schnittstellen**

Grundsätzlich sollten nur die benötigten physikalischen Schnittstellen vorhanden sein. Ist die Hardware vorgegeben und sind nicht benötigte Schnittstellen vorhanden, ist der Zugriff darauf durch bauliche Vorkehrungen zu unterbinden.

**Logische Schnittstelle Netzprotokolle**

Grundsätzlich dürfen nur benötigte Dienste aktiviert sein. Nicht benötigte Protokolle, die in manchen Konfigurationen standardmäßig vorhanden sind, sind zu deaktivieren, wie z. B. Appletalk, IPX oder NetBios. Die Dienste für Protokolle, die Daten im Klartext übertragen wie z. B. telnet, http oder ftp müssen bei erhöhtem Schutzbedarf deaktiviert sein. Falls notwendig, sind für den entsprechenden Zweck sichere Protokollvarianten bzw. Alternativen einzusetzen. SNMP v1 und v2 Dienste sollten deaktiviert sein.

**Logische Schnittstellen Anwendungsebene**

Alle in der Applikation nicht genutzten Schnittstellen müssen so konfiguriert werden, dass ein Zugang über diese Schnittstellen auf das eingebettete System nicht möglich ist. Es dürfen nur die Dienste freigeschaltet sein, die für die Aufgabenerfüllung benötigt werden. Bei komplexen Anwendungen mit erforderlicher Authentisierung beim Zugang ist zu überprüfen, für welche Bereiche der Anwendung die Authentisierung gültig ist. Sind z. B. bei einem Webserver die HTML-Seiten über ein Login geschützt, ist noch nicht sicher gestellt, dass auch der Zugriff auf Konfigurationsdaten per XML oder JSON darüber abgesichert ist. Um derartige Lücken zu finden, können Webseiten analysiert und Objekte mittels eines HTTP-Clients überprüft werden.

Wird auf dem eingebetteten System ein Betriebssystem genutzt, für das es darauf zugeschnittene automatische Schwachstellenscanner gibt, wie z. B. bei Linux-Systemen, sollten damit Verwundbarkeiten entdeckt und wenn möglich anschließend beseitigt werden. Bei allen Systemen ist mit universellen Portscannern oder Programmen zur Generierung von zufälligen oder spezifizierten Paketen, sogenannten packet buildern, nach Schwachstellen zu suchen.

Prüffragen:

- Sind nur benötigte physikalische Schnittstellen vorhanden?
- Sind nur benötigte Dienste aktiviert?
- Ist der Zugang zu Anwendungsschnittstellen durch sichere Authentisierung geschützt?

# M 4.489 Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Beschaffer, Entwickler, Planer

Der Bootprozess eines eingebetteten Systems darf nicht kompromittierbar sein. Es darf nicht möglich sein, von unauthentisierten Bootmedien zu starten oder Daten zu übernehmen. Es muss sichergestellt werden, dass die verwendete Software von einer autorisierten Instanz geschrieben oder freigegeben wurde.

Der Bootprozess sollte abgesichert sein, indem der Bootloader die Integrität des Betriebssystems überprüft und es nur dann lädt, wenn es als korrekt eingestuft wurde. Das Betriebssystem sollte nur starten, wenn der Bootloader durch eine Rückwärtsprüfung als vertrauenswürdig bestätigt wurde.

Dies kann mittels asymmetrischer Kryptografieverfahren überprüft werden. Aktuell (Stand 2015) kommen dafür z. B. Elliptic Curve Digital Signature Algorithm (ECDSA) und RSA (Rivest, Shamir und Adleman) in Kombination mit SHA (secure hash algorithm) in Frage. Von der Original-Software wird ein Hashwert berechnet und mit dem privaten Schlüssel des Herausgebers signiert. Überprüft wird er mit dem öffentlichen Schlüssel. Die Authentizität des öffentlichen Schlüssels muss über PKI-Verfahren sichergestellt werden.

Ein sicherer Bootprozess sollte in Stufen ausgeführt werden. Zuerst muss ein minimaler, bei der Herstellung fest in das ROM programmierter Bootloader (ROM-Loader) ablaufen. Dieser muss über einen vorher fest einprogrammierten kryptographischen Schlüssel verfügen, um seinerseits die digitale Signatur des nächsten Boot-Loaders zu verifizieren. Diesen anfänglichen Verifikationsschlüssel muss die Hardware bereitstellen, er kann über eine einmal programmierbare Sicherung in das ROM integriert oder in einem lokalen Trusted Platform Module (TPM) abgelegt werden, siehe hierzu auch M 4.483 *Einsatz kryptographischer Prozessoren bzw. Koprozessoren (Trusted Platform Module) bei eingebetteten Systemen*. Der ROM-Loader lädt einen weiteren Boot Loader mit mehr Funktionen, der dann das Betriebssystem oder wiederum einen Loader startet. Die Signatur muss ebenfalls im hardwaregeschützten Bereich gespeichert sein, weil mit dem Signaturschlüssel geprüft wird, ob die Komponenten in der zweiten (und ggf. weiteren) Stufe des Boot-Ablaufs echt sind. Die auszuführende Software kann mehrstufig geladen werden, wobei die Signatur der jeweils nächsten Stufe von der aktuellen Stufe geprüft wird. Scheitert eine Signaturverifikation oder wird eine Verbindung unterbrochen, muss angenommen werden, dass der sichere Zustand verletzt ist.

Oft werden in eingebetteten Systemen keine x86 basierten Computer mit BIOS (Basic Input/Output System) oder UEFI (Unified Extensible Firmware Interface) sondern ARM basierte Geräte mit dem Universal Boot Loader (U-Boot) eingesetzt. Die TCG bezieht sich in ihren Spezifikationen aber insbesondere auf eine Implementierung des RTM im pre-BIOS bzw. im UEFI in denen der RTM besonders zu schützen ist. Auf ARM Plattformen gibt es in vielen Fällen allerdings bereits ohne Trusted Computing die Möglichkeit eines gesicherten Starts von Software, wie z. B. ARM Secure Boot oder von nur einmal be-

schreibbarem Speicher, der auch gegen physische Manipulationen geschützt ist.

Prüffragen:

- Wird die Integrität des Betriebssystems durch den Bootloader überprüft?
- Wird die Integrität des Bootloaders durch das Betriebssystem überprüft?
- Ist ein mehrstufiges Boot-Konzept mit kryptografisch sicherer Überprüfung der Einzelschritte realisiert?
- Wird ein sicherer Hardware-Vertrauensanker verwendet?
- Wird im Falle eines ARM-basierten eingebetteten Systems ARM Secure Boot genutzt?
- Wird im Falle von UEFI Secure Boot genutzt?

# M 4.490 Automatische Überwachung der Baugruppenfunktion (BIST) bei eingebetteten Systemen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Beschaffer, Planer, Leiter IT

Mit einem eingebauten Selbsttest (Built-In Self Test, BIST) kann sich ein Schaltkreis, ein Gerät oder System selbst testen. Dazu werden Testsignale erzeugt, an die zu testende Komponente angelegt und die Antwortsignale ausgewertet, meist durch Vergleich mit vorgegebenen richtigen Antwort-Signalen. Bei einem BIST werden die Funktionen der Testumgebung (Automatic Test Equipment, ATE) wie Testsignalgeneratoren oder Auswerteeinheiten ganz oder teilweise direkt auf dem Chip implementiert. Dies führt zu verkürzten Signalpfaden, ungewollte Kopplungen werden verringert und die Signalintegrität auf den Testleitungen wird verbessert.

Ein Selbsttest kann im normalen Betrieb, während der Initialisierungsphase, während Ruhezeiten, vor dem Ausschalten oder außerhalb der Betriebsumgebung als funktionaler diagnostischer Test der Soft- und Hardware erfolgen. Beispiele für verschiedene Arten von BIST sind:

- Logik-BIST: Ein Pseudomuster- oder Pseudozufallsgenerator erzeugt ein Zufallsmuster mit dem die logischen Zustände überprüft werden. Entsprechen die Ausgangszustände nicht der Wahrheitstabelle, dann arbeitet die Logik fehlerhaft.
- Speicher-BIST: Mittels eines Testkreises werden Speicherbausteine ausgelesen und deren Ausgangszustände mit einem vorgegebenen Muster verglichen.
- Signaturanalyse: Signale aus Schaltungsteilen werden über einen längeren Zeitraum gesammelt und daraus eine Signatur ermittelt. Diese wird mit einem Sollwert verglichen und daraus die korrekte oder fehlerhafte Funktion der Gesamtschaltung gefolgert.
- Boundary Scan Test: Mit Hilfe zusätzlicher Zellen, sogenannten Latches, werden Signale über vordefinierte Pfade von außen in die zu testende Schaltung injiziert. Die Signale aus der Schaltung, die an Pins des Schaltkreises anliegen, können über den Scanpfad erfasst werden. Im Normalbetrieb sind die Latches passiv, es besteht kein funktionaler Unterschied zum ursprünglichen Schaltkreis.
- Analog- und Mixed-Signal-BIST: Zuerst werden die digitalen Komponenten mit Hilfe einer digitalen BIST-Schaltung vollständig verifiziert. Dann werden der Analog-Digital-Converter (ADC) und der Digital-Analog-Converter (DAC) verifiziert. Anschließend können andere Komponenten verifiziert werden, indem sie zwischen DAC und ADC mit Hilfe von analogen Multiplexern platziert werden.

Sämtliche Baugruppen des eingebetteten Systems mit erhöhten Anforderungen an die Verfügbarkeit und Integrität sollten integrierte Selbsttesteinrichtungen besitzen. Tests müssen während des Einschaltvorgangs und in angemessenen zeitlichen Intervallen während des Betriebs die Integrität des Systems prüfen. Soweit möglich, sollten die Selbsttestfunktionalitäten auch Sicherheitsfunktionen bzw. Sicherheitseigenschaften der Baugruppe überprüfen.

Bei Komponenten mit höherem Schutzbedarf, z. B. in kritischen Steuerungssystemen, sollte regelmäßig die Integrität der Speicher und I/O-Komponenten

in Rahmen des BIST geprüft werden. Bestehende BIST-Funktionen sind, falls möglich, um die erforderlichen Funktionen zu ergänzen.

Prüffragen:

- Wurde eine Analyse zu den notwendigen Selbsttestmechanismen des eingebetteten Systems durchgeführt?
- Verfügt das eingebettete System über die notwendigen eingebauten Selbsttests?
- Decken die Selbsttests auch Sicherheitsfunktionalitäten ab?

# M 4.491 Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Entwickler

Verbreitete Vorgehensweisen zum Debugging von eingebetteten Systemen sind In-Circuit-Emulation (ICE) und On-Chip-Debugging (OCD). ICE- Geräte ersetzen den eigentlichen Controller auf dem Zielsystem durch eine Hardware, in der die notwendigen Analysefunktionen eingebaut sind. Das später eingesetzte Zielsystem besitzt diese Zusatzfunktionen nicht und stellt somit keine ungewollten Debugging-Möglichkeiten bereit. Aufgrund zeitlicher, technischer oder finanzieller Zwänge kommt allerdings vermehrt OCD zum Einsatz. Dabei werden Debugging-Möglichkeiten auf den Serienbausteinen selbst implementiert. OCD kann somit in den Programmablauf eingreifen, z. B. um Werte aus Registern oder einem Trace-Speicher auszulesen oder zusätzliche kleine Monitoring-Programme auszuführen, die Debug-Informationen sammeln und nach außen geben.

Bei eingebetteten Systemen befindet sich die zu untersuchende Software meist nicht auf demselben Rechner wie der Debugger. Daher wird Remote Debugging verwendet, d. h. der Entwickler startet auf dem eingebetteten System eine Applikation, mit der sich der Debugger auf dem Entwicklungssystem z. B. über Ethernet oder RS232 verbindet.

Wird z. B. der GNU Debuggers (GDB) genutzt, führt das eingebettete System einen GDB-Server aus, bei dem sich der GDB-Client auf dem Entwicklungssystem anmeldet. Der Client bzw. der Programmierer übergeben dem Server auf dem eingebetteten System Anweisungen zum Untersuchen der Applikation. Der Server setzt die Anweisungen um und schickt die Resultate an das Entwicklungssystem zurück.

Soweit möglich, sind die aus der Hard- und Softwareentwicklung im System oder der Software installierten Hilfsmittel zum Debugging vollständig aus dem Entwurf für die Serie zu entfernen. Aus dem Produktionscode von Software sind alle Codeelemente zu entfernen, die nicht Bestandteil der Systemfunktionalität sind. Dazu zählen z. B. Breakpoints und nicht genutzter Code. Wird On-Chip-Debugging genutzt, ist sicherzustellen, dass Debugging-Funktionen nicht durch Unberechtigte genutzt oder aktiviert werden können. Im Bereich der Hardware ist sicherzustellen, dass keine Eingabeschnittstellen für Testsignale und Messpunkte zum Anschluss von Analysatoren aktiviert bzw. für Unberechtigte nutzbar sind.

Prüffragen:

- Sind, soweit möglich keine Debugging-Komponenten auf dem Zielsystem installiert?
- Ist im Falle von On-Chip-Debugging sichergestellt, dass Debugging-Funktionen nicht durch Unberechtigte genutzt oder aktiviert werden können?
- Sind alle Hardware-Debugging-Schnittstellen deaktiviert?

# M 4.492 Sichere Konfiguration und Nutzung eines eingebetteten Webservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Entwickler, Administrator

Einige eingebettete Systeme besitzen einen integrierten Webserver, mit dem Informationen abgerufen und eingesteuert werden können. Dabei handelt es sich für gewöhnlich um einen sogenannten Embedded-Webserver mit eingeschränkter Funktionalität, der für die meist knappen Ressourcen optimiert ist. Auf dem Markt sind zahlreiche eingebettete Webserver verfügbar, sie haben eine geringe Größe, belasten die CPU nur moderat und sind weitgehend plattformunabhängig. Als Hauptaufgabe können sie Webdokumente an den Client via HTTP(S) übertragen. Einige beherrschen zudem das dynamische Erstellen von Dokumenten, etwa per Server-Side Scripting.

Für einen eingebetteten Webserver sollten nur die benötigten Komponenten und Funktionen installiert bzw. aktiviert werden. Der Webserver sollte unter einem Konto mit möglichst geringen Rechten ablaufen. Falls zum Start höhere Privilegien benötigt werden, sollte anschließend in ein nicht privilegiertes Konto gewechselt werden. Es sollten alle für die Sicherheit und die Fehlerbehandlung relevanten Meldungen protokolliert werden, z. B. strukturiert nach erfolgreichen und nicht erfolgreichen Zugriffen, internen Fehlern, fehlerhaften oder unvollständigen HTTP-Anfragen und sonstigen relevanten Systemmeldungen. Diese Protokollierung sollte in der Sicherheitsdokumentation beschrieben sein (weitere Informationen hierzu finden sich in M 2.497 *Erstellung eines Sicherheitskonzepts für die Protokollierung*). Systemeinstellungen sollten möglichst restriktiv sein, z. B. sollte die Anzahl der gleichzeitig möglichen Verbindungen auf das für den Verwendungszweck nötige Maß beschränkt werden und die Größe des internen Caches sollte begrenzt werden. Falls genutzt, sollte der Zugriff auf CGI-Dateien mit einem CGI-Wrapper so kontrolliert werden, dass nur explizit freigegebene Programme ausgeführt werden können. Mit dem Webserver sollte möglichst nur über eine gesicherte SSL-Verbindung kommuniziert werden und der Zugang sollte nur nach einer starken Authentisierung möglich sein.

Prüffragen:

- Sind nur die benötigten Komponenten und Funktionen installiert bzw. aktiviert?
- Wird der Webserver unter einem nicht privilegierten Konto betrieben?
- Werden sicherheitsrelevante Ereignisse protokolliert?
- Sind sämtliche Konfigurationsparameter so restriktiv wie möglich eingestellt?
- Ist der Zugang nur nach starker Authentisierung möglich und die Übertragung verschlüsselt?

# M 4.493 Auswahl einer Entwicklungsumgebung für die Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Leiter Beschaffung

Es wird eine geeignete Entwicklungsumgebung benötigt, um ein Software-Projekt umzusetzen. Die Auswahl erfolgt primär anhand der für das Projekt vorgesehenen Programmiersprache und anhand des geplanten Anwendungstyps. Außerdem sollten optionale Zusatzfunktionen und die Anschaffungs- und Betriebskosten berücksichtigt werden.

Um eine geeignete Entwicklungsumgebung auszuwählen, empfiehlt es sich, die unbedingt geforderten und die optional gewünschten Kriterien tabellarisch den verfügbaren Produkten gegenüberzustellen. Die Auswahlkriterien können hierbei als gleichwertig angesehen werden oder gewichtet einfließen und umfassen beispielsweise:

- Unterstützte Programmiersprachen
- Unterstützte Betriebssysteme
- Kollaborationsmöglichkeiten
- Projekt-Management-Funktionen
- Refactoring-Funktionen
- Anschaffungskosten
- Wartungskosten
- Kompatibilität mit bestehenden Entwicklungssystemen
- Kompatibilität mit bestehenden Projekten (falls erforderlich)

Kommen nach dem objektiven Vergleich verschiedener Entwicklungsumgebungen mehrere Produkte in Frage, kann die Entscheidung mit einem subjektiven Vergleich abgeschlossen werden. Hierbei sind Auswahlkriterien zu beachten, die nicht durch einen konkreten Wert symbolisiert werden können, beispielsweise:

- Bedienbarkeit
- Intuitivität
- Vertrauenswürdigkeit des Herstellers

Prüffragen:

- Wurde eine Liste der erforderlichen und optionalen Auswahlkriterien für eine Entwicklungsumgebung erstellt?
- Wurde eine Entwicklungsumgebung anhand der vorgegebenen Kriterien ausgewählt?

# M 4.494 Sicherer Einsatz einer Entwicklungsumgebung

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Leiter Entwicklung

Aus den Sicherheitsanforderungen für die zu entwickelnde Software ergeben sich Sicherheitsanforderungen an die Entwicklungsumgebung bezüglich Integrität, Vertraulichkeit und Verfügbarkeit. Diese sowie die erforderlichen Sicherheitsmaßnahmen sind zu dokumentieren. Die folgenden Aspekte sollten dabei berücksichtigt werden.

### Abschottung der Entwicklungsumgebung

Die Entwicklung muss abgesichert betrieben werden. Hierzu muss die Entwicklungsumgebung ebenso wie die Testumgebung strikt von der Produktionsumgebung getrennt sein. Die Entwicklungsumgebung sollte dagegen geschützt sein, dass der Arbeitsablauf der Entwicklung unterbrochen wird und es muss sichergestellt sein, dass weder Verfügbarkeit, Vertraulichkeit und Integrität der Entwicklungsumgebung sowie der verarbeiteten Daten durch die Produktionsumgebung noch umgekehrt kompromittiert werden können.

Damit Code-Repositorities und andere Entwicklungsdaten nicht manipuliert werden können, muss der Zugriff auf diese beschränkt werden. Zugriffe auf Entwicklungsdaten müssen einzelnen Benutzern zugeordnet und dokumentiert werden können.

Die Produktionsumgebung muss von der Entwicklungsumgebung abgeschottet sein, beispielsweise durch Netztrennung und Zugriffskontrolle, damit diese nicht unautorisiert verändert oder manipuliert werden kann. Insbesondere muss sichergestellt sein, dass neu erstellte oder geänderte Software nur mittels transparenten und dokumentierten Prozessen sowie durch autorisierte Personen in die Produktionsumgebung übernommen werden kann.

Sichere Systeme können nur in einer sicheren Umgebung entwickelt werden. Dazu sind neben technischen Maßnahmen auch infrastrukturelle und organisatorische Sicherheitsmaßnahmen erforderlich. Beispielsweise müssen die genutzten Räumlichkeiten vor unbefugten Zutritt geschützt sein.

### Kommentare und Dokumentation

Kommentare und weitere, für den Produktionsbetrieb nicht relevante, Informationen sind aus Quelltexten, Konfigurationsdateien und ausführbaren Dateien zu entfernen, bevor diese im Produktionssystem verwendet werden.

Wenn die Entwicklungsumgebung es unterstützt, sollte sie so konfiguriert werden, dass bei der Erstellung von Programmpaketen automatisch alle für den vorgesehenen Verwendungszweck nicht relevanten Informationen entfernt werden. Es ist sicherzustellen, dass hierfür genau dokumentiert ist, welche Informationen im Interesse des Auftraggebers im fertigen Programmpaket enthalten sein sollen. Relevante Kommentare, Dokumentationen und Zusatzinformationen in den Entwicklungsdaten müssen stets erhalten bleiben, um sicherzustellen, dass die Software jederzeit geprüft und gewartet werden kann.

### Absicherung der Arbeitsplätze

Wird die Software an verteilten Arbeitsplätzen und von verschiedenen Personen entwickelt, muss die Verbindung zwischen den Arbeitsplätzen gesichert

sein. Die Kommunikation muss über verschlüsselte Datenverbindungen geführt werden und der Zugriff auf wichtige Komponenten, wie beispielsweise ausgelagerte Code-Repositories, sollte zusätzlich durch Sicherheitsgateways geschützt werden.

Während des gesamten Entwicklungsprozesses ist auf allen IT-Systemen eine aktuelle Software zum Schutz vor Schadprogrammen zu verwenden. Dies gilt auch für den Betrieb im Produktivsystem (siehe B 1.6 *Schutz vor Schadprogrammen*).

Prüffragen:

- Wird die Entwicklungsumgebung getrennt von der Produktionsumgebung betrieben?
- Werden Kommentare und sonstige nicht relevante Informationen entfernt, bevor Programmpakete im Produktivsystem eingesetzt werden?
- Kommunizieren verteilte Arbeitsplätze über eine sichere Verbindung miteinander?
- Ist eine Zugriffskontrolle für die Entwicklungsdaten vorhanden?
- Wird eine aktuelle Virenschutzsoftware verwendet?

# M 4.495 Sicheres Systemdesign bei der Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Leiter Entwicklung

Beim Entwurf von IT-Systemen sind alle verfügbaren Sicherheitsmechanismen zu prüfen und zu beurteilen, ob sie die Sicherheitsanforderungen erfüllen, die sich aus dem Schutzbedarf der geplanten Einsatzumgebung ergeben. Die Sicherheitsmechanismen müssen dann entsprechend implementiert werden, damit alle Sicherheitsanforderungen erfüllt und umgesetzt sind.

Jeder Bedrohung sollte mit angemessenen Sicherheitsmaßnahmen begegnet werden. Vor allem die folgenden Grundregeln müssen beim sicheren Systemdesign beachtet werden:

- Eingabedaten sind vor der Weiterverarbeitung grundsätzlich zu prüfen und zu validieren. Als ungültig klassifizierte Eingabedaten sollten verworfen und nicht weiter verwendet werden.
- Bei Client-Server-Anwendungen sollten die Daten grundsätzlich auf dem Server validiert werden. Validierungen durch den Client erhöhen den Komfort für die Benutzer, bieten aber keine Sicherheit und sind deshalb serverseitig zu wiederholen.
- Zwischen Systemkomponenten sollten Daten grundsätzlich verschlüsselt übertragen werden. Ausnahmen sind zu begründen.
- Für die Software und das IT-System, auf dem die Software ausgeführt wird, ist eine sichere Standard-Konfiguration vorzusehen. Hierbei sind insbesondere sichere Grundeinstellungen des Betriebssystems und der von der Software genutzten Module und Anwendungen vorzunehmen.
- Bei Fehlern oder Ausfall von Komponenten des Systems dürfen keine Informationen (z. B. Versionsnummern oder Dateipfade) preisgegeben werden.
- Der Betrieb der Software muss mit möglichst geringen Benutzerprivilegien möglich sein.

Das Systemdesign ist zu dokumentieren und die vollständige Abdeckung der Sicherheitsanforderungen zu überprüfen. Die Sicherheitsanforderungen müssen im Produktivbetrieb der Software umsetzbar sein und müssen deshalb auch die dortigen Umgebungsbedingungen abdecken (z. B. das verwendete Betriebssystem).

Prüffragen:

- Werden die Grundregeln des sicheren Systemdesigns eingehalten?
- Wurde das Systemdesign dokumentiert und dessen vollständige Abdeckung der Sicherheitsanforderungen überprüft?

# M 4.496 Sichere Installation der entwickelten Software

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Leiter Entwicklung

Voraussetzung für eine sichere Installation der fertigen Software in der Produktivumgebung ist ein erfolgreicher Test nach einem zuvor festgelegten Testverfahren (siehe M 2.568 *Testverfahren für Software*).

Weiterhin müssen die Betriebsprozeduren auf Zuverlässigkeit getestet sein, um Mängel im Produktivbetrieb auszuschließen. Außerdem müssen Notfallpläne bereitstehen, falls bei der Installation oder dem Betrieb der Software Störungen auftreten. Diese müssen Handlungsanweisungen für vorhersehbare Problemfälle und mindestens einen Ansprechpartner enthalten, den der Anwender direkt kontaktieren kann. Außerdem müssen die Administratoren in der Betreuung der Software geschult sein. Dies beinhaltet Wissen darüber, wie die Software konfiguriert wird und auch erweitertes Wissen darüber, wie die Software im Produktivbetrieb genutzt wird, damit Benutzer bei Problemen unterstützt werden können. Weiterhin sollen die Benutzer mit dem System vertraut gemacht worden sein, beispielsweise durch vorbereitende Schulungen oder bereitgestelltes Dokumentationsmaterial.

Für den Installationsprozess muss ein Installationsplan existieren, der alle durchzuführenden Schritte detailliert beschreibt und dabei auch mögliche Fehlerquellen oder Abweichungen zwischen verschiedenen Zielsystemen berücksichtigt. Nach der Installation wird anhand eines dokumentierten Testplans die korrekte Installation überprüft und das System für den Betrieb freigegeben.

Prüffragen:

- Sind die Voraussetzungen für eine sichere Installation der entwickelten Software erfüllt?
- Wird die Installation der entwickelten Software anhand eines existierenden Installationsplans durchgeführt?
- Wird die korrekte Installation der entwickelten Software anhand eines Testplans überprüft?

# M 4.497 Sichere Installation eines Netzmanagement-Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Installation eines Netzmanagement-Systems erfordert eine umfangreiche und sorgfältige Planung. Nach erfolgter Netzanalyse (siehe M 2.140 *Analyse der aktuellen Netzsituation*), Festlegung des Netzmanagement-Konzepts (siehe M 2.143 *Entwicklung eines Netzmanagement-Konzeptes*) und Auswahl eines geeigneten Netzmanagement-Systems (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*) muss die Installation des Produktes detailliert geplant und entsprechend umgesetzt werden. In Abhängigkeit von der dem Management-Produkt zugrunde liegenden Architektur ist für das lokale Netz eine Konfiguration des Netzmanagement-Systems zu erstellen, die dem formulierten Netzmanagement-Konzept Rechnung trägt.

Oft müssen auf den zentralen Rechnern Datenbanksysteme installiert werden, in denen die Managementinformationen von der Managementsoftware persistent abgelegt werden. Je nach Produkt ist hier die Einbindung eines schon vorhandenen Datenbanksystems möglich. Für die Managementsoftware sollte ein dediziertes, ausreichend leistungsfähiges IT-System verwendet werden.

Neben diesen Kriterien, die im Wesentlichen den geregelten technischen Ablauf des Systems garantieren sollen, sind aus Sicherheitsgesichtspunkten die dem Managementsystem zugehörige Software und die entsprechenden Daten in die Schutzbedarfsfeststellung gemäß IT-Grundschutz (siehe BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise*) aufzunehmen. Die Kompromittierung des Netzmanagement-Systems kann den Ausfall des gesamten Netzes nach sich ziehen. Durch unbemerkte Veränderungen am System kann zudem beträchtlicher Schaden entstehen, der auch existenzbedrohende Formen annehmen kann. Sollte der Schutzbedarf der Netzmanagement-Informationen als "hoch" oder "sehr hoch" eingestuft werden, so ist eine ergänzende Sicherheitsanalyse und gegebenenfalls eine Risikoanalyse durchzuführen.

Insbesondere ist bei der Installation auf folgende Punkte zu achten:

- Alle Rechner, auf denen Managementinformationen gelagert werden, sind besonders zu sichern:
- Es sind die Maßnahmen der Bausteine aus Schicht 3, je nach vorliegendem System, durchzuführen.
- Der Zugang zur Managementsoftware ist nur den berechtigten Administratoren und Revisoren zu gestatten.
- Der Zutritt zu den Rechnern sollte beschränkt werden.
- Die Kommunikation zwischen den Managementkomponenten sollte verschlüsselt erfolgen, um zu verhindern, dass Managementinformationen mitgehört und gesammelt werden können. Unterstützt das Produkt keine Verschlüsselung, so sind gesonderte Maßnahmen zu ergreifen, um die Kommunikation abzusichern (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation* oder M 2.579 *Regelmäßige Audits des lokalen Netzes* Aufbau eines Management-Netzes).
  Die Managementsoftware muss in das Datensicherungskonzept eingebunden werden.

Prüffragen:

- Ist das Netzmanagement-System sicher installiert worden?

# M 4.498 Sicherer Einsatz von Single-Sign-On

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Ein Wunschziel für ein zentrales Identitäts- und Berechtigungsmanagement-System ist, dass sich IT-Benutzer einmal authentisieren und danach durchgängig Zugriff auf die IT-Systeme und Anwendungen im Informationsverbund erhalten, für die sie die entsprechenden Berechtigungen haben. Eine solche Lösung wird Single-Sign-On (SSO) genannt. Durch diese ist es für Administratoren einfacher, Identitäten und Berechtigungen zu verwalten, und für Benutzer erleichtert es die IT-Nutzung, da sie sich nur noch einmal anmelden müssen. Aus Sicherheitssicht bringt ein SSO daher viele Vorteile, aber auch einige Risiken und entsprechende Sicherheitsmaßnahmen mit sich:

- Bei einem Identitätsdiebstahl hat ein Angreifer nicht nur Zugriff auf ein System, sondern auf viele. Daher sollten SSO-Systeme immer mit Zwei-Faktor-Authentisierung eingesetzt werden.
- Die Sicherheit des SSO-System bestimmt die Sicherheit der angeschlossenen Systeme und Anwendungen. Daher müssen die für Single-Sign-On genutzten Sicherheitsmechanismen sowie die Passwortgüte (Bildungsregeln, Komplexität, Gültigkeitsdauer) den kumulierten Anforderungen der angeschlossenen Anwendungen bzw. Systeme genügen.
- Für Angreifer sind Authentisierungsinformationen bei SSO besonders interessant. Daher dürfen diese nur verschlüsselt übertragen und gespeichert werden.
- Wenn das zentrale SSO-System ausfällt, kann unter Umständen auf damit verbundene IT-Systeme oder Anwendungen nicht mehr zugegriffen werden. Daher ist hier unbedingt ein Notfallkonzept erforderlich (siehe M 6.166 *Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System*).
- Mobile IT-Systeme sind eventuell zeitweise offline. Trotzdem wollen die Benutzer auch unterwegs arbeiten können. Es muss sichergestellt sein, dass in solchen Situationen ein abgesicherter Zugriff möglich ist.
- Wenn Benutzer sich beim SSO-System nicht anmelden können, beispielsweise weil sie ihr Anmeldetoken oder Passwort vergessen haben, können sie ihre IT erst wieder nutzen, wenn entsprechende Ersatzmaßnahmen vorgenommen wurden.
- Häufig werden bei SSO-Systemen die Zugriffsrechte nicht oder nicht ausreichend entsprechend dem jeweiligen Kontext vergeben, also abhängig von Rolle, Ort, Zeit oder Aktivität, so dass Benutzer für viele Aktionen mit zu weitreichenden Zugriffsberechtigungen arbeiten.
- Benutzer müssen sich bei SSO-Systemen konsequent abmelden, da durch SSO die Sicherheit vieler Systeme von der Zugriffssicherheit abhängt. Es muss überprüft werden, wie eine automatische Abmeldung bei Inaktivität erfolgen kann, da durch SSO auch Systeme mit angebunden sein können, bei denen längere Phasen der Inaktivität normal sein können.
- Die Möglichkeit einer Mehrfachanmeldung am SSO-System sollte deaktiviert werden. Ebenso ist eine automatische Sperrung von Benutzern bei mehrfach fehlgeschlagener Anmeldung am SSO-System empfehlenswert.

In SSO-Systeme können die verbreiteten IT-Systeme und Anwendungen ohne große Anpassungen eingebunden werden, für Nicht-Standard-Lösungen müssen andere Lösungen gefunden werden. Daher werden in der Praxis aus Gründen der Kompatibilität und Wirtschaftlichkeit eher sogenannte Re-

duced-Sign-On-Lösungen mit nicht vollständig institutionsweiten Berechtigungen verwendet.

Benutzer können mehrere Rollen mit unterschiedlichen Berechtigungsprofilen gleichzeitig haben, beispielsweise Administration und Mitarbeiter. Es muss daher überlegt werden, wie bei SSO sichergestellt werden kann, dass Benutzer Aufgaben mit unterschiedlichen Sicherheitsanforderungen nicht unter einer Benutzerkennung mit den maximalen Berechtigungen durchführen (Rollentrennung).

Für verschiedene Rollen sollten Benutzer auch unterschiedliche Systemrollen nutzen, also unter getrennten Benutzerkennungen arbeiten, insbesondere bei unterschiedlichem Sicherheitsanforderungen. So kann beispielsweise verhindert werden, dass mittels einer kompromittierten Benutzerkennung zu viele Berechtigungen durch einen Angreifer missbraucht werden können.

Mitarbeitern sollten jedoch auch nicht zu viele Benutzerkennungen zugeteilt werden, da dies unpraktikabel ist und dadurch die Gefahr steigt, dass durch Umgehungsversuche neue Sicherheitsrisiken entstehen. Deswegen sollte abhängig vom Schutzbedarf der Daten oder IT-Systeme geprüft werden, wie viele Benutzerkennungen nötig sind.

Der Einsatz des XML-Framework Security Assertion Markup Language (SAML) oder von Programmkonstrukten wie beispielsweise FastXPath-basierte Positionsangaben und Transformation von Namespace-Präfixen können die Sicherheit von SSO-Systemen gegen XML-Signature-Wrapping-Angriffe verbessern.

Prüffragen:

- Entsprechen die bei Single-Sign-On genutzten Sicherheitsmechanismen den Anforderungen der angeschlossenen Anwendungen bzw. Systeme?
- Wird bei SSO konsequent Zwei-Faktor-Authentisierung genutzt?
- Werden Authentisierungsinformationen bei SSO ausschließlich verschlüsselt übertragen und gespeichert?

# M 4.499 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, IT-Sicherheitsbeauftragter, Beschaffungsstelle

Bei der Auswahl geeigneter Lösungen für das Identitäts- und Berechtigungsmanagement spielen nicht nur technische Fragen eine Rolle. In der Praxis hat sich gezeigt, dass hierbei organisatorische Aspekte wesentliche Erfolgsfaktoren sind. Ein Identitäts- und Berechtigungsmanagement-System muss in erster Linie auf die Institution und deren jeweilige Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf passen und erst in zweiter Linie in die vorhandene Infrastruktur eingebunden werden. Es muss die in der Institution vorhandenen Vorgaben zum Umgang mit Identitäten und Berechtigungen abbilden können. Dazu gehören beispielsweise die Anforderungen aus M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*.

Identitäts- und Berechtigungsmanagement-Systeme sind komplexe Systeme, deren Einführung sehr viel Wissen über Technik, Geschäftsprozesse und Berechtigungsmodelle benötigt, so dass es häufig erforderlich ist, mit externen Beratern zusammenzuarbeiten. Die Anbindung der verschiedenen IT-Systeme kann durch unterschiedliche technische Ansätze erfolgen, z. B. mit Verzeichnisdiensten. Eine technologische Anforderung ist es, die unterschiedliche Berechtigungsverwaltung heterogener Anwendungen zentral zu integrieren.

Zu klären sind u.a. folgende Punkte:

- Soll eine zentrale oder dezentrale Lösung eingesetzt werden?
- Soll ein Single-Sign-On-Verfahren genutzt werden?
- Soll die Authentikation über Besitz, Wissen und/oder biometrische Eigenschaften erfolgen?
- Soll bei einer zentralen Lösung (Reduced Sign-On) die Anwendung auf Synchronisation oder einem zentralem Datenbank-Abgleich basieren?
- Welche Schnittstellen zur Anbindung von IT-Systemen mit dem Identitäts- und Berechtigungsmanagement-System werden benötigt?

Mit einer Einführung eines Identitäts- und Berechtigungsmanagement-Systems entsteht schnell der Wunsch, dass sich Benutzer nicht an jedem IT-System mit einem anderen Passwort anmelden müssen. Vielmehr möchten sich die Benutzer auch bei großen heterogen Netzen nur am ersten benutzten IT-System authentisieren müssen. Ein solches Verfahren, dass "Single-Sign-On" genannt wird, reicht die Authentisierungsinformationen dann an alle weiteren IT-Systeme weiter.

Aus der Praxis hat es sich bewährt, zunächst einmal ein Reduced-Sign-On anzustreben, also die Anzahl der Anmeldevorgänge je Benutzer zu reduzieren. Bereits dadurch können Benutzer, aber auch die Administratoren deutlich entlastet werden.

Es gibt eine Vielzahl verschiedener Mechanismen zur Identifikation ebenso wie zur Authentikation. Bei der Auswahl geeigneter Mechanismen sollte der Schutzbedarf der damit geschützten Informationen und Geschäftsprozesse im

Vordergrund stehen (siehe auch M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*).

Für eine geeignete Auswahl eines Identitäts- und Berechtigungsmanagement-Systems sind aus den konkreten Anforderungen der Institution Auswahlkriterien abzuleiten (siehe hierzu auch die Maßnahmen M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*, M 4.500 *Sicherer Einsatz von Systemen für Identitäts- und Berechtigungsmanagement*, M 2.555 *Entwicklung eines Authentisierungskonzeptes für Anwendungen* und M 4.498 *Sicherer Einsatz von Single-Sign-On* Sicherer Einsatz von Single-Sign-On).

Im Folgenden sind einige Auswahlkriterien für ein Identitäts- und Berechtigungsmanagement-System beispielhaft aufgelistet:

- Kann der Grundsatz der Funktionstrennung realisiert werden (M 2.5 *Aufgabenverteilung und Funktionstrennung*)?
- Interoperabilität: Ist das Identitäts- und Berechtigungsmanagement-System in der Lage, die unterschiedliche Berechtigungsverwaltung heterogener Anwendungen zentral zu integrieren?
- Unterstützt die Anwendung den Einsatz der geplanten Authentisierungsfaktoren Wissen, Besitz bzw. Biometrie?
- Ist eine Skalierung der Authentisierungsanforderungen je nach Schutzbedarf möglich?
- Sind durchgängige Rechteänderungen bis hin zum Rechteentzug kurzfristig möglich, wenn diese akut benötigt wird (z. B. Mitarbeiter wird fristlos freigesetzt)?
- Werden Authentisierungsdaten bei Speicherung und Verarbeitung ausreichend geschützt (nicht als Klartext, sondern stets verschlüsselt gespeichert bzw. übertragen)?
- Entsprechen die im Identitäts- und Berechtigungsmanagement-System vorhandenen kryptographischen Funktionen dem Schutzbedarf und besitzen sie eine ausreichende Mechanismenstärke (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*)?
- Werden die Authentisierungsdaten sicher verwaltet? Ist sichergestellt, dass beispielsweise Passwörter nie unverschlüsselt auf den entsprechenden IT-Systemen gespeichert werden?
- Wie schnell können die Identitäten, Berechtigungen oder Passwörter geändert werden, z. B. bei Verdacht auf Kompromittierung?
- Kann die Reaktion auf fehlerhafte Authentisierungsversuche entsprechend der Sicherheitsvorgaben eingerichtet werden?
- Lassen sich die sicherheitskritischen Parameter wie Authentisierungsanforderungen entsprechend der Sicherheitsvorgaben konfigurieren?
- Lassen sich auf dem Identitäts- und Berechtigungsmanagement-System differenzierte Rechtestrukturen in zugewiesenen Bereichen für das Verwaltungspersonal einrichten (lesen, schreiben, ausführen, ändern)? Werden die für die Rechteverwaltung relevanten Daten manipulationssicher vom Produkt gespeichert?
- Verfügt das Identitäts- und Berechtigungsmanagement-System über eine angemessene Protokollierung? Ist sichergestellt, dass die Protokollierung von Unberechtigten nicht deaktiviert werden kann? Sind die Protokolle selbst für Unberechtigte weder lesbar noch modifizierbar? Ist die Protokollierung übersichtlich, vollständig und korrekt?
- Verfügt das Identitäts- und Berechtigungsmanagement-System über eine übersichtliche und einfach nutzbare Protokollauswertung?

Prüffragen:

- Ist das ausgewählte Identitäts- und Berechtigungsmanagement-System geeignet, den Grundsatz der Funktionstrennung zu realisieren?
- Werden die Anforderungen aus der Kriterienliste durch das ausgewählte Identitäts- und Berechtigungsmanagement-System abgedeckt?

# M 4.500 Sicherer Einsatz von Systemen für Identitäts- und Berechtigungsmanagement

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Systeme für Identitäts- und Berechtigungsmanagement sind integrierte IT-Systeme, mit denen planmäßig und zielgerichtet die digitalen Identitäten für alle Systeme in einer IT-Infrastruktur weitgehend automatisiert werden können. Ein solches System sollte prozessual alle Vorgänge abdecken, die mit dem Anlegen, dem Löschen und dem Ändern von Berechtigungen und Benutzerkennungen zu tun haben. Dazu gehören:

- Identitätsverwaltung
- Rollenverwaltung
- Verwaltung und Pflege von Benutzerkennungen und -berechtigungen: anlegen, ändern und löschen
- Richtlinienverwaltung

Technisch gesehen besteht ein Identitäts- und Berechtigungsmanagement-System aus einer Datenhaltungskomponente (Datenbank), einem Workflow (Berechtigungsfreigabe etc.) und einer Schnittstellenlösung (Verzeichnisdienste etc.), um Berechtigungen einzustellen. Die einzelnen Komponenten müssen ausreichend abgesichert sein, siehe hierzu die spezifischen Bausteine, z. B. B 1.15 *Löschen und Vernichten von Daten*).

Ein Identitäts- und Berechtigungsmanagement-System kann unterschiedlich aufgebaut sein, beispielsweise

- zentral (alle Identitäten an einem Ort konzentriert)
- föderativ (dezentrale Verteilung von Identitäten über die Grenzen der Institution hinaus)

Um den Administrations- und Pflegeaufwand zu reduzieren, sind geeignete Benutzer- und Rechtemanagement-Werkzeuge hilfreich. Zudem sind für die Einrichtung von Berechtigungen automatisierte Antrags- und Vergabeverfahren empfehlenswert, da hierbei häufig viele Genehmigungsschritte zu durchlaufen sind, die zusammengetragen und verfolgt werden müssen.

Zentrale Werkzeuge zum Identitäts- und Berechtigungsmanagement sind ein beliebtes Angriffsziel, da durch eine Manipulation hier der Zugriff auf viele Systeme und Informationen möglich wäre. Oft sind Werkzeuge zum Identitäts- und Berechtigungsmanagement auch so komplex, dass ein erfolgreicher Angriff nur schwer entdeckt werden kann. Daher ist es wichtig Regeln festzulegen, nach denen bei einem echten oder vermuteten Angriff zu verfahren ist (siehe hierzu B 1.8 *Behandlung von Sicherheitsvorfällen*). Bei zentralen Identitäts- und Berechtigungsmanagement-Systemen, bei denen ein permanenter Zugriff für die Berechtigungsprüfung notwendig ist, sind außerdem Maßnahmen zum Notfallmanagement zu ergreifen (siehe M 6.166 *Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System*).

Prüffragen:

- Sind geeignete Werkzeuge für das Identitäts- und Berechtigungsmanagement-System vorhanden?
- Ist das Identitäts- und Berechtigungsmanagement-System ausreichend vor Angriffen geschützt?

# M 5 Maßnahmenkatalog Kommunikation

M 5.58 Auswahl und Installation von Datenbankschnittstellen-Treibern

M 5.59 Schutz vor DNS-Spoofing bei Authentisierungsmechanismen

M 5.60 Auswahl einer geeigneten Backbone-Technologie

M 5.61 Geeignete physische Segmentierung

M 5.62 Geeignete logische Segmentierung

M 5.63 Einsatz von GnuPG oder PGP

M 5.64 Secure Shell

M 5.65 Einsatz von S-HTTP **- entfallen**

M 5.66 Clientseitige Verwendung von SSL/TLS

M 5.67 Verwendung eines Zeitstempel-Dienstes

M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

M 5.69 Schutz vor aktiven Inhalten

M 5.70 Adreßumsetzung - NAT (Network Address Translation)

M 5.71 Intrusion Detection und Intrusion Response Systeme

M 5.72 Deaktivieren nicht benötigter Netzdienste

M 5.73 Sicherer Betrieb eines Faxservers

M 5.74 Pflege der Faxserver-Adressbücher und der Verteillisten

M 5.75 Schutz vor Überlastung des Faxservers

M 5.76 Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation

M 5.77 Bildung von Teilnetzen

M 5.78 Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung

M 5.79 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung

M 5.80 Schutz vor Abhören der Raumgespräche über Mobiltelefone

M 5.81 Sichere Datenübertragung über Mobiltelefone

M 5.82 Sicherer Einsatz von SAMBA **- entfallen**

M 5.83 Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN **- entfallen**

M 5.84 Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation **- entfallen**

M 5.85 Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail **- entfallen**

M 5.86 Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes **- entfallen**

M 5.87 Vereinbarung über die Anbindung an Netze Dritter

M 5.88 Vereinbarung über Datenaustausch mit Dritten

M 5.89 Konfiguration des sicheren Kanals unter Windows

M 5.90 Einsatz von IPSec unter Windows

M 5.91 Einsatz von Personal Firewalls für Clients

M 5.92 Sichere Internet-Anbindung von Internet-PCs

M 5.93 Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs

M 5.94 Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs

M 5.95 Sicherer E-Commerce bei der Nutzung von Internet-PCs

M 5.96 Sichere Nutzung von Webmail

M 5.97 Absicherung der Kommunikation mit Novell eDirectory

M 5.98 Schutz vor Missbrauch kostenpflichtiger Einwahlnummern

M 5.99 SSL/TLS-Absicherung für Exchange 2000 **- entfallen**

M 5.100 Absicherung der Kommunikation von und zu Exchange-Systemen

M 5.101 Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz **- entfallen**

M 5.102 Installation von URL-Filtern beim IIS-Einsatz **- entfallen**

M 5.103 Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz **- entfallen**

M 5.104 Konfiguration des TCP/IP-Filters beim IIS-Einsatz **- entfallen**

M 5.105 Vorbeugen vor SYN-Attacken auf den IIS **- entfallen**

M 5.106 Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz **- entfallen**

M 5.107 Verwendung von SSL im Apache-Webserver **- entfallen**

M 5.108 Kryptographische Absicherung von Groupware bzw. E-Mail

M 5.109 Einsatz eines E-Mail-Scanners auf dem Mailserver

M 5.110 Absicherung von E-Mail mit SPHINX (S/MIME)

M 5.111 Einrichtung von Access Control Lists auf Routern

M 5.112 Sicherheitsaspekte von Routing-Protokollen

M 5.113 Einsatz des VTAM Session Management Exit unter z/OS

# M 5.1 Entfernen oder Deaktivieren nicht benötigter Leitungen

**Verantwortlich für Initiierung:** Leiter Haustechnik
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

Nicht benötigte Leitungen sind solche Leitungen, die für die Funktion des Gebäudes aufgrund von Nutzungsänderungen oder Modernisierungsmaßnahmen nicht mehr erforderlich sind. Diese Leitungen sollten grundsätzlich vollständig entfernt werden, um die Brandlasten im Gebäude auf das notwendige Mindestmaß zu beschränken und um die vorhandenen Trassen nur im erforderlichen Rahmen zu befüllen. Bei der Entfernung von Leitungen ist darauf zu achten, dass die Brandschottungen nach der Entfernung der Kabel wieder fachgerecht verschlossen werden.

Welche Leitungen nicht mehr benötigt werden, darf erst nach sorgfältiger Prüfung durch die zuständige Organisationseinheit entschieden werden. Die Entscheidung ist zu dokumentieren.

Werden die Änderungen der Verkabelungsinfrastruktur parallel zum Dienstbetrieb durchgeführt, sind die Maßnahmen organisatorisch so zu unterstützen, dass die Beeinträchtigungen des Dienstbetriebes auf ein Minimum reduziert werden. Dazu müssen gegebenenfalls auch Wochenend- und Nachtarbeiten eingeplant werden. Wenn in den vorhandenen Trassen nicht genug Platz für die alten und neuen Kabel ist, so sind neue Trassen für die neuen Kabel zu installieren, um die Umschaltzeit von der noch immer betriebenen alten Infrastruktur auf die neue Infrastruktur so kurz wie möglich zu gestalten.

Trassen und Kabel, die mit der vorhandenen Technik sinnvoll als Reserve weiter genutzt werden können, sind in einem betriebsfähigen Zustand zu erhalten.

Nicht mehr benötigte Rangierungen und Patchungen in Verteilern sind zurück zu bauen und in der Dokumentation zu löschen.

Auch Kabel, die nicht mehr benötigt werden, sind möglichst zu entfernen. Falls das nicht möglich ist, weil die Kabel z. B. unter Putz verlegt wurden, müssen sie durch Kurzschließen deaktiviert und gesichert werden.

In der Betriebsdokumentation sind alle Änderungen revisionsfähig zu dokumentieren.

Es empfiehlt sich, in sinnvollen Zeitabständen und in jedem Fall nach Leitungsarbeiten die Änderungen fachkundig zu prüfen. Diese Prüfungen sind zu protokollieren.

Prüffragen:

- Sind nicht mehr benötigte Leitungen grundsätzlich entfernt worden, um Brandlasten zu vermeiden?
- Wird bei der Entfernung der Kabel darauf geachtet, die Brandschotts wieder ordnungsgemäß zu verschließen?
- Erfolgt die Entscheidung zur Entfernung von Kabeln erst nach Prüfung durch die zuständige Organisationseinheit?
- Sind alle Änderungen der Verkabelung in den Betriebsdokumenten revisionssicher dokumentiert?

# M 5.2 Auswahl einer geeigneten Netz-Topologie

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

In der Informationstechnik wird zwischen der physischen und logischen Netztopologie unterschieden. Die physische und die logische Topologie eines Netzes sind nicht notwendigerweise miteinander identisch. Die physische Topologie beschreibt die Anordnung der Geräte und die Führung der Kabel, um die Geräte physisch miteinander zu verbinden. Bei der logischen Netztopologie handelt es sich um die Zuordnung von Datenflüssen. Sie beschreibt, wie die Daten im Netz übertragen werden und kann durch die Konfiguration der aktiven Netzkomponenten fast beliebig gestaltet werden. Durch virtuelle lokale Netze (VLANs) und Virtualisierung lassen sich zusätzliche logische Strukturen in Netzen bilden.

Im Nachfolgenden wird die physische Netztopologie, also die Führung der Kabel und die Platzierung der Verteiler im Gebäude eingehender behandelt.

Die physische Topologie orientiert sich naturgemäß fast immer an den räumlichen Verhältnissen, unter denen das Netz aufgebaut wird. Dies sind unter anderem:

- Standorte der Netzteilnehmer,
- verfügbarer Platz für Trassen und Kabel (siehe M 1.21 *Ausreichende Trassendimensionierung*),
- erforderliche Kabeltypen (siehe M 1.20 *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht*),
- Anforderungen an den Schutz von Kabeln (siehe M 1.22 *Materielle Sicherung von Leitungen und Verteilern*).

Im Allgemeinen werden zwei Grundformen der Netztopologie unterschieden: der Stern und der Bus. Als Erweiterungen lassen sich aus dem Stern eine baumförmige Struktur und aus dem Bus eine ringförmige Struktur ableiten.

Von praktischer Bedeutung bei Neukonzeption und Nachrüstung von IT-Verkabelungen in Gebäuden sind vor allem die Stern- und die Baumstruktur.

Nachfolgend werden die Vor- und Nachteile möglicher Topologien aufgeführt. Weitere denkbare Topologien, die an dieser Stelle nicht genannt sind, können als Spezialfall der betrachteten Strukturen aufgefasst werden.

**Stern**

Bei einem Stern sind alle Teilnehmer des Netzes über eine dedizierte Leitung mit einem zentralen Knoten verbunden. Vor allem bei der "Collapsed Backbone"-Architektur, bei der ein (logischer) zentraler Switch alle Server und Endgeräte verbindet, wird ein Gebäude physisch sternförmig verkabelt.

Diese Topologie bietet folgende Vorteile:

- Die Beschädigung einer Leitung beeinträchtigt nur den Betrieb des daran angeschlossenen Systems.
- Änderungen der Zuordnung von Netzteilnehmern zum Anschlusspunkt am zentralen Knoten sowie Trennungen einzelner Teilnehmer lassen sich zentral durchführen.
- Mit einer Sternverkabelung können alle denkbaren logischen Topologien nachgebildet werden.

- Dem stehen folgende Nachteile der Stern-Topologie gegenüber:
- Bei einem Ausfall des zentralen Knotens fallen alle angeschlossenen IT-Systeme aus.
- Durch die Einzelanbindung jedes Teilnehmers an den zentralen Knoten ist ein hoher Verkabelungsaufwand erforderlich.

Durch die sternförmige Verkabelung können Reichweitenprobleme in Abhängigkeit vom verwendeten Kabeltyp und eingesetzten Protokoll auftreten (siehe M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*). Zur Verlängerung der Reichweite können Verstärker (Repeater) eingesetzt werden. Das verwendete Protokoll gibt die Anzahl möglicher Verstärker je Anbindung sowie bei Parallelbetrieb in einem Kabel vor. Die dadurch zusätzlich entstehenden Investitions- und Betriebskosten sind in der Wirtschaftlichkeitsbetrachtung zu berücksichtigen und mit Alternativen zu vergleichen. Eine Alternative bei Reichweitenproblemen ist die Realisierung der Verkabelung in einer baumförmigen Struktur.

**Baum**

Eine Baumstruktur entsteht durch die Anbindung mehrerer Sterne an einen zentralen Knoten. Die an den dezentralen Netzknoten sternförmig angeschlossenen Netzteilnehmer werden zu Gruppen zusammengefasst. Die dezentralen Netzknoten sind wiederum über eine oder mehrere dedizierte Leitungen an einem zentralen Netzknoten zusammengeführt.

Die Baum-Topologie bietet folgende Vorteile:

- Für den Anschluss der Systeme an die dezentralen Netzknoten gelten die selben Vorteile wie beim Stern.
- Für neue Teilnehmer muss nur im Bereich des dezentralen Netzknotens neu verkabelt werden.
- Bei entsprechender Auslegung der dezentralen Netzknoten ist ein Datenaustausch zwischen den Teilnehmern eines solchen Knotens auch bei einem Ausfall der anderen Knoten möglich.
- Durch die Verbindung der dezentralen Knoten untereinander über eine Leitung reduziert sich der Verkabelungsaufwand.
- Zur Überwindung großer Entfernungen zwischen den Knoten reicht die Verstärkung auf einer Leitung.
- Für die Verbindung der Knoten ist der Einsatz hochwertigerer (meist teurerer) Kabel sinnvoll, mit denen auch größere Distanzen ohne zusätzliche Verstärkung überwunden werden können. Das bringt gegenüber den sonst notwendigen Verstärkern Vorteile in Bezug auf Ausfallsicherheit und unter Berücksichtigung von Investitions- und Betriebskosten häufig auch eine Kostenreduzierung.

Die Baum-Topologie hat folgende Nachteile:

- Bei Störung eines Übergangs zu einem anderen dezentralen Netzknoten wird der Betrieb mit allen daran angeschlossenen Teilnehmern unterbrochen.
- Die erforderliche Dokumentation und das Management der dezentralen Netzknoten ziehen unter Umständen einen erhöhten Gesamtaufwand für den Betrieb des Netzes nach sich.

Typischer Anwendungsfall der Baum-Topologie ist die Anbindung aller Etagenverteiler eines Gebäudes (Tertiärverkabelung in Sterntopologie) an den Gebäudeverteiler (Sekundärverkabelung) einer Gebäudeverkabelung. Bei entsprechenden Redundanzanforderungen können Etagenverteiler auch an mehrere Gebäudeverteiler angeschlossen werden.

**Vermaschte Netztopologie in Stern- und Baumstruktur**

Die zusätzliche Verbindung von zentralen und bei entsprechender Anforderung auch dezentralen Netzknoten wird als Vermaschung bezeichnet. Hierdurch werden redundante Verbindungen aufgebaut, die zur Erhöhung der Ausfallsicherheit und Verfügbarkeit implementiert werden.

**Bus**

Bei einem Bus werden alle Netzteilnehmer an eine gemeinsame Leitung angeschlossen. Dies geschieht im Allgemeinen durch ein zentrales Kabel, an das mit Stichleitungen die einzelnen Teilnehmer angebunden werden.

Neuere Kabeltypen und -spezifikationen unterstützen die bus-förmige Verkabelung nicht mehr. Diese Topologie spielt bei Erstinstallation oder Modernisierung von IT-Verkabelungen keine Rolle mehr.

**Ring**

Der Ring ist aus topographischer Sicht ein Bus, dessen beide Enden miteinander verbunden sind. Eine Sonderform des Rings besteht in der doppelten Ausführung als Doppelring, wie sie z. B. bei FDDI Verwendung findet.

Zwischenzeitlich in Vergessenheit geraten, gewinnt die ringförmigeTopologie bei Erstinstallation oder Modernisierung von IT-Verkabelungen zunehmend wieder an Bedeutung.

**Verkabelung kleinerer Gebäude**

Bei der Ausstattung kleinerer Gebäude ist eine sternförmige Verkabelung von einem zentralen Knoten zu erwägen. Voraussetzung ist, dass die IT-Verkabelung so geführt werden kann, dass jeder Endgeräteanschluss bei Verwendung von Kupferkabeln bis maximal 90 Meter entfernt liegt (gemäß EN 50173 für Anwendungsneutrale Kommunikationskabelanlagen). Gemäß ISO/IEC 11801 beträgt die Maximallänge bei Kupferkabel 90 m (inklusive Patch- und Anschlusskabel 100 m). Diese Maximallänge kann jedoch überschritten werden, wenn die geforderten elektrischen Übertragungsparameter eingehalten werden Wird diese Maximallänge überschritten, so ist nach Norm die Einhaltung der geforderten elektrischen Übertragungsparameter die führende Größe. Eine entsprechende Produktauswahl schafft hier Reserven für ein Überschreiten der maximal verlegbaren Längen. Eine möglichst separate Wegeführung zu allen Endgeräteanschlüssen erhöht die Ausfallsicherheit.

Sind Endgeräteanschlüsse aufgrund der Entfernung oder starker elektrischer Störgrößen nicht mit Kupferverkabelung zu erschließen, finden Lichtwellenleiterkabel (LWL) Anwendung. Abhängig vom Übertragungsprotokoll und von der Faserqualität sind bei Multimode-LWL bis ca. 2 km überbrückbar. Je höher die Übertragungsbandbreite ist, desto kürzer ist die realisierbare Länge. Deutlich größere Reichweiten können bei entsprechender Anforderung durch den Einsatz von Singlemode-LWL erreicht werden.

**Verkabelung größerer Gebäude**

Bei der Verkabelung größerer Gebäude ist eine baumförmige Struktur angemessen. Vom zentralen Verteilpunkt (Gebäudeverteiler) werden sternförmig die Etagen oder Gebäudeabschnitte angebunden. Von den Technikräumen in den Etagen werden wiederum sternförmig die Endgeräte angebunden. Es ergibt sich somit ein zweistufiger Stern. Es sollte überlegt werden, die Topologie in Schichten zu unterteilen, wobei jeder Schicht, ähnlich wie beim OSI-Refe-

renzmodell, konkrete Aufgaben zugewiesen werden. Bewährt hat sich in diesem Zusammenhang das sogenannte hierarchische Modell, bestehend aus Zugangsschicht, Verteilungsschicht und Kernschicht.

**Zugangsschicht**

Die Zugangsschicht dient dazu, Client-Systeme mit dem LAN der Institution zu verbinden. Hierzu werden typischerweise Layer-2-Switches, Wireless Access Points (WAPs) und Router (beispielsweise zur Einwahl in das LAN oder zur Anbindung von Außenstellen) eingesetzt. Es wird empfohlen, den Zugriff auf Netzressourcen bereits in der Zugangsschicht zu steuern, beispielsweise anhand der MAC-Adresse (Port Security).

**Verteilungsschicht**

Die Verteilungsschicht aggregiert den Verkehr aus den einzelnen Etagenverteilern und sollte daher aus leistungsfähigen Layer-3-Geräten (Router oder Multilayer Switches) bestehen. Abhängig vom Einsatzzweck können hier Zugriffskontrolllisten (Access Control Lists, ACLs) konfiguriert werden. Weiterhin sollten die Ergebnisse der Datenflussanalyse berücksichtigt werden, um die Verteilungsschicht angemessen dimensionieren zu können.

**Kernschicht**

Die Kernschicht stellt die Verbindung sowohl zwischen den Gebäuden untereinander als auch mit der Außenwelt her. Ihre primäre Aufgabe ist es, große Datenmengen schnell weiterleiten zu können. Sie sollte daher aus sehr leistungsstarken Layer-3-Geräten bestehen und den Ergebnissen der Datenflussanalyse enstprechend ausgelegt werden.

Um die Ausfallsicherheit zu erhöhen, ist es zu empfehlen, für eine einfache Redundanz die Kernschicht mit redundaten Layer-3-Geräten zu realisieren. Es ist darauf zu achten, dass die Verkabelung auf separaten Trassen zu den Etagen oder Gebäudeabschnitten geführt wird. Ferner ist die Vermaschung der Gebäudeverteiler anzustreben, um Außenanbindungen z. B. von Carrierleitungen einfach auf beiden Gebäudeverteilern einzuspeisen.

Prüffragen:

- Sind die vorhandenen räumlichen Verhältnisse bei der Planung der physischen Netztopologie berücksichtigt?
- Existieren im Rahmen der physischen Netztopologie Regelungen zur Identifizierung von Standorten der Netzteilnehmer?
- Existieren im Rahmen der physischen Netztopologie Regelungen zur Platzdimensionierung von Trassen und Kabeln?
- Existieren im Rahmen der physischen Netztopologie Regelungen zur Auswahl geeigneter Kabeltypen?
- Existieren im Rahmen der physischen Netztopologie Regelungen zu Schutzanforderungen von Kabeln?
- Existieren im Rahmen der physischen Netztopologie Regelungen zu den verwendeten Kabeltypen und Maximallängen?
- Wurde eine den räumlichen Verhältnissen angemessene Form des Leitungsnetzes gewählt (physische Netztopologie: Stern, Baum oder Kombination aus beidem)?
- Ist die geplante Netztopologie für die vorhandenen räumlichen Verhältnisse geeignet?
- Sind Redundanzen für die Anbindung von Etagen oder Gebäudeabschnitten vorhanden?

# M 5.3 Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik, Planer

Die Auswahl des Kabels aus kommunikationstechnischer Sicht wird bestimmt durch die erforderliche Übertragungsrate (Diese wird auch häufig Bandbreite genannt, was allerdings nicht ganz korrekt ist.) und die Entfernung zwischen den Übertragungseinrichtungen. Zusätzlich zu beachten sind die baulichen Gegebenheiten, d. h. die Trassen und die Umgebungsbedingungen, unter welchen die Kabel verlegt und betrieben werden. Da sich auch diese auf den Kabelaufbau auswirken, sind sie bei der Auswahl ebenso zu berücksichtigen. Vor- und Nachteile werden nachfolgend unter Sicherheitsgesichtspunkten beschrieben.

Die heute eingesetzten Übertragungssysteme verwenden für die kabelgebundene Kommunikation elektrische oder optische Schnittstellen. Entsprechend müssen die Kabel als Übertragungsmedium metallene Leiter für die elektrische Übertragung oder Kunststoff oder Glas - Lichtwellenleiter (LWL) - für die optische Übertragung zur Verfügung stellen.

Im Folgenden werden Kupfer- und Lichtwellenleiterkabel näher betrachtet:

**Twisted-Pair-Kabel**

Bei Kupferkabeln für die IT wird ein symmetrischer Kabelaufbau verwendet. Bei diesem Kabelaufbau werden jeweils zwei Adern miteinander zu einem Paar verdrallt und vier dieser Paare zu einem Kabel (Twisted-Pair-Kabel, TP) miteinander verseilt. Der Durchmesser der Adern, deren Isoliermaterial inklusive der Farbstoffe, die Art der Verseilung und Abschirmung dieser Paare unterscheidet die Kabel hinsichtlich ihrer möglichen Bandbreite und ihrer Störunempfindlichkeit. Für eine einheitliche Bezeichnung der Kabeltypen schlägt die ISO/IEC 11801 "Informationstechnik - Anwendungsneutrale Standortverkabelung" in der 2. Ausgabe folgende Vereinheitlichung der Typenbezeichnungen vor, welche die Konstruktionselemente von außen nach innen gelesen eindeutig bestimmt:

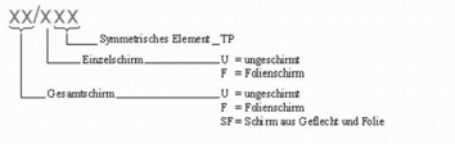



Abbildung: Systematik der Typbezeichnung von Kupferkabeln

Zum Beispiel:

- das ungeschirmte U/UTP,
- das ungeschirmte mit einem Gesamtschirm für alle Aderpaare (F/UTP oder SF/UTP),
- das geschirmte, bei dem lediglich die einzelnen Aderpaare abgeschirmt sind (U/FTP) - früher auch als **P**aare **i**n **M**etall**f**olie (PiMf) bezeichnet - und
- vorgenannter Aufbau mit einer zusätzlichen Gesamtabschirmung (F/FTP, S/FTP und SF/FTP).

Die Normen ordnen Grenzwerte für die Übertragungseigenschaften von Kabeln und Anschlusskomponenten Kategorien und Klassen zu. Die Kategorien beschreiben die Anforderungen und Grenzwerte an die einzelnen Elemente der Verkabelungsinfrastruktur, die Klassen regeln diese für das installierte Gesamtsystem.

Die Übertragungseigenschaften für die einzelnen Komponenten sind derzeit in die Kategorien 1 bis 7 eingeteilt. Hierbei gilt, je höher die Kategorie desto höher ist auch die mögliche Übertragungsbandbreite.

Hohe Übertragungsqualitäten lassen sich zuverlässig nur erzielen, wenn eine in sich harmonische Kombination aus Kabel und Anschlusskomponenten (Buchsen und Stecker) gewählt und fachmännisch installiert wurde. Die Geräte "erkennen" keine verlegte Länge sondern reagieren auf elektrische Signale. Daher sind die elektrischen Grenzwertvorgaben für die Strecken die führende Größe. Gemäß ISO/IEC 11801 beträgt die Maximallänge bei Kupferkabeln 90 m (inklusive Patch- und Anschlusskabel 100 m). Diese Maximallänge kann jedoch überschritten werden, wenn die geforderten elektrischen Übertragungsparameter eingehalten werden.

Das TP-Kabel ist durch die Verkabelungsnormen Standard bei der Verkabelung im sogenannten Access-Bereich auf der Etage. Dieser Kabeltyp hat folgende Vorteile:

- TP-Kabel, insbesondere deren Konfektion, sind bei geringerem Bandbreitenbedarf im Vergleich zu LWL relativ billig.
- TP-Kabel lassen sich relativ einfach verlegen und konfektionieren.
- TP-Kabel können als Universalverkabelung angesehen werden, da andere Dienste ohne größeren technischen Aufwand hierüber genutzt werden können (z. B. Telefonie).
- Die Installationen können messtechnisch leicht überprüft werden.
- TP-Kabel ermöglichen die Stromversorgung von Geräten, die nach den Vorgaben der Spezifikation "Power over Ethernet" (PoE) versorgt werden.

Dem stehen folgende Nachteile gegenüber:

- Durch die bei der Datenübertragung in den Kabeln fließenden Wechselströme und die im Kabel immer vorhandenen geringen Unsymmetrien in der Verseilung der Adern werden elektromagnetische Felder erzeugt, welche in der Umgebung wahrgenommen werden (Abhörgefahr) und Systeme stören können. Aber auch elektromagnetische Felder der Umgebung können wiederum die Übertragung im Kabel stören.
  Durch die Verwendung von Schirmen im Kabelaufbau werden diese Effekte minimiert (vergleiche U/UTP bis SF/FTP). Die Angaben zum Mindestabstand zwischen unterschiedlichen Kabeln, Leitungen und Systemen sowie zur Erdung von Schirmen sind zu beachten.
- Die vorgenannten Effekte wirken auch innerhalb des Kabels. Ungeschirmte Installationskabel (U/UTP) bieten vor dem sogenannten Übersprechen zwischen einzelnen Paaren den geringsten Schutz. Hier wirkt lediglich die Verseilung der einzelnen Adern.

**Lichtwellenleiter (LWL)**

Bei der Übertragung von Signalen in Lichtwellenleitern wird Licht vom sichtbaren bis stark infraroten Bereich verwendet. Zur Erzeugung dieses Lichts werden Dioden oder Laser eingesetzt. Diese wandeln das elektrische Signal in Lichtmoden unterschiedlicher Richtungen bzw. unterschiedlich starker Bündelung.

Der Lichtwellenleiter, auch Faser genannt, besteht aus dem zur Übertragung verwendeten Kern- und einem umgebenden Mantelmaterial. Die Materialien unterscheiden sich in der sogenannten Brechzahl.

Die Verkabelungsstandards definieren für Multimode-LWL die Kategorien OM-1, OM-2 und OM-3. Gegenstand dieser Spezifikationen sind Lichtwellenleiter mit Gradientenprofil der Brechzahl und einem Kern/Mantel-Nenndurchmesser von 50/125 oder 62,5/125 Mikrometern. Für Singlemode-LWL gilt die Kategorie OS-1. Der Kern/Mantel-Nenndurchmesser von Singlemode-LWL beträgt 9/125 Mikrometer.

Während sich in Multimodefasern mehrere Lichtmoden eines Signals einkoppeln, koppelt sich in Singlemodefasern aufgrund des geringen Kerndurchmessers nur eine Lichtmode ein. Dadurch unterscheiden sich die Fasertypen in den möglichen Bandbreiten und den maximalen Längen, die ohne zusätzliche Verstärker erreicht werden können. Die Fasertypen können bei der Verbindung von Systemen in einigen Fällen nicht gemischt werden.

Eingesetzt werden Lichtwellenleiter unter anderem in folgenden Bereichen:

- bei der Überbrückung großer Entfernungen in Weitverkehrsnetzen (Wide Area Network - WAN),
- in Stadtnetzen (Metropolitan Area Network - MAN),
- in Unternehmensnetzen (Local Area Network - LAN) für die Verbindungen zwischen den Gebäuden und in die Etagen,
- in Bereichen mit hohen elektromagnetischen Störstrahlungen sowie
- in Speichernetzen (Storage Area Network - SAN) in Rechenzentren zur Verbindung der Systeme zur Übertragung höchster Datenraten.

Entscheidend für die Qualität der Verbindungen ist auch die Auswahl der Steckverbinder für die Glasfaserinfrastruktur.

Die Verwendung von Lichtwellenleitern bietet folgende Vorteile:

- LWL erlauben hohe Bandbreiten in Verbindung mit großen überbrückbaren Entfernungen im Vergleich zu Kupferkabeln.
- LWL sind unempfindlich gegenüber elektromagnetischen Feldern.
- Es entstehen keinerlei Übersprecheffekte wie bei elektrischen Leitern.
- LWL bieten eine potentialfreie Verbindung zwischen den Endstellen der Verkabelung.
- Ein Abhören ist nur mit hohem technischen Aufwand möglich.
- Kabel mit hohen Faserzahlen können kompakter gebaut werden als vergleichbare Kupferkabel bei deutlich geringerem Gewicht.
- Die Brandlast ist bei LWL im Vergleich zu Kupferkabeln geringer. Die Gründe hierfür sind die im Vergleich geringere erforderliche Menge an Material, der Materialmix im Kabelaufbau und die möglichen hohen Faserzahlen ohne die Bauform massiv zu vergrößern.

Der Einsatz von Lichtwellenleitern ist jedoch mit folgenden Nachteilen verbunden:

- Der Installationspreis für LWL liegt vor allem durch die notwendigen Spleißarbeiten höher als bei Kupferkabeln.
- Die Koppel-Komponenten zum Betrieb von LWL, insbesondere für Singlemode-LWL, sind teurer als solche für Kupferkabel.
- Die LAN-Anbindung über TP-Kabel wird von gängigen Arbeitsplatz-Computern in der Grundausstattung meist besser unterstützt als über LWL. Arbeitsplatz-Clients werden derzeit meist über Kupferkabel an das LAN angeschlossen.

Eine Übersicht über die Längenbeschränkungen von Kabeln für einige der üblichen Protokolle gibt die folgende Tabelle:

| **Netzzugangs-protokoll** | | **Kabeltyp** | **max. Länge** |
|---|---|---|---|
| Ethernet | 10Base-T | TP | 100 m |
| | 10Base-FL Mono-mode | Multimode LWL | 2.000 m |
| | 10Base-FL Sin-glemode | Singlemode LWL | 25.000 m |
| Fast Ethernet | 100Base-TX | TP Cat 5 | 100 m |
| | 100Base-FX | Multimode LWL | 400 m |
| Gigabit Ethernet | 1000Base-T | TP Cat 5e | 100 m |
| | 1000Base-SX | Multimode LWL | 550 m |
| | 1000Base-LX | Multimode LWL | 550 m |
| | 1000Base-LX | Singlemode LWL | 10.000 m |
| 10 Gigabit Ether-net | 10GBase-T | TP Cat 6a | 100 m |
| | 10GBase-LX4 | Multimode LWL | 300 m |
| | 10GBase-LW4 | Singlemode LWL | 10.000 m |
| | 10GBase-SR | Multimode LWL | 300 m |
| | 10GBase-LR | Singlemode LWL | 10.000 m |
| | 10GBase-ER | Singlemode LWL | 40.000 m |
| | 10GBase-LW | Singlemode LWL | 10.000 m |

Tabelle: Längenbeschränkungen gängiger Verkabelungstypen

Zu beachten ist, dass hier die jeweilige maximale Länge genannt ist. Diese setzt sich häufig aus dem eigentlichen Installationskabel und den Anschlusskabeln (Patchkabeln) zusammen. Für 1000Base-T sollte also z. B. die Länge des Installationskabels 90 m nicht überschreiten, um genügend Längenspielraum für Patchkabel zu haben.

**Zusammenfassung**

Im WAN und MAN sind LWL-Verkabelungen mit Singlemode-Fasern Standard. In der LAN-Verkabelung sind diese Fasern heute zwischen den Gebäuden und bei weiter entfernten Etagenverteilern aufgrund der Längeneinschränkungen von 10 Gigabit Ethernet unbedingt zu empfehlen.

Der Einsatz von LWL bis zum Arbeitsplatz und damit der Wegfall der Kupferverkabelung auf der Etage kann nur in einer Gesamtbetrachtung bewertet werden.

Für den Einsatz von LWL sprechen:

- die günstigere Brandlastsituation,
- die bessere Abhörsicherheit von LWL,
- EMV-Neutralität,
- mögliche Einsparungen im Trassenbau,

- Flächeneinsparungen durch die geringere Zahl erforderlicher Verteilerräume und damit Einsparungen in der Elektroverkabelung für die Verteilerräume,
- Vereinfachungen im USV- und Erdungskonzept.

Gegen LWL sprechen andererseits:

- die höheren Kosten für Schnittstellenkarten in den Endgeräten und in den Netzkomponenten,
- die meist weiter bestehende Notwendigkeit einer Telefonverkabelung über Kupferkabel,
- mögliche Einschränkungen für die Umsetzung von Power-over-Ethernet für IP-Telefonie oder auch für den Anschluss von Access-Points im WLAN.

Für Neuinstallationen wie auch bei Modernisierungen ist es daher zu empfehlen, mit einem Fachplaner die Anforderungen aus technischer, sicherheitstechnischer und wirtschaftlicher Sicht zu erarbeiten und auszuwerten (siehe auch M 5.2 *Auswahl einer geeigneten Netz-Topologie*).

Prüffragen:

- Berücksichtigt die Auswahl der Kabeltypen sowohl kommunikations- und sicherheitstechnische als auch bauliche Anforderungen?

# M 5.4 Dokumentation und Kennzeichnung der Verkabelung

**Verantwortlich für Initiierung:** Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

Für die Wartung, Fehlersuche, Instandsetzung und für eine erfolgreiche Überprüfung der Verkabelung ist eine gute Dokumentation und eine eindeutige Kennzeichnung aller zugehörigen Komponenten erforderlich. Die Güte dieser Revisionsdokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit der Unterlagen. In jedem Fall ist ein Verantwortlicher für die Dokumentation der Verkabelung zu benennen.

Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen. Andere Informationen können in Tabellenform oder Schemaplänen geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander. Die Dokumentation sollte somit aus beschreibenden Unterlagen, Listen und Plänen bestehen.

Die beschreibenden Unterlagen, wie z. B. eine Dokumentationsrichtline, enthalten die Informationen über die Abläufe zur Dokumentation, Bezeichnungs- und Kennzeichnungsregelungen. In dieser sollte beispielsweise in allgemeiner Form beschrieben werden, welche Listen und Pläne zu erstellen sind und wie diese auch revisionssicher zu führen sind.

In die Listen- und Bestandspläne sind alle das Netz betreffenden Sachverhalte aufzunehmen. Die Listen sollten unter anderem folgende Informationen enthalten:

- Liefer- und Komponenteninformationen,
- genaue Kabeltypen (bei Lichtwellenleiterkabel auch Faserqualität),
- nutzungsorientierte Kabelkennzeichnung,
- Standorte von Zentralen und Verteilern mit genauen Bezeichnungen und Zugangsregelungen mit Ansprechpartnern zu den Gebäuden und Räumlichkeiten,
- Belegungspläne aller Rangierungen und Verteiler,
- Nutzung aller Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- technische Daten von Anschlusspunkten,
- Gefahrenpunkte,
- vorhandene und zu prüfende Schutzmaßnahmen.

Die Bestandspläne bestehen typischerweise aus:

- Standortübersichten und bemaßten Lageplänen mit der genauen Führung der Trassen und der Primärverkabelung,
- Gebäudeschnitten als Schemapläne und bemaßten Etagengrundrissplänen mit der genauen Lage und Führung der Verteilerräume, Trassen und Kabel sowie den IT-Anschlüssen pro Raum in z. B. Brüstungskanälen und/oder Bodenauslässen,
- Technikraumplänen mit Raumlayout, Doppelbodenraster und Schrankpositionierung, Stromverteilung und Potentialausgleichschiene sowie einer vorhandenen Klimatisierung,
- Schrankansichtsplänen zur lagerichtigen Beschreibung der eingebauten passiven und aktiven Komponenten inklusive der Steckdosenleisten,
- physikalischen und logischen Verbindungsplänen des Netzes.

Es muss möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.

Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, dass alle Arbeiten am Netz rechtzeitig und vollständig demjenigen bekannt werden, der die Dokumentation führt. Es ist z. B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Funktion abhängig zu machen.

Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff zu regeln. Weiterhin sind die Kabel selbst zu kennzeichnen, um die Informationen aus den Bestandsplänen zuordnen zu können. Die Beschriftung der Kabel muss an beiden Enden erfolgen. Im Bedarfsfall kann die Beschriftung auch sich mehrfach wiederholend am Kabel angebracht werden, um es auch bei der Nachverfolgung in der Trasse eindeutig zu identifizieren. Es sind Kennzeichnungsfelder oder Beschriftungsbänder einzusetzen, die manuell oder maschinell dauerhaft lesbar beschriftet werden. Eine Beschriftung mit Folienstift ist häufig nicht ausreichend.

Die Kabel und Leitungen sollten immer so beschriftet oder gekennzeichnet werden, dass daraus lediglich eine Referenzierung in die Dokumentation erfolgen kann. Eine Kennzeichnung, die einen direkten Rückschluss auf die Bedeutung des Kabels oder der Leitung zulässt, ist unbedingt zu vermeiden, soweit dies nicht auf Grund von anderen Regelungen erforderlich ist.

Sinnvollerweise wird bereits bei der Planung von Verkabelungsmaßnahmen in einem solchen Tool mit der Dokumentation begonnen und diese nach der Realisierung vom Planungsstatus in den Produktivstatus übernommen. Auf diesem Wege ist es leichter, die Nutzer der Dokumentation über bevorstehende Änderungen zu informieren und die Dokumentation aktuell zu halten.

Prüffragen:

- Gibt es einen Verantwortlichen für die Dokumentation der Verkabelung (im Hinblick auf Vollständigkeit, Aktualität und Lesbarkeit)?
- Existieren Listen- und Bestandspläne mit allen das Netz betreffenden Informationen?
- Wird sichergestellt, dass alle Arbeiten an der Verkabelung dem verantwortlichen Mitarbeiter für die Dokumentation rechtzeitig und vollständig mitgeteilt werden?
- Wird die Dokumentation der Verkabelung sicher aufbewahrt und der Zugriff entsprechend geregelt?
- Werden die Kabel beschriftet, so dass eine Zuordnung der Informationen aus den Bestandsplänen möglich ist?

# M 5.5 Schadensmindernde Kabelführung

**Verantwortlich für Initiierung:** Planer, Leiter Haustechnik, Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik

Bei der Planung von Kabeltrassen ist darauf zu achten, dass erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollten Trassen nur in den Bereichen verlegt werden, die ausschließlich innerhalb der Räumlichkeiten einer Institution zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollten immer so verlegt werden, dass sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

Der Standort von Geräten sollte so gewählt werden, dass die daran angeschlossenen Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen.

Grundsätzlich ist bei Geräteanschlussleitungen auf eine ausreichende Zugentlastung der Kabel in den Steckern zu achten. Bisweilen kann es sinnvoll sein, auf die vorgesehene Verschraubung von Steckern zu verzichten. Bei überhöhter Zugbelastung werden dann nur Steckverbindungen auseinander gerissen und nicht die Stecker-Kabel- oder Stecker-Geräte-Verlötung.

Tiefgaragen stellen ein großes Problem für eine schadensmindernde Kabelführung dar. Durch die Sicherheitsschaltungen und die langen Offenzeiten von Einfahrtstoren ist der Zutritt von Fremdpersonen zu Tiefgaragen nie auszuschließen. Durch die in der Regel geringen Deckenhöhen ist es mit einfachen Mitteln möglich, sich Zugriff zu dort verlaufenden Trassen zu verschaffen. Durch Trassen im Fahrbereich kann die zulässige Fahrzeughöhe unterschritten werden. Beschädigungen oder Zerstörungen der Trassen und Kabel durch zu hohe Fahrzeuge sind dann nicht auszuschließen.

Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, dass Kabel nicht in Fußboden-, Decken- oder Wandkanälen durch deren Bereiche führen. Alle Kanalsysteme sind gegenüber den fremdgenutzten Bereichen mechanisch fest zu verschließen. Besser ist es, sie an den Bereichsgrenzen enden zu lassen.

Durch Bereiche mit hoher Brandgefahr sollten möglichst keine Kabel verlegt werden. Ist dies nicht möglich und ist der Funktionserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung zu versehen. Ist der Funktionserhalt nur für einzelne Kabel erforderlich, sollte dafür ein entsprechendes Kabel und die dazu gehörige Befestigung gewählt werden. Ein Funktionserhalt-Kabel kann nie allein die geforderte Funktion erfüllen. Die Kabelanlage ist als Ganzes zu betrachten, dazu gehört auch die Befestigung, wie Trassen, Schellen oder Rohre. Ebenso wichtig ist, dass die Kabelanlage nicht durch darüber befindliche Teile ohne Funktionserhalt zerstört werden kann, wenn diese im Brandfall herabfallen.

In Produktionsbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfeldern zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für den Schutz der Kabel gilt sinngemäß das gleiche wie bei der Brandabschottung.

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabeln (ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

Leitungen müssen so verlegt sein, dass ein Sturm sie nicht bewegen kann. Beispielsweise sollte dafür Sorge getragen werden, dass Leitungen auf freien Dachflächen mindestens alle 5m angemessen befestigt sind. Hierbei sollte berücksichtigt werden, dass bei einem Sturm starke Kräfte auf die Kabel oder Kabelstränge wirken können. Außerdem müssen Leitungen geschützt gegen mechanische Beschädigungen verlegt werden, da Gegenstände darauf fallen könnten. Leitungen auf Dachflächen oder in Bereichen, die mit Lamellenwänden verkleidet sind, sollten daher immer in Schutzrohren verlegt sein.

Prüffragen:

- Sind Trassen und einzelne Kabel so verlegt worden, dass sie vor Beschädigungen durch Personen, Fahrzeuge und Maschinen ausreichend geschützt sind?
- Wurde bei Geräteanschlüssen auf eine ausreichende Zugentlastung der Kabel geachtet?
- Ist darauf geachtet worden, dass keine Kabel durch Bereiche mit hoher Brandgefahr verlegt werden oder die Kabel zumindest einen ausreichenden Funktionserhalt aufweisen?
- Sind die Leitungen im Außenbereich so verlegt beziehungsweise befestigt, dass sie vor Sturm geschützt sind?

# M 5.6 Obligatorischer Einsatz eines Netzpasswortes

Diese Maßnahme ist mit Version 2005 entfallen.

# M 5.7 Netzverwaltung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Netze können zentral oder lokal an den einzelnen Knoten verwaltet werden. Das ist neben den technischen Möglichkeiten davon abhängig, wer den Netzknoten administriert. In jedem Fall ist eine zentrale Koordinierung aller Netzaktivitäten einer Behörde oder eines Unternehmens notwendig, damit Redundanzen vermieden werden. Zentral gesteuert werden sollten:

- die Auswahl und Verlegung der Kabel,
- die Auswahl der eingesetzten IT-Systeme und Anwendungen, um Unverträglichkeiten zu vermeiden,
- die zentrale Vergabe von Netzadressen und Benutzer-IDs,
- die organisatorische Zuteilung von Netzkomponenten z. B. zu Abteilungen.

Die einzelnen Netzknoten und die dort angeschlossenen IT-Systeme können auch lokal verwaltet werden.

Die Aufgaben- und Verantwortungsbereiche der Systemverwalter müssen dabei klar spezifiziert und eindeutig geregelt sein (siehe auch M 2.26 *Ernennung eines Administrators und eines Vertreters*).

Prüffragen:

- Wird das Netz von einer zentralen Instanz verwaltet, koordiniert und administriert?
- Sind die Aufgaben- und Verantwortungsbereiche der Netz-Administratoren eindeutig geregelt?

# M 5.8 Regelmäßiger Sicherheitscheck des Netzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Der Netzadministrator sollte regelmäßig, mindestens monatlich, einen Sicherheitscheck des Netzes durchführen. Für praktisch alle Betriebssysteme sind Programme verfügbar oder bereits im Lieferumfang des Betriebssystems oder der Betriebssystem-Distribution enthalten, die entsprechende Funktionen zur Verfügung stellen.

Bei einem solchen Sicherheitscheck sollten beispielsweise folgende Punkte überprüft werden:

- Gibt es Benutzer, deren Passwort nicht den erforderlichen Vorgaben der Passwort-Richtlinie entsprechen?
- Gibt es Benutzer, die längere Zeit das Netz nicht mehr benutzt haben?
- Welche Benutzer besitzen die selben Rechte wie der Administrator?
- Sind Systemprogramme und Systemkonfigurationen unverändert und konsistent?
- Entsprechen die Berechtigungen von
  - Systemprogrammen und Systemkonfigurationen
  - Anwendungsprogrammen und -daten
  - Benutzerverzeichnissen und -daten
  - den Vorgaben der Sicherheitsrichtlinie?
- Welche Netzdienste laufen auf den einzelnen Systemen? Sind sie den Vorgaben der Sicherheitsrichtlinie entsprechend konfiguriert?

Bei einem regelmäßigen Sicherheitscheck können auch Penetrationstests im lokalen Subnetz integriert werden. Dabei kann der "Grad" der Penetrationstests variiert werden (beispielsweise: wöchentlich einfache automatisierte Überprüfungen, monatlich gründlicherer Test mit teilweise manueller Durchführung, einmal jährlich ein grundlegender Test des gesamten Netzes).

Bei der Durchführung des Sicherheitschecks sollte der Netzadministrator seine Schritte so dokumentieren, dass diese (beispielsweise bei einem Verdacht auf ein kompromittiertes System) nachvollzogen werden können. Ebenso zu dokumentieren, sind die Ergebnisse des Sicherheitschecks. Außerdem muss Abweichungen vom "Sollzustand" nachgegangen werden.

Prüffragen:

- Werden regelmäßige Sicherheitschecks (mindestens monatlich) des Netzes durchgeführt?
- Werden bei Sicherheitschecks alle wichtigen Punkte berücksichtigt?
- Werden die Durchführung und die Ergebnisse der Sicherheitschecks dokumentiert?
- Wird Abweichungen vom Sollzustand bei Sicherheitschecks nachgegangen und werden weitere Maßnahmen ergriffen?

# M 5.9 Protokollierung am Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die am Netz-Server mögliche Protokollierung ist in einem sinnvollen Umfang zu aktivieren. In regelmäßigen Abständen muss der Netzadministrator die Protokolldateien des Netz-Servers überprüfen. Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen,
- Stromausfall,
- Daten zur Netzauslastung und -überlastung.

Wie viele Ereignisse darüber hinaus protokolliert werden, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab. Je höher deren Schutzbedarf ist, desto mehr sollte protokolliert werden.

Da die Protokoll-Dateien mit der Zeit sehr umfangreich werden können, sollten die Auswertungsintervalle so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist. Um eine sinnvolle Auswertung zu ermöglichen, sollte jeder Protokoll-Eintrag Benutzer-Kennung bzw. Prozessnummer, Kennzeichnung des Endgeräts, Datum und Uhrzeit enthalten.

Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokoll-Dateien beachtet werden müssen. Um die Nachvollziehbarkeit von Aktionen zu gewährleisten, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch eine Löschungspflicht geben (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Prüffragen:

- Ist die Protokollierung am Netz-Server aktiviert?
- Werden die Protokolldateien regelmäßig vom Netzadministrator ausgewertet?
- Werden die Auswertungen dokumentiert?
- Wurden die gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokolldateien beachtet?

# M 5.10 Restriktive Rechtevergabe

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zugriffsrechte auf Dateien, die auf der Festplatte des Netz-Servers gespeichert sind, müssen restriktiv vergeben werden. Jeder Benutzer erhält nur auf die Dateien ein Zugriffsrecht, die er für seine Aufgabenerfüllung benötigt. Das Zugriffsrecht selbst wiederum wird auf die notwendige Zugriffsart beschränkt (Dazu siehe auch M 2.5 *Aufgabenverteilung und Funktionstrennung*, M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*). So ist es zum Beispiel in den seltensten Fällen notwendig, ein Schreibrecht auf Programmdateien zu vergeben.

Meist darf über die Vererbung von Rechten auf Dateien in Unterverzeichnissen zugegriffen werden, wenn ein Zugriffsrecht auf das übergeordnete Verzeichnis bestand. Daraus ergibt sich, dass Zugriffsrechte auf höchster Ebene (Volume-Ebene) nur sehr eingeschränkt erteilt werden sollten. Insbesondere ist bei der Installation neuer Softwareprodukte die Rechtevergabe erneut zu überprüfen.

Sind die PCs mit Diskettenlaufwerken ausgestattet, so ist auf restriktive Rechtevergabe besonderen Wert zu legen.

Sollte der Speicherplatz des Netz-Servers gering ausgelegt sein, kann eine Beschränkung der maximalen Speicherkapazität, die ein Benutzer auf dem Netz-Server belegen darf, eingestellt werden.

Prüffragen:

- Erfolgt auf zentralen Servern eine restriktive Rechtevergabe?

# M 5.11 Server-Konsole sperren

Diese Maßnahme ist mit Version 2005 entfallen.

# M 5.12 Einrichtung eines zusätzlichen Netzadministrators

Diese Maßnahme ist mit Version 2005 entfallen.

# M 5.13 Geeigneter Einsatz von Elementen zur Netzkopplung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, IT-Sicherheitsbeauftragter

Geräte zur Netzkopplung, wie Router, Switches oder Sicherheitsgateways, verbinden nicht nur Netze, sondern werden auch dazu eingesetzt, um Netze physisch oder logisch zu segmentieren. Durch die Aufteilung von großen Netzen in kleinere Teilnetze kann z. B. die Verfügbarkeit verbessert werden, da ein Fehler nur einen begrenzten Bereich des Netzes betrifft und dort schneller lokalisiert werden kann. Bei zunehmender Anzahl von IT-Systemen können Antwortzeiten inakzeptabel und eine Teilnetzbildung zur Lasttrennung notwendig werden. Ein weiterer Grund für die Segmentierung kann der Schutz von sensitiven Informationen sein, so dass diese nicht auf dem Gesamtnetz verfügbar sind.

Um sich vor externen Angreifern zu schützen, kann es sinnvoll sein, einen Transfer von Paketen nur vom sicheren ins unsichere Netz zuzulassen, zum Schutz von vertraulichen Daten kann es andererseits sinnvoll sein, keinen Transfer von Paketen vom sicheren ins unsichere Netz zuzulassen.

Die Aufteilung in Netzsegmente bzw. die Netzkopplung kann auf verschiedenen Schichten nach dem OSI-Modell erfolgen. Netzkoppelkomponenten in der physischen Schicht (Schicht 1) des OSI-Modells sind z. B. Repeater, in der Sicherungsschicht (Schicht 2) z. B. Bridges oder Switches, auf der Vermittlungsschicht (Schicht 3) z. B. Router und auf der Anwendungsschicht (Schicht 7) im Allgemeinen Sicherheitsgateways.

Unter Berücksichtigung der Anforderungen zur Netzsegmentierung müssen geeignete Netzkopplungselemente nach dem OSI-Referenzmodell ausgewählt werden.

**Repeater**

Repeater arbeiten auf der Schicht 1 des OSI-Referenzmodells und sind einfache Signalverstärker. Dadurch kann die maximale Kabellänge eines bestehenden Netzsegmentes verlängert werden oder es können mehrere Netzsegmente verbunden werden. In früheren LAN-Implementationen wurden Repeater beispielsweise eingesetzt, um bei Ethernet auf Koaxialkabel die maximale Kabellänge auf über 185 m bzw. 500 m (für Thin- bzw. Thick-Ethernetkabel) zu verlängern.

**Bridges**

Bridges verbinden Netze auf der Ebene 2 des OSI-Referenzmodells. Eine Bridge verbindet zwei Netze, die in der Regel dasselbe Logical Link Control (LLC) Protokoll benutzen, aber unterschiedliche Medium Access Control (MAC) Protokolle. So kann z. B. ein Netz, das auf Ethernet basiert mit einem Token-Ring-Netz mithilfe einer Bridge verbunden werden. Eine solche Bridge wird dann Translation-Bridge oder T-Bridge genannt.

Hierdurch ergeben sich drei wesentliche Vorteile:

- Die Bridge trennt Collision-Domains, d. h. performanceverringernde Kollisionen bei CSMA/CD-basierten Netzen gelangen nicht in das andere Segment.

- Eine Bridge leitet nur diejenigen Datenpakete in ein anderes Segment, die dort auch ihre Zieladresse haben. Hierdurch bleibt der Datenverkehr auf das jeweils notwendige Segment beschränkt, wodurch die Abhörsicherheit steigt.
- Schließlich steigt dadurch auch der Datendurchsatz in jedem Segment, da auf jeder Seite der Bridge unabhängig Daten übertragen werden können und somit eine Lasttrennung erfolgt.

Repeater und Bridges werden in modernen Netzen nur noch vereinzelt eingesetzt.

**Switches**

Um Netze auf der Schicht 2 des OSI-Referenzmodells zu segmentieren, werden heutzutage hauptsächlich Switches eingesetzt. Viele Produkte implementieren zusätzlich auch eine Switching-Funktionalität auf der Schicht 3 des OSI-Referenzmodells, erlauben also hiermit auch eine Schicht 3 Segmentierung. Ähnlich wie Bridges verbinden Switches mehrere logische LAN-Segmente miteinander. Im Gegensatz zu Bridges jedoch, bei denen sich mehrere Endgeräte einen Bridge-Port teilen müssen, bildet bei Switches jedes Endgerät eine eigene Kollisionsdomäne.

Somit beruht der Verbindungsaufbau auf den tatsächlichen Erfordernissen. Damit kann jedes angeschlossene Segment mit allen anderen unbeeinflusst von dem Verkehr und der Last der anderen Segmente kommunizieren, solange das entsprechende Segment nicht bereits anderweitig belegt ist. Switches bieten sich vor allem zur Lasttrennung und als zentrale Kopplungskomponente von mehreren Teilsegmenten an. Durch die Kaskadierung von Switches, d. h. durch den Anschluss von nachgeordneten Switches an einen zentralen Switch, lassen sich bei geeigneter Wahl der logischen Netzstruktur sehr leistungsfähige Netze bilden.

Viele Produkte unterstützen inzwischen auch ein Switching auf der Schicht 3 und Schicht 4 des OSI-Referenzmodells (Multi Layer Switching - MLS). Layer-3- bzw. Layer-4-Switches sind Switches, die zusätzlich eine Routing-Funktionalität bieten. Layer-2-Switches verwenden die Ziel-MAC-Adresse im MAC-Header eines Paketes um zu entscheiden, zu welchem Port Datenpakete weitergeleitet werden. Ein Layer-3-Switch behandelt Datenpakete beim ersten Mal wie ein Router (Ziel-IP-Adresse im IP-Header). Alle nachfolgenden Datenpakete des Senders an diesen Empfänger werden daraufhin jedoch auf Schicht 2 des OSI-Referenzmodells (Ziel-MAC-Adresse im MAC-Header) weitergeleitet. Dadurch kann ein solcher Switch einen wesentlich höheren Durchsatz als ein herkömmlicher Router erzielen.

Ein weiteres Unterscheidungsmerkmal zwischen einem Router und einem Layer-3-Switch ist die Anzahl von Ports zum Anschluss von einzelnen Endgeräten. Ein Layer-3-Switch verfügt in der Regel über eine wesentlich größere Portdichte. Durch die Routing-Funktion können Layer-3 oder Layer-4-Switches in lokalen Netzen herkömmliche LAN-to-LAN-Router ersetzen.

Bei der Auswahl von Switches, mit denen ein Collapsed Backbone realisiert werden soll, muss die zur Verfügung gestellte Portdichte berücksichtigt werden. Bei einem "Collapsed backbone" sollte es vermieden werden, mehrere Switches einzusetzen, die nicht über eine gemeinsame (Hochgeschwindigkeits-) Backplane verfügen (siehe M 5.2 *Auswahl einer geeigneten Netz-Topologie*).

**Router**

Router trennen bzw. verbinden Netze auf der Schicht 3 des OSI-Referenzmodells. Damit arbeiten Router nicht mehr protokolltransparent, sondern müssen die im Einsatz befindlichen Protokolle auf der Vermittlungsschicht auch verarbeiten können. Dadurch verlangsamen Router den Datenverkehr zwischen zwei verbundenen Teilnetzen, da sie jedes Paket auf der Schicht 3 auswerten müssen.

Aufgrund ihrer Fähigkeit, Protokolle zu verarbeiten und diese umzusetzen, werden Router vor allem zur LAN-LAN-Kopplung und zur Anbindung eines LANs an ein WAN genutzt. Ein Router kann beispielsweise zwei LANs über eine ISDN-Leitung miteinander verbinden. Hierbei wird das LAN-Protokoll unverändert in das WAN-Protokoll eingekapselt (encapsulation) und übertragen. In großen Netzen, in denen viele Teilnetze durch Router verbunden sind, ist eine wesentliche Aufgabe des Routers die Wegewahl (Routing) zwischen den Teilnetzen. Hierbei können prinzipiell zwei Verfahren unterschieden werden:

- Das statische Routing, bei dem die Wegewahl manuell angegeben wird.
- Das dynamische Routing, bei dem die Wegewahl durch die Router bestimmt und laufend aktualisiert wird. Hierzu stehen mehrere Algorithmen bzw. Protokolle zur Verfügung, die auch den Abgleich der Router untereinander gewährleisten. Die bekanntesten Protokolle sind unter anderem RIP (Routing Information Protocol), OSPF (Open Shortest Path First) und IGRP (Interior Gateway Routing Protocol). Für die Auswahl eines geeigneten Routing-Protokolls ist auch M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten* zu beachten.

Weiterhin kann durch den Einsatz von Filtern eine Zugriffskontrolle gewährleistet werden, d. h. welche Systeme mit welchen Protokollen über den Router in welche Richtung miteinander kommunizieren dürfen.

**Sicherheitsgateway**

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten, dass dazu eingesetzt wird, um IP-Netze sicher zu koppeln. Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet-Intranet dar. Vielmehr können auch zwei organisationsinterne Netze unterschiedlich hohen Schutzbedarf besitzen, zum Beispiel bei der Trennung des Bürokommunikationsnetzes vom Netz der Personalabteilung, in dem besonders schutzwürdige, personenbezogene Daten übertragen werden.

Beim Einsatz eines Sicherheitsgateways ist zwischen Paketfilter und Application-Level-Gateway zu untescheiden.

*Paketfilter* sind IT-Systeme mit spezieller Software, die die Informationen anhand der Header-Daten der unteren Schichten (Transportschicht oder Verbindungsschicht) des OSI-Modells filtern und anhand spezieller Regeln Pakete weiterleiten oder verwerfen (siehe M 2.74 *Geeignete Auswahl eines Paketfilters*). Paketfilter treffen ihre Entscheidungen beispielsweise anhand von Quell- und Ziel-Adressen oder -Ports eines Paketes, ohne den Inhalt zu berücksichtigen.

Ein *Application-Level-Gateway* ist ein IT-System, das die Informationen der Anwendungsschicht, also den tatsächlichen Inhalt (die Nutzdaten) eines Paketes oder mehrerer zusammengehöriger Pakete, filtert und anhand spezieller

Regeln Verbindungen oder auch bestimmte Kommandos verbieten oder erlauben kann (siehe M 2.75 *Geeignete Auswahl eines Application-Level-Gateways* ). Während Paketfilter auf Schicht 3 und 4 des OSI-Referenzmodells arbeiten, arbeiten Application-Level-Gateways auf Schicht 7. Ein Application-Level-Gateway ist im Allgemeinen auf einem IT-System implementiert, das ausschließlich für diese Aufgabe eingesetzt wird und dessen Befehlsumfang auf das Notwendigste reduziert ist.

Prüffragen:

- Werden geeignete Netzkopplungselemente nach dem OSI-Referenzmodell unter Berücksichtigung der Anforderungen zur Netzsegmentierung ausgewählt?

# M 5.14 Absicherung interner Remote-Zugänge von TK-Anlagen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

TK-Anlagen verfügen oft über Fernwartungszugänge für Managementfunktionen. Diese Zugänge können für Administrations- und Wartungstätigkeiten sowie für sonstige Management-Aufgaben, wie die Alarmsignalisierung und -bearbeitung, genutzt werden. Solche Remote-Zugänge sind besonders bei komplexen TK-Anlagen nützlich und teilweise unverzichtbar.

Oft kann der Remote-Zugang über folgende Techniken genutzt werden:

- Zugang über ein IP-Netz
- Direkte Einwahl über Direct Inward System Access (DISA)
- Zugang über dedizierte Management-Ports per Modem

Die Benutzung von Remote-Zugängen sollte so weit wie möglich eingeschränkt werden. Des Weiterem sollten alle Zugriffe und alle Aktivitäten während einer Administrationssitzung protokolliert werden können.

Grundsätzlich lässt sich zwischen

- einem Remote-Zugang im eigenen TK-Anlagenverbund (interner Zugang) und
- einem Remote-Zugang aus anderen Netzen (externer Zugang, siehe M 5.15 *Absicherung externer Remote-Zugänge von TK-Anlagen*)

unterscheiden.

Beim internen Remote-Zugang wird die Absicherung einer Fernwartung innerhalb eines TK-Anlagenverbundes betrachtet. Unter Anlagenverbund wird hierbei eine aus mehreren separaten Anlagenteilen bestehende Gesamtanlage verstanden, die über ein eigenes Leitungsnetz miteinander verbunden ist. Sollte diese Verbindung über öffentliche Vermittlungseinrichtungen geführt sein, so sind zusätzlich die unter M 5.15 *Absicherung externer Remote-Zugänge von TK-Anlagen* beschriebenen Maßnahmen zu realisieren. Bei Vernetzung über geschlossene Benutzergruppen innerhalb öffentlicher Netze oder über virtuelle private Netze (VPN) sollten die Maßnahmen für interne Remote Zugänge und nach Möglichkeit die mit * gekennzeichneten Punkte aus den Maßnahmen für externe Remote-Zugänge umgesetzt werden.

Der wichtigste Aspekt bei der Absicherung des internen Remote-Zuganges ist der, Eindringversuche aus externen Netzen wirksam zu unterbinden und gegebenenfalls auch erkennen zu können. Des weiteren sollten die Zugänge aus dem eigenen Netz auf die berechtigten Stellen und Personen eingeschränkt werden können. Je nach Art der Zugangstechnik existieren hierfür unterschiedliche Methoden.

**Absicherung eines internen Remote-Zugangs über IP-Netze**

Wird die TK-Anlagen an ein IP-Netz angeschlossen, zum Beispiel damit sie konfiguriert und überwacht werden kann, gelten für sie ähnliche Empfehlungen wie für klassische IT-Systeme, darunter Server und Clients. Analog zu diesen IT-Systemen ist die Fernwartung zu schützen (siehe M 1.1 *Einhaltung einschlägiger Normen und Vorschriften*).

Die TK-Anlage muss so konfiguriert werden, dass sich nur berechtigte Administratoren nach einer geeigneten Authentisierung an der TK-Anlage anmelden können. Hierfür ist ein entsprechendes Authentisierungsverfahren auszuwählen (siehe M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*). Wenn möglich, sollte die TK-Anlage so konfiguriert werden, dass nur berechtige IT-Systeme auf sie zugreifen dürfen, beispielsweise durch ein getrenntes Konfigurationsnetz oder Paket-Filter (siehe M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* und M 4.238 *Einsatz eines lokalen Paketfilters*).

Damit die übertragenen Informationen zwischen den IT-Systemen der Administratoren und der TK-Anlage nicht abgehört werden können, sollten die übertragenen Informationen verschlüsselt werden (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

Im Weiterem muss geprüft werden, ob die TK-Anlage in das Sicherheitskonzept gegen Schadprogramme aufgenommen werden sollte.

**Absicherung eines internen Remote-Zugangs via Modem**

Die nachfolgende Abbildung stellt ein typisches Szenario eines internen Remote-Zugangs dar, der über einen Fernadministrationsport via Modem angesprochen wird. Die TK-Anlage PBX 1 wird vom Wartungsplatz aus direkt über die V.24-Wartungsschnittstelle administriert. Die TK-Anlage PBX 2 wird vom Wartungsplatz aus über Modem 1 - PBX 1 - PBX 2 - Modem 2 - V.24-Wartungsschnittstelle administriert.

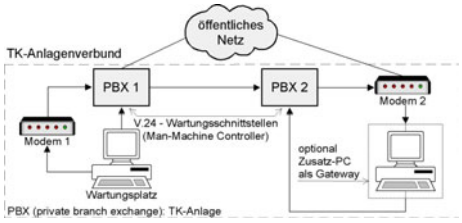



Abbildung: Aufbau einer Fernadministration via Modem

In einem solchem Fall können folgende Maßnahmen zur **Abschottung gegenüber Zugängen aus externen Netzen** ergriffen werden:

- Keine Amtsberechtigung für den Anschluss von Modem 2
  Der Modem-Anschluss, über den der Zugang zum Administrationsport der Anlage geführt wird, sollte in keinem Fall amtsberechtigt sein! Diese Minimalanforderung sollte als erstes überprüft werden. Hiermit wird vermieden, dass das Modem von außerhalb direkt angewählt werden kann.
- Geheimhaltung der Rufnummer des Wartungsports von Modem 2
  Um Missbrauch von vornherein zu erschweren, sollte die Rufnummer des Wartungsapparates nicht in Telefonverzeichnissen veröffentlicht werden. Ihre Kenntnis sollte den sie unmittelbar benötigenden Personen vorbehalten bleiben.
- Verwendung von Standleitungen (optional)
  Die Verwendung von eigenen, nicht über Vermittlungseinrichtungen geführten, Standleitungen für die Remote-Verbindungen, ist eine der sichersten Methoden, um den externen Zugriff auf die Remote-Zugänge zu unterbinden. Da dieses Verfahren in der Regel sehr teuer ist, wird es nur in Ausnahmefällen Anwendung finden können.

Um sicherzustellen, dass nur **die berechtigten Stellen** innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Bildung geschlossener Benutzergruppen (Closed User Group, CUG)
  In einigen TK-Anlagen lassen sich CUGs anlagenübergreifend einrichten. Diese geschlossenen Benutzergruppen stellen eine Art Netz im Netz dar. Alle benötigten Remote-Zugänge sollten daher mit den jeweils zugangsberechtigten Stellen in solchen CUGs zusammengefasst werden.
- Automatischer Rückruf (Callback)
  Die Callback-Option der Modems sollte genutzt werden (siehe M 5.30 *Aktivierung einer vorhandenen Callback-Option*). Wird ein PC-Gateway eingesetzt, so sollte das Callback von dort gestartet werden.
- Beschränkung der Rechte des Remote-Ports (optional)
  Sollte die TK-Anlage eine Rechteverwaltung für verschiedene Ports unterstützen, kann diese genutzt werden, um sicherheitskritische Aktionen über Remote-Zugänge zu unterbinden und nur vor Ort zuzulassen. Viele TK-Anlagen besitzen diese Option jedoch nicht. In solchen Fällen können die über einen Port ausführbaren Transaktionen durch Zusatzprodukte wie Portcontroller beschränkt werden.

Um sicherzustellen, dass **nur die berechtigten Personen** innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Identifikation und Authentisierung,
- Challenge-Response-Verfahren zur Authentisierung (optional).

**Absicherung eines internen Remote-Zugriffes via ISDN-Vernetzung**

Der Remote-Zugriff auf eine TK-Anlage kann auch über ISDN erfolgen. Zu diesem Zweck sind die PCs mit Managementaufgaben mit ISDN-Karten auszurüsten. Um den Zugang abzusichern, sollte eine geschlossene Benutzergruppe durch die Auswertung der Rufnummer des Management-PCs gebildet werden (CLIP: Calling Line Identification and Presentation). In vielen TK-Anlagen ist diese Beschränkung des Remote-Zugangs auf eine Telefonnummer eingebaut.

**Absicherung direkter Systemzugänge (Direct Inward System Access, DISA)**

Direkte Systemzugänge sollten nach Möglichkeit gesperrt werden. Ist dies nicht möglich, so sollten die Berechtigungen so gesetzt werden, dass der direkte Systemzugang nur über einen dedizierten Port erfolgen kann. Auf diese Weise wird es möglich, den DISA-Zugang über ein Gateway zu führen. Ein Beispiel einer solchen Absicherung ist in der folgenden Abbildung dargestellt:

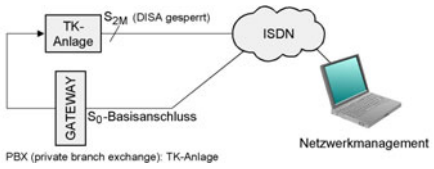



Abbildung: Absicherung eines direkten Systemzuganges

**Einrichtung und Unterbringung eines Netzmanagement-Zentrums**

Der Vorteil eines zentralen Netzmanagements ist, neben einer komfortablen Abwicklungsmöglichkeit der Systemadministration, dass für die alltäglichen

Administrationsarbeiten kein physischer Zutritt zu den TK-Anlagen mehr notwendig ist.

Sollte die Einrichtung eines zentralen Netzmanagements erwogen werden, so ist dies in einem gesicherten Bereich unterzubringen. Der Zutritt zu diesem Zentrum ist durch organisatorische Maßnahmen zu regeln. Entsprechende Vorgaben können dem Baustein B 2.4 *Serverraum* entnommen werden. Die Managementrechner, von welchem die Arbeiten durchgeführt werden können, sollten auch mit geeigneten Maßnahmen abgesichert werden. Beispiele finden sich in B 3.209 *Client unter Windows XP* und B 3.204 *Client unter Unix*.

Prüffragen:

- Ist die externe Fernwartung der TK-Anlage unterbunden?
- Sind die Nutzer des Remote-Zugangs der TK-Anlage bekannt?
- Ist der Zugang zur TK-Fernwartungszentrale auf die notwendigen Personen beschränkt?
- Ist der Administrationszugang der TK-Anlage vor unberechtigten Zugriff geschützt?

# M 5.15 Absicherung externer Remote-Zugänge von TK-Anlagen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Als externer Remote-Zugang wird in dieser Maßnahme jeder Zugriff über die Wartungsschnittstelle der TK-Anlage via öffentliche Vermittlungssysteme und Datennetze, wie dem Internet, angesehen. Dies kann entweder dadurch notwendig werden, dass die einzelnen Anlagen des Verbundes nicht oder nicht nur (siehe Anmerkung) über Standleitungen verbunden sind oder dass auf eine schnelle Unterstützung des Herstellers in Notfällen nicht verzichtet werden kann. In diesen Fällen muss der Wartungsport (Modem) die volle Amtsberechtigung besitzen.

Moderne TK-Anlagen können oft über Datennetze konfiguriert werden. Je nach Netzstruktur befindet sich die TK-Anlage in einem LAN oder in einem separaten Management-Netz. Der direkte Zugriff auf die TK-Anlage, die sich in internen Netzen befindet, von öffentlichen Netzen aus muss verhindert werden. Soll dennoch von einem öffentlichen Datennetz auf die TK-Anlage zugegriffen werden, sollte ein Virtuelles Privates Netz (VPN, siehe B 4.4 *VPN*) genutzt werden. Hierbei wird eine geschützte Datenverbindung zu dem VPN-Endpunkt, der sich in der Regel in der demilitarisierte Zone (DMZ) befindet, generiert. Von dort kann eine Verbindung unter Berücksichtigung der Empfehlungen aus M 5.14 *Absicherung interner Remote-Zugänge von TK-Anlagen* aufgebaut werden.

Die nachfolgende Abbildung stellt ein typisches Szenario eines externen Remote-Zugangs zu einem Fernadministrationsport via Modem dar. Die TK-Anlage wird vom externen Wartungsplatz aus über Modem 1 - öffentliches Netz - PBX - Modem 2 - V.24-Wartungsschnittstelle administriert.

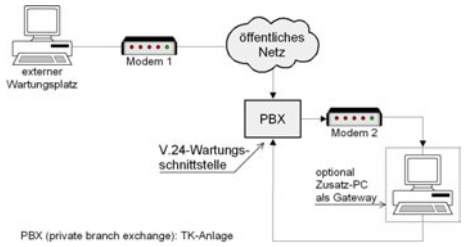



Abbildung: Aufbau einer externen Fernadministration über Modem

Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind - neben den Maßnahmen für interne Remote Zugänge - zusätzliche Sicherungsmaßnahmen unumgänglich.

*Anmerkung:* Einige Anlagen bieten die Möglichkeit, nur die Grundverkehrslast über Standleitungen abzuwickeln und Lastspitzen automatisch über das öffentliche Netz zu routen. Dieser Vorgang wird dem Benutzer nicht signalisiert.

### PC-Gateway (siehe Anmerkung)

Zwischen Wartungsport und Modem sollte ein PC-Gateway geschaltet werden. Dieser muss die folgenden Sicherheitsfunktionen realisieren:

- Identifikation und Authentisierung des Bedieners,

- Abbruch der Verbindung bei sicherheitskritischen Ereignissen,
- Automatischer Rückruf (call back) und
- Protokollierung aller Tätigkeiten.

Darüber hinaus können noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne; dies ist sinnvoll, um in Notfall dem Hersteller oder einem anderen Wartungsunternehmen einen Eingriff zu ermöglichen,
- Einschränkung der Rechte des Wartungspersonals; über eine auf dem Wartungs-PC installierte Zusatzsoftware kann der Benutzer in seinem Handlungsspielraum eingeengt werden, um eine abgestufte Rechteverwaltung zu realisieren,
- "Zwangslogout" bei Leitungsunterbrechung; wird die Verbindung zwischen Fernwartungsstelle und PC-Gateway auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch ein "Zwangslogout" beendet werden.

**Physikalische Abschaltung des Fernwartungszuganges**

Sollte im Normalfall keine Fernwartung benötigt und nur im Bedarfsfall eine solche ermöglicht werden, so empfiehlt sich die physikalische Abschaltung des Zugangs. Im Bedarfsfall kann dieser, eventuell nach telefonischer Rücksprache mit dem Hersteller oder der Wartungsfirma, kurzfristig aktiviert werden.

**Geschlossene Benutzergruppen (Closed User Group, CUG)**

In öffentlichen ISDN- und X.25-Netzen wird das Leistungsmerkmal der Bildung von CUG angeboten. Auf diese Weise wird für einen Benutzer vom Netzbetreiber ein virtuelles "Netz-im-Netz" zur Verfügung gestellt. Die geschlossenen Benutzergruppen können beim Netzbetreiber gegen entsprechende Entgelte beantragt werden.

Alternativ kann überlegt werden, die geschlossenen Benutzergruppen durch Nutzung der ISDN-Hilfsdienste Calling Line Identification and Presentation (CLIP) und Connected Line Identification and Presentation (COLP) selbst zu realisieren. Dies kann, wenn möglich, durch entsprechende Konfiguration der eigenen TK-Anlage oder aber durch entsprechende Auslegung eines PC-Gateways geschehen.

*Anmerkung:* Diese Maßnahme sollte auch bei interner Fernwartung über virtuelle private Netze angewandt werden.

**Vermeidung bzw. Kontrolle direkter Einwahlmöglichkeiten (Dial-In)**

Eine direkte Einwahlmöglichkeit, z. B. aus anderen Netzen über Nachwahl im Mehrfrequenzwahlverfahren, in die TK-Anlage sollte nach Möglichkeit unterbunden werden. Solche Verfahren werden oft für den Zugang zu Serverdiensten genutzt. Sollte ein Unterbinden aus betrieblichen Gründen nicht vermeidbar sein, so empfiehlt sich das vollständige Aktivieren der möglichen Schutzmechanismen und eine regelmäßige Kontrolle auf möglichen Missbrauch.

Prüffragen:

- Wird ein Administrationszugang über öffentliche Netze für die TK-Anlage benötigt?
- Wurde alle nicht benötigten Administrationszugänge deaktiviert?
- Ist der Administrationszugang von TK-Anlagen vor unberechtigtem Zugriff geschützt?

# M 5.16 Übersicht über Netzdienste

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Bevor unter Unix mit der Sicherheitsüberprüfung einzelner Netzdienste und -prozesse begonnen wird, sollte zunächst eine Übersicht darüber erstellt werden, welche Dienste überhaupt zur Verfügung gestellt werden müssen und welche Dienste u. U. schon installiert sind. Für letzteres ist es hilfreich, mit Hilfe des Befehls *ps* und entsprechenden Optionen eine Liste aller Netzprozesse zu erzeugen. Dann sollte man sich über die Aufgabe von jedem dieser Prozesse und darüber, wo er mit welchen Optionen gestartet wird, informieren. Häufig geschieht dies in den Dateien */etc/rc, /etc/rc.net, /etc/rc.local*, die beim Booten des Systems gelesen werden.

Besonders wichtig ist der *inetd*-Daemon, da dieser alle Prozesse, die in der Datei */etc/inetd.conf* aufgeführt sind, starten kann. Auch Konfigurationsdateien wie */etc/services, /etc/protocols, /etc/hosts, /etc/gated.conf* und andere müssen überprüft werden.

Prüffragen:

- Existiert für die Institution eine aktuelle Übersicht der unter Unix benötigten und aktivierten Netzdienste und deren Aufgaben?

# M 5.17 Einsatz der Sicherheitsmechanismen von NFS

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

NFS (Network File System) erlaubt die gemeinsame Benutzung von Dateien auf einem Server von allen Rechnern (Clients) aus, die im selben Netz eingebunden sind und auf dem Server die Rechte dazu bekommen haben. Jeder Server lässt sich auch als Client betreiben und umgekehrt, so dass sichergestellt werden muss, dass jeder Rechner nur mit der für ihn vorgesehenen Funktionalität arbeitet. So ist es z. B. unnötig, den Mount-Daemon *mountd* oder den NFS-Daemon *nfsd* auf einem NFS-Client zu starten.

- Auf einem NFS-Server muss in einer Datei (z. B. */etc/exports* oder */etc/dfs/dfstab*) jedes Dateisystem bzw. Verzeichnis eingetragen werden, das von anderen Rechnern gemountet werden können soll. Für sie muss folgendes gelten:
  - Es sollten nur Dateisysteme exportiert werden, die unbedingt notwendig sind.
  - Mit den Schlüsselwörtern *root* und *access* lassen sich die Rechner genau spezifizieren, für die Dateisysteme zum Export freigegeben werden sollen. Fehlt die Angabe spezieller Rechner, so ist das Dateisystem für alle Rechner freigegeben, was auf keinen Fall geschehen darf!
  - Für Dateisysteme, die nur gelesen werden sollen, und hierzu gehören alle ausführbaren Dateien, sollte die Option *ro* (*read only*) benutzt werden.
  - Normalerweise wird die Benutzernummer des Systemadministrators (UID 0) bei NFS-Anfragen auf die Nummer des Benutzers *nobody* (UID -2 bzw. 65534) umgesetzt, so dass auf Dateien mit der UID 0 über NFS nicht zugegriffen werden kann. Dies gilt nicht für Dateien, die anderen privilegierten Benutzern gehören, wie z. B. *bin* oder *daemon*, was auch in Zusammenhang mit der Aufteilung der Administrationstätigkeiten (M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*) bedacht werden muss, d. h. Dateisysteme mit Dateien dieser Benutzer dürfen nicht exportiert werden. Da jeder Rechner im Netz jede IP annehmen kann und z. B. jeder PC-Benutzer unter DOS *root*-Privilegien hat, sollte also die Umsetzung von *root* auf *nobody* nicht abgeschaltet werden, und es sollte sichergestellt werden, dass ein Eintrag *nobody:*:-2:-2:anonymous user::* in der */etc/passwd* existiert und wirksam ist. In diesem Zusammenhang muss auch beachtet werden, dass jeder Benutzer, der auf einem Netzrechner *root*-Privilegien hat (z. B. als PC-Benutzer) über NFS auch jede Gruppenkennung annehmen kann, so dass also kein exportiertes Verzeichnis und keine exportierte Datei Gruppenschreibrechte besitzen sollte und Lese- und Ausführungsrechte nur, soweit dies unumgänglich ist. Außerdem sollte beachtet werden, dass nicht nur einzelne Dateien, sondern alle darüberliegenden Verzeichnisse geschützt werden müssen!
  - Die Option *anon=-1* sollte benutzt werden, damit anonyme Anfragen verhindert werden. *anon=0* (*root*) sollte niemals benutzt werden, da hierdurch jedem Benutzer Dateizugriffe mit *root*-Rechten möglich werden.

- In Dateien wie z. B. */etc/fstab* oder */etc/vfstab* sind die Dateisysteme eingetragen, die durch einen Befehl wie z. B. *mount -a* oder *mountall* gemountet werden können. Dies kann unter Umständen auch ohne Rückfrage beim Booten geschehen. Diese Datei muss deshalb rechtzeitig auf Korrektheit überprüft werden.
- */etc/exports* und */etc/fstab* (bzw. analoge Dateien auf anderen Systemen) sind Systemdateien, auf die nur der Systemadministrator Zugriff haben darf.
- Zu exportierende Dateisysteme sollten auf einer separaten Platte oder Partition eingerichtet werden, damit z. B. das unbefugte Vollschreiben der Systemplatte durch einen Benutzer von einem anderen Rechner aus verhindert wird.
- Beim Mounten exportierter Dateisysteme muss die Option *nosuid* benutzt werden, um die Ausführung von *suid*-Programmen auf dem Client zu verhindern.
- Wenn möglich, sollte der NFS-Daemon so konfiguriert werden, dass er automatisch eine Überprüfung der Portnummern durchführt, um sicherzustellen, dass Pakete nur von den privilegierten Ports 0 - 1023 akzeptiert werden.
- Zur Kennzeichnung von Dateien werden zwischen Client und Server so genannte File-Handles benutzt, die sich sehr leicht erraten lassen. Sie sollten deshalb mit Hilfe des Programms *fsirand* randomisiert werden.
- Wenn vorhanden, sollte *SECURE-NFS* benutzt werden, so dass die Daten verschlüsselt übertragen werden. Dabei sind folgende Schritte wichtig:
    - Erzeugung von Schlüsseln für alle NFS-Benutzer,
    - Löschen des *public key* für den Benutzer *nobody,*
    - auf dem NIS-Masterserver darf *rpc.ypupdated* nicht laufen,
    - Übertragung der *public key map* auf alle Rechner, bevor *SECURE-NFS* gestartet wird,
    - Benutzung von *keylogin* und *keylogout* zur Erzeugung von *private keys* beim Ein- und Ausloggen,
    - auf jedem Client muss der *keyserv*-Daemon laufen,
    - beim Mounten muss die Option *secure* benutzt werden,
    - die Uhren auf allen Rechnern müssen synchronisiert werden, da die übertragenen Pakete mit Zeitmarken versehen werden, um das Wiedereinspielen von Nachrichten zu verhindern.

Prüffragen:

- Ist sichergestellt, dass jeder Server und jeder Client nur mit der für ihn vorgesehenen Funktionalität arbeitet?
- Sind in der Datei /etc/exports und/oder /etc/dfs/fstab die mountbaren Dateisysteme beziehungsweise Verzeichnisse auf ein notwendiges Maß reduziert?
- Sind in die mountbaren Dateisysteme beziehungsweise Verzeichnisse nur für bestimmte IT-Systeme und/oder Benutzer unter Berücksichtigung der festgelegten Berechtigungsstruktur freigegeben?
- Einsatz von SECURE-NFS: Werden die Sicherheitsmechanismen und -einstellungen zu SECURE-NFS genutzt?

# M 5.18 Einsatz der Sicherheitsmechanismen von NIS

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

NIS (Network Information Service) lässt sich nicht ohne schwerwiegende Sicherheitslücken betreiben und sollte deshalb nur in einer sicheren Umgebung eingesetzt werden.

Für einen NIS-Server gilt folgendes:

- In der Passwortdatei */etc/passwd* darf der Eintrag *+::0:0:::* nicht enthalten sein, da sonst ein Zugang mit dem Namen "+" ohne Passwort existiert. Sollte der Eintrag notwendig sein, muss das Passwort durch ein "*" ersetzt werden (überprüfen, ob der Zugang wirklich gesperrt ist!). Trotzdem bleibt die Gefahr, dass bei einer versehentlichen Löschung der ersten Spalte (das "+") ein privilegierter Zugang ohne Passwort und ohne Benutzername möglich ist!
- Analoges gilt für die Gruppendatei */etc/group* und alle anderen sicherheitsrelevanten Dateien, die über NIS netzweit zugänglich gemacht werden sollen, wie z. B. */etc/hosts, /etc/group* oder */etc/bootparams*.
- Der Server-Prozess *ypserv* sollte nur Anfragen von vorher festgelegten Rechnern beantworten.

Für einen NIS-Client gilt folgendes:

- Der Eintrag *+:*:0:0:::* in der Passwortdatei */etc/passwd* sollte dokumentiert werden (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*), und es muss auf jeden Fall ein Eintrag im Passwortfeld vorhanden sein, damit nicht im Falle einer (beabsichtigten oder nicht beabsichtigten) *Nicht*benutzung von NIS versehentlich ein Zugang mit dem Benutzernamen "+" ohne Passwort geschaffen wird.
- Analoges gilt für die Gruppendatei */etc/group* und alle anderen sicherheitsrelevanten Dateien, die über NIS netzweit zugänglich gemacht werden sollen.
- Der Client-Prozess *ypbind* sollte nur Daten akzeptieren, die von einem privilegierten Port kommen, da er ansonsten Daten (auch Passwörter!) von jedem beliebigen Prozess, der sich als Server ausgibt, bekommen könnte.
- Um zu verhindern, dass der NIS-Administrator auf allen NIS-Clients *root*-Rechte hat, sollte auf jedem NIS-Client ein lokaler Benutzer mit der UID 0 eingerichtet werden.
- Es muss beachtet werden, dass NIS zunächst die lokalen Dateien nach passenden Einträgen absucht, so dass z. B. die Einträge
  *root::0:0:::*
  *+:*:0:0:::*
  in der */etc/passwd* dazu führen, dass nicht das *root*-Passwort aus der NIS-Map benutzt wird, sondern der erste Eintrag ohne Passwort.

Prüffragen:

- Wird NIS (Network Information Service) nur in einer sicheren Umgebung eingesetzt?
- Werden die Sicherheitsmechanismen von NIS sowohl für Server als auch Clients genutzt?

# M 5.19 Einsatz der Sicherheitsmechanismen von sendmail

**Verantwortlich für Initiierung:** Administrator
**Verantwortlich für Umsetzung:** Administrator

Da die Übertragung von Mails die wohl am meisten verbreitete Anwendung in Netzen ist, sind die dafür zuständigen Prozesse von besonderer Bedeutung und einer der häufigsten Angriffspunkte in einem System. Hinzu kommt, dass diese Prozesse häufig das *suid*-Bit gesetzt haben und einem privilegierten Benutzer gehören (z. B. *root* oder *bin*). Ein Fehler in *sendmail* war z. B. einer der Wege, über die sich der Internet-Wurm ausgebreitet hat.

- Beim Starten von *sendmail* lassen sich sehr viele Optionen angeben, die zu Sicherheitsproblemen führen würden, wenn sie mit *root*-Rechten abliefen. Wenn *sendmail* von beliebigen Benutzern aufgerufen werden kann, sollte deshalb überprüft werden, ob es beim Start mit einer dieser Optionen das gesetzte *suid*-Bit ignoriert und mit der UID des Benutzers abläuft. Um Sicherheitsprobleme zu vermeiden, sollte der Administrator sicherstellen, dass *sendmail* nur mit den folgenden Optionen bei gesetztem *suid-root*-Bit von unprivilegierten Benutzern gestartet werden kann: *7, b, C, d, e, E, i, j, L, m, o, p, r, s* und *v.*
- Aufgrund der in der Vergangenheit aufgedeckten Sicherheitsdefizite des Programms *sendmail* muss stets die aktuellste Programmversion eingesetzt werden. Informationen über die aktuellen Versionen erteilen die in M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* angegebenen Stellen wie BSI, CERT, DFN-CERT.
- Der *sendmail*-Prozess darf nicht im Debug-Modus betrieben werden können, da es sonst möglich wird, *root*-Rechte zu erlangen. Man kann dies testen, indem man den Befehl
  *telnet localhost 25*
  eingibt, wobei *localhost* der zu überprüfende Rechnername sein kann und *25* die Portnummer, mit der der *sendmail*-Prozess angesprochen wird. Der Rechner bzw. der *sendmail*-Prozess meldet sich dann mit
  *Trying 123.45.67.8...*
  *Connected to xxx.yy.de.*
  *Escape character is '^]'.*
  *220 xxx Sendmail 4.1/SMI-4.1 ready at Wed, 13 Apr 94 10:04:43 +0200*
  Wenn Sie nun den Befehl *debug, showq* oder bei sehr alten Versionen *wizard* eingeben, sollte dies der Prozess mit
  *500 Command unrecognized*
  ablehnen. Die Verbindung kann mit dem Befehl *quit* wieder beendet werden.
- Die Befehle *vrfy* und *expn* dürfen nicht verfügbar sein, da sie zu einem Mailnamen den zugehörigen Login-Namen ausgeben, so dass sich dann durch Probieren evtl. das zugehörige Passwort herausfinden lässt. Bei Version 8 von *sendmail* lassen sich diese Befehle z. B. durch die Option *p* (privacy) beim Starten abschalten. Ob diese Befehle verfügbar sind, lässt sich wie im vorigen Punkt beschrieben feststellen, also z. B. durch Eingabe des Befehl *vrfy useralias*.
- Die Konfigurationsdatei *sendmail.cf* sollte *root* gehören und auch nur für *root* les- und schreibbar sein. Dasselbe gilt für die darüber stehenden Verzeichnisse, da sich sonst durch ein einfaches Umbenennen dieser Verzeichnisse eine neue *sendmail.cf* Datei erzeugen lässt.

- Die Angabe von ausführbaren Programmen oder von Dateien als gültige Adressen für Empfänger oder Absender muss durch die Konfiguration von *sendmail.cf* verhindert werden oder durch geeignete Maßnahmen auf bestimmte, unbedenkliche Programme und Dateien eingeschränkt werden.
- Das *F*-Kommando (also z. B. *FX/path [^#]*), mit dessen Hilfe Klassen definiert werden, sollte in der Konfigurationsdatei (*sendmail.cf*) nur benutzt werden, um Dateien zu lesen, die systemweit lesbar sind, da es sonst möglich sein kann, dass sicherheitsrelevante Informationen aus geschützten Dateien frei verfügbar werden. Die Programmform des *F*-Kommandos (z. B. *FX|/tmp/prg*) sollte nicht benutzt werden!
- Bei der Definition des Delivery Agents (z. B. *Mlocal*) dürfen nur absolute Pfade angegeben werden (z. B. *P=/bin/mail*). Außerdem sollte das Flag S (*suid*) nur gesetzt werden, wenn die damit evtl. verbundenen Sicherheitsprobleme geklärt sind.
- Jede Datei, in die *sendmail* schreiben könnte, wie z. B. *sendmail.st* für eine Statistik, sollte nur von *root* beschreibbar sein und auch nur in *root* gehörenden Verzeichnissen stehen. Dasselbe gilt für Dateien, die von *sendmail* ausgewertet werden wie z. B. *:include:* in Mailing Listen.
- Privilegierte Benutzer wie *bin* oder *root* sollten keine *.forward* Datei besitzen. Sind nämlich die Benutzer- oder Gruppenschreibrechte für diese Datei falsch gesetzt oder gelingt es einem Benutzer, in eine privilegierte Gruppe zu gelangen, kann er sich eine Shell mit der privilegierten Benutzer-Kennung erzeugen.
  Für normale Benutzer sollte die *.forward*-Datei nur von dem Besitzer beschreibbar sein und muss sich in einem Verzeichnis befinden, das dem Besitzer gehört.
  Falls ein Heimatverzeichnis systemweit beschreibbar sein muss, wie z. B. *uucp*, lässt sich auf folgende Weise verhindern, dass eine schädliche *.forward*-Datei angelegt werden kann: Es muss ein Verzeichnis mit dem Namen *.forward,* den Rechten 000 und dem Besitzer *root* angelegt werden und in diesem eine Datei ebenfalls mit den Rechten 000 und dem Besitzer *root*, so dass niemand außer *root* diese Datei verändern oder löschen kann. Das Homedirectory von *uucp* sollte dann ebenfalls *root* gehören und mit dem Sticky-Bit (*t*) versehen sein. Eine analoge Vorgehensweise empfiehlt sich auch für andere Konfigurationsdateien (z. B. *.login, .cshrc*) in systemweit beschreibbaren Verzeichnissen.
- Aus der Alias-Datei sollte jedes ausführbare Programm entfernt werden, insbesondere auch *uudecode*. Außerdem sollte die Alias-Datei und die zugehörige Datenbank *root* gehören und auch nur für *root* beschreibbar sein.
- Es muss beachtet werden, dass jede empfangene Mail verfälscht sein kann. Dies kann entweder in der Mailqueue geschehen oder durch ein Einloggen auf Port 25. Ersteres lässt sich vermeiden, wenn das Mailqueue-Verzeichnis *root* gehört und die Rechte 0700 besitzt. Die Queue-Dateien sollten die Berechtigung 0600 haben. Die Veränderung einer Mail während ihres Transportes lässt sich nicht vermeiden, so dass die Benutzer darüber aufgeklärt werden müssen, dass z. B. eine Mail von *root*, in der sie dazu aufgefordert werden, ihr Passwort zu ändern, gefälscht sein kann.

Prüffragen:

- Wird sichergestellt, dass sendmail bei gesetztem suid-root-Bit nur mit zulässigen Optionen gestartet werden kann?
- Wird der Betrieb des sendmail-Prozesses im Debug-Modus verhindert?
- Wird die Ausführung der Befehle VRFY und EXPN bei sendmail verhindert?

- Sind die Berechtigungen für relevante Dateien (z. B.sendmail.cf, sendmail.st, alias, queue, :include: in Mailing Listen) und die darüber stehenden Verzeichnisse auf ein notwendiges Maß reduziert?
- Werden bei der Definition des Delivery Agents (z. B.Mlocal) nur absolute Pfade angegeben (z. B. P=/bin/mail)?
- Existieren die forward-Dateien exklusiv nur für unprivilegierte Benutzer?

# M 5.20 Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Mit dem Programm *rlogin* bzw. dem zugehörigen Daemon *rlogind* ist es möglich, sich über eine Netzverbindung auf einem anderen Rechner einzuloggen, wobei allerdings nur das Passwort abgefragt wird, da der Benutzername direkt übergeben wird. Mit den Kommandos *rsh* bzw. *rcp* und dem Daemon *rshd* ist es möglich, auf einem anderen Rechner ein Kommando ausführen zu lassen. Für beide Befehle gibt es die Möglichkeit, Trusted-Hosts zu definieren und zwar entweder benutzerspezifisch im Heimatverzeichnis in der Datei *$HOME/.rhosts* oder systemweit in der Datei */etc/hosts.equiv*. Jeder Rechner, der in einer dieser Dateien eingetragen ist, wird als vertrauenswürdig angesehen, so dass ein Einloggen (mit *rlogin*) bzw. die Ausführung eines Befehles (mit *rsh*) von ihm aus ohne Angabe eines Passwortes möglich ist.

Da es, insbesondere von einem PC aus, sehr leicht ist, jeden beliebigen Rechnernamen vorzutäuschen, muss sichergestellt werden, dass die Dateien *$HOME/.rhosts* und */etc/hosts.equiv* **nicht** vorhanden sind oder dass sie leer sind und der Benutzer keine Zugriffsrechte auf sie hat. Hierzu sollten regelmäßig die Heimatverzeichnisse der Benutzer untersucht werden, oder es sollte verhindert werden, dass die Daemons *rlogind* und *rshd* gestartet werden können (siehe hierzu die Datei */etc/inetd.conf* und Maßnahme M 5.16 *Übersicht über Netzdienste*). Sollte die Benutzung der Datei */etc/hosts.equiv* unumgänglich sein, muss sichergestellt sein, dass kein Eintrag *'+'* vorhanden ist, da hierdurch jeder Rechner vertrauenswürdig würde.

Als Ersatz für die r-Dienste kann Secure Shell (*ssh*) genutzt werden, wobei umfangreiche Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität zum Einsatz kommen (siehe auch M 5.64 *Secure Shell*). Wenn *ssh* zum Einsatz kommt, sollten nach Möglichkeit die r-Dienste abgeschaltet werden, damit die Sicherheitsmaßnahmen nicht umgangen werden können. Dies setzt allerdings voraus, dass alle Kommunikationspartner über geeignete Implementierungen von *ssh* verfügen.

Prüffragen:

- Wird die missbräuchliche Nutzung der Dateien $HOME/.rhosts und /etc/hosts.equiv beziehungsweise der Daemons rlogind und rshd unterbunden?
- Werden nach Möglichkeit stärkere Verfahren (zum Beispiel SSH ) eingesetzt und auf schwächere Verfahren (z. B.rlogin, rsh und rcp ) verzichtet?

# M 5.21 Sicherer Einsatz von telnet, ftp, tftp und rexec

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Das Kommando *telnet hostname* ermöglicht es, sich nach Eingabe eines Benutzernamens und des zugehörigen Passwortes auf dem Rechner *hostname* einzuloggen. Mit *ftp* ist es möglich, größere Datenmengen zu kopieren, und *rexec* erlaubt die Ausführung von Kommandos auf einem anderen Rechner ohne ein vorhergehendes Anmelden. Bei allen drei Programmen werden die eingegebenen Benutzernamen und Passwörter unverschlüsselt über das Netz übertragen, so dass sie nur benutzt werden dürfen, wenn sichergestellt ist, dass das Netz nicht abgehört werden kann (siehe G 5.7 *Abhören von Leitungen*). Alle Aufrufe von *telnet, ftp* und *rexec* sind zu protokollieren. Insbesondere ist auf fehlgeschlagene Verbindungsversuche von externen IT-Systemen zu achten.

Beim Einsatz des Daemons *ftpd* muss beachtet werden, dass ähnlich wie bei *sendmail* (siehe M 5.19 *Einsatz der Sicherheitsmechanismen von sendmail*) immer wieder neue schwerwiegende Sicherheitslücken festgestellt werden, die es u. U. ermöglichen, ohne Passwort Administratorrechte zu bekommen (siehe hierzu die CERT-Mitteilung CA-94-08 vom 14.04.1994). Es sollten keine *ftp*-Versionen eingesetzt werden, die älter sind als die dort beschriebenen.

Weiterhin sollten in die Datei */etc/ftpusers* alle Benutzernamen eingetragen werden, für die ein *ftp*-Zugang nicht erlaubt werden soll. Hierzu gehören z. B. *root, uucp* und *bin*. Bei der Einrichtung von neuen Benutzern ist darauf zu achten, diese in */etc/ftpusers* einzutragen, wenn sie gemäß ihrem Rechteprofil keinen ftp-Zugang haben dürfen (siehe auch M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

Mit Hilfe von *.netrc*-Dateien werden automatische FTP-Zugriffe auf entfernten IT-Systemen erlaubt. Damit dies möglich ist, enthalten *.netrc*-Dateien die benötigten Passwörter. Daher muss sichergestellt werden, dass keine *.netrc*-Dateien in den Benutzerverzeichnissen vorhanden sind oder dass sie leer sind und der Benutzer keine Zugriffsrechte auf diese hat.

Der Einsatz des Daemons *tftpd, rexd* und *rexecd* muss verhindert werden (z. B. durch Entfernen des entsprechenden Eintrags in der Datei */etc/inetd.conf*), oder es muss zumindest sichergestellt sein, dass beim Einsatz von *tftp* den Benutzern aus dem Login-Verzeichnis nur eingeschränkte Dateizugriffe möglich sind (siehe auch M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*). Dies lässt sich überprüfen, indem man Folgendes eingibt:

*tftp hostname*
*tftp>get /etc/passwd /tmp/txt*

Meldet sich der *tftp*-Daemon nicht mit einer Fehlermeldung, muss seine Benutzung verhindert werden.

Muss für den Startvorgang von aktiven Netzkomponenten oder X-Terminals *tftp* doch eingesetzt werden, ist dies unbedingt zu dokumentieren und zu begründen. Außerdem ist beim Einsatz von *tftp* sicherzustellen, dass der *tftp*-Daemon mit der Option *-sverzeichnis* gestartet wird. Dabei ist für *verzeichnis* das ausschließlich für den Daemon sichtbare Verzeichnis einzusetzen.

Als Ersatz für *telnet* und *rexec* kann Secure Shell (*ssh*) genutzt werden, wobei umfangreiche Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität zum Einsatz kommen (siehe auch M 5.64 *Secure Shell*). Durch Tunneling ist es auch möglich, *ftp* mit sicherer Verschlüsselung zu betreiben. Wenn *ssh* zum Einsatz kommt, sollten daher nach Möglichkeit diese Dienste abgeschaltet werden, damit die Sicherheitsmaßnahmen nicht umgangen werden können. Dies setzt allerdings voraus, dass alle Kommunikationspartner über geeignete Implementierungen von *ssh* verfügen.

Prüffragen:

- Wird auf den Einsatz der Programme TELNET, FTP und REXEC verzichtet beziehungsweise erfolgt deren Einsatz nur, wenn sichergestellt ist, dass das Netz nicht abgehört werden kann?
- Einsatz von FTP: Wird der FTP-Zugang für alle unberechtigten Benutzer (zum Beispiel in der Datei /etc/ftpusers) unterbunden?
- Wird die Nutzung der relevanten Dateien (z. B. .netrc) und Daemons (z. B. TFTP, rexd und REXEC) konsequent unterbunden?

# M 5.22 Kompatibilitätsprüfung des Sender- und Empfängersystems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche

Abhängig vom Grad der Kompatibilität von Empfänger- und Sendersystem lassen sich Informationen mehr oder weniger zuverlässig per Datenträgeraustausch übertragen. Dabei sind je nach Komplexität auszutauschender Daten unterschiedliche Anforderungen an die Kompatibilität zu stellen. Vor Einrichtung eines regelmäßigen Datenträgeraustausches sollte daher die Übereinstimmung folgender Eigenschaften überprüft werden, um im Vorfeld Inkompatibilitäten festzustellen und wo erforderlich Abhilfe zu schaffen:

- Physikalisches Medium:
  Notwendig ist natürlich, dass die **physikalischen Medien** von Empfänger- und Sendersystem übereinstimmen. Dabei reicht aber mechanische Äquivalenz noch nicht aus, denn die Nichtübereinstimmung von Parametern wie Geschwindigkeit bei Bändern kann zu Problemen führen.
- Zeichencode (z. B. ASCII oder EBCDIC):
  Stimmen Sender- und Empfängersystem im verwendeten **Zeichencode** überein, so sind mit Hilfe des physikalischen Lesens einzelne Sektoren bzw. Blöcke im Klartext lesbar, die unzusammenhängend auf dem Datenträger verteilt sein können. Stimmen die verwendeten Zeichencodes nicht überein, werden die übertragenen Daten falsch interpretiert.
- Formatierung des Betriebs- bzw. Dateisystem des Datenträgers:
  Verfügen beide Systeme darüber hinaus über das **gleiche Betriebs- und Dateisystem** oder sieht das Empfängerbetriebssystem vor, Formatierungen anderer Betriebssystem zu lesen (nicht alle Unix-Betriebssysteme können NTFS-Datenträger einlesen), dann können alle Dateien, wie sie beim Absender vorlagen, wiederhergestellt werden. Dies ist für Informationen ausreichend, die keiner weiteren Formatierung, wie sie von den meisten Anwendungsprogrammen (z. B. Textverarbeitungsprogrammen) vorgenommen werden, unterliegen.
- Anwendungssoftware:
  Wurden Anwendungsprogramme zur Erzeugung der zu übermittelten Dateien verwendet, ist auf **Versionsgleichheit** dieser Programme zu achten, da die Dateiformate evtl. unterschiedlich sein können. Die Versionsgleichheit muss nicht bestehen, wenn die Programmversionen aufwärts- bzw. abwärtskompatibel sind.
- Sicherheitssoftware und Sicherheitsparameter:
  Werden darüber hinaus Sicherheitsprodukte oder Schutzmechanismen bestimmter Anwendungsprogramme (siehe M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*) verwendet, so ist die Kompatibilität dieser Produkte sicherzustellen.
  Über die verwendeten **Schlüssel** oder **Passwörter** müssen sich Absender und Empfänger auf geeignetem Wege verständigen.

Treten Inkompatibilitäten auf, so sind zusätzliche Vorkehrungen bzw. Produkte bereitzustellen, die eine entsprechende Konvertierung vorsehen, oder die Absender- und Empfängersysteme sind geeignet auszustatten.

Prüffragen:

- Ist der Einsatz kompatibler IT-Produkte auf Sender- und Empfängerseite sichergestellt?

# M 5.23 Auswahl einer geeigneten Versandart für Datenträger

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Neben den in M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen sollte sich die Versandart der Datenträger am Gefährdungspotential orientieren. Hinsichtlich Verfügbarkeit ist die Versandart derart auszuwählen, dass eine rechtzeitige Zustellung garantiert werden kann. Je mehr Personen mit der Beförderung befasst und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt, desto weniger kann im allgemeinen die Vertraulichkeit und Integrität garantiert werden. Dementsprechend sind angemessene Versandarten auszuwählen.

Man kann dabei z. B. zwischen folgenden Versandarten wählen:

- Post (mit verschiedenen Versandangeboten, die unterschiedliche Garantien für die Transportgeschwindigkeit und Absicherung umfassen),
- Kurierdienste,
- persönlicher Kurier und
- persönliche Übergabe.

Für eine Behörde oder ein Unternehmen empfiehlt es sich, eine Liste zu führen, in der für verschiedene Datenträger und deren Schutzbedarf angemessene Versandarten vorgeschlagen werden. Dies erleichtert den Mitarbeitern die Auswahl nicht nur in Bezug auf das bestmögliche Preis-Leistungs-Verhältnis, sondern auch auf die optimale Sicherheit. Diese Liste sollte mindestens folgende Aspekte umfassen:

- durchschnittliche Transportzeit der Versandart bzw. des Kuriers
- Vertrauenswürdigkeit der Versandart bzw. des Kuriers
- Kosten.

Prüffragen:

- Orientiert sich die Versandart der Datenträger am Schutzbedarf der zu übermittelnden Informationen?

# M 5.24 Nutzung eines geeigneten Faxvorblattes

**Verantwortlich für Initiierung:** Leiter Innerer Dienst
**Verantwortlich für Umsetzung:** Benutzer, Fax-Verantwortlicher

Um einen geordneten und nachvollziehbaren Fax-Austausch zu erzielen, ist die Nutzung eines standardisierten Faxvorblattes vorzusehen. Damit kann insbesondere geprüft werden, ob eine erhaltene Faxsendung vollständig empfangen und ausgedruckt wurde.

Das Faxvorblatt sollte beinhalten:

- Rufnummer des Faxgerätes,
- Name des Absenders (mit Telefonnummer und vollständiger Adresse),
- Telefonnummer eines Ansprechpartners bei Übertragungsproblemen,
- Name des Empfängers (mit Rufnummer des Faxgerätes und ggf. vollständiger Adresse),
- Seitenzahl einschließlich Faxvorblatt,
- ggf. Dringlichkeitsvermerk (evtl. gestuft) und
- Unterschrift des Absenders.

Die Bitte, fehlgeleitete Sendungen weiterzuleiten oder den Absender zu informieren, ist sinnvoll.

Prüffragen:

- Wird ein standardisiertes Faxvorblatt genutzt?

# M 5.25 Nutzung von Sende- und Empfangsprotokollen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fax-Verantwortlicher, IT-Sicherheitsbeauftragter, Fax-Poststelle

Bei der Nutzung von Fax-Diensten ist bei der Verwendung von Sende- und Empfangsprotokollen zwischen herkömmlichen Faxgeräten und Faxservern zu unterscheiden.

**Einsatz eines herkömmlichen Faxgerätes**

Listenmäßige Protokolle von Übertragungsvorgängen, die automatisch vom Faxgerät geführt werden (Kommunikationsjournal), sind regelmäßig auszudrucken. Es bedarf einer Festlegung, wer diese Ausdrucke veranlasst, wo und wie lange sie aufbewahrt werden und in welcher Weise sie stichprobenartigen Prüfungen auf Unregelmäßigkeiten unterzogen werden. Auf die Erfordernisse des Bundesdatenschutzgesetz (BDSG) ist Rücksicht zu nehmen. Insbesondere ist der Zugriff Unbefugter zu verhindern.

Es sollte zusätzlich ein Faxtagebuch geführt werden, aus dem ersichtlich wird, wer wann ein Fax an wen versandt hat. Optional kann darüber hinaus ein Faxeingangsbuch geführt werden.

Es sei darauf hingewiesen, dass eine weitere Kontrollmöglichkeit besteht, wenn das Faxgerät an eine moderne TK-Anlage angeschlossen ist. Dann ist es u. U. möglich, die Gebührendatensätze der Faxnummer in der TK-Anlage auszuwerten (siehe auch M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*).

**Einsatz eines Faxservers:**

Auch auf Faxservern ist es möglich, die Übertragungsvorgänge zu protokollieren. Diese Protokolle sollten regelmäßig ausgewertet und archiviert werden. Es bedarf insbesondere der Festlegung von Rahmenbedingungen und Zuständigkeiten für die Auswertung und Archivierung der Protokolle.

So ist z. B. denkbar, dass die Fax-Poststelle für diese Tätigkeiten zuständig ist, die Auswertung der Protokolle aber nur im Beisein eines Betriebs- oder Personalratsmitgliedes bzw. eines Angehörigen der Revision oder des Datenschutzes erfolgen darf. Auch hier gilt, dass die Erfordernisse des BDSG zu berücksichtigen sind und insbesondere der Zugriff Unbefugter zu verhindern ist.

Bei der Verwendung von Faxservern ist die manuelle Führung von Fax-Tagebüchern nicht sinnvoll. Vielmehr dürfte die lückenlose Archivierung der Sende- und Empfangsprotokolle ausreichend sein.

Teilweise besteht auch die Möglichkeit, anfallende Gebührendatensätze für abgehende Faxsendungen vom Faxserver für eine verursachungsgerechte Verrechnung zu nutzen.

Prüffragen:

- Werden Fax-Übertragungsvorgänge protokolliert?
- Ist festgelegt, wer die Fax-Übertragungsprotokolle regelmäßig auswertet und auf Unregelmäßigkeiten prüft?

- Ist festgelegt, wo und wie lange die Sende- und Empfangsprotokolle des Faxgerätes aufbewahrt werden?
- Haben nur berechtigte Personen Zugriff auf die Sende- und Empfangsprotokolle des Faxgerätes?
- Wird ein Faxtagebuch geführt, aus dem ersichtlich ist, wer wann ein Fax an wen versandt hat?

# M 5.26 Telefonische Ankündigung einer Faxsendung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Benutzer

Wichtige Faxsendungen mit vertraulichen oder finanzwirksamen Inhalten (z. B. Angebote) oder termingebundene Faxsendungen sollten vor Absendung beim Empfänger (zum Beispiel per Telefon) angemeldet werden. Der Empfänger hat dann die Möglichkeit, zum entsprechenden Faxgerät zu gehen und dort das für ihn eingehende Fax direkt entgegenzunehmen, so dass kein anderer das Fax entnehmen kann.

Die Benutzer sollten von Vorgesetzten angewiesen werden, vertrauliche oder wichtige Faxsendungen anzukündigen.

Prüffragen:

- Ist festgelegt, welche vertraulichen oder wichtigen Faxsendungen vor Absendung beim Empfänger anzukündigen sind?

# M 5.27 Telefonische Rückversicherung über korrekten Faxempfang

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Benutzer

Bei wichtigen Faxsendungen sollte beim Empfänger nachgefragt werden, ob die Faxsendung vollständig empfangen, ausgedruckt und ihm übergeben wurde. Die Mitarbeiter sollten hierzu angewiesen werden. Die telefonische Bestätigung kann auch auf dem Fax-Vordruck erbeten werden.

Hilfreich sind in diesem Zusammenhang die von einigen Faxgeräten als Leistungsmerkmal angebotenen Einzelsendeberichte, die Fehler beim Versand anzeigen können.

Prüffragen:

- Sind die Mitarbeiter angewiesen, sich bei wichtigen Faxsendungen den vollständigen Erhalt vom Empfänger bestätigen zu lassen?

# M 5.28 Telefonische Rückversicherung über korrekten Faxabsender

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte
**Verantwortlich für Umsetzung:** Benutzer

Bei wichtigen oder ungewöhnlichen Faxsendungen sollte in Erwägung gezogen werden, sich beim Faxabsender zu vergewissern, dass das Fax von ihm abgesandt und nicht von einem Dritten gefälscht wurde. Dies kann auf einfache Weise durch einen telefonischen Rückruf erfolgen. Die erforderliche Rufnummer ist im allgemeinen auf dem Faxvorblatt dokumentiert, sollte aber, da sie gefälscht sein könnte, verifiziert werden.

Prüffragen:

- Wird die Callback-Funktion eines Modems nur auf der passiven Seite der Datenübertragung aktiviert (von der Dateien abgerufen oder auf der Dateien eingespielt werden)?
- Werden die voreingestellten Rufnummern des Callback bei Modems regelmäßig kontrolliert und aktualisiert?
- Sind die Empfänger von wichtigen oder ungewöhnlichen Faxsendungen gehalten, sich über die Korrektheit des Inhalts beim Faxabsender zu vergewissern?

# M 5.29 Gelegentliche Kontrolle programmierter Zieladressen und Protokolle

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fax-Verantwortlicher

Bei programmierbaren Kurzwahltasten oder Zieladressenspeicherung sollte gelegentlich überprüft werden, ob die gewünschte mit der einprogrammierten Faxnummer übereinstimmt und ob sie noch benötigt wird. Damit wird verhindert, dass eine von einem Unberechtigten eingegebene fremde Faxnummer längere Zeit statt der korrekten Nummer genutzt wird. Außerdem werden eventuell übersehene Änderungen der gewünschten Zielrufnummern frühzeitig entdeckt.

Prüffragen:

- Werden programmierte Kurzwahl- oder Zieladressenspeicher regelmäßig auf Aktualität und Korrektheit überprüft?

# M 5.30 Aktivierung einer vorhandenen Callback-Option

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Viele Modems bieten die Option automatischer Rückruf (Callback). Ist diese Option aktiviert, trennt das Modem, wenn es einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Leitung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, dass ein nicht autorisierter Anrufer diesen Modem-Zugang missbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Das erforderliche Kommando ist der Bedienungsanleitung zu entnehmen, üblicherweise wird das Kommando *AT%S* benutzt. Vor der Aktivierung der Callback-Option ist festzulegen, welche Nummer zurückgerufen werden soll.

Manche Modems bieten auch die Möglichkeit, einen automatischen Rückruf mit einer Passwortabfrage zu verbinden. Das angerufene Modem fordert dabei nach dem Verbindungsaufbau das anrufende Modem zu einer Passworteingabe auf. Im angerufenen Modem wird die Gültigkeit des Passwortes überprüft. Jedem gültigen Passwort ist eine Rufnummer zugeordnet, die dann zurückgerufen wird. Dabei kann meist eine Liste von Rückrufnummern im lokalen Modem angelegt werden, so dass von verschiedenen Orten aus Verbindung mit dem lokalen Modem aufgebaut werden kann.

Es ist darauf zu achten, dass der automatische Rückruf nur auf einer Seite aktiviert ist, da der Mechanismus sonst in eine Endlosschleife führt. Callback sollte auf der passiven Seite aktiviert sein, also auf der Seite, von der Dateien abgerufen oder auf der Dateien eingespielt werden. Ein typisches Beispiel ist der Außendienstmitarbeiter, der mit einem IT-System in seiner Organisation in Verbindung treten will. Hier muss Callback auf dem organisationsinternen Modem aktiviert sein.

Es sollte sichergestellt sein, dass die voreingestellten Rufnummern des Callback sporadisch kontrolliert und aktualisiert werden.

Ein Callback kann außer durch das Modem auch von der Applikation ausgelöst werden. Wenn die eingesetzte Applikation diese Option bietet, sollte das Callback von der Applikation und nicht vom Modem ausgelöst werden. Wenn das Modem ein Callback auslöst, kann ein Angreifer versuchen, in dem Moment, wenn das Modem den Callback starten will, dieses anzuwählen und damit den Callback abzufangen. Wenn die Applikation den Callback durchführt, ist es für einen Angreifer wesentlich schwieriger, den richtigen Moment abzupassen.

# M 5.31 Geeignete Modem-Konfiguration

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die meisten Modems arbeiten nach dem Hayes-Standard (auch AT-Standard genannt). Dies ist ein nicht normierter, herstellerabhängiger Standard. Die Basis-Befehlssätze der verschiedenen Modems stimmen größtenteils überein. Größere Abweichungen gibt es in den erweiterten Befehlssätzen. Es ist wichtig, den Befehlssatz des eingesetzten Modems daraufhin zu überprüfen, wie die im folgenden beschriebenen Funktionen umgesetzt sind und ob durch fehlerhafte Konfiguration Sicherheitslücken entstehen können.

Die gewählten Einstellungen sollten im nichtflüchtigen Speicher des Modems gespeichert werden (siehe auch M 1.38 *Geeignete Aufstellung eines Modems*). Außerdem sollten sie auf Papier ausgedruckt werden, so dass sie jederzeit mit der aktuellen Einstellung verglichen werden können.

Nachfolgend werden einige sicherheitsrelevante Konfigurationen vorgestellt:

**Auto-Answer**

Über das Register S0 kann eingestellt werden, dass das Modem einen ankommenden Ruf automatisch nach einer einzustellenden Anzahl von Klingelzeichen entgegennimmt. Mit der Einstellung *S0=0* wird dies verhindert und erzwungen, dass Anrufe manuell entgegengenommen werden müssen.

Diese Einstellung sollte gewählt werden, wenn verhindert werden soll, dass von außen unbemerkt eine Verbindung aufgebaut werden kann. Ansonsten ist ein Callback-Mechanismus einzusetzen (siehe M 5.30 *Aktivierung einer vorhandenen Callback-Option*).

**Fernkonfiguration des Modems**

Manche Modems können so eingestellt werden, dass sie von entfernten Modems fernkonfiguriert werden können. Es ist darauf zu achten, dass diese Möglichkeit ausgeschaltet ist. Zum Problem der Fernwartung über Modems siehe M 5.33 *Absicherung von Fernwartung*.

**Passwortgeschützte Speicherung von (Rückruf-)Nummern**

Bei der Speicherung von Telefonnummern oder Rückrufnummern im nichtflüchtigen Speicher des Modems können diese bei vielen Modellen durch ein Passwort geschützt werden. Wenn diese Möglichkeit vorhanden ist, sollte sie genutzt und die Passwörter entsprechend M 2.11 *Regelung des Passwortgebrauchs* gewählt werden. Bei einigen Modems wird nach Eingabe eines bestimmten Befehls eine Liste der Rufnummern **mit** den zugehörigen Passwörtern angezeigt. Daher sollte der Zugang zum Modem nur befugten Personen möglich sein (siehe M 1.38 *Geeignete Aufstellung eines Modems*).

Prüffragen:

- Sind Modems so konfiguriert, dass keine Sicherheitslücken offen bleiben?
- Ist die Modem-Konfiguration dokumentiert?
- Verhinderung des unbemerkten Verbindungsaufbaus von außen: Wird die automatische Rufannahme deaktiviert?
- Ist die Möglichkeit zur Fernkonfiguration des Modems deaktiviert?

# M 5.32 Sicherer Einsatz von Kommunikationssoftware

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die Sicherheit des Rechnerzugangs über Modem hängt entscheidend von der eingesetzten Kommunikationssoftware ab.

Fast jede Kommunikationssoftware bietet die Möglichkeit, Telefonnummern und andere Daten von Kommunikationspartnern zu speichern. Dies sind personenbezogene Daten, die entsprechend geschützt werden müssen.

Passwörter für den Zugang auf andere Rechner oder Modems sollten nicht in der Kommunikationssoftware gespeichert werden, auch wenn das komfortabel erscheinen mag. Jeder, der Zugang zum IT-System und der Kommunikationssoftware hat, kann dann unter fremdem Benutzernamen Zugang in andere Systeme erlangen (siehe auch M 1.38 *Geeignete Aufstellung eines Modems* und M 2.8 *Vergabe von Zugriffsrechten*).

Etliche Kommunikationsprogramme bieten die Möglichkeit, die Datenübertragung im Hintergrund und damit unbeobachtet laufen zu lassen, z. B. unter Windows. Dies sollte nur bei vertrauenswürdigen Kommunikationspartnern genutzt werden, da hierbei ein Kommunikationspartner die Dateiübertragung abbrechen und u. U. andere Daten als abgesprochen vom oder zum lokalen Rechner übertragen könnte. Damit könnten beispielsweise Computer-Viren auf den lokalen Rechner eingeschleust oder vertrauliche Daten kopiert werden. Es gibt außerdem auch Übertragungsprotokolle, die eine Vollduplex-Übertragung, also gleichzeitiges Senden und Empfangen zulassen. Solche Übertragungsprotokolle sollten nur mit vertrauenswürdigen Kommunikationspartnern benutzt werden, da dies einer Datenübertragung im Hintergrund entspricht.

Verfügt die Kommunikationssoftware über eine Passwortabsicherung oder über Protokollierungsfunktionen, muss sie aktiviert werden.

Prüffragen:

- Werden Kontaktdaten von Kommunikationspartnern in der eingesetzten Kommunikationssoftware ausreichend geschützt?
- Wird das Speichern von Passwörtern in der Kommunikationssoftware verhindert bzw. untersagt?
- Werden vorhandene Sicherheitsmechanismen in der Kommunikationssoftware wie Passwortabsicherung oder Protokollierungsfunktionen genutzt?

# M 5.33 Absicherung von Fernwartung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Die Fernwartung von IT-Systemen birgt besondere Sicherheitsrisiken. Bei der Fernwartung ist zu unterscheiden, ob internes oder externes Wartungspersonal auf die IT-Systeme zugreift. Damit Administratoren IT-Benutzern schnell helfen können, ohne dass sie sich zum Aufstellungsort der jeweiligen IT-Systeme begeben müssen, werden bei der IT-Betreuung häufig Fernwartungszugänge genutzt. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich.

Das zu wartende IT-System muss die folgenden Sicherheitsfunktionen realisieren:

- Der Aufbau der Verbindung für eine Fernwartung sollte immer vom lokalen IT-System initiiert werden. Dies kann durch Anruf des zu wartenden IT-Systems bei der Fernwartungsstelle oder über einen automatischen Rückruf (Callback) realisiert werden.
- Der Benutzer des IT-Systems muss dem Fernzugriff explizit zustimmen, z. B. über eine entsprechende Bestätigung am System. Er sollte alle Tätigkeiten während des Fernzugriffs beobachten.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden (siehe M 5.34 *Einsatz von Einmalpasswörtern*).
- Die Durchführung einer Fernwartung muss protokolliert werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
- Einschränkung der Rechte des Wartungspersonals: Das Wartungspersonal sollte nicht die vollen Administrator-Rechte besitzen. Es sollte eine abgestufte Rechteverwaltung realisiert werden, bei Unix-Systemen ist außerdem M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix*zu beachten, bei PC-Netzen M 2.38 *Aufteilung der Administrationstätigkeiten*
  (Das Wartungspersonal sollte nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.)
- auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzer-Kennung existieren, unter der möglichst alle Wartungsarbeiten durchgeführt werden,
- wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch einen "Zwangslogout" beendet werden.

**Externe Fernwartung**

Fernwartung über externe Netze oder durch Dritte ist besonders kritisch. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist

dies nicht möglich, so sind zusätzlich zu den oben genannten Sicherheitsmaßnahmen folgende Punkte zu beachten:

- Bei einer Fernwartung über externe Kommunikationsverbindungen, müssen die Zugänge und die Verbindungen abgesichert werden. Das Fernwartungspersonal muss sich authentisieren und die übertragenen Daten müssen verschlüsselt werden. Beispielsweise kann die Anbindung per VPN oder exklusiv genutzte Verbindungen realisiert werden.
- Wenn dies technisch möglich ist, sollten alle Tätigkeiten während der Administration von Dritten durch eigene IT-Experten beobachtet werden. Beispielsweise können bei der Fernadministration eines Clients über eine graphische Benutzeroberfläche oft alle Ein- und Ausgaben am zu wartenden IT-System angezeigt und aufgezeichnet werden. Auch wenn Fernwartung durch Dritte genutzt wird, weil intern das Know-How oder die Kapazität nicht verfügbar ist, kann das externe Wartungspersonal nicht unbeaufsichtigt gelassen werden (siehe auch M 2.3 *Datenträgerverwaltung*). Bei Unklarheiten über die Vorgänge sollte der lokale IT-Experte sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.
- Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.
- Alle Remote-Administrationsvorgänge müssen aufgezeichnet werden. Dabei ist zumindest Anfang und Ende der Fernwartung sowie die Beteiligten festzuhalten. Wenn auf dem gewarteten IT-System niemand die Fernzugriffe beobachten kann, müssen alle Tätigkeiten bei der Durchführung der Fernwartung auf dem zu wartenden IT-System protokolliert werden.

Entsprechend M 3.55 *Vertraulichkeitsvereinbarungen* sind auch mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Prüffragen:

- Ist sichergestellt, dass Fernwartung nur durchgeführt wird, wenn angemessene Sicherheitsmaßnahmen ergriffen werden?
- Ist sichergestellt, dass Fernwartungszugriffe immer nur vom lokalen IT-System initiiert werden können?
- Wird die Durchführung der Fernwartung ausreichend protokolliert?

# M 5.34 Einsatz von Einmalpasswörtern

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

In Netzen, in denen Passwörter unverschlüsselt übertragen werden, können diese relativ einfach abgehört werden. Außerdem können Implementierungs- oder Protokollfehler in Betriebssystemen und Applikationssoftware dazu führen, dass auch verschlüsselte Passwörter kompromittiert werden können.

Daher empfiehlt sich die Verwendung von Einmalpasswörtern, also Passwörtern, die nach einmaligem Gebrauch gewechselt werden müssen. Einmalpasswörter können software- oder hardwaregestützt erzeugt werden.

Bei der Verwendung von Einmalpasswörtern muss der Benutzer das Einmalpasswort auf dem lokalen IT-System oder über ein Token generieren oder aus einer Liste einlesen, die vom entfernten IT-System generiert worden ist und die sicher aufzubewahren ist. Das entfernte IT-System muss dann das Einmalpasswort verifizieren.

Token, die die Generierung von Einmalpasswörtern übernehmen, sind kleine tragbare Hardware-Komponenten. Dies können zum Beispiel Chipkarten oder taschenrechnerähnliche Geräte sein. Der Benutzer muss sich zunächst gegenüber dem Token authentisieren. Nach erfolgter Benutzer-Authentisierung authentisiert sich dann entweder der Token selbständig gegenüber dem Server oder er zeigt dem Benutzer an einem Display das am Client einzugebende Einmalpasswort an.

Nachdem immer mehr sensible Informationen nur durch Passwörter vor Fremdzugriff geschützt sind, kommt Einmalpasswortsystemen und hardwarebasierten Authentikationsmethoden ein wachsender Stellenwert zu.

Nachdem immer mehr sensible Informationen nur durch Passwörter vor Fremdzugriff geschützt sind, kommt Einmalpasswortsystemen und hardwarebasierten Authentikationsmethoden ein wachsender Stellenwert zu.

Viele hardwarebasierte Systeme bieten auch die Möglichkeit, "Single-Sign-On"-Lösungen aufzubauen. Über "Single-Sign-On"-Verfahren wird erreicht, dass sich Benutzer nicht an jedem IT-System oder an jeder Anwendung mit einem anderen Passwort ausweisen müssen. Stattdessen melden sich die Benutzer an einem IT-System oder an einem besonderen Portal an und können dann ohne zusätzliche manuelle Authentisierung weitere Anwendungen oder IT-Systeme nutzen.

Durch hardwarebasierte Einmalpasswortsysteme werden außerdem viele der unter M 2.11 *Regelung des Passwortgebrauchs* aufgeführten Regelungen, die die einzelnen Benutzer beachten müssen, überflüssig, da dies von den Einmalpasswortsystemen übernommen wird.

Prüffragen:

- Ist sichergestellt, dass keine wiederverwendbaren Passwörter unverschlüsselt über das Netz übertragen werden?

# M 5.35 Einsatz der Sicherheitsmechanismen von UUCP

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Das im Standardumfang von Unix-Systemen enthaltene und ebenfalls für andere Betriebssysteme verfügbare Programmpaket UUCP (Unix-to-Unix Copy) erlaubt den Datenaustausch zwischen IT-Systemen und die Ausführung von Kommandos auf entfernten IT-Systemen. Voraussetzung ist lediglich die Kompatibilität der *uucico*-Programme auf den beiden beteiligten Systemen. UUCP ist stark verbreitet, auch wenn seine Bedeutung zurückgegangen ist z.B. durch die Möglichkeit, Rechner über ISDN mittels TCP/IP zu verbinden.

UUCP wird in der Regel zum Austausch von E-Mail und News zwischen Rechnern benutzt (*uucp*). Es ermöglicht auch das Einloggen (*cu*) und das Ausführen von Programmen (*uux*) auf fremden Rechnern.

Es gibt verschiedene UUCP-Varianten: Neben der Implementation von Peter Honeyman, David Nowitz und Brian E. Redman von 1983 (HoneyDanBer UUCP) werden auch häufig das ursprüngliche UUCP-System der AT&T UNIX Version 7, dessen zweite Version aktuell ist (diese UUCP-Implementation wird daher auch Version 2 UUCP genannt) oder das Tahoe-UUCP (das mit BSD 4.3 ausgeliefert wurde) eingesetzt.

Die eingesetzte UUCP-Variante kann an den Dateien im Verzeichnis */usr/lib/uucp* (auf einigen Systemen */etc/uucp*) erkannt werden: Bei Version 2 UUCP findet sich hier die Datei *L.sys*, beim HoneyDanBer UUCP die Datei *Systems*.

Version 2 UUCP hat gravierende Sicherheitsprobleme (Fehler in *uucico*, Gefahr fehlerhafter Konfiguration durch die komplizierte Form der sicherheitsrelevanten Administrationsdateien). Sie sollte daher nicht benutzt werden, stattdessen sollte das HoneyDanBer UUCP eingesetzt werden.

Allgemein sollten folgende Sicherheitsfragen beim Einsatz von UUCP bedacht werden:

- Die Administration von UUCP setzt eine intensive Beschäftigung mit den Konfigurationsmöglichkeiten und den zugehörigen Dateien voraus. Es muss berücksichtigt werden, dass es zwischen den UUCP-Paketen der verschiedenen Unix-Derivate Abweichungen geben kann, auch wenn diese auf dem HoneyDanBer UUCP basieren.
- Für die Administration der UUCP-Dateien, -Programme und -Verzeichnisse gelten dieselben Anforderungen wie für die Administration von Systemdateien und -verzeichnissen (siehe M 2.25 *Dokumentation der Systemkonfiguration*, M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*, M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*).
- Auf den meisten Systemen gibt es einen Benutzer namens *uucp*. Diesem Benutzer gehören die UUCP-Dateien, -Programme und -Verzeichnisse. Es ist sicherzustellen, dass dieser Account ein Passwort gemäß den Vorgaben der Maßnahme M 2.11 *Regelung des Passwortgebrauchs* hat.
  Das Heimatverzeichnis für den Benutzer *uucp* darf nicht das öffentliche Verzeichnis */usr/spool/uucppublic* sein, sondern ein eigenes, auf das nur der Benutzer *uucp* Zugriff hat.

- Für jedes IT-System, das sich per UUCP am lokalen IT-System anmelden können soll, muss in der */etc/passwd* eine eigene Benutzer-Kennung und ein Passwort eingetragen werden. Als UID darf nicht die des Benutzers *uucp* gewählt werden, sondern für jedes entfernte IT-System eine beliebige individuelle UID.
- UUCP-Passwörter werden bei Kommunikationsanforderungen unverschlüsselt übertragen und sind in der entsprechenden UUCP-Konfigurationsdatei für Anforderungen an entfernte Rechner unverschlüsselt gespeichert. Je nach Anwendung und Umgebung (insbesondere bei Benutzung von Weitverkehrsnetzen) sind entsprechende Sicherheitsmaßnahmen wie z. B. der Einsatz von Einmalpasswörtern zu ergreifen.

Für die Benutzung von UUCP müssen verschiedene Konfigurationsdateien eingerichtet werden. Alle Einstellungen sollten dokumentiert und Abweichungen der im Folgenden vorgeschlagenen Einstellungen kurz begründet werden, damit später nachvollziehbar ist, wozu diese Änderung notwendig war.

Die Verwaltung der folgenden Dateien muss besonders sorgfältig gehandhabt werden, da sie sicherheitskritische Informationen enthalten. Sie befinden sich im Verzeichnis */usr/lib/uucp* bzw. */etc/uucp*). Auf diese Verzeichnisse darf nur der Benutzer *uucp* schreibenden Zugriff haben.

- *Systems*: Diese Datei enthält die für einen Verbindungsaufbau mit entfernten IT-Systemen benötigten Informationen. Hier können für jedes einzelne IT-System die Zeiträume festgelegt werden, in denen die Übertragung per UUCP zugelassen ist. Diese Zeiträume sind möglichst eng zu fassen. Die Datei enthält außerdem die Telefonnummern und Login-Sequenzen der IT-Systeme, zu denen per UUCP eine Verbindung aufgebaut werden kann. Auf *Systems* darf nur der Eigentümer *uucp* lesenden Zugriff haben, da hier auch die Passwörter für die entfernten IT-Systeme eingetragen sind.
- *Permissions*: Hier werden Zugriffsrechte für entfernte Systeme festgelegt. Bei Auslieferung sind in *Permissions* keine IT-Systeme eingetragen, d. h. über UUCP sind keine Zugriffe möglich. Für jeden Rechner, der anrufen und sich einloggen darf, und für jeden Rechner, der angerufen werden darf, müssen hier Einstellungen zur Festlegung der jeweilig notwendigen Zugriffsrechte und anderer Bedingungen vorgenommen werden. Die Zugriffsrechte für die IT-Systeme, die vom lokalen IT-System angerufen werden, werden unter den auf MACHINE folgenden Einträgen spezifiziert, die für die anrufenden IT-System unter den auf LOGNAME folgenden. Durch Ausnutzung dieser Konfigurationsmöglichkeiten kann die Sicherheit beachtlich erhöht werden.
  Mit dem Kommando *uucheck -v* sollten die in der Datei *Permissions* gesetzten Optionen regelmäßig überprüft werden. Die Optionen sollten wie folgt gesetzt sein:

  - **REQUEST**
    Diese Option sollte auf NO (Default-Wert) gesetzt sein, um entfernten Systemen das Lesen lokaler Dateien zu verbieten.
  - **COMMANDS**
    Hier darf auf keinen Fall ALL eingetragen sein, es dürfen nur die Kommandos zugelassen werden, die nötig sind wie *rnews* oder *rmail*. Die Kommandos sollen mit vollem Pfadnamen angegeben werden.
  - **WRITE/READ**
    Wenn diese Optionen nicht angegeben sind, ist der schreibende bzw. lesende Zugriff ausschließlich auf das Verzeichnis */usr/spool/uucppublic* möglich.

Falls hiermit Verzeichnisse angegeben werden, auf die zugegriffen werden darf, ist zu dokumentieren, auf welche und warum. Auf keinen Fall darf hier das Root-Verzeichnis oder das Verzeichnis, in dem sich die UUCP-Konfigurationsdateien befinden, eingetragen sein.

- **NOWRITE/NOREAD**
  Hiermit werden Ausnahmen zu den mit WRITE/READ festgelegten Optionen festgelegt. Verzeichnisse mit sensitiven Inhalten sollten hier generell aufgeführt werden. Dann kann nicht dadurch, dass das Setzen von Restriktionen vergessen wird, von entfernten IT-Systemen auf solche Verzeichnisse zugegriffen werden, wenn darüberliegende Verzeichnisse über READ/WRITE freigegeben werden.
- **PUBDIR**
  Hiermit kann statt */usr/spool/uucppublic* ein anderes öffentliches UUCP-Verzeichnis angegeben werden. Bei UUCP-Kommunikation mit mehreren IT-Systemen sollte für jedes IT-System ein eigenes UUCP-Verzeichnis angegeben werden.
- **CALLBACK**
  Wenn CALLBACK auf YES gesetzt ist, muss das lokale IT-System das anrufende IT-System zurückrufen, bevor ein Datenaustausch stattfinden kann. Dies macht natürlich nur für LOGNAME Einträge Sinn. Es sollte zwischen den Kommunikationspartnern abgesprochen sein, welche einen CALLBACK aktiviert.
- **MYNAME**
  Wenn MYNAME=*name* gesetzt ist, identifiziert sich das lokale System beim Aufbau einer UUCP-Verbindung beim entfernten System nicht mit dem Rechnernamen, sondern mit *name*. Diese Möglichkeit sollte benutzt werden, um sich mit einem Namen identifizieren zu können, der nur speziell für diese Verbindung benutzt wird und daher nicht so leicht herausgefunden werden kann.
- **VALIDATE**
  Wenn VALIDATE=*namen* gesetzt ist, können nur die unter *namen* aufgeführten IT-Systeme über die unter LOGNAME angegebenen Systemnamen eine Verbindung aufbauen. Bei dieser Option muss unbedingt ein Eintrag vorhanden sein, da sonst ein entferntes IT-System eine Maskerade durchführen könnte, indem über MYNAME ein anderer Rechnername vorgespiegelt wird.
- **SENDFILES**
  Hier sollte die Voreinstellung (SENDFILE=CALL) beibehalten werden, da dann lokal in der Queue befindliche Aufträge nur nach extern übertragen werden, wenn das lokale IT-System die Verbindung aufgebaut hat.

- Die Datei */usr/lib/uucp/remote.unknown* des HoneyDanBer UUCP wird ausgeführt, wenn ein unbekanntes, also ein nicht in der Datei *Systems* eingetragenes IT-System einen Verbindungsaufbau versucht. Es protokolliert den Versuch und weist ihn ab. Wenn *remote.unknown* nicht ausführbar ist, geht das lokale IT-System auf alle Verbindungsanforderungen entfernter IT-Systeme ein. Es muss daher darauf geachtet werden, dass *remote.unknown* stets ausführbar ist. *remote.unknown* ist je nach Unix-System als ausführbares Shellskript oder als C-Programm realisiert. Falls *remote.unknown* auf dem lokalen IT-System als Shellskript realisiert ist, sollte es aus Sicherheitsgründen durch ein Programm ersetzt werden. Sonst besteht die Gefahr, dass ein anrufendes IT-System ein Kommando wie "cat < /etc/passwd" als Systemnamen einträgt, das dann zur Ausführung gelangen kann.
- Für UUCP gibt es einige Cleanup-Shellskripte, die automatisch über den *crontab*-Dämon ausgeführt werden. Dies darf nicht von *root* initiiert wer-

den, wie es auf vielen Systemen üblich ist, sondern muss durch den Benutzer *uucp* erfolgen.

Bei der Benutzung von UUCP werden automatisch verschiedene Protokollierungsdateien angelegt. Beim HoneyDanBer UUCP finden sich diese in Unterverzeichnissen von */usr/spool*. Hier werden erfolgreiche und abgelehnte Verbindungsversuche festgehalten, die gesendeten und empfangenen Datenmengen, Fehlermeldungen und Datentransferstatistiken. Diese Protokollierungsdateien müssen regelmäßig ausgewertet werden (siehe auch M 4.25 *Einsatz der Protokollierung im Unix-System*).

Prüffragen:

- Werden die Sicherheitsmechanismen von uucp genutzt?
- Entspricht das Sicherheitsniveau der Administration von uucp-Dateien, -Programmen und Verzeichnissen dem von Systemdateien und -verzeichnissen?

# M 5.36 Verschlüsselung unter Unix und Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 5.37 Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 5.38 Sichere Einbindung von DOS-PCs in ein Unix-Netz

Diese Maßnahme ist mit Version 2006 entfallen.

# M 5.39 Sicherer Einsatz der Protokolle und Dienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die folgenden kurzen Beschreibungen häufig im Internet verwendeter Protokolle und Dienste sollen als Hinweis dienen, welche Informationen von diesen Protokollen übertragen werden und somit für eine Filterung durch ein Sicherheitsgateway zur Verfügung stehen. Des weiteren ist kurz beschrieben, welche Randbedingungen beim Einsatz der verschiedenen Protokolle und Dienste zu beachten sind.

### Grundlegende Protokolle der tieferen Schichten des ISO/OSI Schichtenmodells

#### IP

Das Internet Protocol (IP) ist das Protokoll, auf dem praktisch alle gebräuchlichen Protokolle in lokalen Netzen aufbauen. IP ist ein verbindungsloses Protokoll. Ein IP-Header enthält u. a. zwei 32-Bit Adressen (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

Da die IP-Adressen leicht gefälscht werden können (siehe auch G 5.48 *IP-Spoofing*), können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden, also nur wenn sichergestellt ist, dass die Adressen nicht geändert werden können. Beispielsweise dürfen Pakete, die von außen kommen, aber als Quelladresse eine Adresse aus dem zu schützenden Netz haben, von dem Sicherheitsgateway nicht durchgelassen werden.

#### ARP

Das Address Resolution Protocol (ARP) dient dazu, zu einer 32-Bit großen IP-Adresse die zugehörige 48-Bit lange MAC-Adresse ("Media Access Control", auch Hardware- oder Ethernet-Adresse genannt) zu finden. Jeder Rechner führt für andere Stationen in seiner Broadcast-Domain eine Tabelle, in der die Zuordnung zwischen IP- und Hardware-Adressen gespeichert ist. Falls in dieser Tabelle kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der IP-Adresse ausgesandt, zu der die MAC-Adresse gesucht wird. Der Rechner mit dieser IP-Adresse sendet dann ein ARP-Antwort-Paket mit seiner MAC-Adresse zurück. ARP-Antwort-Pakete sind nicht manipulationssicher ("ARP-Spoofing", siehe auch G 5.112 *Manipulation von ARP-Tabellen*).

#### ICMP

Das Internet Control Message Protocol (ICMP, spezifiziert in RFC 792) hat die Aufgabe, Fehler- und Diagnoseinformationen für IP zu transportieren. Es wird intern von IP, TCP oder UDP angestoßen und verarbeitet. ICMP kennt eine Anzahl verschiedener sogenannter Nachrichtentypen für verschiedene Zwecke.

Je nach Einsatzszenario sollten bestimmte ICMP Nachrichtentypen selektiv zugelassen beziehungsweise blockiert werden. Zur Behandlung von ICMP am Sicherheitsgateway siehe M 5.120 *Behandlung von ICMP am Sicherheitsgateway*.

**Routing Protokolle**

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routing-Tabellen zu ermöglichen. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren. Dynamisches Routing sollte daher nur in ganz bestimmten Topographien angewendet werden.

Am Sicherheitsgateway sollten Routing-Protokolle nur im unbedingt notwendigen Umfang eingesetzt werden. Wo dies möglich ist sollten nur sichere Routing-Protokolle eingesetzt werden. Mehr Informationen finden sich in M 5.112 *Sicherheitsaspekte von Routing-Protokollen*.

**UDP**

Das User Datagram Protocol (UDP) ist ein verbindungsloses Protokoll der Transportschicht. Es gibt keine Transportquittungen oder andere Sicherheitsmaßnahmen für die Korrektheit der Übertragung. Der Header enthält (analog zu TCP) unter anderem zwei 16-Bit Portnummern, die aber unabhängig von den bei TCP benutzten Portnummern sind. Da sie leicht gefälscht werden können, können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden.

Da in der Protokolldefinition keine Unterscheidung zwischen einem Verbindungsaufbau und einer Datenübertragung vorgesehen ist, muss diese Unterscheidung von einer Komponente des Sicherheitsgateways übernommen werden. Es muss eine Kontrolle über den Zustand der Verbindung möglich sein, und es muss möglich sein, die Zugehörigkeit eines Paketes zu einer Verbindung eindeutig festzustellen.

Dies kann z. B. erreicht werden, indem bei einem UDP-Verbindungsaufbau der Zielport gespeichert und temporär freigegeben wird, Antwortpakete nur zu diesem Port durchgelassen werden und nach der Beendigung der Verbindung oder nach einem Timeout der Port wieder gesperrt wird.

**Protokolle der Anwendungsschicht**

**DNS**

Der Domain Name Service (DNS) dient zur Umsetzung von Rechnernamen in IP-Adressen und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. DNS kann sowohl über TCP als auch über UDP abgewickelt werden, der Server benutzt bei beiden Träger-Protokollen standardmäßig den Port 53. Meist wird UDP als Trägerprotokoll verwendet.

Die übertragenen Informationen sind nicht durch kryptographische Verfahren geschützt, so dass durch gefälschte Daten Spoofing-Angriffe möglich sind (siehe auch G 5.78 *DNS-Spoofing*). Dies sollte insbesondere bei DNS-Antworten aus dem Internet berücksichtigt werden.

Prinzipiell muss beachtet werden, dass alle von DNS zur Verfügung gestellten Informationen missbraucht werden können.

Zur Integration von DNS ist ein Sicherheitsgateway erforderlich (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway* und M 5.118 *Integration eines DNS-Servers in ein Sicherheitsgateway* .

**SMTP**

Das Simple Mail Transfer Protocol (SMTP) wird für die Übertragung von E-Mail benutzt. SMTP-Server (Mail-Server, auch Mail Transport Agents (MTAs) genannt) benutzen standardmäßig den TCP-Port 25. SMTP, das im RFC 821 definiert wird, besteht aus einer geringen Zahl von Kommandos, die teilweise aus Sicherheitssicht bedenklich sind.

Mit den Befehlen *VRFY* und *EXPN* können beispielsweise interne Informationen über Benutzer abgerufen werden, daher sollte die Verwendung dieser Befehle nur innerhalb des geschützten Netzes erlaubt werden. Für nicht vertrauenswürdige Benutzer, insbesondere für Anfragen aus dem Internet, sind *VRFY* und *EXPN* entweder am ALG (Application-Level-Gateway) oder direkt auf dem MTA (Mail Transport Agent, Mail-Server) zu sperren.

Idealerweise sollte ein Sicherheitsgateway in der Lage sein, SMTP-Verbindungen zwischen vertrauenswürdigen Benutzern zu verschlüsseln. Sinnvoll ist dies aber nur dann, wenn ein starker Authentisierungsmechanismus benutzt wird.

**HTTP**

Das Hypertext Transfer Protokoll (HTTP) wird für die Übertragung von Daten zwischen WWW-Clients (meist Webbrowsern) und Webservern benutzt. HTTP und diverse Erweiterungen werden in einer Reihe von RFCs definiert, der RFC 2616, in dem die aktuelle Variante HTTP 1.1 spezifiziert wird, enthält eine Reihe von Referenzen auf ältere Dokumente. Standardmäßig benutzt ein Webserver den TCP-Port 80.

HTTP ist ein Klartextprotokoll, das keine Unterstützung für eine sichere Authentisierung und keine Gewährleistung für die Vertraulichkeit und Integrität der übertragenen Daten bietet. Dies sollte bei der Entscheidung, welche Transaktionen über HTTP abgewickelt werden können, berücksichtigt werden.

Weitere Informationen über Maßnahmen im Zusammenhang mit HTTP finden sich in M 4.222 *Festlegung geeigneter Einstellungen von Sicherheitsproxies* und M 4.100 *Sicherheitsgateways und aktive Inhalte*.

**HTTPS**

HTTPS (HTTP über SSL bzw. HTTP über TLS) ist eine Variante von HTTP, bei der Authentisierung und Datenübertragung durch Verschlüsselung und Zertifikate geschützt werden können. HTTPS wird im RFC 2818 spezifiziert. Meist benutzt ein Webserver, der HTTPS unterstützt, den TCP-Port 443.

Beim Einsatz von HTTPS muss beachtet werden, dass TLS auch einen Betriebsmodus kennt, in dem keine Verschlüsselung stattfindet. Bei entsprechenden Sicherheitsanforderungen sollte am HTTPS-Proxy verhindert werden, dass entsprechende Verbindungen aufgebaut werden können.

Weitere Informationen finden sich in M 4.222 *Festlegung geeigneter Einstellungen von Sicherheitsproxies* und M 4.100 *Sicherheitsgateways und aktive Inhalte*, sowie in M 5.66 *Clientseitige Verwendung von SSL/TLS*.

**Secure Shell / Secure Copy**

Das Secure Shell (SSH) Protokoll erlaubt den Aufbau einer gesicherten Kommandozeilen-Verbindung zu einem entfernten Rechner. Das SSH-Protokoll erlaubt eine gesicherte Authentisierung mit einer Reihe verschiedener Authentisierungsmechanismen (unter anderem über Benutzername und Passwort, mit speziellen Zertifikaten, über eine zentral verwaltete PKI-Infrastruktur oder über Kerberos). SSH eignet sich daher als Ersatz für Telnet. Wo immer möglich sollte Telnet durch SSH ersetzt werden. Standardmäßig benutzt ein SSH-Server den TCP-Port 22.

Zur SSH-Protokollfamilie gehört auch das Protokoll SCP (Secure Copy Protocol), das zur Übertragung von Dateien die Authentisierungs- und Verschlüsselungsmechanismen von SSH benutzt. SCP stellt eine sichere Alternative zu FTP dar.

Für SSH existiert eine Reihe verschiedener Implementierungen für praktisch alle gebräuchlichen Betriebssysteme, sowie zusätzlich betriebssystemunabhängige Implementierungen beispielsweise in Java. Die verschiedenen Implementierungen unterscheiden sich jedoch teilweise bei der Anzahl der unterstützten Authentisierungsmechanismen und in anderen Details.

Die meisten SSH-Clients bieten zusätzlich die Möglichkeit, andere Protokolle über eine bestehende SSH-Verbindung zu "tunneln" und so die Nachteile beispielsweise von Klartextprotokollen zu vermeiden. Andererseits stellt diese Option auch ein gewisses Risiko dar, da auf diese Weise Datenübertragungen "versteckt" werden können. Beim Einsatz von SSH sollte daher sorgfältig geprüft werden, mit welchen Kommunikationspartnern Verbindungen zugelassen werden. Gegebenenfalls sollte ein entsprechender Sicherheitsproxy eingesetzt werden, der die verschlüsselte Verbindung am Sicherheitsgateway unterbricht.

Die ursprüngliche Version des SSH-Protokolls (ssh1) besitzt einen Designfehler, der einen Man-in-the-Middle Angriff zulässt. Aus diesem Grund wurde eine neue Version des Protokolls (ssh2) entwickelt, die diese Schwachstelle beseitigt. Die Protokollversion ssh1 sollte zumindest über öffentliche Netze hinweg nicht mehr verwendet werden. Wird für SSH ein Sicherheitsproxy auf dem Sicherheitsgateway eingesetzt, so sollte der Proxy die Möglichkeit bieten, ssh2-Verbindungen zu erzwingen und keine ssh1-Verbindungen zuzulassen.

**Telnet**

Das Telnet-Protokoll wird in RFC 854 spezifiziert. Es erlaubt (analog zu SSH) den Aufbau einer Terminalsitzung auf einem entfernten Rechner. Telnet ist ein Klartextprotokoll, das keine Mechanismen zur Sicherung der Authentisierungsinformationen und der übertragenen Daten und Kommandos bietet. Ein Telnet-Server benutzt standardmäßig den TCP-Port 23.

Da Telnet einen vollständigen Kommandozeilenzugriff auf einen Rechner erlaubt, jedoch keine Sicherungsmechanismen bietet, sollte Telnet wo immer möglich durch SSH ersetzt werden. Alternativ können Telnet-Verbindungen über SSH getunnelt werden. Falls aus zwingenden Gründen ein Ersatz von Telnet durch SSH oder ein Tunneln nicht möglich ist, kann im internen Netz weiterhin Telnet eingesetzt werden. Dabei sollten jedoch die erlaubten Kommunikationsverbindungen über entsprechende Paketfilterregeln auf das unbedingt notwendige Maß beschränkt werden. Für Administrationstätigkeiten

sollte Telnet allenfalls noch in einem besonders abgeschotteten Administrationsnetz eingesetzt werden.

Telnet-Verbindungen können von einem Angreifer übernommen werden, der Zugriff auf eine Netzkomponente besitzt, über die die betreffende Verbindung läuft (siehe G 5.89 *Hijacking von Netz-Verbindungen*). Auf ungesicherten Verbindungen (öffentliche Netze) sollte Telnet daher auch dann nicht mehr eingesetzt werden, wenn der eingesetzte Telnet-Server erweiterte Authentisierungsmechanismen wie Einmalpasswörter unterstützt.

**FTP**

Das File Transfer Protocol (FTP) wird im RFC 959 spezifiziert. Es ermöglicht den Austausch von Dateien zwischen entfernten Rechnern. Wie Telnet ist FTP ein Klartextprotokoll, das keine Sicherung der übertragenen Authentisierungsinformationen und Daten bietet.

Bei Benutzung von FTP werden zwei Verbindungen aufgebaut, wobei die Kommandos über den TCP-Port 21 übertragen werden und die Daten über TCP-Port 20. Telnet definiert eine Anzahl an Standard-Befehlen, mit denen Art und Format der Datenübertragung gesteuert werden und die einem FTP Client eine Navigation im Dateibaum eines FTP-Servers erlauben. Für das Sicherheitsgateway sind diese Standardbefehle relevant, da nur diese tatsächlich übertragen werden.

Eine FTP-Kommandoverbindung wird vom Client zum Port 21 des Servers aufgebaut. Für die Datenverbindungen gibt es bei FTP zwei Betriebsmodi, den *Active* und den *Passive Mode*. Beim *Active Mode* baut der FTP-Server die Datenverbindung zum Client auf, beim *Passive Mode* wird auch die Datenverbindung vom Client aus aufgebaut.

Der *Active Mode* stellt eine Sicherheitslücke dar, da sich ein Angreifer als Server ausgeben kann und auf diese Weise die Möglichkeit bekommen würde, eine Verbindung ins interne Netz aufzubauen. Falls FTP eingesetzt wird, so sollte stets der *Passive Mode* verwendet werden, bei dem sowohl die Kommando- als auch die Datenverbindung vom zu schützenden ins externe Netz stattfinden.

Alle Befehle, die Dateien oder Verzeichnisse manipulieren oder lesen (*CWD, CDUP, RETR, STOR, DELE, LIST, NLIST*), müssen an eine entsprechende Rechteverwaltung gekoppelt sein. Zugriffe nicht vertrauenswürdiger Benutzer werden damit auf bestimmte Dateien eingeschränkt oder ganz unterbunden. Dies setzt einen starken Authentisierungsmechanismus voraus.

Auch der Befehl *SYST*, mit dem ein Client nach der Betriebssystem-Version des Servers fragt, sollte an eine Rechteverwaltung gekoppelt sein bzw. für nicht vertrauenswürdige Benutzer gesperrt werden.

Ferner muss es möglich sein, die Übertragung der Dateien, der Verzeichnisinformationen und der Passwörter zu verschlüsseln.

FTP sollte nicht zur Übertragung schutzbedürftiger Daten über öffentliche Netze verwendet werden. Sollen schutzbedürftige Daten über eine externe FTP-Verbindung übertragen werden, müssen sie auf andere Weise geschützt (beispielsweise verschlüsselt) werden. Nach Möglichkeit sollte FTP durch ein sicheres Protokoll wie SCP ersetzt werden.

Häufig wird FTP eingesetzt, um Dateien von öffentlich zugänglichen Servern abzurufen. Sofern dafür keine Authentisierungsinformationen benutzt werden,

die auch auf anderen Systemen verwendet werden (beispielsweise beim *anonymous FTP*), ist dies so lange unkritisch, wie keine Anforderungen an die Integrität und Authentizität der abgerufenen Daten gestellt werden (beispielsweise Abruf von Informationsmaterial). Sind die Integrität und Authentizität der Daten wichtig (beispielsweise beim Herunterladen von Programmpaketen, Patches oder wichtiger Dokumente), so sollten vom Anbieter digitale Signaturen zur Verfügung gestellt werden, mit denen die Unverfälschtheit der Daten geprüft werden kann.

**POP3 und IMAP**

Die Protokolle POP3 (Post Office Protocol Version 3, spezifiziert in RFC 1939) und IMAP (Internet Message Access Protocol, spezifiziert in RFC 3501) werden von E-Mail-Clients eingesetzt, um E-Mails von einem Mailserver abzurufen (POP3) oder auf dem Mailserver zu verwalten (IMAP).

Die Standard-Ports für diese Protokolle sind die Ports 110/TCP (POP3) und 143/TCP (IMAP). Beide Protokolle sind Klartextprotokolle und sollten daher nicht über öffentliche Netze verwendet werden. Für beide Protokolle existieren Varianten, bei denen die Verbindungen durch Verschlüsselung (SSL bzw. TLS) gesichert werden: POP3s (Standard-Port 995/TCP) und IMAPs (Standard-Port 993/TCP).

Auch wenn nur im internen Netz E-Mails abgerufen werden sollen wird empfohlen, möglichst nur die abgesicherten Varianten POP3s oder IMAPs einzusetzen. Sollen E-Mails von einem externen POP3 oder IMAP-Server (etwa bei einem E-Mail-Provider) abgerufen werden, so sollten unbedingt die abgesicherten Versionen der Protokolle verwendet werden, gegebenenfalls mit einer Unterbrechung der verschlüsselten Verbindung an einem entsprechenden Sicherheitsproxy.

**Weitere Dienste**

**Verteilte Dateisysteme**

Verteilte Dateisysteme, bei denen Daten nicht lokal auf einem Rechner, sondern auf einem Dateiserver gespeichert sind, auf den über das Netz zugegriffen wird, existieren seit langem und sind aus der IT-Welt nicht mehr wegzudenken.

Das verbreitetste Beispiel ist die Laufwerksfreigabe unter Microsoft Windows, das zu Grunde liegende Protokoll ist SMB / CIFS (Server Message Block / Common Internet File System). Für dieses Protokoll existiert mit SAMBA auch eine Implementierung für diverse Unix-Derivate.

In der Unix-Welt werden verteilte Dateisysteme seit langem über NFS (Network File System) realisiert. Für NFS existieren auch Implementierungen für Windows. Außerdem gibt es eine Reihe anderer verteilter Dateisysteme wie AFS.

Verteilte Dateisysteme sollten nach Möglichkeit nicht über Sicherheitsgateways hinweg eingesetzt werden, da sie eine Reihe von Problemen mit sich bringen (Sicherheit der Authentisierung, Sicherheit der übertragenen Daten), die einen sicheren Einsatz über ein Sicherheitsgateway hinweg schwierig machen.

Ist in Einzelfällen doch ein Zugriff auf ein verteiltes Dateisystem notwendig, so sollte dieser prinzipiell durch eine VPN-Lösung abgesichert werden.

**Remote-Desktop Protokolle (Window Terminal Server, X-Windows etc.)**

Sowohl Microsoft Windows als auch das X-Window-System, mit dem unter Unix graphische Oberflächen realisiert werden, bieten die Möglichkeit, einzelne Fenster oder die gesamte Arbeitsoberfläche auch auf einem entfernten Rechner darzustellen.

Ein Remote-Desktop Protokoll, das keine oder nur schwache Sicherheitsfunktionen bietet, sollte auch im internen Netz nur in Ausnahmefällen eingesetzt werden, über das Sicherheitsgateway hinweg sollten Remote-Desktop Protokolle prinzipiell nicht verwendet werden. Muss dies in Ausnahmefällen trotzdem geschehen, so sollten unbedingt zusätzliche Maßnahmen ergriffen werden, etwa der Einsatz eines geeigneten VPN, das eine entsprechend gesicherte Verbindung zur Verfügung stellt.

**Streaming-Protokolle**

Für die Übertragung von Multimedia-Daten (Audio- und Video-Streaming) existiert eine Reihe von Protokollen mit unterschiedlichen Charakteristiken im Bezug auf Bandbreiten und verwendete Ports. Diese Protokolle sind meist für Sicherheitsgateways nicht unproblematisch, da sie teilweise schlecht über Paketfilterregeln abzusichern sind. Im Zweifelsfall sollte daher auf Streaming-Anwendungen verzichtet werden oder entsprechende Angebote können über gesonderte Internet-PCs (siehe Baustein B 3.208 *Internet-PC*) abgerufen werden.

**Voice over IP**

Es existieren verschiedene Lösungen, die es ermöglichen, Sprachkommunikation über IP-Netze zu übertragen (*Voice over IP, VoIP*). Bei VoIP-Lösungen sind normalerweise mehrere verschiedene Protokolle notwendig, beispielsweise unterschiedliche Protokolle für die Signalisierung und für die Übertragung der Gesprächsdaten selbst.

VoIP-Lösungen, (beispielsweise solche, die dem H.323 Standard entsprechen) sind für Sicherheitsgateways oft problematisch, da verwendete Ports teilweise dynamisch zwischen Endgeräten ausgehandelt werden und daher keine einfache Absicherung über Paketfilter möglich ist.

Soll eine VoIP-Lösung eingesetzt werden, bei der auch eine Kommunikation über VoIP mit Gesprächspartnern außerhalb des eigenen Netzes stattfinden soll, so ist in jedem Fall eine zusätzliche Sicherheitsbetrachtung notwendig um zu vermeiden, dass durch die Anforderungen der VoIP-Lösung die Sicherheit des Netzes dadurch gefährdet wird, dass die Einstellungen des Sicherheitsgateway zu sehr "geöffnet" werden müssen.

**NTP**

Das in RFC 1305 spezifizierte Network Time Protocol (NTP) dient dazu, von einem Zeitserver ein genaues Zeitsignal zu beziehen.

Wird im internen Netz, von Servern oder von Komponenten des Sicherheitsgateways NTP zur Zeitsynchronisation genutzt, so sollte nach Möglichkeit entweder ein eigener Zeitserver im internen Netz oder im Sicherheitsgateway eingesetzt werden. Gegebenenfalls kann ein NTP-Proxy genutzt werden, der seine Zeitinformationen von einem der zentralen Zeitserver bezieht und der dann für die internen Rechner als Zeitserver agiert. Siehe auch M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*.

**NNTP**

Das in RFC 977 spezifizierte Network News Transfer Protocol (NNTP) wird für die Übertragung von Newsartikeln benutzt. Ein Newsserver benutzt standardmäßig den TCP-Port 119. Wie die meisten anderen "frühen" Internetprotokolle ist auch NNTP ein Klartextprotokoll.

Wird ein interner Newsserver betrieben oder soll vom internen Netz auf einen externen Newsserver zugegriffen werden, so muss das Sicherheitsgateway in der Lage sein, den Transport bestimmter Newsgruppen ganz zu verhindern oder nur für einige Rechner zuzulassen. Es muss sichergestellt werden, dass beim Versenden eigener News keine Informationen über das zu schützende Netz (z. B. die Rechnernamen) ins externe Netz gelangen.

**"r-Dienste"**

Die so genannten "r-Dienste" wie rlogin, rsh, rcp und andere basieren auf UDP und bieten keine Möglichkeiten für eine sichere Authentisierung und für die Absicherung der Verbindung.

Diese Dienste sollten auch im internen Netz nur noch in Ausnahmefällen benutzt werden. Über ein Sicherheitsgateway hinweg sollten sie keinesfalls eingesetzt werden. Das Sicherheitsgateway sollte entsprechende Pakete blockieren.

Für die meisten Anwendungsfälle bietet SSH einen vollwertigen Ersatz für die "r-Dienste".

**Hinweis zu den so genannten "Privilegierten Ports"**

Bei einer TCP/IP-Kommunikation baut in der Regel ein Client-Prozess von einem zufälligen Port mit einer Portnummer > 1023 eine Verbindung zu einem Server-Prozess mit einer Portnummer < 1024 (well-known-port) auf. Die Ports mit einer Nummer < 1024 werden auch als privilegierte Ports bezeichnet, da sie beispielsweise unter Unix nur von Prozessen mit Root-Berechtigung benutzt werden dürfen.

Diese Einschränkung, dass Ports < 1024 nur von Prozessen mit Root-Berechtigung benutzt werden dürfen, ist aber nur eine Konvention, die auch umgangen werden kann und die ohnehin in dem Fall keine Rolle spielt, wenn ein Angreifer die Kontrolle über einen Rechner übernommen hat. Daher darf in einem Sicherheitskonzept nicht vorausgesetzt werden, dass tatsächlich alle IT-Systeme ihre privilegierten Ports auf diese Weise schützen. Auch wenn z. B. mit FTP auf die Ports 20 oder 21 zugegriffen wird, darf dies also nicht als sichere Verbindung angesehen werden.

Prüffragen:

- Werden von extern gesendete Pakete, die mit einer Quelladresse aus dem internen Netz versehen sind (Stichwort: IP-Spoofing) auf dem Sicherheitsgateway geblockt?
- Werden auf dem Sicherheitsgateway ausschließlich sichere Routing-Protokolle eingesetzt?
- Findet auf dem Sicherheitsgateway eine Zustands- und Zugehörigkeitskontrolle für UDP-Verbindungen statt?
- Betrifft das Protokoll SMTP: Werden VRFY- und EXPN-Anfragen aus dem Internet durch das Application-Level-Gateway oder den Mail-Server blockiert?

- Erfolgen SMTP-Vebindungen über das Sicherheitsgateway zwischen vertrauenswürdigen Benutzern verschlüsselt und mit starken Authentisierungsmechanismen?
- Ist festgelegt mit welchen Kommunikationspartnern Verbindungen via SSH zugelassen sind?
- Werden bei Einsatz eines Sicherheitsproxies auf dem Sicherheitsgateway für SSH SSHv2-Verbindungen erzwungen und SSH Version 1-Verbindungen unterbunden?
- Wird auf den Einsatz von TELNET soweit möglich verzichtet und werden stattdessen verschlüsselte Protokolle wie beispielsweise SSHv2 genutzt?
- Wird bei FTP ausschließlich der Passive Mode verwendet?
- Sind alle FTP-Befehle an eine Rechteverwaltung gekoppelt?
- Wird der Einsatz von verteilten Dateisystemen über das Sicherheitsgateway hinweg verhindert?
- Werden erforderliche Zugriffe auf verteilte Dateisysteme über das Sicherheitsgateway hinweg durch ein VPN abgesichert?
- Wird der Einsatz von direkten Remote-Desktop Verbindungen über das Sicherheitsgateway hinweg verhindert?
- Wird der erforderliche Einsatz von Remote-Desktop Protokollen über das Sicherheitsgateway hinweg durch eine VPN-Lösung abgesichert?
- Werden Streaming-Protokolle, sofern nicht durch Streaming-Anwendungen zwingend erforderlich, durch das Sicherheitsgateway blockiert?
- Existiert für die Nutzung von VoIP eine zusätzliche Sicherheitsbetrachtung, die den Sicherheitsanforderungen der Organisation entspricht?
- Ist auf dem Sicherheitsgateway festgelegt, welche NNTP-Kommunikation zugelassen oder zu blockieren sind?
- Werden auf dem Sicherheitsgateway Pakete der r-Dienste wie beispielsweise rlogin, rsh, rcp blockiert?
- Existiert eine Übersicht der auf dem Sicherheitsgateway zugelassenen Protokolle?

# M 5.40 Sichere Einbindung von DOS-PCs in ein Windows NT Netz

Diese Maßnahme ist mit Version 2006 entfallen.

# M 5.41 Sichere Konfiguration des Fernzugriffs unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 5.42 Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 5.43 Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 5.44 Einseitiger Verbindungsaufbau

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

In den meisten Fällen gibt es für ein Modem genau einen Telefonanschluss. Über diesen Telefonanschluss initiiert das Modem einerseits ausgehende Anrufe und nimmt andererseits auch die eingehenden Anrufe entgegen. Damit kein Angreifer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann, sollte hier zumindest ein Callback-Mechanismus eingesetzt werden (siehe auch M 5.30 *Aktivierung einer vorhandenen Callback-Option*).

Trotz eines aktivierten Callback kann das Problem bestehen, dass eine kommende Verbindung nicht ausgelöst wird, solange der Anrufer nicht auflegt. Die öffentliche Vermittlungsstelle löst eine solche Verbindung erst nach einem gewissen Zeitraum aus. Dies Problem tritt in erster Linie dann auf, wenn keine TK-Anlage die Verbindung zusätzlich auslöst.

Damit kann ein Angreifer einen Callback initiieren, aber gleichzeitig die Leitung belegt halten, so dass das Modem zwar korrekt die gespeicherte Rufnummer für den Callback anwählt, aber nach wie vor mit dem Angreifer verbunden bleibt.

Um dies zu verhindern, sollte zunächst überprüft werden, ob eine kommende Verbindung auch dann getrennt wird, wenn der Anrufer nicht auflegt. Ist dies nicht der Fall und kann es außerdem nicht gewährleistet werden, dass alle Modem-Verbindung durch einen Betreuer überwacht werden, sollte überlegt werden, mit getrennten Telefonanschlüssen mit einseitigem Verbindungsaufbau zu arbeiten, d. h. mit einem Anschluss für gehende und einem für kommende Verbindungen. Dies erfordert für jeden Anschluss ein eigenes Modem und die Durchführung des Callback über die Applikation. Dabei ist darauf zu achten, dass das Modem für gehende Verbindungen keine Anrufe automatisch entgegennimmt (*S0=0*, d. h. kein Auto-Answer). Damit vom Modem für kommende Verbindungen keine Verbindungen nach außen aufgebaut werden können, sollte der Modem-Anschluss entweder an der internen TK-Anlage für gehende Verbindungen gesperrt werden oder eine entsprechende Sperre bei der Telekom beantragt werden.

Prüffragen:

- Wird der Callback-Mechanismus des Modems zur Verhinderung unbemerkter Zugriffe von außen eingesetzt?
- Ist sichergestellt, dass das Modem eine kommende Verbindung auch dann trennt, wenn der Anrufer nicht auflegt?

# M 5.45 Sichere Nutzung von Browsern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Browser sind Programme zum Betrachten von Webseiten. Sie werden nicht nur auf Arbeitsplatzrechnern eingesetzt, sondern auch auf mobilen Endgeräten wie PDAs und Mobiltelefonen. Browser können unabhängig vom Betriebssystem, aber teilweise nur mit Hilfe von Plug-Ins bzw. Add-Ons, eine Vielzahl unterschiedlicher Medienformate anzeigen und abspielen. Sie können durch unsachgemäße Handhabung, durch eine unzureichende Konfiguration oder durch Programmierfehler Sicherheitsprobleme verursachen.

Eine Gefährdung der lokalen Daten geht beispielsweise von Programmen aus, die aus dem Internet geladen und ohne Nachfrage auf dem Endgerät ausgeführt werden (z. B. ActiveX-Programme, Java-Applets oder Ähnliches). Auch innerhalb von Dokumenten, Bildern oder Animationen können Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und zu Schäden führen können.

Die Vielzahl der Funktionen bringt komplexe Konfigurationsmöglichkeiten und potentielle Sicherheitsprobleme mit sich. Um solche Probleme zu vermeiden, sollten die im Folgenden beschriebenen Maßnahmen umgesetzt werden.

### Grundfunktionen

Die Standardeinstellungen der meisten Browser sind häufig unsicher. Daher sollten als erstes die Sicherheitseinstellungen an die Erfordernisse der Institution angepasst werden.

### Aufruf externer Dateien

Beim Aufrufen externer Dateien und/oder Programme kann eine Vielzahl von Sicherheitsproblemen auftreten, wie z. B. das Ausführen von Schadsoftware. Die Benutzer dürfen sich bei der Internet-Nutzung nie darauf verlassen, dass die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen. Für Benutzer ist es nur schwer einzuschätzen, ob Internet-Inhalte vertrauenswürdig sind und nicht manipuliert wurden.

Bei der Konfiguration des Browsers ist darauf zu achten, dass beim Herunterladen von Dateien die zugehörigen Anwendungen nicht automatisch gestartet werden, da die Dateien Schadsoftware enthalten könnten (siehe dazu auch M 4.3 *Einsatz von Viren-Schutzprogrammen*). Die entsprechenden Dateien sollten stattdessen zunächst gespeichert, auf Schadprogramme untersucht und erst dann gestartet werden. Eine Alternative ist die Nutzung von Viewern, die beispielsweise bei der Anzeige von Office-Dateien die Ausführung von Makros nicht unterstützen.

Alle Benutzer müssen darauf hingewiesen werden, dass sie selbst dafür verantwortlich sind, beim Aufruf oder Herunterladen von Dateien alle festgelegten Vorsichtsmaßnahmen zu ergreifen. Trotz aller Sicherheitsmaßnahmen in einer Institution bleiben Restrisiken.

### Plug-Ins und Zusatzprogramme

Es gibt Dateiformate, die von Browsern nicht direkt verarbeitet werden können. Für den Aufruf dieser Formate werden zusätzliche Programme benötigt, die häufig von Drittanbietern zur Verfügung gestellt und als so genannte *Plug-Ins*

oder *Add-Ons* in den Browser integriert werden. Die Anzeige der betreffenden Datei erfolgt dann nicht in einem eigenen Anwendungsfenster, sondern direkt im Browser. Zu den weit verbreiteten Plug-Ins bzw. Add-Ons gehören Flash Player oder Java.

Zusatzprogramme, wie beispielsweise Viewer, sind eigenständige Programme, die in der Lage sind, bestimmte Dateiformate zu verarbeiten. Der Aufruf eines solchen Zusatzprogramms wird über eine Konfigurationsdatei des Browsers gesteuert, in der Dateityp und Programm verknüpft sind.

Bei der Installation von Programmen müssen die institutionsinternen Sicherheitsregeln beachtet werden. Insbesondere dürfen nur getestete und zugelassene Programme installiert werden. Vor der Installation für den Wirkbetrieb sollten auf Stand-alone-Rechnern Tests der Programme durchgeführt werden. Die Berechtigung zum Installieren von Software sollte auf die Administratoren beschränkt werden (siehe dazu auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen* und M 4.65 *Test neuer Hard- und Software*). Zudem sollten nur Plug-Ins, Add-Ons oder Zusatzprogramme installiert werden, die unbedingt benötigt werden, da jedes hinzugefügtes Programm auch ein potentielles Sicherheitsrisiko darstellt.

**Aktive Inhalte**

Die meisten Sicherheitsprobleme bei der Internet-Nutzung tauchen im Zusammenhang mit aktiven Inhalten wie JavaScript, ActiveX, Flash oder Java, aber auch im Zusammenhang mit anderen Plug-Ins und Add-Ons auf. Aktive Inhalte werden über den Browser auf dem Client ausgeführt anstatt auf dem Server. Dies kann zu Sicherheitsproblemen auf dem Client führen. Um ein internes Netz vor Missbrauch durch aktive Inhalte aus dem Internet zu schützen, sollte soweit wie möglich auf deren Ausführung verzichtet werden (siehe dazu M 5.69 *Schutz vor aktiven Inhalten*).

**Verschlüsselung**

Das Übertragungsprotokoll HTTP (*Hypertext Transfer Protocol*) überträgt alle Informationen im Klartext. Daher ist die Vertraulichkeit der übertragenen Informationen nicht gewährleistet. Auch wenn ein Webangebot passwortgeschützt ist, heißt das nicht automatisch, dass die Authentisierungsdaten verschlüsselt übertragen werden.

Falls bei einem Webangebot die Angabe sensitiver Informationen (etwa der Kreditkartennummer oder Bankverbindung, aber auch nur personenbezogener Daten) erforderlich ist, sollte daher auf eine mit Hilfe des HTTPS-Protokolls verschlüsselte Verbindung geachtet werden (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*).

**Nutzung vorhandener Sicherheitsfunktionalitäten**

Die vorhandenen Sicherheitsfunktionalitäten der Browser (insbesondere die Rückfrage vor dem Ausführen von Programmen) sollten auf jeden Fall genutzt werden. Um die Angriffs- und Missbrauchsmöglichkeiten bei Browsern zu minimieren, sollten grundsätzlich nur die Funktionen aktiviert werden, die zur Erledigung der entsprechenden Aufgaben benötigt werden.

Ein Teil der oben beschriebenen Maßnahmen liegt im Verantwortungsbereich der Benutzer, da deren Umsetzung, wie beispielsweise die Aktivierung bestimmter Optionen, nicht ständig durch die Systemadministration überprüft werden kann. Wenn möglich, sollten jedoch administrationsseitig Maßnahmen ergriffen werden, die die Veränderung bestimmter Einstellungen durch Benut-

zer erschweren oder ganz unterbinden. Beispielsweise können bei einigen Produkten bestimmte Konfigurationsdateien schreibgeschützt werden.

In jedem Fall muss aber die Systemadministration durch die Vorgabe sicherer Grundeinstellungen dafür sorgen, dass ohne Benutzereingriff ein größtmögliches Maß an Sicherheit erzielt wird.

**Informationsbeschaffung über Sicherheitslücken**

Da immer wieder neue Sicherheitslücken in Browsern bekannt werden, ist eine regelmäßige Informationsbeschaffung über solche Sicherheitslücken und deren Beseitigung erforderlich. Hierbei braucht nicht unbedingt die Beschaffung der aktuellsten Version des Produkts im Vordergrund zu stehen, da durch neue Programmteile auch neue Sicherheitsprobleme auftreten können. In jedem Fall sollte jedoch durch das Einspielen von Patches sichergestellt werden, dass bekannte Sicherheitslücken beseitigt werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Dabei darf nicht vergessen werden, dass auch für Plug-Ins bzw. Add-ons immer wieder Patches erscheinen. Diese müssen ebenfalls zeitnah eingespielt werden.

Wenn mit Hilfe des Browsers wichtige Anwendungen des Unternehmens bzw. der Behörde bedient werden oder wenn ein erhöhter Schutzbedarf in Bezug auf Verfügbarkeit vorliegt, sollten die Patches auf jeden Fall vorher auf einem Testsystem getestet werden. Dabei sollte geprüft werden, ob keine unerwünschten Seiteneffekte auftreten, die den sicheren und reibungslosen Betrieb stören.

Prüffragen:

- Existiert eine Internet-Sicherheitsrichtlinie?
- Ist dokumentiert, welcher Browser und gegebenenfalls Plug-Ins eingesetzt werden und wie diese zu konfigurieren sind?
- Ist der Browser so konfiguriert, dass potentiell gefährliche Dateitypen nicht direkt ausgeführt, sondern allenfalls lokal gespeichert werden?
- Werden Datenschutzaspekte bei der Konfiguration des Browsers berücksichtigt?
- Sind die Benutzer im Umgang mit WWW-Browsern geschult und sensibilisiert worden?
- Sind Maßnahmen getroffen, um eigenmächtiges Installieren von Software und Plug-Ins zu verhindern?
- Wurden Regelungen zur privaten Internetnutzung getroffen?

# M 5.46 Einsatz von Stand-alone-Systemen zur Nutzung des Internets

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN entstehen, zu verringern, ist es sinnvoll Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu einem LAN haben.

Hierfür bieten die verschiedenen Betriebssysteme unterschiedliche Möglichkeiten mit jeweils spezifischen Gefährdungen für die Vertraulichkeit und Integrität der Daten auf diesem Rechner.

Detailliertere Beschreibungen, wie Stand-alone-Systeme sicher zur Nutzung des Internets eingesetzt werden können, finden sich im Baustein B 3.208 *Internet-PC*.

Prüffragen:

- Werden Rechner eingesetzt, die ausschließlich über einen Internetzugriff verfügen und keine Anbindungen zu anderen oder vertrauenswürdigen internen Netzwerken besitzen?

# M 5.47 Einrichten einer Closed User Group

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Das Integrated Services Digital Network (ISDN) ermöglicht die Einrichtung einer geschlossenen Benutzergruppe (GBG), auch als Closed User Group (CUG) bezeichnet. Merkmal einer solchen Gruppe ist, dass alle Teilnehmer einer CUG untereinander über das öffentliche ISDN kommunizieren können, Verbindungswünsche von außerhalb der CUG an CUG-Teilnehmer jedoch genauso abgewiesen werden wie Verbindungswünsche von CUG-Teilnehmer an Teilnehmer des öffentlichen ISDN.

**Funktionsweise**

Alle Kommunikationspartner sind Mitglied in einer Closed User Group des Netzbetreibers (z. B. Deutsche Telekom AG). Die Berechtigungsprüfung zur Kommunikation erfolgt über den einer CUG eindeutig zugeordneten Interlock Code durch die jeweilige digitale Vermittlungsstelle (DIV) der Kommunikationspartner. Zu Beginn übermittelt der rufende Kommunikationspartner eine Verbindungsanforderung an die ihm zugeordnete DIV. Die DIV fügt der Verbindungsanforderung nicht nur die ISDN-Rufnummer des rufenden Kommunikationspartners, sondern auch den eindeutigen Interlock Code der entsprechenden Closed User Group hinzu. Die DIV des gerufenen Kommunikationspartners erkennt anhand des Interlock Codes, ob der Verbindungsanforderung stattgegeben werden kann. Ist die Identifikation erfolgreich, wird der Verbindungswunsch an den gerufenen Kommunikationspartner weiter vermittelt.

Vorteilhaft an der beschriebenen Funktionalität ist, dass unerlaubte Zugriffsversuche bereits von der DIV des Netzbetreibers abgewiesen werden und nicht bis zu Netzkoppelelementen eines Kommunikationspartners gelangen.

Nachteilig ist, dass Änderungen der Mitgliedschaft in einer CUG immer dem Netzbetreiber mitgeteilt werden müssen, da nur dieser die notwendigen Berechtigungsänderungen durchführen kann. Weiterhin bedeutet dies auch, dass der Netzbetreiber die vollständige Kontrolle über die Mitgliedschaft in einer CUG besitzt und von ihm vorgenommene Änderungen durch den Nutzer einer CUG nicht kontrolliert werden können. Hingewiesen werden soll ebenfalls darauf, dass sowohl für das Einrichten als auch für den Betrieb einer CUG durch einen Netzbetreiber einmalige und fortlaufende Kosten entstehen.

Das Einrichten einer Closed User Group durch den Betreiber eines öffentlichen Netzes empfiehlt sich immer dann, wenn

- Hard- und Software für andere Verfahren (z. B. M 5.48 *Authentisierung mittels CLIP/COLP*) erst beschafft werden müsste,
- die Mitglieder einer CUG nur selten wechseln und
- der Netzbetreiber ausreichend vertrauenswürdig ist.

Prüffragen:

- Wurden Sicherheitsanforderungen für den Betrieb und die Nutzung von Closed User Groups festgelegt?

# M 5.48 Authentisierung mittels CLIP/ COLP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Das Integrated Services Digital Network (ISDN) liefert die Möglichkeit, Rufnummern von Teilnehmern nicht nur für die öffentlichen Vermittlungskomponenten, sondern auch direkt für die beteiligten Kommunikationspartner zu signalisieren. Diese ISDN-Leistungsmerkmale bezeichnet man als

- CLIP = **C**alling **L**ine **I**dentification **P**resentation und
- COLP = **Co**nnected **L**ine Identification **P**resentation oder allgemeiner als
- Rufnummernanzeige.

Die Auswertung der Rufnummernangabe kann von den jeweiligen Kommunikationspartnern zur Authentisierung genutzt werden.

**Funktionsweise**

In einem ersten Schritt wird seitens des rufenden Kommunikationspartners eine Verbindungsanforderung an die ihm zugeordnete digitale Vermittlungsstelle (DIV) abgesetzt. Die DIV vermittelt die Verbindungsanforderung an den zu rufenden Kommunikationspartner innerhalb des ISDN incl. der Rufnummer des rufenden Kommunikationspartners. Die gegenüberliegende DIV vermittelt anschließend den Verbindungswunsch an die ISDN-Kommunikationseinrichtung des gewünschten Kommunikationspartners. Anhand der übermittelten Rufnummer kann diese Kommunikationseinrichtung (z. B. ein ISDN-Router oder eine TK-Anlage) den rufenden Kommunikationspartner identifizieren (CLIP). Bei erfolgreicher Identifikation wird der Verbindungswunsch angenommen und der Datenaustausch kann beginnen.

Vorteilhaft an der beschriebenen Funktionalität ist, dass die Identifikation durch Komponenten der jeweiligen Kommunikationspartner (ISDN-Router, TK-Anlage) durchgeführt wird und somit vollständig in deren Kontrollbereich liegt.

Nachteilig ist, dass die über den ISDN-D-Kanal übertragenen Rufnummern grundsätzlich manipulierbar sind (siehe G 5.63 *Manipulationen über den ISDN-D-Kanal*). Eine einfache Authentisierung durch die übermittelte Rufnummer ist somit entweder nur in Zusammenhang mit dem Einsatz einer Callback-Funktion (siehe M 5.49 *Callback basierend auf CLIP/COLP*) oder in Kombination mit dem Einsatz eines D-Kanal-Filters (siehe M 4.62 *Einsatz eines D-Kanal-Filters*), das Protokollmanipulationen aufdeckt, möglich.

Prüffragen:

- Können die eingesetzten ISDN-Komponenten die Leistungsmerkmale CLIP und COLP verarbeiten?

# M 5.49 Callback basierend auf CLIP/ COLP

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Viele Kommunikationskarten bieten die Option automatischer Rückruf (Callback). Ist diese Option aktiviert, trennt die Kommunikationskarte, wenn sie einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Verbindung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, dass ein nicht autorisierter Anrufer diesen Fernzugang missbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Mit Hilfe des ISDN ist eine Variante des Callback zu einer festen Rufnummer möglich: Die angesprochene ISDN-Karte prüft mit Hilfe des ISDN-Leistungsmerkmals Calling Line Identification Presentation (CLIP), von welcher Stelle aus die Verbindungsanforderung erfolgte, und vergleicht die übermittelte Rufnummer mit einer Rufnummerntabelle. Wurde über CLIP eine gültige Rufnummer übermittelt, wird die in der Rufnummerntabelle hinterlegte Rufnummer zurückgerufen.

Vorteilhaft ist gegenüber der ausschließlichen Authentisierung über CLIP/ COLP (siehe M 5.48 *Authentisierung mittels CLIP/COLP*), dass selbst beim Vorspiegeln einer autorisierten Rufnummer von einem nicht autorisierten Teilnehmer aus keine Verbindung zustande kommt, da der nicht autorisierte Teilnehmer tatsächlich ja nicht unter der vorgegebenen Rückrufnummer erreichbar ist.

Prüffragen:

- Wird Callback immer dann eingesetzt, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll?
- Werden die in der Rufnummerntabelle hinterlegten Rufnummern regelmäßig auf ihre Aktualität und ihren Bedarf überprüft?

# M 5.50 Authentisierung mittels PAP/ CHAP

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Viele ISDN-Karten unterstützen die Kommunikation über das Point-to-Point Protocol (RFC 1661), nachdem eine ISDN-Wählverbindung aufgebaut wurde. Innerhalb dieses Internet-Standards werden auch Authentisierungsprotokolle, wie das Password Authentication Protocol (PAP) und das Challenge Handshake Authentication Protocol (CHAP) angeboten (RFC 1994). Bietet die verwendete ISDN-Karte diese Funktionalitäten, sollte zur Authentisierung anstelle des Password Authentication Protocols das Challenge-Handshake Authentication Protocol genutzt werden, da bei PAP das zur Authentisierung verwendete Passwort unverschlüsselt übertragen wird.

Die bei PAP bzw. CHAP verwendeten Passwörter werden im Allgemeinen nicht bei jeder Authentisierung vom Benutzer erneut eingegeben, sondern in den IT-Systemen gespeichert. Damit sich diese Verfahren auch nach einer erneuten Installation wieder aufsetzen lassen, sollten die benötigten Passwörter notiert und sicher verwahrt werden (siehe M 2.22 *Hinterlegen des Passwortes*).

**Funktionsweise**

Bei CHAP werden grundsätzlich zwei Kommunikationspartner unterschieden: Authenticator und Peer. Dabei handelt es sich beim Authenticator um den Kommunikationspartner, der die Authentisierung abfordert, und beim Peer um den Kommunikationspartner, der die Authentisierung erbringen soll. Im Allgemeinen wird also der Authenticator der Server sein, an dem sich der Benutzer von seinem IT-System aus als Peer anmelden will.

Bei CHAP wird auf beiden Seiten die Kenntnis eines gemeinsamen Geheimnisses (Passwort) überprüft. Dabei wird das Geheimnis nicht im Klartext über die Leitung gesandt und durch die Einbindung von Zufallszahlen vor Wiedereinspielen geschützt.

Das eingesetzte Challenge-Response-Protokoll läuft wie folgt ab:

In einem ersten Schritt errechnet der Authenticator eine Zufallszahl. Mittels eines Hash-Algorithmus wird der Hashwert der eben berechneten Zufallszahl gebildet. Eine Hashfunktion ist eine Rechenvorschrift, durch die eine Eingabe beliebiger Länge in einen Ausgabewert fester (im Allgemeinen kürzerer) Länge umgewandelt wird. Eine Einweg-Hashfunktion funktioniert nur in eine Richtung, d. h. aus der Eingabe lässt sich problemlos der Hashwert berechnen, aber es sollte sehr schwer bis unmöglich sein, zu einem Hashwert passende Eingabedaten zu berechnen.

Im nächsten Schritt überträgt der Authenticator das so genannte Challenge, also die eben errechnete Zufallszahl, an den Peer. Da Authenticator und Peer über den gleichen Hash-Algorithmus verfügen, kann in einem vierten Schritt ebenfalls der Peer den Hashwert der eben übermittelten Zufallszahl bilden. Der Peer berechnet den Hashwert über die drei Werte Identifier (Benutzer-Kennung), Secret (Passwort) und der gesendeten Zufallszahl. Den Hashwert überträgt er dann als Antwort an den Authenticator. Der Authenticator überprüft die Korrektheit des Passworts, indem er ebenfalls den entsprechenden Hashwert berechnet und mit dem übermittelten Hashwert vergleicht. Fällt

der Vergleich positiv aus, hat sich der Peer gegenüber dem Authenticator authentisiert und die Kommunikationsverbindung kann aufgebaut werden.

Die Authentisierung nach dem eben beschriebenen Verfahren sollte auch während einer bestehenden Kommunikationsverbindung mehrfach wiederholt werden, um auch Attacken auf bereits bestehende Verbindungen zu verhindern. Dies wird, ohne das der Benutzer eingreifen muss, in zufälligen Zeitabständen durch den Authenticator angestoßen.

Prüffragen:

- Sofern die eingesetzte ISDN-Karte PAP/CHAP unterstützt: Wird CHAP zur Authentisierung genutzt und auf PAP verzichtet?
- Werden die für PAP beziehungsweise CHAP verwendeten Passwörter sicher hinterlegt?

# M 5.51 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Telearbeiter

Erfolgt im Rahmen der Telearbeit eine Datenübertragung zwischen einem Telearbeitsrechner und dem Kommunikationsrechner der Institution, werden dabei dienstliche Informationen üblicherweise über öffentliche Kommunikationsnetze übertragen. Da weder die Institution noch die Telearbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit in einem öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen erforderlich.

Generell muss die Datenübertragung zwischen Telearbeitsrechner und Institution folgende Sicherheitsanforderungen erfüllen:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten*: Es muss durch eine ausreichend sichere Verschlüsselung erreicht werden, dass auch durch Abhören der Kommunikation zwischen Telearbeitsrechner und Kommunikationsrechner der Institution kein Rückschluss auf den Inhalt der Daten möglich ist. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten*: Die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben. Um absichtliche Manipulationen während der Datenübertragung detektieren zu können, sollten die Daten signiert und/oder verschlüsselt werden.
- *Sicherstellung der Verfügbarkeit der Datenübertragung*: Falls zeitliche Verzögerungen bei der Telearbeit nur schwer zu tolerieren sind, sollte ein redundant ausgelegtes öffentliches Kommunikationsnetz als Übertragungsweg ausgewählt werden, so dass ein Ausfall einzelner Verbindungsstrecken nicht den Totalausfall der Kommunikationsmöglichkeiten bedeutet. Auf eine redundante Einführung der Netzanbindung an den Telearbeitsrechner und die Schnittstelle der Institution kann gegebenenfalls verzichtet werden.
- *Sicherstellung der Authentizität der Daten*: Bei der Übertragung von Daten zwischen Telearbeitsrechner und Institution muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, so dass eine Maskerade ausgeschlossen werden kann. Dies bedeutet, dass Daten mit Absender "Telearbeitsrechner" auch tatsächlich von dort stammen. Ebenso muss der Ursprung von Institutionsdaten zweifelsfrei auf die Institution zurückgeführt werden können.
- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung*: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann an wen übertragen wurden.
- *Sicherstellung des Datenempfangs*: Ist es für die Telearbeit von Bedeutung, ob Daten korrekt empfangen wurden, können Quittungsmechanismen eingesetzt werden, aus denen hervorgeht, ob der Empfänger die Daten korrekt empfangen hat.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten.

Prüffragen:

- Erfüllen die eingesetzten Kommunikationsprotokolle und Sicherheitsmechanismen die Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution?
- Ist die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten zwischen Telearbeitsrechner und Institution sowie die die Authentizität der Kommunikationspartner gewährleistet?

# M 5.52 Sicherheitstechnische Anforderungen an den Kommunikationsrechner

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Je nach Art der Telearbeit und der dabei durchzuführenden Aufgaben gestaltet sich der Zugriff eines Telearbeiters auf Institutionsdaten anders. Denkbar ist es, dass zwischen Telearbeiter und Institution nur E-Mails ausgetauscht werden. Andererseits kann auch ein Zugriff auf Server in der Institution für den Telearbeiter notwendig sein. Unabhängig von den Zugriffsweisen muss der Kommunikationsrechner der Institution dennoch im Allgemeinen folgende Sicherheitsanforderungen erfüllen:

- *Identifikation und Authentisierung*: Sämtliche Benutzer des Kommunikationsrechners, also Administratoren, Mitarbeiter in der Institution und Telearbeiter, müssen sich vor einem Zugriff auf den Rechner identifizieren und authentisieren. Nach mehrfachen Fehlversuchen ist der Zugang zu sperren. Voreingestellte Passwörter sind zu ändern.
  Gegebenenfalls muss es für den Kommunikationsrechner auch möglich sein, während der Datenübertragung eine erneute Authentisierung des Telearbeiters oder des Telearbeitsrechners anzustoßen, um aufgeschaltete Angreifer abzuwehren.
  Im Rahmen der Identifikation und Authentisierung der Benutzer sollte auch zusätzlich eine Identifizierung der Telearbeitsrechner stattfinden (zum Beispiel über Rufnummern und Callback-Verfahren).
  Es ist zu überlegen, für die Absicherung der Zugriffe bei der Telearbeit nur starke Authentisierungsverfahren einzusetzen. Hierfür könnten beispielsweise Chipkarten, sogenannte Token oder auch biometrische Verfahren eingesetzt werden.
- *Rollentrennung*: Die Rollen von Administratoren und Benutzern des Kommunikationsrechners sind zu trennen. Eine Rechtevergabe darf ausschließlich Administratoren möglich sein.
- *Rechteverwaltung und -kontrolle*: Der Zugriff auf Dateien des Kommunikationsrechners darf nur im Rahmen der gebilligten Rechte erfolgen können. Darüber hinaus muss insbesondere der Zugang zu angeschlossenen Rechnern in der Institution und darauf gespeicherten Dateien reglementiert sein. Zugangs- und Zugriffsmöglichkeiten sind auf das notwendige Mindestmaß zu beschränken.
  Bei Systemabsturz oder bei Unregelmäßigkeiten muss der Kommunikationsrechner in einen sicheren Zustand übergehen, indem gegebenenfalls kein Zugriff mehr möglich ist.
- *Minimalität der Dienste*: Dienste, die durch den Kommunikationsrechner zur Verfügung gestellt werden, müssen dem Minimalitätsprinzip unterliegen: alles ist verboten, was nicht ausdrücklich erlaubt wird. Die Dienste selbst sind auf den Umfang zu beschränken, der für die Aufgaben der Telearbeiter notwendig ist.
- *Protokollierung*: Datenübertragungen vom, zum und über den Kommunikationsrechner sind mit Uhrzeit, Benutzer, Adressen und Dienst zu protokollieren.
  Den Administratoren bzw. Revisoren sollten Werkzeuge zur Verfügung stehen, um die Protokolldaten auszuwerten. Dabei sollten Auffälligkeiten automatisch gemeldet werden.
- *Automatische Computer-Viren-Prüfung*: Übertragene Daten sind einer automatischen Prüfung auf Computer-Viren zu unterziehen.

- *Verschlüsselung*: Daten, die auf dem Kommunikationsrechner für die Telearbeiter vorgehalten werden, sind bei einem entsprechender Schutzbedarf bezüglich der Vertraulichkeit (in Abstimmung mit der organisationsweiten Informationssicherheitsrichtlinie) zu verschlüsseln. Generell sollte die Kommunikation zwischen Telearbeitsrechner und Kommunikationsrechner verschlüsselt werden.
- *Vermeidung oder Absicherung von Fernadministration*: Benötigt der Kommunikationsrechner keine Fernadministration, so sind sämtliche Funktionalitäten zur Fernadministration zu sperren. Da in der Regel aber die Fernadministration benötigt wird, muss sie ausreichend abgesichert werden (z. B. über einen VPN-Tunnel oder durch eine dedizierte Verbindung). Jegliche Fernadministration darf nur nach vorhergehender erfolgreicher Identifikation und Authentisierung stattfinden. Es sollte überlegt werden, die Tätigkeiten während der Fernadministration zu protokollieren. Administrationszugangsdaten und Konfigurationsdaten dürfen nur verschlüsselt übertragen werden. Voreingestellte Passwörter und kryptographische Schlüssel sind zu ändern.

Prüffragen:

- Ist der Kommunikationsrechner entsprechend den Sicherheitsanforderungen konfiguriert?
- Müssen sich sämtliche Benutzer des Kommunikationsrechners vor einem Zugriff auf den Rechner identifizieren und authentisieren?
- Sind die Zugangs- und Zugriffsmöglichkeiten auf den Kommunikationsrechner auf das notwendige Mindestmaß beschränkt?

# M 5.53 Schutz vor Mailbomben

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.54 Umgang mit unerwünschten E-Mails

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Unerwünschte E-Mails, welche auch unter dem Begriff "Spam" bekannt sind, werden in Massen verschickt, belästigen die Empfänger und stören den laufenden Betrieb der IT-Infrastruktur, angefangen bei den E-Mail-übertragenden Systemen bis zu den Clients der Benutzer. Zu den unerwünschten E-Mails gehören Kettenbriefe, unerwünschte Werbung, Bettelbriefe, Junkmails, Phishing-E-Mails und E-Mails mit Schadcode im Anhang. Gefährlich wird es insbesondere dann, wenn E-Mail-Anhänge ausgeführt werden, die E-Mail HTML-basiert ist oder die Mail-Empfänger über Links in der E-Mail auf manipulierte Webseiten gelockt werden sollen.

Durch die Überhäufung mit unerwünschten E-Mails oder durch absichtliche Überlastung durch eingehende E-Mails kann nicht nur das E-Mail-System blockiert werden, sondern es kann auch für den Empfänger solcher E-Mails teuer werden. Kosten entstehen unter anderem durch Übertragungsgebühren, insbesondere dann, wenn Bilder oder Multimediadateien in den unerwünschten E-Mails enthalten sind. Dazu kommt auch noch Kosten für die Filterung der E-Mails und/oder die Arbeitszeit der Mitarbeiter, die benötigt wird, um die eingegangene Spam-Mails zu sichten und zu löschen.

Um sich vor unerwünschten E-Mails zu schützen, sollte jeder Benutzer die Weitergabe seiner E-Mail-Adresse auf das Nötigste einschränken. Besonders vorsichtig sollten Benutzer mit der Herausgabe der Adresse beispielsweise in Newsgroups oder Mailinglisten, bei Gewinnspielen, bei Umfragen oder in ähnlichen Formularen sein. In diesen Fällen sollte die Einrichtung einer Wegwerfadresse in Betracht gezogen werden, um eine möglicherweise personalisierte "Hauptadresse" nicht unnötig in fremde Hände zu geben.

Umgekehrt sollte auch darauf geachtet werden, die E-Mail-Adressen von Kommunikationspartnern nicht ungeprüft weiterzugeben. Besonders wenn mehrere Personen gleichzeitig mit einer E-Mail angeschrieben werden, sollte nicht jeder wissen, wer noch unter welcher E-Mail-Adresse angeschrieben worden ist. Um dies zu vermeiden, kann z. B. die Funktion "BCC" (*Blind Carbon Copy*) genutzt werden, die praktisch jeder E-Mail-Client bietet.

Auch sollte der eigene Rechner stets frei von Schadsoftware bleiben, da es Schadsoftware gibt, die die lokalen Adressbücher auslesen und auf Spamverteilerlisten setzen.

Grundsätzlich sollten alle Benutzer Spam ignorieren und löschen. Keinesfalls darf geantwortet, Links in der E-Mail gefolgt oder Anhänge ausgeführt werden, da dies negative Auswirkungen haben kann. Eine Bestätigung über die erfolgreiche Zustellung der E-Mail ist gleichzeitig eine Bestätigung, dass die E-Mail-Adresse für die Zustellung von Spam benutzbar ist und dass der Empfänger diese E-Mails auch liest. Zusätzlich existiert das Risiko, dass Rechner mit Schadsoftware infiziert und somit Bestandteil eines Botnetzes werden. Darüber sollten auch alle Mitarbeiter informiert werden.

Mögliche Maßnahmen gegen unerwünschte E-Mails sind die folgenden:

- Um Spam zu vermeiden oder wenigstens für die Empfänger erkennbar zu machen, ist es notwendig, unerwünschte E-Mails maschinell und auto-

matisch zu erkennen und abzuweisen bzw. zu markieren. Dazu muss ein entsprechendes E-Mail-Filtersysteme betrieben werden (mehr dazu ist in Maßnahme M 5.109 *Einsatz eines E-Mail-Scanners auf dem Mailserver* beschrieben).

- Unerwünschte E-Mails enthalten außerdem häufig Anhänge, die ungeahnte Nebeneffekte auslösen können, oder Dateiformate, die als potentiell problematisch eingeschätzt werden. Alle Betroffenen sollten sich der Problematik bewusst sein und entsprechende Vorkehrungen treffen (siehe M 4.199 *Vermeidung problematischer Dateiformate*).
- Die meisten E-Mail-Clients können so konfiguriert werden, dass sie als unerwünscht markierte E-Mails in separate Ordner verschieben. Entsprechende Filterregeln können durch die Benutzer bzw. die Administratoren eingerichtet werden. Die Benutzer sollten hierüber informiert werden.
- Einige E-Mail-Clients besitzen auch eigene Erkennungsmechanismen gegen unerwünschte E-Mails. Diese können die Benutzer aktivieren, um ihre Posteingänge entsprechend zu klassifizieren.
- Jede Institution sollte festlegen, ob ihre Mitarbeiter Artikel in Newsgruppen posten dürfen und wenn ja, in welcher Form und zu welchen Themen. Dabei sind die Benutzer darauf hinzuweisen, dass die Netiquette zu beachten ist, insbesondere ist die Verbreitung von für die Allgemeinheit irrelevanten Informationen zu unterlassen.
- Es kann unter Umständen sinnvoll sein, keine leicht erratbaren E-Mailadressen zu verwenden (siehe auch M 2.122 *Einheitliche E-Mail-Adressen*).
  Wenn die Angabe einer Adresse für Mailinglisten, Abfragen oder ähnliches erforderlich ist, besteht eine andere Möglichkeit darin, eine spezielle E-Mail-Adresse dafür einzurichten. E-Mail an diese Adresse kann dann gefiltert, ignoriert oder gelöscht werden. Falls hierzu keine Absenderadressen aus der eigenen Domain gewählt werden sollen, kommen hierfür auch die Anbieter von kostenlosen E-Mail-Accounts in Betracht.
- Auf keinen Fall sollte versucht werden, Spam-Verursacher durch Mailbomben oder ähnliches zu bestrafen. Spam sollte nicht einmal durch ein Reply beantwortet werden. Häufig sind die Absenderangaben in Spam-Mails gefälscht. Antworten erreichen dann nur Unschuldige oder kommen als unzustellbar zurück. Auf jeden Fall verursachen auch Antworten wiederum ein erhöhtes Netzaufkommen und im schlimmsten Fall bestätigen sie Werbemailern sogar noch die Korrektheit angeschriebener E-Mail-Adressen.
- Auch wenn in der unerwünschten E-Mail die Möglichkeit angeboten wird, sich für weitere E-Mails streichen zu lassen, sollte auf keinen Fall auf solche E-Mails reagiert werden. Anderenfalls kann der Spammer die Antwort als Bestätigung nutzen, dass die angeschriebene E-Mail-Adresse korrekt ist.
- Eine weitere Maßnahme gegen akute Belästigung durch Spam ist die Benachrichtigung des eigenen Mailproviders sowie des Mailproviders des Verursachers, damit diese gegen den Verursacher vorgehen können. Allerdings sollte dabei berücksichtigt werden, dass nicht alle Mailprovider zeitnah auf solche Beschwerden reagieren.

Dabei ist zu beachten, dass nicht alle dieser Maßnahmen in allen Umgebungen sinnvoll sind, weil sie diverse Einschränkungen mit sich bringen. So kann es einerseits sinnvoll sein, nicht aus den Benutzernamen abgeleitete E-Mailadressen zu verwenden, um sich vor unerwünschten Werbemails zu schützen. Andererseits können abstrakte E-Mailadressen die Kommunikation mit Externen erschweren, da sie schwerer zu merken sind. Die Form der E-Mailadressen muss auf jeden Fall den organisationsinternen Regelungen genügen.

Durch die Eintragung auf Mailinglisten kann ebenfalls eine hohe Mailbelastung entstehen. Generell sollte regelmäßig überprüft werden, ob die in einer Mailingliste diskutierten Inhalte das Lesen lohnen, sonst ist sie abzubestellen. Die Benutzer müssen darüber informiert sein, dass nach der Eintragung auf Mailinglisten die dadurch entstehende Mailbelastung regelmäßig, d. h. möglichst täglich, zu kontrollieren ist. In größeren Institutionen sollten für die Arbeit interessante Mailinglisten nur über einen Mitarbeiter (z. B. den Mail-Administrator) abonniert werden und dann zentral allen zur Verfügung gestellt werden.

Auch bei der Gestaltung von Webseiten sollte an Spam gedacht werden. Spammer versuchen unter anderem ihren Adresspool dadurch zu erweitern, dass sie mit Tools Webseiten automatisch darauf absuchen, ob dort E-Mail-Adressen genannt sind, z. B. für Nachfragen. Es gibt leider kaum wirksame Möglichkeiten, solche automatischen Auswerte-Tools scheitern zu lassen. Daher sollte genau überlegt werden, ob und welche E-Mail-Adressen auf Webseiten bekannt gegeben werden. Hierfür können beispielsweise aufgabenbezogene E-Mail-Adressen eingerichtet werden. Auch diese werden natürlich mit Spam belästigt werden, aber das Problem kann auf diese Weise begrenzt werden. Für die Sichtung der eingehenden Mails und die Trennung der "echten" Mail-Eingänge vom Spam sollte ausreichend Zeit vorgesehen werden.

Prüffragen:

- Sind die Benutzer über die Problematik und den Umgang mit Spam informiert und sensibilisiert?
- Werden E-Mail-Filterprogramme in Abstimmung mit dem Datenschutzbeauftragten, dem Personalrat und den Benutzern eingesetzt?
- Gibt es eine Regelung für die Verwendung von Newsgroups und Mailinglisten?
- Wird die Spam-Problematik bei der Gestaltung von Webseiten berücksichtigt?

# M 5.55 Kontrolle von Alias-Dateien und Verteilerlisten

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.56 Sicherer Betrieb eines Mailservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der sichere Betrieb eines Mailservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Der Mailserver nimmt von anderen Mailservern E-Mails entgegen und leitet sie an die angeschlossenen Benutzer oder Mailserver weiter. Weiterhin reicht der Mailserver die gesendeten E-Mails lokaler Benutzer an externe Mailserver weiter. Der Mailserver muss hierbei sicherstellen, dass lokale E-Mails der angeschlossenen Benutzer nur intern weitergeleitet werden und nicht in das öffentliche Netz gelangen können.

Ein Mailserver speichert die E-Mail bis zur Weitergabe zwischen. Viele Internet-Provider und Administratoren archivieren zusätzlich die ein- und ausgehenden E-Mails. Damit Unbefugte nicht über den Mailserver auf Nachrichteninhalte zugreifen können, muss der Mailserver gegen unbefugten Zugriff gesichert sein. Dafür sollte er gesichert (in einem Serverraum oder Serverschrank) aufgestellt sein. Für den ordnungsgemäßen Betrieb sind Administratoren und Stellvertreter zu benennen und zum Betrieb des Mailservers und dem zugrunde liegenden Betriebssystems zu schulen. Es muss ein Postmaster- und Abuse-Account eingerichtet werden (siehe auch M 2.456 *Sichere Administration von Groupware-Systemen*).

Auf die Mailboxen der lokal angeschlossenen Benutzer dürfen nur diese Zugriff haben. Auf die Bereiche, in denen E-Mails nur temporär für die Weiterleitung zwischengespeichert werden (z. B. Spooldateien), ist der Zugriff auch für die lokalen Benutzer zu unterbinden.

Es muss regelmäßig kontrolliert werden, ob die Verbindung mit den benachbarten Mailservern, insbesondere dem Mailserver des Mailproviders, noch stabil ist. Es muss regelmäßig überprüft werden, ob der für die Zwischenspeicherung der Mail zur Verfügung stehende Plattenplatz noch ausreicht, da ansonsten kein weiterer Nachrichtenaustausch möglich ist.

Umfang und Inhalt der Protokollierung der Aktivitäten des Mailservers sind festzulegen. Die Protokolldaten müssen regelmäßig ausgewertet werden, vor allem um festzustellen, ob Angriffe auf den Mailserver erfolgt sind und welche Auswirkungen diese nach sich gezogen haben.

Von der Verfügbarkeit des Mailservers sollten keine weiteren Dienste abhängig sein, beispielweise sollte der Mailserver nicht gleichzeitig auch als Fileserver dienen. Es sollte jederzeit kurzfristig möglich sein, ihn abzuschalten, z. B. bei Denial-of-Service-Angriffen oder bei Verdacht auf Manipulationen (siehe auch M 4.97 *Ein Dienst pro Server*).

Die Benutzernamen auf dem Mailserver sollten nicht aus den E-Mailadressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzer-Accounts zu erschweren.

**MX-Einträge und Relaying**

Das Internet-Namensschema DNS sieht es vor, mittels eines so genannten MX-Eintrags einen bestimmten Server als *Mailexchanger* zu kennzeichnen. Normalerweise sollten dann E-Mails zwischen Rechnern verschiedener Do-

mains nur über den jeweils "zuständigen" Mailexchanger weiter geleitet werden. Das Weiterleiten von E-Mails zwischen verschiedenen Domains wird als *Relaying* bezeichnet. Ein Mailserver sollte davor geschützt werden, als Spam-Relay verwendet zu werden. Dafür sollte der Mailserver so konfiguriert sein, dass er E-Mails nur für die eigene Organisation entgegennimmt und nur E-Mails verschickt, die von Mitarbeitern der Organisation stammen. Der Mailserver sollte eingehende E-Mails nur dann annehmen, wenn entweder die IP-Adresse des absendenden Mailservers in einem vom Administrator explizit zugelassenen IP-Netz liegt oder wenn er selbst für die Empfängeradresse als Mail-Exchanger fungiert. Alle anderen E-Mails sollten mit einer Fehlermeldung abgewiesen werden.

Berechtigte Benutzer können trotz dieser Maßnahmen weiterhin E-Mails an beliebige Empfänger versenden, ebenso können sie E-Mails von beliebigen Absendern empfangen. Durch die oben beschriebene Filterung eingehender E-Mails wird jedoch verhindert, dass der Mailserver von externen Nutzern als Spam-Relay missbraucht werden kann.

Sollten versehentlich IP-Netze, aus denen E-Mails angenommen werden sollen, nicht in obiger Liste stehen, muss der Administrator des Mailservers davon in Kenntnis gesetzt werden, damit er diese nachtragen kann.

**Non Delivery Notifications**

Grundsätzlich sind Non Delivery Notifications RFC-konform und sinnvoll, um bei temporären Fehlern an den Mailsystemen die Absender von E-Mails zu informieren, dass die E-Mails nicht zugestellt werden konnten. Die Erzeugung von Non Delivery Notifications muss sich aber auf den Fehlerfall beschränken und muss weitestgehend minimiert werden.

So ist es unbedingt zu vermeiden, dass Non Delivery Notifications aufgrund falscher Empfängeradressen erzeugt werden. Vielmehr ist dafür zu sorgen, dass E-Mails, für die die Institution nicht zuständig ist, gar nicht erst angenommen werden. Dabei ist zwingend darauf zu achten, dass ein Dienstleister, der im Vorfeld die E-Mails einer Institution überprüft, auch weiß, welche E-Mails angenommen werden müssen und welche nicht, so dass dieser nicht die Non Delivery Notifications erzeugen muss, falls die E-Mails nicht zustellbar sind. Wird dies nicht beachtet, können Spammer den Versand von Non Delivery Notifications ausnutzen, um Dritte im Namen der Institution mit Spam zu beschicken.

Um die Risiken, die durch Non Delivery Notifications entstehen, zu vermeiden, kann folgendes Vorgehen ratsam sein: Non Delivery Notifications werden grundsätzlich erlaubt. Gleichzeitig werden alle E-Mail übertragenden Systeme der Institution und die E-Mail-Systeme vorgelagerter Dienstleister (bis zu dem Server auf den der MX-Record zeigt) aufeinander abgestimmt, so dass Non Delivery Notifications nur noch in einem Fehlerfall erzeugt werden. Es dürfen unter anderem keine Non Delivery Notifications erzeugt werden, weil ein Empfänger nicht existiert, weil ein Mailsystem eine E-Mail zu groß befindet, obwohl ein vorgelagerter Mailserver diese bereits angenommen hat, oder weil ein Postfach voll ist.

Der Administrator sollte sich eine Alarmierung einrichten, die ihm mitteilt, dass ein System Non Delivery Notifications erzeugt. Er sollte dann prüfen, warum dies geschieht und den Fehler umgehend beseitigen.

**Grundsatz:** Für eine Domain muss von der ersten Annahme durch die IP-Adresse des MX-Records bis zum Postfach des Benutzers sichergestellt wer-

den, dass die E-Mails transportiert werden und nicht durch widersprüchliche Konfiguration der beteiligten Mailrelays zu Non Delivery Notifications führen.

Die Problematik der Non Delivery Notifications weist auf ein grundsätzliches Problem der E-Mail-Kommunikation hin. Der Absender einer E-Mail ist frei wählbar und kann gefälscht werden. Schickt jemand eine E-Mail mit gefälschtem Absender an ein automatisch antwortendes System, sendet dieses die Nachrichten an die gefälschten Absender-Adressen. Dies kann ein Angreifer nutzen, um einen Dritten im Namen der Institution anzugreifen und mit E-Mails zu fluten. Für dieses Angriffsszenario eignen sich nahezu alle Systeme, die E-Mails automatisch beantworten. Auch Abwesenheitsnachrichten, Eingangsbestätigungen und Weiterleitungen sind aus diesem Grund nur mit äußerster Vorsicht zu betreiben.

Folgende Maßnahmen müssen zum Schutz ergriffen werden:

- Schon als Spam klassifizierte E-Mails dürfen nicht automatisch beantwortet oder weitergeleitet werden.
- Die Absenderadresse der Antwort bzw. Weiterleitung muss eine Adresse aus dem Namensraum der Institution sein. Der Absender der eingehenden E-Mail darf nicht verwendet werden.
- Es muss verhindert werden, dass ein bestimmtes Ziel (Zieladresse oder Zieldomain) unkontrolliert mit einer großen Anzahl von E-Mails beschickt wird. Bei Abwesenheitsassistenten kann dies realisiert werden, indem einen Absender nur einmalig eine Abwesenheitsbenachrichtigung geschickt wird.

Naturgemäß muss der Mailserver aus dem Internet erreichbar sein. Daher sollte der Server durch entsprechende Maßnahmen auch auf Netzebene abgesichert werden. Dies kann beispielsweise dadurch geschehen, dass von einer vorgeschalteten Firewall Verbindungen von außen nur zu den entsprechenden Ports zugelassen werden. Noch besser ist es, den Mailserver in einer Demilitarisierten Zone (DMZ) anzusiedeln und auch die Verbindungen zum internen Netz auf die notwendigen Protokolle und Dienste zu beschränken.

Es ist festzulegen, welche Protokolle und Dienste am Mailserver erlaubt sind. Beispielsweise ist es meist nötig, SMTP (TCP-Port 25) nach außen und innen zuzulassen. Hingegen sollten die Protokolle POP3 oder IMAP (TCP Ports 110 bzw. 143, je nachdem, auf welche Art und Weise Mails vom Server abgerufen werden) nur für Zugriffe aus dem internen Netz zugelassen werden. Sowohl für POP3 als auch für IMAP existieren Varianten, bei denen Anmeldung und Datenübertragung durch SSL gesichert werden. Falls die eingesetzte Software diese Varianten unterstützt, sollten sie nach Möglichkeit auch eingesetzt werden.

E-Mails sind eines der verbreitetsten Medien, um Spam und Schadsoftware zu verbreiten. Um sich hiergegen abzusichern, gibt es verschiedene Strategien (siehe auch M 2.154 *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme*). Die Erfahrung hat gezeigt, dass E-Mails sowohl an der Firewall oder auf dem Mailserver als auch auf jedem Client-Rechner überprüft werden sollten (siehe M 5.109 *Einsatz eines E-Mail-Scanners auf dem Mailserver*). Alle eingesetzten Viren-Schutzprogramme müssen regelmäßig aktualisiert werden.

Wenn eine Institution keinen eigenen Mailserver betreibt, sondern über einen oder mehrere Mail-Clients direkt auf den Mailserver eines Providers zugreift, sollte mit dem Provider abgeklärt werden, welche Regelungen dort gelten und

welche Sicherheitsmaßnahmen ergriffen worden sind (siehe M 2.123 *Auswahl eines Groupware- oder Mailproviders*).

Prüffragen:

- Ist der Mailserver gegen unbefugten Zugriff gesichert aufgestellt?
- Gibt es einen für die Verwaltung des Mailservers entsprechend geschulten Administrator und Stellvertreter?
- Haben nur die lokal angeschlossenen Benutzer Zugriff auf ihre Mailboxen?
- Ist der Zugriff für die lokalen Benutzer auf die Bereiche, in denen E-Mails nur temporär für die Weiterleitung zwischengespeichert werden ( z. B. Spooldateien), unterbunden?
- Werden die Aktivitäten auf dem Mailserver regelmäßig protokolliert und diese Protokollierungen regelmäßig ausgewertet?
- Wird regelmäßig kontrolliert, ob die Verbindung mit den benachbarten Mailservern, insbesondere dem Mailserver des Mailproviders, noch stabil ist, und ob der zur Verfügung stehende Plattenplatz noch ausreicht?
- Gibt es eine Richtlinie, welche Protokolle und Dienste am Mailserver erlaubt sind?
- Ist der Mailserver derart konfiguriert, dass er nicht als Spam Relay missbraucht werden kann?

# M 5.57 Sichere Konfiguration der Groupware-/Mail-Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die Groupware-Programme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Die Benutzer müssen darauf hingewiesen werden, dass sie die Konfiguration nicht selbsttätig ändern dürfen.

Bei der Konfiguration der Groupware-Clients sollten die folgenden Punkte berücksichtigt werden:

- Als Reply-Adresse muss die "offizielle" E-Mail-Adresse des Benutzers eingestellt werden. Dadurch wird vermieden, dass interne E-Mail-Adressen auf diesem Weg nach außen weitergegeben werden.
- Um die Netzbelastung niedrig zu halten, sollte der Mail-Client nicht zu häufig den Mailserver auf neue Nachrichten überprüfen. Ein automatischer Abholversuch alle 30 Minuten wird als Standardwert empfohlen und ist meist ausreichend. Falls Benutzer eine dringende Nachricht erwarten, sollten sie das E-Mail-Programm manuell dazu veranlassen, in ihrer Mailbox nachzusehen.
- Werden die Nachrichten per POP3 (Post Office Protocol Version 3) vom Mailserver abgeholt, so sollten sie dort auch gelöscht werden. Auf diese Weise kann ein mehrmaliges Abholen derselben Nachrichten verhindert und Speicherprobleme am Mailserver vermieden werden. Werden die Nachrichten auf dem Mailserver gespeichert und wird über IMAP (Internet Message Access Protocol) darauf zugegriffen, so sollte eine Größenbeschränkung für das serverseitige Postfach eingerichtet werden. Die Benutzer müssen in diesem Fall regelmäßig Mails vom Server löschen beziehungsweise in lokale Postfächer verschieben. Beim Erreichen der Obergrenze für die Postfachgröße sollten die Benutzer auf geeignete Weise darauf hingewiesen werden, beispielsweise mit einer entsprechenden Mail. Die Nachricht kann etwa folgendermaßen lauten:
  "Ihr Postfach hat eine oder mehrere vom Administrator festgelegte Größenbeschränkungen überschritten.
  Die aktuelle Postfachgröße beträgt xxx MB.
  Maximale Postfachgröße: Sie werden benachrichtigt, wenn die Postfachgröße yyy MB überschreitet.
  Sie können möglicherweise keine neuen Nachrichten senden und empfangen, bis Sie die Postfachgröße verringern. Um Platz freizumachen, löschen oder verschieben Sie Objekte in lokale Ordner."

**E-Mails im HTML-Format**

HTML-formatierte E-Mails können aktive Inhalte (beispielsweise Javascript, Flash, ActiveX oder Java) enthalten. Deshalb kommt es gerade durch HTML-formatierte E-Mails, etwa im Zusammenspiel mit Sicherheitslücken in E-Mail-Clients, oft zu Problemen. Um dies zu vermeiden, sollten E-Mail-Programme so eingestellt sein, dass sie aktive Inhalte in HTML-formatierten E-Mails nicht ohne Rückfrage ausführen. Möglichst sollten auch nur E-Mail-Clients eingesetzt werden, die HTML-formatierte E-Mails als solche vor dem Öffnen kenntlich machen. Falls der E-Mail-Client die Option bietet, HTML-formatierte E-Mails nicht automatisch formatiert darzustellen, sondern beim ersten Öffnen die Nachricht nur als Text (HTML-Quelltext) anzuzeigen, so sollte diese Möglichkeit genutzt werden.

Wegen der möglichen Gefahren durch HTML-formatierte E-Mails sollten möglichst keine HTML-formatierten E-Mails verschickt werden. In der Konfiguration des E-Mail-Clients sollte "Nur Text" als Standardformat für neue E-Mails festgelegt werden. Falls unbedingt Formatierungselemente, wie z. B. Schriftart und Farbe, benötigt werden, kann das RTF-Format verwendet werden.

**E-Mail-Anhänge**

E-Mail-Anhänge (Attachments) sind ein beliebtes Transportmedium für Computer-Viren, Trojanische Pferde, Würmer und andere Schadprogramme. E-Mail-Programme sollten deshalb so eingestellt werden, dass Anhänge nicht versehentlich gestartet werden können, sondern das Programm vor der Ausführung warnt bzw. zumindest nachfragt, ob die Datei geöffnet werden soll. Das Betriebssystem bzw. der E-Mail-Client sollte außerdem so eingerichtet sein, dass Dateien zunächst nur in Viewern oder anderen Darstellungsprogrammen angezeigt werden, die eventuell in den Dateien enthaltenen Programmcode, wie Makros oder Skripte, nicht ausführen.

**Vorschau-Funktion**

Einige Client-Programme bieten eine Vorschau-Funktion für E-Mails an. Dabei wird der Inhalt einer ausgewählten E-Mail angezeigt, ohne dass sie explizit vom Benutzer geöffnet wurde. Dadurch besteht die Gefahr, dass schädliche Inhalte in E-Mails unbeabsichtigt ausgeführt werden. Die Vorschau-Funktion sollte daher deaktiviert werden.

**Konfiguration der E-Mail-Filterregeln**

Unerwünschte E-Mails, vor allem Spam-Mails stören das produktive Arbeiten. Generell wird empfohlen, Spam auf dem Server zu filtern. Dies hat den Vorteil, dass alle E-Mails konsistent gefiltert werden und beschränkt den administrativen Aufwand auf einen definierten Punkt. Zusätzlich kann auch auf den Clients gefiltert werden.

Die meisten E-Mail-Clients können so konfiguriert werden, dass sie als unerwünscht markierte E-Mails in separate Ordner verschieben. Entsprechende Filterregeln können durch die Benutzer bzw. die Administratoren eingerichtet werden. Die Benutzer sollten hierüber informiert werden.

**Automatische Weiterleitung von E-Mails**

Bei der zunehmenden Mobilität in Behörden und Unternehmen wird zunehmend gewünscht, immer und von beliebigen Orten aus auf E-Mail zugreifen zu können. Ein Mechanismus hierfür ist die automatische Weiterleitung von E-Mails. Durch unbedacht eingerichtete Weiterleitungen besteht jedoch die Gefahr des Daten- bzw. Vertraulichkeitsverlustes. Dies kann z. B. dann vorkommen, wenn E-Mails unerwartet vertrauliche Mitteilungen enthalten. Es wird daher empfohlen, E-Mails nicht automatisiert weiterzuleiten.

Es ist insbesondere davon abzuraten, dienstliche E-Mails an private E-Mail-Postfächer weiterzuleiten. Die Kommunikation wird von einer Institution durch verschiedenste Maßnahmen geschützt, um die Integrität und Vertraulichkeit von Nachrichten, die Authentizität der Absender und die Verfügbarkeit des E-Mail-Dienstes sicherzustellen.

Durch eine Weiterleitung dienstlicher E-Mails an private E-Mail-Postfächer werden diese Sicherheitsmaßnahmen unter Umständen unterlaufen. So muss ein Angreifer nur die Schutzmechanismen eines privaten Rechners überwin-

den, um an vertrauliche dienstliche Daten sowie an Informationen für weitere Angriffe auf dienstliche Systeme der Institution zu gelangen.

Prüffragen:

- E-Mail-Client, dass keine weitere Konfiguration durch den Benutzer erforderlich ist?
- Werden die Benutzer darauf hingewiesen, dass sie die Konfiguration nicht selbsttätig ändern dürfen?
- Wird das Speichern von Passwörtern in der Kommunikationssoftware verhindert beziehungsweise untersagt?
- Gibt es eine Größenbeschränkung für das Server-seitige Postfach?
- Werden Dateianhänge auf Festplatte gespeichert, bevor sie ausgeführt werden?
- Werden vor dem Starten von Dateianhängen die Dateien mit einem Viren-Schutzprogramm überprüft?

# M 5.58 Auswahl und Installation von Datenbankschnittstellen-Treibern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Datenbankschnittstellen-Treiber, wie z.B. ODBC- (Open Database Connectivity), IDAPI- (Integrated Database Application Programming Interface) oder JDBC-Treiber (Java Database Connectivity), installieren zwischen Datenbankanwendungen und dem jeweiligen Datenbankprotokoll eine zusätzliche Software-Schicht. Durch die Installation des zur Datenbank passenden Treibers wird zwischen Anwendung und Datenbank eine einheitliche Schnittstelle geschaffen, über die die Kommunikation (Absetzen von Datenbankanfragen, Lesen von Daten) zur Datenbank abgewickelt wird. Die zugehörige ANSI-SQL-konforme SQL-Schnittstelle ermöglicht das Erstellen von Anwendungen, ohne auf die jeweiligen Spezifika unterschiedlicher Datenbank-Produkte Rücksicht nehmen zu müssen. Bei einem Wechsel der Datenbank-Software muss deshalb die Anwendung im Idealfall nicht angepasst werden, sondern es reicht aus, den Treiber auszutauschen. Ursprünglich für Produkte der Firmen Microsoft, Sun, etc. entwickelt, haben sich Datenbankschnittstellen-Treiber inzwischen als Standard etabliert und sind für alle gängigen Datenbank-Produkte erhältlich.

Bei der Auswahl eines Treibers müssen verschiedene Kriterien berücksichtigt werden. Die wichtigsten sind nachfolgend aufgeführt:

- Welche Treiber existieren für die anzusprechende Datenbank-Version?
- Welche Treiber existieren für die Betriebssystem-Version des Rechners, auf dem das Anwendungsprogramm läuft?
- Sollen Treiber des Datenbankherstellers (meist kostenlos) oder Treiber von Drittfirmen ausgewählt werden?
- Welcher SQL-Sprachumfang wird durch die Schnittstelle abgebildet?
- Welche sonstigen Anforderungen bringt die eingesetzte Rechnerarchitektur und die verwendete Software mit sich?

Anhand dieser Kriterien, und gegebenenfalls zusätzlicher Anforderungen, die vom Einsatzszenario abhängen, sollte ein geeigneter Treiber ausgewählt werden. Im Nachhinein sollte regelmäßig die getroffene Treiberauswahl überprüft werden. Anlass dazu können neben turnusmäßig vorgesehenen Systemprüfungen unter anderem Software-Upgrades der Datenbank oder des Betriebssystems bzw. neue Treiber-Versionen sein.

Bei der Installation von Datenbankschnittstellen-Treibern ist darauf zu achten, dass durch Fehler oder Nachlässigkeiten keine Sicherheitslücken hinsichtlich der Zugangskontrolle zum Datenbanksystem entstehen.

Um eine Anwendung mit einer Datenbank zu verbinden, muss mittels des Datenbankschnittstellen-Treibers eine sogenannte Datenquelle eingerichtet werden, die dann die Kommunikation zwischen Anwendung und Datenbank unterstützt. Diese Installation sollte nur von einem Administrator durchgeführt werden.

Einige Anwendungen installieren Datenquellen für Beispieldatenbanken oder unbenutzte Datenbankschnittstellen-Treiber. Um einen unerwünschten, even-

tuell unkontrollierten Zugriff über diese Datenquellen bzw. Treiber zu verhindern, sollten alle nicht benötigten Datenquellen und Treiber entfernt werden.

**Beispiel:**

Für Microsoft Access Datenbanken ist die Verwendung von Benutzer-Kennungen optional und muss vom Entwickler explizit aktiviert werden. Wird die Zugangskontrolle aktiviert, so werden die Benutzer-Kennungen und Gruppenzugehörigkeiten über eine separate Microsoft Access Datenbank verwaltet, die sogenannte Arbeitsgruppen-Informationsdatei, die als eigene Datei (Standardname ab Microsoft Access 97: *system.mdw*, davor *system.mda*) gespeichert wird.

Bei der Installation eines ODBC-Treibers für den Zugriff auf eine Microsoft Access Datenbank wird die Arbeitsgruppen-Informationsdatei nicht automatisch integriert. Die Default-Einstellungen während der Installation lassen eine eventuell existierende Arbeitsgruppen-Informationsdatei unberücksichtigt. Wurde also während der Installation des ODBC-Treibers die Arbeitsgruppen-Informationsdatei nicht explizit angegeben, so führt dies unter Umständen dazu, dass ohne Identifizierung anhand der Arbeitsgruppen-Informationsdatei mittels ODBC auf die Datenbank zugegriffen werden kann. Somit kann gegebenenfalls die Zugangskontrolle unterlaufen werden.

Um dies zu verhindern, sind die Rechte in der jeweiligen Access-Anwendung so zu setzen, dass der Zugriff auf die Microsoft Access Datenbank nur mit der spezifizierten Arbeitsgruppen-Informationsdatei erfolgen kann.

Zusätzlich kann regelmäßig geprüft werden, ob die Arbeitsgruppen-Informationsdatei integriert ist, da dieser Mechanismus jederzeit wieder rückgängig gemacht bzw. manipuliert werden kann.

Prüffragen:

- Sind Kriterien für die Auswahl von Datenbankschnittstellen-Treibern festgelegt und berücksichtigt worden?
- Wird die getroffene Auswahl von Datenbankschnittstellen-Treibern regelmäßig überprüft?
- Sind alle nicht benötigten Datenquellen für Beispiel-Datenbanken und Datenbankschnittstellen-Treiber entfernt oder deaktiviert worden?

# M 5.59 Schutz vor DNS-Spoofing bei Authentisierungsmechanismen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Gefahr durch DNS-Spoofing bei der Authentisierung besteht dann, wenn diese anhand eines Rechnernamens durchgeführt wird. Das sollte durch eine der folgenden Konfigurationen (auch in Kombination) erschwert werden:

1. Es sollten IP-Adressen, keine Hostnamen verwendet werden.

2. Wenn Hostnamen verwendet werden, sollten alle Namen über Einträge in der Datei */etc/hosts* lokal aufgelöst werden.

3. Wenn Hostnamen verwendet werden und diese nicht lokal aufgelöst werden können, sollten alle Namen direkt von einem DNS-Server aufgelöst werden, der für diese Namen der so genannte Primary oder Secondary DNS-Server ist, das heißt, er hat sie nicht in einem temporären Cache, sondern dauerhaft abgespeichert.

Punkt 1 bietet die höchste, Punkt 3 die niedrigste Sicherheit. Das Ziel obiger Konfigurationen ist es, die Zuordnung zwischen IP-Adressen und Rechnernamen vor Manipulationen zu schützen. Auf keinen Fall sollte eine hostbasierte Authentisierung über einen Hostnamen gewährt werden, wenn die Namensauflösung nicht direkt ausgeführt werden kann, also ein Cache zwischengeschaltet ist.

Prüffragen:

- Wird bei hostbasierten Authentisierungsmechanismen auf die Verwendung von Hostnamen verzichtet?

# M 5.60 Auswahl einer geeigneten Backbone-Technologie

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT, IT-Sicherheitsbeauftragter

Die Auswahl des Netzprotokolls im Backbone-Bereich ist ein entscheidender Faktor für den Schutz der Verfügbarkeit der Anwendungen in einem lokalen Netz, da das gewählte Protokoll die Performance des Netzes und die zur Verfügung stehende Übertragungskapazität wesentlich beeinflusst.

In der Vergangenheit wurden im Backbone-Bereich folgende Basis-Technologien eingesetzt: Ethernet, Token-Ring, FDDI und ATM. Wenn neue Netze aufgebaut oder bestehende Netze erweitert werden, wird im Allgemeinen Ethernet eingesetzt. Ethernet gilt inzwischen als de facto Standard, auch im Backbone-Bereich, sodass es bei Auswahl einer geeigneten Backbone-Technologie im Wesentlichen um die Auswahl einer geeigneten Ausprägung des Ethernet Standards geht.

Eine generelle Empfehlung, unter Sicherheitsgesichtspunkten eine bestimmte Backbone-Technologie auszuwählen, kann nicht gegeben werden, da viele individuelle Aspekte betrachtet werden müssen.

Nachfolgend werden die einzelne Varianten des Ethernet Standards beschrieben.

**Ethernet**

Die Ethernet-Technologie wird im **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers (IEEE) 802.3 Standard beschrieben und basiert auf dem CSMA/CD-Zugriffsverfahren (Carrier Sense Multiple Access / Collision Detection). Bei diesem Verfahren greifen alle Endgeräte gleichberechtigt auf das Übertragungsmedium zu, obwohl es jeweils nur exklusiv durch ein Endgerät genutzt werden kann. Sobald ein Endgerät Daten übertragen möchte, prüft es zunächst, ob das Medium für die Benutzung zur Verfügung steht (Carrier Sense). Ist dies der Fall, beginnt es mit der Datenübertragung. Geschieht dies durch mehrere Endgeräte gleichzeitig (Multiple Access), kommt es zu einer Kollision, die von den betroffenen Endgeräten erkannt wird (Collision Detection) und zu einer erneuten Prüfung des Mediums mit anschließender Wiederholung der Übertragung führt.

CSMA/CD ist ein stochastisches Verfahren und kann deshalb keine dedizierten Bandbreiten zusichern. Aus diesem Grund ist es beispielsweise für Multimedia-Anwendungen weniger geeignet, die einen festen Durchsatz benötigen. Auf Ethernet-basierten Netzen kann somit im Allgemeinen keine bestimmte Betriebsgüte (Quality of Service - QoS) zugesichert werden.

Es gibt verschiedene Varianten des Ethernet, die sich prinzipiell in der unterstützten Übertragungsrate und in den Anforderungen an der Kabelinfrastruktur und den aktiven Netzkomponenten unterscheiden:

- **Standard Ethernet**
  Standard Ethernet ist der Vorläufer der anderen Varianten.
  Es ist durch eine Übertragungsrate von 10 Mbit/s gekennzeichnet. Für Standard Ethernet wird entweder eine Twisted-Pair-Verkabelung (mindestens CAT-3) mit aktiven Vermittlungseinheiten, wie Hubs oder Switches, eine busförmige BNC-Verkabelung, eine Verkabelung mit AUI-Schnittstel-

le oder Lichtwellenleiter vorausgesetzt. In heutigen Netzen spielt Standard Ethernet kaum noch eine Rolle.

- **Fast Ethernet**
  Aufgrund der steigenden Anzahl vernetzter Rechner und der damit verbundenen Netzlast wurde eine Weiterentwicklung des Standard Ethernet zwingend notwendig, um den gestiegenen Bedürfnissen Rechnung zu tragen. Dies führte zur Entwicklung des Fast Ethernet mit einer Übertragungsrate von 100 Mbit/s. Dies reicht zurzeit für die meisten lokale Netze aus. Für den Anschluss der Endgeräte am Access-Switch sollte mindestens Fast Ethernet eingesetzt werden.
- **Gigabit Ethernet**
  Da die Einführung von Fast Ethernet sehr erfolgreich verlief, wurde die Forderung nach einer noch schnelleren Backbone-Technik basierend auf Ethernet laut. Dies führte 1996 zur Gründung der Gigabit-Ethernet-Allianz (GEA) mit mehreren namhaften Herstellern, die eine Übertragungsrate von 1 Gbit/s erreichen wollen. Auf Grund der fallenden Anschaffungspreise wird Gigabit Ethernet zunehmend für den Anschluss von den Endgeräten am Access-Switch eingesetzt. Wird Kupfer als Übertragungsmedium gewählt, sollten mindestens CAT-5-Kabel verwendet werden. Da dies auch oft bei Fast Ethernet eingesetzt wird, könnte von einer bestehenden Kabelinfrastruktur auf Gigabit Ethernet gewechselt werden.
- **10 Gigabit Ethernet**
  10 Gigabit Ethernet ermöglicht den Informationsaustausch über acht verschiedenen Medientypen. Neben Kupferkabel (mindestens CAT-6, besser CAT-7) können sieben Glasfaserarten genutzt werden. Auf Grund des hohen Preises und der geringen Verbreitung bietet sich der Einsatz von 10 Gigabit Ethernet nur im Backbone-Bereich an.
- **40 und 100 Gigabit Ethernet**
  Die nächste Generation der Ethernet-Varianten ist 40/100 Gigabit Ethernet. Augrund der teilweise noch sehr hohen Preise werden diese Varianten derzeit kaum eingesetzt.

Eine allgemeine Empfehlung zur Auswahl einer Backbone-Technologie kann, wie bereits eingangs erwähnt, nicht gegeben werden. Hier spielen neben Sicherheitsanforderungen auch Kriterien zur Zukunftssicherheit, Wirtschaftlichkeit, Skalierbarkeit und Integration vorhandener Komponenten eine Rolle. Je nach ausgewähltem Protokoll können nur bestimmte Kabeltypen eingesetzt werden, die wiederum durch bestimmte Längenrestriktionen eingeschränkt sind (siehe auch M 5.2 *Auswahl einer geeigneten Netz-Topologie*).

Die Auswahl einer geeigneten Backbone-Technologie muss auf Basis der festgestellten Anforderungen an den Backbone-Bereich des lokalen Netzes in Bezug auf Verfügbarkeit, Bandbreite und Performance erfolgen. Diese Anforderungen müssen definiert und dokumentiert werden.

Prüffragen:

- Sind die Anforderungen an den Backbone-Bereich des lokalen Netzes in Bezug auf Verfügbarkeit, Bandbreite und Performance definiert und dokumentiert?
- Erfolgte die Auswahl geeigneter Backbone-Technologie auf Basis der festgestellten Anforderungen?

# M 5.61 Geeignete physische Segmentierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Unter einer physischen Segmentierung wird der Vorgang der Segmentbildung mit Hilfe von Netzkomponenten auf Schicht 1, 2 oder 3 des OSI-Referenzmodells verstanden. Durch eine geeignete physische Segmentierung können die erforderlichen Sicherheitsmaßnahmen in den Teilnetzen entsprechend dem jeweiligen Schutzbedarf an Verfügbarkeit, Integrität und Vertraulichkeit ausgewählt werden, wenn entsprechende Netzkomponenten (siehe M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*) geeignet eingesetzt werden. Ein zielgerechter Zuschnitt der Netzsicherheit erleichtert es, die erforderlichen Sicherheitsmaßnahmen umzusetzen und zu pflegen.

Daher muss beim Entwurf oder bei grundlegenden Änderungen eines lokalen Netzes auf eine geeignete physische Segmentierung geachtet werden.

**Verfügbarkeit**

Unter dem Gesichtspunkt der Verfügbarkeit wird auch die Performance eines Netzes betrachtet. Diese kann erhöht werden, wenn das Netz auf den entsprechenden Schichten des OSI-Modells 1, 2 oder 3 segmentiert wird. Bei einer Auftrennung auf der Schicht 1 kann die geringste Erhöhung der Verfügbarkeit in den Einzelsegmenten, aber der höchste Durchsatz zwischen den Segmenten und bei einer Trennung auf Schicht 3 die größte Erhöhung der Verfügbarkeit und der geringste Durchsatz zwischen den Segmenten erzielt werden.

In früheren LAN-Implementationen wurden Netze auf Schicht 1 mit Hilfe von Repeatern segmentiert. Dadurch konnte die Verfügbarkeit des Netzes erhöht werden, weil elektrische Fehler des einen Segmentes das andere nicht beeinflussen konnten.

Um Netze auf Schicht 2 zu segmentieren, werden Layer-2-Switches eingesetzt. Dadurch kann die Verfügbarkeit bzw. Performance eines Netzes erhöht werden, weil Layer-2-Switches für jedes IT-System, das an einem Switch-Port angeschlossen ist, eine individuelle Kollisionsdomäne erzeugen. Die IT-Systeme müssen sich nicht, wie es früher beispielsweise bei Hubs der Fall war, die verfügbare Übertragungskapazität mit anderen Netzteilnehmern teilen. Dies führt dazu, dass der Verkehr lokal bleibt und andere Segmente entlastet werden.

Besteht ein Netz allerdings ausschließlich aus Layer-2-Switches, dann werden Broadcast-Pakete an alle angeschlossenenen IT-Systeme (Switches, Arbeitsstationen, Servers etc.) versendet. Vergrößert sich der Broadcast-Verkehr, beispielsweise wenn neue IT-Systeme in das Netz hinzugefügt werden, dann wächst die Gefahr von Überlastungen in den einzelnen Netzsegmenten. Um dies zu verhindern, wird empfohlen, große Broadcast-Domänen in kleinere Broadcast-Domänen zu unterteilen und diese dann mit mit Hilfe von Layer-3-Switches oder Routern miteinander zu verbinden.

Werden Router zur Segmentierung eingesetzt, dann kann der Netzverkehr auf Layer 3 fast vollständig kontrolliert werden. Insbesondere werden keine Broadcasts zwischen Segmenten (Teilnetzen) weitergeleitet, die durch einen

Router getrennt sind. Somit kann ein Broadcaststurm auf dem einen Segment das andere nicht beeinflussen.

Ausgehend von den Ergebnissen einer durchgeführten Verkehrsflussanalyse (siehe M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*) sollte eine physische Segmentierung vorgenommen werden, um den Durchsatz bzw. die Performance im erforderlichen Maße zu erhöhen.

**Beispiel**:

Ein Netz besteht ausschließlich aus Layer-2-Switches (flaches Netz). Um die Verfügbarkeit bzw. Performance des Netzes zu erhöhen, werden kleinere Broadcast-Domänen gebildet, indem einige Layer-2-Switches durch Layer-3-Switches oder Router ersetzt werden.

**Vertraulichkeit**

Um die Vertraulichkeit von Daten in einem Netz entsprechend ihres Schutzbedarfs gewährleisten zu können, sind alle Maßnahmen geeignet, die einen unkontrollierten Austausch von Daten zwischen zwei Segmenten verhindern. Verglichen mit Hubs oder Repeatern stärken Router und Switches die Vertraulichkeit, weil sie den Datenverkehr auf Schicht 2 bzw. 3 kontrollieren können bzw. dediziert auf Port-Ebene Segmente verbinden oder trennen können. Router und Layer-3-Switches bieten die umfassendsten Kontrollmöglichkeiten der hier behandelten Komponenten. Mit Hilfe von Routern bzw. Layer-3-Switches kann nicht nur der Zugang und die Wegewahl in andere Netze bestimmt werden, sondern zusätzlich auch, welcher Netzteilnehmer mit Systemen in anderen Segmenten auf welcher Basis kommunizieren darf. Durch den Ausschluss bestimmter Layer-3-Protokolle am Router kann verhindert werden, dass Daten entsprechender Protokolle in andere Segmente gelangen. Dies geschieht durch die Definition geeigneter Filterregeln (Access Control Lists, ACLs) in den Routern, die auf Protokollebene gebildet werden können. So können beispielsweise einzelne TCP- und UDP-Ports für den Übergang in das andere Segment selektiv gesperrt oder freigegeben werden.

**Beispiel:** Durch die Trennung eines Netzes mit Hilfe eines Routers und eine entsprechende Konfiguration der Filterregeln kann erreicht werden, dass keine Kommunikation zwischen den Segmenten möglich ist. Somit kann ein Segment auch nicht vom jeweils anderen abgehört werden. Ebenso werden keine Broadcast-Paketen zwischen den Teilnetzen übertragen. Außerdem müssen die Filter standardmäßig derart konfiguriert sein, dass zunächst die Kommunikation maximal eingeschränkt und erst nach Bedarf und dienstebezogen freigegeben wird. Hierbei sollte ggf. eine IP-bezogene Filterung berücksichtigt werden.

**Daten- und Netzintegrität**

Die Integrität der Daten bis zur Schicht 3 wird in der Regel durch das eingesetzte Netzzugangsprotokoll sichergestellt, während die Sicherstellung der Netzintegrität, also dem Übereinstimmen der aktuellen Netzsituation mit der geplanten und vorgesehenen physischen und logischen Segmentierung, zusätzliche Maßnahmen erfordert. Diese Maßnahmen müssen sicherstellen, dass keine unautorisierten oder fehlgeleiteten Kommunikationsverbindungen aufgebaut oder unautorisierten Systemzugriffe durchgeführt werden, die im integren Netzzustand unterbunden sind.

Die Netzintegrität wird daher im Wesentlichen dadurch sichergestellt, dass

- Veränderungen unmittelbar an Netzkomponenten (Umrangierungen, Installation neuer, nicht autorisierter Komponenten etc.) verhindert oder zumindest erkannt werden (Hardware-bezogene Sicherheit),
- Veränderungen an der Konfiguration der Netzkomponenten (z. B. an Routing-Protokollen, an der Port-Switching-Matrix oder an der VLAN-Zuweisung) verhindert oder zumindest erkannt werden (Software-bezogene Sicherheit).

Dazu ist es erforderlich, den Zugang zu den Netzkomponenten mit ausreichender Stärke zu verwehren (z. B. durch Infrastrukturmaßnahmen bezüglich Verteilerraum, Verkabelung etc.) und das Netzmanagement so zu konzipieren, dass unberechtigte Zugriffe über das Netz auf die Netzkomponenten verhindert werden.

Eine Erhöhung des Schutzes bezüglich der Integrität der Daten auf Schicht 3 (z. B. der Anwendungsdaten) kann nicht alleine durch den Einsatz von Netzkomponenten erreicht, aber ein gezielter Angriff auf die Datenintegrität kann erschwert werden. Hierzu können Netzkomponenten verwendet werden, die das Mithören und Verändern von Datenpaketen verhindern. Dies sind z. B. Switches und Router, die ein Netz in Segmente bzw. Teilnetze aufspalten können, zwischen denen der Datenverkehr kontrolliert, beschränkt oder konfiguriert werden soll.

Zusätzlich ist durch die geeignete Dimensionierung und Auswahl von Netzkomponenten dafür Sorge zu tragen, dass weder durch deren Überlastung noch durch deren Fehlfunktion Datenpakete verloren gehen können bzw. verfälscht werden.

Prüffragen:

- Wurde das lokale Netz geeignet physisch segmentiert?

# M 5.62 Geeignete logische Segmentierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Mit Hilfe geeigneter aktiver Netzkomponenten ist es möglich, trotz einer festen physischen Segmentierung des Netzes dieses darüber hinaus auch noch logisch zu segmentieren. Die Möglichkeit hierzu bieten so genannte virtuelle LANs (VLANs). Mit VLANs können Gruppen im Netz so zusammengefasst werden, als ob sie in dem selben physischen Segment wären. Hierdurch ergibt sich vor allem die Möglichkeit, Gruppen dynamisch und zeitnah neu zu bilden bzw. umzugruppieren, ohne dass hierfür in die physische Vernetzung eingegriffen werden muss.

Es gibt zwei Arten von VLANs: statische und dynamische VLANs. Bei statischen VLANs (auch portbasierte VLANs genannt) werden einzelne Switch-Ports fest einem VLAN zugeordnet, unabhängig vom angeschlossenen Gerät. Bei dynamischen VLANs wird die Zugehörigkeit eines VLANs beispielsweise über die MAC-Adresse oder IP-Adresse des angeschlossenen Geräts gesteuert. Da sich diese Inhalte leicht manipulieren lassen, sollte auch schon bei normalem Schutzbedarf nach Möglichkeit darauf verzichtet werden, dynamische VLANs zu verwenden. Daher werden diese im Folgenden nicht weiter betrachtet.

Um effektiv ein Netz mit VLANs zu trennen, kann eine Architektur gewählt werden, die aus vier Zonen besteht:

- Internes Netz,
- Sicherheitsgateway-Zone (ALG-Zone),
- Internet-Anbindung und
- Management-Zone) besteht (siehe M 2.476 *Konzeption für die sichere Internet-Anbindung*). Die Zonen müssen physisch getrennt werden. Darauf basierend können dann entsprechende Teilnetze gebildet werden (siehe auch M 5.77 *Bildung von Teilnetzen*).

Auf jeden Fall müssen nachfolgende grundlegende Bedingungen an Teilnetze hinsichtlich des Schutzbedarfs erfüllt sein:

- Innerhalb eines VLANs sollten sich nur Fachverfahren / Arbeitsgruppen desselben Schutzbedarfs befinden.
- Der Schutzbedarf der zu trennenden Teilnetze darf nur entweder "normal" oder "hoch" sein. Bei sehr hohem Schutzbedarf dürfen aus Sicherheitsgründen keine VLANs eingesetzt werden.
- Ist der Schutzbedarf der zu trennenden Teilnetze gleich, dann ist der Einsatz von VLANs grundsätzlich unbedenklich. Eine Ausnahme besteht jedoch für den Fall, dass die Inhaber der VLANs unterschiedliche Institutionen sind. In diesem Fall sollte die Trennung entweder physisch erfolgen oder es sollte Verschlüsselung eingesetzt werden, um die übertragenen Informationen vor unbefugtem Zugriff zu schützen.
- Ist der Schutzbedarf der zu trennenden Teilnetze unterschiedlich, dann ist der Einsatz von VLANs abhängig von den Einsatzsszenarien (siehe Einsatzszenarien von VLANs).

Neben den oben erwähnten grundlegenden Bedingungen hinsichtlich des Schutzbedarfs sind außerdem die folgenden allgemeinen bzw. technischen Anforderungen an die Netzkoppelelemente zu beachten:

- Auf keinen Fall darf durch ein VLAN eine Verbindung zwischen einer Zone vor einem Application-Level-Gateway (Anbindung an das Internet) und dem dahinter liegenden internen Netz geschaffen werden.
- VLANs bieten keinen nennenswerten Schutz vor Abhören an der physischen Übertragungstechnik (Kabel, Stecker, Schnittstellen etc.). Werden beispielsweise Passwörter im Klartext übertragen, dann können diese abgehört werden. Daher müssen zusätzliche Sicherheitsmaßnahmen, wie zum Beispiel Verschlüsselung umgesetzt werden.
- Backplane und Uplinkports der eingesetzten aktiven Netzkomponenten müssen über einen ausreichenden Durchsatz verfügen.
- Die eingesetzten Switches müssen sicher konfiguriert werden (siehe M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches* Sichere Netz-Grundkonfiguration von Routern und Switches*).*

**Einsatzszenarien von VLANs**

Bei den nachfolgenden Szenarien wird von einer Netzarchitektur ausgegangen, die aus vier Zonen besteht (siehe auch M 2.476 *Konzeption für die sichere Internet-Anbindung*).

**Szenario 1: Einsatz von VLANs im internen Netz**

Im internen Netz dürfen VLANs eingesetzt werden, um Teilnetze mit unterschiedlichem Schutzbedarf voneinander zu trennen. Eine Ausnahme besteht jedoch für den folgenden Fall: Die VLANs an einem Switch haben den selben Schutzbedarf, erfüllen dieselben Aufgaben, aber gehören unterschiedlichen Institutionen an. In diesem Fall sollte die Trennung entweder physisch erfolgen oder es sollte Verschlüsselung eingesetzt werden, um die übertragenen Informationen vor unbefugtem Zugriff zu schützen.

**Szenario 2: Einsatz von VLANS in der ALG-Zone**

Es wird empfohlen, die ALG-Zone in zwei Subzonen (externe und interne DMZ) aufzuteilen. In der externen DMZ sollten IT-Systeme platziert werden, die eine öffentliche IP-Adresse haben, damit sie aus dem Internet erreichbar sein können. In der internen DMZ sollten IT-Systeme stehen, die üblicherweise eine private IP-Adresse haben und damit grundsätzlich aus dem Internet nicht direkt erreichbar sind. Innerhalb der jeweiligen DMZ dürfen VLANs zur Trennung eingesetzt werden. Eine interne DMZ sollte jedoch nicht von einer externen DMZ durch VLANs getrennt werden.

**Szenario 3: Einsatz von VLANS in der Management-Zone**

Physisch getrennte Management-Netze dürfen durch VLANs separiert werden. Es ist jedoch darauf zu achten, dass der äußere Paketfilter sowie die daran angeschlossenen Geräte in einem eigenen Teilnetz stehen und nicht dadurch, dass VLANs eingesetzt werden, unter der Umgehung des ALGs eine Verbindung zwischen dem äußerem Paketfilter mit dem internen Netz geschaffen wird.

Prüffragen:

- Befinden sich innerhalb eines VLANs ausschließlich Fachverfahren bzw. Arbeitsgruppen desselben Schutzbedarfs?
- Wurden die Zonen untereinander physisch getrennt?

- Ist sichergestellt, dass bei sehr hohem Schutzbedarf keine VLANs eingesetzt werden?
- Ist sichergestellt, dass es keine Verbindungen zwischen einer Zone vor einem Application-Level-Gateway (Anbindung an das Internet) und dahinter liegenden internen Netzen gibt?
- Werden Daten in VLANs angemessen vor Abhören geschützt, zum Beispiel durch Verschlüsselung?
- Internes Netz: Erfolgt bei VLANs, die unterschiedlichen Institutionen angehören, eine saubere Trennung (physisch oder durch Verschlüsselung)?

# M 5.63 Einsatz von GnuPG oder PGP

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

GNU Privacy Guard (GnuPG) und Pretty Good Privacy (PGP) sind weit verbreitete Programme, mit denen Nachrichten und Dateien ver- und entschlüsselt sowie mit einer digitalen Signatur (auch elektronische Unterschrift genannt) versehen werden können. Beide Tools implementieren Funktionen, die im OpenPGP-Standard (RFC 2440) definiert sind. Durch Verschlüsselung kann die Vertraulichkeit von Informationen geschützt werden, mit digitalen Signaturen kann überprüft werden, ob eine Datei bzw. eine Nachricht authentisch ist und nicht manipuliert wurde. Sowohl mit GnuPG als auch mit PGP können weiterhin die Aufgaben des Schlüsselmanagements, wie z. B. Hinzufügen und Entfernen von Schlüsseln, wahrgenommen werden.

**Verschlüsselung und digitale Signatur**

Bei GnuPG und PGP werden symmetrische und asymmetrische kryptographische Verfahren eingesetzt. Symmetrische, wie AES und IDEA, dienen zur Datenverschlüsselung, asymmetrische wie ElGamal, RSA und DSA/DSS zum Schlüsselmanagement bzw. zur Signaturbildung.

Beide Tools erzeugen und verwenden öffentliche und private Schlüssel in so genannten Schlüsselpaaren. Zu jedem privaten Schlüssel gibt es genau einen öffentlichen Schlüssel. Es ist praktisch ausgeschlossen, nur mit Kenntnis des öffentlichen Schlüssels den privaten Schlüssel zu errechnen. Eine Nachricht, die mit einem öffentlichen Schlüssel verschlüsselt bzw. mit dem privaten Schlüssel signiert wurde, kann nur mit dem zugehörigen privaten Schlüssel entschlüsselt bzw. mit dem öffentlichen Schlüssel des Absenders verifiziert werden. Der öffentliche Schlüssel kann jedem bekannt gemacht werden. Er dient dazu, Nachrichten an den Besitzer des privaten Schlüssels zu verschlüsseln.

Zum Nachweis von unautorisierten Manipulationen und somit zum Schutz vor Veränderungen einer Nachricht berechnet GnuPG bzw. PGP unter Zuhilfenahme des privaten Schlüssels des Absenders einen Prüfcode über die Nachricht, die digitale Signatur. Jeder Kommunikationspartner kann mit Hilfe des öffentlichen Schlüssels des Absenders der Nachricht feststellen, ob der am Ende der Nachricht stehende Prüfcode zu der erhaltenen Nachricht passt oder ob die Nachricht unautorisiert verändert wurde.

Auf technischer Ebene findet aus Sicherheitsgründen in der Regel eine Trennung zwischen den Schlüsseln für digitale Signaturen und den Schlüsseln für Verschlüsselung statt. Dies ist für den Benutzer meist transparent.

Empfehlenswert beim Einsatz von GnuPG oder PGP ist die Kombination der beiden zuvor beschriebenen Funktionalitäten. Nachrichten bzw. Dateien sollten standardmäßig zunächst mit dem privaten Schlüssel des Absenders signiert und anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden, um einen höchstmöglichen Schutz zu erreichen.

**Versionen**

Sowohl GnuPG als auch PGP stehen für die gängigsten Rechnerplattformen (Unix, GNU/Linux, Microsoft Windows) zur Verfügung. Von PGP gibt es auch

Versionen für MacOS. Bei GnuPG handelt es sich um Freie Software/Open Source, die derzeit aktuelle Version ist 1.2.3.

Gängige Versionen von PGP sind 2.6.3i, und 5.x bis 8.x. Die Versionen ab 5.x sind mit einer graphischen Benutzeroberfläche ausgestattet, aber nicht vollständig abwärtskompatibel zu den Vorgängerversionen.

Aufgrund der fehlenden Abwärtskompatibilität ist es empfehlenswert, vor dem Austausch von verschlüsselten Nachrichten nachzufragen, welche PGP-Version von den Kommunikationspartnern verwendet wird. Die nach wie vor weit verbreitete Version 2.6.3i ist kommandozeilenorientiert, kann aber mit Zusatzprogrammen in graphische Benutzeroberflächen und E-Mail-Clients eingebunden werden. PGP kann über verschiedene Quellen bezogen werden, u. a. Freeware-Versionen von diversen WWW-, FTP- oder E-Mail-Servern.

Auch untereinander sind GnuPG und PGP derzeit nicht vollständig interoperabel. Ursache hierfür sind einerseits Software-Patente (der von einigen PGP-Versionen standardmäßig verwendete Algorithmus IDEA ist patentiert) und andererseits kleine Abweichungen vom OpenPGP-Standard. Mit dem Auslaufen des RSA-Patents ist jedoch eine wesentliche Hürde weggefallen. RSA wird von GnuPG ab der Version 1.0.3 unterstützt.

Um diese Probleme zu umgehen, sollte - wenn möglich - nur eines der beiden Tools eingesetzt werden. Falls dies nicht möglich ist, sollten ausschließlich OpenPGP-kompatible Schlüssel verwendet werden. Auf diese Weise wird auch sichergestellt, dass die Kommunikationspartner mit Triple-DES über einen gemeinsamen symmetrischen Algorithmus verfügen. Das oben beschriebene Interoperabilitätsproblem durch die Verwendung von IDEA tritt dann nicht auf. Näheres hierzu findet sich in der Liste der häufig gestellten Fragen und Antworten auf der WWW-Seite des GnuPG-Projekts *www.gnupg.org* und *www.gnupg.de*.

Ab der Version 5 von PGP wurde die umstrittene Funktion *Corporate Message Recovery* (CMR) eingeführt. CMR bietet die Möglichkeit, Dateien oder Nachrichten, die von einer Person für eine Zweite verschlüsselt wurden, gleichzeitig für eine dritte Person entschlüsselbar zu machen. Die Verwendung eines solchen "Drittschlüssels" kann durch die Konfiguration vom Administrator zwingend vorgegeben werden.

Die PGP-Version 7 enthält zwei weitere Funktionen, mit denen unter Umständen Sicherheitsfunktionen unterlaufen werden können. Zum einen wurde ein Server-basierter Wiederherstellungsmechanismus für Schlüssel eingeführt, mit dem ein Benutzer Schlüssel weiterverwenden kann, wenn er beispielsweise die zugehörige Passphrase vergessen hat. Die andere Funktion ist das *Passphrase Caching*, bei dem die Passphrase zwischengespeichert wird, damit diese beim Wechsel zwischen verschiedenen PGP-Teilsystemen nicht jedes Mal neu durch den Benutzer eingegeben werden muss. Einen vergleichbaren Mechanismus gibt es auch in der Version 2.6.3i, bei der die Passphrase in einer Umgebungsvariable gespeichert werden kann. Dieser Mechanismus sollte nicht verwendet werden.

Insbesondere beim Einsatz von GnuPG oder PGP unter Betriebssystemen der Windows-Familie ist zu beachten, dass die Sicherheitsmechanismen dieser Tools durch die Ausnutzung von Sicherheitsmängeln des Betriebssystems möglicherweise unterlaufen werden können.

**Sichere Installation und Bedienung**

Bei GnuPG und PGP werden zwar als sicher anerkannte kryptographische Verfahren eingesetzt, durch falsche Konfiguration oder Fehlbedienung kann es aber zu einer Abschwächung des Sicherheitsniveaus kommen. Die Installation und Konfiguration inklusive der Schlüsselgenerierung ist bei GnuPG und PGP wie bei den meisten komplexeren Kryptoprodukten nicht ganz einfach. Damit sich keine Bedienungsfehler einschleichen können, ist die Einarbeitung in das jeweilige Produkt und in einige kryptographische Grundbegriffe notwendig.

Daher sollte sich in Organisationen ein Mitarbeiter in den Umgang mit dem Tool einarbeiten und als Ansprechpartner zur Verfügung stehen. Dieser sollte dann die anderen Benutzer in die sichere Bedienung von GnuPG bzw. PGP einweisen, insbesondere sollten Verschlüsselung, Signatur und Schlüsselmanagement intensiv geübt werden, bevor ein Benutzer das Programm verwendet. Weiterhin ist es empfehlenswert, dass innerhalb einzelner Organisationen eine einheitliche Programmversion verwendet wird, um die zuvor beschriebenen Kompatibilitätsprobleme zu vermeiden. Sowohl zu GnuPG als auch zu PGP gehört eine umfangreiche Dokumentation, die vor der Verwendung gelesen werden sollte. Da erfahrungsgemäß nicht alle Benutzer die Geduld aufbringen, diese zu lesen, empfiehlt es sich, eine schriftliche Einweisung auszuarbeiten, die auf die Organisationseigenheiten angepasst ist.

Falls Benutzer Fragen zu GnuPG oder PGP haben, die über die mitgelieferte Dokumentation hinausgehen, gibt es diverse Möglichkeiten:

- Zunächst gibt es im Internet eine Sammlung der häufigsten Fragen und Antworten (Frequently Asked Questions - FAQ) zu GnuPG (z. B. unter *www.gnupg.org*) und PGP (z. B. unter *www.pgpi.org* bzw. *www.pgp.com*) sowie deutschsprachige Anleitungen und Ausführungen.
- Über Newsgruppen wie *alt.security.pgp*, *de.comp.security*, *sci.crypt* oder Mailinglisten ist es sehr schnell möglich, Antworten zu Problemen zu bekommen.
- Es gibt mehrere Bücher zu PGP.

**Schlüsselgenerierung**

Jeder Benutzer erzeugt bei GnuPG und PGP sein "Schlüsselpaar" selbst. Hierbei sollten folgende Punkte beachtet werden:

- Bei der Generierung der DSA/DSS- bzw. RSA-Schlüssel können verschiedene Schlüssellängen gewählt werden. Hierbei ist zu beachten, dass mit der Schlüssellänge die Entzifferungsresistenz zunimmt, aber auch die Performance sinkt. Als Schlüssellänge sollte daher 1024 Bit gewählt werden.
- Bei der Schlüsselerzeugung muss eine so genannte *Passphrase* (auch *Mantra* genannt) eingegeben werden, die die Datei mit den privaten Schlüsseln vor unbefugtem Zugriff schützt. Wie jedes Passwort sollte auch dieses nicht leicht zu erraten sein.
  Es kursieren z. B. trojanische Pferde, die gezielt die Datei mit den privaten Schlüsseln (SECRING.*) suchen und an Externe per E-Mail senden. Wenn dann die Passphrase zu einfach gewählt war, bietet sie Brute-Force-Angriffen (automatisiertes Passwortraten) keinen ausreichenden Widerstand. Daher sollte die Passphrase mindestens aus zehn Zeichen bestehen und Sonderzeichen enthalten.

Trojanische Pferde werden zwar in der Regel von Viren-Schutzprogrammen erkannt, dies setzt jedoch voraus, dass das beim Benutzer installierte Programm (bzw. dessen Datenbasis) hinreichend aktuell ist.
- Zu den öffentlichen Schlüsseln gehört eine Benutzer-ID, die möglichst eindeutig sein sollte und zudem die E-Mail-Adresse enthält, z. B. *benutzer@bsi.bund.de*.
- Zur Schlüsselgenerierung benötigen GnuPG und PGP möglichst zufällige Startwerte. Die einzelnen Programme und Versionen verwenden unterschiedliche Verfahren, um diese zufälligen Werte zu erzeugen. Beispielsweise wird der Benutzer gebeten, beliebigen Text einzutippen. Hierbei sollte besser "echter" Text eingegeben werden, z. B. kann dieser Absatz abgetippt werden. Einfach auf der Tastatur "herumklimpern" erzeugt meist schlechtere Ergebnisse, da die zeitlichen Abstände zwischen den Tastendrücken u. U. zu kurz und zu regelmäßig sind.

**Schlüsselaufbewahrung**

Die privaten Schlüssel werden in der Datei SECRING.* gespeichert. Entscheidend für den sicheren Betrieb ist, dass der Inhalt dieser Datei vertraulich bleibt und vor Manipulationen geschützt wird. Der Zugriff auf diese Datei ist zwar durch die Passphrase geschützt, trotzdem sollte sie nicht auf lokalen Netzen gehalten werden, nicht einmal auf nicht genügend gesicherten Stand-Alone-Systemen. Schlüsselringe (Sammlungen von Schlüsseln) sollten auf Diskette gespeichert werden, die der Benutzer sorgfältig verwahren muss. Der Einsatz von Chipkarten zur Schlüsselspeicherung ist vorzuziehen.

Weiterhin sollte eine Sicherungskopie der Datei SECRING.* angelegt, sowie die Passphrase notiert werden. Die Sicherungskopie und die Passphrase sollten sicher und am besten getrennt verwahrt werden, damit nicht durch einen Festplattencrash oder durch Fehlbedienung der private Schlüssel verloren geht. Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt worden sind, lassen sich in diesem Fall nicht mehr entschlüsseln.

Das Aufschreiben und Hinterlegen der Passphrase an einem gesicherten Ort sollten hierbei als kritischer Vorgang betrachtet werden, die ausschließlich der Notfallvorsorge dienen. Die abgeschlossene Schublade eines Schreibtisches oder ähnlich "sichere" Orte können **keinesfalls** als Aufbewahrungsort für den geheimen Schlüssel oder für die Passphrase empfohlen werden.

**Revocation Certificate**

Nach der Schlüsselgenerierung sollte ein so genanntes *Revocation Certificate* erzeugt und ausgedruckt oder auf einer Diskette gespeichert werden. Damit kann der öffentliche Schlüssel widerrufen werden, wenn die Passphrase vergessen wird oder der private Schlüssel aus anderen Gründen nicht mehr zur Verfügung steht. Das *Revocation Certificate* sollte sicher verwahrt werden, damit der öffentliche Schlüssel nicht unberechtigt widerrufen werden kann.

**Schlüsselverteilung**

Damit ein Empfänger die digitale Signatur eines Senders einer Datei überprüfen kann bzw. damit der Sender eine Nachricht für einen bestimmten Empfänger verschlüsseln kann, benötigt er den öffentlichen Schlüssel seines Kommunikationspartners. Diesen kann er auf verschiedene Weisen erhalten, z. B. per Attachment einer E-Mail oder von einem WWW-Server, er muss sich aber davon überzeugen, dass dieser Schlüssel wirklich zu der angegebenen Person gehört. Für eine kryptographisch abgesicherte Zuordnung einer Person

zu ihrem öffentlichen Schlüssel werden Zertifikate verwendet, die ein vertrauenswürdiger Dritter vergibt.

Bei GnuPG und PGP kann jeder Benutzer die öffentlichen Schlüssel anderer Personen mit Zertifikaten beglaubigen. Ein Benutzer sollte einen öffentlichen Schlüssel aber nur dann zertifizieren, wenn er die Identität des Schlüsselinhabers kennt oder überprüft hat und der öffentliche Schlüssel persönlich übergeben wurde.

Alternativ kann die Echtheit eines öffentlichen Schlüssels auch über den so genannten *Fingerprint* verifiziert werden. Hierbei wird eine Zahlenfolge (Hashwert) aus dem öffentlichen Schlüssel berechnet und an diesen angehängt. Nach Übersendung eines öffentlichen Schlüssels kann nun mit dem Absender diese Zahlenfolge, z. B. telefonisch, verglichen werden, um nach der Bestätigung des Fingerprints den übersandten öffentlichen Schlüssel zu zertifizieren.

**Zertifizierungshierarchie - Web of Trust - Internet-Keyserver**

Prinzipiell können GnuPG und PGP sowohl in einer Zertifizierungshierarchie als auch in einem *Web of Trust* eingesetzt werden. Beim *Web of Trust* wird auf die Zertifikate anderer Benutzer vertraut, in einer Zertifizierungshierarchie beglaubigen vertrauenswürdige Dritte, so genannte Zertifizierungsstellen, die Schlüssel aller ihrer Benutzer auf zuverlässige und nachvollziehbare Weise.

In einem Unternehmen oder einer Behörde sollte im Intranet eine Zertifizierungshierarchie aufgebaut werden. Der Betreuer sollte alle Schlüssel für seinen Organisationsbereich bzw. für die gesamte Organisation zertifizieren. Die zertifizierten öffentlichen Schlüssel sollten im Intranet auf einem Server allen Mitarbeitern zugänglich sein, der Zugriff auf diesen Bereich sollte dabei ausschließlich *lesend* (Read-only) sein. Die Methode des *Web of Trust* sollte nur für die private Kommunikation benutzt werden.

Im Internet können öffentliche Schlüssel auf so genannten Keyservern eingestellt werden. Diese dürfen aber keinesfalls mit Zertifizierungsstellen verwechselt werden. Keyserver nehmen Schlüssel von überall in Empfang und verteilen sie auf Anfrage weiter. Es sollte klar sein, dass Schlüssel, die man von einem Keyserver erhält, von diesem in keiner Weise überprüft wurden.

Um die Echtheit eines öffentlichen Schlüssels, der auf einem Keyserver eingestellt wurde, nachzuprüfen, sollte dies mit Hilfe des bereits erwähnten Fingerprints durchgeführt werden.

**Eigensignatur des öffentlichen Schlüssels**

Durch die Selbstsignatur des öffentlichen Schlüssels wird nur die Benutzer-ID als Teil eines öffentlichen Schlüssels von GnuPG bzw. PGP unterschrieben. Mit Hilfe dieser Selbstsignatur ist es möglich, einen Denial-of-Service-Angriff (siehe G 5.28 *Verhinderung von Diensten*) zu entdecken, dieser kann jedoch durch die Selbstsignatur des öffentlichen Schlüssels nicht verhindert werden. Da die Benutzer-ID eines öffentlichen Schlüssels nicht verschlüsselt ist, kann sie verfälscht werden. Dies hätte zur Folge, dass bei Verwendung dieses "verfälschten" Schlüssels, die verschlüsselten E-Mails den Eigentümer dieses Schlüssels nicht mehr erreichen, da sie an eine andere E-Mail-Adresse umgeleitet werden. Die Vertraulichkeit der verschlüsselten Nachricht wird hierdurch nicht gefährdet, da das Entschlüsseln der Nachricht ausschließlich mit dem privaten Schlüssel erfolgen kann.

**Key Recovery**

Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind im Allgemeinen auch die damit geschützten Daten verloren. In den kommerziellen Versionen ab 5.0 bietet PGP Funktionen zur Datenwiedergewinnung für solche Fälle an. Diese Funktionen werden auch als Key Recovery bezeichnet. Diese Funktionalität kann durch Wiederherstellung gespeicherter, verschlüsselter Daten einem Datenverlust vorbeugen, wenn ein Schlüssel oder das Zugriffspaßwort verloren ging.

Bei älteren Versionen von PGP sind Fehler in der ADK-Implementierung (Additional Decryption Key) bekannt geworden, die für Angriffe ausgenutzt werden können. Hiervon sind insbesondere die PGP-Versionen vor 6.5.8 betroffen. Es sollte daher eine hinreichend aktuelle Version eingesetzt werden, bei der möglichst alle bekannt gewordenen sicherheitsrelevanten Fehler beseitigt sind. GnuPG ignoriert grundsätzlich alle ADKs.

Wenn die Wiedergewinnungsfunktion von PGP genutzt werden soll, müssen ein oder zwei zusätzliche Schlüssel (ADK, Additional Decryption Keys) erzeugt werden. Bei der Schlüsselgenerierung werden diese "Nachschlüssel" an die neu erzeugten Schlüssel angebunden und alle Daten, die mit den neuen Schlüsseln verschlüsselt werden, enthalten zusätzlich eine Verschlüsselung des Sitzungsschlüssels mit den ADKs. So ist es im Notfall möglich, die Daten unter Verwendung dieser ADKs, ohne Nutzung des Originalschlüssels zu entschlüsseln. Damit bietet PGP die Funktion *Message Recovery* ohne zentrale Speicherung der Wiederherstellungsinformationen.

Die Nutzung des Key Recovery kann durch entsprechende Voreinstellungen der Clients erzwungen werden, so dass diese Funktionalität nicht von den einzelnen Benutzern unterlaufen werden kann. Allerdings hängt dann die Sicherheit der gesamten Verschlüsselung von der Vertraulichkeit der ADKs ab. Sind diese offen gelegt, können alle Daten mit ihnen entschlüsselt werden.

Um einem Missbrauch dieser höchst sensitiven Funktion vorzubeugen, ist es unabdingbar, dass die ADKs durch ein besonders sorgfältig ausgewähltes, sicher verwahrtes Passwort geschützt werden. Zusätzlich können ab der PGP-Version 6.0 Schlüssel auch in Teile aufgeteilt werden, so dass zu ihrer Nutzung mehrere Personen gemeinsam aktiv werden müssen. Diese Form der Vier-Augen-Kontrolle sollte bei Einsatz von ADKs unbedingt genutzt werden. Als weiterer Schutz kann vorgesehen werden, dass Benutzer jedes Mal gewarnt werden, wenn sie Daten mit einem Schlüssel verschlüsseln, an den ADKs angebunden werden.

Ehe PGP mit Key Recovery eingesetzt wird, sollten die Vor- und Nachteile gegeneinander abgewogen werden. Auf der einen Seite wird zwar einem Datenverlust durch Verlust des Schlüssels vorgebeugt, auf der anderen Seite entsteht ein zentraler Schwachpunkt des Verschlüsselungssystems. Diese Funktion sollte daher nur dann genutzt werden, wenn PGP zur Verschlüsselung gespeicherter Daten eingesetzt wird. Bei einer Nutzung rein für die Kommunikationssicherung kann bei einem Schlüsselverlust auch einfach erneut die E-Mail angefordert werden. Es sollte auch geprüft werden, ob als Alternative die Hinterlegung des Passworts an einer sicheren Stelle in einem geschlossenen Umschlag und die Erstellung von Sicherheitskopien der privaten Schlüsseldateien nicht zu bevorzugen wäre.

**Key Reconstruction**

Die Version 7 von PGP bietet eine weitere Möglichkeit, Problemen durch verloren gegangene Schlüssel, beispielsweise durch vergessene Passphrase, vorzubeugen. Hierzu wird der Schlüssel in mehrere Teile aufgespalten, überschlüsselt und auf einem Wiederherstellungs-Server abgespeichert. Bei der Hinterlegung legt der Benutzer fünf Frage/Antwort-Kombinationen fest. Mindestens drei der fünf Fragen muss der Benutzer korrekt beantworten, um seinen Schlüssel wiederherstellen zu können.

Bei dieser Funktion besteht die Gefahr, dass Benutzer Fragen festlegen, deren Antworten durch Dritte erraten oder ermittelt werden können, beispielsweise Namen von Verwandten oder Geburtsdaten. Als Folge können u. U. Dritte unberechtigt auf Schlüssel des Benutzers zugreifen. Da sich die Qualität der Frage/Antwort-Kombinationen in der Regel auch nicht überprüfen lässt, sollte diese Funktion nicht genutzt werden. Stattdessen wird empfohlen, eine Sicherheitskopie der privaten Schlüsseldateien auf einem Datenträger anzufertigen und den Datenträger an einem abgesicherten Ort zu verwahren. Auch die zugehörige Passphrase ist in einem geschlossenen Umschlag zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*).

**Single Sign-On**

Unter den Bezeichnungen *Single Sign-On* und *Passphrase Caching* bietet PGP ab der Version 7 einen Mechanismus an, die vom Benutzer eingegebene Passphrase zwischenzuspeichern, damit der Benutzer sie nicht bei jeder Aktion neu eingeben muss. Hierdurch besteht die Gefahr, dass unberechtigte Personen mit der Identität des Benutzers Dokumente ver- oder entschlüsseln bzw. digital signieren können, wenn der Benutzer kurzzeitig seinen Arbeitsplatz verlässt.

Falls die Funktion *Passphrase Caching* von PGP genutzt werden soll, muss daher auf jeden Fall sichergestellt sein, dass der Rechner des Benutzers auch bei kurzzeitigem Verlassen des Arbeitsplatzes unmittelbar gesperrt wird. Dies kann beispielsweise mit der Funktion Arbeitsstation sperren von Windows NT erfolgen, sofern ein starkes Benutzerpasswort vergeben ist, oder mit Hilfe einer Chipkartenlösung zur Benutzer-Authentisierung. In allen anderen Fällen sollte im Dialogfeld *PGP Options* die Option *Do not cache passphrase* aktiviert werden.

Prüffragen:

- Werden hinreichend aktuelle Versionen eingesetzt, wobei die Kompatibilität intern und mit etwaigen Kommunikationspartnern sichergestellt ist?
- Werden Benutzer für das Produkt einschließlich notwendiger kryptographischer Grundlagen geschult?
- Wird bei der Schlüsselgenerierung für ausreichend lange Schlüssel und Passphrases gesorgt?
- Gibt es Regelungen zur Aufbewahrung von Schlüsseln gegen deren Verlust und Kompromittierung?
- Werden öffentliche Schlüssel nur dann zertifiziert, wenn diese zuvor persönlich übergeben oder der Fingerprint sicher verifiziert wurde?
- Wird Passphrase Caching unterbunden oder zumindest durch begleitende Maßnahmen abgesichert?

# M 5.64 Secure Shell

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ohne spezielle Erweiterungen bieten die Protokolle *telnet* und *ftp* nur rudimentäre Mechanismen zur Authentisierung. In der Regel wird eine einfache Abfrage von Benutzer-Kennung und Passwort durchgeführt, die dann - ebenso wie die Nutzdaten - im Klartext gesendet werden. Die Vertraulichkeit der Authentisierungs- und Nutzdaten ist also nicht gesichert. Die verwandten Protokolle *rsh*, *rlogin* und *rcp*, die oft unter der Bezeichnung r-Dienste zusammengefasst werden, weisen ähnliche Sicherheitsmängel auf.

Secure Shell (*ssh*) kann als Ersatz für die r-Dienste genutzt werden, wobei umfangreiche Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität zum Einsatz kommen. Hierzu wird ein hybrides Verschlüsselungsverfahren, also eine Kombination aus asymmetrischer und symmetrischer Verschlüsselung, verwendet. Angesiedelt ist die Secure Shell auf Schicht 7 (Anwendungsschicht) des ISO/OSI-Referenzmodells, allerdings können auch andere Protokolle wie das *X11*-Protokoll, das von der graphischen Oberfläche X-Window verwendet wird, über *ssh* transportiert werden.

Derzeit basiert Secure Shell auf drei Protokollen, die aufeinander aufbauen und für die jeweils ein Internet-Draft existiert.

- Das unterste Protokoll ist das *Transport Layer Protocol*. Dieses Protokoll leistet den Großteil der Sicherungsfunktionen von *ssh*, nämlich Authentisierung auf Host-Ebene, Verschlüsselung und Schutz der Datenintegrität. Die kryptographischen Algorithmen sind zwischen den Kommunikationspartnern aushandelbar.
- Das mittlere Protokoll ist das *User Authentication Protocol*. Dies erlaubt die Authentisierung auf Benutzer-Ebene, wobei auch hier das Verfahren ausgehandelt werden kann. Wenn zur Authentisierung eine einfache Übertragung von Benutzer-Kennung und Passwort verwendet wird, so ist die Vertraulichkeit dieser Informationen gegenüber dem Kommunikationsweg durch das darunterliegende *Transport Layer Protocol* gesichert. Empfohlen wird jedoch die Authentisierung durch ein Public-Key-Verfahren.
- Das *Connection Protocol* baut auf den beiden vorhergehenden Protokollen auf und erlaubt den Aufbau von mehreren logischen Nutzkanälen. Die Daten auf diesen Nutzkanälen werden gemeinsam über eine einzelne abgesicherte Secure Shell-Verbindung übertragen.

Für alle gängigen Unix-Betriebssysteme existieren Implementierungen sowohl von *ssh*-Clients als auch von *ssh*-Servern. Darüber hinaus gibt es *ssh*-Clients unter anderem für Windows, Mac OS und als Java-Applet.

Grundsätzlich ist der Einsatz von Secure Shell zu empfehlen, wenn die Funktionalitäten der r-Dienste über Kommunikationskanäle genutzt werden, die nicht ausreichend gegen Kompromittierung und/oder Manipulation gesichert sind (z. B. über das Internet). Im folgenden werden einige Hinweise für den sicheren Einsatz von *ssh* gegeben.

Von besonderer Bedeutung ist die Gefährdung durch so genannte *man-in-the-middle*-Attacken. Hierbei filtert der Angreifer den gesamten Verkehr zwischen den Kommunikationspartnern und reicht gefälschte öffentliche Schlüssel weiter. Ist es den Kommunikationspartnern nicht möglich, die öffentlichen Schlüssel zu prüfen, kann der Angreifer den gesamten Verkehr lesen und manipulieren, indem er die Daten jeweils selbst entschlüsselt, dann liest bzw. modi-

fiziert und schließlich mit einem anderen Schlüssel verschlüsselt und weiterleitet. Dies kann mit Hilfe eines geeigneten Schlüssel-/Zertifikatmanagements verhindert werden. Beim praktischen Einsatz von Secure Shell wird jedoch oft eine Kompromisslösung angewandt, die den Einsatz von *ssh* ohne jede zusätzliche Infrastruktur erlaubt. Dabei wird bei einem Verbindungsaufbau zu einem Host, dessen öffentlicher Schlüssel noch nicht bekannt ist, dieser über das unsichere Netz gesendet und in einer lokalen Datenbank abgelegt. Bei allen nachfolgenden Verbindungen mit diesem Host kann dessen öffentlicher Schlüssel dann anhand der lokalen Datenbank überprüft werden. Im Rahmen des Sicherheitskonzeptes muss geklärt werden, ob dieses Verfahren, das eine reduzierte Sicherheit gegenüber *man-in-the-middle*-Angriffen bietet, für die vorliegende Anwendung ausreichend ist.

In den Internet-Drafts sind kryptographische Verfahren festgelegt, die von den Secure Shell-Implementierungen zur Verfügung gestellt werden müssen. Optional können jedoch zusätzliche kryptographische Algorithmen implementiert werden. Die tatsächlich benutzten Verfahren werden beim Verbindungsaufbau ausgehandelt. Durch Wahl geeigneter Client- und Server-Programme und durch entsprechende Konfiguration ist sicherzustellen, dass sich *ssh*-Client und *ssh*-Server auf qualifizierte kryptographische Algorithmen einigen, die den Sicherheitsanforderungen genügen.

Wenn *ssh* zum Einsatz kommt, sollten nach Möglichkeit alle anderen Protokolle, deren Funktionalität durch Secure Shell abgedeckt wird, also z. B.die r-Dienste und *telnet*, vollständig abgeschaltet werden, damit die Sicherheitsmaßnahmen nicht umgangen werden können. Dies setzt allerdings voraus, dass alle Kommunikationspartner über geeignete Implementierungen verfügen.

Von älteren Implementierungen von *ssh* sind sicherheitsrelevante Programmfehler bekannt. Es sollte daher eine Version verwendet werden, bei der solche Mängel beseitigt sind. Die Kompatibilität zwischen Implementierungen, deren Programmversionen sich stark unterscheiden, ist unter Umständen problematisch. Ein Mischbetrieb sollte deshalb möglichst vermieden werden.

Zu beachten ist, dass beim Einsatz von *ssh* über Firewalls eine inhaltssensitive Kontrolle des Datenstroms nicht mehr möglich ist.

Prüffragen:

- Bei hohen Schutzbedarf vor man-in-the-middle-Angriffen: Wird ein geeignetes Schüsselmanagement und Zertifikatmanagement verwendet?
- Wird nach Möglichkeit nur eine einzige aktuelle Version von ssh verwendet?

# M 5.65 Einsatz von S-HTTP

Diese Maßnahme ist mit Version 2005 entfallen.

# M 5.66 Clientseitige Verwendung von SSL/TLS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Das bei der Web-Nutzung am häufigsten verwendete Sicherheitsprotokoll ist SSL/TLS (Secure Socket Layer/Transport Layer Security). Die erste Version des SSL-Protokolls (SSL v 1.0) wurde von Netscape entwickelt. Neuere Versionen sind unter der Bezeichnung TLS in verschiedenen RFCs standardisiert. SSL/TLS wird von allen aktuelleren Browsern unterstützt. Mit SSL/TLS können Verbindungen abgesichert werden:

- durch Verschlüsselung der Verbindungsinhalte,
- durch Überprüfung der Vollständigkeit und Korrektheit der übertragenen Daten,
- durch Prüfung der Identität des Servers und
- optional durch Prüfung der Identität der Client-Seite.

Zu Beginn einer neuen mit SSL/TLS abgesicherten Kommunikationsverbindung findet ein sogenannter Handshake zwischen Client und Server statt. Hierbei verständigen sich Client und Server über die kryptographischen Algorithmen, die für Schlüsselaustausch, Verschlüsselung und Integritätssicherung eingesetzt werden. Außerdem einigen sich Client und Server über die SSL-Version, die verwendet wird. Zusätzlich sendet der Server sein X.509-Zertifikat an den Client. Optional kann auch der Client dem Server sein X.509-Zertifikat übermitteln, falls dies vom Server angefordert wird. Mit Hilfe eines asymmetrischen Verschlüsselungsverfahrens wird anschließend ein symmetrischer Schlüssel sicher ausgetauscht. Für die Verschlüsselung der eigentlichen Datenübertragung wird nun ein symmetrisches Verfahren benutzt, weil hiermit dies große Datenmengen schneller verschlüsselt werden können. Bei jeder Transaktion wird ein anderer symmetrischer Schlüssel als "Session Key" ausgehandelt, mit dem dann die Verbindung verschlüsselt wird.

Ein Benutzer kann Webseiten, die eine SSL/TLS-gesicherte Datenübertragung ermöglichen, beispielsweise daran erkennen, dass die Internet-Adresse um ein "s" erweitert ist (https://www...). Zusätzlich werden solche Webseiten bei den meisten gängigen Browsern auch besonders gekennzeichnet, beispielsweise durch ein angezeigtes Symbol (Schlüssel, Vorhängeschloss etc.) oder durch eine farbliche Markierung der Internet-Adresse.

Die Nutzung von SSL/TLS ist nicht auf HTTP-Clients und -Server beschränkt. Auch Protokolle wie SMTP, FTP, IMAP oder LDAP können durch SSL/TLS kryptographisch abgesichert werden, allerdings setzt dies voraus, dass die betreffenden Clients und Server diese Sicherheitsfunktion jeweils unterstützen.

SSL/TLS besteht aus zwei Schichten. Auf der oberen Schicht arbeitet das SSL/TLS Handshake Protokoll. Dieses dient dem Client und dem Server dazu, sich gegenseitig zu authentisieren sowie dazu, für den anschließenden Datenverkehr einen Schlüssel und einen Verschlüsselungsalgorithmus auszuhandeln. Die untere Schicht, das SSL/TLS Record Protokoll, das die Schnittstelle zur TCP-Schicht bildet, ver- und entschlüsselt den eigentlichen Datenverkehr. Da SSL/TLS für den Zugriff auf TCP auf der Socket-Schnittstelle aufsetzt und diese durch eine sicherheitserweiterte Version ersetzt, ist es auch für andere Dienste verwendbar.

**Versionsnummer**

Es existieren mehrere SSL/TLS-Protokollversionen, wie SSL v2, SSL v3, TLS v1.0, TLS v1.1 und TLS v1.2. SSL v1 wurde nicht veröffentlicht. Um eine sichere Verbindung zwischen Client und Server zu gewährleisten, sollte mindestens TLS 1.2 verwendet werden.

TLS 1.1 bietet ausreichende Sicherheit, aber im Vergleich zu TLS 1.2 weist es jedoch einige Schwächen auf, z. B. sind in TLS 1.1 noch Cipher-Suites vorhanden, die auf IDEA und DES basieren, in TLS 1.2 nicht mehr.

TLS 1.0 kann in bestehenden Client-Anwendungen übergangsweise weiter eingesetzt werden, falls eine sofortige Migration zu TLS 1.1 oder vorzugsweise TLS 1.2 nicht möglich ist und geeignete Maßnahmen gegen Chosen-Plaintext-Angriffe (z. B. BEAST) auf die CBC-Implementierung getroffen werden. Generell sollte jedoch eine Migration zu TLS 1.2 schnellstmöglich erfolgen. SSL v2 und SSL v3 dürfen nicht mehr eingesetzt werden.

**Algorithmen und Schlüssellängen**

Bei SSL/TLS können verschiedene kryptographische Algorithmen mit verschiedenen Schlüssellängen eingesetzt werden (siehe hierzu auch M 3.23 *Einführung in kryptographische Grundbegriffe*). Beim Verbindungsaufbau einigen sich Client und Server auf die in der Sitzung verwendeten Verfahren.

Durch die Auswahl der Produkte (Browser, Webserver, Plug-In etc.) und geeignete Konfiguration ist sicherzustellen, dass bei der SSL/TLS-geschützten Kommunikation ausschließlich Algorithmen und Schlüssellängen zum Einsatz kommen, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen. Darüber hinaus sollten die verwendeten Cipher-Suites Perfect Forward Secrecy (PFS) unterstützen (siehe TR-02102-2).Weitere Hinweise zu Algorithmen und Schlüssellängen finden sich in der Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*.

**Zertifikate**

Es ist schwierig, bei der Datenkommunikation über offene Netze die Identität der Kommunikationspartner zu überprüfen, da nicht sichergestellt ist, dass Namensangaben korrekt sind. Bei SSL/TLS erfolgt die Überprüfung der Identität des Kommunikationspartners über so genannte Zertifikate. Zertifikate enthalten deren öffentliche Schlüssel sowie eine Bestätigung einer weiteren Instanz über die korrekte Zuordnung des öffentlichen Schlüssels zu dessen "Besitzer", hier also ein Server oder Client. Der Wert eines Zertifikates hängt also nicht zuletzt davon ab, wie vertrauenswürdig diese Bestätigungsinstanz (auch Trustcenter oder Zertifizierungsstelle genannt) ist. Die Echtheit des Zertifikates lässt sich wiederum mit dem öffentlichen Schlüssel der Bestätigungsinstanz überprüfen.

Alle gängigen Browser enthalten bereits bei der Installation SSL/TLS-Zertifikate einiger Zertifizierungsstellen. Diese Zertifizierungsstellen haben sehr unterschiedliche Sicherheitsleitlinien und Bedingungen, unter denen sie Zertifikate erteilen. Bevor sicherheitskritische Informationen über eine SSL/TLS-geschützte Verbindung übertragen werden, sollte deshalb die Sicherheitsrichtlinie der jeweiligen Zertifizierungsstellen geprüft werden.

Bei der Aufnahme eines neuen Zertifikates sollte darauf geachtet werden, dieses erst nach Überprüfung des "Fingerprints" zu aktivieren. Der Fingerprint

ist eine hexadezimale Zahl, die zusammen mit dem Zertifikat übermittelt wird. Zusätzlich sollte sie auf einem anderen Weg übermittelt und verglichen werden, da diese die Korrektheit des Zertifikats sicherstellen soll.

Betreiber von Webservern, die mit den Besuchern ihrer Webseiten sicherheitsrelevante Daten austauschen wollen, sollten hierzu einen kryptographisch abgesicherten Weg anbieten, also z. B. SSL/TLS.

In der Vergangenheit ist es bereits vorgekommen, dass Zertifizierungsstellen kompromittiert und dadurch Hunderte gefälschte Zertifikate ausgestellt wurden, darunter auch solche für Nachrichtendienste, Online-Portale, andere Zertifizierungsstellen und Anonymisierungsdienste. Durch Widerrufslisten und Validierungsprotokolle wie OCSP (Online Certificate Status Protocol) können gefälschte, manipulierte oder veraltete Zertifikate allerdings zeitnah als ungültig erklärt werden. Daher sollte die Validierung von Zertifikaten in Anwendungsprogrammen wie Browsern und E-Mail-Clients aktiviert werden. Dabei ist OCSP der Verwendung von Zertifikatswiderruflisten (Certificate Revocation Lists, CRLs) vorzuziehen, da OCSP zeitnahe Aktualisierungen über das Internet erlaubt.

Kann ein Zertifikat nicht validiert werden, beispielsweise weil der OSCP-Server nicht erreicht oder auf die Widerrufslisten nicht zugegriffen werden kann, dann gibt es aus Sicht des Clients zwei Möglichkeiten: Er kann die Verbindung beenden oder ein eventuell manipuliertes oder ungültiges Zertifikat akzeptieren. Die Entscheidung, was in solchen Fällen zu tun ist, sollte mit den Sicherheitsrichtlinien der Institution in Einklang stehen.

**Session Renegotation und TLS-Kompression**

Clientseitig sollte die Session Renegotiation deaktiviert werden. Allgemeine Informationen zur Funktionsweise von Session Renegotiation sind in M 5.177 *Serverseitige Verwendung von SSL/TLS* zu finden.

TLS bietet die Möglichkeit, die übertragenen Daten vor der Verschlüsselung zu komprimieren. Dies kann dazu führen, dass Seitenkanalangriffe auf die Verschlüsselung über die Länge der verschlüsselten Daten, durchgeführt werden. Ein Beispiel hierfür ist CRIME (Compression Retro Info-leak Made Easy), ein 2012 vorgestellter Seitenkanal-Angriff, der das Ziel hat, eine HTTPS-Sitzung zu übernehmen. Um dies zu verhindern, sollte die TLS-Kompression deaktiviert werden.

**Hinweis:** Beim Einsatz von SSL/TLS ist zu beachten, dass verschlüsselte Daten hinsichtlich aktiver Inhalte und Schadprogramme nicht zentral, also z. B. am Sicherheitsgateway, überprüft werden können. Dies muss bei der Sicherheitskonzeption berücksichtigt werden, damit keine Sicherheitslücken entstehen. Weitere Empfehlungen hierzu finden sich unter anderem im Baustein B 1.6 *Schutz vor Schadprogrammen*.

Prüffragen:

- Unterstützen die eingesetzten Client-Produkte eine sichere Version von SSL/TLS?
- Ist sichergestellt, dass die eingesetzten Clients kryptographische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen?
- Wird die Sicherheitsrichtlinie der jeweiligen Zertifizierungsstellen geprüft, bevor sicherheitskritische Informationen über eine SSL/TLS-geschützte Verbindung übertragen werden?

- Wird auch bei der Nutzung von SSL/TLS ein ausreichender Schutz vor Schadprogrammen und unerlaubten aktiven Inhalten gewährleistet?
- Wird darauf geachtet, dass neue Zertifikate erst nach Überprüfung des "Fingerprints" aktiviert werden?
- Ist sichergestellt, dass die Validierung von Zertifikaten den Sicherheitsrichtlinien der Institution entspricht?
- Sind Session Renegotiation und TLS-Kompression deaktiviert?

# M 5.67 Verwendung eines Zeitstempel-Dienstes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die im Header einer E-Mail eingetragenen Zeitinformationen können relativ einfach manipuliert werden. Ist es erforderlich, den exakten Absende- oder Empfangszeitpunkt einer E-Mail zu kennen, muss ein Zeitstempeldienst benutzt werden. Ein Zeitstempel ist ein Zeiteintrag von einer neutralen Stelle, der nicht mehr zu verfälschen ist. Er wird von einem Zeitstempel-Server entweder vollautomatisch, d. h. transparent für den Benutzer, oder auf Anforderung durch den Absender aufgebracht.

Ein Zeitstempel besteht aus einem Zeitstempel-Zertifikat, in dem das aktuelle Datum und die aktuelle Uhrzeit sowie die Identität des Zeitstempel-Dienstes selbst dokumentiert werden, sowie aus einer digitalen Signatur über E-Mail und Zertifikat. Hiermit dokumentiert und bestätigt der Zeitstempel die Existenz einer bestimmten Nachricht mit einem bestimmten Inhalt zu einem bestimmten Zeitpunkt. Die Sicherstellung der Authentizität der E-Mail durch den Zeitstempel setzt voraus, dass der Absender seinerseits die E-Mail digital signiert hat.

Ein Zeitstempel-Dienst kann sowohl in einem internen Netz als auch im Internet angeboten und genutzt werden. Er nimmt als Server im Internet/Intranet signierte Dateien oder auch nur deren Signaturen entgegen und versieht diese mit einem synchronisierten Zeitstempel. Alles zusammen wird vom Zeitstempel-Dienst wiederum signiert und wahlweise an den Empfänger weitergeleitet oder auch zurück an den Absender geschickt.

Prüffragen:

- Bei Erfordernis zur Sicherstellung des exakten Absende- oder Empfangszeitpunkt einer E-Mail: Wird ein Zeitstempeldienst verwendet?

# M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Kommunikationsnetze transportieren Daten zwischen IT-Systemen. Dabei werden die Daten selten über eine dedizierte Kommunikationsleitung zwischen den an der Kommunikation beteiligten Partnern übertragen. Vielmehr werden die Daten über viele Zwischenstationen geleitet. Je nach Kommunikationsmedium und verwendeter Technik können die Daten von den Zwischenstationen unberechtigt abgehört werden, oder auch von im jeweiligen Vermittlungsnetz angesiedelten Dritten (z. B. bei der Verwendung des Ethernet-Protokolls ohne Punkt-zu-Punkt-Vernetzung). Da die zu übertragenden Daten nicht von unberechtigten Dritten abgehört, verändert oder zur späteren Wiedereinspeisung in das Netz (Replay-Attacke) benutzt werden sollen, muss ein geeigneter Mechanismus eingesetzt werden, der dies verhindert. Verschlüsselung der Daten mit - wenn nötig - gegenseitiger Authentisierung der Kommunikationspartner kann diese Gefahr (je nach Stärke des gewählten Verschlüsselungsverfahrens sowie der Sicherheit der verwendeten Schlüssel) reduzieren (siehe auch Baustein B 1.7 *Kryptokonzept*).

In der Regel kommunizieren Anwendungen miteinander, um anwendungsbezogene Informationen auszutauschen. Die Verschlüsselung der Daten kann nun auf mehreren Ebenen geschehen:

- Auf Applikationsebene: Die kommunizierenden Applikationen müssen dabei jeweils über die entsprechenden Ver- und Entschlüsselungsmechanismen verfügen.
- Auf Betriebssystemebene: Die Verschlüsselung wird vom lokalen Betriebssystem durchgeführt. Jegliche Kommunikation über das Netz wird automatisch oder auf Anforderung verschlüsselt.
- Auf Netzkoppelelementebene: Die Verschlüsselung findet zwischen den Netzkoppelelementen (z. B. Router) statt.

Die einzelnen Mechanismen besitzen spezifische Vor- und Nachteile. Die Verschlüsselung auf Applikationsebene hat den Vorteil, dass die Verschlüsselung vollständig der Kontrolle der jeweiligen Applikation unterliegt. Ein Nachteil ist, dass zur verschlüsselten Kommunikation nur eine mit demselben Verschlüsselungsmechanismus ausgestattete Partnerapplikation in Frage kommt. Weiterhin können entsprechende Authentisierungsmechanismen zwischen den beiden Partnerapplikationen zur Anwendung kommen.

Im Gegensatz dazu findet die Verschlüsselung im Fall der Verschlüsselung auf Betriebssystemebene transparent für jede Applikation statt. Jede Applikation kann mit jeder anderen Applikation verschlüsselt kommunizieren, sofern das Betriebssystem, unter dem die Partnerapplikation abläuft, über den Verschlüsselungsmechanismus verfügt. Nachteilig wirkt sich hier aus, dass bei einer Authentisierung lediglich die Rechner gegenseitig authentisiert werden können, und nicht die jeweiligen Partnerapplikationen.

Der Einsatz von verschlüsselnden Netzkoppelelementen besitzt den Vorteil, dass applikations- und rechnerseitig keine Verschlüsselungsmechanismen vorhanden sein müssen; die Verschlüsselung ist auch hier transparent für die Kommunikationspartner. Allerdings findet die Kommunikation auf der Strecke bis zum ersten verschlüsselnden Netzkoppelelement unverschlüsselt statt und

birgt damit ein Restrisiko. Authentisierung ist hier nur zwischen den Koppelelementen möglich. Die eigentlichen Kommunikationspartner werden hier nicht authentisiert.

Werden sensitive Daten über ein Netz (auch innerhalb des Intranets) übertragen, empfiehlt sich der Einsatz von Verschlüsselungsmechanismen. Bieten die eingesetzten Applikationen keinen eigenen Verschlüsselungsmechanismus an oder wird das angebotene Verfahren als zu schwach eingestuft, so sollte von der Möglichkeit der betriebssystemseitigen Verschlüsselung Gebrauch gemacht werden. Hier bieten sich z. B. Verfahren wie SSL an, die zur transparenten Verschlüsselung auf Betriebssystemebene entworfen wurden. Je nach Sicherheitspolitik können auch verschlüsselnde Netzkoppelelemente eingesetzt werden, etwa um ein virtuelles privates Netz (VPN) mit einem Kommunikationspartner über das Internet zu realisieren (Entsprechende Softwaremechanismen sind in der Regel auch in Firewall-Systemen (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) verfügbar).

Beim Einsatz von verschlüsselter Kommunikation und gegenseitiger Authentisierung sind umfangreiche Planungen im Rahmen der Sicherheitspolitik eines Unternehmens bzw. einer Behörde nötig. Im Rahmen der hier angesprochenen Kommunikationsverschlüsselungen sind insbesondere folgende Punkte zu beachten:

- Welche Verfahren sollen zur Verschlüsselung benutzt werden bzw. werden angeboten (z. B. in Routern)?
- Unterstützen/Nutzen die eingesetzten Verschlüsselungsmechanismen existierende oder geplante Standards (IPSec, IPv4, IPv6, IKE)?
- Sind gemäß der Sicherheitspolitik ausreichend starke Verfahren und entsprechend lange Schlüssel gewählt worden?
- Werden die Schlüssel sicher aufbewahrt?
- Werden die Schlüssel in einer sicheren Umgebung erzeugt, und gelangen sie auf sicherem Weg zum notwendigen Einsatzpunkt (Rechner, Softwarekomponente)?
- Sind Schlüssel-Recovery-Mechanismen nötig?

Bei der Nutzung von Zertifikaten zur Authentisierung von Kommunikationspartnern sind hier ähnliche Fragestellungen zu beachten.

Prüffragen:

- Wird der Einsatz von Verschlüsselungsverfahren zur Netzkommunikation in die Sicherheitspolitik des Unternehmens eingebettet?
- Ist definiert, welche Verfahren und welche Schlüssellänge zur Verschlüsselung zum Einsatz kommen sollen?
- Kann die Sicherheit der Schlüssel zur Verschlüsselung bei Erzeugung, Transport und Aufbewahrung gewährleistet werden?

# M 5.69 Schutz vor aktiven Inhalten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Beim Anzeigen von Webseiten im Browser werden häufig nicht nur Texte, Bilder und Multimedia-Inhalte geladen, sondern gleichzeitig auch Programmcodes (aktive Inhalte) ausgeführt, gegebenenfalls mittels geeigneter Plug-Ins. Bekannte Beispiele für aktive Inhalte sind JavaScript, Java-Applets, ActiveX-Elemente, Flash etc. Werden aktive Inhalte im Browser ausgeführt, kann dies zu Sicherheitsproblemen führen, etwa wenn dadurch Schadprogramme auf den Computer geladen werden oder wenn Angreifer versuchen, mittels aktiver Inhalte unerlaubt auf Daten zuzugreifen. Die gängigen Browser enthalten Sicherheitsmechanismen, die die Zugriffsmöglichkeiten von aktiven Inhalten einschränken. Es werden jedoch immer wieder Schwachstellen und Möglichkeiten bekannt, diese Sicherheitsmechanismen zu unterlaufen.

Um ein internes Netz vor Missbrauch durch aktive Inhalte aus dem Internet zu schützen, sind mehrere Vorgehensweisen denkbar, die im Folgenden vorgestellt werden.

### Aktive Inhalte auf der Firewall herausfiltern

Dies ist die sicherste und deshalb empfohlene Methode für den Zugriff auf das Internet, da hiermit weiterhin die Firewall die Hauptkontrolle übernehmen kann. Um die Entgegennahme von aktiven Inhalten zu verhindern, wird auf dem Application Level Gateway (ALG) ein Proxy benötigt, der HTML-Seiten auf aktive Inhalte untersucht. Findet er diese, müssen sie aus der Seite herausgefiltert werden. Es gibt eine Reihe von ALGs, die diese Funktionalität bieten (siehe M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*).

Es muss allerdings davon ausgegangen werden, dass diese Lösung, obwohl sie die sicherste ist, in Zukunft eine immer geringere Akzeptanz finden wird, da die Anzahl der Web-Seiten zunimmt, die nicht sinnvoll genutzt werden können, wenn die aktiven Inhalte herausgefiltert wurden.

**Hinweis:** Auch in E-Mails können aktive Inhalte versteckt sein, daher sollten auch diese daraufhin überprüft werden.

Zu beachten ist bei diesem Ansatz weiterhin, dass aktive Inhalte auch aus TLS/SSL-verschlüsselten Datenströmen herausgefiltert werden müssen. TLS/SSL-verschlüsselte Datenströme müssen somit an der Netzgrenze, beispielsweise auf dem ALG, terminiert werden. Auch diese Funktionalität wird inzwischen von einer Reihe von Firewall-Produkten angeboten.

### Ausführung aktiver Inhalte im Browser deaktivieren

Bei zentral administrierten Arbeitsplatzrechnern ist es denkbar, die Rechte der einzelnen Benutzer so weit einzuschränken, dass diese die Sicherheitseinstellungen ihres Browsers nicht mehr ändern können. Diese könnten dann so konfiguriert werden, dass aktive Inhalte nicht ausgeführt werden. Hierbei kann dann auch auf dem Application Level Gateway auf die Filterung nach aktiven Inhalten verzichtet werden.

### Aktive Inhalte auf schädlichen Code prüfen

Analog zu klassischen Viren-Schutzprogrammen gibt es Schutz-Software, die aktive Inhalte daraufhin durchsucht, ob darin schädlicher Code enthalten ist.

Wenn die Software eine Gefahr erkennt, verweigert sie den Zugriff auf den verdächtigen Code. Die Schutz-Software zur Prüfung auf schädlichen Code kann Client-seitig oder an der Netzgrenze eingesetzt werden.

Zu beachten ist allerdings, dass dieser Ansatz keinen absoluten Schutz bietet, da es passieren kann, dass die Schutz-Software eine schädliche Web-Seite oder ein schädliches Element nicht als solches erkennt. Prinzipbedingt liegt die Erkennungsquote unter 100%. Wie bei klassischen Viren-Schutzprogrammen ist es wichtig, dass die Schutz-Software und deren Datenbanken regelmäßig aktualisiert werden.

**Aktive Inhalte in einer gesonderten Umgebung ausführen**

Es gibt mehrere technische Möglichkeiten, die Ausführung aktiver Inhalte in eine gesonderte, abgeschottete Umgebung zu verlagern, um das Risiko zu reduzieren.

- Terminal-Server: Der Browser wird vom Client auf einen hierfür bereitgestellten Terminal-Server verlagert, der sich in einem gesonderten Netzsegment befindet. Vom Client wird über ein Terminal-Server-Protokoll (VNC, RDP, ICA, X11 etc.) auf den Terminal-Server zugegriffen. Der Browser wird auf diese Weise ferngesteuert. Die Kommunikationsmöglichkeiten zwischen dem Terminal-Server und dem lokalen Netz werden durch entsprechende netztechnische Maßnahmen auf ein Minimum reduziert.
- Virtuelle IT-Systeme: Der Browser wird in ein gesondertes virtuelles IT-System verlagert, das vom Client aus genutzt werden kann. Die Kommunikationsmöglichkeiten zwischen dem virtuellen IT-System und dem Client sowie dem lokalen Netz werden durch Konfigurationsmaßnahmen auf ein Minimum reduziert. Diese Lösung kann auch komplett auf dem Client realisiert werden.
- Betriebssystemmechanismen: Einige Betriebssystem bieten, gegebenenfalls mit Zusatzkomponenten, erweiterte Möglichkeiten, verschiedene Prozesse gegeneinander abzuschotten. Beispiele hierfür sind SELinux und AppArmor. Auch diese Mechanismen können genutzt werden, um aktive Inhalte in einer gesonderten Umgebung auszuführen.

**Aktive Inhalte selektiv ausführen**

Es ist möglich, die Ausführung aktiver Inhalte auf bestimmte Web-Seiten zu beschränken oder den Benutzern zu erlauben, die Ausführung aktiver Inhalte im Browser selbst ein- und auszuschalten. Es gibt auch Plug-Ins, die das Ein- und Ausschalten für die Benutzer komfortabler machen. Allerdings ist diese Vorgehensweise in vielen Fällen nicht praxisgerecht.

Einige Arten von aktiven Inhalten, beispielsweise ActiveX-Elemente, können vom Herausgeber mit einer digitalen Signatur versehen werden. Eine verifizierte und gültige Signatur kann Aufschluss über die Herkunft eines Elementes geben. Eine verlässliche Aussage darüber, ob ein Element schädlichen Code enthält, lässt sich jedoch anhand der Signatur nicht treffen.

**Empfehlungen**

- Die Ausführung aktiver Inhalte sollte nur dann erlaubt werden, wenn dies für die jeweilige Fachaufgabe erforderlich ist.
- Plug-Ins, die der Ausführung aktiver Inhalte dienen, sollten nur installiert werden, wenn dies für die jeweilige Fachaufgabe erforderlich ist.
- Bevor aktive Inhalte ausgeführt werden, sollten sie (zentral oder lokal) durch aktuelle Schutz-Software auf schädlichen Code geprüft werden.
- Aktive Inhalte in Form von ActiveX sollten, wenn überhaupt, nur dann ausgeführt werden, wenn sie aus einer vertrauenswürdigen Quelle kommen,

d. h. wenn sie signiert sind, diese Signatur auch verifiziert wurde und der Signierer vertrauenswürdig ist.

Unter Abwägung der Risikolage und der fachlichen Anforderungen muss eine Entscheidung getroffen werden, wie mit aktiven Inhalten umgegangen wird. Es empfiehlt sich, diese Entscheidung zu dokumentieren.

Prüffragen:

- Bei zentraler Filterung von aktiven Inhalten: Sind SSL-basierte WWW-Zugriffe nicht erlaubt?
- Liegt eine abgestimmte Vorgehensweise zum Schutz gegen aktive Inhalte vor?

# M 5.70 Adreßumsetzung - NAT (Network Address Translation)

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Network Address Translation (NAT) ist ein Mechanismus, bei dem eine aktive Netzkomponente (in der Regel ein Router) bei der Weiterleitung eines Paketes die IP-Adresse des Paketes verändert. Der Router speichert in einer Tabelle die Zuordnung der internen Adresse und des internen Quell-Ports zur externen Adresse, Zielport und dem Port, den der Router selbst für das veränderte Paket gewählt hat und setzt die Antwortpakete entsprechend um.

NAT kann zu verschiedenen Zwecken verwendet werden:

- NAT kann verhindern, dass anhand der IP-Adressen im lokalen Netz auf dessen Struktur rückgeschlossen wird, denn vom externen Netz aus ist nur die IP-Adresse des NAT-Gateways sichtbar. Dies verhindert gleichzeitig, dass Angreifer von außen direkt einzelne Rechner im internen Netz attackieren können.
- Im lokalen Netz werden oft mehr IP-Adressen benötigt, als offiziell registriert sind. Bei Verwendung eines NAT-Gateways wird für jedes Netz nur eine einzige offizielle IP-Adresse zwingend benötigt, die internen Adressen können beliebig gewählt werden.
  Beim Aufbau eines internen Netzes sollten interne Adressen unbedingt nur aus den Bereichen gewählt werden, die offiziell für solche Zwecke vorgesehen sind (siehe RFC 1918 - *Address Allocation for Private Internets*). Diese Bereiche sind:

  - 10.0.0.0 - 10.255.255.255 (8-Bit Netzmaske)
  - 172.16.0.0 - 172.31.255.255 (12-Bit Netzmaske)
  - 192.168.0.0 - 192.168.255.255 (16-Bit Netzmaske)

  Diese Adressen werden im "allgemeinen Internet" nicht geroutet und müssen daher am Gateway zum Internet in eine offiziell zugeteilte IP-Adresse umgesetzt werden.
- Gelegentlich wurden beim Aufbau eines internen Netzes einfach beliebige IP-Adressen verwendet. Beim Anschluss eines solchen Netzes an das Internet können diese bisher verwendeten IP-Adressen dann oft nicht benutzt werden, da der betreffende Adressbereich an andere Institutionen vergeben wurde. Um nicht alle Rechner neu konfigurieren zu müssen, kann eine Adressumsetzung von den internen zu den offiziell registrierten externen Adressen sinnvoll sein. Allerdings werden in diesem Fall oft Probleme bei der Namensauflösung eintreten und die Rechner, denen die intern verwendeten Adressen im Internet zugeordnet sind, werden aus dem internen Netz nicht erreichbar sein.
  Auch bei einem Wechsel des Internet-Providers kann dieser Fall eintreten.
- Beim Zusammenschluss zweier Netze, bei denen IP-Adressen aus den Bereichen des RFC-1918 gewählt wurden, kann ebenfalls eine Adressumsetzung notwendig werden, wenn in beiden Netzen dieselben Adressen verwendet wurden.

Eine Umsetzung der internen in eine oder mehrere offiziell registrierte IP-Adressen und umgekehrt erfolgt über eine Adressumsetzungskomponente. Auch Proxies verfügen über eine implizite Adressumsetzung, da der Proxy extern nur seine offizielle Adresse verwendet und die Datenpakete an die jeweiligen internen Rechner weiterleitet.

Eine Adressumsetzung durch Router oder dedizierte Paketfilter kann entweder statisch oder dynamisch geschehen. Die statische Adressumsetzung ist einfach und schnell. Es wird jeder internen Adresse genau eine externe zugeordnet. Hierzu wird natürlich für jede interne Adresse genau eine externe benötigt.

Häufiger findet die dynamische Adressumsetzung Verwendung, insbesondere wenn die Anzahl der internen IP-Adressen größer ist als die der extern sichtbaren ist sie Voraussetzung. Im Router oder Paketfilter wird eine Zuordnungstabelle geführt, in der die internen Adressen mit dazugehöriger Portnummer eines Pakets einer externen Adresse mit neuer Portnummer zugeordnet wird. Häufig wird nach außen hin nur eine IP-Adresse sichtbar gemacht, die über die Portnummer-Zuordnung alle internen IP-Adressen verbirgt.

Eine Folge der dynamischen Adressumsetzung ist, dass ein Verbindungsaufbau zu einem internen Rechner aus dem Internet normalerweise nicht möglich ist. Soll dies doch möglich sein, so muss das Sicherheitsgateway "Destination NAT" bzw. "Port Forwarding" beherrschen (siehe unten).

Bestimmte Dienste müssen bei Adressumsetzung besonders behandelt werden (z. B. traceroute oder ftp).

**Zugriff von außen bei NAT**

Für einen Verbindungsaufbau von außen (z. B. bei Anfragen an einen Web-Server) werden am NAT-Gateway alle Pakete, die an einen bestimmten Port gerichtet sind, umgesetzt und an einen entsprechenden Port des Servers weitergeleitet. Dieser Mechanismus wird auch als "Destination NAT" oder "Port-Forwarding" bezeichnet. Mit den Antwortpaketen des Servers verfährt das NAT-Gateway analog.

Prüffragen:

- Entsprechen die für das interne Netz vergebenen internen Adressen dem RFC 1918 Standard?
- Ist der Einsatz von NAT mit den Sicherheitsrichtlinien der Organisation abgestimmt?
- Entspricht das eingesetzte Portforwarding den Sicherheitsbestimmungen der Organisation?

# M 5.71 Intrusion Detection und Intrusion Response Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Eine der wesentlichen Aufgaben eines Firewall-Administrators ist es, die anfallenden Protokolldaten zu analysieren, um dadurch Angriffe zeitnah erkennen zu können. Aufgrund der Fülle der Daten und der Vielzahl und Komplexität der verschiedenen Angriffsmöglichkeiten entsteht dadurch ein beträchtlicher Arbeitsaufwand. Intrusion Detection (ID) und Intrusion Response (IR) Systeme können hierbei helfen.

Ziel eines ID-Systems muss es sein, einen durchschnittlichen Administrator soweit zu unterstützen, dass dieser auch ohne tief greifende Kenntnisse im Bereich Internet-Sicherheit in der Lage ist, einen Angriff in einer großen Anzahl von Protokolldaten zu erkennen. IR-Systeme dagegen dienen dazu, automatisch Gegenmaßnahmen einzuleiten, sobald ein Angriff erkannt wurde.

Im Idealfall verfügen diese Programme über ebenso viel Informationen wie ein guter Administrator und sind daher in der Lage, in beliebigen Protokolldaten nicht nur einen Angriff zu erkennen, sondern auch noch Aussagen über die Stärke der Bedrohung und die notwendigen Gegenmaßnahmen zu machen. Zurzeit ist dies allerdings noch ein Gebiet, welches intensiv erforscht wird, sodass wesentliche Verbesserungen an den vorhandenen Programmen jederzeit möglich sind.

Intrusion Detection Systeme lassen sich im wesentlichen in zwei Klassen einteilen: Signaturanalyse und Anomalie-Erkennung.

Die Signaturanalyse beruht auf der Annahme, dass sich viele Angriffe anhand einer bestimmten Abfolge von Protokolldaten erkennen lassen. Ein Beispiel ist das so genannte Portscanning. Als Vorarbeit für einen Angriff wird zunächst festgestellt, welche Dienste auf dem angegriffenen Rechner ansprechbar sind, d. h. zu welchen TCP-Ports eine Verbindung aufgebaut werden kann. Hierzu wird mithilfe eines Programms ein Verbindungsaufbaupaket nacheinander an alle TCP-Ports geschickt. Erfolgt ein Verbindungsaufbau, ist dort ein Dienst installiert und kann angegriffen werden. Die entsprechende Signatur, also Erkennungsmerkmal, dieses Angriffs ist einfach: Verbindungsaufbaupakete, die nacheinander an alle TCP-Ports geschickt werden.

Es zeigen sich aber auch sofort die Probleme bei dieser Art der Angriffserkennung: In welcher Reihenfolge müssen die Ports angesprochen werden und in welchen zeitlichen Abständen, damit ein Angriff von einem normalen Betrieb unterschieden werden kann? Aktuelle Portscanning-Programme arbeiten so, dass nicht nacheinander Port-1, Port-2 bis Port n angesprochen werden, sondern dies in zufälliger Reihenfolge erfolgt. Auch können die Pakete nicht direkt nacheinander verschickt werden, sondern in zufälligen Zeitabständen (z. B. 1 s, 100 ms, 333 ms, 5 s ...). Dies macht die Erstellung einer Signatur schwierig.

Eine subtile Variante des Portscanning besteht darin, einzelne Pakete von verschiedenen Quelladressen zu senden. In Verbindung mit der oben aufgezeigten zeitlich versetzten Initiierung der Pakete ist die Wahrscheinlichkeit gegenwärtig sehr hoch, dass ein solcher Angriff unerkannt bleibt.

Bei der Anomalie-Erkennung geht man andererseits davon aus, dass sich das normale Verhalten der Benutzer oder Rechner statistisch erfassen lässt und wertet Abweichungen hiervon als Angriff. Ein Beispiel hierfür ist der Zeitraum, in dem eine Benutzerin normalerweise an ihrem Rechner angemeldet ist. Arbeitet sie z. B. fast immer montags bis freitags in der Zeit von 8.00 Uhr bis 17.00 Uhr mit Abweichungen von maximal 2 Stunden, so kann eine Aktivität am Samstag oder um 24.00 Uhr als Angriff gewertet werden. Das Problem bei der Anomalie-Erkennung ist die Festlegung des normalen Verhaltens. Hierfür lassen sich zwar mit Hilfe von Schwellwerten oder Wahrscheinlichkeitsbetrachtungen einige Aussagen machen. Ob es sinnvoll ist, eine Aktivität des Benutzers A am Montag um 19.10 Uhr sofort als Angriff zu bewerten, erscheint fraglich. Auch ändert sich das normale Verhalten eines Benutzers in Regel, sodass eine Anpassung vorgenommen werden muss. Wer aber sagt dem ID-System, dass diese Verhaltensänderung regulär ist und kein Angriff?

Des Weiteren ist eine Unterteilung der ID-Systeme nach der Art der Datenaufnahme sinnvoll. Diese kann entweder mithilfe eines dedizierten Sniffers irgendwo im Netz erfolgen (Netzbasiertes ID-System), oder Teil der normalen Protokollierungsfunktionalität auf einem der angeschlossenen Rechner (Hostbasierte ID-Systeme) sein. Beides hat Vor- und Nachteile. Die netzbasierten Systeme haben zwar die Möglichkeit, einen umfassenden Angriff, der gleichzeitig verschiedene Rechner betrifft, leichter zu erkennen. Es ist aber erheblich schwieriger, komplexe Angriffe (z. B. über weitere Zwischenstationen) auf einen Rechner zu erkennen. Darüber hinaus können netzbasierte Systeme keine verschlüsselten Daten analysieren. Für die hostbasierten ID-Systeme gilt andererseits, dass für ihren Einsatz u. U. umfangreiche Änderungen an den Protokollierungsfunktionen der Rechner notwendig sind.

Da auch bei der automatischen Auswertung von Protokollinformationen die Datenschutzbestimmungen oder Personalvereinbarungen beachtet werden müssen, kann es unter Umständen notwendig werden, diese Daten pseudonymisiert abzulegen.

Vor der Kopplung von ID-, IR-System und Firewall sollten folgende Aspekte beachtet werden:

- Ist es möglich, gezielt einen Angriff auf die Firewall zu initiieren, der vom ID-System irrtümlich als echter Angriff gewertet wird? Eine daraufhin vom IR-System ausgelöste Sperrung bestimmter Dienste über die Firewall kann erhebliche Konsequenzen auf die Verfügbarkeit haben.
- Die Interaktion zwischen ID-, IR-System und Firewall sollte hinreichend transparent dokumentiert sein. Nur so ist es möglich, zu jedem Zeitpunkt abzuschätzen, von wem die Firewall administriert wird: vom IR-System oder vom Administrationspersonal. Im Zweifelsfall sollten Entscheidungen des Administrationspersonals Vorrang haben.

Um Angriffe gegen ein ID-System selbst auszuschließen, sollten diese vom Netz her weitestgehend unsichtbar sein. Einfachste Maßnahme ist die Zuweisung einer IP-Adresse, die im Internet nicht geroutet wird. Empfohlen sei weiterhin die Deaktivierung des Protokolls ARP für das entsprechende Interface, sodass weder auf ARP- noch auf IP-Pakete reagiert wird.

Prüffragen:

- Erfolgt Einbruchserkennung und Einbruchsabwehr mittels Intrusion Detection oder Intrusion Response Systemen?

# M 5.72 Deaktivieren nicht benötigter Netzdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um auf einem Unix-System alle nicht benötigten Netz-Dienste zu deaktivieren, ist folgendermaßen vorzugehen:

Für den Start von Netzdiensten gibt es unter Unix zwei Möglichkeiten: über den Serverdienst *inetd*, der in der Datei */etc/inetd.conf* konfiguriert wird, und über die Startup-Dateien, die sich in */etc/rc.d/init.d* bzw. */etc/init.d* befinden. Zum Abschalten nicht benötigter Dienste in der Datei */etc/inetd.conf* muss die jeweilige Zeile mit # auskommentiert werden. Bei einer Standardinstallation sind in der Regel mehr Dienste konfiguriert als nötig sind. Darunter befinden sich immer wieder Dienste, die eine Gefährdung darstellen können. Daher sollten so wenig Dienste wie möglich freigeschaltet werden, also nur die Dienste, die auf dem jeweiligen System unabdingbar benötigt werden (siehe auch M 4.95 *Minimales Betriebssystem* und M 4.97 *Ein Dienst pro Server*).

Die Dienste, die durch die Startup-Dateien initiiert werden, werden über Links aus den Unterverzeichnissen */etc/rc**X**.d* oder */etc/rc.d/rc**X**.d* referenziert, wobei ***X*** für das jeweilige Unix-Runlevel steht, in dem die Startup-Datei aufgerufen wird. Zum Deaktivieren der nicht benötigten Dienste können die nicht benötigten Dienste in ein Unterverzeichnis verschoben werden, damit man sie bei Bedarf wieder aktivieren kann. Dies kann z. B. wie folgt aussehen:

*cd rc3.d; mkdir .s; mv S85sendmail .s/*

Die aktuell aktiven Dienste können mit dem Befehl *netstat -a* identifiziert werden.

Prüffragen:

- Sind nur die Netzdienste freigeschaltet, die auf dem System unabdingbar benötigt werden?

# M 5.73 Sicherer Betrieb eines Faxservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fax-Poststelle

Der sichere Betrieb eines Faxservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Eingehende Faxsendungen nimmt der Faxserver von anderen Faxservern oder Faxgeräten entgegen und leitet sie, wenn die Funktion des automatischen Fax-Routing aktiviert ist, an die angeschlossenen Benutzer weiter. Ausgehende Faxsendungen der angeschlossenen Benutzer werden vom Faxserver entgegengenommen und an den Empfänger weitergeleitet. Der Faxserver muss zudem sicherstellen, dass lokale Faxsendungen, d. h. Faxsendungen von einem Arbeitsplatz zu einem anderen innerhalb der gleichen Organisation(seinheit), nur intern und nicht über das öffentliche Netz weitergeleitet werden.

Zum sicheren Betrieb eines Faxservers ist es u. a. erforderlich, dass nach der Beschaffung und Installation die Konfiguration des Betriebssystems und der Faxserver-Applikation ausgiebig getestet wird. Auf evtl. auftretende Fehlermeldungen ist - soweit dies möglich ist - mit Änderungen an der Konfiguration zu reagieren. An die Testphase sollte sich ein Pilotversuch anschließen. Erst wenn der Faxserver auch in dieser Phase fehlerfrei arbeitet, sollte die Freigabe für den Wirkbetrieb erfolgen. Die Konfigurationsparameter sollten, ebenso wie alle Änderungen an der Konfiguration, sorgfältig dokumentiert werden.

Faxserver speichern alle eingehenden und ausgehenden Faxsendungen. Die Dauer der Speicherung hängt von den Leistungsmerkmalen der Faxserver-Applikation und der Konfiguration ab. So ist es z. B. möglich, dass ausgehende Faxsendungen nur bis zur Erledigung des Sendeauftrages zwischengespeichert und dann gelöscht werden. Ebenso kann es sein, dass eingehende Faxsendungen nur bis zur Weiterleitung an den Empfänger zwischengespeichert werden und anschließend die Löschung erfolgt. Denkbar ist aber auch, dass grundsätzlich alle ein- und ausgehenden Faxsendungen auf dem Faxserver solange gespeichert werden, bis die Löschung durch den jeweiligen Benutzer oder durch die Fax-Poststelle bzw. den Administrator erfolgt. Die Löschung kann bei einigen Faxservern auch automatisch nach einer gewissen Zeitspanne erfolgen. So können z. B. alle Faxsendungen, die älter als 3 Monate sind, automatisch gelöscht werden. In Abhängigkeit vom Einsatzkonzept sind Regelungen für die Löschung von Faxdaten auf dem Faxserver zu treffen. Gleichzeitig ist zu regeln, wo und in welchem Umfang eine Archivierung von Faxdaten zu erfolgen hat. Generell sollten Faxdaten nicht länger als unbedingt nötig auf dem Faxserver verbleiben.

Es muss ausgeschlossen werden, dass Unbefugte auf Faxsendungen zugreifen können. Daher muss zunächst der Faxserver physikalisch gegen unbefugten Zugriff gesichert werden. Dies kann nur durch die gesicherte Aufstellung des Servers in einem Serverraum oder einem Serverschrank erfolgen (siehe Baustein B 2.4 *Serverraum* und Baustein B 2.7 *Schutzschränke*).

Um den störungsfreien Betrieb des Faxservers sicherzustellen, ist zudem festzulegen, wer für die Administration der Hardware-Komponenten, des Betriebssystems und der Faxserver-Applikation zuständig ist. Es sollte eine Fax-Poststelle eingerichtet werden (siehe auch M 2.180 *Einrichten einer Fax-Poststelle*). Das Administrationspersonal und das in der Fax-Poststelle eingesetz-

te Personal sind im Umgang mit dem Betriebssystem und der Faxserver-Applikation zu schulen. Um Störungen des Betriebs durch Fehlbedienungen zu vermeiden, sind weiterhin auch die Benutzer im Umgang mit der Faxclient-Applikation zu schulen.

Auf Faxservern können oftmals an Benutzer und Benutzergruppen folgende Berechtigungen für eingehende Faxsendungen vergeben werden:

- lesen,
- weiterleiten,
- löschen.

Für ausgehende Faxsendungen können oftmals folgende Rechte vergeben werden:

- senden,
- anhalten,
- löschen,
- ändern der Sendeoptionen.

Die Berechtigungen sind gemäß den Festlegungen in der Faxsicherheitsleitlinie zu vergeben (siehe auch M 2.178 *Erstellung einer Sicherheitsleitlinie für die Faxnutzung*).

Sofern nicht durch technische Maßnahmen sichergestellt wird, dass Faxsendungen sofort weitergeleitet werden, ist zudem durch die Vergabe entsprechender Zugriffsrechte sicherzustellen, dass nur berechtigte Benutzer auf die entsprechenden "Postfächer" auf dem Server zugreifen können.

Generell sollte ein Zugriff auf temporäre Bereiche, in denen die Faxserver-Applikation Faxsendungen vor Abgang bzw. vor Verteilung an den Empfänger zwischenspeichert, nur privilegierten Benutzern (Administratoren, Fax-Poststelle) vorbehalten bleiben.

Regelmäßig sind die Verbindungen des Faxservers mit der Telekommunikationsanlage bzw. mit dem öffentlichen Telefonnetz auf Funktion zu überprüfen. Sofern der Faxserver mit internen Kommunikationssystemen, wie z. B. einem E-Mail-System oder einem Workflow-System, zusammenarbeitet, ist ebenfalls regelmäßig die Funktion dieser Verbindungen zu überprüfen.

Außerdem muss regelmäßig geprüft werden, ob der für die Speicherung von Faxsendungen zur Verfügung stehende Festplattenplatz noch ausreichend ist (siehe auch M 5.75 *Schutz vor Überlastung des Faxservers*). Bei erschöpftem Festplattenplatz können keine weiteren Faxsendungen mehr empfangen oder versandt werden.

Die Aktivitäten des Faxservers sind gemäß den Festlegungen in der Faxsicherheitsleitlinie zu protokollieren und die Protokolle sind regelmäßig zu kontrollieren (siehe auch M 2.64 *Kontrolle der Protokolldateien* und M 5.25 *Nutzung von Sende- und Empfangsprotokollen*). Bei der Festlegung von Umfang und Inhalt der Protokollierung ist auf eine frühzeitige Beteiligung des Personal- bzw. Betriebsrates zu achten.

Vorbehalte gegen den Einsatz eines Faxservers bestehen häufig aufgrund der Tatsache, dass dabei ein IT-System, das in das LAN integriert ist, über das öffentliche Telekommunikationsnetz erreicht werden kann.

Durch sorgfältige Auswahl und Konfiguration von Kommunikationskarten, Betriebssystem und Faxserver-Applikation sowie durch eine sichere netztopolo-

gische Anordnung des Servers kann die Gefahr eines Einbruchs in das Netz bzw. in den Faxserver bis auf ein geringes Restrisiko minimiert werden.

Beim Einsatz von aktiven ISDN-Karten sollten Leistungsmerkmale, die nicht zum Empfang und Senden von Faxen notwendig sind, deaktivert werden (siehe M 4.59 *Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten*).

Sofern dedizierte Faxkarten zum Einsatz kommen, sind auch zunächst die entsprechenden Leistungsmerkmale genau zu untersuchen. Auch hier gilt, dass nicht benötigte Merkmale - soweit dies möglich ist - abzuschalten sind.

Der Faxserver sollte keine anderen Dienste als den Fax-Dienst anbieten. Insbesondere sollte ein Faxserver nicht gleichzeitig als Daten-, Drucker-, E-Mail- oder Internet-Server bzw. als Remote-Access-Rechner verwendet werden. Um einem Einbruch über das Telekommunikationsnetz entgegenzuwirken, muss das Betriebssystem so "schlank" wie möglich installiert werden. Dies bedeutet, dass auf die Installation von für den Betrieb nicht zwingend notwendigen Diensten und Protokollen verzichtet wird. Hierzu ein Beispiel: Wenn auf einem Faxserver der Telnet-Dienst nicht gestartet ist, kann auch kein entsprechender Angriff zum Erfolg führen. Bei der Festlegung der benötigten Dienste und Protokolle darf nie vergessen werden, dass Gefährdungen häufig erst durch die Kombination von verschiedenen Diensten und Protokollen entstehen.

Die sichere netztopologische Anordnung des Faxservers ist unter anderem davon abhängig, ob und ggf. welche Art von Firewall in der Organisation im Einsatz ist.

Ein Faxserver hat jeweils mindestens eine Schnittstelle zum Telekommunikationsnetz und zum LAN. Die Anordnung des Faxservers im Netz sollte so erfolgen, dass im Falle eines erfolgreichen Angriffs auf den Faxserver nicht in das gesamte Netz eingebrochen werden kann. Andererseits sollte es auch nicht möglich sein, den Faxserver von innerhalb des Netzes aus erfolgreich zu attackieren. Denkbar wäre hier z. B. ein Angriff eines Außentäters aus dem Internet. Gelingt solch ein Angriff, so ist der Täter in der Lage, über den Faxserver der angegriffenen Organisation das Versenden von Faxen zu veranlassen. Dies kostet Gebühren und, was ggf. noch schlimmer ist, führt unter Umständen zu Ansehensverlust. Auch ist ein Angreifer im Falle eines erfolgreichen Angriffs in der Lage, unbefugt Kenntnis von den auf dem Faxserver (zwischen-) gespeicherten Faxsendungen zu nehmen. Angriffe eines Innentäters über das LAN sind in vergleichbarer Weise denkbar.

Da ein Faxserver meistens nicht die einzige IT-Komponente mit Anschluss an ein externes Netz ist, ist in der Regel zum Schutz des internen Netzes ohnehin eine Abschottung gegenüber externen Netzen vorhanden (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Sofern als Internet-Firewall ein Screened Subnet (Konfiguration 1 aus M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*) vorhanden ist, sollte der Faxserver zwischen dem inneren Paketfilter und dem Application Gateway (siehe Abbildung "Einbindung eines Faxservers in ein Firewall-System") eingebunden werden. Die Schutzwirkung gegenüber Angriffen aus dem unsicheren Netz ist durch den Application Gateway und den äußeren Paketfilter hinreichend groß. Gegen Angriffe aus dem internen Netz wird der Faxserver durch den inneren Paketfilter geschützt.

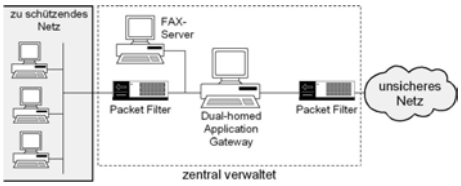



Abbildung: Einbindung eines Faxservers in ein Firewall-System

Bei allen anderen Firewall-Kombinationen, insbesondere solchen mit nur einem Paketfilter, oder wenn bisher keine Firewall vorhanden ist, sollte der Faxserver direkt in das sichere Netz eingebunden werden. Sofern das entstehende Restrisiko aufgrund des Schutzbedarfs als nicht tragbar angesehen wird, muss entweder eine Absicherung mittels eigenem Paketfilter erfolgen, oder die Telekommunikationsanlage muss so konfiguriert werden, dass nur abgehende Verbindungen zulässig sind. Für eingehende Faxsendungen muss in diesem Fall ein herkömmliches Faxgerät oder ein Stand-alone-System mit entsprechender Faxapplikation eingesetzt werden, mit der Folge, dass eingehende Faxsendungen nur manuell an die Empfänger verteilt werden können.

Prüffragen:

- Erfolgt die Freigabe für den Wirkbetrieb von Faxservern erst nach einem fehlerfreien Testbetrieb?
- Werden die Konfigurationsparameter sowie alle Änderungen an der Konfiguration des Faxservers dokumentiert?
- Ist die Archivierung von Faxdaten der Faxserver geregelt?
- Ist die Löschung von Faxdaten auf Faxservern geregelt?
- Sind die zuständigen Administratoren der Hardware-Komponenten, des Betriebssystems und der Faxserver-Applikation benannt?
- Sind die Adminstratoren und das in der Fax-Poststelle eingesetzte Personal für die Bedienung der Faxserver-Umgebung geschult?
- Sind die Benutzer im Umgang mit der Faxclient-Applikation geschult?
- Erfolgt die Vergabe von Berechtigungen auf Faxservern gemäß den Festlegungen in der Faxsicherheitsleitlinie?
- Ist sichergestellt, dass ausschließlich berechtigte Benutzer auf die entsprechenden Postfächer von Faxserver zugreifen können?
- Werden die Verbindungen von Faxservern mit der TK-Anlage beziehungsweise dem öffentlichen Telefonnetz regelmäßig auf ihre Funktion überprüft?
- Erfolgt eine regelmäßige Prüfung des freien Festplattenplatzes von Faxservern?
- Werden bei der Festlegung von Umfang und Inhalt der Protokollierung von Faxservern der Personal- bzw. Betriebsrat beteiligt?
- Einsatz von aktiven ISDN-Karten: Sind alle nicht benötigten Leistungsmerkmale der ISDN-Karten deaktiviert?
- Ist sichergestellt, dass der Faxserver ausschließlich den Fax-Dienst anbietet und nicht für weitere zusätzliche Dienste genutzt wird?
- Ist der Faxserver innerhalb des Netzes so angeordnet, dass im Falle eines erfolgreichen Angriffs auf den Faxserver nicht in das gesamte Netz eingebrochen werden kann?

# M 5.74 Pflege der Faxserver-Adressbücher und der Verteillisten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fax-Poststelle

Die meisten Faxserver bieten sowohl zentrale als auch individuelle Adressbücher an. Zentrale Adressbücher stehen allen Benutzern eines Faxservers zur Verfügung und sollten zentral durch die Fax-Poststelle gepflegt werden. Individuelle Adressbücher können von jedem Benutzer erstellt werden, stehen aber in der Regel auch nur dem Ersteller zur Verfügung.

In besonderem Maße sind die zentralen Adressbücher gegen unbefugte Veränderung zu schützen. Dazu sind entweder über die Faxserver-Applikation oder - sofern dies nicht möglich ist - mit Mitteln des Betriebssystems die Berechtigungen so zu vergeben, dass nur die Fax-Poststelle die zentralen Adressbücher verändern kann.

Regelmäßig sollte durch die Fax-Poststelle die Integrität und Aktualität der zentralen Adressbücher überprüft werden. Die meisten Faxserver lassen es zu, mehrere Empfänger in den Adressbüchern zu Gruppen zusammenzufassen. Sofern es einem Angreifer gelingt, solche Gruppen zu manipulieren, können er oder andere Unbefugte Kenntnis von vertraulichen Faxsendungen erhalten. Die Fax-Poststelle sollte daher auch die Zuordnung von Empfängern zu den einzelnen Gruppen regelmäßig auf Aktualität überprüfen. Sofern in einer Organisation zwischen den Arbeitsplätzen Daten über den Faxserver per Fax ausgetauscht werden, müssen durch die Fax-Poststelle auch interne Adressbücher aktuell gehalten werden.

Außerdem sind die Benutzer zur regelmäßigen Kontrolle der von ihnen benutzten Einträge zu verpflichten. Dies gilt sowohl für zentrale als auch für individuelle Adressbücher.

Durch den Faxserver werden Verteillisten dazu benutzt, um eingehende Faxsendungen an die Empfänger weiterzuleiten. Falsche Zuordnungen in den Verteillisten können dazu führen, dass Unbefugte Kenntnis von Faxsendungen mit vertraulichem Inhalt erhalten. Die Verteillisten sollten daher von der Fax-Poststelle regelmäßig auf Aktualität und Integrität überprüft werden.

Um die Pflege von Adressbüchern und Verteillisten zu gewährleisten, muss die Fax-Poststelle über das Ausscheiden von Mitarbeitern informiert werden.

Damit durchgeführte Administrationsarbeiten nachvollzogen werden können, sollten die Eintragungen und Veränderungen an den zentralen Adressbüchern und an den Verteillisten dokumentiert werden.

Prüffragen:

- Werden die zentralen Faxserver-Adressbücher gegen unbefugte Veränderungen geschützt?
- Wird die Integrität und Aktualität der zentralen Faxserver-Adressbücher und Verteilerlisten regelmäßig überprüft?
- Ist gewährleistet, dass zur Pflege der Adressbücher und Verteilerlisten die Fax-Poststelle über das Ausscheiden von Mitarbeitern informiert wird?

- Werden Eintragungen und Veränderungen an den zentralen Faxserver-Adressbüchern und Verteilerlisten nachvollziehbar dokumentiert?

# M 5.75 Schutz vor Überlastung des Faxservers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fax-Poststelle

Ein Faxserver kann sowohl durch eingehende als auch durch ausgehende Faxsendungen überlastet werden. Eine Überlastung des Faxservers kann dazu führen, dass zeitweilig keine weiteren Faxsendungen mehr empfangen oder versandt werden können. Es ist auch denkbar, dass im Falle der Überlastung das Betriebssystem oder die Faxserver-Applikation abstürzt und der Faxserver vorübergehend gar nicht mehr verfügbar ist.

Eine Art der Überlastung des Faxservers liegt vor, wenn alle Kanäle, die durch die Kommunikationskarten bereitgestellt werden, durch eingehende und ausgehende Faxsendungen blockiert werden. Folge ist, dass weitere Faxe erst dann wieder empfangen oder gesendet werden können, wenn ein Kanal frei wird. Dieser Effekt tritt auch auf, wenn alle von der Telekommunikationsgesellschaft zur Verfügung gestellten Leitungen durch eingehende und ausgehende Faxsendungen belegt werden.

Vor der Beschaffung eines oder mehrerer Faxserver ist zunächst das voraussichtliche Faxvolumen abzuschätzen. Sodann sind ausreichend leistungsfähige Komponenten zu beschaffen. Außerdem sollte darauf geachtet werden, dass genügend Telekommunikationsleitungen zur Verfügung stehen.

Außerdem sollten die Protokolle des Faxservers regelmäßig kontrolliert werden, um feststellen zu können, ob der Server zu bestimmten Zeiten überlastet oder die Grenze der Belastbarkeit erreicht wird.

Eine Überlastung des Faxservers kann dadurch erfolgen, dass intern versucht wird, eine große Anzahl von Faxen zu versenden. Unter ungünstigen Umständen kann dies zum Absturz der Faxserver-Applikation oder des Betriebssystems führen. Auslöser kann z. B. eine sehr große Anzahl von Serienfax-Sendungen sein. Es sollte daher schon in der Test- oder in der Pilotierungsphase versucht werden, die Belastungsgrenze zu ermitteln. Um diese Belastungsgrenze nicht zu überschreiten, sollte den Benutzern z. B. mittels geeigneter Dienstanweisung der maximale Umfang einer Serien-Faxsendung vorgegeben werden. Umfangreiche Serien-Faxsendungen sind dann auf mehrere Sendungen aufzuteilen. Zu Zeiten hoher Belastung des Faxservers sollte durch eine entsprechende Dienstanweisung oder durch eine entsprechende Vergabe von Berechtigungen am Faxserver sichergestellt werden, dass Faxe nur in dringenden Fällen gesendet werden. Sinnvoll kann auch die Vorgabe sein, Faxe möglichst nur zeitversetzt in der Nacht zu senden, was zudem noch Gebühren spart.

Wenn festgestellt wird, dass der Faxserver immer durch die gleichen Senderrufnummern mittels einer entsprechenden Anzahl von Faxsendungen zu ganz bestimmten Zeiten blockiert wird, ist zunächst zu ermitteln, wer die Absender sind und um welche Art von Faxsendungen es sich handelt. Sofern die Faxsendungen von der Organisation benötigt werden, kann versucht werden, mit den Absendern Zeiten auszuhandeln, in denen problemlos Faxsendungen entgegengenommen werden können. Sofern die Faxsendungen nicht benötigt werden (z. B. nicht angeforderte Werbe-Faxsendungen), kann versucht werden, die Absenderrufnummern über die Faxserver-Applikation oder über die Telekommunikationsanlage zu sperren. Dies ist aber nur möglich, sofern

die Absenderkennung (CSID = Caller Sender Identification) nicht verschleiert bzw. bei Verwendung von ISDN die Rufnummernübermittlung seitens des Absenders nicht unterdrückt wurde. Sofern die Faxnummer des Absenders nicht zu ermitteln sind, bleibt nur noch die Möglichkeit, die vorhandenen Kapazitäten - wie oben beschrieben - zu erweitern.

Problematisch kann auch die Festplattenkapazität eines Faxservers sein. Dabei ist die Gefahr, die Festplattenkapazität durch einen Angriff von außen gezielt zu erschöpfen, eher gering. Eine gefaxte DIN A4 Seite ist ca. 70 kB groß. Geht man von heute üblichen Festplattengrößen von mehreren Gigabyte aus, so ist auch angesichts der anfallenden Gebühren ein entsprechender Angriff eher unwahrscheinlich. Grundsätzlich werden alle eingehenden und ausgehenden Faxsendungen auf der Festplatte des Faxservers (zwischen-) gespeichert. Der weitere Ablauf hängt dann von der Faxserver-Applikation und ggf. auch von der Konfiguration ab. So ist z. B. denkbar, dass alle Faxsendungen dauerhaft auf der Festplatte des Faxservers gespeichert bzw. archiviert werden. Bei dieser Betriebsart kann - abhängig vom Faxvolumen - sehr schnell die Festplattenkapazität erschöpft werden. Es sollte in diesem Fall sichergestellt werden, dass Ausgangs-Faxsendungen und bereits gelesene Eingangs-Faxsendungen möglichst zeitnah auf externe Datenträger archiviert und auf dem Faxserver gelöscht werden. Dazu sollte der den Benutzern auf dem Faxserver zur Verfügung gestellte Speicherplatz begrenzt werden. Außerdem sollte z. B. durch Dienstanweisung sichergestellt werden, dass Faxsendungen, die nicht mehr benötigt werden, zu löschen sind. Dies gilt insbesondere für unverlangt erhaltene Werbe-Faxsendungen. Durch die Fax-Poststelle ist regelmäßig der freie Speicherplatz auf der Festplatte des Faxservers zu überprüfen.

Prüffragen:

- Werden vor Beschaffung eines Faxservers das voraussichtliche Faxvolumen abgeschätzt und entsprechend leistungsfähige Komponenten ausgewählt?
- Werden die Protokolle von Fax-Servern regelmäßig kontrolliert, um Engpässen durch Überbelastungen rechtzeitig entgegenwirken zu können?
- Werden nicht mehr benötigte Faxdaten zeitnah vom Faxserver gelöscht?

# M 5.76 Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

### Absicherung der Datenverbindung

Wird über ein Virtual Private Network (VPN) auf ein LAN zugegriffen, so erfolgt der Zugriff typischerweise über eine externe Datenverbindung. So wird beispielsweise bei einer direkten Einwahl (Direct Dial-In) das Netz eines Telekommunikationsanbieters benutzt. Wird die Verbindung über das Internet aufgebaut, werden die Daten über die Netze der beteiligten Internetdienstanbieter (und eventuell deren Kooperationspartner) geleitet. Da über eine VPN-Verbindung die direkte Anbindung an ein LAN erfolgt, muss der zur Datenübertragung benutzte Netzpfad so abgesichert werden, dass die Vertraulichkeit, Integrität und Authentizität gewährleistet ist. Die Absicherung wird durch das Verschlüsseln und gegebenenfalls Signieren der ausgetauschten Datenpakete erreicht, nachdem die Kommunikationspartner authentisiert wurden (siehe auch M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*). Im VPN-Umfeld haben sich verschiedene Verfahren und Mechanismen zur Absicherung der Kommunikationsverbindung herausgebildet, wie beispielsweise das Tunneling.

Die Wahl des Verfahrens, das zur Absicherung einer VPN-Verbindung zu benutzen ist, kann unter anderem von folgenden Faktoren beeinflusst werden:

- von den Sicherheitsanforderungen an die Stärke der Verfahren (hierdurch werden beispielsweise die Schlüssellängen bestimmt),
- von den auf Protokollebene einsetzbaren Verfahren,
- von den durch die VPN-Hardware und -Software unterstützten Verfahren.

Generell gilt:

- Ein VPN-Produkt bietet in der Regel eine Auswahl von unterstützten Standardverfahren zur Kommunikationsabsicherung an. Hier sollte eine möglichst breite Unterstützung von Verfahren angestrebt werden.
- Die zum Datentransport benutzten Protokolle bieten selbst schon Sicherheitsmechanismen an. Diese können vom VPN-Produkt genutzt werden. Alternativ kann das VPN-Produkt auch eigene Verfahren anbieten.

Die Sicherheitsmechanismen basieren auf unterschiedlichen kryptographischen Verfahren. Die Maßnahme M 3.23 *Einführung in kryptographische Grundbegriffe* enthält eine kurze Einführung in kryptographische Grundbegriffe.

### Verschlüsseln von Protokollverbindungen: Tunneling

Wird eine verschlüsselte Datenverbindung zwischen zwei Kommunikationspartnern aufgebaut, so realisiert diese Verbindung einen "sicheren Kanal". Durch diesen Kanal können beliebige Daten sicher mit dem zugrunde liegenden Kommunikationsprotokoll (beispielsweise IP) übertragen werden. Stellen die übertragenen Daten selbst die Datenpakete eines Kommunikationsprotokolls dar, so spricht man auch von einem "Tunnel".

Das Protokoll, das verwendet wird, um die Daten zu verschlüsseln, die verschlüsselten Daten durch den Tunnel zu übertragen und die Verbindung zu

verwalten, wird auch als Tunnel-Protokoll bezeichnet. Bei Tunnel-Protokollen kann unterschieden werden,

- auf welchem Transport-Protokoll sie aufbauen und welcher Protokoll-Schicht (OSI-Layer) sie zuzuordnen sind (siehe auch M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*),
- welche Protokolle über die Tunnel-Verbindung übertragen werden können,
- welche kryptographischen Verfahren zur Realisierung des Tunnels unterstützt werden,
- ob die Endpunkte des Tunnels authentisiert werden und
- ob über eine Verbindung des benutzten Transport-Protokolls der Aufbau mehrerer paralleler Tunnel möglich ist.

Das Tunnel-Protokoll ist im Wesentlichen zuständig für

- Verwaltung des bzw. der Tunnel: Aufbau, Aufrechterhaltung und Abbau,
- Aushandeln der zu verwendenden kryptographischen Verfahren für die Realisierung des Tunnels: Schlüsselaustauschverfahren, Verschlüsselungsverfahren und Signaturverfahren,
- Ver- und Entpacken der Datenpakete der durch den Tunnel übertragbaren Protokolle sowie
- Ver- und Entschlüsseln der Datenpakete.

Bei der Wahl der eingesetzten VPN-Hardware und -Software sollte darauf geachtet werden, dass möglichst mehrere verschiedene und etablierte Verschlüsselungsverfahren unterstützt werden. Dadurch erhöht sich die Wahrscheinlichkeit, dass zwischen Client und Server geeignete Verfahren ausgehandelt werden können.

**Übersicht über gängige Tunnel-Protokolle**

Im VPN-Umfeld haben sich folgende Tunnel-Protokolle etabliert:

- PPTP (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- IPSec (Internet Protocol Security)
- TLS/SSL (Transport Layer Security, Secure Sockets Layer)

Die Protokolle besitzen die aus der folgenden Tabelle ersichtlichen Charakteristika:

| **Tunnel-Protokoll** | **Schicht** | **Transportierte Protokolle** | **Benötigtes darunter liegendes Protokoll** | **Anzahl der unterstützten Tunnel** | **Tunnel Authentisierung** |
|---|---|---|---|---|---|
| PPTP | 2 | IP, IPX, NetBEUI | IP | 1 | Nein |
| L2TP | 2 | IP, IPX, NetBEUI | IP, X.25, Frame Relay, ATM | mehrere | Ja |
| IPSec | 3 | IP | IP | 1 | Ja |
| TLS/SSL | 4 | IP, HTTP, SMTP, ... | IP | mehrere | Ja |

Tabelle: Protokolle

Ein in der Praxis wichtiger Aspekt ist, dass die ausgewählten Tunnel-Protokolle und die festgelegten kryptographischen Verfahren von allen beteiligten Tunnel-Endpunkten unterstützt werden müssen. Im Folgenden werden die gängigsten Tunnel-Protokolle kurz beschrieben.

**PPTP (Point to Point Tunneling Protocol)**

PPTP ist ein Tunnel-Protokoll auf Schicht 2. Es dient dazu, PPP-Verbindungen (Point to Point Protocol) über ein IP-Netz aufzubauen. Über die so hergestellte PPP-Verbindung können dann beispielsweise IP-Pakete transportiert ("getunnelt") werden. Die Sicherheitsfunktionen zur Authentisierung, Schlüsselverwaltung und Verschlüsselung werden von PPP bereitgestellt, häufig unter Nutzung des Microsoft Point-to-Point Encryption Protocol (MPPE). Im Sprachgebrauch wird jedoch oft nicht zwischen dem eigentlichen PPTP und der Kombination PPTP/PPP/MPPE unterschieden.

In gängigen Implementierungen dieses Tunnel-Verfahrens wurden Sicherheitslücken entdeckt, insbesondere in Zusammenhang mit schwachen Passwörtern. Ohne zusätzliche Sicherheitsmechanismen sollte PPTP daher nicht als VPN-Lösung eingesetzt werden.

**L2TP (Layer 2 Tunneling Protocol)**

Ähnlich wie PPTP dient L2TP in der Version 2 (L2TPv2) dazu, PPP-Verbindungen über paketvermittelte Netze aufzubauen. Im Gegensatz zu PPTP können bei L2TP jedoch neben IP auch andere Techniken als Trägernetz dienen, beispielsweise ATM. Für die Tunnel-Funktionalität nutzt L2TP dabei Mechanismen des von der Firma Cisco entworfenen Protokolls L2F (Layer 2 Forwarding).

L2TP bietet selbst keine Funktionen zur Verschlüsselung der Datenpakete an. Eine solche Verschlüsselung muss entweder vom Trägernetz oder von den transportierten Protokollen geleistet werden. L2TP wird daher häufig in Kombination mit IPSec (siehe unten) eingesetzt.

**IPSec (Internet Protocol Security)**

IPSec ist ein Protokoll auf Schicht 3, das Funktionen zur Verschlüsselung und Integritätssicherung für IP-Kommunikation bietet. In Kombination mit dem IKE-Verfahren (Internet Key Exchange, früher ISAKMP/Oakley) kann auch ein automatisierter Schlüsselaustausch sowie eine Authentisierung der Tunnel-Endpunkte erfolgen. Auch über das von der Firma Sun Microsystems stammende Verfahren SKIP (Simple Key Management for Internet Protocol) kann ein Schlüsselaustausch für IPSec-Kommunikation erfolgen. Ein manueller Schlüsselaustausch wird durch IPSec ebenfalls unterstützt. Die Authentisierung der Benutzer muss jedoch über andere Verfahren erfolgen.

IPSec ist ein komplexes Protokoll, das mehrere unterschiedliche Optionen und Betriebsmodi bietet. Weiterhin sind die eingesetzten kryptographischen Verfahren in der Spezifikation nicht abschließend festgelegt, sondern es sind lediglich Mindestanforderungen aufgeführt. Beim Einsatz von IPSec muss daher im Rahmen der Konfiguration sichergestellt werden, dass die für den vorliegenden Anwendungsfall ermittelten Sicherheitsanforderungen erfüllt werden und dass geeignete kryptographische Verfahren verwendet werden. Weitere Empfehlungen hierzu finden sich in den Maßnahmen M 5.149 *Sichere Anbindung eines externen Netzes mit IPSec* und M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*.

**TLS/SSL (Transport Layer Security, Secure Sockets Layer)**

TLS/SSL ist ein weit verbreitetes Verfahren, um Transportsicherheit beispielsweise für Web-Anwendungen oder E-Mail-Übertragung bereitzustellen. Einerseits können über TLS/SSL unterschiedliche Anwendungsprotokolle, wie z. B. HTTP, SMTP, POP oder IMAP, transportiert werden. Andererseits ist es mit Hilfe spezieller Software-Komponenten auch möglich, IP-Tunnel über TLS/SSL aufzubauen. Aufgrund seiner Arbeitsweise lässt sich TLS/SSL nicht eindeutig einer bestimmten Protokollschicht zuordnen, häufig wird es jedoch als Schicht-4-Protokoll bezeichnet.

TLS/SSL bietet Sicherheitsfunktionen zur Authentisierung und Verschlüsselung sowie zum Schlüsselaustausch und Integritätsschutz. Ähnlich wie bei IPSec sind die hierfür erforderlichen kryptographischen Verfahren in der Spezifikation nicht abschließend festgelegt. Vielmehr handeln die beteiligten Kommunikationspartner die verwendeten Verfahren beim jeweiligen Verbindungsaufbau aus. Es muss daher im Rahmen der Konfiguration sichergestellt werden, dass die ermittelten Sicherheitsanforderungen erfüllt werden und dass geeignete kryptographische Verfahren verwendet werden. Weitere Hinweise hierzu finden sich in den Maßnahmen M 5.148 *Sichere Anbindung eines externen Netzes mit OpenVPN*, M 5.66 *Clientseitige Verwendung von SSL/TLS*, und M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*.

**Sonstige Tunnel-Protokolle**

VPN-Lösungen können nicht nur über die oben genannten Tunnel-Protokolle, sondern auch über andere Verfahren aufgebaut werden. Ein Beispiel ist der Einsatz des Produktes OpenSSH für VPN-Zwecke. OpenSSH wurde primär als verschlüsselter Ersatz für telnet, ftp und die r-Dienste entwickelt, kann jedoch auch VPN-Verbindungen absichern.

Weiterhin werden Produkte am Markt angeboten, die proprietäre Tunnel- bzw. Verschlüsselungsverfahren nutzen. Der Einsatz proprietärer Verfahren sollte vermieden werden, da sich deren Sicherheitseigenschaften häufig nur schwer beurteilen lassen. Stattdessen sollten Verfahren eingesetzt werden, die sich an gängigen Standards und öffentlich verfügbaren Spezifikationen orientieren.

Prüffragen:

- Entsprechen die verwendeten kryptographischen Verfahren und Schlüssellängen dem Stand der Technik?
- Ist sichergestellt, dass zwischen den beteiligten VPN-Komponenten geeignete kryptographische Verfahren ausgehandelt werden?

# M 5.77 Bildung von Teilnetzen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

IT-Systeme in Behörden und Unternehmen sind typischerweise in lokale Netze (LANs) integriert, die ihrerseits wieder mit anderen Netzen verbunden sind. Allein aus technischen Gründen ist es bei mittleren und größeren Netzen meist erforderlich, ein LAN in mehrere Teilnetze aufzuteilen.

Die Bildung von Teilnetzen ist jedoch auch aus Gründen der Informationssicherheit empfehlenswert. Einerseits können sensitive Daten auf bestimmte Bereiche innerhalb des LANs begrenzt werden (Vertraulichkeit), andererseits kann verhindert werden, dass Störungen in oder Angriffe auf ein Teilnetz die Funktionsfähigkeit anderer Teilnetze beeinträchtigen (Integrität und Verfügbarkeit).

Oft werden in Institutionen in der Regel große, aber einfache Netze aufgebaut, die ohne zusätzliche Sicherheitszonen auskommen. Dabei werden alle IT-Systeme einem einheitlichen Netz zugeordnet, an dessen Schnittstelle zum Internet eine zentrale Sicherheitsgateway-Lösung (siehe B 3.301 *Sicherheitsgateway (Firewall)*) zum Schutz des Netzes zuständig ist. Eine solche einfache Sicherheitsarchitektur bietet jedoch gegen Angreifer oder Schadsoftware häufig ein zu geringes Maß an Sicherheit, da das gesamte Netz mit all seinen Komponenten und Daten offen steht, wenn das Sicherheitsgateway überwunden worden ist. Angesichts dieser Gefährdung sollten Institutionen Maßnahmen ergreifen, um ihr Netz und damit die angeschlossenen IT-Systeme wie beispielsweise Server, Arbeitsplatz-PCs, Storage-Systeme etc. abzusichern. Eine mögliche Maßnahmen in diesem Zusammenhang ist es, das Netz in separate Bereiche (sogenannte Zonen) zu untergliedern, die dann voneinander durch eigene Sicherheitsgateways (Application-Level-Gateway oder Paket Filter) getrennt beziehungsweise abgesichert werden. Innerhalb der jeweiligen Zonen können dann Teilnetze gebildet werden. Bewährt hat sich eine Aufteilung in vier Zonen: Internes Netz, Sicherheitsgateway-Zone (ALG-Zone), Internet-Anbindung und Management-Zone (siehe auch M 2.476 *Konzeption für die sichere Internet-Anbindung*).

**Internes Netz**

Die erste Zone umfasst das interne Netz. Sie enthält alle Client-Systeme sowie alle Infrastruktur- und Anwendungsserver, die für den autonomen, lokalen LAN-Betrieb benötigt werden. Bei der Bildung von Teilnetzen im internen Netz wird empfohlen, zunächst festzulegen, welche IT-Systeme jeweils in einem gemeinsamen Teilnetz betrieben werden sollen. Es wird empfohlen, dabei auf die Ergebnisse der Schutzbedarfsfeststellung zurückzugreifen und wie folgt vorzugehen:

- Alle IT-Systeme in einem Teilnetz sollten in Bezug auf den Grundwert Vertraulichkeit den selben Schutzbedarf haben. Hierdurch wird erreicht, dass sensitive Daten möglichst auf speziell geschützte Teilnetze begrenzt werden. Entsprechend erforderliche Schutzmaßnahmen können auf diese Teilnetze konzentriert werden.
- IT-Systeme mit einem hohen Schutzbedarf in Bezug auf Verfügbarkeit oder Integrität sollten möglichst jeweils in einem eigenen Teilnetz betrieben werden. Hierdurch wird erreicht, dass der ordnungsgemäße Betrieb dieser Komponenten bei Störungen in anderen Teilnetzen nicht beein-

trächtigt wird. Weiterhin können dadurch Störungen schneller eingegrenzt und behoben werden.

Darüber hinaus sollte darüber nachgedacht werden, Arbeitsplatz-PCs und Server in getrennten Segmenten zu platzieren, um Server vor dem Einfluss fehlkonfigurierter oder potenziell manipulierter Clients zu schützen.

Auch kann eine beliebige Anzahl weiterer Teilnetze (LAN-Segmente) eingerichtet werden, etwa um Benutzer je nach ihren Rollen in gesonderten Client-Bereichen anzusiedeln oder um IT-Systeme mit besonderen Anforderungen, beispielsweise an die Quality-of-Service (zum Beispiel IP-Telefone), in einem eigenen Teilnetz zu betreiben.

**Sicherheitsgateway-Zone (ALG-Zone)**

Die Sicherheitsgateway-Zone besteht, außer bei kleinen oder sehr kleinen Netzen, in der Regel aus einem äußeren Paketfilter, einem Application-Level-Gateway in der Mitte und einem inneren Paketfilter (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*). Nach Möglichkeit sollte die ALG-Zone in zwei Bereiche (interne und externe DMZ) unterteilt werden. In der externen DMZ sollten Anwendungen platziert werden, die dafür eingesetzt werden, Dienste im Internet anzubieten. Beispiele hierfür sind der externe Webserver, DNS-Server oder FTP-Server. Externe Zugriffe sollten in der externen DMZ terminiert werden. In der internen DMZ sollten solche Anwendungen betrieben werden, die nachgelagerte Dienste anbieten. Beispiele hierfür sind Anwendungsserver, Datenbankserver oder VPN-Server. Die vorgelagerten Server (z. B. Webserver) können dann bei Bedarf auf Rechner in nachgelagerten Sicherheitszonen (z. B. Datenbanken) zurückgreifen, um ihre Dienste bereitzustellen.

Je nach Einsatzzweck des LANs können auch weitere Dienste in der externen DMZ platziert werden. Abhängig vom Schutzbedarf ist es auch möglich, weitere DMZs in der externen DMZ-Zone zu bilden, um unterschiedliche Internet-Dienste in getrennten Sicherheitszonen zu betreiben.

**Internet-Anbindung**

Die dritte Zone umfasst die Komponenten zur Internet-Anbindung. Sie enthält im einfachsten Fall einen einzelnen Router, der mit dem Netz eines Internet-Diensteanbieters verbunden ist. Bei höheren Anforderungen an die Verfügbarkeit muss die Anbindung redundant ausgelegt werden.

**Management-Zone**

In der Management-Zone könnten alle Management-Daten zentral gesammelt und verarbeitet werden. Hier könnte auch ein Zeitserver untergebracht werden, mit dem sämtliche Systemuhren im Netz synchronisiert werden.

**Auswahl geeigneter Komponenten**

Nachdem Teilnetze gebildet worden sind, besteht der zweite Schritt in der Auswahl geeigneter Komponenten für die Kopplung der gebildeten Teilnetze. Empfehlungen hierzu finden sich in der Maßnahme M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*.

Empfehlungen für die technische Realisierung der Segmentierung im LAN sind in M 5.61 *Geeignete physische Segmentierung* und M 5.62 *Geeignete logische Segmentierung* enthalten.

Prüffragen:

- Ist das lokale Netz gemäß den Ergebnissen der Schutzbedarfsfeststellung sinnvoll in Zonen und Teilnetze aufgeteilt worden?
- Ist festgelegt worden, welche Netzkoppelelemente für die Aufteilung in Teilnetze zu verwenden sind?

# M 5.78 Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Bei der Mobil-Kommunikation müssen die mobilen Kommunikationspartner aus technischen Gründen geortet werden können, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls im Zuge des Verbindungsaufbaus Informationen über ihren Standort ab. Diese Standortinformationen könnten durch den Netz- oder Dienstbetreiber, aber eventuell auch von Dritten, zur Bildung personen- oder gerätebezogener "Bewegungsprofile" verwendet werden.

Bei modernen Mobiltelefonen besitzen gegebenenfalls einige Applikationen Zugriff auf das Internet und den eingebauten GPS-Empfänger und geben Standortinformationen weiter, mit denen Dritte ebenfalls Bewegungsprofile erstellen können. Applikationen, die diese Rechte aus nicht funktionsbezogenen Gründen anfordern, sollten nicht installiert werden. Bei allen anderen Applikationen muss zwischen der Gefahr, Bewegungsprofile zu ermöglichen, und dem Nutzen der Applikation abgewogen werden.

Werden Bewegungsprofile als Gefährdung angesehen, dann sollten, falls umsetzbar, die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert. Lokalisierungen über das Radio Resource Location Protocol (RRLP) können damit jedoch nicht abgewehrt werden, da hierbei sowohl die Telefonnummer als auch die International Mobile Equipment Identity (IMEI) ermittelt wird.

Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte der Akku entfernt werden.

Prüffragen:

- Ist die Frage geklärt, ob Bewegungsprofile sich negativ auswirken können?

# M 5.79 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Im Mobilfunknetz werden in der Regel den beteiligten Kommunikationspartnern die jeweiligen Rufnummern angezeigt. Ob dies tatsächlich geschieht, hängt von der technischen Ausstattung und der Konfiguration seitens der Mobiltelefone bzw. der Netzbetreiber bzw. Mobilfunkanbieter ab.

Am Mobiltelefon kann mit der Funktion Rufnummernunterdrückung (für den nächsten bzw. alle weiteren Anrufe) verhindert werden, dass die eigene Rufnummer im Display des Angerufenen angezeigt wird. Diese Option ist in den Menüs der Mobiltelefone oft unter Bezeichnungen wie Inkognito oder Anonym zu finden. Beim SMS-Versand mit einem Mobiltelefon ist eine Rufnummernunterdrückung in der Regel nicht möglich. Das Verhalten der Voice-Mailbox sollte im Einzelfall verifiziert werden, ebenso wie das Gesamtverhalten von Rufnummernunterdrückungs-Aktionen im Ausland.

Die Rufnummernunterdrückung kann bei Geräten, die den GSM-Standard unterstützen, mit folgenden GSM-Codes für den nächsten Anruf gesteuert werden:

- Eigene Rufnummer zeigen *31#Rufnummer
- Eigene Rufnummer nicht zeigen #31#Rufnummer

Über den Netzbetreiber kann auch kontinuierlich eine Rufnummernunterdrückung aktiviert werden.

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer bzw. Gerät und Nutzer möglich. Die Zuordnung z. B. zu einer Behörde oder einem Unternehmen bleibt aber bestehen.

Außer über die Signalisierung der Rufnummer kann die Mobiltelefonnummer einer bestimmten Person auch über öffentliche Telefonbücher ermittelt werden, wenn sie dort eingetragen ist. Beim Abschluss eines Mobilfunkvertrages sollte daher genau überlegt werden, ob bzw. in welcher Form eine Eintragung in öffentliche Telefonbücher sinnvoll ist. Auch in internen Telefonbüchern und bei einzelnen Datenabfragen (Formulare, Gewinnspiele, etc.) sollten Mobiltelefonnummern nicht gedankenlos preisgegeben werden.

Prüffragen:

- Wird die Rufnummer in erforderlichen Fällen für ausgehende Anrufe unterdrückt?
- Sind in öffentlichen Telefonbüchern ausschließlich die dafür vorgesehenen Rufnummern veröffentlicht?

# M 5.80 Schutz vor Abhören der Raumgespräche über Mobiltelefone

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Wer sicher ausschließen will, dass Raumgespräche über Mobiltelefone abgehört werden, muss dafür sorgen, dass kein Mobiltelefon in den zu schützenden Raum mitgenommen wird. Wenn die Sicherheitsleitlinie einer Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Ohne entsprechende Kontrollen ist ein einfacher Hinweis aber meist wirkungslos.

Es reicht als Schutz nicht aus, Mobiltelefone einfach auszuschalten bzw. in den Standby oder Flugmodus zu bringen. Sofern sie entsprechend manipuliert sind, können sie über Funk unbemerkt eingeschaltet werden.

**Mobiltelefon-Detektoren**

Mobiltelefon-Detektoren sind Geräte, die erkennen, wenn in einem abgegrenzten Bereich ein oder mehrere Mobiltelefone in den Sendebetrieb (Gesprächsverbindungsaufbau) gehen.

Es gibt aktive und passive Detektoren. Passive Warngeräte melden Mobiltelefone, die sich im Sendebetrieb befinden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, bei einem entsprechenden Schutzbedarf solche Warngeräte zu installieren und diese bei Gesprächen mit vertraulichem Inhalt zu aktivieren. Moderne Mobiltelefone benötigen allerdings zum Abhören keine stehende Funkverbindung, sondern können das Gespräch aufzeichnen und die Sounddatei mit Verzögerung über das Mobilfunknetz übertragen. Daher schützen passive Mobiltelefon-Detektoren nur bedingt davor, dass Raumgespräche abgehört werden.

Um auch Mobiltelefone zu erkennen, die im Ruhebetrieb (Standby) sind, wäre ein aktiver Sendeteil für den Detektor notwendig. Mithilfe dieses Sendeteils kann das Mobiltelefon dazu gebracht werden, in den Sendebetrieb zu gehen. Danach kann es dann mit einem Detektor erkannt werden. Mithilfe dieser aktiven Detektoren lassen sich so alle eingeschalteten Mobiltelefone detektieren. Später eingeschaltete Geräte müssen sich bei der Basisstation anmelden und können bei diesem Einbuchungsvorgang ebenfalls detektiert werden. Die Störsender können auch so eingesetzt werden, dass sie in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist.

Derzeit können aber nur passive Mobiltelefon-Detektoren empfohlen werden. Aktive Detektoren sind zwar ebenfalls sinnvoll, sie besitzen jedoch keine Betriebsgenehmigung für Deutschland. Auch Sender, die den Mobilfunkbetrieb stören, sind in Deutschland nicht zugelassen. Mobiltelefone können auch als Diktiergeräte genutzt werden. Lautlos und in den Flugmodus geschaltete Geräte können problemlos Besprechungen aufzeichnen, selbst aktive Mobiltelefon-Detektoren sind dann keine geeignete Gegenmaßnahme.

Prüffragen:

- Ist sichergestellt, dass Mobiltelefone nicht in abhörgeschützten Räumen verwendet werden?

# M 5.81 Sichere Datenübertragung über Mobiltelefone

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, IT-Sicherheitsbeauftragter

Mobiltelefone werden für die Sprachübertragung eingesetzt, es können aber auch Daten und Faxe damit übermittelt werden. Für einige dieser Dienste wird zusätzliches Zubehör benötigt. Moderne Mobiltelefone sind in der Regel dauerhaft mit dem Internet verbunden, um Chat-Nachrichten oder E-Mails zu empfangen. Benutzen Mobiltelefone den LTE-Standard, wird jegliche Kommunikation als Datenübertragung über das Internet-Protokoll (IP) realisiert.

**Kurzmitteilungen**

Mit dem Kurznachrichtendienst (Short Message Service, SMS) lassen sich Texte mit maximal 160 Zeichen von einem Mobiltelefon zum anderen oder auch an E-Mail-Adressen senden. Längere Nachrichten werden dabei in der Regel automatisch vom Mobiltelefon in mehrere Kurzmitteilungen aufgeteilt. Die Übertragung von Kurzmitteilungen erfolgt immer über eine Kurzmitteilungs-Zentrale, die die Nachrichten an den jeweiligen Empfänger weiterleitet.

Kurzmitteilungen werden im Mobiltelefon gespeichert, solange Speicherplatz verfügbar ist. Wenn kein ausreichender Speicherplatz (oft bei älteren oder extrem preisgünstigen Modellen) mehr frei ist, können keine weiteren Kurzmitteilungen empfangen werden. Der Netzbetreiber versucht nur über einen begrenzten Zeitraum, weitere Nachrichten abzusetzen. Wenn nicht rechtzeitig Speicherplatz freigemacht wird, werden die Kurzmitteilungen beim Netzbetreiber gelöscht.

Teilweise kann auch über das Mobiltelefon der Zeitraum, über den Kurzmitteilungen beim Netzbetreiber zwischengespeichert werden, verändert werden. Die Voreinstellung liegt im Allgemeinen zwischen 24 und 48 Stunden. Wenn der Vertrag mit dem Netzbetreiber es nicht vorsieht, kann hierüber allerdings der Speicherungszeitraum nicht erhöht werden. Er sollte auch nicht verringert werden.

Je nach Mobilfunkanbieter besteht die Möglichkeit, dass der Absender der Kurznachricht eine automatische Empfangsbestätigung erhält. Damit sichergestellt wird, ob die Nachrichten (siehe G 5.27 *Nichtanerkennung einer Nachricht*) empfangen wurden, sollten Empfangsbestätigungen aktiviert werden. Damit lässt sich zusätzlich auch nachvollziehen, ob die Nachricht wegen zu kurzer Speicherfristen bei der Kurzmitteilungs-Zentrale womöglich nicht zugestellt wurde (siehe G 4.32 *Nichtzustellung einer Nachricht*). Die Empfangsbestätigungen sollten so lange wie nötig auf dem Mobiltelefon gespeichert werden.

Um Kurzmitteilungen verschicken zu können, muss die Rufnummer der Kurzmitteilungs-Zentrale (SMS-Gateway) über das entsprechende Menü am Mobiltelefon voreingestellt werden. Meist ist dies schon auf der SIM-Karte vom Netzbetreiber vorkonfiguriert worden.

Im Internet gibt es diverse Angebote, Kurzmitteilungen mit minimalen Kosten zu versenden. Ein Angreifer kann also ohne großen Aufwand eine große Anzahl von SMS-Nachrichten an ein Mobiltelefon versenden. SMS-Spam wirkt sich ebenso aus wie E-Mail-Spam (siehe G 5.75 *Überlastung durch eingehende E-Mails*). Die Mailbox bzw. der Speicherplatz reicht nicht aus und ernsthaf-

te Nachrichten kommen nicht durch. Darüber hinaus entstehen dem Benutzer eventuell hohe Kosten. Hiergegen hilft neben der Sperrung von Drittanbieter-Diensten durch den Provider bzw. Mobilfunkanbieter, im Vorfeld die eigene Rufnummer nicht zu breit zu streuen, also z. B. auf den Eintrag in Telefonbücher zu verzichten, bzw. im Schadensfall eine Zeit lang ganz auf SMS-Empfang zu verzichten.

Eine Identifikation des Absenders ist bei SMS nicht zuverlässig möglich. Sie erfolgt maximal über die Rufnummer des Absenders und diese wird je nach Netzbetreiber bzw. Konfiguration des Mobiltelefons nicht immer mit übertragen. Beim Versand von Kurzmitteilungen über das Internet erfolgt im Allgemeinen überhaupt keine eindeutige Identifizierung. Dies sollte allen Benutzern klar sein, um die Echtheit einer Nachricht richtig einschätzen zu können. Je nach Inhalt einer empfangenen Kurzmitteilung ist es sinnvoll nachzufragen, ob diese wirklich vom angegebenen Absender stammt.

**Faxe**

Es können Faxe über ein mit dem Mobiltelefon gekoppeltes IT-System (z. B. Notebook) gesendet und empfangen werden.

Dabei ist ähnlich wie bei herkömmlichen Faxgeräten (siehe Baustein B 3.402 *Faxgerät*) zu beachten, dass

- der Speicherplatz des Mobiltelefons durch empfangene Faxe überlastet werden kann,
- es je nach Bedeutung von Faxen erforderlich sein kann, davon Kopien anzufertigen, was beim Mobiltelefon unter Umständen schwierig ist,
- es sinnvoll sein kann, die Rufnummern von bestimmten Faxempfängern bzw. Absendern zu sperren.

Außerdem empfiehlt sich,

- nach dem Versand nachzufragen, ob das Fax lesbar angekommen ist,
- nach dem Empfang nachzufragen, ob das Fax wirklich vom angegebenen Absender stammt,
- ab und zu die programmierten Zieladressen zu kontrollieren.

**E-Mail**

Über Mobiltelefone können neben Kurzmitteilungen auch E-Mails empfangen und verschickt werden. Bei älteren Endgeräten sind E-Mails wie Kurzmitteilungen auf 160 Zeichen begrenzt. Wenn dieser Service vom Netzbetreiber eingerichtet worden ist, erhält das Mobiltelefon eine eigene E-Mail-Adresse. In der Regel besitzen Mobiltelefone heute jedoch E-Mail-Clients, die E-Mails wie ein PC verarbeiten können. Besitzen Mobiltelefone keinen E-Mail-Client aber einen Browser, so können E-Mails in der Regel über eine Web-Oberfläche verarbeitet werden.

Bei einigen Netzbetreibern können E-Mail-Dienste mit anderen Diensten kombiniert werden. So können eingehende E-Mails von einem Sprachcomputer vorgelesen werden, an ein Faxgerät oder eine andere E-Mail-Adresse weitergeleitet werden. Ausgehende E-Mails können ins Mobiltelefon gesprochen und als Audiodatei versandt werden.

Wie Kurzmitteilungen und Faxe können auch E-Mails schnell den vorhandenen Speicherplatz (bei älteren oder extrem preisgünstigen Geräten) ausschöpfen. Der E-Mail-Client sollte daher so eingestellt werden, dass Dateianhänge nur bei Bedarf, also wenn der Benutzer sie explizit anfragt, nachgeladen werden.

Potenzielle Sicherheitsprobleme und Maßnahmen für E-Mail sind in Baustein B 5.3 *Groupware* beschrieben. Dabei ist zu beachten, dass die E-Mail-Funktionalität bei Mobiltelefonen stark eingeschränkt ist gegenüber anderen E-Mail-Anwendungen. Ebenso wie SMS ist E-Mail hier eher für die Übermittlung kurzer und kurzlebiger Nachrichten gedacht. Sicherheitsmaßnahmen wie Verschlüsselung oder Signatur sind in der Regel nur mit Smartphones möglich. Alternativ gibt es noch spezielle Geräte oder zusätzliche Module, mit denen verschlüsselte oder signierte Nachrichten mit einem Mobiltelefon übermittelt werden können.

**Instant Messenger**

Auf einigen Mobiltelefonen und den meisten Smartphones sind Instant Messenger vorhanden oder lassen sich nachträglich installieren. Mit Instant Messengern können Nachrichten, aber auch Dateien wie z. B. Bilder, Filme, und Office-Dokumente übertragen werden. Auch Instant Messenger, die über das Internet-Relay-Chat-(IRC)-System funktionieren, sind vielfach im Einsatz. Die Kommunikation über Instant Messenger sollte, wenn möglich, Ende-zu-Ende-verschlüsselt erfolgen. Es dürfen nur vertrauenswürdige IRC-Server bzw. Instant-Message-Provider verwendet werden. In diesem Fall ist die Vertraulichkeit der Kommunikation gegenüber Kurznachrichten deutlich erhöht. Dubiose Dateiübertragungen sollten abgelehnt werden. Instant Messenger haben zudem gegenüber den Kurznachrichten den Vorteil, dass Kosten nach Datenmenge und nicht nach Anzahl der Nachrichten entstehen. Zusätzlich besitzen viele Instant Messenger die Funktion der Empfangsbestätigung, die auch genutzt werden sollte, um der Gefahr der Nichtanerkennung von Nachrichten (siehe G 5.27 *Nichtanerkennung einer Nachricht*) zu begegnen.

**Datenübertragung**

Ein Mobiltelefon kann je nach Modell mit einem weiteren IT-System (z. B. einem Notebook oder einem Organizer) gekoppelt werden und dann leichter auch größere Datenmengen übertragen. Dabei kann die Kopplung auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beiden Geräte unterstützen.

**Einsteckkarte:** Eine Einsteckkarte (PC-Card, PCMCIA) ist die ursprünglich konventionelle, aber mittlerweile kaum noch eingesetzte Lösung zur Verbindung von Mobiltelefon und Notebook. Die meisten Einsteckkarten können allerdings nur an Mobiltelefone eines bestimmten Herstellers angeschlossen werden.

**Softmodem:** Bei dieser Lösung wird statt einer Einsteckkarte eine spezielle Software auf dem Notebook installiert. Das Mobiltelefon wird dann einfach über die serielle (oder USB) Schnittstelle mit dem Notebook verbunden. Diese Lösung ist meist preiswerter als eine Einsteckkarte.

**Infrarot:** Über eine Infrarot-Schnittstelle können Daten auch ohne Kabel vom Mobiltelefon zu einem anderen Gerät (z. B. Laptop oder Organizer) übertragen werden. Dazu muss sowohl das Mobiltelefon als auch das Partnergerät den Infrarot Übertragungsstandard IrDA unterstützen. IrDA ist ein weltweiter Standard für die Datenübertragung über Infrarot, wird aber für Datenübertragungen heute kaum noch eingesetzt (siehe M 4.255 *Nutzung von IrDA-Schnittstellen*).

**Bluetooth:** Bluetooth ist ein etablierter Standard, nach dem Geräte per Funk über Entfernungen von 1 bis 100m (je nach Bluetooth-Klasse) miteinander Daten austauschen können. (siehe B 4.8 *Bluetooth*).

**WLAN:** Über Wireless-LAN kann ein Mobiltelefon mit einem Rechnernetz verbunden werden oder es kann selbst als sogenannter WLAN-Hotspot fungieren ("Tethering") und eine Internetverbindung für andere IT-Systeme bereitstellen. Die WLAN-Verbindung sollte dabei über WPA kryptografisch abgesichert werden. Weitere Details zum Einsatz von WLAN sind im Baustein B 4.6 *WLAN* zu finden.

Bei der Datenübertragung z. B. von einem Laptop über das Mobilfunknetz sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Applikationen, die dies einfach ermöglichen. Die Verschlüsselung vor der Übertragung sichert die Informationen auf der gesamten Strecke zwischen Absender und Empfänger. Dies geht über die bei GSM standardmäßige Absicherung der Luftschnittstelle zwischen Mobiltelefon und Basisstation hinaus. Das ist notwendig, weil die Verschlüsselung über das GSM-Netz auf der Luftschnittstelle als gebrochen gilt. Bei schlechter Umsetzung bietet die Verschlüsselung bei der Übertragung mit UMTS auch keinen besseren Schutz als bei der Übertragung mit GSM. Werden die Daten hingegen mithilfe von Programmen auf dem Endgerät verschlüsselt, können die Nachrichten zudem noch digital signiert werden. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist im B 1.7 *Kryptokonzept* beschrieben. Alternativ zur Verschlüsselung der Daten bieten moderne Mobiltelefone vielfach die Möglichkeit, verschlüsselte VPN-Tunnel zu etablieren, womit die Datenübertragung zwischen Mobiltelefon und anderen Netzteilnehmern ebenfalls hinreichend abgesichert werden kann. Alternativ könnte ein vorhandener Laptop auch als VPN-Endpunkt verwendet werden, über diesen das Mobiltelefon eine geschützte Datenverbindung aufbauen kann. Wird VPN verwendet, besteht überdies der Vorteil, dass die Verschlüsselung transparent ist und keine weitere Benutzerinteraktion benötigt.

Besitzt das Mobiltelefon einen Browser und E-Mail-Client, so ist es über diese Kanäle so verwundbar wie ein PC. Unbedacht heruntergeladene Dateien, Klingeltöne, aber auch Drive-by-Infektionen können die Geräte ebenso funktionsuntüchtig machen wie stationäre Computer.

Die Datenübertragung sollte in allen Organisationen klar geregelt sein. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen (siehe M 2.204 *Verhinderung ungesicherter Netzzugänge*).

Damit durch die Datenübertragung über GSM-Schnittstellen keine Sicherheitslücken entstehen, sollte diese restriktiv gehandhabt werden. So sollten bei IT-Systemen, auf denen sensitive Daten verarbeitet werden, keine Mobilfunkkarten zugelassen werden bzw. Verbindungen über das Mobilfunknetz immer mit verschlüsselten VPN-Tunneln abgesichert sein. Dies gilt ebenso bei allen IT-Systemen, die an einem Rechner-Netz angebunden sind, damit hier nicht der durch eine Firewall eigentlich vorhandene Schutz unterhöhlt werden kann.

Prüffragen:

- Gibt es Regelungen, welche Daten über Mobiltelefone übertragen werden dürfen?
- Gibt es Regelungen, welche Schnittstellen zu benutzen sind und wie verschlüsselt werden soll?

# M 5.82 Sicherer Einsatz von SAMBA

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen. Alle Inhalte zum Thema SAMBA sind in den Baustein B 5.17 *Samba* überführt worden.

# M 5.83 Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN

Die Maßnahme ist in der 15. Ergänzungslieferung 2016 entfallen. Nähere Informationen zum Thema Virtuelle Private Netze befinden sich im Baustein B 4.4 *VPN*.

# M 5.84 Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 5.85 Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 5.86 Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 4.429 *Sichere Konfiguration von Lotus Notes/Domino* integriert.

# M 5.87 Vereinbarung über die Anbindung an Netze Dritter

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Immer mehr Unternehmen und Behörden schließen ihre bisher nach außen abgeschotteten Netze zu Netzverbünden zusammen, so genannten Extranets. Bei der Anbindung des eigenen internen Netzes an Netze Dritter ist es erforderlich, dass eine detaillierte Vereinbarung (Data Connection Agreement - DCA) geschlossen wird, bevor eine Netzanbindung erfolgt. Hierdurch muss genau definiert werden, wer dadurch Zugriff auf das eigene Netz erhält, unter welchen Bedingungen und auf welche Bereiche und Dienste des eigenen Netzes Zugriff gegeben werden soll. Ebenso wichtig ist dabei auch die andere Richtung, also die Frage, wer aus der eigenen Organisation mit welchen Zugriffsrechten und zu welchen Bedingungen Zugriff auf ein Fremdnetz erhalten soll.

Eine solche Vereinbarung soll folgende Bestandteile umfassen:

- eine Beschreibung dessen, was die Vereinbarung insgesamt umfasst,
- eine Festlegung der Verantwortlichen (Wer trägt die Verantwortung für die Einhaltung der Vertragsbedingungen?),
- die Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse,
- die erforderlichen technischen Informationen, also Festlegungen darüber,
    - welche Dienste (z. B. telnet, ftp, http) zur Verfügung gestellt werden,
    - welche IT-Plattformen, Anwendungen und Datenformate unterstützt werden,
    - welche Verfügbarkeit zu gewährleisten ist (Performance, maximale Ausfallrate),
    - wer was protokollieren darf bzw. muss, wo die Protokolldaten abgelegt werden und wer auf die Protokolldaten zugreifen darf (dies kann insbesondere in Notsituationen wichtig sein),
    - inwieweit ein regelmäßiger Austausch von Protokolldaten erfolgen soll,
    - welche Sicherheitsmaßnahmen gewährleistet werden müssen,
- eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden,
- eine Haftungs- bzw. Schadensersatzregelung (hierin sollten unter anderem die Bedingungen für die Trennung der Netzanbindung, Haftung bei Computenviren oder Hackerangriffen, Vertragsstrafen bei nicht erfüllter Leistung bzw. Haftungsübernahme bei Inanspruchnahme für fremde Inhalte geklärt sein),
- eine Regelung über Auskunftspflichten bei aufgetretenen Sicherheitslücken,
- eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen),
- eine Beschreibung, inwieweit weitere Vertragspartner in die Vereinbarung eingebunden werden, z. B. durch gemeinsame Nutzung von Applikationen oder als Dienstleister für einen der Vertragspartner,

- die Laufzeit der Vereinbarung (Technik entwickelt sich schnell weiter, d. h. auch die Vereinbarungen über deren Nutzung müssen ständig angepasst werden).

Die Vereinbarung sollte durch die Personen abgeschlossen werden, die auch für deren Einhaltung die Verantwortung tragen. Dafür ist zunächst zu klären, wer die Verantwortung für die Netzanbindung tragen sollte, da hier üblicherweise unterschiedliche Bereiche eines Unternehmens bzw. einer Behörde involviert sind. Sinnvollerweise sollte hierzu ein Team gebildet werden, bei dem zumindest der IT-Sicherheitsbeauftragte, der IT-Leiter, der Fachverantwortliche und der Datenschutzbeauftragte beteiligt sind. Bei kritischen Entscheidungen, z. B. ob die Verbindung wegen Problemen zeitweise getrennt werden soll, sollten **alle** oben genannten Personen beteiligt werden, da sich deren Interessen erfahrungsgemäß stark voneinander unterscheiden können.

Bevor eine Netzanbindung aktiviert wird, sollten alle Sicherheitsmängel auf beiden Seiten ausgeräumt worden sein. Hier sollte auch ein Weg gefunden werden, sich von dem Sicherheitsniveau seiner Partner zu überzeugen, beispielsweise durch Basis-Sicherheitschecks oder Stichproben vor Ort. Auf keinen Fall darf die Beseitigung von Sicherheitslücken in den Echtbetrieb verschoben werden, da die Erfahrung lehrt, dass diese niedriger priorisiert werden als reine Verfügbarkeitsprobleme.

Dritten sollten nur die Dienste zur Verfügung gestellt werden, die zum einen vertraglich vereinbart worden sind und zum anderen unbedingt erforderlich sind. Auf welche Bereiche des eigenen Netzes Dritten Zugriff gewährt wird, muss abhängig gemacht werden von der Art der bestehenden Beziehungen zwischen den Kommunikationspartnern und vom Vertrauen in die Kommunikationspartner. Bei ausländischen Partnern müssen unbedingt deren nationale Gesetze berücksichtigt werden, z. B. in den Bereichen Kryptographie bzw. Urheberrecht.

Falls durch die Netzanbindung Sicherheitsvorfälle auftreten, muss klar definiert sein, wer wann die Verbindung trennen darf, wer darüber zu informieren ist und welche Eskalationsschritte vorzusehen sind.

Prüffragen:

- Werden vor der Anbindung eines eigenen Netzes an Netze Dritter alle sicherheitsrelevanten Aspekte in einer Vereinbarung schriftlich festgelegt?
- Ist definiert, wer aus seinem Netz auf welche Bereiche und Dienste des jeweils anderen Netzes zugreifen darf?
- Sind Ansprechpartner sowohl für organisatorische als auch technische Fragestellungen der Netzanbindung benannt
- Sind alle Sicherheitslücken beseitigt und das geforderte Sicherheitsniveau nachweislich erreicht, bevor die Netzanbindung aktiviert wird?
- Ist für den Fall von Sicherheitsproblemen durch die Netzanbindung festgelegt, wer darüber zu informieren ist und welche Eskalationsschritte einzuleiten sind?

# M 5.88 Vereinbarung über Datenaustausch mit Dritten

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Ein Datenaustausch mit anderen Unternehmen und Behörden kann z. B. über Datenträgeraustausch oder E-Mail erfolgen. Neben den Sicherheitsmaßnahmen, die bereits beim sporadischen Datenaustausch zu beachten sind, sollten bei einem regelmäßigen Datenaustausch mit festen Kommunikationspartnern Vereinbarungen getroffen werden, um diesen möglichst reibungslos zu gestalten.

Eine solche Vereinbarung sollte folgende Bestandteile umfassen:

- Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse,
- die erforderlichen technischen Informationen, also Festlegungen darüber,
  - welche Anwendungen und Datenformate unterstützt werden,
  - welche Verfügbarkeit zu gewährleisten ist, also wie häufig beispielsweise die E-Mail zu lesen und wie schnell sie zu beantworten ist,
- welche Sicherheitsmaßnahmen beim Datenaustausch gewährleistet werden müssen, also z. B.
  - dass die Daten vor und nach dem Austausch auf Computer-Viren zu überprüfen sind,
  - wie die Daten vor Transportschäden und unbefugtem Zugriff zu schützen sind (verschlossene Behältnisse, Checksummen, Verschlüsselung),
  - wie das Schlüsselmanagement geregelt ist,
  - dass die Daten auf der Senderseite frühestens nach der Bestätigung des korrekten Empfangs gelöscht werden dürfen, falls eine Löschung erforderlich ist,
- eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden,
- eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen),
- eine Verpflichtung auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z. B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen.

Weitere Punkte, die in eine solche Vereinbarung aufgenommen werden sollten, finden sich in M 2.45 *Regelung des Datenträgeraustausches* und M 2.455 *Festlegung einer Sicherheitsrichtlinie für Groupware*.

Prüffragen:

- Sind für den regelmäßigen Datenaustausch mit festen Kommunikationspartnern die erforderlichen Sicherheitsmaßnahmen vereinbart?
- Sind Datenformate und die sichere Form des Datenaustauschs festgelegt?

- Sind Ansprechpartner sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse beim Datenaustausch mit Dritten benannt?
- Sind Verfügbarkeiten und Reaktionszeiten beim Datenaustausch mit Dritten vereinbart?
- Ist festgelegt, welche ausgetauschten Daten zu welchen Zwecken genutzt werden dürfen?

# M 5.89 Konfiguration des sicheren Kanals unter Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zwischen Rechnern einer Windows-Domäne müssen administrative Daten ausgetauscht werden. So tauschen beispielsweise Domänen-Controller einer Domäne Verwaltungsdaten aus. Generell werden dabei sensitive Daten transportiert, die abgesichert übertragen werden müssen. Schon unter Windows NT stand dafür der so genannte *Sichere Kanal* (englisch *Secure Channel*) zur Verfügung. Auch unter Windows ab Version 2000 wird dieser Mechanismus genutzt und muss entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten konfiguriert werden. Hierbei werden als Sicherheitsmechanismen die Authentisierung der beiden Kommunikationspartner, Verschlüsselung zur Wahrung der Vertraulichkeit und Signaturen zur Absicherung der Integrität eingesetzt.

Die Konfiguration des sicheren Kanals erfolgt über Gruppenrichtlinien. Bei deren Konfiguration ist Folgendes zu berücksichtigen:

- Die gegenseitige Authentisierung ist immer gewährleistet, Verschlüsselung und Signatur können jedoch unabhängig voneinander gefordert werden. Unterstützt der Kommunikationspartner die geforderte Absicherung nicht, wird diese nicht eingesetzt. Die Kommunikation erfolgt dann ungesichert.
- Verschlüsselung oder Signatur können als notwendige Voraussetzung für die Kommunikationsaufnahme spezifiziert werden. Unterstützt der Kommunikationspartner die Absicherung nicht, wird keine Kommunikation aufgebaut. Dies kann zum Beispiel zur Folge haben, dass sich Clients nicht an einer Domäne anmelden können. Diese Option sollte nur aktiviert werden, wenn alle IT-Systeme einer Domäne und alle IT-Systeme aller vertrauten Domänen das Verschlüsseln und Signieren unterstützen.
- Die Stärke des zur Verschlüsselung erzeugten Sitzungsschlüssels lässt sich vom Windows NT Niveau auf das Niveau von Windows 2000 oder höher erhöhen. Von dieser Option darf jedoch nur Gebrauch gemacht werden, wenn alle IT-Systeme einer Domäne und alle IT-Systeme aller vertrauten Domänen ausschließlich mit einer Version ab Windows 2000 betrieben werden. Ist sie aktiviert, können sich IT-Systeme, auf denen frühere Betriebssysteme installiert sind, nicht mehr an der Domäne anmelden.

Die für die Konfiguration relevanten Gruppenrichtlinienparameter unter Windows 2000 sind:

- Sicherer Kanal: Daten des sicheren Kanals digital signieren (wenn möglich)
- Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)
- Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)
- Sicherer Kanal: Starker Sitzungsschlüssel erforderlich (Verschlüsselung mit 128 Bit, immer wenn Windows 2000 oder höher)

Diese Parameter finden sich unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*.

Bei Clients ab Windows XP lauten die Einstellungen:

- Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)
- Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)
- Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Verschlüsselung mit 128 Bit, immer wenn Windows 2000 oder höher)
- Domänenmitglied: Änderungen von Computerkennwörtern deaktivieren
- Domänenmitglied: Maximalalter von Computerkennwörtern (Standard: 30 Tage, sollte im Normalfall nicht auf größere Werte geändert werden)

Diese Parameter finden sich unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*. Alle Optionen sollten entsprechend aktiviert werden.

Prüffragen:

- Ist der Sichere Kanal unter Windows entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten konfiguriert worden?
- Wurden bei der Konfiguration des Sicheren Kanals unter Windows alle relevanten Gruppenrichtlinienparameter berücksichtigt?

# M 5.90 Einsatz von IPSec unter Windows

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zur Absicherung der Kommunikation bietet Windows eine IPSec-konforme Implementierung an. IPSec ist ein internationaler Standard, der die kryptographische Absicherung IP-basierter Kommunikation erlaubt. Es muss jeweils im Einzelfall entschieden werden, ob IPSec zur Kommunikationsabsicherung eingesetzt werden soll. Dies ist schon bei der Planung des Windows-Einsatzes zu berücksichtigen und mittels einer Richtlinie zu definieren.

IPSec umfasst folgende Funktionen:

- Gegenseitige Authentisierung der Kommunikationsendpunkte
- Sicherung der Integrität der übertragenen Daten durch digitale Signaturen
- Sicherung der Vertraulichkeit der übertragenen Daten oder des gesamten IP-Datenpakets durch Verschlüsselung (Tunnel-Modus)

Allgemeine Hinweise zur Auswahl geeigneter kryptographischer Verfahren finden sich in M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*. Als Hash-Verfahren sollte beim Einsatz von IPSec ein Algorithmus der SHA-2-Familie verwendet werden, also SHA-224, SHA-256, SHA-384 oder SHA-512.

Diese werden etwa im IPSec-Client, der auf Clients ab Windows Vista Teil der Firewall ist, unterstützt. Die Funktion ist seit Windows 7 standardmäßig und unter Windows Vista seit dem Service Pack 1 verfügbar. Ohne Service Pack 1 unterstützt dieser IPSec-Client unter Windows Vista nur die schwächeren Hash-Verfahren MD5 und SHA1. Diese sollten nicht mehr eingesetzt werden.

Damit neben der Integrität und Vertraulichkeit der übertragenen Daten auch sichergestellt werden kann, dass die Daten zwischen den korrekten Kommunikationspartnern ausgetauscht werden, müssen sich diese authentisieren. Die Windows-Implementierung erlaubt folgende Verfahren zur Authentisierung der Kommunikationsendpunkte:

- Es kann das Kerberos-Protokoll eingesetzt werden, sofern sich beide Kommunikationspartner innerhalb derselben Active-Directory-Struktur befinden. Hierbei findet die normale Windows Authentisierung statt. Dieses Verfahren beruht auf symmetrischen Schlüsseln, die zur Verschlüsselung der so genannten Kerberos-Tickets eingesetzt werden.
- Es können X.509-Zertifikate eingesetzt werden. Hierbei erfolgt die Authentisierung, basierend auf asymmetrischen Schlüsseln, auf Grund der Zertifikatsinformationen. In der Regel wird ein so genanntes Challenge-Response-Verfahren eingesetzt. Es überprüft, ob der zu authentisierende Benutzer im Besitz des korrekten privaten Schlüssels ist. Die IPSec-Funktion *DirectAccess* verwendet diese Variante. Die Authentifizierungsmethode mit X.509-Zertifikaten sollte genutzt werden, wenn ein Internetzugriff, ein Remotezugriff auf Unternehmensressourcen, die Kommunikation mit externen Geschäftspartnern oder die Verwendung von Computern ohne das Kerberos-Protokoll erforderlich sind.

Im Rahmen des ersten IPSec-Verbindungsaufbaus werden zunächst die nachfolgend zu benutzenden Algorithmen und Verfahren zur Authentisierung, Integritätssicherung und Wahrung der Vertraulichkeit zwischen den Kommunikationspartnern ausgehandelt und in der so genannten *Security Association* (SA) gespeichert.

Diese in der SA gespeicherten Parameter werden für alle zukünftigen Kommunikationsverbindungen benutzt, bis die Gültigkeit der SA-Parameter erlischt und die Verfahren neu ausgehandelt werden. Dies erfolgt in der Regel vollautomatisch durch die Komponenten der IPSec-Implementierung.

Für die eigentliche Verschlüsselung müssen Schlüssel, der so genannte Master- und der Session-Key (Sitzungsschlüssel), generiert werden. In der Regel wird der Master-Key, von dem alle weiteren Schlüssel abgeleitet werden, pro Verbindung nur einmal erzeugt, der Session-Key hingegen periodisch mehrfach. Es besteht die Möglichkeit, auch den Master-Key periodisch neu zu erzeugen, was jedoch eine erneute Authentisierung der Kommunikationspartner erfordert. In der Regel erfolgt die erneute Authentisierung automatisch durch die Komponenten der IPSec-Implementierung, so dass die Performance im Wesentlichen dadurch beeinflusst wird.

IPSec kennt zwei verschiedene Methoden zur Absicherung der Kommunikation: ESP (Encapsulated Security Payload) und AH (Authentication Header). Ab Windows Server 2008 wird AH nicht mehr unterstützt, da diese Methode aufgrund der damit verbundenen Nachteile (keine Umsetzung von Netzwerkadressen per NAT möglich) kaum praktische Bedeutung hat.

Zur Steuerung der IPSec-basierten Kommunikation bietet Windows so genannte IPSec-Richtlinien (IPSec-Policies) an, die angeben, welche IPSec-Parameter für eine Verbindung zu benutzen sind. Ab Windows Vista und Windows Server 2008 werden die IPSec-Richtlinien auch *Verbindungssicherheitsregeln* genannt. Über verschiedene Richtlinien lässt sich erreichen,

- dass IT-Systeme ausschließlich IPSec-geschützte Verbindungen annehmen,
- dass IT-Systeme IPSec-geschützte Verbindungen beim Kommunikationspartner anfordern, jedoch auch ungeschützte Kommunikation zulassen, falls der Partner kein IPSec-Protokol unterstützt,
- oder dass die IPSec-basierte Kommunikation ausgeschlossen wird.

Windows bietet ab Version 2000 drei vordefinierte IPSec-Richtlinien an, die ab Windows Vista und Windows Server 2008 entfallen:

- Client (nur Antwort): für IT-Systeme, die nur auf Anforderung des Kommunikationspartners die IPSec-Absicherung aushandeln und ansonsten keine Kommunikationsabsicherung betreiben.
- Server (Sicherheit anfordern): für IT-Systeme, die von ihren Kommunikationspartnern IPSec-geschützte Verbindungen anfordern, jedoch auch Verbindungen ohne Schutz akzeptieren, falls der Kommunikationspartner IPSec nicht unterstützt.
- Server (Sicherheit erforderlich): für IT-Systeme, die ausschließlich IPSec-geschützte Verbindungen aufbauen sollen und ungesicherte Verbindungswünsche ablehnen.

Diese vordefinierten Regeln können den lokalen Anforderungen detailliert angepasst werden. Dabei empfiehlt es sich, zunächst eine Kopie anzulegen und die Veränderungen an der Kopie der Richtlinie durchzuführen.

Im Rahmen einer IPSec-Richtlinie werden so genannte Filterregeln genutzt, um unterschiedliche IPSec-Parameter, zum Beispiel in Abhängigkeit vom verwendeten Protokoll, definieren zu können. Beispielsweise kann festgelegt werden, dass HTTP unverschlüsselt bleibt, FTP dagegen immer verschlüsselt wird.

Die Windows-Versionen ab Windows Vista ermöglichen die Konfiguration der IPSec-Richtlinien über Gruppenrichtlinien unter *Computerkonfiguration* | *Windows-Einstellungen* | *Windows-Firewall mit erweiterter Sicherheit* | *Verbindungssicherheitsregeln,* bei Windows Server 2008 findet sich der Konfigurationseditor unter *Verwaltung* | *Windows-Firewall mit erweiterter Sicherheit* | *Verbindungsregeln. Ab Windows* Vista und Windows Server 2008 stellt Microsoft keine vordefinierten IPSec-Richtlinien zur Verfügung. Der *Assistent für neue Verbindungssicherheitsregeln* hilft aber bei deren Konfiguration. IPSec wird entweder über Gruppenrichtlinien oder lokal im Eigenschaftsdialog für Netzverbindungen aktiviert. Die Aktivierung im Eigenschaftsdialog steht ab Windows Vista und Windows Server 2008 nicht zur Verfügung. Hier wird IPSec durch die Erstellung von Verbindungssicherheitsregeln in der Windows-Firewall konfiguriert und aktiviert.

Ab Windows Server 2008 wurde die Konfiguration von Regeln für die lokale Firewall und IPSec in der Oberfläche zusammengeführt, um die Administration zu vereinfachen und Fehlerquellen aus sich widersprechenden IPSec- und Firewallregeln zu beseitigen.

Generell ist für die Nutzung von IPSec unter Windows Folgendes zu berücksichtigen:

- Vor dem Einsatz von IPSec muss geprüft werden, ob die mit der Aktivierung verbundenen Performance-Einbußen toleriert werden können. Unter Umständen sollte über den Einsatz von Netzadaptern mit TCP/IP-Offload-Engine (TOE) nachgedacht werden, um rechenintensive Aufgaben bezüglich des TCP/IP-Protokollstacks auf dem Netzadapter auszuführen, um die CPU zu entlasten.
- Zum stärkeren Schutz der Session-Keys sollte die Option *Perfect Forward Secrecy (PFS)* aktiviert sein. Dies stellt sicher, dass nach der Kompromittierung eines Session-Keys ausschließlich die mit diesem einzelnen Session-Key verschlüsselten Daten entschlüsselt werden können. Dies wird dadurch erreicht,
- dass ein Session-Key, der zum Verschlüsseln von Daten benutzt wurde, nicht benutzt wird, um weitere Schlüssel zu erzeugen, und
- dass das Schlüsselausgangsmaterial, das zum Erzeugen eines Session-Keys benutzt wurde, nicht ein weiteres Mal zum Erzeugen eines Session-Keys benutzt wird.
  Dies hat zwar geringe Performance-Einbußen zur Folge, diese fallen in der Regel jedoch nicht ins Gewicht.
- Für Verbindungen mit hohem Schutzbedarf kann auch für den Master-Key die Option PFS aktiviert werden. Dies führt jedoch zu stärkeren Performance-Einbußen als PFS für Session-Keys, da hier jedes Mal eine Authentisierung der Kommunikationspartner durchgeführt werden muss.
- Für jeden konkreten Fall muss entschieden werden, welche Mechanismen und Verfahren zur Authentisierung und zur Sicherung der Integrität und Vertraulichkeit im Rahmen der IPSec-Verhandlung während des Verbindungsaufbaus zur Verfügung stehen sollen. Es muss berücksichtigt werden, dass zwischen den Kommunikationspartnern jeweils mindestens ein Verfahren existieren muss, das beide Partner unterstützen.
- Werden eigene IPSec-Richtlinien erstellt, so muss unbedingt immer eine so genannte *Standardantwortregel* definiert werden. Diese greift dann, wenn keine andere Filterregel der Richtlinie Anwendung findet. Fehlt die *Standardantwortregel,* kann es vorkommen, dass keine Verbindung zwischen den Kommunikationspartnern zustande kommt. Die Standardantwortregel wird für den Einsatz von *DirectAccess* nicht gebraucht.

- Die Filterregeln einer IPSec-Richtlinie erlauben es, unter anderem die IP-Sec-Absicherung auch an die IP-Adresse des Kommunikationspartners zu binden, so dass die Verschlüsselung in Abhängigkeit vom Kommunikationspartner aktiviert werden kann.
- Wird zur Authentisierung der Kerberos-Mechanismus verwendet, erfolgt die Authentisierung nicht IPSec-abgesichert, da Kerberos nicht im Rahmen der IPSec-Verbindung abgewickelt wird.
  Nach Einspielen des Windows 2000 Service Pack 1 kann die IPSec-Absicherung auch für das Kerberos-Protokoll aktiviert werden. Dazu ist jedoch ein Eingriff in die Registry notwendig (siehe dazu auch die Microsoft Knowledgebase Artikel KB254728 und KB811832):
  Unter *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSEC* (ab Windows Vista unter *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *PolicyAgent*) muss der Schlüssel *NoDefaultExempt* vom Typ *REG_DWORD* mit dem Wert 1 eingetragen werden.
- Um das korrekte Funktionieren des IPSec-Verbindungsaufbaus und der IPSec-Kommunikation zu prüfen, stellt Windows 2000 das Programm *ipsecmon.exe*, Windows XP das MMC Snap-in *IP-Sicherheitsmonitor* und ab Windows Vista und Windows Server 2008 das Snap-in *Windows-Firewall mit erweiterter Sicherheit* zur Verfügung. Das Programm oder Snap-in kann zur Eingrenzung der Fehlerquelle benutzt werden, falls Probleme mit IPSec-Verbindungen bestehen. Das Programm ist jedoch relativ einfach aufgebaut, so dass es nur zu einer ersten Ursachenforschung verwendet werden kann.
- IPSec sollte unter anderem in Kombination mit EFS-verschlüsselten Dateien eingesetzt werden (siehe auch M 4.147 *Sichere Nutzung von EFS unter Windows*), wenn diese auf Servern lagern und abgesichert über das Netz zu einem Client transportiert werden sollen. Außer IPSec kann auch jeder andere Mechanismus zur Absicherung der Netzkommunikation genutzt werden, um serverseitig gespeicherte EFS-Dateien beim Transport zu schützen.
- Soll die Kommunikation mit einem System, auf dem nicht Windows als Betriebssystem installiert ist, mittels IPSec geschützt werden, so ist die Interoperabilität und korrekte Funktion in einem praktischen Test zu überprüfen. Zwar ist das IPSec-Verfahren standardisiert, im Einzelfall ergeben sich jedoch unter Umständen auch bei standardisierten Verfahren Kompatibilitätsprobleme.

Prüffragen:

- Ist eine IPSec-Richtlinie vorhanden?
- Ist die Performance der beteiligten IT-Systeme für eine IPSec-Kommunikation ausreichend?
- Wurde die Option Perfect Forward Secrecy (PFS) aktiviert?
- Wurde überprüft, ob der IPSec-Verbindungsaufbau korrekt durchgeführt wird?
- Wurde eine Standardantwortregel definiert?

# M 5.91 Einsatz von Personal Firewalls für Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Personal Firewalls kontrollieren und unterbinden Zugriffe auf Clients über angebundene IT-Netze bzw. von Clients auf diese Netze. Je nach Art des Netzdienstes und der Richtung des Verbindungsaufbaus kann von der Personal Firewall des Client ein Kommunikationsaufbau gestattet oder abgewiesen werden. Eine Personal Firewall könnte beispielsweise so konfiguriert sein, dass alle Verbindungen, die von dem Client aufgebaut werden, erlaubt und alle von außen ankommenden Anfragen blockiert werden.

Personal Firewalls können nach unterschiedlichen Prinzipien arbeiten:

- Zustandslose ("stateless") Personal Firewalls entscheiden anhand von Eigenschaften wie Quell- und Ziel-Adressen oder -Ports der bei der Kommunikation übertragenen Datenpakete darüber, ob die Verbindung erlaubt oder abgewiesen werden soll. Im Wesentlichen wird hierzu die Absender- bzw. Zieladresse und Port-Nummer des Dienstes herangezogen. Zustandslose Personal Firewalls können oft mit präparierten Paketen umgangen werden.
- Kontextsensitive ("stateful") Personal Firewalls berücksichtigen bei der Entscheidung auch vorangegangene Pakete. So kann eine kontextsensitive Personal Firewall ein zu prüfendes Paket in den Kontext einer Verbindung bringen und nur dann erlauben, wenn die Verbindung selbst zulässig ist. Nicht in den Verbindungskontext passende Pakete werden verworfen.
- Anwendungsfirewalls (Applicationfirewall) können Netzverkehr auf Basis der Anwendung, die eine Verbindung aufbauen will, prüfen. Dazu verfügt die Applikations-Firewall über eine Whitelist, in der die kommunikationsberechtigten Anwendungen eingetragen sind. Anwendungen, die nicht auf der Whitelist stehen, können keine Verbindungen über das Netz aufbauen oder entgegennehmen.

Viele Betriebssysteme beinhalten bereits eine Personal Firewall. Diese braucht oft nur aktiviert werden und je nach Betriebssystem stehen unterschiedlich umfangreiche Funktionen zur Verfügung. Zusätzlich werden von diversen Drittherstellern Sicherheitslösungen ("Security Suite") angeboten, die unter anderem eine Personal Firewall beinhalten. Oft sind die im Betriebssystem integrierten Personal Firewalls im Gegensatz zu den Sicherheitslösungen weniger umfangreich und unkomfortabler. Dafür können diese bordeigenen Lösungen sofort aktiviert werden und es entstehen keine zusätzlichen Kosten für die Beschaffung. Wenn eine Personal Firewall eingesetzt werden soll, ist zu entscheiden, ob die bordeigene Personal Firewall oder eine Lösung von einem Dritthersteller eingesetzt werden soll, auf einen Mischbetrieb sollte verzichtet werden.

### Einsatzumgebungen

Als alleinige Maßnahme für die Absicherung eines Behörden- oder Unternehmensnetzes gegenüber Angriffen aus dem Internet sind Personal Firewalls ungenügend. Der alleinige Einsatz von Personal Firewalls bringt folgende Nachteile mit sich:

- Alle direkt ans Internet angeschlossenen Clients müssen besonders gehärtet werden, d. h. die potentiellen Schwachstellen des Betriebssystems

müssen behoben werden, da der Client nicht durch andere IT-Systeme, wie Sicherheitsgateways, geschützt wird.
- Wie bei jeder dezentral eingesetzten Software ist das Management und die Auswertung der Protokolldaten der einzelnen Personal Firewalls aufwendig.

Es sollte geprüft werden, auf welchen Clients und mit welchen Rahmenbedingungen eine Personal Firewall eingesetzt werden soll. Da Clients in einem LAN durch ein Sicherheitsgateway geschützt werden, kann auf den Einsatz von Personal Firewalls auf den Clients in der Regel verzichtet werden. Bei einem höheren Schutzbedarf sollte der Einsatz von Personal Firewalls geprüft werden.

Mobile genutzte IT-Systeme wie Laptops sollten unbedingt durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz geschützt werden, wenn sie direkt an das Internet angeschlossen werden.

Ebenso sollten auf Internet-PCs, d. h. Computern, die ausschließlich für die Nutzung des Internets bereitgestellt werden und keine Verbindung zum Behörden- bzw. Unternehmensnetz haben, Personal Firewalls installiert sein.

Aufgrund des vielfältigen Funktionsumfangs der verschiedenen Varianten von Personal Firewalls und deren Komplexität muss dabei jedoch eine kompetente Administration sichergestellt sein, die Benutzer sollten sie weder selber konfigurieren müssen noch die Einstellungen ändern dürfen.

**Personal Firewalls als Bestandteil einer Sicherheitslösung (Security Suite)**

Personal Firewalls werden inzwischen von einer Vielzahl von Herstellern angeboten. Zum Teil ist der Einsatz für private Anwender sogar kostenlos. Im kommerziellen oder behördlichen Umfeld müssen jedoch in der Regel Lizenzen erworben werden. Personal Firewalls werden häufig in Fachzeitschriften getestet. Die Ergebnisse dieser Tests können bei der Auswahl eines für den vorliegenden Einsatzzweck geeigneten Produkts helfen.

Als Ergänzung zu einem zentralen Sicherheitsgateway (Firewall) kann der Einsatz von Personal Firewalls als Teil einer Sicherheitslösung durchaus sinnvoll sein. Prinzipiell ist es z. B. bei umfangreichen Sicherheitslösungen von Drittherstellern, die eine Personal Firewall beinhalten, möglich, mit ihnen die Prüfung auf Schadsoftware, die über E-Mail, Java, ActiveX oder ähnliche Mechanismen übertragen werden kann, auf den Clients vorzunehmen. Hierfür können Mechanismen wie Sandboxing eingesetzt werden, mit denen der Zugriff von Applikationen, die vom Internet auf das lokale System übertragen werden (Java, ActiveX, etc.), eingeschränkt werden kann. Mit diesen oft umfangreichen Sicherheitslösungen wird die Aufgabe der Prüfung auf Schadsoftware dezentralisiert und damit das Firewall-System entlastet. Ein weiterer Vorteil liegt darin, dass die Problematik der Filterung von verschlüsselten Daten auf der Firewall umgangen werden kann.

**Konfiguration**

Bei Konfiguration und Betrieb einer Personal Firewall sollten folgende Aspekte berücksichtigt werden:

- Die Filterregeln sollten so restriktiv wie möglich eingestellt werden. Dabei gilt der Grundsatz: *Alles was nicht ausdrücklich erlaubt ist, ist verboten.* Es wird empfohlen, dass abgehende Verbindungen nur von dafür zugelassenen Anwendungen oder Diensten aufgebaut werden dürfen. Ba-

sierend auf der IP-Adresse des Zielsystems, der Port-Nummer des benötigten Dienstes und der zugreifenden Anwendung bzw. des zugreifenden Dienstes könnten folgende vom Client aufgebaute Zugriffe beschränkt bzw. erlaubt werden:

- zu Datei- und Druck-Servern
- zum Internet für den Browser über das Sicherheitsgateway
- zum E-Mail- und Kalender-Server für die E-Mail- und Kalenderanwendung
- zu Update-Servern im lokalen Netz für die Aktualisierung von Betriebssystem, Anwendungen und insbesondere des Virenschutzprogramms
- Kommunikation zum eventuell vorhandenen zentralen Protokollierungsdienst für alle Dienste und Anwendungen, die Meldungen protokollieren
  Ankommende Verbindungen sollten auf die für Fernwartung, Software-Verteilung, Systemaktualisierung und Überwachung erforderlichen Dienste und die hierfür verwendeten Server-Systeme beschränkt werden.
- Die Filterregeln der Personal Firewall sollten nach der erstmaligen Konfiguration daraufhin getestet werden, ob die erlaubten Ereignisse zugelassen und unerlaubte Ereignisse unterbunden werden.
- Die korrekte Konfiguration der Filterregeln sollte in sporadischen Abständen überprüft werden, wenn die Installation des Clients nicht ohnehin regelmäßig gelöscht und anhand eines Festplatten-Abbildes (Images) erneut aufgespielt wird, z. B. bei Internet-PCs.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten die Regeln der Personal Firewall auch speziellen Programmen zugeordnet werden. Dadurch kann unter Umständen erkannt und verhindert werden, dass ein anderes als die vorgesehenen Client-Programme Verbindungen zu Rechnern im Internet aufbaut oder annimmt.
- Da viele der Prüfmechanismen einer Personal Firewall auf aktuellen Erkenntnissen beruhen, müssen vom Hersteller veröffentlichte Patches bzw. Updates regelmäßig eingespielt werden. Dabei ist sicherzustellen, dass die dafür erforderlichen Dateien von einer vertrauenswürdigen Quelle, beispielsweise direkt vom Hersteller, bezogen werden.
- Die Personal Firewall muss so konfiguriert werden, dass die Benutzer nicht durch eine Vielzahl von Warnmeldungen belästigt werden, die sie nicht interpretieren können.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten sicherheitsrelevante Ereignisse protokolliert werden. Die Protokolldaten sollten regelmäßig durch fachkundiges Personal ausgewertet werden. Die Hinweise in M 2.110 *Datenschutzaspekte bei der Protokollierung* sind zu beachten.

Einige Produkte verfügen über die Möglichkeit, mit einer sehr restriktiven Grundkonfiguration zu starten und danach die Einstellungen im laufenden Betrieb zu verfeinern. Dabei wird jedes Mal, wenn ein sicherheitsrelevantes Ereignis auftritt, für das bisher noch keine eindeutige Regel existiert, der Benutzer gefragt, ob dieses Ereignis zulässig ist. Ein Beispiel für ein solches sicherheitsrelevantes Ereignis ist der Zugriff eines bestimmten installierten Programms auf das Internet. Auf der Grundlage der Antworten des Benutzers ermittelt die Personal Firewall Schritt für Schritt die gewünschte Konfiguration, z. B. die Filterregeln.

Der Vorteil dieser inkrementellen Konfiguration ist, dass dadurch die Komplexität der Administration reduziert werden kann. Nachteilig ist jedoch, dass Benutzer in der Regel nicht ohne Weiteres beurteilen können, ob ein bestimmtes Ereignis zulässig ist oder nicht. Die inkrementelle Konfiguration der Personal Firewall kann daher nur dann empfohlen werden, wenn den Benutzern entweder präzise Vorgaben gemacht werden, wie sie auf Rückfragen des Programms antworten sollen oder wenn dies unter Anleitung eines Administrators, z. B. durch telefonische Rückfragen, erfolgt.

Prüffragen:

- Existiert ein Konzept für den Einsatz von Personal Firewalls?
- Sind die Filterregeln der Personal Firewall so restriktiv wie möglich eingestellt?
- Wird die korrekte Konfiguration der Filterregeln der Personal Firewall regelmäßig getestet?
- Werden vom Hersteller veröffentlichte Patches bzw. Updates zur Behebung sicherheitsrelevanter Schwachstellen der Personal Firewall installiert?
- Wurde die Personal Firewall so konfiguriert, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können?

# M 5.92 Sichere Internet-Anbindung von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Für den ordnungsgemäßen Betrieb eines Internet-PCs ist die sichere Anbindung an das Internet aufgrund des speziellen Einsatzszenarios besonders wichtig. Die Internet-Anbindung sollte daher sorgfältig geplant werden. Dabei sollten folgende Teilaspekte berücksichtigt werden:

**Auswahl eines geeigneten Internet Service Providers (ISP)**

Die Anbindung an das Internet geschieht über einen ISP, der die für die Nutzung des Internets notwendige Technik und Dienstleistungen zur Verfügung stellt. Die Anbieter am Markt unterscheiden sich dabei in Bezug auf Umfang, Qualität und Preis der Dienstleistungen. Die Auswahl eines geeigneten ISPs muss anhand der Anforderungen an die Internet-Anbindung getroffen werden:

- Bietet der ISP die gewünschte Verbindungstechnik, d. h. Modem, ISDN, DSL usw., an?
- Erfüllt der ISP die Anforderungen an die minimale bzw. durchschnittliche Bandbreite und die Verfügbarkeit des Internet-Zugangs? Hierzu sollten auch Testberichte in Fachzeitschriften zu Rate gezogen werden.
- Bietet der ISP die benötigten Zusatzdienstleistungen an, z. B. für E-Mail oder News, oder soll hierfür auf einen weiteren Dienstleister zurückgegriffen werden?
- Stellt der ISP die erforderlichen Sicherheitsmechanismen für die angebotenen Dienstleistungen bereit? Werden beispielsweise Proxy-Server für WWW und FTP zur Verfügung gestellt und kann E-Mail auch SSL-geschützt abgeholt werden?
- Macht der ISP Angaben zum Umgang mit personenbezogenen Daten oder mit Informationen über die Behörde bzw. das Unternehmen? Decken sich diese Angaben mit den eigenen Anforderungen an den Datenschutz?
- ISPs bieten unterschiedliche Preismodelle für die Internet-Anbindung an. Beispielsweise kann zwischen pauschalen, zeitabhängigen und volumenabhängigen Gebühren unterschieden werden. Ist das Preismodell für den Einsatzzweck des Internet-PCs geeignet?
- Anhand der Anforderungen an die Verfügbarkeit der Internet-Anbindung sollte geprüft werden, ob es erforderlich ist, aus Redundanzgründen Verträge mit zwei oder sogar mehr Providern abzuschließen.

Weitere Empfehlungen zur geeigneten Auswahl eines Internet Service Providers finden sich in Maßnahme M 2.176 *Geeignete Auswahl eines Internet Service Providers*.

**Beschaffung geeigneter Netzkomponenten für die Internet-Anbindung**

Je nachdem, ob mit der Internet-Anbindung nur ein einzelner Internet-PCs oder ein ganzer Pool solcher Internet-PCs versorgt werden soll, ergeben sich unterschiedliche Anforderungen an die hierfür erforderlichen Hardware-Komponenten. Bei der Beschaffung sollten die folgenden Aspekte berücksichtigt werden:

- Falls ein einzelner Internet-PC an das Internet angebunden werden soll, kommt in vielen Fällen ein Modem oder eine ISDN-Karte zum Einsatz. Kompatibilitätsprobleme zwischen diesen Geräten und dem Einwahl-Server beim ISP treten inzwischen nur noch selten auf. Modems und ISDN-

Karten sind sehr preiswert und lassen sich bei technischem Defekt schnell ersetzen. Falls erhöhte Anforderungen an die Verfügbarkeit bestehen, sollten Ersatzgeräte vorgehalten werden.
- Falls ein Internet-PC-Pool versorgt werden soll oder falls aus anderen Gründen hohe Bandbreiten benötigt werden, kommen häufig spezielle Router, z. B. DSL-Router, für die Internet-Anbindung zum Einsatz. Falls die Geräte nicht vom ISP zur Verfügung gestellt werden, ist eine präzise Abstimmung erforderlich, um Kompatibilitätsprobleme zu vermeiden. Bei erhöhten Verfügbarkeitsanforderungen sollte geprüft werden, ob der ISP entsprechende Dienstleistungen anbietet, beispielsweise Austausch des Routers innerhalb einer vorgegebenen Zeitspanne, Vorhalten eines Ersatzgerätes, usw.

**Sichere Konfiguration und Betrieb der Internet-Anbindung**

Für den sicheren und ordnungsgemäßen Betrieb der Internet-Anbindung sollten folgende Empfehlungen berücksichtigt werden:

- Alle Konfigurationseinstellungen für die Internet-Anbindung sollten dokumentiert werden, damit sie bei Datenverlust schnell wiederhergestellt und Abweichungen erkannt werden können.
- Für Zugriffe über die Protokolle HTTP und FTP sollten möglichst so genannte Proxy-Server verwendet werden. Diese Proxy-Server leiten Anfragen von Clients als "Stellvertreter" an den gewünschten HTTP- bzw. FTP-Server weiter. Dadurch ergibt sich unter anderem der Vorteil, dass restriktivere Regeln auf evtl. eingesetzten Paketfiltern konfiguriert werden können. ISP betreiben in der Regel entsprechende Proxy-Server.
- Server beim ISP oder im Internet, die öfter genutzt werden, beispielsweise E-Mail-Server, Proxy-Server usw., sollten immer über ihre IP-Adresse angesprochen werden. Diese IP-Adressen sollten in allen betroffenen Komponenten fest eingestellt werden. Dadurch verringert sich die Gefahr durch so genannte DNS-Spoofing-Angriffe.
- Falls ein Internet-Zugang mit dynamischen IP-Adressen genutzt wird, sollte ab und zu die Verbindung getrennt werden, damit dem Client bei der nächsten Einwahl eine neue IP-Adresse zugeordnet wird. Dies ist besonders wichtig bei pauschalen Gebühren ("flat rate"). Durch solche Wechsel der IP-Adresse werden gezielte Angriffe erschwert.
- Voreingestellte Passwörter, z. B. für die Einwahl beim Internet Service Provider, müssen geändert werden. Empfehlungen hierzu finden sich in M 2.11 *Regelung des Passwortgebrauchs*.
- Der Zugriff auf die Konfigurationsdateien für die Internet-Anbindung sollte auf die zuständigen Administratoren beschränkt werden, wenn das verwendete Betriebssystem dies zulässt.
- Falls die verwendete Kommunikations-Software oder die eingesetzten Modem-, ISDN- oder DSL-Geräte Funktionen zur Fernsteuerung bieten, müssen diese deaktiviert oder gut geschützt werden.
- Falls die Internet-Anbindung durch Einwahl erfolgt, sollten die Rufnummern für die Einwahl beim ISP fest eingetragen werden.
- Das Modem bzw. die ISDN-Komponente sollte die Verbindung unterbrechen, wenn der Benutzer sich abmeldet bzw. die Internet-Anwendung beendet.
- Falls für die Authentisierung bei der Einwahl beim Internet Service Provider zwischen dem PAP- und dem CHAP-Verfahren gewählt werden kann, sollte besser CHAP genutzt werden. Dadurch wird vermieden, dass die Authentisierungsdaten im Klartext übertragen werden (siehe auch M 5.50 *Authentisierung mittels PAP/CHAP*).

- Alle nicht benötigten Funktionen, wie z. B. das Aktivieren der Kommunikationsverbindung von außen, müssen abgeschaltet werden. Eingehende Anrufe dürfen nicht angenommen werden.
- Die verwendeten Zieladressen und die eingestellten Parameter sollten gelegentlich kontrolliert werden (siehe auch M 5.29 *Gelegentliche Kontrolle programmierter Zieladressen und Protokolle*).

Prüffragen:

- Erfüllt der Internet Service Provider die Anforderungen an die Verfügbarkeit des Internet-Zugangs?
- Stellt der ISP die erforderlichen IT-Sicherheitsmechanismen für die angebotenen Dienstleistungen bereit?
- Genügen die Angaben des ISP zum Umgang mit persönlichen Daten den Anforderungen der Institution an den Datenschutz?
- Ist die Beschaffung geeigneter Netzkomponenten für die Internet-Anbindung mit den Anforderungen der Institution abgestimmt?
- Sind die Konfigurationseinstellungen für die Internet-Anbindung dokumentiert?
- Ist der Zugriff auf die Konfigurationsdateien für die Internet-Anbindung auf die zuständigen Administratoren eingeschränkt?
- Sind bei der eingesetzten Kommunikations-Software und Hardware die Funktionen zur Fernsteuerung deaktiviert oder gegen unautorisierte Zugriffe geschützt?
- Bei Internet-Anbindung durch Einwahl: Sind die Rufnummern des ISP fest eingetragen?
- Ist sichergestellt, dass Authentisierungsdaten von Internet-PCs nicht im Klartext übertragen werden?
- Sind auf Internet-PCs nicht benötigte Funktionen und Dienste für die Internet-Anbindung abgeschaltet beziehungsweise deaktiviert?

# M 5.93 Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das World Wide Web (WWW) ist sicherlich einer der wichtigsten Dienste, die im Internet angeboten werden. Neben dem reinen Abrufen von Informationen dient es heute auch als Plattform für interaktive Angebote, wie z. B. im E-Business und E-Government. Auf Internet-PCs wird daher in den meisten Fällen ein Browser, d. h. ein Client-Programm für die Nutzung von WWW-Angeboten, benötigt. Populäre WWW-Browser sind z. B. *Firefox*, *Microsoft Internet Explorer* und *Opera*, *Google Chrome* und *Safari*.

Die Browser-Technik hat sich rasant weiterentwickelt. Von der ursprünglichen Funktion, Text und Bilder aus dem Internet zu laden und anzuzeigen, haben sich WWW-Browser zu universellen Frontends für netzbasierte Anwendungen entwickelt. Browser können eine Vielzahl unterschiedlicher Medienformate anzeigen und abspielen und dienen außerdem als Ablaufumgebung für Programme und Skripten, so genannten aktiven Inhalten. Zu letzteren gehören unter anderem die Technologien *Java*, *Javascript* und *ActiveX*. Der Funktionsumfang moderner Browser kann durch so genannte *Plug-Ins* zusätzlich erweitert werden.

Diese Vielzahl von Funktionen bringt komplexe Konfigurationsmöglichkeiten und potentielle Sicherheitsprobleme mit sich. Die nachfolgenden Empfehlungen zur Konfiguration von Browsern beim Einsatz von Internet-PCs sollen diesen Sicherheitsaspekten Rechnung tragen.

**Installation**

Die Grundsatzempfehlung, nur benötigte Software-Komponenten zu installieren, gilt für WWW-Browser ganz besonders, speziell für die zahlreichen verfügbaren Plug-Ins. Diese dienen meist dazu, bestimmte Medienformate, z. B. Videos oder Radioprogramme, anzuzeigen oder abzuspielen. Dabei besteht die grundsätzliche Gefahr, dass durch Design- oder Implementierungsfehler in den Plug-Ins beim Aufruf entsprechender Webseiten unerwünschte Aktionen ausgelöst werden, z. B. Manipulation oder Kompromittierung lokaler Daten. Es sollten daher nur die Plug-Ins installiert werden, die für die tägliche Arbeit auch wirklich erforderlich sind.

Software-Schwachstellen sind nicht nur in Plug-Ins, sondern vielfach auch in Browsern selbst bekannt geworden. Diese Schwachstellen können dazu ausgenutzt werden, Sicherheitsmechanismen zu umgehen oder anderweitig Schäden auszulösen. Browser-Hersteller veröffentlichen daher häufig Patches, Updates oder Anleitungen zur Behebung dieser Sicherheitslücken. Die Administration sollte sich daher regelmäßig auf den Webseiten des jeweiligen Browser-Herstellers über aktuelle Sicherheitslücken informieren und evtl. bereitgestellte Updates bzw. Patches installieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Ein weiteres Problemfeld ist der Aufruf externer Programme aus dem Browser heraus. Die meisten Browser bieten die Möglichkeit, Dateien nach dem Download direkt mit dem zugeordneten Anwendungsprogramm zu öffnen oder zu starten. Da die heruntergeladenen Dateien oft aus unbekannten Quellen

stammen, besteht die Gefahr, dass beim Öffnen oder Starten unerwünschte Aktionen ausgelöst werden. Ursache können dabei z. B. Pufferüberläufe in den Anwendungsprogrammen oder schädliche, in die Dateien eingebettete Makros sein. Um das Risiko zu minimieren, sollten auf einem Internet-PC daher so wenig Anwendungsprogramme wie möglich installiert werden. Zur Anzeige von Fremdformaten, z. B. Word- oder Excel-Dateien, sollten möglichst Viewer-Programme verwendet werden, die die Ausführung von Makros nicht unterstützen.

Alle installierten Software-Komponenten, wie z. B. Plug-Ins, Patches, Updates und Viewer-Programme, sollten ausschließlich aus vertrauenswürdigen Quellen bezogen werden, beispielsweise direkt vom Hersteller oder offiziellen Spiegel-Servern.

**Konfiguration**

Die verbreiteten WWW-Browser haben komplexe Konfigurationsmöglichkeiten. Viele Optionen haben Auswirkungen auf den sicheren Betrieb des Browsers und damit auch auf die Informationssicherheit des Internet-PCs. Nach einer Standard-Installation entsprechen die Browser-Einstellungen in der Regel nicht den Sicherheitsanforderungen. Die einzelnen Konfigurationseinstellungen sollten daher systematisch überprüft und ggf. angepasst werden. Grundlage hierfür sind die Vorgaben im Einsatzkonzept und in den Richtlinien für Internet-PCs (siehe Maßnahmen M 2.234 *Konzeption von Internet-PCs* und M 2.235 *Richtlinien für die Nutzung von Internet-PCs*). Die folgenden Empfehlungen sollten bei der Konfiguration berücksichtigt werden.

Wenn der Internet Service Provider (ISP) einen Proxy-Server anbietet, sollte dieser auch genutzt werden. Hierzu müssen im Browser die IP-Adresse und die Port-Nummer des Proxy-Servers eingetragen werden. Bei einigen Browsern müssen diese Informationen für jeden unterstützten Dienst separat angegeben werden. Proxy-Server unterstützten in der Regel mindestens die Dienste HTTP, HTTPS und FTP. Die benötigten IP-Adressen und Port-Nummern sollten den Informationen des ISPs entnommen oder dort erfragt werden.

Unter *aktiven Inhalten* sind Computerprogramme zu verstehen, die in Internet-Seiten enthalten sind oder beim Betrachten einer Internet-Seite automatisiert nachgeladen werden. Ausgeführt werden diese Computerprogramme auf dem Computer des Internet-Nutzers entweder vom jeweiligen WWW-Browser oder von dem darunter liegenden Betriebssystem. Wichtige Beispiele für aktive Inhalte sind die Technologien *Javascript*, *Java* und *ActiveX*. Wie bei jedem Computerprogramm besteht bei aktiven Inhalten die Gefahr, dass von dem Programmcode nicht nur sinnvolle Aktionen durchgeführt werden, sondern auch unerwünschte oder sogar schädliche Aktionen. Aktive Inhalte können also beispielsweise Viren transportieren oder Trojanische Pferde darstellen.

Die Browser enthalten zwar einige Sicherheitsfunktionen zum Schutz vor schädlichen aktiven Inhalten, in der Vergangenheit sind jedoch zahlreiche Software-Schwachstellen bekannt geworden, die zum Aushebeln dieser Sicherheitsfunktionen ausgenutzt werden können (siehe auch M 5.69 *Schutz vor aktiven Inhalten*).

In den gängigen Browsern kann eingestellt werden, wie mit aktiven Inhalten umgegangen werden soll. Aus den oben genannten Gründen sollte die Ausführung aktiver Inhalte nur dann im Browser freigeschaltet werden, wenn dies im Einsatzkonzept bzw. in den Richtlinien für Internet-PCs ausdrücklich vor-

gesehen ist. In diesem Fall sollten nur die Technologien aktiviert werden, die für die tägliche Arbeit benötigt werden, z. B. Javascript.

Einige Browser bieten die Möglichkeit, persönliche Informationen oder Passwörter abzuspeichern, damit diese automatisch in WWW-Formulare eingetragen bzw. als Authentisierungsdaten an den WWW-Server gesendet werden können und somit nicht jedes Mal eingetippt werden müssen. Der Internet Explorer bietet dies z. B. unter dem Stichwort *AutoVervollständigen* an. Diese Funktion sollte nicht verwendet werden, da sonst die Gefahr besteht, dass unbeabsichtigt Passwörter, persönliche Informationen oder Informationen über die Behörde bzw. das Unternehmen weitergegeben werden.

Auch für den Zugriff auf FTP-Server bieten einige Browser die Möglichkeit an, automatisch Benutzernamen und Passwörter zu übermitteln. Damit nicht unbeabsichtigt Passwörter an Dritte weitergegeben werden, sollte der Browser so konfiguriert werden, dass standardmäßig nur anonyme Anmeldungen erfolgen.

Bei einigen Browsern kann konfiguriert werden, ob heruntergeladene Dateien automatisch geöffnet oder gespeichert werden sollen oder ob der Benutzer gefragt werden soll. Damit Dateien nicht versehentlich geöffnet oder gestartet werden, sollte diese Option auf *Speichern* oder *Benutzer fragen* eingestellt werden.

Mit Hilfe so genannter *Cookies* können WWW-Server auf dem Internet-PC Daten hinterlegen und später wieder abrufen. Diese Funktion wird häufig für virtuelle Warenkörbe bei Internet-Shops benötigt. Aus Sicht der Informationssicherheit sind Cookies weitgehend unproblematisch. Allerdings lassen sich mit Hilfe von Cookies auch Profile über das Verhalten von Benutzern erstellen, so dass es u. U. aus Gründen des Datenschutzes wünschenswert ist, das Abspeichern von Cookies zu deaktivieren. Gängige Browser können auch so konfiguriert werden, dass der Benutzer gefragt wird, wenn ein WWW-Server versucht, ein Cookie zu setzen. Je nachdem, welche WWW-Angebote typischerweise genutzt werden, wird der Benutzer dadurch jedoch durch eine Vielzahl von Dialogfenstern belästigt und bei der Arbeit behindert. Es muss daher anhand des konkreten Anwendungsfalls entschieden werden, wie bei der Nutzung von Internet-PCs mit Cookies umgegangen wird.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) sind Protokolle, mit denen die Kommunikation zwischen WWW-Server und WWW-Browser kryptographisch geschützt werden kann. Die Absicherung durch SSL/TLS sollte immer genutzt werden, wenn sie Server-seitig angeboten wird.

Dies ist besonders wichtig bei der Übertragung personenbezogener Daten, beispielsweise wenn E-Mails vom Server abgeholt werden.

Für die Authentisierung der Kommunikationspartner können Zertifikate eingesetzt werden, in der Praxis werden meist jedoch nur SSL-Zertifikate für WWW-Server ausgestellt.

Falls zusätzlich eine Authentisierung des Clients erforderlich ist, erfolgt diese meist auf andere Weise, z. B. mit Hilfe von Benutzername und Passwort (siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS*).

Die Echtheit eines SSL-Zertifikats kann die Browser-Software meist anhand der digitalen Signatur einer Zertifizierungsstelle überprüfen. Die Zertifikate einiger etablierter Zertifizierungsstellen werden bei den gängigen Browsern mitgeliefert. Einige Server-Betreiber greifen jedoch auf andere Zertifizierungs-

stellen zurück, so dass die Echtheit des SSL-Zertifikats nicht direkt überprüft werden kann. Falls häufig auf einen solchen WWW-Server zugegriffen werden muss, sollte das Zertifikat der entsprechenden Zertifizierungsstelle in den Browser importiert werden, wenn es verfügbar ist. Um die Echtheit dieses Zertifikats sicherzustellen, sollte vor dem Import der so genannte *Fingerprint* auf einem unabhängigen Weg, z. B. via Fax, Telefon oder E-Mail, übermittelt und verglichen werden. Nur dann können Benutzer davon ausgehen, dass der Server tatsächlich zu dem gewünschten Betreiber gehört.

Um die Angriffs- und Missbrauchsmöglichkeiten bei WWW-Browsern zu minimieren, sollten grundsätzlich nur die Funktionen aktiviert werden, die zur Erledigung der Fachaufgabe benötigt werden.

**Betrieb**

Daten und Programme sollten von möglichst vertrauenswürdigen Quellen heruntergeladen werden. Hierfür bieten sich z. B. das Internet-Angebot des Herstellers bzw. Herausgebers der Informationen oder offizielle Spiegelserver ("Mirrors") an. Dateien und Programme aus dem Internet sollten auf Computer-Viren geprüft werden, wenn das entsprechende Dateiformat befallen werden kann. Dateien und Programme sollten daher nach dem Download nicht automatisch aus dem Browser heraus geöffnet bzw. gestartet, sondern zunächst abgespeichert werden.

Wie bereits oben erläutert, können Cookies auch dazu verwendet werden, Profile über das Verhalten von Benutzern zu erstellen. Falls das Speichern von Cookies grundsätzlich erlaubt wird, sollten sie daher regelmäßig gelöscht werden. Dies geschieht entweder aus dem Browser heraus oder durch Löschen der entsprechenden Datei, in der die Cookies gespeichert werden. Im Internet sind eine Reihe von Shareware-Tools verfügbar, mit denen die Verwaltung gespeicherter Cookies möglich ist.

Der *Cache* eines Browsers dient dazu, WWW-Seiten lokal zwischenzuspeichern, damit sie nicht neu aus dem Internet geladen werden müssen, wenn der Benutzer sie noch einmal aufruft. Dies verkürzt die Antwortzeiten bei der WWW-Nutzung. Besonders beim "Einkauf über das Internet" werden oftmals vertrauliche Informationen, z. B. Kreditkartennummern, übertragen. Diese Informationen werden unter Umständen im Cache des Browsers zwischengespeichert.

Dadurch besteht die Gefahr, dass diese Informationen unberechtigterweise aus dem Cache ausgelesen und missbraucht werden. Falls der Zugang zum Internet-PC nicht wirksam geschützt ist, sollte der Cache des Browsers daher nach der Übertragung von vertraulichen Informationen gelöscht werden. Alternativ kann die Cache-Funktion auch bei der Konfiguration vollständig deaktiviert werden.

Prüffragen:

- Werden bei Browsern nur die benötigten Software-Komponenten - insbesondere Plug-Ins - installiert?
- Werden die seitens des Herstellers bereitgestellten Browser-Updates und Patches regelmäßig und zeitnah installiert?
- Ist sichergestellt, dass Software-Komponenten des Browser wie Plug-Ins, Patches, Updates, Viewer ausschließlich aus vertrauenswürdigen Quellen bezogen werden?

- Ist die Ausführung aktiver Inhalte im Browser nur soweit erlaubt, wie dies im Einsatzkonzept beziehungsweise in den Richtlinien für Internet-PCs ausdrücklich vorgesehen ist?
- Wird auf eine Speicherung von Benutzerdaten oder Passwörtern für WWW-Formulare verzichtet?
- Ist sichergestellt, dass heruntergeladene Dateien nicht automatisch geöffnet werden?
- Werden heruntergeladene Dateien mit einem Viren-Schutzprogramm geprüft, bevor sie geöffnet beziehungsweise gestartet werden?

# M 5.94 Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

E-Mail ist einer der wichtigsten Intranet- und Internet-Dienste. In der modernen Bürokommunikation wird E-Mail als Ergänzung, teilweise auch als Ersatz für die klassischen Kommunikationswege, wie Telefon, Telefax, Brief und Fernschreiber, verwendet. Eine erhebliche Aufwertung hat der E-Mail-Verkehr auch durch die Möglichkeit erfahren, Dateien in Form von *Attachments* zu transportieren. Dadurch wird E-Mail vielfach auch als Groupware-Lösung benutzt, beispielweise wenn mehrere Kommunikationspartner nacheinander an einem Dokument arbeiten.

Auf technischer Ebene gibt es unterschiedliche Verfahren, E-Mail zu nutzen. Eine Möglichkeit ist die Verwendung von Webmail-Diensten, wie sie von mehreren Dienstleistern im Internet angeboten werden, z. B. Web.de oder gmx. Diese Angebote stellen dem Benutzer alle benötigten Funktionen zum Empfangen, Lesen, Verfassen, Senden und Verwalten von E-Mails über eine WWW-Schnittstelle zur Verfügung. Die Nutzung geschieht somit - wie jedes andere WWW-Angebot - über einen Browser. Die Vorteile von Webmail-Diensten sind,

- dass neben dem Browser keine weiteren Software-Komponenten auf dem Client installiert werden müssen und
- dass der Benutzer daher für die Nutzung von E-Mail nicht an einen bestimmten Computer oder Ort gebunden ist.

Nachteilig ist jedoch, dass die Sicherheit der E-Mail-Nutzung weitgehend in der Hand des Webmail-Providers liegt. Empfehlungen zur sicheren Nutzung von Webmail finden sich in Maßnahme M 5.96 *Sichere Nutzung von Webmail*.

Das klassische Verfahren für die Nutzung von E-Mail ist die Verwendung eines entsprechenden Client-Programms, beispielsweise Microsoft Outlook, Outlook Express, Thunderbird oder KMail. Um eingehende E-Mail vom Provider abzuholen, wird meist das Protokoll POP3 (Post Office Protocol Version 3) oder IMAP (Internet Message Access Protocol) verwendet. Ausgehende E-Mail wird mit Hilfe des Protokolls SMTP (Simple Mail Transfer Protocol) versendet. Hierzu müssen bei der Konfiguration des Client-Programms die Adressen der Server für ausgehende und eingehende E-Mails eingetragen werden. Es wird empfohlen, die IP-Adressen dieser Server beim Provider zu erfragen und fest im Client-Programm einzustellen.

Bevor eingehende E-Mail vom Provider zum Client übertragen werden kann, muss sich der Client in der Regel beim E-Mail-Server authentisieren. Diese Authentisierung geschieht meist durch ein Passwort, das im Klartext an den jeweiligen Server übermittelt wird, wenn keine zusätzlichen Sicherheitsmaßnahmen eingesetzt werden. Dadurch besteht die Gefahr, dass das Passwort beim Transport über das Internet mitgelesen und anschließend missbraucht wird. Um dies zu verhindern, sollte die gesamte Kommunikation mit dem E-Mail-Server mit Hilfe von TLS/SSL verschlüsselt werden. Dies schützt auch die E-Mails bei der Übertragung vor Kompromittierung und Manipulation. Die Möglichkeit, den Zugriff über POP3 oder IMAP mit Hilfe von TLS/SSL abzusichern, bieten inzwischen viele Provider an (siehe auch RFC 2595).

Das Passwort für den Zugriff auf den E-Mail-Server beim Provider sollte ausreichend lang und nicht leicht zu erraten sein, damit Unbefugte nicht auf die E-Mail zugreifen können. Es sollte außerdem regelmäßig gewechselt werden. Die Frage, ob das E-Mail-Passwort auf dem Internet-PC abgespeichert werden darf oder ob es bei jedem Zugriff neu eingegeben werden muss, kann nicht allgemein beantwortet werden. Dies hängt davon ab, wie viele Authentisierungsprozesse der Benutzer insgesamt durchlaufen muss (Anmeldung am Client, Einwahl beim ISP, usw.) und wie groß die Gefahr durch missbräuchliche Nutzung eingeschätzt wird. Weitere Empfehlungen zu Passwörtern sind in Maßnahme M 2.11 *Regelung des Passwortgebrauchs* aufgeführt.

Einige E-Mail-Clients bieten die Möglichkeit, E-Mails im HTML- oder Rich Text Format (RTF) zu erstellen. Beim HTML-Format besteht das Problem, dass darin auch aktive Inhalte, z. B. Javascript, und Verweise auf andere Objekte im Internet enthalten sein können. Dies hat schon mehrfach zu Sicherheitsproblemen geführt. Daher sollten keine E-Mails im HTML-Format versendet werden. Falls unbedingt Formatierungselemente, wie z. B. Schriftart und Farbe, benötigt werden, ist stattdessen das RTF-Format zu verwenden. Die Client-Programme sollten daher so konfiguriert werden, dass sie E-Mails im reinen Text-Format oder im RTF-Format erstellen und versenden.

Für eingehende HTML-formatierte E-Mails sollte der Client so konfiguriert werden, dass er bei der Anzeige solcher E-Mails keine aktiven Inhalte ausführt. Einige E-Mail-Clients zeigen HTML-formatierte E-Mails nicht selbst an, sondern starten einen externen Viewer oder Browser. In diesem Fall sollte ein Viewer bzw. Browser verwendet werden, der keine aktiven Inhalte ausführt. Außerdem sollte sichergestellt sein, dass beim Lesen der E-Mail keine Zugriffe auf andere Objekte im Internet erfolgen, beispielsweise indem die Internet-Verbindung vorher getrennt wird. Alternativ können HTML-formatierte E-Mails auch mit einem reinen Text-Editor geöffnet werden. Aufgrund der enthaltenen Steuerelemente (*Tags*) lässt sich der Inhalt dabei jedoch meist schwer lesen.

Einige Client-Programme bieten eine Vorschau-Funktion für E-Mails an. Dabei wird der Inhalt einer ausgewählten E-Mail angezeigt, ohne dass sie explizit vom Benutzer geöffnet wurde. Dadurch besteht die Gefahr, dass schädliche Inhalte in E-Mails unbeabsichtigt ausgeführt werden. Die Vorschau-Funktion sollte daher deaktiviert werden.

Attachments, d. h. Dateien, die als Anlage zum eigentlichen Text in der E-Mail enthalten sind, sind ein beliebtes Transportmedium für Computer-Viren, Würmer und andere Schadprogramme. Die im E-Mail-Programm angezeigte Dateinamenserweiterung (*.jpg*, *.exe*, usw.) stimmt außerdem nicht immer mit dem tatsächlichen Dateityp überein. Es gibt Techniken, mit denen in bestimmten Client-Programmen die tatsächliche Dateinamenserweiterung verborgen werden kann. Attachments in eingehenden E-Mails sollten daher grundsätzlich mit Misstrauen behandelt werden, insbesondere wenn die Übersendung nicht abgesprochen oder der Absender unbekannt ist. Vor dem Öffnen bzw. Starten sollten Attachments abgespeichert und mit einem Viren-Schutzprogramm geprüft werden.

Ausführbare Dateien und Dateien, die Änderungen an der Systemkonfiguration vornehmen können, beispielsweise *.exe*, *.vbs*, *.reg* unter Windows oder Shell-Skripten unter Linux, sollten nicht ohne Zustimmung der Administration gestartet werden. Vorsicht ist auch bei Attachments geboten, die offenbar keinen Bezug zur üblichen Geschäftsbeziehung mit dem Absender haben, z. B. Erotik-Angebote vom Steuerberater, oder wenn die E-Mail in einer anderen Sprache als sonst verfasst ist. Bei solchen Auffälligkeiten sollten die eventuell

enthaltenen Attachments zunächst nicht geöffnet, sondern die Administration oder der IT-Sicherheitsbeauftragte verständigt werden. Zur Klärung kann auch beim Absender nachgefragt werden, was es mit den Attachments auf sich hat.

Unter Windows sollten möglichst nur solche Programme als Standardapplikationen konfiguriert werden, die keine Makros bzw. eingebetteten Skripten ausführen können. Für die meisten verbreiteten Dokumenten- bzw. Dateitypen, z. B. Word- oder Excel-Dateien, sind entsprechende Viewer verfügbar. Auf die Installation der vollwertigen Anwendungsprogramme, beispielsweise Microsoft Office, sollte nach Möglichkeit ganz verzichtet werden. Anstelle der Default-Einstellung *Zusammenführen* sollte für den Dateityp *.reg* ein Editor als Standardapplikation konfiguriert werden. Anderenfalls werden die in der Datei enthaltenen Registry-Einträge bei einem Doppelklick oder bei einem anderweitig ausgelösten Öffnen der Datei in die Registry des Internet-PCs eingetragen. Durch diese Konfigurationsänderung können u. a. Sicherheitseinstellungen ungewollt deaktiviert werden. Die Standardapplikation für Dateitypen kann vom Explorer aus über das Dialogfeld *Ansicht* | *Optionen* | *Dateitypen* geändert werden.

Auch via E-Mail werden in vielen Fällen Informationen übertragen, deren Vertraulichkeit und Integrität beim Transport vom Sender zum Empfänger geschützt werden müssen. Hierfür können Verschlüsselung und digitale Signaturen eingesetzt werden. Problematisch ist dabei, dass sich unterschiedliche Verfahren, wie S/MIME, GnuPG bzw. PGP und MailTrusT, für die kryptographische Absicherung von E-Mail etabliert haben, die gar nicht oder nur teilweise interoperabel sind. Bevor Verschlüsselung oder digitale Signatur für E-Mails eingesetzt werden kann, muss daher eine Abstimmung mit den Kommunikationspartnern darüber erfolgen, welches oder welche Verfahren verwendet werden (siehe auch M 5.63 *Einsatz von GnuPG oder PGP*). Die hierzu benötigten Software-Komponenten werden häufig als Plug-Ins für gängige E-Mail-Programme angeboten. Falls mehrere verschiedene Plug-Ins zur E-Mail-Verschlüsselung verwendet werden sollen, ist darauf zu achten, dass keine technischen Probleme dadurch entstehen, dass diese in das gleiche E-Mail-Programm installiert werden.

Beim Empfang bzw. beim Lesen eingehender Nachrichten bieten gängige E-Mail-Programme die Möglichkeit, Empfangs- oder Lesebestätigungen anzufordern. Für eine Empfangsbestätigung muss der Server des Empfängers den DSN-Standard (Delivery Service Notification) unterstützen, für eine Lesebestätigung muss der E-Mail-Client den MDN-Standard (Message Disposition Notification) unterstützen. Abhängig vom E-Mail-Client kann dieser so eingestellt werden, dass er eine Bestätigungsanforderung immer, nie oder nur bei bestimmten Absender(kreisen) beantwortet.

Aus Sicht der Informationssicherheit sind solche Bestätigungsnachrichten in der Regel unproblematisch. Im Zusammenhang mit Werbe-E-Mails, die unspezifisch an eine große Anzahl von E-Mail-Adressen versendet werden, kann diese Funktion jedoch unerwünscht sein. Dem Absender wird dadurch signalisiert, dass die jeweilige E-Mail-Adresse existiert und ggf. auch dass die Werbe-E-Mail gelesen wurde.

Eingehende oder ausgehende E-Mails können bei einigen E-Mail-Clients auf Wunsch automatisch an einen festgelegten E-Mail-Empfänger oder eine Verteilerliste gesendet werden, beispielsweise als BCC (Blind Carbon Copy). Bei Thunderbird können hierfür entsprechende E-Mail-Adressen z. B. unter *Einstellungen* | *Konten* | *Kopien & Ordner* | *BCC* an diese E-Mail-Adressen eingetragen werden. Diese Funktion sollte nur verwendet werden, wenn sicher-

gestellt ist, dass alle Personen, die auf die dort eingetragene E-Mail-Adresse zugreifen können, alle eingehenden bzw. ausgehenden E-Mails lesen dürfen. Anderenfalls besteht die Gefahr, dass vertrauliche Informationen ungewollt an Dritte weitergegeben werden.

Bei einigen Versionen des Betriebssystems Windows wird das Client-Programm Outlook Express mitgeliefert. Falls dieses Programm nicht benötigt wird, z. B. weil ein anderes Client-Programm eingesetzt oder ein Webmail-Dienst genutzt wird, sollte Outlook Express deinstalliert werden.

Für alle auf dem Internet-PC installieren Software-Komponenten muss sichergestellt sein, dass alle verfügbaren sicherheitsrelevanten Patches und Updates zeitnah eingespielt werden.

Prüffragen:

- Erfolgt bei der Verwendung von externen Webmail-Diensten die gesamte Kommunikation verschlüsselt?
- Ist das Passwort für den Zugriff auf den E-Mail-Server des Providers ausreichend komplex und wird darüber hinaus regelmäßig gewechselt?
- Ist festgelegt, in welchem Format E-Mails zu erstellen und zu versenden sind?
- Sind die E-Mail-Clients so konfiguriert, dass aktive Inhalte von E-Mails nicht ausgeführt werden?
- Ist sichergestellt, dass E-Mail-Anhänge vor dem Öffnen mit einem Viren-Schutzprogramm geprüft werden?
- Existieren Regelungen für E-Mail-Anhänge mit ausführbaren beziehungsweise sicherheitskritischen Dateien?
- Ist geregelt, wie und ob eine automatische E-Mail-Weiterleitung zu erfolgen hat?

# M 5.95 Sicherer E-Commerce bei der Nutzung von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Internet wird heute nicht nur zur Informationsgewinnung und Kommunikation, sondern auch intensiv als Plattform für die Abwicklung von Geschäfts- oder Verwaltungsvorgängen genutzt. Beispiele hierfür sind Online-Bestellungen, Konto- oder Wertpapiertransaktionen und E-Government-Anwendungen.

E-Commerce- und E-Government-Anwendungen haben in der Regel höhere Sicherheitsanforderungen als die reine Informationsgewinnung über das World Wide Web. Insbesondere muss sichergestellt werden, dass Online-Transaktionen und -Bestellungen bei der Verarbeitung auf dem Internet-PC und bei der Übertragung über das Internet nicht manipuliert werden. Falls ein Internet-PC auch für E-Commerce oder E-Government-Anwendungen genutzt wird, sollten daher die nachfolgenden Empfehlungen berücksichtigt werden.

Bevor eine Geschäftsbeziehung mit einem Anbieter über das Internet aufgenommen wird, sollte geprüft werden, ob dessen Grundsätze in Bezug auf Datenschutz und Datensicherheit mit den eigenen Anforderungen vereinbar sind. Der Anbieter sollte hierzu Informationen auf dem Webserver bereitstellen.

Zum Schutz vor Computer-Viren, Trojanischen Pferden und anderen Schadprogrammen muss ein Viren-Schutzprogramm installiert werden, dessen Datenbank regelmäßig aktualisiert wird. Weitere Empfehlungen hierzu finden sich in Baustein B 1.6 *Schutz vor Schadprogrammen* und Maßnahme M 4.3 *Einsatz von Viren-Schutzprogrammen*.

Die für die E-Commerce- bzw. E-Government-Anwendungen erforderlichen Datenbestände und Konfigurationseinstellungen müssen regelmäßig gesichert werden (siehe auch M 6.79 *Datensicherung beim Einsatz von Internet-PCs*). Andernfalls besteht die Gefahr, dass die Anwendung beim Ausfall des Internet-PCs oder bei versehentlicher Löschung nicht zeitnah wiederhergestellt oder getätigte (Trans)aktionen nicht nachvollzogen werden können.

Falls für die Anwendung spezielle Software-Komponenten, z. B. Online-Banking-Programme, benötigt werden, sollten diese ausschließlich von vertrauenswürdigen Quellen bezogen werden, möglichst direkt vom Anbieter bzw. Hersteller. Für diese Software-Komponenten muss regelmäßig geprüft werden, ob sicherheitsrelevante Patches oder Updates existieren. Diese müssen eingespielt werden. Software und Updates sind vor der Installation auf Schadprogramme zu prüfen.

Falls ein Internet-PC regelmäßig für E-Commerce- oder E-Government-Anwendungen genutzt wird, sollte er einem festen Benutzer zugeordnet und ausschließlich für diese Anwendungen verwendet werden. Anderenfalls besteht die Gefahr, dass später nicht nachvollziehbar ist, welcher Benutzer eine bestimmte Aktion vorgenommen hat.

Bei vielen Anwendungen im E-Commerce und E-Government wird der WWW-Browser als Client-Programm verwendet.

Als Schutzmechanismus für die Übertragung kommt dabei in der Regel das TLS/SSL-Protokoll zum Einsatz. Dabei werden Vertraulichkeit und Integrität der Daten mit Hilfe kryptographischer Verfahren geschützt. Eine TLS/SSL-

Verbindung erkennt man im Browser daran, dass die Adresse (URL) mit *https:* statt mit *http:* beginnt, und bei den gängigen Browsern auch an einem besonderen Symbol, z. B. einem geschlossenen Schloss.

Webbasierte E-Commerce- und E-Government-Anwendungen sollten ausschließlich über TLS/SSL genutzt werden. Der Anbieter sollte die gesamte Web-Anwendung über TLS/SSL bereitstellen. Es ist darauf zu achten, dass ein Browser verwendet wird, der starke kryptographische Verfahren unterstützt, insbesondere 128 Bit Schlüssellänge. Dies ist bei einigen älteren Browsern aufgrund von Export-Restriktionen nicht der Fall.

Für die Authentisierung des WWW-Servers kommen beim TLS/SSL-Protokoll Zertifikate zum Einsatz. Bei der Nutzung von E-Commerce- oder E-Government-Anwendungen über TLS/SSL sollten die Benutzer sporadisch überprüfen, ob das Server-Zertifikat gültig ist und ob sie tatsächlich mit dem gewünschten Server verbunden sind. Hierzu ist es erforderlich, dass die Benutzer für die Bedienung des WWW-Browsers geschult werden und ihnen Hinweise zur Verfügung gestellt werden, wie sie die Überprüfung bei der konkreten Installation und Konfiguration vornehmen.

Prüffragen:

- Ist sichergestellt, dass Online-Transaktionen und -Bestellungen bei der Verarbeitung auf dem Internet-PC und bei der Übertragung über das Internet nicht manipuliert werden?
- Sind die allgemeinen Geschäftsbedingungen des E-Commerce-Dienstleisters mit den Anforderungen der Institution vereinbar, insbesondere im Bereich Datenschutz und Datensicherheit?
- Wird eine regelmäßige Sicherung der Datenbestände und Konfigurationseinstellungen der E-Commerce-Anwendungen durchgeführt?
- Ist sichergestellt, dass E-Commerce- und E-Government-Anwendungen ausschließlich über TLS/SSL genutzt werden?
- Wird die Gültigkeit der eingesetzten Server-Zertifikate von E Commerce-Anbietern überprüft?

# M 5.96 Sichere Nutzung von Webmail

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Nicht jede Institution betreibt einen eigenen Mailserver, sondern nutzt die entsprechenden Dienstleistungen von externen Anbietern. Dabei ist Webmail eine einfache, benutzerfreundliche Variante, um über die Webserver der Anbieter auf Maildienste zuzugreifen. Mit Webmail werden alle Internet-basierten E-Mail-Dienste bezeichnet, bei denen zur Benutzung nur ein Browser als Client und eine Internet-Anbindung benötigt wird. Dazu gehören z. B. die Angebote von Web.de, Freenet.de oder gmx.de. Webbasierte E-Mail-Dienste erlauben den Zugriff auf E-Mails unabhängig vom Ort und Provider.

Bei der ersten Anmeldung bei einem Webmail-Dienstleister müssen in der Regel Name und Adresse des Benutzers, die gewünschte E-Mail-Adresse und ein Zugangspasswort angegeben werden. Einige Anbieter verlangen eine schriftliche Bestätigung der Anmeldung. Das gewählte Passwort dient bei nachfolgenden Anmeldungen zur Authentisierung. Der Benutzer erhält dann ein oder mehrere E-Mail-Adressen sowie ein Benutzerkonto, über das E-Mail empfangen, weiterverarbeitet und gesendet werden kann.

Es gibt eine Vielzahl von Anbietern von Webmaildiensten, viele davon bieten ihre Dienstleistungen sogar kostenlos an. Es ist zu beachten, dass diese sich nicht nur im Funktionsumfang unterscheiden (z. B. Postfachgröße, Fax, SMS, Spamfilter, etc.), sondern auch das Sicherheitsniveau stark variieren kann, bis hin zu gravierenden Sicherheitslücken.

Bei der Auswahl eines Dienstleisters sollte daher sorgfältig vorgegangen werden. Wichtig sind insbesondere die folgenden Punkte:

- Die Allgemeinen Geschäftsbedingungen (AGBs) sollten zunächst einmal überhaupt auffindbar und abrufbar sein, außerdem sollten sie verständlich sein und keinen unakzeptablen Bedingungen enthalten. Letzteres heißt u. a., dass der Datenschutz gewährleistet sein sollte. Der Kunde sollte also nicht der Weitergabe seiner personenbezogenen Daten zustimmen müssen, was häufig in Werbeflut resultiert. Ebenso sollten gravierende Änderungen der Dienstleistungen und Kostenstrukturen rechtzeitig angekündigt werden, damit die Kunden reagieren können (z. B. Posteingänge umleiten, Postfächer sichern).
- Bei Vielreisenden ist ein weltweiter Zugriff auf die Postfächer wichtig. Außerdem sollte generell getestet werden, wie lange der Versand bzw. Empfang von E-Mails dauert.
- Neben der Benutzerfreundlichkeit des Angebotes sollte auch untersucht werden, ob Onlinehilfen, FAQs oder andere Dokumentation vorhanden ist. Außerdem sollte die Erreichbarkeit und Kompetenz des Supportteams hinterfragt werden (per E-Mail, Telefon oder Fax).
- Bei der Bewertung der Sicherheit des Angebotes sollten die technischen und organisatorischen Sicherheitsvorkehrungen betrachtet werden:
    - Es sollte möglich sein, über eine verschlüsselte Verbindung auf das Benutzerkonto zuzugreifen, z. B. über SSL.
    - Die E-Mail sollte verschlüsselt bzw. digital signiert werden können.
    - Es ist zu hinterfragen, ob eine Prüfung der Identität von Neukunden stattfindet, ob es beispielsweise möglich ist, sich unter falschem Namen oder falscher Adresse anzumelden oder sich fehlleitende E-

Mailadressen wie *support@...* auszusuchen. Die Identität des Kunden sollte postalisch geprüft werden.
- Jeder kann einmal ein Passwort vergessen. Trotzdem ist es kein gutes Zeichen, sondern falsch verstandene Benutzerfreundlichkeit, wenn man bei der Hotline ohne große Nachfragen ein neues Passwort erhält. Hier müssen vernünftige Sicherheitsüberprüfungen eingebaut sein.
- Für den Zugriff auf die Webmail-Dienste sollten keine aktiven Inhalte akzeptiert werden müssen (Java, JavaScript, ActiveX).
- Eine Virenprüfung der ein- und ausgehenden E-Mail sollte selbstverständlich sein.
- Spamfilterung sollte möglich sein.

Auch bei der Nutzung von Webmail-Diensten sind einige Punkte zu beachten:

- Das Passwort für den Zugriff auf die Webmail-Dienste sollte geeignet gewählt sein, also lang genug (mindestens 8 Stellen) und kompliziert genug (Zahlen, Buchstaben und Sonderzeichen). Das Passwort sollte regelmäßig gewechselt werden. Es darf auf keinen Fall auf dem PC abgespeichert oder am PC aufbewahrt werden. Weitere Hinweise zur Passwortauswahl finden sich in M 2.11 *Regelung des Passwortgebrauchs*.
- Für den Zugriff auf das Benutzerkonto sollte SSL benutzt werden.
- E-Mail sollte möglichst verschlüsselt bzw. digital signiert werden. Hierzu ist in der Regel eine Abstimmung mit dem Empfänger darüber erforderlich, welche kryptographischen Verfahren und Programme hierfür auf beiden Seiten zur Verfügung stehen.
- Auch wenn der Anbieter Virenschutz verspricht, sollten Dateianhänge außerdem auf dem eigenen Rechner auf Viren überprüft werden.
- Eingehende E-Mails sollten regelmäßig gelesen werden. Wichtige E-Mails sollten lokal gespeichert werden. Außerdem sollten die Postfächer regelmäßig aufgeräumt werden, also lokal bereits gespeicherte oder unwichtige E-Mails gelöscht werden. Darüber hinaus sollten die Postfächer regelmäßig auf lokale Datenträger gespeichert werden, aber auch die lokal gespeicherten E-Mails sorgfältig gesichert werden.
- Der Webmail-Dienst sollte immer über den Log-Out-Button oder ähnliche Mechanismen verlassen werden, damit keine anderen Benutzer des lokalen PCs auf die Webmail zugreifen können.

HTML-formatierte E-Mails können Sicherheitsprobleme verursachen (siehe G 5.103 *Missbrauch von Webmail*). Es sollte vermieden werden, HTML-formatierte E-Mails oder solche mit aktiven Inhalten zu versenden. Der Provider sollte die Möglichkeit anbieten, dass eventuell in eingehender E-Mail enthaltene aktive Inhalte herausgefiltert werden. Außerdem sollten E-Mail-Clients gewählt werden, bei denen HTML-formatierte E-Mails als solche zu erkennen sind, damit der Benutzer diese nicht unbewusst öffnet.

Prüffragen:

- Sind die allgemeinen Geschäftsbedingungen des Webmail-Dienstleisters mit den Anforderungen der Institution vereinbar?
- Entsprechen die vom Webmail-Dienstleister angebotenen technischen und organisatorischen Sicherheitsmaßnahmen den Anforderungen der Institution?
- Sind die für die Webmail-Dienste eingesetzten Passwörter ausreichend komplex und werden regelmäßig gewechselt?
- Ist die lokale Speicherung von E-Mails bei der Nutzung von Webmail-Diensten und das Bearbeiten des Postfaches geregelt?
- Gibt es Regelungen für die sichere Nutzung von Webmail-Diensten?

# M 5.97 Absicherung der Kommunikation mit Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Der Datenaustausch zwischen eDirectory-Client und -Server erfolgt über Netzverbindungen. Je nach eDirectory-System und Netzstruktur werden die Kommunikationspakete, die neben Verzeichnisinhalten unter Umständen auch Authentisierungsinformationen enthalten können, ungeschützt übertragen.

Dabei können abhängig vom installiertem Betriebssystem unterschiedliche Netzprotokolle zum Einsatz kommen. So kann ein Zugriff auf eDirectory sowohl über das Novell-eigene NDAP erfolgen, das auf dem *Netware Core Protocol* (NCP) aufsetzt, als auch über das standardisierte Protokoll LDAP. Der Transport der Daten erfolgt dabei für NDAP über IP- oder IPX-Netze und für LDAP ausschließlich über IP-Netze.

Die Benutzer-Authentisierung beim Zugriff über NDAP erfolgt nach einem proprietären Verfahren, das keine Authentisierungsdaten direkt über das Netz transportiert. Die Kommunikation zwischen Client und Server wird jedoch bei Verwendung von NDAP nicht grundsätzlich verschlüsselt, es ist die Angelegenheit des eingesetzten (NDAP-Clients, die Verschlüsselung der Kommunikation zu sicherzustellen. Daher sollte der Zugriff auf eDirectory über dieses Protokoll nur innerhalb des Intranets möglich sein.

Soll von außen über NDAP auf einen eDirectory-Server zugegriffen werden, so ist eine entsprechende Absicherung der Kommunikationsverbindung zwischen Client und Server zu realisieren, die die Vertraulichkeit der übertragenen Daten hinreichend schützt. Dies kann z. B. durch Verwendung eines *Virtuellen Privaten Netzes* (VPN) erreicht werden.

Der Zugriff auf eDirectory über LDAP bietet spezielle Möglichkeiten zur Verschlüsselung (Einsatz von SSL) aber auch spezielle Risiken (Einrichtung des anonymen Zugriffs). Auf diese Sicherheitsaspekte wird in Maßnahme M 4.158 *Einrichten des LDAP-Zugriffs auf Novell eDirectory* eingegangen.

Weiterhin können Administratoren über einen Fernzugang auf das System zugreifen. Ein Beispiel hierfür ist das Novell-eigene Werkzeug *iMonitor*, mit dem über einen Browser auf Daten des Systemmonitors zugegriffen werden kann (siehe M 4.160 *Überwachen von Novell eDirectory*).

Da die im iMonitor verfügbaren Daten wesentliche Einblicke in den Aufbau und die Konfiguration einer eDirectory-Installation geben, muss auch dieser indirekte Zugang zum eDirectory abgesichert werden. Es sollte deshalb nur autorisierten Benutzern möglich sein, über HTTP auf den iMonitor zuzugreifen. Die Übertragung sollte außerdem durch TLS/SSL geschützt werden (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*).

**Beispiel:** Steht ein eDirectory-Server für den LDAP-Zugriff von außen innerhalb des Screened-Subnet eines Firewall-Systems, so sollte auf diesen Server kein HTTP-Zugriff möglich sein.

Prüffragen:

- Zugriff von außen über NDAP auf einen eDirectory-Verzeichnisdienst: Ist eine Absicherung der Kommunikationsverbindung zwischen Client und Server realisiert?
- Ist es nur autorisierten Benutzern möglich, über HTTP auf den iMonitor von eDirectory zuzugreifen?

# M 5.98 Schutz vor Missbrauch kostenpflichtiger Einwahlnummern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Kostenpflichtige Internet-Angebote werden häufig über die Telefonrechnung abgerechnet, indem die Benutzer über spezielle Einwahl-Programme auf kostenintensive Telefonnummern umgelenkt werden. Dies können beispielsweise 0900er Nummern sein.

Die dafür benutzten Webdialer sind Programme, die auf dem Rechner einen neuen Internetzugang einrichten. Nach dem Download und der Installation auf dem PC wählt sich der Dialer ins Internet ein. Eine zu dieser Zeit bereits bestehende Internetverbindung wird in der Regel zuvor getrennt. (Dies funktioniert allerdings nur über Wählzugänge, nicht jedoch über DSL oder ähnliche Techniken.)

Die kostenpflichtigen Inhalte können dann über diese Verbindung abgerufen werden. Dabei ist die vom Webdialer benutzte Einwahlnummer maßgeblich für die Höhe der anfallenden Kosten. Sowohl pro Einwahl als auch pro Zeiteinheit können hohe Gebühren anfallen.

Was ursprünglich als einfache und anonyme Zahlungsmethode im Internet gedacht war, wird leider in letzter Zeit zunehmend missbraucht, um auf Internet-PCs vom Benutzer unbemerkt solche Webdialer zu installieren. Solche Webdialer können z. B. über Trojanische Pferde oder beim Aufruf einer Webseite unauffällig installiert werden. Sie verursachen dann massiv Kosten, ohne dass die Benutzer dies merken und ohne dass dem eine angemessene Leistung gegenübersteht.

Um sich vor solchen Problemen zu schützen,

- sollten die Benutzer darüber aufgeklärt werden, was Webdialer sind und wie sich solche bösartigen Programme verbreiten,
- zu jedem Internet-PC sollten Einzelverbindungsnachweise vom Telekommunikationsanbieter verlangt werden (Dies ist in Deutschland kostenlos.),
- sollte erwogen werden, "teure" Telefonnummern, wie 0900er Nummern generell oder bestimmte Nummernblöcke, sperren zu lassen,
- sollten aktive Inhalte, insbesondere ActiveX, möglichst deaktiviert werden.

Generell sollten keine Programme installiert werden, die angeblich kostenlose oder schnellere Verbindungen zu Web-Seiten mit dubiosen Inhalten versprechen.

Prüffragen:

- Werden die Benutzer von Internet-PCs über Gefahren von Webdialern aufgeklärt?
- Werden für jeden Internet-PC Einzelverbindungsnachweise erstellt?
- Wird überlegt, teure Einwahlnummern für Internet-PCs zu sperren?

# M 5.99 SSL/TLS-Absicherung für Exchange 2000

Diese Maßnahme ist mit der 13. Ergänzungslieferung entfallen. Die Inhalte wurden in M 5.100 *Absicherung der Kommunikation von und zu Exchange-Systemen* integriert.

# M 5.100 Absicherung der Kommunikation von und zu Exchange-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Groupware-Server kommuniziert mit Groupware-Clients, Browsern, Telefonie- sowie Kommunikationsanwendungen und anderen Groupware-Systemen. Auch zwischen einzelnen Groupware-Systemkomponenten findet ein Datenaustausch statt. Die Kommunikation erfolgt über das lokale Netz und/ oder externe Netze. In allen Fällen werden Daten übertragen, die geschützt werden müssen. Dies sind nicht nur die Daten, die genutzt werden, um Benutzer zu authentisieren (z. B. Benutzername und Passwort), sondern auch Geschäftsinformationen und im privaten Umfeld persönliche Daten.

Es muss daher entschieden werden, mit welchen Schutzmechanismen die Kommunikation abgesichert wird.

Bei der Übertragung schützenswerter Daten von und zu Groupware-Systemen sollten diese möglichst verschlüsselt werden. Zum Schutz der Daten können unterschiedliche Verfahren eingesetzt werden. Es ist daher zu entscheiden, welches Verfahren unter Kosten-Nutzen-Aspekten das günstigste ist. Die Entscheidung ist nachvollziehbar zu dokumentieren.

**Einsatz von IPSec**

IPSec bietet eine generelle Absicherung der Kommunikation auf IP-Ebene: Alle Datenpakete werden verschlüsselt und integritätsgeschützt. Vorteilhaft an diesem Verfahren ist, dass beim Einsatz von IPsec auf Microsoft Exchange-Systemebene keine zusätzlichen Konfigurationen durchzuführen sind, da der IPSec-Schutz auf Betriebssystem-Ebene konfiguriert wird.

Für eine Absicherung der E-Mail-Kommunikation stehen mehrere mögliche Lösungsansätze zur Verfügung:

- Auf physikalischer Ebene ist eine Linkverschlüsselung denkbar, jedoch im Allgemeinen nicht praktikabel.
- Auf Netzebene ist die Einrichtung eines Virtuellen Privaten Netzes (VPN) möglich.

Wegen der hohen Verbreitung des Internet-Protokolls IP wird dabei in der Regel IPSec oder andere VPN-Lösungen verwendet. IPSec erlaubt die Absicherung von IP-Verbindungen zwischen Standorten, zwischen Endgeräten und auch von Endgeräten zu Standorten. Es können sowohl fest vorkonfigurierte Schlüssel (Preshared Keys) als auch Public Key Infrastrukturen (PKI) für das Schlüsselmanagement verwendet werden.

Um auf Basis von IPSec eine Absicherung der Exchange-Kommunikation zu erreichen, müssen alle am E-Mail-Routing beteiligten Rechner über IPSec kommunizieren.

In reinen Windows-Netzen (Versionen ab Windows 2000) ist IPSec standardmäßig ohne zusätzliche Lizenzen verfügbar. Es entsteht jedoch administrativer Aufwand für die Konfiguration. Weitere Informationen finden sich in M 5.90 Einsatz von IPSec unter Windows.

**Einsatz von TLS/SSL**

Für alle HTTP-basierten Zugriffe ist SSL grundsätzlich zu empfehlen. Dies gilt auch für die interne Kommunikation zwischen Komponenten des Microsoft Exchange-Systems und anderen Komponenten, die die Möglichkeit der SSL-Absicherung bieten. In allen Einsatzszenarien ist die Verschlüsselung der Übertragungswege zwischen einem Client und einem Microsoft-Exchange-Server sinnvoll oder erforderlich. Dies betrifft besonders die Übertragung sensitiver Daten über nicht vertrauenswürdige Kommunikationswege, wie beispielsweise das Internet. Gerade in einer Microsoft-Exchange-Umgebung sollte hierfür das SSL- bzw. TLS-Protokoll (siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS*) eingesetzt werden. Die Entscheidung über einen optionalen oder erzwungenen Einsatz von SSL/TLS sollte vom Standort der zugreifenden Clients und dem Schutzbedarf der übertragenen Daten abhängig gemacht werden. Die Verschlüsselung der Übertragungsstrecke ermöglicht auch die Verwendung von schwächeren Authentisierungsmechanismen, wie z. B. die Kennwort-basierte Klartext-Authentisierung.

**Absicherung der Client-Server-Kommunikation**

Ist ein Microsoft Outlook-Client als Exchange-Client konfiguriert, kann die Kommunikation geschützt werden . Verwendet Microsoft Outlook nur die Internet-Protokolle (POP3, IMAP4, SMTP, NNTP) beim Zugriff auf den Exchange-Server, so sollte die Verbindung mit TLS abgesichert werden. Dies gilt generell auch für den Zugriff auf andere E-Mail-Server.

Eines der möglichen Szenarien für den Einsatz von SSL/TLS ergibt sich aus der Zugriffsmöglichkeit auf einen Exchange-Server über Outlook Web Access (OWA). Die Verschlüsselung der Übertragungswege hat hier zwischen dem Web-Browser und dem (hier erforderlichen) IIS-Server zu erfolgen.

Über das HTTP-Protokoll können unterschiedliche Dienste eines Microsoft-Exchange-Systems angesprochen werden. Der Client-Zugriff auf die Postfachspeicher erfolgt in der Regel über HTTP. Die HTTP-Dienste müssen generell sicher konfiguriert sein, so dass einerseits Zugriffe, die schützenswerte Daten übertragen, mit SSL/TLS geschützt und andererseits nur die benötigten Dienste aktiviert werden.

Dabei sind die über HTTP zugreifbaren RPC-Schnittstellen und WebDAV-Schnittstellen mit besonderen Risiken verbunden:

**RPC-Schnittstelle**

Die RPC-Schnittstelle ist grundsätzlich mit SSL abzusichern. Weitere Details finden sich in M 2.481 Planung des Einsatzes von Exchange für Outlook Anywhere.

**WebDAV-Schnittstelle**

Das WebDAV-Protokoll (Web-based Distributed Authoring and Versioning) erlaubt einen dateisystemähnlichen Zugriff auf Informationen über das HTTP-Protokoll. Da der WebDAV-Zugriff bei Exchange unter Umständen auch auf das lokale Dateisystem des Clients erfolgen kann, muss dieses vor unberechtigten Zugriffen geschützt werden. Dabei sollte der Schutz der über WebDAV angebotenen Daten im Vordergrund stehen. Falls aber ein Angreifer über WebDAV auf das lokale Dateisystem zugreifen kann, können dadurch weitere Angriffe vorbereitet werden. Daher sollte der Zugriff auf WebDAV nur authen-

tisiert und über SSL geschützt erfolgen. Zusätzlich ist immer auf die strenge Vergabe von Berechtigungen zu achten.

**Absicherung der Server-Server-Kommunikation**

Die Server-Server-Kommunikation muss unter Exchange dann verschlüsselt werden, wenn vertrauliche Daten über ungesicherte Netze übertragen werden oder die Authentisierung an einem der Server mittels Klartext-Authentisierung stattfindet.

Die zur Verfügung stehenden Verschlüsselungsmechanismen hängen von den verwendeten Exchange-Konnektoren ab. Insofern ist bei der Wahl des Konnektors auch darauf zu achten, welche Verschlüsselungsmechanismen dadurch benutzt werden können.

**Absicherung der Nachrichten-Kommunikation**

Auf Nachrichten-Ebene haben sich in der Praxis zur Absicherung von E-Mails auf S/MIME und OpenPGP basierende Programme durchgesetzt. Das Schlüsselmanagement von S/MIME setzt den Betrieb einer Public-Key-Infrastruktur (PKI) voraus. PGP setzt dagegen auf ein offenes Schlüsselmanagement und verlangt keinen Aufbau einer zentralen PKI.

Die Absicherung auf Nachrichten-Ebene wird von Drittherstellern in der Regel als Plug-In-Lösung für einen oder mehrere E-Mail-Clients realisiert (siehe M 5.110 *Absicherung von E-Mail mit SPHINX (S/MIME)*).

Auch auf der Ebene des Dateisystems sind Lösungen, z. B. in Form von Shell-Erweiterungen, zur Verschlüsselung und Signatur einzelner Dateien verfügbar. Derart geschützte Dateien können dann als Dateianhänge via E-Mail versendet werden.

**Public Key Infrastruktur**

Microsoft Outlook bietet einen eingebauten Mechanismus zur E-Mail-Verschlüsselung auf Basis von S/MIME. Dieser nutzt die Vertrauensbeziehungen einer Public Key Infrastruktur, die mit Hilfe der eigenen Windows Enterprise CA (Certification Authority) oder einer fremden CA betrieben werden kann. Die von einer CA selbstsignierten Wurzelzertifikate müssen dem System zur Verfügung stehen. Dazu sollten die als vertrauenswürdig geltenden Wurzelzertifikate für alle Outlook-Clients zentral über eine Windows-Gruppenrichtlinie konfiguriert werden.

**Weitere Sicherheitsvorkehrungen**

Um einen sicheren Betrieb einer PKI zu gewährleisten, sind die folgenden Vorkehrungen zu treffen:

- Absicherung der eingesetzten Komponenten und
- Verwendung von Zertifikatsrückruflisten (Certificate Revocation List, CRL).

Zusätzlich zu den allgemein bekannten Systemkomponenten von Microsoft Exchange-Server müssen noch die Komponenten abgesichert werden, die für den Betrieb von Exchange mit Verschlüsselungs- und Signatur-Funktionalität zuständig sind.

Beim Rückruf eines oder mehrerer Benutzerzertifikate spielt die Gültigkeitsdauer der Zertifikatsrückrufliste eine wesentliche Rolle. Es wird empfohlen, die CRL nach einem Rückruf sofort zu veröffentlichen und nicht auf den nächsten

eingeplanten Zeitpunkt der Veröffentlichung zu warten. Es ist jedoch zu beachten, dass durch die Veröffentlichung einer neuen CRL die alte Liste nicht automatisch ihre Gültigkeit verliert und somit die Clients, die bereits eine gültige CRL besitzen, von der neuen keinen Gebrauch machen müssen. Generell empfiehlt es sich daher, die Gültigkeitsdauer von CRLs relativ kurz zu bemessen, so dass die Clients entsprechend häufig ihre CRLs erneuern müssen.

Wie diese Anforderungen konkret umzusetzen sind, kann den Informationen aus dem Microsoft Technet entnommen werden, beispielsweise für die Version 2010 in folgenden Dokumenten:

- Eine Übersicht der Netzwerkschnittstellen bietet "Exchange Network Port Reference: Exchange 2010 Help".
- Die Nutzung von Outlook Web Access ist standardmäßig für jeden E-Mail-Benutzer möglich. Zugriffseinschränkungen und Segmentierung der Zugriffsobjekte sind dabei adäquate Mittel der Wahl, um eine sichere Konfiguration von Outlook Web Access durchzuführen, siehe auch "Understanding Security for Outlook Web App: Exchange 2010 Help".
- Outlook Anywhere (früher RPC-over-HTTP) wird unter "Understanding Outlook Anywhere: Exchange 2010 Help" behandelt.
- ActiveSync wird unter "Understanding Client Access: Exchange 2010 Help" behandelt.
- In Exchange 2010 wird die WebDAV-Schnittstelle nicht mehr unterstützt.
- Die TLS-Absicherung bei Transport-Servern wird unter "TLS Functionality and Related Terminology in Exchange 2010: Exchange 2010 Help" beschrieben. Die Deaktivierung der TLS-Absicherung wird nicht empfohlen.
- Die Absicherung von Unified-Messaging-Servern wird unter "Securing Unified Messaging Network Traffic: Exchange 2010 Help" beschrieben.
- Für Client-Access-Server und weitere Exchange Server-Rollen sind die in "Securing Client Access Servers: Exchange 2010 Help" beschriebenen Vorgaben zu beachten.

Prüffragen:

- Wurde nachvollziehbar entschieden, mit welchen Schutzmechanismen die Kommunikation von und zu Exchange-Systemen abgesichert wird?
- Wird die Übertragung schützenswerter Daten von und zu Microsoft Exchange-Systemen verschlüsselt?
- Sind vorhandene WebDAV-Schnittstellen abgesichert?

# M 5.101 Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.102 Installation von URL-Filtern beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.103 Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.104 Konfiguration des TCP/IP-Filters beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.105 Vorbeugen vor SYN-Attacken auf den IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.106 Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.107 Verwendung von SSL im Apache-Webserver

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 5.108 Kryptographische Absicherung von Groupware bzw. E-Mail

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Ein Groupware-System kommuniziert mit Groupware-Clients, Browsern, Telefonie- sowie Kommunikationsanwendungen und anderen Groupware-Systemen. Auch zwischen den Groupware-Systemkomponenten findet ein Datenaustausch statt. Die Kommunikation erfolgt über das lokale Netz und/oder externe Netze. In allen Fällen werden Daten übertragen, die geschützt werden müssen. Dies sind nicht nur die Daten, die genutzt werden, um Benutzer zu authentisieren (z. B. Benutzername und Passwort), sondern auch geschäftsrelevante Informationen. Es muss daher entschieden werden, mit welchen Schutzmechanismen die Kommunikation abgesichert wird.

Verschlüsselung und digitale Signaturen dienen dem Schutz der Integrität und Vertraulichkeit sowie auch der Nicht-Abstreitbarkeit elektronisch übermittelter Nachrichten.

Damit elektronische Kommunikation wie E-Mail nicht unterwegs verändert oder mitgelesen werden kann, muss sie kryptographisch abgesichert werden. Dabei kann die Vertraulichkeit durch Verschlüsselung und die Integrität, Authentizität und Nicht-Abstreitbarkeit durch digitale Signaturen erreicht werden.

Generell ist die kryptographische Absicherung von Groupware bzw. E-Mail auf drei Ebenen möglich:

**Netz-zu-Netz**

Hierbei wird die Kommunikation von einem Netzübergabepunkt zum anderen abgesichert, z. B. durch den Aufbau eines VPN (Virtual Private Network, siehe dazu auch Baustein B 4.4 *VPN*).

Vorteil: Die vorgegebene Verschlüsselung funktioniert unabhängig von Benutzereingriffen. Statt vielen Benutzern müssen nur einzelne Administratoren geschult werden.

Nachteile: Es sind keine individuellen Einstellungen möglich, z. B. für digitale Signaturen. Diese Lösung kann außerdem nur für einzelne Gruppen von vorher festgelegten Kommunikationspartnern eingesetzt werden.

Dies ist eine gute Lösung, wenn Organisationen oder Organisationsteile, die geographisch getrennt sind, häufig über einen sicheren Kanal kommunizieren wollen.

**Client-zu-Web-/Mailserver: z. B. TLS/SSL, Proxy-Lösung**

Bei der Proxy-Lösung wird jede Mail auf dem E-Mail-Server ver- bzw. entschlüsselt und im Klartext an den Client weitergeleitet.

Vorteil: Dies funktioniert unabhängig vom E-Mail-Client. Es ist keine zusätzliche Installation von Kryptoprogrammen bei den E-Mails-Clients erforderlich.

Nachteile: Bei Proxy-Lösungen kann die Konfiguration aufwendig sein. Bei TLS/SSL-Lösungen kann viel falsch gemacht werden.

**Client-zu-Client bzw. "Ende zu Ende"**

Bei der kryptographischen Absicherung von Client-zu-Client werden Funktionalitäten benutzt, die im jeweiligen E-Mail-Client integriert sind oder dort nachträglich installiert werden (z. B. als Plug-In). Bekannte Produkte hierfür sind GnuPG oder PGP. Bei deren Einsatz müssen viele Rahmenbedingungen beachtet werden, damit diese wirklich die Sicherheit bieten, die von ihnen erwartet wird.

In vielen E-Mail-Clients ist mittlerweile bereits die Möglichkeit zur Verschlüsselung und Digitalen Signatur integriert. Dadurch ergibt sich der Vorteil, dass diese Funktionen ohne Zusatzaufwand benutzt werden können. Der E-Mail-Verkehr innerhalb einer Institution kann damit direkt geschützt werden. Der Nachteil ist, dass dabei manchmal kryptographisch schwache Verfahren oder Implementierungen verwendet werden. Häufig treten auch Inkompatibilitäten mit anderen E-Mail-Clients auf.

Als Alternative gibt es eine Reihe von Zusatzprodukten zur Verschlüsselung und Digitalen Signatur. Vorteil: Die Produkte können so ausgewählt werden, dass sie genau auf die Bedingungen und Sicherheitsansprüche innerhalb einer Institution passen. Ein Nachteil ist, dass diese nicht immer für alle E-Mail-Programme verfügbar sind. Bei Updates des E-Mail-Programms ist unsicher, ob das Plug-In noch funktioniert oder auch dafür ein Update benötigt wird. Es kann passieren, dass diese Verschlüsselungsprogramme inkompatibel mit ähnlichen Programmen auf Empfängerseite sind.

Da die Client-zu-Client-Absicherung immer darauf basiert, dass jedem Benutzer kryptographische Schlüssel zugeordnet werden müssen, ist hierzu ein zentrales Schlüsselmanagement notwendig. Dieses muss unter anderem gewährleisten, dass die Schlüssel regelmäßig gewechselt werden, immer aktuell sind und sicher installiert und gespeichert werden, also nur dem Berechtigten zugänglich sind. Dies zieht natürlich einiges an Aufwand nach sich (siehe auch M 2.46 *Geeignetes Schlüsselmanagement*).

Welche Kriterien (z. B. Funktionalität, Benutzerfreundlichkeit, Interoperabilität, Wirtschaftlichkeit, vorliegende Sicherheitsuntersuchungen) bei der Auswahl eines geeigneten kryptographischen Produktes zu beachten sind, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.

Bei der Übertragung schützenswerter Daten zwischen Groupware-Systemen müssen diese angemessen geschützt werden. Hierfür können unterschiedliche Verfahren eingesetzt werden. Es ist daher zu entscheiden, welche Verfahren unter den jeweiligen Rahmenbedingungen angemessen sind. Die Entscheidung ist nachvollziehbar zu dokumentieren.

Prüffragen:

- Bei entsprechendem Schutzbedarf an Vertraulichkeit und Integrität: Gibt es ein Konzept zur kryptographischen Absicherung von E-Mail?

# M 5.109 Einsatz eines E-Mail-Scanners auf dem Mailserver

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Zur Erhöhung der Sicherheit sollte auf dem zentralen Mailserver ein E-Mail-Scanner mit integriertem speicherresidentem Virenschutzprogramm (oft auch E-Mail-Wächter genannt) installiert werden, das sowohl eingehende als auch ausgehende E-Mails, insbesondere deren Anhänge, auf Spam-Merkmale, Computer-Viren und andere schädliche Inhalte überprüft.

Ergänzend zur Einrichtung eines E-Mail-Wächters auf dem Mailserver selbst kann auch am Übergang zum Internet ein so genanntes SMTP-Gateway eingerichtet werden, auf dem die Überprüfung der ein- und ausgehenden E-Mails erfolgt. Die Anbindung an das Internet muss dann so realisiert werden, dass sämtliche SMTP-Verbindungen nur über das SMTP-Gateway abgewickelt werden können.

E-Mail-Scanner arbeiten dabei nach zwei grundsätzlich verschiedenen Ansätzen. Ein "Store-and-Forward"-Scanner nimmt zunächst eine E-Mail an und wendet dann seine Mechanismen an, um die E-Mail zu klassifizieren. Nach der Klassifikation entscheidet der Scanner, was mit der E-Mail geschehen soll (Löschen, Markieren, ...). Das Verfahren hat den Vorteil, dass die E-Mail zuerst angenommen wird und dann in aller Ruhe überprüft werden kann. Dies ist gleichzeitig aber auch ein Nachteil, da man aus juristischer Sicht die E-Mail bereits entgegengenommen hat und somit zur Zustellung an den Benutzer verpflichtet ist. Ein Online-Scanner prüft eine E-Mail bereits während der Annahme einer E-Mail und versucht diese zu klassifizieren. Stellt er fest, dass eine E-Mail unerwünscht sein könnte, kann er sie direkt ablehnen und die E-Mail verbleibt in der Verantwortung des Einlieferers. Dieses Verfahren hat den Vorteil, dass die Benutzer nicht mit markierten E-Mails oder Quarantänemitteilungen überhäuft werden. Nachteilig ist, dass bei einer falschen Klassifikation durch den Scanner die E-Mail nicht mehr lokal vorliegt. Sie liegt physikalisch beim Einlieferer und weder Benutzer noch Administrator haben zunächst Zugriff darauf. Im praktischen Einsatz wird häufig eine Mischung aus beiden Verfahren verwendet. Welche Filtermaßnahmen dabei "online" bzw. nach der Annahme der E-Mail angewendet werden sollen, muss durch eine entsprechende Richtlinie definiert und mit der Leitung abgestimmt werden.

Ebenso wichtig ist es, auch ausgehende E-Mails zu überprüfen. Einerseits kann so möglicherweise eine Infektion im internen Netz entdeckt werden, bevor größerer Schaden entsteht. Andererseits schützt dies aber auch die Behörde bzw. das Unternehmen vor einem eventuellen Ansehensverlust oder gar Schadensersatzansprüchen, die dadurch entstehen könnten, dass virenverseuchte E-Mails an Geschäftspartner verschickt werden. Bei ausgehenden E-Mail-Scannern muss definiert werden, was mit als virenverseucht erkannten E-Mails geschehen soll. Zumindest sollte ein Alarm beim Administrator ausgelöst werden.

Die meisten E-Mail-Wächter bieten umfangreiche Einstellmöglichkeiten im Bezug darauf, was mit "verdächtigen" E-Mails zu tun ist. Beispielsweise können solche E-Mails grundsätzlich gelöscht, markiert zugestellt oder auch auf einem "Quarantäne-Server" zwischengespeichert werden bis feststeht, ob der Inhalt harmlos ist. Eine weitere Möglichkeit ist es, nur eventuell bösartige E-Mail-An-

hänge abzutrennen, während die Nachricht selbst mit einem entsprechenden Hinweis an den Empfänger weitergeleitet wird.

Um Spam-Merkmale in einer E-Mail zu erkennen, unterstützen entsprechende E-Mail-Scanner vielfältige Mechanismen.

Im ersten Schritt werden häufig Black- und Whitelists verwendet, um die Reputation der an der Kommunikation beteiligten fremden IP-Adresse zu verifizieren. Es gibt beispielsweise Listen, die eine Aussage darüber tätigen, ob eine IP-Adresse in der Vergangenheit unerwünschte E-Mails versendet hat oder ob hinter der IP-Adresse ein valider Mailserver steckt. Des Weiteren gibt es Listen, die aussagen, ob sich ein Mailserver hinter einer IP-Adresse RFC-konform verhält, oder ob er sich in einem Einwahlnetz befindet.

Diese Listen werden häufig verwendet, um die Kommunikation mit den IP-Adressen schon frühzeitig zu beenden und gar keine E-Mails anzunehmen. Sie werden von Anbietern gepflegt und sowohl kostenlos als auch kostenpflichtig angeboten. Bei der Nutzung solcher Listen ist zu beachten, dass diese potentiell fehleranfällig sein können. Möglicherweise wird ein Geschäftspartner durch eine Unachtsamkeit auf eine solche Liste gesetzt und man kann in Folge dessen keine E-Mails mehr von diesem Partner erhalten. Weiterhin muss berücksichtigt werden, dass ein Anbieter einer solchen Liste auch die Macht besitzt, zu entscheiden, von welchem Partner die Institution zukünftig noch E-Mails erhalten wird.

Die Anbieter solcher Listen bieten diese häufig über einen DNS-Server an (sogenannte DNSBL, DNS-based Blackhole Lists). Nutzt ein Betreiber eines E-Mail-Scanners eine solche DNSBL, sendet der E-Mail-Scanner die IP-Adressen aller eingehenden E-Mails an den Betreiber der DNSBL. Als Antwort erhält der E-Mail-Scanner eine Aussage, ob die IP-Adresse gelistet ist oder nicht. Durch dieses Verfahren erhält der Anbieter einer DNSBL die IP-Adressen aller mit der Institution kommunizierenden Mailsysteme. Ihm ist es damit möglich umfangreiche Profile über die Mailkommunikation zu erstellen. Um dieses Problem zu vermeiden, bietet es sich an, auf lokale Kopien der Blacklists zurückzugreifen. Viele Anbieter stellen Kopien des Datenbestandes (kostenpflichtig) zur Verfügung.

Die Risiken zum Einsatz von Blacklists müssen vor dem Einsatz überprüft werden. Die Gefahren, die durch den Einsatz entstehen, müssen durch entsprechende Vorsorgemaßnahmen oder Verträge mit dem Anbieter minimiert werden.

**RFC-Konformitätsprüfung**

Ein weiterer wichtiger Prüfschritt ist eine RFC-Konformitätsprüfung während des SMTP-Dialogs. Es ist zu prüfen, ob der einliefernde Mailserver sich mit einem gültigen Namen meldet (HELO/EHLO), ob die IP-Adresse des Servers per DNS rückwärts auflösbar ist, ob die Auflösung des Namens wieder die IP-Adresse ergibt, ob die Syntax des Absenders und des Empfängers der E-Mail korrekt ist und ob der Empfänger überhaupt existiert. Spammer erzeugen hier häufig so viele Fehler, dass viele E-Mails über Konformitätsprüfungen abgelehnt werden können. Im Umkehrschluss bedeutet dies aber auch, dass ein Administrator seine Systeme RFC-konform einrichten muss, damit eigene E-Mails nicht aufgrund solcher Fehler geblockt werden.

**Prüfung von E-Mail-Inhalten**

Im nächsten Schritt werden häufig die Inhalte einer E-Mail überprüft. Hier werden signaturbasierende Filtersysteme verwendet, um unerwünschte E-Mails anhand von Schlüsselbegriffen oder anderer spamtypischer Eigenarten zu erkennen. Häufig arbeiten die Filter nach einem Punktesystem. Erkennt das Filtersystem eine bestimmte negative Eigenschaft, werden Punkte dafür vergeben. Die Punkte aller negativen Eigenschaften werden dann addiert und ergeben somit einen Indikator für die Wahrscheinlichkeit, dass die E-Mail unerwünscht ist. Die Filter, die dazu eingerichtet werden müssen, unterliegen einem ständigen Wandel. Die Vision eines selbständig arbeitenden E-Mail-Scanners bleibt allerdings eine solche. Die Filtersysteme müssen dynamisch an die aktuellen Spamwellen angepasst werden und erfordern händische Eingriffsmöglichkeiten durch den Administrator.

Jeder E-Mail-Scanner sollte auch mindestens eine, besser mehrere Module zur Erkennung von Schadsoftware besitzen. E-Mails mit erkannten Viren sollten nicht zugestellt, sondern in Quarantänen zwischengespeichert werden.

Im Umgang mit Anhängen, die ein Schadpotential haben könnten, aber in denen zum Einlieferungszeitpunkt keine Schadsoftware nachgewiesen werden konnte, muss zunächst eine Richtlinie definiert werden, die entweder aussagt, welche Dateitypen für eine Institution schädlich sind oder welche Dateitypen definitiv unschädlich sind. Sehr kritisch sollte dabei die Notwendigkeit der Übertragung von ausführbaren Anhängen in E-Mails hinterfragt werden. Nach der Definition der Richtlinie kann diese dann mit einer entsprechenden durch "Blacklists" oder "Whitelists" umgesetzt werden. Bei einer "Blacklist" wird eine Liste "verbotener" Dateitypen definiert, die keinesfalls als Anhänge an E-Mails versandt werden dürfen und die auch bei eingehenden E-Mails nicht akzeptiert werden. Ein restriktiverer Ansatz ist die "Whitelist", bei der nur solche Dateitypen als E-Mail-Anhänge zugelassen werden, die auf der festgelegten Liste erlaubter Typen stehen. Bei der Festlegung von Black- oder Whitelists sollte darauf geachtet werden, dass ein vernünftiger Kompromiss zwischen Sicherheit und Funktionalität gefunden wird. Zu laxe Einstellungen führen unter Umständen dazu, dass schädliche Inhalte in das interne Netz gelangen, während zu strenge Einstellungen die Produktivität behindern können.

Da verschlüsselte E-Mails nicht automatisch überprüft werden können, muss auch festgelegt werden, wie mit verschlüsselten E-Mails zu verfahren ist (siehe hierzu auch Bausteine B 1.6 *Schutz vor Schadprogrammen* und B 1.7 *Kryptokonzept*).

Die Mitarbeiter müssen darüber informiert werden, dass E-Mails automatisch gescannt werden und welche Regeln gelten. Außerdem sollte bei der Entscheidung, E-Mails automatisch auf dem Mailserver zu scannen, die Personalvertretung und der Datenschutzbeauftragte beteiligt werden. Je nach Land und der Art der Institution (Behörde oder Firma) müssen eventuell auch noch andere Rechtsvorschriften beachtet werden.

Selbst wenn ein E-Mail-Wächter auf dem Mailserver installiert wurde, sollte keinesfalls auf den Einsatz von Virenscannern auf den Arbeitsplatzrechnern verzichtet werden. Obwohl inzwischen der überwiegende Anteil von Viren und anderen Schadprogrammen per E-Mail verbreitet wird, gibt es doch noch genügend andere Verbreitungsmöglichkeiten für bösartige Programme, beispielsweise über USB-Sticks oder andere Wechselmedien oder über den Dateidownload aus dem Web.

**Notfallpläne gegen Überlastung**

E-Mail übertragende Systeme haben auch häufig damit zu kämpfen, dass sich das zu verarbeitende Volumen schlagartig ändern kann. Selbst wenn die Institution peinlichst auf gute Skalierung der Systeme geachtet hat, kommt der Moment, wo die Systeme überlastet werden. Für diese Momente muss ein Notfallplan vorbereitet werden.

Ein Notfallplan muss definieren, wie schrittweise die Funktionalität des E-Mail-Scanners verschärft werden kann, um das Verarbeitungsvolumen zu senken und welche Auswirkungen dies auf die Kommunikation hat. Da die Auswirkungen häufig mit Einschränkungen verbunden sind, ist die Leitungsebene auf diese Einschränkung hinzuweisen und der Notfallplan mit der Leitungsebene abzustimmen. Die praktische Durchführbarkeit des Notfallplans sollte im Vorfeld geübt werden und, wenn nötig, Anpassungen vorgenommen werden.

Exemplarisch als Notfallmaßnahme sei genannt, dass es möglich ist, den E-Mail-Scanner so zu konfigurieren, dass er nur noch eine Kommunikation zwischen definierten Kommunikationspartnern zulässt. Alle anderen (neuen) Kommunikationspartner werden während der Aktivierung des Notfallplans ausgesperrt.

Prüffragen:

- Ist auf dem zentralen Mailserver ein speicherresidentes Virenschutzprogramm (sogenannte E-Mail-Wächter) installiert, das sowohl eingehende als auch ausgehende E-Mails auf schädliche Inhalte überprüft?
- Gibt es eine Regelung für den Umgang mit verschlüsselten E-Mails, die nicht ohne weiteres gescannt werden können?
- Sind Mitarbeiter, Datenschutzbeauftragter und Personalrat darüber informiert, dass E-Mails gescannt werden?

# M 5.110 Absicherung von E-Mail mit SPHINX (S/MIME)

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Die zunehmende Bedeutung von E-Mail erfordert den Einsatz von Maßnahmen, die eine Vertraulichkeit und Verbindlichkeit gewährleisten. Dies kann durch den breiten Einsatz von Produkten zur Verschlüsselung und digitalen Signatur von E-Mails erreicht werden. Die elektronische Signatur stellt dabei sicher, dass die E-Mail vom angegebenen Absender kommt und unverändert ist. Die Verschlüsselung der Informationen bewirkt, dass nur der rechtmäßige Empfänger die E-Mail lesen kann.

Zu diesem Zweck wurde vom BSI das Projekt SPHINX initiiert, in dessen Rahmen kryptographische Produkte auf internationalen Standards fortentwickelt wurden. Die Interoperabilität, das bedeutet die fehlerfreie Austauschbarkeit von kryptographisch behandelten Nachrichten, der Produkte verschiedener Hersteller und für verschiedene Plattformen wird quartalsweise durch ein Testlabor untersucht und das Ergebnis veröffentlicht.

**Kryptographische Verfahren**

Zur Erreichung einer herstellerunabhängigen Interoperabilität kommen bei SPHINX ausschließlich Produkte zum Einsatz, die auf den Industriestandards S/MIME und "MailTrusT" beruhen. Diese Standards nutzen zur Erzeugung sicherer E-Mails eine Kombination unterschiedlicher kryptographischer Verfahren. Als symmetrisches Verfahren wird der Triple-DES-Algorithmus mit 112 Bit Schlüssellänge zur Verschlüsselung der Daten verwendet. Das eingesetzte Public-Key-Verfahren für die elektronische Signatur und zur Verschlüsselung ist der RSA-Algorithmus mit mindestens 1024 Bit Schlüssellänge. SHA-1 ist der empfohlene Hash-Algorithmus, der zur eindeutigen Abbildung der Nachricht auf einen Wert mit definierter Länge verwendet wird.

Die Zuordnung von kryptographischen Schlüsseln zu Personen wird durch digitale Zertifikate geregelt. Ein Zertifikat ist ein elektronisches Dokument, das im wesentlichen den öffentlichen Schlüssel und den Namen des Schlüsselinhabers enthält. Mit ihrer elektronischen Unterschrift beglaubigt die Zertifizierungsstelle (Trustcenter) die Zuordnung zwischen Schlüssel und Person. Bei SPHINX werden standardisierte Zertifikate gemäß der ITU-Empfehlung X.509 Version 3 verwendet.

Das Vertrauen zwischen den Kommunikationspartnern besteht im Kern im Vertrauen auf die digitalen Zertifikate und der Glaubwürdigkeit aller Angaben, die es enthält. Für die öffentliche Verwaltung wurden bereits durch mehrere Trustcenter Zertifikate ausgestellt. Diese Trustcenter werden durch die übergeordnete Wurzelzertifizierungsstelle des BSI überprüft und in der PKI (Public Key Infrastruktur) der öffentlichen Verwaltung zusammengeschlossen. Damit unterliegen alle ausgestellten Zertifikate dem Standard des IT-Grundschutzes in allen Fragen der Informationssicherheit. Für den Kontakt zum Bürger und zu Firmen wurde die Verwaltungs-PKI in die European Bridge-CA integriert, die unabhängige PKI miteinander vertrauenswürdig verbindet.

Eine weitere Anforderung zur Bildung des Vertrauens ist der Schutz des geheimen Schlüssels eines Benutzers. Dazu kann der geheime (oder persönliche) Schlüssel entweder in einer speziellen Datei oder einer Chipkarte gespeichert werden. Im Allgemeinen wird diese Datei bzw. die Chipkarte als Personal-Se-

curity-Environment (PSE) bezeichnet, also persönliche Sicherheitsumgebung. PSEs sind kryptographisch geschützt und können nur mittels Passwort zur Benutzung aktiviert werden. Für den sicheren Umgang mit dem Passwort und der Datei bzw. der Chipkarte ist der Eigentümer verantwortlich.

**Sichere Installation und Bedienung**

Bei SPHINX-Produkten handelt es sich in der Regel um sogenannte Plugin-Produkte. Sie ergänzen das vorhandene E-Mail-Produkt mit als sicher anerkannte kryptographische Verfahren.

Durch falsche Konfiguration oder Fehlbedienung kann es aber zu einer Abschwächung des Sicherheitsniveaus kommen.

Die Konfiguration ist bei SPHINX-Produkten wie bei den meisten komplexeren Kryptoprodukten nicht selbsterklärend. Damit sich keine Administrationsfehler einschleichen, ist die Einarbeitung in das genutzte SPHINX-Produkt notwendig. In Unternehmen und Behörden sollte ein Mitarbeiter der IT-Administration in den Umgang mit dem SPHINX-Produkt eingearbeitet werden und als technischer Ansprechpartner zur Verfügung stehen.

Um Verständnis für die Anwendung der neuen Funktionalitäten beim Benutzer zu erreichen, ist die Vermittlung von einigen kryptographischen Grundbegriffen notwendig. Die Abläufe zur Beantragung eines Zertifikates und die Bedienung des SPHINX-Produktes sollten geschult werden. In Unternehmen und Behörden sollten ausgewählte Benutzer in den Umgang mit dem SPHINX-Produkt eingearbeitet werden und als Multiplikatoren die weiteren Benutzer im Umgang mit dem Produkt einweisen. Eine Schulung durch den Hersteller bzw. Vertreiber des Produktes ist vorzuziehen. Insbesondere sollte das Erzeugen von signierten und verschlüsselten E-Mails bzw. der Empfang dieser geübt werden, bevor ein Benutzer das Programm verwendet.

Es ist empfehlenswert, dass innerhalb einzelner Organisationen ein einheitliches SPHINX-Produkt, besser noch eine einheitliche Programmversion verwendet wird. Damit können Aufwände bei der Administration, Schulung, Betreuung und Software-Pflege gering gehalten werden.

Zu jedem SPHINX-Produkt gehört eine umfangreiche Dokumentation, die vor der Verwendung gelesen werden sollte. Sie sollte vor ihrer Verteilung an die Anwender auf die Eigenheiten der Organisation angepasst werden. Damit lässt sich eine höhere Akzeptanz bei der Produkteinführung erreichen.

**Schlüsselaufbewahrung**

Die privaten Schlüssel werden in der Personal-Security-Environment (PSE) abgelegt. Entscheidend für den sicheren Betrieb ist, dass der Inhalt der PSE vertraulich bleibt und vor Manipulationen geschützt wird. Das genutzte Passwort ist nach den in M 2.11 *Regelung des Passwortgebrauchs* beschriebenen Passwortregeln zu bilden und sicher zu verwahren. Eine Weitergabe, ungewollt oder wissentlich, befähigt andere Personen im Namen des Eigentümers elektronisch zu unterschreiben.

Ist die PSE eine Datei, so spricht man von einer Soft-PSE. Diese ist durch das Passwort kryptographisch geschützt. Es wird empfohlen, sie nicht auf Netzlaufwerken zu speichern, da sonst weitere Sicherheitsmaßnahmen ergriffen werden müssen. Der Einsatz von Chipkarten zur Schlüsselspeicherung ist vorzuziehen. Aber auch bei Chipkarten muss das verwendete Passwort sicher

verwahrt werden. Bei den Chipkarten, die bei SPHINX zum Einsatz kommen, kann keine Kopie angelegt werden.

Von der Soft-PSE sollte eine Sicherungskopie angelegt sowie das Passwort notiert werden. Die Sicherungskopie und das Passwort sollten sicher, am besten getrennt verwahrt werden. So kann sichergestellt werden, dass bei einem Festplattencrash oder einer Fehlbedienung die PSE nicht verloren geht. Nachrichten, die verschlüsselt wurden, lassen sich bei Verlust der PSE nicht mehr entschlüsseln.

Das Aufschreiben und Hinterlegen des Passworts an einem gesicherten Ort sollte hierbei als kritischer Vorgang betrachtet werden, der ausschließlich der Notfallvorsorge dient. Die abgeschlossene Schublade eines Schreibtisches oder ähnlich "sichere" Orte können **keinesfalls** als Aufbewahrungsort für die PSE oder das Passwort empfohlen werden.

**Schlüsselverteilung**

Damit ein Empfänger die elektronische Signatur des Senders einer Datei überprüfen kann bzw. der Sender eine Nachricht für einen bestimmten Empfänger verschlüsseln kann, benötigt er das digitale Zertifikat seines Kommunikationspartners. Dieses kann er auf verschiedene Arten erhalten, z. B. per Anlage einer E-Mail oder von einem speziellen Internet-Server (Verzeichnis), manchmal auch von einem WWW-Server.

SPHINX-Produkte unterstützen den Benutzer bei der Überprüfung der digitalen Zertifikate. Der Benutzer muss bei den meisten Produkten beim ersten Empfang das Zertifikat seines Kommunikationspartners einer E-Mailadresse manuell zuordnen. Neben dem Zertifikat des Kommunikationspartners wird zur automatischen Überprüfung das Zertifikat des ausstellenden Trustcenters benötigt. Die erforderlichen Zertifikate werden meistens als Anlage in der signierten E-Mail mit übertragen. Das Zertifikat der Wurzelzertifizierungsstelle sollte vorhanden oder durch den IT-Service vorinstalliert worden sein.

Damit ein Benutzer in den Besitz eines eigenen Zertifikats gelangt, werden von ihm Zertifikats-Beantragung und Identifikation gefordert. Beides wickelt er in Zusammenarbeit mit der Registrierungsstelle ab. Bei Behörden, Firmen, Organisationen sind diese meist beim Inneren Dienst bzw. Werkschutz zu finden. Trustcenter unterhalten meist Registrierungsstellen in ihren Filialen. Die Registrierungsstelle prüft die Zertifikatsanträge auf Richtigkeit und identifiziert den Benutzer anhand seines Dienst- oder Personalausweis. Werden Chipkarten ausgegeben, so sind sie in der Regel ebenfalls dort zu erhalten. Bei Soft-PSEs erfolgt die Zusendung elektronisch, meistens per E-Mail.

Prüffragen:

- Sind die Zuständigkeiten für die Administration und die technische Benutzer-Unterstützung geregelt?
- Werden Benutzer für das Produkt einschließlich notwendiger kryptographischer Grundlagen geschult?
- Gibt es Regelungen zur Speicherung und Aufbewahrung von Schlüsseln und Passwörtern gegen deren Verlust und Kompromittierung?

# M 5.111 Einrichtung von Access Control Lists auf Routern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die vielfältigen Zugriffsmöglichkeiten für die Nutzung und die Administration von Routern und Switches können mit Hilfe von Access Control Lists (ACLs) kontrolliert werden. Der Zugriff kann für einzelne Rechner oder Netze und für die jeweilige Zugriffsmethode festgelegt werden.

Mittels der ACL erfolgt die Festlegung, welche Rechner oder Netze auf den Router oder den Switch über Dienste wie bspw. TELNET, SNMP, HTTP, etc. zugreifen können. Das folgende Beispiel zeigt eine entsprechende ACL eines Cisco-Routers zur Zugriffsbeschränkung für den Dienst TELNET auf das Netzkoppelelement selbst:

*access-list 102 permit tcp host 163.183.200.22 any eq 23 log*

*access-list 102 permit tcp host 163.183.200.24 any eq 23 log*

*access-list 102 deny ip any any log*

Die Festlegung der ACLs muss entsprechend den Vorgaben der Sicherheitsrichtlinie erfolgen. Insbesondere sollte ein generelles Vorgehen für den Fall festgelegt werden, dass keine spezifischen Regeln existieren. In diesem Zusammenhang gibt es grundsätzlich die beiden Ansätze "Was nicht verboten ist, ist erlaubt" (Blacklist) und "Was nicht erlaubt ist, ist verboten" (Whitelist). Bei der Konfiguration sollte generell der restriktivere Whitelist-Ansatz bevorzugt werden, da beim reinen Blacklist-Ansatz nahezu zwangsläufig Lücken bestehen bleiben.

Mit Hilfe von ACLs kann nicht nur der Zugriff auf das Netzkoppelelement selbst, sondern auch der Datenverkehr über das Netzkoppelelement kontrolliert werden. Insbesondere Router werden als Paketfilter in lokalen Netzen und Weitverkehrsnetzen eingesetzt. Der Router kontrolliert in diesem Fall den Datenverkehr pro Interface und Richtung (inbound und outbound) zwischen den angeschlossenen Subnetzen.

Für verbindungsbehaftete Protokolle (beispielsweise TCP) gibt es zudem die Möglichkeit, ACLs zu definieren, die den Status der Verbindung berücksichtigen. Dies erlaubt es, vorzugeben, dass bestimmte Verbindungen nur in einer Richtung durch den Router erlaubt sind (beispielsweise Telnet-Verbindungen "von innen nach außen"). Dabei lässt der Router Pakete in der Gegenrichtung passieren, wenn sie Antwortpakete zu einer bestehenden Verbindung sind, weist jedoch Pakete zurück mit denen ein Verbindungsaufbau in der verbotenen Richtung versucht werden soll.

Verbindungslose Protokolle wie UDP lassen sich nur unzureichend mit einem herkömmlichen Paketfilter absichern. Für diesen Zweck wird deshalb oftmals ein Stateful-Inspection-System verwendet. Dabei führt das System eine Tabelle, in der gespeichert wird, ob und von wo innerhalb einer festgelegten Zeitspanne ein "erlaubtes" Paket (beispielsweise eine DNS-Anfrage) an eine bestimmte Adresse gesendet wurde.

Wird innerhalb der festgelegten Zeit ein Paket in der entgegengesetzten Richtung registriert, so wird dies als Antwort auf die gespeicherte Anfrage interpre-

tiert und durchgelassen. Pakete, zu denen es keine entsprechende Anfrage gibt, werden abgewiesen.

In der Regel werden innerhalb einer ACL mindestens folgende Kriterien ausgewertet:

- Quelladresse (IP-Adresse im IP-Header) des Pakets
- Zieladresse (IP-Adresse im IP-Header) des Pakets
- Verwendetes Protokoll und gegebenenfalls Portnummer (z. B. Port 80/TCP für HTTP oder 25/TCP für SMTP)

Zum Erkennen von Problemen wie beispielsweise Konfigurationsfehlern oder Angriffsversuchen im Netz sind ACLs immer derart zu konfigurieren, dass abgewiesene Zugriffsversuche protokolliert werden. Hierzu ist jedem Eintrag in der ACL das entsprechende Protokoll-Kommando anzufügen. Die Protokolldateien werden so zu einer wertvollen Datenquelle im Umgang mit Problemen und Angriffen im Netz.

Die Erstellung einer ACL muss entsprechend den Vorgaben der Sicherheitsrichtlinie erfolgen. Nach Möglichkeit sollten Vorlagen (Templates) erstellt werden, die immer wieder verwendet werden können und nur gegebenenfalls geringfügig modifiziert werden müssen.

Bei der Nutzung von ACLs muss beachtet werden, dass damit eine gewisse Performance-Einbuße verbunden ist. Meist ist diese zwar selbst bei komplizierteren Regeln vernachlässigbar, wenn aber ein Router bereits mit einer erheblichen Auslastung betrieben wird, dann sollte vor einer Erweiterung der ACLs sicherheitshalber geprüft werden, ob das Gerät die erweiterten Regeln noch verarbeiten kann.

Nachfolgend sind als Beispiel einige Filterregeln anhand eines Auszugs aus einer Access Control List für einen Router des Herstellers Cisco dargestellt. Es wird davon ausgegangen, dass es sich um eine eingehende Zugriffsliste (inbound) handelt. Folgende Dienste sollen eingehend erlaubt, sonstige Verbindungen verboten werden:

- SMTP zum internen MAIL-SERVER
- TELNET zu einem internen TELNET-SERVER
- HTTP zum internen WEB-SERVER
- HTTPS zum internen WEB-SERVER

*access-list 103 permit tcp any any established*

*access-list 103 permit tcp any host MAIL-SERVER eq smtp*

*access-list 103 permit tcp any host TELNET-SERVER eq telnet*

*access-list 103 permit tcp any host WEB-SERVER eq www*

*access-list 103 permit tcp any host WEB-SERVER eq 443*

*access-list 103 deny ip any any log*

Prüffragen:

- Entspricht die Festlegung der ACLs der Router und Switches den Vorgaben der Sicherheitsrichtlinie?
- Wird für die Konfiguration der ACLs das Whitelist-Verfahren eingesetzt?
- Werden durch die ACLs abgewiesene Zugriffsversuche protokolliert?

# M 5.112 Sicherheitsaspekte von Routing-Protokollen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

### Authentisierung

Idealerweise sollten nur Routing-Protokolle eingesetzt werden, die eine sichere Authentisierung der Router beim Austausch von Routing-Informationen unterstützen. Sobald Updates von Routing-Tabellen versendet werden, muss eine Authentisierung des Routers stattfinden, der diese Routing-Updates versendet hat. Damit wird erreicht, dass ein Router nur zuverlässige Routing-Informationen von einer vertrauten Quelle (Router) verarbeitet. Ohne eine Authentisierung beim Austausch von Routing-Informationen wird die Sicherheit des Netzes durch unautorisierte oder absichtlich gefälschte Routing-Updates gefährdet.

Zusätzliche Sicherheit wird durch die Einrichtung von Access Control Lists erreicht, so dass nur definierte IP-Adressen Routing-Informationen austauschen dürfen.

Dynamische Routing-Protokolle sollten ausschließlich in sicheren Netzen verwendet werden. In demilitarisierten Zonen (DMZ) dürfen sie nicht eingesetzt werden. Gelingt es nämlich einem Angreifer, Datenpakete beim Austausch von Routing-Informationen in der DMZ mitzulesen, so kann er daraus Kenntnisse über die interne Netzstruktur erlangen. In demilitarisierten Zonen sollten stattdessen statische Routen eingetragen werden.

Folgende Routing-Protokolle unterstützen eine Authentisierung beim Austausch von Routing-Informationen:

- Border Gateway Protocol (BGPv4)
- Open Shortest Path First (OSPFv2)
- Routing Information Protocol in der Version 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)
- Intermediate-System-to Intermediate-System (IS-IS)

Die Authentisierung eines Routers, der Routing-Updates versendet, wird durch den Austausch eines Schlüssels (Passwort) erreicht. Dieser Schlüssel muss allen beteiligten Routern bekannt sein. Der Schlüssel wird bei der Konfiguration des Routers vom Administrator festgelegt. Diese Schlüssel sollten regelmäßig geändert werden.

### Kryptographische Authentisierung

Bei den unterschiedlichen Routing-Protokollen wird zwischen der Klartextauthentisierung und der kryptographischen Authentisierung unterschieden. Es kann nur der Einsatz von Routing-Protokollen empfohlen werden, die eine kryptographische Authentisierung unterstützen.

Bei der kryptographischen Authentisierung wird in der Regel das Hash-Verfahren MD5 verwendet. Statt des eigentlichen Schlüssels wird dabei ein sogenanntes Message-Digest zur Authentisierung versendet. Der Message-Digest wird zwar mit Hilfe des Schlüssels erzeugt, jedoch wird der Schlüssel nicht über das Netz gesendet.

Damit wird verhindert, dass der Schlüssel im Netz mitgelesen werden kann. Hinsichtlich des Schlüsselmanagements ist zu beachten, dass die Schlüssel so verteilt und erneuert werden müssen, dass sie vor unbefugtem Mitlesen oder Abhören geschützt sind.

Folgende Protokolle unterstützen eine kryptographische Authentisierung:

- Border Gateway Protocol (BGPv4)
- Open Shortest Path First (OSPFv2)
- Routing Information Protocol in der Version 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)
- Intermediate-System-to-Intermediate-System (IS-IS)

**Hinweis:** Im Hash-Algorithmus MD5 wurden kryptographische Schwächen gefunden. Es sollte deshalb möglichst ein stärkerer Algorithmus verwendet werden. Bessere Hash-Algorithmen als MD5 werden jedoch von den Routing-Protokollen und -Produkten noch nicht durchgängig unterstützt. RFC 4822 spezifiziert, wie Hash-Algorithmen der SHA-Familie zur Authentisierung beim Einsatz von RIPv2 genutzt werden können. Durch den Rückgriff auf IPSec können grundsätzlich auch bei OSPFv3 (OSPF for IPv6) stärkere Hash-Algorithmen als MD5 verwendet werden. Trotz der bekannten Schwächen von MD5 bietet eine MD5-basierte Authentisierung insgesamt ein höheres Sicherheitsniveau als eine Klartext-Authentisierung.

**Schlüsselverwaltung**

Einige Routing-Protokolle bieten eine Verwaltung von Schlüsseln unter Verwendung sogenannter Schlüsselketten an. Eine Schlüsselkette besteht aus einer Reihe von festgelegten Schlüsseln. Diese Schlüssel werden von den Routern im Rotationsverfahren verwendet. Dies verringert die Wahrscheinlichkeit, dass die Schlüssel ausgespäht werden. Der Schlüssel innerhalb einer Schlüsselkette besitzt nur für einen definierten Zeitraum Gültigkeit. Hier ist es wichtig, dass die Router die genaue Uhrzeit besitzen, damit der Schlüssel synchron gewechselt wird. Dies kann durch die Angabe eines internen NTP-Servers erreicht werden. Idealerweise sollte der interne NTP-Server mit einer Funkuhr verbunden sein.

Folgende Protokolle unterstützen die Schlüsselverwaltung:

- Routing Information Protocol in der Version 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)

Die folgende Tabelle stellt die unterschiedlichen Merkmale von Routing-Protokollen aus sicherheitstechnischer Sicht in Bezug auf die Authentisierung dar:

| **Protokollname** | **Authentisierung** | **Klartext** | **Hash** | **Protokoll RFCs** |
|---|---|---|---|---|
| RIPv1 | Nein | | | RFC 1058 |
| IGRP | Nein | | | Proprietär (Cisco) |
| RIPv2 | Ja | Ja | Ja | RFC 2453, 4822 |
| EIGRP | Ja | | Ja | Proprietär (Cisco) |
| OSPFv2 | Ja | Ja | Ja | RFC 2328 |
| IS-IS | Ja | Ja | Ja | RFC 1195, 5304 |

| Protokollname | Authentisierung | Klartext | Hash | Protokoll RFCs |
|---|---|---|---|---|
| BGPv4 | Ja | | Ja | RFC 4271 |

Tabelle: Authentisierung bei unterschiedlichen Routing-Protokollen

Prüffragen:

- Wurde festgelegt, ob eine Authentisierung der Router bei Routingupdates erforderlich ist?
- Erfolgt die Verteilung und Erneuerung der Schlüssel zur Authentisierung der Router geschützt gegenüber unbefugtem Mitlesen oder Abhören?
- Erfolgt eine regelmäßige Änderung der zum Versand der Routing-Updates genutzten Schlüssel zur Authentisierung der Router?
- Ist sichergestellt, dass durch Routing-Pakete keine Informationen über die interne Netzstruktur nach außen übertragen werden?
- Wird in demilitarisierten Zonen auf den Einsatz von dynamischen Routing-Protokollen verzichtet und werden stattdessen statische Routen genutzt?
- Sind klar abgegrenzte Routing-Domänen definiert?
- Wurde anhand des jeweiligen Schutzbedarfs entschieden, ob eine Authentisierung der Router erforderlich ist?

# M 5.113 Einsatz des VTAM Session Management Exit unter z/OS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche

Die z/OS-Komponente VTAM (*Virtual Telecommunication Access Method*) bietet die Möglichkeit, den Login-Vorgang durch einen *VTAM Session Management Exit* (*ISTEXCAA*) zusätzlich zu schützen. Dieser *Exit* wird während des Session-Aufbaus und -Abbaus von VTAM aus angesprochen und erlaubt die folgenden Funktionen:

- Session Authorization
  Prüfen und Erlauben/Ablehnen von *Logical Unit Sessions*
- Session Accounting
  Sammeln von *Session-Accounting*-Datenzur späteren Auswertung
- Adjacent SSCP Selection
  Auswahl eines *System Service Control Point* nach definierten Regeln (Routing)
- Unterstützung des Session Takeover im Rahmen von XRF Application Processing

Für die beiden ersten Funktionen wird der *VTAM Session Management Exit* häufig eingesetzt, für die beiden letzten dagegen nur in wenigen Sonderfällen. Der *VTAM Session Management Exit* muss vom Betreiber selbst erstellt oder beschafft werden. Der Hersteller liefert keinen *VTAM Session Management Exit* mit dem Betriebssystem aus.

Für den Einsatz des *VTAM Session Management Exits* sollten die folgenden Empfehlungen beachtet werden.

**Hinweise zur Programmierung**

*Assembler-Kenntnisse*

Der *Exit* muss in Assembler programmiert werden. Zudem werden gute Kenntnisse der VTAM-Software vorausgesetzt. Wenn die notwendigen Kenntnisse nicht vorliegen, ist zu überlegen, ob am Markt verfügbare alternative Software-Produkte eingesetzt werden sollten. Diese sind häufig einfacher und sicherer zu installieren.

*Performance*

Der *Exit* kann die VTAM-Performance erheblich beeinflussen. Deshalb ist darauf zu achten, dass beim Durchlaufen des *Exits* keine zeitaufwendigen Aktivitäten, wie z. B. das Lesen von Dateien, stattfinden.

*Definitionen*

Alle Definitionen, die der *Exit* während des Betriebs benutzt, sollten dynamisch nachladbar sein, ohne dass Betriebsfunktionen gestoppt werden müssen.

Das Regelwerk (*Policy*) für den *Exit* sollte möglichst extern definierbar sein (keine Definitionen im Programm).

**Unterstützte Funktionen**

Es sollten mindestens folgende Funktionen im *Exit* unterstützt werden:

- Schreiben eines LOG-Eintrags (*Syslog*)
- Schreiben eines SMF-Records
- Schnittstelle zu WTO (*Write to Operator*) für Abweisungen

Damit ist eine nachträgliche Kontrolle der abgewiesenen Login-Versuche möglich. Als Option können zusätzlich Statistik-Informationen geführt werden, jedoch können diese Informationen auch aus den SMF-Records abgeleitet werden.

**Schutz der Sicherheitsregeln**

Das Regelwerk (*Policy*) des *Exits* sollte in einer separaten Datei geführt werden, die beim ersten Durchlaufen des *Exits* in den Hauptspeicher geladen wird. Es sollten nur die Mitarbeiter Zugriff auf diese Datei haben, deren Tätigkeit dies erfordert. Dies gilt besonders dann, wenn das Regelwerk des *Exits* in der aktuellen *VTAMLST*-Datei geführt wird. Es ist zu überlegen, ob die Verkettung von verschiedenen *VTAMLST*-Dateien helfen kann, die Sicherheit des Betriebs zu erhöhen. Verschiedene *VTAMLST*-Dateien erlauben unterschiedliche Zugriffsrechte, wobei die verketteten Dateien in Bezug auf die Verarbeitung wie eine Datei behandelt werden. Eine Vertretungsregelung ist vorzusehen.

**VTAM Kommandos**

Der *VTAM Session Management Exit* kann während des Betriebs durch das *VTAM Modify*-Kommando dynamisch aktiviert bzw. deaktiviert werden. Durch entsprechende RACF-Definitionen ist sicherzustellen, dass nur die Mitarbeiter Zugang zu diesem Kommando haben, deren Tätigkeit dies erfordert. Eine Vertretungsregelung ist vorzusehen.

**Einsatz von NetView ALIAS Name Translation**

Im *VTAM Session Management Exit* können Funktionen zur *ALIAS Name Translation* eingesetzt werden. Parallel hierzu kann auch die *NetView ALIAS Name Translation Facility* verwendet werden. Letzteres wird durch ein Flag angezeigt. Wenn beides eingesetzt wird, ist darauf zu achten, dass beide Möglichkeiten zur *ALIAS Name Translation* aufeinander abgestimmt und widerspruchsfrei sind. Beispielsweise dürfen keine unterschiedlichen *Aliase* für den selben Namen gesetzt werden.

Prüffragen:

- Wird bei der Exit-Programmierung unter z/OS darauf geachtet, dass alle Definitionen, die der Exit während des Betriebes benutzt, dynamisch nachladbar sind, ohne dass Betriebsfunktionen gestoppt werden müssen?
- Wird bei der Exit-Programmierung unter z/OS darauf geachtet, dass keine Definitionen im Programm vorhanden sind, sondern dass das Regelwerk (Policy) für den Exit extern definierbar ist?
- Wird unter z/OS das Regelwerk (Policy) des Exits in einer separaten Datei geführt, die beim ersten Durchlauf des Exits in den Hauptspeicher geladen wird?
- Wird durch z/OS-RACF-Definitionen sichergestellt, dass zu dem VTAM Modify-Kommando nur die Mitarbeiter Zugang haben, deren Tätigkeit dies erfordert?

# M 5.114 Absicherung der z/OS-Tracefunktionen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Mit Trace-Funktionen können unter z/OS Fehler beim Verbindungsaufbau analysiert werden. Sie können sowohl in VTAM (*Virtual Telecommunication Access Method*), als auch bei TCP/IP benutzt werden. Das GTF (*Generalized Trace Facility*) wird benutzt, um die Trace-Daten zu erfassen und auszuwerten. Darüber hinaus stehen auch die Funktionen NLDM (*Network Logical Data Manager* - eine NetView-Komponente) und ACFTAP (*AdvancedCommunication Facility Trace Analysis Programm*) für die Auswertung von VTAM-Daten zur Verfügung.

Trace-Funktionen zeigen nicht nur Fehler auf, sondern erlauben auch die Darstellung der übertragenen Daten selbst. Deshalb sind die folgenden Hinweise zu beachten:

### Schutz von Trace-Funktionen und GTF

Werden Session-Daten unverschlüsselt übertragen, sind die Passwörter in Klarschrift im Trace lesbar. Zugang zu den Kommandos, die Traces initiieren können, darf deshalb nur den Mitarbeitern gegeben werden, die GTF im Rahmen ihrer Tätigkeit benötigen. Die Zahl dieser Mitarbeiter sollte möglichst klein gehalten werden, um das Risiko von Vertraulichkeitsverletzungen zu minimieren.

### Schutz von GTF-Dateien

Die GTF-Auswertungen werden in Dateien gesichert. Diese Dateien müssen so geschützt werden, dass nur die zuständigen Mitarbeiter darauf Zugriff haben (insbesondere *Universal Access=NONE*). Dies gilt auch für Kopien dieser Dateien.

### NLDM Traces

Die Trace-Funktion von NLDM sollte normalerweise deaktiviert sein und nur im Bedarfsfall aktiviert werden. Sie sollte nur den zuständigen Mitarbeitern zur Verfügung stehen.

### Schutz von ACFTAP

Das Programm ACFTAP sollte so geschützt werden, dass nur die zuständigen Mitarbeiter Zugriff auf dieses Programm haben.

### Session-Daten

Um die Passwörter vor unbefugtem Mitlesen bei der Übertragung zu schützen, sollte überlegt werden, die Session-Daten verschlüsselt zu übertragen. Es wird empfohlen, dies mindestens für die Verbindungen der RACF-Administratoren (*Resource Access Control Facility*) vorzusehen.

Prüffragen:

- Ist sichergestellt, dass nur Mitarbeiter Traces unter z/OS initiieren können, die GTF im Rahmen ihrer Tätigkeit benötigen?

- Sind die GTF-Auswertungen unter z/OS so geschützt, dass nur die zuständigen Mitarbeiter darauf Zugriff haben?
- Ist die Trace-Funktion von NLDM unter z/OS deaktiviert?
- Ist ACFTAP unter z/OS so geschützt, dass nur die zuständigen Mitarbeiter Zugriff auf dieses Programm haben?
- Werden bei der z/OS-Tracefunktion die Session-Daten verschlüsselt übertragen, um Passwörter vor unbefugtem Mitlesen bei der Übertragung zu schützen?

# M 5.115 Integration eines Webservers in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Die Integration eines Webservers in ein Sicherheitsgateway ist in vielen Fällen kritisch, da ein Webserver oft hohe Anforderungen an die Netz-Bandbreite stellt. Neben der Sicherstellung der Verfügbarkeit ist zum Schutz vor gezielten Angriffen auch die Wahl der richtigen Variante zur Server-Platzierung wichtig, da Webserver auf Grund ihrer hohen "Sichtbarkeit" besonders Angriffen ausgesetzt sind und in Webserver-Programmen in der Vergangenheit oft Sicherheitslücken vorhanden waren.

Im folgenden werden drei Szenarien beschrieben, wie ein Webserver in ein Sicherheitsgateway integriert werden kann:

- Integration ohne Verwendung eines Reverse Proxy
- Integration unter Verwendung eines Reverse Proxy, der die Auslastung des Webservers reduzieren soll.
- Integration unter Verwendung eines Reverse Proxy und mit zusätzlicher Absicherung durch einen weiteren Paketfilter.

In allen drei Fällen wird der Server nicht hinter einem ALG, sondern nur hinter einem Paketfilter aufgestellt, da der ALG den Gesamtdurchsatz des Systems unter Umständen zu stark beeinträchtigen kann. Daher sind die Empfehlungen auch dann anwendbar, wenn nur ein einfaches Sicherheitsgateway (bestehend nur aus einem Paketfilter) eingesetzt wird. Der Webserver sollte in keinem Fall im internen Netz angesiedelt werden.

Bei besonderen Sicherheitsanforderungen kann es trotzdem erforderlich sein, den Webserver mit einem eigenen ALG abzusichern, der den Webserver und darauf betriebene Webanwendungen vor bestimmten Arten von Angriffen (Cross-Site Scripting, Command Injection und ähnliches) schützt. Entsprechende ALGs existieren von verschiedenen Anbietern. Bei komplexeren Webanwendungen wird der Einsatz eines solchen ALG empfohlen.

### Webserver ohne Verwendung eines Reverse Proxy

Bestehen keine besonderen Anforderungen an die Sicherheit des Webservers selbst und kann der Server die ankommenden Anfragen problemlos bewältigen, so bietet es sich an, den Webserver in einer eigenen DMZ des externen Paketfilters anzusiedeln.

Durch entsprechende Paketfilterregeln sollte sichergestellt werden, dass der Webserver vor Angriffen von außen so weit wie möglich geschützt wird. Zusätzlich sollte durch weitere Filterregeln dafür gesorgt werden, dass ein Angreifer selbst nach einer erfolgreichen Kompromittierung des Webservers selbst so wenig weiteren Schaden wie möglich anrichten kann. In der folgenden Tabelle sind Empfehlungen zusammengestellt.

| Quelle | Ziel | Entscheidung | Bemerkungen |
|---|---|---|---|
| **Allgemein** | | | |
| Webserver | externes Netz und internes Netz | Nur Pakete erlauben, die zu einer Verbindung gehören, die vom an- | Der Webserver antwortet nur auf Anfragen. Eigene Verbindungen |

| Quelle | Ziel | Entscheidung | Bemerkungen |
|---|---|---|---|
| | | deren Rechner initiiert wurde | brauchen nicht aufgebaut zu werden |
| **Kommunikation des Webservers mit dem Internet** | | | |
| Externes Netz | Webserver Port 80 | erlauben | Port 80 ist der Standardport |
| Externes Netz | andere Ports des Webservers | verbieten | |
| **Kommunikation des Webservers mit dem internen Netz** | | | |
| Internes Netz | Webserver Port 80 | erlauben | Nutzung des Webservers auch vom internen Netz aus |
| Internes Netz (gegebenenfalls Einschränkung auf Administrationsnetz) | Webserver Port 22 (SSH) | erlauben | Administration und Datenübertragung erfolgen per SSH und SCP |
| Internes Netz | andere Ports des Webservers | verbieten | |
| **Protokollierung** | | | |
| Webserver | Loghost UDP-Port 514 | erlauben | Übertragung der Protokolldaten zum Loghost |

Dabei wird davon ausgegangen, dass die Administration des Webservers aus dem internen Netz über eine SSH-Verbindung abgewickelt wird und dass die WWW-Daten per SCP auf den Webserver übertragen werden. Weiter wird davon ausgegangen, dass auf dem Webserver kein DNS verwendet wird. Eine Namensauflösung ist zum normalen Betrieb nicht notwendig. Für die Erstellung von Zugriffsstatistiken oder sonstigen Auswertungen kann sie gegebenenfalls später erfolgen. Die auf dem Webserver anfallenden Protokolldaten werden über das Netz an einen eigenen Loghost geschickt (siehe auch M 4.225 *Einsatz eines Protokollierungsservers in einem Sicherheitsgateway*).

Dadurch, dass keine Verbindungen zugelassen werden, die vom Webserver aus initiiert werden, kann beispielsweise ein Angreifer, der den Webserver kompromittiert hat, entscheidend behindert werden. Meist benötigt ein Angreifer nämlich zur Fortsetzung seines Angriffs nach dem Einbruch weitere Tools, die er von externen Rechnern nachlädt. Wenn dies wegen entsprechender Paketfilterregeln nicht möglich oder deutlich erschwert ist, so brechen weniger geschickte oder entschlossene Angreifer (beispielsweise *Script Kiddies*) den Angriff eventuell sogar ab.

Falls die Administration des Webservers auf andere Weise abgewickelt oder die WWW-Daten auf andere Weise auf den Webserver übertragen werden,

so sollten für die jeweils genutzten Protokolle entsprechende Filterregeln umgesetzt werden.

**Webserver unter Verwendung eines Reverse Proxy**

Im ersten Szenario trägt der Webserver die gesamte Belastung durch eingehende Anfragen. Soll der Webserver von eingehenden Anfragen entlastet werden, kann ein Reverse Proxy eingesetzt werden, der häufig wiederkehrende Anfragen aus seinem Cache beantwortet und so die Belastung des Webservers selbst reduziert.

Zur Erzielung eines möglichst hohen Durchsatzes ist es notwendig, Webserver und Reverse Proxy in der gleichen DMZ aufzustellen. Der Zugriff aus dem nicht-vertrauenswürdigen Netz sollte nur auf den Reverse Proxy gestattet sein, der direkte Zugriff auf den Webserver aus dem nicht-vertrauenswürdigen Netz sollte durch den äußeren Paketfilter unterbunden werden.

**Webserver und Reverse Proxy in getrennten DMZs**

Reverse Proxies wurden meist nicht primär unter dem Aspekt der Sicherheit entwickelt. Daher sollte gegebenenfalls in Betracht gezogen werden, den Reverse Proxy durch einen weiteren Paketfilter vom Webserver zu trennen. Dies erhöht die Sicherheit für den Webserver, kann aber andererseits zu einer Reduzierung der zur Verfügung stehenden Bandbreite führen.

Auf diese Weise können bei einer etwaigen Kompromittierung des Reverse Proxy unerwünschte Zugriffe vom Reverse Proxy auf den Webserver (z. B. auf Administrationsports) unterbunden werden. Diese Lösung ist in der folgenden Abbildung dargestellt.

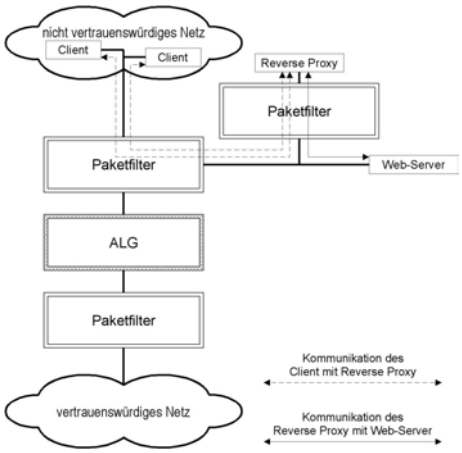



Abbildung: Integration eines Webservers unter Verwendung eines (reverse) Caching-Proxy und eines weiteren Paketfilters zur zusätzlichen Absicherung des Webservers

Diese Lösung ist äquivalent dazu, den Reverse Proxy und den Webserver in unterschiedlichen DMZs des äußeren Paketfilters anzusiedeln. Ob die zusätzliche Filterstufe eingesetzt werden soll muss im konkreten Einsatzszenario abgewogen werden.

Prüffragen:

- Grenzen entsprechende Paketfilterregeln die ein- und ausgehenden Verbindungen des Webserver auf das erforderliche Maß ein?

- Betrifft Webserver unter Verwendung eines Reverse Proxy: Ist der Reverse Proxy in der selben DMZ aufgestellt, wie der Web-Server, wenn ein hoher Datendurchsatz erforderlich ist?
- Betrifft Webserver unter Verwendung eines Reverse Proxy: Wird der direkte Zugriff auf den Web-Server aus dem nicht-vertrauenswürdigem Netz durch einen äußeren Paketfilter unterbunden?
- Betrifft Webserver und Reverse Proxy in getrennten DMZ: Wird der Reverse Proxy durch einen zusätzlichen Paketfilter vom Web-Server getrennt?

# M 5.116 Integration eines E-Mailservers in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bei der Frage der Integration eines E-Mailservers in ein Sicherheitsgateway werden zwei Szenarien betrachtet: Im ersten Fall geht es nur darum, den Dienst E-Mail für ein einzelnes vertrauenswürdiges Netz zur Verfügung zu stellen, im zweiten Fall soll E-Mail für mehrere vertrauenswürdige Netze bereitgestellt werden.

Bei beiden Szenarien werden interne E-Mailserver in den vertrauenswürdigen Netzen betrieben. Ein E-Mailserver innerhalb des vertrauenswürdigen Netzes wird zur Verwaltung der Alias-Datenbank, mit der die Benutzeradressen auf ein einheitliches Format umgesetzt werden können, gegebenenfalls für einen POP- oder IMAP-Daemon oder auch als Gateway zum Übergang in ein anderes Mailsystem (z. B. X.400) eingesetzt. Alle internen Mails werden an diesen Server geschickt und von dort gegebenenfalls über einen externen Mailserver nach außen weitergeleitet.

Die Nutzung eines internen Mailservers ist aus verschiedenen Gründen empfehlenswert:

- E-Mails zwischen Rechnern innerhalb der vertrauenswürdigen Netze verlassen diese Netze nicht, da sie von den jeweiligen internen Mailservern verarbeitet werden.
- Wird der interne Mailserver gleichzeitig als Groupware-Server eingesetzt, so könnte dies zu einer unnötig hohen Belastung des ALG führen.
- Ein Groupware-Server ist auf diese Weise besser vor Angriffen von außen geschützt, da er weiter vom nicht-vertrauenswürdigen Netz entfernt ist.

Es wird allerdings empfohlen, die Mail- bzw. Groupware-Server im internen Netz zusätzlich zumindest durch Paketfilterregeln auch vor unberechtigtem Zugriff aus dem internen Netz geschützt werden. Dies entspricht der Aufstellung des Servers in einer eigenen DMZ des inneren Paketfilters. Bei besonderen Sicherheitsanforderungen im internen Netz sollte dies unbedingt geschehen.

Im Unterschied zum Webserver, bei dem eine Aufstellung "möglichst weit außen" im Sicherheitsgateway empfohlen wird, stellt die hier empfohlene Anordnung für E-Mailserver eine Aufstellung "möglichst weit innen" dar. Der Grund dafür ist, dass auf diese Weise auch bei Ausfall der Internetanbindung immer noch interne E-Mails geschickt werden können.

**Anbindung eines einzelnen vertrauenswürdigen Netzes**

Soll nur für ein einzelnes vertrauenswürdiges Netz ein Mailserver eingesetzt werden, so genügt der interne Mailserver alleine. Der ALG agiert in diesem Fall als "Smart Host" für den internen Mailserver.

Ein Smart Host ist ein Rechner, über den alle E-Mails eines Netzes geleitet werden. Wenn der ALG als Smart Host für den internen Mailserver konfiguriert ist, so braucht der interne Mailserver für abgehende E-Mails nicht zu ermitteln, welches der Mailserver der Empfänger-Domain ist, sondern er leitet die E-Mails einfach an den Smart Host weiter, der die Aufgabe übernimmt, den richtigen Empfänger-Mailserver zu ermitteln. Dies kann ebenfalls wieder ein Smart Host (beispielsweise beim Internet-Dienstleister) sein; wenn der ALG

als Smart Host für das interne Netz eingesetzt wird, so wird dies normalerweise der Fall sein. Smart Hosts werden auch gelegentlich als Mail-Relays bezeichnet.

Für eintreffende E-Mails agiert der ALG entweder als Mail Exchanger, der alle eingehenden E-Mails von den Absender-Mailservern entgegennimmt und an den internen Mailserver weiterleitet, oder als Smart Host für einen externen Mail-Exchanger.

**Anbindung mehrerer vertrauenswürdiger Netze**

Wenn ein Sicherheitsgateway für mehrere vertrauenswürdige Netze gemeinsam eingesetzt wird, etwa als gemeinsamer Internet-Zugang für mehrere Standorte einer Organisation, so ist der oben beschriebene einfache Aufbau oft nicht mehr machbar.

Versand und Empfang von E-Mails sollten bei diesem Szenario zweistufig erfolgen: Nach wie vor sollten in den vertrauenswürdigen Netzen eigene Mailserver eingesetzt werden, über die interne E-Mails direkt verschickt werden können. Zusätzlich ist es sinnvoll, einen zentralen Mailserver in der DMZ einzusetzen, der als zentraler Mail Exchanger für die vertrauenswürdigen Netze agiert und über den externe E-Mails abgewickelt werden. Je nach Produkt kann ein solcher E-Mailserver in der DMZ bereits in das ALG integriert sein.

Die folgende Abbildung zeigt einen solchen Aufbau mit zwei vertrauenswürdigen Netzen mit jeweils einem internen Mailserver, die mit einem nicht-vertrauenswürdigen Netz (beispielsweise dem Internet) verbunden sind. Die beiden internen Mailserver sind zuständig für unterschiedliche (Sub-) Domains, d. h. der Mailserver in der DMZ entscheidet, zu welchem internen Mailserver eintreffende E-Mails weitergeleitet werden.

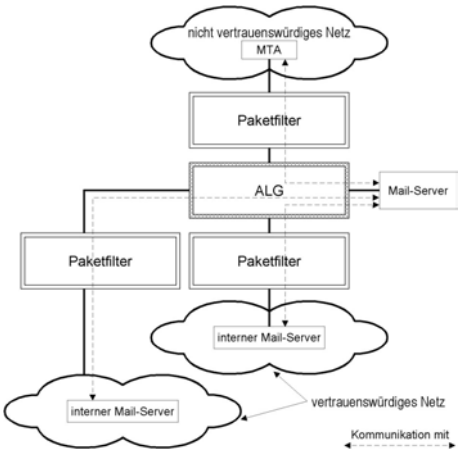



Abbildung: Platzierung der internen MTAs und des Mailservers zur Anbindung von zwei vertrauenswürdigen Netzen (an der Schnittstelle des ALG zur DMZ müssen zwei SMTP-Proxies eingerichtet werden, z. B. unter Zuhilfenahme von virtuellen IP-Adressen).

Eingehende externe E-Mails passieren die MTAs wie folgt:

1. MTA im nicht-vertrauenswürdigen Netz (beim Absender oder beim Internet-Dienstleister)

2. MTA in der DMZ. Dieser trifft die Entscheidung, in welches der beiden vertrauenswürdigen Netze (bzw. an welchen MTA) die E-Mail weitergeleitet werden muss.
3. Mailserver im jeweiligen vertrauenswürdigen Netz

Ausgehende E-Mails passieren die MTAs in der umgekehrten Reihenfolge.

**E-Mailserver bei einfachen Sicherheitsgateways**

Wird nur ein einfaches Sicherheitsgateway bestehend aus einem Paketfilter eingesetzt, so wird empfohlen, den E-Mailserver in einer DMZ des Paketfilters anzusiedeln. Wegen des fehlenden ALGs ist der Schutz des Mailservers vor einer Kompromittierung von außen dabei geringer. Die Aufstellung in der DMZ bietet im Ausgleich einen etwas höheren Schutz des internen Netzes bei einer Kompromittierung des Mailservers, als wenn der Server direkt im internen Netz angesiedelt würde.

Soll auch bei einem Ausfall der externen (Internet-) Anbindung das Verschicken interner E-Mails noch gewährleistet sein, so kann der E-Mail-Server in das interne Netz verlegt werden und zusätzlich ein Mailserver (MTA) in einer DMZ des Paketfilters angesiedelt werden, der als externer Mail-Exchanger agiert. Diese Lösung stellt eine gewissermaßen eine Mischung aus den oben beschriebenen komplexeren Lösungen dar.

Prüffragen:

- Wird der E-Mail-Server mindestens durch einen Paketfilter vor unberechtigten Zugriffen aus dem internen Netz geschützt?
- Wird der Versand von E-Mails an externe Adressen über ein gesondertes Mail Relay geführt?
- Entsprechen die Kommunikationsverbindungen (externe wie auch interne) gegenüber dem E-Mail-Server den Sicherheitsvorgaben der Organisation?

# M 5.117 Integration eines Datenbank-Servers in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Bei der Aufstellung von Datenbank-Servern zum Zugriff aus einem nicht-vertrauenswürdigen Netz sind zwei Haupt-Anwendungsfälle zu unterscheiden:

1. Zugriff auf die Daten der Datenbank über ein Web-Frontend
2. Direkter Zugriff auf die Daten der Datenbank (z. B. mittels SQL)

Beide Anwendungsfälle werden in den folgenden beiden Abschnitten beschrieben:

**Zugriff über Web-Frontend**

Der Webserver und der Datenbank-Server sollten in unterschiedlichen DMZ stehen, damit bei einer Kompromittierung des Webservers ein Schutz des Datenbank-Servers durch einen Proxy des Application Level Gateways (ALG) besteht. Der Schutz durch den Proxy ist allerdings nur gering, beispielsweise wird der TCP/IP-Stack des Datenbank-Servers geschützt. Zudem können Angriffe auf Basis von TCP/IP-Header-Daten verhindert werden. Falls keine besonderen Sicherheitsanforderungen bestehen, so kann der Server auch in der gleichen DMZ wie der Webserver aufgestellt werden.

Der Aufbau und die Kommunikationsbeziehungen sind in diesem Fall wie folgt:

- Der Zugriff vom Internet aus erfolgt ausschließlich per HTTP oder HTTPS auf den Webserver. Die Zugriffe werden durch das ALG entsprechend abgesichert.
- Eine auf dem Webserver laufende Anwendung setzt die Anfrage in entsprechende Datenbankabfragen um, führt diese Abfragen auf der Datenbank aus und bereitet die Ergebnisse entsprechend auf.
- Die Administration des Datenbankrechners, des Datenbanksystems und die Pflege der Daten in der Datenbank erfolgen über entsprechend abgesicherte Verbindungen aus dem internen Netz.

Diese Verbindungen sind ebenfalls in der folgenden Abbildung dargestellt.

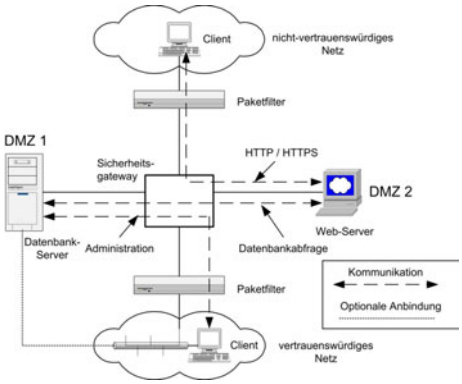



Abbildung 1: Zugriff auf eine Datenbank durch Nutzung eines Web-Frontend

Der Client im nicht-vertrauenswürdigen Netz kann ausschließlich an den Webserver über Webseiten Anfragen stellen, ein direkter Zugriff auf die Datenbank selbst ist nicht möglich.

Bei diesem Aufbau ist es über die Absicherung auf der Transportebene hinaus wichtig, dass die Anwendung auf dem Webserver, welche die Anfragen und Ergebnisse aufbereitet, entsprechend sicher programmiert ist und keine Möglichkeiten für Angriffe auf die Datenbank (beispielsweise SQL Injection) bietet. Falls über das Web-Frontend sogar direkt Datenbankanfragen in der betreffenden Datenbanksprache (beispielsweise SQL) formuliert werden können sollte der Zugriff auf das Web-Frontend nur über HTTPS erfolgen.

**Direkter Zugriff**

Soll auf die Datenbank direkt aus dem nicht-vertrauenswürdigen Netz heraus zugegriffen werden, so sollte der Server in einer eigenen DMZ aufgestellt werden. Da nur wenige Proxies für Datenbankprotokolle existieren, ist der Einsatz eines TCP- oder UDP-Relays oftmals unumgänglich.

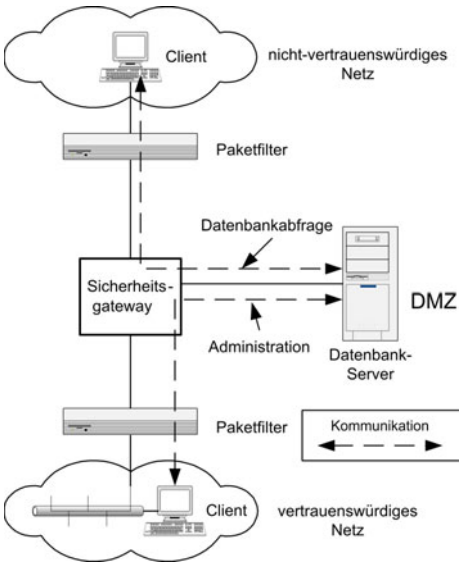



Abbildung 2: Direkter Zugriff auf eine Datenbank

Da sich, wegen der fehlenden Sicherheitsproxies für Datenbankabfrage-Protokolle kaum mittels Sicherheitsproxies kontrollieren lassen, ist die zuerst vorgestellte Lösung mit einem Web-Frontend in der Regel die sichere Variante.

Je nach dem Schutzbedarf der Daten in der Datenbank wird dringend empfohlen, nicht die "Echtdatenbank" für den externen Zugriff freizugeben, sondern nur eine Kopie der Daten auf einer separaten Datenbank, die in entsprechenden Intervallen mit der "Echtdatenbank" synchronisiert wird.

Prüffragen:

- Sofern ein Zugriff auf die Daten der Datenbank aus einem nicht-vertrauenswürdigen Netz über ein Web-Frontend erfolgt, befinden sich Webserver und Datenbank-Server in unterschiedlichen DMZ?
- Erfolgt die Administration der im Sicherheitsgateway integrierten Server über einen vertrauenswürdigen Pfad?
- Betrifft Datenbankzugriff über Web-Frontend: Werden direkte Datenbankzugriffe aus dem externen Netzwerk unterbunden?
- Sofern ein direkter Zugriff auf die Daten der Datenbank aus einem nicht vertrauenswürdigen Netz heraus erfolgen muss, befindet sich der Datenbank-Server in einer eigenen DMZ zusätzlich geschützt durch einen Proxy oder nur als Kopie der führenden Datenbank?
- Betrifft den direkten Datenbankzugriff aus einem unsicheren Netzwerk: Befindet sich der Datenbank-Server in einer DMZ?

# M 5.118 Integration eines DNS-Servers in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Das Domain Name System (DNS) dient zur Umsetzung von Rechnernamen in IP-Adressen und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. Diese Informationen sind teilweise für die korrekte Funktion der Internetanbindung erforderlich, beispielsweise Informationen über DNS-Server oder Mail-Exchanger für eine Domain. Andererseits können Domain-Informationen auch von potenziellen Angreifern bei der Vorbereitung von Angriffen ausgenutzt werden. Hat ein Rechner beispielsweise einen Namen wie "mssql01", so kann ein Angreifer daraus schließen, dass es sich vermutlich um einen Rechner mit Microsoft-Betriebssystem handelt, auf dem ein Microsoft SQL-Server läuft.

Bei DNS sollte daher eine Trennung zwischen der Namensauflösung für interne Zwecke und der Namensauflösung "nach außen" eingeführt werden. Interne Domain-Informationen sollten vor dem nicht-vertrauenswürdigen Netz verborgen werden. Rechner im internen Netz sollten selbst dann keinen von außen auflösbaren DNS-Namen erhalten, wenn sie eine "öffentliche" IP-Adresse besitzen. Werden im internen Netz private IP-Adressen aus den Adressbereichen des RFC 1918 verwendet, so müssen diese ohnehin durch einen internen Nameserver aufgelöst werden.

Gerade DNS-Server-Produkte waren in der Vergangenheit wegen Sicherheitslücken immer wieder eine Quelle von Problemen. Wegen der besonderen Bedeutung der Domain-Informationen und der erhöhten Anfälligkeit der DNS-Software als Grundlage für Angriffe ist ein besonderer Aufbau notwendig, um Domain-Informationen sicher bereitstellen und nutzen zu können.

**DNS-Server in einem dreistufigen Sicherheitsgateway**

Für eine sichere Integration von DNS in ein dreistufiges Sicherheitsgateway bietet sich der in der folgenden Abbildung gezeigte Aufbau an, bei dem keine direkte Verbindung zwischen einem Client im vertrauenswürdigen Netz und einem DNS-Server im nicht-vertrauenswürdigen Netz (und umgekehrt) stattfindet. Es werden zwei getrennte DNS-Server eingesetzt.

Der Advertising DNS-Server, der die extern verfügbaren Informationen enthält, wird in einer DMZ des äußeren Paketfilters angesiedelt. Er ist als "Primary Nameserver" für die Domain des vertrauenswürdigen Netzes eingerichtet und enthält nur die unbedingt notwendigen Informationen, beispielsweise:

- Name und IP-Adresse des externen Mailservers (MX-Eintrag)
- Namen und Adressen von Informationsservern, die Informationen für die Öffentlichkeit anbieten. Dabei muss zwischen den Servern, die vor dem Application Level Gateway (ALG) angesiedelt sind und denen, die hinter dem ALG angesiedelt sind, unterschieden werden. Bei Ersteren muss die Adresse des Servers selbst eingetragen sein, bei Letzteren die Adresse des ALG.

Der Resolving DNS-Server wird in einer DMZ des inneren Paketfilters aufgestellt. Er enthält die Informationen über die Rechner des internen Netzes. Für Rechner des internen Netzes wird der Resolving DNS-Server als DNS-Server eingetragen: Alle Clients des vertrauenswürdigen Netzes nutzen ausschließlich den Resolving DNS-Server, bei Unix-Rechnern beispielsweise mit-

tels Einträgen in der Datei */etc/resolv.conf.* Benötigt ein Client im vertrauenswürdigen Netz eine Domain-Information aus dem nicht-vertrauenswürdigen Netz, so stellt er die Anfrage an den Resolving DNS-Server. Als "Forwarder" nutzt dieser einen öffentlichen DNS-Server (oder gegebenenfalls. einen extra eingerichteten Forwarder) für Anfragen, die externe Namen betreffen. Der direkte Zugriff auf den Resolving DNS-Server aus dem nicht-vertrauenswürdigen Netz sollte durch Paketfilterregeln unterbunden werden, sodass die Domain-Informationen des vertrauenswürdigen Netzes nur im vertrauenswürdigen Netz sichtbar sind.

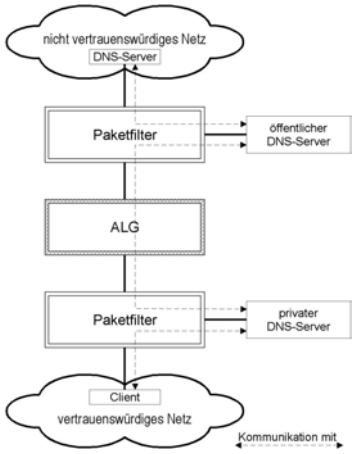



Abbildung 1: Integration der DNS-Server zur sicheren Kommunikation von vertrauenswürdigem und nicht-vertrauenswürdigem Netz

Der eingesetzte Paketfilter muss so konfiguriert werden, dass zwischen den DNS-Servern nur der DNS-Dienst gestattet ist, d. h. Port 53 als (je nach betrachteter Richtung) Quell- bzw. Zielport. Vom Advertising DNS-Server sollten keinerlei Verbindungen ins interne Netz zugelassen werden. Die Administration des Servers sollte über entsprechend abgesicherte Verbindungen (SSH) erfolgen.

In der folgenden Tabelle wird eine mögliche Konfiguration für Zugriffsregelungen beschrieben, die über entsprechende Paketfilterregeln umgesetzt werden kann. Dabei wird davon ausgegangen, dass die Administration der Server über eine SSH-Verbindung aus dem internen Netz erfolgt und dass für DNS als Trägerprotokoll UDP verwendet wird. Protokolldaten werden über Syslog auf einen Logserver übertragen.

| **Quelle** | **Ziel** | **Entscheidung** | **Bemerkungen** |
|---|---|---|---|
| **Kommunikation des öffentlichen DNS-Servers mit dem Internet** | | | |
| Externes Netz | Advertising DNS-Server UDP Port 53 | erlauben | DNS-Anfragen und Antworten aus dem öffentlichen Netz |
| Externes Netz | andere Ports des Advertising DNS-Servers | verbieten | |
| Advertising DNS-Server | DNS-Server im Internet, alle Ports TCP und UDP | erlauben | Auflösung von externen Namen |

| Quelle | Ziel | Entscheidung | Bemerkungen |
|---|---|---|---|
| | | | durch den DNS-Server |
| **Kommunikation des externen DNS-Servers mit dem internen Netz** | | | |
| Advertising DNS-Server | Alle Verbindungen ins interne Netz | verbieten | |
| Internes Netz (ggfs. Einschränkung auf Administrationsnetz) | Advertising DNS-Server Port 22 (SSH) | erlauben | Administration und Datenübertragung erfolgen per SSH und SCP |
| Internes Netz | Alle anderen Zugriffe auf den Advertising DNS-Server | verbieten | DNS-Anfragen aus dem internen Netz erfolgen über den internen Server |
| **Kommunikation der beiden DNS-Server untereinander** | | | |
| Resolving DNS-Server | Advertising DNS-Server UDP Port 53 | erlauben | Der Resolving DNS-Server leitet Anfragen an den Advertising Server weiter (ggf. kann ein eigener Forwarder eingerichtet werden) |
| Advertising DNS-Server | Resolving DNS-Server alle Ports UDP | erlauben | |
| **Kommunikation des internen DNS-Servers mit dem internen Netz** | | | |
| Internes Netz | Resolving DNS-Server UDP Port 53 | erlauben | DNS-Anfragen aus dem internen Netz erfolgen über den Resolving DNS-Server |
| Resolving DNS-Server, UDP Port 53 | Internes Netz | erlauben | DNS-Antworten in das interne Netz |
| Resolving DNS-Server, sonstige Quellports | Internes Netz | verbieten | |

| Quelle | Ziel | Entscheidung | Bemerkungen |
|---|---|---|---|
| Internes Netz (ggf.. Einschränkung auf Administrationsnetz) | Resolving DNS-Server Port 22 (SSH) | erlauben | Administration und Datenübertragung erfolgen per SSH und SCP |
| **Protokollierung** | | | |
| Resolving und Advertising DNS-Server | Loghost UDP-Port 514 | erlauben | Übertragung der Protokolldaten zum Loghost |

Tabelle: Konfiguration für Zugriffsregeln

**DNS-Server in einem einfachen Sicherheitsgateway**

Wird nur ein einfaches Sicherheitsgateway (Paketfilter) eingesetzt, so wird empfohlen, trotzdem zwei getrennte DNS-Server (Advertising und Resolving DNS-Server) einzusetzen. Wenn die beiden DNS-Server in zwei getrennten DMZ des Paketfilters angesiedelt werden, können dieselben Regeln eingesetzt werden, wie oben beschrieben.

Ist der Aufwand für die Einrichtung zweier getrennter DMZ zu groß oder können aus technischen Gründen keine zwei getrennten DMZ eingerichtet werden, so kann gegebenenfalls auf einfachere Konstruktionen zurückgegriffen werden. Diese bieten allerdings nur einen geringeren Schutz und es muss daher im Einzelfall abgewogen werden, ob das Sicherheitsniveau noch akzeptabel ist.

Der Advertising DNS-Server sollte in jedem Fall in einer DMZ des Paketfilters angesiedelt werden. Der Resolving DNS-Server kann gegebenenfalls im internen Netz stehen.

Wenn nur ein DNS-Server zur Verfügung steht, der sowohl die interne als auch die externe Namensauflösung übernehmen muss, so sollte dieser in einer DMZ des Paketfilters aufgestellt werden. Wenn möglich sollte in diesem Fall die DNS-Server-Software so konfiguriert werden, dass zwischen Anfragen aus dem internen und solchen aus dem externen Netz unterschieden wird und gegebenenfalls unterschiedliche Daten geliefert werden. Diese Lösung bietet jedoch nur für kleine Netze ohne besondere Anforderungen an die Sicherheit einen ausreichenden Schutz.

**Domain-Registrierung bei externem Dienstleister**

Bei dieser Alternative werden wichtige Domain-Informationen bei einem externen Dienstleister gespeichert und nicht durch einen eigenen DNS-Server bereitgestellt. Der Unterschied zu den eben beschriebenen Szenarien besteht im Wesentlichen im Wegfall der Advertising DNS-Server. DNS-Anfragen aus dem externen Netz nach Domain-Informationen aus dem internen Netz werden nicht an den organisationsinternen Advertising DNS-Server, sondern an den DNS-Server des externen Dienstleisters gesendet und von diesem beantwortet. Der Resolving DNS-Server greift bei Anfragen nach externen DNS-Namen oder IP-Adressen direkt über das Sicherheitsgateway hinweg auf einen DNS-Server im externen Netz, meistens betrieben durch den Internet-Provider, zu.

Auch bei dieser Integrationsvariante sollten nur die unbedingt notwendigen Domain-Informationen extern angeboten werden, beispielsweise Name und IP-Adresse des Mailservers und des ALG. Bei besonders unbedenklichen or-

ganisationsinternen Nutzern kann der Resolving DNS-Server auch im internen Netz, anstatt in einer DMZ des inneren Paketfilters betrieben werden, was die Administration des Paketfilters, wenn auch nur in geringem Maße), erleichtert.

Vorteile dieser Variante sind die geringen Investitionskosten und die geringe Komplexität bei der Integration in ein Sicherheitsgateway. Zudem verfügt ein Dienstleister möglicherweise über redundante Systeme, was bei einer organisationsinternen Lösung oftmals nicht der Fall ist.

Prüffragen:

- Wird eine Trennung der Namensauflösung für interne Adressen und der Namensauflösung für externe Adressen umgesetzt?
- Sind die auf dem öffentlichen DNS-Server eingetragenen Informationen so weit möglich eingegrenzt?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Ist ein öffentlicher DNS-Server als Primary Nameserver für die Domain des vertrauenswürdigen Netzes eingerichtet?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Ist der private DNS-Server in einer DMZ des inneren Paketfilters aufgestellt?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Verwenden alle Clients des vertrauenswürdigen Netzes ausschließlich den privaten DNS-Server?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Nutzt der private DNS-Server den öffentlichen DNS-Server als Forwarder für Anfragen, die externe Namen betreffen?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Wird der direkte Zugriff auf den privaten DNS-Server aus dem nicht-vertrauenswürdigen Netz durch Paketfilterregeln unterbunden?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Sind die Paketfilter so konfiguriert, dass zwischen den DNS-Servern nur der DNS-Dienst gestattet ist?
- Betrifft DNS-Server in einem dreistufigen Sicherheitsgateway: Ist sichergestellt, dass vom öffentlichen DNS-Server keinerlei Verbindungen ins interne Netz zugelassen werden?
- Betrifft DNS-Server in einem einfachen Sicherheitsgateway: Ist der öffentliche DNS-Server in einer getrennten DMZ des Paketfilters angesiedelt?

# M 5.119 Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter

Zur Bereitstellung einer komplexen Web-Applikation ALGALG(beispielsweise einer E-Government-Anwendung oder eines Online-Shop) sind aufgrund des erhöhten Schutzbedarfs weitergehende Schutzmaßnahmen notwendig. Im Folgenden wird zu diesem Spezialfall ein Standardaufbau zur Bereitstellung einer Web-Applikation, bestehend aus Webserver, Applikationsserver und Datenbankserver, vorgeschlagen.

**Architektur mit zwei ALGs und Paketfiltern**

Das Sicherheitsgateway ist so angelegt, dass alle Server durch ein ALG voneinander getrennt sind, um unberechtigte Übergriffe von einem Server auf einen anderen zu unterbinden und eine Kontrolle über die eingesetzten Protokolle zu erhalten. Der Webserver ist sowohl durch einen Paketfilter als auch durch ein ALG abgesichert, um einen höchstmöglichen Schutz vor Angreifern aus dem nicht-vertrauenswürdigem Netz zu bieten.

Der Aufbau wurde so gewählt, dass jeder Server im Anwendungszusammenhang maximal zwei Kommunikationsverbindungen eingehen kann, die jeweils durch entsprechende ALGs abgesichert sind. Die folgende Tabelle stellt die Kommunikationsverbindungen zusammen:

| **Server** | **Kommunikation mit** | **Protokoll** | **Bemerkung** |
|---|---|---|---|
| Webserver | Client aus dem externen Netz | HTTPS | Gegebenenfalls kann die verschlüsselte Verbindung bereits am ALG terminiert werden. Siehe auch M 5.115 *Integration eines Webservers in ein Sicherheitsgateway* |
| Webserver | Applikations-Server | Anwendungs-spezifische Protokolle, beispielsweise SOAP, RPC, Corba o.ä. | Für die Protokolle existieren ebenfalls Sicherheits-proxies |
| Applikations-Server | Datenbank-Server | Datenbank Protokoll | Siehe auch M 5.117 *Integration eines Datenbank-Servers in* |

| Server | Kommunikation mit | Protokoll | Bemerkung |
|---|---|---|---|
| | | | *ein Sicherheitsgateway* |

Tabelle: Kommunikationsverbindungen

Zusätzlich sind jeweils eventuell noch Zugriffe zur Administration aus dem internen Netz notwendig. Diese müssen auf entsprechende Administrationsrechner beschränkt werden und dürfen nur über entsprechend abgesicherte Protokolle (beispielsweise SSH) abgewickelt werden. Es sollte geprüft werden, ob auf eine physikalische Verbindung zu dem vertrauenswürdigen Netz ganz verzichtet werden kann, um einem Angriff durch Innentäter vorzubauen.

Die folgende Abbildung zeigt noch einmal die oben beschriebene Architektur. Die jeweils zugelassenen Kommunikationsverbindungen sind eingetragen.

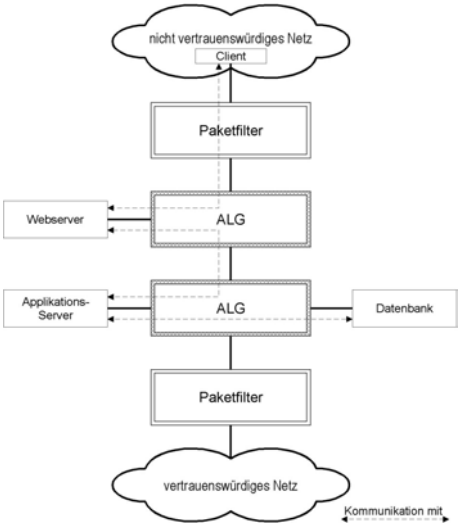



Abbildung 1: Aufbau einer typischen Web-Applikation bestehend aus Webserver, Applikationsserver und Datenbank.

**Vereinfachte Architektur ohne ALGs**

Falls die Anwendung keine besonderen Sicherheitsanforderungen stellt können eventuell die ALGs wegfallen und der Webserver kann in einer DMZ des äußeren Paketfilters aufgestellt werden, der Applikations- und der Datenbankserver in separaten DMZs des inneren Paketfilters. Die Kommunikationsbeziehungen werden in diesem Fall nur durch entsprechende Paketfilterregeln eingeschränkt.

In diesem Fall besteht allerdings nicht mehr die Möglichkeit zur Kontrolle des Inhalts der Kommunikation. Wird auf ALG zwischen dem Client und dem Webserver verzichtet (Reverse-HTTP-Proxy) können beispielsweise keine HTTP-Anfragen aus dem nicht-vertrauenswürdigen Netz mehr auf Konformität mit der HTTP-Spezifikation überprüft und auf (im jeweiligen Zusammenhang) ungewöhnliche Inhalte getestet werden.

Es wird dringend empfohlen, zumindest für den Zugriff der Clients auf den Webserver ein entsprechendes ALG (Reverse-HTTP-Proxy) einzusetzen.

Die folgende Abbildung zeigt die vereinfachte Architektur mit zwei Paketfiltern. Die Kommunikationsbeziehungen sind wie in der obigen Tabelle beschrieben, nur dass keine protokollspezifischen Sicherheitsproxies eingesetzt werden.

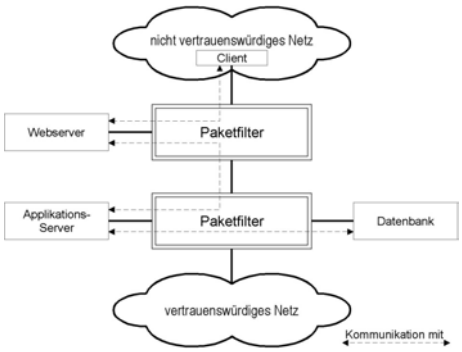



Abbildung 2: Aufbau einer typischen Web-Applikation bestehend aus Webserver, Applikationsserver und Datenbank ohne Verwendung von ALGs

Ob für die jeweils eingesetzte Webapplikation der vereinfachte Aufbau ausreichend ist muss im Einzelfall geklärt werden. Die Entscheidung muss anhand des Schutzbedarfs der verarbeiteten Daten getroffen werden, keinesfalls dürfen ausschließlich Kostenargumente den Ausschlag geben. Die Entscheidung und die Gründe dafür müssen dokumentiert werden und es muss regelmäßig geprüft werden, ob sich die Voraussetzungen nicht geändert haben. Insbesondere bei Änderungen und Erweiterungen der Webanwendung muss sichergestellt sein, dass die Architektur noch den Sicherheitsanforderungen entspricht.

Die folgenden Punkte können bei den Erwägungen als Hinweise dienen:

- Für Webanwendungen, auf die nur aus einem "relativ vertrauenswürdigen Netz" zugegriffen wird, bietet auch der vereinfachte Aufbau meist ein ausreichendes Sicherheitsniveau.
- Handelt es sich bei der Webanwendung um eine Anwendung, auf die über das Internet zugegriffen werden kann oder haben die verarbeiteten Daten einen hohen Schutzbedarf, so sollte mindestens ein Reverse-HTTP-Proxy zur Absicherung des Webservers vor Angriffen aus dem Internet eingesetzt werden.
- Werden auf dem Datenbankserver, der zu der Webapplikation gehört, noch weitere Datenbanken betrieben, so muss auch der Schutzbedarf dieser Daten in die Überlegungen einbezogen werden. In diesem Fall kommt der sicheren und sorgfältigen Konfiguration des Datenbankservers eine besondere Bedeutung zu. In diesem Fall wird der Einsatz eines Sicherheitsproxies für die Datenbankzugriffe dringend empfohlen.

Prüffragen:

- Betrifft Architektur mit zwei ALGs und Paketfiltern: Sind alle Server durch ein ALG voneinander getrennt, um unberechtigte Übergriffe von einem Server auf einen anderen zu unterbinden?
- Betrifft Architektur mit zwei ALGs und Paketfiltern: Ist der Web-Server durch einen Paketfilter und durch ein ALGabgesichert, um einen zusätzlichen Schutz gegenüber externen Angreifern zu bieten?
- Betrifft vereinfachte Architektur ohne ALGs: Sind der Webserver,wie auch der Applikations- und der Datenbank-Server in einer separaten DMZ des Paketfilters untergebracht?

- Betrifft vereinfachte Architektur ohne ALGs: Wird für externe Zugriffe auf den Webserver ein Reverse-HTTP-Proxy eingesetzt?
- Sind die Entscheidungen und Gründe zur gewählten Architektur der Integration der Web-Anwendung dokumentiert?
- Wird sichergestellt, dass Änderungen der Web-Anwendung den Sicherheitsanforderungen der Organisation entsprechen?
- Betrifft Datenbankserver der Web-Anwendung auf denen weitere Datenbanken betrieben werden: Wird für alle Datenbank-Instanzen ein Sicherheitsproxy für die Datenbankzugriffe eingesetzt?

# M 5.120 Behandlung von ICMP am Sicherheitsgateway

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Das Internet Control Message Protocol (ICMP, spezifiziert in RFC 792) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen für IP zu transportieren. Es wird intern von IP, TCP oder UDP angestoßen und verarbeitet. ICMP kennt eine Anzahl verschiedener so genannter Nachrichtentypen für verschiedene Zwecke. Neben vielen nützlichen Funktionen gibt es in ICMP einige Nachrichtentypen, mit denen Angreifer sich wichtige Informationen über ein Netz verschaffen können, oder die direkt für Angriffe benutzt werden können (siehe G 5.50 *Missbrauch des ICMP-Protokolls-Missbrauch des ICMP-Protokolls*).

Leider ist jedoch der radikale Ansatz, ICMP grundsätzlich am Sicherheitsgateway zu blockieren, ebenfalls keine befriedigende Lösung, da bestimmte Funktionen dann nicht mehr verfügbar sind. Auf Befehle wie *ping* oder *traceroute* kann zwar in der Regel auf normalen Arbeitsplatzrechnern und Servern verzichtet werden, eine globale Blockierung von ICMP am Sicherheitsgateway kann aber zu Beeinträchtigungen führen, die schwer zu diagnostizieren sind.

Daher sollte überlegt werden, sowohl am Sicherheitsgateway als auch gegebenenfalls an einem lokalen Paketfilter auf den einzelnen IT-Systemen eine selektive ICMP-Filterung vorzunehmen, sofern dieser die entsprechenden Möglichkeiten zur Verfügung stellt. Dabei sollten der Einsatzzweck des Rechners (Server oder Arbeitsplatzrechner), der Schutzbedarf und bei einzelnen Rechnern die am Sicherheitsgateway getroffenen Maßnahmen berücksichtigt werden. Beispielsweise kann für das interne Netz eine größere Zahl von Nachrichtentypen zugelassen werden, als für das externe Netz.

Die ICMP-Nachricht *Echo Request* (Nachrichtentyp 8) wird beispielsweise von Programmen wie dem Kommandozeilentool *ping* ausgeschickt und dient dazu herauszufinden, ob ein Rechner prinzipiell erreichbar ist. Der Rechner antwortet darauf mit einem Echo Reply (Nachrichtentyp 0). Werden ICMP Echo Requests aus dem externen Netz ins interne Netz durchgelassen, so kann dies von einem Angreifer ausgenutzt werden, um das interne Netz zu "kartographieren".

Die ICMP-Nachricht *Destination Unreachable* (Nachrichtentyp 3) wird beispielsweise dann erzeugt, wenn ein Rechner oder ein Netz nicht erreichbar ist, und kann dazu missbraucht werden, alle Verbindungen zwischen den beteiligten Rechnern zu unterbrechen. Trotzdem ist gerade die Nachricht Destination Unreachable für das Funktionieren der Protokolle der höheren Schichten wichtig. Beispielsweise ist der Subtyp *"Fragmentation Needed but the Don't Fragment Bit was Set"* (Nachrichtentyp 3, Code 4) wichtig für die Funktion der Ermittlung der maximal möglichen Paketgröße für eine bestimmte Verbindung ("Path MTU Discovery").

Die ICMP-Nachricht *Redirect* (Nachrichtentyp 5) wird ausgesandt, wenn ein Gateway erkennt, dass das Paket direkt an ein anderes Gateway geschickt werden kann, also bisher ein Umweg benutzt wurde. Der kürzere Weg wird dann in die Routingtabelle des Absenders eingetragen. Dieses kann von Angreifern missbraucht werden, um Routen über eigene Angriffsrechner zu kon-

figurieren. Daher sollten ICMP-Redirect Nachrichten am Sicherheitsgateway blockiert werden.

Bei den anderen Meldungen ist abzuwägen, ob Informationen, die eventuell nach außen geliefert werden, für einen Angriff missbraucht werden können.

**Rechner im internen Netz**

Die nachfolgende Tabelle zeigt eine mögliche Einstellung für ein Sicherheitsgateway, welches das interne Netz einer Organisation vom Internet trennt. Diese Einstellungen stellen für die meisten Zwecke einen akzeptablen Kompromiss zwischen Sicherheit und Funktionalität dar:

| ICMP Nachricht | Ankommend | Abgehend | Bemerkung |
|---|---|---|---|
| Echo Request (Typ 8) | blockieren | zulassen | |
| Echo Reply (Typ 0) | zulassen | blockieren | Erlaubt zusammen mit der darüber stehenden Einstellung das "pingen" von innen nach außen, aber nicht umgekehrt |
| Destination unreachable (Typ 3) | zulassen | zulassen | Eventuell feinere Unterscheidung anhand des Nachrichtencodes treffen |
| Time exceeded (Typ 11) | zulassen | zulassen | Eventuell ausgehende Nachrichten blockieren |
| Redirect (Typ 5) | blockieren | blockieren | |
| Andere Typen | blockieren | blockieren | |

Tabelle 1: ICMP für Rechner im internen Netz

Da "pingen" keine besondere Rolle für das Funktionieren eines Netzes spielt, sollte auch bei normalem Schutzbedarf überlegt werden, die Typen Echo Request und Echo Response komplett zu sperren.

Bei höheren Sicherheitsanforderungen sollte die Anzahl der erlaubten abgehenden ICMP-Typen weiter eingeschränkt werden.

**"Öffentliche" Server in der DMZ**

Für Server, die in einer Demilitarisierten Zone des Sicherheitsgateway aufgestellt sind und die öffentlich zugängliche Dienste anbieten kann es sinnvoll sein, zusätzliche Nachrichtentypen zu erlauben. Der Schutz vor dem "Ausspähen" einer internen Netzstruktur spielt in diesem Fall keine Rolle, da diese Rechner ohnehin von außen erreichbar sein müssen. Die folgende Tabelle kann dafür als Anhaltspunkt dienen:

| ICMP Nachricht | Ankommend | Abgehend | Bemerkung |
|---|---|---|---|
| Echo Request und Echo Reply (Typen 0 und 8) | zulassen | zulassen | |
| Destination unreachable (Typ 3) | zulassen | zulassen | Eventuell feinere Unterscheidung anhand des Nachrichtencodes treffen |
| Time exceeded (Typ 11) | zulassen | zulassen | |
| Source Quench (Typ 4) | zulassen | blockieren | |
| Redirect (Typ 5) | blockieren | blockieren | |
| Andere Typen | blockieren | blockieren | |

Tabelle 2: ICMP für "öffentliche" Server in der DMZ

**Komponenten des Sicherheitsgateways**

Komponenten des Sicherheitsgateways selbst sollten für den normalen Netzverkehr so transparent wie möglich sein. Daher ist es bei diesen Systemen empfehlenswert, überhaupt keine ICMP-Nachrichten zu generieren, weder selbständig noch als Antwort auf ankommende ICMP-Nachrichten. Es ist sinnvoll, diese Einstellung direkt am jeweiligen System zu treffen, sofern entsprechende Konfigurationsmöglichkeiten vorhanden sind. Anderenfalls sollten entsprechende Pakete am äußeren Paketfilter blockiert werden.

**ICMP bei besonderen Sicherheitsanforderungen**

Für IT-Systeme und Netze mit besonderen Sicherheitsanforderungen wird empfohlen, sämtliche ICMP-Nachrichten zu blockieren, eventuell mit Ausnahme von Nachrichten des Nachrichtentyps 3, Nachrichtencode 4 ("Fragmentation Needed but the Don't Fragment Bit was Set"). Diese Ausnahme vermeidet Probleme in Verbindung mit der sogenannten "Path MTU Discovery" (Ermittlung der maximal möglichen Paketgröße für eine bestimmte Verbindung).

**ICMP im internen Netz**

Auch im internen Netz kann es sinnvoll sein, ICMP ganz oder teilweise zu blockieren. An internen Sicherheitsgateways, die ein Netz mit besonderen Sicherheitsanforderungen von einem Netz mit normalem Schutzbedarf trennen wird empfohlen, im Bezug auf ICMP die selben Einstellungen zu wählen, wie sie oben für die Trennung des internen Netzes vom Internet empfohlen werden.

**ICMP und Stateful Inspection**

Manche Hersteller von Paketfiltern oder Sicherheitsgateways bieten bei Ihren Produkten die Möglichkeit, auch für ICMP eine Art Stateful Inspection vorzunehmen. Auf Grund seines Einsatzzweckes eignet sich ICMP aber besonders schlecht für Stateful Inspection. Wegen der Fehleranfälligkeit einer entsprechenden Konfiguration und dem vergleichsweise geringen Nutzen wird davon abgeraten, entsprechende Optionen zu aktivieren.

Prüffragen:

- Ist der Einsatz von zugelassenen ICMP Nachrichtentypen am Sicherheitsgateway restriktiv eingeschränkt?
- Werden ICMP-Redirect Nachrichten am Sicherheitsgateway blockiert?
- Wird das aktive Versenden von ICMP-Nachrichten durch die Komponenten des Sicherheitsgateways unterbunden?
- Ist dokumentiert, welche ICMP-Nachrichten in welche Richtungen zugelassen sind ?

# M 5.121 Sichere Kommunikation von unterwegs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Über mobile Endgeräte wie Laptops, Smartphones, Tablets oder PDAs soll auch häufig unterwegs auf Daten aus dem Internet oder dem internen Netz einer Institution zugegriffen werden. Dabei werden üblicherweise öffentliche Kommunikationsnetze benutzt. Da weder die Institution noch die mobilen Mitarbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen zum Schutz der Informationen erforderlich.

Generell muss die Datenübertragung zwischen einem mobilen Endgerät und dem LAN einer Institution folgende Sicherheitsanforderungen erfüllen:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten*: Die Datenübertragung muss ausreichend sicher verschlüsselt werden. Auch wer die Kommunikation abhört, soll nicht auf den Inhalt der Daten rückschließen können. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten*: Die eingesetzten Übertragungsprotokolle müssen die Möglichkeit bieten, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.
- *Sicherstellung der Authentizität der Daten*: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass eine Maskerade oder ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck muss eine gegenseitige Authentisierung der Kommunikationspartner (beispielsweise über digitale Zertifikate) erfolgen.
- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung*: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.

Wenn mit mobilen Endgeräten über öffentliche Netze auf interne Ressourcen zugegriffen werden soll, so wird der Einsatz eines Virtual Private Network (VPN) dringend empfohlen. Entsprechende Produkte sind von diversen Herstellern und für praktisch alle gebräuchlichen Plattformen verfügbar. Auf Daten oder Systeme mit hohem Schutzbedarf darf nicht ohne entsprechende Sicherungsmaßnahmen zugegriffen werden. Betreibt die Institution in ihrem Netz einen Filter für Schadsoftware, so sollte die Netzverbindung des mobilen Endgerätes durch diesen Filter geleitet werden, um so das Endgerät besser vor Schadsoftware zu schützen.

Für den Zugriff auf Internet-Anwendungen, bei denen schützenswerte Daten wie personenbezogene Daten, interne Informationen oder Kontendaten ausgetauscht werden, muss zumindest SSL zur Verschlüsselung genutzt werden (siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS*).

**Kopplung mit anderen IT-Systemen**

Beim Einsatz mobiler Endgeräte wie Laptops, Smartphones, Tablets oder PDAs sollen häufig auch Daten mit anderen IT-Systemen ausgetauscht werden, etwa mit Geschäftspartnern. Auch für den Zugriff auf das Internet ist häufig die Kopplung mit anderen IT-Systemen erforderlich. Dies kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Infrarot-, Bluetooth-, WLAN- oder GSM-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden, zum anderen müssen die eigenen IT-Systeme sicher konfiguriert sein. Dazu gehören bei mobilen Clients Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.

Soll ein mobiles Endgerät an fremde Netze oder an das Internet angeschlossen werden, so sollte das System grundsätzlich über eine Personal Firewall abgesichert werden (siehe M 5.91 *Einsatz von Personal Firewalls für Clients* ).

**Nutzung fremder IT-Systeme**

Beim Einsatz mobiler Endgeräte wie Laptops, Smartphones, Tablets oder PDAs sollen häufig auch Daten mit anderen IT-Systemen ausgetauscht werden, etwa mit Geschäftspartnern. Auch für den Zugriff auf das Internet ist häufig die Kopplung mit anderen IT-Systemen erforderlich. Dies kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Infrarot-, Bluetooth-, WLAN- oder GSM-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden, zum anderen müssen die eigenen IT-Systeme sicher konfiguriert sein. Dazu gehören bei mobilen Clients Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.

In allen Organisationen sollte klar geregelt sein, auf welche Daten von unterwegs zugegriffen werden darf und auf welche nicht. Vor allem muss allen IT-Benutzern bekannt sein, unter welchen Randbedingungen sie Daten über externe Netze oder direkt mit fremden IT-Systemen austauschen dürfen (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen* und M 2.218 *Regelung der Mitnahme von Datenträgern und IT-Komponenten*).

Prüffragen:

- Werden bei der Datenübertragung die Daten ausreichend geschützt?
- Wird beim Datenaustausch das eigene IT-System ausreichend geschützt?

# M 5.122 Sicherer Anschluss von Laptops an lokale Netze

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Laptops haben als mobile IT-Geräte ein höheres Gefährdungspotential als stationäre IT-Systeme, die ausschließlich in einer kontrollierten Umgebung betrieben werden. Daher ist es wichtig, festzulegen, welche Regelungen beim Anschluss von Laptops an LANs zu beachten sind, um zu vermeiden, dass dadurch der sichere Betrieb des LANs und anderer damit gekoppelter IT-Systeme beeinträchtigt wird, z. B. durch Schadsoftware.

Wenn ein Laptop nach einem externen Einsatz wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden soll, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist.

Sofern Laptops bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Es ist sinnvoll, vor einem Zugriff auf das Produktivnetz zu überprüfen, ob Personal Firewall, andere Sicherheitsprogramme und Sicherheitspatches auf dem Laptop auf dem aktuellsten Stand sind. Empfehlenswert ist es, über entsprechende Tools diese Prüfungen automatisiert durchzuführen, so dass bei Sicherheitsmängeln der Zugriff auf das interne Netz abgewiesen werden kann.

Die auf dem Laptop installierten Internet-Anwendungsprogramme, vor allem Browser und E-Mail-Client, sollten mit sicheren Einstellungen betrieben werden (siehe hierzu M 5.45 *Sichere Nutzung von Browsern* und M 5.57 *Sichere Konfiguration der Groupware-/Mail-Clients*). Die Änderung der voreingestellten Optionen durch den Benutzer sollte administrativ unterbunden werden. Zusätzlich könnten Tools eingesetzt werden, die die Funktionalität des Browsers einschränken, so dass dieser in einer Sandbox-ähnlichen Umgebung ausgeführt wird.

### Zertifikate/MAC-Adressen

Es muss sichergestellt sein, dass nicht jeder beliebige Laptop sich an ein LAN anmelden kann. Bevor einem Laptop ein Zugriff auf ein LAN gestattet wird, muss dieser sich erfolgreich gegenüber einem Authentikationsserver authentisiert haben.

Um zu überprüfen, welche Geräte grundsätzlich zum Netzzugriff berechtigt sind, können beispielsweise Geräte-Zertifikate oder MAC-Adressen benutzt werden. Zu beachten ist hierbei allerdings, dass MAC-Adressen gefälscht werden können und deshalb nicht als alleiniges Authentisierungskriterium herangezogen werden sollten.

### Zugriffsbeschränkungen

Es muss sichergestellt werden, dass ein VPN-Nutzer ausschließlich auf die zur Aufgabenerledigung notwendigen Dienste auf den Servern im LAN zugreifen kann. Dies könnte beispielsweise sichergestellt werden durch eine benut-

zerbezogene Authentisierung auf Anwendungsebene *und* die Kontrolle des Verkehrs mit Hilfe von Paketfiltern (Paketfilter alleine sind aufgrund der Fälschbarkeit der IP-Adressen nicht ausreichend).

**VPN**

Zugriffe von einem Laptop von außerhalb auf das interne Netz sollten ausschließlich über VPN gesichert erfolgen. Ermöglicht die Institution einen Abruf von dienstlichen E-Mails über das Internet mittels einer Web-Mail-Lösung, so ist sicherzustellen, dass die E-Mails ausschließlich verschlüsselt vom Server auf das Laptop übertragen werden (z. B. mittels SSL). Allerdings muss hierbei nicht nur der Transportkanal, sondern auch das Endsystem selbst besonders abgesichert werden. Ein Laptop kann kompromittiert werden, wenn neben der VPN-Nutzung gleichzeitig auch noch Standardprotokolle wie z. B. HTTP oder SMTP im Internet genutzt werden. Daher sollten Laptops möglichst so abgesichert werden, dass bei bestehender VPN-Verbindung in das interne Netz keine anderen Verbindungen möglich sind (Split-Tunneling). Dabei muss gewährleistet sein, dass alle abgehenden Datenpakete des Clients in den Tunnel gehen und ausschließlich Datenpakete aus dem Tunnel akzeptiert werden.

Es sollte in diesem Zusammenhang auch darauf geachtet werden, dass neben dem VPN-gesicherten Laptop-Zugriff auf das interne Netz nicht gleichzeitig andere Netzzugriffe möglich sind. Insbesondere darf während der VPN-Zugriffe kein WLAN oder Bluetooth auf dem Laptop aktiv sein. Weitere Hinweise zur Übertragungssicherheit finden sich in M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation*.

Ein mobiles IT-System kann leicht in falsche Hände geraten. Die Verbindung in das interne Netz (der Tunnelaufbau) sollte daher nicht automatisiert, sondern erst nach einer Authentisierung erfolgen. Weitere Empfehlungen des BSI zum sicheren Aufbau und Betrieb von VPNs finden sich auf der Webseite www.bsi.bund.de, Stichwort Internet-Sicherheit.

**DHCP**

Über das Dynamic Host Configuration Protocol (DHCP) werden in IP-basierten Netzen den angeschlossenen Clients automatisch temporäre IP-Adressen sowie Routing- und DNS-Server-Informationen zugewiesen, so dass der Laptop zum Internet-Zugriff nicht mehr vom Benutzer konfiguriert werden muss.

Wenn DHCP aktiviert ist, wird einem IT-System automatisch eine gültige IP-Adresse für das lokale Netz zugewiesen und kann somit auf alle freigegebenen Ordner und Laufwerke zugreifen. Als Abhilfe sollte zum einen DHCP auf dem Laptop deaktiviert werden, wenn es nicht benötigt wird (dann müssen allerdings die IP-Adressen manuell verteilt werden). Zum anderen sollte bei der IP-Adressvergabe zusätzlich über die MAC-Adresse überprüft werden, ob der Client zum Netz zugelassen werden sollte.

**Internet-Zugriffe**

Es muss geregelt werden, ob Laptops direkt auf das Internet zugreifen dürfen. Der kritische Punkt hierbei ist, dass dabei die institutionseigenen Sicherheitsgateways und Sicherheitsmechanismen umgangen werden, dies also potentiell Sicherheitsprobleme nach sich ziehen kann. Es gibt verschiedene Lösungsmöglichkeiten, die je nach Sicherheitsanforderungen und Einsatzumgebung ausgewählt werden müssen:

- Verbot direkter Internet-Zugriffe: Diese Lösung hat natürlich den Vorteil, dass sie am einfachsten umzusetzen ist. Sie ist allerdings auch die ein-

schränkenste Möglichkeit und wird daher nicht einfach durchzusetzen sein.
- Nutzung verschiedener Benutzerkennungen: Auf Betriebssystem-Ebene sollten in diesem Fall zwei verschiedene Benutzerkennungen genutzt werden, einmal für die allgemeine geschäftliche Nutzung und einmal für Internet-Zugriff. Hierbei sollte die Internet-Kennung nur über minimale Rechte verfügen.
- Nutzung verschiedener Partitionen/Betriebssysteminstallationen: Bei dieser Lösung werden verschiedene Partitionen genutzt, die möglichst stark getrennt sind, beispielsweise durch unterschiedliche Betriebs- und Dateisysteme. Je stärker die Trennung ist, desto höher sind die Hürden, um die Beeinträchtigung der Produktiv-Umgebung durch Schadsoftware aus dem Internet oder ähnliches zu verhindern.
- Virtuelle Maschinen: Hierbei erfolgt die direkte Nutzung des Internets ausschließlich über ein Betriebssystem, das in einer virtuellen Maschine (z. B. User Mode Linux, UML) betrieben wird. Durch die virtuelle Maschine wird der benutzte Browser stärker vom eigentlichen Host-Betriebssystem getrennt, als dies bei einer Nutzung ohne virtuelle Maschine der Fall ist. Allerdings besteht bei dieser Variante das Restrisiko, dass Schadprogramme - z. B. mit JavaScript erzeugt - mittels Copy&Paste zwischen dem Host-Betriebssystem und dem virtuellen Betriebssystem hin- und herkopiert werden können. Das Host-Betriebssystem könnte sich in diesem Fall bei der nächsten VPN-Einwahl in einem unsicheren Zustand befinden.
- Verwendung von Boot-CDs: Hierbei wird für die Internet-Nutzung von einem schreibgeschützten Medium wie einer CD-ROM eine internetfähige Betriebsumgebung hergestellt, wobei die Nutzbarkeit dadurch eingeschränkt wird, dass notwendige IP-Informationen evtl. von Hand eingetragen werden müssen. Hierzu kann beispielsweise Knoppix verwendet werden, eine komplett von CD lauffähige Zusammenstellung von GNU/Linux-Software (siehe *www.knoppix.org*).
- Internet-Zugriff nur über VPN (über Intranet über institutionseigenen Sicherheitsgateway ins Intranet). Dies hat den Vorteil, dass gefährliche Inhalte aussortiert werden.

**Authentisierung der VPN-Nutzung**

Bevor ein VPN aufgebaut wird, sollte die Authentizität des Benutzers mit starken Authentisierungsverfahren sichergestellt werden.

Starke Authentisierungsverfahren sind beispielsweise Einmal-Passwort- oder Challenge-Response-Verfahren.

**Protokollierung**

Die Nutzung der Server-Dienste sollte durch Protokollierung der Zugriffe nachvollziehbar sein. Dabei sollte auch erkennbar sein, ob der Laptop-Zugriff aus dem Unternehmen bzw. der Behörde oder von extern erfolgte.

**Temporäre Daten**

Es sollte sichergestellt werden, dass alle zwischengespeicherten Authentisierungsinformationen, die den Aufbau eines VPNs ermöglichen, nach dem Ende der VPN-Nutzung automatisch gelöscht werden. Dies gilt sowohl für absichtlich als auch unabsichtlich beendete VPN-Verbindungen. Zusätzlich sollte beispielsweise bei Browser-basierten SSL-VPNs darauf geachtet werden, dass sämtliche Zwischenspeicher deaktiviert werden, damit Authentisierungsinformationen erst gar nicht temporär gespeichert werden und einem Angreifer die Wiederherstellung der VPN-Verbindung erleichtern.

Prüffragen:

- Ist der sichere Anschluss von Laptops an LANs geregelt?
- Sind alle Laptops wirksam vor schädlichem Code und vor Angriffen aus Fremdnetzen geschützt?
- Wird das Betriebssystem und die installierte Software von Laptops auf dem aktuellen Stand gehalten?
- Ist der sichere Zugriff von Laptops auf das Internet geregelt?
- Ist sichergestellt, dass nur zugelassene Laptops sich am LAN anmelden können?
- Werden alle Laptop-Zugriffe von außerhalb auf das interne Netz über VPN abgesichert?

# M 5.123 Absicherung der Netzkommunikation unter Windows

**Verantwortlich für Initiierung:** Administrator, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Die Sicherheit einer Windows Infrastruktur wird nicht ausschließlich von der sicheren Konfiguration und dem sicheren Betrieb einzelner Systeme bestimmt. Die Gesamtsicherheit hängt auch wesentlich von der Sicherheit in der Netzkommunikation ab, die unter anderem durch die Absicherung der Kommunikationswege (Signaturen, Verschlüsselung) und die verwendeten Authentisierungsmechanismen bestimmt wird.

Generell gilt, dass nicht verwendete Netzkomponenten (z. B. *Datei- und Druckerfreigabe für Microsoft-Netzwerke*) von existierenden Schnittstellen zu entfernen sind. Die Beurteilung, welche Netzprotokolle entfernt werden sollten, hat anhand konkreter Umstände und im Einzelfall zu erfolgen.

### Sicherer Kanal

Die Kommunikation eines Clients mit einem Domain Controller erfolgt über den so genannten *Sicheren Kanal*, der unter anderem für die Übertragung der Authentisierungsdaten verwendet wird. Die Daten des Sicheren Kanals werden mit einem Sitzungsschlüssel verschlüsselt. Das jeweilige Computer-Konto des Clients (automatisch von Windows verwaltet) wird für den Aufbau dieses Kanals verwendet. Die regelmäßigen Änderungen des Kennworts für das Computer-Konto sind maßgebend für die Sicherheit des Sicheren Kanals (siehe M 5.89 *Konfiguration des sicheren Kanals unter Windows*).

### Signieren und Verschlüsseln der Kommunikation

Alle Daten, die über den Sicheren Kanal übertragen werden, sollten signiert und verschlüsselt werden. Standardmäßig erfolgt dies nur dann, wenn beide Kommunikationspartner die gleichen Verfahren verwenden. Unterstützt einer der beiden Partner die Verschlüsselung oder das Signieren nicht, erfolgt die Kommunikation ungeschützt (Richtlinien *Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)* und *Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen)*. Wird die Richtlinie *Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)* aktiviert, muss die Kommunikation signiert oder verschlüsselt werden. Unterstützen beide Partner nicht die gleichen Verfahren, wird keine Verbindung aufgebaut. Diese Option wird für den Einsatz empfohlen, wenn alle Domain Controller der Domäne und aller vertrauten Domänen mindestens Windows 2000 ausführen.

Das SMB-Protokoll (Server Message Block) unterstützt nicht nur eine gegenseitige Authentisierung, sondern erlaubt auch das Signieren der SMB-Pakete. Durch die Authentisierung und das Signieren werden Man-in-the-Middle-Angriffe verhindert.

Die SMB-Signaturen werden mit folgenden Richtlinien unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* konfiguriert:

- *Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt),*
- *Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer)*,
- *Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)*,
- *Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)*.

Standardmäßig werden Signaturen für SMB-Pakete unter Windows nicht erzwungen, aktiviert ist lediglich die Richtlinie *Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt)*. Nur wenn auf dem SMB-Server das Signieren der Pakete aktiviert wurde, wird die Kommunikation signiert. Es besteht jedoch die Möglichkeit, die Signaturen zu erzwingen. Hierfür sind die restlichen oben aufgeführten Richtlinien zu aktivieren.

Das Aktivieren der Richtlinien zum Signieren der SMB-Kommunikation kann sich auf die Kompatibilität mit Clients, Diensten und Anwendungen auswirken. Vor der Aktivierung dieser Einstellungen sind daher Kompatibilitätstests erforderlich.

Nicht alle SMB-Server von Drittanbietern unterstützen die Kennwortverschlüsselung während der Authentisierung. Wird mit dem SMB-Protokoll auf einen solchen Server zugegriffen, kann das Kennwort unverschlüsselt übertragen werden, wenn die Richtlinie *Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden* aktiviert ist. Allerdings sollte die Übertragung ungeschützter Kennwörter nicht zugelassen werden, das heißt die genannte Richtlinie darf nicht aktiviert werden.

Windows erlaubt das Festlegen der minimalen Sitzungssicherheit für die Kommunikation auf Anwendungsebene (z. B. zwischen RPC-Komponenten). Folgende Optionen können in den beiden Richtlinien *Netzwerksicherheit: minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients)* und *Netzwerksicherheit: minimale Sitzungssicherheit für NTLM-SSP-basierte Server (einschließlich sicherer RPC-Server)* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* gewählt werden:

- NTLMv2-Sitzungssicherheit erfordern,
- 128-Bit-Verschlüsselung erfordern.

Standardmäßig werden keine Minimaloptionen festgelegt. Werden auf allen IT-Systemen Client-Betriebssysteme ab Windows XP und Server-Betriebssysteme ab Windows Server 2003 mit aktivierter 128-Bit-Verschlüsselung ausgeführt, sind die Optionen für die NTLMv2-Authentisierung und 128-Bit-Verschlüsselung zu aktivieren.

**Starker Authentisierungsmechanismus**

Die Güte des Authentisierungsverfahrens bei Netzanmeldungen spielt ebenfalls eine signifikante Rolle für die Gewährleistung der Sicherheit. Insgesamt können vier Authentisierungsmechanismen verwendet werden: LM, NTLMv1, NTLMv2 und Kerberos. Vor Windows 2000 wurde zunächst das LM-Verfahren und ab Windows NT das NTLM-Verfahren (in zwei Versionen) eingesetzt. Die alten Verfahren haben jedoch Schwächen, so dass aus einem übertragenen Authentisierungswert das Kennwort bestimmt werden kann. Den besten Schutz bieten die Version 2 des NTLM Protokolls sowie Kerberos. Kerberos

ist als Standardprotokoll für die Authentisierung bei Benutzeranmeldung implementiert. NTLM ermöglicht die Kompatibilität mit älteren Systemen.

Bei Kerberos handelt es sich um ein kryptographisches Netzprotokoll zur verteilten Authentisierung. Kerberos realisiert eine Authentisierung innerhalb des Netzes, inklusive eines Schlüsselaustausches, ohne das den beteiligten Stellen ein gemeinsamer Schlüssel bekannt ist. Erreicht wird dies durch die Einführung einer weiteren Protokollinstanz.

In reinen Windows-Netzen (mit Client- und Server-Betriebssystemen ab Windows 2000) sollte möglichst Kerberos als das sicherste verfügbare Verfahren eingesetzt werden. Ist ein Einsatz von Kerberos nicht möglich, so wird automatisch die Authentisierung mittels NTLMv2 umgesetzt. Die älteren Protokolle sollten aufgrund ihrer Schwächen abgelehnt werden. Dazu ist in der zugehörigen Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Netzwerksicherheit: LAN Manager-Authentifizierungsebene* der Wert *Nur NTLMv2-Antworten senden\LM& NTLM verweigern* einzustellen.

Die Speicherung der LAN Manager-Hashwerte bei Kennwortänderungen sollte deaktiviert werden. Dies wird durch das Aktivieren der Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern* erreicht.

Sind noch ältere Systeme im Einsatz (Windows 9x bzw. Windows NT 4.0 vor Service Pack 4), so kann es aus Kompatibilitätsgründen notwendig sein, auch andere Authentisierungsmechanismen zuzulassen, was aus Sicherheitssicht jedoch nicht empfohlen wird. Grundsätzlich wird empfohlen, die älteren Systeme mit Hilfe entsprechender Service Packs zu aktualisieren (Windows NT 4.0 Service Pack 4 oder höher) oder Zusatzsoftware zu verwenden (NTLMv2 ist zusammen mit dem optionalen Client für Verzeichnisdienste auch unter Windows 95/98 verfügbar).

**Anonymer Zugriff**

Anonyme Zugänge über das Netzwerk sollten grundsätzlich nicht möglich sein (sogenannte NULL SESSIONS). Unter Windows XP ist es standardmäßig vorgesehen, bestimmte Aktivitäten wie das Aufzählen von SAM-Konten anonym durchzuführen. Diese Funktionalität ist durch das Aktivieren der Richtlinien *Netzwerkzugriff: Anonyme SID-/Namensübersetzung nicht erlauben*, *Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben* und *Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben* (unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) explizit abzuschalten. Die Richtlinie *Netzwerkzugriff: Die Verwendung von "Jeder"-Berechtigungen für anonyme Benutzer ermöglichen* ist zu deaktivieren. Unter IT-Systemen ab Windows Vista ist diese Richtlinie bereits in der Standardeinstellung deaktiviert.

**Netzkommunikation mit DirectAccess absichern**

Ab Windows 7 und Windows Server 2008 R2 ermöglicht die Funktion DirectAccess eine permanente logische Verbindung eines Clients mit dem Netz des Informationsverbundes, unabhängig von der Art der Netzanbindung. Bei dem Verfahren erfolgt die Netzkommunikation über eine Tunnelverbindung vom Client zu anderen Computern der Windows-Domäne. Der Tunnel kann sowohl von externen Netzen aus als auch innerhalb des Netzes des Informa-

tionsverbundes verwendet werden. Er bleibt solange bestehen, wie das Windows-System eine Netzverbindung hat.

Unter Verwendung von DirectAccess stellt der Client die Verbindung zum Netz des Informationsverbundes bereits vor der Benutzeranmeldung mittels Zertifikat her. Somit werden zum Beispiel GPO Updates und neue Richtlinien übernommen, bevor sich der Nutzer mit seinem Account angemeldet hat. Für die Datenübertragung nach der Benutzeranmeldung sind in der Grundkonfiguration keine Sicherheitsmaßnahmen vorgesehen. Lediglich die Computer-Authentisierung der Clients erfolgt verschlüsselt. Deshalb sollte die Übertragung mit zertifikatsbasiertem IPSec gesichert werden. Dafür ist eine PKI nötig, die im Netz des Informationsverbundes aufgebaut werden sollte. Für die Konfiguration von IPSec ist die Maßnahme M 5.90 *Einsatz von IPSec unter Windows* umzusetzen.

Standardmäßig ist keine einheitliche Sicherheitsprotokollierung für DirectAccess an Windows Clients voreingestellt. Überwachungsmöglichkeiten sind unter anderem hier zu finden:

- *gpedit.msc* | *...* | *Erweiterte Überwachungsrichtlinienkonfiguration* | *Anmelden/Abmelden* | *IPSec ...*
- *perfmon.exe* | *Leistungsüberwachung* | *Leistungsindikatoren* (z. B. IP-HTTPS, Teredo, IPSec, WFP)

Diese Protokolle können sehr schnell wachsen und die Arbeitsfähigkeit des Rechners beeinträchtigen. Daher sollten die Überwachungseinstellungen gemeinsam mit den Serverkomponenten von DirectAccess sorgfältig auf die Anforderungen des Informationsverbunds abgestimmt werden. Eine Protokollierung auf Clientseite muss sichergestellt sein.

Prüffragen:

- Sind alle nicht verwendeten Netzwerkkomponenten von existierenden Schnittstellen entfernt worden?
- Wird das Kennwort für das Computer-Konto regelmäßig geändert?
- Werden alle Daten, die über den Sicheren Kanal übertragen werden, signiert und verschlüsselt?
- Werden anonyme Zugänge über das Netzwerk verhindert?
- Wird Kerberos als Authentisierungsverfahren oder mindestens NTLMv2-Authentisierung genutzt sowie die 128-Bit-Verschlüsselung aktiviert, wenn auf allen Rechnern Client-Betriebssysteme ab Windows XP bzw. Server-Betriebssysteme ab Windows Server 2003 mit aktivierter 128-Bit-Verschlüsselung ausgeführt werden?
- Wurde gewährleistet, dass auch ältere Clients das NTLMv2 Verfahren zur Authentisierung verwenden (z. B. durch das Einspielen entsprechender Service Packs oder zusätzlicher Software)?
- Wurde anonymen Zugängen über das Netz die Berechtigung "Jeder" entzogen?

# M 5.124 Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

In Besprechungs-, Veranstaltungs- und Schulungsräumen sind einerseits häufig IT-Systeme wie Beamer oder Schulungsrechner fest installiert, andererseits werden dorthin auch mobile IT-Systeme wie Laptops häufig mitgebracht. Dabei ist oft auch gewünscht, dass diese IT-Systeme miteinander, mit dem Internet oder dem institutionsinternen Intranet vernetzt werden können.

Da fremde IT aber zunächst immer als nicht vertrauenswürdig betrachtet werden sollte, sollte eine unkontrollierte Anbindung von durch Besucher mitgebrachten IT-Systemen an interne LANs unterbunden werden. Es sollte auch möglichst keine direkte Kopplung von mitgebrachten und internen IT-Systemen stattfinden. Hierbei sind zumindest alle Sicherheitsmaßnahmen umzusetzen, die in Baustein B 5.2 *Datenträgeraustausch* beschrieben sind.

Grundsätzlich können folgende Zugriffsarten gewünscht sein:

- LAN-Zugriff für alle Raumnutzer, ohne Zugriff auf Internet
- LAN-Zugriff für Mitarbeiter
- Direkter Internet-Zugriff für alle Raumnutzer
- Internet-Zugriff über LAN für alle Raumnutzer
- Internet-Zugriff über LAN für Mitarbeiter

Im folgenden wird beschrieben, wie diese verschiedenen Zugriffsarten zu bewerten und abzusichern sind:

Aus Sicherheitssicht die beste und einfachste Lösung ist es, einen Zugriff aus Besprechungs-, Veranstaltungs- und Schulungsräumen auf interne LANs generell zu unterbinden. Im sichersten Fall sollten gar keine entsprechenden Anschlüsse installiert werden, um auszuschließen, dass Institutionsfremde sich mit dem internen Netz verbinden können.

Dies ist allerdings nicht immer möglich. Wenn eigene Mitarbeiter aus Besprechungs-, Veranstaltungs- und Schulungsräumen auf das Intranet zugreifen können sollen, sind mindestens folgende Maßnahmen zu ergreifen (siehe M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*):

- Der Zugriff auf ein LAN sollte auf hierfür zugelassene IT-Systeme beschränkt werden. Dies sollte beispielsweise über die Prüfung der MAC-Adressen, über rechnergebundene Zertifikate oder über eine Benutzerauthentisierung sichergestellt werden.
- Besprechungs-, Veranstaltungs- und Schulungsräume sollten durch einen restriktiv konfigurierten Paketfilter vom LAN getrennt werden, um unerwünschte Kommunikation unterbinden zu können. Dadurch können unter anderem die Auswirkungen der auf den angeschlossenen Rechnern eventuell vorhandenen Schadsoftware gemindert werden.
- Es muss sichergestellt werden, dass Dritte den Datenverkehr bei der LAN-Nutzung durch Mitarbeiter nicht mitlesen bzw. mitschneiden können. Dies könnte zum einen erfolgen, indem die Infrastruktur so geschaffen wird, dass weitere Rechner den Anschluss des Mitarbeiters nicht mitnutzen können (z. B. durch Verzicht auf Hubs). Zum anderen könnte eine verschlüs-

selte Kommunikation eingesetzt werden, die erst nach einer entsprechenden Authentisierung des Mitarbeiters aufgebaut werden kann.
- Nach Möglichkeit sollte kein Dynamic Host Configuration Protocol (DHCP) für die Zugänge zum LAN angeboten werden. Angeschlossene Fremdrechner sind somit nicht automatisch in das Netz integriert und müssen von Hand konfiguriert werden (die hauseigenen Rechner müssten in diesem Fall entsprechend vorkonfiguriert sein). Denkbar wäre auch statisches DHCP, dass nur den anhand der MAC-Adresse erkannten, hauseigenen Rechnern die Netzinfrastrukturinformationen zuordnet.

Zunehmend sind in Besprechungs-, Veranstaltungs- und Schulungsräumen aber auch direkte Internet-Zugänge zu finden, z. B. über dedizierte DSL-Zugänge. Die Zugänge werden häufig als Internet-Steckdosen gekennzeichnet. Hierüber können Besucher beispielsweise auf ihr Heimat-Netz zugreifen. Diese Internet-Zugänge dürfen aus Sicherheitsgründen nicht direkt mit dem Intranet verbunden werden, damit der zentrale Sicherheitsgateway nicht umgangen werden kann. Es muss auch ausgeschlossen werden, dass ein Rechner gleichzeitig eine Verbindung zu Intranet und Internet aufbauen kann. In diesem Fall wird die ursprüngliche hardwaremäßige Trennung der beiden Netze aufgehoben. Wenn Besprechungs-, Veranstaltungs- und Schulungsräume mit dem Internet direkt vernetzt werden sollen, sollte der Zugang mit einem Paketfilter abgesichert sein, um die angeschlossenen IT-Systeme Systeme vor Standardangriffen auf Ports zu schützen. Ein einfacher Sicherheitsproxy kann darüber hinaus die angeschlossenen Rechner vor den Gefährdungen durch aktive Inhalte schützen und die Zugriffe auf Web-Seiten im Rahmen der datenschutzrechtlichen Möglichkeiten protokollieren.

Es sollte darauf verzichtet werden, fremden Mitarbeitern einen Zugang zum Internet anzubieten, der das institutionsinterne Netz als Vermittlungsnetz nutzt. Es kann z. B. aufgrund von Konfigurationsfehlern nie ausgeschlossen werden, dass fremde Mitarbeiter sich trotz eingeschränkter Zugriffsmöglichkeiten einen Zugang zu schutzwürdigen Informationen oder Anwendungen verschaffen.

Wenn ein direkter LAN-Zugriff unterbunden ist, kann eigenen Mitarbeiter auch der Zugriff auf das LAN aus Besprechungs-, Veranstaltungs- und Schulungsräumen heraus über ein VPN über das Internet ermöglicht werden (siehe M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*).

Für den Aufbau von WLANs zur Bereitstellung eines Internetzugangs sollten die entsprechenden Sicherheitsmaßnahmen ergriffen werden.

Prüffragen:

- Ist sichergestellt, dass eine direkte Kopplung von mitgebrachten und internen IT-Systemen unterbunden wird?
- Ist ein Zugriff auf das LAN ausschließlich auf hierfür zugelassene IT-Systeme beschränkt?
- Wird verhindert, dass Dritte den internen Datenverkehr mitlesen beziehungsweise mitschneiden können?
- Wird verhindert, dass Rechner in Besprechungs-, Veranstaltungs- und Schulungsräumen gleichzeitig eine Verbindung zum Intranet und zum Internet aufbauen können?

# M 5.125 Absicherung der Kommunikation von und zu SAP Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein SAP System kommuniziert über das lokale Netz mit SAP Clients, Browsern, Applikationen und anderen SAP Systemen. Auch zwischen den SAP Systemkomponenten findet Datenaustausch statt. In allen Fällen werden Daten übertragen, die geschützt werden müssen. Dies sind nicht nur die Daten, die genutzt werden, um Benutzer zu authentisieren (z. B. Benutzername und Passwort, SSO-Tickets, SAPSSO2-Cookie), sondern auch Geschäftsdaten, die im Rahmen der aufgerufenen Funktionen verarbeitet werden.

Es muss daher entschieden werden, ob und mit welchem Schutzmechanismus die Kommunikation abgesichert wird. Die Kommunikationsmethoden können im Wesentlichen in folgende Klassen unterteilt werden:

- RFC-Kommunikation:
  Hier werden die Daten im Klartext übertragen. Protokolle, die auf RFC aufsetzten, beispielsweise DIAG, das von SAPGui-Clients genutzt wird, komprimieren die Daten. Dies ist jedoch kein Schutzmechanismus. Zudem kann die Kompression ausgeschaltet werden.
- HTTP-basierte Kommunikation:
  Die Daten werden in Klartext-Form übertragen.
- TCP/IP-Kommunikation:
  Die Daten werden in Klartext-Form übertragen.

Bei der Übertragung schützenswerter Daten von und zu SAP Systemen sollten diese verschlüsselt werden. Zum Schutz der Daten können unterschiedliche Verfahren eingesetzt werden. Es ist daher zu entscheiden, welches Verfahren unter Kosten-Nutzen-Aspekten das günstigste ist. Die Entscheidung ist nachvollziehbar zu dokumentieren.

### Einsatz von IPSec

IPSec bietet eine generelle Absicherung der Kommunikation auf IP-Ebene: Alle Datenpakete werden verschlüsselt und integritätsgeschützt. Vorteilhaft an diesem Verfahren ist, dass auf SAP System-Ebene keine zusätzlichen Konfigurationen durchzuführen sind, da der IPSec-Schutz auf Betriebssystem-Ebene konfiguriert wird.

Werden SAP Systeme in reinen Windows-Netzen betrieben (Versionen ab Windows 2000), ist IPSec standardmäßig und ohne Mehrkosten (z. B. für Lizenzen) verfügbar. Es entsteht jedoch administrativer Aufwand für die Konfiguration. Weitere Informationen finden sich in M 5.90 *Einsatz von IPSec unter Windows*.

Beim Einsatz von IPSec wird sowohl die Kommunikation des ABAP- als auch des Java-Stacks geschützt.

### Einsatz von SNC

Innerhalb des SAP Systems kann die Kommunikation mit SNC (Secure Network Communications) geschützt werden. SNC ist jedoch nur eine standardisierte Schnittstelle, so dass SNC-konforme Schutzbibliotheken (auch SNC-Bi-

bliothek, SNC-Modul oder SNC-Implementierung genannt) zusätzlich erworben, lizenziert und installiert werden müssen.

SNC bietet unterschiedliche Schutzlevel an. Im Wesentlichen wird jedoch Authentisierung und Verschlüsselung angeboten. Je nach SNC-Bibliothek können dabei unterschiedliche Algorithmen eingesetzt werden. SNC bietet eine generelle Absicherung der Kommunikation auf SAP System-Ebene.

Bei der Beschaffung von SNC-Implementierungen ist Folgendes zu berücksichtigen:

- Welche Algorithmen werden angeboten? Es ist auf ausreichend sichere Algorithmen mit ausreichend langen Schlüsseln zu achten. Proprietäre und nicht offen gelegte Verschlüsselungsverfahren sind zu vermeiden.
- Wie ist das Preis- und Lizenzmodell? Für große Unternehmen oder Behörden können hier nicht zu vernachlässigende Kosten entstehen.
- Die Authentisierung erfolgt bei SNC außerhalb des SAP Systems. Wie werden die SNC-Benutzer verwaltet? Müssen die Benutzer über ein separates Werkzeug verwaltet werden oder erfolgt eine Integration in bestehende Verwaltungsstrukturen (z. B. LDAP-Server, Windows Active Directory)?

Von SAP sind SNC-Implementierungen kostenfrei verfügbar, die unter Windows einsetzbar sind. Hier kann zwischen einer NTLM-basierten Variante, die lediglich Authentisierung bietet, und einer Kerberos-basierten Variante, die Authentisierung und Verschlüsselung unterstützt, gewählt werden.

SNC schützt beim Einsatz sowohl die Kommunikation des ABAP- als auch des Java-Stacks, ist jedoch jeweils separat zu konfigurieren.

Quellen für SAP Dokumentationen zur SNC-Konfiguration finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Einsatz von SSL**

Für alle HTTP-basierten Zugriffe ist SSL grundsätzlich zu empfehlen. Dies gilt auch für die interne Kommunikation zwischen Komponenten des SAP Systems und anderen Komponenten, die die Möglichkeit der SSL-Absicherung bieten (z. B. beim LDAP-Zugriff).

Da SSL Verschlüsselungsmechanismen nutzt, SAP jedoch aufgrund unterschiedlicher Export-/Import-Bestimmungen in den verschiedenen Ländern Verschlüsselungsmechanismen nicht standardmäßig ausliefert, muss die Verschlüsslungsbibliothek (SAP Cryptographic Library, SAP Cryptolib) zusätzlich installiert werden. Es ist zu beachten, dass die SSL-Unterstützung für den ABAP-Stack und den Java-Stack separat zu installieren ist.

SSL verhandelt das eingesetzte Schutzverfahren dynamisch zwischen den Kommunikationspartnern. Daher sollten schwache Verfahren aus der Liste der erlaubten Verfahren (der so genannten Cipher-Suite) gelöscht werden.

Hinweise auf detaillierte Anleitung zur Installation und Konfiguration von SSL finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Wird die Kommunikation von und zu SAP Systemen angemessen abgesichert?
- Ist nachvollziehbar dokumentiert, mit welchen Schutzmechanismen die Übertragung schützenswerter Daten von und zu SAP Systemen erfolgt?

- SNC (Secure Network Communications) zur Kommunikation von und zu SAP Systemen: Wird auf sichere Algorithmen mit ausreichend langen Schlüsseln geachtet?

# M 5.126 Absicherung der SAP RFC-Schnittstelle

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Remote Function Call (RFC) Mechanismus ist für den ABAP-Stack die primäre Kommunikationsschnittstelle für die System-zu-System-Kommunikation. Auch der Java-Stack unterstützt die RFC-Kommunikation über den Java Connector (JCo).

Hinweise auf SAP Dokumentationen zur RFC-Kommunikation finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**RFC-Berechtigungen restriktiv vergeben**

Berechtigungen zum Aufruf von RFC-fähigen ABAP-Programmen (dann auch RFC-fähige Bausteine genannt) werden über das Berechtigungsobjekt S_RFC gesteuert. Jeder RFC-fähige Baustein erfordert je nach Funktionalität weitere Berechtigungen, die über zusätzliche Berechtigungsobjekte geprüft werden. Da der Aufruf meist über das Netz erfolgt, ist das SAP System über die RFC-Schnittstelle aus der Entfernung potentiell angreifbar.

Die RFC-Berechtigungen müssen daher geplant und restriktiv vergeben werden. Durch das S_RFC Berechtigungsobjekt kann gesteuert werden, auf welche RFC-Funktionsbausteine ein Benutzer zugreifen darf. Dabei unterliegt das Berechtigungsobjekt folgenden wichtigen Beschränkungen:

- Die Beschränkung kann nur auf Funktionsgruppen erfolgen, da nur der Wert RFC_TYPE = "FUGR" unterstützt wird.
- Die Prüfung des Parameters RFC_NAME, der die Liste der betroffenen Funktionsgruppen enthält, ist auf achtzehn Zeichen beschränkt. Die Liste kann zwar länger eingegeben werden, jedoch werden nur die ersten achtzehn Zeichen geprüft.

Der Zugriff kann also nur auf alle Funktionsbausteine einer Funktionsgruppe erteilt werden, und unter Umständen müssen mehrere Berechtigungen erstellt werden.

Generell sollte die S_RFC Berechtigung nicht den Zugriff auf alle RFC-Bausteine erlauben. Die Einstellung RFC_NAME="*" ist zu vermeiden. Es gibt in einem SAP System mehrere tausend RFC-fähige Funktionsbausteine, die damit zum Zugriff freigeschaltet würden. Auch auf RFC-fähige Bausteine von neu installierten Applikationen und Modulen könnte so automatisch zugegriffen werden. Ob die aufgerufene RFC-Funktion jedoch erfolgreich ausgeführt wird, hängt dann noch von Zugriffsprüfungen ab, die die RFC-Funktion selbst durchführt.

Werden die RFC-Berechtigungen geplant, ist zu bedenken, dass es unterschiedliche RFC-Typen (z. B. synchron, asynchron) gibt. Daher müssen alle Typen in die Planung einbezogen werden.

Die Berechtigung S_RFC ist nicht für den Java-Stack relevant.

Ausgehende RFC-Zugriffe können über das Berechtigungsobjekt S_ICF beschränkt werden, das den Zugriff auf Destinationen regelt (siehe M 4.263 *Absicherung von SAP Destinationen*).

**Java-Stack RFC**

Der Java Connector (JCo) bietet für den Java-Stack die Möglichkeit, über RFC zu kommunizieren. Dabei wird jedoch standardmäßig von den Systemkomponenten nur von ausgehenden RFC-Calls (Java-Stack als RFC-Client) Gebrauch gemacht. Zugriffe erfolgen auf den eigenen ABAP-Stack (z. B. um Benutzer und Rollen des ABAP-Stacks verfügbar zu machen) oder über Destinationen auf andere SAP Systeme oder externe RFC-Server.

Folgendes ist beim Einsatz des Java Connectors zu bedenken:

- Der Java-Stack nutzt den (ABAP-Stack-) Benutzer SAPJSF zum Zugriff auf den ABAP-Stack. Dieser muss während der Installation mit einem starken Passwort versehen werden.
- Die Destinationen (Destination-Service) im Java-Stack müssen vor unberechtigtem Zugriff geschützt werden.

Für Java-Stack RFC-Server-Programme ist Folgendes zu beachten:

- RFC-Server müssen durch eigene Programme implementiert werden. RFC-Server-Instanzen können über die JCo-Programmierschnittstelle erzeugt werden.
- Die JCo-RFC-Server-Implementierung bietet nur reine RFC-Kommunikationsfunktionen. Insbesondere Berechtigungen müssen zwingend durch die eigene Programmimplementierung geprüft und verwaltet werden.

**Absicherung der RFC-Kommunikation mit SNC**

Ergibt die Schutzbedarfsfeststellung, dass Kommunikationsstrecken geschützt werden müssen, auf denen RFC eingesetzt wird, so kann SNC empfohlen werden. M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen* enthält weitere Informationen dazu.

**Sichere Verwendung von "Trusted System"-Beziehungen**

Zwischen SAP Systemen können Vertrauensbeziehungen eingerichtet werden, so dass Benutzer beim RFC-Zugriff kein Passwort angeben müssen. Beim Zugriff prüft das vertrauende SAP System (Trusting System), ob der Zugriff von einem vertrauten SAP System (Trusted System) aus erfolgt.

Über das Berechtigungsobjekt S_RFCACL kann im Zielsystem gesteuert werden, welche Benutzer Aufrufe ohne Passwortangabe durchführen dürfen. Dabei kann unter anderem nach SAP System-ID (SAPSID), Mandant und aufrufender Transaktion unterschieden werden.

Generell ist Folgendes zu beachten:

- Trusted System Beziehungen sollten nur nach reiflicher Überlegung und Risikobewertung eingesetzt werden.
- Für das Berechtigungsobjekt S_RFCACL sollten keine Blanko-Einstellungen mit "*" enthalten sein.
- Für RFC-Destinationen, die in vertrauenden SAP Systemen enden, sollten keine Benutzerinformation gespeichert werden, da sonst im vertrauenden System nicht mehr nach den aufrufenden Benutzern unterschieden werden kann.

Weitere Informationsquellen zum Thema finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**RFC-Client-Programme: Konfiguration der sideinfo Datei**

Für RFC-Clients kann über die Datei "sideinfo" eine globale Konfiguration für den RFC-Zugriff erfolgen. In der Datei können auch Authentisierungsinformationen angegeben werden, die dann für RFC-Zugriffe (genauer: beim Aufbau der unterliegenden CPIC-Kommunikation) genutzt werden. Alle Informationen sind in der Datei im Klartext gespeichert.

Folgendes sollte daher beachtet werden:

- Der Einsatz der sideinfo Datei sollte gut überlegt werden.
- Die Informationen der sideinfo Datei kann von allen lokalen RFC-Client-Programmen genutzt werden.
- Authentisierungsinformationen sollten nicht in der sideinfo Datei gespeichert werden. Die Anmeldeinformationen sollten durch das Client-Programm vom Benutzer erfragt werden.
- Die sideinfo Datei darf für Benutzer, die RFC-Client-Programme starten, nur lesend zugreifbar sein. Schreibzugriffe dürfen nur für den berechtigten Administrator möglich sein.

Die sideinfo Datei kann in einem SAP System an mehreren Stellen genutzt werden und kommt insbesondere auch auf dem SAP Gateway zum Einsatz.

Hinweise auf Detailinformationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**Externe (non-SAP) RFC-Server sicher nutzen**

Mit Hilfe des RFC Software Development Kits (RFC SDK) können RFC-Server-Programme erstellt werden, die ihre Funktionen über RFC anbieten. Werden externe RFC-Server-Programme eingesetzt ist Folgendes zu bedenken:

- Die Standard SAP Sicherheitsmechanismen und Verfahren (Authentisierung, Autorisierung, Verwaltung) sind für den externen RFC-Server nicht verfügbar.
- Die angebotenen Sicherheitsmechanismen hängen ausschließlich von der Implementierung des RFC-Server-Programms ab.
- Die Verwaltung von Benutzern und Berechtigungen kann durch das Server-Programm oder durch externe Komponenten erfolgen. Es sind auch Implementierungen möglich, die die RFC-Funktionen für jeden Zugreifenden ohne weitere Prüfungen verfügbar machen.

Bei Eigenentwicklungen oder bei der Beschaffung von Software sollte daher darauf geachtet werden, dass die gewünschten Sicherheitsanforderungen erfüllt werden.

Für die Installation von externen RFC-Servern ist darauf zu achten, dass ausschließlich die RFC-Bibliothek installiert wird. Insbesondere ist zu vermeiden, dass das gesamte RFC Software Development Kit (RFC SDK), das für die Entwicklung vom RFC-basierten Programmen genutzt wird, installiert und zugreifbar ist. Dies muss durch den Software-Verteilungsprozess sichergestellt werden.

Für Rechner, auf denen das RFC SDK installiert werden muss (z. B. Entwicklungsrechner), sollte der Zugriff auf die Programme im "bin"-Verzeichnis (Standardpfad: <Installationsverzeichnis>/Sap/rfcsdk/bin) der SDK-Installation beschränkt werden. Die Programme können unter anderem zum RFC-Zugriff auf SAP Systeme (startrfc) oder zum Starten von RFC-Servern (rfcexec) genutzt werden.

Die Zugriffsmöglichkeiten auf SAP Systeme (z. B. Produktion) sind für Rechner, auf denen das RFC SDK installiert ist, auf Netz-Ebene zu beschränken.

Angaben zu weiteren Informationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**secinfo Datei für SAP Gateway konfigurieren**

Externe RFC-Server-Programme registrieren sich in der Regel bei der SAP Systemkomponente SAP Gateway, die die Client-Zugriffe auf die externen RFC-Server-Programme vermittelt. Diese können auf externe Anforderung auch explizit durch das SAP Gateway gestartet werden.

Die Zugriffs- und Startmöglichkeiten, die externen Zugreifern zur Verfügung stehen, werden über die Konfigurationsdatei "secinfo" gesteuert. Die Datei wird nicht automatisch erzeugt und muss daher unbedingt manuell erstellt werden. Existiert die Datei nicht, werden keine Beschränkungen umgesetzt, so dass jeder mit der technischen Zugriffsmöglichkeit beliebige Programme auf dem SAP Gateway-Rechner starten kann. Es genügt zunächst, eine leere Datei zu erzeugen, um zu erreichen, dass keine Berechtigungen bestehen. Danach können dann Berechtigungen und Zugriffseinschränkungen konfiguriert werden. Die Datei muss im "data"-Verzeichnis des SAP Gateways, also genauer der Gateway-Instanz, abgelegt sein (Standardpfad: /usr/sap/<Instanzname>/data).

Alternativ kann auch der Profilparameter "gw/rem_start" mit der Einstellung "DISABLED" genutzt werden, wenn generell keine externen RFC-Server-Programme zum Einsatz kommen.

Hinweise auf nähere Informationen dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Sind im SAP System die RFC-Berechtigungen geplant und restriktiv vergeben?
- Sind in der sideinfo Datei des SAP Systems keine Authentisierungsinformationen gespeichert?
- Ist sichergestellt, dass nur berechtigte SAP Administratoren Schreibzugriff auf die sideinfo Datei besitzen?
- Ist die Zugriffsmöglichkeit auf SAP Systeme, auf denen RFC SDK installiert ist, auf Netz-Ebene beschränkt?
- Ist im SAP Gateway System die Datei secinfo zur Sicherung der Zugriffs- und Startmöglichkeiten erstellt worden?

# M 5.127 Absicherung des SAP Internet Connection Framework (ICF)

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Das Internet Connection Framework (ICF) eines SAP Systems erlaubt den HTTP-basierten Zugriff auf Funktionen des ABAP-Stacks. Daneben wird durch das ICF auch das Simple Mail Transport Protocol (SMTP) unterstützt. Es können verschiedene Dienste (Services) angesprochen werden. Die Dienste sind in einer dateisystemähnlichen Baumstruktur hierarchisch angeordnet. Der HTTP-Zugriffspfad (URL-Pfad-Anteil) wird durch den Pfad in der Baumstruktur bestimmt. Für die Administration des ICF wird die Transaktion SICF benutzt.

Die nachfolgend aufgeführten Empfehlungen sollten im Zusammenhang mit dem ICF beachtet werden.

Hinweise auf SAP Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

### Aktive ICF-Dienste

Es sollten nur die benötigten Dienste aktiviert werden. Für jeden aktivierten Dienst sollte dessen Funktion bekannt sein. Es ist empfehlenswert, zu jedem Dienst kurz zu notieren, welche Funktion er hat und ob er aktiviert werden darf.

Nach der Installation eines SAP Systems sind alle ICF-Dienste deaktiviert. Dennoch wird eine Prüfung dieses Sachverhaltes empfohlen. Auch nach der Installation von Updates und neuer ICF-Dienste sollte dies geprüft werden.

Die Möglichkeit, die komplette ICF-Baumhierarchie, die unter einem ICF-Objekt hängt, auf einmal zu aktivieren, sollte nicht genutzt werden. Dienste sollten immer einzeln aktiviert werden.

### SSL-Schutz

Für den Zugriff auf ICF-Dienste kann einzeln konfiguriert werden, ob die Kommunikation beim Zugriff mit SSL geschützt sein muss. Es kann hier generell empfohlen werden (siehe M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*), SSL für alle Dienste zu aktivieren, um die übertragenen Daten vor unberechtigter Kenntnisnahme zu schützen. Da sich die auf einem ICF-Objekt eingestellten Eigenschaften in den Unterbaum vererben, genügt es, dazu die Konfiguration auf dem Wurzelknoten anzupassen.

### Authentisierte Zugriffe

Für jeden ICF-Dienst muss definiert werden, mit welcher Authentisierungsvariante der Zugriff erlaubt werden soll. Dies gilt insbesondere für Eigenentwicklungen.

In der Regel empfiehlt sich folgende Konfiguration für die Benutzerauthentisierung:

- Anonyme Anmeldedaten: keine Werte eintragen.
- Sicherheitsanforderung: SSL
- Basic Authentication: Standard SAP-Benutzer

Soll auf Dienste anonym zugegriffen werden, müssen Anmeldeinformationen unter "Anonyme Anmeldedaten" angegeben werden. Alle anonymen Zugriffe erfolgen dann unter dem eingetragenen Benutzer. In diesem Fall sollten ausschließlich technische Benutzer verwendet werden, die vom Typ Service sind. Dialogbenutzer sollten nicht genutzt werden.

Es muss beachtet werden, dass die Anmeldedaten für anonyme Zugriffe, die für ein ICF-Objekt definiert sind, auch für alle Unterobjekte im Unterbaum gelten. Unterschiedliche Anmeldedaten (z. B. Client, Benutzer, Sprache) die auf verschiedenen Objekten definiert sind, die auf dem Baumpfad zu einem bestimmten Objekt liegen, können sich auch überlagern.

Generell findet nach dem Aufruf eines ICF-Dienstes (z. B. einer Business Server Pages Applikation, BSP) auch immer die normale Prüfung auf die von der Applikation genutzten Berechtigungsobjekte statt.

**ICF-Administration**

Die administrativen Transaktionen SICF (ICF Dienst-Verwaltung) und SMICM (ICF-Monitor) sind vor unberechtigten Zugriffen zu schützen (Berechtigungsobjekt: S_TCODE).

In produktiven Systemen sollten die Funktionen, die das detaillierte Protokollieren von Client-Anfragen erlauben (z. B. Debugging, Trace, Laufzeitanalyse, Recorder), nicht genutzt werden. Fehlersituationen sollten im Test- und Akzeptanzsystem untersucht werden.

**ICF-Zugriffsberechtigungen**

Personen, die auf ICF-Dienste zugreifen, sollten nicht gleichzeitig über die Dialogschnittstelle (SAPGui) Zugriff auf das SAP System besitzen, so dass den Personen ein Service-Benutzer zugeordnet werden kann.

Die Zugriffsberechtigung auf ICF-Dienste sollte restriktiv vergeben werden. Das Berechtigungsobjekt S_ICF wird für die Berechtigungsprüfung herangezogen. Für die Zugriffskontrolle auf ICF-Dienste muss folgende Konfiguration gewählt werden:

- Für das Feld ICF_FIELD muss der Wert "SERVICE" eingetragen werden.
- Für das Feld ICF_VALUE muss die Zeichenkette genutzt werden, die im betroffenen ICF-Dienst unter "Service-Daten/Service Optionen/SAP-Berechtigung" eingetragen ist. Ist für mehrere Dienste die gleiche Zeichenkette eingetragen, so kann der Zugriff auf all diese Dienste über eine Berechtigung gesteuert werden (siehe dazu auch M 4.263 *Absicherung von SAP Destinationen*).

**Informationen auf Fehlerseiten**

Die Fehlerseiten von ICF-Diensten sollten keine internen Informationen enthalten. Dies gilt insbesondere für selbst erstellte Dienste.

Prüffragen:

- Sind im SAP System nur die benötigten ICF-Dienste aktiviert worden?
- Wird zu jedem aktivierten ICF-Dienst im SAP System notiert, welche Funktionen er hat und geprüft ob er aktiviert werden darf?
- Wird nach der Installation von Updates oder neuer ICF-Dienste im SAP System geprüft, ob keine ungewollten ICF-Dienste aktiviert sind?

- Werden detaillierte Protokollierung von Client-Anfragen im produktiven SAP System vermieden und Fehlersituationen stattdessen im Test- beziehungsweise Akzeptanzsystem untersucht?
- Werden im SAP System die Zugriffsberechtigungen auf ICF-Dienste restriktiv vergeben?

# M 5.128 Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Application-Link-Enabling-Schnittstelle (ALE) wird als Kommunikationsmechanismus zur Integration von Geschäftsprozessen über mehrere SAP Systeme oder andere externe Systeme hinweg genutzt. Über die Schnittstelle werden Geschäftsdaten und Systemdaten (z. B. beim Einsatz der Zentralen Benutzerverwaltung) zwischen Sender- und Empfänger-System transportiert. Die Verarbeitung erfolgt in den Empfänger-Systemen automatisiert. Daher muss die ALE-Schnittstelle abgesichert werden. Dabei ist Folgendes zu beachten:

- ALE nutzt das RFC-Protokoll (genauer: transaktionaler RFC, tRFC) zur Datenübertragung. Daher sind alle RFC-spezifischen Sicherheitsmaßnahmen umzusetzen (siehe M 5.126 *Absicherung der SAP RFC-Schnittstelle*).
- ALE-Destinationen im Sender-System sind zu schützen, da hier Authentisierungsinformationen hinterlegt werden müssen (siehe M 4.263 *Absicherung von SAP Destinationen*).
- ALE-Berechtigungen im Empfänger-System sind restriktiv zu vergeben (siehe auch M 4.261 *Sicherer Umgang mit kritischen SAP Berechtigungen*).
- ALE-Administrationsberechtigungen dürfen nur den berechtigten Administratoren zugeordnet werden.
- Für die Benutzerkennungen, die in Sender-Systemen für ALE-Destinationen eingetragen sind, dürfen im Empfänger-System keinen ALE-Administrationsberechtigungen bestehen.
- Benutzerkennungen, die in Sender-Systemen für ALE-Destinationen eingetragen sind, müssen im Empfänger-System vom Typ "Kommunikation" sein.
- Normale Benutzer dürfen keine ALE-Berechtigungen besitzen.
- Für externe Nicht-SAP Systeme müssen die zum Zugriff auf die ALE-Schnittstelle genutzten Authentisierungsinformationen geschützt abgelegt sein. Die Informationen sollten nur für die Systemkomponenten oder ALE-Administratoren zugreifbar sein.

Hinweise auf weitere Informationen zur Absicherung der ALE-Schnittstelle finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Ist die ALE-Schnittstelle im SAP System abgesichert?
- Sind im SAP System nur den berechtigten Administratoren die ALE-Administrationsberechtigungen zugeordnet?
- Bei Zugriff auf die ALE-Schnittstelle über Nicht-SAP Systeme: Werden Authentisierungsinformationen geschützt abgelegt?

# M 5.129 Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Über die HTTP-Schnittstelle können unterschiedliche Dienste eines SAP-Systems angesprochen werden. Der Zugriff auf die Funktionen und Applikationen des Java-Stack erfolgt in der Regel über HTTP. Der ABAP-Stack ist über das Internet Connection Framework (ICF) mittels HTTP zugreifbar. Die HTTP-Schnittstelle muss generell sicher konfiguriert sein, so dass einerseits Zugriffe, die schützenswerte Daten übertragen, mit SSL geschützt sind und andererseits nur die benötigten Dienste aktiviert werden.

Die folgenden über HTTP zugreifbaren Schnittstellen sind mit besonderen Risiken verbunden:

- SOAP-Schnittstelle
- WebDAV-Schnittstelle
- Content-Server-Schnittstelle

Folgendes ist zu beachten:

**SOAP-Schnittstelle**

Das Simple Object Access Protocol (SOAP) ist ein Protokoll, über das Web-Dienste angesprochen werden können. Für die SOAP-Schnittstelle eines SAP Systems ist Folgendes zu berücksichtigen:

- Die SOAP-Schnittstelle (ABAP-Stack und Java-Stack) sollte nur authentisiert zugreifbar sein.
- Der SOAP-Zugriff ist über SSL zu schützen.
- Der ABAP-Stack stellt einen SOAP Dienst zum Aufruf von RFC-fähigen Bausteinen (ICF-Pfad: /sap/bc/soap/rfc) zur Verfügung. Ist dieser aktiv, können RFC-Bausteine über HTTP aufgerufen werden. Der Schutz des RFC-Ports eines SAP Systems durch Firewalls wird dadurch umgangen. Daher sollte der Dienst nur mit ausreichenden Sicherheitsvorkehrungen aktiviert werden. Gleiches gilt für den XML-basierten RFC-Dienst (ICF-Pfad: /sap/bc/xrfc).
- Der durch den Java-Stack angebotene Schutz durch WS-Security (Web Service Security, Standardsammlung der Organisationen W3C und OASIS) gilt nur für die in SOAP-Nachrichten übertragenen Daten. Damit ist auf Applikationsebene nicht prüfbar, ob die Daten über eine authentisierte Verbindung übertragen wurden. Authentisierungsdaten sollten daher im Rahmen der Applikation geprüft werden, wenn die Sender-Identität wichtig ist. Dazu müssen die Authentisierungsdaten in den SOAP-Nachrichten enthalten sein. Die Daten sind vor unberechtigter Kenntnisnahme zu schützen.

Generell muss auch die über SOAP angesprochene Applikation durch entsprechende Berechtigungsprüfungen die eigene Sicherheit sicherstellen.

SAP Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

**WebDAV-Schnittstelle**

Das WebDAV-Protokoll (Web-based Distributed Authoring and Versioning) erlaubt einen dateisystemähnlichen Zugriff auf Informationen über das HTTP-Protokoll. Der WebDAV-Zugriff kann durch den ABAP- und den Java-Stack angeboten werden, wenn entsprechende Produkte oder Applikationen zum Einsatz kommen. Für den ABAP-Stack ist dies beispielsweise Knowledge Warehouse (KW, ICF-Pfad: /sap/bc/kw/fs), für den Java-Stack ist dies beispielsweise die Komponente Collaboration Management (CM, SAP Enterprise Portal Komponente).

Da der WebDAV-Zugriff unter Umständen auch auf das lokale Dateisystem erfolgen kann, muss dieses vor unberechtigten Zugriffen geschützt werden. Dabei steht der Schutz der über WebDAV angeboten Daten zwar im Vordergrund, kann ein Angreifer aber so auf das lokale Dateisystem zugreifen, können dadurch weitere Angriffe vorbereitet werden. Daher sollte der Zugriff nur authentisiert und über SSL geschützt erfolgen. Zusätzlich ist immer auf die Vergabe von Berechtigungen zu achten.

**Content-Server-Schnittstelle**

Über die Content-Server-Schnittstelle kann auf Dokument-Archive (Repositories) zugegriffen werden. Ist die Schnittstelle ungeschützt, so können Informationen und Dokumente über verfügbare Repositories abgerufen werden. Folgendes ist zu beachten:

- Die Content-Server-Schnittstelle (ICF-Pfad /sap/bc/contentserver) ist nur zu aktivieren, wenn sie benötigt wird.
- Der Zugriff sollte nur authentisiert und über SSL erfolgen.
- Beim Zugriff auf die Administrationsschnittstelle ist die Passwort-Abfrage zu erzwingen. Dazu ist der Parameter "AdminSecurity" in der Datei ContentServer.ini auf den Wert "1" zu setzen.
- Es ist zu beachten, dass die Administration innerhalb des SAP Systems über die Transaktion CSADMIN (und auch ICF-Einstellungen) und außerhalb des SAP Systems (z. B. ini-Datei) erfolgen muss.

Hinweise auf weitere Dokumentationen finden sich inM 2.346 *Nutzung der SAP Dokumentation*.

Prüffragen:

- Sind im SAP System für die HTTP-Schnittstelle nur die benötigten Dienste aktiviert?
- Ist im SAP System die HTTP-Schnittstelle so konfiguriert, dass schützenswerte Daten mit SSL geschützt übertragen werden?
- Ist im SAP-System der SOAP-Zugriff über SSL geschützt?
- Erfolgt der WebDAV-Zugriff nur authentisiert und über SSL geschützt?
- Ist sichergestellt, dass die Content-Server-Schnittstelle im SAP System nur aktiviert ist, wenn sie benötigt wird?
- Erfolgt im SAP System der Zugriff auf die Content-Server-Schnittstelle nur authentisiert und über SSL?

# M 5.130 Absicherung des SANs durch Segmentierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator

Ein Storage Area Network (SAN) wird in der Regel durch ein dediziertes Speichernetz, häufig als Fibre-Channel (FC-SAN) realisiert, zwischen Speichersystemen und angeschlossenen Servern oder Endgeräten geschaffen. Ein oder mehrere Switches, die miteinander verbunden sind, bilden dabei eine Fabric. An die Switches werden Server angeschlossen, denen Speicher aus den Ressourcen des Speichersystems zugewiesen wird.

Speichersysteme, Server und deren Betriebssysteme können unabhängig voneinander auch mehrfach zugeordnet werden. So werden einerseits verschiedenen Servern unterschiedliche (logische) Speicherressourcen auf einem Speichersystem zugeordnet, andererseits können einem Server mehrere (räumlich getrennte) Speichersysteme zugeordnet werden, um Redundanz für den Server und damit dessen Anwendungen zu erreichen.

Demzufolge ist die Verwaltung und Rechtezuordnung der Speicherressourcen im SAN anzupassen. Es muss dabei sichergestellt werden, dass keine Daten aufgrund eines falschen Zugriffs zerstört werden und dass Server nur mit "ihrem" Ausschnitt der Speichereinheiten im SAN arbeiten. Dies wird erreicht, indem das SAN in logische Segmente (VSANs) eingeteilt wird, sodass nur die Geräte innerhalb eines Segmentes miteinander kommunizieren können.

Die Segmentierung bringt außerdem weitere Vorteile mit sich:

- Speicherkomponenten, die Interoperabilitätsprobleme miteinander aufweisen, können so in getrennten Segmenten eingesetzt werden.
- Wichtige Anwendungen können einzelne Ports und damit eine bestimmte Bandbreite (QoS - Quality of Service) zugewiesen bekommen.
- Zu schützende Daten können damit besser isoliert werden.
- Verbesserung der Skalierbarkeit, da neue Endgeräte nicht auf Anhieb mit allen anderen kommunizieren können.

Um eine sinnvolle Segmentierung sicherzustellen, sollte ein Konzept für die Zuordnung der SAN-Ressourcen erarbeitet werden. Die Informationen zur aktuellen Zuordnung der SAN-Ressourcen müssen stets dokumentiert und im Notfall verfügbar sein. Die aktuelle Ressourcenzuordnung sollte mithilfe der Verwaltungswerkzeuge einfach und übersichtlich erkennbar sein.

**Segmentierung bei FC-SANs**

Die interne Verwaltung und Zuordnung der Geräte in einem FC-SAN erfolgt über World Wide Names (WWNs). Sie entsprechen in gewisser Weise den MAC-Adressen von Ethernet-Netzadaptern.

Die Segmentierung eines FC-SANs erfolgt durch Einteilung in VSANs und in Zonen (Zoning). VSAN und Zoning-Funktionen werden auf den Switch-Komponenten im SAN konfiguriert. Ein VSAN oder eine Zone kann Server, Speichersubsysteme und Switchports als Mitglieder beinhalten.

Die einzelnen Funktionen zur Segmentierung werden nachfolgend näher beschrieben:

**Zoning**

Es wird zwischen Soft- und Hard-Zoning unterschieden. Soft-Zoning (WWN-Zoning) und Hard-Zoning (Port-Zoning) unterscheiden sich hinsichtlich ihrer Angriffsmöglichkeiten und hinsichtlich des Administrationsaufwands, der für eine sichere Konfiguration notwendig ist.

**Soft-Zoning**

SAN-Geräte (HBA-Port, Switchport etc.) haben einen eindeutigen World Wide Name. Beim Soft-Zoning werden Zonen durch die Gruppierung dieser eindeutigen WWNs gebildet. Die Zuordnung von Switchports und SAN-Geräten zu Zonen erfolgt durch einen SAN-internen Namensserver. Wenn sich ein SAN-Gerät an der Fabric anmeldet, teilt der Namensserver nur WWNs von Geräten der gleichen Zone mit.

Administrationsaufwand:

- Die Vorteile des Soft-Zonings liegen im geringeren Administrationsaufwand im Vergleich zum Hard-Zoning. Änderungen des Hardwarestandorts oder der Verkabelung müssen nicht berücksichtigt werden, da sie "mitwandern". Soft-Zoning ist damit insgesamt flexibler und dynamischer einsetzbar, was vor allem in sich ändernden Umgebungen zum Tragen kommt.

Angriffsmöglichkeiten:

- Soft-Zoning ermöglicht es einem Angreifer, mittels WWN-Spoofing Zugang zu einer Kommunikationsgruppe und somit Zugriff auf die für diese WWN freigegebenen Netzressourcen zu erlangen.
- Datenübertragungen zu gültigen WWNs werden nicht verhindert. Manche Betriebssysteme speichern WWNs intern und halten sie in einem Cache vor. Daher kann es vorkommen, dass ein solches System auf Speichergeräte zugreift, die nach Willen des Administrators gar nicht mehr in der Zone enthalten sind.

Das Risiko beim Einsatz von Soft-Zoning sollte, gerade bei besonders schutzbedürftigen Daten, genau analysiert werden und entschieden werden, ob es für die Institution tragbar ist oder nicht.

**Hard-Zoning**

Hard-Zoning wird über die feste Portzuordnung im SAN-Switch selbst realisiert. Der Begriff Hard-Zoning begründet sich durch die feste Zuordnung von physischen Ports zueinander.

Hard-Zoning wird häufig auch als Port-Zoning bezeichnet. Die Segmentierung im SAN wird hergestellt, indem in Routingtabellen auf SAN-Switches Zonen ausschließlich über die Portnummern der Switches gebildet werden. Dadurch sind genau die Geräte, deren Portnummern als eine Zone zusammengestellt sind, Mitglied dieser Zone. Diese statische Zuordnung erzwingt, dass kein Datenverkehr zwischen Ports unterschiedlicher Zonen stattfindet.

Administrationsaufwand:

- Änderungen der Hardwarekonfiguration oder Standortwechsel von SAN-Geräten erfordern eine manuelle Anpassung des Zonings, also der Zuordnungstabellen. Die Umsetzung eines Hard-Zonings ist daher im Vergleich zum Soft-Zoning mit größerem administrativen Aufwand verbunden.

Angriffsmöglichkeiten:

- Hard-Zoning beugt dem WWN-Spoofing vor. Da hier die Kommunikation mithilfe der Ports definiert ist, können Angriffe mittels WWN-Spoofing nicht gelingen.
- Ein echtes Risiko beim Hard-Zoning besteht nur dann, wenn physischer Zugang zum Switch besteht. In der Folge ist der Zugriff auf alle Netzressourcen ermöglicht, die für diesen Port freigegeben sind.

Da der physische Zugang zu Hardware für Unbefugte in der Regel nur schwer zu erlangen ist, wird das erreichbare Sicherheitsniveau durch Hard-Zoning als höher angesehen als das durch Soft-Zoning realisierbare Sicherheitsniveau. Für Informationen mit höherem Schutzbedarf sollte daher Hard-Zoning zum Einsatz kommen. Die erhöhte Sicherheit sollte aber in einer sinnvollen Relation zum höheren Aufwand stehen.

**Kombination von Hard- und Soft-Zoning**

Die Kombination der beschriebenen Zoning-Verfahren erfolgt durch die Bildung von Zonen mittels Gruppierung eindeutiger WWNs bei gleichzeitiger Zuordnung spezifischer Portnummern der Switches zu einer solchen Gruppe. Sie ermöglicht damit die Verhinderung der jeweiligen spezifischen Angriffsmöglichkeiten.

Der damit einhergehende Administrationsaufwand erhöht sich entsprechend gegenüber dem getrennten Einsatz der Zoning-Varianten. Diese Variante wird daher nur bei sehr hohem Schutzbedarf empfohlen bzw. auch für niedrigeren Schutzbedarf, wenn der Aufwand als gerechtfertigt gewertet wird.

**LUN-Binding und -Masking**

Speichersysteme in einem SAN stellen die eingebauten Platten als logische Einheiten zur Verfügung. Diese können über ihre LUN (Logical Unit Number) adressiert werden. Um zu verhindern, dass jeder Rechner, der in einer Zone mit einem Speichersystem stationiert ist, alle logischen oder physischen Platten dieses Systems sieht, werden LUN-Binding und LUN-Masking eingesetzt.

LUN-Binding ordnet die jeweiligen LUNs einer RAID-Gruppe oder einem Festplattenpool zu. Dazu werden Zugriffspfade zwischen adressierbaren Einheiten eines Speicherpools und den Fibre-Channel-Ports der Speichersysteme definiert.

Bei LUN-Masking werden Zugriffstabellen auf dem Plattensubsystem definiert, in denen die eindeutigen WWN-Adressen der zugriffsberechtigten Server registriert sind. Alle anderen (maskierten) Platten sind für den Server unsichtbar.

Auf diese Weise kann auch eine fehlerhafte Konfiguration oder Bedienung eines Rechners mit SAN-Anschluss nur noch Auswirkungen auf die für ihn sichtbar gemachten (maskierten) Platten (LUNs) haben.

Bei der Zuordnung von Ressourcen in Speichernetzen sollte stets eine Kombination aus Zoning, LUN-Binding und LUN-Masking zum Einsatz kommen.

**Virtuelle SANs (VSANs)**

Analog zur Segmentierung von LANs in virtuelle Teilnetze (VLANs) ist auch die Segmentierung eines SANs in VSANs möglich. Dieses Konzept erweitert das Konzept des Zonings und bietet sowohl einen besseren Zugriffsschutz auf

die Daten und Applikationen als auch Schutz vor einer breiteren Wirkung von Störungen, die so auf einen Teil des Netzes begrenzt werden können.

In einem VSAN werden mehrere Ports und damit mehrere Endgeräte einer Fibre-Channel-Fabric zu einer virtuellen Fabric, einem VSAN, zusammengefasst. Somit werden auf ein und derselben physischen Netzinfrastruktur mehrere virtuell getrennte Fabrics eingerichtet. Ein Switch kann dabei mehreren virtuellen SAN-Teilnetzen angehören. Für jedes VSAN werden separate Fabric-Dienste wie Namensserver und Zoning realisiert. VSANs schränken also, über das reine Zoning hinaus, nicht nur die gegenseitige Sichtbarkeit von Endgeräten, sondern auch die gegenseitige Sichtbarkeit der Fabric-Konfigurationen ein.

Zoning findet unabhängig von einer Trennung in VSANs statt. Eine Zone kann sich nicht über mehrere VSANs erstrecken.

Durch Zoning wird der Zugriff und Datenfluss zwischen den Geräten reguliert. VSANs erlauben zusätzlich, alle in einem Teilnetz bereitgestellten Dienste zu isolieren und innerhalb des VSANs "abzukapseln".

Wenn ausschließlich Zoning eingesetzt wird, bildet die gesamte Hardware des Speichernetzes eine "Sicherheitsdomäne". Wenn auf der Netzhardware des Speichernetzes VSANs konfiguriert werden, wird die Hardware logisch in verschiedene "Sicherheitsdomänen" aufgeteilt. Innerhalb dieser Domänen können dann "domäneninterne" Mechanismen wie Zoning (Hard- oder Soft-Zoning) eingesetzt werden.

Beim Einsatz von N-Port-IP-Virtualisierung (NPIV) ist darauf zu achten, dass eine eindeutige Zuordnung des World Wide Port Name (WWPN) zu einem Server erfolgt.

**Segmentierung bei iSCSI**

Die Segmentierung im iSCSI-Speichernetz erfolgt im Speichergerät analog zum Anschluss eines über FC-LUN angeschlossenen Gerätes. Der Unterschied liegt in der Verbindungszuweisung zwischen dem Server und dem Speichergerät.

Der iSCSI-HBA (Host Bus Adapter) wird als "Initiator" und der Port am Speichergerät als "Target" bezeichnet. Über mitgelieferte Managementsoftware werden beide über ihre iSCSI-ID miteinander bekannt gemacht.

Um den Verbindungsaufbau abzusichern und die Authentizität von Initiator (Server) und Target (Festplatten) sicherzustellen, werden intern Sicherheitsprotokolle wie CHAP (Challenge Handshake Authentication Protocol) oder iSNS (Internet Storage Naming Service) verwendet.

Die Zuordnung von LUNs zu den angeschlossenen Servern im Speichersystem erfolgt ähnlich dem LUN-Masking und LUN-Binding mit WWNs auf Basis der iSCSI-Initiator- und Target-ID. Bei Nutzung von iSCSI empfiehlt sich der Einsatz sogenannter Netzadapter mit TCP/IP Offload Engine (I/OAT). Diese entlasten den Server von intensiven Rechenoperationen beim Auspacken der eigentlichen iSCSI-Daten aus den TCP/IP-Paketen.

Prüffragen:

- Existiert ein schriftlich fixiertes Konzept für die Zuordnung von SAN-Ressourcen zu Servern?

- Ist die aktuelle Zoning-Konfiguration dokumentiert und auch in Notfällen verfügbar?
- Ist die aktuelle Ressourcenzuordnung mithilfe von Verwaltungswerkzeugen einfach und übersichtlich erkennbar?
- Wurde anhand der Sicherheitsanforderungen und des Administrationsaufwands entschieden, welche Segmentierung in welchem Szenario zum Einsatz kommt?

# M 5.131 Absicherung von IP-Protokollen unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der TCP/IP-Stack ist nach einer Standardinstallation aktiviert. Die voreingestellten Sicherheitseinstellungen sind ein Kompromiss zwischen Sicherheit auf der einen und Abwärtskompatibilität und Offenheit gegenüber anderen Systemen auf der anderen Seite. Dies ist nur in Einzelfällen und dort auch nur bedingt ausreichend, daher ist zu überlegen, die Basiseinstellung auf ein höheres Sicherheitsniveau anzuheben. Erweitere Einstellungen zur Vorbeugung gegen Denial-of-Service-Attacken finden sich in der Maßnahme M 4.279 *Erweiterte Sicherheitsaspekte für Windows Server 2003*.

Hinweis: Ab Windows Server 2003 mit Service Pack 1 setzt der *Sicherheitskonfigurations-Assistent* (SCW) zur Vorbeugung gegen Denial-of-Service-Attacken (siehe G 4.22 *Software-Schwachstellen oder -Fehler*) einige weitere Einstellungen bei bestimmten Rollen automatisch (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*).

**Kommunikationsprotokolle der Internetprotokoll-Suite**

Einige Protokolle des TCP/IP-Stacks können optional konfiguriert werden. Sie sind in unterschiedlicher Qualität in die Sicherheitsarchitektur des Betriebssystems integriert und bieten zudem häufig keine ausreichende Authentisierung und Integritätssicherung. Nach einer Standardinstallation ist auf einem Windows Server 2003 System kein unsicheres Protokoll konfiguriert. Wird ein optionales Protokoll installiert, müssen Mechanismen zum Schutz der ausgetauschten Informationen (z. B. kryptographische Funktionen, Authentisierungsfunktionen) entsprechend dem Anwendungsbereich und dem Sicherheitsbedarf konfiguriert werden.

In den Hilfsmitteln zum IT-Grundschutz (siehe *Hilfsmittel zum Windows Server 2003*) wird eine Übersicht von Protokollen der Internetprotokollsuite in verschiedenen Bereichen von Windows Server 2003 gegeben. Hier sind Hinweise zum geeigneten Umgang mit diesen Protokollen enthalten.

Besonders großen Einfluss auf die Sicherheit und Stabilität von Windows-Server-2003 Infrastrukturen haben die Protokolle zur IP-Adressenverteilung (DHCP) und zur Namenauflösung (DNS und WINS). Hierfür sind geeignete, nach den jeweiligen Einsatzbereichen differenzierte Konzepte für die gesamte Infrastruktur erforderlich. Eine Orientierung zum Erreichen des erforderlichen Sicherheitsniveaus findet sich in den Hilfsmitteln zum IT-Grundschutz (siehe *DHCP/DNS/WINS als Infrastrukturdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Sonstige Protokollgruppen wie IP-Routing-, Multicast- und *Quality-of-Service*-Protokolle (QoS) kommen zum Einsatz, wenn der Server für spezielle Rollen konfiguriert ist. Ansonsten sollten sie deaktiviert sein. Für einen sicheren Betrieb gilt generell:

- Es ist das am besten geeignete Protokoll auszuwählen, alle anderen Protokolle müssen deaktiviert werden.
- Speziell für Protokolle der Anwendungsschicht ist immer für Integrität und verschlüsselte Authentisierung in einer Windows-Server-2003-Umgebung zu sorgen, möglichst mittels NTLMv2 oder Kerberos.

- Bei höherem Schutzbedarf müssen die Nutzdaten verschlüsselt werden.
- Der Einsatz des gewünschten Protokolls sollte in der Richtlinie für den IT-Verbund und die betroffenen IT-Systeme definiert und entsprechende Sicherheitsanforderungen formuliert werden.
- Der Einsatz von IPSec sollte überlegt werden, wenn ein gewünschtes Protokoll unter Windows Server 2003 den Sicherheitsanforderungen nicht entspricht (siehe M 5.90 *Einsatz von IPSec unter Windows*).

**Dokumentation**

Alle aktiven Netz-Protokolle des Servers sind zu erfassen. Wurde der Server mittels einer Vorlage des SCW konfiguriert, ist die Vorlage für eine Mindestdokumentation ausreichend (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*). Die effektiven Authentisierungs- und Verschlüsselungsmethoden sowie der Einsatzzweck sind für jedes Protokoll zu dokumentieren.

Prüffragen:

- Sind die effektiven Authentisierungs- und Verschlüsselungsmethoden sowie der Einsatzzweck für jedes Protokoll dokumentiert?
- Ist der TCP/IP-Stack des Servers ausreichend gegen DoS-Attacken geschützt?
- Sind keine unsicheren Netz-Protokolle konfiguriert?
- Wurden alle nicht benötigten Netz-Protokolle deaktiviert?
- Ist für die IP-Adressenverteilung (DHCP) und Namenauflösung (DNS und WINS) ein geeignetes Infrastrukturkonzept entwickelt und umgesetzt?
- Sind alle optionalen IP-Protokolle ausreichend abgesichert, z. B. durch Authentisierung und kryptographische Verfahren?

# M 5.132 Sicherer Einsatz von WebDAV unter Windows Server 2003

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Mit Hilfe von Web Distributed Authoring and Versioning (WebDAV) ist es möglich, Dateien eines Windows 2000 Servers/Windows Servers 2003 über eine HTTP-fähige Netzverbindung bereitzustellen. WebDAV ist unter Windows Server 2003 vor allem deshalb eine bessere Alternative zu FTP, weil sie eine geschützte Authentisierung von Windows-Benutzerkonten ermöglicht. Auch einige zusätzlich erhältliche Serverapplikationen bieten eine WebDAV-Schnittstelle, z. B. Microsoft Exchange Server und Windows Sharepoint Services. Geeignete WebDAV-Clients sind der Maßnahme M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* zu entnehmen.

Die Planung des Einsatzes von WebDAV sollte wenigstens folgende Punkte berücksichtigen:

- Auf dem Server werden Internet Information Services (IIS) benötigt.
- Über WebDAV-Freigaben können am Client zwar Dateien direkt auf dem Server bearbeitet werden (die Dateien werden dann automatisch gesperrt), ausführbare Programme können jedoch nicht direkt vom Server gestartet werden. Generell muss die geplante Client-Software erst auf Verträglichkeit mit WebDAV-Verbindungen hin getestet werden.
  Wie exponiert ist der WebDAV-Zugang (Intranet/Extranet/Internet)? Oder wird er nur sporadisch im LAN verwendet, z. B. für administrative Zwecke? Diese Fragen haben Einfluss auf die Sicherheitsanforderungen an den Authentisierungsprozess (z. B. anonym, Basis-Authentisierung über https, Kerberos usw.) und über die Art der Benutzerverwaltung. Auch die Anforderungen an die Absicherung des Servers an sich sind davon betroffen. Ergebnis der Frage kann sein, dass WebDAV mit anonymem Zugriff im Internet veröffentlicht werden soll und eine hohe Besucherzahl erwartet wird. Dann wäre der gesamte Server mit den Maßnahmen für öffentliche Webserver abzusichern (siehe Baustein B 5.10 *Internet Information Server*).
  Ein designbedingter Aspekt hierbei ist, dass bei Windows Server 2003 WebDAV auf demselben Server aktiviert werden muss, der die gewünschten Dateien bereithält. Im Hinblick auf Sicherheits-Gateways und DMZ-Szenarien ist keine Trennung zwischen Dateiserver und WebDAV-Server möglich.
  Ein anderes Ergebnis kann sein, dass gelegentlich ein Administrator auf kurzem Wege eine Softwareimage-Datei von einem Helpdesk-Server der Active-Directory-Domäne herunterladen muss. In diesem Fall könnte der Administrator bedarfsweise eine WebDAV-Freigabe erstellen und sich mittels seines Domänen-Benutzerkontos (Kerberos-Authentisierung) die WebDAV-Freigabe auf einen Laufwerksbuchstaben verbinden. Sofern M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* bereits umgesetzt worden ist, wäre der weitere Aufwand gering.
- Sollen die Daten während der Übertragung verschlüsselt werden? Den einfachsten und zugleich einen sicheren Weg für eine Ende-zu-Ende-Verschlüsselung stellt ein sicherer Kanal mittels HTTPS dar, welcher im IIS konfiguriert wird. Nicht alle WebDAV-Clients unterstützen jedoch HTTPS optimal. Alternativ kann auch die Nutzung von VPN oder IPSec in Betracht gezogen werden, wobei der Aufwand verglichen zum Sicherheitsgewinn

deutlich höher liegt. In jedem Fall ist ein Verfahren zu wählen, mit dem eine Ende-zu-Ende-Verschlüsselung sichergestellt werden kann.
- Wenn kein sicherer Kanal (HTTPS) zur Verschlüsselung verwendet werden kann, dann müssen die geplanten WebDAV-Clients wenigstens Digest-Authentisierung oder die integrierte Windows-Authentisierung (NTLMv2 oder Kerberos) unterstützen. Das trifft auch zu, wenn VPN anstelle von HTTPS verwendet wird. Der Authentisierungsvorgang kann sonst nicht ausreichend geschützt werden.
- Nach einer Standardinstallation von Windows Server 2003 ist der Webclient-Dienst aus Sicherheitsgründen deaktiviert. Es ist zu empfehlen, diese Standardeinstellung zu belassen und am Server darauf zu verzichten. Für den reinen Dateitransfer zu administrativen Zwecken genügt ein HTTP/HTTPS-Browser für den Zugriff auf WebDAV-Freigaben. Für die Authentisierungsmechanismen des HTTP/HTTPS-Browsers und die Verschlüsselung gelten die gleichen Anforderungen wie bei einem WebDAV-Client (die meisten Browser unterstützen die in Punkt 4. genannten Authentisierungsmechanismen).

**Verwenden von Laufwerksbuchstaben und Verschlüsselung**

Windows XP enthält einen WebDAV-Redirector, der eine WebDAV-Freigabe einem Laufwerksbuchstaben zuordnen kann. Dies kann aus Gründen der Kompatibilität zu älteren Programmen nützlich sein. Jedoch funktioniert diese Zuordnung nicht über HTTPS-Verbindungen. Ist die Verwendung von Laufwerksbuchstaben und HTTPS notwendig, müssen hierfür Programme von Drittanbietern in Betracht gezogen werden. Eine unverschlüsselte Verbindung lediglich über HTTP ist nicht zu empfehlen.

Alternativ zu HTTPS ist auch mit EFS eine Verschlüsselung der übertragenen Daten möglich. Die Daten werden auf dem Client verschlüsselt und dann in verschlüsselter Form zum Server übertragen, wo sie auch verschlüsselt abgelegt werden. Diese Möglichkeit beschränkt sich auf Windows 2000/XP und auf eine Dateigröße von bis zu 60 Megabyte. Das Verfahren mit EFS ist in normalen IT-Umgebungen nicht zu empfehlen, da hierbei zusätzliche Risiken entstehen (G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*) und gegebenenfalls weitere Maßnahmen umzusetzen sind (M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*) umzusetzen sind.

Prüffragen:

- Ist der Webclient auf dem Windows Server 2003 deaktiviert, sofern dieser nicht benötigt wird?
- Entspricht der WebDAV-Zugang den Authentisierungs- und Verschlüsselungsrichtlinien der Organisation?
- Sind die Internet Information Services (IIS) auf dem WebDAV-Server der Einsatzumgebung entsprechend sicher konfiguriert?

# M 5.133 Auswahl eines VoIP-Signalisierungsprotokolls

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Beim Einsatz von VoIP werden die Steuerinformationen und die eigentlichen Sprachdaten in der Regel getrennt voneinander, mittels unterschiedlicher Übertragungsprotokolle transportiert. Steuerinformationen, wie beispielsweise der Zustand "besetzt", werden über Signalisierungsprotokolle, zum Beispiel H.323 oder SIP (Session Initiation Protocol), übermittelt. Für die Übertragung der Sprachdaten ist hingegen ein Medientransportprotokoll, in der Regel RTP (Real-Time Transport Protocol), zuständig. Nur bei sehr wenigen Protokollen, wie IAX (InterAsterisk eXchange), erfolgt keine Trennung von Steuer- und Medieninformationen.

Es gibt verschiedene Signalisierungsprotokolle. Da diese Protokolle untereinander nicht kompatibel sind, spielt die Auswahl für den Aufbau eines VoIP-Netzes eine wichtige Rolle. VoIP-Komponenten, die kein gemeinsames Protokoll unterstützen, können ohne ein Gateway nicht miteinander kommunizieren. Der Einsatz eines Gateways, das die Anweisungen von einem Protokoll in ein anderes übersetzt, ist sehr aufwendig und umständlich. Daher ist darauf zu achten, dass möglichst nur ein Signalisierungsprotokoll eingesetzt wird.

Die Auswahl der eingesetzten VoIP-Komponenten beeinflusst stark die Auswahl des Signalisierungsprotokolls, da viele VoIP-Komponenten nur ein bestimmtes Signalisierungsprotokoll unterstützen. Bezüglich der Sicherheit spielen die Unterschiede zwischen den Protokollen nur eine geringe Rolle. Es sollte dokumentiert werden, welches Signalisierungsprotokoll ausgewählt wurde.

Im Folgenden werden die verbreiteten Signalisierungsprotokolle H.323 und SIP betrachtet. Neben diesen Protokollen werden auch jeweils alle Arten von VoIP-Komponenten, die für einen Gesprächsaufbau mindestens benötigt werden, vorgestellt.

**H.323**

Die Protokollgruppe um H.323 beschreibt die Übertragung von Echtzeitinformationen (Video, Audio, Daten) in paketorientierten Transportnetzen. H.323 wurde ursprünglich als Umsetzung des ISDN D-Kanal Protokolls Q.931 auf ein IP-basiertes Netz entwickelt. Innerhalb von dieser Protokollgruppe sind die Protokolle H.225.0, H.245 und H.450 und H.235 definiert. H.323 beschreibt den Rahmen der Signalisierungsprotokolle, H.225.0 die eigentliche Signalisierung, H.245 die Kontrolle der Übertragung der Sprachinformationen und H.450 die eigentliche Telefonie-Funktion. Die optionale Unterstützung von H.235 bietet Schutz der Integrität und Vertraulichkeit der Signalisierung. Vertiefende Informationen sind bei der International Telecommunications Union (ITU) zu finden, von der die Protokolle festgelegt wurden. Audio- und Videodaten werden per UDP, Faxdaten per UDP oder TCP übertragen. Vor der Übertragung dieser Echtzeitdaten werden so genannte logische RTP- und RTCP-Kanäle zwischen den Endpunkten (Terminals) aufgebaut.

An einer H.323-Kommunikation können folgende Komponenten beteiligt sein:

- Terminals stellen die Endpunkte einer H.323-Kommunikation beim Benutzer dar. Diese Endgeräte verfügen in der Regel über einen Lautsprecher und ein Mikrofon und bieten dem Benutzer die Möglichkeit, mit einem

anderen Gesprächsteilnehmer eine Verbindung aufzubauen. Eine direkte Verbindung zwischen den Endgeräten ist nur bei bekannter IP-Adresse möglich.
- Gatekeeper werden zur Verwaltung eingesetzt. Da die direkte Verbindungsaufnahme zwischen Terminals nur bei bekannten IP-Adressen möglich ist, agiert ein Gatekeeper als zentrale Steuerkomponente in H.323-Netzen.
- Die Multipoint Control Unit (MCU) ermöglicht Konferenzen, also Gespräche zwischen mehr als zwei Anwendern. In der optionalen MCU laufen sämtliche Medienströme von den Teilnehmern zusammen.
- Gateways realisieren die Übergänge in andere Netze und nehmen dabei die Anpassung der Nutzdaten und der Signalisierungsinformation vor. Beispielsweise vermitteln Gateways zwischen IP- und leitungsvermittelnden Telefonnetzen.

Der größte Nachteil von H.323 ist die Komplexität des Protokolls. Die Vielzahl der verschiedenen Protokolle lässt H.323 sehr unübersichtlich und aufwendig wirken. Diese Komplexität erschwert die Fehlersuche und kann zu Mehrkosten führen. Erschwerend kommt hinzu, dass das im Folgenden vorstellte SIP von vielen Herstellern bei neueren Produkten priorisiert wird.

**Session Initiation Protocol (SIP)**

SIP ist ein textbasierendes Client-Server-Sitzungssignalisierungsprotokoll der IETF (Internet Engineering Task Force), das zur Steuerung des Verbindungsauf- und -abbaus von Multimediadiensten verwendet und in RFC 3261 beschrieben wird. Weitere Funktionalitäten, wie Videokonferenzen, Instant Messaging, verteilte Computerspiele und anderen Applikationen benötigen eine Erweiterung der SIP-Spezifikation. Diese sind in separaten RFCs zu finden. Der Multimedia-Nachrichtenstrom, wie die Sprachinformationen bei einem Telefonat, wird mit RTP gebildet. Die Signalisierung wird in der Praxis oft mit SSL bzw. TLS (Transport Layer Security) oder IPSec geschützt.

Das Adressierungsschema von SIP ähnelt stark dem einer E-Mail-Adresse (sip:benutzername@provider-name.org). Die Lokalisierung erfolg über DNS (Domain Name System). SIP unterstützt Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-IP-Verbindungen. Durch das einfache Klartextdesign der SIP-Pakete und der geringen Komplexität erfährt SIP eine immer größere Verbreitung.

Folgende VoIP-Komponenten können bei einer Kommunikation über SIP beteiligt sein:

- Die Endgeräte (Telefon, Softphone, Gateway) werden als User Agents (UA) bezeichnet. Ein User Agent kann die Rolle eines Clients bzw. eines Servers einnehmen. Der Initiator eines Gesprächs arbeitet als User Agent Server (UAS), der Gerufene als User Agent Client (UAC). Ein SIP-Endsystem beinhaltet immer beide Funktionen.
- Der Location Server liefert bei einer entsprechende Nachfrage die IP-Adresse des gewünschten Gesprächspartners. Dieser kann über den Benutzernamen identifiziert werden.
- Ein Registrar ermöglicht den Benutzern die Anmeldung und Registrierung. Hierfür meldet sich das Endgerät mit einer Kennung (Benutzername, Kennwort) und seiner SIP-Adresse an den Registrar an. Der Registrar gibt die Adresse (IP-Adresse) des Endgeräts dem Location Server bekannt, unter der er öffentlich erreichbar ist. Aufgrund dieser Registrierung kann das Endgerät lokalisiert werden.
- Ein SIP-Proxy nimmt die Rolle eines Vermittlers ein, der die Signalisierungsnachrichten bearbeitet oder weiterleitet. Ein User Agent sendet eine Anfrage an den SIP-Proxy. Der SIP-Proxy interpretiert die Anfrage

und adressiert sie, nach entsprechender Bearbeitung, an den User Agent. Wenn nötig, wird eine Nachricht durch den SIP-Proxy verändert.

Obwohl SIP standardisiert wurde, wird es oft von den Herstellern von VoIP-Komponenten unterschiedlich interpretiert. Diese fehlende Interoperabilität führt dazu, dass nicht alle VoIP-Funktionen bei VoIP-Netzen, an denen Komponenten von verschiedenen Herstellern beteiligt sind, vollständig zur Verfügung stehen. Hiervon ist meist die Authentisierung zwischen den Systemen, die Verschlüsselung und die Bereitstellung von Mehrwertdiensten betroffen. Bei der Beschaffung von VoIP-Komponenten sollte daher deren Interoperabilität mit vorhandenen Komponenten überprüft werden.

Beim Einsatz von SIP in Firewall- bzw. NAT-Umgebungen sind weiterhin einige Besonderheiten zu beachten. Endgeräte, die sich in NAT-Umgebungen befinden, können beispielsweise nur mit hohen Aufwand mit VoIP-Systemen außerhalb der NAT-Umgebung kommunizieren. Weitere Informationen hierzu sind in der Maßnahme M 5.137 *Einsatz von NAT für VoIP* zu finden.

Prüffragen:

- Wird nur ein Signalisierungsprotokoll eingesetzt und die Auswahl dokumentiert?
- Wird darauf geachtet, dass die VoIP-Komponenten das ausgewählte Signalisierungsprotokoll unterstützen?

# M 5.134 Sichere Signalisierung bei VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Weitaus wichtiger als der Schutz der Medienströme ist die Sicherstellung der Integrität und Vertraulichkeit der Signalisierungsinformationen beim Einsatz von VoIP. Eine Möglichkeit hierfür ist der Transport der Signalisierungsinformationen über verschlüsselte VPN-Kanäle. Eine weitere Möglichkeit besteht im Einsatz von Signalisierungsprotokollen, die eigene Schutzmechanismen bereitstellen. Die beiden wichtigsten Protokolle zur VoIP-Signalisierung sind SIP und H.225 (Setup-Signalisierung) sowie H.245 (Aufbau der logischen Kanäle) innerhalb des H.323 Frameworks. Die Sicherheitsmechanismen dieser Signalisierungsprotokolle werden im Folgenden beschrieben.

Neben diesen Protokollen gibt es weitere Signalisierungsprotokolle wie IAX2, das über keine eigenen Sicherheitsmechanismen verfügt. Darüber hinaus existieren spezielle Signalisierungsprotokolle, wie beispielsweise MGCP, zur Steuerung von Media Gateways, die ebenfalls keine eigenen Sicherheitsmechanismen bieten. Die Absicherung dieser Protokolle muss daher im Allgemeinen durch geeignete Sicherheitsmaßnahmen auf der Vermittlungsschicht erfolgen.

**H.235**

Grundsätzlich kann die Signalisierung über das Framework H.323 durch Sicherheitsmechanismen auf der Transport- oder Vermittlungsschicht (beispielsweise SSL bzw. TLS oder IPSec) geschützt werden. Diese vom Signalisierungsprotokoll unabhängigen Mechanismen können für Umgebungen mit erhöhten Sicherheitsanforderungen eingesetzt werden. Im Weiterem kann zusätzlich, auch als einziger Schutz der Signalisierung bei normalem Schutzbedarf, das Protokoll H.235 zum Schutz der Integrität und Vertraulichkeit genutzt werden. Es muss entschieden werden, ob und wie die Signalisierung mit H.323 geschützt werden soll. Die Entscheidung ist zu dokumentieren.

H.235 definiert umfangreiche Sicherheitsmechanismen zum Schutz von H.323-basierter Telefonie. Die spezifizierten Mechanismen umfassen insbesondere den Schutz der Anrufsignalisierung (H.225/Q.931) und des Steuerungskanals (H.245) sowie die Sicherheit des Medienstroms.

H.235 betrachtet alle Systemkomponenten, die Endpunkte eines verschlüsselten H.245 Kontrollkanals oder eines verschlüsselten logischen Kanals sind, als vertrauenswürdige Komponenten, die entsprechend authentisiert werden müssen. Beispiele für vertrauenswürdige und zu authentisierende Systemkomponenten sind Gateways.

Eine der folgenden Arten der Authentisierung sollte ausgewählt werden:

a) Authentisierung mittels symmetrischer Kryptographie und eines gemeinsamen, zuvor ausgetauschten Geheimnisses (beispielsweise eines Passwortes). Als kryptographische Verfahren können entweder symmetrische Verschlüsselungsverfahren oder Keyed-Hash-Funktionen dienen, wobei das gemeinsame Geheimnis jeweils als symmetrischer kryptographischer Schlüssel verwendet oder kryptographisch sicher daraus abgeleitet wird.

b) Authentisierung basierend auf zertifizierten öffentlichen Schlüsseln und signierten Nachrichten.

Jedes dieser Verfahren kann jeweils mit zwei Nachrichten unter Verwendung von Zeitstempeln oder mit drei Nachrichten mit zufälligen Challenges als Challenge-Response-Protokoll implementiert werden.

c) Diffie-Hellman-Schlüsselvereinbarungsprotokoll mit optionaler Authentisierung: In einer ersten Phase führen beide Kommunikationsparteien ein Diffie-Hellman-Schlüsselvereinbarungsprotokoll basierend auf zertifizierten öffentlichen Schlüsseln durch. Der dabei erzeugte gemeinsame symmetrische Schlüssel wird in der optionalen zweiten Authentisierungsphase zur eigentlichen Authentisierung, basierend auf symmetrischer Verschlüsselung, verwendet.

H.235 spezifiziert im Weiterem einen Mechanismus (Media Anti-Spam), über den ein Empfänger von RTP-Paketen effizient überprüfen kann, ob ein RTP-Paket authentisch ist und von einem autorisierten Sender stammt. Dazu wird ein kurzer MAC (Message Authentication Code) über ausgewählte Felder des RTP-Paketes berechnet, den der Empfänger prüft, bevor er mit der eigentlichen Verarbeitung des RTP-Paketes beginnt. Der MAC kann entweder durch einen Verschlüsselungsalgorithmus oder durch eine Keyed-Hash-Funktion berechnet werden. Dieser Mechanismus ist zur Abwehr von DoS-Angriffen durch RTP-Flooding und SPIT auf bekannt gewordenen RTP-Ports gedacht und sollte, wenn möglich, aktiviert werden.

Wird die Kommunikation über H.235 von den VoIP-Gateways nicht unterstützt, so ist dringend zu empfehlen, den Zugriff auf das Gateway auf Basis von IP-Adressen und H.323-Identitäten so weit wie möglich einzuschränken. Dafür empfiehlt sich der Einsatz eines Gatekeepers und die Einschränkung des Zugriffs auf das VoIP-Gateway nur im "Routed Mode". Im Gegensatz zum "Bridged Mode", bei dem der Gatekeeper nur an der Authentisierung und die Registrierung beteiligt ist, findet beim "Routed Mode" die gesamte Signalisierung über den Gatekeeper statt.

**SIP**

Ein grundlegendes Problem in der Absicherung von Signalisierungsprotokollen, wie beispielsweise SIP, besteht darin, dass bei der Signalisierung häufig mehrere Komponenten (Endgeräte und Server) involviert sind, die jeweils Teile der Signalisierungsnachrichten lesen oder sogar verändern müssen. Aus diesem Grund ist eine einfache Anwendung von Ende-zu-Ende Sicherheitsmechanismen nicht möglich, anwendungsspezifische Anpassungen müssen vorgenommen werden.

Der SIP-Standard befürwortet deshalb die Verwendung von Sicherheitsmechanismen auf Schichten unterhalb der Anwendungsschicht. Dabei wird nur jeweils die Kommunikation zwischen den einzelnen SIP-Komponenten (UA, Proxy-, Registrar-, Redirect- und Location-Server) abgesichert, was häufig als "Hop-by-Hop"-Sicherheit bezeichnet wird.

Als weiteres Argument für "Hop-by-Hop"-Sicherheitsmechanismen wird im Standard SIP 2.0 darauf hingewiesen, dass den Servern ohnehin in gewissem Umfang vertraut werden muss. Hier sollte jedoch deutlich zwischen Vertrauen bezüglich Signalisierung und Vertrauen bezüglich des Medientransports, d. h. der Sprachdaten, unterschieden werden. Bei erhöhten Sicherheitsanforderungen sollte deshalb geprüft werden, ob zusätzlich geeignete Ende-zu-Ende-Sicherheitsmechanismen zum Schutz des Medientransports erforderlich sind. Dies betrifft beispielsweise auch den Schlüsselaustausch für SRTP.

Besonders bei erhöhten Sicherheitsanforderungen sollte die Signalisierung mit SIP mit SSL bzw. TLS (Transport Layer Security) geschützt werden. Die SIP-Spezifikation RFC 3261 schreibt vor, dass alle konformen SIP-Server (Proxy-Server, Redirect-Server, Location-Server und Registrar-Server) das TLS-Protokoll mit gegenseitiger Authentisierung sowie Einweg-Authentisierung unterstützen müssen. Die Endgeräte sollten TLS verwenden, um ihre Kommunikation mit Proxy-, Redirect- sowie Registrar-Servern zu schützen.

Prüffragen:

- Ist die Integrität und Vertraulichkeit der Signalisierungsinformationen gewährleistet?
- Bei H.235-Nutzung: Ist dokumentiert wie die Signalisierung geschützt wird?
- Bei H.235-Nutzung: Werden die Authentisierungsdaten verschlüsselt übertragen?
- Falls dasVoIP-Gateway den H.235 Codec nicht unterstützt: Wird der Zugriff auf das VoIP-Gateway durch IP-Adressen und H.323-Identitäten so weit wie möglich eingeschränkt?
- Bei SIP-Nutzung und erhöhte Sicherheitsanforderungen: Werden zusätzlich Ende-zu-Ende-Sicherheitsmechanismen für den Medientransport und die Signalisierung benutzt?

# M 5.135 Sicherer Medientransport mit SRTP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Das Real-Time Transport Protocol (RTP) wird zur Übertragung von Mediendaten der IP-Telefonie und das Real-Time Streaming Protocol (RTSP) zu deren Kontrolle eingesetzt. Beide Protokolle bieten keine eigenen Schutzmechanismen gegen das Abhören und gegen Manipulationen von IP-Telefonaten an. Erweiterungen von RTP/RTCP sind SRTP/SRTCP, die Schutzmechanismen für die Übertragung zur Verfügung stellen. Beim Einsatz von VoIP sollte überlegt werden, die Nutzdaten durch den Einsatz von SRTP/SRTCP zu schützen. Die Entscheidung ist zu dokumentieren.

### Überblick

SRTP kann in VoIP eingesetzt werden, um Vertraulichkeit, Authentizität und Schutz gegen Replay-Angriffe (Wiedereinspielen von Nachrichten) für die Medienübertragung auf Basis von RTP zu erreichen. Es ermöglicht eine sichere Unicast- und Broadcast-Übertragung. Zum Transport werden die RTP/RTCP-Pakete in SRTP/SRTCP-Pakete eingebettet.

### Schlüsselmanagement

Das Protokoll SRTP definiert einen Masterschlüssel und jeweils einen Sitzungsschlüssel für Verschlüsselung und Authentisierung. SRTP enthält keinen eigenen Mechanismus zur Erzeugung und Verwaltung der mindestens 128 Bit langen Masterschlüssel. Dies muss mit anderen Standards, wie z. B. Multimedia Internet Keying (MIKEY) realisiert werden.

Falls SRTP eingesetzt wird, ist festzulegen, in welchen zeitlichen Abständen der Masterschlüssel einerseits und die Sitzungsschlüssel andererseits gewechselt werden.

### Verschlüsselung

Bei der Verwendung von SRTP im Rahmen von VoIP sollte in der Regel das symmetrische Verschlüsselungsverfahren AES-CTR (Advanced Encryption Standard - Counter Mode) aktiviert werden. Es eignet sich sowohl für Ende-zu-Ende- als auch für abschnittsweise ("Hop-by-Hop") Verschlüsselung.

### Authentizität und Integrität

Authentizität und Integrität von RTP-Nachrichten können in SRTP mittels der Funktion HMAC-SHA1 in Kombination mit einem entsprechenden Sitzungsschlüssel gesichert werden. Dabei beträgt die empfohlene Länge der übertragenen Prüfsumme 80 Bit. Demnach muss die 160 Bit lange Prüfsumme aus HMAC-SHA1 auf 80 Bit reduziert werden. Diese Anpassung verringert zwar die Übertragungsgröße von SRTP-Paketen, schwächt aber den Integritätsschutz der Nachrichten. Daher sollte diese Anpassung nur in Ausnahmefällen aktiviert werden. Alternativ können auch Funktionen verwendet werden, die auf anderen anerkannten Hash-Algorithmen basieren. Für die Auswahl ist zu beachten, dass in einigen verbreiteten Hash-Algorithmen kryptographische Schwächen entdeckt wurden (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Die Auswahl der Hash-Funktion ist zu begründen und dokumentieren.

Der gleiche Sicherheitsmechanismus ist auch für SRTCP vorgesehen.

SRTP erlaubt eine schwächere Authentisierung (z. B. 32 Bit) beziehungsweise gar keine Authentisierung von Nachrichten für solche Anwendungen, bei denen es unwahrscheinlich ist, dass der Angreifer eine verschlüsselte Nachricht so manipulieren kann, dass eine spätere Entschlüsselung eine sinnvolle Nachricht liefern wird. Wenn möglich, sollte die schwächere Authentisierung für RTP-Pakete nicht verwendet werden. Für RTCP sollte bei erhöhten Sicherheitsanforderungen der oben beschriebene Schutz mittels HMAC-SHA1-Prüfsumme aktiviert werden.

**Schutz gegen Replay-Angriffe (Wiedereinspielen von Nachrichten)**

SRTP bietet Schutz gegen Replay-Angriffe, bei denen ein Angreifer abgefangene RTP- oder RTCP-Pakete speichert und diese später erneut verschickt, um unter anderem Denial of Service Angriffe durchzuführen. Um das Wiedereinspielen von Nachrichten verhindern zu können, muss ein Integritätsschutz und Nachrichten-Authentisierung vorhanden sein. Der Empfänger von SRTP-Paketen führt dann eine so genannte Replay-Liste, die Kennzahlen von vorher empfangenen authentischen Paketen enthält.

Die maximal mögliche Anzahl der gespeicherten Kennzahlen muss vorher festgelegt werden. Beim Empfang eines neuen Pakets wird diese Liste auf Übereinstimmungen untersucht, und die wiederholten Pakete werden verworfen. Bei IP-Telefonen, die einen geringeren Speicher besitzen, ist die Länge der Replay-Liste ein Sicherheitsparameter, der im Fall von erhöhten Sicherheitsanforderungen berücksichtigt werden sollte. Der Umfang der Replay-Liste ist größtmöglich auszuwählen und die Entscheidung ist zu dokumentieren.

**Schlüsselmanagement mit MIKEY**

MIKEY (Multimedia Internet KEYing) beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln sowie weiteren Sicherheitsparametern zwischen den Teilnehmern. In VoIP kann MIKEY für den Austausch des Masterschlüssels und weiterer Sicherheitsparameter benutzt werden, um eine sichere SRTP-Übertragung zwischen den Endgeräten zu ermöglichen.

MIKEY ist unabhängig vom darunterliegenden Signalisierungsprotokoll, wie H.323 oder SIP. Zudem unterstützt MIKEY einen parallelen Austausch von Schlüsseln und Sicherheitsparametern für unterschiedliche Kommunikationssitzungen und Kommunikationsprotokolle. Demnach ist es möglich, RTP- und RTCP-Verbindungen getrennt voneinander abzusichern. Mit dem Bündelungskonzept von Kommunikationssitzungen erlaubt es MIKEY, einen gemeinsamen Masterschlüssel für mehrere parallele Sitzungen zu benutzen. Somit können z. B. VoIP-Konferenzen effizienter abgesichert werden.

Falls der Einsatz von VoIP mit Hilfe kryptographischer Mechanismen abgesichert werden soll, müssen die von den VoIP-Systemen unterstützten Verfahren für den Schlüsselaustausch in Erfahrung gebracht werden. Von diesen Verfahren ist ein geeignetes Verfahren festzulegen und die getroffene Wahl ist zu dokumentieren.

Prüffragen:

- Sind die Gründe für beziehungsweise gegen den Einsatz von SRTP dokumentiert?

- Bei Einsatz von SRTP: sind die sicherheitsrelevanten Optionen der Implementierung des Protokolls dokumentiert?

# M 5.136 Dienstgüte und Netzmanagement bei VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Das Netzmanagement bildet ein wichtiges Glied in der Kette der Sicherung eines VoIP-Dienstes. Neben dem Schutz vor Angriffen dient das Netzmanagement im Wesentlichen der Verfügbarkeit und der Güte des Dienstes. Risiken, wie beispielsweise ein Ausfall durch Überlastung, können damit verringert werden.

### DiffServ und Class-of-Service nach IEEE 802.1p

Ein wichtiger Ansatz für die Sicherstellung der Dienstgüte in IP-Netzen sind die so genannten Differentiated Services (DiffServ). Beim DiffServ-Ansatz werden einzelne Datenströme nach ihren Anforderungen an die Dienstgüte klassifiziert. Die technische Umsetzung erfolgt über das Feld TOS (Type Of Service) im IP-Header der Datenpakete. Einzelnen Klassen werden bestimmte Werte des TOS-Feldes im IP-Header zugeordnet. Entsprechend dem Wert des TOS-Feldes wird das Datenpaket in den Netzknoten priorisiert behandelt.

Damit die benötigte Dienstgüte in der Sicherungsschicht gewährleistet werden kann, wird die Markierung gemäß DiffServ auf das Feld Class of Service (CoS) im Ethernet-Rahmen abgebildet. Die Verwendung der CoS-Bits ist im IEEE-Standard 802.1p festgelegt. Diese zusätzliche Markierung im Ethernet-Rahmen soll die Weiterleitung der Pakete in Layer-2-Geräten, wie Switches, die den IP-Header (Layer 3) nicht auswerten, beeinflussen.

Beim Einsatz von DiffServ muss sichergestellt werden, dass die Datenpakete mit genau der DiffServ-Klasse markiert werden, die für die jeweilige Kommunikationsart vorgesehen ist. Hierzu gehört auch, dass überprüft wird, ob eine Kommunikationsart zur Reservierung von bevorzugten Ressourcen berechtigt ist und ob die tatsächliche Kennzeichnung der Datenpakete mit der jeweils vorgesehenen Klasse übereinstimmt (Policing).

Unterstützen die VoIP-Netze das Modell der Differentiated Services, so muss dies lückenlos implementiert werden. Fehlt beispielsweise das Policing im DiffServ-Netz, können Anwendungen ihre Datenpakete mit unzulässig hoher Priorität markieren, wodurch eventuell die Sprachströme massive Paketverluste erfahren und Sprachverbindungen nicht mehr möglich sind.

VoIP-Dienste sind in einem DiffServ-Netz aber nicht nur durch mutwillige Eingriffe gefährdet. Eine falsche Dimensionierung der Netzkomponenten kann zur punktuellen Überlastung von Verbindungen oder Netzressourcen (Prozessoren der Router, Firewalls) führen und damit ebenfalls den Dienst zum Erliegen bringen.

### Overprovisioning

Häufig werden beim Einsatz von IP-Telefonie die Markierungen der Datenströme nicht berücksichtigt. Es wird davon ausgegangen, dass moderne lokale Netze sowie WANs ausreichend überdimensioniert sind, um Stauungen in Warteschlangen zu vermeiden. Dieser Ansatz wird als Overprovisioning bezeichnet. Im Fall von Overprovisioning ist ein permanentes Monitoring potentieller Engpässe im Netz notwendig. Dabei bildet nicht zwangsläufig die Datenrate einer Strecke den Flaschenhals einer Verbindung. Es kann genauso

die CPU-Performance eines Routers, die Backplane eines Switches oder die Durchsatzrate einer Firewall sein. Entscheidend ist deshalb ein lückenloses Monitoring der CPU-Last und der Auslastung einzelner Verbindungen in den Netzen sowie periodische Analysen, beispielsweise mit Hilfe von aktiven Messungen der Einweg-Verzögerungen.

Bei der Verwendung des Overprovisioning muss beachtet werden, dass keine festen Garantien der Qualität von Sprachanwendungen gegeben werden können. Vielmehr bauen die Aussagen und Abschätzungen auf Erfahrungswerte aus der Vergangenheit. Das Verhalten der Netze kann sich durch die Einführung neuer Anwendungen, wie beispielsweise Videokonferenzen oder Grid-Computing, gänzlich ändern. Speziell beim Einsatz von Overprovisioning können VoIP-Anwendungen durch das Auftreten großer Datenströme stark beeinträchtigt werden.

**MPLS**

MPLS (Multi Protocol Label Switching) kann in Weitverkehrsnetzen verwendet werden, um Kanäle mit garantierter Bandbreite für Sprachverbindungen vom restlichen Verkehr zu isolieren. Damit kann das Prinzip des Overprovisioning auf einzelne MPLS-Kanäle angewendet werden. Da VoIP-Verkehr weniger Schwankungen der Datenrate als sonstiger IP-Verkehr hat, ist davon auszugehen, dass VoIP-Kanäle stärker gefüllt werden können als Strecken, auf denen VoIP-Verkehr zusammen mit dem restlichen Datenverkehr übertragen wird.

Es ist zu beachten, dass MPLS hauptsächlich Vorteile hinsichtlich der Dienstgüte, jedoch nur einen geringen Schutz von Vertraulichkeit und Integrität der Datenübertragung bieten kann. Die Datenpakete der MPLS-Kanäle werden, ähnlich einem VLAN-Tagging, mit einem zusätzlichen Header versehen und unverschlüsselt mit dem restlichen Verkehr übertragen. Somit können solche Kanäle, ähnlich wie Ethernet-Verkehr, mit einem geeigneten Sniffer an bestimmten Komponenten des Netzes eventuell abgehört und manipuliert werden.

**Traffic Shaping**

Traffic Shaping wird in Gateways zwischen lokalen und Weitverkehrsnetzen eingesetzt, um die Datenrate bestimmter, in der Regel nachrangiger, Verkehrsarten zu drosseln. Beispiele hierfür sind Datenübertragungen, wie FTP-Verbindungen, bei denen zeitliche Verzögerungen toleriert werden können. Die Erfahrung zeigt jedoch, dass diese Maßnahmen relativ leicht umgangen werden können, wenn beim Traffic Shaping ausschließlich die Portnummern der Datenpakete als Kriterium herangezogen werden.

**Resource Reservation Protocol (RSVP)**

Das Resource Reservation Protocol (RSVP) dient einer Ende-zu-Ende-Signalisierung der Dienstgüte für einzelne Datenströme. Ursprünglich wurde RSVP für die Realisierung von so genannten Integrated Services (IntServ) in IP-Netzen konzipiert, das im Gegensatz zu DiffServ eine durchgängige Dienstgüte garantieren kann. Für den Einsatz von RSVP in der ursprünglichen Form müssen alle Vermittlungsknoten, Betriebssysteme sowie Anwendungen das Protokoll beherrschen. Zurzeit ist sowohl die Unterstützung in den Betriebssystemen als auch in den Anwendungen unzureichend oder gar nicht gegeben. Somit kommen RSVP und IntServ für VoIP derzeit nicht in Betracht.

Prüffragen:

- Bei Einsatz eines VoIP-Netzmanagements: Kann die Verfügbarkeit und Qualität des VoIP-Dienstes kontrolliert und verbessert werden?
- Bei Einsatz eines VoIP-Netzmanagements: Können potentielle Sicherheitsvorfälle im Rahmen des VoIP-Dienstes ermittelt und identifiziert werden?

# M 5.137 Einsatz von NAT für VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

NAT (Network Address Translation) ermöglicht das Übersetzen von privaten/internen IP-Adressen in öffentliche/externe IP-Adressen. Bei dieser Adressumwandlung werden durch ein entsprechendes NAT-Gateway private Quell-IP-Adressen und die dazugehörigen privaten Quell-Ports in öffentliche Quell-IP-Adressen mit öffentlichen Quell-Ports übersetzt. Damit das NAT-Gateway Rückpakete bzw. eingehende Pakete, die an die öffentliche IP-Adresse gerichtet sind, an den richtigen internen Host weiterleiten kann, unterhält es eine entsprechende Zuordnungstabelle zwischen öffentlichen IP-Adressen/Ports und privaten IP-Adressen/Ports.

Durch NAT werden im UDP- bzw. TCP-Header des Medienstroms die Quell-IP-Adresse und die Quell-Portnummer modifiziert. Die Angaben über die Quell-IP-Adresse und den Quell-Port im Nachrichtenteil der Signalisierungsnachricht bleiben dagegen unverändert. Als Folge können keine Medienströme an ein VoIP-Telefon, das sich hinter einem NAT-Gateway befindet, gesendet werden. VoIP-Geräte, die sich im Internet befinden, können keinen Medienstrom zu einem VoIP-Telefon senden, das sich hinter einem NAT-Gateway befindet, da die private IP-Adresse nicht ins Internet geroutet wird.

In den folgenden Abschnitten werden Möglichkeiten aufgezeigt, die einen VoIP-Betrieb in einer NAT-Umgebung ermöglichen.

**MIDCOM**

MIDCOM steht für Middlebox Commmunications und ist ein Entwurf der IETF, der eine Lösung für die NAT- und Firewall-Problematik im Zusammenhang mit VoIP bietet. Ein MIDCOM-System besteht aus einer Middlebox und einem Server, der die Middlebox steuert bzw. konfiguriert. Der Steuerungsserver ist ein VoIP-Server (H.323-Gatekeeper, SIP-Proxy, etc.), der sich im Signalisierungspfad befindet und den Austausch der SDP-Daten (Session Description Protocol) verfolgt. Anhand dieser Daten steuert der Server über das MIDCOM-Protokoll die Middlebox (NAT-Gateway, Firewall), die die Zuordnungen in die NAT-Tabelle einträgt und die entsprechenden Ports öffnet. In der folgenden Abbildung ist die MIDCOM-Architektur skizziert.

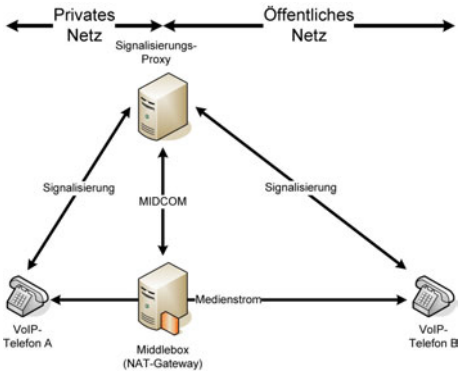



Abbildung: Darstellung der MIDCOM-Architektur

Da der Steuerungsserver selbst mit dem Internet kommunizieren muss, ist dieser Server ebenfalls durch eine Firewall zu schützen. Ein erfolgreicher Angriff auf den Steuerungsserver ermöglicht unter Umständen weitere Angriffe, ins-

besondere auf die von ihm kontrollierte Middlebox (NAT-Gateway, Firewall). Dies kann weitere erhebliche Gefährdungen nach sich ziehen.

**Session Border Controller**

Da sich MIDCOM noch im Entwurfsstadium befindet, haben Hersteller begonnen, proprietäre Lösungen auf den Markt zu bringen, die die NAT- und Firewall-Problematik lösen. Diese Session Border Controller bieten häufig Zusatzfunktionen, wie beispielsweise die Überwachung von Service Level Agreements (SLA), Rufannahmesteuerung (Call Admission Control) und Gebührenermittlung (Billing). Die Systeme werden als Appliances oder Server angeboten. Die folgende Abbildung zeigt ein Beispiel des Einsatzes eines Session Border Controllers, der aus einem Signalisierungs- und einem RTP-Proxy besteht.

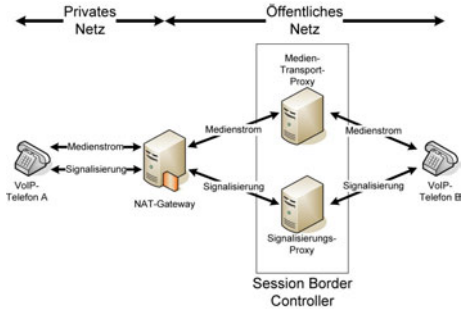



Abbildung: Beispiel für den Einsatz eines Session Border Controllers

Sämtlicher Verkehr (Signalisierung und Medienstrom) läuft in diesem Beispiel über den Session Border Controller. Dem VoIP-Telefon B ist die tatsächliche IP-Adresse des VoIP-Telefons A nicht bekannt.

**UPnP**

UPnP (Universal Plug and Play) ist ein Industriestandard, der vor allem im Heimbereich immer größere Verbreitung findet. Mit der UPnP-Architektur soll die Vernetzung von PCs und Endgeräten (beispielsweise Drucker, Scanner, WLAN Access Points) vereinfacht werden. Durch UPnP können Applikationen die öffentliche IP-Adresse des NAT-Gateways lernen, die zu verwendenden NAT-Zuordnungen vorgeben und nach der Beendigung einer Sitzung wieder entfernen. Es kann auch eine so genannte Lease Time vorgegeben werden, die die Dauer der Gültigkeit einer NAT-Zuordnung festlegt. Werden mehrere NAT-Gateways hintereinander geschaltet, kann mit UPnP kein NAT-Durchgang erzielt werden.

**STUN**

Mit Hilfe von STUN (Simple Traversal of User Datagram Protocol (UDP) Through NATs) wird Endsystemen, die sich hinter einem NAT-Gateway befinden, ermöglicht, ihre öffentliche IP-Adresse zu ermitteln und die NAT-Zuordnung des Gateways zu lernen. Symmetric NAT wird von STUN jedoch nicht unterstützt. Die NAT-Zuordnungen werden bei VoIP im Signalisierungsprotokoll übertragen, so dass eingehende RTP-Ströme an die entsprechende NAT-Zuordnung adressiert werden, um so das VoIP-Telefon zu erreichen, das sich hinter dem NAT-Gateway befindet. Die STUN-Technologie wird bereits von vielen VoIP-Telefonen unterstützt und von den meisten VoIP-Providern angeboten.

**TURN**

TURN (Traversal Using Relay NAT) erlaubt Systemen hinter einem NAT-Gateway bzw. einer Firewall, eingehende TCP- und UDP-Verbindungen zu empfangen. Gleichzeitig wird verhindert, dass diese Möglichkeit für den Betrieb von öffentlich erreichbaren Servern, wie Webserver oder E-Mail-Server, genutzt werden kann, indem je Kombination aus IP-Adresse und Port nur eine Sitzung zu einem Peer erlaubt wird. Im Gegensatz zu STUN können mit TURN auch Systeme hinter symmetrischen NAT-Gateways eingehende Verbindungen empfangen. TURN ist ein einfaches Client/Server-Protokoll, wobei die Authentisierung auf der Basis von Passwörtern erfolgt.

**ICE**

Da bei TURN sämtliche Medienströme über den TURN-Server geführt werden, ist es sinnvoll, einen TURN-Server nur dann einzusetzen, wenn mit STUN der Empfang eingehender Verbindungen nicht möglich ist. ICE (Interactive Connectivity Establishment) stellt eine Methode für SIP dar, um einen NAT-Durchgang auf Grundlage mehrerer über SDP bekannt gegebener Adressen zu ermöglichen, wobei auf die Protokolle STUN, TURN, RSIP und MIDCOM zurückgegriffen wird. Es wird davon ausgegangen, dass einem Client mehrere Adressen (beispielsweise von STUN oder TURN gelernte Adressen) zur Verfügung stehen, über die er Medienströme empfangen kann. Da die Endsysteme nicht wissen, welche Adresse funktioniert, werden die Adressen nacheinander nach ihrer Priorität geprüft, wobei die Adresse mit der höchsten Priorität als erstes getestet wird. Die Prioritäten werden anhand der geringsten Kosten und dem Maximum an QoS (Quality of Service) festgelegt und dann nacheinander innerhalb des SDP aufgeführt. ICE ist für SIP konzipiert, funktioniert jedoch auch mit RTSP und H.323 und ermöglicht, dass ein Endgerät unabhängig von der NAT-Umgebung betrieben werden kann.

Wird das LAN über einen NAT-Gateway an das Internet angeschlossen, ist zu empfehlen, eine der vorgestellten Mechanismen auszuwählen. Die Entscheidung ist zu dokumentieren.

Prüffragen:

- Wird NAT (Network Adress Translation) im Rahmen des VoIP-Betriebs eingesetzt?
- Ist die VoIP-Architektur gemäß der Sicherheitsrichtlinie nach dem Stand der Technik abgesichert?
- Wird die Kommunikation der VoIP-Komponenten über Verfahren und Protokolle nach dem Stand der Technik umgesetzt?

# M 5.138 Einsatz von RADIUS-Servern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In großen Netzen sollten möglichst Authentisierungsserver eingesetzt werden, wie z. B. RADIUS-Server. RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur Authentisierung, Autorisierung und zum Accounting (AAA-System) von Benutzern für die zentralen Absicherung von Verbindungen dient. Das Protokoll ist in mehreren RFCs beschrieben, der wesentliche ist RFC 2865.

Ein Authentisierungsserver soll gewährleisten, dass ausschließlich berechtigte Nutzer auf das interne Netz zugreifen können, der Zugriff kann zusätzlich auf bestimmte Endgeräten eingeschränkt werden. Hierbei findet zunächst eine Identifikation, z. B. anhand einer Kennung, und anschließend die Authentikation, z. B. über ein Passwort, statt. Die Übertragung dieser Daten sollte verschlüsselt erfolgen. Hierbei wird häufig das Protokoll EAP (Extensible Authentication Protocol) genutzt. Die Authentisierung erfolgt bei EAP Port-basiert und beruht auf dem Standard IEEE 802.1X. Dies bedeutet, dass der Zugang zum Netz erst dann erlaubt wird, wenn sich der Client eindeutig am RADIUS-Server identifiziert hat.

Die zum Einsatz kommenden Authentisierungsserver sind geeignet abzusichern (siehe M 4.250 *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*).

Für die Shared Secrets zwischen RADIUS-Server und RADIUS-Client sind ausreichend lange, komplexe kryptographische Schlüssel zu verwenden. Dabei kann, wenn die administrativen Möglichkeiten gegeben sind, für jede RADIUS-Client-Server-Beziehung ein anderes Shared Secret verwendet werden.

Für RADIUS sollten Komponenten eingesetzt werden, die den Anforderungen aus den RFCs zu RADIUS entsprechen, um eine größtmögliche Interoperabilität zwischen den verschiedenen Komponenten sicherzustellen. Die Authentisierungs- und Abrechnungsprotokolle sollten in einem gesonderten Datenbanksystem gespeichert werden können.

Die RADIUS-Kommunikation sollte auf Port 1812 bzw. 1813 beschränkt werden. Die Ports 1645 bzw. 1646 sollten nach Möglichkeit nicht verwendet werden. Andere Ports sind zu schließen, soweit technisch möglich. Die RADIUS-Kommunikation des Servers ist auf die dem Server bekannten und authentischen RADIUS-Clients zu beschränken.

Bei hohem Schutzbedarf hinsichtlich der Vertraulichkeit der Authentisierungsinformationen ist IPSec zur Sicherung der RADIUS-Kommunikation empfehlenswert, wobei jedoch nicht auf die RADIUS-eigenen Verfahren zur Absicherung der Kommunikation verzichtet werden sollte. Ebenso ist hierbei über einen Einsatz eines redundanten RADIUS-Servers nachzudenken.

Die Richtlinien, nach denen ein RADIUS-Server eine Authentisierungsanfrage beantwortet, sollten so restriktiv wie möglich gewählt werden. Hierbei sollten die zulässigen Einwahlzeiten, die MAC-Adresse und der Port-Typ des sich verbindenden RADIUS-Clients, sowie die IP-Adresse des RADIUS-Clients und die EAP-Methode zur Authentikation festgelegt werden.

Prüffragen:

- Existiert beim zentralen, netzbasierten Authentisierungsdienst eine Regelung für Remote Dial-In Verbindungen?
- Sind die Ports zur RADIUS-Kommunikation auf das erforderliche Maß beschränkt (z. B. Port 1812 beziehungsweise 1813)?
- Bei hohem Schutzbedarf an Vertraulichkeit: Wird zusätzlich zu den RADIUS-eigenen Verfahren IPSec zur Absicherung der Kommunikation eingesetzt?
- Bei hoher Verfügbarkeit: ist der RADIUS-Dienst redundant ausgelegt?
- Ist der RADIUS-Dienst auf Seiten des Authentisierungsservers auf autorisierte RADIUS-Clients beschränkt?
- Sind die Richtlinien des RADIUS-Servers zur Annahme von Authentisierungsanfragen möglichst restriktiv gewählt?

# M 5.139 Sichere Anbindung eines WLANs an ein LAN

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Ziel bei der Nutzung von WLAN-Komponenten ist häufig die bequeme und mobile Anbindung an andere Netze. Dies können andere WLANs, aber auch existierende LANs in der eigenen Institution sein. Hierbei sollten zwei Sicherheitsaspekte unterschieden werden:

- der Schutz der benutzten WLAN-Komponenten vor Missbrauch bei der Nutzung fremder Netze und
- der Schutz der internen LANs gegen Missbrauch von außen.

Bei der Anbindung eines WLANs an ein LAN muss der Übergang zwischen WLAN und LAN entsprechend des höheren Schutzbedarfs abgesichert werden. Diesen hat im Allgemeinen das LAN. Bei der WLAN-Kopplung mit einem LAN sind grundsätzlich zwei Ansätze möglich:

- Es kann versucht werden, im WLAN ein Sicherheitsniveau zu erreichen, dass dem innerhalb des vorhandenen drahtgebundenen LANs entspricht. Dazu müssen aber im Allgemeinen die bei Standard-WLAN-Komponenten integrierten Sicherheitsmechanismen erweitert, beispielsweise durch stärkere Kryptoalgorithmen, sowie ein hoher Aufwand für zusätzliche Absicherungen betrieben werden.
- Auf der anderen Seite kann ein pragmatischer Ansatz gewählt werden, bei dem davon ausgegangen wird, dass sowohl die auf der Funkstrecke übertragenen Daten als auch die WLAN-Komponenten nicht dem Sicherheitsniveau des LAN entsprechen. Daher sind Zugriffe aus dem WLAN hierbei wie solche aus dem Internet zu behandeln und somit nur über ein Sicherheitsgateway zuzulassen. Diese Vorgehensweise ist zu empfehlen.

Je höherwertiger die Absicherung auf der Luftschnittstelle und der aktiven Komponenten des Distribution System ist, desto weniger umfangreich müssen die am Übergabepunkt zum LAN zu realisierenden Maßnahmen ausfallen. In jedem Fall muss aber am Übergabepunkt eine vollständige Sperrung der WLAN-Kommunikation ins interne LAN möglich sein, sobald ein Angriff auf das WLAN erkannt wird.

Das Koppelelement zwischen dem Distribution System des WLANs und LAN muss mindestens ein Layer-3-Router sein, um eine effektive Trennung der Broadcast-Domänen zu erreichen. Der Einsatz weitergehender Mechanismen, etwa eines dynamischen Paketfilters anstelle eines Routers, muss je nach Einsatzumgebung und entsprechend des Schutzbedarfs entschieden werden.

Bei höherem Schutzbedarf sollte außerdem die Sicherheit der Authentisierung verbessert werden, beispielsweise durch den Einsatz von EAP-TLS, so dass eine gegenseitige starke Authentikation zwischen den WLAN-Clients und einem Authentikationsserver innerhalb des LANs möglich ist.

Prüffragen:

- Ist am WLAN-Übergabepunkt eine vollständige Sperrung der WLAN-Kommunikation ins interne LAN möglich?
- Wird als Koppelelement zwischen WLAN und LAN mindestens ein Layer-3-Router eingesetzt?

# M 5.140 Aufbau eines Distribution Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein Distribution System ist ein Netz, das Access Points untereinander und mit der weiteren Infrastruktur, wie z. B. einem kabelgebundenen Netz, verbindet. Generell werden zwei Arten von Distribution Systemen unterschieden:

- kabelgebundenes Distribution System:
  Alle Access Points werden untereinander und mit der weiteren Infrastruktur verkabelt.
- Wireless Distribution System:
  Eine direkte Verkabelung zwischen den Access Points ist hierbei nicht mehr notwendig. Allein die Stromversorgung muss für jeden Access Point gewährleistet sein.

In beiden Fällen sollte die Kommunikation zwischen den Access Points stets verschlüsselt statt finden, um die Vertraulichkeit der übermittelten Daten zu gewährleisten. Bei einem kabelgebundenen Distribution System können hierfür beispielsweise IPSec-VPN-Tunnel eingesetzt werden, bei einem Wireless Distribution System nach IEEE 802.11i kann zusätzlich CCMP verwendet werden. Bei einem Wireless Distribution System ist neben dem Schutz der Vertraulichkeit und Integrität aber auch die Verfügbarkeit wesentlich und es sollten Maßnahmen ergriffen werden, um eventuelle Denial-of-Service-Angriffe usw. zu unterbinden. Durch den Einsatz von Wireless Intrusion Detection Systemen und regelmäßige Sicherheitschecks können Schwachstellen schnell gefunden und entsprechende Gegenmaßnahmen eingeleitet werden.

Beim Aufbau eines Distribution Systems muss darüber hinaus die prinzipielle Entscheidung getroffen werden, ob aus Sicherheitsgründen eine eigene Infrastruktur aufgebaut bzw. geschaltet wird, also eine physikalische Segmentierung zur Infrastruktur des internen LANs erfolgt. Als Alternative kann geprüft werden, ob eine logische Segmentierung durch VLANs ausreichend ist.

Wird eine eigene physikalische Infrastruktur für das Distrubtion System eingerichtet, so spielt vor allem die räumliche Ausdehnung des Versorgungsgebietes eine wesentliche Rolle. In der Regel werden mehrere Access Points durch Layer-2- bzw. Layer-3-Switches zusammengefasst, wobei eine Skalierung bei 12, 24 oder 48 Ports je Switch üblich ist. Sollen beispielsweise 100 Access Points miteinander zu einem Distribution System verbunden werden, so sind somit drei bis zehn Switches erforderlich. Eine direkte Verbindung der Access Points an Switches im zentralen Serverraum ist in der Regel nicht möglich, somit müssen die Switches über das gesamte Areal, das mit WLAN ausgestattet werden soll, verteilt werden. Dabei ist zu gewährleisten, dass die Switches ausreichend vor einem externen Zugriff geschützt sind und dass je nach Verfügbarkeit des Distribution Systems für eine Redundanz bei den Switches gesorgt ist. Für den Aufbau einer eigenen physikalischen Infrastruktur sind allerdings größere Investitionen und zusätzliche Sicherheitsmaßnahmen notwendig.

Bei einer logischen Segmentierung werden zur Kontrolle des Datenflusses über die Access Switches des kabelbasierten LANs virtuelle LANs (VLANs) gebildet. Soll eine Segmentierung von WLAN-Clients innerhalb des Distribution Systems erfolgen, muss beim Access Point zusätzlich eine Zuordnung eines WLAN-Clients zu einem VLAN erfolgen. Die Konfiguration eines logischen

Distribution Systems innerhalb einer bestehenden LAN-Infrastruktur ist unter betriebstechnischen und damit unter Verfügbarkeitsaspekten nicht ganz unproblematisch und setzt extrem gut geschulte Administratoren voraus. Solange die gesamte LAN- und WLAN-Infrastruktur nur normal verfügbar sein soll, ist die Konfiguration von VLANs ein gangbarer Weg. Sobald allerdings eine höhere Verfügbarkeit angestrebt wird, sind VLANs für ein Distribution System nicht zu empfehlen.

Prüffragen:

- Erfolgt die Kommunikation zwischen den Access Points verschlüsselt?
- Existieren bei einem Wireless Distribution System Maßnahmen zur Unterbindung von Angriffen (z. B. Denial-of-Service)?
- Sind die eingesetzten Maßnahmen zur physikalischen und/oder logischen Netzsegmentierung dokumentiert?

# M 5.141 Regelmäßige Sicherheitschecks in WLANs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es sollte regelmäßig, mindestens monatlich, ein WLAN-Sicherheitscheck durchgeführt werden.

WLANs sollten regelmäßig mit WLAN-Analysatoren und Netz-Sniffern überprüft werden, ob es eventuell Sicherheitslücken wie schwache Passwörtern, mangelhafte Verschlüsselung oder einen aktiven SSID-Broadcast gibt. Aber auch nach unbefugt installierten WLANs sollte gesucht werden.

**Netz-Analyse-Programme**

Zur Überwachung und Analyse von Dienstequalität und Sicherheit sind in WLANs ebenso wie auch in anderen Netzen spezifische Werkzeuge hilfreich. Für einen sicheren Betrieb von WLANs ist die Überprüfung, in wie weit die vorgegebenen Sicherheitsrichtlinien eingehalten werden und wie es um die Verfügbarkeit des WLANs bestellt ist, besonders wichtig. Zu letzterem gehören auch Messungen der Performance und Fehleranalysen. Nützlich sind aber auch Tools, die einen Überblick über alle aktiven WLAN-Teilnehmer, sowie über bisher erkannte Netzteilnehmer geben.

Netz-Analyse- oder Sniffer-Programme lesen Datenströme mit und untersuchen die übermittelten Datenpakete nach verschiedenen, einstellbaren Kriterien. Sie können beispielsweise nach bestimmten Mustern in den Datenpaketen suchen oder Routing-Information auswerten.

Netz-Analyse-Tools sollten regelmäßig eingesetzt werden, um

- nach unautorisierten WLANs innerhalb der Institutionsgrenzen zu suchen,
- regelmäßig zu überprüfen, ob alle notwendigen Sicherheitsmechanismen aktiviert wurden,
- um Funklöcher aufzuspüren und die Signalqualität von Funknetzen auszuwerten.

**Überwachung der WLAN-Infrastruktur**

Zur Überwachung der WLAN-Infrastruktur kann im einfachsten Fall eine Standortaufnahme über einen mit Spezial-Software ausgestatten WLAN-Client als Stichprobe durchgeführt werden, mit dem das Versorgungsgebiet abgelaufen wird. Hierdurch kann der Betrieb von unerlaubt aufgestellten Access Points ermittelt werden.

Eine bessere Kontrolle ist aber bei Einsatz eines WLAN-Management-Systems gegeben, mit dessen Hilfe regelmäßig folgende Aktion durchgeführt werden sollten:

- Erkennung von Fremdgeräten, insbesondere fremder Access Points
- Durchführung von Wireless Site Surveys, also Untersuchungen, um Informationen zu Abdeckung, Datenraten, Bandbreite, QoS usw. über ein WLAN zu erhalten
- Protokollierung von Anmeldezeiten
- Überwachung der Konfiguration von WLAN-Netzelementen

**Einsatz eines Wireless Intrusion Detection Systems**

Bei der Planung eines Access Point-basierten Wireless Intrusion Detection Systems (IDS) sollte zunächst festgelegt werden, ob eine eigene Messinfrastruktur aufgebaut wird oder die im Produktivnetz verwendeten Access Points und WLAN-Clients in bestimmten Intervallen in einen Messmodus geschaltet werden. Wird hierbei keine vollständige Erfassung des zu überwachenden Bereichs realisiert, können Angriffe im WLAN auf Funkebene nicht erkannt werden. Darüber hinaus ist zu berücksichtigen, dass ein Access Point bzw. WLAN-Client im Messbetrieb keine Daten übertragen kann und damit eine Reduktion der Performance und gegebenenfalls der Verfügbarkeit der WLAN-Datenübertragung in Kauf genommen wird. Ebenso bleibt bei der Nutzung der zum Produktivnetz gehörenden Access Points im Scan-Modus immer ein Zeitfenster bestehen, in dem keine Überwachung auf der Luftschnittstelle möglich ist.

In jedem Fall muss beim Einsatz eines Intrusion Detection Systems oder gar eines Intrusion Prevention System (IPS) das normale Kommunikationsverhalten im WLAN ermittelt bzw. auf Basis von Messungen definiert werden (siehe auch M 5.71 *Intrusion Detection und Intrusion Response Systeme*).

**Alarm- und Fehlerbehandlung**

Die WLAN-Administration sollte über eine Alarm- und Fehlerbehandlung verfügen. Hierbei sind folgende Aufgaben durch die Administratoren wahrzunehmen:

- Auswertung und Bewertung von Alarmen, z. B. bei einer Häufung von fehlgeschlagenen Authentisierungsversuchen an einem Access Point
- Auswertung von Statistiken zur Fehlersuche
- Auslösung von Maßnahmen bei einem vermuteten Sicherheitsvorfall
- Anpassung von Schwellwerten zur Alarmauslösung an eine geänderte WLAN-Nutzung

**Penetrationstest**

Im Zuge eines Sicherheitschecks kann ein WLAN auch mit Hilfe von Penetrationstests auf Schwachstellen untersucht werden. Dabei sind alle getroffenen Sicherheitsmaßnahmen genau zu prüfen, ob diese den Angriffen gewachsen sind, gegen die sie wirken sollen. Ein Penetrationstest sollte mindestens halbjährlich, spätestens jedoch jährlich, erfolgen.

**Dokumentation**

Bei der Durchführung des Sicherheitschecks sollten die Administratoren alle Schritte so dokumentieren, dass sie (beispielsweise bei einem Verdacht auf ein kompromittiertes System) nachvollzogen werden können. Die Ergebnisse des Sicherheitschecks müssen dokumentiert werden, Abweichungen vom Soll zustand muss nachgegangen werden.

Prüffragen:

- Finden regelmäßige Überprüfungen hinsichtlich der WLAN-Verfügbarkeit statt?
- Wird mit den durchzuführenden Überprüfungen die Einhaltung der vorgegebenen Sicherheitsrichtlinien kontrolliert?
- Existiert für die Administratoren eine Regelung zur Behandlung von Fehler- und Alarmmeldungen?

- Werden die Ergebnisse von Sicherheitsuntersuchungen nachvollziehbar dokumentiert, mit dem Soll-Zustand abgeglichen und wird Abweichungen nachgegangen?

# M 5.142 Abnahme der IT-Verkabelung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Eine Abnahme darf erst dann erfolgen, wenn alle durchzuführenden Aufgaben abgeschlossen sind, der Ausführende die Maßnahme zur Abnahme gemeldet hat und sich bei den Kontrollen durch den Auftraggeber keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin sollte zeitlich so gewählt werden, dass die Kontrollen zur Abnahme in ausreichender Zeit vorbereitet werden können.

Der Abschluss aller durchzuführenden Aufgaben wird im Allgemeinen durch das Aufmaß dieser Leistungen bestätigt. Neben der korrekten Abrechnung und dem tatsächlichen Umfang der Leistungen sind bei der Abnahme die Aspekte der Informationssicherheit zu kontrollieren.

Als vorbereitende Kontrollen sind nachfolgende Punkte sinnvoll:

- Alle zur Installation gehörenden Dokumentationen sind auf Vollständigkeit und Plausibilität zu überprüfen.
- Vor allem die Messprotokolle sind auf ihre Werte zu überprüfen. Es ist zu empfehlen, besonders auffällige Messergebnisse für eine Nachmessung im Rahmen der Abnahme auszuwählen.

Die Durchführung der Abnahme umfasst folgende Kontrollen und Tätigkeiten:

- Eintragungen in Grundriss-, Lage- und Schrankansichtspläne werden während der Abnahme auf Richtigkeit überprüft.
- Die Lieferung wird auf die richtige Anzahl und die geforderte Qualität kontrolliert.
- Die fachliche Ausführung der Leistungen wird überprüft. Es empfiehlt sich, durch Stichproben z. B. die Installation von Datendosen genau zu kontrollieren, die Einhaltung von Biegeradien und die Verlegung in Trassen zu überprüfen.
- Auffällige Messergebnisse, die bei der Vorbereitung der Abnahme identifiziert wurden, werden nachgemessen.
- Die abgenommenen Anlagenteile, die Mängel und die erforderlichen Nach- und Restarbeiten werden protokolliert.
- Für die Behebung von Mängeln sowie für die Erledigung von Nach- und Restarbeiten werden feste Termine vereinbart, die auch zwingend eingehalten werden müssen.
- Die Garantie und Gewährleistungsfristen werden festgehalten.

Es empfiehlt sich, das Abnahmeprotokoll als Checkliste vorzubereiten. Die Checkliste sollte auch Punkte zu allgemeinen Anforderungen an die Betriebsräume enthalten, welche über den Rahmen der Maßnahme hinausgehen, um den allgemeinen Zustand und die Qualität der Anlagen festzuhalten. Dadurch wird der Betrieb der Anlagen umsichtig unterstützt und Ausfällen vorgebeugt.

Diese Punkte sind nicht relevant für die Abnahme der IT-Verkabelung und werden im Nachgang an die zuständige Stelle weitergeleitet.

Es empfiehlt sich, die Checklisten für die Abnahme so zu gestalten, dass diese bereits die Installation- und Inbetriebnahme dokumentieren sowie die Maßnahmen zur Vorbereitung der Abnahme protokollieren. Die Checklisten sollten sich auf das notwendige Maß beschränken. Daher ist es sinnvoll, die enthaltenen Punkte zu hinterfragen, wo nötig zu ergänzen und um unwesentliche Punkte zu bereinigen.

Das Abnahmeprotokoll ist von den Teilnehmern und Verantwortlichen rechtsverbindlich zu unterzeichnen.

Nach der Abnahme müssen die Mängelbehebung sowie die Nach- und Restarbeiten kontrolliert werden. Soweit dies vertraglich und rechtlich zulässig ist, sollten erst danach die Rechnungen freigegeben werden. Die zusätzlich festgestellten Anmerkungen sind an die betroffenen Fachabteilungen weiterzuleiten.

Prüffragen:

- Wird die IT-Verkabelung nach Abschluss der Installation einem Abnahmeprozess unterzogen, der auch die Aspekte der IT-Sicherheit umfasst?
- Enthält die Abnahmedokumentation Angaben über Zuständigkeiten und Fristen für die Behebung von Mängeln, Nach- und Restarbeiten sowie zu Garantie und Gewährleistungsfristen?
- Existiert ein von den Teilnehmern und Verantwortlichen unterzeichnetes Abnahmeprotokoll zur IT-Verkabelung?

# M 5.143 Laufende Fortschreibung und Revision der Netzdokumentation

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Netze sind einer laufenden Veränderung durch Nachverkabelungen, Umbau und Erweiterungsmaßnahmen bis hin zu Updates und Upgrades von aktiven Netzkomponenten unterworfen. Entsprechend muss die Dokumentation der IT-Verkabelung als ein elementarer Bestandteil einer jeden Veränderung im Netz betrachtet und behandelt werden. Erst nach Abschluss der Dokumentation gilt die Änderungsmaßnahme auch als vollständig erledigt.

Neben der allgemeinen Betriebssicherheit und Nachvollziehbarkeit dient eine konsistente Dokumentation der IT-Verkabelung auch folgenden Zielen:

- kurze Umschaltzeiten bei Netzerweiterungen,
- einfache Fehlereingrenzung und -suche,
- kurze Wiederherstellungszeiten im Fehlerfall,
- Wirtschaftlichkeit von Wartungsverträgen.

Wichtig ist, dass alle von der Änderung betroffenen Dokumentationsbereiche leicht erfasst und angepasst werden können. Eine Dokumentationsrichtlinie vereinfacht den Umgang mit der Dokumentation. Sie sollte die Abläufe, die Dokumentationsbereiche und die Vorgaben beschreiben, beispielsweise auch Namens- und Nummerierungsschemata.

Außerdem sollte geprüft werden, ob der Einsatz eines Dokumentenmanagements für die Netzdokumentation zweckmäßig ist. Ein Dokumentenmanagement kann unter anderem folgende Aspekte bei der Dokumentation erleichtern:

- Dokumentation von Änderungen bereits während der Planungsphase,
- Information aller beteiligten Personen über die Planungen,
- Integration von Freigabeprozessen,
- Archivierung von Altdokumentation.

Verschiedene Software-Werkzeuge können darüber hinaus die Dokumentation der Kabel und der Netzkomponenten inklusive deren Verschaltung unterstützen. Manche dieser Werkzeuge ermöglichen die Kopplung und Integration mit Netzmanagementsystemen. Auch die aktive Überwachung von Patchungen in der passiven Infrastruktur wird unterstützt.

Prüffragen:

- Werden Veränderungen im Netz umgehend in der Dokumentation der IT-Verkabelung erfasst, so dass diese nachvollziehbar auf dem aktuellen Stand ist?

# M 5.144 Rückbau der IT-Verkabelung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter Haustechnik

Wenn IT-Verkabelung endgültig nicht mehr benötigt wird, so ist sie fachgerecht zu entfernen. Während die Tertiärverkabelung oft so lange wie das Gebäude selbst genutzt wird, kommt es im Bereich der Sekundärverkabelung und bei der internen Verkabelung von Serverräumen und Technikräumen häufiger vor, dass die vorhandenen Kabel durch leistungsfähigere ersetzt werden.

Leider werden die alten Kabel bei einer Neuverkabelung in der Praxis oft nicht entfernt, sondern die neuen Kabel werden auf die alten Kabel verlegt. Dies betrifft die Verlegetrassen und besonders auch Doppelböden. Ein solches Vorgehen verschlechtert die Übersichtlichkeit und erhöht die vorhandenen Brandlasten. Zudem kann die Verschlechterung der Luftdurchströmung klimatechnische Probleme nach sich ziehen. Daher empfiehlt es sich, die Trassenbelegung vorausschauend hinsichtlich eines späteren Rückbaus zu planen und die Nachverkabelungen zu kontrollieren. Eine sich daraus ergebende Erweiterung der Trassen ist rechtzeitig zu berücksichtigen. Es ist deshalb eine Übersicht über nicht mehr benötigte Kabel aufzustellen und anhand dieser Dokumentation der Abbau/Ausbau der Kabel zu belegen. Anschliessend muss die Dokumentation, in der der Bestand der IT-Verkabelung aufgeführt ist, aktualisiert werden.

Prüffragen:

- Werden endgültig nicht mehr benötigte Kabel zur Reduzierung der Brandlasten, zur Verbesserung der Übersicht und gegebenenfalls zur Gewährleistung der Kälteversorgung entfernt?
- Existiert eine Übersicht über nicht mehr benötigte Leitungen?

# M 5.145 Sicherer Einsatz von CUPS

**Verantwortlich für Initiierung:** Administrator, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei Unix-Systemen wird häufig das netzfähige Drucksystem Common Unix Printing System (CUPS) verwendet. CUPS ist zu vielen anderen Drucksystemen kompatibel, wie CIFS/SMB (Common Internet File System/ Server Message Block), das Datei- und Druckerfreigaben unter Windows ermöglicht.

Folgende Aspekte, die in der Planung (siehe M 2.397 *Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten*) oder bei der Auswahl (siehe M 4.304 *Verwaltung von Druckern*) festgelegt wurden, müssen für den sicheren Einsatz von CUPS berücksichtigt werden:

**Allgemeine Aspekte**

- Lokaler Betrieb oder zentraler Druckserver
  CUPS kann als verteilte Anwendung (Client auf Arbeitsplatz-PC mit entferntem Server) oder lokal betrieben werden. Entsprechend muss bei der Konfiguration unterschieden werden, ob sich der CUPS-Client und der CUPS-Server auf dem selben IT-System oder auf verschiedenen IT-Systemen befinden. Wenn sie sich auf verschiedenen IT-Systemen befinden, ist die IP-Adresse oder der Rechnername des jeweiligen Servers in der Konfigurationsdatei (*client.conf*) des CUPS-Clients festzulegen. Bei einer lokalen Nutzung muss dort hingegen die Loopback-Adresse (127.0.0.1) oder der Rechnername "localhost" eingetragen werden. Der CUPS-Server muss bei lokaler Nutzung mit Hilfe des Konfigurationseintrages "Listen" in der Datei *cupsd.conf* an die Loopback-Adresse gebunden werden, damit der Dienst nicht aus dem Netz erreichbar ist. Unabhängig davon, ob nur lokale IT-Systeme auf den Drucker zugreifen dürfen, kann CUPS zentral administriert werden. Dienste wie SSH oder der CUPS-Webserver (siehe Abschnitt zur Administration) ermöglichen es weiterhin, Einstellungen über das Netz vorzunehmen.
- Verwaltungs- und Statusinformationen
  Die Clients müssen regelmäßig über die verfügbaren Drucker und deren Status informiert werden. Beim "Broadcasting" sendet der Server in regelmäßigen Abständen unaufgefordert eine Nachricht an alle Druckclients und beim "Polling" ruft der Druckclient die Informationen vom Server ab.
  Soll die Informationsverteilung über die verfügbaren Drucker nicht mit Polling oder Broadcasting, sondern über manuelle Einträge erfolgen, ist dies durch den Eintrag "Browsing" in der *cupsd.conf* auszuschalten ("off"). Soll "Browsing" genutzt werden, ist der Zugriff nur auf die zwingend benötigten Rechner oder, wenn nötig, auf Netze zu beschränken.
- Verschlüsselung
  Wenn die Druckaufträge oder Statusabfragen verschlüsselt übertragen werden sollen, muss ein Protokoll eingesetzt werden, das dies unterstützt. Das bei CUPS voreingestellte Internet Printing Protcol (IPP) kann durch den optionalen Einsatz von TLS/SSL (Transport Layer Security / Secure Sockets Layer) verschlüsselt kommunizieren.
  Für die Verschlüsselung ist in der Konfigurationsdatei des CUPS-Clients (*client.conf*) der Eintrag "Encryption" erforderlich. Es wird empfohlen, diesen Wert möglichst auf "Always" zu setzen. Zusätzlich müssen hierfür TLS/SSL-Zertifikate und kryptographische Schlüssel auf dem CUPS-Server bereitgestellt werden.
- Hochverfügbarkeit

CUPS kann als Bestandteil eines hochverfügbaren Drucksystems betrieben werden. Dies bedarf einer detaillierten Planung der damit verbundenen organisatorischen und technischen Aspekte. Insbesondere muss festgelegt werden, welcher grundlegende Ansatz zur Erreichung des angestrebten Verfügbarkeitsniveaus verfolgt wird, beispielsweise "failover-switching" oder "load-balancing".
Für "failover-switching" müssen in der Konfigurationsdatei *cupsd.conf* so genannte implizite Druckklassen definiert werden (Konfigurationseintrag "ImplicitClasses On"). Vertiefende Informationen zu dieser Technik sind in der Dokumentation von CUPS zu finden.

**Zugriff auf Drucker**

- Benutzerverwaltung
  Auf Druckserver sollten nur berechtigte Benutzer zugreifen können. Die dafür benötigte Rechteverwaltung kann entweder auf dem Druckserver selbst gepflegt werden, oder es kann ein vorhandener Authentisierungsdienst eingebunden werden. Normale Benutzer sollten auf einem Druckserver nur die Drucker-Applikation benutzen können und keinen Zugriff auf die Dateien und Verzeichnisse dieses Servers haben.
  Da in der Regel die Benutzer den Druckserver nur zum Drucken nutzen sollen und sich nicht direkt auf diesem Server anmelden sollen, beispielsweise mit SSH, sollte die Systembenutzergruppe von der Druckerbenutzergruppe getrennt werden. Druckerbenutzer sollten so angelegt werden, dass sie bis auf das Drucken keine weiteren Rechte auf dem Druckserver besitzen. Beispielsweise können mit dem Programmaufruf "lppasswd -a *benutzername*" Druckerbenutzer angelegt werden.
  Die Zuordnung, welche Benutzer auf welche Drucker zugreifen dürfen, kann in der Datei *cupsd.conf* vorgenommen werden. Auch hier gilt der Grundsatz, dass Benutzern möglichst nur die tatsächlich erforderlichen Zugriffsrechte eingeräumt werden sollten.
  Die Einstellung, dass alle Benutzer auf alle Drucker zugreifen dürfen, sollte vermieden werden. Eine Ausnahme in dieser Hinsicht ist der Betrieb von lokalen Druckern. Wenn es nur wenige Druckerbenutzer für ein IT-System gibt und wenn alle Druckerbenutzer ohnehin auch gleichzeitig Systembenutzer sind, brauchen keine separaten Druckerbenutzer angelegt werden.
- Authentisierungsverfahren:
  CUPS unterstützt verschiedene Verfahren zur Authentisierung, wie "HTTP-Basic", "HTTP-Digest" oder Authentisierung anhand von Zertifikaten. Das Authentisierungsverfahren kann über den Eintrag "AuthType" in der Konfigurationsdatei *cupsd.conf* festgelegt werden. Da bei "HTTP-Basic" Benutzernamen und Passwörter im Klartext über ein Netz übertragen werden, sollte dieses Verfahren nicht ohne zusätzliche Sicherheitsvorkehrungen eingesetzt werden. Stattdessen sollten Zertifikate oder "HTTP-Digest" als Authentisierungsmethode verwendet werden.

**Administration**

Die Administration von CUPS darf nur von hierzu autorisierten Personen durchgeführt werden. Diese können in der Sektion "/admin" der Konfigurationsdatei *cupsd.conf* festgelegt werden.

Bei CUPS können zahlreiche Konfigurationseinstellungen über einen mitgelieferten Webserver durchgeführt werden. Die Zugriffsmöglichkeiten auf den Webserver über Netze sind auf das erforderliche Mindestmaß zu beschränken. In der Konfigurationsdatei *cupsd.conf* in der Sektion "/admin" können die Rechner eingetragen werden, die auf den Webserver zugreifen dürfen. Alternativ kann ein lokaler Paketfilter eingesetzt werden, um die Zugriffsmöglichkeiten auf den Webserver zu beschränken.

**Protokollierung**

CUPS bietet vielfältige Möglichkeiten zur Protokollierung von Ereignissen. Viele Aspekte, die in der Maßnahme M 4.302 *Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten* erläutert sind, können durch entsprechende Einträge in der Konfigurationsdatei *cupsd.conf* umgesetzt werden. Der Detaillierungsgrad der Protokolle kann beispielsweise durch den Eintrag "LogLevel" festgelegt werden.

**Archivierung**

CUPS bietet Funktionen zur elektronischen Archivierung von ausgedruckten Dokumenten im Dateisystem des Druckservers. Hierzu dient der Konfigurationseintrag "PreserveJobs" in der Datei *cupsd.conf*. Als Option kann dabei auch die maximale Anzahl der archivierten Dokumente festgelegt werden. Ältere Einträge werden in diesem Fall von neuen Dokumenten überschrieben. Wenn Archive angelegt werden sollen, müssen die archivierten Dokumente durch entsprechende Mechanismen vor unbefugtem Zugriff und vor Datenverlusten geschützt werden. Weitere Hinweise finden sich im Baustein B 1.12 *Archivierung*.

Prüffragen:

- Entspricht die Konfiguration von CUPS den festgelegten Regelungen zum Drucken und Multifunktionsgeräten?
- Wird der administrative Zugriff auf den CUPS-Server beschränkt?
- Können auf den Druckserver nur berechtigte Benutzer zugreifen?

# M 5.146 Netztrennung beim Einsatz von Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Häufig ist es unter wirtschaftlichen oder praktischen Gesichtspunkten nicht zweckmäßig, separate Geräte zum Drucken, Scannen, Kopieren und Fax-Versand/Empfang einzusetzen. Als Alternative sind Multifunktionsgeräte, die auch als All-in-One-Geräte bezeichnet werden, erhältlich, die mehrere oder sogar alle diese Funktionen in einem Gerät unterstützen. Teilweise bieten diese Geräte auch zusätzliche Kommunikationsschnittstellen, beispielsweise für Webzugriffe.

Multifunktionsgeräte haben meist gegenüber Einzelgeräten einen geringeren Administrationsaufwand und benötigen weniger Anschlussleitungen (Energie- und gegebenenfalls auch Datenleitungen). Multifunktionsgeräte können in der Regel entweder direkt oder über ein LAN an Arbeitsplatzrechner angeschlossen werden.

Einige Geräte bieten eine Fax- und DFÜ-Funktionalität, die den Anschluss an ein Telefonnetz voraussetzt, so dass über die Kopplung mit anderen IT-Systemen eine physische Verbindung zwischen dem LAN und dem Telefonnetz entstehen kann. Falls diese Verbindung nicht von einem Sicherheitsgateway kontrolliert wird, sind hierüber unter Umständen unkontrollierte Internet-Zugriffe möglich, so dass beispielsweise Unberechtigte von außen auf das LAN zugreifen könnten. Der unberechtigte Aufbau von Datenverbindungen muss in jedem Fall unterbunden werden.

Eine Ausnahme sind Multifunktionsgeräte mit Fax-Funktionalität, die nicht an ein Telefonnetz angeschlossen werden müssen. Diese Geräte scannen Dokumente ein und senden sie über eine Datenverbindung an einen zentralen Fax-Server, der sich typischerweise ebenfalls im LAN befindet. Erst der Fax-Server, der an das Telefonnetz angeschlossen ist, versendet das Fax an den eigentlichen Empfänger. Beim Einsatz eines Fax-Servers müssen die in Baustein B 5.6 *Faxserver* empfohlenen Maßnahmen umgesetzt werden.

Beim Einsatz von Multifunktionsgeräten, die an ein Telefonnetz angeschlossen werden können, muss zunächst entschieden werden, ob dieser Anschluss tatsächlich erforderlich ist, das heißt, ob die entsprechende Fax- oder DFÜ-Funktionalität benötigt wird. Falls auf den Anschluss an das Telefonnetz verzichtet werden kann, sind nach Möglichkeit folgende Schutzmaßnahmen zu ergreifen:

- Die Fax- bzw. DFÜ-Funktionalität ist auf dem Gerät zu deaktivieren.
- Das Kabel für den Anschluss an das Telefonnetz ist zu entfernen. Keinesfalls darf das Kabel in die Telefondose eingesteckt werden.
- Wenn sich das Gerät an einem frei zugänglichen Ort befindet, sollten möglichst die Telefondosen in dem jeweiligen Raum deaktiviert oder die Schnittstelle zum Telefonnetz aus dem Gerät ausgebaut werden. Ist beides nicht möglich, sollte regelmäßig kontrolliert werden, ob nicht unbefugt die Verbindung zum Telefonnetz hergestellt worden ist.

Wenn die Fax- oder DFÜ-Funktionalität des Multifunktionsgerätes genutzt werden soll, muss sichergestellt sein, dass der hierfür erforderliche Anschluss

an das Telefonnetz nicht zu unkontrollierten Datenverbindungen zwischen dem LAN und Fremdnetzen führen kann. Folgende Ansätze sind möglich:

- Das Multifunktionsgerät wird an einen Stand-Alone-PC angeschlossen, das heißt an einen Rechner, der nicht mit dem LAN verbunden ist. Nachteilig bei diesem Ansatz ist, dass Daten in vielen Fällen mit Hilfe von Datenträgern zwischen dem Stand-Alone-PC und dem LAN transportiert werden müssen.
- Eine Alternative ist, das Multifunktionsgerät oder den Rechner, an den das Multifunktionsgerät angeschlossen ist, mit Hilfe eines zusätzlichen Sicherheitsgateways vom LAN zu trennen. Der Baustein B 3.301 *Sicherheitsgateway (Firewall)* ist zu beachten.
- Eine weitere Alternative ist, das Multifunktionsgerät oder den Rechner, an dem das Multifunktionsgerät angeschlossen ist, in einer DeMilitarisierte Zone (DMZ) eines bestehenden Sicherheitsgateways zu platzieren. Auch in diesem Fall ist der Baustein B 3.301 *Sicherheitsgateway (Firewall)* anzuwenden.

Alle genannten Lösungsansätze müssen systematisch im Sicherheitskonzept berücksichtigt werden und erfordern zusätzliche Sicherheitsmaßnahmen, beispielsweise zum Schutz vor schädlichem Code, wie Computer-Viren oder Trojanischen Pferden.

Prüffragen:

- Kann die Fax- und DFÜ-Funktionalität des Multifunktionsgeräts abgeschaltet werden?
- Werden unkontrollierte Datenverbindungen zwischen dem LAN und Fremdnetzen zuverlässig unterbunden?

# M 5.147 Absicherung der Kommunikation mit Verzeichnisdiensten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Der Datenaustausch zwischen Client und Verzeichnisdienst-Server erfolgt über Netzverbindungen. Je nach Verzeichnisdienst-System und Netzstruktur werden die Kommunikationspakete, die neben Verzeichnisinhalten unter Umständen auch Authentisierungsinformationen enthalten können, ungeschützt übertragen.

Dabei können abhängig vom installiertem Betriebssystem unterschiedliche Netzprotokolle zum Einsatz kommen. In aller Regel erfolgt der Zugriff auf Verzeichnisdienste über das standardisierte Protokoll LDAP, kann aber auch über proprietäre Protokolle geschehen. Der Transport der Daten erfolgt dabei für LDAP ausschließlich über IP-Netze.

Die Benutzer-Authentisierung kann dabei nach Verfahren erfolgen, die keine Authentisierungsdaten direkt über das Netz transportieren. Die Kommunikation zwischen Client und Server wird jedoch nicht grundsätzlich verschlüsselt. Es ist auch die Angelegenheit des eingesetzten Clients, die Verschlüsselung der Kommunikation sicherzustellen.

Soll von außen auf einen Verzeichnisdienst-Server zugegriffen werden, so ist eine entsprechende Absicherung der Kommunikationsverbindung zwischen Client und Server zu realisieren, die die Vertraulichkeit der übertragenen Daten hinreichend schützt. Dies kann z. B. durch Verwendung eines Virtuellen Privaten Netzes (VPN) erreicht werden.

Im Falle einer serviceorientierten Architektur (SOA) sind zum Schutz von Service-Einträgen in einer Service-Registry sämtliche Anfragen an die Registratur auf Gültigkeit des Nutzers (Consumers) zu überprüfen:

- Nutzt der jeweilige Consumer ein gültiges Zertifikat?
- Stimmen die erforderlichen Zugriffsattribute mit der lokalen WS-Policy überein?
- Ist die Anfrage des Consumers in der übermittelten SOAP-Nachricht signiert?

Erst wenn diese Anforderungen erfüllt sind, darf die Service-Registry die Anfrage des Consumers beantworten.

Administratoren haben oft die Möglichkeit, über einen Fernzugang auf das Verzeichnisdienst-System zuzugreifen. Beispiele sind Terminalservices oder Web-basierte Dienste, mit denen über einen Browser auf Daten des Systems zugegriffen werden kann.

Da die im Fernzugriff verfügbaren Daten wesentliche Einblicke in den Aufbau und die Konfiguration einer Verzeichnisdienst-Installation geben, muss auch dieser indirekte Zugang zum Verzeichnisdienst abgesichert werden. Protokolle, die keine ausreichenden Sicherheitseigenschaften mitbringen, sollten - wenn überhaupt - nur innerhalb gesicherter Netze verwendet werden. Wenn auf den Verzeichnisdienst per HTTP zugegriffen werden kann, muss eine Authentisierung von allen Benutzern erzwungen werden, anonyme Zugriffe dürfen über diesen Weg nicht erlaubt werden. Die Übertragung der Au-

thentisierungsdaten sollte außerdem durch TLS/SSL geschützt werden (siehe M 4.310 *Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste*).

Prüffragen:

- Werden Zugriffe auf Daten des Verzeichnisdienstes über Außenverbindungen angemessen abgesichert?
- Wurde definiert, auf welche Systemdaten von welchen Netzen und mit welchen Werkzeugen zugegriffen werden darf?
- Im Falle einer SOA: Ist ein Zugriffsschutz auf Service-Registries realisiert?

# M 5.148 Sichere Anbindung eines externen Netzes mit OpenVPN

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wenn Daten über gemietete Leitungen oder öffentliche Netze, die nicht der Kontrolle der Institution unterstehen, übertragen werden, so müssen diese angemessen geschützt werden. Geschieht dies nicht, könnten die übertragenen Daten abgehört bzw. manipuliert werden. Unter Umständen hat ein Angreifer sogar die Möglichkeit, sich als berechtigter Kommunikationspartner auszugeben oder könnte die VPN-Endpunkte manipulieren. OpenVPN ist eine freie Software unter der GNU GPL (General Public License), welche die Herstellung Virtueller Privater Netze (VPN) über verschlüsselte TLS/SSL-Verbindungen ermöglicht. Grundsätzlich eignet sich OpenVPN für den Aufbau von Site-to-Site-VPNs, End-to-End-VPNs und Remote-Access-VPNs.

OpenVPN greift zur Verschlüsselung auf die Bibliotheken des Programms OpenSSL zu und verwendet wahlweise UDP oder TCP als Transportprotokoll. Der Einsatz von TLS/SSL als Tunnel-Protokoll erlaubt es im Gegensatz zu IPSec nicht, die Informationen in den IP-Headern der Datenpakete zu schützen. Ein Vorteil ist jedoch, dass es bei TLS/SSL nicht die Fülle der auf beiden Seiten abzustimmenden Konfigurationsparameter wie bei IPSec gibt.

**Sicherer Einsatz von OpenVPN**

Da OpenVPN auf TLS/SSL basiert, sind die in M 5.66 *Clientseitige Verwendung von SSL/TLS* gegebenen Empfehlungen zu beachten. Für den sicheren Einsatz von OpenVPN sollte das zugrunde liegende Betriebssystem entsprechend abgesichert und gehärtet werden (z. B. nur unbedingt erforderliche Programmpakete installieren). Die für den Betrieb von OpenVPN benötigten kryptographischen Schlüssel müssen sicher erzeugt, zwischen den Kommunikationspartnern ausgetauscht und verwaltet werden. Weiterhin müssen sichere Authentisierungs und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet werden. Vertiefende Informationen zur Auswahl von Verschlüsselungs- und Authentisierungsverfahren sind in Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* zu finden.

Eine zertifikatsbasierte Authentisierung ist die sicherste Form der Anmeldung. Hierbei besitzen die VPN-Komponenten (z. B. Server und Server beziehungsweise Server und Client) jeweils private und öffentliche Schlüssel. Bei der Verwendung von Zertifikaten muss während des Authentisierungsvorgangs der Status des Zertifikats bei einer PKI überprüft werden. Hierbei muss gewährleistet werden, dass der OpenVPN-Server, nur Verbindungen zulässt, die von einer ihm bekannten Zertifizierungsstelle signiert wurden. Zur Erhöhung der Sicherheit sollte überlegt werden, die Zertifikate der VPN-Benutzer auf eine Chipkarte oder einen anderen sicheren Token auszulagern.

Für die VPN-Server ist es insbesondere wichtig, dass ausschließlich die erforderlichen Dienste auf der äußeren Netzschnittstelle aus dem nicht-vertrauenswürdigen Netz erreichbar sind. Verbindungen dürfen lediglich zu den notwendigen Systemen und Diensten erlaubt werden und außer den erforderlichen Diensten dürfen auf einem VPN-Server keine weiteren aktiv sein.

Um VPN-Server vor Angriffen zu schützen, müssen diese gemäß M 4.224 *Integration von VPN-Komponenten in ein Sicherheitsgateway* in die Sicherheitsinfrastruktur eingegliedert werden.

**Funktionstest des VPNs**

Wie in Maßnahme M 4.319 *Sichere Installation von VPN-Endgeräten* beschrieben, muss jedes VPN vor dem Einsatz im Echtbetrieb entsprechend auf korrekte Funktion (vor allem der Sicherheitsmechanismen) geprüft werden. Dies sollte in einer separaten Testumgebung erfolgen, da es andernfalls nicht auszuschließen ist, dass Daten aus der Produktivumgebung ungeschützt über das Internet gesendet werden. Für den Fall, dass das VPN nicht wie gewünscht funktioniert, bietet die Dokumentation von OpenVPN umfangreiche Hilfestellung.

Prüffragen:

- Ist das IT-System, auf dem OpenVPN betrieben wird, abgesichert und gehärtet?
- Werden beim OpenVPN-Einsatz sichere Authentisierungs und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet?
- Erfüllt das beim OpenVPN-Einsatz gewählte Verfahren zum Schlüsselaustausch die Sicherheitsanforderungen?
- Ist sichergestellt, dass VPN-Verbindungen beim OpenVPN-Einsatz nur zwischen den hierfür vorgesehenen IT-Systemen und Diensten aufgebaut werden können?

# M 5.149 Sichere Anbindung eines externen Netzes mit IPSec

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Internet Protocol Security (IPSec) ist ein Standard, der über eine Reihe von RFCs und Internet-Drafts der IEEE definiert wird. IPSec besteht aus einer Reihe von Protokollen zur Verschlüsselung, Integritätssicherung, Authentisierung und Schlüsselverwaltung bei der IP-Kommunikation. Mittels IPSec können für die Benutzer weitgehend transparente sichere Verbindungen von Rechnersystemen realisiert werden. IPSec wird beispielsweise in Wirtschaft und Verwaltung häufig zur VPN-Implementierung eingesetzt.

In IPSec werden verschiedene Sicherheitsmechanismen beschrieben wie

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

Der Authentication Header ermöglicht eine Authentisierung der übertragenen Daten und soll somit mögliche IP-Spoofing- oder Session-Hijacking-Angriffe wirkungsvoll unterbinden. Encapsulating Security Payload ermöglicht neben der Authentisierung auch eine Verschlüsselung der übertragenen Daten. Da ESP auch ohne Verschlüsselung und somit zur reinen Authentisierung verwendet werden kann, ist der Einsatz von AH nicht weit verbreitet.

Um möglichst flexible Verbindungsvarianten zu erlauben, bietet IPSec die beiden Betriebsarten:

- Transportmodus
- Tunnelmodus

Im Transportmodus wird der IP-Header der Ursprungspakete übernommen und dient dem Routing. Verschlüsselt wird im Transportmodus lediglich der Paket-Inhalt, nicht aber der IP-Header. Dieser Modus eignet sich nur für Kommunikationsverbindungen, bei denen die Tunnelendpunkte gleichzeitig die Kommunikationsendpunkte darstellen, also beispielsweise bei einer direkten Client-Server-Kommunikation. Da die für die Übertragung benötigten Informationen nicht verschlüsselt sind, können die eventuell dazwischen liegenden Router sie direkt verarbeiten.

Im Tunnelmodus wird das ganze Paket einschließlich des IP-Headers verschlüsselt, um auch interne Adressinformationen vor unberechtigtem Zugriff zu schützen. Ein Angreifer kann dadurch nur die Tunnelendpunkte feststellen, nicht aber den gesamten Weg der Verbindung nachvollziehen.

Anhand des jeweiligen Einsatzgebietes muss für das VPN eine passende Betriebsart gewählt werden. Bei Verbindungen von Netzen verschiedener Standorte sollte ESP in Kombination mit dem Tunnelmodus verwendet werden. Bei der Kommunikation zweier Rechner im LAN sollte der Transportmodus gewählt werden.

**Schlüsselverwaltung bei IPSec**

Zur Schlüsselerzeugung und -verteilung nutzt IPSec das Internet Key Exchange Protokoll (IKE). IKE beschreibt, wie Sicherheitsparameter ausgehandelt und gemeinsame Schlüssel ausgetauscht werden. IKE gliedert sich in folgende zwei Phasen:

Phase 1 dient der Aushandlung einer "ISAKMP Security Association", wobei "ISAKMP" für "Internet Security Association and Key Management Protocol" steht. Eine Security Association (SA) beschreibt einen authentisierten, verschlüsselten Kanal und besteht in der Regel aus einem Sicherheitsparameterindex, der Ziel-IP-Adresse und einem Security Protocol Identifier. Die SA kann entweder im Main Mode oder im Aggressive Mode ausgehandelt werden.

Die Modi unterscheiden sich durch die Anzahl der auszutauschenden Nachrichten und die Verschlüsselung der ausgetauschten Daten. Beim Main Mode wird im ersten Schritt von beiden Kommunikationspartnern ein gemeinsamer geheimer Schlüssel nach dem Diffie-Hellman-Schlüsselaustauschverfahren berechnet. Die eigentlichen Authentisierungsdaten werden mit diesem Schlüssel geschützt übertragen. Die Authentisierung kann mit Hilfe einer nur den beiden Gesprächspartnern bekannten Zeichenkette (Pre-Shared-Key, PSK) oder mit Hilfe von Zertifikaten erfolgen. In dieser ersten Phase werden für die Aushandlung im Main Mode sechs Nachrichten benötigt.

Der Aggressive Mode hingegen kommt mit nur drei Nachrichten aus, weil für die Authentisierungsdaten kein eigener Schlüssel ausgehandelt wird. Statt dessen wird aus dem Pre-Shared-Key mit Hilfe einer Hashfunktion eine Prüfsumme gebildet und übertragen.

Es ist für die sichere Anbindung eines externen Netzes mit IPSec ein geeigneter Modus auszuwählen. Der Aggressive Mode bietet zwar Geschwindigkeitsvorteile gegenüber dem Main Mode, sollte aber nur in Ausnahmefälle eingesetzt werden, da er unsicherer ist. Beispielsweise kann durch einen Wörterbuch- oder Brute-Force-Angriff der Pre-Shared-Key aus der Prüfsumme ermittelt werden.

Um die Schwächen des IKE Aggressive Modus beim Gebrauch von Pre-Shared-Keys auszubessern, wird von einigen Herstellern das XAUTH-Verfahren unterstützt. Hierbei wird das IKE-Protokoll erweitert, sodass Mechanismen wie RADIUS und andere eingesetzt werden können.

In Phase 2 werden die SAs und Schlüssel ausgehandelt, mit denen ein Sicherungsprotokoll wie IPSec oder jedes andere Protokoll, das kryptographisches Schlüsselmaterial benötigt, arbeiten soll.

Für eine sichere IPSec-Konfiguration sind folgende Punkte zu beachten:

- Der Schlüsselaustausch muss mit einem sicheren Verfahren mit ausreichender Schlüssellänge durchgeführt werden. Für den Diffie-Hellman-Schlüsselaustausch sollte z. B. eine MODP Gruppe gemäß RFC 3526 mit mindestens 2048 Bit verwendet werden.
- Für die symmetrische Verschlüsselung müssen sichere kryptographische Verfahren mit ausreichender Schlüssellänge (AES-128, AES-256) angewandt werden.
- Es müssen Hash-Algorithmen mit ausreichender Länge (z. B. SHA-256, SHA-384 oder SHA-512) verwendet werden.
- Die Authentisierungsverfahren müssen dem Stand der Technik entsprechen. Es dürfen keine für den vorliegenden Anwendungsfall relevanten Schwachstellen bekannt sein.
- Timeouts der IKE-Phasen 1 und 2 sollten nicht zu groß gewählt werden, beispielsweise höchstens 20 Sekunden für Phase 1 und 15 Sekunden für Phase 2.
- Für Remote-Access-VPNs sollte auf Pre-Shared-Keys (PSKs) als Authentisierungsmethode verzichtet werden, da z. B. die Schlüsselverwaltung hierbei sehr aufwändig ist.

- Falls Pre-Shared-Keys verwendet werden, müssen hierfür sichere Schlüssel gewählt werden, da die Schlüssel sonst mit Hilfe von Wörterbuchattacken ermittelt werden können.
- Es muss sich sowohl der VPN-Client gegenüber dem VPN-Server als auch der VPN-Server gegenüber dem VPN-Client authentisieren.
- Bei Verwendung von Zertifikaten zur Authentisierung muss während jedes Authentisierungsvorgangs der Status des Zertifikats bei der PKI überprüft werden.

Um über nicht-vertrauenswürdige Netze eine geschützte VPN-Datenkommunikation zu führen, müssen die zentralen Server auch aus dem nicht-vertrauenswürdigen Netz erreichbar sein. Zum Schutz vor Angriffen auf das LAN muss dabei die Angriffsfläche minimiert werden. Daher werden an die beteiligten VPN-Server zusätzlich folgende Anforderungen gestellt:

- Neben den Netzdiensten für die IPSec-Kommunikation sollte der VPN-Server keine weiteren Netzdienste anbieten.
- Es sollten möglichst nur die notwendigsten Verbindungen vom VPN-Server ins LAN aufgebaut werden.
- Da es sich bei IPSec um eine sehr komplexe Protokoll-Familie mit mehreren Diensten handelt, sollten nicht benötigte Dienste abgeschaltet werden. Wenn möglich, sollten nur die Dienste IKE, ESP und gegebenenfalls AH freigeschaltet werden.

Welche Dienste angeboten und welche Berechtigungen vergeben werden, sollte nachvollziehbar dokumentiert werden.

Für die kontinuierliche Verbesserung der Sicherheit des VPNs müssen außerdem die in Maßnahme M 4.321 *Sicherer Betrieb eines VPNs* dargestellten Empfehlungen beachtet werden.

Weitere kryptografische Empfehlungen können der aktuell gültigen Fassung der Technichen Richtlinie TR-02102-3 des BSI entnommen werden. Die jeweils aktuelle Version der Technischen Richtlinie finden sie auf den Webseiten des BSI.

Prüffragen:

- Wird IPSec in einer passenden Betriebsart (Mode) eingesetzt?
- Wurden die an das VPN gestellten Sicherheitsanforderungen bei der IPSec-Konfiguration entsprechend umgesetzt?
- Erfüllt das bei der IPSec-Konfiguration gewählte Verfahren zum Schlüsselaustausch die Sicherheitsanforderungen?
- Ist gewährleistet, dass bei IPSec-Nutzung nur ausreichend sichere kryptographische Verfahren zur Verschlüsselung und Authentisierung verwendet werden?
- Sind auf den VPN-Endpunkten nur die Dienste erreichbar, die für die IPSec-Kommunikation tatsächlich erforderlich sind?

# M 5.150 Durchführung von Penetrationstests

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Penetrationstests sind erprobte und geeignete Vorgehen, um die aktuelle Sicherheit von IT-Systemen und IT-Anwendungen festzustellen.

Das BSI setzt hierbei zwei Testmethoden ein, IS-Penetrationstests sowie IS-Webchecks. Der IS-Penetrationstest ist die Vorgehensweise zur Untersuchung des aktuellen Sicherheitsniveaus von IT-Systemen und Netzen. Mittels eines IS-Webchecks wird das aktuelle Sicherheitsniveau des Internetauftritts beziehungsweise von Web-Services einer Institution ermittelt.

Penetrationstests dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund, eines einzelnen IT-Systems oder einer Internetpräsenz abzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen. Für sicherheitskritische Netze und Systeme sollten regelmäßig Penetrationstests erfolgen.

Im Detail werden dabei die installierten Anwendungen (Webanwendung, Mailserver, Web-Service) beziehungsweise die zugrunde liegenden Trägersysteme (Betriebssystem, Datenbank etc.) überprüft.

Typische Ansatzpunkte für einen Penetrationstest sind:

- Netzkoppelelemente (Router, Switches, Gateways),
- Sicherheitsgateway (Paketfilter, Intrusion Detection System, Virenscanner),
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme),
- Telekommunikationsanlagen,
- Webanwendungen (zum Beispiel Internetauftritt, Vorgangsbearbeitung, Webshop),
- Web-Services (zum Beispiel REST-Interface,SOAP-API-,SOA),
- Clients,
- Drahtlose Netze (zum Beispiel WLAN, Bluetooth) und
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen).

Üblicherweise werden Penetrationstests in Blackbox-Tests und Whitebox-Tests unterteilt. Bei einem Blackbox-Test stehen dabei den Penetrationstestern lediglich die Adressinformationen des Zieles zur Verfügung, weitere Informationen werden ihnen nicht mitgeteilt. Mittels der Vorgehensweise "Blackbox-Test" soll damit der Angriff eines typischen Außentäters mit unvollständigen Kenntnissen über das Zielsystem simuliert werden. Dagegen verfügen die Penetrationstester bei einem Whitebox-Test über umfangreiche, für sie notwendige Informationen über die zu testenden Systeme. Dazu gehören beispielsweise Informationen über IP-Adressen, das interne Netz, die eingesetzte Soft- und Hardware. Diese Angaben werden ihnen zuvor vom Auftraggeber mitgeteilt.

Es ist jedoch fraglich, ob die Unterscheidung zwischen den Vorgehensweisen "Blackbox-Test" und "Whitebox-Test" heute noch sinnvoll ist. Beispielsweise besteht bei einem Blackbox-Test aufgrund nicht vorliegender Informationen ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden

zu verursachen. Weiterhin könnten beispielsweise Schwachstellen aufgrund nicht mitgeteilter Informationen übersehen werden.

Zudem besteht die Gefahr, dass im Rahmen eines Blackbox-Tests der Angriff eines informierten Innentäters nicht berücksichtigt wird.

Den Penetrationstestern sollten daher heutzutage alle für die Testdurchführung notwendigen Informationen über die zu testenden Systeme zur Verfügung gestellt werden, um eventuell mit dem Test verbundene Risiken minimieren zu können und eine möglichst vollständige Schwachstellensuche zu ermöglichen.

Die Klassifizierung von Penetrationstests in eine weitestgehend automatisierte Schwachstellensuche ("Vulnerability Scan") sowie eine in großen Teilen manuelle Sicherheitsrevision erscheint daher nach heutigem Kenntnisstand praxisnäher und erfolgsorientierter.

**Personelle und fachliche Anforderungen an einen Dienstleister für Penetrationstests**

Penetrationstests sind anspruchsvolle und diffizile Aufgaben, die auch Auswirkungen auf den IT-Betrieb haben können. Daher sollte hierfür nur hinreichend qualifiziertes und zuverlässiges Personal mit themenübergreifenden Kenntnissen auf folgenden Gebieten eingesetzt werden:

- Administration von Betriebssystemen und Anwendungen
- Netzwerkprotokolle und Auswertung von Netzwerkverkehr
- Sicherheitsprodukte (zum Beispiel Sicherheitsgateways, Intrusion Detection Systeme)
- Programmiersprachen
- Schwachstellenscanner
- Audit- und Administrationssoftware

Werden externe Dienstleister mit der Durchführung von Penetrationstests beauftragt, so sollte darauf geachtet werden, dass ein qualifizierter und vertrauenswürdiger Dienstleister ausgewählt wird (siehe auch M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters*), der entsprechend qualifizierte und zuverlässige Mitarbeiter bereitstellen kann.

Weiterhin sollten Anbieter von Penetrationstests dem Auftraggeber eine strukturierte Methodik zu deren Durchführung vorstellen können, auf deren Basis die jeweilige individuelle Vorgehensweise ausgearbeitet werden kann.

**Strukturierung und Vorgehensweise für einen Penetrationstest**

In einer Vorbereitungsphase müssen zunächst zwischen dem Auftraggeber und dem Auftragnehmer die Ziele sowie der Umfang des Penetrationstests so genau wie möglich festgelegt werden. Der Penetrationstester sollte hierbei dem Auftraggeber eine strukturierte Vorgehensweise, welche zwischen den Parteien abzustimmen ist, vorstellen.

Während des Abstimmungsprozesses sollte beachtet werden, dass unter Umständen Dritte über den geplanten Penetrationstest informiert beziehungsweise daran beteiligt werden müssen.

In der Regel müssen beispielsweise die Personalvertretung und der Datenschutzbeauftragte, häufig auch Externe, wie der Internet Service Provider oder der Webhoster, in das Vorhaben einbezogen werden.

Zwischen dem Auftraggeber und dem Dienstleister sollten bestimmte Voraussetzungen bereits im Vorfeld vereinbart werden. Hierzu zählen insbesondere:

- Vereinbarungen über die Verschwiegenheitspflichten
- Vereinbarungen über den Einsatz von Hard- und Software
- Vereinbarungen über die zu testenden IT-Systeme und IT-Anwendungen
- Festlegung von erlaubten und unerlaubten Aktivitäten der Penetrationstester, um Schäden möglichst zu vermeiden
- Vereinbarungen über den Umgang mit Datenträgern vor, während und nach Abschluss des Penetrationstests, da die Datenträger zum Beispiel sensible Informationen über die Testergebnisse enthalten können
- Festlegungen über den Ort der Durchführung sowie zur Auswertung und Berichterstellung für den Penetrationstest
- Festlegung eines Terminplans einschließlich Wartungsfenster für die Durchführung der Tests
- Detaillierte Vereinbarungen über den Zugang zum Internet beziehungsweise den Anschluss von Testsystemen an das Internet während der Durchführung und der Auswertung von Penetrationstests
- Vereinbarungen über Zuständigkeiten und die Erreichbarkeit von Ansprechpartnern sowie zur Notfallvorsorge

In der sich anschließenden Informationsphase sammeln die Penetrationstester möglichst viele Informationen über das zu testende Objekt. Zur Vorbereitung der Tests werden die gewonnenen Informationen anschließend hinsichtlich potenzieller Schwachstellen ausgewertet.

In der eigentlichen Testphase eines Penetrationstests sollten nach Möglichkeit die Testverfahren vermieden werden, welche ein destruktives Ergebnis für die untersuchten IT-Systeme oder IT-Anwendungen zur Folge haben könnten.

So zielen beispielsweise DoS-Angriffe (Denial of Service) darauf ab, den Zugriff auf einzelne Dienste, Systeme oder Netzsegmente zu unterbinden. Die Feststellung, ob derartige Attacken möglich sind, kann jedoch oftmals im Vorfeld durch eine Systemanalyse geklärt werden, sodass solche Angriffe während eines Penetrationstests überflüssig werden.

Sollen dennoch DoS-Angriffe oder ähnliche destruktive Angriffe im Rahmen eines Penetrationstests durchgeführt werden, sollte dies außerhalb der produktiven Nutzungszeiten des Systems erfolgen. Gegebenenfalls kann ein derartiger Angriff auch anhand eines Testsystems simuliert werden. Diese Vorgehensweisen sollten ausdrücklich vereinbart werden.

Erst danach werden aktive Eindringungsversuche unternommen. Dabei müssen die vereinbarten Wartungsfenster und der Terminplan strikt eingehalten werden. Wenn Änderungen am zeitlichen Ablauf erforderlich sind, muss dies auf jeden Fall mit dem Auftraggeber abgestimmt werden.

Anderenfalls besteht die erhöhte Gefahr, dass auf der Seite des Auftraggebers bestimmte Aktivitäten der Penetrationstester mit echten Angriffen verwechselt werden. Empfehlenswert ist die vollständige Aufzeichnung und Dokumentation des Penetrationstests.

Um möglichst aussagekräftige Ergebnisse zu erhalten, sollte darauf geachtet werden, dass die Penetrationstests unmittelbar an dem zu testenden IT-System sowie unter Umgehung von vorgeschalteten Komponenten wie zum Beispiel Paketfilter, Web Application Firewall durchgeführt werden. Liegen besondere Gründe vor, den Test mit aktiven vorgeschalteten Sicherheitskomponenten durchzuführen, so ist zu beachten, dass dabei eventuell Sicherheits-

probleme in der Anwendung selbst unentdeckt bleiben, weil die vorgelagerten Komponenten die Angriffsversuche im Penetrationstest abfangen. Solche unentdeckten Schwachstellen bilden jedoch ein relevantes Risiko, denn häufig können mit einem abgewandelten Angriff die Schutzsysteme ausgehebelt und die Schwachstellen ausgenutzt werden.

**Typische Angriffstechniken**

*Netzwerk- und Portscanning:* Netzwerk- und Portscanning werden genutzt, um die in einem Netz aktiven IT-Systeme aufzufinden und die dort angebotenen Dienste (Ports) zu identifizieren.

Seitens der IT-Administration werden solche Abfragen dazu genutzt, den aktuellen Status der eingesetzten IT-Systeme abzufragen. Allerdings kann ein Angreifer unter Umständen mit Hilfe dieser Informationen vorhandene Schwachstellen auf den einzelnen IT-Systemen identifizieren und basierend auf diesen Informationen einen Angriff durchführen.

*Ausnutzung mangelhafter Eingabeüberprüfung:* Als Eingabeüberprüfung wird das Verfahren bezeichnet, mit dem die Benutzereingaben (Daten), die einer Anwendung zur weiteren Bearbeitung übergeben werden, vorher gefiltert, bereinigt oder zurückgewiesen werden.

Diese Filterung soll verhindern, dass der Anwendung schädlicher Code übergeben werden kann, dessen Verarbeitung zu einem Fehlverhalten führt wie zum Beispiel der Offenlegung vertraulicher Informationen.

Angriffsmethoden, mit denen ein derartiges Fehlverhalten hervorgerufen werden kann, sind zum Beispiel "Cross-Site Scripting (XSS)", "Cross-Site Request Forgery (XSRF)", "Injection", "Injection", "OS Injection", "Fuzzing" sowie im Bereich von Web-Services "XMLExternal Entity-Angriffe (XEE)" oder sogenannte "XML-Bomben".

Teilweise lassen sich auch Schwachstellen der verwendeten Protokolle und sonstigen Techniken ausnutzen, um Schaden zu bewirken, zum Beispiel mittels Angriffen auf veraltete SSL/TLS-Versionen oder etwa durch "XML Signature Wrapping (XSW)" bei Web-Services.

*Denial-of-Service-Angriffe (DoS):* Diese Angriffe zielen darauf ab, einen oder mehrere der zur Verfügung gestellten Dienste außer Betrieb zu setzen. Dies kann unter anderem mittels einer durch vermehrte Anfragen gesteigerten Last, durch ein massiv erhöhtes Datenaufkommen (zum Beispiel E-Mails), aber auch durch gezieltes Ausnutzen möglicher Softwarefehler durchgeführt werden. Ein bekanntes Beispiel für einen DoS-Angriff ist der "Ping of Death".

*Information Gathering:* Als "Information Gathering" wird die Sammlung aller Informationen bezeichnet, welche im weiteren für einen Angriff nützlich sein könnten. Beispiele für solche Informationen sind etwa das verwendete Nummerierungsschema für Verzeichnisse oder Server oder Erkenntnisse über Web-Service-Schnittstellen, die durch WSDL-Scanning gewonnen werden.

*Social Engineering:* Als "Social Engineering" werden beispielsweise fingierte Anrufe oder sonstige Kontaktaufnahmen mit Personen bezeichnet, die das betrachtete IT-System bedienen. Das Ziel ist meist, dadurch vertrauliche Informationen wie zum Beispiel Passwörter zu erhalten (siehe auch G 5.42 *Social Engineering*).

*War Dialing:* Hierunter wird der automatisierte und systematische Versuch verstanden, Telefonnummern, die in Verbindung mit einem Modem stehen, aus-

zuforschen. Dabei werden die Telefonnummern des Zielsystems angerufen und auf ein antwortendes Modem hin abgeprüft.

*Passwort-Attacken:* Hierbei wird die Sicherheit beziehungsweise Stärke von Passwörtern mittels sogenannter Wörterbuchangriffe, Brute-Force-Attacken oder durch Entschlüsselungsversuche getestet.

*Ausnutzen von Software-Schwachstellen:* Bei diesen Angriffen wird beispielsweise getestet, ob die installierte Software anfällig für bestimmte Exploits ist, fehlerhaft konfiguriert ist, Schwachstellen aufweist oder veraltet ist. Häufig wird auch untersucht, ob etwa bekannte Schwachstellen der Standardinstallation des jeweiligen Produkts im vorliegenden Fall ausgenutzt werden können.

*Kryptographische Angriffe:* Hierbei werden beispielsweise die Stärke und die Implementierung der eingesetzten Verschlüsselungsmechanismen und -protokolle sowie der Schlüsselverwaltung untersucht.

*Infrastruktur-Untersuchungen:* Im Rahmen von Infrastruktur-Untersuchungen werden unter anderem bauliche Sicherungsmaßnahmen, Zutritts- und Schließeinrichtungen, aber auch die Entsorgung von Material durchleuchtet. Eine Variante hiervon ist das sogenannte "Dumpster Diving", also das Suchen nützlicher Unterlagen oder Datenträger im Abfall (zum Beispiel Papierkörbe, Abfallcontainer).

In der Auswertungs- und Berichtsphase werden die Ergebnisse gesammelt, ausgewertet und in Form eines Berichts zusammengestellt. Alle während des Penetrationstests gewonnenen Informationen sind hierbei entsprechend gesichert aufzubewahren. Der Auftraggeber sollte den Auftragnehmer im Vorfeld dazu verpflichten, alle Aufzeichnungen über den Penetrationstest vollumfänglich an den Auftraggeber zu übergeben beziehungsweise zu vernichten.

Der Bericht muss neben einer Auflistung der gefundenen Schwachstellen auch Maßnahmenempfehlungen enthalten, wie mit den entdeckten Schwachstellen umgegangen werden sollte. Empfehlenswert ist hierbei zudem die Erstellung eines Umsetzungsplans für die in dem Bericht aufgeführten Maßnahmenempfehlungen einschließlich einer Priorisierung. Für das Management sollte der Abschlussbericht außerdem eine Zusammenfassung enthalten, in der die wesentlichen Prüfungsergebnisse und ein Überblick über die empfohlene weitere Vorgehensweise dargestellt sind. Der Abschlussbericht muss dem IT-Sicherheitsbeauftragten und den verantwortlichen Führungskräften vorgelegt werden.

Begleitend zu allen Phasen eines Penetrationstests ist eine gemeinsame Dokumentation der einzelnen Vereinbarungen und Ergebnisse durch den Auftraggeber und den Auftragnehmer empfehlenswert.

Prüffragen:

- Wird für Penetrationstests ausschließlich zuverlässiges und qualifiziertes Personal eingesetzt?
- Ist sichergestellt, dass ausschließlich vertrauenswürdige und qualifizierte Dienstleister mit Penetrationstests beauftragt werden?
- Ist sichergestellt, dass die Ergebnisse von Penetrationstests ausreichend geschützt und vertraulich behandelt werden?
- Werden die Abschlussberichte über Penetrationstests dem IT-Sicherheitsbeauftragten und den verantwortlichen Führungskräften vorgelegt?

- Wurden mit allen Auftragnehmern für Penetrationstests vorab detaillierte Vereinbarungen zur Durchführung und Auswertung von Penetrationstests abgeschlossen?
- Wurde im Vorfeld der Penetrationstests das Einverständnis aller zuständigen Stellen eingeholt?
- Wurden die Ansprechpartner und deren Erreichbarkeit für den Zeitraum der Durchführung von Penetrationstests verbindlich festgelegt?

# M 5.151 Sichere Konfiguration des Samba Web Administration Tools

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Beim Samba Web Administration Tool (SWAT) handelt es sich um ein webbasiertes Konfigurationsprogramm, dass seit Version 2.0 fester Bestandteil von Samba ist. Je nach Distribution wird SWAT mit den Samba-Server Paketen mitinstalliert oder als optionale Pakete angeboten. SWAT wird über einen Internet Dämon (zum Beispiel inetd oder xinetd) gestartet und kann nicht als eigener Dämon betrieben zu werden.

Beim Einsatz von SWAT sollte berücksichtigt werden, dass SWAT bei Änderungen die Datei smb.conf komplett neu schreibt. Dabei werden auch alle Kommentarzeilen sowie alle Parameter, deren Werte den Standardwerten entsprechen, gelöscht. Auch die Parameter "include" und "copy" werden entfernt. Der Einsatz von SWAT ist nicht möglich, wenn einer dieser Parameter benötigt wird. Parameterwerte in Anführungszeichen in der smb.conf werden von SWAT nach dem ersten Anführungszeichen (") gelöscht.

### Deaktivieren oder Einschränken des Zugriffs auf SWAT

Wird SWAT nicht zur Administration und Konfiguration des Samba-Servers eingesetzt, so wird empfohlen, SWAT zu deinstallieren. Ist dies nicht möglich, ist der Start von SWAT über den Internet Dämon zu deaktivieren. Im Fall von xinetd wird der Start des SWAT-Dienstes meist über die Datei /etc/xinet.d/swat oder /etc/xinet.d/samba gesteuert. Mit dem Parameter "disable = yes" wird verhindert, dass der Internet Dämon SWAT bei eingehenden Anfragen startet.

Wird SWAT nur zur Administration und Konfiguration eines lokalen Samba-Servers genutzt, muss die Erreichbarkeit von SWAT auf Anfragen des lokalen Rechners begrenzt werden. Das gewährleistet beim Internet Dämon xinetd der Parameter "only_from = localhost" in der entsprechenden Konfigurationsdatei (in der Regel /etc/xinetd.conf).

Wenn SWAT zur Administration und Konfiguration des Samba-Servers von entfernten Rechnern aus eingesetzt wird, sollte überlegt werden, den Zugriff entsprechend einzuschränken. Der Zugriff auf SWAT sollte nur Rechnern erlaubt sein, auf denen er benötigt wird. Wird der Internet Dämon xinetd eingesetzt, kann dies über den Parameter "only_from" in der entsprechenden Konfigurationsdatei erreicht werden (beispielsweise "only_from = 128.138.193.0 128.138.204.0").

### Sichere Übertragung von Anmeldedaten

SWAT darf zur Administration des Samba-Servers nur über vertrauenswürdige Netze eingesetzt werden. Da SWAT das Hypertext Transfer Protocol Secure (HTTPS)-Protokoll nicht unterstützt, werden sämtliche Informationen im Klartext übertragen. Besteht ein hoher Schutzbedarf, wird empfohlen auf SWAT zu verzichten oder die Kommunikation zu verschlüsseln. Möglichkeiten für eine Verschlüsselung wäre ein Virtual Private Network (VPN) oder ein kryptographischer Tunnel.

Im Folgenden ist aufgeführt wie die Kommunikation über einen kryptographischen Tunnel mit Hilfe des Programms "stunnel" (Version 4) realisiert werden kann.

Zuerst muss mittels openssl ein Zertifikat für stunnel generiert werden. Das Kommando dazu lautet wie folgt:

*root# /usr/bin/openssl req -new -x509 -days 365 -nodes *
*config /usr/share/doc/packages/stunnel/stunnel.cnf *
*out /etc/stunnel/stunnel.pem -keyout /etc/stunnel/stunnel.pem*

Es kann sein, dass stunnel das Zertifikat und den Schlüssel an einer anderen Stelle erwartet. Das kann mit dem Kommando stunnel -Version in Erfahrung gebracht werden. Gegebenenfalls muss entweder die stunnel-Konfiguration oder das oben angeführte openssl Kommando angepasst werden. Anschließend muss mit dem Befehl chmod 600 /etc/stunnel/stunnel.pem sichergestellt werden, dass der private Schlüssel und das Zertifikat vor unautorisiertem Zugriff ausreichend geschützt sind. Andernfalls startet stunnel nicht.

Anschließend muss die Konfigurationsdatei /etc/stunnel/swat.conf erstellt werden:

*exec = /usr/sbin/swat*
*execargs = swat*
*Die xinetd Konfigurationsdatei muss folgendermaßen angepasst werden:*
*server swat*
*{*
*socket_type = stream*
*wait = no*
*user = root*
*port = 901*
*server = /usr/sbin/stunnnel*
*server_args = /etc/stunnnel/swat.conf*
*disable = no*
*}*

Nachdem xinetd die neue Konfiguration eingelesen hat, ist SWAT über die URL https://<IP oder DNS-Name des Samba-Servers:901 erreichbar.

**Authentisierungs- und Autorisierungsschema von SWAT**

SWAT benutzt ein sehr einfaches Authentisierungs- und Autorisierungsschema. Die Authentisierung erfolgt über die lokalen Mechanismen des Servers, auf dem SWAT läuft. SWAT akzeptiert jeden Benutzer, der sich auf dem Server erfolgreich authentisieren kann. Jeder Benutzer, der Leserechte im Dateisystem auf die Konfigurationsdatei smb.conf des Samba-Servers hat, kann sich anschließend die Konfiguration ausgeben lassen. Benutzer die zusätzlich Schreibrechte auf die Konfigurationsdatei smb.conf haben, dürfen Veränderungen an der Konfiguration vornehmen.

Sämtliche weitere Operationen, wie den Neustart des Samba-Servers oder das Beenden von Verbindungen zum Samba-Server, kann nur der Benutzer mit der User Identification (UID) Nummer 0. Normalerweise ist das der Benutzer mit der Bezeichnung "root".

Prüffragen:

- Ist den Administratoren bewusst, dass SWAT bei Änderungen die Datei smb.conf komplett neu schreibt?
- Wurde SWAT deinstalliert oder deaktiviert, falls SWAT nicht für die Administration und Konfiguration von Samba verwendet wird?
- Ist die Erreichbarkeit von SWAT auf Anfragen des lokalen Rechners begrenzt, falls SWAT nur zur Administration und Konfiguration eines lokalen Samba-Servers genutzt wird?
- Ist die Erreichbarkeit von SWAT auf Anfragen von vertrauenswürdigen Rechnern begrenzt, falls SWAT zur Administration und Konfiguration von entfernten Rechnern aus benutzt wird?
- Wird SWAT nur über vertrauenswürdige Netze eingesetzt, beziehungsweise wird die Kommunikation verschlüsselt?
- Wird SWAT über eine gesicherte HTTPS-Verbindung eingesetzt?

# M 5.152 Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Als "Peer-to-Peer" (oft auch "P2P" abgekürzt) wird ein Informationsaustausch bezeichnet, der zwischen gleichberechtigten IT-Systemen ("Peers") durchgeführt wird. Jedes IT-System kann hierbei Dienste anbieten oder nutzen. Über die hierfür aufgebaute Kommunikationsverbindung können sich mehrere IT-Systeme Ressourcen dezentral untereinander teilen. Somit werden die typischen Funktionen eines Servers und eines Clients auf einem IT-System vereint.

Oft werden Peer-to-Peer-Anwendungen genutzt, um folgende Dienste anderen Peers bereitzustellen:

- Nutzung von Druckern, die lokal an einem IT-System angeschlossen sind, durch Benutzer an anderen IT-Systemen,
- Zugriff auf Speicherbereiche der im IT-System eingebauten oder lokal angeschlossenen Festplatten ("File-Sharing"),
- Direktkommunikation über Kurzmitteilungen ("Messaging") und
- Internettelefonie.

**Vorteile von Peer-to-Peer-Diensten**

Im Gegensatz zu einer servergestützten Architektur haben Peer-to-Peer-Dienste zahlreiche Vorteile:

- Ein dedizierter Server verursacht in der Anschaffung und im Betrieb zusätzliche Kosten.
- Fällt der zentrale Server aus, stehen die Ressourcen nicht mehr zur Verfügung ("Single Point of Failure"). Fällt bei Peer-to-Peer-Diensten ein Client aus, können im Allgemeinen genügend andere Clients einspringen.
- Geographisch benachbarte Clients können effizienter Informationen direkt untereinander austauschen, als wenn hierfür ein Server benutzt wird, der sich weit entfernt befindet.
- Server benötigen eine höhere Bandbreite, mehr CPU-Leistung und umfangreicheren Festplatten- und Arbeitsspeicher als Clients. Diese Anforderungen können in Peer-to-Peer-Netzen auf die Clients verteilt und dort ungenutzte Ressourcen verwendet werden.
- Freigegebene Informationen liegen oft auf mehreren Clients gleichzeitig und damit redundant vor.

Die Nutzung von Peer-to-Peer-Diensten hat allerdings auch eine Vielzahl von Nachteilen, die in vielen Fällen auf der fehlenden Zentralisierung zurückzuführen sind (siehe auch G 2.147 *Fehlende Zentralisierung durch Peer-to-Peer*). Beispielsweise können die ausgetauschten Informationen nicht zentral auf Schadsoftware untersucht werden.

**Architektur**

Je nach Anforderungen können Peer-to-Peer-Dienste nur in einem lokalen Netz oder im gesamten Internet genutzt werden. Die Anzahl der IT-Systeme, die sich untereinander diese Ressourcen teilen können, reichen von nur wenigen, ausgewählten Peers bis zu einer unüberschaubaren Menge von unbe-

kannten Peers. Generell kann aber zwischen zwei Arten von Peer-to-Peer-Diensten unterschieden werden:

- Lokale Peer-to-Peer-Dienste
  Bei lokalen Peer-to-Peer-Diensten können einzelne Clients anderen Clients in einem LAN Ressourcen freigeben. Diese Freigaben können oft direkt vom Betriebssystem verwaltet werden. Ein Beispiel hierfür ist die Datei- und Druckerfreigabe in Windows-Betriebssystemen.
  Der Zugriff dieser Dienste kann oft über Passwörter oder eine Auswahl an IP-Adressen eingeschränkt werden. In der Regel werden diese Dienste nicht über das lokale Netz hinaus genutzt und werden am Sicherheitsgateway (Firewall) abgewiesen.
  Da für diese Dienste kein eigener Server benötigt wird, können Kosten für die Beschaffung von Hard- und Software eingespart werden.

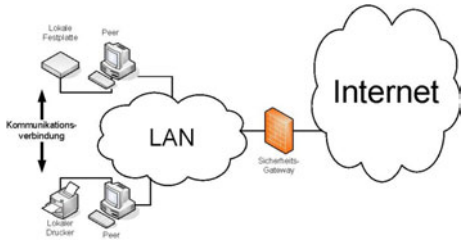



Abbildung: Lokale Peer-to-Peer-Dienste in einem LAN

- Öffentliche Peer-to-Peer-Dienste
  Um Informationen mit Anwendern, die keinen Zugriff auf das LAN haben, auszutauschen, können öffentliche Peer-to-Peer-Dienste eingesetzt werden. Hierfür müssen in der Regel zusätzliche Applikationen auf dem jeweiligen IT-System installiert werden, damit diese die von anderen Peers bereitgestellten Dienste nutzen zu können. Da bei Peer-to-Peer-Diensten direkt zwischen zwei oder mehreren IT-Systemen Informationen ausgetauscht werden, sind für einen Verbindungsaufbau zusätzliche Informationen nötig, wie diese IT-Systeme erreichbar sind. Aus diesem Grund sollte es besonders bei großen Peer-to-Peer-Netzen eine Übersicht geben, auf welchem Peer welche Ressourcen bereitgestellt werden.
  Prinzipiell werden folgende Typen unterschieden:

  - Zentrale Peer-to-Peer-Dienste:
    Die installierte Applikation baut eine Verbindung zu einem Server auf, der Informationen zu anderen Peers verwaltet. Hierfür muss vorher die Applikation des Peers Informationen über die Ressourcen, die er bereitstellen möchte, an den Server übertragen. Erst nach diesem Schritt kann in der Regel ein IT-System auf Informationen über die anderen angemeldeten Peers zugreifen. Hierzu gehören beispielsweise die IP-Adresse, der Benutzer und die bereitgestellten Inhalte. Mit Hilfe dieser Informationen kann eine direkte Verbindung zu dem entfernten Peer aufgebaut und dessen Ressourcen genutzt werden.
    Fällt der zentrale Server aus, stehen die Kontaktinformationen der angeschlossenen IT-Systeme nicht mehr zur Verfügung und die Peers können keine Datenverbindung mehr untereinander aufbauen. Dies hat den Ausfall des gesamten Peer-to-Peer-Netzes zur Folge.
  - Dezentrale Peer-to-Peer-Dienste:
    Bei dezentralen Peer-to-Peer-Diensten wird kein zentraler Server, der die angeschlossenen Benutzer verwaltet, benötigt. Die IT-Systeme der Benutzer dieser Dienste bauen untereinander Datenverbin-

dungen auf, um Informationen über die bereitgestellten Ressourcen auszutauschen. Hierbei können nicht nur die Ressourcen der IT-Systeme, mit denen direkt eine Verbindung aufgebaut wird, durchsucht werden, sondern auch Informationen über andere Peers, die hiermit wiederum eine Datenverbindung aufgebaut haben, abgerufen werden. Da jeder Peer mit mehreren Peers eine Verbindung aufbauen kann, entsteht ein Netz, über das jeder Peer Informationen zu den bereitgestellten Ressourcen anderer Peers abrufen kann.
Diese dezentralen Peer-To-Peer-Dienste setzen voraus, dass die Applikation mit einem Peer aufgebaut werden muss, der Bestandteil dieses Netzes ist, um ebenfalls Mitglied des Netzes werden zu können. Die hierfür benötigten Kontaktinformationen müssen vorher bekannt sein. Da viele Netze von einer großen Menge von angeschlossenen IT-Systemen profitieren, werden diese Kontaktinformationen oft auf Webseiten veröffentlicht.

- Hybride Peer-to-Peer-Dienste
  Hybride Peer-to-Peer-Dienste sind mit zentralen Peer-to-Peer-Diensten vergleichbar, mit dem Unterschied, dass mehrere voneinander unabhängige Server eingesetzt werden können. Wie bei zentralen Peer-to-Peer-Diensten übermitteln die Peers einem Server die Ressourcen, die sie bereitstellen und Kontaktinformationen, wie sie erreicht werden können. Die Server wiederum teilen diese Informationen weiteren Servern mit. Bei Bedarf können die Peers auf die Ressourcen anderer Peers zugreifen, die nicht vom selben Server verwaltet werden.

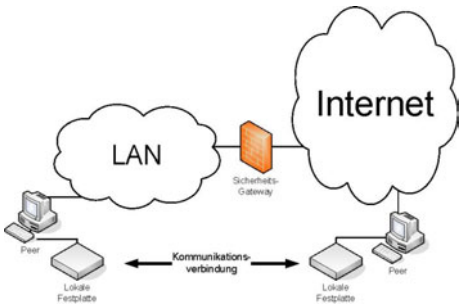



Abbildung: Öffentliches Peer-to-Peer über das Internet (File-Sharing)

**Alternativen für den Einsatz von Peer-to-Peer-Diensten**

Nur bei wenigen Diensten ist eine Peer-to-Peer-Kommunikation zwischen IT-Systemen zwingend erforderlich. Beispielsweise können Ressourcen auch zentral von Servern bereitgestellt werden. Erst durch einen Einsatz von Servern können Vorgaben zentral umgesetzt werden, beispielsweise dass nur berechtigte Personen auf die Informationen zugreifen dürfen. Folgende Dienste, die typischerweise über Peer-to-Peer-Netze verteilt werden können, können zentralisiert bereitgestellt werden:

- Bereitstellung von Druckern
  Wenn mehrere Personen in einem LAN Zugriff auf Drucker benötigen, können diese zentral im Netz bereitgestellt werden. Hierfür eignet sich der Einsatz netzfähiger Drucker und die Verwaltung über Druckserver (siehe B 3.406 *Drucker, Kopierer und Multifunktionsgeräte*).
- File-Sharing
  Statt Speicher auf mehreren Clients ("Peers") im LAN freizugeben, können die Informationen zentral auf einem Dateiserver abgelegt werden. Sollen nur die Benutzer innerhalb eines LANs auf den Server zugreifen dürfen, können beispielsweise Samba-Server (siehe B 5.17 *Samba*) oder

NFS-Server (siehe B 3.102 *Server unter Unix*) die Informationen bereitstellen. Sollen auch externe Benutzer auf die Informationen zugreifen dürfen, könnten die Informationen auf einen extern erreichbaren Webserver (siehe B 5.4 *Webserver*) abgelegt werden.

- Messaging
  Wenn es nötig ist, Kurzmitteilungen zu versenden und nicht auf E-Mail zurückgegriffen werden soll, ist zu überlegen, einen Instant Messaging Server, wie beispielsweise Jabber, zu betreiben. Über diesen Server könnten die Nachrichten zentralisiert auf Schadsoftware überprüft werden.
  Auch die Kommunikation mit externen Gesprächspartnern kann mit Hilfe eines zentralen Instant Messaging Server, der von der Institution betrieben wird und sowohl von intern als auch von extern erreichbar ist, erfolgen.
- VoIP (Voice over Internet Protocol) und Internettelefonie
  VoIP-Lösungen, wie im Baustein B 4.7 *VoIP* beschrieben, unterscheiden zwischen der Signalisierung und dem Medientransport. Für die Signalisierung werden oft Server vorausgesetzt, auf denen die Teilnehmer verwaltet werden. Nachdem über die Signalisierung ein Gespräch zwischen zwei oder mehreren Benutzern eingeleitet wurde, werden bei vielen Lösungen die Sprachinformationen direkt zwischen den Benutzern ausgetauscht. Diese Art von Peer-to-Peer ist in einem LAN sinnvoll und sollte genutzt werden.
  Über die Grenzen eines LANs hinweg sollte Peer-to-Peer nicht zur Telefonie genutzt werden, beispielsweise sollte eine Institution keine VoIP-Kommunikation zulassen, um mit externen Gesprächspartner zu kommunizieren ("Internettelefonie"). Auch in diesem Fall sollte sowohl die Signalisierung als auch der Medientransport auf einem Konzentrator, ähnlich einem Proxy, gebündelt werden (siehe M 4.289 *Einschränkung der Erreichbarkeit über VoIP*). Auf dieser Weise wird der direkte Verbindungsaufbau einzelner Peers auf externe Gesprächspartner, die sich beispielsweise im Internet befinden können, vermieden.

**Empfehlungen für den Einsatz von lokalen Peer-to-Peer-Diensten**

Wenn möglich, sollten statt Freigaben über Peer-to-Peer-Dienste dedizierte Server zum Informationsaustausch genutzt werden. In Ausnahmefällen ist aber auch der Einsatz von Peer-to-Peer-Lösungen nötig, wie beispielsweise bei VoIP. Daher ist festzulegen:

- welche Peer-to-Peer-Dienste genutzt,
- welche Informationen ausgetauscht und
- welche Dienste genutzt

werden dürfen. Wenn erforderlich, sind die Benutzer für die Nutzung von Peer-to-Peer-Diensten zu schulen. Es ist darauf zu achten, dass sich die Peer-to-Peer-Dienste nur auf das LAN beschränken.

**Empfehlungen für den Einsatz von öffentlichen Peer-to-Peer-Diensten**

Generell muss der unkontrollierte Informationsfluss aus einem LAN unterbunden werden. Hierzu gehören auch direkte Peer-to-Peer-Verbindungen von Peers zu IT-Systemen, die sich nicht im LAN befinden. Durch die fehlende Zentralisierung können unkontrolliert Informationen das LAN verlassen (z. B. vertrauliche Informationen) oder hinein gelangen (z. B. Schadsoftware). Durch folgende Maßnahmen kann die Nutzung von öffentlichen Peer-to-Peer-Diensten verhindert werden:

- Lokale Paketfilter
  Durch den Einsatz lokaler Paketfilter kann die Kommunikation der Clients auf wenige IT-Systeme beschränkt werden. Beispielsweise könnten die

Filterregeln so festgelegt werden, dass nur mit Servern kommuniziert werden darf.
Auf Grundlage der IP-Adresse des Servers und der Portnummer des erlaubten Dienstes kann ein unerwünschter Kommunikationsaufbau erschwert werden. Durch den Einsatz von lokalen Paketfiltern kann sowohl die Verwendung von lokalen als auch öffentlichen Peer-to-Peer-Netzen unterbunden werden.

- Zentrale Filterung am Sicherheitsgateway (Firewall)
  Generell sollte das Sicherheitsgateway nur die notwendige Kommunikation in oder aus dem lokalen Netz zulassen, alle anderen Verbindungen sollten abgewiesen werden (siehe B 3.301 *Sicherheitsgateway (Firewall)*). Verhindert das Sicherheitsgateway die Kommunikation der Clients aus dem LAN mit IT-Systemen im Internet, kann die Nutzung von öffentlichen Peer-to-Peer-Netzen verhindert werden.
- Richtlinie
  Neben technischen Empfehlungen sollte den Mitarbeitern der Institution auch die Verwendung von Peer-to-Peer-Diensten untersagt werden. Diese Anweisung kann in der Sicherheitsrichtlinie für Benutzer formuliert werden.

Wenn in der Institution Peer-to-Peer-Dienste genutzt werden sollen, muss dies durch die Leitungsebene der Institution beschlossen werden. Der IT-Sicherheitsbeauftragte muss hierbei einbezogen werden, außerdem ist die Entscheidung inklusive der Restrisiken zu dokumentieren.

Prüffragen:

- Existiert eine Richtlinie, die den Einsatz von Peer-to-Peer-Diensten regelt?
- Ist dokumentiert, welche Peer-to-Peer-Dienste von wem genutzt werden, und welche Informationen dabei ausgetauscht werden?
- Werden Maßnahmen ergriffen um den unautorisierten Einsatz (Personen, Informationen, Dienste) von Peer-to-Peer-Diensten zu verhindern?
- Wurde der Einsatz von Peer-to-Peer-Diensten von der Geschäftsleitung genehmigt und die Restrisiken dokumentiert und angenommen?

# M 5.153 Planung des Netzes für virtuelle Infrastrukturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Virtualisierungsserver müssen allen virtuellen IT-Systemen den Zugriff auf von diesen benötigte Infrastrukturkomponenten wie Netze und Speichernetze, sowie auf Infrastrukturdienste wie DNS oder DHCP ermöglichen. Hierbei sind die folgenden Aspekte bei der Planung der Netzanbindung der Virtualisierungsserver zu beachten:

- Netzanbindung der Virtualisierungsserver
  Virtualisierungsserver benötigen in der Regel Zugriff auf Infrastrukturdienste wie DNS sowie auf Speichernetze. Weiterhin werden sie häufig über das Netz administriert und bestimmte Virtualisierungsfunktionen wie die *Live Migration*, also das Verschieben eines virtuellen IT-Systems im laufenden Betrieb von einem Virtualisierungsserver auf den anderen, nutzen ebenfalls Netzverbindungen zwischen den Virtualisierungsservern. Daher werden auf den Virtualisierungsservern selbst Netzschnittstellen für diese Zwecke benötigt. Da über diese Schnittstellen auch die virtuellen IT-Systeme, die auf dem Virtualisierungsserver betrieben werden, verwaltet werden können, sind diese Schnittstellen besonders zu schützen und in einem Verwaltungsnetz zu betreiben. Der Zugriff auf dieses Verwaltungsnetz stellt das virtuelle Pendant des Zugangs zum Rechenzentrum oder Serverraum dar und sollte genau wie der Zutritt zu Serverräumen restriktiv gehandhabt werden (siehe auch Maßnahme M 1.58 *Technische und organisatorische Vorgaben für Serverräume*). Das Verwaltungsnetz sollte deshalb separat betrieben werden, um sicherzustellen, dass die Verwaltungsfunktionen der Virtualisierungsserver nur von den vorgesehenen Arbeitsstationen aus und nur für die berechtigten Administratoren erreichbar sind. Das Verwaltungsnetz sollte insbesondere von den Netzen der virtuellen IT-Systeme getrennt werden.
  Es muss des Weiteren geprüft werden, ob für die Virtualisierungsfunktion *Live Migration* ein dediziertes Netz geschaffen werden soll. Da bei einer *Live Migration* die Hauptspeicherinhalte eines virtuellen IT-Systems möglicherweise unverschlüsselt über das Netz übertragen werden, kann eine solche Trennung je nach Schutzbedarf der virtuellen IT-Systeme notwendig sein.
- Netzanbindung der virtuellen IT-Systeme
  Für virtuelle IT-Systeme (virtuelle Server, Clients und gegebenenfalls virtuelle Switche) sind die Maßnahmen des Bausteins B 3.101 *Allgemeiner Server* und B 3.302 *Router und Switches* genauso umzusetzen wie für physische. Bezüglich der Netzanbindung virtueller IT-Systeme sind bei der Planung einige Besonderheiten zu beachten. Virtuelle IT-Systeme nutzen die physischen Netzschnittstellen der Virtualisierungsserver, um auf Netze zuzugreifen. Hierbei existiert in der Regel keine direkte, eindeutige Zuordnung von Schnittstellen zu virtuellen IT-Systemen. Dies bedeutet, dass sich bei einigen Virtualisierungsprodukten mehrere virtuelle IT-Systeme dieselbe physische Schnittstelle teilen können. Da bei einer Störung dieser Schnittstelle gleich mehrere virtuelle IT-Systeme vom Netz getrennt werden, wird empfohlen, dass die Verfügbarkeit dieser mehrfach genutzten Netzschnittstellen gesteigert wird (*Kumulationsprinzip*). Dies kann z. B. durch redundante Netzschnittstellen und Techniken wie *IEEE 802.3ad* (*Link Aggregation Control Protocol - LACP*) oder anderer *Load Balancing*-Verfahren geschehen. Hierbei ist besonders zu beachten, dass die Ver-

wendung solcher Protokolle in der Regel eine angepasste Konfiguration auf dem physischen Switch erfordert, an den diese Schnittstellen angeschlossen sind. Falls möglich, sind die physischen Schnittstellen mit unterschiedlichen Switchen zu verbinden.

**Trennung von Netzsegmenten**

Virtualisierungsserver werden oft mit einer Vielzahl von Netzen verbunden. Einige Virtualisierungsprodukte verfügen über Funktionen, um mehrere *VLANs* über eine physische Schnittstelle (*Port Trunking* gemäß *IEEE 802.1q*) zu nutzen. Es ist zudem möglich, auch in der virtuellen Infrastruktur *VLANs* zur Netzsegmentierung zu verwenden. Genügen zur Segmentierung der Netze *VLANs*, die lediglich eine logische Trennung darstellen, kann dies auch innerhalb der virtuellen Infrastruktur geschehen. Die virtuellen Netzkarten der betreffenden virtuellen IT-Systeme sind dann so auf physische Netzschnittstellen zu verteilen, dass diese nur untereinander Netzpakete austauschen können.

Wurden vor der Virtualisierung Netze aufgrund unterschiedlichen Schutzbedarfs physikalisch getrennt, müssen diese Netze auch in virtuellen Umgebungen voneinander isoliert werden. Es ist dann zu prüfen, ob die Mechanismen zur Netztrennung, sowie der Kapselung und Isolation der virtuellen IT-Systeme in der eingesetzten Virtualisierungslösung ausreichen, um virtuelle IT-Systeme mit hohem Schutzbedarf gemeinsam mit solchen niedrigen Schutzbedarfs auf einem Virtualisierungsserver betreiben zu können. Diese Prüfung kann z. B. darin bestehen, dass der Hersteller der betreffenden Virtualisierungslösung die genannten Mechanismen für diesen Einsatzzweck (Trennung von Maschinen unterschiedlichen Schutzbedarfs) als geeignet bezeichnet und dies durch eine entsprechende Zertifizierung nachweist.

Bei erhöhtem Schutzbedarf kann der Betrieb der jeweiligen Netze auf einem einzelnen Virtualisierungsserver jedoch problematisch sein, beispielsweise wenn Administratoren der virtuellen Infrastruktur keinen Zugriff auf virtuelle IT-Systeme in bestimmten Netzen außerhalb ihres Verantwortungsbereichs haben sollen. In diesem Fall sind die virtuellen Maschinen, die Zugang zu den betreffenden Netzen haben müssen, auf isolierten dedizierten Virtualisierungsservern bereitzustellen. Gegebenenfalls sollte das betreffende IT-System statt in einer virtuellen Umgebungen auf einem physischen IT-System betrieben werden.

**Hochverfügbare virtuelle Infrastrukturen**

Der kumulierte Schutzbedarf der einzelnen virtuellen IT-Systeme kann zu einem hohen oder sehr hohen Schutzbedarf dieses Virtualisierungsservers führen. In einem solchen Fall wird daher empfohlen, mehrere Virtualisierungsserver beispielsweise zu einem Cluster zu verbinden. Hierbei werden die virtuellen IT-Systeme auf den verbleibenden Virtualisierungsservern neu gestartet, wenn einer der Virtualisierungsserver im Cluster ausgefallen ist.

Fällt die Kommunikation zwischen mehreren Systemen eines Clusterverbundes gleichzeitig aus, muss jedes System entscheiden können, ob es selbst oder die anderen Systeme von dem Ausfall betroffen sind (*Isolationsproblem*), damit die durch einen Serverausfall betroffenen virtuellen IT-Systeme nicht mehrfach neu gestartet werden. Dieses Isolationsproblem wird in der Regel dadurch gelöst, dass ein Clustersystem prüft, ob bestimmter Ressourcen wie z. B. das Standardgateway erreichbar sind. Kann es diese Ressourcen nicht erreichen, betrachtet es sich als isoliert und entfernt sich selbst aus dem Cluster, je nach Konfiguration werden die auf ihm betriebenen virtuellen IT-Systeme dabei gestoppt.

Daher wird empfohlen, bei der Planung eines solchen Virtualisierungsclusters zu ermittelt, welche Ressourcen zur Prüfung der Isolation herangezogen werden. Diese Ressourcen sind dann in der Rechenzentrumsinfrastruktur mit einer ausreichenden Verfügbarkeit bereitzustellen. Die Netzverbindungen zwischen den Virtualisierungsservern, die Bestandteil des Clusters sind, sind ebenfalls mit einer ausreichenden Verfügbarkeit auszulegen.

Prüffragen:

- Wurde für die Verwaltung der virtuellen Infrastruktur ein getrenntes Verwaltungsnetz realisiert?
- Ist geprüft worden, ob für Virtualisierungsfunktionen wie die Live Migration ein eigenes Netz realisiert werden muss?
- Wurde für die Anbindung der produktiven Gastsysteme ein getrenntes Netz realisiert?
- Ist die Verfügbarkeit der für virtuelle IT-Systeme genutzten Netzschnittstellen ausreichend geplant?
- Ist die Trennung der Netzsegmente durch das eingesetzte Virtualisierungsprodukt ausreichend sichergestellt, wenn virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver betrieben werden?
- Sind die Netzverbindungen eines Clusters aus Virtualisierungsservern mit einer ausreichenden Verfügbarkeit geplant worden?

# M 5.154 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Virtualisierungsserver benötigen eine Vielzahl von Kommunikationsbeziehungen. Dies sind einerseits Verbindungen zu Verwaltungsnetzen und bei Bedarf Verbindungen zu Speichernetzen, um entsprechende Ressourcen des Rechenzentrums nutzen zu können. Andererseits stellen sie für die virtuellen IT-Systeme die jeweiligen Netzverbindungen zur Verfügung.

Hierbei kommen bei den verschiedenen Virtualisierungsprodukten unterschiedliche Techniken zum Einsatz. Bei einigen Virtualisierungsprodukten werden den einzelnen virtuellen IT-Systemen jeweils eigene Netzwerkkarten zugeordnet, die direkt mit den zu nutzenden Netzen verbunden sind. Dies können virtuelle oder physische Netzwerkkarten sein.

Bei anderen Virtualisierungsprodukten werden vollständige Netzinfrastrukturen innerhalb des Virtualisierungsservers abgebildet. Hierfür werden virtuelle Switches erzeugt, die zum einen für die virtuellen IT-Systeme die notwendigen Netzverbindungen bereitstellen und zum anderen den Übergang des virtuellen Netzes in das physische Netz steuern. Dabei ist es auch möglich, rein virtuelle Netze zu erzeugen, die keinen Übergang in das physische Netz besitzen.

Einige der Virtualisierungslösungen unterstützen ebenfalls die Möglichkeit, neben einer physischen eine logische Segmentierung, wie mit einem VLAN (*Virtual Local Area Network*), zu etablieren.

Weiterhin ist die Art und Weise, wie die Kommunikation zwischen virtuellen IT-Systemen untereinander realisiert wird, höchst unterschiedlich. Teilweise wird die Kommunikation zwischen virtuellen IT-Systemen in unterschiedlichen Netzen auf dem gleichen Virtualisierungsserver durch das physische Netz geleitet (Beispiel: *Citrix XenServer*, *Sun VirtualBox* oder *VMware ESX*), teilweise wird diese Kommunikation immer innerhalb der Virtualisierungsschicht durch geleitet, so dass keine Routinginstanz außerhalb der Virtualisierungsschicht an der Kommunikation beteiligt ist (*Sun Solaris Containers*).

Für eine sichere Konfiguration der Netze der Virtualisierungsserver sind mehrere Aspekte zu betrachten:

- Die Verwaltungsschnittstellen der Virtualisierungsserver sollten in einem eigenen Netz angeschlossen werden. Dieses ist physisch oder logisch von dem Netz zu trennen, in dem die virtuellen IT-Systeme betrieben werden. Eine logische Netztrennung ausschließlich mittels *VLAN* ohne darüber hinaus gehende Maßnahmen reicht an dieser Stelle nicht aus, da die Virtualisierungsserver über die Verwaltungsschnittstellen schützenswerte Informationen austauschen.
- Eine Authentisierung muss für alle Benutzer der Verwaltungsschnittstellen erzwungen werden, anonyme Zugriffe dürfen nicht erlaubt werden. Die Übertragung der Authentisierungsdaten sollte außerdem verschlüsselt erfolgen. Des Weiteren sollten die Verwaltungsschnittstellen durch lokale Paketfilter auf dem Virtualisierungsserver selbst geschützt werden.
- In für den Speichernetzzugriff genutzten Netzen kann auf die Targets (=Festplatte) und Initiatoren (=Server) zugegriffen werden. Hierdurch kön-

nen den Virtualisierungsservern oder den virtuellen IT-Systemen gefälschte Initiatoren oder Targets präsentiert werden. Daher ist der Zugriff auf Ressourcen der Speichernetze über ein geeignetes Authentisierungsverfahren zu sichern. Die hierfür verwendeten Netze müssen ebenfalls von den Netzen der virtuellen IT-Systeme separiert werden. Siehe hierzu auch M 5.130 *Absicherung des SANs durch Segmentierung*.

- Werden in einer virtualisierten Infrastruktur Funktionen wie die Migration zur Laufzeit (*VMotion, XENmotion, Live Migration*) genutzt, erfolgt der Transport der Laufzeitumgebung der virtuellen IT-Systeme über das Netz von einem Virtualisierungsserver zum anderen. Hierbei werden alle in dem IT-System verarbeiteten Daten über das Netz übertragen. Diese Daten sind möglicherweise hoch schutzbedürftig. Aus diesem Grunde sollte das für diesen Zweck verwendete Netz ebenfalls separiert werden.
- Die Kommunikation der virtuellen IT-Systeme mit anderen virtuellen oder physischen IT-Systemen sollte detailliert geplant werden. Hierbei ist sicherzustellen, dass bestehende Sicherheitsrichtlinien beachtet werden. Im Netz existierende Sicherheitsgateways oder Monitoring-Systeme dürfen nicht mit den Mitteln der Virtualisierung umgangen werden können. Dies betrifft insbesondere Virtualisierungsprodukte, bei denen der Netzverkehr zwischen virtualisierten IT-Systemen nicht zwingend über physische Netze geführt wird (siehe oben, Beispiele: *SUN Solaris Containers* und *VMware ESX Server*).
- Müssen virtuelle IT-Systeme mit mehreren Netzen verbunden werden, muss geeignet sichergestellt werden, dass über diese keine unerwünschten Netzverbindungen aufgebaut werden können. Es sollten insbesondere keine Verbindungen zwischen Verwaltungsnetzen der Virtualisierungsserver und den Netzen der produktiven virtuellen IT-Systeme ermöglicht werden, um einer Kompromittierung der Virtualisierungsserver durch ein kompromittiertes virtuelles IT-System vorzubeugen.
- In virtuellen Infrastrukturen können auch virtuelle Sicherheitsgateways (virtuelle Firewalls) betrieben werden. Der Einsatz solcher Gateways direkt am Perimeter des eigenen Netzes und somit zur Trennung von Netzen stark unterschiedlichen Schutzbedarfs sollte jedoch genau geprüft werden. Zur Trennung interner Netze mit nicht stark unterschiedlichem Schutzbedarf hingegen sind virtuelle Sicherheitsgateways denkbar. Die Planung solcher Gateways ist sorgfältig durchzuführen. Es muss dabei bedacht werden, dass je nach gewähltem Virtualisierungsprodukt der Netzverkehr durch die Virtualisierungsschicht nicht so geroutet wird, wie dies möglicherweise erwartet wird. Zudem ist nicht gewährleistet, dass die Schutzfunktion des virtuellen Sicherheitsgateways für andere virtuelle oder physische IT-Systeme auch dann noch gegeben ist, wenn die Virtualisierungsserver selbst kompromittiert worden sind. Eine Umgehung dieser Sicherheitsgateways ist nach einer Kompromittierung der Virtualisierungsserver sehr leicht zu realisieren. Da Sicherheitsgateways häufig ebenfalls das Ziel von Angriffen darstellen, sollte davon abgesehen werden, die Virtualisierungsserver selbst ausschließlich durch virtuelle Sicherheitsgateways zu schützen. In solchen Fällen ist eine geeignete Aufteilung der beteiligten Netze über Sicherheitsgateways notwendig. Siehe auch B 3.301 *Sicherheitsgateway (Firewall)*.
- Virtuelle IT-Systeme sind bezüglich ihrer Netzintegration und ihres Schutzes durch Sicherheitsgateways genauso zu behandeln wie physische IT-Systeme, da die Virtualisierungsserver diesen in der Regel keinen zusätzlichen Schutz bieten.

Prüffragen:

- Sind Verwaltungs- und Administrationsnetz vom Netz der virtuellen IT-Systeme separiert und ist diese Trennung gemessen am Schutzbedarf der virtuellen IT-Systeme ausreichend?
- Ist ein anonymer Zugriff auf die Verwaltungsschnittstellen der Virtualisierungsserver ausgeschlossen?
- Existiert ein geeignetes Authentisierungsverfahren für den Zugriff auf Speichernetzressourcen und sind die Speichernetze von den Netzen der virtuellen IT-Systeme separiert?
- Sind die Netze für Live Migrationen von den Netzen der virtuellen IT-Systeme separiert?
- Werden bestehende Sicherheitsrichtlinien bei den Netzverbindungen zwischen virtuellen und physischen IT-Systemen beachtet?
- Ist sichergestellt, dass Sicherheitsgateways und Monitoring-Systeme nicht mit virtuellen Netzen umgangen werden können?
- Ist ausgeschlossen, dass über virtuelle IT-Systeme, die mit mehreren Netzen verbunden sind, unerwünschte Netzverbindungen aufgebaut werden können?
- Falls virtuelle Sicherheitsateways eingesetzt werden sollen: Steht die Nutzung virtueller Sicherheitsateways in Einklang mit den Sicherheitsanforderungen des Informationsverbunds?

# M 5.155 Datenschutz-Aspekte bei der Internet-Nutzung

**Verantwortlich für Initiierung:** Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Bei der Internet-Nutzung werden an vielen Stellen Daten erfasst, die z. B. für Kundenprofile zusammengestellt werden können. Etliche dieser Daten werden mit Wissen und Zustimmung der Benutzer erfasst, andere unbemerkt im Hintergrund. Benutzer können durch richtiges Verhalten aber vermeiden, unerwünschte Datenspuren zu hinterlassen.

**Cookies**

HTTP-Cookies stellen eine Möglichkeit dar, Informationen für bestimmte Webseiten lokal in einem speziellen Dateiverzeichnis auf dem Internet-Client zu speichern. Sie dienen der zeitlich beschränkten Archivierung von Informationen. Cookies können beispielsweise von Betreibern von Webseiten genutzt werden, um Benutzereinstellungen für personalisierte Webangebote oder "Einkaufskörbe" in Onlineshops zu realisieren oder auch um zielgruppenorientierte Werbung zu platzieren. Dabei sind die Informationen in der Regel nicht im Cookie selbst gespeichert. Vielmehr ist ein Cookie eine Art Seriennummer, über die beim Webseiten-Betreiber gespeicherte Informationen Benutzern zugeordnet werden können. Ein Cookie enthält typischerweise

- Informationen über die Webseiten, an die es zurückgeschickt werden soll (beispielsweise nur an den Server, von dem es erzeugt wurde oder an alle Server in der Domain des Servers, von dem es erzeugt wurde),
- eine Gültigkeitsdauer (beispielsweise nur für die laufende Browsersitzung oder bis zu einem vorgegebenen Ablaufdatum) und
- andere, vom Betreiber des Webservers frei vorgebbare Daten, etwa eine Benutzer-Kennung oder eine Session-ID.

Im Gegensatz dazu werden Flash Cookies, auch Local Shared Objects (LSO) genannt, durch Flash-Animationen erzeugt. Sie dienen dazu, benutzerspezifische Einstellungen bei der Nutzung von Flash-Dateien auf dem Benutzerrechner zu speichern, beispielsweise die eingestellte Lautstärke des Benutzers. Sie werden vom Flash-Player erzeugt und sind Browser-unabhängig. Dadurch können sie allerdings auch nicht über die Browser-Einstellungen gesteuert, also z. B. automatisch gelöscht, werden. Unabhängig vom eingesetzten Betriebssystem werden die Flash Cookies in dem Verzeichnis "Anwendungsdaten" des Benutzers abgelegt.

In den Browser-Einstellungen sollte die generelle Annahme von Cookies deaktiviert werden. Die Annahme von Flash Cookies muss im Flash-Player selbst deaktiviert werden. Browser sollten so konfiguriert werden, dass Benutzer vor der Speicherung eines Cookies gefragt werden, ob dieses akzeptiert werden soll. Cookies können auch für die Dauer einer Sitzung erlaubt, aber die dauerhafte Speicherung blockiert werden. Einige Browser erlauben eine relativ detaillierte Einstellung der Kriterien, nach denen Cookies akzeptiert oder zurückgewiesen werden. Die folgenden Punkte können als Grundlage für die Entscheidung dienen, ob ein Cookie abgelehnt werden sollte oder ob es unbedenklich ist:

- Cookies, die an Server aus einer *anderen* Domain zurückgeschickt werden sollen, als der Domain des Servers, von dem die aktuell besuchte Seite stammt (Third-Party-Cookies), sollten generell abgelehnt werden. Hier-

unter fallen insbesondere Cookies von Werbeanbietern, die Banner innerhalb der besuchten Webseite anbieten.
- Cookies, die an alle Server in einer bestimmten Domain zurückgeschickt werden sollen, und nicht nur an den Server, von dem die aktuell besuchte Seite stammt, sollten normalerweise abgelehnt werden.
- Es sollten alle Cookies mit außergewöhnlich langer Lebensdauer abgelehnt werden.
- Cookies, die zur Speicherung von Benutzereinstellungen für personalisierte Webseiten dienen, können akzeptiert werden. Um solche Cookies zu identifizieren ist allerdings stets die Entscheidung des Benutzers notwendig. Seriöse Anbieter zeigen oft auf den Seiten, auf denen ein Benutzer seine Einstellungen treffen kann, einen Hinweis an, dass die Einstellungen in einem Cookie gespeichert werden sollen.
- Cookies, die nur für die aktuelle Browser-Sitzung Gültigkeit besitzen (oft auch *Session-Cookies* genannt) und nur an den jeweiligen Server zurück geschickt werden, können in der Regel akzeptiert werden.

Allerdings müssen die Benutzer dann einige kleinere Einschränkungen bei der Internet-Nutzung in Kauf nehmen, beispielsweise müssen bei der wiederholten Nutzung einer Webseite bestimmte Daten erneut eingeben werden.

Die Benutzer sollten sich regelmäßig die aktuell gespeicherten Cookies anzeigen lassen und diese gegebenenfalls selektiv löschen. Besser ist es, den Browser so zu konfigurieren, dass er die gesammelten Cookies beim Beenden löscht. Flash-Cookies werden jedoch nicht von der Löschoption im Browser berücksichtigt. Sie müssen händisch oder mit spezieller Software aus den entsprechenden Ordnern gelöscht werden.

**Datensammlungen (History, Hotlists und Cache)**

Browser sammeln auch intern Daten über die Internet-Nutzung der verschiedenen Benutzer, beispielsweise über History (Liste der zuletzt besuchten Internetseiten), Cache, Download-Übersichten, gespeicherte Such- und Formulardaten und Passwörter. Die Benutzer von Browsern müssen darüber informiert sein, wo auf ihren lokalen IT-Systemen diese Daten gespeichert werden und wie sie diese löschen können. Zudem muss sichergestellt sein, dass nur Befugte darauf Zugriff haben. Bei den meisten Browsern ist es möglich, alle Daten und Dateien, die auf das persönliche Surfverhalten zurückschließen lassen, per Mausklick oder automatisch beim Beenden zu löschen.

Die Dateien auf Proxy-Servern sind besonders sensibel, da auf einem Proxy-Server alle externen Internet-Zugriffe aller Mitarbeiter protokolliert werden, inklusive der IP-Adresse des Clients, der die Anfrage gestartet hat, und der nachgefragten URL. Mit Hilfe der IP-Adresse des Clients ist es in der Regel möglich, auf einen konkreten Mitarbeiter zurückzuschließen. Ein schlecht administrierter Proxy-Server kann daher massive Datenschutzverletzungen nach sich ziehen.

Von den meisten Browsern werden viele Informationen über den Benutzer und sein Nutzerverhalten gesammelt, von denen dieser vielleicht nicht will, dass sie weitergegeben werden. Zu diesen Informationen gehören:

- Favoriten,
- abgerufene Webseiten bzw. Informationen im Cache,
- History-Datenbank bzw. URL-Liste,
- Cookie-Liste,
- Informationen über Benutzer, die im Browser gespeichert und eventuell auch weitergegeben werden.

**Verlaufsanzeige (History-Datenbank)**

In der History oder der Verlaufsanzeige werden die Web-Adressen gespeichert, die vom Benutzer aufgerufen wurden. Praktisch alle Browser führen ein Protokoll über die URLs, die der Benutzer innerhalb eines bestimmten Zeitraums abgerufen hat (*Chronik* bei Firefox, *Verlauf* beim Microsoft Internet Explorer). Ein solches Protokoll kann sich entweder nur über die aktuelle Sitzung erstrecken oder auch Informationen über vergangene Sitzungen enthalten.

Diese Datenbank enthält Informationen über besuchte Webseiten und abgerufene Seiten (URL und Titel). Auch interne Dokumente, die im Browser geöffnet werden, werden mit diesen Informationen in der Datenbank verzeichnet. Dadurch können eventuell sensitive, vertrauliche Informationen preisgegeben werden.

Die History-Datenbank sollte regelmäßig aufgeräumt werden. Die meisten Browser bieten in ihren Konfigurationsdialogen die Möglichkeit, die History-Datenbank komplett zu leeren, z. B. bei jedem Schließen des Browsers. Außerdem kann meist festgelegt werden, welcher Zeitraum von der History-Datenbank abgedeckt werden soll, ältere Informationen werden automatisch gelöscht.

**Informationen über Benutzer**

In einem Browser können diverse Informationen über Benutzer gespeichert und eventuell auch weitergegeben werden, z. B. Name, E-Mail-Adresse, Organisation, Telefonnummer. Hier sollte genau überlegt werden, welche personenbezogenen Informationen hierüber weitergegeben werden sollen. Es empfiehlt sich, hier mit Angaben möglichst sparsam zu sein.

Viele Browser bieten die Möglichkeit, die Eingaben des Benutzers für bestimmte Web-Formulare zu speichern und beim nächsten Aufruf der entsprechenden Seite automatisch einzufügen. Von dieser Option sollte allenfalls in Ausnahmefällen Gebrauch gemacht werden. In keinem Fall sollten Zugangspasswörter auf diese Weise gespeichert werden. Sofern die Möglichkeit besteht, die Daten verschlüsselt abzuspeichern, sollte diese unbedingt genutzt werden.

**Informationen im Browser-Cache**

Im Browser-Cache werden alle Elemente der besuchten Webseiten wie beispielsweise Texte, Stylesheets, Bilddateien oder Töne, abgelegt. Sofern der Cache nicht geleert wird, verkürzt sich die Ladezeit der Seite bei einem erneuten Besuch da die Webseite nicht aus dem Internet, sondern aus dem Browser-Cache geladen wird. Zuvor überprüft der Browser, ob benötigte Dateien bereits im Cache vorhanden sind, oder ob sie erneut aus dem Internet geladen werden müssen. Die Dateien im Browser-Cache können, ähnlich wie die History-Datenbank, dazu verwendet werden, die vom Benutzer abgerufenen Informationen zu rekonstruieren. Dies kann zum Erstellen von Benutzerprofilen missbraucht werden. Im Extremfall kann es sogar dazu führen, dass vertrauliche Informationen an die Öffentlichkeit gelangen, wenn beispielsweise ein am Arbeitsplatz im Intranet genutztes Notebook außerhalb der Behörde oder des Betriebes genutzt wird und abhanden kommt.

Daher sollte der Cache ebenso wie der Verlaufsordner regelmäßig gelöscht oder die Cache-Funktion direkt bei der Konfiguration des Browsers vollständig deaktiviert werden. Es ist empfehlenswert, die Größe des Caches auf 0 MByte zu setzen, um ein Zwischenspeichern von Dateien zu verhindern. Wenn auf

mit SSL gesicherte Webseiten zugegriffen wird, dient dies oft dazu, sensible Informationen wie Kreditkartennummern verschlüsselt über das Internet zu übertragen. Seiten dieser Art sollten, sofern diese Einstellungsoption verfügbar ist, direkt von der Ablage im Cache ausgenommen werden.

Damit Benutzer keine unerwünschten Datenspuren hinterlassen, sollten sie darüber informiert sein, wie sie diese durch richtiges Verhalten und optimale Konfiguration vermeiden können.

Prüffragen:

- Sind Benutzer informiert, wie sie unerwünschte Datenspuren bei der Internet-Nutzung vermeiden können?

# M 5.156 Sichere Nutzung von Twitter

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Mit dem Mikro-Blogging-Dienst Twitter können registrierte Benutzer in kurzen Nachrichten mit maximal 140 Zeichen Neuigkeiten und Informationen austauschen. Die Benutzer können sich bei anderen Benutzern als "Follower" registrieren, so dass sie deren Textnachrichten empfangen.

Bei der Anmeldung an diesen Internet-Dienst müssen Vor- und Nachname, ein Benutzername und ein Passwort sowie eine E-Mail-Adresse angegeben werden. Aus dem Benutzernamen ergibt sich die URL zu der entsprechenden Twitterseite des Benutzers: http://twitter.com/Benutzername. Das gewählte Passwort muss mindestens 6 Zeichen lang sein, weitere Vorgaben existieren nicht. Die Benutzer werden jedoch darauf hingewiesen, dass sie möglichst komplizierte Passwörter wählen sollten ("Be tricky!"). Um Identitätsdiebstahl vorzubeugen, sollten übliche Passwortregelungen beachtet werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs*).

Die Benutzerkennungen können bei der Anmeldung frei ausgewählt werden. Dadurch ist die Nutzung falscher Identitäten möglich. Es können Namen von bekannten, berühmten Persönlichkeiten oder Institutionen ausgewählt und in deren Namen Nachrichten geschrieben werden.

Die Twitter-Betreiber bieten auch die Möglichkeit über "Verified Accounts" ("Verifiziertes Konto") Benutzerkennungen, bei denen die Identität geprüft wurde, mit einem Symbol zu markieren. Diese Option wird bisher allerdings nur selten angeboten.

Der Umgang mit Twitter und ähnlichen Webdiensten sollte in jeder Institution klar geregelt sein. Hierbei gibt es mehrere Varianten:

- Die Institution könnte die Twitter-Nutzung generell verbieten. Dies muss dann natürlich den Mitarbeitern bekannt gegeben werden. Das Verbot kann außerdem technisch durch Filterung bezüglich der bekannten Web-Plattformen unterstützt werden, wobei berücksichtigt werden sollte, dass Benutzer immer neue Wege finden können, um auf solche Dienste zuzugreifen.
- Es gibt auch Institutionen, in denen Twitter offiziell für dienstliche Zwecke freigegeben ist, beispielsweise um aktiv über eigene Dienstleistungen oder Produkte über Twitter zu informieren.

Eine Behörde oder ein Unternehmen sollte klare Regelungen aufstellen, in denen beschrieben ist,

- ob Twitter dienstlich genutzt werden darf, und wenn ja, unter welchen Rahmenbedingungen (z. B. bei der Weitergabe von Informationen, Nutzung von Pseudonymen, etc.) und
- was Mitarbeiter bei der dienstlichen oder privaten Nutzung von Twitter beachten sollten.

Wie bei allen Internet-Diensten sollten die Geschäftsbedingungen vor einer Registrierung als Benutzer sorgfältig daraufhin geprüft werden, ob die genannten Bedingungen aus der eigenen Sicht akzeptabel sind. Die Geschäftsbedingungen des Twitter-Dienstes erlauben eine Nutzung der angegebenen Benutzerinformationen für Werbezwecke.

Twitter ist für die schnelle und breit gestreute Informationsweitergabe bekannt. Häufig werden Informationen über Twitter in so kurzer Zeit weitergegeben, dass beispielsweise Nachrichtendienste diese noch nicht erhalten oder verifizieren konnten. Twitter-Nachrichten werden oft unautorisiert oder ungeprüft weitergegeben. Vor jeder Weitergabe oder -nutzung von Meldungen sollte daher deren Wahrheitsgehalt überprüft werden.

Durch die Textbeschränkung auf 140 Zeichen werden über Twitter oft nur Kurz-URLs weitergegeben. Kurz-URLs haben in der Regel ein Format, das z. B. wie folgt aussieht: *http://kurzurl.com/d9khqp*. Hinter diesem Link verbirgt sich der eigentliche Link, auf den verwiesen werden soll. Dies kann problematisch sein, weil dadurch nicht auf einen Blick erkannt werden kann, wohin die Kurz-URL führt und Benutzer auf Webseiten mit Schadsoftware gelockt werden können.

Kurz-URLs könnten auch von den sogenannten Spam-Followern ausgenutzt werden. Darunter verbergen sich maschinell generierte Accounts, die von Zeit zu Zeit Nachrichten erzeugen. Diese enthalten wie Accounts von realen Personen Nachrichten und Linktipps. Die Links in den verschiedenen Nachrichten suggerieren unterschiedliche und interessante Linkziele, verweisen jedoch immer auf die gleiche Zielseite. Damit Benutzer auch tatsächlich auf die Links klicken, werden viele Accounts geschaffen und untereinander verlinkt bzw. mit Followern versehen. Diese Accounts verfolgen weitere echte Accounts und erhoffen sich viele Klicks auf die entsprechenden Links. So wird Spam dann zusätzlich von aktiven Accounts rechtmäßiger Twitter-Mitglieder aus verbreitet.

Prüffragen:

- Ist die Nutzung von Twitter in der Institution klar geregelt?

# M 5.157 Sichere Nutzung von sozialen Netzwerken

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Soziale Netzwerke sind im Web zur Verfügung gestellte Plattformen, wie beispielsweise MySpace, LinkedIn, Facebook oder Xing, die konzeptionell ähnlich aufgestellt sind, deren Inhalte sich jedoch unterscheiden. Die inhaltliche Ausgestaltung wird von den entsprechenden Nutzern selbst übernommen. So werden soziale Netzwerke genutzt, um alte Freunde oder Arbeitskollegen wiederzufinden, selbst gefunden zu werden, oder auch, um berufliche Kontakte zu knüpfen. Neben der Erstellung eines Profils, mit dem die Online-Identität präsentiert wird, geht es auf den Plattformen um die Vernetzung der Benutzer untereinander. Diese Verknüpfung erfolgt aufgrund von sozialen Interaktionen zwischen den Benutzern und wird mit Hilfe spezieller Plattformfunktionen im Datenbestand der Software gespeichert.

Soziale Netzwerke werden zur Kommunikation und zum Datenaustausch der Benutzer untereinander genutzt. Je nach Ausrichtung der Plattform können dort zusätzlich neben persönlichen Daten auch Fotos oder andere Informationen eingestellt und verschiedene Anwendungen genutzt werden.

Um Teil eines sozialen Netzwerkes zu werden, ist die Registrierung an der entsprechenden Plattform notwendig. Neben Benutzernamen und Passwort werden oftmals weitere persönliche Informationen erfasst. Welche weiteren persönlichen oder auch dienstlichen Informationen preisgegeben werden, richtet sich nach dem jeweiligen Benutzer und der Intention der Nutzung. Gerade die Vielzahl von Informationen über die eigene Person dient dazu, in den Netzwerken wahrgenommen zu werden und mitwirken zu können. Es muss jedem Benutzer jedoch auch klar gemacht werden, dass alle Informationen über Benutzer als Grundlage für Social Engineering Angriffe genutzt werden können (siehe auch M 3.5 *Schulung zu Sicherheitsmaßnahmen*)

Mit den Hintergrundinformationen können Angreifer versuchen, sich das Vertrauen ihrer Opfer zu erschleichen und diese zu weiteren Handlungen zu überreden, beispielsweise bestimmte Dateien zu öffnen. Jede Information, die ein Benutzer über sich ins Internet stellt, sollte also sorgfältig abgewogen werden. Informationen, und dazu gehören auch Fotos, Videos und Zitate, können im Internet leicht eingestellt, von anderen Personen aber auch schnell weiterverbreitet werden.

Aufgrund dessen sollte sich jeder Benutzer eines sozialen Netzwerkes über den Diensteanbieter informieren, vor allem über die Vertragsgrundlagen, die bei Nutzung dieser Dienste akzeptieren werden müssen. Es sollte beispielsweise überprüft werden,

- welche persönlichen Daten für eine Anmeldung beim Diensteanbieter angegeben werden müssen,
- ob und wie der Diensteanbieter die Benutzerdaten vor unbefugten Zugriff schützt, z. B. ob die virtuelle Identität vor Missbrauch durch Dritte geschützt wird,
- wie die Datenübertragung abgesichert ist, also ob z. B. die Kommunikation grundsätzlich oder partiell verschlüsselt wird (typischerweise mit SSL), ob Passwörter oder Session-Cookies ausschließlich verschlüsselt übertragen werden,

- ob der Diensteanbieter Benutzerprofile erstellt und an Dritte weiter gibt, z. B. um über gezielte Werbung die Plattform zu finanzieren,
- ob die Benutzerdaten jederzeit eigenständig und vollständig gelöscht werden können.

Vor der Anmeldung bei einem sozialen Netzwerk sollten die Benutzer prüfen, wie die Plattform den Datenschutz handhabt. Sofern die Benutzer eigenständig Datenschutz-Optionen konfigurieren können, sollten diese möglichst restriktiv eingestellt werden. Die möglichen Freigaben von Daten für andere Benutzer sollten restriktiv gehandhabt werden, also z. B. in einem "öffentlichen Profil" nur die nötigsten Informationen eingestellt werden.

Benutzer sozialer Netzwerke sollten genau überlegen, welche Kontakte sie akzeptieren und welchen anderen Nutzern sie welche Informationen weitergeben. Es sollten überall nur die Informationen eingegeben werden, die für die Interaktion auf den jeweiligen Plattformen benötigt werden. Informationen über Dritte sollten nur nach Absprache mit diesen weitergegeben werden.

Der Umgang mit sozialen Netzwerken sollte in einer Behörde bzw. einem Unternehmen klar geregelt sein. Hierbei gibt es mehrere Varianten:

- Institutionen können beschließen, die Nutzung von sozialen Netzwerken generell zu verbieten. Dies muss dann natürlich den Mitarbeitern bekannt gegeben werden. Das Verbot kann außerdem technisch durch Filterung bezüglich der bekannten Anbieter unterstützt werden, wobei berücksichtigt werden sollte, dass Benutzer immer neue Wege finden können, um auf solche Dienste zuzugreifen.
- Es gibt auch Institutionen, in denen soziale Netzwerke offiziell für dienstliche Zwecke freigegeben ist, beispielsweise um aktuelle Informationen von Interessengruppen und Gremien zu beziehen oder auch, um aktiv eigene Dienstleistungen oder Produkte über soziale Netzwerke zu vermarkten.

Eine Behörde oder ein Unternehmen sollte klare Regelungen aufstellen, in denen beschrieben ist,

- ob soziale Netzwerke dienstlich genutzt werden dürfen,
- unter welchen Rahmenbedingungen sie dienstlich genutzt werden dürfen (z. B. bei der Weitergabe von Informationen, Schutz vor Schadsoftware, Nutzung von Pseudonymen, etc.),
- was Mitarbeiter bei der Nutzung von sozialen Netzwerken beachten sollten.

Benutzer sollten geschäftliche und private Nutzung von sozialen Netzwerken nicht vermischen und die Regelungen ihrer Institutionen kennen.

Prüffragen:

- Ist die Nutzung von sozialen Netzwerken in der Institution klar geregelt?
- Werden die Mitarbeiter über die Gefahren der Nutzung von sozialen Netzwerken informiert?

# M 5.158 Nutzung von Web-Speicherplatz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Als Web-Speicherplatz (oder auch Online-Festplatte) wird Speicherplatz bei Internet-Anbietern bezeichnet. Kunden erhalten diesen von einem Web-Anbieter zugeteilt, um Dateien längerfristig zu speichern und einfach über das Internet auf die Daten zugreifen zu können. Vor allem mobile Mitarbeiter schätzen diese Möglichkeit, da sie von beliebigen Standorten schnell und uneingeschränkt auf ihre Daten zugreifen können. Auch zum Austausch größerer Datenmengen werden diese Dienste gerne genutzt. Hierin liegt allerdings auch ein großes Risiko, denn der Zugriff auf externe Speichermöglichkeiten macht Datenflüsse schwerer kontrollierbar.

Der Schutz der Vertraulichkeit der Daten hängt nicht nur davon ab, ob die Datenkommunikation und Speicherung beim Anbieter ausreichend abgesichert ist, sondern auch von der Frage, von welchen externen IT-Systemen diese abgerufen werden, was danach mit ihnen passiert und wo sie wiederum gespeichert werden.

Typische Probleme hier sind beispielsweise:

- Mitarbeiter nutzen externen Web-Speicherplatz, um firmeninterne Daten in einem Internet-Cafe oder bei einer anderen Firma abzurufen. Durch eine unzureichende Absicherung der übertragenen Informationen (sowohl Authentisierungs- als auch Nutzdaten) können anschließend auch Unbefugte auf weitere dort gespeicherte firmeninterne Daten zugreifen.
- Ein Mitarbeiter ruft von zu Hause Daten ab, um diese am Wochenende zu bearbeiten. Da sein privater PC mit Schadsoftware verseucht ist, wurden auch die bearbeiteten Dateien infiziert.

Die Verfügbarkeit der gespeicherten Daten hängt von mehreren Faktoren ab: Verfügbarkeit der Internetanbindung und der Systeme beim Anbieter. Bei einer längerfristigen Speicherung von Daten muss zudem das Geschäftsmodell des Anbieters geprüft werden, um einzuschätzen, ob ein dauerhafter Betrieb und gleichbleibende Rahmenbedingungen gewährleistet werden.

Geschwindigkeit der Anbindung: Soll der Web-Speicherplatz als Speicherort für die Datensicherung genutzt werden, ist nicht nur die Zeit wichtig, die benötigt wird, um die zu sichernden Informationen zum Anbieter zu übertragen, sondern auch die Zeit, die benötigt wird, um die Datensicherung wieder einzuspielen. Für eine professionelle Datensicherung sind die meisten anderen Lösungen für Datensicherungen innerhalb der eigenen Institution schneller und besser kontrollierbar (und möglicherweise auch kostengünstiger).

Der Umgang mit Web-Speicherplatz sollte in jeder Institution klar geregelt sein. Hierbei gibt es mehrere Varianten:

- Institutionen können die Nutzung von Web-Speicherplatz generell verbieten. Dies muss den Mitarbeitern bekannt gegeben werden. Das Verbot kann außerdem technisch durch Filterung bezüglich der bekannten Anbieter unterstützt werden, wobei berücksichtigt werden sollte, dass Benutzer immer neue Wege finden können, um auf solche Dienste zuzugreifen.
- Die Institution kann die Nutzung Web-Speicherplatz offiziell für dienstliche Zwecke freigegeben und dafür geeignete Rahmenbedingungen festlegen.

Eine Behörde oder ein Unternehmen sollte auf jeden Fall klare Regelungen zur Nutzung solcher Dienstleistungen aufstellen (siehe auch M 2.460 *Geregelte Nutzung von externen Dienstleistungen*). Hierin sollten unter anderem die folgenden Punkte geklärt sein:

- Dienstliche und private Nutzung sollten nicht vermischt werden.
- Es ist zu klären, unter welchen Rahmenbedingungen Web-Speicherplatz dienstlich genutzt werden darf (z. B. bei der Weitergabe von Informationen, Schutz vor Schadsoftware, etc.).
- Die Geschäftsbedingungen von Anbietern von Web-Speicherplatz sollten vor einer Nutzung sorgfältig geprüft daraufhin werden, ob die genannten Bedingungen aus der eigenen Sicht akzeptabel sind.
- Die Zugriffsrechte auf Web-Speicherplatz müssen genau festgelegt und regelmäßig aktualisiert werden, damit nur autorisierte Personen auf die gespeicherten Daten zugreifen können.
- Der Datenaustausch sollte auf jeden Fall per SSL/TSL-Verschlüsselung gesichert werden.
- Zusätzlich müssen vertrauliche Daten verschlüsselt gespeichert werden, um sie vor unbefugtem Zugriff zu schützen.
- Es ist festzulegen, von wo (Umgebungssicherheit) und auf welche IT-Systeme gespeicherte Daten abgerufen werden dürfen.

Prüffragen:

- Ist die Nutzung von Web-Speicherplatz in der Institution klar geregelt?

# M 5.159 Übersicht über Protokolle und Kommunikationsstandards für Webserver

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Über (Kommunikations-)Protokolle wird in der IT der Informationsaustausch zwischen Prozessen bzw. IT-Komponenten geregelt (siehe auch M 5.39 *Sicherer Einsatz der Protokolle und Dienste*). Damit auch Prozesse von Applikationen, die von verschiedenen Entwicklern erstellt wurden, miteinander kommunizieren können, müssen die Informationen nach vorher festgelegten Regeln übertragen werden. Diese Vorschrift wird als Protokoll bezeichnet. Diese Prozesse können beispielsweise Serverdienste oder Clientapplikationen sein. Auch zwischen lokalen Prozessen kann der Austausch von Informationen über Protokolle geregelt werden.

Im Zusammenhang von Webservern werden zahlreiche verschiedene Protokolle eingesetzt, die im folgenden beschrieben werden:

**Hypertext Transfer Protocol (HTTP)**

Das am häufigsten eingesetzte Protokoll zur Datenübertragung im Web ist HTTP. Es handelt sich dabei um ein Protokoll der Anwendungsschicht des TCP/IP-Referenzmodells. Die Version 1.1 ist in RFC 2616 definiert und basiert auf dem Client-Server-Prinzip. Das bedeutet, dass stets vom Client eine Anfrage gestellt wird (Request), welche vom Web-Server beantwortet wird (Response). Das Protokoll arbeitet zustandslos, was bedeutet, dass nach erfolgter Datenübertragung (z. B.einer Web-Seite) die Verbindung zum Server wieder geschlossen und nicht aufrechterhalten wird.

Bei HTTP handelt es sich um ein Klartextprotokoll, wodurch alle übertragenen Daten von einem möglichen Angreifer mitgelesen werden können. Eine entsprechende Verbesserung bietet HTTPS, welches eine verschlüsselte Verbindung auf Basis von TLS oder SSL zwischen Web-Server und Browser ermöglicht.

**HTTPS**

HTTPS (HTTP über SSL bzw. HTTP über TLS) ist eine Variante von HTTP, bei der Authentisierung und Datenübertragung durch Verschlüsselung und Zertifikate geschützt werden können. HTTPS wird im RFC 2818 spezifiziert.

Meist benutzt ein Webserver, der HTTPS unterstützt, den TCP-Port 443. Beim Einsatz von HTTPS muss beachtet werden, dass TLS auch einen Betriebsmodus kennt, in dem keine Verschlüsselung stattfindet. Bei entsprechenden Sicherheitsanforderungen sollte am HTTPS-Proxy verhindert werden, dass entsprechende Verbindungen aufgebaut werden können.

**WebDAV**

WebDAV steht für "Web-based Distributed Authoring and Versioning" und ist ein offener Standard zur Bereitstellung und Verwaltung von Dateien auf einem Web-Server. WebDAV erweitert die Version 1.1 des HTTP-Standards um zusätzliche Funktionen. Die WebDAV-Kommunikation zwischen Client und Server erfolgt ausschließlich über den HTTP-Port 80. Dies stellt einen wesentlichen Vorteil gegenüber anderen Protokollen mit vergleichbaren Funktionen,

wie etwa FTP, dar. Diese verwenden für Befehls- und Datenaustausch unterschiedliche Verbindungen, wodurch es häufig zu Konfigurationsproblemen bei Paketfiltern kommt.

Neben einfachen Datei-Operationen wie dem Hochladen, Umbenennen und Löschen von Dateien bietet WebDAV auch eine Versionskontrolle, die es erlaubt, Dateien mit mehreren Benutzern zu bearbeiten. Um all diese Funktionen nutzen zu können ist jedoch eine vorherige Authentisierung der einzelnen Benutzer über die in HTTP zur Verfügung stehenden Authentisierungsverfahren erforderlich. Für jeden Benutzer können unterschiedliche Berechtigungen vergeben werden. Dabei können beispielsweise auch nur bestimmte Dateitypen erlaubt oder verboten werden. So können die Dateiendungen von ausführbaren Dateien (wie .exe) blockiert werden, um einer unbeabsichtigten Verbreitung von Schadprogrammen vorzubeugen.

**XML-RPC**

XML-RPC (Extensible Markup Language Remote Procedure Call) ist ein Protokoll zum Aufruf von Funktionen auf entfernten Systemen, wobei die übertragenen Daten in einer XML-Struktur abgebildet werden. Die eigentliche Übertragung der XML-RPC-Nachrichten wird mit Hilfe von HTTP durchgeführt. Remote Procedure Calls (RPCs), wie sie beispielsweise durch XML-RPC umgesetzt werden, stellen die wesentliche Grundlage für verteilte Systeme dar. Sie ermöglichen es, Funktionen auf entfernten Systemen über ein Netz aufzurufen.

Da Funktionsaufrufe und Rückgabewerte in XML abgebildet werden, erfolgt eine Abstraktion von den zugrunde liegenden Programmiersprachen und Betriebssystemen. Dies bedeutet, dass Aufrufe unabhängig von der konkret verwendeten Programmiersprache bzw. des Betriebssystems erfolgen können. Funktionsaufrufe bestehen dabei aus dem Namen der Funktion, die aufgerufen werden soll, und den dazugehörigen Parametern. Funktionsrückgabe-Werte werden in einer ähnlichen Struktur wieder vom Server an den Client zurückgeliefert.

In XML-RPC sind keine dezidierten Sicherheitsmaßnahmen vorgesehen. Es ist daher erforderlich, diese in der Programmlogik jenes Systems zu implementieren, welches XML-RPC für entfernte Funktionsaufrufe verwendet.

**SOAP**

SOAP stand ursprünglich für "Simple Object Access Protocol". Dieses Akronym wird jedoch seit der Version 1.2 nicht mehr verwendet, da dieses die Funktionalität des Protokolls verfälschend beschreibt. Es handelt sich um ein Rahmenwerk, das den Austausch von Daten zwischen Systemen über ein Netz regelt. Mit SOAP werden Aufrufe von Funktionen auf entfernten Systemen ermöglicht. Es kann somit als Nachfolger von XML-RPC verstanden werden. SOAP-Nachrichten basieren ebenfalls auf einer XML-Struktur und können mit Hilfe unterschiedlicher Protokolle übertragen werden. Beispiele dafür sind sowohl das für E-Mail-Übertragungen bekannte SMTP als auch das bereits besprochene HTTP. Um eine verschlüsselte Verbindung einsetzen zu können, ist auch die Verwendung von HTTPS möglich. Eines der wichtigsten Anwendungsgebiete von SOAP ist die Bereitstellung und Nutzung von Web-Services.

**Datenbankkonnektoren**

Datenbankkonnektoren stellen eine standardisierte Schnittstelle zu Datenbanken und den zugehörigen Datenbank-Management-Systemen (DBMS) zur

Verfügung. Sie ermöglichen es, unabhängig vom verwendeten DBMS, auf die in der Datenbank abgelegten Daten zuzugreifen oder diese zu verändern. Zusätzlich übernimmt ein Datenbankkonnektor den Auf- und Abbau sowie die Verwaltung einer Datenbankverbindung. Dadurch wird die Implementierung von Datenbankzugriffen im Zuge der Softwareentwicklung wesentlich vereinfacht. Datenbankkonnektoren erlauben einen sehr einfachen Zugriff auf Tabellen von Datenbanken oder Funktionen eines DBMS. Für die Verwaltung der Datenbanken und deren Inhalten verwenden Datenbankkonnektoren bekannte Datenbanksprachen wie etwa SQL. Bekannte Datenbankkonnektoren sind unter anderem ODBC (Open Database Connectivity) und JDBC (Java Database Connectivity).

**SQL**

SQL ist ein Akronym für "Structured Query Language" und dient als Datenbanksprache. Mit Hilfe von SQL-Anweisungen können Datenbestände definiert, abgefragt und verändert werden. Somit werden in SQL die Elemente von Datenverarbeitungssprache, Datenbeschreibungssprache und Datenaufsichtssprache vereint. Obwohl auch andere Datenbanksprachen existieren, hat sich SQL bei allen gängigen Datenbanken etabliert und ist auch von ANSI und ISO standardisiert.

Für Anwendungen und Web-Angebote, die auf SQL-Anweisungen für Datenbank-Abfragen zurückgreifen, müssen einige Sicherheitsmaßnahmen umgesetzt werden. Beispielsweise muss eine Anfälligkeit für SQL-Injections vermieden werden. Bei SQL-Injections handelt es sich um Schwachstellen bei Web-Angeboten, welche ungewollten Zugriff auf Datenbankinhalte erlauben. Diese Schwachstellen entstehen dann, wenn Web-Angebote Benutzereingaben nicht ausreichend filtern und Angreifer die SQL-Abfrage beeinflussen können. Können SQL-Abfragen manipuliert werden, besteht die Möglichkeit, Datenbestände vollständig auszulesen, zu verändern oder zu löschen.

Eine gebräuchliche Maßnahme zum Schutz vor SQL-Injections ist die Verwendung von Stored Procedures. Dabei handelt es sich um eine Funktion des DBMS, zusammenhängende Anweisungen und Abläufe als fertige Prozeduren zu speichern. Dadurch hat ein Angreifer nicht mehr die Möglichkeit, die SQL-Abfrage durch eine SQL-Injection zu verändern. Ein ähnlicher Schutz gegen SQL-Injections kann mit Hilfe von Frameworks erreicht werden. Frameworks, wie z. B. Hibernate, bilden eine zusätzliche Abstraktionsschicht zwischen Datenbank und der Implementierung des Datenbankzugriffs. Das Framework bietet dabei eine Schnittstelle für Programmierer, welche von der tatsächlich verwendeten Datenbank unabhängig ist und welche zur Ablage beliebiger Objekte geeignet ist.

Werden keine Stored Procedures oder Frameworks eingesetzt, so müssen alle Daten, die von Benutzern stammen und als Datenbankeingabe verwendet werden, einer Eingabevalidierung unterzogen werden. Dabei werden die Zeichen gefiltert, mit denen die SQL-Anweisung und somit die Durchführung der Datenbankabfrage beeinflusst werden kann. Anwendungen, die SQL-Anweisungen für Datenbank-Abfragen verwenden, sind immer wieder anfällig für SQL-Injection-Angriffe.

**Techniken für den Aufruf entfernter Prozeduren**

Eine bekannte und oftmals eingesetzte Technik zum Aufruf entfernter Prozeduren ist CORBA (Common Object Request Broker Architecture). Dabei handelt es sich um einen Standard für verteilte Systeme, der es ermöglicht, Kommunikationsverbindungen zwischen Prozessen auf unterschiedlichen Syste-

men aufzubauen und Daten auszutauschen. Durch eine von Programmiersprachen unabhängige Schnittstellen-Definition (Interface Definition Language, IDL) können Programme, die in unterschiedlichen Programmiersprachen implementiert wurden, miteinander kommunizieren. Um eine Kommunikationsverbindung zwischen zwei Prozessen aufbauen zu können, werden auf beiden Seiten sogenannte Object Request Broker (ORB) benötigt. Diese werden in der von der jeweiligen Seite verwendeten Programmiersprache implementiert und haben die Aufgabe, Daten zu empfangen beziehungsweise zu versenden. Die Kommunikation zwischen einzelnen ORBs kann entweder über herstellerspezifische Protokolle oder über das herstellerunabhängige Internet Inter-ORB Protocol (IIOP) erfolgen.

Ähnliche Konzepte wie CORBA stehen auch in verschiedenen Programmiersprachen zur Verfügung. Zwei der gebräuchlichsten Möglichkeiten in diesem Zusammenhang sind RMI (Remote Method Invocation) und DCOM (Distributed Component Object Model). Das aus dem Java-Umfeld stammende RMI erlaubt den Aufruf von entfernten Java-Methoden. DCOM stellt ein objektorientiertes RPC-System auf dem DCE-Standard zur Verfügung. Bei DCE (Distributed Computing Environment) handelt es sich um einen Industriestandard für verteilte Anwendungen, welches auf dem Client-Server-Modell basiert.

Da offene Architekturen mit Funktionsaufrufen über Systemgrenzen hinweg eine Vielzahl an Schnittstellen bieten, muss besonderes Augenmerk darauf gelegt werden, wer auf diese Schnittstellen zugreifen darf und welche Daten übertragen werden. Sicherheitsaspekte, insbesondere die Authentisierung von Teilnehmern, werden in der CORBA Security Specification abgedeckt.

# M 5.160 Authentisierung gegenüber Webservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um die Identität von Benutzern feststellen und ihnen entsprechende Rechte zuteilen zu können, gibt es unterschiedliche Mechanismen, die in den folgenden Abschnitten vorgestellt werden. Hat sich ein Benutzer erfolgreich authentisiert (beispielsweise durch Angabe von Benutzername und Passwort), so wird ihm eine sogenannte Session zugewiesen. Bei einer Session handelt es sich um eine Sitzung, die einem Benutzer zugeordnet ist und die eine zum Server hergestellte aktive Verbindung bezeichnet. Sessions sind notwendig, da das bei Web-Anwendungen verwendete Protokoll (HTTP) zustandslos ist. Jede Anfrage an einen Webserver wird unabhängig von allen anderen zuvor eingetroffenen Anfragen bearbeitet. Um bei Web-Angeboten dennoch von Benutzern abhängige Zustände abbilden zu können (z. B.den Anmeldestatus eines Benutzers oder den Inhalt eines Warenkorbs), werden Sessions verwendet.

Eine Session wird durch eine eindeutige Session-ID identifiziert. Diese wird nach einer erfolgreichen Anmeldung zum Client übertragen und bei jeder weiteren Anfrage an den Server wieder mitgesandt. Dadurch erkennt der Webserver, dass die Anfrage in einem bestimmten Kontext steht und kann sie einem Benutzer zuordnen.

### Formular-basierte Authentisierung

Die Formular-basierte Authentisierung ist eine weit verbreitete Authentisierungsmethode und wird bei den meisten Web-Anwendungen eingesetzt. Dabei werden die Anmeldedaten über ein Formular an die Web-Anwendung übergeben. Die Authentisierung des Benutzers erfolgt dann durch die Web-Anwendung, welche überprüft, ob die übergebenen Anmeldedaten für den angegebenen Benutzer korrekt sind. Der Vorteil dieser Art der Authentisierung ist die nahtlose Einbindung der Anmelde-Funktion in eine Web-Anwendung, da die Angabe der Anmeldedaten einfach über Eingabefelder in der Web-Anwendung erfolgt. Da die Authentisierung durch die Web-Anwendung vorgenommen wird, ist zudem eine sehr flexible Handhabung von Anmeldeversuchen (z. B. Handhabung von fehlgeschlagenen Anmeldeversuchen, Fehlermeldungen) möglich. Eine erhöhte Flexibilität birgt allerdings auch das Problem von Schwächen in der Implementierung mit sich. So muss beispielsweise darauf geachtet werden, dass die Anmeldedaten über eine gesicherte Verbindung übertragen werden.

### Basic Access Authentication

HTTP Basic Access Authentication wurde im Rahmen von HTTP/1.0 in RFC 1945 spezifiziert und stellt einen einfachen Authentisierungsmechanismus zur Verfügung. Der Anmeldevorgang wird dabei jedoch nicht über die Web-Anwendung, sondern durch den Webserver selbst durchgeführt. Die Anmeldedaten werden dabei nur Base64-codiert und nicht verschlüsselt versendet, weshalb diese Art der Authentisierung nur über eine gesicherte Kommunikation benutzt werden darf. Ist der Angreifer in der Lage, die Kommunikation abzuhören, so kann dieser die Kodierung umkehren und Benutzername und Passwort im Klartext auslesen. Basic Access Authentication bietet einen Schutz auf Verzeichnis-Ebene, da definiert werden kann, welcher Benutzer welche Zugriffsfunktionen auf welche Verzeichnisse anwenden darf. Diese Art der Authen-

tisierung wird von allen gängigen Webservern und Browsern unterstützt, gilt jedoch als veraltet und wird kaum noch verwendet.

**Digest Access Authentication**

Digest Access Authentication basiert auf der Basic Access Authentication, wurde jedoch um Sicherheitsfunktionen erweitert. So werden beispielsweise anstatt der Anmeldedaten nur noch eine entsprechende MD5-Prüfsumme übertragen. MD5 kann zwar nicht mehr für alle Anwendungsgebiete als sicher angesehen werden. Die Möglichkeit zum Auffinden von Kollisionen, die bei MD5 besteht, hat jedoch auf die Authentisierung keine Auswirkung, da hier Zufallszahlen verwendet werden. In die MD5-Prüfsumme fließt die bei jedem Authentisierungsversuch neu vom Server bestimmte Zufallszahl ein. Auf diese Weise kann eine sichere Authentisierung auch über ungesicherte Kanäle erfolgen. Spezifiziert ist die Digest Access Authentication in RFC 2617.

**Host-basierte Authentisierung**

Bei der Host-basierten Authentisierung werden die Zugriffsrechte auf Basis der IP-Adresse bestimmt. Diese Art der Authentisierung ist jedoch anfällig für IP-Spoofing. Dabei fälscht ein Angreifer die IP-Adresse der von ihm gesandten Netzpakete, wodurch die darin enthaltenen Anfragen unter anderen Zugriffsrechten ausgeführt werden.

**Zertifikate**

Zertifikat-basierte Authentisierung basiert auf einer Public-Key-Infrastruktur. Der Nachweis der Identität erfolgt dabei über ein Zertifikat, welches den öffentlichen Schlüssel einer Entität (z. B. Benutzer) beinhaltet und von einer Zertifizierungsstelle signiert sein muss. Die Zertifizierungsstelle ist somit auch für die Verifizierung der Identität vor Signieren des Zertifikats verantwortlich. In der Regel wird dies von einer eigenen Registrierungsstelle erledigt.

Meist kommt bei der Zertifikat-basierter Authentisierung ein sogenanntes Zwei-Faktor-Verfahren zum Einsatz. Dies bedeutet, dass zum Nachweis der Identität nicht nur der Besitz des Zertifikats, sondern auch ein weiterer Faktor, typischerweise ein Passwort, erforderlich ist. Je nach Anwendungsgebiet kann die Speicherung des Zertifikats auf unterschiedlichen Medien erfolgen. Beispiele hierfür sind Token, Chipkarten oder Software-Zertifikatsspeicher.

**Cookies**

Cookies sind in der Regel kleine Text-Dateien, die Informationen über HTTP-Sitzungen lokal auf Client-Seite speichern. Diese werden bei erneuten Anfragen an einen Webserver in der HTTP-Kopfzeile mitgesendet und erlauben somit dem Server ein Wiedererkennen des Clients. Der Server kann mit Hilfe des Cookies beispielsweise erkennen, welcher Benutzer eine Anfrage sendet.

Im Cookie können außer einer eindeutigen ID noch andere Informationen gespeichert werden. Ein Beispiel hierfür ist die Angabe, für welche Domain und welchen Pfad ein Cookie gültig ist. Da das Mitsenden von Cookies vom Browser geregelt wird, ist dieser auch dafür verantwortlich, dass sie nur von der zugehörigen Domain, wie vom Server definiert, ausgelesen werden können. Cookies können zusätzlich Flags enthalten. Wird das httponly-Flag gesetzt, so kann das Cookie von JavaScript nicht mehr gelesen oder verändert werden.

Mit Hilfe von Cross-Site Scripting ist es möglich, Cookies von anfälligen Domains zu stehlen und sich damit beispielsweise gegenüber einem Webserver als ein anderer Benutzer auszugeben. Ein Angreifer schleust dabei Code in

die Web-Anwendung ein, welcher auf dem Client des Benutzers ausgeführt wird und dem Angreifer das gewünschte Cookie im Hintergrund übermittelt.

# M 5.161 Erstellung von dynamischen Web-Angeboten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um dynamische Web-Angebote zur Verfügung stellen zu können, ist eine Programmlogik auf Server-Seite notwendig. In vielen Fällen kann diese Funktion vom Webserver übernommen werden, z. B. über einfache Skripte oder Server Side Includes (SSI). Bei komplexen Web-Angeboten wird jedoch häufig ein Web-Anwendungsserver mit einem entsprechenden Framework eingesetzt. Der Web-Anwendungsserver muss jedoch nicht notwendigerweise vom Webserver getrennt sein, da viele gängige Webserver bereits einen Web-Anwendungsserver integriert haben (z. B. Tomcat bei Apache). Die Web-Anwendungsserver beziehungsweise die zugehörigen Frameworks erlauben die Realisierung von umfassenden Web-Angeboten. Darüber hinaus wird durch diese der Zugriff auf Hintergrund- oder Alt-Systeme wesentlich vereinfacht. Häufig eingesetzte Programmiersprachen und Frameworks für dynamische Web-Angebote werden in den folgenden Abschnitten beschrieben.

### CGI

CGI ist das Akronym für Common Gateway Interface und ist eine Methode, um Web-Seiten dynamisch und interaktiv zu gestalten. Die Generierung von dynamischen Inhalten wird dabei über externe Anwendungen, die vom Webserver aufgerufen werden, realisiert. Für diese Aufrufe stellt CGI eine Schnittstelle zwischen Webserver und System-Anwendung zur Verfügung. Es handelt sich daher bei CGI um keine Programmiersprache, sondern lediglich um eine Funktionalität, um Programme vom Webserver aus auszuführen. CGI-Programme können daher mit beliebigen Programmiersprachen erstellt werden, sofern sich diese vom Webserver aus aufrufen lassen. Abhängig von der verwendeten Technik liegt eine CGI-Applikation entweder als Binärdatei oder als Skript vor. Typische Beispiele für CGI-Sprachen sind C, Perl, TCL, Unix-Shell und viele andere mehr.

Da die dynamischen Funktionen von CGI-Programmen realisiert werden, müssen diese auch das benötigte Sicherheitsniveau gewährleisten. Dies bedeutet beispielsweise, dass die Überprüfung von Parametern von jedem CGI-Programm selbst durchgeführt werden muss.

### SSI

Ähnlich wie CGI sind auch Server Side Includes (SSI) eine Methode, um dynamische Seiten zu erzeugen. SSI erlauben es, beliebige Dateien oder die Rückgabewerte von Systembefehlen in ein Web-Angebot einzubinden. Die Möglichkeiten, dynamische Web-Angebote zu gestalten, sind jedoch mit SSI eher begrenzt, weshalb SSI heute nur noch wenig in Verwendung ist.

Analog zu CGI ist es auch bei SSI möglich, Schwachstellen über die eingebunden Systembefehle auszunutzen. Kann beispielsweise der Pfad einer eingebundenen Datei beeinflusst werden, so können bestimmte Dateien auf dem Server ausgelesen beziehungsweise Befehle auf dem System ausgeführt werden.

**PHP**

PHP (Akronym für "PHP: Hypertext Preprocessor") ist eine Skript-Sprache, die es ermöglicht, dynamische Web-Angebote zu realisieren. Seit Version 4 wurde PHP um Aspekte der objektorientierten Programmierung erweitert. Wesentliche Eigenschaften von PHP sind die leichte Erlernbarkeit und die breite Unterstützung für Datenbankanbindungen.

Zudem bietet PHP eine Vielzahl an Sicherheitsfunktionen. Beispielsweise erlaubt die Verwendung von sogenannten Magic Quotes ein automatisches Erkennen und Maskieren von potenziell gefährlichen Zeichen. Auf diese Weise können viele gebräuchliche Angriffe erschwert werden. Eine weitere Sicherheitsfunktion ist das Open Base Dir, welches den Zugriff auf Dateien außerhalb eines definierten Verzeichnisses verhindert, wodurch auch die Möglichkeiten für einen Angreifer eingeschränkt sind. PHP erlaubt zudem eine Restriktion von potenziell gefährlichen Funktionen. Mit Hilfe des sogenannten Safe-Mode ist eine Einschränkung von zahlreichen Rechten möglich. Dies ist vor allem in einer Multi-Domain-Umgebung sinnvoll, in welcher mehrere Web-Angebote auf demselben Server betrieben werden.

Trotz dieser Sicherheitsfunktionen gibt es aufgrund verschiedener Funktionen (z. B. register_globals) auch einige Probleme in PHP. Diese Funktion ermöglicht beispielsweise beim Aufruf eines PHP-Skripts die Angabe von beliebigen Variablen, wodurch es einem Angreifer erleichtert wird, das Web-Angebot zu kompromittieren. In der Vergangenheit sind in PHP eine Vielzahl von Schwachstellen aufgetreten.

Neben PHP konnten sich noch weitere Skriptsprachen für die Realisierung von dynamischen Web-Angeboten etablieren. Die bekanntesten Beispiele sind Ruby, Python und Perl. Im Wesentlichen bieten all diese Skriptsprachen ähnliche Funktionen und sind daher auch ähnlichen Sicherheitsproblemen ausgesetzt. Es hat sich gezeigt, dass ein Großteil der bekannten Schwachstellen in Web-Anwendungen unabhängig von der verwendeten Programmiersprache ist.

**JSP (Java Server Pages)**

Java Server Pages werden in erster Linie für die Präsentationsschicht von Java-Web-Anwendungen verwendet. Die darzustellenden Daten werden meist in sogenannten JavaBeans (Container zur Datenübertragung) abgelegt, welche einen einfachen Zugriff erlauben. Es ist jedoch auch möglich, Geschäfts-Logik in JSP-Seiten zu implementieren. Dies führt allerdings zu einer unsauberen Trennung zwischen Funktion und Darstellung der Daten und steht auch im Gegensatz zum Model-View-Controller-Ansatz. Dieser sieht eine klare Trennung zwischen Daten, Funktion und Präsentation vor.

**J2EE**

Die Java Enterprise Edition, abgekürzt J2EE, spezifiziert eine Softwarearchitektur für transaktionsbasierte Java-Anwendungen. Damit ist es möglich, dynamische Inhalte durch das Einbetten von Java-Code in HTML- und XML-Dokumenten zu erstellen.

Java bietet eine Reihe von Sicherheitsfunktionen. So ist Java beispielsweise typensicher, was eine Überprüfung des Datentyps von Variablen und Parametern bei deren Verwendung impliziert. Java verhindert per Design Speicher-Management-Schwachstellen wie Buffer Overflows und Heap Overflows in der Anwendung. Damit ist ein Angreifer nicht mehr in der Lage, die Kontrol-

le über ein Programm zu erlangen, indem er den Speicherbereich des Programms mit manipulierten Eingaben befüllt. Andere Schwachstellen-Klassen stellen jedoch auch in Java eine Gefährdung dar. Mit Hilfe einer sogenannten Sandbox bietet Java jedoch die Möglichkeit, Code in einer sicheren und abgeschotteten Umgebung auszuführen, ohne dass dabei das Betriebssystem gefährdet wird. Mit Hilfe von J2EE Security ist zudem eine restriktive Verwaltung von Systemressourcen möglich.

**ASP/ASP.NET/Mono**

Active Server Pages (ASP) wird vor allem in Microsoft-Umgebungen verwendet, da diese Technologie in erster Linie auf dem Microsoft Internet Information Server lauffähig ist. Bei ASP handelt es sich allerdings nicht um eine eigene Programmiersprache, sondern um ein Framework, welches das Verfassen der Programmlogik in unterschiedlichen Programmiersprachen ermöglicht. ASP wird jedoch nicht mehr weiterentwickelt, sondern wurde durch dessen Nachfolger ASP.NET ersetzt. Mit Mono steht neben der Implementierung von Microsoft auch zusätzlich eine unter Unix lauffähige Variante zur Verfügung.

Für ASP.NET existiert eine Reihe von Sicherheitsfunktionen. Ein Beispiel dafür ist der Gatekeeper-Mechanismus, der aus unterschiedlichen Modulen besteht und verschiedene Sicherheitsfunktionen anbietet (z. B. Filter, Authentisierung, ...). Zudem steht ein eigenes Anti-Cross-Site-Scripting-Framework zur Verfügung. Mit Hilfe eines weiteren Frameworks kann eine rollenbasierte Zugriffskontrolle umgesetzt werden.

**Web-Service**

Ein Web-Service ist mit einer Web-Anwendung vergleichbar. Der Unterschied besteht darin, dass die Ausgabe von Ergebnissen nicht für einen Browser aufbereitet wird, sondern in anders strukturierter Form (z. B. SOAP) zur Verfügung gestellt wird. Durch die Vernetzung von Web-Services kann eine Service-orientierte Architektur (SOA) aufgebaut werden. Dabei werden einzelne Teile einer Anwendung als Web-Service implementiert. Diese können dann fortlaufend von mehreren Anwendungen genutzt werden. Auf diese Weise wird die Wiederverwendbarkeit von Funktionen erhöht und die Wartung der einzelnen Anwendungsteile erleichtert.

Da Web-Services die gleichen Protokolle wie Web-Anwendungen verwenden, sind sie hinsichtlich der Sicherheitsanforderungen mit Web-Anwendungen gleichzusetzen. Es existiert ein eigener Standard für Web-Service-Security (WS-Security). Auf Grund der Offenheit einer Service-orientierten Architektur muss im Vergleich zu geschlossenen Architekturen in besonderer Weise auf Zugriffsschutz geachtet werden. Für die Kommunikation mit Web-Services sind folglich die Anforderungen an Authentizität, Integrität und Vertraulichkeit besonders hoch. Das Abhören von Anfragen und den zugehörigen Antworten im Klartext sowie die Fälschung oder Veränderung von Nachrichten muss verhindert werden.

Die notwendigen Sicherheitsanforderungen können durch entsprechenden Einsatz von kryptografischen Verfahren erreicht werden. Im Sinne einer Service-orientierten Architektur ist es auch möglich, einzelne Sicherheitsmaßnahmen als eigene Services zu implementieren.

Ein wichtiger Begriff im Zusammenhang mit Web-Services ist WSDL (Web Service Description Language). Mit Hilfe von WSDL werden funktionale Angaben zu einem Web-Service gemacht, die erforderlich sind, um einen solchen Service nutzen zu können. Eine WSDL-Datei stellt die Beschreibung

der Schnittstelle eines Web-Services dar. Es legt dar, welche Funktionen das Web-Service zur Verfügung stellt, wie diese aufgerufen werden und welche Parameter zum Aufruf benötigt werden. Eine WSDL-Datei enthält folglich die wesentlichen Informationen (z. B. Zugangspunkt und -protokoll), um die Nutzung von Web-Services zu ermöglichen.

Sicherheitsaspekte in Zusammenhang mit WSDL betreffen vor allem die erforderlichen XML-Parser. Diese sind notwendig, um die an den Web-Service übertragenen Daten zu verarbeiten. Da als Parser oft Eigenentwicklungen zum Einsatz kommen, sind diese für eine Vielzahl von Angriffen anfällig. Dabei werden meist absichtlich falsch gestaltete XML-Nachrichten verwendet, die zum Absturz des Parsers oder des gesamten Web-Services führen können. Ein Beispiel dafür ist eine XML-Bombe. Dabei handelt es sich um ein XML-Dokument, dessen Teilelemente mehrfach auf sich selbst referenzieren, wodurch Probleme beim Einlesen des Dokuments durch den Parser entstehen können.

Eine weitere Bedrohung für Web-Services ist das Ausspähen und Wiedereinspielen von unzureichend geschützten SOAP-Nachrichten (ein sogenannter Replay-Angriff). Dabei werden bereits übertragene und von einem Angreifer aufgezeichnete SOAP-Nachrichten beliebige weitere Male übermittelt und dadurch die Anweisungen eines legitimen Benutzers auf dem Server erneut zur Ausführung gebracht. Durch den Vorgang können Datenbestände auf der Seite des Servicebetreibers unautorisiert geändert oder gelöscht werden.

**AJAX/Atlas**

Atlas ist ein Framework für AJAX (Asynchronous JavaScript and XML), welches als Web-Service läuft. Mit Hilfe dieser Technologie wird versucht, Programme, die bisher nur auf PCs eingesetzt wurden, als Web-Anwendung nachzubilden. Dies bedeutet, dass Teile von Web-Seiten nachgeladen werden können, ohne dass der Rest der Seite erneut aufgebaut werden muss. Damit wird im Gegensatz zu herkömmlichen Anwendungen eine viel bessere Performance erzielt.

Der Einsatz von AJAX wird allerdings nicht empfohlen, da hierfür Benutzer auf den Clients Aktive Inhalte zulassen müssen. Bei der Verwendung Aktiver Inhalte bestehen vor allem Gefahren durch Session Riding und Cross-Site-Scripting.

**Streaming Services**

Mit Hilfe von Streaming Services werden in erster Linie Audio- und Videodaten zu Clients übertragen. Dies erfordert auf der Client-Seite jedoch die Verwendung spezieller Programme oder Plug-Ins für den Browser. Um Berechtigungskonzepte für die dargestellten Inhalte durchsetzen zu können, werden oft sogenannte Digital-Rights-Management-Systeme (DRMS) verwendet. Diese stellen beispielsweise sicher, dass ein Client Daten nur dann anzeigen oder kopieren kann, wenn er die entsprechenden Rechte in Form einer Lizenz besitzt.

Streaming Services verwenden ein Reihe von Protokollen, um Daten an die Clients zu senden. Am gebräuchlichsten sind dabei das Real Time Streaming Protocol (RTSP) und das Resource Reservation Protocol (RSVP).

# M 5.162 Planung der Leitungskapazitäten beim Einsatz von Terminalservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In einem klassischen Client-Server Netz unterliegt die Netzlast zwischen dem Client und dem Server starken punktuellen Schwankungen, beispielsweise während der Übertragung einer Datei. Benötigt die Client-Anwendung jedoch gerade keine neue Information, wird auch keine Bandbreite benötigt.

In einer Terminalserver-Umgebung hingegen, müssen oft auch dann Daten über das Netz übertragen werden, wenn sich nur geringfügige Änderungen an der Benutzersicht ergeben. Dafür ist der Datenstrom insgesamt leichter zu kontrollieren. Einerseits können Ein- und Ausgabedaten effektiv komprimiert und durch Bandbreitenmanagement begrenzt werden, andererseits entsteht zwischen dem Terminal und dem Terminalserver für jeden Benutzer nur ein einzelner Datenstrom pro Sitzung. Vom Terminalserver gehen dann gegebenenfalls Verbindungen etwa zu Datei-, Datenbank- oder E-Mail-Diensten aus. Die Dateien selbst verlassen hierbei zu keiner Zeit den Terminalserver, sondern werden lediglich auf dem Client angezeigt.

Die erforderlichen Bandbreiten für die verschiedenen Umsetzungen des Terminalserver-Konzepts variieren sehr stark. Sitzungen mittels RDP sind im Schnitt mit 250 kbit/s zu veranschlagen, Citrix empfiehlt 160 kbit/s für das dort verwendete ICA Protokoll, X11 nimmt ohne zusätzliche Maßnahmen sogar um 4 bis 5 Mbit/s in Anspruch. Ein typisches 100 Mbit Netz ist so bereits mit 15 aktiven X-Window Terminals ausgelastet, da 30% zusätzlicher Bedarf für das darunter liegende TCP/IP Protokoll mit einkalkuliert werden muss. Durch Kompression und Puffer-Mechanismen mit Proxysystemen, wie NX oder FreeNX, kann die Datenmenge jedoch effektiv auf durchschnittlich 40 kbit/s reduziert werden.

Die hier genannten Werte sind für die Planung lediglich als grobe Richtwerte zu verstehen. In der Praxis ist es daher unbedingt notwendig, die konkrete Anwendungssituation zu analysieren. Applikationen, die eine rasche Aktualisierung großer Bereiche des Bildschirminhaltes erfordern, belasten das Netz naturgemäß wesentlich stärker als solche, bei denen sich nur gelegentlich einzelne Zeichen in Benutzerdialogen ändern. Grafisch aufwändige Benutzeroberflächen reduzieren ebenso die Anzahl der über eine gegebene Leitungskapazität bedienbaren Benutzer, wie das Verhalten der Anwender selbst maßgeblich das Belastungsprofil des Netzes beeinflusst.

Falls für das geplante Szenario im Vorfeld keine genauen Erfahrungswerte vorliegen, sollten daher bei größeren Installationen realistische Tests der konkreten Konfiguration durchgeführt werden, so dass fundierte Aussagen über die zu erwartenden Datenmengen und die dafür notwendigen Netz-Ressourcen getroffen werden können. Dies kann, entweder in Feldtests mit realen Benutzergruppen, oder durch synthetische Tests mit Hilfe von skriptgesteuerten Zugriffssimulationen geschehen. In beiden Fällen sind vor der Auswertung Reaktionszeiten festzulegen, die nicht überschritten werden dürfen.

Darüber hinaus sollten Reserven geschaffen werden, so dass höhere Anforderungen in der Zukunft, etwa durch eine Expansion der Benutzerzahl oder

Anwendungsaktualisierungen im gewissen Rahmen abgefedert werden können.

Wird bei der Bedarfsermittlung festgestellt, dass die vorhandenen Leitungskapazitäten zu den einzelnen Terminals nicht ausreichend dimensioniert sind, da sie mit anderen im Netz bereitgestellten Diensten konkurrieren, bietet der Einsatz von Bandbreitenmanagement die Möglichkeit, durch Priorisierung des Datenverkehrs Engpässe zu beseitigen. Daneben sind Terminalserver besonders geeignet, dem Benutzer am Arbeitsplatz schnelle Speichernetze mit verhältnismäßig geringem Aufwand zur Verfügung zu stellen. Die Anbindung nachgelagerter Dienste kann so über ein zweites Netz, z. B. mit besonders leistungsfähigen Techniken wie iSCSI oder Fibre Channel, direkt am Terminalserver erfolgen und damit das Netz zwischen dem Terminal und dem Terminalserver nachhaltig entlasten.

Insbesondere bei der Bereitstellung von Terminalserver-Diensten über WAN Strecken (Wide Area Network), ist neben der Bandbreite die Latenz einer Verbindung von erheblicher Bedeutung. Da die Bildschirmausgabe der Applikationen nahezu synchron mit der Verarbeitung auf dem Terminalserver verläuft, sind kurze Paketlaufzeiten auf das entfernte System entscheidend für ein verzögerungsfreies Arbeiten. Ein höheres Datenaufkommen aufgrund von zusätzlichen Protokollschichten, z. B. von verschlüsselten Fernzugängen in VPN-Systemen, ist dabei genauso zu berücksichtigen, wie Fehlerkorrekturmechanismen der Leitungsanbieter, die die Signallaufzeiten zusätzlich negativ beeinflussen können.

Prüffragen:

- Wurde die erforderliche Bandbreite, die zu erwartende Zahl der Nutzer und die maximale Anzahl paralleler Sitzungen für den Zugriff auf den Terminalserver ermittelt?
- Werden über das gleiche Netz noch andere Dienste bereitgestellt, die die verfügbare Bandbreite oder Latenz reduzieren? Wurde in diesem Fall überprüft, ob diese die Terminalserver-Nutzung beinträchtigen?
- Für den Fall, dass anderer Netzverkehr die Terminalserver-Nutzung über das tolerierbare Maß hinaus beeinträchtigen kann, wurden Maßnahmen ergriffen, um die Auswirkungen angemessen zu kompensieren?

# M 5.163 Restriktive Rechtevergabe auf Terminalservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Innerhalb von Mehrbenutzerumgebungen, wie sie Terminalserver-Systeme darstellen, ist die Abschottung der Anwender gegeneinander sowie gegenüber riskanten Systemfunktionen von erheblicher Bedeutung. Zur Gewährleistung eines störungsfreien Betriebs und zum Schutz der Vertraulichkeit, der innerhalb einzelner Benutzersitzungen verarbeiteten Daten, müssen die Rechte restriktiv vergeben werden.

Der Terminalserver-Dienst beispielsweise unter Microsoft Windows Server 2003 bietet hierzu bereits während der Installation Auswahlmöglichkeiten an, um diverse Schutzmaßnahmen im Betriebssystem zu etablieren. Diese Einstellungen wirken ebenfalls, wenn Citrix Presentation Server als Terminalserver-Lösung eingesetzt wird.

Die sicherere Basisinstallation ist dabei stets als Ausgangspunkt für weitere Schutzmaßnahmen zu verwenden. Sie wird durch die Option *Full-Security* anstatt *Relaxed-Security* ausgewählt. *Relaxed-Security* ist in diesem Zusammenhang als Kompatibilitätsmodus zu verstehen, der den Betrieb von Anwendungen ermöglicht, die nicht für aktuelle Terminalserver-Umgebungen entwickelt wurden. Die Verwendung dieses Modus führt jedoch zu sicherheitskritischen Dateiberechtigungen in Systemverzeichnissen und weitreichenden Zugriffsmöglichkeiten auf die Registrierungsdatenbank (Windows Registry).

Der Einsatz des Modus *"Relaxed-Security"* sollte daher nur in begründeten Ausnahmefällen und nach einer genauen Bewertung der individuellen Gefährdungslage in Betracht gezogen werden. In jedem Fall sind die Rechte für Applikationen und deren Benutzer nachträglich auf das unbedingt notwendige Maß zu reduzieren. Diesbezüglich können beispielsweise Werkzeuge herangezogen werden, die Dateioperationen der Software überwachen und Zugriffe auf die Registrierungsdatenbank protokollieren.

Es sollte zudem, neben der Anwendung, die diesen unsicheren Modus benötigt, keine weitere Applikation auf dem gleichen Terminalserver bereitgestellt werden.

Anwendungen auf Terminalservern können auf verschiedenen Wegen genutzt werden. Neben dem Zugriff mittels Terminalsoftware auf eine vollständige Benutzeroberfläche (Desktop), besteht die Möglichkeit der Übermittlung einer Liste autorisierter Anwendungen. Nur diese stehen dann für den Benutzer innerhalb des Terminalserver-Clients oder auf einem Webserver zur Verfügung.

Dieser Publikationsmechanismus beugt Fehlbedienungen vor und erleichtert den Benutzern die Erledigung ihrer Aufgaben, verhindert jedoch vorsätzliche Zugriffe auf Programme außerhalb der Freigabeliste nicht. So können ohne besondere Vorkehrungen unter Umständen über Benutzerdialoge in erlaubten Anwendungen nicht autorisierte Applikationen ausgeführt werden.

Um Terminalserver-Systeme erfolgreich abzusichern, sind daher weitere Punkte zu beachten. Terminalserver-Systeme sind auf dedizierten, gegebenenfalls virtualisierten, Systemen zu installieren, um die Komplexität der Zugangs- und Zugriffsmöglichkeiten auf andere Dienste zu begrenzen. So ist es etwa notwendig, Benutzern von Terminalservern unter Microsoft Windows

Server 2003 lokale Anmelderechte zu geben. Dies führt bei gleichzeitiger Verwendung des Terminalservers als Domänencontroller zu einer Rechteausweitung der Benutzer auf alle Verwaltungsserver, auch auf solche Maschinen, die keine Terminalserver sind. In der Standardkonfiguration installierte und nicht benötigte Dienste sollten folglich deaktiviert werden. Dies betrifft auch etwaig vorhandene Routing-Funktionalitäten.

Neu aufgesetzte Applikationsserver sind vor der Inbetriebnahme auf den jeweils neuesten Softwarestand zu bringen und es wird dringend empfohlen, diese vorher vom Netz zu isolieren. Überdies sind nicht benötigte Benutzerkonten und Gruppen zu entfernen oder zu deaktivieren.

Auf allen Terminalserver-Systemen sollten Anti-Viren-Produkte installiert werden.

Anwendungen mit unterschiedlichen Schutz- und Sicherheitsniveaus sollten auf unterschiedlichen Terminalservern bereitgestellt werden. Ist dies aus organisatorischen Gründen nicht möglich oder sinnvoll, sind alle Applikationen wie die installierte Software mit dem höchsten Schutzbedarf zu behandeln.

Es ist ein Dateisystem zu verwenden, das Zugriffsrechte auf Benutzerebene differenziert, wiez. B.:

- Schreib- und Lesezugriffe auf nicht benötigte Dateien müssen dabei verhindert werden (z. B. durch einfaches Löschen der obsoleten Datei oder durch das Setzen von entsprechenden Berechtigungen).
- Auf die Verwendung von Verweisen innerhalb des Dateisystems (z. B. symbolische Links, NTFS-Joins etc.) sollte, wenn möglich, verzichtet werden.
- Administrationswerkzeuge dürfen nur von autorisierten Administratoren ausgeführt werden können.
- Die Berechtigung, nachträglich Software zu installieren, darf allein den Administratoren obliegen.
- In Terminalserver-Umgebungen sollte die Möglichkeit zur Ausführung von Software in einem fremden Benutzerkontext, etwa durch Befehle wie "runas" oder "sudo" deaktiviert werden.
- Speziell auf Systemen mit hohem Schutzbedarf sollten autorisierte Programme in einer Positivliste geführt werden. Nur Software die dort freigegeben ist, wird vom Betriebssystem dann ausgeführt. Realisiert werden kann dies bei Windows Betriebssystemen beispielsweise mit Appsec. Für Linux können Erweiterungen wie SELinux und AppArmor und für Solaris-Systeme RBAC (Role based access control) und Privileges genutzt werden. Es existieren darüber hinaus einige weitere Lösungen von Drittanbietern, die über den Funktionsumfang der Betriebssystemmittel teilweise hinausgehen.

Mit einer Sitzungsspiegelung, auch Shadowing genannt, ist das Betrachten einer fremden Benutzersitzung gemeint. Die Bildschirmausgabe des Benutzers wird auf einem oder mehreren weiteren Clients angezeigt, eventuell kann auch die Steuerung der Eingabegeräte übernommen werden. Vorwiegend bei Schulungen oder zu Administrationszwecken wird dieses Verfahren eingesetzt. Ohne Kenntnisnahme oder Zustimmung des Anwenders darf eine Sitzungsspiegelung nicht vorgenommen werden. Dies ist in der Konfiguration des Terminalservers administrativ zu erzwingen.

Zum Schutz von nachgelagerten Systemen, wie etwa Systemen zur Datenhaltung oder weiteren verarbeitenden Systemen, sind weitere Maßnahmen mit

dem Fokus auf die Kommunikation der Applikationen zu ihren Backends zu verwirklichen.

Die Applikationsszenarien *spezialisierte Anwendungen* und *allgemeine Anwendungen* sollen dies verdeutlichen.

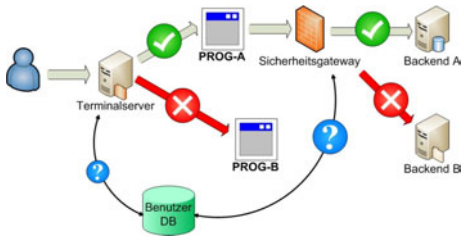



Abbildung: Abschottung nachgelagerter Dienste

**Spezialisierte Anwendungen**

Spezialisierte Anwendungen sind hier als Software ohne frei konfigurierbares Backend definiert.

Das Programm kann weder dazu benutzt werden, mit einem nicht vorgesehenen nachgelagerten System zu kommunizieren, noch ist es für den Benutzer möglich, über einen autorisierten Dienst, Zugang zu einem anderen nicht erlaubten Backend zu bekommen.

In diesem Fall genügen die bereits vorgestellten Methoden zum Absicherung der Umgebung.

Ein Beispiel wäre eine Anwendung, die Zugriff auf eine fest definierte Datenbank hat. Des Weiteren verfügt der Benutzer über keine Eingabemöglichkeiten der Zugangsparameter, außer den Anmeldedaten zu der Vordergrundapplikation (Frontend).

**Allgemeine Anwendungen**

Nicht spezialisierte, also allgemeine Anwendungen wie SQL-Konsolen oder Browser sind hierbei wesentlich sicherheitskritischer. Das trifft insbesondere deshalb auf Terminalserver-Umgebungen zu, da die Terminalserver Zugang zu all den Backends haben müssen, die aufgrund der Anforderungen der Benutzer notwendig sind.

Eine Möglichkeit dieses Problem zu umgehen, besteht darin, solche Programme auf getrennten Terminalservern zu betreiben und diese durch individuelle demilitarisierte Zonen von den verbotenen Hintergrundsystemen zu isolieren.

Bei einer sehr großen Zahl an bereitzustellenden Applikationen wird diese Herangehensweise sehr schnell komplex, unübersichtlich und unwirtschaftlich. Zudem schwinden rasch die Vorteile einer zentralisierten Architektur gegenüber der klassischen Client-Server-Anbindung.

Alternativ kann gegebenenfalls ein Sicherheitsgateway zwischen Terminalserver und dem nachgelagerten Dienst eingesetzt werden, das Kommunikationsbeziehungen auf der Basis von Regeln ermöglicht, welche die Benutzeranmeldung, Anwendung und Backend verknüpfen.

Die Abbildung *Abschottung nachgelagerter Dienste* verdeutlicht diese Vorgehensweise. Dem Benutzer wird hier nur über das Programm Prog-A Zugriff auf das Backend A gewährt und der Zugriff auf Backend B unterbunden.

Prüffragen:

- Werden die Zugriffsrechte der Benutzer auf Ressourcen der Terminalserver restriktiv vergeben?
- Werden die Zugriffsrechte der Benutzer von Terminalservern auf nachgelagerte Dienste (Backends) restriktiv vergeben?
- Wird bei Terminalservern, die im unsicheren "Relaxed-Security" Modus betrieben werden, nur eine Applikation auf einem Terminalserver bereitgestellt?
- Werden Terminalserver-Dienste nur auf dedizierten, gegebenenfalls virtualisierten, Systemen installiert?
- Wurden alle in der Standardkonfiguration installierten und nicht benötigten Dienste, Benutzerkonten und Gruppen auf Terminalservern entfernt oder deaktiviert?
- Wurden auf allen Terminalserver-Systemen Anti-Viren-Produkte installiert?

# M 5.164 Sichere Nutzung eines Terminalservers aus einem entfernten Netz

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Verbinden sich Terminalserver und deren Clients über ein unsicheres Netz, ist primär ein wirksamer Schutz der Netzübergänge durch Sicherheitsgateways zu gewährleisten. Zudem sind Vorkehrungen zu treffen, damit die Kommunikation nicht belauscht, verändert oder gestört werden kann. Das weitere Vorgehen hängt von der Auswahl der nachfolgend differenzierten Verbindungsarten ab.

Einige Terminalserver-Systeme bieten eine protokollinterne Verschlüsselung an. In der Standardkonfiguration ist diese jedoch üblicherweise auf die Anforderungen in lokalen Netzen ausgelegt. Regulär sind daher geringe Schlüssellängen voreingestellt, die in einem kontrollierbaren Netz ausreichen könnten. Häufig wird hier auch auf die bidirektionale Verschlüsselung zwischen Terminal und Terminalserver zugunsten einer Ressourcen schonenderen Verbindung verzichtet. Lediglich die Benutzereingaben, jedoch nicht die von dem Server zurückgesandte Bildschirmausgabe wird dann verschlüsselt. Daneben können innerhalb des Protokolls weitere Datenströme (*Virtual Channels*), etwa zur Anbindung von lokalen Datenträgern, Schnittstellen oder Druckern des Clients, unverschlüsselt eingebettet werden.

Um die Kommunikation über ein unsicheres Netz zu schützen, ist daher vorab zu prüfen, welche kryptographischen Verfahren und Schlüssellängen in der zu betreibenden Konfiguration Verwendung finden und auf welche Elemente der Kommunikation die Verschlüsselung angewendet wird. Eine sichere Kommunikation kann nur dann gewährleistet werden, wenn der gesamte Datenstrom einschließlich der Authentisierung, in Sender- und Empfängerrichtung abgesichert wird. Geeignete Verfahren der protokollinternen Verschlüsselung nutzen dabei derzeit *Secure Socket Layer* (SSL) oder *Transport Layer Security* (TLS) mit mindestens 128 Bit Schlüssellänge.

In die Betrachtung sind sowohl die Einstellungen des Servers, als auch die des Clients einzubeziehen. Hierbei müssen die Einstellungen des Servers und die des Clients überstimmen, um einen gesicherten Verbindungsaufbau administrativ zu erzwingen.

Stehen, wie bei dem X-Window System, keine protokollinternen Verschlüsselungsmechanismen zur Verfügung, kann die Absicherung der Verbindung auch durch einen kryptographisch gesicherten Tunnel realisiert werden. Für das X-Window System hat sich dabei die Methode *X11-Forwarding* mit Hilfe der *Secure Shell* (M 5.64 *Secure Shell*) etabliert. Ferner existiert mit NX eine modifizierte Alternative zum X11-Protokoll, die eine sichere Authentikation und den verschlüsselten Transport von Terminalserver-Sitzungen mit X-Window, RDP und VNC ermöglicht.

Zum Schutz von Terminalserver-Sitzungen kann auch ein virtuelles privates Netz (VPN) einsetzt werden (siehe auch B 4.4 *VPN*). Der Vorteil dieser Vorgehensweise ist die automatische Kapselung aller Elemente des Datenstroms durch das VPN. Auf eine weitergehende Analyse der Sicherheit des Terminal-

serverprotokolls kann hierbei verzichtet werden, da eine sichere Anmeldung und Verschlüsselung durch das VPN garantiert wird.

Bei Verwendung eines VPN ist jedoch zu beachten, dass sich der Zugriff des entfernten Clients auch auf andere Dienste als den des Terminalservers erstrecken kann. Des Weiteren sind protokollinterne Verfahren auf die technischen Besonderheiten der jeweiligen Terminalserver-Umgebung optimiert und können daher in der Regel effizienter die verfügbare Bandbreite nutzen, als virtuelle private Netze.

Über den Schutz des Perimeterbereichs und des Übertragungsweges hinaus sind die betreffenden Client-Systeme zu berücksichtigen. Insbesondere Zugriffe über Rechner in öffentlichen Bereichen, wie Internetcafés, stellen ein hohes Sicherheitsrisiko dar, da Informationen wie der Anmeldename und das Passwort gegebenenfalls durch Dritte mitgelesen werden können. Auch mobile IT-Systeme und stationäre Telearbeitsplätze sind schwer kontrollierbar und können von ihrem ursprünglich autorisierten Softwarestand abweichen.

Daher sind besonders hohe Anforderungen an den Anmeldeprozess zu stellen, wenn der Zugang über unsichere Clients erlaubt werden soll. In diesem Szenario könnte somit mindestens eine Zwei-Faktor-Authentisierung genutzt werden. Hierbei wird beim Autorisierungsvorgang z. B. zusätzlich zu Benutzernamen und Passwort eine nur einmal gültige Kennung, auch *One-Time-Password* (OTP) genannt, verlangt. Diese Kennung kann durch ein mobiles Gerät (Token) erzeugt werden. Der Besitz des Gerätes und das Wissen um Benutzernamen und Passwort sind hierbei sich ergänzende Sicherheitsmerkmale, die dem Missbrauch einer einmalig erspähten Benutzeranmeldung entgegenwirken. Besonders in dem Fall, in dem über Portallösungen, wie zum Beispiel über eine Weboberfläche über das Internet auf Dienste des Terminalservers zugegriffen werden kann, sollte eine Zwei-Faktor-Authentisierung in Betracht gezogen werden.

Darüber hinaus ist es sinnvoll, Abstufungen im Berechtigungskonzept für den Zugriff auf die verschiedenen möglichen Informationskanäle, in Abhängigkeit von der Sicherheit des Clients, einzuführen. Öffentlich zugänglichen IT-Systemen sollte der Dateiaustausch zwischen Terminalserver und Terminal sowie der Zugriff auf Schnittstellen verwehrt bleiben. Zudem sollte es den Benutzern nicht erlaubt sein, Inhalte der Zwischenablage des Servers auf den Client zu übertragen.

Verschiedene Terminalserver-Lösungen bieten eine Analyse des Clients während des Anmeldevorgangs an. Hierbei wird der Hardware- und Softwarestand sowie die Aktualität des Virenschutzes abgefragt und mit den hinterlegten Richtlinien verglichen. Auf diese Weise kann durch eine technische Maßnahme eine Unterscheidung zwischen sicheren und unsicheren Clients getroffen werden.

Prüffragen:

- Ist die Terminalserver-Umgebung durch ein Sicherheitsgateway geschützt?
- Werden alle Informationen zum oder vom Terminalserver in einem verschlüsselten Datenstrom übertragen?
- Wird die Übertragung von Informationen vom Server zum Client über die Zwischenablage unterbunden, wenn der Zugriff auf Terminalserver über unsichere Clients erfolgt?

- Wird eine Zwei-Faktor-Authentisierung z. B. mittels Einmalpasswort verlangt, wenn der Zugriff auf Terminalserver über unsichere Clients erfolgt?

# M 5.165 Deaktivieren nicht benötigter Mac OS X-Netzdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Nicht benötigte Netzdienste sollten deaktiviert werden, da diese Systemressourcen belegen und ein Angriffsziel darstellen können. Dazu sind Administratorrechte notwendig. Wurden Veränderungen an den Systemdiensten vorgenommen, sind diese zu dokumentieren. Weiterhin sollte regelmäßig überprüft werden, ob nur nach dem Sicherheitskonzept zulässige Dienste aktiviert und über das Netz erreichbar sind.

Die verfügbaren Dienste werden in den Systemeinstellungen unter dem Menüpunkt "Freigaben" aufgelistet. Im Regelfall sollte ein Client-Betriebssystem keine oder nur wenige Dienste in einem Netz anbieten. Je nach Einsatzgebiet muss eine individuelle Entscheidung getroffen werden, ob und welcher Dienst aktiviert bleiben sollte.

Zur Verwaltung verwendete Dienste, wie zum Beispiel der "Apple Remote Desktop" (TCP-Port 5900), "entfernte Anmeldung" (SSH-Zugriff, TCP-Port 22) oder Netzdienste des Viren-Schutzprogramms müssen aktiviert bleiben.

Wird in einem Netz der Dienst "Bonjour" nicht verwendet, sollte dieser ebenfalls deaktiviert werden, da er Systemressourcen belegt und einen weiteren Angriffspunkt darstellt.

Mit den folgenden Befehlen wird der Netzdienst Bonjour deaktiviert:

sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.

plist

sudo launchctl unload -w/System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.

plist

Wird das Internetprotokoll in der Version 6 (IPv6) nicht eingesetzt, sollte es ebenfalls deaktiviert werden. Die Mittel, um IPv6 zu deaktivieren, finden sich in den Systemeinstellungen unter "Netzwerk", bei den weiteren Optionen der jeweiligen Netzwerkkarte.

Wird das Betriebssystem aktualisiert, könnten Dienste unbeabsichtigt wieder aktiviert werden. Daher sollte nach jeder Aktualisierung geprüft werden, ob die Dienste weiterhin deaktiviert sind.

Prüffragen:

- Wurden alle nicht benötigten Netzdienste von Mac OS X deaktiviert?
- Wurden die Veränderungen an Mac OS X Systemdiensten dokumentiert?
- Sind die zur Verwaltung von Mac OS X notwendigen Dienste noch aktiv?
- Wird regelmäßig, insbesondere nach Systemaktualisierungen, überprüft, ob nach wie vor nur freigegebene Dienste von Mac OS X über das Netz erreichbar sind?

# M 5.166 Konfiguration der Mac OS X Personal Firewall

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zu den Sicherheitsmechanismen, die Mac OS X mitbringt, gehört eine Personal Firewall. Eine Personal Firewall bietet diverse Sicherheitsfunktionen wie eine Paketfilter-Funktion, um die Netzkommunikation bestimmter ein- und ausgehender Verbindungen des lokalen Systems zu unterbinden.

Bevor die Personal Firewall unter Mac OS X eingesetzt wird, müssen zwei Fakten überprüft werden. Mit der Personal Firewall können ein- oder ausgehende Verbindungen gefiltert werden oder der Zugriff von Programmen und Diensten auf das Internet eingeschränkt werden. Bevor für einzelne Programme die Netzkommunikation abgeschaltet wird, sollte geprüft werden, ob es möglich ist, die Netzkommunikation Programm-intern abzuschalten. Außerdem sollte geprüft werden, ob bei dem jeweiligen Programm oder Dienst nach dem Sperren der Netzkommunikation keine unerwünschten Nebeneffekte auftreten. Wird direkt versucht, mit einer Personal Firewall die Netzkommunikation eines Programms zu unterbinden, können Probleme auftreten, da ein Programm auf die Netzkommunikation angewiesen sein kann und auf eine Antwort aus dem Netz wartet, bevor das Programm weiter ausgeführt wird.

Der Einsatz einer Personal Firewall, die direkt auf dem zu schützenden Client-Computer betrieben wird, ersetzt in keinem Fall ein eigenständiges Sicherheitsgateway (Firewall), dass das gesamte interne Netz der Institution schützt. Um Mac OS X Rechner bei höherem Schutzbedarf vor Angriffen aus dem lokalen Netz zu schützen, kann der Einsatz einer Personal Firewall sinnvoll sein. Bei einem mobilen Einsatz von Mac OS X Rechnern ist die Nutzung einer Personal Firewall immer empfehlenswert, um den Rechner vor Angriffen aus dem Internet zu schützen.

Vor dem Einsatz einer Personal Firewall muss festgelegt werden, welche Programme Netzzugriff erhalten sollen und welche nicht. Generell ist zunächst jegliche Netzkommunikation zu blockieren, im zweiten Schritt werden nur die gewünschten Ports oder Anwendungen freigeschaltet. Bei der Einstellung der Personal Firewall sollte den Empfehlungen in Maßnahme M 4.238 Einsatz eines lokalen Paketfilters gefolgt werden.

Mac OS X bietet zwei Firewalls, die auf unterschiedlichen Ebenen arbeiten:

- Anwendungsfirewall
  Die Anwendungsfirewall ermöglicht das Sperren und das Freigeben der Kommunikation von bestimmten Anwendungsprogrammen. Dazu muss der Anwender nicht wissen, welcher Port verwendet wird. Die Anwendungsfirewall überprüft auch die Signatur eines Programms. Es ist nicht möglich, ein für die Netzkommunikation freigegebenes Programm zu manipulieren, ohne dass eine erneute Firewall-Regeldefinition abgefragt wird. Unter Mac OS X ist die Anwendungsfirewall im Auslieferungszustand deaktiviert. Diese sollte unter "*Systemeinstellungen* | *Sicherheit* | *Firewall*" aktiviert werden. Über den Menüpunkt "*weitere Optionen*" ist es möglich, die Einstellungen anzupassen:
  Mit der Option "*Alle eingehenden Verbindungen blocken*" werden nur die folgenden Mac OS X Datenverbindungs- bzw. Kommunikationsdienste erlaubt:

- configd: Zur Implementierung von DHCP und anderen Netzkonfigurationsdiensten
- mDNSResponder: Zur Implementierung von Bonjour
- racoon: Zur Implementierung von IPSec

  Bemerkung: Werden Freigaben wie beispielsweise "Dateifreigabe" oder "Entferne Anmeldung" aktiviert, öffnet Mac OS X selbstständig die notwendigen Ports in der Firewall, über den die Dienste kommunizieren können.
  Wird die Option "*Alle eingehenden Verbindungen blocken*" nicht verwendet, wird über die Liste der Anwendungsfirewall definiert, welche Dienste und Programme zum Öffnen von Ports in der Firewall berechtigt sind. Mit einem Mausklick auf das "+"-Symbol können Programme dieser Liste hinzugefügt werden. Nachdem ein Programm zu dieser Liste hinzugefügt wurde, muss definiert werden, ob eingehende Verbindungen für dieses Programm erlaubt oder blockiert werden sollen. Auch Befehlszeilenprogramme können zu dieser Liste hinzufügt werden. Beim Hinzufügen einer Anwendungssoftware zu dieser Liste ergänzt Mac OS X das Programm um eine digitale Signatur, falls dies nicht zuvor schon einmal geschehen ist. Wird ein Programm nachträglich verändert, dass sich in der Liste befindet, wird der Anwender erneut aufgefordert, für das Programme eingehende Netzverbindungen zu erlauben oder zu blockieren. Auch für Programme ohne digitale Signatur, die sich nicht in dieser Liste befinden, wird dem Anwender ein Dialogfeld mit Optionen zum Erlauben oder Blockieren von Verbindungen angezeigt. Sobald der Anwender die Verbindungen erlaubt oder blockiert, versieht Mac OS X das Programm mit einer digitalen Signatur und fügt es automatisch, einschließlich der vergebenen Berechtigungen, zur Liste der Anwendungsfirewall hinzu.
  Wird die Option "*Signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen*" aktiviert, können alle Programme, die mit einer digitalen Signatur versehen sind, eingehende Verbindungen empfangen, auch wenn die Programme nicht in der Liste angezeigt werden. Diese digitale Signatur muss von einer Zertifizierungsstelle (CA) ausgestellt worden sein, der Apple vertraut. Seit der Version Leopard wurde jede ausführbare Betriebssystemkomponente von Apple mit einer digitalen Signatur versehen und kann eingehende Verbindungen empfangen. Auch digital signierte Programme, die automatisch von anderen Programmen geöffnet werden, können zu dieser Gruppe gehören. Soll der Netzzugriff eines Programms mit einer digitalen Signatur über die Firewall blockiert werden, muss das Programm zuerst zur Application Firewall Liste hinzufügt und dann ausdrücklich die Verbindungen blockiert werden. Wird der Zugriff eines Programms über die Firewall blockiert, kann das zu Störungen des Programms oder anderer, darauf basierender Programme führen oder die Leistung anderer verwendeter Programme und Dienste beeinflussen. Da diese Option nicht transparent ist, sollte von der Verwendung abgesehen werden.
  Die Option "*Tarn-Modus aktivieren*" sollte nicht verwendet werden, da diese Option dem Internetstandard RFC1122 widerspricht. Durch einen aktivierten Tarn-Modus werden keine Antworten auf Anfragen gesendet, die von einer blockierten Anwendung ausgehen. Ping ist beispielsweise eine der ICMP-Nachrichten, die durch den Tarnmodus nicht mehr funktionieren. Der Tarn-Modus bietet darüber hinaus aber keinen Schutz. Wäre der Rechner tatsächlich nicht vorhanden, würde die letzte Station vor dem Rechner an den Sender melden, dass das Ziel nicht erreichbar ist. Im Tarnmodus kommt jedoch keine Nachricht zurück. Daraus kann der Sender schließen, dass der Rechner da ist, aber nicht antwortet.
- Der Paketfilter bzw. IP-Firewall (ipfw)

  Die andere bei Mac OS mitgelieferte Personal Firewall ist die IP-Firewall (ipfw) beziehungsweise der Paketfilter. Der Paketfilter arbeitet auf einer

niedrigeren OSI-Schicht und hat Vorrang vor der Anwendungsfirewall. Die IP-Firewall ipfw ist nur für das Internet-Protokoll in der Version 4 geeignet, soll der Datenverkehr von IPv6 kontrolliert werden, kann die Kommandozeilenapplikation IP6FW eingesetzt werden. Werden beide Versionen des Internet-Protokolls eingesetzt, so sind zwangsläufig mehrere Dateien für die Konfiguration der Firewall notwendig, wobei sich der Unterschied größtenteils auf die Adressformate von IPv4 und IPv6 beschränkt.

Die IP-Firewall und die Anwendungsfirewall können parallel betrieben werden und ermöglichen zusammen eine umfassende Regelung der Netzkommunikation. Die Anwendungsfirewall kann in den Systemeinstellungen unter Sicherheit in dem Menüreiter "*Firewall"* aktiviert und konfiguriert werden.

Mit ipfw ist es möglich, feinere Regeln zu definieren, als mit der Anwendungsfirewall. Die Handhabung ist etwas komplizierter, da sie über die Kommandozeile konfiguriert wird.

Um mit ipfw eine TCP-Verbindung zu verschiedenen Servern auf Port 80 zu blockieren, kann folgender Befehl verwendet werden:

ipfw add 500 deny tcp from any to any dst-port 80

Jede Firewall-Regel hat eine Nummer und wird von der höchsten bis zur niedrigsten Nummer vom System abgearbeitet. Somit kann eine Regel durch eine andere Regel verändert oder ungültig werden. Da ipfw sehr systemnah arbeitet, sind Administrationsrechte notwendig, um Befehle auszuführen. Wird ein umfangreiches Firewall-Regelwerk erstellt, so sollte der Inhalt in eine Konfigurationsdatei ausgelagert werden. Um die Regeln aus dieser Konfigurationsdatei automatisch zu laden, ist ein Shellscript notwendig, das wie folgt aussehen kann:

#!/bin/sh

# bisherige FW-Regeln entfernen

/sbin/ipfw -q flush

#IPFW ausführen und Regeln aus Datei laden

/sbin/ipfw -q /ABLAGEORT/Firewall-Regelwerk.conf

# Logging nach /var/log/system.log aktivieren

/usr/sbin/sysctl -w net.inet.ip.fw.verbose=1

Anschließend müssen entsprechende Rechte auf das Shellscript vergeben werden, damit die Befehle ausgeführt werden können:

sudo chown root:admin Shellscript.sh

sudo chmod 544 Shellscript.sh

Nach diesem Schritt muss das Shellscript bei jedem Computerstart ausgeführt werden. Unter Mac OS X wird von Apple die Verwendung von "*launchd*" für diese Aufgabe empfohlen. Der Systemdienst "*launchd*" benötigt zum Starten von Programmen eine speziell formatierte Datei (Plist) im Verzeichnis */Library/LaunchDaemons*. Der Inhalt dieser Datei sieht wie folgt aus:

<?xml version="1.0" encoding="UTF-8"?>

<?DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

<key>Label</key>

<string>com.apple.firewall</string>

<key>ProgramArguments</key>

<array>

<string>/usr/local/bin/Shellscript.sh</string>

</array>

<key>RunAtLoad</key>

<true/>

</dict>

</plist>

Als letzten Schritt muss diese Plist-Datei entsprechende Rechte erhalten, beispielsweise mit dem folgenden Befehl:

sudo chown root:admin NameDer.plist

Die Änderungen können direkt ohne vorangegangenen Neustart mit dem folgenden Befehl eingelesen und aktiviert werden:

sudo launchctl load /Library/LaunchDaemons/NameDer.plist

Die Protokolldatei der Personal Firewall, zu finden unter */private/var/log/ipfw.log,* sollte regelmäßig auf Auffälligkeiten, zum Beispiel auf eine hohe Anzahl fehlgeschlagener Fernzugriffe und Anmeldeversuche, überprüft werden. Firewall-Logdateien können sehr schnell wachsen und eine erhebliche Menge an Speicherplatz belegen. Es ist daher sinnvoll zu klären, welche Regeln eine hohe Priorität haben und protokolliert werden sollten und welche nicht. Ein entsprechender Befehl kann wie folgt aussehen:

ipfw allow log tcp from any to any dst-port 6112-6119

Mit diesem Befehl werden alle Verbindungsversuche zu einem Server auf TCP-Basis zu Port 6112 bis 6119 protokolliert.

Prüffragen:

- Wurde festgelegt, welche Programme unter Mac OS X Netzzugriff erhalten?
- Wurde die Personal Firewall von Mac OS X aktiviert und entsprechend den Empfehlungen eingestellt?
- Wird die Protokolldatei der Personal Firewall von Mac OS X regelmäßig auf Auffälligkeiten untersucht?

# M 5.167 Sicherheit beim Fernzugriff unter Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Mac OS X ab der Version Panther (10.3) beinhaltet den Netzdienst Apple Remote Desktop zur Fernwartung. Die Serverkomponente basiert auf dem Virtual Network Computing (VNC)-Protokoll und ist in der Lage ist, mit jedem VNC-Client zu kommunizieren, unabhängig von Betriebssystem und Hersteller.

Die Client-Komponente wurde jedoch erst ab der Mac OS X Version Leopard (10.5) in das Betriebssystem als "Bildschirmfreigabe" integriert. Ist die Bildschirmfreigabe in den Systemeinstellungen unter dem Menüpunkt "Freigaben" aktiviert, so kann jeder mit entsprechenden Zugriffsberechtigungen auf das IT-System unter Mac OS X zugreifen. Um die Sicherheit zu erhöhen, sollten die Option "*VNC-Benutzer dürfen den Bildschirm mit dem folgenden Kennwort steuern*" aktiviert und triviale Passwortformen vermieden werden (siehe M 2.11 *Regelung des Passwortgebrauchs*). Weiterhin darf die Bildschirmfreigabe nur ausgewählten Benutzergruppen zugänglich sein.

Ab Mac OS X Leopard (10.5) wird die verschlüsselte Übertragung der Fernsteuerungsdaten über VNC unterstützt, welche auch aktiviert werden sollte. In den Einstellungen der Bildschirmfreigabe auf Clients ist dann die Option "*Alle Netzwerkdaten verschlüsseln (sicherer)*" zu wählen, um nicht nur Kennwörter und Tastatureingaben zu verschlüsseln, sondern die gesamte Datenübertragung.

Unterstützt die VNC-Software keine verschlüsselte Datenübertragung oder wird ein älteres Mac OS X Betriebssystem eingesetzt, so empfiehlt sich die Nutzung eines SSH-Tunnels oder eines VPNs zur sicheren Datenübertragung.

Prüffragen:

- Ist für die Bildschirmfreigabe von Mac OS X stets ein Passwort notwendig?
- Wurde der Zugriff auf die Bildschirmfreigabe von Mac OS X nur für bestimmte Benutzergruppen freigegeben?

# M 5.168 Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Webanwendungen und Web-Services verwenden häufig Hintergrundsysteme, zum Beispiel für die Datenhaltung in einer Datenbank oder für die Authentisierung durch einen Identitätsspeicher. Die Daten sind auch bei der Übermittlung und Speicherung in Hintergrundsystemen ausreichend zu schützen. Dazu müssen die Hintergrundsysteme sicher an die Webanwendung oder den Web-Service angebunden sein.

Typische Hintergrundsysteme von Webanwendungen und Web-Services sind:

- Datenbanken,
- Verzeichnisdienste,
- Middleware,
- Web-Services und
- Legacy-Systeme.

Zur sicheren Anbindung von Hintergrundsystemen sollten folgende Punkte beachtet werden:

**Platzierung von und Zugriff auf die Hintergrundsysteme**

Die Benutzer der Webanwendung beziehungsweise Aufrufer des Web-Service sollten nicht direkt auf die Hintergrundsysteme zugreifen können, da so gegebenenfalls Schutzmaßnahmen umgangen werden. Stattdessen sollte der Zugriff ausschließlich über vordefinierte Schnittstellen und Funktionen der Webanwendung oder des Web-Service möglich sein.

Darüber hinaus sollte bei hohem Schutzbedarf die Verbindung zu den Hintergrundsystemen zusätzlich geschützt werden. Hierzu sollten sich die Systeme vor der Datenübertragung authentisieren und die übertragenen Daten verschlüsseln, sodass sie nicht unbemerkt mitgelesen oder geändert werden können (zum Beispiel mittels SSL/TLS; siehe auch M 5.66 *Clientseitige Verwendung von SSL/TLS* und M 5.177 *Serverseitige Verwendung von SSL/TLS*).

Werden die beteiligten IT-Systeme über unsichere Kanäle angebunden, so sollte in jedem Fall ein kryptographisch abgesicherter Tunnel mit entsprechender Verschlüsselung und Authentisierung verwendet werden.

Zugriffe auf Hintergrundsysteme sollten mit minimalen Rechten erfolgen. Hierfür sollten Dienstekonten auf dem jeweiligen Hintergrundsystem eingerichtet werden.

Wird für den Zugriff auf ein Hintergrundsystem ein einziges Dienstekonto verwendet, werden alle Anfragen im Sicherheitskontext dieses Dienstekontos bearbeitet. Dies gilt dann sowohl für Zugriffe von Benutzern mit eingeschränkten Zugriffsberechtigungen als auch für die Zugriffe administrativer Benutzer. Um dies zu verhindern, sollten mehrere Dienstekonten mit unterschiedlichen Zugriffsrechten für ein Hintergrundsystem verwendet werden.

Bei einer geeigneten Systemumgebung (zum Beispiel bei der Verwendung eines Verzeichnisdienstes, der sowohl von der Webanwendung als auch für das Hintergrundsystem zur Verwaltung der Benutzer verwendet wird) können die Benutzerkonten an das Hintergrundsystem weitergeleitet werden. Auf diese Weise können die Privilegien auf die notwendigen Rechte des jeweils an der Webanwendung angemeldeten Benutzers limitiert werden.

Es ist darauf zu achten, dass für unauthentisierte Zugriffe auf die Webanwendung ein eigenes Dienstekonto im Verzeichnisdienst mit eingeschränkten Berechtigungen verwendet wird.

**Enterprise Service Bus**

Im Kontext sogenannter Service-Orientierter Architekturen (SOA) werden Webanwendungen und Web-Services häufig über einen Enterprise Service Bus (ESB) als zentrale Kommunikationsinfrastruktur an Hintergrundsysteme angebunden. Dadurch wird erreicht, dass für jede Anwendung jeweils nur die Schnittstelle zum ESB definiert und realisiert werden muss, und nicht viele separate Schnittstellen zu anderen Anwendungen und Diensten. In einem eigenen Verzeichnis ("Repository") speichert der ESB Metainformationen über die angeschlossenen Dienste.

Zusätzlich kann der ESB auch zentrale Sicherheitsfunktionen realisieren, um die angeschlossenen Anwendungen weiter zu schützen. Solche Sicherheitsfunktionen können beispielsweise Replay-Attacken erkennen und abwehren oder XML-Daten auf potenziell schädliche Inhalte prüfen, aber auch den Nachrichtenaustausch zentral und revisionssicher protokollieren.

Beim Einsatz eines ESB muss sichergestellt werden, dass sich alle Dienste gegenüber dem ESB authentisieren, bevor ihnen ein Zugriff erlaubt wird. Dies gilt auch für Zugriffe auf das ESB-Repository. Der ESB muss so in die Netzarchitektur integriert werden, dass ein Zugriff nur von den Servern der angeschlossenen Anwendungen und Dienste möglich ist und ein Zugriff von außen auf den ESB ausgeschlossen wird. Dazu sollte der ESB ein eigenes logisches Netzsegment erhalten.

Der ESB muss eine eigene Berechtigungsprüfung durchführen, um zu prüfen, ob ein Zugriff auf den angefragten Dienst durch den anfragenden Dienst beziehungsweise die anfragende Anwendung zulässig ist. Dabei muss insbesondere sicher ausgeschlossen werden, dass Anwendungen oder Dienste mit Außenkontakt auf interne Dienste zugreifen, die dafür nicht vorgesehen sind. Solche Anwendungen dürfen auch nicht über das ESB-Repository Kenntnis von internen Diensten und ihren Schnittstellen erlangen.

Sofern die service-orientierte Architektur mehrere Sicherheitsdomänen umspannt, zum Beispiel eine DMZ mit extern aufrufbaren Services und ein internes Netz mit Backend-Systemen, so muss auch der ESB in entsprechende Sicherheitsdomänen mit kontrollierten Übergängen aufgeteilt werden, oder es müssen mehrere ESB für die einzelnen Sicherheitszonen realisiert werden.

Sofern der ESB nicht ausschließlich lokal in einem geschützten RZ-Netz kommuniziert, muss die Kommunikation zwischen ESB und den angeschlossenen Anwendungen geeignet gesichert werden (Authentisierung und Verschlüsselung).

Durch die Bündelung der Kommunikation vieler Anwendungen und Dienste kommt der Verfügbarkeit des ESB eine besondere Bedeutung zu. Dies ist bei

der Realisierung und beim Betrieb des ESB entsprechend durch Redundanzen und eine geeignete Überwachung des Dienstes zu berücksichtigen.

Prüffragen:

- Ist der Zugriff auf Hintergrundsysteme von Webanwendungen oder Web-Services ausschließlich über definierte Schnittstellen und von definierten Systemen aus möglich?
- Wird der Datenverkehr zwischen den Benutzern und der Webanwendung beziehungsweise den Anwendungen, Web-Services und weiteren Diensten sowie den Hintergrundsystemen durch Sicherheitsgateways (Firewalls) reglementiert?
- Werden die Verbindungen zwischen Webanwendungen oder Web-Services und Hintergrundsystemen bei hohem Schutzbedarf durch eine Transportverschlüsselung geschützt?
- Ist sichergestellt, dass Anfragen der Webanwendung oder des Web-Service an Hintergrundsysteme nur mit minimalen Rechten auf diesen ausgeführt werden?
- Ist beim Einsatz eines ESB ein eigenes logisches Netzsegment für den ESB vorgesehen? Ist der Zugriff auf den ESB ausschließlich durch die angeschlossenen Anwendungen und Dienste möglich?
- Ist eine Segmentierung nach Zonen entsprechend den vorhandenen Sicherheitsdomänen im ESB durchgehalten, nötigenfalls bis hin zur Auftrennung in mehrere ESB?
- Werden alle Zugriffe auf den ESB authentisiert und bei der Kommunikation über Standort- und Netzgrenzen hinweg ausreichend gesichert/verschlüsselt?
- Sind bei der Realisierung und beim Betrieb des ESB geeignete Maßnahmen zur Sicherstellung einer angemessenen Verfügbarkeit umgesetzt?

# M 5.169 Systemarchitektur einer Webanwendung

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen
**Verantwortlich für Umsetzung:** Administrator

Webanwendungen verwenden im Allgemeinen mehrere IT-Systemkomponenten wie z. B. Webserver, Web-Applikationsserver und Hintergrundsysteme. Als Grundlage für den sicheren Betrieb einer Webanwendung muss eine geeignete Systemarchitektur gewählt werden.

Beim Entwurf der Systemarchitektur der Webanwendung und der Vernetzung der beteiligten IT-Systeme sollten die folgenden Punkte berücksichtigt werden.

### Trennung nach Server-Rollen

Die Serverdienste der Webanwendung (z. B. Webserver, Applikationsserver, Datenbankserver) sollten jeweils auf separaten IT-Systemen betrieben werden. Kann bei diesem Ansatz eine Schwachstelle im System einer exponierten Komponente (z. B. im Webserver) ausgenutzt werden, so sind die auf anderen Systemkomponenten (z. B. der Datenbank) gespeicherten Daten hiervon nicht direkt betroffen.

Eine Trennung der Server-Rollen kann auch durch eine Servervirtualisierung umgesetzt werden. Wird von der Servervirtualisierung Gebrauch gemacht, so ist bei der Umsetzung der Baustein B 3.304 *Virtualisierung* zu berücksichtigen.

### Eingeschränkte Konten für Serverprozesse der Systemkomponenten

Es sollten jeweils eigene Konten für die unterschiedlichen Serverprozesse der Systemkomponenten verwendet werden (z. B. ein eigener Systembenutzer für den Webserverprozess). Dabei sind die Rechte dieser Dienstekonten auf Betriebssystemebene soweit einzuschränken, dass nur auf die erforderlichen Ressourcen und Dateien des Betriebssystems zugegriffen werden kann. Auf diese Weise verfügt ein Angreifer auch nach einer erfolgreichen Kompromittierung eines Server-Prozesses nur über eingeschränkte Rechte, sodass der Zugriff auf Betriebssystemebene erschwert wird.

### Mehrschichtige Netzwerkarchitektur

Die IT-Systemkomponenten der Webanwendung sollten im Sicherheitsgateway in demilitarisierten Zonen (DMZ) entsprechend des Schutzbedarfs entkoppelt werden (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*).

Die Netzwerkarchitektur sollte einen mehrschichtigen (Multi-Tier) Ansatz verfolgen. Dabei sollten mindestens die folgenden Sicherheitszonen berücksichtigt werden:

- Webschicht
  Diese Schicht grenzt an das nicht vertrauenswürdige Netz (z. B. Internet) und stellt die exponierte Schicht mit direkten Zugriffen durch Benutzer dar. Paketfilter zwischen angrenzenden Netzen (z. B. Anwendungsschicht und Internet) sollten den Datenverkehr filtern, sodass kein direkter Zugriff aus dem nicht vertrauenswürdigen Netz über die Netzgrenzen der Webschicht hinaus möglich ist. In dieser Schicht sollten Systeme wie der Webserver

platziert werden, die eine exponierte Stellung einnehmen und z. B. den direkten Zugriff durch Benutzer erfordern.
- Anwendungsschicht
  Die Anwendungsschicht sollte zum einen an die Webschicht und zum anderen an die Datenschicht angrenzen. Der Netzverkehr zu den angrenzenden Netzen sollte durch Paketfilter gefiltert werden, sodass kein direkter Zugriff zwischen den angrenzenden Netzen möglich ist. In diesem Netzsegment sollten Systeme und Server mit der Anwendungslogik (z. B. der Applikationsserver mit der Webanwendung) platziert sein. Die Systeme greifen auf Daten aus der angrenzenden Datenschicht zu (z. B. Datenbanken), bereiten diese auf und stellen sie Systemen in der Webschicht (z. B. dem Webserver) zur Verfügung.
- Datenschicht
  Die Datenschicht ist die vertrauenswürdigste Zone der mehrschichtigen Architektur. Paketfilter zwischen den angrenzenden Netzen sollten den Datenverkehr reglementieren. In dieser Schicht sollten die Hintergrundsysteme der Webanwendung wie z. B. Datenbanken, Verzeichnisdienst und Legacy-Systeme aufgestellt sein. Der Zugriff auf diese Systeme sollte ausschließlich von angrenzenden Netzen aus möglich sein (z. B. Anwendungsschicht). Die Datenschicht ist als separate Zone umzusetzen und sollte nicht in andere Zonen integriert werden (z. B. Intranet).

Es sollte aus den oben genannten Zonen nicht auf Systeme im Intranet zugegriffen werden können. Falls z. B. für die Authentisierung an der Webanwendung ein Verzeichnisdienst eingesetzt wird, sollte hierfür nach Möglichkeit eine eigene Domäne auf dedizierter Hardware verwendet werden.

Eine Filterung des Datenverkehrs sollte durch getrennte Filterkomponenten erfolgen (z. B. Paketfilter). Bei hohem Schutzbedarf sollten die Filterkomponenten durch Systeme mit Filterfunktionen auf höheren Protokollebenen (z. B. Application Level Gateway) ersetzt oder ergänzt werden. Das Application Level Gateway sollte dabei in einer eigenen Sicherheitszone integriert werden, die noch vor den Systemen der Webschicht die Anfragen der Benutzer entgegennimmt.

**Einsatz von Web Application Firewalls**

Bei der Filterung auf höheren Protokollebenen kann auf den Einsatz von Web Application Firewalls (WAF) zurückgegriffen werden. Da eine WAF das HTTP-Protokoll und die darüber übertragenen Daten analysiert, können Angriffsmuster auf Anwendungsebene bereits an der WAF gefiltert werden. Auf diese Weise werden Angriffsversuche frühzeitig erkannt und nicht mehr an die Webanwendung weitergeleitet.

Die Filterung an der WAF kann üblicherweise auf zwei Arten erfolgen.

- An eine Webanwendung gesendete Daten werden auf bekannte Angriffsmuster untersucht. Die Angriffsmuster werden vom Hersteller der WAF zur Verfügung gestellt und umfassen sowohl typische Zeichenketten, die bei allgemeinen Angriffen gegen Webanwendungen (z. B. SQL-Injection) verwendet werden, als auch spezifische Angriffsmuster, die Standard-Softwareprodukte betreffen. Damit bekannte Angriffe zuverlässig erkannt werden, müssen die Angriffssignaturen ähnlich wie bei einem Virenscanner regelmäßig aktualisiert werden.
- Wird keine Standardsoftware eingesetzt oder soll ein zusätzlicher Schutz erreicht werden, können für WAF üblicherweise auch eigene Filterregeln erstellt werden. Dabei wird beispielsweise definiert, welche Eingabedaten für die Webanwendung zugelassen werden. Diese Methode erfordert

einen hohen Konfigurationsaufwand und eine genaue Kenntnis über die von der Webanwendung verarbeiteten Daten.

Prüffragen:

- Ist eine Trennung der Serverdienste bei Webanwendungen auf jeweils separate IT-Systeme vorgesehen (Trennung nach Server-Rollen)?
- Werden eingeschränkte Konten für Serverprozesse der Systemkomponenten von Webanwendungen verwendet?
- Wird für die Webanwendung ein mehrschichtiger (Multi-Tier) Ansatz bei der Netzwerkarchitektur umgesetzt?
- Bei dem Einsatz von Web Application Firewalls: Ist die Konfiguration der WAF auf die zu schützende Webanwendung angepasst worden?
- Bei dem Einsatz von Web Application Firewalls: Werden die Angriffssignaturen für die WAF regelmäßig aktualisiert?

# M 5.170 Sichere Kommunikationsverbindungen beim Einsatz von OpenLDAP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Kommunikation zwischen einem slapd-Server und seinen Kommunikationspartnern sollte verschlüsselt werden, um die ausgetauschten Informationen vor Kenntnisnahme oder Veränderung durch unberechtigte Personen zu schützen. Hierbei können die Kommunikationspartner Clients und andere Server sein, beispielsweise im Rahmen von Partitionierung und Replikation.

### StartTLS und ldaps://

Um OpenLDAP mittels TLS/SSL abzusichern, sind vorrangig StartTLS und ldaps:// zu verwenden (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*):

- **StartTLS** ist eine in RFC 2830 definierte LDAP "extended operation", die in LDAPv3 als Standardmechanismus verwendet wird, um die Übertragungssicherheit zu gewährleisten. Eine TLS-gesicherte Übertragung wird auf einer bereits bestehenden LDAP-Verbindung aufgebaut, die gesamte Kommunikation läuft über Port 389.
- Bei **ldaps://** hingegen wird bereits der Verbindungsaufbau verschlüsselt vorgenommen. Der slapd-Server muss dafür an einem zusätzlichen Port auf Verbindungen warten, üblicherweise wird der Port 636 verwendet.

Obwohl OpenLDAP beide Verbindungsvarianten unterstützt, wird empfohlen, StartTLS einzusetzen. Vorteile von StartTLS sind die Standard-Konformität und die Vermeidung eines weiteren geöffneten Ports/Dienstes an einer zentralen Netzkomponente. Es ist jedoch möglich, dass ein Kommunikationspartner StartTLS nicht unterstützt. Ferner sind Fälle bekannt, in denen LDAP-Clients vertrauliche Informationen insbesondere zur Authentisierung über eine LDAP-Verbindung ausgetauscht haben, bevor die Verarbeitung von StartTLS abgeschlossen war. Die Übertragung erfolgte zum Teil ungesichert. In diesen Fällen ist es sinnvoll, ldaps:// zu verwenden. SSLv2 sollte weder für StartTLS noch für ldaps:// verwendet werden.

### Konfiguration mit Zertifikaten

Für die verschlüsselte Kommunikation muss ein Server-Zertifikat vorliegen, das als Distinguished Name (DN) des Zertifikats den vollständig angegebenen Rechnernamen des Servers beinhaltet. Soll die Kommunikation auch die zertifikatsbasierte Identitätsfeststellung des Benutzers umfassen, benötigt der Benutzer ebenfalls ein X.509-Zertifikat. Falls die DN-Einträge im Zertifikat eines Benutzers und in seinem Eintrag im Verzeichnis nicht übereinstimmen, ist eine Zuordnung (Mapping) durchzuführen.

Die Konfiguration für verschlüsselte Verbindungen ist sowohl auf dem Server, als auch auf dem Client vorzunehmen. Für den slapd-Server sind die Einstellungen in den globalen Direktiven der Konfigurationsdatei "slapd.conf" vorzunehmen, für die ldap*-Werkzeuge von OpenLDAP in der lokalen ldap.conf. Die Einstellungen der ldap.conf können durch die benutzerspezifische Konfigurationsdatei .ldaprc überschrieben werden, Benutzer-Zertifikate sind dort in jedem Fall einzutragen. Für andere Werkzeuge und Clients ist die jeweilige Dokumentation zu konsultieren.

Es sind unter anderem folgende Parameter zu setzen:

**TLSCACertificateFile (Server) bzw. TLS_CACERT (Client oder Benutzer)**

Der Eintrag verweist auf die Datei, die den öffentlichen Schlüssel beziehungsweise das Wurzelzertifikat einer vertrauenswürdigen Zertifizierungsstelle beinhaltet. Es können mehrere Dateien angegeben werden.

**TLSCACertificatePath (Server) bzw. TLS_CACERTDIR (Client oder Benutzer)**

Statt der Dateien im vorgenannten Parameter können ein oder mehrere Pfade beschrieben werden, in denen die Dateien zu finden sind.

**TLSCertificateFile (Server) bzw. TLS_CERT (Benutzer, nicht Client)**

Der Parameter bezeichnet die Datei, die das eigene Zertifikat beziehungsweise den öffentlichen Schlüssel beinhaltet.

**TLSCertificateKeyFile (Server) bzw. TLS_KEY (Benutzer, nicht Client)**

Dieser Parameter verweist auf den geheimen Schlüssel, der in jedem Fall zu schützen ist. Die Zugriffsrechte für die Datei müssen sorgsam gesetzt werden, damit nur der jeweilige Benutzer (oder der Benutzer, mit dessen Rechten der slapd-Server betrieben wird) auf die Datei zugreifen kann.

**TLSCipherSuite (nur Server)**

Der Eintrag listet die zulässigen Verschlüsselungsverfahren in der bevorzugten Reihenfolge auf und ist abhängig von der verwendeten SSL/TLS Implementierung. Je weniger und je stärkere Verschlüsselungsverfahren angegeben werden, desto besser, so sollte SSLv2 vermieden werden. Keinesfalls darf hier der Eintrag "NULL" (keine Verschlüsselung) stehen.

**TLSRandFile (Server) bzw. TLS_RANDFILE (Client oder Benutzer)**

Die Angabe bezeichnet die Quelle für Zufallswerte. Die Datei liefert den Ausgangswert (Seed), auf dessen Grundlage mit mathematischen Funktionen ausreichend zufällige Zahlenwerte als Sitzungsschlüssel erzeugt werden. Die Angabe wird auf den meisten Linux- und Unix-Systemen nicht benötigt, da /dev/urandom für diesen Zweck verfügbar ist.

**TLSVerifyClient (Server) bzw. TLS_REQCERT (Client oder Benutzer)**

Dieser Parameter bestimmt, inwieweit Zertifikate der jeweiligen Gegenseite geprüft werden. Mögliche Werte sind:

- **never:** Das Zertifikat der Gegenseite wird nie geprüft (Voreinstellung für Server, diese identifizieren keine Clients). Dieser Wert darf nicht gesetzt werden, falls SASL eingesetzt wird und SASL wiederum TLS/SSL zur Authentisierung verwenden soll. Dann muss das Zertifikat des Clients oder Benutzers geprüft werden, da er darüber authentisiert wird.
- **allow**: Ein Zertifikat wird angefragt, aber wenn dieses nicht geliefert wird oder die Überprüfung fehlschlägt, hat dies keine Auswirkungen.
- **try**: Ein Zertifikat wird angefragt. Wird keines geliefert, hat dies keine Auswirkungen. Wird ein Zertifikat geliefert und dessen Überprüfung schlägt fehl, wird die Sitzung abgebrochen.

- **demand**: Ein Zertifikat muss geliefert und erfolgreich geprüft werden, andernfalls wird die Sitzung abgebrochen (Voreinstellung für Clients, diese müssen sich über die Identität des Servers vergewissern)

**Aufbau einer gesicherten Verbindung**

Für StartTLS unterstützen alle ldap*-Werkzeuge von OpenLDAP die Flags "-Z" und "-ZZ". "Z" bedeutet, dass eine verschlüsselte Verbindung versucht und bei Erfolg genutzt werden soll. "ZZ" hingegen bedeutet, dass die Verschlüsselung erfolgreich durchgeführt werden muss, bevor das Kommando ausgeführt werden darf. Für andere Clients, die einen slapd-Server kontaktieren, ist die jeweilige Dokumentation zu beachten.

ldaps:// wird in der Regel durch die entsprechende Zieladresse mit ldaps://... statt ldap://... gestartet, alternativ durch einen generellen Eintrag in der URI Direktive der clientspezifischen Konfigurationsdatei "ldap.conf".

Wenn Overlays verwendet werden, ist zu berücksichtigen, dass diese teilweise eigene Sub-Direktiven für TLS/SSL anbieten, wenn sie zu einem Datenaustausch zwischen Servern führen. Das gilt unter anderem für die Overlays "syncprov" und "chain".

**Einschränkung des Netzverkehrs**

Um die Kommunikation weiter abzusichern, bietet OpenLDAP die Funktion "selective listening" und die Einbindung der Systemapplikation TCP Wrapper an. "Selective listening" beschränkt die Annahme von Operationen auf bestimmte Absender-IP-Adressen. TCP Wrappers stellt eine regelbasierte Überwachung der TCP/IP-Kommunikation bereit. Es wird empfohlen, auf "selective listening" und TCP Wrapper zu verzichten. Vielmehr ist darauf zu achten, dass der Server bereits auf Betriebssystemebene adäquat geschützt ist (siehe M 4.238 *Einsatz eines lokalen Paketfilters*). Eine zusätzliche Überwachung des Netzverkehrs durch OpenLDAP führt zu einem unnötigen Administrationsaufwand und letztlich dazu, dass OpenLDAP eine Funktion übernimmt, für die die Anwendung nicht konzipiert wurde.

**Abweichende Ports**

Gelegentlich wird empfohlen, Verzeichnisdienste so zu konfigurieren, dass diese andere Ports als 389 beziehungsweise 636 verwenden. Dies soll direkte Angriffe auf bekannt gewordene Schwächen einer LDAP-Version erschweren. Von dieser Empfehlung wird abgeraten, da ein minimaler Sicherheitsgewinn mit einem umfangreichen und deshalb fehlerträchtigen Administrationsaufwand erkauft wird. Unter Umständen kommt es auch zu Funktionseinschränkungen bei nicht hinreichend konfigurierbaren Clients.

Prüffragen:

- Wird die Kommunikation zwischen slapd-Server und seinen Kommunikationspartnern verschlüsselt?
- Wird SSLv2 weder für StartTLS noch für ldaps:// verwendet?

# M 5.171 Sichere Kommunikation zu einem zentralen Protokollierungsserver

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der zentralen Protokollierung werden die Informationen der überwachten IT-Systeme und Anwendungen über das Netz zu einem zentralen Protokollierungsserver übertragen, um sie zu sammeln, auszuwerten und zu speichern. Da die Protokolldaten auch personenbezogene Informationen enthalten können, müssen diese vor unberechtigtem Zugriff (einsehen, verändern oder löschen) geschützt werden.

Um zu verhindern, dass die Protokolldaten während der Übertragung auf den zentralen Protokollierungsserver abgehört oder manipuliert werden, lassen sie sich entweder verschlüsselt oder über ein eigenes Administrationsnetz (Out-of-Band) übertragen. Auf diese Weise wird auch die Integrität und Vertraulichkeit der Protokollmeldungen erhöht.

**Vertraulichkeit für sensitive Informationen**

Einige Datenquellen generieren Protokollmeldungen, die eine konkrete Zuordnung zu einer Person ermöglichen. Es ist daher wichtig, die Vertraulichkeit von Protokolldaten auch während der Übertragung sicherstellen zu können, beispielsweise durch Absichern der Verbindung mit Hilfe von SSL (siehe M 5.66 *Clientseitige Verwendung von SSL/TLS*) oder durch Verschlüsseln der Daten. Auch ein eigenes Administrationsnetz (Out-of-Band) kann helfen, die Daten während der Übertragung zu schützen.

**Integrität und Vollständigkeit der Protokolldaten**

Wenn Protokollinformationen im Zusammenhang mit IT-Frühwarnung und im Bereich der Computer-Forensik verwendet werden sollen, ist es wichtig, dass weder Beweise für Sicherheitsvorfälle noch die Beweiskraft der gesammelten Informationen verloren gehen. Des Weiteren sollte eine Authentisierung zwischen dem Protokollierungsserver und dem IT-System stattfinden, das die Protokolldaten liefert. So lassen sich Man-in-the-Middle-Angriffe erschweren und Daten werden nicht versehentlich an nicht-autorisierte Stellen versendet. Daher sind Mechanismen zur Verfügung zu stellen, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen.

Protokolldaten müssen richtig und vollständig sein. Das ist sowohl für die Beweiskraft als auch aus technischer Sicht notwendig.

Da in größeren Informationsverbünden oft viele Protokolldaten anfallen, muss dafür gesorgt werden, dass die Bandbreite ausreicht, um die Protokollinformationen zu übertragen und dass keine Protokollinformationen durch temporäre Bandbreitenengpässe verloren gehen. Ebenso ist sicherzustellen, dass die Übertragung der Protokolldaten nicht die Übertragung der Nutzdaten behindert. Die Protokollmeldungen könnten über ein getrenntes Administrationsnetz (Out-of-Band) statt über das eigentliche Datennetz (In-Band) übertragen werden. In Abhängigkeit des Schutzbedarfs sollte abgewogen werden, ob es sinnvoll und technisch realisierbar ist, eine logische oder eine physikalische Trennung von Protokoll- und Nutzdaten vorzunehmen.

**Beispiele einer sicheren Kommunikation**

Die folgenden Maßnahmen zeigen, wie sich Verfügbarkeit, Integrität und Vertraulichkeit während der Übertragung von Protokolldaten gewährleisten lassen. Die Empfehlungen können sowohl einzeln als auch in Kombination eingesetzt werden.

- Software-Agenten:
  Hierbei wird Software auf dem zu überwachenden System installiert. Die Software überträgt die gesammelten Protokolldaten verschlüsselt zum zentralen Protokollierungsserver. Ein wesentlicher Vorteil ist, dass diese überwachten Systeme alle mit dem gleichen Protokollierungsstandard arbeiten und somit ein Teil der Normalisierung dezentral ausgeführt werden kann. Dies setzt voraus, dass die Agentensoftware auf dem IT-System installiert werden kann, was bei Netzelementen wie Routern oder Sicherheitsgateways oft nicht möglich ist.
- Layer 2-Trennung:
  Beim Einsatz von Switches sollte beachtet werden, dass VLANs (virtuelle lokale Netze) nicht entwickelt wurden, um Sicherheitsanforderungen bei der Trennung von Netzen zu erfüllen. VLANs bieten eine Vielzahl von Angriffspunkten, sodass immer zusätzliche Maßnahmen umzusetzen sind, insbesondere um schutzbedürftige Netze zu trennen. Vertiefende Informationen zu VLANs sind in M 2.277 *Funktionsweise eines Switches* zu finden.
- Layer 3-Trennung:
  Routingfähige Komponenten entscheiden anhand eines Protokolls auf der Ebene 3 des OSI-Schichtenmodells und sind daher ein ideales Kopplungselement. Zusätzlich ist es möglich, mit Routern eine strukturierte IP-Netztrennung durchzuführen. Der Nachteil ist jedoch, dass sich ein Router in der Regel den Speicher für Prozesse, das Schnittstellenmanagement und die Zugangslisten teilt und es deshalb zu Ressourcenengpässen kommen kann. Ein detailliertes Routing, wie Subnetztrennung, autonomes Systemrouting und Ähnliches kann auch in Hinsicht auf die Administration sehr komplex werden.
- VPN-Verbindung:
  Diese Variante bietet sich für Komponenten mit höherem Schutzbedarf in Hinblick auf Vertraulichkeit und Integrität an, die beispielsweise über ein öffentliches Netz angebunden werden. Die IT-Systeme müssen über untereinander kompatible Mechanismen verfügen, um VPNs nutzen zu können. Alternativ lassen sich die IT-Systeme auch an VPN-Appliances anschließen, welche die verschlüsselte Verbindung herstellen.
- Out-of-Band-Management (Administrationsnetz):
  Beim Out-of-Band-Management wird ein separates LAN für die Übertragung der Protokolldaten genutzt. Da dieses LAN ausschließlich für die Protokollierung und eventuell für die Administration zur Verfügung steht, wird bei einer konsequenten Netztrennung der Zugriff für Angreifer erschwert. Out-of-Band-Management ist in der Regel aufwendiger als andere Verfahren, weil am protokollierenden IT-System ein zusätzliches Netzinterface und eine unabhängige Netzinfrastruktur im Informationsverbund benötigt werden. Der Vorteil eines Administrationsnetzes ist, dass Protokolle (insbesondere SNMP Version 1) eingesetzt werden können, die als unsicher bekannt sind, aber mangels verfügbarer Alternativlösungen eingesetzt werden müssen, um den Betrieb, beispielsweise durch IT-Frühwarnungssysteme, zu überwachen.

Prüffragen:

- Werden die Protokolldaten vor unberechtigtem Zugriff geschützt?

- Wird ein gesicherter Übertragungsweg für die Protokollinformationen zur Verfügung gestellt?
- Findet zwischen Protokollierungsserver und IT-System eine Authentisierung statt?
- Werden Mechanismen eingesetzt, die Integrität und Authentizität der Informationen schützen?

# M 5.172 Sichere Zeitsynchronisation bei der zentralen Protokollierung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Protokollierung muss aufgetretenen Ereignissen eine aktuelle Uhrzeit zugeordnet werden, um die Auswertung im Nachhinein zu ermöglichen. Es ist darauf zu achten, dass alle IT-Systeme die gleiche Zeitbasis nutzen. Damit auch in einem großen Informationsverbund alle Systeme zeitsynchron sind, wird in der Regel ein zentraler Network Time Server benutzt. Dieser stellt den zentralen Zeittakt zum Beispiel über das Network Time Protokoll (NTP) zur Verfügung (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*). Alle weiteren Systeme im Informationsverbund synchronisieren sich über diesen externen Zeittakt.

**Störungen der Zeitsynchronisation**

Eine Störung der Zeitsynchronisation kann Probleme bei der zentralen Protokollierung verursachen. Zum Beispiel kann das Auftreten eines Fehler nicht mehr eindeutig dem korrekten Zeitpunkt zugeordnet werden. Möglicherweise verändert sich durch die fehlerhafte Zeitbasis auch die Abfolge von Meldungen, sodass bei der Analyse eine falsche Sequenz der Protokolldaten angezeigt wird.

Ein weiteres Problem ergibt sich, wenn in einem Informationsverbund die Zeit als Grundlage herangezogen wird, um zu überprüfen, ob vertragliche Vereinbarungen bezüglich Service Level Agreements (SLAs) eingehalten wurden. Eine fehlerhafte oder fehlende Zeitsynchronisation der IT-Systeme oder des zentralen Protokollsystems kann dazu führen, dass die Protokollierung nicht zur Beweissicherung herangezogen werden kann. Aus diesem Grund muss sichergestellt sein, dass alle Protokolldateien mit aktuellem Datum und Uhrzeit versehen werden. Hier ist zusätzlich auf eine einheitliche Darstellung der Datums- und Zeiteinstellung in der Protokolldatei zu achten. Werden die Protokolldaten automatisch ausgewertet, sollten alle Protokolldateien ein einheitliches Datums- und Uhrzeitformat enthalten, damit keine Missverständnisse bei der Analyse auftreten.

Um sicherzustellen, dass bei einer zentralen Protokollierung in einem Informationsverbund mit höherem Schutzbedarf alle beteiligten IT-Systeme immer die korrekte Uhrzeit erhalten, kann ein mehrstufiges Zeittakt-Konzept eingesetzt werden. Dabei wird die Systemzeit außer über den NTP-Dienst auch über ein DCF-Funkmodul bereitgestellt.

Prüffragen:

- Wird die Systemzeit aller IT-Systeme im Informationsverbund synchronisiert, um Angriffe auf IT-Systeme und Anwendungen oder deren Fehlfunktionen erkennen zu können?
- Wird darauf geachtet, dass das Datum- und Zeitformat der Protokolldateien einheitlich ist?

# M 5.173 Nutzung von Kurz-URLs und QR-Codes

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, Leiter IT

Webseiten werden üblicherweise über eine URL (Uniform Resource Locator) angesteuert, die daher auch Web-Adresse genannt wird. Die Komplexität vieler Webseiten führt häufig zu relativ langen Web-Adressen, die schwer zu merken sind und vor allem bei mobilen Endgeräten wie Smartphones nicht in einer Zeile dargestellt werden können. Daher haben sich verschiedene Methoden entwickelt, um den Benutzern die Nutzung von Webadressen zu erleichtern. Prominente Vertreter sind Kurz-URLs und QR-Codes.

**Kurz-URLs**

Kurz-URLs bezeichnen einen weitverbreiteten Dienst im Internet, bei dem lange URLs durch kürzere URLs ersetzt werden. Kurz-URLs sind vergleichbar mit einem Link-Text in HTML, der auch beliebig kurz gewählt werden kann. Anders als bei solchen Links auf Internetseiten ist die Zuordnung zwischen kurzer und langer URL dabei in einer Datenbank hinterlegt und daher nicht so leicht erkennbar. Gründe für die weite Verbreitung von Kurz-URLs sind unter anderen:

- Durch Kurz-URLs können Zeilenumbrüche von URLs in E-Mails vermieden werden. Durch einen Zeilenumbruch in einer URL bedeutet es meist mehr Aufwand, den zugeschickten Link zu öffnen. Kurz-URLs sind für gewöhnlich so kurz, dass sie nicht umgebrochen werden müssen.
- Um Links in Mikro-Blog-Einträgen wie etwa Tweets von Twitter einzubetten, können keine langen URLs benutzt werden. Mikro-Blogs besitzen eine starke Zeichenbeschränkung von in der Regel 140 Zeichen pro Eintrag, da Mikro-Blogs von den Nutzern für gewöhnlich am Handy und nicht am PC verfasst werden. Daher haben sich Kurz-URLs als die gängige Form von Links in Mikro-Blog-Einträgen durchgesetzt.
- Kurz-URLs erleichtern es, Referenzen und Verweisen in Zeitschriftenartikeln zu folgen. Viele Artikel in papiergebundenen Zeitschriften verweisen auf Quellen aus dem Internet bzw. enthalten Hinweise zu Internetseiten. Anders als bei Online-Artikeln müssen diese per Hand abgetippt werden. Kurz-URLs verringern den Aufwand dafür erheblich.

Neben all diesen Vorteilen können Kurz-URLs aber auch Gefährdungen mit sich bringen (siehe G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*). Die Mitarbeiter der Institution sollten für diese Probleme sensibilisiert werden. Alle Mitarbeiter sollten wissen, dass Kurz-URLs mit Vorsicht zu genießen sind.

Um nicht auf andere als die gewünschten Webseiten weitergeleitet zu werden, können die Vorschaudienste von Kurz-URL-Anbietern genutzt werden. Dort wird einerseits die dahinter verborgene Adresse angezeigt und andererseits ein Bild der Seite gezeigt. Diese Funktion gibt es auch direkt als Erweiterung für gängige Internetbrowser. Die Vorschaufunktion von Kurz-URLs sollte möglichst immer genutzt werden. Anbieter von Kurz-URLs ohne eine Vorschaufunktion sollten nicht verwendet werden. Allerdings kann die Vorschaufunktion durch iterative Kurz-URLs ausgehebelt werden. Iterativ heißt eine Kurz-URL, wenn sie selbst auf eine andere Kurz-URL (statt auf eine echte Seite) verweist. Es sollten daher möglichst nur Anbieter von Kurz-URLs benutzt werden, welche iterative Kurz-URLs verbieten. Schwerer zu unterbinden sind ite-

rative Kurz-URLs über mehrere Anbieter hinweg. Da iterative Kurz-URLs keinen praktischen Nutzen außer für Angreifer haben, sollten Benutzer iterative Kurz-URLs generell nicht anklicken.

Das Risiko, durch Kurz-URLs auf ungewünschte oder gefährliche Seiten im Internet geleitet zu werden, kann nur verringert, aber nicht ausgeschlossen werden. Damit schädliche Auswirkungen vermieden werden, müssen unbedingt die aktuellen Sicherheitsupdates für Browser und Betriebssystem eingespielt sein sowie ein Virenscanner aktiv sein.

Zusätzlich zu diesen Maßnahmen kann eine Institution entscheiden, dass Kurz-URLs ein zu großes Risiko darstellen und daher nicht verwendet werden dürfen. In diesem Fall kann der Zugang zu Kurz-URL-Dienstanbieter gesperrt werden, z. B. über entsprechende Filterregeln.

**Nutzung von QR-Code**

Um Anwendern das Abtippen von Kurz-URLs, WLAN-Zugangsdaten, Telefonnummern und anderen Informationen abzunehmen, werden vermehrt QR-Codes (Quick Response Codes) verwendet. Hierbei werden Daten in einer Abbildung, einem meist quadratischen Pixelmuster, so kodiert, dass sie zuverlässig von IT-Systeme ausgelesen werden können. Hierfür ist es erforderlich, über Endgeräte wie Smartphones mit entsprechender Ausstattung den QR-Code abzufotografieren oder einzuscannen, um die hierin kodierten Informationen auslesen zu können.

Die Spezifikation von QR-Code ist offen gelegt und QR-Codes können lizenz- und kostenfrei verwendet werden, so dass sie mittlerweile stark verbreitet sind. Klassische QR-Codes können Informationen bis zu 2.953 Byte beinhalten. QR-Codes verfügen über eine hohe Fehlertoleranz, je nach Fehlerkorrektur-Level können zwischen 7% und 30% beschädigter Informationen eines QR-Codes rekonstruiert werden. Neben den verbreiteten QR-Codes gibt es Weiterentwicklungen, in denen Informationen (teilweise) verschlüsselt abgelegt werden, die besonders kleine Abmessungen haben oder in denen Bilder, Texte oder Logos erkennbar sind.

Die in QR-Codes abgelegten Informationen können nicht ohne Weiteres von den Benutzern gelesen werden. Dadurch ergeben sich, ähnlich wie bei Kurz-URLs, einige Gefährdungen (siehe G 5.177 *Missbrauch von Kurz-URLs oder QR-Codes*). Ein Benutzer könnte beispielsweise auf seinem Endgerät einen QR-Code einlesen, der auf über die darin kodierte URL auf eine mit Schadsoftware infizierte Webseite verweist. Daher muss darauf geachtet werden, dass auf dem Endgerät nach dem Einlesen eines QR-Codes keine weiteren Aktionen automatisch ausgeführt werden. Bei einer URL sollte also zuerst die dahinter verborgene Adresse angezeigt werden, bevor die entsprechende Web-Seite geöffnet wird. Generell sollte nach dem Einlesen auch keine Telefonnummer automatisch angerufen oder eine SMS versendet werden, Benutzer sollten ausgehende Anrufe erst bestätigen, bevor gewählt wird.

Das Sicherheitsmanagement sollte deswegen die Mitarbeiter über den Umgang mit QR-Codes aufklären. Außerdem sollten auf den Endgeräten nur QR-Applikationen eingesetzt werden, bei denen nach dem Einlesen von QR-Codes keine Aktionen automatisch ausgeführt werden, sondern diese vorher vom Benutzer bestätigt werden müssen.

Sollen Informationen für einen kleinen Benutzerkreis veröffentlicht werden, kann überlegt werden, die hierin abgelegten Informationen zu verschlüsseln. Beispielsweise können hierfür Secure-QR-Codes (SQRC) verwendet werden.

Dafür müssen die eingesetzten Lesegeräte beziehungsweise IT-Systeme diese natürlich auch dekodieren können.

Prüffragen:

- Sind die Mitarbeiter für die Kurz-URL-Problematik sensibilisiert?
- Werden die Inhalte von Kurz-URLs und QR-Codes vor der Ausführung angezeigt?

# M 5.174 Absicherung der Kommunikation zum Cloud-Zugriff

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Cloud-Diensteanbieter stellen öffentliche Schnittstellen zur Interaktion mit den Cloud-Benutzern bereit. Oft geschieht dies über Webschnittstellen. Über diese Schnittstellen läuft der zentrale Zugriff von Cloud-Benutzern auf die durch den Cloud-Diensteanbieter bereitgestellten Cloud-Dienste. Hierbei müssen sichere Schnittstellen und Protokolle genutzt werden, die eine verschlüsselte Kommunikation zwischen Cloud-Diensteanbieter und Cloud-Benutzer ermöglichen.

### Verschlüsselung und Authentisierung

Zur Absicherung der Kommunikation müssen den anerkannten Regeln der Technik entsprechende sichere Protokolle mit ausreichender Verschlüsselung und Authentisierung eingesetzt werden. Sichere Protokolle können mit Hilfe von Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* ermittelt werden. Sehr hilfreich ist hierbei die Technische Richtlinie TR-02102-2 *Kryptographische Verfahren: Empfehlungen und Schlüssellängen* des BSI.

### Leitbild: HTTPS statt HTTP

Als grundlegendes Beispiel gilt, dass alle webbasierten Cloud-Angebote über HTTPS abgesichert werden müssen. Hierbei ist die Maßnahme M 5.177 *Serverseitige Verwendung von SSL/TLS* des Bausteins B 5.21 *Webanwendungen* umzusetzen.

Für webbasierte Zugriffe wird abgesicherte Kommunikation oft über eine Client-Server-Kommunikation via HTTPS realisiert, bei der der Client das serverseitige Zertifikat prüfen kann. Für Cloud-Dienste mit sicherheitsrelevanten Daten müssen dabei Zertifikate von vertrauenswürdigen Zertifizierungsstellen eingesetzt werden. Bei nicht sicherheitsrelevanten Daten genügen selbst erstellte Zertifikate. Letzteres gilt z. B. für Private-Cloud-Dienste, die in Bezug auf Vertraulichkeit unkritisch sind.

### Dienstspezifische Absicherung oder Absicherung der Netzverbindung

Die Forderung nach abgesicherter Kommunikation gilt neben HTTPS für alle über Cloud Computing bereitgestellten Cloud-Dienste.

Denkbar wäre zum Beispiel eine Nutzung eines Verzeichnisdienstes über Cloud-Dienste, wobei dienstspezifische Protokolle eingesetzt werden (hier z. B. LDAP). Bei der Verwendung von LDAP muss ebenfalls durchgängig die verschlüsselte Variante LDAP eingesetzt werden, bei der die Absicherung der unterliegenden Netzverbindung mit *Transport Layer Security* (TLS, häufig noch unter dem älteren Namen SSL angesprochen) erfolgt.

### Sichere Behandlung der Passwörter

Bei der Verwendung von Passwörtern sind einige grundlegende Sicherheitsmaßnahmen zu berücksichtigen. Eine ausreichende Passwort-Policy muss

umgesetzt sein. Näheres dazu ist der Maßnahme M 2.11 *Regelung des Passwortgebrauchs* zu entnehmen.

Die Passwörter für Webanwendungen sollten mit sogenannten Passwort-Salts versehen werden, die als zufälliges Prefix mit den Passwörten zusammen verschlüsselt werden. Diese Funktion verhindert, dass die Passwörter auf einfache Art vorberechnet werden können.

Passwörter dürfen nicht im Cache des Clients vorgehalten werden, dieses ist server- bzw. anwendungsseitig zu verhindern. Die Autocomplete-Funktion muss für Passwörter ebenfalls deaktiviert sein.

**Session Management**

Zur Absicherung von Session-IDs in der Webanwendung sind die Inhalte der Maßnahme M 4.361 *Sichere Konfiguration von Webanwendungen* zu berücksichtigen. Weitere Anforderungen sind der Maßnahme M 4.394 *Session-Management bei Webanwendungen und Web-Services* zu entnehmen.

Prüffragen:

- Nutzt die Kommunikation zum Cloud-Zugriff HTTPS (statt HTTP) oder ist sie anderweitig durch TLS / SSL abgesichert?
- Wo kein HTTP zum Einsatz kommt: Besteht eine andere angemessene Absicherung durch dienstspezifische Protokolle?
- Bei Kommunikation über öffentliche Netze: Werden Zertifikate für HTTPS (oder andere Verschlüsselungsverfahren) von einer offiziellen Zertifizierungsstelle (Certification Authority, CA) bezogen?

# M 5.175 Einsatz eines XML-Gateways

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Durch eine klassische Firewall kann sichergestellt werden, dass in geschlossenen Umgebungen nur Endgeräte mit berechtigten IP-Adressen auf einen Web-Service zugreifen können (*Whitelisting*) oder dass bei im Internet verfügbaren Web-Services IP-Adressen, von denen Angriffe, etwa durch Botnetze, ausgehen, gesperrt werden können (*Blacklisting*). Zu Details siehe M 4.454 *Schutz vor unerlaubter Nutzung von Web-Services*. Derartige Firewalls sind jedoch typischerweise nicht in der Lage, SOAP-Nachrichten zu analysieren und Angriffe auf der Anwendungsschicht (SOAP/HTTP) zu erkennen. Daher sollte, insbesondere bei erhöhtem Schutzbedarf, zum Schutz von Web-Services der Einsatz eines sogenannten XML-Gateways in Erwägung gezogen werden, das diese Filterung auf XML-Ebene leistet.

Ein XML-Gateway ist eine Infrastrukturkomponente, die zwischen Web-Service und Consumer geschaltet wird und dabei als eine Firewall für Nachrichten in einer Web-Service-Infrastruktur agiert. Sie leistet damit für Web-Services das, was eine Web Application Firewall (WAF) für Webanwendungen ausführt. Beide stellen Ausprägungen sogenannter Application Level Gateways (ALG) für unterschiedliche Anwendungsprotokolle dar. Das XML-Gateway fängt XML-Nachrichten ab, um sie nach definierten Vorgaben zu analysieren, bevor sie an den Web-Service weitergeleitet werden. Dafür kommt üblicherweise ein leistungsstarker, gehärteter Parser zum Einsatz, der eine definierte Sicherheitsrichtlinie anwendet und teilweise auch über Heuristiken verfügt, die das Erlernen typischer Kommunikationen erlaubt. So können etwa plötzlich sprunghaft anwachsende Nachrichtengrößen erkannt werden und definierte Aktionen und Alarme auslösen.

Ein XML-Gateway (auch als *XML-Firewall*, *Web-Service-Firewall*, *Web-Service-Security-Gateway* oder *XML-SOAP-Proxy* bezeichnet) ist eine Komponente, die dem Schutz von Diensten vor Angriffen über XML-basierte Schnittstellen dient, indem es XML-Daten prüft, die die Institution erreichen oder verlassen. XML-Gateways können als eigenständige Systeme oder auch als Komponente eines Enterprise Service Bus (ESB) realisiert werden.

Folgende Funktionen werden typischerweise bereitgestellt:

- Auslagerung von Authentisierung und Autorisierung an das Gateway
- Zugriffskontrolle durch Zertifikate, SAML, LDAP, RADIUS und ähnliche Methoden
- Begrenzung von Datenraten als Maßnahme gegen Denial-of-Service-Angriffe
- Ver- und Entschlüsselung auf Transport- oder Nachrichtenebene
- Anbringung und Prüfung von XML-Signaturen
- Kontrolle von Datenflüssen
- Validierung von XML-Nachrichten anhand von Schemata und Policys
- Schutz vor in XML eingebetteten Angriffen wie Cross-Site Scripting, SQL-Injection oder Command-Injection
- Schutz vor bestimmten SOAP-/XML-spezifischen Angriffen wie zu großen Nachrichten, zu stark verschlüsselten Elementen, rekursivem Parsen, bösartig manipulierten Schemata oder WSDL-Dateien sowie Angriffen auf das Routing
- Scannen von SOAP-Body sowie SOAP-Attachments auf Schadsoftware

- Unterstützung verschiedener Web-Service-Sicherheitsstandards wie WS-Security, WS-SecureConversation, WS-Trust oder WS-Federation
- Auslösen von Alarmen, teilweise durch Anomalie-Erkennung in der Kommunikation
- Teilweise auch Dienstvirtualisierung durch URL-Rewriting, XSL-Transformationen und SOAP-basiertes Routing

Modelle verschiedener Hersteller unterscheiden sich vor allem im Daten-Durchsatz und der Latenz der Verbindung, in Funktionen zur Sicherstellung der Verfügbarkeit durch redundante Systeme, den vorhandenen Zertifizierungen (etwa nach Common Criteria), Unterstützung für Identitäts- und Zugriffsmanagement (etwa durch SAML, OAuth oder für SSO-Lösungen), Konfigurationsmöglichkeiten und Erweiterbarkeit.

Für den Einsatz eines XML-Gateways sollte daher im ersten Schritt eine Anforderungsanalyse erfolgen, in der die erforderlichen und wünschenswerten Funktionen ermittelt werden. Werden XML-Gateways bei höherem Schutzbedarf eingesetzt, sollten zudem die zu erreichenden Sicherheitsziele definiert werden.

XML-Gateways sind in der Lage, den eingehenden Datenverkehr auf bösartige Inhalte zu untersuchen und diese herauszufiltern, damit eine Verarbeitung auf dem Endsystem gar nicht erst erfolgen kann. So können zum Beispiel vom Angreifer konstruierte fehlerhafte XML-Nachrichten bereits am Gateway herausgefiltert werden (siehe G 5.183 *Angriffe auf XML*). Die Gateways bieten oft auch eine ausgehende Datenflusskontrolle an, die zu verhindern versucht, dass sensible Inhalte aus dem internen Netz exfiltriert werden.

Damit kann ein XML-Gateway die meisten Aufgaben übernehmen, die in den Maßnahmen M 4.454 *Schutz vor unerlaubter Nutzung von Web-Services* und M 4.393 *Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services* gefordert werden. Die Validierung eines Schemas etwa (siehe M 4.454 *Schutz vor unerlaubter Nutzung von Web-Services*) kann entweder bereits am XML-Gateway oder direkt auf dem System erfolgen, welches den Web-Service bereitstellt. Die Entscheidung, an welcher Stelle die Validierung erfolgen soll, ist bereits in der Planung zu dokumentieren, da dies auch Auswirkungen auf die Gesamtarchitektur haben kann.

Folgende Vorteile ergeben sich beim Einsatz eines XML-Gateways:

- XML-Gateways sind für ihren Einsatzzweck optimiert. Das bedeutet in der Regel, dass sie speziell gehärtet und dadurch robust sind.
- Da in die Entwicklung viel Wissen über XML-basierte Angriffe und entsprechende Sicherheitsmaßnahmen geflossen ist, erlauben XML-Gateways die sichere Nutzung von Web-Services, wenn sie richtig konfiguriert werden.
- Einer der größten Vorteile eines XML-Gateways ist die Verwaltung der verschiedenen Aspekte einer Web-Service-Sicherheitsrichtlinie an einer zentralen Stelle (häufig in einem Web-Interface), anstatt für jeden Dienst einzeln. Dies kann helfen, Konzeptions- und Konfigurationsfehler zu vermeiden. Das Managementinterface ist geeignet abzusichern.

Nachteile, die aus dem Einsatz eines XML-Gateways erwachsen können, sind die folgenden:

- Wie bei anderen ALGs auch ist die Konfiguration eines XML-Gateways nicht trivial, sondern erfordert sorgfältige Planung und gründliches Testen. Dies gilt nicht nur für die Inbetriebnahme, sondern auch für alle Änderungen am Kommunikationsverhalten der betroffenen Web-Services.

- Ein XML-Gateway ist zwar wartungsarm, aber nicht wartungsfrei. Auch hier sollten regelmäßig Software- und Signaturupdates eingespielt werden, falls der Hersteller solche anbietet. Auch auf das Bekanntwerden von Schwachstellen für das Gateway sollte geachtet und reagiert werden.
- Durch den Einbau eines weiteren Systems in die Verarbeitungskette steigt das Risiko eines Verlusts der Verfügbarkeit durch Konfigurations-, Software- oder Hardwarefehler. Bei hohem Verfügbarkeitsbedarf sollte eine redundante Auslegung erfolgen.
- Insbesondere wenn das Gateway auch die Prüfung auf Schadsoftware übernimmt, können Fehlalarme zu Beeinträchtigungen der Funktionalität und Verfügbarkeit führen. Daher ist neben ausführlichem Testen auch eine Abwägung der Risiken gegeneinander durchzuführen sowie gegebenenfalls ein Notfallkonzept zu erstellen.
- Bestimmte Angriffstypen sind komplex und entwickeln sich laufend weiter, sodass nicht davon ausgegangen werden darf, dass das XML-Gateway jede Variante des Angriffs erkennen kann. Beispiele sind XML Signature Wrapping-Angriffe (XSW) oder neuere Angriffe auf TLS/SSL wie etwa CRIME.
- Gerade bei ressourcenkritischen Services mit vielen kryptographischen Operationen kann der Einsatz eines Gateways notwendig sein, um die Rechenlast bewältigen zu können. Gleichzeitig kann das Gateway dadurch einen Flaschenhals darstellen, auf dessen innere Funktion und Leistung der Betreiber weniger Einfluss hat als auf den Web-Service selbst. Dies macht umsichtige Planung und Tests notwendig.

Ähnlich einer Web-Application Firewall (WAF) kann der Einsatz einer XML-Firewall ein falsches Gefühl von Sicherheit erzeugen und dazu führen, dass Sicherheitsmaßnahmen in der Softwareentwicklung und im Betrieb von Web-Services vernachlässigt werden. Dies ist häufig fatal, da für die meisten Gateways im Lauf der Zeit Methoden bekannt werden, wie deren Filterfunktionen umgangen werden können. Die Notwendigkeit von robustem Code und Sicherheitschecks im Dienst selbst wird dadurch also nicht obsolet.

Typischerweise wird ein XML-Gateway wie andere ALGs auch in einem neutralen Grenznetz (DMZ) positioniert. Zu empfehlen ist auch hier der P-A-P-Aufbau mit vor- und nachgeschaltetem Paketfilter und dem XML-Gateway in der Mitte, was erheblich bessere Kontroll- und Protokollierungsmöglichkeiten bietet (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*). Zudem können die beiden Paketfilter das XML-Gateway selbst vor einfachen Attacken schützen und komplexitätsbedingte Fehlkonfigurationen dort teilweise kompensieren. Darüber hinaus können sie das Gateway bei der Filterung von unerwünschtem Datenverkehr (zum Beispiel durch Internet-Würmer) unterstützen und eine Überlastung zumindest hinauszögern.

Da ein XML-Gateway ein komplexes System darstellt, sind in allen Phasen des Lebenszyklus von Konzeption bis Notfallvorsorge detaillierte Anforderungen zu stellen. Daher ist das XML-Gateway selbst im Sicherheitskonzept anhand des Bausteins B 3.301 *Sicherheitsgateway (Firewall)* zu behandeln.

Prüffragen:

- Wurde in einer Anforderungsanalyse bestimmt, welche Funktionen eines XML-Gateways benötigt werden?
- Wurde die Entscheidung getroffen und dokumentiert, an welcher Stelle die Validierung von Nachrichten durchgeführt werden soll?
- Ist sichergestellt, dass in der Anwendungsentwicklung weiter die Forderungen nach robustem Code und Überprüfung der Eingangsdaten berücksichtigt werden?

- Ist die Platzierung des XML-Gateways geplant und begründet, etwa in der DMZ und zwischen zwei Paketfiltern (P-A-P)?
- Wurde das XML-Gateway selbst im Sicherheitskonzept erfasst und mit dem Baustein B 3.301 *Sicherheitsgateway (Firewall)* abgebildet?

# M 5.176 Sichere Anbindung von Smartphones, Tablets und PDAs an das Netz der Institution

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter IT

Smartphones, Tablets und PDAs werden in der Regel kabellos mit dem Netz der Institution verbunden, z. B. über WLAN oder das mobile Telekommunikationsnetz. Grundsätzlich sollte die Verbindung zwischen Endgerät und dem Netz der Institution durchgehend verschlüsselt sein. Das lässt sich mit einem verschlüsselten VPN-Tunnel realisieren (siehe Baustein B 4.4 *VPN*), der zwischen dem Endgerät und einem VPN-Server der Institution aufgebaut wird. So wird vermieden, dass Schwächen der mobilen Telekommunikationsnetze oder einer unverschlüsselten WLAN-Verbindung die Vertraulichkeit gefährden. Greift das Endgerät über das verschlüsselte WLAN der Institution auf das Netz der Institution zu, so kann überlegt werden, ob der VPN-Tunnel entbehrlich ist.

Smartphones, Tablets und PDAs sollten innerhalb der Institution in einem eigenen Netzsegment untergebracht sein (siehe Maßnahme M 5.7 *Netzverwaltung*). Werden diese oder vergleichbare Endgeräte in einem Informationsverbund eingesetzt, sollte die Segmentierung durch eine Netzzugangskontrolle ergänzt werden. Sie sollte zusätzlich überprüfen, ob:

- auf den mobilen Endgeräten alle aktuellen Systempatches vorhanden sind,
- alle Anwendungen die neuesten Updates besitzen,
- die Virensignatur-Datenbank aktuell ist und
- alle weiteren Einstellungen am Endgerät, z. B. Passwortgestaltung und Zeitdauer bis zum automatischen Sperren, den Vorgaben entsprechen.

Sollte die Netzzugangskontrolle feststellen, dass ein Smartphone, Tablet oder PDA in einem dieser Punkte abweicht, so ist es in ein Quarantäne-Netzsegment zu verschieben. Dort kann der Agent der Netzzugangskontrolle das Gerät entsprechend den Sicherheitsvorgaben aktualisieren beziehungsweise den Benutzer anleiten, geänderte Einstellungen am Endgerät wieder rückgängig zu machen. Im Anschluss kann das Endgerät wieder aus dem Quarantäne-Bereich entfernt werden.

Sollte ein Smartphone, Tablet oder PDA gestohlen oder verloren gegangen sein und eine Meldung hierüber vorliegen, so ist der Zugang dieses Endgerätes zum Netz der Institution zu sperren (siehe Maßnahme M 6.159 *Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs*). Bei höherem Schutzbedarf muss zudem geprüft werden, ob mit dem Endgerät in der Zwischenzeit bereits unbefugt auf Informationen der Institution zugegriffen wurde und ob entsprechend den Richtlinien zur Behandlung von Sicherheitsvorfällen weitere Maßnahmen zu ergreifen sind (siehe Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*). Dafür sind im Vorfeld entsprechende Protokollfunktionen der Netzzugangskontrolle zu nutzen.

Prüffragen:

- Werden Smartphones, Tablets und PDAs innerhalb der Institution in einem eigenen Netzsegment untergebracht?
- Werden auffällige Smartphones, Tablets oder PDAs in ein Quarantäne-Netzsegment verschoben?

# M 5.177 Serverseitige Verwendung von SSL/TLS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Transport Layer Security (TLS) ist eine Weiterentwicklung von Secure Sockets Layer (SSL) und wird dazu verwendet, Informationen während der Übertragung in Netzen, in der Regel zwischen Serverdiensten und Clients oder zwischen Serverdiensten untereinander kryptographisch abzusichern. Konfigurationshinweise, wie SSL/TLS auf Clients verwendet werden sollte, und allgemeine Informationen zur Funktionsweise von SSL/TLS sind in M 5.66 *Clientseitige Verwendung von SSL/TLS* zu finden. Clients können die Verschlüsselung über SSL/TLS nur dann nutzen, wenn diese von den Serverdiensten unterstützt wird. SSL/TLS kann dazu eingesetzt werden, Informationen aus der Anwendungsschicht (z. B. HTTP, LDAP, POP3, IMAP und SMTP) verschlüsselt über TCP/IP zu übertragen. Überdies können mittels SSL/TLS auch sichere VPNs (Virtuelle Private Netze) aufgebaut werden. Mit OpenVPN, einer unter der GNU GPL (General Public License) frei verfügbaren Software, können VPNs mittels SSL/TLS verschlüsselte Verbindungen realisiert werden. Vertiefende Informationen zu VPNs sind in B 4.4 *VPN* zu finden.

In der Regel ist es bei vielen Serverdiensten nur ein geringer Mehraufwand, diese so zu konfigurieren, dass eine SSL/TLS-Verschlüsselung unterstützt wird, oder so, dass diese für einen Informationsaustausch ausschließlich genutzt wird. Daher ist für alle Serverdienste zu prüfen, ob mit vertretbarem Aufwand eine Verschlüsselung über SSL/TLS möglich und praktikabel ist. Ist dies mit vertretbarem Aufwand möglich, sollte die SSL/TLS-Verschlüsselung aktiviert werden. Generell sollte der interne und externe Nachrichtenstrom von und zu LDAP-, E-Mail- und Webservern mit SSL/TLS verschlüsselt werden.

**Auswahl einer vertrauenswürdigen Zertifizierungsstelle**

Zu Beginn eines neuen mit SSL/TLS abgesicherten Kommunikationsaufbaus findet ein sogenannter Handshake zwischen Client und Server statt. Hierbei verständigen sich Client und Server über die kryptographischen Algorithmen, die für Schlüsselaustausch, Verschlüsselung und Integritätssicherung eingesetzt werden. Außerdem einigen sich Client und Server über die SSL-Version, die verwendet wird. Zusätzlich dazu sendet der Server sein X.509-Zertifikat an den Client. Optional kann der Server auch so konfiguriert werden, dass auch der Client aufgefordert wird, dem Server sein X.509-Zertifikat zu übermitteln.

Die Identität der Kommunikationspartner wird hierbei über diese Zertifikate geprüft. X.509-Zertifikate enthalten die öffentlichen Schlüssel sowie eine Bestätigung einer weiteren Instanz, der Zertifizierungsstelle oder auch Trustcenter oder Certificate Authority (CA) genannt, über die korrekte Zuordnung des öffentlichen Schlüssels zu dessen "Besitzer". Der Wert eines Zertifikates hängt davon ab, welche Felder des X.509-Zertifikats von der Zertifizierungsstelle geprüft werden, bevor das Zertifikat ausgestellt wird, und wie vertrauenswürdig die Zertifizierungsstelle selbst ist. Daher spielt die Auswahl einer vertrauenswürdigen Zertifizierungsstelle eine wichtige Rolle.

Aufgrund der Vielzahl von Zertifizierungsstellen auf dem Markt sollte eine Institution die Zertifizierungsstelle sorgfältig auswählen. Es ist ratsam, die für

den späteren Betrieb wesentlichen Auswahlkriterien im Vorfeld festzulegen. Zu diesen können beispielsweise gehören:

- ob das Root-Zertifikat schon in CA-Listen der Clients, wie dem Browser, enthalten ist,
- wo sich Sitz und Rechtsstand der Zertifizierungsstelle befinden, und auch wo der Sitz des technischen Betriebs sich befindet,
- was die geschäftliche Ausrichtung der Zertifizierungsstelle ist (Ist CA-Betrieb ein zentrales Geschäftsfeld?), was die angebotenen CA-Dienste umfassen (z. B. OSCP, CRL),
- welches Sicherheitsniveau die Zertifizierungsstelle nachweisen kann,
- wie gut Umfang und Qualität des technischen Supports sind,
- wie hoch die Zertifikatskosten sind.

Grundsätzlich sollten die Kosten eines Zertifikats jedoch keinesfalls das allein ausschlaggebende Kriterium darstellen. Wird der angebotene Serverdienst von einem beschränkten Benutzerkreis verwendet, z. B. nur innerhalb eines LANs, kann ein Zertifikat auch ohne die Beteiligung einer Zertifizierungsstelle selbst erstellt und signiert und auf alle Clients eingespielt werden, auf denen der Serverdienst genutzt werden soll,

**Extended Validation Zertifikate**

Um Angriffe mit gefälschten Webseiten zu erschweren und der Problematik entgegen zu wirken, dass diverse Zertifizierungsstellen SSL/TLS-Anträge nicht immer zuverlässig prüfen, wurden Extended Validation Zertifikate zum Umgang mit Zertifikaten mit höheren Sicherheitsanforderungen eingeführt. Diese sollen verhindern, dass, wenn ein Zertifikat ausgestellt wird, eine CA nur den Domainnamen prüft. Darüber hinaus soll die CA außerdem noch eindeutig nachvollziehen, von wem die betreffende Domain registriert wurde. Im Unterschied zu den normalen X.509 SSL/TLS-Zertifikaten wird bei diesen erweiterten Zertifikaten (Extended Validation SSL-Zertifikate, EV-SSL) die Identität des Antragstellers ausführlicher überprüft. Hierbei verpflichten sich die beteiligten Zertifizierungsstellen und Browser-Hersteller, die "Guidelines for the Issuance and Management of Extended Validation Certificates" des CA/Browser Forums einzuhalten. Danach sind unter anderem folgende Kriterien vom Antragsteller zu erfüllen:

- Identitätsnachweis und Adresse des Antragstellers,
- Nachweis, dass der Antragsteller alleiniger Eigentümer der Domain ist,
- Bestätigung, dass antragstellende Person überhaupt berechtigt ist, den Antrag zu stellen und
- Hauptkontaktperson.

Zusätzlich darf der Antragsteller oder die antragstellende Person auf keiner Liste mit verbotenen Organisationen oder Personen stehen. Außerdem darf das Land, in dem sich der Sitz oder der Rechtsstand des Antragstellers befindet, weder Handelsembargos oder irgendwelchen anderen Sanktionen ausgesetzt sein, die durch dasjenige Land verhängt wurden, dessen Gesetzgebung die Zertifizierungsstelle unterliegt.

Für die Anwender sind EV-SSL-Zertifikate daran zu erkennen, dass in den unterstützten Browsern bestimmte Bereiche, wie die URL im Adressfeld oder das von vielen Browsern verwendete Vorhängeschlosssymbol, das eine verschlüsselte Seite kennzeichnet, grün hinterlegt ist. Je nach Konfiguration des Sicherheitsgateways (Firewall), hinter dem die Benutzer auf Webseiten mit EV-SSL-Zertifikaten zugreifen, kann es aber vorkommen, dass diese Markierungen in den Browsern der Clients nicht angezeigt werden. Wird beispielsweise der Nachrichtenfluss zwischen Client und Webserver von einem Proxy

ent- und wieder neu verschlüsselt, wird im Browser lediglich das SSL/TLS-Zertifikat des Sicherheitsgateways angezeigt.

Neben den höheren finanziellen Kosten, die für die Ausstellung eines EV-SSL-Zertifikats entstehen können, dauert die Antragstellung in der Regel auch länger, da zusätzliche Informationen von der Zertifizierungsstelle überprüft werden. Wenn es möglich ist, wird empfohlen, diesen zusätzlichen Aufwand in Kauf zu nehmen. Insbesondere in Bereichen, in denen Informationen mit höherem Schutzbedarf bezüglich Vertraulichkeit und Integrität übertragen werden, sollten EV-SSL-Zertifikate bevorzugt eingesetzt werden.

**Common Name Eintrag**

Browser zeigen immer eine Sicherheitswarnung an, wenn der im Zertifikat einer Webseite eingetragene Common Name (Allgemeiner Name) nicht mit dem vollständigen DNS-Name (Fully Qualified Domain Name) übereinstimmt, über den der Server im Web erreichbar ist. Daher sollte sichergestellt sein, dass der Common Name zu der URL passt, die tatsächlich verwendet wird, um mit dem Server zu kommunizieren. Wenn es möglich ist, sollten Wildcard-Zertifikate (z. B. *.example.de) vermieden werden. Diese werden häufig eingesetzt, um mit einem einzelnen Zertifikat mehrere Subdomains abzusichern.

**Vollständige Zertifikatskette**

Da für die Prüfung der hierarchischen Zertifikatskette durch den Browser auch alle Zwischen-Zertifikate benötigt werden, reicht das SSL-Zertifikat des Servers alleine nicht aus. Deshalb sollte der Server so konfiguriert werden, dass beim Verbindungsaufbau alle erforderlichen Zertifikate an den Client gesendet werden. Dazu sollte die Zertifikatskette im Webserver entsprechend hinterlegt werden.

Zu beachten ist außerdem, dass neben Zertifikate, die fehlen, auch abgelaufene oder gesperrte Zertifikate die Prüfung der Zertifikatskette fehlschlagen lassen. Nur wenn alle Zertifikate gültig sind und beim Verbindungsaufbau übertragen wurden, kann die Zertifikatskette erfolgreich geprüft werden.

**Auswahl einer SSL/TLS Protokollversion**

Derzeit existieren fünf SSL/TLS-Protokollversionen: SSL v2, SSL v3, TLS v1.0, TLS v1.1 und TLS v1.2. SSL v1 wurde nicht veröffentlicht. Um eine sichere Verbindung zwischen Client und Server zu gewährleisten, sollte TLS 1.2 verwendet werden. TLS 1.1 bietet ausreichende Sicherheit, aber im Vergleich zu TLS 1.2 weist es jedoch einige Schwächen auf, z. B. sind in TLS 1.1 noch Cipher-Suites vorhanden, die auf IDEA und DES basieren, in TLS 1.2 nicht mehr. TLS 1.0 kann in bestehenden Anwendungen übergangsweise weiter eingesetzt werden, falls eine sofortige Migration zu TLS 1.1 oder vorzugsweise TLS 1.2 nicht möglich ist und geeignete Maßnahmen gegen Chosen-Plaintext-Angriffe (z. B. BEAST) auf die CBC-Implementierung getroffen werden. Generell sollte jedoch eine Migration zu TLS 1.2 schnellstmöglich erfolgen.SSL v2 und SSL v3 dürfen nicht mehr eingesetzt werden.

**Sichere Cipher-Suites**

SSL/TLS nutzt Cipher-Suites, die bestimmen, wie sicher eine HTTPS-Verbindung ist. Jede Suite besteht aus spezifischen Modulen. Wenn ein bestimmtes Modul als unsicher oder schwach eingestuft wird, kann durch die Veränderung der Cipher Suite zu einem sichereren Modul gewechselt werden.

Da die Verwendung schwacher Cipher Suites clientseitig erzwungen werden kann, ist es erforderlich, serverseitig nur solche anzubieten, die Authentisierung und Verschlüsselung mit einer ausreichenden Stärke einsetzen. Darüber hinaus sollten die verwendeten Cipher-Suites Perfect Forward Secrecy (PFS) unterstützen (siehe TR-02102-2).

Weitere Hinweise zu kryptografischen Algorithmen und Schlüssellängen sind in der Technischen Richtlinie des BSI Kryptographische Verfahren: Empfehlungen und Schlüssellängen - Teil 2 Verwendung von TLS (TR-02102-2) und M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* enthalten.

**Session Renegotiation/TLS-Kompression**

Mittels der sogenannten Session Renegotiation (Session-Neuverhandlung) können sowohl Client als auch Server die Parameter einer bestehenden HTTPS-Sitzung neu aushandeln. Aufgrund eines Fehlers in der Spezifikation des TLS-Protokolls (RFC 5246) ist es einem Man-in-the-Middle-Angreifer möglich, die Session Renegotiation zu missbrauchen, um beliebige Inhalte in eine existierende HTTPS-Sitzung einzufügen. Mittlerweile wurde das TLS-Protokoll erweitert (RFC 5746) und dieser Designfehler behoben. Generell sollte überlegt werden, ob serverseitig die Session Renegotiation erforderlich ist. Ist dies der Fall, dann sollte diese sicher konfiguriert werden, also auf Basis des RFC 5746. Eine Renegotiation, die durch den Client initiiert wird, sollte vom Server abgelehnt werden.

Darüber hinaus sollte die TLS-Kompression deaktiviert werden.

**Webserverspezifische Aspekte**

Generell wird empfohlen, die auf Webservern zur Verfügung gestellten Inhalte bei der Übertragung vom Server zum Client und umgekehrt mittels SSL/TLS zu schützen.

Wenn möglich, sollte darauf verzichtet werden, Webseiten mit gemischten Inhalten anzubieten. Als Webseite mit gemischtem Inhalt wird eine Seite bezeichnet, die zwar Verschlüsselung nutzt, dabei aber auch unverschlüsselte Inhalte (z. B. JavaScript-, CSS-Dateien oder Bilder) einbindet. Ein Man-in-the-Middle-Angreifer kann die Übertragung einer einzelnen unverschlüsselten Datei ausnutzen, um eine HTTPS-Session zu übernehmen. Da Webseiten mit gemischten Inhalten zudem üblicherweise Browser-Warnungen erzeugen, wird dadurch die Benutzerfreundlichkeit verschlechtert.

HTTP Strict Transport Security (HSTS) ist eine weitere Methode, die gegen bekannte Schwächen von SSL schützt. Damit wird erschwert, dass ein Besucher durch einen Angriff oder serverseitige Konfigurationsprobleme von einer gesicherten auf eine ungesicherte Seite umgeleitet wird. Befindet sich ein Angreifer beispielsweise in demselben WLAN wie das Opfer, könnte er so die Session Cookies mitlesen und die HTTPS-Session übernehmen. Um HSTS zu aktivieren, muss der HSTS-Header auf dem Server konfiguriert werden.

**Schutz des privaten Serverschlüssels**

Ein besonders wichtiger Sicherheitsaspekt beim Einsatz von SSL/TLS ist der Schutz des privaten Serverschlüssels. Daher ist es ratsam, den Server so zu konfigurieren, dass der private Serverschlüssel beim Start des Servers durch Passworteingabe freigegeben werden muss. Besteht der Verdacht, dass der private Schlüssel kompromittiert wurde, so muss das zugrunde liegende Zerti-

fikat widerrufen werden. Weitere Hinweise zum Umgang mit kryptografischen Schlüsseln sind in M 2.46 *Geeignetes Schlüsselmanagement* zu finden.

**Validierung**

Die Auswirkungen von Konfigurationsänderungen auf dem Server lassen sich nicht immer mit Bestimmtheit vorhersagen. Auch Software Updates können mitunter zu überraschenden Änderungen führen. Es wird daher empfohlen, die SSL/TLS Konfiguration vor der Freigabe zur Nutzung auf Fehler zu prüfen und den Status in periodischen Abständen (regelmäßig) zu validieren.

Prüffragen:

- Bieten alle Serverdienste, bei denen es sinnvoll und möglich ist, die Informationen verschlüsselt über SSL/TLS an?
- Wurde sorgfältig eine Zertifizierungsstelle ausgewählt?
- Wurde der Common Name sorgfältig ausgewählt?
- Wurde die vollständige Zertifikatskette im Webserver hinterlegt?
- Unterstützen die eingesetzten Server-Produkte eine sichere Version von SSL/TLS?
- Ist sichergestellt, dass die eingesetzten Server kryptographische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen?
- Wurde die Session Renegotiation deaktiviert oder erfolgt diese auf Basis des RFC 5746? Wurde die clientseitige Renegotiation deaktiviert?
- Wird bei Webseiten auf gemischten Inhalten verzichtet?
- Wurde die TLS-Kompression deaktiviert?
- Wird der private Serverschlüssel durch ein Passwort geschützt?
- Wurde die SSL/TLS Konfiguration vor der Freigabe zur Nutzung auf Fehler geprüft und wird der Status in periodischen Abständen validiert?

# M 6 Maßnahmenkatalog Notfallvorsorge

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

M 6.2 Notfall-Definition, Notfall-Verantwortlicher **- entfallen**

M 6.3 Erstellung eines Notfall-Handbuches **- entfallen**

M 6.4 Dokumentation der Kapazitätsanforderungen der IT-Anwendungen **- entfallen**

M 6.5 Definition des eingeschränkten IT-Betriebs **- entfallen**

M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten **- entfallen**

M 6.7 Regelung der Verantwortung im Notfall **- entfallen**

M 6.8 Alarmierungsplan **- entfallen**

M 6.9 Notfall-Pläne für ausgewählte Schadensereignisse **- entfallen**

M 6.10 Notfall-Plan für DFÜ-Ausfall **- entfallen**

M 6.11 Erstellung eines Wiederanlaufplans **- entfallen**

M 6.12 Durchführung von Notfallübungen **- entfallen**

M 6.13 Erstellung eines Datensicherungsplans **- entfallen**

M 6.14 Ersatzbeschaffungsplan **- entfallen**

M 6.15 Lieferantenvereinbarungen **- entfallen**

M 6.16 Abschließen von Versicherungen

M 6.17 Alarmierungsplan und Brandschutzübungen

M 6.18 Redundante Leitungsführung

M 6.19 Datensicherung am PC **- entfallen**

M 6.20 Geeignete Aufbewahrung der Backup-Datenträger

M 6.21 Sicherungskopie der eingesetzten Software

M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen

M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen

M 6.24 Erstellen eines Notfall-Bootmediums

M 6.25 Regelmäßige Datensicherung der Server-Festplatte **- entfallen**

M 6.26 Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten

M 6.27 Sicheres Update des BIOS

M 6.28 Vereinbarung über Lieferzeiten lebensnotwendiger TK-Baugruppen **- entfallen**

M 6.29 TK-Basisanschluss für Notrufe

M 6.30 Katastrophenschaltung **- entfallen**

M 6.31 Verhaltensregeln nach Verlust der Systemintegrität

M 6.32 Regelmäßige Datensicherung

M 6.33 Entwicklung eines Datensicherungskonzepts

M 6.34 Erhebung der Einflussfaktoren der Datensicherung

M 6.35 Festlegung der Verfahrensweise für die Datensicherung

M 6.36 Festlegung des Minimaldatensicherungskonzeptes

M 6.37 Dokumentation der Datensicherung

M 6.38 Sicherungskopie der übermittelten Daten

M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung

M 6.40 Regelmäßige Batterieprüfung/-wechsel **- entfallen**

M 6.41 Übungen zur Datenrekonstruktion

M 6.42 Erstellung von Rettungsdisketten für Windows NT **- entfallen**

M 6.43 Einsatz redundanter Windows-Server

M 6.44 Datensicherung unter Windows NT **- entfallen**

M 6.45 Datensicherung unter Windows 95 **- entfallen**

M 6.46 Erstellung von Rettungsdisketten für Windows 95 **- entfallen**

M 6.47 Datensicherung bei der Telearbeit

M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität

M 6.49 Datensicherung einer Datenbank

M 6.50 Archivierung von Datenbeständen

M 6.51 Wiederherstellung einer Datenbank

M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten

M 6.53 Redundante Auslegung der Netzkomponenten

M 6.54 Verhaltensregeln nach Verlust der Netzintegrität

M 6.55 Reduzierung der Wiederanlaufzeit für Novell Netware Server **- entfallen**

M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren

M 6.57 Erstellen eines Notfallplans für den Ausfall des Managementsystems

M 6.58 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen

M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle

M 6.61 Eskalationsstrategie für Sicherheitsvorfälle

M 6.62 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen

M 6.63 Untersuchung und Bewertung eines Sicherheitsvorfalls **- entfallen**

M 6.64 Behebung von Sicherheitsvorfällen

M 6.65 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen

M 6.66 Nachbereitung von Sicherheitsvorfällen

M 6.67 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

M 6.68 Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen

M 6.69 Notfallvorsorge und Ausfallsicherheit bei Faxservern

M 6.70 Erstellen eines Notfallplans für den Ausfall des RAS-Systems **- entfallen**

M 6.71 Datensicherung bei mobiler Nutzung des IT-Systems

M 6.72 Ausfallvorsorge bei Mobiltelefonen

M 6.73 Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung

M 6.74 Notfallarchiv

M 6.75 Redundante Kommunikationsverbindungen

M 6.76 Erstellen eines Notfallplans für den Ausfall von Windows-Systemen

M 6.77 Erstellung von Rettungsdisketten für Windows 2000 **- entfallen**

M 6.78 Datensicherung unter Windows Clients

M 6.79 Datensicherung beim Einsatz von Internet-PCs

M 6.80 Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes **- entfallen**

M 6.81 Erstellen von Datensicherungen für Novell eDirectory

M 6.82 Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen **- entfallen**

M 6.83 Notfallvorsorge beim Outsourcing

M 6.84 Regelmäßige Datensicherung der System- und Archivdaten

M 6.85 Erstellung eines Notfallplans für den Ausfall des IIS **- entfallen**

M 6.86 Schutz vor schädlichem Code auf dem IIS **- entfallen**

M 6.87 Datensicherung auf dem IIS **- entfallen**

M 6.88 Erstellen eines Notfallplans für den Webserver

M 6.89 Notfallvorsorge für einen Apache-Webserver **- entfallen**

M 6.90 Datensicherung und Archivierung bei Groupware und E-Mail

M 6.91 Datensicherung und Recovery bei Routern und Switches

M 6.92 Notfallvorsorge bei Routern und Switches

M 6.93 Notfallvorsorge für z/OS-Systeme

M 6.94 Notfallvorsorge bei Sicherheitsgateways

M 6.95 Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs

M 6.96 Notfallvorsorge für einen Server

M 6.97 Notfallvorsorge für SAP Systeme

M 6.98 Notfallvorsorge und Notfallreaktion für Speicherlösungen

M 6.99 Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server

M 6.100 Erstellung eines Notfallplans für den Ausfall von VoIP

M 6.101 Datensicherung bei VoIP

M 6.102 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

M 6.103 Redundanzen für die Primärverkabelung

M 6.104 Redundanzen für die Gebäudeverkabelung

M 6.105 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten

M 6.106 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes

M 6.107 Erstellung von Datensicherungen für Verzeichnisdienste

M 6.108 Datensicherung für Domänen-Controller

M 6.109 Notfallplan für den Ausfall eines VPNs

M 6.110 Festlegung des Geltungsbereichs und der Notfallmanagementstrategie

| | |
|---|---|
| M 6.111 | Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene |
| M 6.112 | Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement |
| M 6.113 | Bereitstellung angemessener Ressourcen für das Notfallmanagement |
| M 6.114 | Erstellung eines Notfallkonzepts |
| M 6.115 | Integration der Mitarbeiter in den Notfallmanagement-Prozess |
| M 6.116 | Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse |
| M 6.117 | Tests und Notfallübungen |
| M 6.118 | Überprüfung und Aufrechterhaltung der Notfallmaßnahmen |
| M 6.119 | Dokumentation im Notfallmanagement-Prozess |
| M 6.120 | Überprüfung und Steuerung des Notfallmanagement-Systems |
| M 6.121 | Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen |
| M 6.122 | Definition eines Sicherheitsvorfalls |
| M 6.123 | Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen |
| M 6.124 | Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung |
| M 6.125 | Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen |
| M 6.126 | Einführung in die Computer-Forensik |
| M 6.127 | Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen |
| M 6.128 | Schulung an Beweismittelsicherungswerkzeugen |
| M 6.129 | Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen |
| M 6.130 | Erkennen und Erfassen von Sicherheitsvorfällen |
| M 6.131 | Qualifizieren und Bewerten von Sicherheitsvorfällen |
| M 6.132 | Eindämmen der Auswirkung von Sicherheitsvorfällen |
| M 6.133 | Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen |

# M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Verantwortliche der einzelnen Anwendungen

Für die in einem IT-System betriebenen IT-Anwendungen und deren Daten sind die Verfügbarkeitsanforderungen festzustellen. Da eine IT-Anwendung nicht zwingend jeden Bestandteil des IT-Systems benötigt, sind die Verfügbarkeitsanforderungen der IT-Anwendungen auf die wesentlichen Komponenten des IT-Systems abzubilden. Das Ergebnis dieser Arbeit kann in Form einer Übersicht mit folgenden Inhalten dargestellt werden:

| IT-System | IT-Komponente | IT-Anwendung | tolerierbare Ausfallzeit |
|---|---|---|---|
| Zentralsystem | Host | Reisekosten | 5 Arbeitstage |
| | | Buchhaltung | **3 Stunden** |
| | DFÜ | E-Mail | 3 Arbeitstage |
| | | Buchhaltung | **1 Arbeitstag** |
| | Drucker | Reisekosten | 10 Arbeitstage |
| | | Buchhaltung | 2 Arbeitstage |
| | | Einsatzplanung | **1 Arbeitstag** |
| LAN | Server | Datenerfassung | 1 Arbeitstag |
| | | Leitstelle | **4 Stunden** |
| | PC | Datenerfassung | 10 Arbeitstage |
| | PC | Leitstelle | **4 Stunden** |

(Lesart: Die IT-Komponente Host im IT-System "Zentralsystem" hat aufgrund der IT-Anwendung Buchhaltung eine maximal tolerierbare Ausfallzeit von 3 Stunden.)

Eine praktikable Vorgehensweise ist es, zu den einzelnen IT-Anwendungen den Verfahrensverantwortlichen nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen, um danach die Ergebnisse nach IT-System und Komponenten geordnet in der Tabelle aufzuführen.

Die Übersicht erleichtert es, die besonders zeitkritischen Komponenten des IT-Systems zu extrahieren, für die die Notfallvorsorge unumgänglich ist. Bei Ausfall einer Komponente gibt diese Übersicht darüber hinaus Auskunft über die betroffenen IT-Anwendungen und deren Verfügbarkeitsanforderungen.

Die Anforderungen an die Verfügbarkeit sind von den Anwendern bzw. Fachabteilungen zu begründen, sofern dies nicht schon an anderer Stelle geschehen ist. Die Verfügbarkeitsanforderungen sind von der Behörden- bzw. Unternehmensleitung zu bestätigen.

Bei Ausfall einer Komponente des IT-Systems ermöglicht diese Übersicht eine schnelle Aussage, ab wann ein Notfall vorliegt. Dass ein Notfall auch bei Ausfall einer besonders zeitkritischen Komponente nicht zwingend eintreten muss, lässt sich anhand eines Ersatzbeschaffungsplans und einer Untersuchung über interne und externe Ausweichmöglichkeiten ermitteln.

Prüffragen:

- Sind für die in den ITSystemen betriebenen Anwendungen und deren Daten die Verfügbarkeitsanforderungen definiert?
- Existiert eine Dokumentation über die tolerierbaren Ausfallzeiten?

# M 6.2 Notfall-Definition, Notfall-Verantwortlicher

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.3 Erstellung eines Notfall-Handbuches

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.4 Dokumentation der Kapazitätsanforderungen der IT-Anwendungen

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.5 Definition des eingeschränkten IT-Betriebs

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.7 Regelung der Verantwortung im Notfall

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.8 Alarmierungsplan

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.9 Notfall-Pläne für ausgewählte Schadensereignisse

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.10 Notfall-Plan für DFÜ-Ausfall

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.11 Erstellung eines Wiederanlaufplans

Die Ma¿nahme ist 2009 mit der 11. Erg¿nzungslieferung entfallen und ist inhaltlich in anderen Ma¿nahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.12 Durchführung von Notfallübungen

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.13 Erstellung eines Datensicherungsplans

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.14 Ersatzbeschaffungsplan

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.15 Lieferantenvereinbarungen

Die Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen und ist inhaltlich in anderen Maßnahmen des Bausteins B 1.3 *Notfallmanagement* aufgegangen.

# M 6.16 Abschließen von Versicherungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung

Jede Institution muss entscheiden, wie mit den Restrisiken umgegangen wird, die auch nach Umsetzung von Sicherheitsmaßnahmen verbleiben. Durch das Abschließen einer Versicherung kann der finanzielle Schaden gesenkt werden. Auch Folgeschäden, die durch den Ausfall der betroffenen Geschäftsprozesse entstehen, können durch entsprechende Versicherungen (z. B. Versicherung gegen Betriebsunterbrechungen durch Feuer) teilweise versichert werden. Zu beachten ist aber, dass es auch nicht versicherbare Restrisiken geben kann. Dies betrifft beispielsweise Imageschäden. Bei Abschluss einer Versicherung sollten daher die besonderen Rahmenbedingungen und etwaige Ausschlussklauseln berücksichtigt werden. Zu beachten ist auch, dass eventuell eine längere Zeitspanne finanziell überbrückt werden muss, bis die Versicherung den Schaden ersetzt.

Für deutsche Behörden ist der Abschluss von Versicherungen unüblich.

Die Versicherungsarten lassen sich gliedern in:

- Drittschaden (Haftpflichtversicherung)
  - Personen-, Sachschäden inklusive Umweltschäden sowie Vermögensschäden
- Eigenschaden (Sachversicherung, inklusive Softwareschäden)
  - Gebäudeversicherung
  - Sachinhaltsversicherung
  - Ertragsausfallversicherung (Versicherung gegen Betriebsunterbrechungen)
  - Elektronikversicherung
  - Vertrauensschadenversicherung (z. B. Versicherung gegen Computer-Missbrauch)
- Rechtsschutzversicherung

Unter den Hilfsmittel zum IT-Grundschutz findet sich eine Tabelle, die einen kurzen Überblick gibt, welche Versicherungen in welchen Bereichen helfen können, die finanziellen Auswirkungen von potenziellen Schäden zu reduzieren.

Prüffragen:

- Ist geprüft worden, ob für Restrisiken Versicherungen abgeschlossen werden sollen, um eventuelle Schäden abzudecken?
- Wurde der notwendige Versicherungsschutz auch in der Höhe ermittelt?
- Wird regelmäßig überprüft, dass die bestehenden Versicherungen der aktuellen Lage entsprechen?

# M 6.17 Alarmierungsplan und Brandschutzübungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Brandschutzbeauftragter
**Verantwortlich für Umsetzung:** Brandschutzbeauftragter

Es ist erforderlich, Pläne für die im Brandfall zu ergreifenden Maßnahmen zu erstellen. In einem solchen Plan ist z. B. niederzulegen,

- welche Maßnahmen bei welchen Ereignissen zu treffen sind,
- ob und wie Gebäudeteile evtl. zu räumen sind (Personen und Geräte),
- wer zu informieren ist und
- welche hilfeleistenden Kräfte zu informieren sind.

Ergänzt werden kann der Alarmierungsplan um Verhaltensregeln für den Brandfall, die allen Mitarbeitern bekannt zu geben sind. Dazu siehe auch Baustein B 1.3 *Notfallmanagement*.

Der beste Alarmierungsplan nützt allerdings wenig, wenn nicht sichergestellt ist, dass die darin aufgelisteten Maßnahmen richtig und praktikabel sind. Es ist also erforderlich, den Alarmplan regelmäßig zu prüfen und zu aktualisieren. Eine dieser Prüfungsmaßnahmen ist die Durchführung von Brandschutzübungen.

**Beispiel:**

- Eine im Herbst 2012in einem 21-geschossigen Bonner Bürogebäude durchgeführte Brandschutzübung hat gezeigt, dass viele Mitarbeiter nicht wussten, wo ein Feuerlöscher oder wo das nächste Treppenhaus ist. Im Ernstfall kann diese Unkenntnis zu einer Katastrophe führen. Teilweise wurde die Übung ignoriert, man verließ aus Bequemlichkeit den Raum nicht.

Gerade in Brandschutzübungen soll das richtige Verhalten im Brandfall geschult und geübt werden, um Menschenleben zu schützen und Schäden u. a. für die IT zu vermeiden. Die Durchführung solcher Übungen ist vorher mit der Behörden- bzw. Unternehmensleitung abzustimmen.

Prüffragen:

- Gibt es einen schriftlich dokumentierten Alarmierungsplan?
- Wurden Brandschutzübungen durchgeführt?

# M 6.18 Redundante Leitungsführung

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Haustechnik

Bei der redundanten Leitungsführung werden zwischen geeigneten Punkten im Netz neben den im normalen Betrieb genutzten Leitungen zusätzliche Verbindungen eingerichtet. Diese sollten über eine andere Trasse geführt werden. Dadurch besteht die Möglichkeit, bei Störungen auf die redundante Verbindung umzuschalten. Diese Umschaltung kann automatisch oder von Hand erfolgen. Die automatische Umschaltung ist an einer Stelle anzuzeigen, die die Störungsbeseitigung auf der normalen Leitung veranlasst.

Die Funktionsfähigkeit von redundanten Leitungen ist in sinnvollen Zeitabständen durch tatsächliche Nutzung auf ihre Funktionsfähigkeit hin zu überprüfen. Die Dimensionierung, die Prüfintervalle und die grundsätzliche Notwendigkeit von redundanten Leitungen ist direkt von der Verfügbarkeitsanforderung an das Netz abhängig. Ebenso muss man das Verhältnis der Bereitstellungszeit der redundanten Leitung zur Wiederherstellungszeit der normalen Leitung berücksichtigen. Es ist allerdings von entscheidender Bedeutung, ob es sich um Leitungen im öffentlichen Bereich (z. B. Telekom) oder im privaten Bereich handelt.

- Bei Leitungen im öffentlichen Bereich hat der Benutzer keinen Einfluss auf deren Schutz. Das öffentliche Netz stellt grundsätzlich eine ausreichende Zahl von redundanten Leitungen zur Verfügung. Meistens reicht es aus, bei Ausfall einer Verbindung (gleichgültig ob Festverbindung oder Wählleitung) durch Aufbau einer Wählleitung die Verbindung wiederherzustellen. Die Schaltung von redundanten Festverbindungen ist in der Regel zu teuer und meistens verzichtbar.
- In einem privaten Netz kann der Betreiber die Sicherheit von Leitungen wesentlich beeinflussen. Kostenüberlegungen führen meist dazu, dass es keine redundanten Leitungen gibt. In privaten Netzen verursachen redundante Leitungen jedoch außer den Herstellungskosten keine laufenden Ausgaben.

Prüffragen:

- Sind redundante Leitungen über eine andere Trasse geführt?
- Wird die Funktionstüchtigkeit von redundanten Leitungen regelmäßig überprüft?

# M 6.19 Datensicherung am PC

Diese Maßnahme ist mit Version 2005 entfallen.

# M 6.20 Geeignete Aufbewahrung der Backup-Datenträger

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Administrator

Backup-Datenträger unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.
- Ein ausreichend schneller Zugriff muss im Bedarfsfall gewährleistet sein.
- Der Aufbewahrungsort muss auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern gewährleisten.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

Zu beachten sind auch die Anforderungen aus M 2.3 *Datenträgerverwaltung*.

Prüffragen:

- Sind Backup-Datenträger vor unbefugtem Zugriff geschützt?
- Werden die Backup-Datenträger räumlich getrennt von den Herkunftssystemen aufbewahrt?
- Erfüllt der Aufbewahrungsort von Backup-Datenträgern neben den geforderten Zugriffsmöglichkeiten auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern?

# M 6.21 Sicherungskopie der eingesetzten Software

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Bei Problemen mit IT-Systemen ist es oft nötig, die eingesetzten Betriebssysteme und Anwendungen zeitnah neu installieren zu können. Hierfür müssen alle Dateien, die zur Installation benötigt werden, vorliegen. Daher ist es erforderlich, Kopien anzufertigen und an geeigneter Stelle zu archivieren.

Wird die Software auf Datenträgern (z. B. DVDs, CDs oder USB-Sticks) ausgeliefert, sollte von den Originaldatenträgern erworbener Software bzw. von der Originalsoftware bei Eigenentwicklungen eine Sicherungskopie erstellt werden, von der bei Bedarf die Software wieder eingespielt werden kann. Die Originaldatenträger und die Sicherungskopien sind getrennt voneinander aufzubewahren.

Insbesondere Anwendungen werden oft nicht auf Datenträgern ausgeliefert, sondern nur als separate Installationsdateien, als Bestandteil einer Paket- oder Softwareverwaltung oder als Quelltextpakete. Auch diese Installationsquellen sollten an einem geeigneten Ort hinterlegt werden.

Um kostenpflichtige Betriebssysteme oder Anwendungen zu installieren, müssen oft Lizenznummern während der Installation eingegeben werden. Aus diesem Grund ist es nötig, dass neben den Installationsquellen auch diese Lizenznummern geeignet hinterlegt werden. Ein unerlaubter Zugriff auf die Installationsmedien und die Lizenznummern, z. B. zur Erstellung einer Raubkopie, muss ausgeschlossen sein.

Wurde die Software aus Quelltexten übersetzt, so sollte die Dokumentation sämtliche beim Übersetzen verwendeten Optionen (insbesondere die Optionen, mit denen ein etwaiges Skript "configure" aufgerufen wurde) enthalten. Wurde die Software aus einem Binärpaket installiert, so sollten alle Schritte dokumentiert werden, mit denen die Installation später nachvollzogen werden kann.

Jede Änderung an einer Konfigurationsdatei sollte dokumentiert werden. Es empfiehlt sich, eine Versionsverwaltung einzusetzen. Zusätzlich müssen alle Konfigurationsdateien regelmäßig gesichert werden.

Prüffragen:

- Sind die notwendigen Pakete und Informationen vorhanden, um die Software im Notfall schnell neu installieren zu können?
- Sind Sicherungskopien der eingesetzten Software angefertigt worden?
- Werden die Installationsquellen und eventuelle Lizenznummern an einen geeigneten Ort aufbewahrt?
- Werden die verwendeten Optionen beim Übersetzen aus Quelltexten und Änderungen an der Konfiguration dokumentiert?

# M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Für die Rekonstruktion eines Datenbestandes muss geprüft werden, ob mit den vorhandenen Sicherungskopien der Daten ein solches Vorhaben durchgeführt werden kann. Durch technische Defekte, falsche Parametrisierung, einer schlichten Überalterung der Medien, einer unzureichenden Datenträgerverwaltung oder der Nichteinhaltung von Regeln, die in einem Datensicherungskonzept gefordert werden, ist es möglich, dass eine Rekonstruktion eines Datenbestandes nicht möglich ist. Daher ist es notwendig, dass sporadisch überprüft wird, ob die erzeugten Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können.

Prüffragen:

- Wird sporadisch überprüft, ob die gesicherten Daten wieder eingespielt werden können?

# M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

**Verhaltensregeln für den Benutzer**

Ist ein IT-System mit Schadprogrammen infiziert oder besteht der Verdacht, dass es infiziert ist, gilt vor allem: Ruhe bewahren. Panik oder vorschnelles Handeln führen oft erst zu einem Schaden, bzw. vergrößern diesen noch. Von oberster Priorität ist, die weitere Ausbreitung der Schadprogramme zu verhindern.

Neben der Entdeckung und Meldung von Schadprogrammen durch das Viren-Schutzprogramm können folgende Anzeichen auf eine Infektion mit Schadprogrammen hinweisen:

- Häufige Abstürze von Programmen
- Unerklärliches Systemverhalten
- Unerklärliche Fehlermeldungen
- Nutzung unbekannter Dienste
- Unerwartete Netz-Zugriffe
- Unerklärliche Veränderungen von Datei-Inhalten
- Ständige Verringerung des freien Speicherplatzes, ohne dass etwas gespeichert wurde
- Versand von E-Mails ohne Aktion des Benutzers
- Nicht auffindbare Dateien
- Kein Zugriff auf einzelne Laufwerke oder Datenträger
- Probleme beim Starten des PCs
- Unerklärliche Veränderungen von Icons
- Probleme beim Verändern oder Abspeichern von Dateien

Dabei sollte berücksichtigt werden, dass diese Anzeichen nicht zwingend auf einen Befall durch Schadprogramme zurückzuführen sind. Die oben genannten Effekte können auch Anzeichen für einen Hard- bzw. Softwarefehler sein und bedürfen aus diesem Grund einer genauen Untersuchung.

Ein entdecktes Schadprogramm (bzw. der Verdacht) ist unverzüglich zu melden. Dabei sollte dem Benutzer eine einheitliche Meldestelle zur Verfügung stehen (z. B. ein User Help Desk, Support oder ähnliches). Weitere Hinweise hierzu finden sich in M 2.158 *Meldung von Schadprogramm-Infektionen*.

Bei einer Schadprogramm-Infektion oder einem entsprechenden Verdacht darf der Benutzer nicht weiter mit dem IT-System arbeiten. Stattdessen wartet er auf weitere Anweisungen von den zentralen Ansprechpartnern.

**Verhaltensregeln für den verantwortlichen Ansprechpartner**

Alle nachfolgend beschriebenen weiteren Aktionen werden durch den verantwortlichen Ansprechpartner durchgeführt bzw. eingeleitet.

Bis zur Klärung des Sachverhalts sollte das betroffene IT-System als erstes von allen Datennetzen getrennt werden. Falls das betroffene System drahtlos kommunizieren kann, muss es sofort ausgeschaltet werden, da anders keine schnelle und wirksame Trennung vom Datennetz erreicht werden kann.

Unkoordiniertes Handeln führt im Schadenfall häufig zu noch größeren Schäden. Aus diesem Grund sollte der Verantwortliche gut geschult sein, wenn er versucht, das befallene System von Schadprogrammen zu befreien. Im Zweifelsfall ist es besser, eine weitere fachkundige Person hinzuzuziehen. Trotz möglicherweise hoher Honorarkosten kann dies günstiger sein, als das spätere Beheben der Folgen einer Fehlreaktion.

Oberstes Ziel sollte sein, eine weitere Ausbreitung des Schadprogramms zu verhindern. Folgende Maßnahmen sind dafür erforderlich:

- Information von Mitarbeitern
- Gegebenenfalls Information von Externen/Geschäftspartnern
- Gegebenenfalls Deaktivierung von IT-Systemen oder bestimmten Diensten
- Beweissicherung
- Beseitigung des Schadprogramms
- Feststellen der Quelle

Viren-Schutzprogramme können erkannte Infektionen unter Umständen automatisch entfernen. Dabei werden infizierte Dateien bereinigt, das heißt, der originale Dateizustand wird wieder hergestellt. Ob dies möglich ist, hängt jedoch unter anderem von der Art des jeweiligen Schadprogramms ab, da einige Schadprogramme auch Daten- oder Code-Bereiche überschreiben. Eigenständige Schadprogramme können vom Viren-Schutzprogramm in der Regel ebenfalls gelöscht werden. Alternativ werden infizierte Dateien in einen Quarantäne-Bereich gestellt und können gegebenenfalls zu einem späteren Zeitpunkt näher ausgewertet werden.

**Vorgehen bei einer erkannten Infektion**

Ein möglicherweise infiziertes IT-System darf nicht mehr produktiv genutzt werden, bis feststeht, dass alle Schadprogramme erfolgreich entfernt wurden.

Wenn eine Infektion erkannt wurde, sollte das IT-System von einem Schadprogramm-freien System- bzw. Boot-Datenträger gestartet (gebootet) werden. Entsprechende CD-ROMs können mit verschiedenen Viren-Schutzprogrammen hergestellt werden. Es gibt auch Boot-CD-ROMs mit vorinstalliertem Unix-/Linux-Betriebssystem und bereits vollständig implementierten Viren-Schutzprogrammen für solche Notfälle. Alternativ kann auch ein entsprechend vorbereiteter USB-Stick verwendet werden.

Weiterhin muss das IT-System mit zumindest einem aktualisierten Viren-Schutzprogramm (aktueller Programmcode und aktuelle Schadprogramm-Signaturen) überprüft werden, um festzustellen, ob tatsächlich ein Schadprogramm vorhanden ist und um welches Schadprogramm es sich handelt. Durch die Suche mit mehreren unterschiedlichen Viren-Schutzprogrammen kann die Sicherheit erhöht werden. Über die Suche und deren Ergebnisse sollte ein Protokoll erstellt werden.

Danach kann das Schadprogramm abhängig vom jeweiligen Schadprogramm-Typ entfernt werden. In der Regel können hierfür entsprechende Funktionen des Viren-Schutzprogramms eingesetzt werden.

Ist die automatische Entfernung nicht möglich, muss beim Hersteller der Viren-Schutzprogramme recherchiert werden, ob das Schadprogramm tatsächlich rückstandsfrei entfernt werden kann. In den meisten Fällen helfen die Informationen des Herstellers des Viren-Schutzprogramms weiter. Darin sind

die Funktionsweise des entdeckten Schadprogramms und die Beseitigung zumeist detailliert beschrieben.

Kann das Schadprogramm nicht vollständig entfernt werden, ist eine Wiederherstellung des Systems aus einer Datensicherung (siehe M 6.32 *Regelmäßige Datensicherung*) oder eine Neuinstallation erforderlich.

Die Festplatte(n) und alle anderen möglicherweise betroffenen Datenträger müssen nach Entfernung des Schadprogramms noch einmal überprüft werden, um sicherstellen, dass das Schadprogramm auch wirklich komplett entfernt wurde. Im Anschluss daran muss die Boot-Reihenfolge des Rechners wieder so eingestellt werden, dass nur von der Festplatte gebootet wird.

Sollte das Schadprogramm Daten gelöscht oder verändert haben, die weiter benötigt werden, muss versucht werden, die Daten aus Datensicherungen (siehe M 6.32 *Regelmäßige Datensicherung*), Kopien oder anderen zuverlässigen Quellen zu rekonstruieren. Für die Wiederherstellung der Programme können beispielsweise Sicherungskopien (siehe M 6.21 *Sicherungskopie der eingesetzten Software*), Original-Datenträger oder vertrauenswürdige Web-Seiten des Herstellers herangezogen werden.

Alle von den infizierten Rechnern aus genutzten Zugangskennungen und Passwörter müssen zeitnah geändert werden, um Missbrauch vorzubeugen.

**Ursachenforschung und Schadensanalyse**

Abschließend sollte versucht werden, die Ursache der Infektion festzustellen. Ist die Quelle auf Original-Datenträger zurückzuführen, sollte der Hersteller und das BSI informiert werden. War die Ursache eine Datei oder E-Mail, dann muss der Ersteller und/oder Absender der Datei benachrichtigt werden. Wenn Daten von einem infizierten Rechner verschickt wurden, sollten die Empfänger dieser Daten benachrichtigt werden (siehe M 2.158 *Meldung von Schadprogramm-Infektionen*).

Wichtig ist, dass der Befall durch Schadprogramme nicht nur analysiert, sondern auch dokumentiert wird. Diese Dokumentation und die Analyse des Vorfalls bilden die Grundlage für die Aktualisierung des Sicherheitskonzepts gegen Schadprogramme.

Das Ziel ist, wirksame Gegenmaßnahmen zu ergreifen, damit sich ein solcher oder ähnlicher Vorfall möglichst nicht wiederholt.

Prüffragen:

- Werden IT-Systeme, die mit Schadprogrammen infiziert sind oder bei denen der Verdacht besteht, dass sie mit Schadprogrammen infiziert sind, unverzüglich von allen Datennetzen getrennt?
- Wird ein möglicherweise infiziertes IT-System erst dann wieder produktiv genutzt, wenn feststeht, dass alle Schadprogramme erfolgreich entfernt wurden?
- Werden alle von infizierten Rechnern aus genutzten Zugangskennungen und Passwörter zeitnah geändert?
- Gibt es jeweils geeignete Verhaltensregeln für Benutzer und Fachkräfte, wie beim Auftreten von Schadprogrammen zu verfahren ist?
- Wurden die Verhaltensregeln beim Auftreten von Schadprogrammen dem jeweiligen Zielpublikum in geeigneter Form bekannt gegeben?
- Sind die verantwortlichen Ansprechpartner hinsichtlich des Auftretens von Schadprogrammen geschult?

- Fließen die Erkenntnisse aus der Analyse von Schadprogramm-Vorfällen in die Aktualisierung des Sicherheitskonzepts gegen Schadprogramme mit ein?

# M 6.24 Erstellen eines Notfall-Bootmediums

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Einrichtung eines Rechners sollte ein Bootmedium erstellt werden, das bei Ausfall einer Festplatte zum Starten des Systems oder bei Auftreten eines Schadprogramms zum Erzeugen eines kontrollierten Systemzustands genutzt werden kann. Solche Medien können beispielsweise CDs sein, deren Erstellung das jeweilige Betriebssystem eventuell anbietet, es können aber auch eigens eingerichtete CDs oder portable Laufwerke (beispielsweise USB-Sticks oder externe Festplatten mit USB- oder Firewire-Schnittstelle) erstellt werden. Art und Umfang des Notfall-Bootmediums richten sich nach dem Einsatzzweck des Rechners und den vorhandenen Schnittstellen.

Das Notfall-Bootmedium kann unter anderem bei folgenden Problemen zum Einsatz kommen:

- Datenverlust durch Fehlbedienung,
- Bedienungs- und Administrationsfehler, die die Benutzung und einen Neustart verhindern,
- Infektion des Systems mit Schadprogrammen (beispielsweise Computer-Viren),
- Kompromittierung des Systems durch einen Angreifer, oder auch
- Hardware-Probleme.

Idealerweise sollte das Notfall-Bootmedium alle Programme und Daten enthalten, die zu einer Untersuchung und - falls möglich - der Behebung der Probleme benötigt werden. Gegebenenfalls können unterschiedliche Medien für verschiedene Problemszenarien erstellt werden.

Als "Grundausstattung" für ein Notfall-Bootmedium werden folgende Programme empfohlen:

- Viren-Schutzprogramme mit aktuellen Signaturen,
- Programme zur Bearbeitung von Konfigurationsdateien oder Datenbanken des Systems (Editoren für Dateien, Registry oder ähnliches),
- Programm zur Wiederherstellung des Bootsektors und des MBR (Master Boot Record) der Systemplatte,
- Backup- / Recovery-Programme,
- Diagnoseprogramme zur Analyse von Hardware-Defekten.

Darüber hinaus können Programme zur weitergehenden Analyse hinzugefügt werden, etwa zur forensischen Untersuchung eines kompromittierten Systems.

Dabei ist es wichtig, dass alle Programme und Bibliotheken ausschließlich vom Bootmedium geladen werden. Es dürfen keine Komponenten des installierten Systems verwendet werden. Bei der Erstellung des Bootmediums ist außerdem darauf zu achten, dass neben den notwendigen Programmen auch alle Treiber vorhanden sind, die für den Zugriff auf die eingebauten Platten des Rechners benötigt werden. Dazu zählen beispielsweise Treiber für Festplattencontroller (insbesondere RAID-Controller) und Treiber für eine Festplattenverschlüsselung oder Festplattenkomprimierung.

Falls das Bootmedium genügend Speicherplatz bietet, können weitere Programme oder Dokumentation auf dem Medium gespeichert werden. Beispiels-

weise kann es die Effizienz der Fehlersuche erhöhen, wenn auf dem Bootmedium stets eine aktuelle Dokumentation der Systemkonfiguration enthalten ist.

Das Notfall-Bootmedium muss selbst frei von Viren und anderen Schadprogrammen sein. Es dürfen deshalb nur Programme eingesetzt werden, die aus vertrauenswürdigen Quellen (etwa direkt von der CD des Herstellers) stammen oder deren digitale Signatur überprüft wurde. Zumindest einmal nach der Erstellung sowie bei jeder Änderung sollte das Bootmedium außerdem mit einem Viren-Schutzprogramm überprüft werden.

Es ist nicht unbedingt notwendig, für jedes System ein eigenes Bootmedium zu erstellen. Ein entsprechend flexibel angelegtes Bootmedium kann für eine große Anzahl verschiedener Systeme ausreichend sein. Auf dem Bootmedium braucht nicht einmal notwendigerweise das selbe Betriebssystem eingesetzt zu werden, wie auf dem Zielsystem selbst. Aus Gründen der Kompatibilität ist dies jedoch oft vorteilhaft. Es muss allerdings unbedingt durch entsprechende Tests sichergestellt werden, dass das Medium auch wirklich bei allen Rechnern funktioniert, für die es eingesetzt werden soll. Je nach Betriebssystem müssen außerdem noch systemspezifische Aspekte beachtet werden, die in den jeweiligen IT-Grundschutz-Bausteinen beschrieben werden.

Nach Veränderungen am Zielsystem, etwa einem Update des Betriebssystems oder Konfigurationsänderungen, muss gegebenenfalls das Notfall-Bootmedium und die darauf gespeicherte Dokumentation aktualisiert werden. Änderungen am Bootmedium müssen dokumentiert werden.

Das Notfall-Bootmedium muss für die Systembetreuer schnell greifbar sein, damit im Falle einer Störung nicht wertvolle Zeit verloren geht. Andererseits muss es auch so sicher aufbewahrt werden, dass Unbefugte keinen Zugriff darauf haben.

Die Funktion des Notfall-Bootmediums sollte regelmäßig getestet und die Bedienung der darauf gespeicherten Programme geübt werden, damit sichergestellt ist, dass das Medium im Fall von Problemen funktioniert und die Administratoren mit der Bedienung vertraut sind. Es sollte überlegt werden, mit dem Medium eine kurze gedruckte Anleitung aufzubewahren, die für typische Einsatzszenarien die wichtigsten Schritte zusammenfasst.

Prüffragen:

- Stehen Notfall-Bootmedien zur Verfügung, mit denen die IT-Systeme gestartet und in einen kontrollierten Zustand versetzt werden können?
- Werden alle Programme und Bibliotheken ausschließlich vom Bootmedium geladen?
- Enthalten die Notfall-Bootmedien alle erforderlichen Programme, Treiber und Daten?
- Werden die Notfall-Bootmedien zumindest bei Erstellung und Änderung auf Schadprogramme überprüft?
- Werden Inhalte für Bootmedien aus sicheren Quellen bezogen?
- Werden die Notfall-Bootmedien auf einem aktuellen Stand gehalten?
- Ist sichergestellt, dass nur die hierzu berechtigten Personen auf die Notfall-Bootmedien zugreifen können?
- Werden Bootmedien nach dem Erstellen getestet?

# M 6.25 Regelmäßige Datensicherung der Server-Festplatte

Diese Maßnahme ist mit Version 2005 entfallen.

# M 6.26 Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten

**Verantwortlich für Initiierung:** TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Die Konfigurations- und Anwendungsdaten der eingesetzten TK-Anlage sind regelmäßig zu sichern, insbesondere nachdem sich diese geändert haben. Dazu muss ein entsprechendes Konzept erstellt und mit den allgemeinen Konzepten der Datensicherung abgestimmt werden (siehe B 1.4 *Datensicherungskonzept*). Aufgrund der Ähnlichkeit kann sich das Konzept an dem für die aktiven Netzkomponenten orientieren (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*). Bei Hybrid- oder VoIP-TK-Anlagen kann die Systeminstallation und -konfiguration über Images, Snapshots, Software- und Konfigurationssicherung gesichert werden (siehe dazu auch M 6.101 *Datensicherung bei VoIP*).

Auch Anwendungsdaten wie Kontaktinformationen oder Abrechnungsdaten sollten gesichert werden. Sicherungszeitpunkte und Formen müssen die Anforderungen an den maximal tolerablen Datenverlust berücksichtigen. Die entsprechenden Festlegungen sind in einen Gesamt-Datensicherungsplan des zentralen IT-Bereichs aufzunehmen.

Wesentlich ist, dass in jedem Fall mit Hilfe der getroffenen Vorkehrungen der aktuelle Zustand vor Eintreten einer Störung oder eines Notfalls wiederhergestellt werden kann.

Es ist in regelmäßigen Abständen zu prüfen, ob diese Sicherungen auch tatsächlich als Basis für eine Systemwiederherstellung funktionsfähig sind. Typische Prüfungen dieser Art sind:

- Prüfung von Datenträgern mit System- oder Datensicherungen auf Lesbarkeit
- Prüfung von Images auf Lauffähigkeit nach Probeinstallation auf Testsystemen oder vergleichbarer Ersatzhardware.

Die durchgeführten Tests und Testergebnisse sind zu dokumentieren.

Prüffragen:

- Wird im Rahmen der Ersteinrichtung sowie bei jeder Änderung und in regelmäßigen Abständen eine Datensicherung der TK-Anlagen-Konfigurationsdaten durchgeführt?
- Wurde ein Konzept für TK-Anlagen erstellt und mit den allgemeinen Konzepten der Datensicherung für Server und Netzkomponenten abgestimmt?
- Wird getestet, ob die Sicherungen von TK-Anlagen auch tatsächlich als Basis für eine Systemwiederherstellung genutzt werden können?

# M 6.27 Sicheres Update des BIOS

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Viele IT-Systeme, beispielsweise PCs, benötigen für den Start bzw. für den Betrieb ein *Basic Input Output System* (BIOS). Dieses BIOS setzt sich aus Programmcode und Daten zusammen und dient dazu, wichtige Konfigurationseinstellungen am IT-System vorzunehmen und elementare Ein-/Ausgabe-Funktionen bereitzustellen. In vielen Fällen wird mit diesen Funktionen das eigentliche Betriebssystem geladen, das dann entweder selbst die Kontrolle über die Hardware übernimmt oder weiterhin auf BIOS-Funktionen zurückgreift. Gespeichert wird das BIOS meist in speziellen Speicherbausteinen (z. B. EEPROM oder Flash-EPROM), deren Inhalt auch beim Abschalten der Stromversorgung erhalten bleibt.

Insbesondere bei PCs hat die Vielfalt der Konfigurationsmöglichkeiten dazu geführt, dass das BIOS sehr komplex und damit auch fehleranfälliger geworden ist. Viele Hersteller sind daher dazu übergegangen, einen Update-Mechanismus für das BIOS zu implementieren und regelmäßig fehlerbereinigte Versionen des BIOS zur Verfügung zu stellen. Zur Durchführung des BIOS-Updates bietet der Hersteller meist auch ein spezielles Programm an, mit dem der Inhalt der entsprechenden Speicherbausteine überschrieben werden kann. Wird ein spezielles Programm zum Update des BIOS angeboten, so ist die Vertrauenswürdigkeit seiner Quelle, seine Aktualität und Virenfreiheit sicher zu stellen.

Da das BIOS direkt auf die Hardware zugreift und noch vor Betriebssystemen und Bootloadern geladen wird, sind Manipulationen am BIOS besonders schwer zu entdecken. Aus diesem Grund dürfen nur Administratoren das Recht zur Installation eines neuen BIOS haben.

Grundsätzlich sollte der Update-Mechanismus für das BIOS genutzt werden, um IT-Systeme mit möglichst fehlerfreien BIOS-Versionen auszustatten. Dabei sind jedoch folgende Hinweise zu beachten:

- Als erstes sollte vom derzeit installierten BIOS eine Datensicherung durchgeführt werden. Hierzu bietet die vom Hersteller angebotene Software in der Regel die Möglichkeit, das installierte BIOS auszulesen und als Datei abzuspeichern. Falls sich nach dem BIOS-Update Probleme ergeben, kann diese BIOS-Version wiederhergestellt werden. Falls das Mainboard über ein redundantes BIOS auf einem getrennten Chip verfügt, kann auf die Sicherung verzichtet werden.
- Bei zentralen IT-Systemen, beispielsweise Servern, Netzkoppelelementen und TK-Anlagen, sollten die jeweils aktuell verwendete und die davor letzte funktionsfähige BIOS-Version archiviert werden. Dabei ist darauf zu achten, dass die Datei eindeutig dem jeweiligen IT-System zugeordnet werden kann.
- In vielen Fällen hat ein BIOS-Update Einfluss auf die gespeicherten Konfigurationsdaten. Unter Umständen werden dabei alle vorgenommenen Einstellungen auf Standardwerte zurückgesetzt und gehen somit verloren. Ein modernes BIOS für PCs ist zwar in der Lage, viele Konfigurationsdaten selbst zu ermitteln ("Auto Detect"), insbesondere bei spezielleren Geräten kann es jedoch erforderlich sein, die vorgenommenen Einstellungen vor dem BIOS-Update zu dokumentieren. Hierzu sollten die Empfehlungen des Herstellers beachtet werden.

- Ein Angreifer könnte versuchen, eine ältere BIOS-Version wiederaufzuspielen, um deren Schwachstellen auszunutzen. BIOS-Updates sollten daher (zumindest in Bereichen mit hohem Schutzbedarf) im Rahmen des Patch- und Änderungsmanagements dokumentiert werden.
- BIOS-Updates und Software zum Einspielen von BIOS-Updates werden vom Hersteller oft im Internet zur Verfügung gestellt. Es ist darauf zu achten, dass beides nur vom Hersteller selbst oder von offiziellen Spiegelservern bezogen wird. Im Zweifelsfall sollte beim Hersteller nachgefragt werden, ob eine bestimmte im Internet bereitgestellte Version tatsächlich vom Hersteller freigegeben wurde.
- Inkompatibilitäten oder beschädigte Dateien können dazu führen, dass ein IT-System nach einem BIOS-Update nicht mehr funktioniert. Oft ist es nicht einmal mehr möglich, die vorhergehende, funktionsfähige BIOS-Version wiederherzustellen. In der Regel kann dann nur noch der Händler oder der Hersteller das Gerät wieder betriebsbereit machen, und das IT-System steht unter Umständen längere Zeit nicht zur Verfügung. Daher muss vor dem BIOS-Update sichergestellt werden, dass eine geeignete Ausweichlösung (z. B. ein Ersatzgerät) zur Verfügung steht, falls ein solcher Ausfall nicht toleriert werden kann.
- Neue BIOS-Versionen sollten vor dem Einsatz möglichst getestet werden. Möglich ist dies jedoch nur, wenn mehrere IT-Systeme vorhanden sind, die alle mit dem gleichen BIOS arbeiten. In diesem Fall sollte die neue BIOS-Version zunächst nur auf einem dieser IT-Systeme installiert und dieses Gerät einige Zeit im Betrieb beobachtet werden. Wenn sich dabei keine Probleme zeigen, können die übrigen IT-Systeme nachgezogen werden.
  Hinweis: Es mag attraktiv erscheinen, diesen Test in einer virtuellen Umgebung durch zu führen. Da eine virtuelle Umgebung aber nie exakt die vorhandene Hardware der realen Maschine simuliert, kann solch einem Test nicht vertraut werden. Die Lauffähigkeit eines neuen BIOS muss daher auf einem realen System überprüft werden.
- Einige Hersteller empfehlen für ihre Geräte nicht einfach die neueste BIOS-Version. Stattdessen gibt es Tabellen, in denen abhängig von Einsatzszenario oder Modellnummer des IT-Systems eine bestimmte BIOS-Version empfohlen wird. Dies betrifft hauptsächlich Netzkoppelelemente. Die Empfehlungen des Herstellers sollten beachtet werden.

Prüffragen:

- Wird vor einem BIOS-Update die vorhandene, lauffähige BIOS-Version gesichert?
- Ist sichergestellt, dass eine BIOS-Veränderung nur durch einen Administrator erfolgen kann?
- Werden BIOS-Updates und die dafür benötigten Programme ausschließlich aus vertrauenswürdigen Quellen bezogen?

# M 6.28 Vereinbarung über Lieferzeiten lebensnotwendiger TK-Baugruppen

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.29 TK-Basisanschluss für Notrufe

**Verantwortlich für Initiierung:** TK-Anlagen-Verantwortlicher
**Verantwortlich für Umsetzung:** Administrator

Bei einem Total- oder Teilausfall der TK-Anlage kann es geschehen, dass über die an diese Anlage angeschlossenen Amtsleitungen keine Verbindungen mehr möglich sind. Um dennoch Hilfe heranholen zu können, ist es sinnvoll, einen völlig separaten Basis-Anschluss bzw. analogen Fernsprechanschluss einzurichten.

Prüffragen:

- Existiert eine Regelung für einen Notfallplan bei Ausfall des TK-Systems?
- Ausfall des TK-Systems: Existiert eine redunddante Kommunikationsmöglichkeit über dedizierte Kanäle beziehungsweise Anschlüsse?

# M 6.30 Katastrophenschaltung

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.31 Verhaltensregeln nach Verlust der Systemintegrität

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Falls sich das Unix-System in nicht vorgesehener Weise verhält (zum Beispiel undefiniertes Systemverhalten, nicht auffindbare Daten, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde), kann ein Verlust der Systemintegrität vorliegen. Dieser kann durch missbräuchliche Nutzung des Systems verursacht worden sein, zum Beispiel durch Veränderungen der Systemeinstellungen, Einspielen eines Trojanisches Pferdes oder eines Computer-Virus.

Dann sollten die Benutzer folgende Punkte beachten:

- Ruhe bewahren!
- Benachrichtigen Sie den Administrator.
- Beenden Sie laufende Programme.

Der Administrator sollte folgende Schritte durchführen:

- Herunterfahren des Systems,
- Hochfahren des Systems, so dass nur Zugriff von der Konsole aus möglich ist (z. B. Single-User-Modus),
- Anfertigung einer Komplettdatensicherung (Dies ist beispielsweise hilfreich, wenn bei der nachfolgenden Untersuchung Daten oder Spuren zerstört werden.),
- Überprüfung der ausführbaren Dateien auf sichtbare Veränderungen, z. B. Erstellungsdatum und Dateigröße (Da diese von einem Angreifer auch wieder auf ihre Ursprungswerte zurückgesetzt werden können, sollte die Integrität der Dateien mit Prüfsummenverfahren wie *tripwire* überprüft werden.),
- Löschen der ausführbaren Dateien und Wiedereinspielen der Original-Dateien von schreibgeschützten Datenträgern (siehe M 6.21 *Sicherungskopie der eingesetzten Software*) (keine Programme aus der Datensicherung wiedereinspielen),
- Überprüfen und ggf. Wiedereinspielen der Systemverzeichnisse und -dateien und ihrer Attribute (z. B. */etc/inetd.conf*, */etc/hosts.equiv*, *cron*- und *at*-jobs, etc.),
- Überprüfung der Attribute aller Benutzerverzeichnisse und -dateien z. B. mit Prüfsummenverfahren wie *tripwire* und gegebenenfalls Zurücksetzen auf Minimal-Einstellungen (nur Rechte für den Eigentümer, keine *root*-Dateien in Benutzerbereichen, *.rhost*- und *.forward*-Dateien, auch gesperrte Accounts),
- Änderung aller Passwörter,
- Benachrichtigung der Benutzer mit der Bitte, ihre Bereiche auf Unregelmäßigkeiten zu prüfen.

Nach der Änderung aller Passwörter müssen diese den betroffenen Benutzern mitgeteilt werden. Hierbei sollte **kein** allen Benutzern bekanntes Passwort oder Ableitungsschema benutzt werden. Besser ist es, die Passwörter zufällig zu erzeugen und den Benutzern auf zuverlässigem Weg mitzuteilen, z. B. in versiegelten Umschlägen. Diese Passwörter sollten unmittelbar nach der Erstanmeldung geändert werden.

Wenn Anzeichen auf einen vorsätzlichen Angriff gegen ein Unix-System vorliegen, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Alarmplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen über den Vorfall zu unterrichten sind (siehe auch M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*). Der Alarmplan enthält gegebenenfalls auch Informationen darüber, ob und wie der Datenschutzbeauftragte und die Rechtsabteilung zu beteiligen sind.

Falls sich Probleme ergeben, können Sie sich an die Hotline des BSI wenden unter Telefon 0228-9582-5222 oder E-Mail *certbund@bsi.bund.de*.

Falls Daten gelöscht oder unerwünscht geändert wurden, können diese aus den Datensicherungen wiedereingespielt werden.

Prüffragen:

- Existieren Verhaltensregeln nach Verlust der Systemintegrität?
- Existiert ein geeigneter Alarmplan zur Schadensminimierung?

# M 6.32 Regelmäßige Datensicherung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden.

Es müssen mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen abgeleitet werden können. Dokumentationen, Programm- und Programmablaufbeschreibungen sind gemäß M 2.111 *Bereithalten von Handbüchern* vorzuhalten.

Empfehlenswert ist die Erstellung eines Datensicherungskonzepts.

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist folgendes festzulegen:

- Zeitintervall
  Beispiele: täglich, wöchentlich, monatlich
- Zeitpunkt
  Beispiele: nachts, freitags abends
- Anzahl der aufzubewahrenden Generationen
  Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitag-Abend-Sicherungen der letzten zwei Monate.
- Umfang der zu sichernden Daten
  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.
  Beispiel: selbst erstellte Dateien und individuelle Konfigurationsdateien
- Speichermedien (abhängig von der Datenmenge)
  Beispiele: Bänder, Kassetten, CDs oder DVDs, Festplatten
- Vorherige Löschung der Datenträger vor Wiederverwendung (z. B. bei Bändern oder Kassetten)
- Zuständigkeit für die Durchführung (Administrator, Benutzer)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)
- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wieder eingespielt werden. Daher und zur Senkung der Kosten sollten zwischen den Komplettsicherungen regelmäßig differentielle oder inkrementelle Sicherungen durchgeführt werden. Hinweise zu den verschiedenen Arten von Datensicherungen finden sich in M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*.

Eine differentielle oder inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist separat zu entscheiden, ob sie von der regelmäßigen Datensicherung erfasst werden muss. Dies hängt beispielsweise davon ab, wie aufwendig eine Neuinstallation und das Einspielen von Patches und Updates ist. Unter Umständen ist es ausreichend, Sicherungskopien von den Originaldatenträgern anzufertigen.

Es muss regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können.

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um gegebenenfalls auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Falls bei vernetzten Rechnern nur die Server-Platten gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den Benutzern oder automatisch dorthin überspielt werden. Bei größeren Änderungen an IT-Systemen oder im Informationsverbund muss der Datensicherungsprozess entsprechend angepasst werden.

Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, wobei darauf zu achten ist, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich sein muss (siehe M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*).

Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

Prüffragen:

- Bei vertraulichen Daten, gegebenenfalls auch bei Auslagerung der Backups: Werden die gesicherten Daten verschlüsselt gespeichert?
- Werden zumindest alle Daten, die nicht aus anderen Informationen abgeleitet werden können, regelmäßig gesichert?
- Ist festgelegt, wie die Datensicherungen organisatorisch und technisch ablaufen?
- Entspricht das festgelegte Verfahren für die Datensicherungen den Verfügbarkeitsanforderungen?
- Sind die Benutzer über die Festlegungen zur Durchführung von Datensicherungen informiert?
- Wird regelmäßig getestet, ob die gesicherten Daten problemlos zurückgespielt werden können?

# M 6.33 Entwicklung eines Datensicherungskonzepts

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT, Verantwortliche der einzelnen Anwendungen

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Die technischen Möglichkeiten, Datensicherungen durchzuführen, sind vielfältig. Jedoch wird die Auswahl immer von den genannten Faktoren bestimmt. Daher gilt es zunächst, die Einflussgrößen der IT-Systeme und der damit realisierten IT-Anwendungen zu bestimmen und nachvollziehbar zu dokumentieren. Anschließend muss die geeignete Verfahrensweise entwickelt und dokumentiert werden. Zum Abschluss muss durch die Behörden-/Unternehmensleitung die Durchführung angeordnet werden.

Das Datensicherungskonzept muss für die Gewährleistung einer funktionierenden Datensicherung die Datenrestaurierbarkeit mittels praktischer Übungen als Verpflichtung vorsehen (siehe M 6.41 *Übungen zur Datenrekonstruktion*).

Die Ergebnisse sollten aktualisierbar und erweiterbar in einem Datensicherungskonzept niedergelegt werden. Ein möglicher Aufbau eines Datensicherungskonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

**Inhaltsverzeichnis Datensicherungskonzept**

**1. Definitionen**
- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Vollsicherung, inkrementelle Datensicherung

**2. Gefährdungslage zur Motivation**
- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

**3. Einflussfaktoren je IT-System**
- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten

- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

**4. Datensicherungsplan je IT-System**
**4.1 Festlegungen je Datenart**

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

**4.2 Festlegung der Vorgehensweise bei der Datenrestaurierung**
- Randbedingungen für das Datensicherungsarchiv
    - Vertragsgestaltung (bei externen Archiven)
    - Refresh-Zyklen der Datensicherung
    - Bestandsverzeichnis
    - Löschen von Datensicherungen
    - Vernichtung von unbrauchbaren Datenträgern
- Vorhalten von arbeitsfähigen Lesegeräten

**5. Minimaldatensicherungskonzept**

**6. Verpflichtung der Mitarbeiter zur Datensicherung**

**7. Sporadische Restaurierungsübungen**

Einzelne Punkte dieses Datensicherungskonzepts werden in den Maßnahmen M 6.34 *Erhebung der Einflussfaktoren der Datensicherung*, M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*, M 6.37 *Dokumentation der Datensicherung*, M 6.41 *Übungen zur Datenrekonstruktion* und M 2.41 *Verpflichtung der Mitarbeiter zur Datensicherung* näher ausgeführt, so dass nach Bearbeitung dieser Maßnahmen für jedes relevante IT-System die wesentlichen Teile eines anwenderspezifischen Datensicherungskonzepts erstellt sind.

Prüffragen:

- Existiert ein aktuelles Datensicherungskonzept?
- Sind sämtliche betroffenen IT-Systeme im Datensicherungskonzept aufgeführt?
- Sind die Mitarbeiter über den sie betreffenden Teil des Datensicherungskonzepts unterrichtet?
- Wird die Umsetzung des Datensicherungskonzepts regelmäßig kontrolliert?

# M 6.34 Erhebung der Einflussfaktoren der Datensicherung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Verantwortliche der einzelnen Anwendungen

Für jedes IT-System, eventuell sogar für einzelne IT-Anwendungen mit besonderer Bedeutung, müssen die nachfolgenden Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren.

Nachfolgend soll an einem fiktiven Beispiel aufgezeigt werden, wie die Ermittlung der Einflussfaktoren in der Praxis vollzogen werden kann. Das Beispiel geht von einem servergestützten LAN mit 10 angeschlossenen PCs als Workstations aus. Das IT-System dient der Auftragsbearbeitung mittels einer Kundendatenbank. Die Anwendungsdaten werden zentral auf dem Netzserver gespeichert.

Im einzelnen muss ermittelt werden:

**Spezifikation der zu sichernden Daten**

Ermittelt werden sollte der Datenbestand des IT-Systems (der IT-Anwendung), der für die Erledigung der Fachaufgaben erforderlich ist. Dazu gehören die Anwendungs- und Betriebssoftware, die Systemdaten (z. B. Initialisierungsdateien, Makrodefinitionen, Konfigurationsdaten, Textbausteine, Passwortdateien, Zugriffsrechtedateien), die Anwendungsdaten selbst und Protokolldaten (Login-Protokollierung, Protokolle über Sicherheitsverletzungen, Datenübertragungsprotokolle, ...).

**Beispielergebnis 1: Spezifikation der zu sichernden Daten**

IT-System: Servergestütztes LAN mit 10 angeschlossenen PCs
Zu sichernde Daten:

- Software:
  Netzbetriebssystem, Betriebssysteme der PCs, Textverarbeitungssoftware, Datenbank-Software etc. in Form von Standardsoftware
- Systemdaten:
  am Netz-Server: Systeminterne Einstellungen (z. B. Rechtestruktur, Passworte)
  an den PCs: Initialisierungsdateien der Textverarbeitungssoftware und der Datenbank-Software, Makrodefinitionen und Textbausteine
- Anwendungsdaten auf dem Netz-Server:
  Dateien mit Schriftverkehr, Kundendatenbank
- Protokolldaten auf dem Netz-Server:
  Protokollierung der Netzaktivitäten

**Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten**

Für die im ersten Schritt spezifizierten Daten müssen nun die Verfügbarkeitsanforderungen festgelegt werden. Ein erprobtes Maß dazu ist die Angabe der maximal tolerierbaren Ausfallzeit (mtA). Sie gibt an, über welchen Zeitraum die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss. Betrachtet werden

sollte dabei auch, ob aufgrund der Papierlage ohne IT-Unterstützung kurzfristig weitergearbeitet werden kann.

**Beispielergebnis 2: Verfügbarkeitsanforderungen**

- Software: mtA 1 Tag
- Systemdaten:
  - am Netz-Server: mtA 1 Tag
  - am PC: mtA 1 Woche (auf *einen* PC kann bis zu einer Woche verzichtet werden)
- Anwendungsdaten:
  - Dateien mit Schriftverkehr: mtA 1 Woche
  - Kundendatenbank: mtA 1 Tag
- Protokolldaten: mtA 3 Tage

**Rekonstruktionsaufwand der Daten ohne Datensicherung**

Um ein unter wirtschaftlichen Gesichtspunkten angemessenes Datensicherungskonzept zu entwickeln, ist es notwendig zu wissen, ob und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden können, wenn eine Datensicherung nicht zur Verfügung steht. Untersucht werden sollte, aus welchen Quellen die Daten rekonstruiert werden können. Beispiele hierfür sind die Aktenlage, Ausdrucke, Mikrofiche, Befragungen und Erhebungen.

Gemessen werden sollte der pekuniäre Aufwand oder der Arbeitsaufwand von Datenerfassungskräften in Arbeitstagen (AT).

**Beispielergebnis 3: Rekonstruktionsaufwand**

- Software:
  Wiederbeschaffung durch Kauf und anschließender Installation innerhalb eines Tages (sofern keine Originalsoftware mehr vorliegt)
- Systemdaten:
  - am Netz-Server: manuelle Rekonstruktion: 1 AT
  - am PC: 1 AT
- Anwendungsdaten:
  Dateien mit Schriftverkehr: zielorientierte Erfassung aus aktueller Papierlage: 10 AT (eine vollständige Nacherfassung des Schriftverkehrs ist nicht erforderlich)
  Kundendatenbank: Kompletterfassung aus Papierlage: 10 AT
- Protokolldaten:
  nicht rekonstruierbar, da kein Ausdruck auf Papier erfolgt

**Datenvolumen**

Für die Auswahl des Speichermediums ist ein entscheidender Faktor das gespeicherte und zu sichernde Datenvolumen. Die erforderliche Angabe richtet sich ausschließlich auf die zu sichernden Daten und sollte als Maßeinheit Megabyte (MB) benutzen.

**Beispielergebnis 4: Datenvolumen**

- Software: 100 MB
- Systemdaten:
  - am Netz-Server: 2 MB
  - am PC: 0,3 MB

- Anwendungsdaten:
  - Dateien mit Schriftverkehr: 100 MB
  - Kundendatenbank: 10 MB
- Protokolldaten: 10 MB (wöchentliche Kontrolle nebst Löschung)

**Änderungsvolumen**

Um die Häufigkeit der Datensicherung und das adäquate Sicherungsverfahren bestimmen zu können, muss bekannt sein, wieviele Daten/Dateien sich in einem bestimmten Zeitabschnitt ändern. Als Arbeitsgröße wäre hier eine Einheit MB/Woche denkbar. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.

**Beispielergebnis 5: Änderungsvolumen**

- Software: durchschnittlich 50 MB bei einem Versionswechsel, höchstens einmal jährlich
- Systemdaten:
  - am Netz-Server: 0,1 MB/Woche
  - am PC: 0,1 MB/Woche
- Anwendungsdaten:
  - Dateien mit Schriftverkehr: 1 MB/Woche durch neue Dateien
  - Kundendatenbank: 10 MB/Woche durch Änderungen in der Datenbank (die Datenbank kann nur vollständig gesichert werden).
- Protokolldaten: 10 MB/Woche

**Änderungszeitpunkte der Daten**

Es gibt IT-Anwendungen, bei denen sich Datenänderungen nur zu bestimmten Terminen ergeben, wie zum Beispiel der Abrechnungslauf zur Lohnbuchhaltung zum Monatsende. In solchen Fällen ist eine Datensicherung unverzüglich nach einem solchen Termin sinnvoll. Daher sollte für die zu sichernden Daten angegeben werden, ob sie sich täglich, wöchentlich oder zu bestimmten Terminen ändern.

**Beispielergebnis 6: Änderungszeitpunkte**

- Software: Änderungen nur bei einem Versionswechsel
- Systemdaten: häufige Änderungen
- Anwendungsdaten:
  - Dateien mit Schriftverkehr: tägliche Änderungen
  - Kundendatenbank: tägliche Änderungen
- Protokolldaten: ständige Änderung

**Fristen**

Für die Daten ist zu klären, ob bestimmte Fristen einzuhalten sind. Hierbei kann es sich um Aufbewahrungsfristen oder auch um Löschfristen im Zusammenhang mit personenbezogenen Daten handeln. Diese Fristen sind bei der Festlegung der Datensicherung zu berücksichtigen.

**Beispielergebnis 7: Fristen**

- Software:
  Aufbewahrung der Datensicherungsbestände ist nicht erforderlich
- Systemdaten:
  Aufbewahrung der Datensicherungsbestände ist nicht erforderlich
- Anwendungsdaten:

Dateien mit Schriftverkehr: Aufbewahrungsfrist für Buchungsbelege beträgt sechs Jahre (§257 HGB); ein (Jahres-) Datensicherungsbestand ist für diese Zeit aufzuheben
Kundendatenbank: Aufbewahrung der Daten ist nicht erforderlich, Löschfristen sind gemäß BDSG (§20 bzw. § 35) zu beachten

- Protokolldaten:
  nach der wöchentlichen Auswertung der Protokolldaten müssen regelmäßig 2 MB der Daten für ein Jahr bzw. bis zur Prüfung durch den Datenschutzbeauftragten aufbewahrt werden

**Vertraulichkeitsbedarf der Daten**

Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie. Bei der Zusammenführung von Sicherungskopien mit gleichem Vertraulichkeitsbedarf auf einem Datenträger, kann sich durch die Kumulation ein höherer Vertraulichkeitsbedarf der gespeicherten Daten ergeben. Anzugeben ist also, wie hoch der Vertraulichkeitsbedarf der einzelnen zu sichernden Daten ist und zusätzlich, welche Kombinationen von Daten einen höheren Vertraulichkeitsbedarf haben als die Daten selbst.

**Beispielergebnis 8: Vertraulichkeitsbedarf**

- Software:
  geringer Vertraulichkeitsbedarf, da es sich um öffentlich zugängliche Daten handelt, lediglich Copyright-Vereinbarungen sind zu beachten
- Systemdaten:
  - am Netz-Server: mittel vertraulich (Passworte sind verschlüsselt gespeichert)
  - am PC: nicht vertraulich
- Anwendungsdaten:
  - Dateien mit Schriftverkehr: Einzeldateien besitzen mittleren Vertraulichkeitsbedarf, sämtliche Dateien zusammen einen hohen Vertraulichkeitsbedarf
  - Kundendatenbank: hoher Vertraulichkeitsbedarf
- Protokolldaten: hoher Vertraulichkeitsbedarf (personenbezogene Daten, die ein Nutzungsprofil ermöglichen)

**Integritätsbedarf der Daten**

Für Datensicherungen muss sichergestellt sein, dass die Daten integer gespeichert wurden und während der Aufbewahrungszeit nicht verändert werden. Dies ist um so wichtiger, je höher der Integritätsbedarf der Nutzdaten ist. Daher ist für die Datensicherungen anzugeben, wie hoch der Integritätsbedarf ist.

**Beispielergebnis 9: Integritätsbedarf**

- Software: Die Software muss hohe Integritätsansprüche erfüllen.
- Systemdaten:
  - am Netz-Server: hoher Integritätsbedarf (wegen Rechteverwaltung)
  - am PC: hoher Integritätsanspruch
- Anwendungsdaten:
  - Dateien mit Schriftverkehr: Einzeldateien besitzen einen mittleren Integritätsbedarf
  - Kundendatenbank: hoher Integritätsbedarf
- Protokolldaten:

Die Daten besitzen bis zur Auswertung einen hohen Integritätsbedarf, nach der Auswertung besitzen nur noch die aufzubewahrenden Daten einen mittleren Integritätsbedarf.

**Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer**

Um entscheiden zu können, wer die Datensicherung durchführt, der IT-Benutzer selbst oder speziell beauftragte Mitarbeiter bzw. die Systemadministratoren, ist ausschlaggebend, über welche Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer verfügt und welche Werkzeuge ihm zur Verfügung gestellt werden können. Falls die zeitliche Belastung bei der Durchführung einer Datensicherung für IT-Benutzer zu hoch ist, sollte dies angegeben werden.

**Beispielergebnis 10: Kenntnisse**

- Der Netzadministrator verfügt über ausreichende Kenntnisse, die Datensicherung am Netz-Server durchzuführen. Die IT-Benutzer des PCs verfügen über ausreichende Kenntnisse und Fähigkeiten, die Datensicherung der PC-Systemdaten selbständig durchzuführen.

Prüffragen:

- Wurden bei der Erhebung der Einflussfaktoren der Datensicherung sowohl die Administratoren als auch die IT-Anwender eingebunden?
- Werden neue Anforderungen an die Datensicherung zeitnah in einem aktualisierten Datensicherungskonzept berücksichtigt?

# M 6.35 Festlegung der Verfahrensweise für die Datensicherung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, IT-Sicherheitsbeauftragter

Die Verfahrensweise, wie die Datensicherung durchzuführen ist, wird von den in M 6.34 *Erhebung der Einflussfaktoren der Datensicherung* erhobenen Einflussfaktoren bestimmt. Für jedes IT-System und für jede Datenart muss die Verfahrensweise der Datensicherung festgelegt werden. Bei Bedarf ist sogar noch eine Unterscheidung für einzelne IT-Anwendungen des IT-Systems vorzunehmen, wenn sich hier differente Datensicherungsstrategien ergeben, was insbesondere im Großrechnerbereich sinnvoll sein kann.

Folgende Modalitäten einer Datensicherung sind für die Festlegung einer Verfahrensweise für die Datensicherung zu betrachten:

- Art der Datensicherung,
- Häufigkeit und Zeitpunkt der Datensicherung,
- Anzahl der Generationen,
- Vorgehensweise und Speichermedium,
- Verantwortlichkeit für die Datensicherung,
- Aufbewahrungsort,
- Anforderungen an das Datensicherungsarchiv,
- Transportmodalitäten und
- Aufbewahrungsmodalität.

In der nachfolgenden Tabelle werden die Abhängigkeiten zwischen den Modalitäten einer Datensicherung und den Einflussfaktoren dargestellt und anschließend erläutert:

| | **Art der Datensicherung** | **Häufigkeit und Zeitpunkte der Datens.** | **Anzahl der Generationen** | **Vorgehensweise und Speichermedium** | **Verantwortlichkeit für Datens.** | **Aufbewahrungsort** | **Anforderungen an DS-Archiv** | **Transportmodalitäten** | **Aufbewahrungsmodalität** |
|---|---|---|---|---|---|---|---|---|---|
| Verfügbarkeitsanforderungen | X | (X) | X | X | X | X | X | X | |
| Rekonstruktionsaufwand ohne | | (X) | X | | | | | | |

| | **Art der Datensicherung** | **Häufigkeit und Zeitpunkte der Datens.** | **Anzahl der Generationen** | **Vorgehensweise und Speichermedium** | **Verantwortlichkeit für Datens.** | **Aufbewahrungsort** | **Anforderungen an DS-Archiv** | **Transportmodalitäten** | **Aufbewahrungsmodalität** |
|---|---|---|---|---|---|---|---|---|---|
| Datens. | | | | | | | | | |
| Datenvolumen | X | | X | X | | X | X | X | |
| Änderungsvolumen | X | X | X | X | | | | | |
| Änderungszeitpunkte der Daten | (X) | X | | | | | | (X) | |
| Fristen | | | | X | | | X | | X |
| Vertraulichkeitsbedarf der Daten | | | | (X) | X | | X | X | X |
| Integritätsbedarf der Daten | | | (X) | (X) | X | | X | X | X |
| Kenntnisse der IT-Benutzer | X | | | X | X | | | | |

X bedeutet direkter Einfluss, (X) bedeutet indirekter Einfluss

Tabelle: Datensicherung

Erläuterungen:

**Art der Datensicherung**

Folgende Datensicherungsarten lassen sich aufzeigen:

- **Volldatensicherung**: bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einen zusätzlichen Datenträger gespeichert. Es wird dabei nicht berücksichtigt, ob die Dateien sich seit der letzten Datensicherung geändert haben oder nicht. Daher benötigt eine Volldatensicherung einen hohen Speicherbedarf. Der Vorteil ist, dass die Daten vollständig für den Sicherungszeitpunkt vorliegen und die Restaurierung von Dateien einfach und schnell möglich ist, da nur die betroffenen Dateien aus der letzten Volldatensicherung extrahiert werden müssen. Werden Volldatensicherungen selten durchgeführt, so kann sich durch umfangreiche nachträgliche Änderungen innerhalb einer Datei ein hoher Nacherfassungsaufwand ergeben.
- **Inkrementelle Datensicherung**: bei der inkrementellen Datensicherung werden im Gegensatz zur Volldatensicherung nur die Dateien gesichert, die sich gegenüber der letzten Datensicherung (Volldatensicherung oder inkrementelle Sicherung) geändert haben. Dies spart Speicherplatz und verkürzt die erforderliche Zeit für die Datensicherung. Für die Restaurierung der Daten ergibt sich i. allg. ein höherer Zeitbedarf, da die Dateien aus Datensicherungen verschiedener Zeitpunkte extrahiert werden müssen. Die inkrementelle Datensicherung basiert immer auf einer Volldatensicherung. In periodischen Zeitabständen werden Volldatensicherungen erzeugt, in der Zeit dazwischen werden eine oder mehrere inkrementelle Datensicherungen vollzogen. Bei der Restaurierung wird die letzte Volldatensicherung als Grundlage genommen, die um die in der Zwischenzeit geänderten Dateien aus den inkrementellen Sicherungen ergänzt wird.
- **Differentielle Datensicherung**: bei der differentiellen Datensicherung werden nur die Dateien gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben. Eine differentielle Datensicherung benötigt mehr Speicherplatz als eine inkrementelle, Dateien lassen sich aber einfacher und schneller restaurieren. Für die Restaurierung der Daten reicht die letzte Volldatensicherung sowie die aktuellste differentielle, nicht wie bei der inkrementellen, wo unter Umständen mehrere Datensicherungen nacheinander eingelesen werden müssen.
- **Hinweis:** Häufig wird auch **Datenspiegelung** als Datensicherungsmethode bezeichnet. Bei der Datenspiegelung werden die Daten redundant und zeitgleich auf verschiedenen Datenträgern gespeichert. Da so der Ausfall eines dieser Speicher ohne Zeitverlust überbrückt werden kann, steigert Datenspiegelung die Verfügbarkeit. Es ersetzt allerdings keine Datensicherung, da es nicht gegen Gefährdungen wie Diebstahl, Brand oder unbeabsichtigte Datenlöschung hilft.

Eine spezielle Form dieser genannten Datensicherungsstrategien ist die Image-Datensicherung. Bei der Image-Datensicherung werden nicht die einzelnen Dateien eines Festplattenstapels gesichert, sondern die physikalischen Sektoren der Festplatte.

Es handelt sich dabei um eine Vollsicherung, die sehr schnell auf eine gleichartige Festplatte restauriert werden kann.

Eine weitere Form ist das Hierarchische Speicher-Management (HSM). Hierbei geht es in erster Linie um die wirtschaftliche Ausnutzung teurer Speicher. Dateien werden abhängig von der Häufigkeit, mit der auf sie zugegriffen wird, auf schnellen Online-Speichern (Festplatten) gehalten, auf Nearline-Speicher (automatische Datenträger-Wechselsysteme) ausgelagert oder auf Offline-Speichern (Magnetbänder) archiviert. Gleichzeitig bieten diese HSM-Sy-

steme i. A. auch automatische Datensicherungsroutinen kombiniert aus inkrementeller Datensicherung und Volldatensicherung.

Eine redundante Datenspeicherung bieten RAID-Systeme an (Redundant Array of Inexpensive Disks). Das RAID-Konzept beschreibt die Verbindung von mehreren Festplatten unter dem Kommando eines sogenannten Array-Controllers. Man unterscheidet verschiedene RAID-Level, wovon RAID-Level 1 die Datenspiegelung beschreibt.

RAID-Systeme ersetzen keine Datensicherung! RAID-Systeme helfen nicht bei Diebstahl oder Brand, daher müssen auch die auf RAID-Systemen gespeicherten Daten auf zusätzliche Medien gesichert werden und diese Medien auch in anderen Brandabschnitten untergebracht werden.

Für die Entscheidung, welche Datensicherungsstrategie angewendet werden soll, sind die folgenden Einflussfaktoren zu berücksichtigen, um eine für die Anforderungen geeignete und gleichzeitig wirtschaftliche Form zu finden:

*Verfügbarkeitsanforderungen:*

Sind die Verfügbarkeitsanforderungen sehr hoch, so ist eine Datenspiegelung in Erwägung zu ziehen, sind die Verfügbarkeitsanforderungen hoch, so sollte einer Volldatensicherung gegenüber der inkrementellen Datensicherung der Vorzug gegeben werden.

*Datenvolumen und Änderungsvolumen*:

Entspricht das Änderungsvolumen annähernd dem Datenvolumen (z. B. bei der Nutzung einer Datenbank), so verringert sich die Speicherplatzersparnis der inkrementellen Datensicherung so stark, dass eine Vollsicherung in Erwägung gezogen werden kann. Ist jedoch das Änderungsvolumen erheblich kleiner als das Datenvolumen, so spart die inkrementelle Datensicherung Speicherplatz und damit Kosten im großen Umfang.

*Änderungszeitpunkte der Daten*:

Einen geringen Einfluss auf die Datensicherungsstrategie können die Änderungszeitpunkte der Daten haben. Gibt es Zeitpunkte, an denen anwendungsbezogen der Komplettdatenbestand gesichert werden muss (z. B. nach buchhalterischen Wochen-, Monats- oder Jahresabschlüsse), so kommt zu diesen Zeitpunkten nur eine Vollsicherung in Frage.

Kenntnisse der IT-Benutzer:

Die Implementierung einer Datenspiegelung setzt entsprechende Kenntnisse des Systemadministrators voraus, erfordert jedoch auf Seiten der IT-Benutzer keinerlei Kenntnisse.
Eine Volldatensicherung lässt sich auch von einem IT-Benutzer mit geringen Systemkenntnissen durchführen. Demgegenüber erfordert eine inkrementelle Datensicherung schon mehr Systemkenntnisse und Erfahrungen im Umgang mit Datensicherungen.

**Häufigkeit und Zeitpunkte der Datensicherung**

Tritt ein Datenverlust ein (z. B. durch Headcrash auf der Festplatte), so müssen zur Restaurierung der Daten sämtliche Datenänderungen seit der letzten Datensicherung nochmals vollzogen werden. Je kürzer der zeitliche Abstand der Datensicherungen ist, um so geringer ist i. allg. auch der für eine Restaurierung und Nacherfassung erforderliche Zeitaufwand. Gleichzeitig muss be-

achtet werden, dass der Zeitpunkt der Datensicherung nicht nur periodisch (täglich, wöchentlich, werktags, ...) gewählt werden kann, sondern dass auch ereignisabhängige Datensicherungen (z. B. nach x Transaktionen, nach Ausführung eines bestimmten Programms, nach Systemänderungen) notwendig sein können.

Zur Auswahl der Häufigkeit und Zeitpunkte der Datensicherung sind folgende Einflussfaktoren zu beachten.

*Verfügbarkeitsanforderungen, Rekonstruktionsaufwand ohne Datensicherung und Änderungsvolumen:*

Der zeitliche Abstand der Datensicherungen ist so zu wählen, dass die Restaurierungs- und Nacherfassungszeit (Rekonstruktionsaufwand der geänderten Daten, für die keine Datensicherung vorhanden ist) der in diesem Zeitraum geänderten Daten (Änderungsvolumen) kleiner als die maximal tolerierbare Ausfallzeit ist.

*Änderungszeitpunkte der Daten:*

Gibt es Zeitpunkte, an denen sich die Daten in großem Umfang ändern (z. B. Programmlauf für Gehaltszahlung oder Versionswechsel der Software) oder an denen der Komplettdatenbestand vorliegen muss, so bietet es sich an, unmittelbar danach eine Volldatensicherung durchzuführen. Dazu sind neben den periodischen die ereignisabhängigen Datensicherungszeitpunkte festzulegen.

**Anzahl der Generationen**

Einerseits werden Datensicherungen in kurzen Zeitabständen wiederholt, um eine Kopie eines möglichst aktuellen Datenbestandes verfügbar zu haben, andererseits muss die Datensicherung gewährleisten, dass gesicherte Daten möglichst lange aufbewahrt werden. Bezeichnet man eine Volldatensicherung als Generation, so bedarf es einer Festlegung der Anzahl der aufzubewahrenden Generationen und des zeitlichen Abstandes, der zwischen den Generationen liegen muss. Diese Anforderungen lassen sich an folgenden Beispielen erläutern:

- Wird eine Datei absichtlich oder unabsichtlich gelöscht, so ist diese Datei in allen späteren Datensicherungen nicht mehr verfügbar. Stellt sich heraus, dass diese gelöschte Datei dennoch benötigt wird, so muss zur Restaurierung auf eine ältere Datensicherung zurückgegriffen werden, die zeitlich vor dem Löschen erstellt wurde. Ist eine solche Generation nicht mehr vorhanden, so muss die Datei neu erfasst werden.
- Tritt ein Integritätsverlust in einer Datei auf (z. B. durch einen technischen Defekt, durch unbeabsichtigtes Ändern einer Datei oder durch einen Computer-Virus), so ist es wahrscheinlich, dass dies nicht direkt, sondern erst zeitlich versetzt bemerkt wird. Um die Integrität der Datei wiederherstellen zu können, muss dann auf eine Generation zurückgegriffen werden, die vor dem Integritätsverlust erstellt wurde.
- Es kann nicht ausgeschlossen werden, dass die Erstellung einer Datensicherung fehlerhaft oder unvollständig durchgeführt wurde. In diesem Fall ist es oftmals hilfreich, wenn auf eine weitere Generation zurückgegriffen werden kann.

Um diese Vorteile des Generationenprinzips aufrechterhalten zu können, muss jedoch eine Randbedingung eingehalten werden: der zeitliche Abstand der Generationen darf ein Mindestmaß nicht unterschreiten. Beispiel: In einem automatisierten Datensicherungsverfahren kommt es zu wiederholten Abbrü-

chen des Datensicherungslaufs. Hierdurch würden nacheinander sämtliche Generationen überschrieben werden. Verhindert werden kann dies, indem vor Überschreiben einer Generation das Mindestalter überprüft und nur dann überschrieben wird, wenn dieses Alter überschritten ist.

Charakterisieren lässt sich ein Generationsprinzip durch zwei Größen: das *Mindestalter* der ältesten Generation und die *Anzahl* der verfügbaren Generationen. Dabei gilt:

- je höher das Mindestalter der ältesten Generation ist, je größer ist die Wahrscheinlichkeit, dass zu einer Datei mit Integritätsverlust (eine gelöschte Datei, die im Nachhinein als notwendig erkannt wird, ist ebenfalls darunter zu fassen) noch eine Vorläuferversion vorhanden ist,
- je größer die Anzahl der verfügbaren Generationen ist, um so aktueller ist die angeforderte Vorläuferversion.

Die Anzahl der Generationen steht aber im direkten Zusammenhang mit den Kosten der Datensicherung, da Datenträger in ausreichender Zahl zur Verfügung stehen müssen. Dies folgt aus der Notwendigkeit, dass für jede Generation eigene Datenträger benutzt werden sollten. Aus Wirtschaftlichkeitsgründen muss daher die Anzahl der Generationen auf ein sinnvolles Maß beschränkt werden.

Für die Wahl der Parameter des Generationsprinzips ergeben sich folgende Einflüsse:

Verfügbarkeitsanforderungen und Integritätsbedarf der Daten:

Je höher die Verfügbarkeitsanforderungen oder der Integritätsbedarf der Daten sind, umso mehr Generationen müssen vorhanden sein, um im Fall des Integritätsverlustes die Restaurierungszeit zu minimieren.
Wenn der Verlust einer Datei oder eine Integritätsverletzung möglicherweise erst sehr spät bemerkt werden kann, sind zusätzliche Quartals- oder Jahressicherungsdatenbestände empfehlenswert.

*Rekonstruktionsaufwand ohne Datensicherung*:

Sind die Daten zwar umfangreich, aber auch ohne Datensicherung rekonstruierbar, so kann dies als eine weitere "Pseudo-Generation" ins Kalkül gezogen werden.

*Datenvolumen*:

Je höher das Datenvolumen ist, desto höher sind auch die Kosten einer Generation aufgrund des benötigten Speicherplatzes. Ein hohes Datenvolumen kann deshalb die Anzahl der Generationen aus wirtschaftlichen Gründen beschränken.

*Änderungsvolumen*:

Je höher das Änderungsvolumen ist, um so kürzer sollten die Zeitabstände zwischen den Generationen sein, um eine möglichst zeitnahe Version der betreffenden Datei zu haben, um den Restaurierungsaufwand durch Nachbearbeitung gering zu halten.

**Vorgehensweise und Speichermedium**

Nach der Festlegung der Art der Datensicherung, der Häufigkeit und des Generationenprinzips gilt es nun, die Vorgehensweise einschließlich des erforderlichen und wirtschaftlich angemessenen Datenträgers auszuwählen. Zu-

nächst sollen einige gängige Datensicherungsverfahren beispielhaft aufgezeigt werden:

Beispiel 1: Manuelle dezentrale Datensicherung am PC
Bei nichtvernetzten PCs wird die Datensicherung vom IT-Anwender meist manuell als Vollsicherung der Anwendungsdaten durchgeführt. Als Speichermedium werden CDs oder DVDs verwendet.

Beispiel 2: Manuelle zentrale Datensicherung im Unix-System
Für Unix-Systeme mit angeschlossenen Terminals oder PCs mit Terminalemulation bietet sich aufgrund des zentralen Datenbestandes die zentrale Datensicherung an. Sie wird oft als Kombination von wöchentlichen Vollsicherungen und täglichen inkrementellen Datensicherungen mittels Streamer-Tapes vom Unix-Administrator manuell durchgeführt.

Beispiel 3: Manuelle zentrale Datensicherung im lokalen Netz
Im Bereich eines lokalen Netzes mit angeschlossenen PCs wird vielfach die Datensicherung dergestalt durchgeführt, dass der angeschlossene PC-Benutzer seine zu sichernden Anwendungsdaten auf einem zentralen Server im Netz ablegt und dass dann der Netzadministrator die Daten dieses Servers zentral sichert, wozu eine wöchentliche Vollsicherung und eine tägliche inkrementelle Sicherung durchgeführt werden.

Beispiel 4: Automatische zentrale Datensicherung im Großrechnerbereich
Vergleichbar dem Beispiel 2 werden im Großrechnerbereich zentrale Datensicherungen als Kombination von wöchentlichen Vollsicherungen und täglichen inkrementellen Datensicherungen durchgeführt. Vielfach wird dies automatisch mit Hilfe eines Tools (HSM) initiiert. Für einzelne IT-Anwendungen werden vielfach noch zusätzliche ereignisorientierte Volldatensicherungen vollzogen.

Beispiel 5: Automatische zentrale Datensicherung im verteilten System
Eine weitere Variante besteht aus der Kombination der Beispiele 3 und 4. Die lokalen Daten der verteilten Systeme werden auf einen zentralen Großrechner bzw. auf einen zentralen Server übertragen, auf dem die Datensicherung als Kombination von Vollsicherungen und inkrementellen Datensicherungen durchgeführt wird.

Beispiel 6: Voll-automatische zentrale Datensicherung dezentral gespeicherter Daten im verteilten System
Im Gegensatz zum vorangegangenen Beispiel erfolgt hier der Transfer vom dezentralen zum zentralen System automatisch. Mittlerweile werden Tools angeboten, die einen Zugriff von einem zentralen Datensicherungsserver auf die dezentralen Datenbestände erlauben. Eine Datensicherung kann somit transparent für den dezentralen Anwender zentral erfolgen.

Um das Datenvolumen auf dem Speichermedium zu minimieren, können zusätzlich Datenkompressionsalgorithmen angewandt werden. Teilweise kann das Datenvolumen damit um bis zu 80 % reduziert werden. Es ist bei Anwendung der Kompression sicherzustellen, dass die gewählten Parameter und Algorithmen im Rahmen der Datensicherung dokumentiert und für die Datenrestaurierung (Dekompression) vorgehalten werden.

Für die **Vorgehensweise** gibt es zwei Parameter, die festgelegt werden müssen: den *Automatisierungsgrad* und die *Zentralisierung* (Speicherort).

Beim Automatisierungsgrad ist zwischen manuell und automatisch zu unterscheiden:

- Manuelle Datensicherung bedeutet, dass der Anstoß zur Datensicherung manuell gegeben wird. Vorteilhaft kann sein, dass der Ausführende individuell den Termin der Datensicherung dem Arbeitsablauf anpassen kann. Nachteilig ist, dass die Wirksamkeit und Güte der Datensicherung dann von der Motivation und Disziplin des Ausführenden abhängt. Durch Krankheit oder sonstige Abwesenheitsgründe können Datensicherungen ausfallen.
- Automatische Datensicherungen werden programmgesteuert zu bestimmten Terminen angestoßen. Vorteilhaft ist, dass die Disziplin und Zuverlässigkeit der Ausführenden nachrangig ist, wenn der Terminplan vollständig und aktuell ist. Nachteilig kann sein, dass die Steuerungsprogramme Kosten verursachen, der Terminplan aktuellen Änderungen angepasst werden muss oder wichtige Änderungen nicht unmittelbar gesichert werden.

Bezüglich der Zentralisierung sind zentral und dezentral durchgeführte Datensicherungen zu unterscheiden:

- Zentrale Datensicherungen zeichnen sich dadurch aus, dass der Speicherort und die Durchführung der Datensicherung am zentralen IT-System von einem Ausführenden durchgeführt werden. Diese Verfahrensweise hat den Vorteil, dass nur ein Mitarbeiter intensiv geschult werden muss und die IT-Anwender des IT-Systems von dieser Arbeit entlastet werden. Vorteilhaft ist weiterhin, dass durch das höhere zentrale Datenaufkommen kostengünstigere Speichermedien verwendet werden können. Nachteilig ist, dass evtl. vertrauliche Daten übertragen und von nicht Befugten eingesehen werden könnten.
- Dezentrale Datensicherungen werden von den IT-Anwendern selbst durchgeführt, ohne dass die Daten auf ein zentrales IT-System übertragen werden müssen. Vorteilhaft ist, dass der IT-Anwender die Kontrolle über die Daten und die Backup-Datenträger behält, insbesondere wenn es sich um vertrauliche Daten handelt. Nachteilig ist, dass die konsequente Datensicherung damit von der Zuverlässigkeit der IT-Anwender abhängt und dass dezentrale Lösungen den IT-Anwendern Zeitaufwand abfordern.

Nach der Entscheidung, ob die Datensicherung manuell oder automatisch, zentral oder dezentral durchgeführt wird, muss nun der geeignete Datenträger für die Datensicherung gefunden werden. Dazu können folgende Parameter betrachtet werden:

- **Datenträger-Anforderungszeit:** der Zeitaufwand für die Vorbereitung der Daten-Restaurierung ist bestimmt durch die Zeit, die benötigt wird, den erforderlichen Datensicherungs-Datenträger zu identifizieren und im System verfügbar zu machen. Kassetten in einem Roboter-System können innerhalb von Minuten zur Restaurierung bereit stehen, ausgelagerte Bänder müssen unter Umständen erst aufwendig transportiert und aufgelegt werden.
- **Zugriffszeit, Transferrate:** der Zeitaufwand für die Erstellung und Restaurierung der Daten selbst hängt von der mittleren Zugriffszeit auf die Daten des Datenträgers und von der Datentransferrate ab. Festplatten erlauben einen Zugriff auf bestimmte Dateien im Millisekunden-Bereich, ein Magnetband muss erst zur entsprechenden Stelle gespult werden. Bei der Auswahl des Datenträgers ist zu berücksichtigen, dass bei entsprechend hohen Transferraten es nicht zu einer Überlastung der Übertragungskanäle kommen darf.
- **Praktikabilität/Speicherkapazität:** je umständlicher die Datensicherung ist, um so größer ist die Gefahr, dass sie fehlerhaft vollzogen oder von

den Verantwortlichen überhaupt nicht durchgeführt wird. Datenträger mit zu kleiner Speicherkapazität verhindern eine effektive Datensicherung, da der ständige Wechsel zeitaufwendig und fehleranfällig ist.
- **Kosten:** die Kosten für die Datensicherung, also Beschaffungskosten für Lese-/ Schreibgeräte und Datenträger, erforderliche Rechen- und Arbeitszeit müssen in einem angemessenen Verhältnis zum Sicherungszweck stehen. Hierbei ist auch die Lebensdauer der Datenträger und der Zuverlässigkeit zu berücksichtigen.

Auf keinen Fall dürfen die laufenden Datensicherungskosten die Summe der Restaurierungskosten ohne Datensicherung und der Folgeschäden übersteigen. Die folgenden Einflussgrößen müssen dabei beachtet werden:

*Verfügbarkeitsanforderungen*:

Je höher die Verfügbarkeitsanforderungen sind, desto schneller muss auf die Datenträger als Speichermedium der Datensicherung zugegriffen werden können und desto schneller müssen die benötigten Daten vom Datenträger wieder einspielbar sein.
Aus Verfügbarkeitsgründen muss sichergestellt sein, dass die Speichermedien auch bei Ausfall eines Lesegerätes zur Restaurierung genutzt werden können. Die Kompatibilität und Funktion eines Ersatzgerätes ist zu gewährleisten.

*Daten- und Änderungsvolumen*:

Mit zunehmenden Datenvolumen werden i. allg. preisgünstige Bandspeichermedien wie Magnetbänder oder Bandkassetten (Data Cartridge) benutzt.

*Fristen*:

Müssen Löschfristen eingehalten werden (z. B. bei personenbezogenen Daten), so muss das ausgewählte Speichermedium die Löschung ermöglichen. Speichermedien, die nicht oder nur mit großem Aufwand löschbar sind (z. B. WORM), sollten in diesem Fall vermieden werden.

*Vertraulichkeitsbedarf und Integritätsbedarf der Daten*:

Ist der Vertraulichkeits- oder Integritätsbedarf der zu sichernden Daten hoch, so überträgt sich dieser Schutzbedarf auch auf die zur Datensicherung eingesetzten Datenträger. Ist eine Verschlüsselung der Datensicherung nicht möglich, kann über die Auswahl von Datenträgern nachgedacht werden, die aufgrund ihrer kompakten Bauart und Transportabilität in Datensicherungsschränken oder Tresoren untergebracht werden können.

*Kenntnisse der IT-Benutzer*:
Die Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer entscheiden darüber, ob eine Verfahrensweise gewählt werden kann, in der der IT-Benutzer selbst manuell für die Datensicherung tätig wird, ob andere ausgebildete Personen die Datensicherung dezentral durchführen oder ob eine automatisierte Datensicherung praktikabler ist.

**Verantwortlichkeit für die Datensicherung**

Für die Entscheidung, wer für die Durchführung der Datensicherung verantwortlich ist, kommen drei Personengruppen in Frage. Zunächst kann es der IT-Benutzer selbst sein (typischerweise bei dezentralen und nichtvernetzen IT-Systemen), der Systemverwalter oder ein für die Datensicherung speziell ausgebildeter Administrator. Wird die Datensicherung nicht vom Benutzer selbst durchgeführt, sind die Verantwortlichen auf Verschwiegenheit bezüglich der

Dateninhalte zu verpflichten und ggf. eine Verschlüsselung in Betracht zu ziehen.

Darüber hinaus sind die Entscheidungsträger zu benennen, die eine Daten-Restaurierung veranlassen können. Zu klären ist weiterhin, wer berechtigt ist, auf Datensicherungsträger zuzugreifen, insbesondere wenn sie in Datensicherungsarchiven ausgelagert sind. Es muss sichergestellt sein, dass nur Berechtigte Zutritt erhalten. Abschließend ist zu definieren, wer berechtigt ist, eine Daten-Restaurierung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

Bei der Festlegung der Verantwortlichkeit ist insbesondere der Vertraulichkeits-, Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen Mitarbeiter zu betrachten. Es muss sichergestellt werden, dass der Verantwortliche erreichbar ist und ein Vertreter benannt und eingearbeitet wird.

Als Einflussfaktor ist zu beachten:

*Kenntnisse der IT-Anwender*:

Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer entscheiden darüber, ob die Datensicherung eigenverantwortlich je IT-Benutzer durchgeführt werden sollte. Sind die Kenntnisse der IT-Benutzer nicht ausreichend, ist die Verantwortung dem Systemadministrator oder einer speziell ausgebildeten Person zu übertragen.

**Aufbewahrungsort**

Grundsätzlich sollten Datensicherungsmedien und Originaldatenträger in unterschiedlichen Brandabschnitten aufbewahrt werden. Werden Datensicherungsmedien in einem anderen Gebäude oder außerhalb des Betriebsgeländes aufbewahrt, so sinkt die Wahrscheinlichkeit, dass in einem Katastrophenfall die Datensicherungen in Mitleidenschaft gezogen werden. Je weiter jedoch die Datenträger von der zur Restaurierung notwendigen IT-Peripherie (z. B. Bandstation) entfernt ist, desto länger können die Transportwege und Transportzeiten sein, und desto länger ist die Gesamtrestaurierungszeit. Als Einflussfaktor ist daher zu betrachten:

*Verfügbarkeitsanforderungen*:

Je höher die Verfügbarkeitsanforderungen sind, um so schneller müssen die Datenträger der Datensicherung verfügbar sein. Werden aus Sicherheitsgründen die Datenträger extern ausgelagert, so ist bei sehr hohen Verfügbarkeitsanforderungen zu erwägen, Kopien der Datensicherung zusätzlich in unmittelbarer Nähe des IT-Systems vorzuhalten.

*Vertraulichkeitsbedarf und Integritätsbedarf der Daten*:

Je höher dieser Bedarf ist, um so besser muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich i. allg. nur durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen, siehe Baustein B 2.5 *Datenträgerarchiv*.

*Datenvolumen:*

Mit steigendem Datenenvolumen gewinnt die Sicherheit des Aufbewahrungsortes an Bedeutung.

**Anforderungen an das Datensicherungsarchiv**

Aufgrund der Konzentration von Daten auf Datensicherungsmedien besitzen diese einen mindestens ebenso hohen Schutzbedarf bezüglich Vertraulichkeit und Integrität wie die gesicherten Daten selbst. Bei der Aufbewahrung in einem zentralen Datensicherungsarchiv sind daher entsprechend wirksame Sicherheitsmaßnahmen wie z. B. Zutrittskontrolle notwendig.

Zusätzlich muss durch organisatorische und personelle Maßnahmen (Datenträgerverwaltung) sichergestellt werden, dass der schnelle und gezielte Zugriff auf benötigte Datenträger möglich ist. Hierzu sind die Maßnahme M 2.3 *Datenträgerverwaltung* und Baustein B 2.5 *Datenträgerarchiv* zu beachten.

Folgende Einflussfaktoren müssen beachtet werden:

*Verfügbarkeitsanforderungen*:

Je höher die Verfügbarkeitsanforderungen sind, um so schneller muss der gezielte Zugriff auf benötigte Datenträger möglich sein. Wenn eine manuelle Bestandsführung den Verfügbarkeitsanforderungen nicht genügt, können automatisierte Zugriffsverfahren (z. B. Roboter-Kassettenarchiv) zum Einsatz kommen.

*Datenvolumen*:

Das Datenvolumen bestimmt letztendlich die Anzahl der aufzubewahrenden Datenträger. Für entsprechend große Datenvolumen ist eine ausreichende Aufbewahrungskapazität im Datenträgerarchiv vorzusehen.

*Fristen*:

Sind Löschungsfristen einzuhalten, muss die Organisation des Datensicherungsarchivs dem angepasst sein und ggf. müssen auch die erforderlichen Löscheinrichtungen vorhanden sein. Zu den vorgegebenen Löschungszeitpunkten ist im Datensicherungsarchiv die Löschung zu initiieren bzw. durchzuführen und zu dokumentieren. Ist eine Löschung technisch nicht möglich, so ist durch organisatorische Maßnahmen eine Wiederverwendung zu löschender Daten zu verhindern.

*Vertraulichkeits- und Integritätsbedarf der Daten*:

Je höher dieser Bedarf ist, um so besser muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich i. allg. nur durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen vergleichbar dem Baustein B 2.5 *Datenträgerarchiv*.

**Transportmodalitäten**

Bei der Durchführung einer Datensicherung werden Daten transportiert. Sei es, dass sie über ein Netz oder eine Leitung übertragen werden, sei es, dass Datenträger zum Datenträgerarchiv transportiert werden. Dabei gilt es folgendes zu beachten:

*Verfügbarkeitsanforderungen*:

Je höher die Verfügbarkeitsanforderungen sind, desto schneller müssen die Daten zur Restaurierung bereitstellbar sein. Dies ist bei der Auswahl des Da-

tenübertragungsmediums bzw. bei Auswahl des Datenträger-Transportweges zu berücksichtigen.

*Datenvolumen*:

Wenn zur Datenrestaurierung die Daten über ein Netz übertragen werden, so muss bei der Auswahl der Übertragungskapazität des Netzes das Datenvolumen beachtet werden. Es muss gewährleistet sein, dass das Datenvolumen innerhalb der erforderlichen Zeit (Verfügbarkeitsanforderung) übertragen werden kann.

*Änderungszeitpunkte der Daten:*

Werden Datensicherungen über ein Netz durchgeführt (insbesondere zu ausgewählten Terminen), kann aufgrund des zu übertragenen Datenvolumens ein Kapazitätsengpass entstehen. Daher ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen.

*Vertraulichkeits- und Integritätsbedarf der Daten*:

Je höher dieser Bedarf ist, um so besser muss verhindert werden, dass die Daten auf dem Transport abgehört, unbefugt kopiert oder manipuliert werden. Bei Datenübertragungen ist schließlich eine Verschlüsselung oder ein kryptographischer Manipulationsschutz zu überdenken, beim physikalischen Transport sind sichere Behältnisse und Wege zu benutzen und ggf. auch der Nutzen und Aufwand einer Verschlüsselung abzuwägen.

**Aufbewahrungsmodalität**

Im Rahmen des Datensicherungskonzeptes sollte mitbetrachtet werden, ob für bestimmte Daten Aufbewahrungs- oder Löschfristen einzuhalten sind.

*Fristen:*

Falls Aufbewahrungsfristen einzuhalten sind, kann dem durch die Archivierung einer Datensicherungsgeneration nachgekommen werden. Sind die Aufbewahrungsfristen lang, so ist zusätzlich sicherzustellen, dass die erforderlichen Lesegeräte bevorratet werden und dass unter Umständen ein Refresh (erneutes Aufspielen der magnetisch gespeicherten Daten) bei magnetischen Datenträgern erforderlich werden kann, da diese mit der Zeit ihre Magnetisierung und damit den Dateninhalt verlieren.
Falls Löschfristen einzuhalten sind, muss der organisatorische Ablauf festgelegt werden und ggf. müssen auch die erforderlichen Löscheinrichtungen vorhanden sein. Zu den vorgegebenen Löschungszeitpunkten ist die Löschung zu initiieren bzw. durchzuführen.

Prüffragen:

- Wurde für jedes IT-System und für jede Datenart die Verfahrensweise der Datensicherung festgelegt?
- Wurden Art, Häufigkeit und Zeitpunkte der Datensicherungen festgelegt?
- Wurden die Verantwortlichkeiten für die Datensicherungen festgelegt?
- Wurden die Transport- und - Aufbewahrungsmodalitäten für die Datensicherungen geklärt?

# M 6.36 Festlegung des Minimaldatensicherungskonzeptes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Für ein Unternehmen/eine Behörde ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde.

Ein Beispiel soll dies erläutern:

**Minimaldatensicherungskonzept**

**Software:**

Sämtliche Software, erworben oder selbst erstellt, ist einmalig mittels einer Vollsicherung zu sichern.

**Systemdaten:**

Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.

**Anwendungsdaten:**

Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

**Protokolldaten:**

Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

Prüffragen:

- Wurde festgelegt, welche Minimalforderungen zur Datensicherung eingehalten werden müssen?

# M 6.37 Dokumentation der Datensicherung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Verantwortliche für die Datensicherung

In einem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat. Für eine ordnungsgemäße und funktionierende Datensicherung ist eine Dokumentation erforderlich. So ist bei der Erstellung der Datensicherung für jedes IT-System zu dokumentieren:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes. Auch hier muss eine Beschreibung der erforderlichen Hard- und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

Prüffragen:

- Ist die Vorgehensweise für die Erstellung von Datensicherungen sowie für die Wiederherstellung eines Datensicherungsbestandes ausreichend dokumentiert?

# M 6.38 Sicherungskopie der übermittelten Daten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Benutzer

Sind die zu übertragenden Daten nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, sollte eine Sicherungskopie dieser Daten vorgehalten werden. Bei Verlust oder Beschädigung des Datenträgers kann der Versand mit geringfügigem Aufwand erneut erfolgen.

Prüffragen:

- Wird eine Sicherungskopie der zu übertragenden Daten vorgehalten, falls die Daten nur zu diesem Zweck zusammengestellt wurden und nicht auf einem weiteren Medium gespeichert sind?

# M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Beschaffer, Fax-Verantwortlicher

Es sollte in den Not- und Katastrophenplan eine Liste von Fachhändlern für Faxgeräte aufgenommen werden, bei denen im Notfall unverzüglich neue Geräte beschafft werden können, wenn eine Reparatur aus Zeitgründen nicht möglich ist.

Prüffragen:

- Ist im Notfallplan eine Liste von Fachhändlern für Faxgeräte enthalten, bei denen unverzüglich Ersatzgeräte beschafft werden können?

# M 6.40 Regelmäßige Batterieprüfung/-wechsel

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.41 Übungen zur Datenrekonstruktion

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Verantwortliche für die Datensicherung

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss sporadisch, zumindestens aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Hierbei muss zumindest einmal nachgewiesen werden, dass eine vollständige Datenrekonstruktion (z. B. der Gesamtdatenbestand eines Servers) möglich ist. Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht.

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten gegebenenfalls auf einem Ausweich-IT-System installiert werden müssen und
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

Prüffragen:

- Wird die Wiederherstellung von Datensicherungsbeständen sporadisch getestet?

# M 6.42 Erstellung von Rettungsdisketten für Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 6.43 Einsatz redundanter Windows-Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

In Abhängigkeit von den Verfügbarkeitsanforderungen der Daten und Anwendungen ist eine Redundanz zu schaffen, die einem Totalverlust der Daten mit akzeptablem Aufwand vorbeugt. Je nach diesen Anforderungen sind Teile des Datenbestandes oder auch der gesamte Datenbestand parallel auf mehreren Plattenspeichern zu führen, so dass auch bei Ausfall eines Plattenlaufwerks dessen Daten nicht verloren sind und die Benutzer weiterarbeiten können, ohne auf das Wiedereinspielen einer Datensicherung warten zu müssen.

Die Systeme können je nach den definierten Verfügbarkeitsanforderungen so ausgelegt werden, dass bei Ausfall eines Servers dessen Aufgaben von einem oder mehreren anderen Servern übernommen werden können. Dabei muss jedoch dafür gesorgt werden, dass diese verteilten Datenbestände konsistent bleiben, und dies muss auch bei Ausfall einzelner Geräte gewährleistet bleiben. In dieser Beziehung bestehen gravierende Unterschiede hinsichtlich der Leistungsfähigkeit verschiedener Redundanzkonzepte:

- Eine direkte physikalische Redundanz lässt sich mit RAID-Plattensystemen (RAID: Redundant Array of Independent Disks) erreichen. Zu beachten ist bei der Entscheidung für dieses Verfahren, dass der räumliche Abstand zwischen den einzelnen Platten eines RAID-Systems starken Einschränkungen unterworfen ist, so dass im Falle eines Brandes oder eines ähnlichen Schadens alle Parallelkopien gleichermaßen zerstört werden. RAID-Systeme sind daher kein Ersatz für Datensicherungen.
- Durch Einsatz von Windows 2000 Clustern können parallele Kopien des Datenbestandes verteilt auf verschiedene Platten und unter Kontrolle verschiedener Rechner geführt werden. Durch die Verwendung leistungsstarker Cluster mit bis zu vier Servern lässt sich die Zahl der Serversysteme reduzieren, was wiederum zu einer Reduktion des Administrationsaufwandes und damit zu einer Verbesserung der Sicherheit führt.
- Die Replikation einzelner Verzeichnisse erlaubt eine ähnlich weite Verteilung der Daten, doch stehen hier keine Synchronisationsmechanismen zur Verfügung, die es erlauben, auch die aktuell in Bearbeitung befindlichen Dateien konsistent parallel zu führen. Ein Ausfall des primären Plattenlaufwerks führt hier somit immer zu mehr oder weniger großen Datenverlusten. Der Einsatz der Replikatordienste unter Windows 2000 sollte daher auf die Fälle beschränkt bleiben, in denen nur an einer Stelle geändert wird, und er darf keinesfalls als Ersatz für die regelmäßige Durchführung von Datensicherungen angesehen werden.

Um einem Ausfall der Server vorzubeugen, sind diese bei Bedarf redundant auszulegen. Hier stehen mehrere Möglichkeiten zur Verfügung, unter denen, ausgehend von der tolerierbaren Ausfallzeit, eine geeignete Alternative auszuwählen ist:

- Wenn Ausfälle in der Größenordnung einer halben Stunde tolerierbar sind, ist ein separater Rechner zur Verfügung zu stellen, der bei Ausfall eines Servers dessen Aufgaben übernimmt. Um Zugriff auf die Daten des ausgefallenen Servers zu erhalten, müssen dessen Plattenlaufwerke auf den Ausweichrechner umgeschaltet werden.
- Wenn Ausfälle von maximal einigen Minuten tolerierbar sind, ist ein Cluster-System mit Zugriff aller Rechner auf alle Platten einzusetzen. Das Sy-

stem ist so zu konfigurieren, dass bei Ausfall eines Servers automatisch auf einen Ersatzrechner innerhalb des Systems umgeschaltet wird.
- Wenn äußerstenfalls Ausfälle im Sekundenbereich toleriert werden können, ist der Einsatz eines voll redundanten, ausfallsicheren Systems mit parallel arbeitenden mehrfachen CPUs erforderlich. In diesem Fall bleibt ein Ausfall einer CPU oder eines Hauptspeichermoduls für den Benutzer unbemerkbar. Diese Lösung bietet somit die größte Ausfallsicherheit, doch ist sie gleichzeitig auch erheblich aufwendiger und teurer als die beiden anderen Lösungen, so dass man nur bei extremen Anforderungen an die Verfügbarkeit auf sie zurückgreifen wird. Windows 2000 kann derzeit so hohe Anforderungen nicht erfüllen, so dass in diesem Fall Spezialsysteme einzusetzen sind, die unter anderen Betriebssystemen laufen.

Es muss in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind, und im Rahmen einer detaillierten Planung der System- und Netzarchitektur muss dann eine geeignete Kombination redundanter Rechner und/oder Plattenlaufwerke gefunden werden, die diesen Anforderungen genügt.

Prüffragen:

- Sind Redundanzen geschaffen, um einem Totalverlust der Daten mit einem akzeptablen Aufwand vorzubeugen?
- Ist bei verteilten Datenbeständen eine Konsistenz derselbigen sichergestellt?
- Ist auch bei Ausfall einzelner Geräte eine Konsistenz der Datenbestände gewährleistet?
- Sind die Verfügbarkeitsanforderungen der Datenbestände mit den Sicherheitsrichtlinien der Organisation abgestimmt?
- Existiert eine detaillierte Auflistung der System- und Netzarchitektur zur Darstellung der bestehenden Redundanzen?

# M 6.44 Datensicherung unter Windows NT

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 6.45 Datensicherung unter Windows 95

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 6.46 Erstellung von Rettungsdisketten für Windows 95

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 6.47 Datensicherung bei der Telearbeit

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Telearbeiter

Bei der Telearbeit können Daten auf verschiedenen IT-Systemen und an verschiedenen Orten verarbeitet werden, also beispielsweise auf Servern und Clients in der Institution, aber auch auf Clients am Telearbeitsplatz. Die Datensicherung aller relevanten Daten am Telearbeitsplatz muss sichergestellt sein. Das Datensicherungskonzept der Institution darf sich nicht nur auf die Server beschränken, sondern muss auch die Telearbeitsplätze miteinbeziehen. Generell bieten sich folgende Verfahren zur Datensicherung am Telearbeitsplatz an:

- **Datensicherung auf externen Datenträgern**
  Hierfür müssen die Telearbeitsplätze über die notwendige technische Ausstattung verfügen. Dazu gehören neben den erforderlichen externen Datenträgern die notwendige Hard- und Software des Rechners. Außerdem müssen die Telearbeiter geschult sein, um die Datensicherungen selbstständig anfertigen zu können.
- **Datensicherung über Netz**
  Die Sicherung der lokalen Daten kann auch über die Anbindung an das Netz der Institution erfolgen. Vorteilhaft ist hierbei, dass die Datensicherung nicht von den Telearbeitern selbstständig durchgeführt werden muss und diese auch keine Datenträger verwalten müssen.
  Entscheidend bei der Datensicherung über eine Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichend ist. Die Datenübertragung darf nicht zu lange dauern und bei gleichzeitigem Zugriff auf entfernte Ressourcen zu übermäßigen Verzögerungen führen. Bei gängigen Zugangstechnologien (z. B. ISDN, Modem) können daher nur geringe Datenmengen pro Sicherungsvorgang transportiert werden. Je nach Datensicherungsprogramm besteht die Möglichkeit, nur die Änderungen des Datenbestands seit der letzten Datensicherung zu übertragen (inkrementelle Datensicherung). In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.
  Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen (siehe auch M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*). Hierdurch erhöht sich jedoch unter Umständen der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst automatisiert ablaufen, so dass die Telearbeiter nur wenige Aktionen selbst durchführen müssen. Wenn die Mitarbeit der Benutzer erforderlich ist, sollten sie zur regelmäßigen Durchführung der Datensicherung verpflichtet werden (siehe M 2.41 *Verpflichtung der Mitarbeiter zur Datensicherung*). Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können (siehe M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*).

**Aufbewahrung der Backup-Datenträger**

Falls Datensicherungen im häuslichen Bereich durchgeführt werden, müssen Backup-Datenträger dort verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der Telearbeiter selber bzw. sein Vertreter darauf Zugriff hat.

Jeweils eine Generation der Backup-Datenträger sollte jedoch in der Institution aufbewahrt werden, damit im Katastrophenfall der Vertreter auf die Backup-Datenträger zugreifen kann.

Prüffragen:

- Werden alle Daten, die bei der Telearbeit bearbeitet werden, regelmäßig gesichert?
- Ist das gewählte Verfahren zur Datensicherung für das Volumen des Datenbestands geeignet und ausreichend?
- Sind bei der Datensicherung möglichst wenig Aktionen des Telearbeiters erforderlich?
- Ist eine Generation Backup-Datenträger in der Institution hinterlegt?

# M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Falls sich das Datenbanksystem in nicht vorgesehener Weise verhält (zum Beispiel undefiniertes Systemverhalten, nicht auffindbare Tabellen oder Datensätze, veränderte Tabelleninhalte, unerklärlich langes Antwortzeitverhalten oder ähnliches), kann ein Verlust der Datenbankintegrität vorliegen. Dieser kann auch durch missbräuchliche Nutzung des Systems verursacht worden sein, zum Beispiel durch Veränderungen der Systemeinstellungen.

Für solche Problemfälle sollte ein Konzept (Wiederherstellungskonzept) erstellt werden, das Prüfungen, Entscheidungen und Aktionen beschreibt, um die Datenbank auf schnellem und sicherem Wege wieder zur Verfügung stellen zu können (siehe M 6.51 *Wiederherstellung einer Datenbank*).

Ein weiterer wichtiger Aspekt ist die Benachrichtigung der Benutzer der Datenbank. Dies sollte unverzüglich nach Auftreten von Anzeichen für einen Integritätsverlust erfolgen, bevor die Arbeiten zur Wiederherstellung beginnen. Für diesen Fall und für die Situation, dass einem Benutzer Unregelmäßigkeiten bei der Nutzung der Datenbank auffallen, sollten den Benutzern Verhaltensregeln in Form eines Merkblattes an die Hand gegeben werden, das mindestens folgende Punkte enthalten sollte:

- Ruhe bewahren!
- Benachrichtigen Sie den Datenbankadministrator
- Greifen Sie nicht mehr auf die Datenbank zu
- Befolgen Sie die Anweisungen des Datenbankadministrators

Der Datenbankadministrator sollte genau nach dem Wiederherstellungskonzept vorgehen, das unter anderem folgende Schritte vorsehen sollte, die je nach Fehlerursache durchzuführen sind:

**Information**
- Umgehende Benachrichtigung aller betroffenen Benutzer mit der Bitte, keine weiteren Datenbankzugriffe durchzuführen und auf neue Anweisungen zu warten.
- Turnusmäßige Information der betroffenen Benutzer über den aktuellen Stand der Fehlerbehebung.

**Sicherung des aktuellen Zustands**
- Herunterfahren des Datenbanksystems.
- Hochfahren des Datenbanksystems im Exklusiv-Modus (falls dies vom Datenbanksystem unterstützt wird).
- Sichern aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sichern aller relevanten Protokolldateien.

**Analyse und Interpretation**
- Überprüfung und Interpretation der Protokolldateien nach Auffälligkeiten (in Zusammenarbeit mit dem Revisor und/oder dem IT-Sicherheitsbeauftragten).
- Überprüfung der Zugriffsrechte auf Systemtabellen.

- Überprüfung der Datenbank-Software auf sichtbare Veränderungen, z. B. Erstellungsdatum und Größe der entsprechenden Dateien. (Da diese von einem Angreifer auch wieder auf ihre Ursprungswerte zurückgesetzt werden können, sollte ein Prüfsummenverfahren eingesetzt werden.)

**Situationsabhängige Reaktion**

- Löschen der Datenbank-Software und Wiedereinspielen der Original-Dateien von schreibgeschützten Datenträgern (siehe M 6.21 *Sicherungskopie der eingesetzten Software*). Programme aus existierenden Datensicherungen sollten nur dann wiedereingespielt werden, wenn hinreichend sicher ist, dass die wiedereingespielte Software den Fehler nicht bereits enthält.
- Zurücksetzen der Passwörter.
- Zurücksetzen der Zugriffsrechte auf Systemtabellen.
- Benachrichtigung der Benutzer mit der Bitte, ihre Bereiche auf Unregelmäßigkeiten zu prüfen.

Nach dem Zurücksetzen der Passwörter auf ein Default-Passwort müssen die Benutzer unverzüglich aufgefordert werden, bei der nächsten Anmeldung neue Passwörter zu vergeben und hierbei die Vorgaben der Passwortrichtlinie zu beachten. Ist das Zurücksetzen auf ein Default-Passwort nicht möglich oder durch die Passwortrichtlinie untersagt, sollten die Passwörter zufällig erzeugt und den Benutzern auf zuverlässigem Weg mitgeteilt werden, z. B. in versiegelten Umschlägen. Diese Passwörter sollten direkt nach der Erstanmeldung geändert werden. Der Administrator sollte kontrollieren, dass die Default-Passwörter unmittelbar abgeändert wurden.

Falls Daten gelöscht oder unerwünscht geändert wurden, können diese aus den Datensicherungen wiedereingespielt werden (siehe M 6.51 *Wiederherstellung einer Datenbank*).

Wenn Anzeichen auf einen vorsätzlichen Angriff gegen eine Datenbank vorliegen, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Alarmplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen über den Vorfall zu unterrichten sind (siehe auchM 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*). Der Alarmplan enthält gegebenenfalls auch Informationen darüber, ob und wie der Datenschutzbeauftragte und die Rechtsabteilung zu beteiligen sind.

Prüffragen:

- Gibt es ein getestetes Wiederherstellungskonzept, das bei Verlust der Datenbankintegrität angewendet werden kann und Prüfungen, Entscheidungen und Aktionen beschreibt, um die Datenbank schnell und sicher wieder zur Verfügung stellen zu können?
- Gibt es Verhaltensregeln für die Benutzer bei ungewöhnlichem Systemverhalten der Datenbank?
- Gibt es ein erprobtes Verfahren zur schnellen und sicheren Vergabe von Passwörtern (nach Wiederherstellung der Datenbank)?
- Gibt es einen getesteten Alarmplan, nach dem bei einem vermuteten Angriff gegen die Datenbank Maßnahmen zur Schadensbegrenzung eingeleitet werden?

# M 6.49 Datensicherung einer Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Sicherung der Daten eines Datenbanksystems kann in aller Regel nicht mit den Datensicherungsprogrammen auf Betriebssystemebene vollständig abgedeckt werden. Letztere bilden in den meisten Fällen lediglich das Bindeglied, um die zu sichernden Daten auf ein Sicherungsmedium zu schreiben. Zur Sicherung des DBMS und der Daten müssen dagegen für die meisten Datenbankprodukte zusätzlich die jeweiligen Dienstprogramme des DBMS eingesetzt werden.

Die einfachste Möglichkeit einer Datenbanksicherung, die zugleich die sicherste darstellt, ist eine Komplettsicherung der Datenbank in heruntergefahrenem Zustand. Dabei werden alle zur Datenbank gehörenden Dateien auf dem Sicherungsmedium gesichert. Meist ist dieses Vorgehen allerdings aus Gründen der Verfügbarkeitsanforderungen an die Datenbank oder aufgrund des zu sichernden Datenvolumens nicht durchführbar.

Eine Alternative zur oben beschriebenen Komplettsicherung ist eine Online-Sicherung der Datenbank. Die Sicherung erfolgt dann während des laufenden Betriebs, d. h. die Datenbank muss nicht heruntergefahren werden. Die Nachteile dieser Sicherungsart sind, dass Inkonsistenzen nicht explizit ausgeschlossen werden können, und dass auch in diesem Fall bei einer Zerstörung der Datenbank eine (Offline-) Komplettsicherung existieren muss, auf der aufbauend die Online-Sicherungen zurückgespielt werden können. Online-Sicherungen sollten aus diesem Grund nur dann durchgeführt werden, wenn eine permanente Verfügbarkeit der Datenbank gefordert ist. Auf eine Offline-Komplettsicherung, die in vertretbar großen Zeitabständen durchgeführt werden kann, sollte trotzdem nicht verzichtet werden.

Partielle Datenbanksicherungen stellen eine weitere Möglichkeit dar. Sie sollten immer dann verwendet werden, wenn das zu sichernde Datenvolumen zu groß ist, um eine vollständige Sicherung durchführen zu können. Dies kann daraus resultieren, dass die Kapazitäten der Sicherungsmedien nicht ausreichen oder dass der zur Verfügung stehende Zeitrahmen je Sicherung nicht genügt, um eine vollständige Sicherung durchführen zu können.

Falls möglich, so sollten in jedem Fall alle Transaktionen zwischen zwei Offline-Komplettsicherungen archiviert werden. Oracle bietet dazu beispielsweise die Möglichkeit an, indem der sogenannte ARCHIVE-Mode für die Datenbank aktiviert wird. Transaktionen werden bei Oracle in sogenannten Log-Dateien protokolliert, von denen es mehrere gibt. Diese werden nacheinander beschrieben und sobald alle Log-Dateien voll sind, so wird wieder die erste Log-Datei überschrieben. Der ARCHIVE-Mode erstellt von diesen Log-Dateien eine Sicherungskopie, bevor sie wieder überschrieben werden. Auf diese Art und Weise können bei einer Zerstörung der Datenbank alle Transaktionen komplett rekonstruiert werden. Auch hierfür ist allerdings die Existenz einer Komplettsicherung der Datenbank die Voraussetzung. Die Dauer eines solchen Recovery wächst mit der Anzahl der zurückzuspielenden Archiv-Log-Dateien an.

Für die Datensicherung eines Datenbanksystems muss ein eigenes Datensicherungskonzept erstellt werden. Einflussfaktoren für ein solches Konzept sind:

- **Verfügbarkeitsanforderungen an die Datenbank**
  Wenn beispielsweise eine Datenbank werktags rund um die Uhr zur Verfügung stehen muss, so kann eine Komplettsicherung nur am Wochenende durchgeführt werden, da dies im allgemeinen ein Herunterfahren der Datenbank erfordert.
- **Datenvolumen**
  Das gesamte zu sichernde Datenvolumen muss mit den zur Verfügung stehenden Sicherungskapazitäten verglichen werden. Dabei muss festgestellt werden, ob die Sicherungskapazitäten (z. B. ein DAT-Tape pro Sicherungslauf) für das entsprechende Datenvolumen der Datenbank ausreichend dimensioniert sind.
  Falls dies nicht der Fall ist, muss ein Konzept zur Teilsicherung des Datenvolumens erstellt werden. Dies kann z. B. bedeuten, dass die Daten einzelner Anwendungen oder einzelner Bereiche der Datenbank immer im Wechsel gesichert werden bzw. nur die aktuellen Änderungen. Die Möglichkeiten einer Teilsicherung hängen von der verwendeten Datenbank-Software ab.
- **Maximal verkraftbarer Datenverlust**
  Hier muss festgelegt werden, ob bei einer Zerstörung der Datenbank der Datenverlust eines Tages verkraftbar ist, oder ob die Datenbank bis zur letzten Transaktion wiederherstellbar sein muss. Dies ist im allgemeinen bei einer hohen Anforderung an die Verfügbarkeit bzw. Integrität der Daten der Fall.
- **Wiederanlaufzeit**
  Auch die maximal zulässige Zeitdauer des Wiederherstellens der Datenbank nach einem Absturz muss festgelegt werden, um den Verfügbarkeitsanforderungen zu genügen.
- **Datensicherungsmöglichkeiten der Datenbank-Software**
  Im allgemeinen werden von einer Datenbank-Standardsoftware nicht alle denkbaren Datensicherungsmöglichkeiten unterstützt, wie z. B. eine partielle Datenbanksicherung. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann.

Anhand dieser Informationen kann ein Konzept für die Datensicherung der Datenbank erstellt werden. In diesem Sicherungskonzept wird unter anderem festgelegt (siehe hierzu auch Baustein B 1.4 *Datensicherungskonzept*)

- wer für die ordnungsgemäße Durchführung von Datensicherungen zuständig ist,
- in welchen Zeitabständen eine Datenbanksicherung durchgeführt wird,
- in welcher Art und Weise die Datenbanksicherung zu erfolgen hat,
- zu welchem Zeitpunkt die Datenbanksicherung durchgeführt wird,
- die Spezifikation des zu sichernden Datenvolumens je Sicherung.
- wie die Erstellung von Datensicherungen zu dokumentieren ist, und
- wo die Datensicherungsmedien aufbewahrt werden.

**Beispiel:**

Sicherung von Montag bis Samstag:

- Startzeit: morgens um 3.00h
- Es erfolgt eine vollständige Sicherung der Daten, wobei die Datenbank nicht heruntergefahren, sondern die Möglichkeit der Online-Sicherung des DBMS genutzt wird.

Sicherung am Sonntag

- Startzeit: morgens um 3.00h
- Die Datenbank wird heruntergefahren und es erfolgt eine Komplettsicherung der Datenbank.

Prüffragen:

- Gibt es ein Datensicherungskonzept für das Datenbanksystem, das die besonderen Aspekte der Datenbanksicherung berücksichtigt?

# M 6.50 Archivierung von Datenbeständen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ist eine Archivierung von Daten eines Datenbanksystems erforderlich, so muss dazu ein entsprechendes Konzept erstellt werden, durch das sichergestellt wird, dass die Datenbestände zu einem späteren Zeitpunkt wieder vollständig und konsistent zur Verfügung gestellt werden zu können. Hierbei sind folgende Punkte zu berücksichtigen:

**Archivierung**

- Die zur Verfügung stehenden Archivierungsmöglichkeiten müssen identifiziert werden.
- Es muss dokumentiert werden, welches Datenmodell den zu archivierenden Daten zugrunde liegt.
- Der Zeitpunkt der Archivierung ist zu dokumentieren.
- Die Version des Datenbankmanagementsystems und der benutzten Dienstprogramme sind zu dokumentieren.
- Aufbau, Systematik und Ordnungskriterien des Archivs müssen spezifiziert werden.
- Für alle Archivierungsmedien ist anhand von Herstellerangaben und Erfahrungswerten eine maximale physikalische Lebensdauer zu bestimmen. Entsprechend müssen Zeitpunkte für die Auffrischung des archivierten Datenbestandes festgelegt werden.
- Die geforderte Verfügbarkeit der archivierten Datenbestände ist regelmäßig zu überprüfen und gegebenenfalls an die konkreten Anforderungen anzupassen. Notwendige Anpassungen haben unter anderem Auswirkungen auf die Wahl des Archivierungsmediums sowie auf die Art und Weise der Archivierung. Bei hohen Verfügbarkeitsanforderungen müssen eventuell mehrere historische Versionen der gleichen Datenbanken parallel zugreifbar gehalten werden.
- Es muss sichergestellt sein, dass vorgegebene Aufbewahrungsfristen eingehalten werden.

**Wiedereinspielen**

- Der aktuelle Datenbestand darf von dem archivierten Datenbestand nicht beeinflusst werden.
- Für die Wiedereinspielung von archivierten Datenbeständen muss genügend Speicherplatz zur Verfügung gestellt werden.
- Der archivierte Datenbestand muss wiederherstellbar sein, auch wenn sich zwischenzeitlich das Datenmodell oder die Datenbankversion geändert hat. In diesem Fall müssen das Datenmodell und die entsprechenden Dienstprogramme zum Archivierungszeitpunkt bekannt sein, um den alten Stand wiederherstellen zu können.
- Wenn die wiedereingespielten Daten von einer Anwendung verarbeitet werden sollen, muss auch von dieser Anwendung eine Version vorhanden sein, die das "alte" Datenmodell unterstützt.
- Es muss regelmäßig überprüft werden, ob sich der archivierte Datenbestand wiedereinspielen lässt.

Bei der Archivierung von Datenbeständen, die personenbezogene Daten enthalten, müssen darüber hinaus die Vorschriften der Datenschutzgesetze und die daraus folgenden Regelungen berücksichtigt werden. Dies bedeutet beispielsweise, dass die Betroffenen ein Recht auf Berichtigung, Sperrung bzw.

Löschung der über sie gespeicherten Daten haben. Unter Umständen müssen Daten nach einer gewissen Zeit vollständig, d. h. auch auf den existierenden Sicherungen und Archiven, gelöscht werden. Um dies zu gewährleisten, sind entsprechende technisch-organisatorische Verfahren zu entwickeln. Insbesondere müssen auch nach dem Wiedereinspielen alter Datenbestände alle Korrekturen, Änderungen, Sperrungen bzw. Löschungen erhalten bleiben, die zwischen dem Datum der Sicherung des wiedereingespielten Datenbestands und dem Wiedereinspielen erfolgt sind.

Prüffragen:

- Falls die Archivierung von Daten eines Datenbanksystems erforderlich ist: Existiert ein Konzept für die Archivierung von Daten des Datenbanksystems?
- Gibt es ein getestetes Konzept für das Wiedereinspielen von archivierten Datenbeständen?
- Wurden gesetzliche Vorgaben zur Archivierung berücksichtigt (z. B. Aufbewahrungsfristen, Archivierung von personenbezogenen Daten)?
- Wird das Archivierungskonzept regelmäßig überprüft und gegebenenfalls angepasst?

# M 6.51 Wiederherstellung einer Datenbank

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Für die Wiederherstellung von Datenbanken ist ein Konzept zu erstellen, das die Abläufe des Wiedereinspielens von Datenbanksicherungen regelt. Grundlagen dieses Konzepts sind:

- das Datensicherungskonzept (siehe M 6.49 *Datensicherung einer Datenbank*) und
- die möglichen Fehlersituationen, die ein Wiedereinspielen von Datenbanksicherungen erforderlich machen können (siehe unter anderem auch M 6.48 *Verhaltensregeln nach Verlust der Datenbankintegrität*).

Anhand dieser Punkte ist abzuleiten, welche Datenbanksicherungen in welcher Form wiedereingespielt werden müssen.

Die Wiederherstellung einer Datenbank kann eine komplexe Aufgabe sein, die ein äußerst sorgfältiges Vorgehen erfordert und deren Schritte durch regelmäßige Testläufe geprobt werden sollten. Trotzdem kann es passieren, dass eine Wiederherstellung nicht reibungslos und fehlerfrei funktioniert.

Bei der Wiederherstellung sind zwei Aspekte aufeinander abzustimmen. Einerseits sollte die betroffene Datenbank so schnell wie möglich den Benutzern wieder zur Verfügung stehen, auf der anderen Seite sollte ein möglichst aktueller Stand der Datenbank hergestellt sowie die Schadensursache analysiert werden. Sollte der Ausfall der Datenbank nicht eindeutig auf einen Hardware-Schaden zurückzuführen sein, ist der Umfang der Inkonsistenz oft nur schwer festzustellen. Auch kann die Datenbank nicht immer ohne Probleme bis zur letzten Transaktion vor Entdeckung des Fehlers wiederhergestellt werden.

In solchen Fällen ist zu entscheiden, ob ein begrenzter Aktualitätsverlust oder eher eine längere Betriebsunterbrechung zu vertreten ist. Dies hängt wesentlich vom Einsatzgebiet der Datenbank, von der Art des Fehlers und von der Zeit zwischen dem ersten Auftreten des Fehlers und seiner Entdeckung bzw. der ersten Reaktion darauf ab. Insbesondere bei Schäden durch falsche Administration oder unzulässige Manipulation ist das genaue Ausmaß des Schadens oft schwer festzustellen.

Hierzu sollten Entscheidungsrichtlinien sowie entsprechende Handlungsanweisungen Bestandteil des Wiederherstellungskonzepts sein. Um die Datenbank so schnell wie möglich wieder zur Verfügung zu stellen, sollte die betroffene Datenbank in einem getrennten System oder Speicherbereich wiederhergestellt und für den Benutzer freigegeben werden. Wenn Zugriffsfunktionalitäten von den Daten getrennt sind (siehe M 2.134 *Richtlinien für Datenbank-Anfragen*) kann dies meist für die Benutzer transparent durchgeführt werden.

Auf keinen Fall sollte die zerstörte Datenbank ohne weitere Prüfung (siehe M 6.48 *Verhaltensregeln nach Verlust der Datenbankintegrität*) durch ein einfaches Zurückspielen der Datenbanksicherung überschrieben werden. Häufig lässt sich die für inkonsistent gehaltene Datenbank wieder bereinigen, ohne dass eine vollständige Restaurierung der Datenbank notwendig ist, sondern indem lediglich einzelne Datenbestände wiedergestellt werden. Auch im Fall einer partiellen Wiederherstellung ist abzuwägen, ob zuerst die Datenbank an anderer Stelle auf einem Test-System wiederhergestellt wird und nach der Si-

cherstellung der ordnungsgemäßen Wiederherstellbarkeit die Originaldatenbank bereinigt wird.

Auch wenn sich die beschädigte Datenbank nicht mehr reparieren lässt, sollte sie dennoch zur Analyse und Feststellung der Fehlerursache erhalten bleiben.

Im Wiederherstellungskonzept sollte festgelegt sein, welche Ressourcen in welchem Umfang für den Notfall bereitgehalten werden müssen. Eckpunkte, die hierbei beachtet werden müssen, sind insbesondere Speicherkapazitäten und Festplattenbereiche. Diese Größen sind regelmäßig anhand der aktuellen Datenbankgrößen zu überprüfen, um sicherzustellen, dass im Notfall die Auswirkungen auf andere Datenbanken minimiert werden können.

Prüffragen:

- Gibt es ein Wiederherstellungskonzept für die Datenbank, das die Abläufe des Wiedereinspielens von Datenbanksicherungen regelt?
- Wird die Wiederherstellung der Datenbank in regelmäßigen Testläufen geprobt?
- Enthält das Wiederherstellungskonzept für die Datenbank Entscheidungskriterien für den Umfang des Aktualitätsverlustes der Daten und die Dauer der Betriebsunterbrechung?
- Wird regelmäßig geprüft, ob genügend Speicherkapazitäten für eine Wiederherstellung der Datenbank verfügbar sind?

# M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

An die Verfügbarkeit der zentralen aktiven Netzkomponenten müssen hohe Anforderungen gestellt werden, da in der Regel viele Benutzer davon abhängig sind, dass ein lokales Netz reibungslos funktioniert. Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, müssen alle Konfigurationsdaten der aktiven Netzkomponenten in elektronischer Form gesichert werden (siehe auch M 6.32 *Regelmäßige Datensicherung* und M 6.91 *Datensicherung und Recovery bei Routern und Switches*). Diese Sicherung kann prinzipiell lokal an den einzelnen Komponenten oder vorzugsweise über das Netz, z. B. mit Hilfe eines Netzmanagement-Tools erfolgen. Wurden die Daten elektronisch gesichert, kann in diesem Fall das Wiederherstellen einer Konfiguration schneller und sicherer durchgeführt werden und eine zeitaufwendige manuelle Eingabe entfallen. Das Wiedereinspielen der Daten kann hierbei automatisch, z. B. durch ein zentrales Netzmanagement-Tool oder manuell durch den Eingriff eines Administrators erfolgen.

Bei einer Sicherung der Konfigurationsdaten über das Netz ist jedoch, im Gegensatz zu einer lokalen Sicherung, zu beachten, dass die übertragenen Daten eventuell mitgelesen werden und potentielle Angreifer möglicherweise sicherheitskritische Informationen über die Konfiguration der aktiven Netzkomponenten, wie z. B. Passwörter, und damit möglicherweise über die gesamte Netzkonfiguration erhalten können. Bei der Sicherung von Konfigurationsdateien über das Netz werden im Allgemeinen die Protokolle Trivial File Transfer Protocol (TFTP), FTP (File Transfer Protocol) oder Remote Copy Protocol (RCP) eingesetzt, wobei nach Möglichkeit RCP mit Authentisierung verwendet werden sollte (siehe M 5.20 *Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp*). TFTP bietet dagegen keine Schutzmechanismen vor einem unbefugten Zugriff auf die Konfigurationsdaten (siehe auch M 5.21 *Sicherer Einsatz von telnet, ftp, tftp und rexec*), so dass von dessen Einsatz grundsätzlich abgeraten wird. Falls zur Sicherung der Konfigurationsdateien ein TFTP-Server doch eingesetzt wird, so darf dieser nur im Administrationsnetz erreichbar sein.

Bei allen Sicherungsmethoden muss ein Test durchgeführt werden, ob die Sicherung ordnungsgemäß durchgeführt wurde und die Wiederherstellung der Konfigurationsdaten möglich ist. Dies gilt insbesondere bei der Sicherung über das Netz, da hier nach einem Fehlerfall das Netz u. U. in einem Zustand ist, der keine Wiederherstellung über das Netz ermöglicht.

Prüffragen:

- Erfolgt eine regelmäßige Datensicherung der Konfigurationsdaten der aktiven Netzkomponenten?
- Werden unsichere Protokolle (z. B. fehlende Verschlüsselung bei TFTP, FTP) zur Datensicherung vermieden?
- Wird die Wiederherstellbarkeit der Konfigurationsdaten aktiver Netzkomponenten aus der Sicherung geprüft?

# M 6.53 Redundante Auslegung der Netzkomponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Beschaffungsstelle

An die Verfügbarkeit der zentralen Netzkomponenten müssen hohe Anforderungen gestellt werden, da in der Regel viele Benutzer davon anhängig sind, dass ein lokales Netz reibungslos funktioniert. Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, ist in Abhängigkeit von den entsprechenden Verfügbarkeitsanforderungen im jeweiligen Bereich Redundanz zu schaffen, die einem Teil- oder Totalausfall der relevanten Netzkomponenten mit akzeptablem Aufwand vorbeugt.

Dabei gibt es zwei verschiedene Möglichkeiten, Redundanz zu erreichen:

- Die Netzkomponenten können redundant im Lager vorgehalten werden, um in einem Notfall kurzfristig einen Austausch durchführen zu können. Wird dies nicht beachtet, sind oft langwierige Beschaffungsvorgänge nötig, bevor die Störung behoben werden kann. Alternativ sind Wartungs- bzw. Lieferverträge mit den entsprechenden Herstellern abzuschließen, die einen schnellen Ersatz defekter Komponenten garantieren. Danach können die gesicherten Konfigurationsdaten wieder eingespielt werden, um die Ausfallzeit der betroffenen Netzsegmente so gering wie möglich zu halten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*).
- Es ist weiterhin sinnvoll, bereits bei der Konzeption eines Netzes eine redundante Auslegung der Netzkomponenten einzuplanen. So sollten alle zentralen Switches und je nach den verwendeten Protokollen alle Router zumindest doppelt in das Netz eingebunden sein, um die Anbindung der Server und die Verbindung zwischen den einzelnen Netzkomponenten redundant zu halten. Die korrekte Funktionsweise ist durch eine geeignete logische Netzkonfiguration zu gewährleisten.Abbildung 1: Redundante Verbindungen der Netzkomponenten

Ist je nach Verfügbarkeitsanforderungen auch eine Redundanz im Endgeräte-Bereich nötig, so müssen zusätzlich alle Endgeräte mit zwei Netzadaptern ausgerüstet werden.

Dabei gilt es im konkreten Fall zu prüfen, ob diese Technik von den eingesetzten aktiven Netzkomponenten und Betriebssystemen unterstützt wird.

Weiterhin stellt das Netzteil von aktiven Netzkomponenten eine häufige Störungsursache dar, da diese auf eine stabile Stromversorgung angewiesen sind. Viele Komponenten lassen sich deshalb mit redundanten Netzteilen ausrüsten oder sind hiermit bereits ausgestattet. So lässt sich die Ausfallsicherheit einzelner Netzkomponenten erhöhen, ohne dass zwei Netzkomponenten eingesetzt werden müssen. Durch solch eine Maßnahme wird aber nicht die Ausfallsicherheit der eigentlichen Funktionalität der Netzkomponenten erhöht.

Es muss in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind. Im Rahmen einer detaillierten Planung der System- und Netzarchitektur muss dann ein geeignetes Redundanzkonzept entwickelt werden, welches diesen Anforderungen genügt. In diesem Zusammenhang ist auch die Maßnahme M 6.18 *Redundante Leitungsführung* zu beachten.

Prüffragen:

- Wurden die Verfügbarkeitsanforderungen der zentralen Netzkomponenten ermittelt?
- Werden alle wichtigen Netzkomponenten für Notfälle im Lager vorgehalten beziehungsweise existieren dazu Lieferverträge?

# M 6.54 Verhaltensregeln nach Verlust der Netzintegrität

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Falls sich das Netz in nicht vorgesehener Weise verhält (z. B. Server sind nicht verfügbar, Zugriff auf Netzressourcen ist nicht möglich, Netzperformance bricht dauerhaft ein), kann ein Verlust der Netzintegrität vorliegen. Dieser kann durch missbräuchliche Nutzung des Netzes verursacht worden sein, z. B. durch Veränderungen der Konfigurationen der aktiven Netzkomponenten oder deren Beschädigung.

Dann sollten die Benutzer folgende Punkte beachten:

- Sicherung der Arbeitsergebnisse und ggf. Beendigung aktiver Programme.
- Der Administrator muss über eine geeignete Eskalationsstufe (z. B. User Help Desk) von den Benutzern benachrichtigt werden. Dabei ist sicherzustellen, dass der Administrator durch den Benachrichtigungsprozess in seiner Arbeit nicht wesentlich behindert wird.

Der Netzadministrator sollte folgende Schritte durchführen:

- Eingrenzen des fehlerhaften Verhaltens auf ein Netzsegment bzw. eine Netzkomponente,
- Überprüfen der Konfigurationen der dort vorhandenen aktiven Netzkomponenten (darunter fällt auch die Kontrolle der Passwörter),
- Sichern aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sichern aller relevanten Protokolldateien,
- ggf. Wiedereinspielen der Original-Konfigurationsdaten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*),
- ggf. Überprüfung der eingesetzten Hardware (Verkabelung, Steckverbindungen, aktive Netzkomponenten usw.) auf Defekte und
- Benachrichtigung der Benutzer mit der Bitte, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Wenn Anzeichen auf einen vorsätzlichen Angriff gegen das Netz vorliegen, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Alarmplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen über den Vorfall zu unterrichten sind (siehe auch M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*). Der Alarmplan enthält ggf. auch Informationen darüber, ob und wie der Datenschutzbeauftragte und die Rechtsabteilung zu beteiligen sind.

Prüffragen:

- Ist die Benachrichtung von bestimmten Instanzen (z. B. Administrator, Sicherheitsbeauftragter) gemäß eines festgelegten Eskalationsprozesses/ Alarmplans bei Verlust der Netzintegrität sichergestellt?
- Ist das Vorgehen zur Feststellung der Ursachen sowie zur Schadensminimierung und weiteren Schadensabwehr bei Verlust der Netzintegrität festgelegt?

# M 6.55 Reduzierung der Wiederanlaufzeit für Novell Netware Server

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Beim Einsatz kryptographischer Verfahren darf die Frage der Datensicherung nicht vernachlässigt werden. Neben der Frage, wie sinnvollerweise eine Datensicherung der verschlüsselten Daten erfolgen sollte, muss auch überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen. Daneben ist es noch zweckmäßig, die Konfigurationsdaten der eingesetzten Kryptoprodukte zu sichern.

**Datensicherung der Schlüssel**

Es muss sehr genau überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen, da jede Schlüsselkopie eine potentielle Schwachstelle ist.

Trotzdem kann es aus verschiedenen Gründen notwendig sein, kryptographische Schlüssel zu speichern. Es gibt unterschiedliche Methoden der Schlüsselspeicherung:

- die Speicherung zu Transportzwecken auf einem transportablen Datenträger, z. B. Diskette, Chipkarte (dient vor allem zur Schlüsselverteilung bzw. zum Schlüsselaustausch, siehe M 2.46 *Geeignetes Schlüsselmanagement*),
- die Speicherung in IT-Komponenten, die dauerhaft auf kryptographische Schlüssel zugreifen müssen, also z. B. zur Kommunikationsverschlüsselung und
- die Schlüsselhinterlegung als Vorbeugung gegen Schlüsselverlust oder im Rahmen von Vertretungsregelungen.

Hierbei ist grundsätzlich zu beachten:

- Kryptographische Schlüssel sollten so gespeichert bzw. aufbewahrt werden, dass Unbefugte sie nicht unbemerkt auslesen können. Beispielsweise könnten Schlüssel in spezieller Sicherheitshardware gespeichert werden, die die Schlüssel bei Angriffen automatisch löscht. Falls sie in Software gespeichert werden, sollten sie auf jeden Fall überschlüsselt werden. Hierbei ist zu bedenken, dass die meisten Standard-Anwendungen, bei denen Schlüssel oder Passwörter in der Anwendung gespeichert werden, dies im allgemeinen mit leicht zu brechenden Verfahren geschieht. Als weitere Variante kann auch das Vier-Augen-Prinzip bei der Schlüsselspeicherung benutzt werden, also die Speicherung eines Schlüssels in Schlüsselhälften oder Schlüsselteilen.
- Von Kommunikationsschlüsseln und anderen kurzlebigen Schlüsseln sollten keine Kopien erstellt werden. Damit eine unautorisierte Nutzung ausgeschlossen ist, sollten auch von privaten Signaturschlüsseln i. allg. keine Kopien existieren. Falls jedoch für die Schlüsselspeicherung eine reine Softwarelösung gewählt wurde, d. h. wenn keine Chipkarte o. Ä. verwendet wird, ist das Risiko des Schlüsselverlustes erhöht, z. B. durch Bitfehler oder Festplattendefekt. In diesem Fall ist es unter Umständen weniger aufwendig, eine ausreichend gesicherte Möglichkeit der Schlüsselhinterlegung zu schaffen, als bei jedem Schlüsselverlust alle Kommunikationspartner zu informieren.

- Von langlebigen Schlüsseln, die z. B. zur Archivierung von Daten oder zur Generierung von Kommunikationsschlüsseln eingesetzt werden, sollten auf jeden Fall Sicherungskopien angefertigt werden.

**Datensicherung der verschlüsselten Daten**

Besondere Sorgfalt ist bei der Datensicherung von verschlüsselten Daten bzw. beim Einsatz von Verschlüsselung während der Datenspeicherung notwendig. Treten hierbei Fehler auf, sind nicht nur einige Datensätze, sondern meist alle Daten unbrauchbar.

Die Langzeitspeicherung von verschlüsselten oder signierten Daten bringt viele zusätzliche Probleme mit sich. Hierbei muss nicht nur sichergestellt werden, dass die Datenträger regelmäßig aufgefrischt werden und jederzeit noch die technischen Komponenten zum Verarbeiten dieser zur Verfügung stehen, sondern dass die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik entsprechen. Bei der langfristigen Archivierung von Daten kann es daher sinnvoller sein, diese unverschlüsselt zu speichern und dafür entsprechend sicher zu lagern, also z. B. in Tresoren.

Die verwendeten Kryptomodule sollten vorsichtshalber immer archiviert werden, da die Erfahrung zeigt, dass auch noch nach Jahren Daten auftauchen, die nicht im Archiv gelagert waren.

**Datensicherung der Konfigurationsdaten der eingesetzten Produkte**

Bei komplexeren Kryptoprodukten sollte nicht vergessen werden, deren Konfigurationsdaten zu sichern (siehe auch M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Die gewählte Konfiguration sollte dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.

Prüffragen:

- Sind kryptographische Schlüssel auch bei Datensicherungen vor unbefugtem Auslesen geschützt?
- Werden langlebige kryptographische Schlüssel sicher hinterlegt?
- Wird bei Langzeitspeicherung verschlüsselter Daten regelmäßig geprüft, ob die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik entsprechen?
- Ist sichergestellt, dass auf verschlüsselt gespeicherte Daten auch nach längeren Zeiträumen noch zugegriffen werden kann?
- Werden verwendete Kryptoprodukte archiviert?
- Werden die Konfigurationsdaten von Kryptoprodukten gesichert?

# M 6.57 Erstellen eines Notfallplans für den Ausfall des Managementsystems

**Verantwortlich für Initiierung:** Informationssicherheitsmanagement, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auch ein Managementsystem kann aus verschiedenen Gründen ausfallen, etwa durch einen Rechnerabsturz durch Software- oder Hardwarefehler, durch einen Stromausfall oder Sabotage. Da Managementsysteme vor allem bei größeren Systemen eingesetzt werden, sollten für diese Systeme sowohl ein Notfallvorsorge-Konzept wie in Baustein B 1.3 *Notfallmanagement* beschrieben als auch ein Datensicherungskonzept (siehe Baustein B 1.4 *Datensicherungskonzept*) vorhanden sein.

Im Rahmen eines solchen Notfallvorsorgekonzeptes müssen dann auch für den Ausfall des Managementsystems Regelungen festgelegt und dokumentiert werden. Insbesondere sind Regelungen zu treffen, die Verhaltensrichtlinien für den Ausfall der verschiedenen Managementsystemkomponenten (Manager, Management Server, Managementkonsole) enthalten.

Desweiteren ist die Erstellung eines Wiederanlaufplanes für das Managementsystem insgesamt oder dessen Einzelkomponenten zwingend erforderlich. Im Idealfall sollte ein automatisches Wiederanlaufen des Managementsystems erfolgen. Im Rahmen der Datensicherung sollten für den Fall des Datentotalverlustes (Plattencrash) Sicherungskopien der Managementsystemsoftware vorhanden sein. Der Aufbewahrungsort ist im Notfallhandbuch zu vermerken. Ebenso sind dort die Kenntnisse zu vermerken, die benötigt werden, um Zutritt oder Zugriff zum Aufbewahrungsort zu erhalten, z. B. Namen und Telefonnummern der Mitarbeiter, die erforderliche Tresorkombinationen oder Passwörter kennen (siehe auch M 2.22 *Hinterlegen des Passwortes*).

Prüffragen:

- Sind im Rahmen eines Notfallvorsorgekonzeptes Regelungen für den Ausfall des Managementsystems festgelegt?
- Existiert ein Wiederanlaufplan für das Managementsystem und dessen Einzelkomponenten?

# M 6.58 Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Mit der zunehmenden Einbindung der Informationstechnik in alle Abläufe einer Behörde oder eines Unternehmens nimmt auch die Abhängigkeit von deren korrekten Funktionieren immer weiter zu. Eine wichtige Aufgabe des Sicherheitsmanagements ist daher die Vorbereitung auf den angemessenen Umgang mit Sicherheitsvorfällen aller Art. Sicherheitsvorfälle können durch eine Vielzahl von Ereignissen ausgelöst werden und z. B. zum Verlust der Verfügbarkeit, Integrität und/oder Vertraulichkeit von Daten, einzelnen IT-Systemen oder des gesamten Netzes führen.

Sicherheitsvorfälle, die im Rahmen des Sicherheitsmanagements einer besonderen Behandlung bedürfen, sind solche, die das Potential für große Schäden besitzen. Sicherheitsprobleme, die nur lokal begrenzte und geringfügige Schäden verursachen oder verursachen können, sollten auch in der lokalen Verantwortlichkeit gelöst werden, um das Sicherheitsmanagement nicht zu überlasten.

Die Behandlung von Sicherheitsvorfällen verfolgt als Teil des Informationssicherheitsmanagements dabei folgende Ziele:

- Reaktionsfähigkeit, damit Sicherheitsvorfälle und Sicherheitsprobleme rechtzeitig bemerkt und an eine zuständige Stelle gemeldet werden,
- Entscheidungsfähigkeit, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall handelt,
- Handlungsfähigkeit, damit bei einem Sicherheitsvorfall die notwendigen Maßnahmen kurzfristig ergriffen und umgesetzt werden,
- Schadensminimierung, in dem weitere potentiell betroffene Bereiche rechtzeitig benachrichtigt werden und
- Effektivität, in dem die Fähigkeit zur Behandlung von Sicherheitsvorfällen geübt und überwacht wird.

Um diese Ziele erreichen zu können, ist eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen zu etablieren, also sinnvolle und erprobte Prozesse zum Umgang mit Sicherheitsvorfällen aufzubauen. Abläufe und Regeln für die verschiedenen Arten von Sicherheitsvorfällen sollten klar definiert sein. Zwingende Voraussetzung dafür ist, dass die Behörden- oder Unternehmensleitung beteiligt wird und letztlich die Verfahren zur Behandlung von Sicherheitsvorfällen in Kraft setzt, um die notwendige Sensibilisierung für Informationssicherheit, die Vergabe von Entscheidungskompetenzen und die Unterstützung der Sicherheitsziele zu gewährleisten.

Als Teil des Sicherheitsmanagements sollte die Behandlung von Sicherheitsvorfällen in der Sicherheitsleitlinie bzw. im Sicherheitskonzept der Behörde bzw. des Unternehmens geregelt werden.

Hier ist festzulegen, dass Sicherheitsvorfälle und Sicherheitsprobleme von den Benutzern und Betroffenen dem zuständigen Sicherheitsverantwortlichen gemeldet werden. Darüber hinaus sind die Entscheidungsfindungswege zu beschreiben und die Notwendigkeit für Sicherheitsmaßnahmen zu motivieren.

Die Behandlung von Sicherheitsvorfällen muss außerdem mit dem Notfallmanagement abgestimmt werden, da hier viele ähnliche Vorgehensweisen zum Umgang mit sicherheitsrelevanten Vorfällen vorhanden sind, die gut zusammenarbeiten sollten. Falls es in der Institution eine spezielle Rolle für Störungs- und Fehlerbehebung gibt, ist auch diese mit einzubeziehen.

Neben einer Vorgehensweise sind auch geeignete Organisationsstrukturen zur Behandlung von Sicherheitsvorfällen festzulegen. Hierfür ist zu regeln, wer welche Verantwortung beim Auftreten von Sicherheitsvorfällen hat. Verantwortung tragen dabei unter anderem folgende Gruppen für die exemplarisch beschriebenen Aufgaben:

- Benutzer: Melden von Sicherheitsproblemen und -vorfällen
- Administratoren: Entgegennahme von Meldungen und erste Entscheidungsvorbereitung zwischen Sicherheitsproblem und -vorfall sowie Einleitung der Eskalation
- Verantwortliche für Anwendungen: Beteiligung als Träger des Schutzbedarfs der betroffenen Geschäftsprozesse und Anwendungen bei Entscheidungsfindung und Maßnahmenauswahl
- IT-Sicherheitsbeauftragter bzw. Sicherheitsmanagement: Entgegennahme von Meldungen und Entscheidungsfindung zwischen Sicherheitsproblem und -vorfall, Einschaltung des Eskalationswegs und Einleitung notwendiger Maßnahmen
- Sicherheitsvorfall-Team: ein aus betroffenen Administratoren, IT-Anwendern, IT-Sicherheitsbeauftragten, Öffentlichkeitsarbeit und gegebenenfalls Leitungsebene zusammengesetztes Team zur Abwicklung eines Sicherheitsvorfalls
- Notfallbeauftragter bzw. Notfallmanagement: Entgegennahme von Meldungen und Entscheidungsfindung zwischen Sicherheitsvorfallbehandlung und Eskalation zum Notfallmanagement
- Öffentlichkeitsarbeit bzw. Pressestelle: bei Bedarf Vorbereitung der Informationspolitik bezüglich des Sicherheitsvorfalls
- Revision: Überprüfung des Managementsystems und Nachbereitung eines Sicherheitsvorfalls
- Behörden-/Unternehmensleitung: Abschließende Entscheidungsfindung

Die Verantwortlichkeiten sind zu regeln und in Kraft zu setzen. Näheres ist in Maßnahme M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*.

Je kritischer ein Sicherheitsvorfall ist, desto mehr Kompetenzen werden bei der Behandlung des Sicherheitsvorfalls in der Regel benötigt. Dies kann so weit führen, dass die Behörden- bzw. Unternehmensleitung informiert und eingeschaltet werden muss, um notwendige Maßnahmen wie Verbot der Informationsweitergabe, Einschaltung der Polizei, kostenträchtige Ersatzmaßnahmen etc. einleiten zu können. Ein Sicherheitsvorfall kann aber auch die Eskalation an das Notfallmanagement zur Folge haben. Dazu bedarf es jedoch einer im Vorfeld erarbeiteten Strategie, wer in welchen Fällen hinzuzuziehen ist (siehe M 6.61 *Eskalationsstrategie für Sicherheitsvorfälle*).

Um die Effektivität eines Managementsystems zur Behandlung von Sicherheitsvorfällen messen zu können und um die notwendige Praxis dieser Managementaufgaben zu fördern, sind Übungen bzw. Planspiele durchzuführen. Da dies einen erheblichen Personaleinsatz benötigt und sich auch auf den normalen Geschäftsablauf störend auswirken kann, sollten Übungen auf die wichtigsten Bereiche beschränkt werden. Weitere Anregungen finden sich in

Maßnahme M 6.68 *Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen*.

Die einzelnen Prozesse, Vorgaben und Abläufe sollten sinnvollerweise in einem Dokument zur Vorgehensweise bei der Behandlung von Sicherheitsvorfällen beschrieben werden. Dieses Dokument ist in regelmäßigen Abständen zu aktualisieren und in geeigneter Weise den Betroffenen bekannt zu geben.

Prüffragen:

- Gibt es klar definierte Abläufe und Regeln für die verschiedenen Arten von Sicherheitsvorfällen?
- Ist die Vorgehensweise zur Behandlung von Sicherheitsvorfällen dokumentiert?

# M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um Sicherheitsvorfälle angemessen behandeln zu können, müssen geeignete Organisationsstrukturen vorhanden sein. Je nach Art der Institution, aber auch des Sicherheitsvorfalls müssen unter Umständen andere Personengruppen aktiv werden. Um die richtigen Akteure zu identifizieren, empfiehlt es sich, den zeitlichen Ablauf eines imaginären Sicherheitsvorfalls durchzugehen und zu überlegen, wer in den verschiedenen Phasen eines Sicherheitsvorfalls benötigt wird. Für die handelnden Personengruppen ist festzulegen, welche Aufgaben und Kompetenzen diese haben und auf welche Art sie verpflichtet bzw. unterrichtet werden. Beispielhaft soll dies für einige der typischerweise betroffenen Gruppen beschrieben werden.

**IT-Benutzer**

Aufgabe:

Sobald IT-Benutzer eine sicherheitsrelevante Unregelmäßigkeit bemerken, müssen sie die entsprechenden Verhaltensregeln einhalten und den Sachverhalt melden.

Kompetenz:

IT-Benutzer müssen entscheiden, welcher Meldeweg in dem vorliegenden Fall einzuschlagen ist (siehe M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*).

Verpflichtung / Unterrichtung:

In der Sicherheitsleitlinie des Hauses sollte geregelt sein, dass jeder IT-Benutzer verpflichtet ist, sicherheitsrelevante Unregelmäßigkeiten zu melden. Darüber hinaus sollten alle Benutzer klare und verständliche Handlungsanweisungen schriftlich ausgehändigt bekommen, wie sie sich zu verhalten haben und an wen welche Vorfälle zu melden sind. Diese Handlungsweisungen sollten in der Richtlinie zur Behandlung von Sicherheitsvorfällen definiert sein.

**Administratoren**

Aufgabe:

Die Administratoren erhalten in diesem Zusammenhang die Aufgabe, Meldungen über sicherheitsrelevante Unregelmäßigkeiten, die mit den von ihnen betreuten IT-Systemen verbunden sind, entgegenzunehmen. Anschließend haben sie sich zu entscheiden, ob sie diese Unregelmäßigkeit selbst beheben oder ob sie die nächst höhere Eskalationsebene zu unterrichten haben.

Kompetenz:

Administratoren müssen entscheiden können, ob es sich möglicherweise um ein Sicherheitsproblem handelt, dass sie eigenverantwortlich beheben kön-

nen, ob sie sofort andere Personen hinzuziehen (entsprechend dem Eskalationsplan) und wen sie informieren.

Verpflichtung / Unterrichtung:

Dies sollte in der Stellenbeschreibung sowie der Richtlinie zur Behandlung von Sicherheitsvorfällen festgelegt werden.

**Service Desk**

Aufgabe:

Die zentrale Anlaufstelle des IT-Betriebs (Service Desk) nimmt Störungsmeldungen entgegen. Diese Meldungen werden im Rahmen der Störungsqualifizierung auf das Vorliegen eines Sicherheitsvorfalls geprüft. Abhängig davon werden dann die Mitglieder des Sicherheitsmanagements informiert. In den meisten Fällen, gerade bei größeren Institutionen, wenden sich die Benutzer direkt an den Service Desk und nicht direkt an Administratoren.

Kompetenz:

Der Service Desk muss entscheiden können, wann das Sicherheitsmanagement-Team zu kontaktieren und über den Verdacht eines Sicherheitsvorfalls zu informieren ist. Dazu sollte der Zugriff auf dokumentierte Auslöser und Anzeichen vergangener Sicherheitsvorfälle möglich sein.

Verpflichtung / Unterrichtung:

Die Mitarbeiter des Service Desk müssen auch hinsichtlich der Informationssicherheit und Anzeichen möglicher Sicherheitsvorfälle sensibilisiert sein.

**Change Management Team**

Aufgabe:

Das Change Management Team nimmt IT-Änderungsanträge (IT Change Requests) entgegen. Bei Sicherheitsvorfällen beinhalten diese die notwendigen Maßnahmen zur Schließung der Sicherheitslücken, die durch das Expertenteam für die Sicherheitsvorfallbehandlung umzusetzen sind.

Kompetenz:

Das Change Management Team stellt sicher, dass die notwendigen Maßnahmen schnell, effizient und ohne Auswirkungen auf die Qualität der IT-Services umgesetzt werden.

Verpflichtung / Unterrichtung:

In der Richtlinie zur Behandlung von Sicherheitsvorfällen sollte festgelegt werden, dass Änderungsanträge zur Behebung von Sicherheitsvorfällen als dringliche Änderungen (Emergency Changes) zu behandeln sind und dementsprechend priorisiert im Change Management Prozess behandelt werden müssen.

**IT-Sicherheitsbeauftragter / Sicherheitsmanagement**

Aufgabe:

Der IT-Sicherheitsbeauftragte nimmt Meldungen über Sicherheitsvorfälle entgegen. Er führt die Untersuchung und Bewertung des Vorfalls durch. Er wählt notwendige Maßnahmen aus und veranlasst deren Umsetzung über

das Change Management Team, soweit dies seinen Kompetenzbereich nicht überschreitet. Bei Bedarf ruft er ein Sicherheitsvorfall-Team zusammen bzw. unterrichtet zur Eskalation die Leitungsebene.

Kompetenz:

Er ist befugt, ein aktuelles Ereignis zum Sicherheitsvorfall auszurufen, die Bewertung eines Sicherheitsvorfalls durchzuführen und einen Vorfall weiter zu eskalieren. Darüber hinaus sind ihm finanzielle und personelle Ressourcen bzw. Sonderbeschaffungsrechte zugebilligt, die er zur Behebung von Sicherheitsvorfällen selbständig einsetzen darf. Dies könnten z. B. abhängig von der Größe des Unternehmens oder der Behörde 100.000 Euro und 2 Personenmonate sein.

Verpflichtung / Unterrichtung:

Das Sicherheitsmanagement erarbeitet die Vorgehensweise und die Richtlinie zur Behandlung von Sicherheitsvorfällen. Daher sollten alle IT-Sicherheitsbeauftragten über ihre Aufgaben und Kompetenzen bei der Behandlung von Sicherheitsvorfällen informiert sein.

**Revision**

Aufgabe:

Der Revision kann die Aufgabe übertragen werden, in regelmäßigen Abständen die Wirksamkeit des Managementsystems für Sicherheitsvorfälle zu prüfen. Darüber hinaus kann sie beauftragt werden, bei der Nachbereitung von Sicherheitsvorfällen mitzuwirken.

Kompetenz:

In Absprache mit der Leitungsebene können Prüfungen initiiert und durchgeführt werden.

Verpflichtung / Unterrichtung:

Dies sollte in der Stellenbeschreibung und in der Richtlinie zur Behandlung von Sicherheitsvorfällen festgelegt werden.

**Öffentlichkeitsarbeit / Pressestelle**

Aufgabe:

Die Information der Öffentlichkeit sollte bei schwerwiegenden Sicherheitsvorfällen ausschließlich durch die Pressestelle erfolgen. Dabei sollte der Vorfall nicht beschönigt oder verharmlost, sondern sachlich dargestellt werden, um keinen Imageverlust bei gegenteiligen Informationen zu erleiden.

Kompetenz:

Die Pressestelle muss Informationen über den Sicherheitsvorfall zusammen mit den technischen Experten aufbereiten und mit der Leitungsebene vor der Weitergabe abstimmen.

Verpflichtung / Unterrichtung:

Dies sollte in der Stellenbeschreibung und in der Richtlinie zur Behandlung von Sicherheitsvorfällen festgelegt werden.

**Behörden-/Unternehmensleitung**

Aufgabe:

Sie wird bei schwerwiegenden Sicherheitsvorfällen unterrichtet und gegebenenfalls mit der Entscheidungsfindung konfrontiert.

Kompetenz:

Als die die Gesamtverantwortung tragende Stelle kann sie die Verantwortung an oben genannte Gruppen delegieren. Darüber hinaus kann sie Polizei und Strafverfolgungsbehörden einschalten, wenn der Verdacht auf kriminelle Handlungen besteht.

Verpflichtung / Unterrichtung:

Die Behörden- bzw. Unternehmensleitung muss der Konzeption zur Behandlung von Sicherheitsvorfällen und den darauf aufbauenden Eskalationsplänen zustimmen. Dabei wird die Leitungsebene auch über ihre Rolle bei der Behandlung von Sicherheitsvorfällen unterrichtet.

**Expertenteam für Sicherheitsvorfallbehandlung**

Aufgabe:

Neben diesen Gruppen kann es bei einem schwierigen oder bei schwerwiegenden Sicherheitsvorfällen nötig sein, dass ein Expertenteam zusammengerufen wird, um system- oder standortspezifische Erkennungs-, Sicherstellungs-, Analyse- und Reaktionshandlungen vorzunehmen (siehe auch M 6.123 *Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen*).

Kompetenz:

Die Mitglieder des Expertenteams haben Zugriff auf die verdächtigen Systeme und Zutritt zu den vom Sicherheitsvorfall betroffenen Standorten. Sie sollten befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen.

Verpflichtung / Unterrichtung:

Die Mitglieder des Expertenteams handeln strikt nach der Richtlinie für die Behandlung von Sicherheitsvorfällen und den Anweisungen des IT-Sicherheitsbeauftragten und des Sicherheitsvorfall-Teams. Sämtliche Kommunikation über den Sicherheitsvorfall zu externen und internen Stellen erfolgt über den IT-Sicherheitsbeauftragten oder eine von ihm definierte Person.

**Sicherheitsvorfall-Team**

In großen Institutionen kann es sinnvoll sein, dass neben dem IT-Sicherheitsbeauftragten ein Sicherheitsvorfall-Team benannt wird. Dieses Team hat (im Gegensatz zum Expertenteam für die technische Behandlung von Sicherheitsvorfällen) eine koordinierende Funktion und ermöglicht schnelle Entscheidungsfindungen. Auch dieses Team ist virtuell, muss aber zu schnellen strategischen Entscheidungen in der Lage sein. Daher sind die Mitglieder dieses Teams namentlich zu benennen und die Kontaktdaten müssen an geeigneten Stellen hinterlegt sein.

Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Sicherheitsvorfall zusammentritt, müssen bereits im Vorfeld dessen Mitglieder benannt und in ihre Aufgaben eingewiesen sein, damit die Reaktion auf den Sicherheitsvorfall schnellstmöglich erfolgen kann. Die Mitglieder des Sicherheitsvorfall-Teams sollten befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen. Die hierzu erforderlichen Regelungen sind schriftlich festzuhalten und von der Behörden- bzw. Unternehmensleitung zu autorisieren. Insbesondere ist festzulegen, wer die Leitung dieses Teams übernimmt.

Zu einem Sicherheitsvorfall-Team können (je nach Art des Sicherheitsvorfalls) beispielsweise gehören:

- Behörden-/Unternehmensleitung,
- Sicherheitsmanagement / IT-Sicherheitsbeauftragter,
- Leiter IT,
- Revision,
- Pressestelle,
- Datenschutzbeauftragter,
- Justitiar und
- Personalrat/Betriebsrat.

Falls es erforderlich ist, müssen weitere Bereiche hinzugezogen werden, wie z. B.

- die betroffenen Fachabteilungen (Leiter, IT-Verfahrensverantwortlicher),
- der jeweilige Kundenansprechpartner , wenn Dienstleistungen für interne oder externe Kunden erbracht werden,
- Notfallbeauftragter, Notfallmanagement,
- Administratoren,
- die Bereiche Beschaffung, Haustechnik, Innerer Dienst, Organisation, Personal und
- Brandschutzbeauftragter.

Für die verschiedenen Organisationsformen bei der Behandlung von Sicherheitsvorfällen muss geklärt sein, wer bei Vorfällen welche Maßnahmen koordiniert.

Es sollte im Vorfeld abgeklärt sein, wie mit der im Rahmen von Sicherheitsvorfällen anfallenden Mehrarbeit umzugehen ist, also ob die Arbeitszeitregelungen der Behörde bzw. des Unternehmens um Ausnahmeregelungen für Mehrarbeit, Wochenendarbeit, etc. bei Sicherheitsvorfällen erweitert werden muss. Darüber hinaus ist auch sicherzustellen, dass dieses Team bei Bedarf auch die Diensträume außerhalb der regulären Arbeitszeit nutzen kann.

Prüffragen:

- Sind für alle Personengruppen ihre Aufgaben und Kompetenzen bei Sicherheitsvorfällen festgelegt worden? Sind sie über ihre Aufgaben und Kompetenzen unterrichtet worden?
- Kennen die in die Behandlung von Sicherheitsvorfällen involvierten Mitarbeiter ihre jeweiligen Aufgaben?
- Ist ein Sicherheitsvorfall-Team benannt worden?
- Sind die betroffenen Mitglieder des Teams in ihre Aufgaben eingewiesen worden?
- Wann wurde der Aufbau des Sicherheitsvorfall-Teams zuletzt aktualisiert?

# M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Neben der Festlegung der Rollen, Verantwortlichkeiten und Verhaltensregeln bei Sicherheitsvorfällen sind auch entsprechende Meldewege zu definieren. Hier bietet sich folgendes Muster an:

- Bei Gefährdungen höherer Gewalt wie Feuer, Wasser, Stromausfall, Einbruch und Diebstahl sind die örtlich verfügbaren Einsatzkräfte sowie die technische Einsatzleitung zu unterrichten (Feuerwehr, Haustechnik, Pforte, Wachdienst, ...).
- Bei hardware-technischen Problemen oder bei Unregelmäßigkeiten bei Betrieb der IT-Systeme ist der zuständige Administrator bzw. der Benutzer-Support zu benachrichtigen.
- Bei großflächigen Ausfällen oder sonstigen im Notfallhandbuch aufgeführten Szenarien ist der Notfallbeauftragte und Leiter des Krisenstabs zu informieren.
- Bei vermuteten vorsätzlichen Handlungen und bei ansonsten nicht zuzuordnenden Ereignissen (z. B. Datenmanipulationen, unerlaubter Ausübung von Rechten, Spionage- und Sabotageverdacht) ist der IT-Sicherheitsbeauftragte bzw. das Sicherheitsmanagement zu benachrichtigen.
- Existiert eine zentrale Anlaufstelle für die Meldung von Störungen oder Sicherheitsvorfällen (siehe M 6.125 *Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen*) sollte diese Stelle in den Meldeweg aufgenommen werden, damit dort der Sicherheitsvorfall dokumentiert werden kann und bei Bedarf weitere Meldungen korreliert werden können.

Wichtig ist hier insbesondere, dass allen Mitarbeitern die Ansprechpartner und die Meldewege für alle Arten von Sicherheitsvorfällen bekannt sind. Hierzu könnte z. B. im internen Telefonverzeichnis oder im Intranet eine Liste mit Namen, Telefonnummern und E-Mailadressen der jeweiligen Ansprechpartner enthalten sein. Es darf jedoch weder schwierig noch zeitaufwendig sein, Verdachtsfälle weiterzumelden. Dafür müssen schnelle und sichere Kommunikationsverbindungen bereitstehen. Die Authentizität des Kommunikationspartners und die Vertraulichkeit der über den Verdachtsfall gemeldeten Informationen sind sicherzustellen.

Es sollten alle Mitarbeiter darüber informiert sein, dass Auskünfte über einen Sicherheitsvorfall gegenüber Dritten nur über das Sicherheitsmanagement erfolgen dürfen (siehe auch M 6.65 *Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen*).

Im Vorfeld sollten mit den Mitarbeitern der Presse- und Öffentlichkeitsarbeit Sprachregelungen vereinbart werden, die sicher stellen, dass keine Informationen unbefugt und keine falschen Informationen an die Öffentlichkeit gehen (siehe auch M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*).

Durch Übungen sollte sporadisch überprüft werden, ob die Verhaltensregeln für Sicherheitsvorfälle angemessen und durchführbar sind und ob sie allen Mitarbeitern bekannt sind (siehe auch M 6.68 *Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen*).

Besonders bei Sicherheitsvorfällen zeigt es sich immer wieder, wie wichtig ein gutes Betriebsklima und eine gesunde Kommunikationskultur sind, damit Sicherheitsvorfälle auch umgehend weitergemeldet und offen angegangen werden (siehe auch M 3.8 *Vermeidung von Störungen des Betriebsklimas*

Prüffragen:

- Sind effiziente Meldewege für Sicherheitsvorfälle aufgebaut worden?
- Sind die Ansprechpartner und die Meldewege für alle Arten von Sicherheitsvorfällen allen Mitarbeitern bekannt?
- Liegen alle Kontaktinformationen für die Meldewege in praktikabler Form vor?
- Werden die Informationen über die Meldewege regelmäßig aktualisiert? Sind die vorliegenden Informationen aktuell?

# M 6.61 Eskalationsstrategie für Sicherheitsvorfälle

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Nachdem die Verantwortlichkeiten für Sicherheitsvorfälle geregelt (siehe M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*) und die Verhaltensregeln und Meldewege allen Betroffenen bekanntgegeben worden sind (siehe M 6.60 *Festlegung von Meldewegen für Sicherheitsvorfälle*), ist als Nächstes zu regeln, wie mit eingegangenen Meldungen weiter verfahren wird. Dafür ist eine Eskalationsstrategie zu formulieren. Die Eskalationsstrategie sollte zwischen den Verantwortlichen für Störungs- und Fehlerbehebung (Incident Management) und dem Informationssicherheitsmanagement abgestimmt werden. Dies ist nötig, um eventuell bereits vorhandene Methoden und Verfahren effektiv und effizient mitnutzen zu können (siehe M 6.124 *Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung*).

Derjenige, der eine Meldung über einen Sicherheitsvorfall erhalten hat, muss diesen zunächst untersuchen und bewerten (siehe auch M 6.63 *Untersuchung und Bewertung eines Sicherheitsvorfalls*). Falls es sich tatsächlich um einen Sicherheitsvorfall handelt, müssen weitere Maßnahmen ergriffen werden. Dabei stellen sich folgende Fragen:

- Wer ist im Fall einer Eskalation, also der Ausweitung der Aktionskette, zu unterrichten?
- In welchen Fällen ist eine sofortige Eskalation vorzunehmen?
- Unter welchen Umständen ist ansonsten eine Eskalation durchzuführen?
- Wann wird diese Eskalation vorgenommen (sofort, am nächsten Tag, am nächsten Werktag)?
- Über welche Medien wird die Meldung weitergegeben?

Die Antworten zu diesen Fragen sind in einer Eskalationsstrategie festzuhalten und bekannt zu geben.

Damit die Sicherheitsstörungen ohne Zeitverlust nach der Erkennung und Registrierung von den Verantwortlichen bearbeitet werden können, sind im Vorfeld Eskalationsstrategien, -ansprechpartner und -wege zu definieren. Hierbei ist eine Synchronisierung mit den Eskalationsverfahren der Verantwortlichen für Störungs- und Fehlerbehebung (Incident Management), sowie dem Notfallmanagement zu empfehlen (siehe auch M 6.124 *Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung*).

Es kann zwischen zwei grundsätzlichen Eskalationstypen unterschieden werden, der fachlichen und der hierarchischen Eskalation.

Die fachliche Eskalation bei der Störungs- und Fehlerbehebung (Incident Management) wird eingeleitet, wenn für die Erstlösung im First Level Support keine zutreffende Lösung, z. B. in Form einer Checkliste (Matching Szenario), vorliegt oder das Matching Szenario im Eskalationsweg beispielsweise die Einbeziehung weiterer notwendiger Kompetenzträger vorsieht. Das Sicherheitsmanagement sollte regelmäßig nach den gleichen Bedingungen einbezogen werden. Hierbei sollte insbesondere bei vermuteten Sicherheitsvorfällen, für die im First Level Support kein Matching Szenario vorliegt, sofort in

Richtung Sicherheitsmanagement eskaliert werden. Dem First Level Support sollte daher die aktuelle Eskalationsstrategie vorliegen.

Die hierarchische Eskalation sollte eingeleitet werden, wenn

- neben den oben genannten Voraussetzungen absehbar ist, dass vereinbarte Wiederherstellungszeiten nicht eingehalten werden können oder aber
- im Verlauf der Bearbeitung Entscheidungen getroffen werden müssen, die nicht in der Kompetenz der Bearbeiter liegen, z. B. weil
  - sicherheitskritische Geschäftsprozesse betroffen sind,
  - existenzbedrohende Schäden vermutet werden,
  - kriminelle Handlungen vermutet werden,
  - folgenreiche Flächenstörungen oder Notfälle abzusehen sind, etc.

Es ist erforderlich, dass für die Planung der Eskalationsstrategie ebenfalls die erwarteten Reaktionen und Aktivitäten der Eskalationsinstanz klar definiert werden und die Eskalation nicht nur einen informativen Charakter erhält. Alle durchgeführten Eskalationen sind nachvollziehbar zu dokumentieren.

Die Eskalationsstrategie kann in drei Schritten erstellt werden:

**Schritt 1: Festlegung der Eskalationswege**

Wer für die Behandlung von Sicherheitsvorfällen verantwortlich ist, wurde in Maßnahme M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen* festgelegt. In der Festlegung des Eskalationsweges ist zu definieren, wer an wen eine Meldung weitergibt. Dies lässt sich in einfacher Weise durch einen gerichteten Graphen veranschaulichen. Dabei sollten sowohl die regulären Eskalationswege als auch der Vertretungsfall berücksichtigt werden.

**Beispiel:**

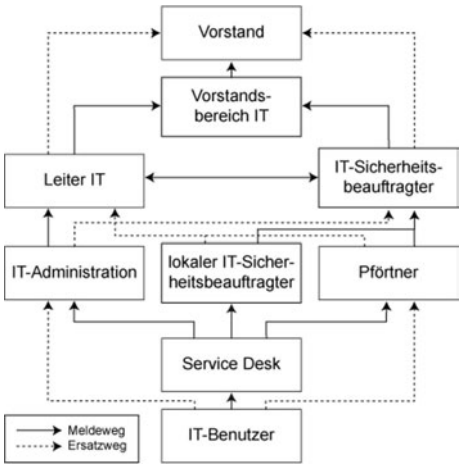



Abbildung: Meldewege für die Behandlung von Sicherheitsvorfällen

**Schritt 2: Entscheidungshilfe für Eskalation**

In diesem Schritt ist zunächst festzulegen, in welchen Fällen eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen durchgeführt werden sollte. Ein Beispiel für eine tabellarische Aufstellung ist:

| Ereignis | sofortige Unterrichtung von |
|---|---|
| Infektion mit einem Computer-Virus | IT-Sicherheitsbeauftragter, Administrator |
| Brand | Pförtner, Brandschutzbeauftragter, Feuerwehr |
| Vorsätzliche Handlungen und vermutete kriminelle Handlungen | IT-Sicherheitsbeauftragter |
| Verdacht auf Werksspionage | IT-Sicherheitsbeauftragter, Vorstand |
| Notwendigkeit, Polizei und Strafverfolgungsbehörden einzuschalten | Vorstand |
| Existenzbedrohende Schäden | Vorstand, Notfallbeauftragter und Leiter des Krisenstab |

Tabelle: Wann muss wer informiert werden

Anschließend ist für die restlichen Fälle vorzugeben, wann eine Eskalation stattzufinden hat. Gründe dafür können sein:

- Die zu erwartende Schadenshöhe übertrifft den Verantwortungsbereich der Stelle, die die Meldung entgegengenommen hat.
- Die Kosten und Ressourcen für die Schadensregulierung übertreffen deren Kompetenzbereich.
- Die Komplexität des Sicherheitsvorfalls übersteigt deren Kompetenz- bzw. Zuständigkeitsbereich.

**Schritt 3: Art und Weise der Eskalation**

Hierbei ist festzulegen, auf welche Weise die jeweils nächste Stelle in der Eskalationskette unterrichtet werden soll. Möglichkeiten dazu sind:

- persönliche Vorsprache
- schriftlicher Bericht
- E-Mail
- Trouble Ticket System
- Telefon, Handy
- Bote mit verschlossenem Umschlag

Werden für die Eskalation Werkzeuge wie z. B. Ticket-Systeme verwendet, müssen diese darauf geprüft werden, dass sie auch während eines Sicherheitsvorfalls oder Notfalls zur Verfügung stehen und damit auch vertrauliche Informationen verarbeitet werden können.

Ebenso ist festzulegen, wann diese Meldung weitergegeben wird. Beispiele sind:

- bei Ereignissen, die Sofortmaßnahmen erfordern, z. B. einer telefonischen Bombendrohung: unverzüglich.
- bei Ereignissen, die eine zügige Bearbeitung erfordern, z. B. Anzeichen auf eine Infektion mit einem Computer-Virus im LAN: sofort innerhalb einer Stunde.
- bei Ereignissen, die zwar beherrscht werden, aber einer Unterrichtung der nächsten Eskalationsstufe erfordern, z. B. Angriffe mit Schadsoftware, die aber bekannt sind und erfolgreich am Sicherheitsgateway blockiert werden: am nächsten Werktag.

Bei der Festlegung der Kriterien für die Weitergabe der Meldungen können unter anderem die Definitionen der fachlichen und hierarchischen Eskalation (siehe oben) einen Beitrag liefern.

Diese Eskalationsstrategie sollten alle möglichen Empfänger von Meldungen über Sicherheitsvorfälle erhalten, um zügige Reaktionen zu ermöglichen. Die Eskalationsstrategie und die Meldewege müssen in Übungen erprobt werden. Dadurch bekommen die Beteiligten auch die notwendige Routine, die hilft, den Stress in Krisensituationen zu verringern. Da sich Meldewege und Einschätzungen von Ereignissen immer wieder ändern können, muss die Eskalationsstrategie regelmäßig überprüft und aktualisiert werden, mindestens einmal jährlich.

Zur Eindämmung eines Sicherheitsvorfalls ist im Allgemeinen kurzfristiges Handeln erforderlich. Eventuell müssen Mitarbeiter aus anderen Projekten abgerufen oder auch außerhalb der Arbeitszeit herangezogen werden. Daher muss auch geregelt sein, wie mit der anfallenden Mehrarbeit umzugehen und wie eine Rufbereitschaft geregelt ist (siehe auch M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*).

Prüffragen:

- Ist eine aktuelle Eskalationsstrategie vorhanden?
- Wird die Eskalationsstrategie regelmäßig überprüft und gegebenenfalls aktualisiert?
- Wurden die Eskalationswege in Übungen erprobt?
- Enthält die Eskalationsstrategie eindeutige Handlungsanweisungen, wer, auf welchem Wege bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen in welchem Zeitraum zu involvieren ist?
- Ist auch geregelt, zu welchen Maßnahmen diese Eskalation führt und welche Aktivitäten ausgelöst werden sollen?
- Werden die Checklisten (Matching Szenarios) des Incident Management regelmäßig um sicherheitsrelevante Themen ergänzt bzw. aktualisiert?
- Sind die für die Eskalationsverfahren verwendeten Werkzeuge auch für vertrauliche Informationen geeignet?
- Stehen die für die Eskalation verwendeten Werkzeuge auch während eines Sicherheitsvorfalls beziehungsweise -notfalls zur Verfügung?

# M 6.62 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Ein Sicherheitsvorfall entsteht erfahrungsgemäß durch eine Verkettung verschiedener Ursachen. Dabei sind typischerweise unterschiedliche Geschäftsprozesse, Anwendungen und IT-Systeme betroffen, wobei die resultierenden Schäden auch sehr verschiedenartig sein können. Daher ist es wichtig, die Prioritäten für die Problembeseitigung möglichst vorab festzulegen. Von dieser Prioritätensetzung hängt unter anderem ab, in welcher Reihenfolge die Probleme angegangen werden sollen.

Des Weiteren orientiert sich eine Prioritätensetzung stark an den Gegebenheiten der jeweiligen Institution. Für die Prioritätensetzung sind folgende Fragen zu bearbeiten:

- Welche Schutzbedarfskategorien und Schadensszenarien sind für die Institution relevant?
- Wie ist der Schutzbedarf der Geschäftsprozesse und Anwendungen? Wie ist daraus abgeleitet der Schutzbedarf der einzelnen IT-Systeme, Räume und Kommunikationsverbindungen?
- In welcher Reihenfolge sollten Schäden der einzelnen Schutzbedarfskategorien und Schadensszenarien behoben werden?
- Welche interne oder externe Rahmenbedingungen sind bei der Prioritätensetzung zu beachten?

Hilfestellung für die Bearbeitung der Fragen bietet eine nach IT-Grundschutz durchgeführte Schutzbedarfsfeststellung. In dieser Schutzbedarfsfeststellung werden die potentiellen Schäden definierten Schadensszenarien zugeordnet und die für die Institution relevanten Informationen und Geschäftsprozesse bezüglich ihres Schutzbedarfs kategorisiert (siehe die entsprechenden Kapitel der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2).

**Beispiel:** Relevante Schadensszenarien sind:

- Verstoß gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- Negative Außenwirkung und
- Finanzielle Auswirkungen.

Ebenso wird im Rahmen der Schutzbedarfsfeststellung eine Definition der Schutzbedarfskategorien anhand von Schadenshöhen erarbeitet.

**Beispiel:** Schadensszenario "Finanzielle Auswirkungen"

| **Schadensszenario "Finanzielle Auswirkungen"** | |
|---|---|
| Schutzbedarf normal | Der finanzielle Schaden bleibt für die Institution tolerabel. |

| **Schadensszenario "Finanzielle Auswirkungen"** | |
|---|---|
| Schutzbedarf hoch | Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend. |
| Schutzbedarf sehr hoch | Der finanzielle Schaden ist für die Institution existenzbedrohend. |

Tabelle: Finanzielle Auswirkungen von Schäden

Diese Definitionen müssen an die individuellen Gegebenheiten der Institution angepasst und konkretisiert werden: Bedeutet in einem Großunternehmen ein Schaden in Höhe von 200.000,- Euro gemessen am Umsatz und am IT-Budget noch einen geringen Schaden, so kann für ein Kleinunternehmen schon ein Schaden in Höhe von 10.000,- Euro existentiell bedrohlich sein. Daher ist es häufig sinnvoll, eine prozentuale Größe als Grenzwert zu definieren, der sich am Gesamtumsatz, am Gesamtgewinn oder an einer ähnlichen Bezugsgröße orientiert.

In einem Beispielunternehmen kann folgende konkrete Festlegung getroffen worden sein:

| **Schadensszenario "Finanzielle Auswirkungen"** | |
|---|---|
| Schutzbedarf normal | Schaden kleiner 25.000,- EUR |
| Schutzbedarf hoch | Schaden zwischen 25.000,- und 5.000.000,- EUR |
| Schutzbedarf sehr hoch | Schaden höher als 5.000.000,- EUR |

Tabelle: Konkretisierung der finanziellen Auswirkungen von Schäden

Anhand dieser Kategorien und Szenarien kann die Prioritätensetzung für die wesentlichen Geschäftsprozesse und IT-Systeme durchgeführt werden, wie im folgenden beschrieben. In einer Tabelle werden in der ersten Spalte die Schadensszenarien aufgeführt. Die drei anschließenden Spalten erhalten als Überschrift die Schutzbedarfskategorien "normal", "hoch" und "sehr hoch". Anschließend wird jeder Kombination von Schadensszenario und Schutzbedarfshöhe eine Priorität zugeordnet. Die Prioritätensetzung kann einerseits durch eine Prioritätenklassifizierung mit Einteilungen wie

1 = besonders wichtig,
2 = wichtig,
3 = nachrangig

oder durch die Festlegung einer Reihenfolge stattfinden.

**Beispiel:**

Betrachtet wird als Institution eine Stadtverwaltung, die dem Bürger ihre Dienstleistungen auch über das Internet anbietet. Dazu kann der Bürger Anträge per E-Mail an die Stadtverwaltung senden und über das Internet die Bearbeitungsfortschritte seines Antrags beobachten. Als Informationsdienst bietet diese Stadtverwaltung einen Internet-Server an.

| Schadensszenarien | Schutzbedarf normal | Schutzbedarf hoch | Schutzbedarf sehr hoch |
|---|---|---|---|
| Verstoß gegen Gesetze, Vorschriften oder Verträge | 2 | 2 | 2 |
| Beeinträchtigung des informationellen Selbstbestimmungsrechts | 2 | 2 | 1 |
| Beeinträchtigung der persönlichen Unversehrtheit | 2 | 1 | 1 |
| Beeinträchtigung der Aufgabenerfüllung | 3 | 3 | 2 |
| Negative Außenwirkung | 3 | 2 | 1 |
| Finanzielle Auswirkungen | 3 | 3 | 2 |

Tabelle: Beispielergebnis mit Prioritätenklassifizierung

In der ersten Tabelle erfolgte die Prioritätenklassifizierung über die Einteilungen von 1 (besonders wichtig) bis 3 (nachrangig). In der zweiten Tabelle wurden die Prioritäten anhand ihrer Reihenfolge festgelegt, von der höchsten Stufe 1 sukzessive absteigend bis zur hier niedrigsten Stufe 18.

| Schadensszenarien | Schutzbedarf normal | Schutzbedarf hoch | Schutzbedarf sehr hoch |
|---|---|---|---|
| Verstoß gegen Gesetze, Vorschriften oder Verträge | 13 | 12 | 11 |
| Beeinträchtigung des informationellen Selbstbestimmungsrechts | 8 | 6 | 3 |
| Beeinträchtigung der persönlichen Unversehrtheit | 5 | 2 | 1 |
| Beeinträchtigung der Aufgabenerfüllung | 15 | 14 | 7 |
| Negative Außenwirkung | 17 | 9 | 4 |
| Finanzielle Auswirkungen | 18 | 16 | 10 |

Tabelle: Beispielergebnis mit Prioritätensetzung durch Reihenfolge

Diese Prioritätensetzung muss durch die Behörden- bzw. Unternehmensleitung gebilligt und in Kraft gesetzt werden. Die Prioritätensetzung ist allen Entscheidungsträgern bei der Behandlung von Sicherheitsvorfällen bekannt zu geben.

Tritt ein Sicherheitsvorfall ein, so kann die Prioritätensetzung wie folgt verwendet werden. Nach der Untersuchung und Bewertung des Sicherheitsvorfalls kann eingeschätzt werden, welche Schäden zu erwarten wären. Diese Schäden können den bekannten Schadensszenarien zugeordnet werden. Anschließend sind diese Schäden für die betroffenen Geschäftsprozesse in die Klassen "normal", "hoch" und "sehr hoch" einzuteilen. Aus der tabellarischen Übersicht der Prioritätensetzung kann dann abgelesen werden, in welcher Reihenfolge die einzelnen Schäden an den betroffenen Geschäftsprozessen behoben werden sollten. Hierbei sollte allerdings beachtet werden, dass die vorab vorgenommene Prioritätensetzung nur eine erste Orientierung bietet. Gegebenenfalls muss sie im individuellen Fall angepasst werden.

**Beispiel:**

Angenommen wird, dass es in der obigen Beispiel-Stadtverwaltung einem Hacker gelungen ist, die Informationen auf dem Internet-Informationsserver zu manipulieren, so dass die Stadtverwaltung verunglimpft wird. Dies wird frühzeitig bemerkt, das Sicherheitsmanagement eingeschaltet und die obige Schadenseinschätzung durchgeführt. Diese hätte zum Ergebnis, dass folgende Schäden zu erwarten sind:

| **Schadensszenarien** | **Schutzbedarf normal** | **Schutzbedarf hoch** | **Schutzbedarf sehr hoch** |
|---|---|---|---|
| Verstoß gegen Gesetze, Vorschriften oder Verträge | S1 | | |
| Beeinträchtigung des informationellen Selbstbestimmungsrechts | | | |
| Beeinträchtigung der persönlichen Unversehrtheit | | | |
| Beeinträchtigung der Aufgabenerfüllung | S2 | | |
| Negative Außenwirkung | | | S3 |
| Finanzielle Auswirkungen | S4 | | |

Tabelle: Schadenskategorisierung

Den Schäden S1, ..., S4 werden anhand der Prioritätensetzung folgende Prioritäten zugeordnet:

Prioritätenklassifizierung: S1 = 2, S2 = 3, S3 = 1, S4 = 3

Prioritätenreihenfolge: S1 = 13, S2 = 15, S3 = 4, S4 = 18

In beiden Fällen würde deutlich, dass die Anstrengungen der Schadensbegrenzung sich zunächst auf den Schaden S3 (negative Außenwirkung) konzentrieren müssten, bevor die anderen Schäden angegangen werden. Im Beispiel würde man, um die negative Außenwirkung zu begrenzen, den manipulierten Internet-Server vom Netz nehmen, um anschließend weitere Maßnahmen zu ergreifen. Hätte man die Schäden der negativen Außenwirkung niedriger priorisiert und hingegen die Beeinträchtigung der Aufgabenerfüllung in den Vordergrund gestellt, würde man gegebenenfalls von der Abschaltung des Internet-Servers als Sofortmaßnahme absehen.

Die Festlegung von Prioritäten kann ähnlich wie in diesem Beispiel oder mit anderen Methoden erfolgen. Wichtig ist, sich **vor** dem Eintritt eines Sicherheitsvorfalls für alle wesentlichen Geschäftsprozesse und IT-Systeme Gedanken über deren Priorisierung zu machen, um im Schadensfall zügig und effektiv handeln zu können.

Prüffragen:

- Liegt eine Prioritätensetzung für die Behandlung von Sicherheitsvorfällen vor? Ist sie aktuell?
- Ist die getroffene Prioritätensetzung mit der Behörden- bzw. Unternehmensleitung abgestimmt?
- Ist die Prioritätensetzung allen Entscheidungsträgern des Managementsystems zur Behandlung von Sicherheitsvorfällen bekannt?
- Sind die Prioritätenklassen im Incident Management (Störungs- und Fehlerbehebung) hinterlegt?

# M 6.63 Untersuchung und Bewertung eines Sicherheitsvorfalls

Diese Maßnahme ist 2009 mit der 11. Ergänzungslieferung entfallen.

# M 6.64 Behebung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Im Rahmen des Incident Managements wird bei der Störungsbehebung kontrolliert, ob eine ähnliche Störung bereits aufgetreten und dafür eine geeignete Lösung vorhanden ist, beispielsweise indem die Fehlerursache behoben wird oder nur dessen Symptome beseitigt oder diese umgangen werden, also ein Workaround gefunden wird.

Da dieser Prozessschritt iterativen Charakter hat und die Störung unterschiedlichen Support-Ebenen entsprechend ihrem fachlichen Wissen zur Analyse und Diagnose zugewiesen werden kann, müssen die Rollen und Verantwortlichkeiten sowie der Informationsfluss bereits im Vorfeld mit dem Sicherheitsmanagement etabliert worden sein.

Es erfolgt also ein Review des Incidents gegen:

- Erfasste Probleme
- Bekannte Fehler (Known Errors)
- Geplante bzw. durchgeführte Änderungen in IT-Komponenten

Wird ein Workaround gefunden, so müssen umgehend die erforderlichen Umsetzungsmaßnahmen eingeleitet werden. Die Bereitstellung eines Workarounds hat zum Ziel, die Benutzer in die Lage zu versetzen, den gestörten Service mindestens in eingeschränkter Form wieder zu nutzen (Wiederanlauf in den eingeschränkten Betrieb). Zusätzlich wird dadurch die Wirkung der Störung auf die Geschäftsprozesse minimiert und mehr Zeit zur Bereitstellung einer endgültigen Lösung gewonnen.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert worden ist, sollten die erforderlichen Maßnahmen zu dessen Behebung ausgewählt und umgesetzt werden. Dazu muss zunächst das Problem eingegrenzt und beseitigt werden und anschließend der "normale" Zustand wiederhergestellt werden (siehe M 6.133 *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen*).

**Bereitstellung des notwendigen Expertenwissens**

Die unabdingbare Voraussetzung für die Untersuchung und Beseitigung einer Sicherheitslücke ist das entsprechende Fachwissen. Daher muss das Personal entsprechend geschult sein oder es müssen Experten zu Rate gezogen werden. Dafür sollte eine Liste mit den Kontaktadressen von einschlägigen internen und externen Experten aus den verschiedenen Themenbereichen vorbereitet sein, damit diese schnell zu Rate gezogen werden können.

Zu den externen Experten gehören unter anderem

- Computer Emergency Response Teams (CERTs) (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*),
- Hersteller bzw. Vertreiber der betroffenen IT-Systeme (siehe auch M 4.107 *Nutzung von Hersteller- und Entwickler-Ressourcen*),
- Hersteller bzw. Vertreiber der eingesetzten Sicherheitssysteme, wie Computer-Viren-Schutzprogramm, Firewall, Zutrittskontrolle, etc.,
- externe Berater mit sicherheitsspezifischem Fachwissen.

Für die Kommunikation mit externen Experten muss vorab ein sicheres Verfahren definiert und eingerichtet werden.

**Reaktion auf vorsätzliche Handlungen**

Bei Sicherheitsvorfällen, die durch einen Angreifer ausgelöst wurden, muss eine Entscheidung darüber getroffen werden, ob der entdeckte Angriff beobachtet oder möglichst schnell Gegenmaßnahmen durchgeführt werden sollen. Natürlich kann versucht werden, den Angreifer "auf frischer Tat" zu ertappen, aber dies birgt auch das Risiko, dass der Angreifer in der Zwischenzeit Daten zerstört, manipuliert oder ausliest.

Leider stellt sich bei der Untersuchung von Sicherheitsproblemen häufig heraus, dass diese von eigenen Mitarbeitern verursacht worden sind. Dies kann durch Versehen, fehlerhafte Arbeitsabläufe oder technische Probleme passieren, aber auch durch Nichtbeachtung von Sicherheitsmaßnahmen oder vorsätzliche Handlungen.

Es muss bei allen intern verursachten Sicherheitsproblemen der Auslöser untersucht werden. In vielen Fällen wird sich zeigen, dass die Probleme aus fehlerhaften oder missverständlichen Regelungen resultieren. Dann müssen die Regelungen entsprechend geändert oder um weitere, z. B. technische Maßnahmen, ergänzt werden.

Sind Sicherheitsprobleme vorsätzlich oder aus Nachlässigkeit verursacht worden, sollten angemessene angemessene Konsequenzen erfolgen.

Prüffragen:

- Existiert eine aktuelle Liste von internen und externen Sicherheitsexperten, die für Fragen aus verschiedenen Themenbereichen hinzugezogen werden können?
- Sind sichere Kommunikationsverfahren mit externen Stellen eingerichtet worden?
- Wird bei allen intern verursachten Sicherheitsproblemen der Auslöser untersucht?

# M 6.65 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT, Pressestelle

Wenn ein Sicherheitsvorfall eingetreten ist, müssen alle davon betroffenen internen und externen Stellen zeitnah darüber informiert werden. Dies sind insbesondere diejenigen Stellen, die direkt durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen oder solche, die Informationen über Sicherheitsvorfälle aufbereiten und bei der Vorbeugung oder Behebung helfen können. Bei Bedarf sollte auch die Öffentlichkeit aufgeklärt werden, insbesondere wenn schon Informationen durchgesickert sind.

Hierzu muss individuell für den Sicherheitsvorfall ein klares Konzept entwickelt werden, wer durch wen in welcher Reihenfolge in welcher Tiefe informiert wird. Dazu muss sichergestellt sein, dass Auskünfte über den Sicherheitsvorfall ausschließlich durch benannte Verantwortliche, wie zum Beispiel das Sicherheitsmanagement oder die Pressestelle, gegeben werden. Dabei sollte dokumentiert werden, wem wann welche Informationen übermittelt wurden. Dies ist zur Nachbereitung wichtig, kann aber auch rechtlich relevant sein.

Wer Informationen in welchem Detaillierungsgrad erhält, hängt natürlich insbesondere vom fachlichen Hintergrund ab. Es sollten keine falschen oder schöngefärbten Informationen weitergegeben werden, da dies zu Verwirrung, Fehleinschätzungen und Imageverlust führen kann.

Beispielhaft soll nachfolgend aufgezeigt werden, welche Stellen typischerweise über welche Inhalte aufgeklärt werden:

**Interne Stellen**

Besteht noch Unklarheit darüber, ob ein Sicherheitsvorfall vorliegt oder wie schwerwiegend er ist, sollten die potentiell betroffenen internen Kräfte gebeten werden, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Sind die erforderlichen Gegenmaßnahmen bei einem Sicherheitsvorfall bekannt, müssen die betroffenen internen Stellen kurzfristig darüber informiert werden, was sie tun müssen, um die Auswirkungen eines Sicherheitsvorfalls zu minimieren oder um den sicheren Zustand wiederherzustellen.

Zu berücksichtigen sind dabei unter anderem folgende Gruppen:

- Leiter IT,
- Leiter von betroffenen Fachabteilungen,
- IT-Benutzer,
- IT-Administratoren,
- IT-Benutzerservice / Service Desk,
- Change Management (für die Erfassung der Maßnahmendurchführung),
- Haustechnik,
- Überwachungspersonal,
- interne Sicherheitskräfte und
- Pförtner.

**Externe Stellen**

Falls der Sicherheitsvorfall nicht intern begrenzt ist, sollten alle externen Stellen, die ebenfalls betroffen sind oder sein können, darüber informiert werden, welches Sicherheitsproblem aufgetreten ist, welche Gegenmaßnahmen notwendig sind und wie die Auswirkungen eingedämmt werden können.

Sollte diese Informationsweitergabe nicht erfolgen, kann dies im Falle des Bekanntwerdens eine weitere konstruktive Zusammenarbeit nachhaltig schädigen und ein bestehendes Vertrauensverhältnis beeinträchtigen.

Zu berücksichtigen sind dabei folgende Gruppen:

- Kunden,
- Lieferanten,
- freie Mitarbeiter,
- Subunternehmen,
- IT-Service-Dienstleister,
- Stellen, zu denen Kommunikationsverbindungen existieren,
- Software-Entwicklungsunternehmen und
- Netzbetreiber.

Je nach Art des Vorfalls kann es außerdem notwendig sein, die Polizei bzw. einen Rechtsbeistand hinzuzuziehen.

**Öffentlichkeit**

Bei größeren oder komplexeren Sicherheitsvorfällen kann es notwendig sein, die Öffentlichkeit aufzuklären. Alle Pressekontakte sollten hierbei ausschließlich über den Pressesprecher laufen. Dazu ist sicherzustellen, dass der Pressesprecher über den Sicherheitsvorfall, über Schadenshöhe und erforderliche Gegenmaßnahmen und über benachrichtigte Stellen ausreichend vorab informiert wird.

Die Informationen für die Öffentlichkeit sollten jedoch so weit abstrahiert werden, dass keine Nachahmer animiert werden.

Bei allen Personen, die Informationen über Sicherheitsvorfälle einholen wollen, ist es wichtig, deren Identität zu überprüfen, damit sich der Angreifer nicht über den Erfolg seiner Attacke auf dem Laufenden halten kann.

**Sicherheitsgemeinde**

Ist der Sicherheitsvorfall auf eine noch nicht bekannte Sicherheitslücke zurückzuführen, sollte diese Erkenntnis nicht verheimlicht, sondern an weitere Stellen geleitet werden, damit vor der Sicherheitslücke gewarnt wird und Gegenmaßnahmen entwickelt werden können. Als Adressaten kommen dabei typischerweise folgende Stellen in Betracht:

- Hersteller des Computer-Viren-Suchprogramms, wenn der Verdacht besteht, dass ein neuartiger Computer-Virus oder andere Schadsoftware IT-Systeme infiziert hat, aber der Viren-Scanner diese nicht erkennt,
- Hersteller des Betriebssystems oder der Applikationssoftware, falls die Sicherheitslücke darin aufgetreten ist,
- externes Computer Emergency Response Team (CERT, siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*), wenn der Sicherheitsvorfall auf system- oder applikationsspezifischen Sicherheitslücken beruht,
- IT- bzw. Sicherheitsfachpresse oder
- für Informationssicherheit zuständige öffentliche Stellen wie das BSI.

**Beispiel:**

Es wurde bemerkt, dass sporadisch Daten auf PCs manipuliert oder unauffindbar waren. Nach Meldung und anschließender Untersuchung stellte sich heraus, dass ein bislang unbekannter Computer-Virus aufgetreten ist. Dieser Virus verbreitet sich über an E-Mail angehängte Dateien. In diesem Fall sollten folgende Stellen umgehend benachrichtigt werden:

- Leiter IT,
- IT-Benutzer,
- IT-Administratoren,
- IT-Benutzerservice,
- sämtliche Stellen, mit denen seit dem ersten Auftreten des Computer-Virus Daten ausgetauscht wurden,
- Hersteller des Computer-Viren-Suchprogramms, da der Viren-Scanner diesen nicht erkannt hat und
- ein Computer Emergency Response Team.

Prüffragen:

- Ist gewährleistet, dass alle betroffenen internen und externen Stellen zeitnah darüber informiert werden, wenn ein Sicherheitsvorfall eingetreten ist? Ist gewährleistet, dass sie über die erforderlichen Maßnahmen informiert werden, um die Auswirkungen eines Sicherheitsvorfalls zu minimieren und um den sicheren Zustand wiederherzustellen?
- Ist geklärt, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt?
- Ist sichergestellt, dass keine unautorisierte Person Informationen über den Sicherheitsvorfall weitergibt?
- Liegt für die letzten Sicherheitsvorfälle die Beschreibung vor, wer durch wen in welcher Reihenfolge in welcher Tiefe informiert wurde?

# M 6.66 Nachbereitung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Revisor

Aus jedem Sicherheitsvorfall kann man etwas lernen. Um aus einem eingetretenen Sicherheitsvorfall den maximalen Lerneffekt ziehen zu können, darf die Nachbereitung nicht vernachlässigt werden. Oftmals lassen sich daraus Verbesserungen im Umgang mit Sicherheitsvorfällen herausarbeiten oder Rückschlüsse auf die Wirksamkeit des Sicherheitsmanagements bzw. der vorhandenen Sicherheitsmaßnahmen ziehen. Dabei sind unter anderem folgende Aspekte zu beachten:

**Reaktionszeit**

Untersucht werden sollte, wie schnell der Sicherheitsvorfall bemerkt wurde und welche Informationen für die Bewertung zur Verfügung standen. Dabei ist zu prüfen, ob es sinnvoll ist, technische Detektionsmaßnahmen nachzurüsten.

Darüber hinaus sollte auch der Frage nachgegangen werden, wie lange es dauerte, bis die Meldung den erforderlichen Meldeweg durchlaufen hat. Schließlich sollte der Aspekt betrachtet werden, wie schnell die Entscheidungen über die zu treffenden Maßnahmen erfolgten, wie lange deren Umsetzung dauerte und wann die Benachrichtigung der betroffenen internen und externen Stellen erfolgte.

Bei der Rückverfolgung des Meldewegs sollte überprüft werden, ob der Meldeweg jedem bekannt war oder ob zusätzliche Sensibilisierungsmaßnahmen und Informationen notwendig sind.

**Wirksamkeit der Eskalationsstrategie**

Anhand des konkreten Sicherheitsvorfalls sollte untersucht werden, ob die festgelegte Eskalationsstrategie eingehalten wurde, welche zusätzlichen Informationen notwendig sind und ob eine Anpassung der Eskalationsstrategie notwendig ist.

**Effektivität der Untersuchung**

In einer Rückschau sollte betrachtet werden, ob die Einschätzung der Schadenshöhe des Sicherheitsvorfalls korrekt war, ob die berücksichtigten Prioritäten angemessen waren und ob ein für die Untersuchung geeignetes Sicherheitsvorfall-Team eingesetzt wurde.

**Benachrichtigung betroffener Stellen**

Überprüft werden sollte, ob tatsächlich sämtliche betroffenen Stellen benachrichtigt wurden und ob die Benachrichtigung zeitlich ausreichend schnell war. Unter Umständen müssen schnellere Wege der Benachrichtigung gefunden werden.

**Rückmeldung an meldende Stelle**

Diejenigen Stellen, die einen Sicherheitsvorfall entdeckt haben und diesen an die zuständigen Experten weitergemeldet haben, sollten darüber informiert werden, wann der Sicherheitsvorfall erfolgreich behoben wurde, welche Schä-

den entstanden sind und welche Maßnahmen ergriffen wurden. Dies zeigt, dass solche Meldungen ernst genommen werden und fördert die Motivation. Zusätzlich könnte auch eine Belobigung oder Belohnung für die korrekte Weitermeldung ausgesprochen werden, um für das Betriebsklima ein Signal zu setzen, wie wichtig das Meldewesen für Sicherheitsvorfälle ist.

**Tätermotivation**

Stellt sich heraus, dass der Sicherheitsvorfall auf eine vorsätzliche Handlung zurückzuführen ist, sollte die Motivation des Täters untersucht werden. Handelt es sich dabei um einen Innentäter, kommt der Motivation eine besondere Bedeutung zu. Stellt sich heraus, dass die Ursache im Bereich des Betriebsklimas zu sehen ist, sollte dies auch der Leitungsebene bekanntgegeben werden, da zu erwarten ist, dass Fehlhandlungen und vorsätzliche Handlungen wiederholt auftreten werden.

**Bericht**

Die Leitungsebene der Institution sollte mindestens einmal jährlich einen aufbereiteten Bericht über Anzahl, Ursachen und Auswirkungen der Sicherheitsvorfälle erhalten. Je nach Relevanz der Nachbereitungsergebnisse sollte die Leitungsebene sofort unterrichtet werden, um Verbesserungen oder Aktionen zu veranlassen. Daher kann es sinnvoll sein, diese Nachbereitung durch eine Organisationseinheit durchzuführen, die nicht Teil des Meldeplans ist.

**Entwicklung einer Handlungsanweisung**

Im Rahmen der Nachbereitung eines Sicherheitsvorfalls ist es sinnvoll, aus den Erfahrungen heraus eine Handlungsanweisung zu erstellen bzw. zu überarbeiten, wie bei Auftreten eines vergleichbaren Sicherheitsvorfalls zu verfahren ist. Da jetzt die Probleme real bearbeitet wurden, können Handlungsanweisungen noch effizienter ausgearbeitet werden als bei der Erstellung auf einer theoretischen Basis. Darüber hinaus beweist der aufgetretene Sicherheitsvorfall, dass ein Bedarf für eine Handlungsanweisung konkret für diese Art von Sicherheitsvorfall gegeben ist. Eine derart erstellte Handlungsanweisung ist den relevanten Personengruppen in geeigneter Weise bekannt zu geben. Unter Umständen kann es sinnvoll sein, dann auch die Notfalldokumentation zu aktualisieren.

Prüffragen:

- Wurde eine standardisierte Nachbereitung der letzten Sicherheitsvorfälle durchgeführt?
- Wurde untersucht, wie schnell Sicherheitsvorfälle bemerkt und behoben wurden? Wurde untersucht, ob die Meldewege funktionierten, ausreichend Informationen für die Bewertung zur Verfügung standen und die Detektionsmaßnahmen wirksam waren? Waren die ergriffenen Maßnahmen und Aktivitäten wirksam und effizient?
- Wurden die Erfahrungen aus vergangenen Sicherheitsvorfällen genutzt, um daraus Handlungsanweisungen für vergleichbare Sicherheitsvorfälle zu erstellen?
- Werden die Handlungsanweisungen den relevanten Personengruppen bekanntgegeben?
- Werden die Handlungsanweisungen auf Basis neuer Erkenntnisse regelmäßig aktualisiert?
- Findet eine jährliche Unterrichtung der Leitungsebene über die Sicherheitsvorfälle statt?

# M 6.67 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Neben der Prävention kommt auch der Detektion von Sicherheitsvorfällen große Bedeutung zu. Es gibt eine Reihe von sicherheitsrelevanten Unregelmäßigkeiten, die mit entsprechender technischer Unterstützung automatisiert und daher frühzeitig erkannt werden können. Diese Detektionsmaßnahmen erhöhen meist die Zuverlässigkeit der Feststellung und verkürzen die Zeit zwischen Auftreten und Erkennen einer Unregelmäßigkeit drastisch. Dem Gewinn an Reaktionsfähigkeit und -zeit steht jedoch der Aufwand zur Implementation und Kontrolle gegenüber, der vorher abgeschätzt werden sollte. Praktisch unverzichtbar sind solche Detektionsmaßnahmen, wenn im Schadensfall sehr große Schäden bis hin zu Personenschäden zu erwarten sind.

Beispiele für solche technischen Detektionsmaßnahmen sind:

- Gefahrenmeldeanlage (siehe M 1.18 *Gefahrenmeldeanlage*),
- Fernanzeige von Störungen (siehe M 1.31 *Fernanzeige von Störungen*),
- Computer-Viren-Suchprogramme (siehe M 2.157 *Auswahl eines geeigneten Viren-Schutzprogramms*),
- Intrusion Detection und Intrusion Response Systeme (siehe M 5.71 *Intrusion Detection und Intrusion Response Systeme*),
- Kryptographische Checksummen (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*) oder
- Einsatz eines Security-Realtime-Monitors für z/OS-Systeme, um Sicherheitsverletzungen schneller feststellen zu können.
- Einsatz einer zentralen Protokollanalyse, um eventuelle Angriffe auf IT-Systeme aufzudecken.

Nicht alle Sicherheitsvorfälle lassen sich durch rein technische Maßnahmen rechtzeitig feststellen. Häufig müssen zusätzlich organisatorische Maßnahmen hinzukommen. Die Zuverlässigkeit von technischen Detektionsmaßnahmen ist im Allgemeinen davon abhängig, wie aktuell diese sind und wie gut diese auf die tatsächlichen Gegebenheiten angepasst sind. Die Zuverlässigkeit von organisatorischen Detektionsmaßnahmen hängt stark davon ab, wie zuverlässig die mit deren Umsetzung beauftragten Personen sind, aber auch, in wie weit die Maßnahmen sich im laufenden Betrieb tatsächlich umsetzen lassen. Alle Detektionsmaßnahmen müssen regelmäßig auf ihre Eignung geprüft werden.

Typische Beispiele von Detektionsmaßnahmen, die ganz oder teilweise organisatorischer Natur sind, sind:

- Informationsbeschaffung über Sicherheitslücken (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*)
- Regelmäßiger Sicherheitscheck ausgewählter IT-Systeme (siehe z. B. M 4.93 *Regelmäßige Integritätsprüfung*, M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*, M 5.141 *Regelmäßige Sicherheitschecks in WLANs*)
- Regelmäßige Auswertung von Protokoll-Dateien (siehe z. B. M 2.64 *Kontrolle der Protokolldateien*, M 4.5 *Protokollierung bei TK-Anlagen*, M 4.25 *Einsatz der Protokollierung im Unix-System*, M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*, M 5.9 *Protokollierung am Server*)

- Auswertung von SMF-Datensätzen unter z/OS (siehe M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). Informationen aus diesen SMF-Datensätzen können entweder für Batch-Reports oder als Quelle für Security-Realtime-Monitore benutzt werden, die ihrerseits eine zentrale Kontroll-Konsole ansteuern können. Solche zentralen Konsolen werden von verschiedenen Herstellern im Rahmen von Automationsprodukten angeboten.

Es sollte eine Übersicht über die eingesetzten Detektionsmaßnahmen geben.

Die erkannten Sicherheitsvorfälle sollten direkt als Störung registriert werden, damit sie vom ersten Auftreten bis zur Lösung nachvollziehbar dokumentiert werden können. Daher ist zu regeln, in welchen Systemen diese erfasst werden. Außerdem muss dem Service Desk bekannt sein, welche Informationen bei der Erstmeldung eines Sicherheitsvorfalls zu registrieren sind (sofern bereits bei der Meldung erkennbar ist, dass es sich um einen Sicherheitsvorfall handelt).

Prüffragen:

- Gibt es eine Übersicht über die eingesetzten Detektionsmaßnahmen?
- Werden die eingesetzten Detektionsmaßnahmen regelmäßig auf Eignung geprüft?
- Ist sichergestellt, dass Auffälligkeiten in Protokoll-Dateien erkannt und gemeldet werden?
- Ist im Incident Management (Störungs- und Fehlerbehebung) bekannt, welche Informationen bei der Erstmeldung eines Sicherheitsvorfalls zu registrieren sind?
- Ist sichergestellt, dass die erkannten Sicherheitsvorfälle als Störung registriert werden und ist geregelt, in welchen Systemen diese erfasst werden?

# M 6.68 Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Revisor

Das Managementsystem zur Behandlung von Sicherheitsvorfällen muss regelmäßig auf seine Aktualität und Wirksamkeit geprüft werden. Daneben sollten auch die darin formulierten Maßnahmen regelmäßig daraufhin getestet werden, ob sie

- den betroffenen Mitarbeitern bekannt sind,
- unter Stress umsetzbar sind, also auch bei einem Sicherheitsvorfall, der einen ungeordnet ablaufenden Betrieb zur Folge hat, und
- in den Betriebsablauf integrierbar sind.

Um die Wirksamkeit zu testen, sollte durch simulierte Schadensereignisse überprüft werden, ob der festgelegte Handlungsablauf eingehalten wird bzw. überhaupt eingehalten werden kann. Ist er das nicht, müssen entsprechende Änderungen eingebracht werden.

Dazu könnten sowohl angekündigte als auch unangekündigte Übungen durchgeführt werden.

Bei allen unangekündigten Übungen dürfen auf keinen Fall irgendwelche Aktionen ausgelöst werden, die zu irgendeinem nicht oder nur schwer behebbaren Schaden an IT-Systemen, Daten oder sonstigem führen können. Ebenso sollten Geschäftsprozesse und der IT-Betrieb so wenig wie möglich beeinträchtigt werden.

Sehr genau sollte vor dem Beginn jeder Übung überlegt werden, wer alles vorab darüber informiert wird. Es ist immer unbedingt sicherzustellen, dass die Übung durch die Behörden- bzw. Unternehmensleitung autorisiert ist. Manchmal kann es nützlich sein, bestimmte Personengruppen nicht zu informieren, z. B. die Pförtner oder die Administratoren. Es sollte aber sichergestellt sein, dass dabei die Situation unter Kontrolle bleibt. Es sollte also vermieden werden, dass z. B. Polizei oder Feuerwehr alarmiert oder alle Netzverbindungen der Behörde bzw. des Unternehmens gekappt werden.

**Beispiele:**

- Rufen Sie bei der Telefonzentrale ihres Unternehmens bzw. Behörde an und geben Sie sich als Computer-Experte aus, der eine Schwachstelle in Ihrem internen Netz entdeckt hat, über die Angreifer eindringen könnten. Wahlweise können Sie sich auch als Journalist ausgeben, der darüber informiert sein will, dass ein Hacker ins interne Netz eingebrochen ist und sensitive Daten kopiert hat. Es können auch solche Mitarbeiter angerufen werden, an die typischerweise in solchen Fällen verwiesen wird, also beispielsweise der Pressesprecher oder der Leiter IT. Bei einem solchen Anruf sollte sich zeigen, ob intern Panik ausbricht oder ob gezielt die Aktionen eingeleitet werden, die in einem solchen Fall adäquat wären.
- An einem beliebigen Tag könnten alle bei einer Computer-Viren-Infektion durchzuführenden Handlungen und Meldewege getestet werden. Hierbei müssen nicht unbedingt alle Beteiligten vorher informiert werden, spätestens aber in dem Moment, wo sie in die Handlungskette integriert werden.

Ein weiterer Aspekt der Effizienzprüfung ist die Auswertung von Messgrößen, die beispielsweise während der Aufnahme, Meldung und Eskalation von Sicherheitsvorfällen anfallen können. So lassen sich zum Beispiel die Zeiträume von der Erstmeldung zur Eskalation und verbindlichen Bestätigung eines Sicherheitsvorfalls aufnehmen und nach einer Auswertung optimieren. Findet die Meldung eines Sicherheitsvorfalls am zentralen Service Desk statt, können die dort bereits vorhandenen Mechanismen zur Effizienzmessung herangezogen und im Nachhinein bewertet werden.

Prüffragen:

- Wird das Managementsystem zur Behandlung von Sicherheitsvorfällen regelmäßig auf seine Aktualität und Wirksamkeit geprüft?
- Werden dazu Übungen durchgeführt?
- Werden die Übungen vorher mit der Leitungsebene abgestimmt?
- Werden Messgrößen für die Behandlung von Sicherheitsvorfällen festgelegt?

# M 6.69 Notfallvorsorge und Ausfallsicherheit bei Faxservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Fax-Poststelle

Die Maßnahmen für Notfallvorsorge und Ausfallsicherheit von Faxservern sind abhängig vom Volumen, das über den oder die Faxserver abgewickelt wird und von den Anforderungen an die Verfügbarkeit dieses Dienstes.

Zunächst ist grundsätzlich sicherzustellen, dass alle Konfigurationsparameter der benutzten Kommunikationskarten, des Betriebssystems und der Faxserver-Applikation dokumentiert werden. Bei Veränderungen an der Konfiguration ist die Dokumentation entsprechend zu aktualisieren. Nur so kann sichergestellt werden, dass im Notfall ein Faxserver in kürzester Zeit neu installiert werden kann.

Weiterhin sollten in regelmäßigen Abständen gemäß den Festlegungen des Datensicherungskonzeptes und der Sicherheitspolitik Datensicherungen durchgeführt werden. Dabei sollten neben den Datenpartitionen auch die Partitionen, auf denen sich das Betriebssystem und die Faxserver-Applikation befinden, mit in die Datensicherung einbezogen werden.

Die auf dem Faxserver gespeicherten Faxsendungen müssen regelmäßig gesichert werden. Sofern eine dauerhafte Archivierung von Faxdaten gewünscht ist, sollte diese nicht auf dem Faxserver sondern auf externen Datenmedien erfolgen.

Um bei einem Ausfall des Faxservers bzw. des Netzes auch weiterhin Faxe versenden und empfangen zu können, sollten ggf. ein oder mehrere herkömmliche Faxgeräte vorgehalten werden. Die Anzahl der benötigten Geräte ist vom Volumen an ein- und ausgehenden Faxsendungen im Notfall abhängig. Sinnvoll ist, als Notfallreserve die Faxgeräte zu verwahren, die schon vor Installation des Faxservers verwendet wurden.

Alle weiteren Maßnahmen zur Erhöhung der Ausfallsicherheit verursachen z. T. erhebliche Kosten und werden daher wohl nur bei höheren Anforderungen an die Verfügbarkeit in Betracht kommen und müssen einzeln erwogen werden.

Zunächst kann das IT-System, auf dem der Faxserver installiert ist, mit einem RAID-System ausgerüstet werden. Dabei werden mehrere Festplatten zu einem Stapel zusammengefasst und die darauf befindlichen Daten unter Bildung von Redundanzen auf die verschiedenen Festplatten verteilt. Dies führt z. B. bei einem so genannten RAID Level 5 dazu, dass auch beim Ausfall einer Festplatte keine Datenverluste auftreten. Allerdings verringert sich beim Einsatz der RAID-Technologie die freie Gesamtkapazität der Festplatten wegen der Redundanzbildung. Außerdem muss berücksichtigt werden, dass diese Lösung kein Ersatz für die externe Datensicherung ist und auch nicht vor dem Gesamtausfall des Systems schützt.

Ausfallsicherheit kann auch durch den Einsatz mehrerer Faxserver erreicht werden. Sofern ein Server ausfällt, kann die Last auf die anderen Server verteilt werden. Vorteilhaft an dieser Lösung ist zudem, dass auch eine Lasttrennung erreicht wird und die Gefahr einer Überlastung eines einzelnen Faxservers vermindert wird. Nachteilig ist allerdings, dass eingegangene Faxsendun-

gen, die sich auf dem ausgefallenen Server befinden, zumindest für die Dauer des Ausfalls nicht mehr verfügbar sind.

Sofern Ausfälle bei Faxservern aufgrund der Verfügbarkeitsanforderungen allenfalls im Minutenbereich tolerierbar sind, bietet sich der Einsatz redundanter Server an. Für jeden Faxserver, der in ein solches Redundanzkonzept eingebunden wird, ist dann ein zweiter Server verfügbar, auf den die entsprechenden Daten repliziert werden. Diese Lösung bietet - ggf. in Kombination mit RAID-Systemen - die höchstmögliche Ausfallsicherheit, verursacht aber auch erhebliche Kosten.

Prüffragen:

- Erfolgt eine regelmäßige Datensicherung des Faxservers gemäß den Festlegungen des Datensicherungskonzeptes?
- Werden die auf dem Fax-Server gespeicherten Faxsendungen regelmäßig gesichert?
- Stehen für einen Notbetrieb entsprechende Fax-Ausweich-Systeme zur Verfügung?

# M 6.70 Erstellen eines Notfallplans für den Ausfall des RAS-Systems

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen. Alle relevanten Inhalte wurden in M 6.109 *Notfallplan für den Ausfall eines VPNs* integriert.

# M 6.71 Datensicherung bei mobiler Nutzung des IT-Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

IT-Systeme im mobilen Einsatz (z. B. Laptops, Notebooks) sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über Datenträger oder über temporäre Netzanbindungen. Letztere können beispielsweise durch Remote Access oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei mobilen IT-Systemen meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden.

Generell bieten sich folgende Verfahren zur Datensicherung an:

- **Datensicherung auf externen Datenträgern**
  Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass ein geeignetes Laufwerk und genügend Datenträger mitgeführt werden müssen und dass für den Benutzer zusätzlicher Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht. Die Datenträger sollten eine ausreichende Speicherkapazität besitzen, so dass der Benutzer nicht mehrere Datenträger pro Sicherungsvorgang in das Laufwerk einlegen muss. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhanden kommen und dadurch sensitive Daten kompromittiert werden können. Die Datenträger und das mobile IT-System sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des IT-Systems die Datenträger nicht ebenfalls abhanden kommen.
  Die Speicherung auf externen Datenträgern zur Datensicherung bietet sich insbesondere an, wenn auch der Datenaustausch mit anderen IT-Systemen über externe Datenträger erfolgt. Diese beiden Prozesse können u. U. kombiniert werden. Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Institution eingepflegt werden.
- **Datensicherung über temporäre Netzverbindungen**
  Wenn die Möglichkeit besteht, das IT-System regelmäßig an ein Netz anzuschließen, beispielsweise über Remote Access, kann die Sicherung der lokalen Daten auch über die Netzanbindung erfolgen. Vorteilhaft ist hier, dass der Benutzer keine Datenträger verwalten und auch kein entsprechendes Laufwerk mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von Remote Access nach jedem Einwahlvorgang automatisch gestartet werden.
  Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Bei gängigen Zugangstechnologien (z. B. ISDN, Modem, Mobiltelefon) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an,

lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.
Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen (siehe auch M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*). Hierdurch erhöht sich jedoch u. U. der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst weitgehend automatisiert werden, so dass die Benutzer möglichst wenig Aktionen selbst durchführen müssen. Wenn die Mitarbeit der Benutzer erforderlich ist, sollten sie zur regelmäßigen Durchführung der Datensicherung verpflichtet werden (siehe M 2.41 *Verpflichtung der Mitarbeiter zur Datensicherung*). Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können (siehe M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*).

Prüffragen:

- Ist die Datensicherung bei mobiler Nutzung des IT-Systems geregelt?

# M 6.72 Ausfallvorsorge bei Mobiltelefonen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer, Leiter IT

Ein Mobiltelefon kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn es dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vorne herein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Der Ladezustand und die Funktionsfähigkeit des Mobiltelefon-Akkus sollten regelmäßig überprüft werden (siehe auch M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen*).

Alle auf dem Mobiltelefon gespeicherten Daten wie Telefonbucheintragungen, Nachrichten, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie PINs und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihrem Schutzbedarf sicher aufbewahrt werden
- Alle Daten, die auf der SIM-Karte gespeichert sind, also z. B. Telefonbücher, können über SIM-Kartenleser und entsprechende Software in einen PC eingelesen und dort verwaltet werden. Dies hat außerdem den Vorteil, dass Adressdaten auf dem PC leichter gepflegt und mit anderen Adressdatenbanken synchronisiert werden können. Insbesondere wenn mehrere Mobiltelefone benutzt werden (siehe auch M 2.190 *Einrichtung eines Mobiltelefon-Pools*) ist ein Abgleich der Telefonbücher auf diesem Weg sinnvoll. Wenn nur die Daten auf der SIM-Karte gesichert werden, sind alle Benutzer darauf hinzuweisen, dass sie auch nur dort Rufnummern und Ähnliches speichern sollten. Da diese Methode in der Regel weitere Hardware (den SIM-Kartenleser) benötigt und die Speicherkapazität der SIM-Karte gegenüber dem Telefonspeicher deutlich geringer ist, sollte aber besser der Telefonspeicher für Adressbücher verwendet werden. Diese Variante hat überdies den Vorteil, dass die Kontakt-Daten dabei je nach Modell im vCard-Format vorliegen können, das von vielen verschiedenen IT-Systemen (Mobiltelefonen, Smartphones und PCs) verarbeitet werden kann.
- Das Mobiltelefon kann auch mit einem weiteren IT System, z. B. einem Notebook oder einem Organizer, gekoppelt werden, sodass die zu sichernden Daten auf diesem Weg ausgetauscht werden falls eine geeignete Synchronisations-Software für das gewählte Mobiltelefon existiert (siehe auch M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Dabei können sowohl die auf der SIM-Karte als auch die im Gerät gespeicherten Daten gesichert werden.

Wenn ein Mobiltelefon kontinuierlich verfügbar sein soll, sollte ein Ersatz-Mobiltelefon oder aber ein Ersatz-Akku (wenn möglich), mitgeführt werden.

Wenn Mobiltelefone im Rahmen von Alarmierungen eingesetzt werden, also wenn z. B. die Einbruchmeldeanlage Alarmmeldungen über GSM absetzt oder Notfallpersonal über Mobiltelefone benachrichtigt werden soll, muss immer eine Ausweichmöglichkeit vorgesehen sein.

**Reparatur**

Bei Defekten des Mobiltelefons oder einzelner Komponenten sollten Reparaturen nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie Mobiltelefonen lohnt sich eine Reparatur häufig nicht, sodass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein Mobiltelefon kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des Mobiltelefons bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor das Mobiltelefon zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. der Anrufspeicher, gespeicherte E Mails und das Telefonbuch im Gerät gelöscht werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollten die SIM-Karte und ggf. entnehmbare Speicherkarten entfernt werden. Bei vielen Mobiltelefon-Modellen empfiehlt es sich, einen dort möglichen Firmware-Reset durchzuführen.

Prüffragen:

- Werden die auf Mobiltelefonen gespeicherten Daten in regelmäßigen Abständen auf einem anderen Medium gesichert?
- Werden vor Reparaturen alle vertraulichen Daten vom Mobiltelefon gelöscht (und vorher gesichert)?

# M 6.73 Notfallplanung und Notfallübungen für die Lotus Notes/Domino-Umgebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Notfallbeauftragter, Leiter IT

**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter, Notfallbeauftragter

Für die Lotus Notes/Domino-Umgebung ist eine angemessene Notfallplanung, in Abhängigkeit von der in der übergeordneten Geschäftsfortführungsplanung festgelegten Notfallplanungsrelevanz, zu erstellen (siehe dazu auch Baustein B 1.3 *Notfallmanagement*). Diese muss alle Aspekte der Notfallvorsorge und auch die nach Eintritt eines Notfalls notwendigen Schritte zur Wiederherstellung und zum Wiederanlauf der Umgebung beinhalten.

In der Notfallplanung sind relevante Notfallszenarien für die Lotus Notes/Domino-Umgebung zu betrachten. Insbesondere sind auch der Ausfall von Notes/Domino als Basis des institutionsweiten Identitätsmanagements und der Ausfall des externen, zentralen Identitätsmanagements (beide nur bei entsprechender Relevanz) in den Notfallszenarien zu berücksichtigen.

Ziel der Notfallplanung darf nicht nur die Wiederherstellung und der Wiederanlauf einzelner Komponenten sein, sondern vor allem die Wiederherstellung und der Wiederanlauf der Lotus Notes/Domino-Umgebung. Daher sind eine Wiederherstellung der Daten unter Berücksichtigung der Replikationsproblematik und eine synchronisierte Wiederherstellung der Komponenten unter Berücksichtigung aller Komponentenabhängigkeiten in der Notfallplanung anzustreben. Es ist möglich, die Wiederherstellung eingeschränkter Umgebungen vorzusehen, in denen nur die wichtigsten Dienste betrieben werden.

Clustering auf unterschiedlichen Ebenen (Betriebssystem, Lotus Notes/Domino-Umgebung) und redundante Datenhaltung über entsprechende Speicherlösungen stellen primär Hilfsmittel zur Sicherung einer hohen oder sehr hohen Verfügbarkeit von Lotus Notes/Domino dar und ersetzen keine Notfallplanung. Dennoch können sie, bei entsprechender Konfiguration, dabei helfen, diverse Notfallszenarien effizient zu lösen.

Die von Lotus Notes/Domino angebotenen Mechanismen zur Wiederherstellung (z. B. Wiederherstellung für Notes-IDs), Zurücksetzen von Kennwörtern in einer ID-Vault (ab Version 8.5), Failover für die Verzeichnisverwaltung, Datenbankreparatur (*Fixup, Compact, Updall*) und automatischem Wiederanlauf (*Fault Recovery*) sind unter genauer Kenntnis ihrer Funktionsweise in der Notfallplanung zu verwenden.

Besonderes Augenmerk ist auf die Wiederherstellung der Zertifikatsinfrastruktur zu legen. Das Notfallszenario einer Kompromittierung der Zertifikatsinfrastruktur ist dabei zu berücksichtigen.

Wird im Rahmen der neuen Lotus Notes/Domino Versionen (ab Version 8.5) DAOS (*Domino Attachment and Object Service)* eingesetzt, ist die Notfallplanung an das nicht mehr redundante Vorhalten von Anhängen und Objekten anzupassen.

Um sicherzustellen, dass die Notfallplanung für die Lotus Notes/Domino-Umgebung angemessen und praxistauglich ist, ist es erforderlich, Notfallübungen durchzuführen.

Notfallübungen sind detailliert im Vorfeld zu planen. Idealerweise besteht eine übergeordnete Planung für Notfallübungen, die sicherstellt, dass alle notfallrelevanten Informationssysteme in Notfallübungen periodisch zu berücksichtigen sind.

Die Detailplanung und Durchführung von Notfallübungen für die Lotus Notes/Domino-Umgebung sollten auf Notfallszenarien fokussieren, die die Spezifika der Lotus Notes/Domino-Plattform beinhalten (z. B. Kompromittierung der Zertifikatshierarchie von Notes, Korruption der Replikationsmechanismen von Lotus Notes/Domino u. ä.).

Bei der Planung und Durchführung von Notfallübungen sind immer auch die Risiken zu betrachten, die bei der Durchführung von Notfallübungen entstehen können. Es ist daher empfehlenswert zunächst Notfallübungen im kleinen Rahmen durchzuführen und später größere Notfallszenarien zu üben. Insbesondere die Szenarien, wie z. B. die Wiederherstellung korrupter Lotus Notes/Domino-Datenbanken über Reparatur oder die Rücksicherung oder Wiederherstellung übergreifender Datenbankkonsistenz bei Korruption der Replikationsmechanismen sind mit entsprechender Vorsicht im Rahmen von Notfallübungen abzuarbeiten.

Weitere realistische Szenarien für Notfallübungen für die Lotus Notes/Domino-Umgebung sind Denial-of-Service-Angriffe gegen E-Mail- oder Web-Dienste bzw. Kompromittierung der Umgebung durch Nutzung von Schwachstellen eines im Internet angebotenen Dienstes.

Die Durchführung der Notfallübungen ist zu dokumentieren, und die Erkenntnisse aus der Übung müssen in die Verbesserung der Notfallplanung und des Betriebs einfließen.

Prüffragen:

- Ist ein ausreichend detaillierter Notfallplan für die Lotus Notes/Domino-Umgebung vorhanden?
- Berücksichtigt die Notfallplanung für die Lotus Notes/Domino-Umgebung die technischen Gegebenheiten der aktuell eingesetzten Version?
- Sind die betrachteten Notfallszenarien für die Lotus Notes/Domino-Umgebung plausibel und realistisch?
- Wenn DAOS verwendet wird, ist dies in der Notfallplanung berücksichtigt?
- Wurden für die Lotus Notes/Domino-Umgebung Notfallübungen geplant bzw. durchgeführt, die die Spezifika der Plattform berücksichtigen?

# M 6.74 Notfallarchiv

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Ein Notfallarchiv enthält diejenigen Sicherungsdaten, mit denen das Gesamtsystem in sich konsistent wiederhergestellt werden kann.

Keinesfalls darf dieser Datensicherungsbestand aus der gleichen Schadensursache heraus untergehen wie die Produktionsdaten. Er muss auch nach einem Katastrophen-Fall verfügbar bzw. zugänglich sein, d. h., der Zugriff auf die Backup-Datenträger und ihr Transport muss zeitlich in das Fenster passen, das als Rahmen für den Wiederanlauf planmäßig zur Verfügung steht. Die Unterbringung in einem Datenträgersafe oder einem Datenträgersicherheitsarchiv allein ist nicht ausreichend, da

- der Zugang beispielsweise durch Schutt verwehrt sein könnte,
- die vom Schaden betroffene Lokation durch die Feuerwehr oder ermittelnde Stellen für mehrere Tage gesperrt werden könnten oder
- ein Betreten schlichtweg nicht mehr möglich sein kann, beispielsweise aufgrund beeinträchtigter Statik.

Um diese Probleme zu lösen, sollten die Backup-Datenträger ausgelagert werden.

Hier kommen folgende Möglichkeiten in Betracht:

- In einem anderen Bauteil (in der Regel zwei Brandabschnitte entfernt) oder in einem anderen Gebäude kann ein Notfallarchiv eingerichtet werden. Die Datenträger mit den Sicherungen müssen dann zeitnah dorthin transportiert werden. Die dort gelagerten Datensicherungen müssen außerdem gegen unberechtigten Zugriff und vor Sabotage geschützt werden. Je nach Risikolage muss auch an den Schutz vor Feuer, Brandgasen, Wasser und die Zerstörung durch Magnetfelder gedacht werden. Daher kommt eine Unterbringung in einem Datensafe einer geeigneten Klasse oder einem Datenträgersicherungsarchiv in Frage.
- Es werden keine Datenträger zum Auslagerungsort transportiert, stattdessen wird die Datensicherung über Kommunikationsstrecken entweder in ein Roboterarchiv oder auf entfernt unterhaltene gespiegelte Plattenbestände übertragen. Für große Datenvolumina bieten sich hierzu Lichtwellenleiter an, die eine hohe Datenrate und lange Verbindungsstrecken erlauben. Um die Verfügbarkeit zusätzlich zu erhöhen, sollten bei dieser Lösung redundante Leitungswege in Betracht gezogen werden (siehe auch M 6.18 *Redundante Leitungsführung*).

Der Betrieb eines Notfallsarchivs kann auch von externen Dienstleistern übernommen werden, die sowohl den Datentransfer als auch die Datenspeicherung anbieten. Für den Notfall stellen diese Unternehmen auch bei Bedarf Hardware-Komponenten zur kurzfristigen Übernahme der Informationsverarbeitung zur Verfügung. Bei der Wahl externer Dienstleister müssen mit diesen genaue Vereinbarungen und Regelungen über den Leistungsumfang und die zu beachteten Sicherheitsmaßnahmen getroffen werden (siehe M 5.87 *Vereinbarung über die Anbindung an Netze Dritter*).

Prüffragen:

- Ist sichergestellt, dass der Datensicherungsbestand des Notfallarchivs nicht durch die gleiche Schadensursache wie die Produktionsdaten gefährdet ist?

# M 6.75 Redundante Kommunikationsverbindungen

**Verantwortlich für Initiierung:** IS-Management-Team, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Je nach Anforderungen an die Verfügbarkeit kann der Ausfall oder das Nichtzustandekommen von Kommunikationsverbindungen zu erheblichen Beeinträchtigungen führen. Dies gilt sowohl für Telefon- wie LAN- oder WAN-Verbindungen. Die Fehlerquellen können dabei sehr vielfältig sein, so dass sich die Ursachenforschung oft als sehr schwierig erweist.

Da die typischen Arbeitsumgebung immer stärker vernetzt wird, kann der Ausfall von Kommunikationsverbindungen dazu führen, dass wichtige Daten und Informationen nicht ausgetauscht werden können. Dadurch werden unter Umständen Arbeitsabläufe unterbrochen, bis die Verbindung wieder zustande kommt oder bis Ausweichlösungen gefunden werden konnten.

Daher ist es sinnvoll, für die verschiedenen Kommunikationsverbindungen Ausweichlösungen bereitzuhalten (abhängig von deren Schutzbedarf).

**Beispiele:**
- Die telefonische Anbindung einer Einsatzzentrale sollte nicht nur über Festnetz, sondern auch über ein Mobiltelefon gewährleistet sein.
- Für die Anbindung des E-Mail-Servers an die Außenwelt sollte neben dem normalen Internet-Provider ein zweiter vorgesehen sein.
- Neben der E-Mail-Anbindung bzw. neben einem Faxserver sollte auch ein Faxgerät vorhanden sein, für den Fall, dass die Netzanbindung oder der Server ausfällt.

Dabei muss nicht immer ein weiterer Anschluss mit derselben Bandbreite und denselben Qualitätsanforderungen vorgehalten werden. In vielen Fällen reicht es, für den Notfall einen eingeschränkten IT-Betrieb aufrechterhalten zu können (siehe dazu auch Baustein B 1.3 *Notfallmanagement*).

Prüffragen:

- Bestehen für wichtige Netz-Verbindungen entsprechende Ausweichlösungen zur Kommunikation?
- Entsprechen die Ausweichlösungen den technischen Sicherheitsvorgaben der Organisation?

# M 6.76 Erstellen eines Notfallplans für den Ausfall von Windows-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Der Ausfall von einem oder mehreren Windows-Systemen kann bei entsprechender Aufgabe des Windows-Systems gravierende Auswirkungen auf die IT-Umgebung haben, da Benutzer nicht auf die Funktionalitäten zugreifen können, die das Windows-System bereitstellt. Es ist festzulegen, welche Maßnahmen zu treffen sind, um eine Notfallsituation zu vermeiden, die Folgen des Ausfalls zu minimieren und den schnellen, erfolgreichen Wiederanlauf zu gewährleisten. Die bei einem Ausfall (des Servers) benötigten Dokumentationen und Handlungsanweisungen können schützenswerte Informationen enthalten. Sie sind sicher aufzubewahren, um dem Missbrauch der Informationen vorzubeugen. Schützenswerte Informationen können zum Beispiel sein:

- Konfigurationsdaten,
- Lizenzschlüssel, gegebenenfalls Volumenlizenz-Datenträger,
- (administrative) Benutzerkonten und Kennwörter und
- sonstige vertrauliche Informationen, wie z. B. Schlüsselmaterial für die Festplatten-, Netz- oder E-Mail-Verschlüsselung.

Gleichzeitig muss organisatorisch gewährleistet werden, dass diese Informationen bei einem Ausfall den Personen zur Verfügung stehen, die für die Wiederherstellung verantwortlich sind. Der Notfallplan für Windows- Systeme muss in das Notfallkonzept integriert werden (siehe B 1.3 *Notfallmanagement*) und M 6.96 *Notfallvorsorge für einen Server* kompatibel sein.

Die Notfallplanung sollte bereits in die Planung der Systeme einbezogen werden, da bestimmte Verfügbarkeitsvorgaben, die beispielsweise Redundanz erforderlich machen, frühzeitig beachtet werden müssen (siehe M 6.1 *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*). Im Notfallplan sollten eindeutige Kriterien niedergelegt sein, für welche Windows-Systeme der Notfallplan angewendet werden soll.

**Datensicherung**

Im Notfallplan für Windows-Systeme ist darauf hinzuweisen, dass die Umsetzung der Maßnahmen aus B 1.4 *Datensicherungskonzept* für die Bewältigung eines Notfalls realisiert sein muss. Bei Server-Systemen ist auf die Umsetzung von M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server* zu achten.

Die Dokumentation zur Datensicherung ist für den Notfallplan von besonderer Bedeutung. Die Aktualität sollte regelmäßig im Rahmen von Wartungsarbeiten oder Audits überprüft werden. Insbesondere muss der Dokumentation zu entnehmen sein, welchen Umfang die Datensicherung hat, wann die letzte erfolgreiche Datensicherung erstellt wurde und welche Soft- und Hardware für die Datensicherung verwendet wurde.

Das gewählte Datensicherungsverfahren und die dafür verwendete Hard- und Software müssen den Anforderungen an eine Wiederherstellung innerhalb der geforderten Wiederherstellungszeit entsprechen.

**Technische Dokumentation**

Bei einem Ausfall muss eine angemessene technische Dokumentation der Systeme vorliegen. Sie sollte mindestens folgende Punkte enthalten:

- BIOS- und Firmware-Versionen
- Hardwareausstattung
- installierte Windows-Komponenten
- installierte Zusatz-Software
- Netzkonfiguration (siehe *Eigenschaften* der LAN-Verbindungen, zu finden im Netzwerk- und Freigabecenter in der Systemsteuerung)
- Dienste (siehe Dienstekonsole)
- Partitionierung der Festplatten oder des angeschlossenen Festplatten-Systems
- Benutzerkonten und Gruppen mit Berechtigungen
- Freigaben und Freigabeberechtigungen, NTFS-Berechtigungen
- Einstellungen in den Sicherheitsrichtlinien (mittels Vorlagen)

Grundsätzlich sollten im Rahmen der Notfallplanung alle Dokumentationsunterlagen berücksichtigt und gegebenenfalls vervollständigt werden, damit im Notfall keine wichtige Funktionen vergessen werden. Die Dokumentation ist zum Beispiel bei Wartungsarbeiten und bei Veränderungen an Hard- und Software sowie der Systemkonfiguration anzupassen.

Die Aktualisierung der technischen Dokumentation und damit auch des Notfallplans ist Teil des Änderungsmanagements. Es sollte erkennbar sein, durch welche Person Änderungen durchgeführt wurden und wer die Dokumentation aktualisiert hat. Für den Notfallplan müssen alle Dokumentationen vorhanden und lesbar sein.

**Ausweichbetrieb**

Können nur kurze Ausfallzeiten toleriert werden, so ist ein Ausweichbetrieb zu ermöglichen. Beim Ausfall eines einzelnen Systems sollte die Kapazitätsplanung für die Gesamtheit der Systeme so gestaltet sein, dass andere in Betrieb befindliche Systeme die Rollen und Funktionen des ausgefallenen Systems weitgehend übernehmen können. Hierbei ist M 4.276 *Planung des Einsatzes von Windows Server 2003* bzw. M 4.418 *Planung des Einsatzes von Windows Server 2008* oder M 4.420 *Sicherer Einsatz des Wartungscenters unter Windows 7* Sicherer Einsatz des Wartungscenters ab Windows 7 zu beachten.

Für Windows-Server sollte die Beschaffung von Ersatzgeräten überlegt werden, deren Ausstattung den Betrieb eines Windows-Servers inklusive einiger Anwendungen zulässt, falls mehrere Server ausfallen. Um die Umschaltzeit zu minimieren, sollten diese Geräte vorinstalliert und regelmäßig hochgefahren und gewartet werden. Dies gilt bei Einsatz von Windows-Clients ab Vista und Windows-Servern ab Windows Server 2008 auch für die Geräte mit einem KMS (Key Management Service) oder einem MAK-Proxy (Multi Activation Key Proxy), wenn diese Formen der Aktivierung für Volumenlizenzen eingesetzt werden.

Die Entwicklung von Ausweichszenarien kann hohen Aufwand erzeugen. Es empfiehlt sich, Ausweichszenarien schon in der Planungsphase für den Einsatz des Servers zu berücksichtigen. Es sollten konkrete Handlungsanweisungen für die Aufnahme des Ausweichbetriebs vorliegen.

**Wiederanlaufplan**

In Abhängigkeit von der Serverrolle und der IT-Umgebung ergeben sich nach einem Ausfall für das Wiederanlaufen bestimmte Anforderungen an Windows-Systeme. Hierbei sind neben dem betrachteten Server auch Anlaufzeiten der angebundenen IT-Umgebung zu beachten (z. B. Router, andere Server, Standortkonnektoren). Ein Anlaufplan wird mit zunehmender Größe des Informationsverbunds komplexer und muss individuell in Abhängigkeit von der Domänenstruktur und den verwendeten Serverrollen erstellt werden. Ein Mitgliedsserver sollte erst neu gestartet werden, nachdem mindestens ein Domänencontroller mit globalem Katalog, ein Zertifikatsserver zum Abrufen von Zertifikatssperrlisten (falls vorhanden) und alle Infrastrukturserver gestartet sind.

**Test des Notfallplans**

Im Rahmen des Wartungsplans sollte der Notfallplan regelmäßig (z. B. einmal pro Quartal) in einer Testumgebung, aber auch gelegentlich, mit besonderer Vorsicht, in der Produktivumgebung getestet werden. Je häufiger Konfigurationsänderungen zu erwarten sind, desto häufiger sollten Tests durchgeführt werden, um die Aktualität des Notfallplans sicherzustellen. Die Ergebnisse müssen dokumentiert werden und führen gegebenenfalls zu Änderungen am bestehenden Notfallplan. Grundsätzlich sind Wiederherstellungsszenarien zu proben und die Ergebnisse zu dokumentieren (siehe M 6.41 *Übungen zur Datenrekonstruktion*).

**Wiederherstellung**

Im Notfallplan sind die notwendigen Voraussetzungen zur Wiederherstellung durch Neuinstallation festzuhalten. Das Bereitstellungskonzept oder vorhandene Installationskonzepte (im Falle eines Windows Server 2003 Systems M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003*) sind zu berücksichtigen. Dies gilt bei Einsatz von Windows-Clients ab Windows Vista und Windows-Server ab Windows Server 2008 auch für die Geräte mit einem KMS (Key Management Service) oder einem MAK-Proxy (Multi Activation Key Proxy), wenn diese Formen der Aktivierung für Volumenlizenzen eingesetzt werden (siehe hierzu M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* und M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag*). Kritisch sind unter anderem notwendige Treiber für die einzusetzende Hardware. Es kann bei bestimmten RAID-Controllern erforderlich werden, während der Installation Treiber zu installieren. In der Regel werden hierfür vom Hersteller Treiber auf einem Datenträger mitgeliefert oder im Internet auf den Herstellerseiten bereitgestellt. Eine aktuelle Version dieses Treibers muss auf einem Datenträger vorliegen.

Für die Wiederherstellung müssen die Originalsoftware mit den Originaldatenträgern inklusive Produktschlüssel sowie Lizenzinformationen vorhanden sein. Falls kein Volumenlizenzprogramm verwendet wird, ist hinsichtlich der möglicherweise erforderlichen Aktivierung von Windows-Systemen darauf hinzuweisen, dass mehrfache Aktivierungen per Internet mit Hilfe desselben Produktschlüssels auf verschiedenen Festplatten fehlschlagen können. Infolgedessen kann der direkte telefonische Kontakt mit Microsoft erforderlich werden. Microsoft ist dann auf den Systemausfall hinzuweisen.

Bei Einsatz von Windows ab Windows Vista ist auch bei Nutzung von Volumenlizenzen eine erneute Aktivierung der Windows-Clients erforderlich.

Auf die Verfügbarkeit einer stets ausreichenden Anzahl von Lizenzen muss bei der Nutzung von Windows-Clients ab Windows Vista geachtet werden. Bei einer Neuinstallation und einer automatischen Aktivierung über einen MAK-Proxy oder KMS werden durch die Windows-Clients zunächst Lizenzen angefordert. Durch ein Lizenzmanagement muss sicher gestellt werden, dass die benötigte Anzahl von Lizenzen für eine Aktivierung vorhanden ist. Weitere Informationen zur Aktivierung sind in M 4.336 *Aktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* und M 4.343 *Reaktivierung von Windows-Systemen ab Vista bzw. Server 2008 aus einem Volumenlizenzvertrag* zu finden.Die Wiederherstellungsschlüssel der Festplattenverschlüsselung müssen bei Bedarf kurzfristig zur Verfügung gestellt werden können. Bei der Übermittlung muss eine unbefugte Kenntnisnahme ausgeschlossen werden.

Die vorhandenen Authentisierungsmittel und Wiederherstellungsschlüssel für eine vorhandene Festplattenverschlüsselung werden bei einer Neuinstallation der Systeme in der Regel ungültig. Für neu erstellte Authentisierungsmittel und Wiederherstellungsschlüssel muss sicher gestellt werden, dass nur Befugte Zugang dazu haben (siehe M 4.337 *Einsatz von BitLocker Drive Encryption*).

Windows 8 unterstützt die Generierung, Speicherung und Nutzung von kryptographischen Schlüsseln und Zertifikaten mit einem Trusted Platform Module (TPM), also einem in den Rechner eingebauten Kryptochip. Die hier gespeicherten kryptographischen Informationen werden durch übliche Datensicherungsverfahren nicht erfasst. Für die Notfallplanung ist daher zu prüfen, welche kryptographischen Daten im TPM gespeichert werden, und wie diese wiederhergestellt oder neu generiert werden können.

Durch das Anlegen von Replikaten wichtiger Informationen und Dateien auf mehreren Servern kann beim Ausfall einzelner Server auf diese Replikate zugegriffen werden. Damit ist es möglich, Benutzern kurzfristig eine Kopie von Daten anzubieten. Im Rahmen der Notfallplanung sollte geprüft werden, ob und für welche Daten dies notwendig ist. Windows-Server bieten dazu den *File Replication Service* (FRS) an, der auch in Verbindung mit dem DFS (*Distributed File System*) genutzt werden kann. In den Server-Versionen vor Windows Server 2003 R2 sind diese Dienste jedoch nur eingeschränkt für ein Notfallkonzept geeignet und meist mit hohem Aufwand für Test und Wartung verbunden.

Die Notfallplanung ist im Hinblick auf bestimmte Rollen von Windows-Systemen, zum Beispiel DNS-Server und Zertifikatsserver, zu differenzieren, um die vollständige Wiederherstellung gewährleisten zu können. Dazu gehört die Sicherung von rollenspezifischen Systemkomponenten (z. B. Datenbanken des DNS-Dienstes oder der Zertifizierungsstelle) sowie eine umfassende Dokumentation der mit den betreffenden Rollen verbundenen Einstellungen.

Prüffragen:

- Haben die Personen, die für die Wiederherstellung verantwortlich sind, bei einem Ausfall des IT-Systems Zugriff auf alle notwendigen Informationen wie Konfigurationsdaten, Lizenzschlüssel, administrative Benutzerkonten und Kennwörter?
- Existiert ein Notfallplan, und ist er Bestandteil des Notfallkonzeptes der Institution?
- Bei der Verwendung von Ausweichsystemen: Ist die Kapazität der Gesamtheit der Systeme bei einer möglichen Übernahme von Rollen und Funktionen ausreichend, um die ausgefallenen Systeme abzudecken?

- Ist die Aktualität des Notfallplans auch nach Konfigurationsänderungen sichergestellt?
- Sind im Notfallplan die notwendigen Voraussetzungen zur Wiederherstellung durch Neuinstallation festgehalten?
- Wird für die Systemwiederherstellung das vorhandene Bereitstellungs- bzw. Installationskonzept berücksichtigt?
- Ist die vollständige Wiederherstellung von rollenspezifischen Systemkomponenten gewährleistet, und sind die mit den Rollen verbundenen Einstellungen dokumentiert?
- Sind kryptographische Schlüssel und Zertifikate, insbesondere bei der Speicherung im TPM und beim Einsatz einer Festplattenverschlüsselung, in der Notfallplanung geeignet berücksichtigt?
- Sind die für eine Neuinstallation notwendigen Installationsdatenträger und Produktschlüssel vorhanden?
- Sind die notwendigen Dokumentationen und Handlungsanweisungen vor unbefugtem Zugriff geschützt?
- Ist eine aktuelle Dokumentation der Datensicherung vorhanden?
- Entsprechen das gewählte Datensicherungsverfahren und die dafür verwendete Hard- und Software den Anforderungen an eine Wiederherstellung innerhalb der geforderten Wiederherstellungszeit?

# M 6.77 Erstellung von Rettungsdisketten für Windows 2000

Diese Maßnahme ist 2013 mit der 13. Ergänzungslieferung entfallen.

# M 6.78 Datensicherung unter Windows Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Benutzer

Unter Windows 2000 und Windows XP kann die Datensicherung mit dem zum System gehörenden Dienstprogramm *NTBACKUP.EXE* durchgeführt werden. Dabei ist zu beachten, dass dieses Programm nicht in der Lage ist, die Sicherungsmedien generell zu verschlüsseln, so dass diese geschützt aufbewahrt werden müssen. Über EFS verschlüsselte Dateien werden jedoch verschlüsselt gesichert. Datensicherungen, die mit NTBACKUP.EXE durchgeführt wurden, müssen daher vor unbefugtem Zugriff geschützt aufbewahrt werden. Im Unterschied zur in Windows NT mitausgelieferten Version, unterstützt das Backup-Programm auch die Sicherung der Daten in eine Datei, so dass z. B. lokale Dateien in eine Datei auf einen Server geschrieben werden können, von wo aus sie dann durch die Serversicherung auf ein Backup-Medium geschrieben werden.

Bei einer Standardinstallation von Windows Vista steht *NTBACKUP.EXE* nicht zur Verfügung. *NTBACKUP.EXE* kann aber auch unter Windows Vista genutzt werden, etwa um alte Datensicherungen von Windows XP-Systemen rückzusichern. *NTBACKUP.EXE* wird von Microsoft zum Download bereitgestellt. Vor der Installation von *NTBACKUP.EXE* muss die Wechselmedienverwaltung unter *Systemsteuerung* | *Programme* | *Windows-Funktionen ein- oder ausschalten* aktiviert werden.

In der Standardinstallation bietet Windows Vista unter Systemsteuerung | *System und Wartung* | *Sichern und Wiederherstellung* die Sicherung einzelner Dateien und mittels *Windows Complete PC-Sicherungsabbild* das Erstellen von Images von Partitionen an. Das Erstellen eines *Windows Complete PC-Sicherungsabbild* kann auch mit dem Kommandozeilenwerkzeug *wbadmin* durchgeführt werden. Bei der Sicherung einzelner Dateien unterstützt Windows Vista nur die Dateitypen Bilder, Musik, Videos, E-Mail, Dokumente, TV-Sendungen, Komprimierte Dateien und Zusätzliche Dateien. Windows Vista unterstützt nicht die Sicherung der Dateien des Dateityps:

- Systemdateien,
- Programmdateien,
- Dateien auf FAT-formatierten Festplatten,
- Dateien im Papierkorb,
- Temporäre Dateien und
- Benutzerprofileinstellungen

Die Sicherung der Dateien des Dateityps EFS-verschlüsselte Dateien wird unter Windows Vista erst ab Service Pack 1 unterstützt. Für die Sicherung einzelner Dateien oder das Erstellen eines *Windows Complete PC-Sicherungsabbild* unterstützt Windows Vista die Zielorte Festplatte (intern oder extern), Wechseldatenträger wie DVD und CD sowie Netzwerkressourcen.

Bei der Durchführung der Datensicherung sind die folgenden Punkte zu beachten:

- Es ist festzulegen, wann und wie oft auf den Windows-Clients Datensicherungen durchgeführt werden sollen.
- Die Sicherungssoftware ist in der Lage, wichtige Systemdateien, wie die Registry des lokalen Rechners, die COM+ Registrierungen sowie die Startdateien und die Systempartition zu sichern. Dies sollte in regelmäßi-

gen Abständen und nach größeren Änderungen der Konfiguration durchgeführt werden. Dazu sind unter der Option *Systemstatus* die jeweiligen Auswahlboxen zu aktivieren.
- Auf Domänen-Controllern können zusätzlich auch die Active Directory Daten sowie die Daten des SYSVOL-Ordners gesichert werden. Dies sollte bei jedem Backup durchgeführt werden. Die relevanten Optionen sind auf Domänen-Controllern ebenfalls unter der Option *Systemstatus* zu finden.
- Bei der Durchführung der Sicherung sollte unbedingt eine Protokolldatei angelegt werden. Nach Abschluss der Operation ist die Protokolldatei daraufhin zu überprüfen, ob alle zu sichernden Daten auch tatsächlich gesichert werden konnten oder ob während der Sicherung Fehler aufgetreten sind. Dabei ist es empfehlenswert, die Option *Details* unter *Extras / Optionen / Sicherungsprotokoll* zu aktivieren, da damit auch festgestellt werden kann, ob alle zu sichernden Daten gesichert wurden und ob die Verzeichnisse in die Datensicherung einbezogen wurden, die gesichert werden sollten.
- Bei der Wiederherstellung gesicherter Dateien kann deren Zugriffsschutz wiederhergestellt werden, sofern dies in den Eigenschaften des Wiederherstellungsauftrages (Schaltfläche *Wiederherstellung starten / Erweitert*) spezifiziert wurde. Standardmäßig ist diese Option aktiviert. Dies kann nur für Daten erfolgen, die von einem Windows NTFS-Dateisystem stammen.
- Die Auswahl der zu sichernden Dateien und Verzeichnisse kann, im Gegensatz zur Windows NT Version des Programms, in einer Datei gespeichert werden, die später wieder geladen werden kann. Durch diesen Mechanismus ist es auch möglich, mehrere Sicherungsvarianten zu erzeugen, durch die unterschiedliche Daten erfasst werden.
- Sicherungen sollten in regelmäßigen Abständen durchgeführt werden. Mit dem Backup-Programm *NTBACKUP.EXE* ist es möglich, Sicherungsaufträge für bestimmte Zeiten zu planen. Damit kann die Sicherung auch automatisiert erfolgen.

**Systemwiederherstellung**

Die Systemwiederherstellung wurde in Windows XP eingeführt und stellt eine neue Funktionalität dar, die das Wiederherstellen von alten Systemzuständen möglich macht. Die Systemwiederherstellung erstellt einen Zustandsschnapp-schuss wichtiger Systemdateien und einiger Programmdateien. Dieser bildet einen Wiederherstellungspunkt, auf welchen das System später zurückgesetzt werden kann. Wiederherstellungspunkte werden durch Windows zum Beispiel vor dem automatischen Einspielen von Patches gesetzt. Der Einsatz der automatischen Systemwiederherstellung kann in Abhängigkeit von lokalen Umständen und insbesondere von der implementierten Softwareverteilungs-Strategie vorteilhaft sein. Wiederherstellungspunkte können bei Bedarf auch manuell durch einen Administrator gesetzt werden, z. B. vor der Installation von Software.

**Anforderung an Sicherungssoftware**

Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, so ist bei der Auswahl derartiger Sicherungssoftware darauf zu achten, dass sie die folgenden Anforderungen erfüllt:

- Die eingesetzten Dateisysteme, also FAT, NTFS und ggf. auch HPFS, sollten bei der Sicherung und Wiederherstellung unterstützt werden.
- Es muss möglich sein, auch Active Directory Daten sowie die Daten des SYSVOL-Ordners zu sichern.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu

manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren.
- Die Sicherungssoftware sollte den Schutz des Backup-Mediums durch ein Passwort oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien, sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherung sollte auf optische Datenträger wie DVDs sowie auf Festplatten, USB-Laufwerke und Netzlaufwerke erfolgen können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte ausgewählt werden können, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist.
  Dabei sollte einstellbar sein, ob diese Datei immer, nie oder nur in dem Fall überschrieben wird, dass sie älter als die zu rekonstruierende Datei ist, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Zusätzlich zur Durchführung der normalen Datensicherungen ist es unter Windows 2000 empfehlenswert, die aktuelle Systemkonfiguration nach jeder größeren Änderung auf eine Notfalldiskette zu sichern, um sie bei eventuellen Inkonsistenzen wiederherstellen zu können (siehe auch M 6.77 *Erstellung von Rettungsdisketten für Windows 2000*). Der Mechanismus der Notfalldisketten steht für Windows XP und Windows Vista nicht mehr zur Verfügung. Stattdessen kann zur Systemwiederherstellung unter Windows XP und Windows Vista die Wiederherstellungskonsole (Recovery Console) verwendet werden. Die Wiederherstellungskonsole kann entweder von der Installations-CD oder -DVD bzw. den Installations-Disketten gestartet oder in das System integriert werden, so dass es beim Systemstart als Boot-Option angeboten wird. Da die Wiederherstellungskonsole ein mächtiges Werkzeug ist, muss ihr Einsatz durch die entsprechende Einstellung des BIOS bzw. durch die Definition der Wiederherstellungskonsole-Richtlinien (siehe M 4.244 *Sichere Systemkonfiguration von Windows Client-Betriebssystemen*) eingeschränkt werden.

Prüffragen:

- Werden Datensicherungen, die mit dem Dienstprogramm NTBACKUP.EXE durchgeführt worden sind, geschützt aufbewahrt?
- Gibt es Richtlinien wann und wie oft eine Datensicherung unter Windows durchgeführt werden soll?

- Wird bei der Durchführung der Sicherung eine Protokolldatei angelegt?
- Wird diese Protokolldatei nach Abschluss der Sicherung auf Fehler und Auffälligkeiten überprüft?
- Wird der Datensicherungsvorgang dokumentiert?
- Wurden die Anforderungen für die Beschaffung einer Sicherungssoftware definiert?
- Werden bei der Wiederherstellung der Daten die Zugriffsrechte wieder hergestellt?

# M 6.79 Datensicherung beim Einsatz von Internet-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Internet-PCs können in unterschiedlichen Einsatzszenarien verwendet werden. Einerseits können Internet-PCs als Ergänzung zu anderen Zugriffsmöglichkeiten auf das Internet installiert werden, z. B. wenn am Arbeitsplatz-PC zwar ein Internet-Zugang vorhanden ist, aus Sicherheitsgründen jedoch keine aktiven Inhalte wie JavaScript ausgeführt werden dürfen. Andererseits stellen Internet-PCs in vielen Fällen die einzige Möglichkeit dar, das World Wide Web, E-Mail oder andere Internet-Dienste zu nutzen.

Aus diesen Einsatzszenarien ergeben sich auch unterschiedliche Anforderungen an die Verfügbarkeit von Internet-PCs. Hohen oder sehr hohen Verfügbarkeitsanforderungen kann unter anderem durch redundante Auslegung des Internet-PCs und der Internet-Anbindung Rechnung getragen werden. Um bei einem Ausfall des Internet-PCs, z. B. durch technisches Versagen oder durch einen erfolgreichen Angriff, das System zeitnah wiederherstellen zu können, sollte auf jeden Fall ein Konzept für die Datensicherung erstellt werden. Dabei muss unterschieden werden zwischen den System-, Programm- und Konfigurationsdateien einerseits und den Anwendungsdaten andererseits.

**Backup der System-, Programm- und Konfigurationsdateien**

Um den Internet-PC nach einem Ausfall möglichst schnell wiederherstellen zu können, sollte nach der Installation aller benötigten Betriebssystem- und Software-Komponenten und anschließender Konfiguration ein Abbild ("Image") des Systems gespeichert werden.

Hierzu werden entweder alle System-, Programm- und Konfigurationsdateien mit Hilfe eines Backup-Programms gesichert, oder es wird ein spezielles Tool eingesetzt, das den gesamten Inhalt der Festplatte Byte für Byte abspeichert. Im letztgenannten Fall sollten sich währenddessen keine Anwendungsdaten auf der Festplatte befinden.

Es wird empfohlen, ein Image des Systems zu sichern,

- erstmalig, sobald die Installation und Konfiguration des Internet-PCs abgeschlossen ist,
- jedes Mal, wenn Betriebssystem- oder Software-Komponenten installiert, entfernt oder aktualisiert wurden, beispielsweise durch die Installation von Patches,
- jedes Mal, wenn wesentliche oder sicherheitsrelevante Änderungen an der Konfiguration vorgenommen wurden.

Dadurch wird vermieden, dass nach einem Ausfall des Internet-PCs alle Software-Komponenten einzeln installiert und konfiguriert werden müssen. Stattdessen kann das System als Ganzes wiederhergestellt werden.

**Backup der Anwendungsdaten**

Wenn das Nutzungskonzept eine lokale Datenhaltung vorsieht, müssen außer dem System auch die Anwendungsdaten *regelmäßig* gesichert werden.

Hierzu wird empfohlen, auf dem Internet-PC ein oder mehrere Verzeichnisse festzulegen, in denen Anwendungsdateien gespeichert werden dürfen. Der In-

halt dieser Verzeichnisse wird in das Backup einbezogen. Die Benutzer müssen darüber unterrichtet werden, welche Verzeichnisse gesichert werden, und wie sie Dateien dort abspeichern können.

Die zu sichernden Anwendungsdaten können u. U. schnell anwachsen. Im Datensicherungskonzept ist daher auch festzulegen, welche Volumenbeschränkungen es für das Backup gibt und wie bei Überschreitung vorzugehen ist.

**Datensicherungskonzept**

Die Vorgehensweise zur Datensicherung sollte in einem Konzept dokumentiert werden. Das Konzept sollte mindestens folgende Punkte umfassen:

- Umfang der Datensicherung (Verzeichnisse, Partitionen, usw.),
- Häufigkeit und Zeitpunkt der Datensicherung,
- Datensicherungsmedium,
- Verantwortlichkeit für die Datensicherung und
- Aufbewahrungsort der Backup-Datenträger.

Das Datensicherungskonzept muss allen Benutzern des Internet-PCs zur Kenntnis gegeben werden. Weitere Empfehlungen zur Entwicklung eines Datensicherungskonzepts finden sich in Maßnahme M 6.33 *Entwicklung eines Datensicherungskonzepts*.

**Beispiele:**

- Szenario 1:
  Der Internet-PC wird in einem Unternehmen als Zusatzangebot zur Verfügung gestellt, da beim Surfen über das Hausnetz keine aktiven Inhalte ausgeführt werden dürfen. Das System wird mit Hilfe eines Image wöchentlich neu installiert. Die Benutzer sind darüber informiert, dass sie Anwendungsdaten auf dem Internet-PC selbst sichern müssen, wenn sie diese weiter benötigen.
- Szenario 2:
  Das Hausnetz in einem Unternehmen ist nicht an das Internet angeschlossen. Es werden daher mehrere Internet-PCs für die Nutzung von E-Mail installiert und untereinander vernetzt. Ein- und ausgehende E-Mails werden täglich über einen CD-Writer gesichert, der in einen der Internet-PCs eingebaut ist. Ein Administrator und ein Vertreter sind dafür verantwortlich, entsprechende CD-R- bzw. CD-RW-Medien einzulegen und die Datensicherung zu starten.

Prüffragen:

- Wird nach Installation und Konfiguration von Internet-PCs ein Abbild (Image) des Systems erstellt?
- Werden die Anwendungsdaten von Internet-PCs regelmäßig gesichert, sofern das Nutzungskonzept eine lokale Datenhaltung vorsieht?
- Existiert ein Konzept für die Datensicherung von Internet-PCs?
- Ist das Datensicherungskonzept allen Benutzern von Internet-PCs bekannt?

# M 6.80 Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes

Diese Maßnahme ist 2008 mit der 10. Ergänzungslieferung entfallen.

# M 6.81 Erstellen von Datensicherungen für Novell eDirectory

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Datensicherung eines eDirectory-Verzeichnisdienstes sollte zusammen mit einem generellen Server-Backup vorgenommen werden, damit später der Gesamtzustand der Server wiederhergestellt werden kann. Somit hängt der Backup-Prozess auch von dem unterliegenden Betriebssystem ab.

Um konsistente Datensicherungen des eDirectory-Datenbestandes auf einem Server zu erhalten, sollte ein spezielles Backup-Werkzeug verwendet werden. Folgende Werkzeuge hält eDirectory für die Datensicherung bereit:

- unter Netware: *SBCON.NLM*
- unter Windows NT/2000: *SMSENGN.EXE*
- unter Linux, Sun Solaris: *ndsbackup utility*

Neben einer Vollsicherung des Verzeichnisses bieten die Novell-Werkzeuge auch die Möglichkeit, nur Teile des eDirectory zu sichern. Um einzelne eDirectory-Objekte zu archivieren oder wiederherzustellen, muss der vollständige *distinguished name* des Objektes spezifiziert werden. Um den gesamten Baum zu sichern, muss das jeweilige *Tree*-Objekt angegeben werden. Es kann auch gesondert das Schema gesichert werden, hierzu muss das *Schema*-Objekt selektiert werden. Schließlich können auch Teile eines eDirectory-Baums gesichert werden, hierzu muss der entsprechende Container des Baumes ausgewählt werden. Es werden dann sämtliche Objekte unterhalb dieses Containers gesichert.

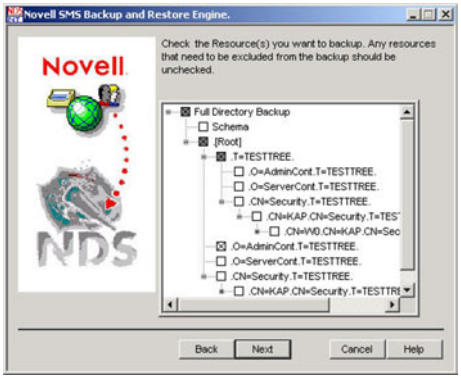



Abbildung: Novell SMS Backup and Restore Engine

Partitionsinformationen können mit diesen Backup-Werkzeugen nicht gesichert werden. Im Wiederherstellungsfall müssen die entsprechenden Teile dann nachträglich partitioniert werden. Zu diesem Zweck sollten unbedingt gedruckte Kopien der Baumstruktur und der Partitionen angefertigt und regelmäßig aktualisiert werden.

Der Backup-Prozess der eDirectory-Utilities kann an die Bedürfnisse der Benutzer angepasst werden. Insbesondere können mittels der Option *Exclude/Include* spezielle eDirectory-Objekte aus der Datensicherung ausgenommen bzw. darin einbezogen werden.

Sicherungskopien sollten in der Regel einmal wöchentlich oder öfter angelegt werden. Dies richtet sich danach, wie häufig sich wichtige Verzeichnisinforma-

tionen ändern. Der Backup-Prozess sollte stets nachvollziehbar protokolliert werden, und anhand des Protokolls sollte nachgeprüft werden, ob tatsächlich sämtliche Daten fehlerfrei gesichert wurden.

### Backup unter Netware

Teil des Netware-Betriebssystems ist *SBCON.NLM*, eine so genannte *Storage Management Engine* (SME). Sie stellt das Back-End dar, welches die Backup/Restore-Requests umsetzt. Vor der Nutzung von *SBCON.NLM* muss zuerst jedoch *QMAN.NLM* geladen werden, damit die von *SBCON.NLM* erzeugten Backup/Restore-Jobs verarbeitet werden können.

Alternativ dazu kann auch mit SMS-kompatiblen Backup/Restore-Utilities gearbeitet werden. Der *Storage Management Data Requester* (SMDR) kommuniziert zwischen der SME und der *Target Service Agent* (TSA)-Software. Das erste Mal, wenn *SMDR.NLM* geladen wird, wird der Benutzer nach diversen Konfigurationsoptionen gefragt, unter anderem, ob ein SMDR-Objekt im eDirectory-Verzeichnisbaum angelegt werden soll.

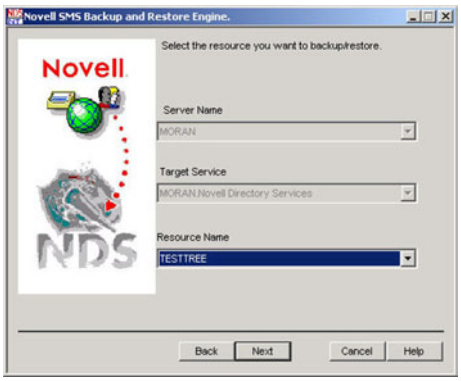



Abbildung: Ressource Name

Die SME und der TSA können sich auf dem selben oder auf verschiedenen Computern befinden. Im verteilten Fall muss auf beiden Seiten SMDR installiert sein. Die *Target Service Agents for NDS* (TSANDS) reichen die Requests zwischen dem SMDR und der eDirectory-Datenbank weiter.

### Backup unter Windows NT/2000

Von Novell wird für die Datensicherung unter Windows NT/2000 die Applikation *SMSENGN.EXE* zur Verfügung gestellt. *SMSENGN.EXE* erzeugt für Daten und Index jeweils eine Datei (*.DAT* beziehungsweise *.IDX*).

Alternativ kann auch hier ein SMS-kompatibles Backup/Restore-Werkzeug verwendet werden. Die oben beschriebenen Komponenten SMDR, TSA und TSANDS kommen dann analog zum Einsatz. Hierbei sind SMDR und TSANDS standardmäßig als NT-Services verfügbar. Sofern diese nicht aktiviert sind, können sie explizit mittels *W32MDR.EXE* unter dem NDS\SMS-Verzeichnis gestartet werden.

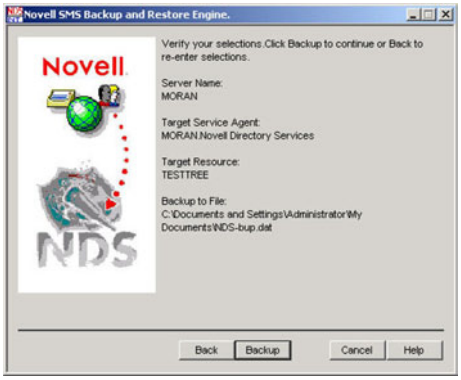



Abbildung: Verify Backup Einstellungen

**Backup unter Linux und Sun Solaris**

Unter Linux und Sun Solaris gibt es für die Datensicherung das Werkzeug *ndsbackup*. Dieses wird über die Kommandozeile gestartet und erlaubt es, eDirectory-Objekte in einer einzelnen Datei *ndsbackupfile* zu speichern. Um eDirectory-Objekte zu sichern, muss deren *full distinguished name* (FDN) spezifiziert werden. Um den gesamten Baum zu speichern, muss das entsprechende Baum-Objekt ausgewählt werden.

Auf der Kommandozeile akzeptiert das Tool eine Reihe von Funktionsbuchstaben, z. B. *c* für *create*, *r* für *restore*, etc., sowie einen Satz von Parametern. Einzelheiten sind dem Administrationshandbuch zu entnehmen.

Prüffragen:

- Erfolgt die Datensicherung eines eDirectory-Verzeichnisdienstes zusammen mit dem Server-Backup?
- Wird der Backup-Prozess nachvollziehbar protokolliert?
- Wird anhand des Backup-Protokolls nachgeprüft, ob tatsächlich sämtliche Daten fehlerfrei gesichert wurden?
- Werden gedruckte Kopien der Baumstruktur und der Partionen angefertigt und regelmäßig aktualisiert?

# M 6.82 Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen

Diese Maßnahme ist mit der 13. Ergänzungslieferung entfallen. Die Inhalte wurden in M 4.166 *Sicherer Betrieb von Exchange-Systemen* integriert.

# M 6.83 Notfallvorsorge beim Outsourcing

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Für die Notfallvorsorge beim Outsourcing gelten grundsätzlich die gleichen Anforderungen wie beim nicht ausgelagerten Betrieb von IT-Systemen. Die Besonderheiten beim Outsourcing-Betrieb ergeben sich dadurch, dass auch die Notfallvorsorge auf unterschiedliche Parteien aufgeteilt ist und durch die Verteilung der IT-Komponenten auch zusätzliche Komponenten neu hinzukommen.

Generell müssen Notfallvorsorgekonzepte für die Systeme beim Auftraggeber, beim Outsourcing-Dienstleister sowie für die Schnittstellen zwischen Auftraggeber und Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren. In M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* sind einige Hinweise gegeben, welche Aspekte bereits im Service Level Agreement geregelt werden sollten. Im Notfallvorsorgekonzept müssen diese Vorgaben genau spezifiziert und im Detail beschrieben werden:

- Zuständigkeiten, Ansprechpartnern und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
- Detailregelungen für die Datensicherung sind zu erstellen (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz).
- Detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen sind zu erstellen.
- Ein Konzept für Notfallübungen, die regelmäßig durchgeführt werden müssen, muss erarbeitet werden.

Die Informationssicherheit hängt in Notfällen entscheidend von der Qualität der Arbeitsanweisungen für das Personal des Outsourcing-Dienstleisters ab. Oftmals werden die Systeme des Auftraggebers von Personal des Dienstleisters betrieben, das keine Detailkenntnisse über die Anwendungen besitzt, die auf den IT-Systemen betrieben werden. Die Verantwortung für die Anwendung liegt dennoch ausschließlich beim Auftraggeber. Tritt ein Fehler in der Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung herbeiführen, ohne umfangreiche Kenntnisse über das System zu besitzen. Durch das Notfallvorsorgekonzept müssen dem Outsourcing-Dienstleister daher genaue Anweisungen zur Verfügung gestellt werden, wie er dabei vorgehen darf. Es kann dabei auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot einer Maschine).

Ein Fehlverhalten einer Anwendung kann technische Ursachen haben (z. B. Datenträger voll, Netzprobleme) oder anwendungsspezifische (z. B. Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung).

Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Outsourcing-Dienstleister den Fehler zwar selbst beheben können. Meist ist aber dennoch eine Kooperation mit dem Auftraggeber notwendig, um ungewünschte Seiteneffekte auf Applikationsebene zu verhindern.

Liegen anwendungsspezifische Probleme vor, benötigt der Outsourcing-Dienstleister detaillierte und umfangreiche Anweisungen sowie Listen mit

Ansprechpartnern auf Seiten des Auftraggebers, damit er richtig reagieren kann. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Batch-Prozessen sind häufig Kenntnisse erforderlich, die nur beim Auftraggeber vorhanden sind.

Wichtig ist in diesem Fall auch, dem Dienstleister Informationen bezüglich des Schutzbedarfs der betroffenen Daten und Systeme zur Verfügung zu stellen, damit mit angemessener Umsicht gehandelt werden kann.

Prüffragen:

- Existiert ein Notfallvorsorgekonzept zum Outsourcing, das die Komponenten beim Auftraggeber, beim Dienstleister sowie die zugehörigen Schnittstellen umfasst?
- Sind im Notfallvorsorgekonzept zum Outsourcing die Zuständigkeiten, Ansprechpartner und Abläufe zwischen Auftraggeber und Dienstleister geregelt?
- Werden regelmäßig gemeinsame Notfallübungen von Auftraggeber und Outsourcing-Dienstleister durchgeführt?

# M 6.84 Regelmäßige Datensicherung der System- und Archivdaten

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Elektronische Archivsysteme unterliegen denselben Risiken hinsichtlich eines Datenverlustes wie andere IT-Systeme auch. Die Auswahl geeigneter Datenträger, z. B. optischer Archivmedien, allein bietet keinen ausreichenden Schutz vor Verlust, beispielsweise bei Zerstörung oder Diebstahl des Archivmediums selbst.

Eine redundante Speicherung der Archivdaten, der zugehörigen Index-Datenbank und der Systemdaten ist daher unerlässlich. Für die Datensicherung ist grundsätzlich die im Baustein B 1.4 *Datensicherungskonzept* genannte Vorgehensweise zu verwenden.

Alternativ zu einer Datensicherung der Archivdaten kann auch eine redundante Speicherung auf physikalisch getrennten und in unterschiedlichen Brandabschnitten aufgestellten Archivsystemen erfolgen. Einige Hersteller von Archivsystemen bieten hierzu Hochverfügbarkeitslösungen an. Trotzdem muss auch in diesem Fall eine Datensicherung des Archivsystems selbst sowie der Index-Datenbank erfolgen.

Folgende Vorgaben sind für die Sicherung der Daten und die Handhabung der Speichermedien zu beachten:

- Es ist eine regelmäßige Datensicherung der archivierten Dokumente und der dazugehörigen Index-Datenbank anzulegen. Dazu kann z. B. folgendes Verfahren angewandt werden:
  - Tagessicherung (automatische Differenzsicherungen werktags),
  - Wochensicherung (automatische Differenzsicherungen) und
  - Gesamtsicherung einmal monatlich und bei der Einrichtung und Änderungen der Konfiguration.
- Es sollten ausschließlich Speichermedien gemäß Herstellerangaben verwendet werden.
- Wird eine Jukebox als Speichereinheit zur Archivierung eingesetzt, ist darauf zu achten, dass die Speichermedien nur programmgesteuert der Jukebox entnommen und darin eingelegt werden können. Ein manuelles und somit unkontrolliertes Entnehmen oder Einlegen der Medien sollte ausgeschlossen werden.
- Es ist zu dokumentieren, welche Medien zu welchem Zeitpunkt im Archivsystem eingesetzt (online) und entnommen (offline) sind, um zu vermeiden, dass Daten unautorisiert auf entnommenen Medien gelöscht oder hinzugefügt werden.
- Alle Medien sind verwechselungssicher zu beschriften.
- Offline-Medien sind sorgfältig aufzubewahren, also so, dass sie einerseits nur für Administratoren zugänglich und andererseits vor schädigenden Umwelteinflüssen geschützt sind. Dies kann beispielsweise durch Aufbewahrung in einem verschlossenen feuersicheren und einbruchgeschützten Stahlschrank (S 120 DIS, VdS Klasse III) erreicht werden.
- Sicherheitskopien der einzelnen Medien sind direkt nach ihrer Erstellung derart räumlich vom Archivsystem zu trennen, dass auch nach einer Zer-

störung des Archivs dessen Daten vollständig rekonstruiert werden können. Die Räumlichkeiten sind vor dem Zutritt Unbefugter zu schützen.
- Die gewählte Verfahrensweise für die Datensicherung ist zu dokumentieren. Außerdem ist zu dokumentieren, wann welche Sicherheitskopien erstellt worden sind und wohin sie ausgelagert wurden (siehe auch M 6.37 *Dokumentation der Datensicherung*).
- Da alle Sicherungsmedien nur eine begrenzte Lebensdauer haben, müssen sie regelmäßig entsprechend den Herstellerempfehlungen durch neue ersetzt werden.
- Alle angelegten Datensicherungen sind regelmäßig auf Lesbarkeit zu testen und gegebenenfalls auf neue Speichermedien zu übertragen.
- In regelmäßigen Abständen und bei Konfigurationsänderungen ist die Verwendbarkeit der Sicherungen und die Restart- und Recovery-Fähigkeit des Systems zu prüfen. Dieser Test geht über das reine Lesen der Sicherungsmedien hinaus und prüft, ob das Archiv anhand der gesicherten Daten ohne Datenverlust neu aufgesetzt werden kann. Das Ergebnis ist zu dokumentieren.
- Bei einer Neuverschlüsselung von Archivdaten (siehe hierzu M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*) müssen auch die auf Backup-Medien vorgehaltenen Daten neu verschlüsselt und alte Medien gelöscht oder vernichtet werden.
- Wenn Datensicherungen wieder in das Archivsystem eingespielt werden, ist zu überprüfen, ob dadurch Datenverluste aufgetreten sind, also ob zu archivierende Daten erneut erfasst werden müssen. Außerdem muss kontrolliert werden, ob für die wieder eingespielten Daten Löschvermerke vorliegen, die berücksichtigt werden müssen.

Prüffragen:

- Werden Archivdaten mit der zugehörigen Index-Datenbank und den Systemdaten redundant gespeichert?
- Jukebox-Benutzung: Können die Speichermedien nur programmgesteuert entnommen und eingelegt werden?
- Werden die Entnahme und das Einsetzen von Archivmedien mit Zeitangabe dokumentiert?
- Werden alle angelegten Datensicherungen regelmäßig auf Lesbarkeit getestet und gegebenenfalls auf neue Speichermedien übertragen?
- Wird in regelmäßigen Abständen oder bei Konfigurationsänderungen am Archivsystem die Restart- und Recovery-Fähigkeit des Archivsystems geprüft und die Ergebnisse dokumentiert?
- Neuverschlüsselung von Archivdaten: Werden Daten auf Backup-Medien neu verschlüsselt und alte Medien gelöscht oder vernichtet?
- Einspielung von der Datensicherung ins Archivsystem: Werden eingespielte Daten nach Datenverlust und Löschvermerken überprüft?

# M 6.85 Erstellung eines Notfallplans für den Ausfall des IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.86 Schutz vor schädlichem Code auf dem IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.87 Datensicherung auf dem IIS

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.88 Erstellen eines Notfallplans für den Webserver

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der teilweise oder komplette Ausfall eines Webservers hat in vielen Fällen gravierende Auswirkungen. So kann der Webserver etwa wesentlicher Bestandteil innerbetrieblicher Arbeitsabläufe oder eines E-Commerce- oder E-Government-Systems sein.

Ein Ausfall des Webservers hat dann auch den Ausfall des Gesamtsystems zur Folge. Falls der Webserver ein öffentliches Webangebot beherbergt, so wird ein Ausfall oder eine Störung auch schnell öffentlich bekannt werden.

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für den Webserver muss in den existierenden Notfallplan integriert werden (siehe Baustein B 1.3 *Notfallmanagement*). Vor allem ist abzuklären, ob für alle anderen Systeme und Netzanbindungen, die zum Betrieb des Webservers benötigt werden, entsprechende Notfallpläne vorhanden sind.
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für den Webserver zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Hierin sollte nicht nur der Webserver selbst, sondern auch das Gesamtsystem, innerhalb dessen der Webserver eingesetzt wird, berücksichtigt werden. Dazu gehören unter Umständen Datenbanken, Applikationsserver oder Proxy-Installationen zur Lastverteilung.
- Bestehen besondere Anforderungen an die Verfügbarkeit des Webservers, so sollten benötigte Komponenten redundant ausgelegt werden. Beispielsweise kann der Webserver selbst in manchen Anwendungen durch die Verwendung eines gemeinsamen, externen Speichersystems redundant ausgelegt werden.
- Zum Betrieb des Webservers im Internet ist eine funktionierende Internet-Anbindung Voraussetzung. Bei bestimmten Konfigurationen ist auch ein korrekt funktionierender DNS-Server nötig. Ein Ausfall dieser Komponenten muss daher ebenfalls in Betracht gezogen werden.
- Wird SSL auf dem Webserver eingesetzt, so muss beim Wiederanlauf des Systems auch der private Schlüssel des SSL-Zertifikates zugreifbar sein. Da dieser durch ein Passwort geschützt sein sollte, muss dieses sicher hinterlegt sein, damit es für den Wiederanlauf verfügbar ist (siehe auch M 2.22 *Hinterlegen des Passwortes*).
- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.

Prüffragen:

- Gibt es ein Konzept zur Notfallvorsorge, das die Folgen eines Ausfalls minimiert und die Handlungen im Falle eines Ausfalls vorgibt?
- Ist die Notfallplanung für den Webserver in den existierenden Notfallplan integriert?
- Gibt es ein Datensicherungskonzept für den Webserver und das Gesamtsystem in dem er eingesetzt wird, welches in das existierende Datensicherungskonzept integriert ist?
- Bei hohen Anforderungen an die Verfügbarkeit: Werden Komponenten des Webservers redundant angelegt?
- Wird der Ausfall der Internet-Anbindung eingeplant?
- DNS-Server benötigt: Wird der Ausfall des DNS-Servers eingeplant?
- Bei SSL-Nutzung: Kann auf den privaten Schlüssel des SSL-Zertifikats bei einem Wiederanlauf des Systems zugegriffen werden?
- Bei SSL-Nutzung: Ist der private Schlüssel des SSL-Zertifikats durch ein Passwort geschützt und dieses Passwort sicher hinterlegt?
- Sind wichtige Aufgaben so beschrieben, dass das Gesamtsystem im Notfall, ohne vorherige Kenntnis der Systemkonfiguration wiederhergestellt werden kann?
- Ist die Systemkonfiguration dokumentiert?
- Gibt es einen Wiederanlaufplan, der das geregelte Hochfahren des Systems gewährleistet?

# M 6.89 Notfallvorsorge für einen Apache-Webserver

Diese Maßnahme ist 2011 mit der 12. Ergänzungslieferung entfallen.

# M 6.90 Datensicherung und Archivierung bei Groupware und E-Mail

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Bei einem Groupware-System müssen regelmäßig Datensicherungen durchgeführt werden. Eine der Applikationen, bei der eine geordnete Datensicherung besonders wichtig ist, ist E-Mail. Die Bedeutung von E-Mail für die interne und externe Kommunikation nimmt ständig zu, daher ist es wichtig, dass die gesendeten bzw. empfangenen Nachrichten auch längerfristig zur Verfügung stehen. Zudem gibt es auch gesetzliche Vorgaben, die eine längerfristige revisionssichere Archivierung von geschäftsrelevanten E-Mails fordern.

Groupware-Systeme bestehen aus vielen Komponenten, die je nach Konfiguration in Datensicherungen einzubeziehen sind. Daher sollte ein Datensicherungskonzept für Groupware erstellt werden, das in das existierende Datensicherungskonzept der Institution integriert werden sollte (siehe auch B 1.4 *Datensicherungskonzept*). Auf Server-Seite werden die wesentlichen Informationen und Daten von Groupware-Systemen in Datenbanken vorgehalten. Hierfür sind die Sicherheitsempfehlungen für die Datensicherungen von allgemeinen Datenbanken umzusetzen (siehe M 6.49 *Datensicherung einer Datenbank*).

Während die Datensicherung der Groupware-Server im Allgemeinen gut geregelt ist, bestehen häufig große Regelungslücken bei der Frage der Datensicherung und Archivierung von E-Mails.

Typischerweise werden E-Mails von einem zentralen Groupware- oder E-Mail-Server zunächst auf Benutzer-PCs oder in Benutzerverzeichnisse verlagert, wo sie bearbeitet und weitergeleitet bzw. abgelegt werden. Während Daten auf Servern im allgemeinen regelmäßig gesichert werden, werden die auf den Clients gespeicherten E-Mails häufig nicht oder unzureichend gesichert. Es sollte auch hierfür eine geregelte Vorgehensweise geben.

Für den Empfang von E-Mails können benutzer- oder aufgabenbezogene E-Mail-Adressen eingerichtet werden. Viele E-Mails, die an eine benutzerbezogene E-Mail-Adresse gerichtet sind, sollten aber einer Reihe von Mitarbeitern zugänglich sein, z. B. in Projektgruppen. Daher ist es wichtig, diese in entsprechenden Projektverzeichnissen auf Servern zu speichern. Häufig müssen bei der Speicherung solcher E-Mails als offizielle Dokumente auch Mindest- bzw. Höchstfristen der Speicherung beachtet werden (siehe Baustein B 1.12 *Archivierung*).

Es sollte grundsätzlich geregelt sein, wie, wann und wo sowohl gesendete als auch empfangene E-Mails archiviert werden, beispielsweise ob zentral oder dezentral von den Benutzern.

Beim Archivieren von verschlüsselter E-Mail müssen einige Punkte beachtet werden (siehe auch M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*):

- E-Mails, die über eine beträchtliche Zeitspanne gespeichert werden sollen, können unlesbar sein, wenn die benutzten kryptographischen Schlüssel nicht mehr vorhanden sind.

- Das Archivieren und das Wiedereinspielen verschlüsselter E-Mails muss sorgfältig geplant werden. Eine Möglichkeit ist z. B., die Nachrichten im Klartext zu speichern. Dabei muss die Vertraulichkeit auf andere Weise sichergestellt werden. Bei einer verschlüsselten Speicherung müssen ebenfalls die Zugangsinformationen gesichert werden, damit sie für eine Wiederherstellung der Daten verfügbar sind.

Prüffragen:

- Gibt es eine geregelte Vorgehensweise für die Sicherung von gesendeten und empfangenen E-Mails auf E-Mail-Clients und E-Mail-Servern?
- Gibt es Regelungen zu Mindest- und Höchstfristen bei der Speicherung von E-Mails, sofern E-Mails als offizielle Dokumente gespeichert werden müssen?
- Gibt es eine dokumentierte Vorgehensweise zum Archivieren von verschlüsselten E-Mails?

# M 6.91 Datensicherung und Recovery bei Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auch Router und Switches sollten in das übergeordnete Datensicherungskonzept einbezogen werden. Dabei kommt insbesondere der Sicherung der Konfigurationsdateien eine hohe Bedeutung zu.

Eine Sicherung von Dateisystemen ist bei aktiven Netzkomponenten nicht möglich. Da im Rahmen einer zentralen Administration Konfigurationsdateien oftmals auf separaten Servern gehalten und auch von dort geladen werden, kann die Sicherung über diese Server erfolgen. Die Konfigurationsdateien auf diesen Servern sind vor unberechtigtem Zugang zu schützen. Dies gilt insbesondere dann, wenn in den Konfigurationsdateien Passwörter im Klartext gespeichert sind.

Falls zur Sicherung der Konfigurationsdateien ein TFTP-Server eingesetzt wird, so darf dieser nur im Administrationsnetz erreichbar sein. Alternativ kann bei einigen Systemen eine Datensicherung auch über die Verwendung von PCMCIA-Speichereinschüben erfolgen.

Um auf die Nutzung der Datensicherung vorbereitet zu sein, müssen regelmäßig Recovery-Übungen zum Wiederherstellen der Sicherung durchgeführt werden (siehe hierzu auch M 6.41 *Übungen zur Datenrekonstruktion*).

Weiterführende Maßnahmen:

M 6.36 *Festlegung des Minimaldatensicherungskonzeptes*

M 6.37 *Dokumentation der Datensicherung*

M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*

M 6.41 *Übungen zur Datenrekonstruktion*

Prüffragen:

- Sind die Router und Switches in dem übergeordneten Datensicherungskonzept der Organisation berücksichtigt?
- Wird eine regelmäßige Datensicherung der Konfigurationsdateien durchgeführt?
- Ist der TFTP-Server, sofern eingesetzt, zur Sicherung der Konfigurationsdateien nur im Administrationsnetz erreichbar?
- Werden regelmäßig Recovery-Übungen zum Wiederherstellen der Konfigurationssicherungen durchgeführt?

# M 6.92 Notfallvorsorge bei Routern und Switches

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

**Fehlerbehandlung bei Routern und Switches**

In jedem IT-Betrieb treten Störungen auf, die von sporadisch auftretenden Fehlverhalten von Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts und dadurch verursachten Netzausfällen reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software beispielsweise auf Grund von Defekten oder Kompromittierungen.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien und als Ergebnis von bereits aufgetretenen Störungen sollten Handlungsanweisungen erstellt werden. Kochbuchartige Dokumentationen aller notwendigen Kommandos, ihrer Anwendung mit den zu erwartenden Ausgaben sind in Situationen, die schnelles Handeln erfordern, besonders hilfreich. Hierzu gehören neben Diagnose und Fehlerbehandlung auch die im normalen Betrieb notwendigen Administrationstätigkeiten. Letztere können typischerweise bereits in der vom Hersteller gelieferten Dokumentation enthalten sein. Für die tägliche Praxis ist es allerdings sinnvoll, eine Gesamtdokumentation in Form eines Betriebshandbuchs zu erstellen.

Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört auch eine geeignete Protokollierung während des Betriebs (siehe auch M 4.205 *Protokollierung bei Routern und Switches*). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden. Dazu existieren sowohl frei verfügbare als auch kommerzielle Programme, oft auch vom Hersteller der Geräte. Die Verwendung geeigneter Werkzeuge ist umso wichtiger, da mit den Systemkommandos nicht immer alle Konfigurationseinstellungen angezeigt werden. Teilweise werden lediglich die von den Standardeinstellungen abweichenden Daten erfasst.

Die Vorgehensweise bei der Fehlerbehandlung lässt sich in die Bereiche Administration, Performancemessung und Diagnose unterteilen. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt:

**Administration**

In einem Betriebshandbuch sollten alle notwendigen Kommandos zu Administration und Konfiguration dokumentiert werden.

Folgende Bereiche sind zu berücksichtigen:

- Einrichten von Nutzern, Vergabe von Berechtigungen
- Update des Betriebssystems
- Konfiguration
    - Interface
    - Line-Ports
    - Access-Control-Lists
    - Routing
- Protokollierung

**Performance**

Folgende Aspekte sollten für Aussagen über die Performance berücksichtigt werden:

- Eingehender und ausgehender Verkehr (pro Interface oder Port)
- Durchsatz oder Verkehr pro Interface
- Statistikinformationen der verwendeten Protokolle

**Diagnose**

Für die Diagnose sollten alle notwendigen Kommandos und die zu erwartenden Ausgaben zur Anzeige der Zustände des Gesamtsystems, der Interfaces und ihrer Konfiguration dokumentiert sein. Viele Kommandos ermöglichen zudem einen Debug-Modus zu Ausgabe umfangreicher Statusinformationen.

Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant:

- Status der Netz-Interfaces und der sonstigen Anschlüsse
- Status der TCP- und UDP-Netzdienste
- Gesamtkonfiguration als Überblick
- Prozesse
- Routing Tabelle und genutzte Routing Protokolle
- ARP-Tabelle
- Angemeldete Nutzer
- DNS und nslookup-Informationen
- Protokollierung (Nutzung der Log-Level, Interpretation der Log-Informationen)

Als weiterführende Maßnahmen sollte M 2.215 *Fehlerbehandlung* betrachtet werden.

**Notfallvorsorge zur Steigerung der Verfügbarkeit**

Durch eine Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit der übergreifenden Störungs- und Notfallvorsorge abzustimmen und sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein B 1.3 *Notfallmanagement*). Hier werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen bez. Aufbau, Inhalt und Form fest.

Folgende Fragestellungen sind für die Notfallvorsorge relevant:

- Welche Anforderungen bestehen an das Monitoring?
- Zusammenstellung der Informationen, die von den für den Betrieb der Netzkomponenten verantwortlichen Stellen immer ausgewertet werden (siehe auch Abschnitt Protokollierung)
    - Wie kann eine frühzeitige Störungserkennung sicher gestellt werden?
- Was sind Gründe für mögliche Störungen?
    - Hardware-Defekte
    - Zu geringe Dimensionierung (Ausfall bei Steigerung der Last)
- Welche Vorsorgemaßnahmen können getroffen werden?
    - Ersatzgeräte
    - Ersatzteile

  - Implementierung von Failover-Lösungen, die im laufenden Betrieb ein Umschalten auf ein Alternativgerät ermöglichen
  - Wartungsverträge
  - Ausbildung der Mitarbeiter
- Welche Service Level Agreements bestehen oder sollten getroffen werden?
  - Hardware-Lieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten)
  - Interne Service Level Anforderungen
- Wie ist eine Diagnose durchzuführen?
  - Statusabfragen
  - Anzeige der Konfiguration
  - Prozesse
  - Routing
  - Angemeldete Nutzer
  - Protokollierung
- Welche Entstörprozeduren müssen durchgeführt werden?
  - Vorgehen bei Ausfall des Komplettsystems (Wiederherstellen von Betriebssystem und Konfiguration)
  - Vorgehen bei Ausfall von Teilkomponenten, bspw. Speicher
- Wer ist im Schadensfall zu benachrichtigen?
  - Server- und Anwendungsadministration
  - Hardware-Lieferant/Ansprechpartner für den Wartungsvertrag
- Welche Dokumente müssen im Schadensfall verfügbar sein?
  - Konfiguration
  - ACLs (Regelwerk)
  - Eingerichtete Nutzer und Berechtigungen
  - Passwörter

Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD-ROMs oder anderen Datenträgern gesondert hinterlegt werden.

- Wie verläuft der Wiederanlauf?
  - Abhängigkeiten zu anderen Netzkomponenten bzw. Bereichen des IT-Verbunds
  - Neuinstallation des Betriebssystems und Konfiguration
  - Zurückspielen einer gesicherten Konfiguration
  - Möglichkeiten eines eingeschränkten Betriebs

Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Gerätetypen und Betriebssystemen berücksichtigt werden.

Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist die Vorhaltung von Ersatzteilen, um bei Hardware-Defekten die Ausfallzeiten zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden.

Prüffragen:

- Sind für Diagnose und Fehlerbehebungen bei Routern und Switches im Vorfeld entsprechende Handlungsanweisungen definiert?
- Sind die im normalen Betrieb der Router und Switches notwendigen Administrationstätigkeiten in einem Betriebshandbuch definiert?
- Sind alle für die Diagnose notwendigen Kommandos und die zugehörige Anzeige der Zustände des Gesamtsystems, der Interfaces und ihrer Konfiguration dokumentiert?
- Existiert ein Konzept für die Notfallvorsorge, das mit der übergreifenden Störungs- und Notfallvorsorge abgestimmt ist?
- Ist sichergestellt, dass die Dokumentationen zur Notfallvorsorge und die darin enthaltenen Handlungsanweisungen in Papierform existieren?
- Werden die in der Notfallvorsorge notwendigen Vorgehensbeschreibungen regelmäßig erprobt?

# M 6.93 Notfallvorsorge für z/OS-Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Zu einem sicheren z/OS-Betrieb gehört es, für verschiedene Notfälle vorbereitet zu sein. Dazu zählen z. B.

- ein Notuser-Verfahren, das notwendig wird, wenn keine Kennung mehr mit bestimmter Funktionalität verfügbar ist,
- ein Verfahren zur Wiederherstellung einer funktionierenden RACF-Datenbank,
- ein z/OS-Backup-System, das sofort aktiviert werden kann und
- ein Notfall-System, das bei Einzelsystemen u. U. benötigt wird, um Fehlerkorrekturen vornehmen zu können.

Die verschiedenen Handlungsempfehlungen zur Notfallvorsorge sind nachfolgend näher beschrieben:

**Notuser-Verfahren**

Zur Notfallvorsorge muss ein Notuser-Verfahren eingerichtet werden. Dieser Notuser kann verwendet werden, falls in einer Notsituation kein RACF-Administrator (*Resource AccessControl Facility*) zur Verfügung steht, bzw. falls alle Kennungen mit *SPECIAL*-Rechten gesperrt sind. Es können eine oder mehrere Notuser-Kennungen eingerichtet werden.

Es sind folgende Regeln zu beachten:

*Zugang zur Notuser-Kennung*

Da die Notuser-Kennung sehr hohe Berechtigungen (*SPECIAL*) im System besitzt, muss die Herausgabe der Notuser-Kennung restriktiv gehandhabt werden.

Der Notuser darf nur vorher festgelegten Personen zugänglich sein. Er sollte nur RACF-Administratoren und Systemprogrammierern mit RACF-Ausbildung zur Verfügung stehen.

*Meldung und Dokumentation der Verwendung des Notusers*

Bei Verwendung des Notusers sind sobald als möglich die RACF-Administration, der Auditor und das Sicherheitsmanagement zu unterrichten. Folgende Informationen müssen gemeldet werden:

- Wer hat den Notuser benutzt?
- Weshalb wurde der Notuser benötigt?
- Wann erfolgte der Zugriff?
- Was wurde mit der Berechtigung des Notuser durchgeführt?

Alle Vorgänge zur Notuser-Kennung sind nachvollziehbar zu dokumentieren und zu archivieren.

*Passwort der Notuser-Kennung*

Beim Login mit der Notuser-Kennung ist das Passwort durch den Benutzer sofort auf ein neues zu ändern. Dies wird durch RACF erzwungen, wenn der Notuser mit einem neuen *Initial-Passwort* versehen wurde.

Nach dem Gebrauch der Notuser-Kennung muss das zugehörige Passwort durch die RACF-Administration wieder neu gesetzt und hinterlegt werden.

*Missbrauch des Notuser-Verfahrens*

Das Notuser-Verfahren darf nicht zur Berechtigungserweiterung im Nicht-Notfall missbraucht werden. Es muss verhindert werden, dass der Notuser aus Bequemlichkeit verwendet wird, um definierte Administrations- und Entscheidungswege zu umgehen.

*Verhindern der Notuser-Sperrung*

Alle Kennungen können nach einer vorgegebenen Zeit wegen Inaktivität gesperrt werden. Die entsprechende Einstellung erfolgt in den *SETROPTS*-Parametern von RACF. Eine solche Sperrung kann auch Notuser-Kennungen betreffen, wenn diese längere Zeit nicht verwendet werden. Es ist zu überlegen, diese automatische Sperrung durch den Einsatz eines Batch-Jobs zu verhindern. Der Batch-Job sollte regelmäßig die Notuser-Kennungen benutzen (z. B. einmal im Monat). Dadurch werden die Zeitstempel in der RACF-Datenbank aktualisiert. Dieser Batch-Job kann über einen Job-Scheduler initiiert werden. Es muss sichergestellt werden, dass das Passwort des Notusers außer den explizit hierzu autorisierten Mitarbeitern niemandem bekannt wird. Hierfür sollte die RACF-Klasse *SURROGAT* zum Einsatz kommen, damit kein Passwort in die *Job Control Language* eingestellt werden muss.

**Verfahren zur Wiederherstellung von z/OS-RACF-Datenbanken**

Die RACF-Datenbank ist der wichtigste und zentrale Speicherort für die Sicherheitseinstellungen eines z/OS-Systems. Soll ein sicherer Betrieb gewährleistet werden, muss die RACF-Datenbank korrekt funktionieren. Um Problemen durch nicht zur Verfügung stehende oder defekte RACF-Datenbanken zu begegnen, sind die folgenden Empfehlungen zu beachten:

*Sicherung der RACF-Datenbanken*

Es ist wichtig, dass die Synchronisierung der RACF-Datenbanken einwandfrei funktioniert. Deshalb muss zur Sicherung aktiver Datenbanken (die Datenbanken, die beim *RVARY*-Display als aktiv gekennzeichnet sind) immer entweder das RACF-Utility *IRRUT200* (von IBM empfohlen) oder *IRRUT400* eingesetzt werden.

Während der Sicherung werden zahlreiche *LOCK*-Funktionen ausgeführt. Deshalb sollte der Batch-Job, der die Sicherung durchführt, in ein Zeitfenster mit möglichst geringer Auslastung gelegt werden.

Die Sicherungen dürfen nicht auf der gleichen Festplatte gespeichert werden, auf der die RACF-Datenbanken im Betrieb liegen.

Es sollte überlegt werden, mehrere Generationen der Sicherungen aufzubewahren. Dabei ist das Wochenende mit zu berücksichtigen.

Die Sicherungskopien der Datenbanken sind - ebenso wie die RACF-Datenbanken selbst - über entsprechende RACF-Profile zu schützen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

*RACF-Datenbankwiederherstellung*

Im z/OS-System gibt es eine *Primary* und eine *Backup* RACF-Datenbank. Diese können im Betrieb umgeschaltet werden. Aus Sicherheitsgründen sind die

beiden Datenbanken auf verschiedenen Platten zu speichern. Treten Fehler in der *Primary* Datenbank auf, so kann durch ein *RVARY SWITCH* Kommando die *Backup* zur *Primary* und die *Primary* zur *Backup* RACF-Datenbank gemacht werden. Die defekte *Backup* RACF-Datenbank kann daraufhin in der Regel gelöscht und durch eine neue ersetzt werden.

Sind beide RACF-Datenbanken fehlerhaft, so ist es in diesem Notfall möglich, die defekte RACF-Datenbank durch eine gültige Sicherungskopie zu ersetzen und hierdurch den Systembetrieb wieder herzustellen (u. U. von einem anderen System aus). Bei Einzelsystemen ist hierfür eventuell ein Notfallsystem notwendig (siehe unten: *Erstellung eines z/OS-Notfallsystems*).

*Nachvollziehbarkeit im Fehlerfall*

Es ist ein Verfahren zur Sicherung und zum Zurückspielen der RACF-Datenbank einzurichten.

Es ist ein Verfahren einzurichten, so dass Änderungen in der RACF-Datenbank in der Zeit zwischen der letzten Sicherung der RACF-Datenbank und dem Zeitpunkt des eingetretenen Notfalls nachvollzogen werden können. Eine Möglichkeit hierfür ist beispielsweise, dass RACF-Änderungen nur durch dokumentierte Batch-Jobs durchgeführt werden dürfen. Eine andere Möglichkeit ist, dass direkt nach RACF-Änderungen die SMF-Datensätze ausgewertet werden. Beide Verfahren müssen nachvollziehbar dokumentiert sein. Die Dokumentation muss den Administratoren vorliegen.

**z/OS-Backup-System**

Bei Systemfehlern, bei denen das z/OS-System (oder auch ein kompletter *Parallel Sysplex Cluster*) nicht mehr gestartet werden kann, ist es wichtig, möglichst schnell das System bzw. die Systeme wieder in einen betriebsbereiten Zustand zu bringen. Solche Ausfälle können beispielsweise auf Grund eines technischen Fehlers oder auch auf Grund fehlerhafter manueller Eingaben vorkommen. Deshalb sollte ein separater Satz von Festplatten vorgehalten werden, der eine Kopie des aktuellen Betriebssystems enthält. Durch einfache Änderung der IPL-Adresse (*Initial Program Load*) kann auf diese Weise ein z/OS-Betriebssystem in den meisten Fällen schnell reaktiviert werden. Die folgenden Empfehlungen sind dabei zu beachten:

*Festplatten-Konzept*

Das Festplatten-Konzept für das z/OS-Betriebssystem und die dazugehörenden Programmprodukte (wie Scheduler, Output-Manager und weitere) muss logisch aufgebaut und klar erkennbar sein. Zusammengehörende Dateien, z. B. des Betriebssystems, dürfen nicht verteilt auf viele unterschiedliche Festplatten gespeichert werden. Es sollten möglichst wenig Festplatten verwendet werden, damit relativ einfach vollständige Sicherungen erstellt werden können.

*Cloning-Prozess*

Für das Erstellen der Backup-Festplatten sollte ein *Cloning*-Prozess entwickelt werden, der mindestens die folgenden Aktionen durchführt:

- Kopieren der System-Residenzen,
- Kopieren der Programmprodukt-Festplatten,
- Kopieren der HFS-Festplatten (*Hierarchical File System*),
- Kopieren der SMP/E-Festplatten (*System Modification Program*),

- Verändern der Volume-Angaben in SMP/E durch die *ZONEEDIT*-Funktion (alte Volume-Angabe durch neue ersetzen) und
- Anpassen der Volume-Angabe im Member *IEASYMnn* der *Parmlib.*

*Wartungskonzeption*

Um den laufenden Betrieb nicht zu gefährden, wird zur Pflege des z/OS-Betriebssystems in der Regel ein separater Festplattensatz verwendet. Es ist zu überlegen, diesen nach erfolgter Wartung als neuen aktiven Plattensatz und die vorherigen Platten als Backup-Satz zu benutzen.

*Einsatz von System-Variablen*

Zur Erleichterung der Definitionen sollten, wo immer technisch möglich und sinnvoll, symbolische Variablen benutzt werden (ab z/OS 1.4 sind bis zu 800 solcher Variablen definierbar). Es sollte überlegt werden, die Katalogeinträge des Masterkatalogs und dessen *ALIAS*-Einträge über solche Techniken variabel zu gestalten, damit ein Wechsel ohne zusätzliche Eingriffe jederzeit möglich ist. Die Benutzung symbolischer Variablen ist in vielen Definitionen möglich, es sollte jedoch berücksichtigt werden, dass einige Definitionen die Variablen noch nicht unterstützen.

*Führung von Arbeitsdateien*

Um unnötigen Wartungsaufwand zu vermeiden, sollten Arbeitsdateien, wie Kataloge, *Parmlibs*, *Proclibs* und Datenbanken von Programmprodukten, nicht doppelt oder sogar mehrfach geführt werden.

**Erstellung eines z/OS-Notfallsystems**

Durch Fehler in maßgeblichen Software-Komponenten, z. B. RACF (*Resource Access Control Facility*) oder Master-Katalog, kann es vorkommen, dass das gesamte System ausfällt. Bei Einzelsystemen muss für diesen Fall kurzfristig ein Notfallsystem zur Verfügung stehen, das ohne große Probleme gestartet werden kann und eine Reparatur des defekten Systems ermöglicht.

Im Gegensatz zu Backup-Systemen ist das Notfallsystem nicht für den Produktivbetrieb gedacht. Bei der Erstellung von Notfallsystemen sind die folgenden Hinweise zu berücksichtigen:

*Unabhängigkeit*

Das Notfallsystem muss komplett unabhängig von den Dateien und Definitionen der Produktionssysteme eingerichtet werden.

*Reduktion auf das Wesentliche*

Das Notfallsystem sollte nicht mehr Software-Funktionen enthalten, als unbedingt für eine Reparatur notwendig sind, damit für das System nicht mehr als eine Festplatte benötigt wird. Dazu gehören die Programme JESx (*Job Entry-Subsystem*), VTAM (*Virtual Telecommunication Access Method*) und TSO (*Time Sharing Option*) mit den dazugehörenden ISPF-Dateien (*Interactive Support Programming Facility*). Es ist zu überlegen, ob ein System ohne JES ausreicht. Dann können jedoch keine Batch-Jobs eingesetzt werden.

*Volume-Angaben*

Alle Prozeduren sind mit *Volume*-Angaben zu versehen, um Abhängigkeiten von Katalogen zu vermeiden. Es sollten deshalb auch keine SMS-Dateien (*System Managed Storage*) verwendet werden.

*VTAM-Terminals*

Es muss eine möglichst einfache VTAM-Prozedur angelegt werden, bei der mindestens ein VTAM *Local Node* vorgesehen ist, der die Adresse einer MCS-Konsole (*Multiple ConsoleSupport*) beinhaltet. Damit ist es möglich, eine VTAM-Verbindung aufzubauen und sich an dem defekten System anzumelden. Bei Änderungen in den VTAM-Konfigurationen ist die Definition des VTAM *Local Node* entsprechend zu aktualisieren.

*Komponenten des Notfall-Systems*

Das Notfallsystem sollte auf einer Festplatte liegen, die mindestens die folgenden Dateien und Komponenten enthält:

- IPL-Text,
- Master-Katalog,
- JESx-Checkpoint und Spool-Datei,
- Page-Dataset,
- System-Dateien (MANx, STGINDEX, LOGREC, DAE),
- Parmlib, Proclib (Logon-Prozedur nicht vergessen),
- SMF-Dateien (SYS1.MANx),
- BROADCAST- und UADS-Dateien und
- RACF-Datenbank.

*User-IDs für den Notfall*

Es müssen mindestens zwei *User-IDs* auf dem Notfallsystem vorhanden sein, die wie die Notuser behandelt werden.

*Permanente Pflege*

Der Zutritt und der Zugang zum Notfallsystem müssen geschützt werden. Änderungen im normalen System müssen zeitnah auf dem Notfallsystem nachvollzogen werden, falls sie für das Notfallsystem relevant sind. Die Funktionsfähigkeit des Notfallsystems ist in periodischen Zeitabständen zu überprüfen.

Prüffragen:

- Ist für das z/OS-System ein Notuser-Verfahren eingerichtet?
- Werden bei der Notfallvorsorge für das z/OS-System alle Vorgänge zur Notuser-Kennung nachvollziehbar dokumetiert und archiviert?
- Werden Sicherungskopien der Datenbanken ebenso wie die RACF-Datenbanken selbst über entsprechende RACF-Profile geschützt?
- Ist ein Verfahren zur Sicherung und zum Zurückspielen der RACF-Datenbank eingerichtet?
- Wird ein z/OS-Backup-System auf einem separaten Satz von Festplatten vorgehalten, der eine Kopie des aktuellen Betriebssystem enthält?
- Wird bei Einzelsystemen ein z/OS-Notfallsystem eingerichtet?

# M 6.94 Notfallvorsorge bei Sicherheitsgateways

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

### Fehlerbehandlung bei Sicherheitsgateways

Sicherheitsgateways spielen eine zentrale Rolle im Hinblick auf die Verfügbarkeit der Netzanbindung einer Organisation. Fehler oder Ausfälle des Sicherheitsgateways oder einzelner Komponenten (von sporadisch auftretenden Fehlverhalten bis zum klar abzugrenzenden Ausfall eines Geräts und dadurch verursachten Netzausfällen) können unmittelbare und schwerwiegende Auswirkungen haben, wenn keine ausreichende Vorsorge für Notfälle getroffen wurde.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien und als Ergebnis von bereits aufgetretenen Störungen sollten Handlungsanweisungen erstellt werden. Kochbuchartige Dokumentationen aller notwendigen Schritte sind in Situationen, die schnelles Handeln erfordern, besonders hilfreich. Hierzu gehören neben Diagnose und Fehlerbehandlung auch die im normalen Betrieb notwendigen Administrationstätigkeiten. Letztere können typischerweise bereits in der vom Hersteller gelieferten Dokumentation enthalten sein. Für die tägliche Praxis ist es allerdings sinnvoll, eine Gesamtdokumentation in Form eines Betriebshandbuchs zu erstellen.

Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört auch eine geeignete Protokollierung während des Betriebs (siehe auch M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden.

Die Vorgehensweise bei der Fehlerbehandlung kann in die Bereiche Administration, Performancemessung und Diagnose unterteilt werden. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt. Für Router, die als Paketfilter Teil eines Sicherheitsgateway sind, sollte M 6.92 *Notfallvorsorge bei Routern und Switches* herangezogen werden.

### Administration

In einem Betriebshandbuch für die einzelnen Komponenten des Sicherheitsgateways sollten alle notwendigen Kommandos und Arbeitsschritte zu Administration und Konfiguration dokumentiert werden. Aus Gründen der Übersichtlichkeit ist es empfehlenswert, dies für jede Komponente getrennt zu machen und zusätzlich ein Übersichtsdokument zu erstellen.

Folgende Bereiche sind zu berücksichtigen:

- Konfiguration des Betriebssystems, insbesondere die Konfiguration der Netzschnittstellen
- Update des Betriebssystems
- Konfiguration der "Funktionskomponenten" (Paketfilter, Sicherheitsproxies, Virenscanner usw.), insbesondere
    - wichtige Kommandos zum Starten und Beenden der Dienste

  - Speicherort und Format der Konfigurationsdateien oder -datenbanken, gegebenenfalls Benutzung der betreffenden Konfigurationswerkzeuge
  - bei Sicherheitsproxies (beispielsweise HTTP-Proxy, E-Mail-Gateway) auch Lage (Partition / Filesystem) der Datenverzeichnisse
- Protokollierung

**Performance**

Folgende Aspekte sollten für Aussagen über die Performance berücksichtigt werden:

- Eingehender und ausgehender Verkehr über die Paketfilter sowie für jedes der Protokolle, für die ein Sicherheitsproxy eingesetzt wird
- Statistikinformationen der verwendeten Protokolle

**Diagnose**

Für die Diagnose sollten alle notwendigen Kommandos und die zu erwartenden Ausgaben zur Anzeige des Betriebszustands aller Komponenten des Sicherheitsgateways und ihrer Konfiguration dokumentiert sein. Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant:

- Gesamtkonfiguration als Überblick
- Status und Konfiguration der Netz-Interfaces und der sonstigen Anschlüsse
- Status der vorhandenen Netzdienste
- Prozesse
- Angemeldete Benutzer
- Protokollierung (Nutzung der Log-Level, Interpretation der Log-Informationen)

Weiterführende Maßnahmen sind in M 2.215 *Fehlerbehandlung* beschrieben.

**Notfallvorsorge zur Steigerung der Verfügbarkeit**

Durch eine Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit der übergreifenden Störungs- und Notfallvorsorge abzustimmen und sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein B 1.3 *Notfallmanagement*). Hier werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen bezüglich Aufbau, Inhalt und Form fest.

Folgende Fragestellungen sind für die Konzeption der Notfallvorsorge relevant:

- Welche Anforderungen bestehen an das Monitoring?
  - Zusammenstellung der Informationen, die von den für den Betrieb der Netzkomponenten verantwortlichen Stellen immer ausgewertet werden (siehe auch Abschnitt Protokollierung)
  - Wie kann eine frühzeitige Störungserkennung sicher gestellt werden? Gibt es eventuell Tools, die eine automatische Alarmierung ermöglichen?
- Was sind Gründe für mögliche Störungen?
  - Angriffe
  - Hardware-Defekte
  - Zu geringe Dimensionierung (Ausfall bei Steigerung der Last)

- Welche Vorsorgemaßnahmen können getroffen werden?
  - Erarbeitung von Alternativkonfigurationen und "Fallback-Strategien" für bestimmte Ausfall- oder Angriffsszenarien (beispielsweise geändertes Routing, alternative Paketfilterregeln)
  - Ersatzgeräte-Implementierung von Failover-Lösungen, die im laufenden Betrieb ein Umschalten auf ein Alternativgerät ermöglichen
  - Wartungsverträge
  - Ausbildung der Mitarbeiter
- Welche Service Level Agreements bestehen oder sollten getroffen werden?
  - Hardware-Lieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten, insbesondere bei Appliances)
  - Interne Service Level Anforderungen
- Wie ist eine Diagnose durchzuführen?
  - Statusabfragen
  - Anzeige der Konfiguration
  - Protokollierung
- Welche Entstörprozeduren müssen durchgeführt werden?
  - Vorgehen bei Ausfall des Komplettsystems (Wiederherstellen von Betriebssystem und Konfiguration)
  - Vorgehen bei Ausfall von Teilkomponenten (beispielsweise Speicher, Festplatten, Netzkarten)
- Wer ist im Schadensfall zu benachrichtigen?
  - Server- und Anwendungsadministration
  - Hardware-Lieferant / Ansprechpartner für den Wartungsvertrag
- Welche Dokumente müssen im Schadensfall verfügbar sein?
  - Konfiguration
  - Paketfilterregeln, Konfiguration für Sicherheitsproxies
  - Passwörter

  Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD-ROMs oder anderen Datenträgern gesondert hinterlegt werden.
- Wie verläuft der Wiederanlauf?
  - Abhängigkeiten zu anderen Bereichen des IT-Verbunds
  - Neuinstallation des Betriebssystems und Konfiguration
  - Zurückspielen einer gesicherten Konfiguration
  - Möglichkeiten eines eingeschränkten Betriebs.

Bei der Planung für einen eingeschränkten Betrieb muss berücksichtigt werden, dass ein eingeschränkter Betrieb des Sicherheitsgateways nicht zur Folge haben darf, dass während dieser Zeit keine ausreichende Absicherung des eigenen Netzes gewährleistet ist. Im Zweifelsfall sollte lieber eine längere Ausfallzeit eines Dienstes hingenommen werden als die Gefahr, dass es wegen "eingeschränkter Sicherheit" zu weiteren Problemen kommt.

Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen unterschiedliche Vorgehensweisen bei unterschiedlichen Geräten und Betriebssystemen berücksichtigt werden.

Bei zentralen Komponenten wie beispielsweise den Paketfiltern des Sicherheitsgateways, der zwischen dem eigenen Netz und dem Internet eingerichtet ist, kann der Ausfall einer Komponente des Sicherheitsgateways den Ausfall der gesamten Internetanbindung nach sich ziehen. Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist daher die Vorhaltung von Ersatzteilen oder Ersatzgeräten, um bei Hardware-Defekten die Ausfallzeiten zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden.

Prüffragen:

- Existieren für typische Ausfallszenarien und aus Ergebnissen von bereits aufgetretenen Störungen entsprechende Handlungsanweisungen?
- Werden regelmäßige Performancemessungen für die Sicherheitsgateway-Komponenten durchgeführt?
- Sind in einem Betriebshandbuch für die einzelnen Komponenten des Sicherheitsgateways alle notwendigen Kommandos und Arbeitsschritte zur Administration und Konfiguration dokumentiert?
- Sind alle notwendigen Kommandos und die zu erwartenden Ausgaben zur Anzeige des Betriebszustands aller Komponenten des Sicherheitsgateways und ihrer Konfiguration dokumentiert?
- Sind die Planungen zur Notfallvorsorge des Sicherheitsgateways mit der übergreifenden Störungs- und Notfallvorsorge der Organisation abgestimmt?
- Liegen die Handlungsanweisungen für die Notfallvorsorge bei Sicherheitsgateways auch in Papierform vor?
- Ist gewährleistet, dass ein eingeschränkter Betrieb des Sicherheitsgateways zu keiner Beeinträchtigung der Absicherung des eigenen Netzes führt?
- Werden Notfallübungen für die Notfallvorsorge bei Sicherheitsgateways durchgeführt?

# M 6.95 Ausfallvorsorge und Datensicherung bei Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Ein Smartphone, Tablet oder PDA kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn er dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vornherein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Der Ladezustand und die Funktionsfähigkeit des Akkus sollten regelmäßig überprüft werden (siehe M 4.31 *Sicherstellung der Energieversorgung im mobilen Einsatz*).

Alle auf dem mobilen Endgerät gespeicherten Daten wie Telefonbucheintragungen, Notizen, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie Passwörter und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihres Schutzbedarfs sicher aufbewahrt werden. Werden die Endgeräte durch eine Mobile-Device-Management-Software zentral gesteuert und konfiguriert, so sind die entsprechenden Profile der Endgeräte zu sichern, sodass sie zügig wieder eingespielt werden können.
- Die Daten auf dem Smartphone, Tablet oder PDA sollten regelmäßig mit einer anderen Stelle, wie z. B. mit einem PC, einem Serverdienst der Institution oder gegebenenfalls mit einem externen Dienstleister synchronisiert werden. Das ersetzt allerdings keine vollständige Datensicherung.
- Es sollte daher regelmäßig auch eine komplette Datensicherung des Smartphones, Tablets oder PDAs auf einem weiteren IT-System, z. B. einem Notebook oder einem Desktop-PC, durchgeführt werden. Besonders empfehlenswert ist die komplette Datensicherung durch ein vollständiges Systemabbild (Snapshot). Die Lösung ist komfortabel und verringert die Zeit für die Installation und Konfiguration eines neuen Gerätes erheblich. Wenn für diese Lösung das IT-System tiefer gehend manipuliert werden muss, wie beispielsweise durch Rooten oder die Installation eines alternativen Recovery bei Android-basierten Geräten, so sollte das Risiko der Manipulation gegen den Vorteil der schnelleren Wiederverfügbarkeit sorgsam abgewogen werden. Gegebenenfalls sind die zusätzlichen Maßnahmen für die Informationssicherheit, die durch das Rooten oder sonstige Maßnahmen nötig werden, so hoch, dass kein Vorteil gegenüber der weniger komfortablen Sicherungsmethode ohne Systemabbild besteht.
- Da bei Smartphones, Tablets und PDAs der vorhandene Speicherplatz beschränkt ist, können die meisten Modelle mit externen Speichermedien erweitert werden (siehe auch M 4.232 *Sichere Nutzung von Zusatzspeicherkarten*). Verbreitet sind hierfür Speicherkarten, z. B. Memory-Cards, die schnell austauschbar sind, sodass sie sich gut eignen, um auch unterwegs Backups durchzuführen. Das ist vor allem dann sinnvoll, wenn ein Benutzer häufig lange abwesend ist und dadurch für längere Zeit keine Synchronisation zwischen IT-System und Smartphone, Tablet oder PDA stattfindet. Wie generell für Datensicherungen gilt auch hier, dass diese sicher verwahrt werden müssen. Wenn die Memory-Cards im Endgerät oder

anderswo unbeaufsichtigt liegen bleiben, können Unbefugte die darauf gespeicherten Daten kopieren. Legen sie anschließend die Memory-Card wieder zurück, werden dabei nicht einmal Spuren hinterlassen.
- Alle Daten, die auf austauschbaren Speicherkarten gespeichert sind, müssen ebenfalls gesichert werden, spätestens bei der nächsten Synchronisation.

Bei den meisten Smartphones, Tablets oder PDAs liegt das Betriebssystem in einem Flash-Speicher, der häufig auch genügend Platz für eine Datensicherung wenigstens der wichtigsten Daten wie der Inhalte des Personal Information Manager (PIM) bietet. Um das komfortabel durchzuführen, gibt es je nach Hersteller mitgelieferte oder zusätzliche Tools. Hierbei sollte beachtet werden, dass nach einem kompletten Reset alle Daten außerhalb des Flash-Speichers gelöscht werden, also auch alle Passwörter zum Zugriffsschutz. Ein Angreifer kann dadurch leicht Zugriff auf den Flash-Speicher und die dort gespeicherten Daten erhalten. Bevor ein Smartphone, Tablet oder PDA weitergegeben wird, z. B. zur Reparatur oder an andere Benutzer, sollten daher alle Daten, auch aus dem Flash-Speicher, gelöscht werden.

Wenn ein Smartphone, Tablet oder PDA kontinuierlich verfügbar sein soll, sollte immer ein Ersatz-Akku mitgeführt werden.

**Reparatur**

Bei Defekten des Smartphones, Tablets, PDAs oder einzelner Komponenten sollten Reparaturen nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie Smartphones, Tablets oder PDAs lohnt sich eine Reparatur häufig nicht, sodass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein Smartphone, Tablet oder PDA kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des jeweiligen Endgerätes bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor ein Smartphone, Tablet oder PDA zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. gespeicherte E Mails und das Telefonbuch im Gerät gelöscht werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollten Zusatzkarten entfernt werden.

Prüffragen:

- Werden der Ladezustand und die Funktionsfähigkeit der PDA-Akkus regelmäßig überprüft?
- Werden die auf PDAs gespeicherten Daten regelmäßig gesichert?
- Werden vor der Weitergabe von PDAs alle Daten gelöscht?

# M 6.96 Notfallvorsorge für einen Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der teilweise oder komplette Ausfall eines Servers kann gravierende Auswirkungen haben, wenn der Server wesentlicher Bestandteil innerbetrieblicher Arbeitsabläufe ist oder ein öffentlich zugängliches Angebot unterstützt (etwa in E-Commerce- oder E-Government-Anwendungen).

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für den Server muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallmanagement*).
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist im Rahmen des allgemeinen Datensicherungskonzepts (siehe auch B 1.4 *Datensicherungskonzept*) ein Datensicherungskonzept für den Server zu erstellen. Darin muss nicht nur der Server selbst berücksichtigt werden, sondern auch die Systeme, von denen der Betrieb des Servers abhängt.
- Im Rahmen von Wartungs- und Serviceverträgen oder durch eigene Lagerhaltung muss die Versorgung mit Ersatzteilen innerhalb einer Frist sichergestellt werden. Die Ausfallzeit ist daher auf ein tragbares Maß zu reduzieren. Bei besonderen Anforderungen an die Verfügbarkeit des Servers muss gegebenenfalls eine Hochverfügbarkeitslösung eingesetzt werden.
- Die Systemkonfiguration muss dokumentiert werden. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann. Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen, sondern Handlungsanweisungen sollten auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD gesondert hinterlegt werden.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.
- Alle notwendigen Vorgehensbeschreibungen müssen regelmäßig überprüft und geprobt werden. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Betriebssysteme berücksichtigt werden.

Prüffragen:

- Existiert ein Notfallplan die Ausfall des IT-Systems?
- Existieren korrespondierende Notfallpläne für die IT-Systeme, die vom / zum Betrieb des Servers abhängen / benötigt werden?
- Existiert ein Datensicherungskonzept für das betroffene IT-Systems?
- Werden Störungs- und Notfallprozeduren regelmäßig getestet?

# M 6.97 Notfallvorsorge für SAP Systeme

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Wie für jedes andere IT-System muss auch für ein SAP System Notfallvorsorge betrieben werden. Damit die Vorbereitung zielgerichtet erfolgt, muss im Rahmen der Planungs- und Konzeptionsphase ein Notfallkonzept erstellt worden sein (siehe M 2.341 *Planung des SAP Einsatzes*), in dem auch die Notfälle definiert sind, die im Rahmen der Notfallvorsorge berücksichtigt werden sollen.

Folgende Notfälle sollten mindestens berücksichtigt werden:

- Ausfall eines SAP Servers
- Ausfall der Datenbank eines SAP Systems
- Kompromittierung eines SAP Systems
- Ausfall des Transportsystems (ABAP) oder der Software-Verteilung (JAVA)
- Ausfall eines kompletten Rechenzentrums

Generell unterscheidet sich ein SAP System im Hinblick auf die Notfallvorsorge nicht von anderen IT-Systemen. Daher sind auch die Notfallvorsorge-Maßnahmen anderer relevanter Bausteine umzusetzen, die auf die IT-Systeme (z. B. Server-Rechner, Client-Rechner, Datenbank) anwendbar sind, aus denen das SAP System besteht.

Die Verantwortlichkeiten im Rahmen der Notfallvorsorge und für die definierten Notfall-Prozeduren müssen eindeutig Personen zugeordnet werden. Es empfiehlt sich, regelmäßig Notfallübungen durchzuführen und die Prozesse anhand der dabei gemachten Erfahrungen anzupassen.

Die Notfallvorsorge sollte mindestens folgende Maßnahmen umfassen und entsprechend der individuellen Anforderungen erweitert werden:

- Ein Notfall-Administrator sollte eingerichtet und Regelungen für den Einsatz festgelegt werden.
- Es müssen regelmäßige Datensicherungen des SAP Systems durchgeführt werden. Die Verfahrensweise und Häufigkeit ist im Datensicherungskonzept festzuhalten.
- Verfahren für das Wiederherstellen eines SAP Systems müssen festgelegt werden.
- Ein Ausweichsystem sollte bei entsprechend hohen Verfügbarkeitsansprüchen vorgehalten werden.

Je nach Einsatzszenario kann auch der Schutz vor Computer-Viren (siehe M 4.271 *Virenschutz für SAP Systeme*) zur Notfallvorsorge gehören.

**Notfall-Administration**

Für den Fall, dass mit normalen Administrator-Benutzerkennungen nicht mehr auf ein SAP System zugegriffen werden kann, wird ein Notfall-Administrator-Konto benötigt. Da ABAP- und Java-Stack jeweils mit einer eigenen Benutzerverwaltung ausgestattet ist, muss in jedem Stack ein Notfall-Administrator-Konto definiert werden.

Im ABAP-Stack kann dieses mit Berechtigungen ausgestattet werden, die der Summe der Profile SAP_ALL und SAP_NEW entsprechen. Damit besitzt der

Notfall-Administrator vollständige Kontrolle über den ABAP-Stack des SAP Systems.

Im Java-Stack muss das Konto der Gruppe der Administratoren zugeordnet sein. Standardmäßig besitzt die Gruppe der Administratoren vollständige Kontrolle über den Java-Stack.

Seit NetWeaver 04 (Java 6.40) ist die Benutzerverwaltung in Java über die User Management Engine (UME) realisiert (siehe auch M 4.267 *Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung*). Diese ist gruppen- und rollenbasiert und unterstützt unterschiedliche Ablageorte für Benutzerkonten. Die Gruppe der Administratoren ist je nach Ablageort unterschiedlich benannt. Werden Benutzerkonten in einer Datenbank oder einem LDAP-Verzeichnis gespeichert, so heißt sie "Administrators". Werden die Benutzerkonten im ABAP-Stack gespeichert, so heißt sie "SAP_J2EE_ADMIN". Benutzer in dieser Gruppe haben keine kompletten administrativen Rechte, sondern nur Rechte für die Basisadministration und Benutzerverwaltung des Java-Stacks. Der generelle Notfallbenutzer für den Java-Stack ist das von SAP vorgegebene Benutzerkonto "SAP*", das aber nur dann verwendet werden kann, wenn der Java-Stack in den so genannten Single-User-Modus geschaltet wurde. In diesem Modus kann sich jedoch ausschließlich der Benutzer "SAP*" anmelden. Daher ist ein weiterer Notfallbenutzer erforderlich, der auch im Normalbetrieb einsetzbar ist.

Die Konten, die zur Notfall-Administration genutzt werden, sind mit starken Passwörtern auszustatten. Die verantwortlichen Personen müssen über den Aufbewahrungsort der Passwörter informiert sein. Nach einem Notfall sind die Passwörter so zu ändern, dass diese nur dann bekannt werden, wenn die Verfahren zur Notfall-Administration angewendet werden.

Es ist zu bedenken, dass die Konten, die zur Notfall-Administration verwendet werden, immer zugreifbar sein müssen. Sie dürfen also auch nicht deaktiviert oder gesperrt werden. Aus diesem Grund müssen die Zugangsdaten stark geschützt sein.

Wird ein Konto zur Notfall-Administration genutzt, ist nicht mehr nachzuvollziehen, welche Person auf das SAP System zugegriffen hat. Daher müssen die System-Administratoren und das Sicherheitsmanagement über den Notfall zeitnah unterrichtet werden. Dabei sind folgende Informationen mitzuteilen:

- Welcher Notfall lag vor?
- Durch wen und wann erfolgte der Zugriff?
- Welche Aktivitäten und Änderungen sind erfolgt?

**Backup**

Zu den regelmäßig durchzuführenden Maßnahmen der Notfallvorsorge gehört die Datensicherung eines SAP Systems. Im Rahmen des institutionsweiten Backup-Konzeptes muss während der Planungsphase auch die Datensicherung für ein SAP System konzipiert werden. Die Verantwortlichkeiten und Prozessabläufe sind zu definieren und umzusetzen.

Im Backup-Konzept muss unter anderem Folgendes festgelegt werden:

- Wann werden welche Komponenten und Daten gesichert?
- Wer besitzt die Berechtigung dazu?
- Wer besitzt die Berechtigung zum Wiederherstellen von Daten?
- Wer besitzt Zugriff auf die archivierten Backup-Daten?

- Wo werden die Backup-Daten sicher gelagert? Hier ist besonders darauf zu achten, dass Backup-Daten räumlich getrennt von Produktivdaten gelagert werden.

Die Daten eines SAP Systems werden zwar vornehmlich in der Datenbank abgelegt, die Datensicherung reduziert sich jedoch nur bei reinen ABAP-Stack-Installationen (z. B. bei SAP R/3 Systemen) darauf, lediglich die Datenbank zu sichern. Insbesondere der Java-Stack erfordert, dass weitere Daten gesichert werden. Dies sind vor allem die Daten aus dem SAP Verzeichnisbaum des Dateisystems.

Für den Java-Stack sind außerdem Sicherungen der Daten (z. B. weitere Datenbanken oder Dateien) durchzuführen, auf die die installierten Applikationen zurückgreifen. Werden diese nicht gesichert, kann es zu Inkonsistenzen in den Applikationsdaten kommen. Die verantwortlichen Administratoren müssen außerdem über den Aufbewahrungsort der Backup-Medien und über den Prozess der Wiederherstellung informiert sein.

Weitere Dokumentationen werden in M 2.346 *Nutzung der SAP Dokumentation* beschrieben.

**Ausweichsystem**

Kleine Unternehmen und Behörden betreiben unter Umständen ein SAP System, bei dem alle Komponenten auf einem Rechner (Single-Server-Installation) installiert sind. Liegt ein Notfall vor, der nicht durch das Einspielen gesicherter Daten behoben werden kann, z. B. bei einem Hardware-Defekt, so ist ein Ersatzsystem zu beschaffen. Da eine Ersatzbeschaffung in der Regel Zeit kostet, kann es zu langen Ausfallzeiten kommen. Daher wird empfohlen, ein Ausweichsystem vorzuhalten, das so weit vorbereitet ist, dass nur noch die letzte Datensicherung eingespielt werden muss, um den Betrieb wieder aufzunehmen.

Prüffragen:

- Wurde für SAP Systeme ein Notfall-Administrator-Konto eingerichtet und dessen Nutzung geregelt?
- Werden regelmäßige Datensicherungen des SAP Systems durchgeführt?
- Wurde ein Verfahren für das Wiederherstellen eines SAP Systems festgelegt?
- Wird bei hohen Verfügbarkeitsansprüchen ein Ausweichsystem für das SAP System vorgehalten?

# M 6.98 Notfallvorsorge und Notfallreaktion für Speicherlösungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Um die Verfügbarkeit und Integrität der Speicherlösung sicherzustellen, sind umfassende Maßnahmen zur Notfallvorsorge erforderlich. Diese können zum einen darin bestehen, rechtzeitig Fehler zu erkennen und zu behandeln und zum anderen aus den Anforderungen an den ordnungsgemäßen Betrieb resultieren. Darüber hinaus ist eine Dokumentation der Maßnahmen zur Notfallvorsorge erforderlich, um im Notfall die angemessene Behandlung sicherstellen zu können.

**Fehlerbehandlung bei Speicherlösungen**

In jedem IT-Betrieb treten Störungen auf, die vom sporadischen Fehlverhalten von Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf solche Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software beispielsweise aufgrund von Defekten oder Kompromittierungen.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische und für bereits aufgetretene Ausfallszenarien sollten Handlungsanweisungen erstellt werden. Eine kochbuchartige Dokumentation von Maßnahmen und Kommandos, die die Fehleranalyse und Fehlerkorrektur unterstützen, ist besonders hilfreich. Besteht in der Institution ein umfassendes Notfallmanagement (siehe Baustein B 1.3 *Notfallmanagement*), sollte es Vorlagen für solche Wiederherstellungspläne geben, die hier genutzt werden sollten. So kann sichergestellt werden, dass das Notfallteam alle Informationen in geeigneter Form vorliegen hat.

Gerade bei komplexen Systemen wie einer Speicherlösung ist die Darstellung von Verknüpfungen und Abhängigkeiten, die sich in jeder Institution individuell gestalten, entscheidend für die Beurteilung von Störungen und schnelles und zielgerichtetes Eingreifen.

Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört eine geeignete Protokollierung während des Betriebs (siehe auch M 2.359 *Überwachung und Verwaltung von Speicherlösungen*). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden. Dazu existieren sowohl frei verfügbare als auch kommerzielle Programme, oft auch vom Hersteller der Speicherlösung und seiner Komponenten. Die Verwendung geeigneter Werkzeuge ist umso wichtiger, da bei komplexen Lösungen nicht die Kontrolle und Steuerung der einzelnen Komponente, sondern die Übersicht über das Zusammenwirken von Hard- und Software der oftmals sehr heterogenen Gesamtlösung gefordert ist.

Die Pläne, um Störungen zu behandeln, und auch das automatisierte Vorgehen in einem Notfall (Umschwenken auf andere SANs, Replikationstests etc.) müssen getestet werden und sollten auch im Rahmen von Notfallübungen mitgeübt werden. Bei Notfalltests und Notfallübungen mit Speicherlösungen weist die Nachbereitung eine Besonderheit auf, da durch Tests und Übungen große

Datenmengen erzeugt werden. Diese Daten können besonderen Schutzbedarf bezüglich Vertraulichkeit aufweisen oder personenbezogene Daten enthalten. Insbesondere in einem solchen Fall, aber auch bei normalem Schutzbedarf müssen die Daten gemäß den Anforderungen nach Abschluss der Übung sicher gelöscht werden (siehe Maßnahme M 2.527 *Sicheres Löschen in SAN-Umgebungen*). Der hierdurch notwendige zusätzliche Aufwand muss in der Planung dieser Tests und Übungen berücksichtigt werden. Auch die Wiederanlauf- und Wiederherstellungspläne müssen die Löschung überflüssiger Daten, die im Rahmen der Bewältigung des Notfalls erzeugt wurden, mit berücksichtigen.

Es muss klar sein, dass gerade bei Speicherlösungen nach Störungen und Notfällen in Verbindung mit Datenverlust eine Rückführung in den Normalbetrieb nur dann möglich ist, wenn eine brauchbare Datensicherung bereitsteht. Eine Prüfung der Wiederherstellbarkeit von Datensicherungen (siehe M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*) muss regelmäßig durchgeführt werden.

Die Vorgehensweise bei der Fehlerbehandlung von Speicherlösungen lässt sich in die Bereiche Administration, Performancemessung und Diagnose unterteilen. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt:

**Administration**

In einem Betriebshandbuch sollten alle notwendigen Kommandos zur Administration und Konfiguration dokumentiert werden.

Folgende Bereiche sind zu berücksichtigen:

- Einrichten von (administrativen) Benutzern, Vergabe von Berechtigungen
- Update von Firmware und Betriebssystem
- Konfiguration
  - der Speicherressourcen
  - der administrativen Zugänge
  - der angeschlossenen Server und Sicherungsgeräte
- Protokollierung

**Performance**

Folgende Aspekte sollten für Beobachtungen und Aussagen über die Performance berücksichtigt werden:

- Belegung der Medien (pro logischem oder physischem Gerät)
- Durchsatz pro Interface (IP, FC etc.), bezogen auf das Gesamtsystem
- Statistikinformationen zur Nutzung

**Diagnose**

Alle für die Fehlerdiagnose ("Debugging") notwendigen Kommandos sowie die zu erwarteten Aussagen und ihre jeweilige Bedeutung sollten dokumentiert sein. Dazu zählen beispielsweise Aussagen über die Zustände der verschiedenen Systemkomponenten und Schnittstellen sowie über die aktuellen Konfigurationen.

Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant:

- Status der Netz-Interfaces und der sonstigen Anschlüsse
- Status der Netzdienste (TCP/IP bei NAS-Systemen, spezifische Informationen beim SAN, z. B. Status der SAN-Switches)
- Status zusätzlicher Komponenten (z. B. Storage-Virtualisierung)

- Gesamtkonfiguration als Überblick
- Prozesse
- Zuordnung
- Angemeldete Benutzer
- Protokollierung (Nutzung der Log-Level, Interpretation der Log-Informationen)

**Notfallvorsorge zur Steigerung der Verfügbarkeit**

Durch die Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit dem übergreifenden Notfallmanagement abzustimmen und sollten sich am allgemeinen Notfallkonzept orientieren (siehe Baustein B 1.3 *Notfallmanagement*). In dem allgemeinen Notfallkonzept werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen beziehungsweise Aufbau, Inhalt und Form fest. Allerdings sollten bei dieser Eingliederung in das allgemeine Notfallmanagement die Besonderheiten bei der Notfallvorsorge und Notfallbehandlung von Speichersystemen nicht unbeachtet bleiben. Die genauen Verfügbarkeitsanforderungen an die Speicherlösungen müssen klar definiert sein.

Folgende Fragestellungen sind für die Notfallvorsorge relevant:

- Was sind Gründe für mögliche Störungen?
  - Hardwaredefekte
  - Zu geringe Dimensionierung (Störung oder Ausfall bei Steigerung der Nutzung)
- Welche Anforderungen bestehen an das Monitoring zur Vermeidung von Notfällen?
- Wie kann eine frühzeitige Störungserkennung sichergestellt werden?
- Zusammenstellung der Informationen, die von den für den Betrieb der Speicherlösungen verantwortlichen Stellen immer ausgewertet werden
- Welche Vorsorgemaßnahmen können getroffen werden?
  - Vorhalten von Ersatzgeräten
  - Vorhalten von Ersatzteilen
  - Umsetzung von Failover-Lösungen, die es ermöglichen, im laufenden Betrieb auf ein Alternativgerät umzuschalten.
  - Abschluss von Wartungsverträgen
  - Ausbildung der Mitarbeiter
  - Umsetzung von Maßnahmen zur Replikation
  - Verbindungen sind redundant auszulegen
  - Redundante Verbindungen über unterschiedliche Trassen
  - Unterschiedliche Carrier pro Verbindung
  - Ausreichende Dimensionierung von Leitungskapazitäten (Notfall)
  - Umsetzung von Maßnahmen zur Daten-Recovery
  - Erstellung eines Betriebshandbuchs
  - Erstellung eines Notfallplans
  - Aufrechterhaltung der Datenkonsistenz
  - Wird die Speicherlösung als Archiv genutzt, das nicht mehr gesichert wird, muss mindestens eine zusätzliche Kopie jedes Objekts vorhanden sein.
- Datenhaltung
  - Für den Notfall ist im Betreiberkonzept festzuhalten, welche Daten gespiegelt werden (redundant vorgehalten werden) bzw. welche Daten im Notfall aus dem vorhandenen Backup wiederhergestellt wer-

den müssen. Die Grundlage für diese Vorgehensweise ergibt sich aus den vorhandenen SLAs.
  - Redundante Auslegung der IP- und FC-Netze
  - Redundante FC-Topologie unter Beachtung einer eineindeutigen WWN Vergabe
  - Redundante LAN-Topologie unter Beachtung einer eineindeutigen IP-Adressvergabe
  - Die Ausfallsicherheit von Segmentierung und Zoning ist durch redundante Auslegung der entsprechenden Netzkomponenten sicherzustellen.
- Besonderheiten bei Cloud-Speicherlösungen
  - Beim Einsatz von Cloud-Speicherlösungen ist darauf zu achten, dass die Orchestrierung ausfallsicher umzusetzen ist.
- Welche Service Level Agreements (SLAs) sollten getroffen werden?
  - Hardwarelieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten)
  - Verwaltung der Service Level Agreements: Es muss sichergestellt werden, dass SLAs rechtzeitig verlängert werden beziehungsweise rechtzeitig an die aktuellen Anforderungen angepasst werden.

Weitere Hinweise zur Notfallvorsorge und Notfallreaktion, gerade wenn an das SAN höherer Schutzbedarf bezüglich Verfügbarkeit besteht, sind im Hochverfügbarkeitskompendium auf den Internetseiten des BSI zu finden.

**Verwaltung von Service Level Agreements:**

SLAs werden in der Regel für einen begrenzten Zeitraum abgeschlossen und nicht immer automatisch verlängert. Darüber hinaus passiert es häufig, dass die Preise für die Verlängerung von SLAs für längere Zeiträume deutlich steigen oder dass diese für veraltete Systeme gar nicht mehr angeboten werden. In diesem Fall sollte geprüft werden, ob möglicherweise eine Investition in neue Speichersysteme langfristig kostengünstiger ist. Dies muss rechtzeitig berücksichtigt und geplant werden.

**Notfallvorsorge bei Cloud-Speicherlösungen**

Bei der Nutzung von Cloud-Speicherlösungen sollte sich eine Institution bereits bei der Auswahl eines Dienstleisters und der entsprechenden Vertragsgestaltung (M 2.356 *Vertragsgestaltung mit Dienstleistern für Speicherlösungen* und M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*) über Notfallvorsorgemaßnahmen des Anbieters erkundigen. Bedingt durch das starke Abhängigkeitsverhältnis von Cloud-Serviceprovidern ist die Notfallvorsorge allein aufseiten der nutzenden Institution nicht ausreichend. Weitere Hinweise zur Notfallvorsorge bei Cloud-Speicherlösungen finden sich unter anderem in M 6.155 *Erstellung eines Notfallkonzeptes für einen Cloud Service*.

**Dokumentation zur Notfallvorsorge**

Das genaue Vorgehen in bestimmten Notfallsituationen muss in einem Notfallplan beschrieben werden. Das Vorgehen sollte folgende Punkte beinhalten:

- Wie ist eine Diagnose durchzuführen? Folgende Informationen können dabei behilflich sein:
  - Statusabfragen
  - Anzeige der Konfiguration
  - Anzeige der laufenden Prozesse
  - Angemeldete Benutzer

    - Protokollierung
- Welche Entstörungsprozeduren müssen durchgeführt werden?
    - Vorgehen bei Ausfall der kompletten Speicherlösung (Wiederherstellen von Betriebssystem und Konfiguration)
    - Vorgehen bei Ausfall von Teilkomponenten, beispielsweise Festplatten
- Wer ist im Schadensfall zu benachrichtigen?
    - Server- und Anwendungsadministration
    - Hardwarelieferant/Ansprechpartner für den Wartungsvertrag
    - Alle notwendigen Informationen zu den Wartungsverträgen und Service Level Agreements, Hotline-Nummern, Kunden- oder Geräteidentifikationsnummern
- Welche Dokumente müssen im Schadensfall verfügbar sein?
    - Wartungsverträge
    - Grundkonfiguration zur (Wieder-)Inbetriebnahme
    - Änderungen der Grundkonfiguration, um die aktuelle Betriebskonfiguration einzurichten
    - Regelwerk für die Zugriffskontrolle (Access Control Lists)
    - Eingerichtete Benutzer und Berechtigungen
    - Passwörter für Notfallzugriffe
- Wie verläuft der Wiederanlauf?
    - Abhängigkeiten zu anderen Systemen des IT-Verbunds
    - Neuinstallation des Betriebssystems und Konfiguration
    - Zurückspielen einer gesicherten Konfiguration
    - Möglichkeiten eines eingeschränkten Betriebs
    - Remote-Betrieb an einem anderen Standort

Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Gerätetypen und Betriebssystemen berücksichtigt werden.

Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf einen externen Datenträger wie CD-ROM oder USB-Stick gesondert hinterlegt werden.

Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist die Vorhaltung von Ersatzteilen, um bei Hardwaredefekten die Ausfallzeiten zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden (Softwarewartung). Gegebenenfalls ist im Rahmen des allgemeinen Notfallmanagements ein gestaffelter Wiederanlauf für die Speicherlösung vorgesehen. In diesem Fall wird erst ein Teil der Speicherlösung wieder in Betrieb genommen, sodass die zeitkritischsten Geschäftsprozesse im nötigen Umfang eines Notbetriebs laufen können. In diesem Fall existieren neben den Wiederherstellungsplänen auch Wiederanlaufpläne, die den gleichen Anforderungen unterworfen sind, wie die Wiederherstellungspläne.

Durch den Einsatz von Speichervirtualisierung ergeben sich neue Möglichkeiten zur Notfallvorsorge. So kann beispielsweise eine redundante Speicherung

auf verschiedenen Speichersystemen durch die Speichervirtualisierung (Distributed LUN) gewährleistet werden. Auf diesem Weg wird ein Hot-Standby der Speicherlösung realisiert, durch das Ausfallzeiten fast gänzlich vermieden werden können.

Prüffragen:

- Existieren Handlungsanweisungen in Form von Maßnahmen und Kommandos, welche die Fehleranalyse und Fehlerkorrektur unterstützen?
- Werden für die Fehlerbehandlung geeignete Werkzeuge genutzt?
- Existiert ein Notfallplan für die eingesetzten Speicherlösungen, der das genaue Vorgehen in bestimmten Notfallsituationen beschreibt?
- Werden die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen regelmäßig erprobt?
- Werden bei den Tests und Übungen sowie im Notfall selbst hinterher die überflüssigen Daten gemäß ihrem Schutzbedarf gelöscht?

# M 6.99 Regelmäßige Sicherung wichtiger Systemkomponenten für Windows-Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Verantwortliche für die Datensicherung

Die Systemkomponenten eines Windows-Servers sind regelmäßig zu sichern, da der Server in Abhängigkeit von seiner Serverrolle ständigen Konfigurationsänderungen unterliegt. Unbeabsichtigte Änderungen, die Fehler im System provozieren können, wie fehlerhaftes Einspielen von Updates, können die Wiederherstellung wichtiger Systemkomponenten erforderlich machen. Wichtige Systemkomponenten sind nicht nur die eigentlichen Systemdateien, sondern auch Konfigurationsdaten, zum Beispiel Registrierdatenbank, IIS-Metabase, Statusinformationen, Datenbanken von DHCP, WINS und Protokolldaten. Die Sicherung kann von einem Sicherungsprogramm durchgeführt werden oder selektiv über das Dateisystem erfolgen, zum Beispiel per Skript. Generell müssen zumindest Statusinformationen und Protokolldaten mit der Windows Server-Sicherung oder einem geeigneten Drittprogramm täglich im Rahmen der Vorgaben eines Datensicherungskonzepts (siehe B 1.4 *Datensicherungskonzept*) gesichert werden.

**Systemstatussicherung (System State)**

Das Sicherungsprogramm von Windows Server 2003 (*Sicherung*) enthält den vordefinierten Sicherungsvorgang *Systemstatussicherung* (englisch *System State*). Er deckt in der Regel alle wichtigen Systemkomponenten aller Serverrollen ab, die in Windows Server 2003 mitgeliefert werden.

Unter Windows Server 2008 hat Microsoft eine neue Lösung für die Sicherung und Wiederherstellung eingeführt, die über die Microsoft Management Console mit dem Snap-In "*Windows-Server-Sicherung*" aufgerufen werden kann. Allerdings ist diese Komponente nicht im Umfang der Standard-Installation enthalten, sie muss separat nachinstalliert werden.

Wichtige Systemkomponenten können sich sowohl auf der Systempartition als auch auf anderen Festplattenpartitionen befinden. Dies hängt unter anderem davon ab, ob bei der Installation einer Komponente alternative Installationspfade konfiguriert wurden, zum Beispiel für Protokolldateien.

Die Systemdaten können mit dem jeweiligen Windows-Sicherungsprogramm gesichert werden. Dabei ermöglicht die Verwendung der Systemstatussicherung des Sicherungsprogramms

Wenn das Sicherungsprogramm beispielsweise auf einem Domänencontroller verwendet wird, werden mit Auswahl des Systemstatus vom bei der Installation gewählten Speicherort alle Systemkomponenten und alle verteilten Dienste gesichert, auf die Active Directory angewiesen ist.

**Beispiele für Systemstatusdaten:**

Systemstatusdaten nach Grundinstallation:

- Systemstartdateien
- Systemregistrierung
- Klassenregistrierungsdatenbank von COM+ (einer Erweiterung zu Component Object Model)

- Protokollierungsdateien
- Zusätzliche Systemstatusdaten auf einem Domaincontroller (exemplarisch):
- Verzeichnis SYSVOL
- DNS-Datenbank
- Active Directory

**Beispiele für weitere rollenspezifische Systemstatusdaten:**

- Clusterdienststatus (soweit installiert)
- Zertifikatsdienste-Datenbank (soweit installiert)

Es ist zu prüfen, ob entsprechend der Serverrolle und der installierten Serverprodukte noch weitere System- und/oder Programmordner außerhalb des vordefinierten Systemstatus gesichert werden müssen. Hierfür kann es erforderlich sein, die gesamte Systempartition sowie weitere Partitionen zu sichern.

**Datensicherungsprogramme**

Die Windows-eigenen Sicherungslösungen beinhalten nur Grundeigenschaften eines Datensicherungsprogramms und genügen nur einem geringen Schutzbedarf. Sie sind lediglich für die Sicherung der Windows-Server-eigenen Systemstatusdateien ausreichend, da sie unter anderem bei der Zuverlässigkeit (Prüfungsmechanismen führen keine Checksummenbildung durch) und Hardwareunterstützung eingeschränkt sind und nur rudimentäre Protokollierung, Überwachung, und Zeitplanung bieten. Es ist entsprechend der Serverrolle und den Anforderungen an die Datensicherung zu prüfen, ob Programme anderer Hersteller zu bevorzugen sind.

**Wiederherstellen von Systemstatusdaten**

Das Windows-Sicherungsprogramm kann nur die komplette Systemstatussicherung wiederherstellen. Programme von Drittanbietern ermöglichen zum Teil die Wiederherstellung von Konfigurationsdaten einzelner Rollen wie dem Active Directory. In jedem Fall muss vor der Wiederherstellung das Basisbetriebssystem identisch eingerichtet worden sein, sonst schlägt die Wiederherstellung entweder ganz fehl oder hinterlässt ein System mit nicht lauffähigen Parametern. Es ist zu klären:

Die Wiederherstellung des Systemstatus sollte niemals auf einem produktiven Server durchgeführt werden, auch nicht zu Überprüfungszwecken. Zur Umsetzung von M 6.41 *Übungen zur Datenrekonstruktion* kommt nur ein separates Testsystem in Frage. Genügt dies nicht dem Schutzbedarf des Systems, muss über alternative Sicherungsstrategien für den Systemstatus nachgedacht werden (z. B. Festplatten-Abbilder, Servervirtualisierung).

**Beispiel für ein Überprüfungsszenario:**

Die Systempartition befindet sich auf einem Laufwerk mit RAID-Level 1 (Spiegelung). Eine Festplatte wird aus dem RAID-Verbund entfernt und offline geschaltet, so dass der Originalzustand des Systems konserviert wird. Anschließend wird die Wiederherstellung des Systemstatus probeweise durchgeführt und das System auf seine Lauffähigkeit hin überprüft. Nach Abschluss des Tests wird die zuvor entfernte Platte wieder online geschaltet und zurückgespiegelt, so dass der Originalzustand wiederhergestellt ist.

**Notfallwiederherstellung (Disaster Recovery)**

Die in dem Datensicherungsprogramm von Windows Server 2003 enthaltene Sicherungskomponente *Automatische Systemwiederherstellung* (Automated

System Recovery, ASR) besteht aus zwei Funktionen. Zum einen gibt es eine Sicherungsfunktion, die aus dem Programm *Sicherung* aufgerufen wird, und zum anderen eine Wiederherstellungsfunktion, die bei der Windows-Server-2003-Installationsroutine mit *F2* aufgerufen werden kann. Bei der vorbereitenden Erstellung des ASR-Datensatzes werden die Systemstatusdaten, Systemdienste und alle mit den Betriebssystemkomponenten verknüpften Datenträger in eine Datei gesichert. Weiterhin wird bei der Erstellung einoder Datenträger mit Informationen zur Sicherung, zu Datenträgerkonfigurationen, wie Basisvolumen und dynamische Volumen und zu Informationen über die Wiederherstellung erstellt. Bei der Wiederherstellung mit ASR werden keine Nutzerdaten wiederhergestellt. Die ASR-Wiederherstellung stellt lediglich das Grundbetriebssystem bereit. Die Nutzerdaten und andere serverrollenabhängigen wichtigen Systemkomponenten müssen mit einer separaten Sicherung gesichert und gegebenenfalls wiederhergestellt werden. Sollte es entsprechend der Serverrolle Systemkomponenten geben, die nicht in einer Standardsicherung enthalten sind, ist zu prüfen, welches Verfahren zur Sicherung der wichtigen Systemkomponenten geeignet ist. ASR ist in so einem Fall nicht ausreichend. Weiterhin ist zu beachten, dass bei dem Verfahren Disketten (und damit ein unzuverlässiges Wechselmedium) notwendig sind und keine automatische regelmäßige Sicherung möglich ist. Daher ist, die für die Serverrolle geeignete Variante zur Sicherung wichtiger Systemdaten zu wählen und dieses Verfahren regelmäßig zu testen. Hierbei sind nicht nur Erfolg der Wiederherstellung, sondern insbesondere auch die benötigte Wiederherstellungszeit ausschlaggebend (siehe M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows-Systemen*).

Ab Windows Server 2008 ist in der Windows-Server-Sicherung die Erzeugung von Datensicherungen möglich, mit denen eine Wiederherstellung des Systems erfolgen kann. Hierbei stehen wahlweise die "vollständige Serversicherung" (mit allen Dateisystemen) und "Bare Metal Recovery" (nur mit den systemnotwendigen Dateisystemen) zur Verfügung. Die Wiederherstellung erfolgt über die Windows-Wiederherstellungsumgebung, die von einem Setup-Datenträger oder durch Drücken von F8 beim Systemstart und die Auswahl der Option *Computer reparieren* aufgerufen werden kann.

Prüffragen:

- Werden die wichtigen Systemkomponenten (z. B. Systemdateien, Konfigurationsdaten, Statusinformationen und Protokolldaten) von Windows Servern regelmäßig gesichert?
- Wurden auf einem Server 2008 die Windows -Server-Sicherung oder ein geeignetes Drittprogramm für die Datensicherung installiert und eingerichtet?
- Ist sichergestellt, dass vor der Wiederherstellung von Systemstatusdaten das Basisbetriebssystem identisch eingerichtet wird und eine Wiederherstellung nicht auf einem produktiven System erfolgt?
- Werden entsprechend der Serverrolle und der Verfügbarkeitsanforderungen die Wiederherstellung und die Wiederherstellungsdauer im Rahmen eines Notfallplans für den Server getestet und verbessert?

# M 6.100 Erstellung eines Notfallplans für den Ausfall von VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der teilweise oder komplette Ausfall der VoIP-Architektur hat in vielen Fällen gravierende Auswirkungen, denn die Telefonie ist meist einer der wichtigsten Dienste in einer Institution. Ein Ausfall kann viele Ursachen haben. Neben VoIP-typischen Problemen kann auch eine Störung einzelner Netzkomponenten zum vollständigen Ausfall des VoIP-Dienstes führen.

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für VoIP muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallmanagement*).
- Bei einem Ausfall von VoIP muss eine Telekommunikation weiter möglich sein. Daher ist zu klären, ob beim VoIP-Ausfall zumindest eine Notfall-Kommunikation möglich ist (zumindest zu Polizei, Feuerwehr). Außerdem muss es möglich sein, einen (externen) Support-Dienstleister zeitnah über den Ausfall zu informieren, damit der Fehler behoben werden kann. Bei einem Ausfall können beispielsweise Mobiltelefone zur Kommunikation genutzt werden, hierfür ist aber Vorsorge zu treffen.
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher sind im Rahmen des allgemeinen Datensicherungskonzepts (siehe auch B 1.4 *Datensicherungskonzept*) Regelungen für die VoIP-Komponenten zu erstellen. Darin muss nicht nur die VoIP-Middleware selbst berücksichtigt werden, sondern auch die Endgeräte mit den von Benutzern vorgenommen Einstellungen, wie beispielsweise Telefonbücher.
- Es müssen Vorkehrungen für den Fall getroffen werden, dass ein IT-System, auf dem ein Softphone betrieben wird, repariert werden soll. Müssen die Anwender für die Erfüllung ihrer Aufgaben telefonisch erreichbar sein, sind entsprechende Maßnahmen zu treffen.

Prüffragen:

- Existiert eine Regelung für einen Notfallplan bei Ausfall des VoIP-Dienstes?
- Existieren korrespondierende Notfallpläne für die IT-Systeme, die vom / zum Betrieb des VoIP-Dienstes abhängen / benötigt werden?
- Ausfall des VoIP-Dienstes: Existiert eine redundante Kommunikationsmöglichkeit über dedizierte Kanäle bzw. Anschlüsse?
- Existiert eine Regelung für ein Datensicherungskonzept der betroffenen VoIP-Komponenten?
- Ausfall des VoIP-Dienstes: Existieren redundante Kommunikationsmöglichkeiten, die die Benutzern im Rahmen ihrer Aufgabenerfüllung temporär nutzen können?

# M 6.101 Datensicherung bei VoIP

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Um bei Fehlkonfigurationen oder einem Ausfall, der nur durch den Austausch einer Komponente behoben werden kann, den VoIP-Betrieb schnell wieder aufnehmen zu können, müssen regelmäßig Sicherungen aller wichtigen Konfigurationsdateien angefertigt werden. Für die Datensicherung ist grundsätzlich die im Baustein B 1.4 *Datensicherungskonzept* genannte Vorgehensweise zu verwenden. Der Umfang der zu sichernden Dateien muss anhand der eingesetzten VoIP-Komponente ermittelt werden. Hierzu gehören unter anderem

- alle VoIP-spezifischen Konfigurationseinstellungen,
- übergeordnete Konfigurationseinstellungen, wie IP-Adressen, Passwörter und alle relevanten Konfigurationen des eingesetzten Betriebssystems,
- Protokolldaten und
- vom Benutzer individuell vorgenommene Einträge, wie persönliche Telefonbücher.

Diese Konfigurationseinstellungen müssen regelmäßig gesichert werden. Vor und nach jeder Änderung der Konfiguration ist ebenfalls eine Sicherung durchzuführen. Dabei ist darauf zu achten, dass mehrere Versionen (Generationen) der Sicherungsdateien gepflegt werden. Eine fehlerhafte Konfiguration kann durch das Einspielen der Version, die davor generiert wurde, oft behoben werden.

Es muss berücksichtigt werden, dass nach einem Release-Wechsel die vorhandenen Konfigurationsdateien eventuell nicht übernommen werden können. Wird nach einem Hardware-Ausfall ein Gerät mit einem aktuelleren oder älteren Release eingesetzt, können die vorhandenen Konfigurationsdateien eventuell nicht direkt übernommen werden. Daher sind bei einem Austausch aktuelle Hersteller-Informationen, beispielsweise aus Changelog-Dateien, zu sichten und zu berücksichtigen. Müssen die Konfigurationsdateien bei einem Release-Wechsel angepasst werden, muss sowohl die alte als auch die neue Version gesichert werden. Bei Problemen mit dem neueren Release kann auf diese Weise auch zu einem späteren Zeitpunkt auf die alte, eventuell stabilere Version gewechselt werden.

Die Datensicherung ist auf IT-Systemen und Medien durchzuführen, die von den für den Betrieb verwendeten IT-Systemen und Medien unabhängig sind. Dies können zum Beispiel Bandlaufwerke, CD-RWs oder andere IT-Systeme sein. Bei der Übertragung auf ein anderes System über ein Netz sollte überlegt werden, die Daten zu verschlüsseln oder über eigenes Administrationsnetz zu übertragen, um sie vor Abhören und Manipulationen zu schützen.

Es müssen regelmäßig Recovery-Übungen durchgeführt werden, um die Wiederherstellbarkeit der Sicherung zu prüfen (siehe hierzu auch M 6.41 *Übungen zur Datenrekonstruktion*).

Prüffragen:

- Existiert eine Regelung zur Festlegung von Inhalten und Umfang der Datensicherung?
- Werden unterschiedliche Versionen von Konfigurationen und Veränderungen nachvollziehbar dokumentiert?
- Sind die Sicherungsdateien der Konfiguration so beschaffen, dass sie im Konfliktfall nachvollzogen und rückgängig gemacht werden können?

- Werden Störungs- und Notfallprozeduren regelmäßig getestet?

# M 6.102 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Falls sich das WLAN in nicht vorgesehener Weise verhält (z. B. WLAN ist längere Zeit nicht verfügbar, Zugriff auf Netzressourcen ist nicht möglich, Netzperformance bricht dauerhaft ein), kann dies durch einen Sicherheitsvorfall verursacht worden sein. Dieser kann durch einen Angreifer, Fehlkonfigurationen oder Systemfehler herbeigeführt worden sein.

Dann sollten die Benutzer folgende Punkte beachten:

- Sie sollten ihre Arbeitsergebnisse sichern, den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Sollten Fehlermeldungen erscheinen oder sich der Client nicht normal verhalten haben, so sollten diese durch die Benutzer genau dokumentiert werden. Ebenso sollte dokumentiert werden, was der Benutzer getan hat bevor bzw. während der Sicherheitsvorfall eingetreten ist. Dadurch kann der Grund für den Vorfall durch die Administratoren eventuell schneller eingegrenzt und schneller Gegenmaßnahmen eingeleitet werden.
- Die Administratoren müssen über eine geeignete Eskalationsstufe (z. B. User Help Desk) von den Benutzern benachrichtigt werden. Dabei ist sicherzustellen, dass der Administrator durch den Benachrichtigungsprozess in seiner Arbeit nicht wesentlich behindert wird.

Die Administratoren sollten bei einem Sicherheitsvorfall passende Gegenmaßnahmen einleiten. Mögliche Aktionen sind z. B.:

- Abschaltung von Access Points
- Sperren der Kommunikation am Übergabepunkt zwischen Distribution System und LAN / Internet
- Herunterfahren von Servern (Web-Server oder Steuerungsserver im Produktionsumfeld oder ähnliches)
- Deaktivierung der WLAN-Schnittstelle des WLAN-Clients
- Überprüfung der Konfigurationen der Access Points
- Sicherung aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sicherung aller relevanten Protokolldateien
- gegebenenfalls Wiedereinspielen der Original-Konfigurationsdaten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*)
- Benachrichtigung der Benutzer mit der Bitte, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Falls Access Points gestohlen worden sind, müssen gezielte Sicherheitsmaßnahmen ergriffen werden, wie z. B.:

- Änderung aller eingesetzten kryptographischen Schlüssel, also z. B. der PSKs im Falle der Verwendung von WPA-PSK bzw. WPA2-PSK
- Konfigurationsänderung auf RADIUS-Servern zum Ausschluss des entwendeten Access Point (IP, Name, RADIUS-Client, Shared Secret, IPSec)

Die möglichen Konsequenzen sicherheitskritischer Ereignisse müssen untersucht werden. Letztlich sind alle erforderlichen Maßnahmen zu ergreifen, um eine missbräuchliche Verwendung von entwendeten Geräten zum Zugriff auf das Netz der Institution auszuschließen. Falls ein WLAN-Client entwendet

worden ist, müssen bei der Verwendung einer zertifikatsbasierten Authentisierung auch die Client-Zertifikate gesperrt werden.

Prüffragen:

- Sind entsprechende Eskalationsstufen bei Sicherheitsvorfällen definiert?
- Sind die verantwortlichen Mitarbeiter für die Behandlung von WLAN-Sicherheitsvorfällen bestimmt?
- Sind Verhaltensregeln und Maßnahmen bei Sicherheitsvorfällen im WLAN-Bereich definiert?

# M 6.103 Redundanzen für die Primärverkabelung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Leiter IT

Oft sind in größeren Liegenschaften mehrere Gebäude an ein Rechenzentrum, das sich in einem dieser Gebäude befindet, sternförmig angebunden. Es ist zu prüfen, ob zumindest für wichtige Gebäude eine redundante, über unabhängige Trassen geführte primäre IT-Verkabelung geschaffen werden soll.

Ebenso ist zu prüfen, ob die Anschlüsse an IT- oder TK-Provider redundant ausgelegt werden sollen. Um hier eine echte Redundanz zu schaffen, muss mit dem Provider geklärt werden, ob wirklich an unterschiedlichen Orten (Ortsvermittlungsstellen) der Anschluss an ein Carrier-Netz geschaffen wird.

Ob eine redundante Primärverkabelung beziehungsweise eine redundante Anbindung an Provider erforderlich ist, ergibt sich aus den Verfügbarkeitsanforderungen der Institution.

### Parallelbetrieb

Innerhalb der Gebäude ist durch den Einsatz geeigneter aktiver Netzkomponenten sicherzustellen, dass die redundanten Leitungen im Betrieb automatisch parallel genutzt werden. So wird gleichzeitig Redundanz geschaffen und die Kapazität erhöht. Dabei ist jedoch zu beachten, dass sich beim Ausfall einer der Leitungen die Übertragungskapazität reduziert. Diese reduzierte Kapazität muss im Notfallvorsorge-Konzept berücksichtigt werden.

### Umschaltung

Wenn die eingesetzte Technik oder die über die Verkabelung realisierten Dienste keinen Parallelbetrieb der redundanten Leitungen erlauben, muss bei Störungen der genutzten Leitung auf die jeweilige Ersatzleitung umgeschaltet werden. Diese Umschaltung kann automatisch oder manuell erfolgen.

Wenn kein Parallelbetrieb möglich ist, sollte in sinnvollen Zeitabständen auf die Ersatzleitungen umgeschaltet werden, auch wenn keine tatsächliche Störung vorliegt. Dies dient dazu, die Ersatzleitungen auf Funktionsfähigkeit zu überprüfen. Die Prüfintervalle sollten aus den Verfügbarkeitsanforderungen abgeleitet werden.

### Überwachung

Redundanzen bei den Kommunikationsverbindungen können in der Regel nur dann das Verfügbarkeitsniveau wirksam steigern, wenn die Funktionsfähigkeit der Verbindungen überwacht wird. Die Überwachung dient dazu, Störungen, Engpässe und sonstige Unregelmäßigkeiten frühzeitig zu erkennen, damit Probleme zeitnah behoben oder sogar vermieden werden können. Ohne Überwachung besteht unter anderem die erhöhte Gefahr, dass Ausfälle von Leitungen nicht erkannt werden und in diesem Fall nur eine scheinbare, aber keine tatsächliche Redundanz besteht.

Prüffragen:

- Wurde geprüft, ob wegen hohen Verfügbarkeitsanforderungen eine redundante Primärverkabelung beziehungsweise eine redundante Anbindung an Provider erforderlich ist?

- Findet eine regelmäßig Prüfung der Funktionsfähigkeit der redundanten Verkabelung statt?

# M 6.104 Redundanzen für die Gebäudeverkabelung

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Haustechnik, Leiter IT

Bei hohen oder sehr hohen Verfügbarkeitsanforderungen sollte überlegt werden, in den relevanten Gebäuden die Sekundär- und Tertiärverkabelung redundant auszulegen.

Dazu wird die Sekundärverkabelung, also die Verbindung der Etagen, über mindestens zwei Steigeschächte geführt, die sich in verschiedenen Brandabschnitten des Gebäudes befinden sollten. Beispielsweise könnte die Sekundärverkabelung an den gegenüberliegenden Gebäudeseiten (z. B. Nord und Süd oder Ost und West) geführt werden.

Alle Räume, in denen Teilnehmer zu versorgen sind, werden jeweils an beide Sekundärverkabelungen angeschlossen. Die Hälfte der Anschlüsse in einem Raum wird dann mit einem Verteiler auf der einen Gebäudeseite verbunden, die andere Hälfte der Anschlüsse wird an einen Verteiler auf der anderen Seite des Gebäudes angeschlossen. In der folgenden Abbildung werden die beiden Gebäudehälften schematisch als "linke" und "rechte" Seite bezeichnet.

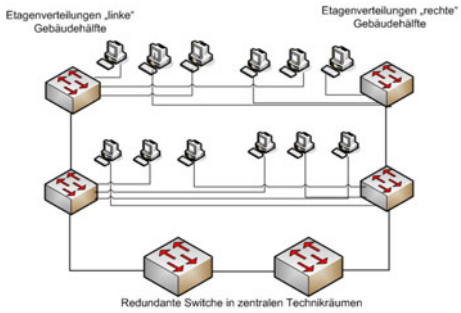



Abbildung 1: Schema einer redundanten Anbindung der Anwender

Damit ist es auch bei einem gravierenden Schaden möglich, den Betrieb auf den Etagen mindestens behelfsweise aufrecht zu erhalten, sofern der Schaden nicht beide Gebäudehälften betrifft.

Prüffragen:

- Wurde geprüft, ob wegen hohen Verfügbarkeitsanforderungen die Sekundär- und Tertiärverkabelung redundant ausgelegt werden sollten?

# M 6.105 Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Ein längerer Ausfall der vorhandenen Drucker, Kopierer und Multifunktionsgeräte ist meist nicht tolerierbar. Besonders der Ausfall zentraler Komponenten, die für die gesamte Drucker-Infrastruktur erforderlich sind, kann zu erheblichen Beeinträchtigungen der Geschäftsprozesse führen. Je nach Verfügbarkeitsanforderungen sind daher geeignete Maßnahmen zu ergreifen, um die Ausfallszeit beziehungsweise die Auswirkungen von Ausfällen zu verringern.

Es ist darauf zu achten, dass immer genügend Verbrauchsmaterial verfügbar ist, z. B. Toner und Papier. Ab einer bestimmten Restmenge, die vom Verbrauch abhängig ist, muss neues Verbrauchsmaterial beschafft und bereitgestellt werden. Weitere Hinweise finden sich in der Maßnahme M 2.52 *Versorgung und Kontrolle der Verbrauchsgüter*.

An jedem Kopierer, Drucker und auch an anderen Komponenten des Drucksystems müssen diverse Konfigurationseinstellungen vorgenommen werden. Um diese Einstellungen nach einem Ausfall oder Austausch schnell wieder korrekt einrichten zu können, müssen die Konfigurationen systematisch dokumentiert werden (siehe auch M 2.25 *Dokumentation der Systemkonfiguration*).

Je weniger Drucker bzw. Kopierer zur Verfügung stehen, desto gravierender ist ein Ausfall eines einzelnen Geräts. Der Ausfall eines Druckservers ist besonders problematisch, da hiervon in der Regel nur ein oder wenige Geräte vorhanden sind.

Um auf Notfälle reagieren zu können, sollte zwischen zentralen Komponenten einerseits und Druckern und Kopierern andererseits unterschieden werden. Bei einem höheren Schutzbedarf bezüglich der Verfügbarkeit sollte überlegt werden, zentrale Komponenten, wie Druckserver, redundant auszulegen. Wenn der einzige zentrale Server ausfällt, könnte sonst unter Umständen im gesamten LAN nicht mehr gedruckt werden.

Dezentrale Komponenten, wie Drucker, sind häufig auf mehreren Etagen oder in verschiedenen Büros eines Gebäudes zu finden. Generell sollte die Druckerlandschaft so gestaltet werden, dass die Benutzer bei dem Ausfall eines Druckers problemlos einen anderen Drucker verwenden können.

- Es sollte überlegt werden, für lokale Drucker, die einen höheren Schutzbedarf bezüglich der Verfügbarkeit haben und direkt an einen Arbeitsplatz angeschlossen werden, Ersatzgeräte bereitzustellen ("Cold Standby"). Bei einem Ausfall könnte der defekte Drucker zeitnah durch das Ersatzgerät ausgetauscht werden.
- Für große Kopierer und Drucker, die von mehreren Personen benutzt werden, sollten Wartungsverträge mit einer dem Schutzbedarf angemessenen Reaktionszeit abgeschlossen werden.
- Es sollte eine Liste von Fachhändlern geführt werden, bei denen unproblematisch neue Geräte beschafft werden können.
- Bei Bedarf können Ersatzteile gelagert werden, die häufig benötigt werden. Dies ist allerdings nur sinnvoll, wenn entsprechendes Fachwissen vorhanden ist, um die Ersatzteile selbstständig austauschen zu können.

Prüffragen:

- Wurden geeignete Maßnahmen ergriffen, um die Ausfallzeiten von Druckern, Kopierern und Multifunktionsgeräten zu verringern?
- Ist immer genug Verbrauchsmaterial für Drucker, Kopierer und Multifunktionsgeräte vorhanden?

# M 6.106 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Der teilweise oder komplette Ausfall eines Verzeichnisdienstes hat in der Regel gravierende Auswirkungen auf die Arbeitsmöglichkeiten von Benutzern. Bei Ausfall eines Verzeichnisdienst-Servers können beispielsweise keine Server-basierten Aktionen mehr ausgeführt werden. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls von Verzeichnisdienst-Komponenten minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für das Verzeichnisdienst-System muss in den existierenden Notfallplan integriert werden (siehe Baustein B 1.3 *Notfallmanagement*).
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Konzept für die Datensicherung der Verzeichnisdatenbank zu erstellen, das in das bisherige Backup-Konzept integriert werden kann oder dieses ablöst. Weitere Hinweise hierzu finden sich in Baustein B 1.4 *Datensicherungskonzept* sowie in Maßnahme M 6.107 *Erstellung von Datensicherungen für Verzeichnisdienste*.
- Werden von wichtigen Informationen und Dateien Replikate auf mehreren Servern angelegt, so kann beim Ausfall einzelner Verzeichnisdienst-Server auf diese Replikate zugegriffen werden. Über die Replikationsmechanismen von Verzeichnisdiensten ist es möglich, Benutzern eine jeweils räumlich nahe Replik von Daten zur Verfügung zu stellen, um so gute Zugriffszeiten und eine hohe Verfügbarkeit der Server zu erreichen (siehe M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst*).
- Ein Verzeichnisdienst bietet die Möglichkeit, die Verzeichnisdatenbank auf mehrere Verzeichnisdienst-Server zu verteilen (partitionieren), so dass jeder Server nur einen Teil der Daten hält. Bei Ausfall eines Verzeichnisdienst-Servers ist somit nur die dort gespeicherte Partition des Verzeichnisses betroffen (siehe M 2.409 *Planung der Partitionierung und Replikation im Verzeichnisdienst*). Bei der Erstellung eines Notfallplans muss darauf geachtet werden, dass alle Partitionen einer Verzeichnisdienst-Installation berücksichtigt werden.
- Die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten ist zu dokumentieren. Alle Aufgaben zur Wiederherstellung des Systems müssen so beschrieben werden, dass sie im Notfall auch von Personal durchgeführt werden können, das keine detaillierten Kenntnisse der vorher vorhandenen Systemkonfiguration hat.
- Durch die Notfallplanung muss sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht.
- Es muss ein Wiederanlaufplan erstellt werden, der einen geregelten Neustart des Verzeichnisdienst-Systems gewährleistet.
- Die Notfallplanung muss die Besonderheiten wichtiger Verzeichnisdienst-Server in Betracht ziehen und darauf eingerichtet sein.

Im Rahmen der Notfallvorsorge sollten unterschiedliche Szenarien betrachtet werden, in denen das Verzeichnisdienst-System oder Teile davon kompromit-

tiert werden. Für diese Szenarien sollte im Notfallplan möglichst präzise beschrieben werden, wie jeweils zu reagieren ist und welche Aktionen auszuführen sind. Die Reaktionen sollten regelmäßig geübt werden.

Die rechtzeitige Notfallplanung mit vorgegebenen Handlungsanweisungen, die auch durch Personen durchgeführt werden können, die nicht mit der Systemadministration vertraut sind, kann im Schadensfall die Auswirkungen abmildern. Es ist zu beachten, dass die entsprechenden Dokumente für die Notfallsituation wichtige und schützenswerte Informationen beinhalten, so dass diese geschützt aufbewahrt werden müssen. Trotzdem müssen die berechtigten Personen im Notfall darauf zugreifen können.

Im Einzelnen sollten mindestens die folgenden Notfallsituationen betrachtet werden:

**Angriffe**

Werden Angriffe auf einen Verzeichnisdienst, beispielsweise durch die Ausweitung der Benutzerrechte, aufgedeckt, kann ohne detaillierte Sicherheitsanalysen nicht davon ausgegangen werden, dass das Löschen des verursachenden Kontos die betroffenen Systeme wieder in einen sicheren Stand bringt. Es muss vielmehr in Betracht gezogen werden, dass Änderungen an der Systemkonfiguration durchgeführt oder Schadprogramme (z. B. Backdoors, Trojanische Pferde) installiert wurden.

Um zuverlässig mögliche Schadprogramme zu entfernen, wird eine komplette Wiederherstellung der betroffenen Verzeichnisdienst-Komponenten empfohlen, so dass eine vertrauenswürdige Basis sichergestellt ist. Hierfür sind die erstellten Datensicherungen zu verwenden, aber auch die Aufzeichnungen über die genaue Konfiguration und die Sicherheitsrichtlinien des Verzeichnisdienstes. Darüber hinaus sind zumindest alle Konten mit erweiterten Rechten (insbesondere die der Administratorengruppen) auf deren Gruppenzugehörigkeit zu prüfen und umgehend mit neuen Passwörtern zu versehen, um die Erfolgschancen von Folge-Angriffen zu minimieren. Bei den Benutzerkonten sollten ebenfalls die Passwörter geändert werden. Des Weiteren ist eine Ursachenforschung zu betreiben und deren Ergebnisse und Erfahrungen in die bestehenden Sicherheitskonzepte zu übernehmen.

**Diebstahl**

Bei Diebstahl von Verzeichnisdienst-Komponenten sind umgehend alle bestehenden Konten, insbesondere die mit erweiterten Rechten, mit neuen Passwörtern zu versehen. Des Weiteren ist auch hier eine ausführliche Sicherheitsanalyse und Ursachenforschung notwendig und auf Basis dieser Ergebnisse vor allem eine umfassende Anpassung der Infrastruktur-Sicherheitsvorkehrungen. Im Zweifelsfall sollte die komplette Verzeichnisdienst-Gesamtstruktur neu aufgesetzt werden.

Sowohl im Falle eines Angriffes als auch bei einem erfolgten Diebstahl sind die verantwortlichen Personen über die verbesserten Sicherheitskonzepte in Kenntnis zu setzen und zu deren Einhaltung anzuhalten.

**Fehlkonfigurationen**

Fehlkonfigurationen im Bereich der Systemadministration können sich im weiteren Verlauf negativ auf die Gesamtstruktur eines Verzeichnisdienstes auswirken. Die Verzeichnisdienst-Systeme sollten regelmäßig auf Fehlkonfigura-

tionen untersucht werden. Sobald solche entdeckt werden, muss deren Ausmaß bewertet werden und mit Korrekturmaßnahmen begonnen werden.

Die notwendigen Änderungen für die Behebung der Konfigurationsfehler können je nach Ausprägung direkt vorgenommen werden oder aber bei umfangreicheren Problemen durch Rückspielen aktueller System-Datensicherungen bis hin zur Neueinrichtung des Systems. Kann die Auswirkung oder die Ursache der Fehlkonfiguration nicht zweifelsfrei ermittelt werden, so wird eine Wiederherstellung des Verzeichnisdienstes mit einem vertrauenswürdigen Stand empfohlen.

Damit gleiche Probleme in Zukunft vermieden werden, sind die Sicherheitsrichtlinien zu prüfen und bei Bedarf anzupassen. Des Weiteren ist die Vorgehensweise innerhalb des Testnetzes und der Produktivumgebung zu analysieren, um durch die im Testnetz gesammelten Erfahrungen die Ausfallzeiten und Fehlkonfigurationen im Produktivnetz auf ein Minimum reduzieren zu können.

**Ausfälle durch Höhere Gewalt**

Durch Gefährdungen aufgrund von höherer Gewalt, z. B. Erdbeben, Überschwemmung, Feuer, Sturmschäden, Kabelbeschädigungen, kann die Verfügbarkeit des Verzeichnisdienstes negativ beeinflusst werden. Hier sind angemessene Maßnahmen zur Erhöhung der Verfügbarkeit zu überlegen, wie beispielsweise redundante Kommunikationsverbindungen oder IT-Systeme.

Prüffragen:

- Wurde eine bedarfsgerechte Notfall-Planung für Verzeichnisdienste durchgeführt?
- Liegen Notfallpläne für den Ausfall wichtiger Verzeichnisdienst-Systeme vor?
- Wurden alle Notfall-Prozeduren für Verzeichnisdienst-Komponenten dokumentiert?

# M 6.107 Erstellung von Datensicherungen für Verzeichnisdienste

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Die Datensicherung eines Verzeichnisdienstes sollte in das globale Datensicherungskonzept der Institution integriert werden.

Um konsistente Datensicherungen des Verzeichnis-Datenbestands auf einem Server zu erhalten, sollte ein spezielles Backup-Werkzeug verwendet werden. Neben einer Vollsicherung des Verzeichnisses bieten die Werkzeuge auch die Möglichkeit, nur Teile des Verzeichnisdienstes zu sichern. Um einzelne Verzeichnisdienst-Objekte zu archivieren oder wiederherzustellen, muss der vollständige Distinguished Name des Objektes spezifiziert werden. Um den gesamten Baum zu sichern, muss das jeweilige Baum-Objekt angegeben werden. Auch das Schema kann gesondert gesichert werden, hierzu muss das Schema-Objekt selektiert werden. Schließlich können ebenfalls Teile eines Verzeichnisdienst-Baums gesichert werden, hierzu muss der entsprechende Container des Baumes ausgewählt werden. Es werden dann sämtliche Objekte unterhalb dieses Containers gesichert.

Partitionsinformationen können mit diesen Backup-Werkzeugen nicht gesichert werden. Im Wiederherstellungsfall müssen die entsprechenden Teile nachträglich partitioniert werden. Daher muss die Partitionierung des Verzeichnisdienstes schriftlich dokumentiert werden, so dass sie nach einem Systemausfall manuell wieder rekonstruiert werden kann. Zu diesem Zweck sollten unbedingt gedruckte Kopien der Baumstruktur und der Partitionen angefertigt und regelmäßig aktualisiert werden.

Prüffragen:

- Ist die Partitionierung des Verzeichnisdienstes schriftlich dokumentiert, so dass sie nach einem Systemausfall manuell wieder rekonstruiert werden kann?

# M 6.108 Datensicherung für Domänen-Controller

**Verantwortlich für Initiierung:** Fachverantwortliche, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Da Domänen-Controller üblicherweise zentrale Authentisierungs- und Autorisierungsaufgaben für den Zugriff auf wichtige Ressourcen im Netz ermöglichen, führt ein Ausfall unmittelbar zu schwerwiegenden Beeinträchtigungen im Netz. Daher muss für die Datensicherung der Domänen-Controller als zentrale IT-Komponenten eine geeignete Vorgehensweise festgelegt werden. Diese sollte entweder im Datensicherungskonzept der Institution oder in einer eigenständigen Datensicherungsrichtlinie dokumentiert sein. Die grundsätzliche Vorgehensweise wird im Baustein B 1.4 *Datensicherungskonzept* beschrieben. Darüber hinaus sind zusätzlich Domänen-Controller-spezifische Besonderheiten bei der Entwicklung der Datensicherungsrichtlinie für Active Directory zu berücksichtigen. Dieses Regelwerk sollte folgende Aspekte berücksichtigen:

- Auf Domänen-Controllern müssen regelmäßig und nachvollziehbar Datensicherungen durchgeführt werden.
- Es sollten für Datensicherungen keine organisationsweiten, allgemeinen Benutzerkonten verwendet werden.
- Datensicherungssysteme sollten nur an Standorten aufgestellt werden, bei denen die Sicherheit der Hardware und Medien gewährleistet ist.
- Es muss regelmäßig getestet werden, ob sich die Domänen-Controller unter Verwendung der Sicherungsmedien wiederherstellen lassen.
- Ausgesonderte Datensicherungsmedien müssen vernichtet werden.

Gegenüber herkömmlichen Server-Sicherungen sollten bei Domänen-Controllern die im Folgenden genannten Punkte zusätzlich betrachtet werden.

Die Wiederherstellung eines ausgefallenen Domänen-Controllers wird selten unter alleiniger Zuhilfenahme von Datensicherungsmedien durchgeführt. Bewährt hat sich hierbei die Hochstufung eines Mitgliedsservers zum Domänen-Controller und anschließende Replizierung der Active Directory-Daten von einem anderen Domänen-Controller. Diese Methode kann allerdings nur dann verwendet werden, wenn durch den Einsatz mehrerer Domänen-Controller nach dem Ausfall eines oder mehrere Systeme noch mindestens ein gültiges Replikat des Active Directory existiert.

Existiert lediglich ein Domänen-Controller oder ist nach dem Ausfall der Domänen-Controller kein ActiveDirectory-Replikat mehr verfügbar, so muss die Wiederherstellung über die Datensicherungsmedien erfolgen. Dabei ist zu beachten, dass unter Umständen Probleme wie fehlerhafte Sicherungsmedien, unvollständige Wiederherstellungsverfahren oder fehlende Verfahrenskenntnisse bei den Verantwortlichen auftreten können. Um diesen Problemen entgegenzuwirken ist sicherzustellen, dass die Administratoren mit den Wiederherstellungsverfahren für die Gesamtstruktur vertraut sind.

**Auswahl kompatibler Sicherungssoftware**

Werden die Metadaten der zu sichernden Dateien vom Datensicherungsprogramm nicht korrekt behandelt, so kann dies ebenso wie bei der Verwendung ungeeigneter Virenschutzprogramme zu einer erhöhten Dateireplizierung durch den File Replication Service (FRS) führen (siehe G 4.68 *Störungen des Active Directory durch unnötige Dateireplizierung*).

Ähnlich wie beim Einsatz von Virenschutz-Programmen (siehe M 2.414 *Computer-Viren-Schutz für Domänen-Controller*) ist daher bei der Auswahl der Datensicherungssoftware zwingend darauf zu achten, dass die einzusetzende Software für die Datensicherung von Domänen-Controllern vom Hersteller freigegeben wurde.

**Besondere Sicherheitsanforderungen**

Das Dienstkonto, mit dem Domänen-Controller gesichert werden, muss über Dienste-Administratorrechte und damit über hohe Rechte verfügen. Um dem Missbrauch dieser Rechte vorzubeugen, sollte der Benutzerkreis, der Zugang zu diesen Konten hat möglichst gering gehalten werden.

Daher empfiehlt es sich, für den Sicherungsagenten auf den Domänen-Controllern andere Dienstkonten zu verwenden als auf den übrigen Servern der Institution. Unterschiedliche Benutzerkonten auf Domänen-Controllern und anderen Servern schützen darüber hinaus den Domänen-Controller zusätzlich, für den Fall, dass ein herkömmlicher Server der Organisation kompromittiert wurde.

Des Weiteren sollten die Mitglieder der Gruppe "Sicherungs-Operatoren" auf Benutzer beschränkt werden, die zur Datensicherung der Systemdateien erforderlich sind. Benutzer, die für die Datensicherung von Anwendungsdaten zuständig sind, sollten nicht Mitglied der Gruppe "Sicherungs-Operatoren" des Domänen-Controllers sein. Vielmehr sollten diese Benutzer als Mitglieder in der lokalen Gruppe "Sicherungs-Operatoren" des jeweiligen Anwendungsservers eingetragen werden.

Die Domänen-Gruppe "Sicherungs-Operatoren" ist standardmäßig nicht besonders geschützt. Um einen entsprechenden Schutz umzusetzen, ist der Zugriff auf das entsprechende AdminSDHolder-Objekt (Containerobjekt zur Speicherung von Berechtigungen) möglichst eng zu reglementieren (siehe *Zugriffsschutz-Anpassung für die Domänen-Gruppe "Sicherungs-Operatoren"* in *Hilfsmittel zum Active Directory*).

Es müssen in regelmäßigen Abständen Datensicherungen der Domänen-Controller durchgeführt werden. Bei der Festlegung eines geeigneten Sicherungsintervalls ist zu berücksichtigen, dass zur Löschung markierte Active Directory-Objekte nicht direkt aus dem ActiveDirectory entfernt, sondern zunächst in einen speziellen Container des Active Directory ("Gelöschte Objekte") verschoben werden. Solche zur Löschung markierten Objekte werden als veraltete oder auch als "Tombstone"-Objekte bezeichnet.

Nach einer einstellbaren Zeitdauer (Standard: 60 Tage) werden die veralteten Objekte dann endgültig gelöscht. Dieses Verfahren hat den Vorteil, dass vermeintlich gelöschte Objekte innerhalb der Frist wieder aktiviert werden können.

Bei der Löschung wird das Konto deaktiviert, so dass es nicht mehr genutzt werden kann. Stellt sich allerdings heraus, dass das Konto voreilig gelöscht wurde, kann es schneller wiederhergestellt werden.

Um Probleme bei der Replizierung zu vermeiden, sollte darauf geachtet werden, dass die Datensicherungen keine bzw. so wenig wie möglich veraltete Objekte mit überschrittener Lebensdauer beinhalten. Um dies sicherzustellen, sollten die Sicherungsmedien nach circa 75% der Lebensdauer von veralteten Objekten im Rahmen der regelmäßigen Sicherung überschrieben werden. Es sollte also möglichst häufig gesichert werden, allerdings sind die Backup-

Medien nach 45 Tagen (bei einer Objektlebensdauer von 60 Tagen) wieder mit neuen Backups zu überschreiben, damit eine Wiederherstellung veralteter Objekte ausgeschlossen wird.

Da die Datensicherungsmedien der Domänen-Controller alle Informationen der Active-Directory-Datenbank beinhalten, sollten für jene die gleichen physikalischen Sicherheitsvorkehrungen getroffen werden, wie sie auch für die Domänen-Controller gelten (siehe hierzu M 4.313 *Bereitstellung von sicheren Domänen-Controllern*, Abschnitt physikalische Sicherheit). Insbesondere für die Sicherung in Niederlassungen muss überprüft werden, ob eine ausreichende Sicherheit der Sicherungshardware und -medien gewährleistet werden kann. Hierfür gibt es folgende Möglichkeiten:

- Es erfolgt keine Datensicherung der Domänen-Controller in den Niederlassungen.
- Die Datensicherung in den Niederlassungen erfolgt mit Hilfe von Remote-Sicherungssystemen (Offline-Medien) in sichere Rechenzentren.
- Die Datensicherung in den Niederlassungen erfolgt mit Hilfe von lokalen Sicherungen auf Datenträgern (Online-Medien.

Diese Optionen sind hinsichtlich des administratorischen Aufwandes, der Verzögerung durch die Wiederherstellung und der Sicherheitsgewährleistung zu prüfen. Der Zustand und die Tauglichkeit der Datensicherungsmedien muss in regelmäßigen Abständen geprüft werden, indem Datenwiederherstellungen durchgeführt werden.

Die vor Ort verwendeten Sicherungsmedien müssen an einer sicheren und überwachten Stelle aufbewahrt werden, um Änderungen oder Diebstähle von Daten zu verhindern. Das Medium selbst ist nur während der Sicherung und Wiederherstellung im entsprechenden Laufwerk einzusetzen. Auch sollten Verfahren erstellt werden, die Unterschriften autorisierter Administratoren vorsehen, wenn Archivsicherungsmedien zurückgeholt werden.

**Auswahl der zu sichernden Domänen-Controller**

Sind Domänen-Controller an mehreren Standorten verteilt (z. B. in Zweigniederlassungen), so sollten Datensicherungslösungen angestrebt werden, die eine angemessene Absicherung des Backup-Verfahrens und der hierfür benutzten Medien zulassen. Es ist darauf zu achten, dass standortübergreifend für alle Domänen-Controller das Datensicherungskonzept angemessen umgesetzt wird. Existieren an einem Standort z. B. keine sichere Lagerungsmöglichkeiten für die Sicherungsmedien, so sollten die Sicherungsmedien an einen geeigneten Standort ausgelagert werden.

Für Niederlassungen sind Remote-Lösungen denkbar, bei denen die zu sichernden Daten an einem zentralen Standort über das Netz eingesammelt werden. Folgende Punkte sind im Rahmen einer Remote-Datensicherungslösung zu beachten:

- Die Integrität und Vertraulichkeit der Daten sind bei der Übertragung über das Netz durch geeignete Maßnahmen zu schützen, z. B. durch Verschlüsseln der zu sichernden Daten vor oder während der Übertragung.
- Es muss ausreichend Bandbreite zur Verfügung stehen, so dass weder der Betrieb noch die Datensicherung während eines Remote-Backups gestört wird.
- Wird die Datensicherung zunächst lokal in den Standorten durchgeführt und dann von einer zentralen Stelle aus die Backup-Medien eingesammelt, so ist der Zugriff entsprechend abzusichern, z. B. ist der Zugriff auf

Dateifreigaben mit den lokal zwischengespeicherten Datensicherungen, auf Domänenadministratoren zu beschränken.

**Inkrementelle Sicherungen**

Zur platzsparenden Datensicherung wird bei Systemdateien häufig auf inkrementelle Datensicherungsverfahren zurückgegriffen. Bei diesen Verfahren werden ausschließlich die Dateien gesichert, die sich seit der letzten Datensicherung geändert haben. Im Falle einer Wiederherstellung bringt dieses Verfahren jedoch auch einen erhöhten Zeitbedarf mit sich. Inkrementelle Datensicherung sollte für Domänen-Controller nicht angewendet werden, auch der Hersteller rät davon ab.

**Wiederherstellungsmethoden**

Wenn trotzdem inkrementelle Datensicherungen angefertigt werden, werden hierbei nur die seit der letzten Komplettsicherung neu erstellten Daten gesichert. Ältere Aktualitätsstände werden nicht berücksichtigt. In Einzelfällen kann allerdings die Anforderung bestehen, ältere Aktualitätsstände wiederherzustellen und entsprechend zu replizieren, z. B. im Zuge einer Roll-Back-Aktion. Die hiervon betroffenen Daten können mit Hilfe des Kommandozeilen-Werkzeugs *ntdsutil* für eine Replizierung priorisiert werden. Bei der Priorisierung wird festgelegt, welche Daten aus der Sicherung wiederhergestellt bzw. welche Daten beibehalten werden sollen. Aus diesem Grund ist das Priorisieren der Daten sorgfältig durchzuführen, da es hierbei sonst zu Inkonsistenzen in der Gesamtstruktur kommen kann, z. B. dass gesperrte oder ungültige Benutzerkonten wieder verfügbar sind.

Die Datensicherung und Wiederherstellung von Domänen-Controllern mittels einer Image-Erstellung wird aufgrund der auftretenden Inkonsistenz beim USN-Rollback (Update Sequence Number Rollback) nicht empfohlen.

**Ausreichende Verfügbarkeit von Sicherungen**

Damit die Datensicherungen im Notfall auch verfügbar sind, muss am Ende jedes Sicherungsvorganges überprüft werden, ob er fehlerfrei durchgeführt werden konnte.

In allen Domänen sollte regelmäßig eine Überprüfung der Datensicherungen durchgeführt werden, um drei Aspekte sicherzustellen:

- Es muss sichergestellt sein, dass in der betreffenden Woche ausreichend Domänen-Controller erfolgreich gesichert wurden.
- Es ist sicherzustellen, dass die erstellten Sicherungsmedien deutlich mit der eindeutigen Bezeichnung des Domänen-Controllers und dem Datum der Datensicherung beschriftet und anschließend sicher aufbewahrt werden. Dabei sollte die Beschriftung der Sicherungsmedien die Funktion des Domänen-Controllers einschließen, um eine spätere Identifizierung zu erleichtern.
- Im Fall einer erfolglosen Datensicherung ist der Fehler schnellstmöglich zu beheben.

Dabei ist in regelmäßigen Abständen zu testen, ob sich die Datensicherungen auch wieder einspielen lassen. Erfolgreich geprüfte Backup-Medien sollten entsprechend gekennzeichnet werden. Diese Tests sind in einer gesonderten Testumgebung, die von der Produktionsumgebung getrennt ist, durchzuführen.

Prüffragen:

- Existiert eine Datensicherungs- und Wiederherstellungsrichtlinie für Domänen-Controller?
- Ist die eingesetzte Sicherungssoftware explizit vom Hersteller für die Datensicherung von Domänen-Controllern freigegeben?
- Ist für die Domänen-Controller ein separates Datensicherungskonto mit Dienste-Administratorenrechten eingerichtet?
- Ist die Anzahl der Mitglieder der Gruppe "Sicherungs-Operatoren" auf das notwendige Maß begrenzt?
- Ist der Zugriff auf das AdminSDHolder-Objekt zum Schutz der Berechtigungen besonders geschützt?
- Werden Datensicherungen der Domänen-Controller in regelmäßigen Abständen und nach einem Verfahren durchgeführt, das veraltete Objekte weitgehend vermeidet?
- Werden die Sicherungsmedien an einem geeigneten, sicheren Standort aufbewahrt?
- Wird der korrekte Ablauf und das Wiedereinspielen von Datensicherungen der Domänen-Controller regelmäßigen Abständen überprüft?

# M 6.109 Notfallplan für den Ausfall eines VPNs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Abhängig von den Anforderungen an die Verfügbarkeit kann der Ausfall eines VPNs schwerwiegende Folgen nach sich ziehen. Um Schäden zu vermeiden bzw. die entstandenen Schäden zu mindern, müssen die erhobenen Verfügbarkeitsanforderungen bereits bei Definition der VPN-Systemarchitektur berücksichtigt werden. Ein VPN-Notfallkonzept dient als Leitfaden für den akuten Schadensfall (z. B. physische Störung, nicht autorisierter Zugriff) und soll der Institution helfen, im Notfall einen Überblick über die zu ergreifenden Aktivitäten zu behalten.

Die Notfallvorsorge für VPNs muss in das existierenden Notfallmanagement (siehe auch Baustein B 1.3 *Notfallmanagement*) integriert werden. Hierfür sind Verfahren und Definitionen von Erstmaßnahmen für den schnellen Übergang in den operativen Betrieb festzulegen.

Je nach Priorisierung der Standorte, Geschäftsprozesse bzw. Organisationseinheiten sind individuelle VPN-Notfallkonzepte zu erstellen, die die jeweils spezifischen Gegebenheiten abbilden. Bei der Erstellung eines Notfallkonzeptes für ein VPN müssen folgende Punkte beachtet werden:

- Welche Störungen, Schäden und Folgeschäden ergeben sich konkret bei Ausfall einer VPN-Verbindung?
- Welche VPN-Verbindungen müssen hochverfügbar sein?
- Wie schnell kann der Ausfall eines VPNs festgestellt werden?
- Können Fehler in den zur Verbindung benutzten Telekommunikationsnetzen schnell als solche erkannt werden? Werden diese dem zuständigen Administrator mitgeteilt (beispielsweise Verbindungsprobleme, Probleme bei der Rufnummernübertragung, Probleme mit der Schaltung von geschlossenen Benutzergruppen)?
- Wie schnell können VPN-Verbindungen bei verschiedenen Ausfallszenarien wiederhergestellt werden (Ersatz von Geräten, Hochfahren des Systems)?
- Beim Ausfall welcher Komponenten muss das VPN abgeschaltet werden, obwohl technisch weiterhin VPN-Verbindungen aufgebaut werden können (z. B. bei Ausfall der Protokollierung, der Kommunikationsverschlüsselung oder des Authentisierungsservers)?
- Steht für die Administration des VPNs in Notfällen ausreichend qualifiziertes Personal zur Verfügung?

Für einzelne Schadensszenarien sollten geeignete Vorgehensweisen in Form einer Notfalldokumentation erarbeitet werden. Darin sollten alle für die Behebung eines Notfalls notwendigen Daten erfasst und so dargestellt sein, dass auch das Vertretungspersonal damit arbeiten kann. Die Notfalldokumentation sollte außerdem Informationen über alternative Verbindungswege enthalten, z. B. alternative Telekommunikationsanbieter oder alternative Übertragungsmedien.

**Notfall-Verantwortlichkeiten**

Personelle Schlüsselpositionen und deren Aufgaben und Befugnisse müssen definiert und dokumentiert werden. Hierbei sollten auch die in Maßnahme

M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen* gegebenen Empfehlungen beachtet werden.

**Einrichten von Notfallrufnummern**

Für Mitarbeiter, vor allem die mobilen Mitarbeiter und Telearbeiter, sollte eine Notfallrufnummer angeboten werden, damit sie VPN-Probleme zeitnah an verantwortliche Stellen kommunizieren können. Außerdem sollte das VPN in den kritischen Zeitabschnitten (z. B. Bürozeiten, Zeiten in denen vornehmlich Daten per VPN ausgetauscht werden) permanent überwacht werden.

**Redundante Kommunikationsverbindungen**

Je nach Priorisierung der Standorte und deren geschäftskritischen Applikationen können erhöhte Anforderungen an die Verfügbarkeit entstehen. Im Falle einer Störung müssen bei erhöhten Anforderungen an die Verfügbarkeit Sekundäranschlüsse zur Verfügung stehen. Der Sekundäranschluss wird nur im Falle einer Störung eingesetzt und kann beispielsweise mit DSL- oder ISDN-Verbindungen realisiert werden. Maßnahme M 6.18 *Redundante Leitungsführung* bietet weitere Hinweise für eine ordnungsgemäße Umsetzung.

**Redundante VPN-Komponenten**

Abhängig von den Anforderungen an die Verfügbarkeit des jeweiligen Standorts kann der Ausfall einer VPN-Komponente zu mehr oder minder großen Problemen führen. Bei hohen Anforderungen an die Verfügbarkeit des VPNs müssen entsprechende Redundanzen bereitgestellt werden. Dies kann, entsprechend den Anforderungen, beispielsweise mittels folgender Mechanismen erreicht werden:

- Clustering (mehrere vernetzte Komponenten zur Erhöhung der Verfügbarkeit),
- Hot Standby (Bereitstellung von initialisierten Ersatzgeräten) oder Cold Standby (Bereitstellung von ausgeschalteten Ersatzgeräten).

Besonders für zentrale VPN-Komponenten, wie beispielsweise VPN-Server im Rahmen eines Remote-Access-VPNs, sollte geprüft werden, ob eine redundante Auslegung erforderlich ist.

Informationen werden über VPNs in der Regel verschlüsselt übertragen. Daher ist zu beachten, dass für die Verschlüsselung entsprechende Ersatzschlüssel vorhanden sein müssen, bzw. neue Schlüssel generiert werden müssen. Dieser Aspekt muss im Schlüsselmanagement berücksichtigt werden.

Die Fehlerquellen für ein VPN können vielfältig sein, daher kann auch die Umsetzung der Maßnahme M 6.53 *Redundante Auslegung der Netzkomponenten* für zusätzliche Ausfallsicherheit sorgen.

**Erstellung eines Wiederanlaufplans**

Um eine schnellstmögliche Wiederaufnahme des Betriebs gewährleisten zu können, muss ein Wiederanlaufplan für jedes betriebene VPN erstellt werden. Hierbei müssen die erforderlichen Schritte festgelegt und dokumentiert werden. Für einen reibungslosen Austausch defekter VPN-Komponenten muss eine aktuelle Sicherung der jeweiligen Konfigurationsdaten zur Verfügung stehen. Hierzu sei auch auf Maßnahme M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten* hingewiesen. Auch die Datenkonsistenz bei der Wiederaufnahme des Betriebs muss gewährleistet sein (siehe B 1.4 *Datensicherungskonzept*).

**Überprüfung der Datenintegrität nach Störungen**

Bei einem Systemabsturz einer oder mehrerer VPN-Komponenten oder einer anderen Störung des VPNs kann nicht immer die Konsistenz der per VPN übertragenen Daten gewährleistet werden. Nach jeder Störung sollte daher die Integrität dieser Daten überprüft und eine Problemanalyse durchgeführt werden, um Wiederholungen möglichst zu vermeiden.

**Notfallkonfiguration**

In bestimmten Situationen kann es erforderlich sein, das VPN mit eingeschränkter Funktionalität oder Leistungsfähigkeit zu betreiben. In diesem Fall muss eine entsprechende Notfallkonfiguration aktiviert werden (siehe auch M 4.320 *Sichere Konfiguration eines VPNs*). Diese dient dazu, die Sicherheit des VPNs (Zugangssicherheit, Zugriffssicherheit, Kommunikationssicherheit) auch bei eingeschränktem Betrieb aufrechtzuerhalten. Dafür muss im Vorfeld abhängig von der Priorisierung der Standorte, Geschäftsprozesse bzw. Organisationseinheiten festgelegt worden sein, in welchen Situationen welche VPN-Notfallkonfiguration ausgewählt wird.

**Durchführung von Notfallübungen**

Die beste Wiederanlaufplanung nützt wenig, wenn sie in der Praxis nicht zweckmäßig ist. Von besonderer Bedeutung ist daher die Durchführung von regelmäßigen Notfallübungen, um Schwachpunkte erkennen und verbessern zu können (siehe auch M 6.12 *Durchführung von Notfallübungen*). Hierbei muss eine revisionsfähige Protokollierung des VPN-Wiederanlaufs gewährleistet werden. Alle Ersatz-VPN-Komponenten, Datensicherungsgeräte, Backup-Datenträger und Sekundärleitungen für Ausweich-Kommunikationsverbindungen müssen in regelmäßigen Abständen auf ihre Funktionsfähigkeit überprüft werden. Die verantwortlichen Personen profitieren ebenfalls von Trainings- und Sensibilisierungsmaßnahmen und können im Ernstfall schneller und effizienter reagieren.

Das VPN-Notfallkonzept muss an die spezifische Situation der Institution angepasst und so ausgestaltet sein, dass kritische Geschäftsprozesse innerhalb der geforderten Zeiten wieder zur Verfügung stehen. Das VPN-Notfallkonzept muss so geschrieben sein, dass es von einem sachverständigen Dritten ausgeführt werden kann. Aufgrund ständiger technischer, organisatorischer und personeller Veränderungen muss das VPN-Notfallkonzept immer aktuell gehalten werden.

Prüffragen:

- Gibt es ein aktuelles Notfallkonzept für den Ausfall eines VPN?
- Ist festgelegt, welche Verfügbarkeitsanforderungen an die unterschiedlichen VPN-Verbindungen bestehen?
- Ist definiert und dokumentiert, wer im Notfall welche Aufgaben und Befugnisse für den VPN-Betrieb hat?
- Wird für Mitarbeiter eine Notfallrufnummer angeboten, über die sie VPN-Probleme melden können?
- Sind die technischen Redundanzen für die festgelegten Verfügbarkeitsanforderungen des VPN-Betriebs angemessen?
- Steht im Notfall ausreichend qualifiziertes Personal für die Wiederherstellung der VPNs zur Verfügung?
- Sind die für den VPN-Wiederanlauf erforderlichen Schritte festgelegt und dokumentiert?
- Wird eine aktuelle Sicherungskopie der Konfigurationsdaten vorgehalten?

- Werden regelmäßig VPN-Notfallübungen durchgeführt?
- Werden die Datensicherungen regelmäßig überprüft, ob sie wiedereingespielt werden können?

# M 6.110 Festlegung des Geltungsbereichs und der Notfallmanagementstrategie

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Notfallbeauftragter

Die ersten Aufgaben bei der Initiierung eines Notfallmanagement-Systems sind die Festlegung des Geltungsbereichs und der Notfallmanagementstrategie. Diese für alle weiteren Arbeiten im Notfallmanagement grundlegenden Schritte sind durch die Institutionsleitung zu initiieren und durchzuführen. Ist bereits ein zentraler Ansprechpartner für das Notfallmanagement, ein Notfallbeauftragter, benannt, so unterstützt er die Institutionsleitung bei dieser Aufgabe.

Der Geltungsbereich des Notfallmanagement-Systems kann die gesamte Institution umfassen oder auch einzelne Teilbereiche. Der Geltungsbereich sollte in sich abgeschlossen, nicht zu eng gefasst sein und die Wert schöpfenden Geschäftsprozesse bzw. relevanten Fachaufgaben, die wichtigsten Ressourcen sowie die benötigten unterstützenden Geschäftsprozesse vollständig enthalten. Es ist hilfreich für die Notfallkonzeption, wenn die Institutionsleitung die aus ihrer Sicht wichtigsten Dienstleistungen und / oder Produkte der Institution benennt. Werden innerhalb dieses Geltungsbereichs beispielsweise bestimmte Geschäftsprozesse explizit ausgeschlossen oder nur eingeschränkt betrachtet, so ist dies zu dokumentieren.

Da das oberste Ziel des Notfallmanagements ist, die Überlebensfähigkeit der Institution zu sichern und zu stabilisieren, ist eine Betrachtung der gesamten Institution anzustreben. Nur so kann ein wirksamer Schutz des Ansehens und der wertschöpfenden Tätigkeiten der Institution und damit der Interessen der wichtigsten Interessengruppen gewährleistet werden.

Grundlage für die nächsten Schritte bei der Etablierung eines Notfallmanagement-Systems ist die Festlegung und Definition der Begriffe Notfall, Krise und Notfallmanagement für die Institution. Der Ausfall einzelner Geschäftsprozesses oder eines kompletten Systems kann eine Störung, ein Notfall oder gar eine Krise für die Institution sein. Da die Abgrenzungen individuell für jede Institution sind und vom Schutzbedarf der Geschäftsprozesse und IT-Systeme abhängen, sollte eine allgemeine Festlegung dieser Begriffe für die Institution erfolgen. Auch der Begriff Notfallmanagement sollte präzisiert werden. Es sollte definiert werden, welche Aufgaben und Kompetenzen das Notfallmanagement-System umfasst, um eine Abgrenzung zu anderen etablierten Managementsystemen der Institution sowie die Schnittstellen zu diesen festzulegen.

Um den Rahmen für die Notfallkonzeption setzen zu können, ist eine Notfallmanagementstrategie, oder kurz Notfallstrategie, festzulegen, die bei der Etablierung eines Notfallmanagement-Systems beachtet werden muss. Die Institutionsleitung hat daher grundlegende Eckpunkte festzulegen, wie beispielsweise,

- welche Ziele mit der Etablierung eines Notfallmanagements verfolgt werden (z. B. Anforderungen durch wichtige Interessengruppen),
- welche Anforderungen an das Notfallmanagement gestellt werden,

- welche Bereitschaft besteht, Risiken einzugehen (Risikoappetit), bzw. wie hoch das Risikoakzeptanzniveau für das Unternehmen bzw. die Behörde liegt,
- welche Arten von Geschäftsunterbrechungen als Existenz bedrohend angesehen werden,
- in welcher Art und ab welcher Größenordnung etwas dagegen unternommen werden soll und
- welche gesetzlichen, vertraglichen oder regulatorischen Vorgaben einzuhalten sind.

Die Ziele des Notfallmanagements sollten sich an den generellen Geschäftszielen und -Aufgaben orientieren und diese unterstützen. Es ist sinnvoll, auch die Ziele anderer Managementsysteme, insbesondere des Sicherheitsmanagementsystems, bei der Festlegung zu berücksichtigen.

Prüffragen:

- Ist der Geltungsbereich des Notfallmanagement-Systems eindeutig festgelegt?
- Ist durch die Institutionsleitung eine Notfallmanagement-Strategie festgelegt, die die angestrebten Ziele und das Risikoakzeptanzniveau darlegt?

# M 6.111 Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Notfallbeauftragter

Mit der Leitlinie zum Notfallmanagement wird nachvollziehbar der Rahmen für die Konzeption und Umsetzung des Notfallmanagement gesetzt. Sie dokumentiert die wesentlichen Eckpunkte des Notfallmanagements in der Institution. Die oberste Behörden- bzw. Unternehmensleitung zeigt damit, dass sie die Verantwortung für das Notfallmanagement übernimmt und hinter allen Vorgaben und Abläufen steht.

**Inhalt der Leitlinie zum Notfallmanagement**

Die Leitlinie zum Notfallmanagement sollte kurz und bündig formuliert sein. Dabei sollten die folgenden Aspekte enthalten sein:

- eine kurze Darstellung, was unter Notfallmanagement verstanden wird,
- der Geltungsbereich des Notfallmanagement-Systems,
- der Stellenwert des Notfallmanagements für die Institution,
- die Zielsetzung des Notfallmanagements,
- die Kernaussagen der Notfallstrategie,
- die Übernahme der Verantwortung durch die oberste Institutionsleitung, die zusätzlich durch die explizite Freigabe per Unterschrift dokumentiert wird.

Optional könnte die Leitlinie folgende Informationen enthalten oder referenzieren:

- die Art der Eingliederung des Notfallmanagement-Systems in die etablierten Management-Systeme der Institution,
- das zugrunde gelegte Vorgehensmodell für die Einrichtung und den Betrieb des Notfallmanagements (bzw. den zugrunde gelegten Standard),
- die Struktur der Aufbauorganisation für das Notfallmanagement mit den wichtigsten Rollen und deren Zuständigkeiten,
- die Verpflichtung der Institutionsleitung, durch regelmäßige Überprüfungen, Tests und Übungen das Notfallmanagement zu optimieren,
- die relevanten Gesetze, Richtlinien und Vorschriften, die zu beachten sind, und
- allgemeine Aussagen zur Erfolgskontrolle des Notfallmanagements.

**Bekanntgabe der Leitlinie zum Notfallmanagement**

Die Leitlinie zum Notfallmanagement ist durch die oberste Institutionsleitung schriftlich freizugeben. Sie ist allen internen und externen Mitarbeitern und gegebenenfalls Kooperationspartnern bekannt zugegeben. Dies sollte so erfolgen, dass der Stellenwert des Notfallmanagements in der Institution deutlich wird.

**Aktualisierung der Leitlinie zum Notfallmanagement**

Die Leitlinie zum Notfallmanagement ist regelmäßig in festgelegten Abständen auf ihre Aktualität hin zu überprüfen und gegebenenfalls anzupassen. Änderungen von Anforderungen, Rahmenbedingungen, Geschäftszielen, Aufgaben, der Notfallmanagement-Strategie oder sonstige relevante Änderungen sollten eine Überprüfung der Leitlinie anstoßen und gegebenenfalls durch eine Aktualisierung einfließen. Bei den rasanten Entwicklungen heutzutage sowohl im Geschäftsbereich wie auch in der IT empfiehlt es sich, die Leitlinie zum Notfallmanagement mindestens alle zwei Jahre zu überarbeiten.

Prüffragen:

- Gibt es eine von der Leitungsebene verabschiedete aktuelle Leitlinie zum Notfallmanagement?
- Enthält die Leitlinie zum Notfallmanagement die wichtigsten Informationen?
- Wird die Leitlinie zum Notfallmanagement regelmäßig überprüft und gegebenenfalls überarbeitet?
- Ist die Leitlinie zum Notfallmanagement allen Mitarbeitern bekannt gegeben worden?

# M 6.112 Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Notfallbeauftragter

**Planung und Einrichtung der Organisationsstruktur für das Notfallmanagement**

Um einen Notfallmanagement-Prozesses erfolgreich planen, umsetzen und aufrechterhalten zu können, muss eine geeignete Aufbauorganisation für das Notfallmanagement vorhanden sein. Dazu sind Rollen zu definieren und die jeweiligen Aufgaben, Pflichten, Rechte und Kompetenzen festzulegen. Die Art und Ausprägung der Organisationsstruktur für das Notfallmanagement hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab.

Bei der Etablierung eines Notfallmanagements kann sich herausstellen, dass innerhalb der Institution bereits Verantwortliche für verschiedene Aspekte des Notfallmanagements benannt sind, es jedoch keine übergreifende Struktur dafür gibt. In diesem Fall muss eine für die Institution geeignete, übergreifende Organisationsstruktur für das Notfallmanagement aufgebaut werden.

Da sich das Notfallmanagement in zwei grundlegende Phasen einteilen lässt, die Notfallvorsorge und die Notfallbewältigung, teilt sich auch die Organisationsstruktur in zwei Bereiche: die Notfallvorsorgeorganisation und die Notfallbewältigungsorganisation.

**Rollen in der Notfallvorsorge**

Die Notfallvorsorgeorganisation ist für die Planung, den Aufbau, den Betrieb und die Verbesserung des Notfallmanagements zuständig. Die zentralen Rollen in der Notfallvorsorgeorganisation sind:

*Unternehmens- bzw. Behördenleitung:*

Die Unternehmens- bzw. Behördenleitung ist für die institutionsweite Sicherstellung des Notfallmanagements verantwortlich.

*Notfallbeauftragter:*

Die zentrale Funktion des Notfallbeauftragten muss in jeder Institution eingerichtet werden, da er für alle Belange des Notfallmanagements zuständig ist.

*Notfallkoordinatoren:*

In größeren Institutionen kann der Notfallbeauftragte durch zusätzliche Notfallkoordinatoren unterstützt werden.

*Notfallvorsorgeteam:*

Das Notfallvorsorgeteam ist eine temporäre Einrichtung, die dem Notfallbeauftragen oder den Notfallkoordinatoren beratend zur Seite steht.

**Rollen in der Notfallbewältigung**

Die Notfallbewältigungsorganisation wird temporär in einem Notfall oder einer Krise aktiv und ist für eine effektive und schnelle Notfallbewältigung inklusive des Wiederanlaufs zuständig. Sie ist im Vorfeld eines Notfalls geeignet festzulegen, aufzubauen und zu dokumentieren. Zu den wichtigsten Rollen in der Notfallbewältigung zählen:

*Krisenentscheidungsgremium:*

Das Krisenentscheidungsgremium gibt die strategische Richtung in einem Notfall oder einer Krise vor und trifft die weitreichenden Entscheidungen, welche über die festgelegte Kompetenzen des Krisenstabsleiters gehen.

*Krisenstab:*

Der Krisenstab ist ein planendes, koordinierendes, informierendes, beratendes und unterstützendes Organ. Er stellt eine besondere temporäre Aufbauorganisation dar, die die normale Aufbauorganisation zur Bewältigung eines Notfalls durchbricht und abteilungsübergreifende Kompetenzen bündelt. Der Krisenstab setzt sich aus einem Leiter, einem Kernteam und einem erweiterten Krisenstabsteam zusammen. Er wird gegebenenfalls durch weitere Fachberater ergänzt.

*Notfallteams:*

Die Notfallteams stellen den operativen Teil der Notfallbewältigung. Diese sind für den Wiederanlauf bzw. die Wiederherstellung von Geschäftsprozessen, Anwendungen oder Systemen zuständig.

Eine detaillierte Beschreibung der Rollen im Notfallmanagement und ihrer Aufgaben sind im BSI-Standard 100-4 *Notfallmanagement* zu finden.

Die für die Notfallorganisation der Institution festgelegten Rollen sind mit ihren Aufgaben, Pflichten und Rechte nachvollziehbar zu dokumentieren. Dazu gehören auch die wesentlichen Arbeitsanweisungen und organisatorischen Regelungen. Es empfiehlt sich, Anforderungsprofile für die Besetzung dieser Rollen zu erstellen. Für alle Rollen sind dafür qualifizierte Mitarbeiter zu benennen.

**Überprüfung der Organisationsstruktur des Notfallmanagements**

Eine einmal aufgebaute Aufbauorganisation für das Notfallmanagement ist nicht statisch. Geschäftsprozesse und Rahmenbedingungen ändern sich permanent, so dass auch die Organisationsstruktur für das Notfallmanagement immer wieder überdacht werden muss. Dabei sollte beispielsweise beleuchtet werden, ob die Aufgaben und Kompetenzen innerhalb des Notfallmanagement-Prozesses ausreichend klar definiert sind, aber auch, ob vorgesehene Aufgaben wie geplant wahrgenommen werden können. Wichtig sind vor allem die folgenden Punkte:

- Überwachung von Verantwortlichkeiten
  Es muss regelmäßig überprüft werden, ob alle Verantwortlichkeiten und Zuständigkeiten eindeutig zugewiesen und diese praxistauglich sind.
- Überprüfung der Einhaltung von Vorgaben
  Es muss regelmäßig geprüft werden, ob alle Prozesse und Abläufe der Notfallorganisation wie vorgesehen angewendet und durchgeführt werden. Gleichzeitig sollte sichergestellt werden, dass die aufgebauten Or-

ganisationsstrukturen für das Notfallmanagement den Anforderungen gerecht werden.
- Beurteilung der Effizienz von Prozessen und organisatorischen Regelungen
  Es muss regelmäßig überprüft werden, ob Prozesse und organisatorische Regelungen des Notfallmanagements praxistauglich und effizient sind.
- Managementbewertungen
  Das Management ist über die Ergebnisse der oben genannten Überprüfungen regelmäßig zu informieren. Die Berichte sind nicht nur notwendig, um dringende oder zeitkritische Probleme zu lösen, sondern enthalten wichtige Informationen, die das Management für die Steuerung des Notfallmanagement-Prozesses benötigt.

Prüffragen:

- Sind die Rollen für das Notfallmanagement den Gegebenheiten der Institution angemessen festgelegt und mit ihren Aufgaben, Pflichten und Kompetenzen schriftlich dokumentiert?
- Sind für alle Rollen im Notfallmanagement qualifizierte Mitarbeiter benannt?
- Wird die Organisationsstruktur im Notfallmanagement regelmäßig auf ihre Praxistauglichkeit, Effektivität und Effizienz hin überprüft?

# M 6.113 Bereitstellung angemessener Ressourcen für das Notfallmanagement

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Notfallbeauftragter

Damit die für das Notfallmanagement gesteckten Ziele erreicht werden können, müssen angemessene Ressourcen bereitgestellt werden.

Planung, Umsetzung, Betrieb, Wartung und Verbesserung eines Notfallmanagements erfordern ausreichende finanzielle und personelle Ressourcen sowie eine geeignete Ausstattung. Diese müssen von der Behörden- bzw. Unternehmensleitung in angemessenem Umfang bereitgestellt werden.

Es ist zu empfehlen, dass der Notfallbeauftragte anhand des Gefährdungspotentials und der Ziele und Aufgaben der Notfallvorsorge und der Notfallbewältigung die benötigten Ressourcen aufzeigt. Dies dient einerseits als Grundlage für die notwendigen Management-Entscheidungen über die Zuteilung der Ressourcen und andererseits zur Festlegung der Projektpläne und der Umsetzungszeiträume.

### Benennung eines Verantwortlichen für das Notfallmanagement

Ohne eine funktionierende Organisationsstruktur für das Notfallmanagement nützen die teuersten technischen Lösungen nichts. Es ist daher durch die oberste Leitungsebene ein Verantwortlicher für das Notfallmanagement aus der Leitungsebene zu benennen, der die entsprechenden Befugnisse besitzt.

### Benennungen von Zuständigen für die Planung, Umsetzung, Betrieb, Wartung und Verbesserung eines Notfallmanagements

Es sind für alle für das Notfallmanagement festgelegten Rollen geeignete Personen zuzuweisen. Die Rollen müssen alle Phasen des Notfallmanagement-Prozesses abdecken, von der Initiierung, Planung, Umsetzung, Wartung, Aufrechterhaltung und der Überprüfung des Notfallmanagements. Auch die nur temporär benötigten Rollen der Notfall- und Krisenbewältigung müssen berücksichtigt werden. Insbesondere ist ein Notfallbeauftragter zu benennen, der der zentrale Ansprechpartner für das Notfallmanagement und zuständiger Koordinator aller anfallender Aufgaben ist.

### Personelle Ressourcen für das Notfallmanagement

Alle Mitarbeiter des Notfallmanagement-Teams sollten über ausreichende Kompetenzen verfügen, um die ihnen mit den Rollen zugewiesenen Aufgaben erfüllen zu können. Sie müssen Zugriff auf erforderliche Ressourcen haben und über ausreichend Zeit für ihre Arbeit verfügen. Dies gilt insbesondere dann, wenn ein Mitarbeiter die Aufgaben in Personalunion neben seinen eigentlichen Tätigkeiten wahrnimmt. Das Notfall-Organigramm ist von der Behörden- bzw. Unternehmensleitung zu autorisieren.

### Bereitstellung von Ressourcen für den IT-Betrieb

Werden durch das Notfallmanagement zusätzliche Anforderungen an die IT gestellt, so ist sicherzustellen, dass dem IT-Betrieb ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des IT-Betriebs (knappes

Budget, überlastete Administratoren und eine unstrukturierte oder schlecht gewartete IT-Landschaft) müssen in der Regel gelöst werden, damit die Notfallvorsorgemaßnahmen wirksam und effizient umgesetzt werden können.

**Zugriff auf externe Ressourcen**

In einzelnen Phasen des Notfallmanagements, wie beispielsweise der Konzeption oder in der Notfallbewältigung, sind Arbeitsspitzen zu erwarten. Um diese bewältigen zu können, müssen entweder intern zusätzliche Mitarbeiter eingesetzt oder auf externe Experten zurückgegriffen werden. Zusätzlich kann es sinnvoll sein, bei fehlendem Know-how oder von Erfahrung temporär auf Experten zurückzugreifen. Der Bedarf muss von den internen Notfallmanagement-Experten kommuniziert werden, damit die Leitungsebene die erforderlichen Ressourcen bereit stellen kann.

**Wirtschaftlichkeitsaspekte**

Die Notfallmanagementstrategie sollte von Beginn an auch Wirtschaftlichkeitsaspekte berücksichtigen. Bei der Auswahl der umzusetzenden Notfallvorsorgemaßnahmen sollten auch die zur Verfügung stehenden Ressourcen berücksichtigt werden. Wenn für bestimmte Maßnahmen keine ausreichende finanzielle, technische oder personelle Unterstützung vorhanden ist, muss die Strategie geändert werden. Wenn aber die formulierten Ziele für das Notfallmanagement und die vorhandenen finanziellen, technischen oder personellen Möglichkeiten zu weit auseinander liegen, müssen sowohl die Ziele wie auch die Strategie grundsätzlich überdacht werden. In diesem Fall muss die Leitungsebene über diese Diskrepanz informiert werden, damit sie gegebenenfalls Korrekturmaßnahmen vornehmen kann.

Bei der Festlegung von Notfallvorsorgemaßnahmen sollten immer die für die Umsetzung benötigten personellen und finanziellen Ressourcen konkret genannt werden. Hierzu gehört die Benennung von Verantwortlichen und anderen Ansprechpartnern, aber auch die Festlegung genauer Terminpläne und der zu beschaffenden Materialien. Es empfiehlt sich außerdem, bei allen geplanten Notfallvorsorgemaßnahmen zu dokumentieren, ob die für eingeplanten Ressourcen termingerecht bereitgestellt wurden und was die Gründe für Projektabweichungen waren. Nur so lassen sich nachhaltige Verbesserungen erreichen und Störungen vermeiden.

Prüffragen:

- Sind die finanziellen, technischen und personellen Ressourcen für die angestrebten Ziele des Notfallmanagements angemessen?
- Verfügen der Notfallbeauftragte beziehungsweise das Notfallmanagement-Team über genügend Zeit für ihre Aufgaben im Notfallmanagement?

# M 6.114 Erstellung eines Notfallkonzepts

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Notfallbeauftragter
**Verantwortlich für Umsetzung:** Notfallbeauftragter

Ein Notfallkonzept dient der Umsetzung der Notfallstrategie und beschreibt die geplante Vorgehensweise, um die für das Notfallmanagement gesetzten Ziele zu erreichen. Das Notfallkonzept umfasst die Gesamtheit der im Notfallmanagement-Prozess erstellten Dokumente. Es besteht aus den zwei wesentlichen Komponenten Notfallvorsorgekonzept und Notfallhandbuch. Damit werden die beiden wesentlichen Aufgaben des Notfallmanagements widergespiegelt, die Robustheit der Geschäftsprozesse zu stärken, um die Wahrscheinlichkeit eines Schadensereignisses zu verringern, und die Behörde bzw. das Unternehmen optimal auf die Bewältigung eines Notfalls oder einer Krise vorzubereiten, um die Schadensauswirkungen zu minimieren. Das Notfallvorsorgekonzept beschreibt die vorliegenden Rahmenbedingungen und beinhaltet alle bei der Konzeption anfallenden Informationen, die nicht zur direkten Bewältigung eines Notfalls beitragen. Die direkt für die Bewältigung eines Notfalls benötigten Informationen wie beispielsweise Kontaktinformationen oder Handlungsanweisungen sind im Notfallhandbuch beschrieben.

Jede konkrete Vorsorgemaßnahme muss sich letztlich auf das Notfallkonzept zurückführen lassen. Aus diesem Grund muss dieses sorgfältig geplant und umgesetzt werden. Die einzelnen, im Folgenden kurz angerissenen Aspekte werden ausführlich im BSI-Standard 100-4 *Notfallmanagement* behandelt.

Voraussetzung für die Erstellung eines Notfallkonzeptes sind grundlegende Kenntnisse über die Institution bzw. den festgelegten Geltungsbereich des Notfallmanagements und ein tiefgreifendes Verständnis der Geschäftstätigkeit. Die benötigten Informationen, zu denen die Stammdaten und eine Übersicht über die Geschäftsprozesse zählen, sind dem Notfallmanagement bereitzustellen. Die Geschäftsprozessübersicht sollte auch die Informationen über Abhängigkeiten zwischen Prozessen enthalten sowie die Informationen, welche Geschäftsprozesse zur Herstellung der Hauptprodukte oder der Erbringung von Hauptdienstleistungen der Institution benötigt werden. Ausgelagerte Prozesse sind ebenfalls in der Geschäftsprozessübersicht zu berücksichtigen, wie auch Zulieferer, Kooperationspartner und Outsourcing-Dienstleister bei den Abhängigkeiten.

Einer der ersten Schritte bei der Konzeption ist es, die Auswirkungen von Geschäftsunterbrechungen zu untersuchen, die Verfügbarkeitsanforderungen an die Geschäftsprozesse und deren benötigten Ressourcen zu ermitteln sowie die benötigten Wiederanlaufzeiten festzulegen.

Hierzu sollte eine Business Impact Analyse (BIA) durchgeführt werden. Es gibt verschiedene Methoden, um die benötigten Ergebnisse zu ermitteln. Dafür ist eine für die Institution angemessene Methode zur Durchführung der BIA auszuwählen, Parameter für die gewählte Methode zu setzen und die Entscheidungen zu dokumentieren.

Die Erfahrung hat gezeigt, dass Methoden, die auf aufwendigen numerischen Betrachtungen beruhen, häufig einen unverhältnismäßig hohen Aufwand erzeugen. Ein pragmatischer Ansatz, der sich gerade für kleine Institutionen eignet, ist beispielsweise, in einem Workshop in Zusammenarbeit mit den Verantwortlichen die relevanten Prozesse zu ermitteln, zu klassifizieren bzw. zu priorisieren.

Die gewählte Methode zur Durchführung einer BIA sollte mindestens folgende Arbeitsschritte enthalten:

- Es ist zu analysieren und zu bewerten, wie sich eine Unterbrechung von Geschäftsprozessen oder Wertketten auf die Behörde bzw. das Unternehmen auswirken und wie sich Schäden während dieser Zeit entwickeln können.
- Für die Geschäftsprozesse sind die Wiederanlaufparameter zu identifizieren bzw. festzulegen. Dazu zählen:
  - die Verfügbarkeitsanforderung, die den Übergang von Störung zu Notfall kennzeichnet,
  - die maximal tolerierbare Ausfallzeit,
  - die Wiederanlaufzeit,
  - das Wiederanlaufniveau und
  - der maximal zulässige Datenverlust.

Zusätzlich empfiehlt es sich, die maximal zulässige Wiederherstellungszeit bzw. den maximal zulässigen Notbetrieb festzulegen.

- Die Geschäftsprozesse sind für den Wiederanlauf zu priorisieren. Eine Einteilung in Wiederanlaufklassen kann sinnvoll sein. Dabei ist jedoch zu beachten, dass die Prioritäten und die Wiederanlaufzeiten wirtschaftlich und mit den gegebenen finanziellen und personellen Ressourcen realisierbar sein müssen. Gegenseitige Abhängigkeiten der Geschäftsprozesse sind zu beachten. Es ist festzulegen, welche Geschäftsprozesse als kritisch für die Institution eingestuft und damit in die weitere Betrachtung für die Konzeption einbezogen werden.
- Mindestens für die kritischen Geschäftsprozesse sind die benötigten Ressourcen für den Normalbetrieb und den Notbetrieb zu erheben sowie der Abhängigkeitsgrad des jeweiligen Geschäftsprozesses von den Ressourcen zu bestimmen. Werden Single-Points-of-Failure identifiziert, so sind diese besonders zu kennzeichnen. Mit Single-Points-of-Failure werden Ressourcen bezeichnet, deren Ausfall einen Komplettausfall von Geschäftsprozessen verursachen würde. Es empfiehlt sich, diese einer schnellen Maßnahmenüberprüfung zuzuführen.
- Für die Ressourcen ist die Kritikalität zu beurteilen und die Verfügbarkeitsanforderung sowie die Wiederanlauf- bzw. Wiederherstellungszeit festzulegen.

Der Notfallbeauftragte koordiniert und führt mit Unterstützung der Notfallkoordinatoren die BIA durch. Wesentliche Ansprech- und Interviewpartner bei der Durchführung der BIA sind die Geschäftsprozess- und Ressourcenverantwortliche. Die Ergebnisse der BIA sind schriftlich zu dokumentieren und durch die Institutionsleitung zu bestätigen.

Detaillierte Informationen für eine mögliche Methode zur Durchführung einer Business Impact Analyse ist im BSI-Standard 100-4 *Notfallmanagement* enthalten.

Um die Ursachen von möglichen Geschäftsprozessunterbrechungen zu finden, ist eine Risikoanalyse durchzuführen. Es sind die Ziele und eine geeignete Methode zur Durchführung der Risikoanalyse festzulegen und zu dokumentieren. Bei der Durchführung der Risikoanalyse kann es hilfreich sein, die bei der BIA identifizierten Auswirkungen von Ausfällen miteinzubeziehen und umgekehrt. Ergebnis der Risikoanalyse ist die Aufstellung der wesentlichen Risiken für die Kontinuität der Geschäftsprozesse und die kritischen Ressourcen der Institution (siehe BSI-Standard 100-3 *Risikoanalyse auf der Basis von IT-Grundschutz*). Für jedes identifizierte Risiko ist zu entscheiden, welche Risi-

kostrategien zur Reduzierung der Auswirkung, Verringerung der Eintrittswahrscheinlichkeit und Minimierung der Ausfallzeit eingesetzt werden sollen.

Um aus den allgemeinen Zielen, dem identifizierten Schutzbedarf und der Risikobewertung den Bedarf ableiten, konkrete Schutzmaßnahmen und Wiederanlaufstrategien festlegen zu können, ist die Erhebung des Ist-Zustandes der kritischen Geschäftsprozesse und deren unterstützenden Ressourcen sinnvoll. Durch den Vergleich der in der BIA festgelegten Soll-Werte für Wiederanlauf und Wiederherstellung sowie dem initial festgelegtem Risikoappetit (Risikoakzeptanzniveau) der Institution mit den aktuell realisierten Wiederanlaufmaßnahmen und Schutzmaßnahmen, werden die vorhandenen Lücken für den Wiederanlauf und die Risikobehandlung identifiziert.

Um diese zu schließen, sind in der weiteren Konzeption sinnvolle Maßnahmen zu identifizieren, die die Ausfallsicherheit der kritischen Geschäftsprozesse und deren benötigten Ressourcen erhöhen, einen zeitgerechten Wiederanlauf bzw. Wiederherstellung ermöglichen und somit die Ausfallzeit und den Schaden bei Eintritt eines Notfalls begrenzen. Es empfiehlt sich, verschiedene Strategieoptionen für die Notfallbewältigung, die Geschäftsfortführung und die Wiederherstellung und Wiederanlauf der Ressourcen zu entwickeln, die

- die festgelegten Anforderungen an die Geschäftsfortführung, den Wiederanlauf und die Wiederherstellung erfüllen,
- in einem sinnvollen Kosten-Nutzen-Verhältnis stehen,
- eine aufeinander abgestimmte, übergreifende Gesamtlösung ergeben und
- dabei auch die wichtigsten Interessengruppen berücksichtigen oder mit einbinden.

Es sind geeignete Strategien auszuwählen und die Entscheidung zu dokumentieren. Dabei sollte auch festgehalten werden, wie die Zusammenarbeit mit Zulieferern, Kooperationspartnern oder Outsourcing-Dienstleistern im Notfall erfolgen soll. IT-Maßnahmen sind gegebenenfalls mit dem Sicherheitsmanagement abzustimmen.

Es ist ein Notfallkonzept bestehend aus Notfallvorsorgekonzept und Notfallhandbuch zu erstellen. Das Notfallvorsorgekonzept enthält alle Informationen, die bei der Konzeption anfallen inklusive der ausgewählten Maßnahmen zur Risikobehandlung und um einen schnellen Wiederanlauf und Wiederherstellung zu ermöglichen. Das Notfallhandbuch enthält die Informationen, die direkt für und bei der Notfallbewältigung benötigt werden. Dazu zählen unter anderem die Geschäftsfortführungspläne, die Wiederanlauf- und Wiederherstellungspläne inklusive Ersatzbeschaffungs- und Ausweichpläne sowie Notfallpläne für Sofortmaßnahmen. Die die Geschäftsfortführungspläne, Wiederanlauf- und Wiederherstellungspläne enthalten sämtliche Informationen, die ein schnelles Aufnehmen eines Notbetriebs ermöglichen und die Wiederherstellung des Normalbetriebs für Prozesse und Ressourcen ermöglichen. Die Pläne sollten die Informationen über die Wiederanlaufzeiten und Prioritäten für die Prozesse und Ressourcen enthalten, sowie verschiedene Wiederanlaufoptionen für verschiedene Schadensereignisse. Notfallpläne für Sofortmaßnahmen sollten unter anderem sicherstellen, dass das Wohlergehen der betroffenen Personen sichergestellt ist.

Je nach Ausprägung der Institution und Integration des Notfallmanagements in das Risikomanagement der Institution, kann das Erstellen eines Krisenstabsleitfadens und eines Krisenkommunikationsplans sinnvoll sein. Der Krisenstabsleitfaden sollte Hilfestellung für die strategische Entscheidungsfindung des Krisenstabs enthalten. Der Krisenkommunikation enthält die Informationen über die Art und Wege der Kommunikation mit den Medien aber auch mit

anderen Interessengruppen, Kriterien wann und unter welchen Bedingungen kommuniziert wird und die Kommunikationsstrategie.

Die verschiedenen Notfallpläne müssen aufeinander abgestimmt sein. Jeder Plan sollte die Informationen enthalten

- wer für das Dokument verantwortlich zeichnet,
- welchen Geltungsbereich der Plan hat,
- für welchen Zweck er zu verwenden ist,
- durch wen, unter welchen Bedingungen und wie der Plan aktiviert wird,
- wie die Kommunikationslinien für diesen Bereich sind und
- detailliert was die Aufgaben und Arbeitsschritte zur Bewältigung des Notfalls sind.

In der Gesamtheit der Pläne sollten folgende Informationen enthalten sein:

- Rollenspezifikationen für die Notfallbewältigung mit Aufgaben, Rechten und Pflichten,
- Kontaktadressen aller Mitarbeiter mit spezifischen Aufgaben in der Notfallbewältigung sowie von externen Kontaktpersonen wie Kooperationspartner, Dienstleister, Hilfsorganisationen oder Aufsichtsbehörden,
- Kriterien für die Deeskalation des Notfalls und die Beschreibung der notwendigen Arbeitsschritte und
- Angaben, wie im Notfall die Lage, Entscheidungen und Aktionen zu protokollieren sind.

Alle Dokumente müssen jeweils durch die Personen zugreifbar, die diese für ihre Aufgaben in der Notfallbewältigung benötigen. Sie müssen für diese verständlich aufbereitet sein. Detailliertere Informationen zum Notfallkonzept sind im BSI-Standard 100-4 *Notfallmanagement* zu finden.

Gleichzeitig mit der Auswahl der einzelnen Maßnahmen und der Erstellung des Notfallkonzepts sollte die Umsetzungsplanung erfolgen. Dafür ist festzuhalten, in welchem Zeitraum die einzelnen Maßnahmen umzusetzen sind und welche passend kombiniert gemeinsam umgesetzt werden können. Außerdem müssen die Maßnahmen nach der Dringlichkeit der Umsetzung priorisiert werden. Im Umsetzungsplan sollte enthalten sein:

- Festlegung von Prioritäten (Umsetzungsreihenfolge): Alle Maßnahmen sollten nach Wichtigkeit und Effektivität priorisiert werden. Grundsätzlich sollten Maßnahmen gegen besonders schwerwiegende Risiken vorrangig umgesetzt werden. Können z. B. aus finanziellen Gründen nicht alle Maßnahmen sofort umgesetzt werden, sollten die Maßnahmen mit der größten Breitenwirkung zuerst umgesetzt werden.
- Bei der Umsetzungsreihenfolge sollten mögliche Zusammenhänge zwischen Maßnahmen berücksichtigt werden.
- Verantwortlichkeiten: Für jede Maßnahme ist festzulegen, wer für deren Initialisierung, Umsetzung und Kontrolle oder Revision verantwortlich ist.

Bei der Auswahl von Notfallmaßnahmen ist deren Angemessenheit und Wirtschaftlichkeit zu beachten. Die Dokumentation sollte konkrete Angaben über Verantwortlichkeiten und Zuständigkeiten sowie geplante Aktivitäten zur Kontrolle, Revision und Überwachung enthalten. Die Reihenfolge für die Umsetzung offener Aktivitäten ist festzuhalten. Außerdem sind die geplanten bzw. eingesetzten Ressourcen für die Umsetzung der einzelnen Notfallmaßnahmen zu dokumentieren.

Bei der Notfallkonzeption ist die Informationssicherheit zu berücksichtigen. Es ist sicherzustellen, dass im Falle eines Notfalls, bei der Inbetriebnahme und dem Betrieb von Ausweichlösungen und der Wiederaufnahme des Normalbetriebs die Informationssicherheit gewährleistet ist. Dazu gehört unter anderem

die Gewährleistung der Vertraulichkeit von Daten (z. B. Zugriffsrechte, Verschlüsselung), Einhaltung der Minimalanforderungen an die Datensicherung und die Einhaltung gesetzlicher Vorgaben (z. B. Archivierung von geschäftsrelevanten Daten). Für alle Notfalllösungen sind Sicherheitskonzepte zu erstellen und Sicherheitsmaßnahmen zu implementieren. Daher ist eine enge Zusammenarbeit mit dem IT-Sicherheitsbeauftragten sicherzustellen.

Ein Notfallkonzept kann vertrauliche Informationen beinhalten, wie z. B. Angaben über Schwachstellen oder Informationen über Schutzmaßnahmen. Solche Informationen können als vertraulicher eingestuft werden und dürfen dann ausschließlich an die zuständigen Personen weitergegeben werden. Das Notfallkonzept sollte daher so gegliedert werden, dass einzelne Teile an den speziellen Adressatenkreis weitergegeben werden können.

Prüffragen:

- Wurden die kritischen Geschäftsprozesse und Ressourcen identifiziert?
- Wurden die wichtigsten, relevanten Risiken für die kritischen Geschäftsprozesse und Ressourcen identifiziert und jeweils eine geeignete Risikostrategie ausgewählt?
- Wurden Kontinuitätsstrategien entwickelt, die einen Wiederanlauf und eine Wiederherstellung der kritischen Geschäftsprozesse in der geforderten Zeit ermöglichen?
- Ist ein aktuelles Notfallkonzept vorhanden?
- Wurden Notfallpläne und Maßnahmen entwickelt und implementiert, die eine effektive Notfallbewältigung ermöglichen und einen schnelle Wiederaufnahme der kritischen Geschäftsprozesse?
- Ist im Notfallkonzept die Informationssicherheit berücksichtigt und wurden entsprechende Sicherheitskonzepte für die Notfalllösungen entwickelt?

# M 6.115 Integration der Mitarbeiter in den Notfallmanagement-Prozess

**Verantwortlich für Initiierung:** Notfallbeauftragter
**Verantwortlich für Umsetzung:** Notfallbeauftragter, Personalabteilung, Vorgesetzte

Notfallmanagement betrifft alle Mitarbeiter. Jeder Einzelne muss durch verantwortungsbewusstes Handeln Schäden vermeiden. Zur Integration der Mitarbeiter in den Notfallmanagement-Prozess sind daher Schulungs- und Sensibilisierungsmaßnahmen durchzuführen, eine Aufgabe, die den gesamten Notfallmanagement-Prozess begleiten muss.

Das Unternehmen oder die Behörde sollte daher einen Prozess für das Schulungs- und Sensibilisierungsprogramm etablieren, in dessen Rahmen ein Schulungs- und Sensibilisierungskonzept zum Thema Notfallmanagement erarbeitet, Schulungsmaßnahmen organisiert und deren Effektivität und Nachhaltigkeit überprüft werden. Das Konzept sollte darauf aufbauen, welche Kenntnisse bei den Mitarbeitern zu ihrem Bereich des Notfallmanagement bereits vorhanden sind. Durch die enge Verzahnung von Notfallmanagement und Sicherheitsmanagement ist auch eine Zusammenarbeit bei den Schulungs- und Sensibilisierungsmaßnahmen sinnvoll.

Den Mitarbeitern müssen die Ziele und die Notwendigkeit des Notfallmanagements vermittelt werden. Sie müssen die Inhalte der Notfallmanagementleitlinie ebenso wie die Ziele und die Aufgaben des Notfallmanagements kennen und verstehen. Jedem Mitarbeiter sollte seine Rolle im Notfallmanagement so vermittelt werden, dass er seine Handlungen an den Grundsätzen des Notfallmanagements orientiert. Das Bewusstsein für das Thema Notfallmanagement und den notwendigen Notfallmaßnahmen muss bei allen Mitarbeitern durch regelmäßige Sensibilisierungsmaßnahmen aufgebaut, erhalten und kontinuierlich erhöht werden.

Dazu gehört auch, dass die Mitarbeiter frühzeitig bei der Planung von Notfallmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt werden. Ziele der Sensibilisierungsmaßnahmen müssen sein, den Mitarbeitern ihre Rolle im Notfallmanagement zu vermitteln und wie sie durch ihr Verhalten zu den Zielen des Notfallmanagements beitragen können.

Mitarbeiter, die eine Rolle in der Notfallvorsorge oder Notfallbewältigung übernommen haben, sind regelmäßig zu schulen. Es ist sicherzustellen, dass sie über das notwendige Wissen, die Kompetenz und die Fähigkeiten verfügen, damit sie ihre aktuellen und zukünftigen Aufgaben im Notfallmanagement erfüllen können.

Daher ist ein Schulungsprogramm zu entwickeln, das

- die vorhandenen Kenntnissen der Mitarbeiter im Notfallmanagement analysiert und
- ein entsprechendes Schulungskonzept entwickelt,
- notwendige Schulungen organisiert oder vermittelt,
- regelmäßig den Erfolg der Maßnahmen überwacht und
- gegebenenfalls das Programm korrigiert und neuen Anforderungen anpasst.

Die durchgeführten Schritte und Maßnahmen des Sensibilisierungs- und Schulungsprogramms zum Notfallmanagement sind schriftlich festzuhalten,

um eine Überprüfung und Erfolgskontrolle zu ermöglichen, die regelmäßig durchzuführen ist.

Prüffragen:

- Werden alle Mitarbeiter regelmäßig für das Thema Notfallmanagement sensibilisiert?
- Gibt es ein Schulungs- und Sensibilisierungskonzept zum Notfallmanagement?
- Werden die Mitarbeiter im Notfallmanagement-Team regelmäßig entsprechend der benötigten Kompetenz geschult?

# M 6.116 Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Notfallbeauftragter

Vor allem in größeren Institutionen existiert häufig bereits ein übergreifendes Risiko-, Sicherheits- und Krisenmanagement. Operationelle Risiken inklusive der IT-Risiken sind integraler Bestandteil des Risikomanagements bzw. des Sicherheitsmanagements. Restrisiken, die trotz Vorsorge vorhanden sind, werden durch das Krisenmanagement abgedeckt.

Im Notfallmanagement werden alle Risiken betrachtet, die zu einer Unterbrechung oder einem Ausfall von kritischen Geschäftsprozessen führen. Damit existieren im Notfallmanagement viele Überschneidungen sowohl mit dem Risikomanagement, mit dem Sicherheitsmanagement, aber auch dem Krisenmanagement. Daher sollten die Methoden zum Management von Risiken aus dem Bereich des Notfallmanagements mit den bereits etablierten Methoden abgestimmt werden. Wichtig ist, dass Arbeitsanweisungen oder Dienstvereinbarungen aus unterschiedlichen Bereichen einer Institution sich nicht widersprechen dürfen.

### Einbeziehung von Aspekten des Notfallmanagements in alle Geschäftsprozesse

Das Leitungsebene muss einen Überblick über die geschäftskritischen Fachaufgaben bzw. Geschäftsprozesse und Informationen haben. Die zuständigen Fachverantwortlichen und das Notfallmanagement-Team müssen konkrete Regeln zur Einbindung von Kontinuitätsaspekten bei der Planung und Umsetzung von Geschäftsprozessen aufstellen (z. B. Schutzmaßnahmen und Klassifizierung).

### Änderungsmanagement

Das Änderungsmanagement beschäftigt sich mit der Planung von Änderungen an Prozessen, Infrastruktur oder Hard- und Software. Es muss durch organisatorische Vorgaben sichergestellt werden, dass dabei Aspekte und Belange des Notfallmanagements berücksichtigt werden.

Prüffragen:

- Ist sichergestellt, dass Aspekte des Notfallmanagements in allen Geschäftsprozessen der Institution berücksichtigt werden?
- Sind die Prozesse, Vorgaben und Verantwortlichkeiten im Notfallmanagement mit dem Risikomanagement, Sicherheitsmanagement und Krisenmanagement abgestimmt (soweit solche Managementsysteme in der Institution vorhanden sind)?

# M 6.117 Tests und Notfallübungen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Notfallbeauftragter
**Verantwortlich für Umsetzung:** Notfallbeauftragter

Um die Wirksamkeit von Maßnahmen im Bereich des Notfallmanagements zu überprüfen, müssen regelmäßig Tests und Notfallübungen durchgeführt werden. Dadurch wird die Validität, Handhabbarkeit und Verständlichkeit des Notfallhandbuchs überprüft. Die wesentlichen Ziele sind dabei, Inkonsistenzen in den Notfallplänen oder Mängel in der Planung und Umsetzung von Notfallmaßnahmen aufzudecken sowie effektive und reibungslose Abläufe in einem Notfall zu trainieren. Typische Übungen sind beispielsweise:

- Funktionstests (z. B. von Stromaggregaten, Klimaanlagen, zentrale Server),
- Durchführung von Brandschutzübungen,
- Durchführung einer Alarmierung und Eskalation,
- Stabsübungen,
- Stabsrahmenübungen,
- der Wiederanlauf nach Ausfall von einzelnen Ressourcen oder Geschäftsprozessen
- Räumung eines Bürogebäudes und Bezug einer Ausweichlokation und
- Ausfall eines Rechenzentrums und Inbetriebnahme des Ausweichrechenzentrums.

Übungen können dabei als Planreviews oder Planbesprechungen am "grünen Tisch", als Simulation oder als realitätsnahe Ernstfallübungen durchgeführt werden.

Die Planung, Konzeption, Durchführung und Auswertung von Tests und Übungen erfordert finanzielle und personelle Ressourcen. Die Ressourcen müssen von der Institutionsleitung bereitgestellt werden. Rollen müssen festgelegt und Mitarbeiter benannt werden. Die Mitarbeiter, die eine Rolle bei der Planung, Konzeption oder Durchführung von Tests und Übungen übernehmen, sind für ihre Aufgaben zu schulen.

Tests und Übungen müssen geplant werden. Nur so kann ein effektiver und effizienter Einsatz von finanziellen und personellen Mitteln für die Überprüfung aller im Geltungsbereich etablierten Notfallmaßnahmen erreicht werden. Tests und Übungen sind regelmäßig und anlassbezogen bei größeren Änderungen im Bereich des Notfallmanagements durchzuführen. Es ist daher eine Mehrjahresplanung durchzuführen, die garantiert, dass der gesamte Geltungsbereich des Notfallmanagements abgedeckt wird. Dabei sollten verschiedene Arten von Tests und Übungen zum Einsatz kommen, um alle Notfallpläne, Notfallmaßnahmen und die Organisationsstruktur der Notfallbewältigung zu prüfen und zu testen. Diese Grobplanung sollte die Art der geplanten Tests, die Ziele, das grobe Zeitraster und eine Aufstellung der benötigten Ressourcen beinhalten. Eine jährlich durchzuführende Zeitplanung sollte die Grobplanung konkretisieren und die konkreten Übungen festlegen.

Die Grob- wie auch die Detailplanung ist von der Institutionsleitung zu genehmigen und abzuzeichnen.

Für jeden Test und jede Übung sollte ein Test- bzw. Übungskonzept erstellt werden. Dieses legt die Details fest, wie Art, Zeitplan, Ressourceneinsatz, Teilnehmer, verfolgte Ziele und Ablauf. Die Erfahrung zeigt, dass durch Seiteneffekte von Tests und Übungen auch Schadensereignisse ausgelöst werden

können. Die Detailplanung ist daher so zu gestalten, dass das Risiko hierfür minimiert wird. Vor Durchführung einer Notfallübung ist das Einverständnis der Behörden- bzw. Unternehmensleitung für die Detailplanung schriftlich einzuholen.

Der Ablauf jedes Tests und jeder Übung ist in einem Protokoll so zu dokumentieren, dass eine Auswertung der Ergebnisse möglich ist. Die Auswertung eines Tests oder Übung ist zu dokumentieren und sollte die Ergebnisse, die Rückmeldungen der Beteiligten sowie der beübten Organisationseinheit und ein Vergleich des Ergebnisses mit den festgelegten Zielen der Übung enthalten. Ergebnisse beinhalten Mängel, Lücken und Vorschläge zur Behebung.

Für die Behebung der erkannten Mängel und Lücken in der Notfallplanung sind Maßnahmen festzulegen, Verantwortliche für die Umsetzung zu benennen und Termine zu setzen. Die zeitgerechte Umsetzung ist durch den Notfallbeauftragten zu kontrollieren.

Prüffragen:

- Existiert eine Grobplanung, die garantiert, dass alle wesentlichen Pläne und Maßnahmen im Geltungsbereich des Notfallmanagements getestet und beübt werden?
- Sind im Notfallmanagement ausreichend Ressourcen für die Planung, Konzeption, Durchführung und Auswertung der Tests und Übungen vorhanden?
- Werden vom Notfallmanagement regelmäßig und anlassbezogen Tests und Notfallübungen verschiedener Art und mit verschiedenen Zielen durchgeführt und dokumentiert?
- Führen bei Notfallübungen aufgedeckte Mängel und Schwachstellen zu einer Überarbeitung der Notfall-Pläne und Notfallmaßnahmen und wird die Umsetzung kontrolliert?

# M 6.118 Überprüfung und Aufrechterhaltung der Notfallmaßnahmen

**Verantwortlich für Initiierung:** Notfallbeauftragter
**Verantwortlich für Umsetzung:** Notfallbeauftragter

Im Notfallmanagement geht es nicht nur darum, das angestrebte Absicherungsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten und fortlaufend zu verbessern. Daher sollten alle Notfallmaßnahmen regelmäßig überprüft werden. Dabei ist zu unterscheiden zwischen der Prüfung, ob bestimmte Maßnahmen geeignet und effizient sind, um die gesteckten Ziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), und der Kontrolle, inwieweit die Notfallmaßnahmen in den einzelnen Bereichen umgesetzt wurden (Revision).

### Regelmäßige und anlassbezogene Prüfungen

Die hierfür notwendigen Überprüfungen, auch Revisionen genannt, sollten zu festgelegten Zeitpunkten durchgeführt werden und können bei gegebenem Anlass auch zwischendurch erfolgen. Die vorhandenen Notfallmaßnahmen sollten mindestens einmal im Jahr überprüft werden. Insbesondere Erkenntnisse aus eingetretenen Notfällen oder Krisen erfordern eine Anpassung der bestehenden Maßnahmen und sollten daher eine Überprüfung initiieren. Aber auch bei Veränderungen im Umfeld sollten die vorhandenen Maßnahmen angepasst werden, beispielsweise wenn

- neue Geschäftsprozesse, Anwendungen oder Komponenten aufgebaut wurden,
- größere Änderungen der Infrastruktur vorgenommen wurden (z. B. Umzug),
- größere organisatorischen Änderungen anstehen (z. B. Outsourcing),
- die Gefährdungslage sich wesentlich geändert hat,
- gravierende Schwachstellen oder Schadensfälle bekannt wurden.

### Koordinierte Vorgehensweise

Es sollte in der Behörde bzw. im Unternehmen festgelegt werden, wie die Tätigkeiten im Zusammenhang mit diesen Überprüfungen zu koordinieren sind. Insbesondere sollte die im Bereich der IT und dem Sicherheitsmanagement durchgeführten Überprüfungen koordiniert werden. Dazu ist zu regeln, welche Maßnahmen wann und von wem zu überprüfen sind, auch damit Doppelarbeit vermieden wird und keine Bereiche innerhalb einer Institution ungeprüft verbleiben.

### Gegenstand der Prüfungen

Es muss geprüft werden, ob Notfallmaßnahmen tatsächlich so umgesetzt sind und eingehalten werden, wie im Notfallkonzept vorgegeben. Hierbei ist zu untersuchen, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden. Zeigt sich dabei, dass Notfallmaßnahmen nicht umgesetzt worden sind oder dass sie in der Praxis nicht greifen, sollten die Ursachen für die Abweichungen ermittelt werden.

Das Notfallkonzept muss regelmäßig aktualisiert, verbessert und an neue Rahmenbedingungen angepasst werden. Es muss regelmäßig geprüft werden, ob die ausgewählten Maßnahmen noch geeignet sind, die Ziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung). Dabei sollte auch die Ef-

fizienz der eingesetzten Notfallmaßnahmen überprüft werden oder ob die Ziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten.

**Durchführung der Prüfungen**

Entsprechend dem jeweiligen Prüfungszweck sind Umfang und Tiefe der Überprüfungen festzulegen. Als Grundlage für alle Überprüfungen dient das Notfallkonzept und die vorhandene Dokumentation des Notfallmanagement-Prozesses.

Eine Überprüfung muss von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen jedoch nicht an der Erstellung der Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Revisoren müssen möglichst unabhängig und neutral sein.

Jede einzelne Überprüfung ist sorgfältig zu planen und durchzuführen. Alle relevanten Feststellungen und Ergebnisse sind in einem Bericht festzuhalten. Dieser sollte neben einer Auswertung auch Korrekturvorschläge enthalten.

Die in den einzelnen Überprüfungen ermittelten Ergebnisse sollten dokumentiert werden. Es muss zudem festgelegt sein, wie mit den Überprüfungsergebnissen zu verfahren ist, da eine Überprüfung nur dann ihre Wirkung zeigt, wenn aufgrund der Überprüfungsergebnisse auch die erforderlichen Korrekturmaßnahmen ergriffen werden. Als mögliche Korrekturmaßnahmen kommen, je nach Ursache, in Frage:

- organisatorische Maßnahmen sind anzupassen,
- personelle Maßnahmen, z. B. Schulungs- und Sensibilisierungsmaßnahmen, sind zu ergreifen oder disziplinarische Maßnahmen einzuleiten,
- infrastrukturelle Maßnahmen, z. B. bauliche Veränderungen, sind zu initiieren,
- technische Maßnahmen, z. B. Änderungen an Systemen, sind vorzunehmen,
- Entscheidungen des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene) sind einzuholen.

Der Bericht sollte dem Leiter des überprüften Bereiches sowie dem Notfallmanagement-Team übergeben werden, die auf dieser Basis die weiteren Schritte konzipieren müssen. Schwerwiegende Probleme sollten direkt der Leitungsebene kommuniziert werden, damit weitreichende Entscheidungen zeitnah getroffen werden können.

Werden bei der Prüfung spezielle Werkzeuge eingesetzt, muss ebenso wie bei der Ergebnisdokumentation sichergestellt sein, dass nur autorisierte Personen darauf Zugriff haben. Der Zugriff auf die unterstützenden Tools sowie die Prüfergebnisse müssen daher besonders geschützt werden.

**Korrekturmaßnahmen**

Erkannte Fehler und Schwachstellen müssen zeitnah abgestellt werden. Der identifizierte Optimierungsbedarf bei Effizienz und Effektivität von Notfallmaßnahmen muss umgesetzt werden.

Aufgrund der Überprüfungsergebnisse sind Entscheidungen über das weitere Vorgehen zu treffen. Insbesondere sind alle erforderlichen Korrekturmaßnahmen in einem Umsetzungsplan festzuhalten. Die Zeitrahmen und die Verantwortlichen für die Umsetzung der Korrekturmaßnahmen sind zu benennen und mit den notwendigen Ressourcen auszustatten.

Es ist ein Prozess aufzusetzen, der die Umsetzung steuert und überwacht. Der aktuelle Status sowie Probleme bei der Umsetzung sind zu dokumentieren. Werden notwendige Korrekturen zum Schließen von Schwachstellen nicht planmäßig durchgeführt, so sind gegebenenfalls zu eskalieren.

Prüffragen:

- Werden regelmäßig und anlassbezogen Überprüfungen der Notfallmaßnahmen durchgeführt?
- Werden die Überprüfungen sorgfältig geplant?
- Werden die Ergebnisse der Überprüfungen ausgewertet und gegebenenfalls in Korrekturmaßnahmen umgesetzt?
- Werden die Korrekturmaßnahmen geplant und die Umsetzung kontrolliert?

# M 6.119 Dokumentation im Notfallmanagement-Prozess

**Verantwortlich für Initiierung:** Notfallbeauftragter
**Verantwortlich für Umsetzung:** Notfallbeauftragter

Der Ablauf des Notfallmanagement-Prozesses, die Arbeitsergebnisse der einzelnen Phasen und wichtige Entscheidungen sollten dokumentiert werden. Eine solche Dokumentation und Protokollierung ist eine wesentliche Grundlage für die Aufrechterhaltung und die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen im Notfallmanagement zu finden und zu beseitigen. Erst durch die kontinuierliche Dokumentation können die Entwicklungen und Entscheidungen im Bereich Notfallmanagement nachvollziehbar zurückverfolgt werden.

Es ist ein nachvollziehbarer Prozess zu etablieren, der für alle alle im Notfallmanagement erstellten Dokumente, Protokolle und Aufzeichnungen sicherstellt, dass diese auffindbar, eindeutig identifiziert, kurzfristig zugänglich und lesbar sind. Jedes Dokument muss sicher gespeichert bzw. verwahrt werden und der Zugriff auf autorisierte Personen zu beschränken, um Missbrauch zu verhindern.

Es ist ein Verfahren zu etablieren, das die regelmäßige wie anlassbezogene Aktualisierung der Dokumente sicherstellt. Veraltete Dokumente, die durch eine neue Version ersetzt wurden, sind als solche zu kennzeichnen, um einer unbeabsichtigten Nutzung vorzubeugen. Für alle im Rahmen des Notfallmanagement erstellten Dokumente ist es wichtig, dass nicht nur die jeweils aktuelle Version, sondern auch die Vorgängerversionen zentral gespeichert und jederzeit abrufbar sind.

Abhängig vom Gegenstand und vom Verwendungszweck sind folgende Arten von Dokumentationen zum Notfallmanagement und dem Notfallmanagement-Prozess zu betrachten:

**Berichte an die Leitungsebene**

Damit die oberste Leitungsebene einer Behörde oder eines Unternehmens die richtigen Entscheidungen in Bezug auf die Steuerung des Notfallmanagements treffen kann, benötigt sie die dafür notwendigen Informationen. Hierfür sollte der Notfallbeauftragte bzw. das Notfallmanagement-Team regelmäßig sowie anlassbezogen Management-Berichte zum Status des Notfallmanagements erstellen.

**Dokumente zum Notfallmanagement**

Folgende Arten von Dokumentationen zum Notfallmanagement sollten erstellt werden:

- die Leitlinie zum Notfallmanagement der Behörde bzw. des Unternehmens
- die Rollenbeschreibungen mit Aufgaben, Rechten und Pflichten
- Übersicht über Ressourcen-Anforderungen und Bereitstellung
- das Notfallvorsorgekonzept mit den Ergebnissen der BIA, die Risikoanalyse, der Kontinuitätsstrategien, erforderlichen Maßnahmen und deren Umsetzung
- das Notfallhandbuch zur effektiven Bewältigung eines Notfalls oder einer Krise mit der Organisationsstruktur für die Notfallbewältigung und den verschiedenen Notfallplänen

- das Sensibilisierungs- und Schulungskonzept, Nachweise der Maßnahmen sowie die Dokumentation der Überprüfung
- Planung, Konzeption und Durchführungsprotokolle von Tests und Übungen
- Planung, Durchführung und Ergebnisse von Revisionen und Überprüfungen (z. B. Prüflisten und Befragungsprotokolle)
- Planung und Durchführung von Korrektur- und Verbesserungsmaßnahmen
- die wesentlichen Arbeiten und Entscheidungen des Notfallmanagement-Teams sollten in Form von z. B. Sitzungsprotokolle und Beschlüssen dokumentiert sein

**Dokumentation von Arbeitsabläufen**

Arbeitsabläufe, organisatorische Vorgaben und Maßnahmen müssen so dokumentiert werden, dass keine Schäden durch Unkenntnis oder Fehlhandlungen entstehen. Es muss bei Notfällen und Krisen möglich sein, den gewünschten Soll-Zustand der Geschäftsprozesse wiederherzustellen. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.

**Dokumentation von Schadensereignissen**

Notfälle, Krisen und deren Behandlung müssen so aufbereitet werden, dass alle damit verbundenen Vorgänge und Entscheidungen nachvollziehbar sind. Ebenso soll es die Dokumentation ermöglichen, Verbesserungen am Notfallvorsorgekonzept und dem Notfallhandbuch vorzunehmen und bekannte Fehler zukünftig zu vermeiden.

**Informationsfluss und Meldewege**

Wichtig für die Notfallbewältigung ist die Beschreibung und zeitnahe Aktualisierung der Melde- und Eskalationswege.

**Dokumentationswesen**

Es ist Aufgabe des Notfallbeauftragten und des unterstützenden Notfallmanagement-Teams stets aktuelle und aussagekräftige Dokumentationen zum Notfallmanagement vorzuhalten. Für alle Dokumentationen im Rahmen des Notfallmanagement-Prozesses sollte es daher eine geregelte Vorgehensweise geben. Dazu gehören z. B. folgende Punkte:

- Dokumentationen müssen verständlich sein. Das bedeutet auch, dass sie zielgruppengerecht gestaltet werden müssen. Berichte an die Leitungsebene haben andere Anforderungen als technische Dokumentationen für Administratoren.
- Dokumentationen müssen aktuell sein. Es muss festgelegt werden, wer sie pflegt. Sie müssen so bezeichnet und abgelegt werden, dass sie im Bedarfsfall schnell gefunden werden können. Es müssen Angaben zu Erstellungsdatum, Version, Quellen und Autoren vorhanden sein. Veraltete Unterlagen müssen sofort aus dem Umlauf genommen und archiviert werden.
- Es sollte ein definiertes Verfahren existieren, um Änderungsvorschläge (inklusive der Erstellung neuer Dokumente) einzubringen, zu beurteilen und gegebenenfalls zu berücksichtigen.
- Neben der schnellen Informationsweitergabe an Berechtigte ist andererseits die Vertraulichkeit von organisationsinternen Details sicherzustellen. Vertrauliche Inhalte müssen als solche klassifiziert werden und die Dokumente sicher verwahrt und bearbeitet werden.

Bei der Pflege der Vielzahl von Dokumente kann ein Dokumentenmanagement hilfreich sein.

Dokumentationen müssen nicht immer in Papierform vorliegen. Das Dokumentationsmedium kann je nach Bedarf gewählt werden. Zur Dokumentation können beispielsweise Übersichtsdiagramme, kurze Sitzungsprotokolle, handschriftliche Notizen oder Software-Tools (z. B. zur Dokumentation der Business Impact Analyse) genutzt werden.

Prüffragen:

- Sind die wesentlichen Dokumente des Notfallmanagement-Systems und der Umsetzung vorhanden?
- Existiert ein Verfahren, das die regelmäßige Aktualisierung der Dokumente sicherstellt, das schnelle Auffinden von Dokumenten ermöglicht und den Zugriff auf autorisierte Personen einschränkt?

# M 6.120 Überprüfung und Steuerung des Notfallmanagement-Systems

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, Notfallbeauftragter
**Verantwortlich für Umsetzung:** Behörden-/Unternehmensleitung, Notfallbeauftragter

Die Institutionsleitung ist für die Prüfung, Steuerung und Verbesserung des Notfallmanagement-Systems verantwortlich. Eine wichtige Grundlage für die zu treffenden Entscheidungen sind übersichtlich und aussagekräftig aufbereitete Informationen zum aktuellen Status des Notfallmanagements in der Institution.

Um das Notfallmanagement-System zu steuern und aufrecht zu erhalten, muss regelmäßig seine Wirksamkeit und Effizienz überprüft werden und diese Ergebnisse auf Leitungsebene bewertet werden. Ziel hierbei ist es, das weitere Vorgehen im Notfallmanagement-Prozess abzustimmen. Daher sind alle erforderlichen Änderungen und Anpassungen am Notfallmanagement-Prozess, wie beispielsweise in den Zielen oder Anforderungen an das Notfallmanagements, aufzuzeigen. Die Ergebnisse müssen dokumentiert und die bisherigen Aufzeichnungen gepflegt werden.

**Regelmäßige Management-Berichte**

Damit die Unternehmens- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Notfallmanagement-Prozesses treffen kann, benötigt sie Eckpunkte über den Stand des Notfallmanagements. Diese Eckpunkte sollten in Management-Berichten aufbereitet werden, die unter anderem folgende Punkte abdecken:

- Ergebnisse von internen Revisionen sowie den Überprüfungen bei Outsourcing-Dienstleister und Zulieferer, mit Mängellisten und Verbesserungsvorschlägen,
- Ergebnisse der Tests und Übungen,
- Rückmeldungen von den verschiedenen Interessengruppen inklusive Kooperationspartner, Outsourcing-Dienstleister, Lieferanten und Aufsichtsbehörden,
- Berichte über aktuelle Risikolage, Schwachstellen und Schadensereignisse, sowie daraus abgeleitete Erkenntnisse und Empfehlungen,
- Berichte über beliebige Änderungen, die Auswirkungen auf das Notfallmanagement haben können (z. B. an der Infrastruktur, in Geschäftsprozessen, bei Dienstleistern),
- Statusberichte zu den etablierten Notfallmaßnahmen, Realisierungs- und Verbesserungsvorhaben,
- Berichte über Schulungs- und Sensibilisierungsmaßnahmen und deren Erfolge,
- Berichte über Änderungen in den gesetzlichen oder vertraglichen Anforderungen an das Notfallmanagement,
- Berichte über bisherige Erfolge und Probleme beim Notfallmanagement-Prozess.

Die Leitungsebene muss vom Notfallmanagement-Team regelmäßig in angemessener Form über die Ergebnisse der Überprüfungen und den Status des Notfallmanagement-Prozesses informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden.

Ein Management-Bericht sollte kurz und übersichtlich sein. Die folgenden Punkte können dabei, je nach aktueller Situation, relevant sein. Allerdings sollte dieser weder überfrachtet noch für die Lageeinschätzung wichtige Informationen verschwiegen werden. Es ist also zu überlegen, aufzeigen

- inwieweit die Vorgaben des Notfallkonzepts in der Institution bereits umgesetzt sind,
- an welchen Stellen noch Lücken und damit Restrisiken bestehen,
- welche Schadensereignisse aufgetreten sind, welche Schäden entstanden sind und welche Schäden verhindert werden konnten,
- welche Ergebnisse interne Überprüfungen erbracht haben,
- inwieweit das erreichte Absicherungsniveau den Anforderungen und der Risikolage der Institution genügt,
- ob sich Rahmenbedingungen geändert haben, so dass weitere Maßnahmen erforderlich sind,
- ob sich die Notfallmaßnahmen als geeignet erwiesen haben oder ob Maßnahmen geändert oder ergänzt werden müssen,
- welche Rückmeldungen es von Kunden, Geschäftspartnern, Mitarbeitern oder der Öffentlichkeit zu Aspekten des Notfallmanagements gab,
- welche Ressourcen für das Notfallmanagement aufgewendet wurden,
- ob und wie die bisherigen Management-Entscheidungen umgesetzt wurden.

Daneben sollte sowohl ein Ausblick auf die zu erwartende Weiterentwicklung des organisationsweiten Notfallmanagements gegeben werden, als auch auf technische Entwicklungen und Verfahrensweisen, die eventuell zur Verbesserung des Notfallmanagement-Prozesses beitragen könnten.

Immer wieder erregen Schadensmeldungen über Geschäftsunterbrechungen die Aufmerksamkeit der Massenmedien. Es hat sich als sinnvoll erwiesen, solche Vorfälle aus anderen Institutionen in den Management-Berichten aufzugreifen und aufzuzeigen, inwieweit die eigene Institution auf ähnliche Vorfälle vorbereitet ist.

**Anlassbezogene Management-Berichte**

Neben den regelmäßigen Management-Berichten kann es notwendig sein, bei überraschend auftretenden Problemen oder aufgrund von Risiken, die aus neuen Entwicklungen resultieren, anlassbezogene Management-Berichte zu erstellen. Dies ist vor allem dann der Fall, wenn diese Probleme nicht auf Arbeitsebene gelöst werden können, weil z. B. materielle Ressourcen außerhalb des bewilligten Rahmens benötigt werden oder weitergehende personelle Regelungen getroffen werden müssen. Auch wenn sich die Risikolage ändert (z. B. durch neue Bedrohungen, neue Technologien, neue Gesetze) kann ein anlassbezogener Management-Bericht sinnvoll sein.

Bei der Abfassung der Management-Berichte sollte berücksichtigt werden, dass sich der Leserkreis in der Regel nicht aus technischen Experten zusammensetzt. Entsprechend sollte sich der Text durch größtmögliche Verständlichkeit und Knappheit auszeichnen, indem gezielt die wesentlichen Punkte, wie beispielsweise bestehende Schwachstellen, aber auch erreichte Erfolge, herausgearbeitet werden.

Am Schluss jedes Management-Berichts, vor allem bei anlassbezogenen Berichten, sollten immer klar priorisierte und mit realistischen Abschätzungen des zu erwartenden Umsetzungsaufwands versehene Maßnahmenvorschläge stehen. Damit wird sichergestellt, dass eine notwendige Entscheidung der Leitungsebene ohne unnötige Verzögerungen herbeigeführt werden kann.

Der Management-Bericht zum Notfallmanagement sollte der Leitungsebene durch ein Mitglied des Notfallmanagement-Teams persönlich präsentiert werden. So können wesentliche Schwerpunkte wie beispielsweise bestehende oder drohende Mängel betont werden. Das Mitglied des Notfallmanagement-Teams steht auch direkt für Rückfragen und weitergehende Erläuterungen zur Verfügung, was erfahrungsgemäß zu einer Beschleunigung des Entscheidungsvorgangs führt.

Darüber hinaus ist der persönliche Kontakt auch wichtig, um Leitungsentscheidungen besser vorbereiten und Probleme schon im Voraus entschärfen zu können. Hilfreich wäre es auch, wenn ein Mitglied der Leitungsebene mit entsprechendem fachlichem Hintergrund und Interesse als Ansprechpartner zur Verfügung steht. Der persönliche Kontakt bietet die Möglichkeit, einen "kleinen Dienstweg" zu etablieren, dessen Existenz sich in dringenden Notfällen als vorteilhaft erweisen kann.

**Management-Entscheidungen**

Das Management entscheidet auf Grundlage der Management-Berichte über notwendige Änderungen, Anpassungen und das weitere Vorgehen im Notfallmanagement-Prozess. Dabei wird die Institutionsleitung bei Bedarf vom Notfallbeauftragten unterstützt. Alle Entscheidungen müssen dokumentiert werden. Dazu gehören insbesondere folgenden Punkte:

- Anpassung des Geltungsbereichs
- Änderung des Risikoakzeptanzniveaus (Risikoappetit)
- Änderungen in der Priorisierung von Geschäftsprozessen
- Änderungen in der Notfallstrategie
- Aktionen zur Verbesserungen der Effektivität des Notfallkonzepts sowie die dafür benötigten Ressourcen
- Veränderungen, die Einfluss auf das Notfallkonzept haben könnten, z. B. bei
    - Geschäftszielen
    - Anforderungen
    - Geschäftsprozessen

Zur kontinuierlichen Verfolgung des Notfallmanagement-Prozesses sollten sämtliche Management-Berichte und Management-Entscheidungen zum Notfallmanagement in geordneter Weise archiviert werden. Diese Dokumentation sollte den Verantwortlichen bei Bedarf kurzfristig zugänglich sein.

Da die Management-Berichte zum Notfallmanagement im Allgemeinen sensitive Informationen über bestehende Schwachstellen und Restrisiken enthalten, ist deren Vertraulichkeit zu schützen. Es müssen angemessene Schutzvorkehrungen getroffen werden, damit keine unbefugten Personen Kenntnis über den Inhalt der Management-Berichte erlangen.

Prüffragen:

- Nimmt die Leitungsebene ihre Aufgabe, das Notfallmanagement-System regelmäßig zu überprüfen, zu bewerten und gegebenenfalls zu korrigieren wahr?
- Wird die Leitungsebene regelmäßig über den Stand des Notfallmanagements durch Managementberichte informiert?

# M 6.121 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Viele Sicherheitsvorfälle werden erst durch falsche Reaktionen zu einem größeren Problem. Dies ist beispielsweise der Fall, wenn überhastet Entscheidungen getroffen werden, etwa wenn spontan Daten durch einen Administrator gelöscht werden, die notwendig gewesen wären, um den Sicherheitsvorfall nachzuvollziehen.

Um jedem Mitarbeiter das richtige Verhalten beim Auftreten eines Sicherheitsvorfalls nahe zu bringen, bietet es sich an, zielgruppenorientierte Richtlinien für die Behandlung von Sicherheitsvorfällen zu erstellen. Dies ermöglicht es auch allen Beteiligten, in Ausnahmesituationen ruhig und besonnen zu handeln.

Für die Administratoren und für die Mitglieder des Sicherheitsmanagements sollte es technische Handlungsanweisungen im Rahmen des Managementsystems zur Sicherheitsvorfallsbehandlung geben. Aber auch die Benutzer müssen frühzeitig einbezogen werden. Ebenso sollte der Umgang bei der Störungs- und Fehlerbehebung (also des Incident Managements) mit Sicherheitsproblemen und sicherheitsrelevanten Service-Anfragen in der Richtlinie geregelt sein. Es empfiehlt sich, eine Richtlinie im Unternehmen bzw. der Behörde zu veröffentlichen, die das angemessene Vorgehen beim Auftreten eines Sicherheitsvorfalls beschreibt und sowohl den Prozess, als auch Melde- und Eskalationswege für alle Mitarbeiter der Institution verbindlich darlegt. Bei der Erstellung der Richtlinie sollte darauf geachtet werden, dass sie vollständig und praktisch anwendbar ist. Die Aufgaben aller Beteiligten müssen darin klar formuliert sein. Von der Richtlinie abweichendes Verhalten sollte nur in dokumentierten Ausnahmefällen gestattet werden.

Zu unterscheiden ist hierbei zwischen allgemein gültigen Verhaltensregeln, die für sämtliche vorstellbaren Sicherheitsvorfälle gelten, und den IT-spezifischen Verhaltensregeln. Folgende allgemein gültige Verhaltensregeln können für alle Arten von sicherheitsrelevanten Unregelmäßigkeiten festgehalten werden:

- Alle Beteiligten sollten Ruhe bewahren und keine übereilten Maßnahmen ergreifen.
- Unregelmäßigkeiten sollten gemäß eines Meldeplans unverzüglich an die entsprechenden Stellen gemeldet werden.
- Gegenmaßnahmen dürfen erst nach Aufforderung durch Berechtigte ergriffen werden.
- Alle Begleitumstände sind durch die Betroffenen ungeschönt, offen und transparent zu erläutern, um damit zur Schadensminderung beizutragen.
- Es sollte eine erste auf den persönlichen Erfahrungen beruhende Einschätzung der möglichen Schadenshöhe, der Folgeschäden, der potentiell intern und extern Betroffenen und möglicher Konsequenzen abgegeben werden.
- Informationen über den Sicherheitsvorfall dürfen nicht unautorisiert an Dritte weitergegeben werden.

Diese allgemeinen Verhaltensregeln müssen in geeigneter Weise allen potentiell betroffenen Mitarbeitern einer Behörde bzw. eines Unternehmens bekanntgegeben werden.

Darüber hinaus können spezifische Verhaltensregeln an die Betroffenen weitergegeben werden, insbesondere an diejenigen, die als Meldestellen für Sicherheitsvorfälle fungieren und die ersten Entscheidungen fällen bzw. die ersten Maßnahmen ergreifen sollen. Dazu gehören Administratoren, IT-Anwendungsverantwortliche und das Sicherheitsmanagement. Zu diesen Verhaltensregeln zählen die in den folgenden Maßnahmen beschriebenen:

- M 6.23 *Verhaltensregeln bei Auftreten von Schadprogrammen*
- M 6.31 *Verhaltensregeln nach Verlust der Systemintegrität*
- M 6.48 *Verhaltensregeln nach Verlust der Datenbankintegrität*
- M 6.54 *Verhaltensregeln nach Verlust der Netzintegrität*
- M 6.102 *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*

Ein Beispiel, wie die in den Richtlinien beschriebenen Verhaltensregeln und der Meldeplan (siehe M 6.61 *Eskalationsstrategie für Sicherheitsvorfälle*) jedem betroffenen Mitarbeiter bekanntgegeben werden können, ist ein von der Behörden- bzw. Unternehmensleitung unterzeichnetes Informationsblatt, auf dem die wichtigsten Informationen zusammengefasst sind und das am Arbeitsplatz und ergänzend im Intranet vorgehalten werden kann. Ein Beispiel für ein solches Informationsblatt findet sich unter den Hilfsmitteln zum IT-Grundschutz. Damit die Information im Ernstfall auch tatsächlich verfügbar ist, ist es nicht sinnvoll, diese nur in elektronischer Form zu verbreiten, da dann auch genau diese Information vom Sicherheitsvorfall betroffen sein könnte.

Alle Informationsblätter zu potentiellen Sicherheitsvorfällen müssen bei jeder relevanten Änderung in der Organisation, den Geschäftsprozessen oder der IT sofort aktualisiert werden, damit die dort beschriebenen Verhaltensregeln noch greifen und die Meldewege korrekt sind.

Prüffragen:

- Gibt es zielgruppenorientierte Richtlinien für die Behandlung von Sicherheitsvorfällen?
- Ist die Richtlinie für Sicherheitsvorfälle praktisch anwendbar und kann jeder Beteiligte seine Aufgaben daraus ersehen?
- Regelt die Richtlinie alle Aspekte der Sicherheitsvorfallsbehandlung?
- Ist diese Richtlinie mit der IT-Leitung beziehungsweise dem IT-Betrieb abgestimmt? Ist sie durch die Behörden- beziehungsweise Unternehmensleitung verabschiedet worden?
- Gibt es klar definierte Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen?
- Ist diese Richtlinie allen Mitarbeitern (insbesondere dem IT-Betrieb und dem First Level Support im Service Desk) bekannt?
- Werden die Verhaltensregeln in der Richtlinie regelmäßig aktualisiert?
- Wurden Schnittstellen zu anderen Managementbereichen wie z. B. zum Notfallmanagement berücksichtigt?

# M 6.122 Definition eines Sicherheitsvorfalls

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Analog der Definition eines Notfalls (siehe M 6.110 *Festlegung des Geltungsbereichs und der Notfallmanagementstrategie*) ist es für die Behandlung von Sicherheitsvorfällen unumgänglich, dass in einem Unternehmen bzw. einer Behörde eine klare Vorstellung davon herrscht, was ein Sicherheitsvorfall ist. Vor allem muss klar sein, wie sich Sicherheitsvorfälle von Störungen im Tagesbetrieb unterscheiden. Nur so ist es möglich, im Rahmen des normalen Störungs- und Fehlerbehebungsprozesses den geeigneten Startpunkt für die besonderen Maßnahmen des Prozesses der Sicherheitsvorfallsbehandlung zu finden. Eine weitestgehend formale Definition ohne zu breite Interpretationsspielräume kann den Start dieses Prozesses zusätzlich erleichtern. Die Definition eines Sicherheitsvorfalls sollte auf dem Schutzbedarf der betroffenen Geschäftsprozesse, IT-Dienste, IT-Systeme bzw. IT-Anwendungen basieren. So lässt sich beispielsweise anhand des Schutzbedarfs bzw. den Ergebnissen einer Business Impact Analyse des direkt oder potentiell betroffenen Systems eine Schwelle definieren, ab wann ein Ereignis ein Sicherheitsvorfall ist. Zusätzlich sollte es dem Sicherheitsmanagement unabhängig von Definitionsgrenzen möglich sein, einen außerordentlichen Sicherheitsvorfall auszurufen.

Eine mögliche Definition eines Sicherheitsvorfalls könnte z. B. lauten: *"Als Sicherheitsvorfall wird in unserem Unternehmen/Behörde ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität unserer Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für unser Unternehmen / Behörde / Kunden / Geschäftspartner entstehen kann."*

Die Definition eines Sicherheitsvorfalls muss allen im Sicherheitsvorfallsbehandlungs-Prozess handelnden Mitarbeitern bekannt sein. Sinnvollerweise sollte die individuelle Definition eines Sicherheitsvorfalls mit der Definition eines Notfalls abgestimmt werden.

Prüffragen:

- Ist eine klare Definition zur Abgrenzung eines Sicherheitsvorfalls von Störfällen getroffen worden?
- Ist die Definition eines Sicherheitsvorfalls mit der eines Notfalls abgestimmt?
- Ist die Definition des Sicherheitsvorfalls allen im Prozess zur Sicherheitsvorfallsbehandlung handelnden Mitarbeitern bekannt?
- Wurde bei der Definition eines Sicherheitsvorfalls der Schutzbedarf der betroffenen Geschäftsprozesse, IT-Services, IT-Systeme beziehungsweise ITAnwendungen betrachtet?
- Lassen sich anhand der Definition Sicherheitsvorfälle von Störungen im Tagesbetrieb deutlich und sinnvoll trennen?

# M 6.123 Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Damit Sicherheitsvorfälle durch den gesamten Lebenszyklus des Sicherheitsvorfallbehandlungsprozesses kompetent begleitet werden können, ist es sinnvoll, hierfür ein Team mit erfahrenen und vertrauenswürdigen Spezialisten zusammenzustellen. Dieses Team kann bei Bedarf durch externe Spezialisten ergänzt werden, um angemessen auf alle Arten von Sicherheitsvorfällen reagieren zu können. Alle Mitglieder des Expertenteams sollten auf ihre Vertrauenswürdigkeit hin überprüft werden (siehe auch M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*).

Es ist dabei darauf zu achten, dass alle Mitglieder des Teams geeignet in die Eskalationswege eingebunden werden. Neben der Einrichtung eines Expertenteams muss sichergestellt werden, dass diesem die für die Behandlung eines Sicherheitsvorfalls notwendigen finanziellen und technischen Ressourcen im Bedarfsfall unverzüglich zur Verfügung gestellt werden.

Die meisten Expertenteams existieren als virtuelle Teams, die nur zur Bearbeitung eines Sicherheitsvorfalls einberufen und durch eine erfahrene Führungskraft geleitet werden. Die Rolle der Führungskraft übernimmt zumeist der IT-Sicherheitsbeauftragte. Die konkrete Zusammensetzung der Teammitglieder hängt in der Regel von der Art des Sicherheitsvorfalls und den betroffenen Systemen bzw. Standorten ab. Abhängig vom Informationsverbund können beispielsweise SAP-, Lotus Notes-, Windows-, Datenbank-, Unix- oder Netz-Spezialisten zum Team gehören. Die Mitglieder des Expertenteams müssen nicht nur umfangreiche Kenntnisse über die eingesetzten Systeme besitzen, sondern auch in der Analyse von Sicherheitsvorfällen an diesen Systemen ausgebildet sein. Um immer richtig auf aktuelle Angriffsvarianten reagieren zu können, müssen sich die Mitglieder des Expertenteams regelmäßig weiterbilden.

Prüffragen:

- Sind die Mitglieder des Expertenteams in die Eskalations- und Meldewege eingebunden?
- Ist das Expertenteam in der Analyse von Sicherheitsvorfällen an den eingesetzten Systemen ausgebildet?
- Stehen dem Expertenteam finanzielle und technische Ressourcen zur Verfügung, um den Sicherheitsvorfall schnell und diskret zu behandeln?
- Wurde die Vertrauenswürdigkeit der Mitglieder des Expertenteams überprüft?
- Werden die Mitglieder des Expertenteams regelmäßig weitergebildet?

# M 6.124 Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Störungs- und Fehlerbehebung (auch Incident Management genannt) hat zur Aufgabe, alle Meldungen von Störungen (englisch: Incidents) sowie Anfragen und Aufträge seitens der Anwender entgegenzunehmen, um die Anwender in ihrer Arbeit zu unterstützen und damit einen reibungslosen IT-Einsatz zu gewährleisten.

Auch Sicherheitsvorfälle gelten in diesem Sinne als Störungen, da hierdurch die Verfügbarkeit, Integrität oder Vertraulichkeit der mit der IT verarbeiteten Informationen beeinträchtigt und damit entsprechende Schäden in den Geschäftsfunktionen verursacht werden können.

Service-Störungen können auch Folge unerkannter Sicherheitsvorfälle sein. Dies ist z. B. der Fall, wenn der Sicherheitsvorfall mit Angriffen verbunden ist, die Schwachstellen nutzen, um IT-Dienste und die dafür benötigten IT-Systeme gezielt zu destabilisieren. Mitunter werden diese Sicherheitsvorfälle erst über ihre Wirkung in Form eingetretener Störungen erkannt. Das primäre Ziel beim Incident Management ist, Störungen schnellstmöglich zu beheben und den vereinbarten Service wiederherzustellen, um die Beeinträchtigung der Geschäftsprozesse so gering wie möglich zu halten.

Ebenso können durch IT-Störungen auch neue Sicherheitslücken verursacht werden, wenn z. B. Sicherheitsmechanismen durch instabile Systeme oder Umgehungslösungen außer Kraft gesetzt werden.

Servicebeeinträchtigungen und Sicherheitsvorfälle können also jeweils sowohl Ursache als auch Wirkung sein. Deshalb sollten diese im Zusammenhang betrachtet und behandelt werden. Daher sollten die möglichen Schnittstellen zwischen Incident Management, Notfallmanagement und Sicherheitsmanagement analysiert und gemeinsam benutzbare Ressourcen identifiziert werden. So sollte das Incident Management für die Belange der Sicherheitsvorfallbehandlung sowie des Notfallmanagements sensibilisiert werden. Zusätzlich sollte das Sicherheitsmanagement lesenden Zugriff auf eingesetzte Incident Management Werkzeuge haben, um bei Bedarf Auffälligkeiten erkennen bzw. Störungsmuster identifizieren zu können.

Die folgende Auflistung veranschaulicht die wesentlichen Prozessschritte im Incident Management. Die referenzierten Maßnahmen der IT-Grundschutz-Kataloge beschreiben, welche Integrationsaspekte hier herangezogen werden sollten, um den Incident Management Prozess auch an den Anforderungen des Informationssicherheitsmanagements auszurichten:

- Erkennen und Erfassen (siehe M 6.130 *Erkennen und Erfassen von Sicherheitsvorfällen*)
- Qualifizieren und Erstlösungsversuch (siehe M 6.131 *Qualifizieren und Bewerten von Sicherheitsvorfällen*)

- Analysieren und Lösung vorschlagen (siehe M 6.131 *Qualifizieren und Bewerten von Sicherheitsvorfällen* und M 6.64 *Behebung von Sicherheitsvorfällen*)
- Lösen und Service wiederherstellen (siehe M 6.64 *Behebung von Sicherheitsvorfällen* und M 6.133 *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen*)
- Überwachen und Steuern der Lösung (siehe M 6.133 *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen* und M 6.134 *Dokumentation von Sicherheitsvorfällen*)
- Störung abschließen (siehe M 6.133 *Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen*)

Die Chancen, Störungen und Sicherheitsvorfälle in einem umfassenden und standardisierten Incident Management behandeln zu können, steigen, wenn die vorgeschlagenen Integrationsaspekte berücksichtigt werden.

Prüffragen:

- Wurden mögliche Schnittstellen zwischen Incident Management, Notfallmanagement und Sicherheitsmanagement analysiert? Wurden eventuell gemeinsam benutzbare Ressourcen identifiziert?
- Ist das Incident Management für Belange der Sicherheitsvorfallbehandlung sowie des Notfallmanagements sensibilisiert?
- Hat das Sicherheitsmanagement lesenden Zugriff auf eingesetzte Incident Management Werkzeuge, um bei Bedarf Auffälligkeiten zu erkennen bzw. Störungsmuster zu identifizieren?

# M 6.125 Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Um die Effizienz bei der Aufnahme von Sicherheitsvorfällen zu steigern, sollte geprüft werden, ob eine zentrale Kontaktstelle für die Meldung von Sicherheitsvorfällen eingerichtet werden sollte.

In der Praxis bieten sich zwei Möglichkeiten für die Meldung von Sicherheitsvorfällen:

- Alle Störungen (inklusive der Sicherheitsvorfälle) werden über die zentrale Störungsannahme, also üblicherweise über den Service Desk im First Level des Incident Management, gemeldet.
- Sicherheitsvorfälle werden über eine separate Meldestelle bei einem dedizierten Ansprechpartner des Sicherheitsmanagements gemeldet.

Für eine zentrale Störungsannahme für alle Störungen spricht:

- Die meisten Anwender sind nicht in der Lage, eine Störung als sicherheitsrelevant einzustufen.
- Das Sicherheitsmanagement könnte bereits vorhandene Infrastruktur und Prozesse im IT-Service-Management nutzen.
- Informationen über Sicherheitsvorfälle könnten gemeinsam mit denen über Störfälle in einer zentralen Datenbank verwaltet werden. Die zentrale Verwaltung in einer gemeinsamen Datenbank wäre möglich, wenn mit starker Authentisierung gearbeitet wird und das Werkzeug eine hinreichend differenzierte Berechtigungsverwaltung erlaubt. In der Praxis stößt man hier derzeit jedoch schnell an praktische Grenzen der Umsetzbarkeit.
  **Hinweis:** Es kann aber sinnvoll sein, Sicherheitsvorfälle, die gegen Sicherheitsrichtlinien verstoßen, gesondert zu behandeln (z. B. interne Angriffe).

Eine zentrale Störungsannahme hat allerdings den Nachteil, dass mehr Personen in sicherheitsrelevanten Sachverhalten geschult werden müssen und die Vertrauenswürdigkeit aller Mitarbeiter der zentralen Annahme überprüft werden, damit keine sensiblen Sachverhalte unerwünscht an die Öffentlichkeit gelangen.

Entscheidet sich die Behörde bzw. das Unternehmen für die Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen, sollten den dort tätigen Mitarbeitern Hilfsmittel und Verfahren für das Erkennen von Sicherheitsvorfällen zur Verfügung gestellt werden (z. B. einen Überblick über den Schutzbedarf der betreuten Systeme). Der ebenfalls benötigte Schulungsbedarf zu Informationssicherheit sollte dabei nicht unterschätzt werden (siehe M 6.129 *Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen*). Wenn eine zentrale Kontaktstelle eingerichtet wird, muss diese auch zu den üblichen Arbeitszeiten erreicht werden können. Informationen über Sicherheitsvorfälle müssen von den Mitarbeitern der Kontaktstelle vertraulich behandelt werden.

Prüffragen:

- Ist die Erreichbarkeit der Kontaktstelle für die Meldung von Sicherheitsvorfällen zu üblichen Arbeitszeiten gewährleistet?

- Sind die Mitarbeiter der zentralen Störungsannahme ausreichend geschult und für die Belange der Informationssicherheit sensibilisiert?
- Werden die Informationen über Sicherheitsvorfälle an der Kontaktstelle vertraulich behandelt?
- Sind die Kontaktdaten für die Meldung von Sicherheitsvorfällen allen Mitarbeitern bekannt?

# M 6.126 Einführung in die Computer-Forensik

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Revisor

Bei einer computer- oder auch digital-forensischen Ermittlung geht es darum, strafbare bzw. anderweitig rechtswidrige oder sozialschädliche Handlungen nachzuweisen und aufzuklären, indem digitale Spuren gesammelt und ausgewertet werden. Die Ziele einer solchen Ermittlung nach einem Systemeinbruch oder einem anderen Sicherheitsvorfall sind in der Regel,

- die Methode oder die Schwachstelle zu identifizieren, die zum Systemeinbruch geführt haben könnte,
- den entstandenen Schaden nach einem Systemeinbruch zu ermitteln,
- den Angreifer zu identifizieren und
- die Beweise für weitere juristische Aktionen zu sichern.

Hierfür müssen die für die Analyse des Vorfalls relevanten Daten von den betroffenen IT-Systemen gesammelt werden. Dabei muss sichergestellt sein, dass so viele Informationen wie möglich von einem kompromittierten System gesammelt werden können, ohne dabei den aktuellen Zustand bzw. Status dieses Systems zu verändern. Für die effektive Ermittlung ist es sinnvoll, im Vorfeld einen Leitfaden für einen Ermittlungsprozess zu erstellen, der alle durchzuführenden Schritte beschreibt.

Nach dem sogenannten *Secure-Analyse-Present (S-A-P)* Modell kann ein Ermittlungsprozess in drei große Phasen eingeteilt werden. In der *Secure-Phase* werden alle Daten sorgfältig erfasst. Hierbei ist darauf zu achten, dass der Untersuchungsbereich sorgfältig abgesichert wird. Zu diesem Zeitpunkt ist oft noch nicht klar, ob der Täter von innen kommt. Möchten die Mitglieder des Expertenteams hier möglichen Manipulationen vorbeugen, sind entsprechende Vorkehrungen zu treffen, damit Innentäter nicht ihre Spuren verwischen können. In dieser Phase wird durch geeignete Methoden der Grundstein gelegt, dass die gesammelten Informationen in einer eventuell späteren juristischen Würdigung ihre Beweiskraft nicht verlieren. Auch wenn in dieser sehr frühen Ermittlungsphase oft noch nicht richtig klar ist, ob eine juristische Klärung angestrebt wird, sollte trotzdem das Beweismaterial gerichtsfest sein. Aus diesem Grund müssen alle Tätigkeiten sorgfältig dokumentiert und protokolliert werden. Die gesammelten Daten müssen auch frühzeitig vor versehentlicher oder gar beabsichtigter Manipulation geschützt werden. Von entsprechenden Hash-Verfahren und dem Vier-Augen-Prinzip ist daher ausgiebig Gebrauch zu machen.

In der *Analyse-Phase* werden die Spuren sorgfältig analysiert und die Ergebnisse objektiv bewertet. Die Schlüsse müssen kritisch hinterfragt werden, um Lücken in der Argumentationskette selbstständig und sicher zu identifizieren.

Während die Secure- und Analyse-Phasen hinsichtlich Detaillierungsgrad und Methode oft unabhängig von der konkreten Fragestellung des Sicherheitsvorfalls sind, sind die Tätigkeiten in der *Present-Phase* davon abhängig, wer in welcher Form von den Ermittlungsergebnissen überzeugt werden muss.

Schlussendlich muss das Ergebnis Personen überzeugen, die während der gesamten Ermittlung nicht anwesend waren und vielleicht auch nicht den technischen Sachverstand aufbringen, alle Details zu verstehen. Dies bedeu-

tet, dass alle Erkenntnisse schlüssig und auch für technische Laien nachvollziehbar dokumentiert und dann überzeugend zielgruppenorientiert präsentiert werden müssen. Die Ergebnisse einer forensischen Untersuchung müssen typischerweise Entscheidungsträgern innerhalb der eigenen Institution, aber durchaus auch externen Entscheidungsträgern und Strafverfolgungsbehörden präsentiert werden.

Unabhängig von der konkreten Fragestellung und dem zu untersuchenden IT-System (Server, Workstation, PDA, Router, Notebook, etc.) lassen sich grundsätzlich einige empfindliche Datentypen identifizieren, die für die Ermittlung von Interesse sind:

- *Flüchtige Daten:* Informationen, die beim geordneten Herunterfahren oder Ausschalten des IT-Systems verloren gehen könnten (Inhalt von Cache und Hauptspeicher, Status der Netzverbindungen, laufende Prozesse, angemeldete Benutzer etc.)
- *Fragile Daten*: Informationen, die zwar auf der Festplatte des IT-Systems gespeichert sind, deren Zustand sich aber beim unsachgemäßen Zugriff ändern kann.
- *Temporär zugängliche Daten*: Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z. B. während der Laufzeit einer Anwendung oder Nutzung einer bestimmten Anwendungsfunktionalität.

Die Kenntnis um die Halbwertzeit dieser Daten ist wichtig, da damit die Reihenfolge der Datensammlung in der Secure-Phase bestimmt wird.

Daraus ergeben sich zwei grundlegende Ermittlungsmethoden in der Computer-Forensik, nämlich Live Response und Post Mortem Analyse:

Die Analyse eines noch aktiven, nicht ausgeschalteten Systems bietet die Möglichkeit, die meisten relevanten flüchtigen Daten zu sammeln und wird *Live Response* genannt. Dieser Ansatz ist sinnvoll, wenn wertvolle flüchtige Daten verloren gehen könnten oder auch das System aus Verfügbarkeits- oder Abhängigkeitsgründen nicht ausgeschaltet werden kann. Eine Live Response Analyse ist auch dann hilfreich, wenn die Gefahr besteht, dass auf den Datenträger nicht mehr zugegriffen werden kann, wenn das System ausgeschaltet wurde. Einer der wesentlichen Vorzüge einer Live Response Analyse liegt darin, dass sich oft nur durch diesen Analyseansatz herausfinden lässt, ob das System auch wirklich angegriffen wurde und ob und wie ein eventuell schadhafter Code aktiv ist. Oft hat man nur zur Laufzeit eines Systems überhaupt eine Chance, Auffälligkeiten zu erkennen, die auf ein Rootkit oder andere schadhafte Software hindeuten. Der Vorteil ist, dass der Prozessspeicher inklusive der gerade auf dem System ablaufenden Ereignisse strukturiert gesichert werden kann.

Eines der Hauptprobleme bei der Live Response Analyse ist allerdings, dass die Reihenfolge der Sicherung der flüchtigen Daten nicht immer zweifelsfrei festgelegt werden kann, da jede Tätigkeit am verdächtigen System auch das verdächtige System selbst verändert. So tauchen beispielsweise bei der Sicherung der Liste der gerade auf dem verdächtigen IT-System laufenden Prozesse auch die für den Sicherungsvorgang verwendeten Befehle auf. Bei unsachgemäßem Tooleinsatz besteht auch die Gefahr, dass weitere Daten zerstört werden bzw. relevante Informationen durch auf dem System installierte Rootkits verschleiert werden können.

Der zweite Untersuchungsansatz wird oft *Post Mortem Analyse* genannt, da er sich mit der Auswertung von Datenträgern bzw. Datenträgerkopien von bereits ausgeschalteten Systemen beschäftigt. Hierbei wird die Analyse an einer

forensischen Kopie des Datenträgers eines kompromittierten Systems durchgeführt. Eine forensische Kopie ist eine bitweise 1:1-Kopie, die als Image-Datei vorliegt. Eine Untersuchung des originalen Datenträgers ohne weitere Sicherungsmechanismen sollte vermieden werden, da die Gefahr der Spurenzerstörung besteht.

Eine Post Mortem Analyse wird durchgeführt, wenn der flüchtige Speicher für den zu klärenden Vorfall nicht relevant ist oder dieser Vorfall schon sehr lange zurückliegt. Die Vorteile der Post Mortem Analyse an einer forensischen Datenträgerkopie ist darin zu sehen, dass flüchtige Daten nicht aus Versehen zerstört werden können und der gesamte Analyseprozess bzw. der Tooleinsatz planbar ist, da die Informationen nicht verloren gehen können. Allerdings liegen hier auch die Nachteile: Es lassen sich nur wenige Aussagen über die Laufzeit treffen und wesentliche Spuren können verborgen bleiben.

Sind für das Verständnis und die Aufklärung des Sicherheitsvorfalls die flüchtigen Daten von Interesse, sollten vor dem Abschalten des verdächtigen Systems die flüchtigen Daten behutsam gesichert werden. Ist dies sorgfältig und fachmännisch geschehen, kann das System vom Stromnetz entfernt werden. Ein normaler System-Shutdown ist dabei möglichst zu vermeiden, da dabei sehr viele fragile Daten unwiederbringlich zerstört werden.

Damit alle Mitarbeiter des Expertenteams für die Behandlung von Sicherheitsvorfällen nachvollziehbar und besonnen die notwendigen Analysen durchführen können, sollten in einem Leitfaden die verschiedenen Untersuchungsschritte beschrieben sein. Dieser Leitfaden sollte unter anderem beinhalten, wie die Daten eines verdächtigen Systems gesichert werden können, Analysepläne für typische Sicherheitsvorfälle sowie die Auswertemethodik. Außerdem sollte er Hinweise für die anzuwendenden Rechtsgrundlagen geben.

Die Methoden der forensischen Untersuchungen sollten regelmäßig auf Optimierungsmöglichkeiten untersucht werden.

Prüffragen:

- Existiert ein Leitfaden, wie die Daten eines verdächtigen Systems gesichert werden können?
- Sind dem Expertenteam für die Behandlung von Sicherheitsvorfällen die Unterschiede der Ermittlungsmethoden bekannt?
- Ist sichergestellt, dass bei Sicherheitsvorfällen die Informationen beweisfest gesammelt werden?
- Werden alle Tätigkeiten im Ermittlungsprozess sorgfältig und manipulationssicher dokumentiert und protokolliert?
- Werden alle Erkenntnisse schlüssig und nachvollziehbar dokumentiert?

# M 6.127 Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Im Vorfeld der Behandlung von Sicherheitsvorfällen müssen Verfahren für die Sicherstellung von anfallenden digitalen Beweismitteln geplant und etabliert werden. Beweismittel sind Tatsachen oder Tatsachenfeststellungen, die als Hilfe zur Wahrheitsfindung im Rahmen einer computer-forensischen Ermittlung bzw. nachfolgenden juristischen Begutachtung dienen. Um die Rechtskraft der Beweismittel und der Vorgehensweise zu klären, sollte überlegt werden, ob zu diesem Thema juristische Beratung notwendig ist. Neben den nötigen technischen Verfahren (siehe *Live Response* und *Post Mortem Analyse* in M 6.126 *Einführung in die Computer-Forensik* sowie M 2.64 *Kontrolle der Protokolldateien* etc.) ist auch die Organisation der Beweissicherung zu beachten. Hierzu gehören beispielsweise vorbereitete Formulare für die Dokumentation der sichergestellten Beweisspuren. Diese Formulare können auch herangezogen werden, um zu erfassen, welche Personen Analysen an den digitalen Beweisspuren vorgenommen haben.

Für die Lagerung von sichergestellten IT-Systemen oder Datenträgern ist ein sicherer Aufbewahrungsort zu wählen. Dieser kann ein Tresorraum oder eine andere Räumlichkeit sein, zu der nur ein minimaler und vertrauenswürdiger Personenkreis Zugang hat.

Werden elektronische Beweisspuren sichergestellt, ist durch den Einsatz von Prüfsummenverfahren während jedes Analyseschrittes die Unversehrtheit der Beweisspuren zu verifizieren. Die Beweisspuren sollten nur auf besonders abgesicherten Systemen gelagert und auf solchen analysiert werden. Diese sollten natürlich sowohl von den möglicherweise kompromittierten IT-Systemen, als auch vom Rest des produktiven Netzes getrennt sein, damit keine Beweise verändert werden.

Die Maßnahmen und Werkzeuge zur Beweissicherung müssen daraufhin überprüft werden, ob sie geeignet sind, die Beweisspuren zuverlässig und manipulationssicher zu sichern.

Die Vorgehensweise zur Beweissicherung muss mit dem IT-Sicherheitsbeauftragten und dem Expertenteam für die Behandlung von Sicherheitsvorfällen abgestimmt werden. Um sicherzustellen, dass Fragen des Datenschutzes berücksichtigt werden, sollte der Datenschutzbeauftragte miteinbezogen werden. Sobald ein Verdacht auf Innentäter besteht, sollte außerdem die Personalvertretung beteiligt werden. Außerdem sollten interne oder externe Juristen hinzugezogen werden, um die eingesetzten Verfahren und Methoden zu bewerten.

Prüffragen:

- Sind Verfahren für die Sicherstellung von anfallenden digitalen Beweismitteln definiert und getestet?
- Sind die etablierten Maßnahmen und Werkzeuge geeignet, die richtigen Beweisspuren zuverlässig und manipulationssicher zu sichern?

- Sind die Beweissicherungsmaßnahmen mit den IT-Sicherheitsbeauftragten und seinem Expertenteam abgestimmt?
- Sind Fragen des Datenschutzes und der Mitbestimmung im Vorfeld geklärt worden?
- Wurden interne oder externe Juristen zur Bewertung der eingesetzten Verfahren und Methoden konsultiert?

# M 6.128 Schulung an Beweismittelsicherungswerkzeugen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter

Die Mitglieder des Expertenteams für die Behandlung von Sicherheitsvorfällen müssen die Werkzeuge für die Sicherung und Analyse der digitalen Beweismittel kennen und deren Einsatz beherrschen, da gerade während einer Live Response Analyse wichtige Daten unbeabsichtigt zerstört werden können. Besonders in Behörden bzw. Unternehmen mit verteilten Standorten können in den ersten Stunden nach Bekanntwerden eines Sicherheitsvorfalls nicht immer Spezialisten des Expertenteams für die Behandlung von Sicherheitsvorfällen vor Ort sein. In solchen Fällen kann lokales, vertrauenswürdiges IT-Personal oder besser noch Informationssicherheitspersonal mit der Sicherung der Beweismittel betraut werden. Hierzu sind diese Personen in den Umgang mit den jeweiligen Werkzeugen einzuweisen. Dies betrifft auch Administratoren von Servern, Sicherheitsgateways oder anderen IT-Systemen, wenn von diesen beispielsweise Protokolldateien gesichert werden müssen. Dadurch lernen die handelnden Personen auch eventuelle Schwächen und Fehler der verwendeten Werkzeuge kennen, die die Analyseergebnisse beeinflussen könnten.

Bei der Auswahl von Werkzeugen zur Sammlung oder Analyse von digitalen Beweisen ist wichtig, die Herkunft dieser Werkzeuge zu kennen. Die Software-Werkzeuge müssen aus vertrauenswürdigen Quellen stammen, also beispielsweise direkt vom Hersteller. Zusätzlich sollten beispielsweise Prüfsummenverfahren verwendet werden, um eine unberechtigte Manipulation der Werkzeuge frühzeitig zu erkennen. Dies ist besonders relevant, wenn Werkzeuge aus dem Open Source Umfeld zum Einsatz kommen sollen, von denen verschiedene Varianten im Umlauf sein können.

Prüffragen:

- Sind Administratoren und auch die Mitglieder des Expertenteams im Umgang mit Beweismittelsicherungswerkzeugen geschult?
- Sind die Schwächen der verwendeten Werkzeuge bekannt?
- Ist die Herkunft von Analyse-Werkzeugen bekannt und vertrauenswürdig?
- Wird zuverlässig überprüft, dass die Software nicht manipuliert wurde?

# M 6.129 Schulung der Mitarbeiter des Service Desk zur Behandlung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Hat sich die Behörde oder das Unternehmen entschieden, Meldungen über Sicherheitsvorfälle über einen zentralen Benutzer-Support, beispielsweise die zentrale Störungsannahme (den zentralen Service Desk des Incident Management), entgegenzunehmen, müssen die entsprechenden Mitarbeiter für die Belange der Informationssicherheit ausreichend sensibilisiert und geschult sein. Dazu müssen sie unter Anderem die Richtlinie für die Behandlung von Sicherheitsvorfällen und die definierten Verhaltensregeln, Eskalations- und Meldewege kennen.

Die Service Desk Mitarbeiter sollten regelmäßig an Informations- und Schulungsveranstaltungen über Informationssicherheit im Allgemeinen und das Erkennen von Sicherheitsvorfällen im Besonderen teilnehmen. Diese können vom IT-Sicherheitsbeauftragten oder von Externen durchgeführt werden, inhaltlich sind sie auf jeden Fall mit dem IT-Sicherheitsbeauftragten abzustimmen.

Darüber hinaus müssen Service Desk Mitarbeiter auf die notwendigen Hilfsmittel zur Erkennung von Sicherheitsvorfällen zugreifen können und in ihre Bedienung geschult sein. Um Sicherheitsvorfälle rechtzeitig und richtig zu erkennen, müssen Service Desk Mitarbeiter anhand ihrer Checklisten die Existenz von einem Sicherheitsvorfall feststellen können. Um die richtigen Maßnahmen einleiten zu können, müssen die Service Desk Mitarbeiter auch den Schutzbedarf der betroffenen Systeme kennen.

Prüffragen:

- Kennen die Mitarbeiter des Service Desk die Richtlinie für die Behandlung von Sicherheitsvorfällen beziehungsweise Notfällen?
- Stehen den Mitarbeitern des Service Desk Hilfsmittel zum Erkennen von Sicherheitsvorfällen zur Verfügung?
- Kann im Service Desk der Schutzbedarf der Systeme erkannt werden, bei denen vermehrt Störungen auftreten?
- Enthalten die Checklisten des Service Desk auch Fragen zur Erkennung von Sicherheitsvorfällen?

# M 6.130 Erkennen und Erfassen von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter, Notfallbeauftragter

Nicht jeder Sicherheitsvorfall ist unmittelbar als solcher zu erkennen. Viele Sicherheitsvorfälle, insbesondere wenn es sich um gezielte vorsätzliche Angriffe auf IT-Systeme handelt, fallen erst nach Tagen oder Wochen auf. Oftmals kommt es auch zu Fehlalarmen, z. B. weil Hard- oder Software-Probleme als Infektion mit Computer-Viren fehlinterpretiert werden.

Um jedoch eine sicherheitsrelevante Unregelmäßigkeit untersuchen und bewerten zu können, müssen bestimmte Analysen schon vorab durchgeführt worden sein. Dazu zählen

- die Erhebung der vorhandenen IT-Struktur und IT-Vernetzung,
- die Erhebung der Ansprechpartner bzw. Benutzer der IT-Systeme,
- die Erhebung der IT-Anwendungen auf den jeweiligen IT-Systemen und
- die Schutzbedarfsfeststellung der Informationen, IT-Systeme und Anwendungen.

Diese Untersuchungen werden im ersten Schritt der Anwendung des IT-Grundschutzes durchgeführt und müssten daher dem Sicherheitsmanagement im Ergebnis vorliegen.

Sicherheitsvorfälle können auf unterschiedlichen Wegen bekannt werden:

- Feststellung durch Benutzer: Diese melden typischerweise Störungen, wie z. B. einen vermuteten oder tatsächlichen Virenbefall, Datenverluste oder Modifikation von Informationen.
- Erkennung durch ein System:
    - Bei der Systemüberwachung (Monitoring) wird bei Überschreitung eines kritischen Grenzwertes ein Ereignis generiert und entweder als Störung an ein Support-Team weitergeleitet oder automatisch an ein Incident Management System übergeben.
    - Ein IDS (Intrusion Detection System) meldet z. B. einen Angriffsversuch oder einen Einbruch in einen Server.
- Feststellung durch Mitarbeiter aus einer IT-Abteilung: Sobald diese Störungen feststellen, registrieren diese sie typischerweise selbst im Störungserfassungssystem.
- Feststellung durch einen externen Partner: Unter Umständen können Externe die ersten sein, die einen Sicherheitsvorfall melden, beispielsweise weil sie Abweichungen vom normalen Verhalten von IT-Dienstleistungen festgestellt haben. In diesem Fall ist es besonders wichtig, dass alle Meldungen ernst genommen und an die richtigen Stellen weitergeleitet werden, da Außenstehende nicht immer die richtigen Ansprechpartner und die intern verwendeten Begriffe kennen.
- Information durch Strafverfolgungsbehörden oder Presse: Leider kann es auch vorkommen, dass die betroffene Institution von Sicherheitsvorfällen erst durch Polizei oder Presse erfährt. Auch hier ist es wichtig, dass diese an die richtigen Ansprechpartner weitergeleitet werden.

Anhand dieser Informationen kann bei einer eingehenden Meldung eines Sicherheitsvorfalls kurzfristig entschieden werden, welches IT-System mit welchen IT-Anwendungen und mit welchem Schutzbedarf betroffen ist. Damit

zeigt sich wie im Folgenden natürlich auch immer, welche geschäftskritischen Informationen und Geschäftsprozesse betroffen sind, ohne das dies jedes Mal explizit genannt wird. Gleichzeitig kann hierüber identifiziert werden, wer als Ansprechpartner benannt ist und kurzfristig zur Entscheidungsfindung hinzugezogen werden kann.

Stellt sich dabei heraus, dass ein IT-System oder eine IT-Anwendung mit einem hohen Schutzbedarf betroffen ist, so liegt ein Sicherheitsvorfall vor und die festgelegten Schritte zu dessen Behandlung sind einzuleiten. Sind hingegen nur IT-Anwendungen und IT-Systeme mit normalem Schutzbedarf betroffen, kann versucht werden, das Sicherheitsproblem lokal zu beheben, wenn nicht zu erwarten ist, dass höher schutzbedürftige Systeme betroffen sein könnten. Dabei sollte aber auch ein möglicher Kumulationseffekt berücksichtigt werden, wenn erkennbar ist, dass eine Vielzahl von IT-Anwendungen und IT-Systemen mit normalem Schutzbedarf betroffen sein könnten.

Zeichnet es sich ab, dass der Sicherheitsvorfall schwerwiegende Folgen haben könnte und eine hinreichend große Komplexität besitzt, kann es sinnvoll sein, das Sicherheitsvorfall-Team (siehe M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*) kurzfristig einzuberufen.

Sind für die Analyse und Behebung des Sicherheitsvorfalls plattform- oder standortspezifische Spezialkenntnisse nötig, kann es sinnvoll sein, das Expertenteam für die Behandlung von Sicherheitsvorfällen (siehe M 6.123 *Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen*) einzuberufen.

Zur Untersuchung und Bewertung des Sicherheitsvorfalls sind als Nächstes folgende Einflussfaktoren zu erheben:

- Welche IT-Systeme und IT-Anwendungen können von dem Sicherheitsvorfall zusätzlich betroffen sein?
- Können Folgeschäden auch durch die Vernetzung der IT-Systeme entstehen?
- Für welche IT-Systeme und IT-Anwendungen können Schäden und Folgeschäden ausgeschlossen werden?
- Wie hoch kann der durch den Sicherheitsvorfall verursachte direkte Schaden oder Folgeschaden sein? Dabei ist insbesondere die Abhängigkeit der verschiedenen IT-Systeme und IT-Anwendungen zu beachten.
- Wodurch wurde der Sicherheitsvorfall ausgelöst (z. B. durch Unachtsamkeit, Angreifer oder Ausfall der Infrastruktur)?
- Wann und an welcher Stelle hat sich der Sicherheitsvorfall ereignet? Dies kann auch weit vor der ersten Beobachtung des Sicherheitsvorfalls liegen. Auch bei dieser Untersuchung sind gut geführte Protokolldateien eine wertvolle Hilfe, aber nur, wenn man sich darauf verlassen kann, dass sie nicht manipuliert worden sind.
- Sind durch den Sicherheitsvorfall nur interne IT-Benutzer oder auch externe Dritte betroffen?
- Wie viele Informationen über den Sicherheitsvorfall sind bereits an die Öffentlichkeit gedrungen?

Stellt sich dabei heraus, dass der Sicherheitsvorfall schwerwiegende Folgen nach sich ziehen kann, ist zumindest die nächste Eskalationsebene zu beteiligen.

Nach dieser Erhebung der Einflussfaktoren sind die Handlungsoptionen zu erarbeiten, die aus Sofortmaßnahmen und ergänzenden Maßnahmen bestehen. Hierbei sind die getroffenen Prioritätenfestlegungen zu beachten (siehe M 6.62 *Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfäl-*

*len*). Dazu sind auch die notwendige Zeitspannen für die Durchführung dieser Maßnahmen und die erforderlichen Kosten und Ressourcen für die Problembehebung und Wiederherstellung abzuschätzen.

Übersteigen Schadenshöhe, Zeit und Kosten eine vorbestimmte Grenze, ist vor der Entscheidung über die Maßnahmenauswahl die nächst höhere Eskalations- und Entscheidungsebene miteinzubeziehen. Im Ergebnis liegen nach einer so strukturierten Untersuchung und Bewertung eines Sicherheitsvorfalls die Handlungsoptionen vor.

Die Erfassung der von Anwendern gemeldeten Störungen erfolgt im Incident Management im First Level Support. Damit ist der First Level Support und der Service Desk von Beginn an in den Bearbeitungszyklus der Störung involviert. Im IT-Betrieb festgestellte Störungen werden in der Regel durch die Administratoren der Systeme selbständig in einem Trouble Ticket System oder mit ähnlichen Werkzeugen erfasst. Die Störungen können also auf unterschiedliche Art und Weise erkannt und entgegengenommen werden. Dies macht deutlich, dass sich eine klare Prozessregelungen für die Steuerung der Störungs- bzw. Sicherheitsvorfallbearbeitung empfiehlt.

Bereits bei der Erfassung einer Störung im First Level Support im Incident Management könnten Indizien darauf hindeuten, dass es sich um einen Sicherheitsvorfall handelt, ohne dass dies den Benutzern bewusst ist. Das Incident Management - in diesem Fall der First Level Support - sollte berücksichtigen, dass die Einbeziehung des Sicherheitsmanagements notwendig sein könnte und die meldende Person entsprechend darauf hingewiesen wird.

Prüffragen:

- Liegen alle erforderlichen Vorab-Analysen wie Schutzbedarfsfeststellung und Strukturanalyse vor?
- Liegen die erforderlichen Informationen aus der Schutzbedarfsfeststellung den Meldestellen (insbesondere im Incident Management) und den nachfolgenden Eskalationsebenen vor?
- Sind Hilfsmittel vorhanden, um die Auswertung von Sicherheitsvorfällen technisch zu unterstützen, beispielsweise Tools zur Auswertung von Protokolldaten?

# M 6.131 Qualifizieren und Bewerten von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Je differenzierter die Klassifizierung einer Störung oder eines Sicherheitsvorfalls erfolgt, desto präziser sind die Steuerung der Bearbeitung und die Auswertung dieser Störung möglich, aber umso aufwendiger sind Abstimmung und Anwendung der Klassifizierung. Deshalb sollte die Klassifizierungsstruktur regelmäßig auf ihre Wirksamkeit und Angemessenheit überprüft werden. Es sollte ein einheitliches Klassifizierungsverfahren für alle Arten von Störungen und Sicherheitsvorfälle geben. Dies sollte zwischen Sicherheitsmanagement und Incident Management (also der Störungs- und Fehlerbehebung) abgestimmt sein.

Die finale Klassifizierung kann sich von der gemeldeten Klassifizierung unterscheiden, da durch die Benutzer üblicherweise bei der Meldung nur Symptome und nicht die Ursache genannt werden oder der Schutzbedarf der betroffenen Systeme erst später erkannt wird. Falls sich die Tragweite eines Sicherheitsvorfalls durch zusätzlich betroffene Systeme ausdehnt, kann dies auch zu einer Neuklassifizierung führen.

Zusammen mit der Klassifizierung sollte die Störung mit weiteren Informationen verknüpft werden, dazu gehören:

- welche Anwendungen, IT-Systeme und Dienste von der Störung betroffen sind,
- welche Mitarbeiter bzw. Arbeitsgruppe zur Störungsbehebung beauftragt wurden,
- ob andere, bereits bekannte Fehler und Probleme, z. B. Sicherheitslücken in IT-Produkten und -Konfigurationen, in Zusammenhang mit der Störung stehen könnten.

Das für die Erfassung von Störungen eingesetzte Werkzeug sollte es ermöglichen, die Störungen mit solchen Klassifikationen und Zusatzinformationen zu erfassen.

Prüffragen:

- Wurde ein einheitliches Klassifizierungsverfahren für Sicherheitsvorfälle und Störungen festgelegt?
- Wurde das Klassifizierungsverfahren für Sicherheitsvorfälle zwischen IT-Sicherheitsmanagement und Incident Management abgestimmt?

# M 6.132 Eindämmen der Auswirkung von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Neben der effektiven Analyse der Ursachen eines Sicherheitsvorfalls ist es ebenfalls wichtig, den aus diesem Sicherheitsvorfall resultierenden Schaden einzudämmen. Die direkten Auswirkungen des Sicherheitsvorfalls müssen unverzüglich erkannt, abgeschätzt und gemindert werden, damit der Schaden kein hohes, sehr hohes oder existenziell bedrohliches Ausmaß erreichen kann. Dazu ist es erforderlich, dass das Sicherheitsmanagement ausreichend Informationen und einen Überblick über die Zusammenhänge von IT- und Geschäftsprozessen, sowie die dafür benötigten IT-Systeme, IT-Anwendungen und sonstige Ressourcen hat. Diese Informationen können beispielsweise aus einer Strukturanalyse, Schutzbedarfsfeststellung und Business Impact Analyse kommen. Nur so lassen sich zuverlässige Aussagen über die Tragweite und den eventuellen Schaden treffen.

Oft ist eine Analyse eines Sicherheitsvorfalls leichter möglich, wenn die betroffenen IT-Systeme oder Standorte isoliert werden und damit die Gefahr eingedämmt wird, dass sich der Schaden auf nicht betroffene Areale ausbreitet.

Mitunter muss auch die Entscheidungen getroffen werden, dass die Eindämmung des Schadens gegenüber der Aufklärung Vorrang hat. Aus diesem Grund sollten für ausgewählte Sicherheitsvorfallsszenarien Worst-Case-Betrachtungen angestellt werden.

Prüffragen:

- Liegen ausreichend Informationen vor, die die Auswirkung eines Sicherheitsvorfalls abschätzbar machen?
- Sind für ausgewählte Sicherheitsvorfallsszenarien Worst-Case-Betrachtungen durchgeführt worden?

# M 6.133 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Zur Beseitigung von Sicherheitslücken müssen die betroffenen IT-Systeme vom Netz genommen und alle Dateien gesichert werden, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten. Hierzu gehören insbesondere alle relevanten Protokolldateien. Da alle betroffenen IT-Systeme insgesamt als unsicher oder manipuliert betrachtet werden sollten, müssen auf jedem dieser IT-Systeme das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden. Neben Programmen müssen aber auch Konfigurationsdateien und Benutzerdateien auf Manipulationen untersucht werden. Sinnvollerweise sollten hierfür Prüfsummenverfahren eingesetzt werden. Dies setzt allerdings voraus, dass die Prüfsummen des "sicheren" Zustandes im Vorfeld erhoben und auf schreibgeschützte Datenträger ausgelagert wurden (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*).

Um sicherzugehen, dass von einem Angreifer hinterlassene Manipulationen wie trojanische Pferde wirklich beseitigt worden sind, sollten die Original-Dateien von schreibgeschützten Datenträgern wiedereingespielt werden. Dabei muss darauf geachtet werden, dass alle sicherheitsrelevanten Konfigurationen und Patches mit aufgespielt werden. Wenn Dateien aus Datensicherungen wiedereingespielt werden, muss sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren, also z. B. nicht bereits mit dem Computer-Virus infiziert sind. Die Untersuchung der Datensicherungen kann andererseits hilfreich sein, um den Beginn eines Angriffs oder einer Computer-Virusinfektion festzustellen.

Vor der Wiederinbetriebnahme nach einem Angriff sollten alle Passwörter auf den betroffenen IT-Systemen geändert werden. Dies schließt auch die IT-Systeme ein, die nicht unmittelbar durch Manipulationen betroffen waren, von denen aber der Angreifer vielleicht bereits Informationen über die Benutzer und/oder Passwörter eingeholt hat.

Nach der Wiederherstellung eines IT-Systems sollte überprüft werden, ob alle Funktionalitäten auch wirklich vollständig wiedereingerichtet wurden. Dazu können Benutzer mit spezifischen Anwendungs- und Datenkenntnissen einbezogen werden.

Es sollte damit gerechnet werden, dass der Angreifer nach dem Wiederherstellen des "sicheren" Zustands eine erneute Attacke versucht. Deshalb sollten die IT-Systeme, insbesondere die Netzübergänge, mit den entsprechenden Überwachungswerkzeugen beobachtet werden. Neben einer erweiterten Logfileanalyse könnten hierfür beispielsweise auch Intrusion Detection und Intrusion Response Systeme zum Einsatz kommen (siehe auch M 5.71 *Intrusion Detection und Intrusion Response Systeme*).

Bei einem Sicherheitsvorfall erfolgt die Umsetzung der Lösung gegebenenfalls von dem verantwortlichen Systemadministrator, dem Expertenteam für die Behandlung von Sicherheitsvorfällen, dem Computer Emergency Respon-

se Team (CERT), dem Hersteller des IT-Systems oder einem Sicherheitsexperten.

In dieser Phase sollte großer Wert auf die Dokumentation der eingeleiteten Maßnahmen gelegt (Workaround, endgültige Lösung, wer ist zu den Maßnahmen der Know How-Träger) und die Wissensdatenbank (Problem- und Lösungsdatenbank) entsprechend aktualisiert werden (siehe auch M 6.134 *Dokumentation von Sicherheitsvorfällen*).

Sollte zur Umsetzung der Lösung ein Änderungsantrag (Change Request) notwendig sein, so wird dieser beim Änderungsmanagement (Change Management) gestellt. In diesem Fall bleibt der Sicherheitsvorfall als "offen" gekennzeichnet, bis die Änderung erfolgreich durchgeführt wurde. Üblicherweise greifen bei kritischen Sicherheitsvorfällen besondere Change-Management-Szenarien (Emergency Changes), die eine umgehende Lösung ermöglichen sollen.

Da gerade bei der Behebung der Störung externe Dienstleister involviert sein können, ist zu regeln, welche Informationen über den Sicherheitsvorfall wem zugänglich gemacht werden dürfen.

Prüffragen:

- Werden bei der Beseitigung von Sicherheitslücken die betroffenen IT-Systeme vom Netz genommen und alle Dateien gesichert, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten?
- Werden auf allen betroffenen IT-Systeme Betriebssystem und alle Applikationen auf Veränderungen untersucht?
- Werden bei der Wiederherstellung der sicheren Betriebsumgebung Anwender für Anwendungsfunktionstest einbezogen?
- Werden nach der Wiederherstellung die IT-Systeme inklusive der Netzübergänge gezielt überwacht, um erneute Angriffe feststellen zu können?

# M 6.134 Dokumentation von Sicherheitsvorfällen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Während der Behebung eines Sicherheitsproblems sollten alle durchgeführten Aktionen möglichst detailliert, idealerweise standardisiert dokumentiert werden,

- um den Überblick über Ursachen, Auswirkungen und Maßnahmen zu behalten,
- um die aufgetretenen Probleme nachvollziehbar zu machen,
- um einen Fehler, der bei der meist zügigen Umsetzung der Gegenmaßnahmen unterlaufen kann, wieder beheben zu können,
- um bereits bekannte Probleme bei einem erneuten Auftreten schneller bereinigen zu können,
- um die Sicherheitslücken schließen und vorbeugende Maßnahmen ausarbeiten zu können und
- um für eine mögliche Strafverfolgung Beweise zu sammeln.

Zu einer solchen Dokumentation gehören nicht nur eine Beschreibung der durchgeführten Aktionen inklusive der Zeitpunkte unter Nennung der handelnden Personen, sondern auch die Protokolldateien der betroffenen IT-Systeme.

Die Vertraulichkeit von Dokumenten zu Sicherheitsvorfällen muss angemessen geschützt werden.

Das Incident Management sollte dafür Sorge tragen, dass die benötigten Informationen vor dem Abschluss der Störung in die jeweiligen Dokumentationssysteme eingepflegt werden. Dafür sind Qualitätssicherungsanforderungen im Vorfeld mit dem Sicherheitsmanagement zu definieren.

Zur standardisierten Dokumentation eines Sicherheitsvorfalls kann das Formular in den Hilfsmitteln zum IT-Grundschutz verwendet werden, das sich auf den BSI-Webseiten findet.

Prüffragen:

- Werden alle Sicherheitsvorfälle nach einem standardisierten Verfahren dokumentiert?
- Ist die Vertraulichkeit bei der Dokumentation und Archivierung der Berichte gewährleistet?

# M 6.135 Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Verantwortliche für die Datensicherung

Der Ausfall eines Samba-Servers kann gravierende Auswirkungen auf die Geschäftsprozesse einer Behörde oder eines Unternehmens haben. Unbeabsichtigte Änderungen, wie zum Beispiel Fehlkonfigurationen oder Hardwarefehler, können die Wiederherstellung wichtiger Systemkomponenten erfordern. Zu den wichtigen Systemkomponenten zählen nicht nur die eigentlichen Systemdateien (zum Beispiel der smbd Dämon des Samba Pakets), sondern auch Konfigurationsdaten (zum Beispiel in *smb.conf*), Statusinformationen (zum Beispiel in den Trivial Database (TDB)-Dateien) und Protokolldaten (zum Beispiel die Logdatei des smbd Dämons). Die Sicherung der Daten muss im Rahmen der Vorgaben eines Datensicherungskonzepts (siehe Baustein B 1.4 *Datensicherungskonzept*) durchgeführt werden.

Bei der Wiederherstellung von Konfigurationsdaten, Statusinformationen und Systemdateien sollte darauf geachtet werden, dass diese zueinander kompatibel sind. Werden beispielsweise zur Wiederherstellung der Konfiguration eines Samba-Servers Konfigurationsdaten verwendet, die ursprünglich mit einer neueren Version des Samba-Pakets in Verwendung waren, so kann dies zu Problemen führen. Möglicherweise kann die ältere Version von Samba einige Parameter in der Konfiguration nicht auswerten, da diese erst in einer späteren Version von Samba hinzugekommen sind. Dies kann zu unerwünschten (Seiten-)Effekten führen bzw. den Betrieb von Samba gänzlich verhindern. Außerdem sollte vor einer Wiederherstellung sichergestellt werden, dass das Basisbetriebssystem identisch eingerichtet wurde (siehe auch M 4.331 *Sichere Konfiguration des Betriebssystems für einen Samba-Server*).

Entsprechend der Serverrolle und den Verfügbarkeitsanforderungen sollte die Wiederherstellung und die Wiederherstellungsdauer im Rahmen eines Notfallplans für den Server regelmäßig getestet und verbessert werden.

Um den Zustand eines Samba-Servers wiederherstellen zu können sollten die folgenden Daten / Informationen regelmäßig gesichert werden:

- Datei smb.conf (Konfigurationsdaten)
- Wichtige TDB-Dateien (Konfigurationsdaten und Statusinformationen)
- Kontoinformationen (Statusinformationen)
- Verzeichnis für Logdateien (Protokolldaten)

In den nachstehenden Abschnitten werden Maßnahmen zum Sichern dieser Daten / Informationen angeführt.

**smb.conf (Konfigurationsdaten)**

Bei der Datei smb.conf handelt es sich um die zentrale Konfigurationsdatei von Samba. Einstellungen zum Verhalten der Samba-Dienste (*nmbd*, *smbd* und *winbindd*) werden in dieser Datei vorgenommen.

Der Speicherort dieser Datei hängt von den Optionen ab, mit denen Samba kompiliert wurde. Mit "smbd -b | grep smb.conf" kann der Speicherort in Erfahrung gebracht werden.

**TDB-Dateien (Konfigurationsdaten und Statusinformationen)**

Samba legt in den TDB-Dateien unterschiedlichste Informationen ab. Hier einige Beispiele:

- Samba legt als Mitglied einer Domäne das Passwort des Computerkontos in der Datei secrets.tdb ab. Bei einem Computerkonto handelt es sich um ein normales Benutzerkonto in der Domänen-Benutzerdatenbank, das für jeden Mitgliedsrechner existiert. Anhand des Passworts dieses Computerkontos authentisieren sich Domänenmitglieder und Domänencontroller gegenseitig. Geht das Passwort des Computerkontos verloren, muss Samba der Domäne neu beitreten.
- In der Funktion als Primary Domain Controller (PDC) speichert Samba in secrets.tdb den Domänen-Security Identifier (SID). Der Verlust des SID bedeutet unter Umständen, dass sämtliche Clients der Domäne erneut beitreten und sämtliche Benutzerprofile an die neue Domäne angepasst werden müssen.
- In anderen TDB-Dateien werden in der Regel nur temporäre Informationen abgelegt, deren Verlust keine Konsequenzen nach sich zieht.

Samba speichert TDB-Dateien in zwei Verzeichnissen. Mit "smbd - b | grep PRIVATE_DIR" kann der Ort des PRIVATE_DIR-Verzeichnisses ermittelt werden, außer wenn in *smb.conf* die Option "private dir" verwendet wurde. In diesem Ordner werden die TDB-Dateien mit vertraulichen Informationen abgelegt. Beim zweiten Verzeichnis handelt es sich um das LOCKDIR-Verzeichnis. Darin werden TDB-Dateien mit nicht vertraulichen Informationen abgelegt. Mit "smbd -b | grep LOCKDIR" kann der Speicherort des LOCKDIR-Verzeichnisses ausgegeben werden, außer wenn in smb.conf die Option "lock directory" verwendet wird.

Es wird empfohlen von allen TDB-Dateien in beiden Verzeichnissen regelmäßig Sicherungskopien zu erstellen. TDB-Dateien, die in Unterverzeichnissen dieser beiden Verzeichnisse abgelegt sind, müssen nicht gesichert werden. Diese enthalten Informationen, die für eine Wiederherstellung nicht nötig sind. Es ist darauf zu achten, dass die Sicherung der TDB-Dateien auf ordnungsgemäße Art erfolgt (siehe Abschnitt "Korrekte Sicherung von TDB-Dateien").

**Kontoinformationen (Statusinformationen)**

Je nachdem, welches Backend (Parameter "passdb backend" in smb.conf) Samba zum Speichern der Kontoinformationen nutzt, muss für die Sicherung ein anderer Weg gewählt werden. In Samba 3.0.0 bis 3.0.23 konnten mehrere Backends gleichzeitig verwendet werden. Frühere sowie spätere Versionen von Samba unterstützen diese Funktion nicht.

Für eine Wiederherstellung ist es notwendig, die Kontoinformationen aus allen eingesetzten Backends regelmäßig zu sichern. Je nachdem, welches oder welche Backends zum Einsatz kommen, werden für die Sicherung der Kontoinformationen folgende Vorgehensweisen empfohlen:

- smbpasswd
  Falls nicht anders über den Parameter "passdb backend" in *smb.conf* konfiguriert (zum Beispiel "passdb backend = smbpasswd:/etc/smb/ priv/ datafile"), hängt der Speicherort dieser Textdatei davon ab, mit welchen Optionen Samba kompiliert wurde. Wenn der Parameter "passdb backend" nicht benutzt wurde, kann der Speicherort mit "smbd -b | grep SMB_PASSWD_FILE" in Erfahrung gebracht werden. Da es sich bei dieser Datei um eine einfache Textdatei handelt, sind bei der Sicherung keine Besonderheiten zu berücksichtigen.

- tdbsam
  Standardmäßig werden die Kontoinformationen in der Datei *passdb.tdb* im Verzeichnis PRIVATE_DIR gespeichert. Der Speicherort kann über den Parameter "passdb backend" in smb.conf verändert werden (zum Beispiel "passdb backend = tdbsam:/etc/smb/priv/datafile.tdb"). Es ist darauf zu achten, dass von dieser TDB-Datei Sicherungen auf ordnungsgemäße Art durchgeführt werden (siehe Abschnitt "Korrekte Sicherung von TDB-Dateien").
- ldapsam
  Sollte kein Prozess für die regelmäßige Sicherung des vollständigen Lightweight Directory Access Protocol (LDAP)-Verzeichnisses in der Behörde oder im Unternehmen existieren, so muss ein eigener Prozess für die Sicherung der für Samba relevanten Kontoinformationen etabliert werden.

**Verzeichnis für Logdateien (Protokolldaten)**

In diesem Verzeichnis speichern nmbd, smbd und winbindd ihre Protokolldateien. Um den Zustand eines Samba-Servers wiederherzustellen, sind die Daten nicht nötig. Doch im Hinblick auf eine nachträgliche Suche nach Fehlerursachen sollten diese Daten regelmäßig gesichert werden.

Falls nicht anders in smb.conf konfiguriert (Option "log file"), hängt der Ort des Verzeichnisses davon ab, mit welchen Optionen Samba kompiliert wurde. In diesem Fall kann das Verzeichnis mit "smbd -b | grep LOGFILEBASE" ermittelt werden.

**Korrekte Sicherung von TDB-Dateien**

Bei TDB handelt es sich um ein binäres Datenbankformat, ähnlich der Berkeley DB, das gleichzeitigen Schreibzugriff von mehreren Prozessen sowie Locking unterstützt. Eine Besonderheit der TDB-Dateien ist, dass die Inhalte der Datenbanken von den Dämonen (nmbd, smbd und winbindd) oft für längere Zeit zwischengespeichert werden und die Inhalte auf der Festplatte zu Laufzeit nicht immer aktuell sein müssen. Außerdem werden beim Schreiben in TDB-Dateien die Zeitstempel der Dateien nicht aktualisiert.

Wenn TDB-Dateien im laufenden Betrieb mit ungeeigneten Programmen (zum Beispiel "cp") gesichert werden, berücksichtigen diese deren Besonderheiten nicht. Die erstellten Sicherungen sind unter Umständen unbrauchbar. Sicherungsmechanismen wie "rsync" haben im Normalbetrieb damit Probleme, dass sich die Zeitstempel der TDB-Dateien nach Schreiboperation nicht ändern. Rsync ist so nicht in der Lage zu erkennen, ob sich am Inhalt der TDB-Dateien etwas geändert hat.

Um eine konsistente Sicherung der Datenbanken zur Laufzeit von Samba zu erstellen, muss die Applikation "tdbbackup" verwendet werden. Der Aufruf "tdbbackup /etc/samba/passdb.tdb" erzeugt die Sicherungsdatei /etc/samba/passdb.tdb.bak. Mit dem Aufruf "tdbbackup -v etc/samba/passdb.tdb" kann die Integrität der Datenbank geprüft werden. Werden Schäden gefunden, so wird eine eventuell vorhandene Backup-Datei benutzt, um die Datenbank wiederherzustellen. Über den Parameter -s kann tdbbackup übermittelt werden, welche Dateinamenserweiterungen bei der Sicherung und der Überprüfung benutzt werden sollen. Denkbar wäre statt .bak eine Datumsangabe wie .20080303.

Prüffragen:

- Werden die für die Wiederherstellung eines Samba-Servers nötigen Systemkomponenten im Rahmen des organisationsweiten Datensicherungskonzepts gesichert?
- Werden die Besonderheiten von TDB-Dateien bei der Sicherung berücksichtigt?
- Wird bei der Wiederherstellung von Konfigurationsdaten, Statusinformationen oder Systemdateien darauf geachtet, dass diese zueinander kompatibel sind?
- Werden, entsprechend der Serverrolle und den Verfügbarkeitsanforderungen, die Wiederherstellung und die Wiederherstellungsdauer im Rahmen eines Notfallplans für den Server getestet und gegebenenfalls verbessert?
- Werden die Kontoinformationen aus allen eingesetzten Backends regelmäßig und ordnungsgemäß gesichert?

# M 6.136 Erstellen eines Notfallplans für den Ausfall eines Samba-Servers

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Bei der Erstellung eines Notfallplans für einen Samba-Server sollten zunächst die in M 6.96 *Notfallvorsorge für einen Server* beschriebenen Aspekte beachtet werden. Zusätzlich sind folgende Punkte zu berücksichtigen:

- Die Installationsquellen (etwa Quelltext- oder Binärpakete), mit denen der Samba-Server installiert wurde, sollten an einem festgelegten Ort hinterlegt werden (siehe auch M 6.21 *Sicherungskopie der eingesetzten Software*).
- Wurde der Samba-Dienst aus den Quelltexten übersetzt, so sollte die Dokumentation sämtliche beim Übersetzen verwendeten Optionen (insbesondere die Optionen, mit denen das configure Skript aufgerufen wurde) enthalten.
- Wurde der Samba-Dienst aus einem Binärpaket installiert, so sollten alle Schritte dokumentiert werden, mit denen die Installation nachvollzogen werden kann.
- Jede Änderung an einer Konfigurationsdatei, insbesondere der Datei smb.conf, sollte dokumentiert werden. Es empfiehlt sich eine Versionsverwaltung einzusetzen. Zusätzlich müssen alle Konfigurationsdateien regelmäßig gesichert werden. In der Maßnahme M 6.135 *Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers* befinden sich weitere Informationen zu diesem Thema.

Prüffragen:

- Sind die notwendigen Pakete und Informationen vorhanden, um den Samba-Server im Notfall schnell neu installieren zu können?
- Werden Änderungen an der Konfiguration dokumentiert?
- Sind die Installationspakete aus denen der Samba-Server installiert wurde an einem festgelegten Ort hinterlegt?
- Wenn der Samba-Server aus einem Quelltextpaket installiert wurde, sind die beim Übersetzen verwendeten Optionen dokumentiert?
- Werden alle Konfigurationsdateien regelmäßig gesichert?

# M 6.137 Treuhänderische Hinterlegung (Escrow)

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Notfallbeauftragter
**Verantwortlich für Umsetzung:** Verantwortliche der einzelnen Anwendungen

Je geschäftskritischer ein Prozess ist, desto wichtiger ist es, diesen gegen einen Ausfall abzusichern. Bei der Lieferung vieler Produkte, die Geschäftsprozesse unterstützen (Software, Maschinen, Automaten etc.), erhält der Käufer nicht alle Bestandteile, die zur Wartung des Produktes notwendig sind. Die Wartung wird in diesem Fall häufig durch den Lieferanten sichergestellt. Fällt der Hersteller oder Lieferant aus, ist das Produkt unter Umständen nicht mehr wartbar. Es sollte geprüft werden, ob dieses Risiko durch eine Hinterlegung (*Escrow*) der fehlenden Bestandteile gemindert werden kann.

Escrow ist die "treuhänderische" Hinterlegung von nicht im Lieferumfang enthaltenen Materialien, die zur Wartung und Pflege eines Produktes notwendig sind, bei einem Dritten (Escrow-Agentur). Bei diesen Materialien kann es sich um Software (ausführbar oder als Quellcode), Handbücher, Konstruktionspläne, Konfigurationszustände, Abnahmedaten, Schlüssel, Passwörter oder andere Bestandteile handeln.

Je nach Art des Produktes können sich Unternehmen oder Behörden mit diesem Instrument beispielsweise gegen folgende Risiken absichern:

- Wegfall der Leistungen eines Auftragnehmers im Hinblick auf Fertigstellung, Pflege oder Weiterentwicklung des Produktes
- Ausfall von Zulieferern von Bauteilen und Baugruppen
- Speziell im Fall von Software: Verlust von Quell- und/oder Objektcodes bei Großschäden im IT-Bereich
- Fehlende Möglichkeiten nachzuweisen, wann welcher Versionsstand vorgelegen hat, beispielsweise im Hinblick auf Urheberrecht, Haftung oder Insolvenz

**Funktionsweise**

Der Anwender eines Produktes sichert mit Escrow die kontinuierliche Fortführung eines oder mehrerer geschäftskritischer Prozesse. Hierzu erhält er das Recht, unter definierten Bedingungen auf das hinterlegte Material zuzugreifen und dieses zur Pflege des Produktes zu nutzen, z. B. wenn der Lieferant die im Vertrag festgelegten Leistungen gegenüber dem Anwender nicht erbringt. Auf der anderen Seite schützt der Lieferant seine Wettbewerbsvorteile und seine Betriebsgeheimnisse, solange wie er seinen Verpflichtungen nachkommt. Die Escrow-Agentur prüft und verwahrt das Material für beide Parteien.

Anwender und Lieferant schließen mit der Escrow-Agentur einen Vertrag, der mindestens folgende Aspekte definiert:

- Sicherung der Rechte und Bedingungen zur Herausgabe des hinterlegten Materials
- Verifikation des Materials
- Fachgerechte Lagerung des Materials und angemessene Absicherung
- Aktualisierung des Materials

Die Bedingungen der Hinterlegung und insbesondere auch die Pflichten der Escrow-Agentur im Hinblick auf die Verifizierung und die Herausgabe sind im Escrow-Vertrag genau zu beschreiben. Die individuelle Ausgestaltung dieses

Vertrages hängt sowohl von der Einschätzung der Risiken, gegen die sich der Hinterleger absichern will, als auch vom Rechtsraum ab.

Folgende Hinweise sollten bei der Formulierung und beim Abschluss des Escrow-Vertrages beachtet werden:

- Diskrepanzen zwischen dem Nutzungsvertrag und dem Escrow-Vertrag müssen vermieden werden.
- Hilfreich ist es, den Nutzungsvertrag und den Escrow-Vertrag parallel abzuschließen. Eine zeitliche Verschiebung könnte Nachteile für den Anwender mit sich bringen.
- Je nach Rechtsraum kann ein Escrow-Vertrag gefährdet werden, wenn er zu spät abgeschlossen wird, z. B. kurz vor der Insolvenz des Lieferanten.
- Die Herausgabe des Materials sollte klar definiert sein. Der Escrow-Vertrag sollte ein genaues Verfahren beinhalten, wie die Herausgabe einzuleiten und durchzuführen ist.
- Die Escrow-Agentur muss für beide Seiten vertrauenswürdig sein und sichere und geeignete Aufbewahrungsmöglichkeiten für das zu hinterlegende Material bieten.
- Die technischen Aspekte der Hinterlegung müssen geregelt werden. Die Escrow-Agentur sollte die nötige technische Kompetenz aufweisen, um die Weiterverwendbarkeit des Materials prüfen und die Nachsorge gegenüber Updates leisten zu können.
- Die Verwendbarkeit des Materials nach der Herausgabe ist bereits bei der Zulieferung geeignet zu prüfen. Die Prüfungstiefe hängt von der Einschätzung der Risiken und der verwendeten Technik ab. Beispiele für Prüfungen sind das Kompilieren einer Software aus dem hinterlegten Quellcode oder das Durchspielen einer Montage-Anleitung.
- Durch die Festlegung geeigneter Update-Zyklen ist das Material aktuell zu halten. Welche Zyklen erforderlich sind, hängt vorrangig von der Einschätzung der Risiken und von den Produktionsprozessen des Anwenders ab.

Prüffragen:

- Wurde geprüft, ob durch die treuhänderische Hinterlegung (Escrow) eine Minderung der Sicherheitsrisiken erreicht werden kann?
- Sind im Escrow-Vertrag alle Bedingungen der Hinterlegung, Aktualisierung und Herausgabe sowie die Rechte und Pflichten der beteiligten Parteien präzise festgelegt?
- Ist sichergestellt, dass der Escrow-Vertrag im Einklang mit dem entsprechenden Nutzungsvertrag steht?
- Verfügt die Escrow-Agentur über die notwendigen Qualifikationen?
- Wird bei der treuhänderischen Hinterlegung geprüft, ob das Material im Falle einer zukünftigen Herausgabe verwendbar ist?

# M 6.138 Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Ausfall von Virtualisierungsservern hat in der Regel weitreichende Folgen für den Informationsverbund. Dies liegt daran, dass nicht nur die Virtualisierungskomponente selbst von dem Ausfall betroffen ist, sondern auch alle virtualisierten IT-Systeme, die auf der Komponente betrieben werden.

Daher kann der Ausfall einer Virtualisierungskomponente nicht isoliert betrachtet werden. Es muss im Rahmen der Planung des Einsatzes der Virtualisierung von IT-Systemen im Rechenzentrum bedacht werden, dass durch die angestrebten Konsolidierungseffekte im Bereich des Hardwareeinsatzes auch das Schadensausmaß eines Ausfalls steigt. Dieses Schadensausmaß ist umso höher, je stärker sich die Konsolidierungseffekte auswirken. Daher muss der Schutzbedarf der Gesamtheit der virtuellen IT-Systeme auf den Schutzbedarf der Virtualisierungskomponenten abgebildet werden. Hierbei müssen das *Maximumprinzip* und das *Kumulationsprinzip* beachtet werden.

Es reicht des Weiteren häufig nicht aus, nur den Ausfall von Virtualisierungsservern, auf denen virtualisierte IT-Systeme betrieben werden, zu betrachten. Weitere IT-Systeme, die für den Betrieb der Virtualisierungsserver notwendig sind, müssen einbezogen werden. Der Ausfall dieser Systeme kann die Verfügbarkeit der Virtualisierungssysteme einschränken. Daher muss für die folgenden Systeme, falls vorhanden, eine Vorgehensweise bei ihrem Ausfall festgelegt werden:

- Virtualisierungsserver
- Verwaltungsserver (insbesondere auch Connection-Broker)
- Lizenzierungsserver

Je nachdem, wie die Virtualisierungssysteme in den Informationsverbund integriert sind, müssen auch weitere Systeme wie Verzeichnisdienste und Dienste zur Namensauflösung mit betrachtet werden.

Da Infrastrukturdienste, wie Verzeichnisdienste oder Namensauflösungsdienste, auch auf virtualisierten IT-Systemen ausgeführt werden können, ist es möglich, dass sich durch den Ausfall einer oder mehrerer Virtualisierungskomponenten eine sehr komplexe Situation ergibt. So muss beispielsweise der Wiederanlauf eines stark virtualisierten Rechenzentrums wegen der sich hierbei häufig ergebenden Dienstabhängigkeiten detailliert geplant werden.

Folgende Aspekte müssen grundsätzlich berücksichtigt werden:

- Die Notfallplanung für Virtualisierungssysteme muss in den existierenden Notfallplan integriert werden (siehe Baustein B 1.3 *Notfallmanagement*).
- Durch einen Systemausfall eines Virtualisierungsservers kann es zu Datenverlusten in allen virtuellen IT-Systemen kommen, die auf dem ausgefallenen Virtualisierungsserver ausgeführt werden. Daher muss für alle virtuellen IT-Systeme geprüft werden, inwieweit die vorhandenen Datensicherungskonzepte (vergleiche dazu Baustein B 1.4 *Datensicherungskonzept*) an die gewählte Virtualisierungstechnik angepasst werden müssen. Es sollte für die virtuellen IT-Systeme geprüft werden, ob die neuen Techniken der Virtualisierung (Snapshots) zur Datensicherung genutzt

werden können und welche Vor- und Nachteile sich hieraus ergeben könnten. Wichtige Images müssen in die Datensicherung einbezogen werden.
- Fällt ein Virtualisierungsserver aus, so fallen alle darauf laufenden virtuellen IT-Systeme ebenfalls aus. Die Wahrscheinlichkeit, dass es bei mindestens einem betroffenen virtuellen IT-System zu einem ernsthaften Datenverlust kommt, steigt mit der Anzahl der betroffenen Systeme. Es ist also bei der Notfallplanung zu berücksichtigen, dass möglicherweise ein umfangreicherer Wiederherstellungsaufwand eingeplant werden muss.
- Werden mehrere Virtualisierungsserver in einer Farm eingesetzt (virtuelle Infrastruktur), ist darauf zu achten, dass eine sinnvolle Gruppierung der virtuellen IT-Systeme gewählt wird. So sollten beispielsweise zwei Systeme, die wechselseitig die Aufgaben des jeweils anderen ausführen können, nicht auf einem Virtualisierungsserver betrieben werden.
- Es muss sichergestellt werden, dass im Notfall für den Umgang mit virtuellen Infrastrukturen geschultes Personal zur Verfügung steht.
- Die Systemkonfiguration der Virtualisierungsserver (siehe M 2.318 *Sichere Installation eines IT-Systems*, M 2.315 *Planung des Servereinsatzes* und M 4.237 *Sichere Grundkonfiguration eines IT-Systems*) muss für die Administratoren jederzeit einsehbar sein. Sie muss so gestaltet sein, dass die Virtualisierungsserver im Notfall auch von Personal wiederhergestellt werden können, das mit der vorher vorhandenen Konfiguration nicht detailliert vertraut ist.
- Es muss ein Wiederanlaufplan erstellt werden, der den geregelten Neustart der Virtualisierungsserver und der mit ihm ausgefallenen virtuellen IT-Systeme gewährleistet.
- Es muss sichergestellt sein, dass die Wiederinbetriebnahme der Virtualisierungssysteme nicht von einem Dienst im Rechenzentrum abhängt, der ausschließlich von einem virtuellen IT-System bereitgestellt wird.

Im Rahmen der Notfallvorsorge sollten unterschiedliche Szenarien betrachtet werden, in dem die Virtualisierungssysteme ganz oder in Teilen kompromittiert worden sind. Für diese Szenarien ist präzise zu beschreiben, wie hierauf zu reagieren ist und welche Aktionen jeweils auszuführen sind. Die Vorgehensweise sollte regelmäßig geübt werden.

Eine rechtzeitige Notfallplanung mit vorgegebenen Handlungsanweisungen, die auch von Personen ausgeführt werden können, die nicht detailliert mit der Administration der Virtualisierungssysteme vertraut sind, kann die Folgen im Schadensfall verringern. Die entsprechenden Dokumente für Notfallsituationen müssen für berechtigte Personen zugreifbar sein. Da sie allerdings wichtige Informationen beinhalten, müssen sie geschützt aufbewahrt werden.

Im Einzelnen sollten mindestens die folgenden Notfallsituationen betrachtet werden:

**Angriff**

Wurden Angriffe auf die Virtualisierungssysteme entdeckt, kann nicht davon ausgegangen werden, dass diese auf die Virtualisierungssysteme selbst begrenzt waren. Es muss vielmehr geprüft werden, ob die auf den Virtualisierungssystemen betriebenen virtuellen IT-Systeme kompromittiert worden sind. Dabei muss in Betracht gezogen werden, dass auf den Virtualisierungsservern selbst, aber auch auf den virtuellen IT-Systemen, Schadprogramme (*Backdoors, Trojanische Pferde*) installiert worden sind. Des Weiteren ist es möglich, dass über die Netzkonfiguration der Virtualisierungsserver unerwünschte Kommunikationswege geöffnet worden sind. Zudem können virtuelle IT-Systeme kopiert worden sein.

Um zuverlässig solche Schadprogramme zu entfernen, wird eine komplette Wiederherstellung der Virtualisierungskomponenten empfohlen. Hierzu können die erstellten Datensicherungen herangezogen werden, aber auch die Dokumentation der Systemkonfiguration und die Installationsanweisungen. Besitzt die eingesetzte Virtualisierungsumgebung eine Benutzerverwaltung zur Steuerung von administrativen Zugriffen, sind die Benutzerkonten, insbesondere die der Superuser, auf korrekte Gruppenmitgliedschaften zu überprüfen. Sämtliche Passwörter sollten geändert werden, um die Erfolgschancen von Folgeangriffen zu senken.

Für die virtualisierten IT-Systeme, die auf den kompromittierten Virtualisierungsservern betrieben worden sind, sollten die in den entsprechenden Notfallplänen für diese Systeme aufgeführten Maßnahmen durchgeführt werden.

**Diebstahl von (physischen) Virtualsierungsservern**

Beim Diebstahl von Virtualisierungsservern sind alle Konten zur Verwaltung der Virtualisierungsserver mit neuen Passwörtern zu versehen. Es muss damit gerechnet werden, dass auch virtuelle IT-Systeme mit dem Virtualisierungsserver gestohlen worden sind, insbesondere dann, wenn diese auf lokalen Festplatten des Virtualisierungsservers abgelegt waren. Auch wenn dies nicht der Fall ist, muss davon ausgegangen werden, dass dem Dieb weite Teile der Systemkonfiguration der virtuellen IT-Systeme und der Virtualisierungsinfrastruktur im Rechenzentrum bekannt geworden sind. Daher muss geprüft werden, inwieweit Verbesserungen oder Veränderungen der Virtualisierungsinfrastruktur dazu dienen können, dass die Infrastruktur einem zukünftigen Angriff besser standhalten kann. Im Zweifelsfall sollte die komplette virtuelle Infrastruktur neu gestaltet werden.

**Diebstahl von virtuellen IT-Systemen**

Der Diebstahl eines virtuellen IT-Systems erfordert in der Regel keinen physischen Zugang zum Rechenzentrum. Ein Angreifer kann virtuelle IT-Systeme über Funktionen der Virtualisierungsserver z. B. kopieren. Hierzu benötigt er nur einen Netzzugang, um auf die Speicherressourcen zugreifen zu können, auf denen die virtuellen IT-Systeme abgelegt sind.

Vorbeugend sind Maßnahmen zu entwickeln, die diese Möglichkeiten erschweren (M 2.477 *Planung einer virtuellen Infrastruktur*, M 4.349 *Sicherer Betrieb von virtuellen Infrastrukturen*). Des Weiteren muss geprüft werden, inwieweit solche Angriffe erkannt werden können.

Die Notfallplanung für virtuelle IT-Systeme sollte daher Regelungen enthalten, welche die Verfahrensweise nach einem solchen Diebstahl beschreiben.

**Fehlkonfigurationen**

Fehlkonfigurationen von Virtualisierungsservern können zu weitreichenden negativen Folgen für den Rechenzentrumsbetrieb führen. Daher ist die Virtualisierungssoftware im Rahmen der Notfallvorsorge regelmäßig auf Fehlkonfigurationen zu überprüfen. Werden solche entdeckt, muss ihr Ausmaß bewertet werden. Hierbei ist insbesondere zu prüfen, ob virtuelle IT-Systeme durch die Fehlkonfiguration betroffen sind.

Die notwendigen Änderungen zur Behebung der Konfigurationsfehler können je nach Ausprägung direkt vorgenommen werden. Es muss allerdings beachtet werden, dass virtuelle IT-Systeme möglicherweise während solcher Änderungen beeinträchtigt werden können. Daher kann es notwendig werden, die

virtuellen IT-Systeme vor Konfigurationsänderungen an den Virtualisierungssystemen herunterzufahren.

**Ausfälle durch höhere Gewalt**

Durch Gefährdungen aufgrund von höherer Gewalt, z. B. Erdbeben, Überschwemmung, Feuer, Sturmschäden, Kabelbeschädigungen, kann die Verfügbarkeit der Virtualisierungsserver negativ beeinflusst werden. Hier sind angemessene Maßnahmen zur Erhöhung der Verfügbarkeit zu prüfen, wie beispielsweise redundante Kommunikationsverbindungen der IT-Systeme.

Prüffragen:

- Wurden die Auswirkungen der mit einer virtuellen Infrastruktur einhergehenden Konsolidierungseffekte auf die Verfügbarkeitsanforderungen der Virtualisierungsserver geprüft?
- Wurde eine Vorgehensweise bei einem Ausfall von Virtualisierungskomponenten festgelegt?
- Wurden die Notfallpläne an die virtuelle Infrastruktur angepasst?
- Wurden die Datensicherungskonzepte an die virtuelle Infrastruktur angepasst?
- Ist sichergestellt, dass im Notfall entsprechende Dokumente und geeignetes Personal zur Verfügung stehen?
- Wurden Regelungen erstellt, die die Verfahrensweise nach einem Diebstahl von virtuellen IT-Systemen beschreiben?
- Werden die Virtualisierungsserver regelmäßig auf Fehler geprüft?
- Wurde die Notwendigkeit für Maßnahmen geprüft, die die Verfügbarkeit in Fällen höherer Gewalt steigern?

# M 6.139 Erstellen eines Notfallplans für DNS-Server

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der Ausfall von DNS in einem Informationsverbund hat gravierende Auswirkungen auf den Betrieb der IT-Infrastruktur. Dabei stellt nicht direkt der Ausfall des DNS-Systems das Problem dar, sondern die daraus resultierende Einschränkung auf DNS basierender Dienste. Webserver sind nicht mehr erreichbar, die Fernwartung funktioniert nicht mehr.

Je nachdem welche DNS-Server ausfallen funktioniert die Namensauflösung innerhalb der Institution und/oder von Außen nicht mehr. Funktioniert die Namensauflösung von Außen nicht mehr, wird dies in der Regel schnell öffentlich bekannt werden, was bei regelmäßigen oder längeren Ausfällen einen Imageschaden zur Folge haben kann.

Es ist daher ein Konzept zu entwerfen, wie im Falle eines Ausfalls die daraus resultierenden Folgen minimiert werden können. Beim Festlegen der Aktivitäten sollten folgende Aspekte berücksichtigt werden:

- Die Notfallplanung für DNS-Server muss in den existierenden Notfallplan integriert werden, siehe dazu Baustein B 1.3 *Notfallmanagement*.
- Ein Systemausfall kann zu Datenverlusten führen. Daher ist ein Datensicherungskonzept für die Zonendateien zu erstellen. Dieses ist in das existierende Datensicherungskonzept zu integrieren, siehe dazu Baustein B 1.4 *Datensicherungskonzept*.
- Neben dem Notfallplan für den DNS-Server muss auch für das darunter liegende Betriebssystem ein Notfallplan existieren.
- Für den Betrieb eines DNS-Servers für Anfragen aus dem Internet wird eine funktionierende Internet-Anbindung vorausgesetzt.
- Die Systemkonfiguration ist zu dokumentieren (siehe M 2.25 *Dokumentation der Systemkonfiguration*). Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall von IT-Angestellten auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.
- War die Störung das Resultat eines Angriffs, muss die Schwachstelle behoben und dokumentiert werden.
- Es muss ein Wiederanlaufplan erstellt werden, damit das oder die IT-System(e) wieder geregelt hochgefahren werden kann/können.
- Der Notfallplan sollte auf seine Durchführbarkeit getestet werden.

Prüffragen:

- Existiert ein Notfallplan für den DNS-Server?
- Wurde der Notfallplan für DNS-Server entsprechend in die bereits vorhandenen Notfallpläne integriert?
- Wurde der Notfallplan für DNS-Server entsprechend dokumentiert?

# M 6.140 Erstellen eines Notfallplans für den Ausfall von Groupware-Systemen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Notfallbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der teilweise oder komplette Ausfall eines Groupware-Systems hat in vielen Fällen gravierende Auswirkungen auf die Arbeitsmöglichkeiten der Benutzer, da alle Server-basierten Aktionen nicht mehr ausgeführt werden können. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten bei einem Ausfall durchzuführen sind.

Die Notfallplanung für das eingesetzte Groupware-System muss den existierenden Notfallplan der Institution berücksichtigen (siehe auch Baustein B 1.3 *Notfallmanagement*).

Die Systemkonfiguration aller Groupware-Komponenten ist zu dokumentieren. Dazu gehören die Beschreibung der Festplattenpartitionen und deren Verwendungszwecke (System, Transaktionsprotokoll, Datenbank etc.) sowie die Dokumentation der Hardware, des Betriebssystems des Groupware-Servers und der erforderlichen Groupware-Dienste.

Wichtige Aufgaben, um das Groupware-System aufrecht erhalten bzw. wieder in Betrieb nehmen zu können, müssen so beschrieben sein, dass sie im Notfall direkt von entsprechend geschultem Personal durchgeführt werden können. Der notwendige Detailgrad der Dokumentation richtet sich hierbei nach den Kenntnissen des Personals, das im Notfall zur Verfügung steht. Ist z. B. eine mehrköpfige Gruppe von geschulten Administratoren in der Institution beschäftigt, so können entsprechende Kenntnisse in der Notfalldokumentation vorausgesetzt werden. Ist dagegen nur ein einzelner geschulter Administrator in der Institution tätig, so sollte die Notfalldokumentation wichtige Maßnahmen so beschreiben, dass sie auch von unabhängigen, sachverständigen Dritten durchgeführt werden können.

Für den sicheren und unterbrechungsfreien Betrieb des Groupware-Systems muss der Groupware-Server stets erreichbar sein. Um die Auswirkung eines Serverausfalls zu verringern, können Groupware-Daten durch Partitionierung auf mehrere Server verteilt werden. Der Ausfall eines einzelnen Servers betrifft dann nur einen Teil der Daten. Die Partitionierung ist bedarfsgerecht zu planen und durchzuführen. In Notfällen müssen zumindest einige der Groupware-Clients benutzbar sein bzw. schnellstmöglich wieder betriebsbereit sein. Das Vorgehen hierzu ist im Notfallplan zu dokumentieren.

Durch einen Systemausfall kann es auch zu Datenverlusten auf den Groupware-Server oder -Clients kommen. Daher ist ein Datensicherungskonzept für Groupware zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Im Rahmen der Notfallvorsorge sollten unterschiedliche Kompromittierungsszenarien berücksichtigt und spezifische Handlungsanweisungen für den Fall der Kompromittierung der Server, einzelner Dienste oder einzelner Benutzerkonten gegeben werden.

Die regelmäßige Durchführung von Notfallübungen zur Systemwiederherstellung wird dringend empfohlen. Die Notfallübungen sollten alle Aspekte eines Systemausfalls bzw. einer Kompromittierung berücksichtigen. Die Verantwortlichen sollten in einer speziellen Testumgebung einzelne Dienste neu aufsetzen (z. B. nach einer Kompromittierung) und die Wiederherstellung üben. Das Testsystem sollte dem Produktivsystem so ähnlich wie möglich sein.

In einigen Fällen sind für die Wiederherstellung von Daten oder für die Reparatur eines Groupware-Systems sensitive Zugangsinformationen, wie z. B. kryptographische Schlüssel oder Kennwörter, notwendig. Es ist darauf zu achten, dass der Notfallplan eine Vorgehensweise für solche Fälle definiert. Weiterhin ist durch die Datensicherung oder andere Maßnahmen zu gewährleisten, dass diese Informationen bei einem Notfall verfügbar sind.

Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Groupware-Systems nach einem Ausfall gewährleistet.

Prüffragen:

- Existiert ein Notfallplan für das eingesetzte Groupware-System?
- Existiert ein Wiederanlaufplan für das Groupware-System?
- Finden regelmäßig Notfallübungen statt?

# M 6.141 Festlegung von Ausweichverfahren bei der Internet-Nutzung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Vorgesetzte, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Personalabteilung

Der Zugriff auf das Internet kann aus verschiedenen Gründen ausfallen oder gestört sein. Es können aber auch einzelne Internet-Dienste in ihrer Funktionsfähigkeit eingeschränkt sein. Es werden zwar häufig und auf mehreren Ebenen Maßnahmen zum Schutz der Verfügbarkeit eingesetzt, trotzdem kann es vorkommen, dass bestimmte Internet-Angebote für die Benutzer zeitweise nicht erreichbar oder nicht nutzbar sein können. Falls der Ausfall der Internet-Nutzung für die Behörde oder das Unternehmen nicht toleriert werden kann, ist es wichtig, entsprechende Ausweichverfahren festzulegen. Diese Ausweichverfahren dienen dazu, Ausfallzeiten in einer Art und Weise zu überbrücken, dass Beeinträchtigungen des ordnungsgemäßen Geschäftsbetriebs vermieden oder zumindest minimiert werden. Im Rahmen des Notfallmanagements sollte daher ein Konzept entworfen werden, wie mit Hilfe von Ausweichverfahren die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

**Beispiel:** In einer Institution buchen Mitarbeiter die Bahnfahrkarten, die sie für Dienstreisen benötigen, selbst im Internet. Damit bei einem Internet-Ausfall keine Verzögerungen entstehen, gibt es für diesen Fall eine telefonische Hotline, über die sie ihre Fahrkarten alternativ buchen können.

Bei der Auswahl von Ausweichverfahren in Bezug auf die Internet-Nutzung sollten mindestens folgende Szenarien unterschieden werden:

- Ausfälle im Bereich des eigenen Netzes
- Ausfälle der Kommunikationsverbindungen zwischen dem eigenen Netz und den genutzten IT-Systemen im Internet
- Ausfälle der genutzten IT-Systeme im Internet selbst

Ausfälle im Bereich des eigenen Netzes (Szenario 1) werden im Rahmen des Bausteins B 1.3 *Notfallmanagement* und der Maßnahmen aus dem Bereich Notfallvorsorge in den übrigen Bausteinen der IT-Grundschutz-Kataloge behandelt.

Die Szenarien 2 und 3 lassen sich nur schwer von der eigenen Institution aus beeinflussen, da die betroffenen technischen Komponenten in der Regel von Dritten betrieben werden. Die Nutzung eines zweiten, alternativen Internet-Providers und gegebenenfalls eines alternativen Kommunikationsweges (siehe auch M 6.75 *Redundante Kommunikationsverbindungen*) bietet einen gewissen Schutz vor bestimmten Ausfällen im Netzbereich. Fallen jedoch größere Netzbereiche aus, kann es passieren, dass geschäftskritische Internet-Angebote nicht erreichbar oder nicht nutzbar sind.

Es sollte daher eine Übersicht über die Internet-Dienste und -Anwendungen erstellt werden, die hohe Verfügbarkeitsanforderungen haben. Für diese sollten dann geeignete Ausweichverfahren festgelegt werden. Diese Übersicht sollte regelmäßig aktualisiert werden.

Es bietet sich an, auch Ausweichverfahren in Betracht zu ziehen, die möglichst vollständig ohne Internet-Dienstleistungen auskommen. Häufig wird dabei auf Telefon- oder Telefax-basierte Kommunikation zurückgegriffen. Zu beachten ist, dass auch hier Querbeziehungen bestehen können, die die Wirksamkeit solcher Ausweichlösungen unter Umständen einschränken. Beispielsweise muss bei der Nutzung von Internet-Telefonie sichergestellt sein, dass ein Ausfall des Internet-Zugangs nicht automatisch auch einen vollständigen Ausfall des Telefonie- und Telefax-Dienstes nach sich zieht. Ein weiteres Beispiel für Querbeziehungen (Abhängigkeiten) ist, dass die Call-Center von Dienstleistern in einigen Fällen ebenfalls auf das korrekte Funktionieren der eigenen Internet-Server angewiesen sind. In diesem Fall nützt es nichts, bei einem Ausfall der Internet-Server eines Dienstleisters dessen Hotline anzurufen, da auch das Call-Center dann vermutlich nicht arbeitsfähig ist.

Grundsätzlich kommt auch die Bearbeitung und Kommunikation auf Papier als Ausweichverfahren in Betracht. Häufig scheiden solche Verfahren jedoch aus, da sich dabei in vielen Fällen zu große Verzögerungen ergeben.

Prüffragen:

- Gibt es eine Übersicht über die Internet-Dienste und -Anwendungen mit hohen Verfügbarkeitsanforderungen?
- Sind für geschäftskritische Internet-Dienste und -Anwendungen Ausweichverfahren festgelegt worden?

# M 6.142 Einsatz von redundanten Terminalservern

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Da vom Ausfall einer Terminalserver-Umgebung zumeist eine größere Anzahl Anwender betroffen sein können, sind Maßnahmen zu ergreifen, damit bei einem Ausfall der Schaden verringert wird.

Zudem können Terminalserver nur beschränkt ausgebaut werden, so dass auftretende Systemlasten gegebenenfalls auf mehrere Server verteilt werden müssen. Nähere Details finden sich hierzu auch in M 2.465 *Analyse der erforderlichen Systemressourcen von Terminalservern*.

Durch Terminalserver-Verbünde können in diesen beiden Fällen die Anforderungen an die Verfügbarkeit gewährleistet werden. Hierfür müssen die Benutzersitzungen geeignet auf die verschiedenen Terminalserver verteilt werden. Zu berücksichtigen ist hierbei, inwieweit die Terminalserver, denen Terminalserver-Sitzungen zugewiesen werden, erreichbar und ausgelastet sind.

In der Praxis kommen in diesem Zusammenhang üblicherweise zwei Verfahren zum Einsatz, Netzlastverteiler (Loadbalancer) und systemeigene Mechanismen der jeweiligen Terminalserver-Lösung.

Interne Lastverteilungslösungen können über die reine Netzlast hinaus meist auch Einflüsse wie die Prozessor- oder Speichernutzung überprüfen. So kann etwa vermieden werden, dass Terminalserver mit wenig Ein- und Ausgabe, jedoch rechenintensiven Prozessen, zu viele Anwender zugeteilt bekommen. In Terminalserver-Umgebungen mit hohen Verfügbarkeitsanforderungen sollten daher Lastverteilungsmechanismen verwendet werden, die diese Faktoren mit berücksichtigen.

Werden Lösungen zur automatischen Sitzungsverteilung eingesetzt, sollte auf ein Sitzungsverzeichnis zurückgegriffen werden. Erst hierdurch wird es möglich, dass eine getrennte Verbindung zu einem bestimmten Terminalserver später erneut aufgebaut wird und der Benutzer seine Sitzung fortsetzten kann.

Die Sitzungsverzeichnisse werden, bei Citrix Presentation Server und Windows Terminalserver, in Datenbanken abgelegt und sollten auf dedizierten Systemen installiert werden. Das Sitzungsverzeichnis heißt beim Terminalserver von Microsoft *Session Directory*. Bei Citrix werden die Sitzungsinformationen im sogenannten *IMA* (*Independent Management Architecture*) *Datastore* und teilweise im *ZDC* (*Zone Data Collector*) mit abgelegt.

Informationen innerhalb dieser Datenbanken sind kritisch für die Sicherheit der Terminalserver-Farm. Sie sollten angemessen vor Ausfall, Manipulation und Missbrauch geschützt werden (siehe auch B 5.7 Datenbanken). In der Grundinstallation haben sowohl das *Session Directory* als auch der *IMA Datastore* ein Standpasswort, das geändert werden muss. Insbesondere wenn auf den Terminalservern Anwendungen bereitgestellt werden, die potentiell einen direkten Datenbankzugriff ermöglichen oder einem hohen Schutzbedarf unterliegen, müssen die Datenbanksysteme in einem separaten Netzsegment betrieben werden. In diesem Fall sollten die Verbindungen von der Terminalserver-Farm, zu den Verwaltungsdiensten durch Firewalls kontrolliert werden.

Prüffragen:

- Wurden redundante Terminalserver zur Ausfallkompensation aufgestellt?
- Werden die Benutzersitzungen geeignet auf die verschiedenen Terminalserver verteilt?
- Wurde das Standardpasswort für die Datenbank des Sitzungsverzeichnisses für Terminalserver geändert?

# M 6.143 Bereitstellung von Terminalserver-Clients aus Depot-Wartung

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Fällt ein Terminalserver-Client aus, stehen die Anwendungen auf dem Terminalserver dem betroffenen Benutzer nicht mehr zur Verfügung. Daher sollten beim Einsatz von Terminals ohne eigenes Betriebssystem (Thin Clients) Ersatz-IT-Systeme bereitgehalten werden. Zum raschen Austausch defekter IT-Systeme kann die erforderliche Terminalsoftware im aktuell benötigten Versionsstand vorinstalliert und konfiguriert werden.

Die Menge der bereitzustellenden Systeme ist hierbei in geeigneter Weise an der Anzahl der Arbeitsplätze und der zu erwartenden Ausfälle zu orientieren. In einer rauen Umgebung, mit beispielsweise großer Schmutz oder Staubbelastung, sowie extremen Temperaturen, kann die Lebensdauer der installierten Clients erheblich reduziert sein. Solche Randbedingungen sind in die Kalkulation mit einzubeziehen.

Die Entnahme von Terminalserver-Clients als Ersatzsystem, sowie die Bereitstellung neuer Systeme sollte dokumentiert werden.

Prüffragen:

- Werden eine ausreichende Menge an Terminalserver-Clients als Ersatzsystemen bereitgehalten?
- Wird die Entnahme von Terminalserver-Clients als Ersatzsystemen dokumentiert?

# M 6.144 Konfiguration von Terminalserver-Clients für die duale Nutzung als normale Client-PCs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Fällt der zentrale Terminalserver-Dienst aus, kann durch die vorsorgliche Installation der Applikationen, die auf dem Terminalserver genutzt werden, auf den Client-PCs vorübergehend ein Notfallbetrieb aufrecht erhalten werden. Voraussetzung hierfür sind Arbeitsplatzrechner, die über ausreichende Ressourcen und ein eigenständiges Betriebssystem verfügen, das in der Lage ist, die Programme auszuführen.

Hierzu kann ein Auswahlmenü eingerichtet werden, das dem Benutzer während des Hochfahrens erlaubt, zwischen der Ausführung des Systems im Client-Server-Modus, oder in der Terminalserver-Konfiguration zu unterscheiden. Auf herkömmlichen Client-PCs (Fat Clients), die bereits im normalen Betrieb autark Anwendungen ausführen können und nur bestimmte Applikationen vom Terminalserver beziehen, besteht zudem die Option der parallelen Installation der Software.

Für die Benutzer sollten Schulungen durchgeführt werden, die die korrekte Verwendung dieser Wahlmöglichkeiten aufzeigen.

Für die Verwendung des Terminals als Client-PC ist ebenfalls der Baustein B 3.102 *Server unter Unix* zu betrachten.

Prüffragen:

- Wurden die Benutzer für die Verwendung der dualen Nutzung von Client-PCs als Terminalserver-Clients geschult?

# M 6.145 Notfallvorsorge für TK-Anlagen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

In jedem IT-Betrieb treten Störungen auf, die vom sporadischen Fehlverhalten der Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software aufgrund von Defekten oder Kompromittierungen und aufgrund von Fehlbehandlung durch die Benutzer.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Es ist zudem sinnvoll, Verantwortliche und Ansprechpartner zu benennen. Für typische und für bereits aufgetretene Schadenssituationen sollten Sofortmaßnahmen und weiterführende Handlungsanweisungen erstellt werden. Eine typische Sofortmaßnahme dieser Art kann darin bestehen, einen separaten PSTN-Anschluss mit einem direkt angebundenem Telefon bereitzuhalten, um Notrufe absetzten zu können. Alternativ oder zusätzlich könnten Mobiltelefone als Ersatz vorgehalten werden.

Mittels der sogenannten Katastrophenschaltung, einer im Vorfeld umzusetzenden Maßnahme, können die vorhandenen ankommenden und abgehenden Telefon-Leitungen vorher festgelegten Anschlüssen zugewiesen werden. Dies gewährleistet, dass in einem Katastrophenfall wichtige Einrichtungen handlungsfähig bleiben.

Für bestimmte Elemente der TK-Anlage kann es sinnvoll sein, Ersatzgeräte festzulegen und bereitzuhalten, um eine unvorhergesehen lange Wartezeit auf gleichwertige Ersatzhardware überbrücken zu können. Die Ersatzgeräte können die Funktionalität sofort wieder herstellen, wenn die eventuell notwendige Konfiguration eingestellt wird. Dazu müssen die TK-Anlagen-Konfigurationsdaten (siehe M 6.26 *Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten*) gesichert worden sein.

Im Vergleich zum Normalbetriebszustand weist eine solche Ausweichlösung häufig Nachteile hinsichtlich ihrer Performance oder Redundanz auf. Typisches Beispiel für eine Ausweichlösung ist ein (ressourcenschwächeres) Testsystem. Alle Ausweichlösungen haben oft gemeinsam, dass mit ihrer Hilfe nicht der Normalbetriebszustand erreicht wird, sondern nur eine bestimmte Zeit überbrückt werden kann. In einem Notfallplan für die TK-Anlage ist daher festzuhalten, welche Ausweichlösungen eingesetzt werden sollen und welche Schritte für deren Inbetriebnahme notwendig sind. Die Bestimmung der geeigneten Wiederanlaufreihenfolge der Komponenten der TK-Anlage hilft bei der Auswahl der unbedingt zu überbrückenden Komponenten und grundlegenden Funktionen. Je grundlegender die Funktionalität eines Teilsystems für die Arbeit mit der TK-Anlage ist, umso früher sollte ein solches Teilsystem wiederhergestellt oder zumindest durch eine funktionsgleiche Ausweichlösung ersetzbar sein.

Es hat sich in der Praxis gezeigt, dass IT-Gesamtlösungen oft zu komplex sind, um alle möglichen Ausfallszenarien vorbereitend durchzuspielen und geeignete Wiederanlauffestlegungen zu treffen. Daher ist eine fallweise Bestimmung über Prioritätsklassen zu empfehlen. Für alle IT-Systeme werden zu-

nächst Prioritätsklassen festgelegt, die sich aus den folgenden Kriterien ableiten lassen:

- technische Abhängigkeiten solcher Dienste untereinander
- Bedeutung für die Geschäftsprozesse der Institution
- Umfang des von ihrer Verfügbarkeit profitierenden Nutzerkreises

Alle Festlegungen, die zur Bestimmung der Wiederanlaufreihenfolge führen, sind im Rahmen der Notfallvorsorge vorbereitend zu dokumentieren (zum Beispiel im Notfallhandbuch der IT). Gerade bei komplexen Systemen ist auch die Darstellung von Verknüpfungen und Abhängigkeiten, die individuell für die Institution sind, entscheidend für die Beurteilung von Störungen und ein schnelles und sicheres Eingreifen.

Soweit nicht alle relevanten Festlegungen für die Notfallbehandlung der TK-Anlage aus einem übergeordneten Notfallhandbuch hervorgehen, sollten diese in einem Notfallplan festgehalten werden. Dieser nennt alle vorbereiteten und vorbereitend festgelegten Sofortmaßnahmen, Ausweichlösungen, Notbetriebsformen und Schritte zu deren Einleitung, sowie typische Schritte auf dem Weg zur Wiederherstellung des Normalbetriebs. Ebenfalls enthalten sind notwendige Kontaktinformationen für den Notfall, Festlegungen hinsichtlich Zuständigkeiten für die Einleitung/Durchführung von Maßnahmen und besondere Meldepflichten in Notfällen.

Die sichere Beherrschung notwendiger Notfallmaßnahmen ist von hoher Bedeutung. Entsprechend sind typische Maßnahmen regelmäßig einzuüben. Sofern dies nicht im Rahmen regelmäßig im Betriebsalltag wiederkehrender Tätigkeiten erfolgt, muss ein Einüben in Form von Notfallübungen erfolgen.

Prüffragen:

- Gibt es einen Notfallplan für TK-Anlagen?
- Werden Notfallübungen bezüglich der TK-Anlage durchgeführt?

# M 6.146 Datensicherung und Wiederherstellung von Mac OS X Clients

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Unter Mac OS X können die Daten mit dem zum System gehörenden Dienstprogramm *Time Machine* gesichert werden. Die Software steht bereits bei einer Standardinstallation von Mac OS X zur Verfügung. *Time Machine* lässt sich auch von den Benutzern leicht konfigurieren, mit dem Programm können vollständige Festplatten oder einzelne Verzeichnisse gesichert werden.

Im ersten Schritt erzeugt *Time Machine* eine vollständige Kopie der zu sichernden Informationen, anschließend werden nur noch Informationen gesichert, die seit der letzten Datensicherung verändert wurden oder neu hinzugekommen sind (inkrementelle Datensicherung).

Werden die Informationen mit *Time Machine* gesichert, sollten folgende Punkte beachtet werden:

- die Daten auf den Sicherungsmedien sind nicht verschlüsselt, daher müssen sie vor unbefugtem Zugriff geschützt aufbewahrt werden,
- die gesicherten Informationen werden nicht komprimiert und können mehr als den eingeplanten Speicherplatz belegen,
- eine vollständige Wiederherstellung der gespeicherten Daten kann zeitintensiv sein,
- die Datensicherung erfolgt automatisch alle 30 Minuten nach dem Start des IT-Systems, wenn das Dienstprogramm aktiviert ist, allerdings können Benutzer ein Backup manuell zu jedem Zeitpunkt auslösen,
- im laufenden Betrieb werden nur Daten gesichert, die nicht mit File Vault verschlüsselt sind. Eine Datensicherung der mit File Vault verschlüsselten Daten kann mit *Time Machine* erst durchgeführt werden, nachdem sich der Benutzer vom System abgemeldet hat,
- es können bei einer Sicherung über ein Datennetz ohne zusätzliche Systemeingriffe nur spezielle Network-Attached-Storage-Systeme (NAS) genutzt werden und
- bei der Wiederherstellung des kompletten Systems muss die Mac OS X Installations-DVD vorliegen und der Client unter Mac OS X muss von dieser DVD gestartet werden, da sich die Wiederherstellungsprogramme auf der DVD befinden.

Aufgrund dieser und weiterer limitierender Faktoren ist der Einsatz von *Time Machine* prinzipiell nur beschränkt zu empfehlen und stark abhängig von den lokalen Gegebenheiten. Bei der Wahl einer Datensicherungssoftware in heterogenen Umgebungen wird empfohlen, ein Programm zur Datensicherung einzusetzen, dass mehrere Plattformen wie Mac OS X, Windows und Linux unterstützt.

Mit *Time Machine* können Datensicherungen auf externen Datenträgern, anderen Mac OS X Systemen oder auf einem internen Datenträger, von dem das System nicht gestartet wurde, abgelegt werden. Sollen lokal angeschlossene Datenträger zur Datensicherung genutzt werden, müssen diese mit dem Dateisystem "Mac OS Extended (Journaled)" formatiert sein. Alternativ kann eine Datensicherung in einem freigegebenen Verzeichnis auf einem entfernten System im Netz abgelegt werden. Voraussetzung hierfür ist die Nutzung

des Apple Filing Protocols (AFP). Das SMB/CIFS-Protokoll kann mit folgendem Befehl auf der Konsole aktiviert werden:

defaults write com.apple.systempreferences TMShowUnsupportedNetworkVolumes 1

Die Variable "TMShowUnsupportedNetworkVolumes" ist ein inoffizieller Weg, um weitere Netzprotokolle freizuschalten. Damit kann aber kein fehlerfreier Einsatz garantiert werden und Apple gewährt auch keine Unterstützung für dieses Vorgehen.

*Time Machine* kann in den Systemeinstellungen unter "Time Machine" aktiviert werden. Anschließend muss ein kompatibles Laufwerk zur Ablage der Datensicherung gewählt werden. *Time Machine* erstellt eine Kopie aller auf der Festplatte befindlichen Daten. Sollen Daten von der Datensicherung nicht erfasst werden, lassen sich Ausnahmen in den Optionen definieren. Reicht der verfügbare Speicherplatz nicht mehr aus, um eine Datensicherung durchzuführen, wird der Anwender darauf aufmerksam gemacht, dass er entweder ältere Datensicherungen löschen muss, oder das das Programm automatisch ältere Sicherungen löscht, bis genug Speicherplatz zur Verfügung steht..

Bei der Durchführung einer Datensicherung sind die folgenden Punkte zu beachten:

- *Time Machine* kann alle Systemdateien, die zum Start des lokalen Rechners notwendig sind, sichern. Eine Datensicherung sollte automatisch in regelmäßigen Abständen und manuell nach größeren Änderungen der Konfiguration durchgeführt werden.
- Nach Abschluss der Datensicherung ist die zugehörige Protokolldatei */var/log/system.log* daraufhin zu überprüfen, ob während der Sicherung Fehler aufgetreten sind. Die Protokolldatei kann über das Mac OS-Dienstprogramm "Konsole" eingesehen werden. Die Datensicherung wird vom Prozess "*backupd*" erstellt, sodass nach allen Meldungen mit diesem Prozessnamen gesucht werden kann. Da in der Protokolldatei */var/log/system.log* unter anderem vertrauliche Informationen aufgelistet sind, kann sie nur ein Benutzer mit Administrator-Privilegien einsehen.
- Wenn File Vault aktiviert wurde, muss sich der Benutzer erst vom System abmelden, bevor eine Datensicherung mit Time Machine durchgeführt werden kann. Ist der Client unter Mac OS X gesperrt oder befindet er sich im Ruhezustand, ist keine Datensicherung möglich.

**Systemwiederherstellung**

Um ein komplettes System wiederherzustellen, muss der Client von der Mac OS X Installations-DVD gestartet werden, da sich die Wiederherstellungs-Programme auf der DVD befinden. Dazu muss während des Startvorganges die Taste "C" gedrückt gehalten werden. Nach Auswahl der Menüsprache findet sich in den Dienstprogrammen die Möglichkeit, eine Datenwiederherstellung durchzuführen. Anschließend müssen der Datenträger, auf der sich die Datensicherung befindet, und die Festplatte, die wiederhergestellt werden soll, ausgewählt werden.

*Time Machine* kann auch nur ausgewählte Dateien wiederherstellen. Dazu müssen in den verschiedenen, hintereinander dargestellten, zeitlich geordneten Fenstern die Objekte in der gewünschten Version ausgewählt und über die Schaltfläche "Wiederherstellen" zum Zielort kopiert werden.

**Anforderung an Sicherungssoftware für Mac OS X Clients**

Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, ist bei der Auswahl der Sicherungssoftware darauf zu achten, dass sie so viele der folgenden Anforderungen wie möglich erfüllt:

- Die bei Mac OS X eingesetzten Dateisysteme HFS und HFS+ müssen bei der Sicherung und Wiederherstellung unterstützt werden. Weitere unterstützte Dateisysteme wie FAT und NTFS sind von Vorteil.
- Es muss möglich sein, Sicherungen automatisch zu frei definierbaren Zeiten oder in einstellbaren Intervallen durchführen zu lassen, ohne dass Eingriffe außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern erforderlich wären.
- Die Sicherungssoftware muss den Schutz des Backup-Mediums vor unbefugtem Zugriff durch ein Passwort oder besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Von Vorteil ist es, wenn ein oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen informiert werden können.
- Das Erstellen von Include- und Exclude-Listen muss möglich sein. Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche übersprungen werden können. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe zu benutzen.
- Die Sicherung sollte auf verschiedenen Datenträgern wie optischen Datenträgern (DVDs, CDs, ...) sowie auf Festplatten, Bandlaufwerken, USB-Laufwerken und Netzlaufwerken erfolgen können.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung einer Volldatensicherung sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte ausgewählt werden können, ob die Dateien am ursprünglichen oder an einem anderen Ort wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte einstellbar sein, ob diese Datei immer, nie oder nur in dem Fall überschrieben wird, dass sie älter ist als die zu rekonstruierende Datei, oder dass in diesem Fall eine explizite Anfrage an den Benutzer erfolgt.

Prüffragen:

- Gibt es Regelungen, um Daten unter Mac OS X zu sichern und wiederherzustellen?
- Werden Mac OS X Datensicherungen, die mit dem Dienstprogramm Time Machine durchgeführt worden sind, vor unbefugtem Zugriff geschützt aufbewahrt?
- Sind für die Administratoren Fehler oder Störfälle bei der Sicherung zeitnah ersichtlich, zum Beispiel durch die Auswertung der Protokolldatei oder eine automatische Benachrichtigung per E-Mail?

# M 6.147 Wiederherstellung von Systemparametern beim Einsatz von Mac OS X

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Benutzer

Falls ein Mac OS X System nicht mehr startet oder Probleme mit der Lesbarkeit von Dateien auftreten, gibt es verschiedene Handlungsmöglichkeiten. Benutzer und Administratoren sind über die Maßnahmen zur Wiederherstellung von Systemparametern beim Einsatz von Mac OS X zu informieren. Um eine mit *Time Machine* erzeugte Datensicherung wiederherzustellen, müssen die Empfehlungen in M 6.146 *Datensicherung und Wiederherstellung von Mac OS X Clients* beachtet werden. Um Fehler bei der Nutzung eines Clients unter Mac OS X zu finden, die einen normalen Betriebssystem-Start verhindern, kann zwischen verschiedenen Startmodi gewählt werden. Da diese Startmodi zum Teil nur verfügbar sind, wenn kein EFI-Firmware-Passwort gesetzt wurde, muss dieses vorher temporär entfernt werden. Auf der Installations-DVD von Mac OS X ist eine Applikation mit dem Namen "*Open Firmware Password Utility*" zu finden, mit der das Firmware-Passwort zurückgesetzt werden kann.

**Single-User-Mode**

Wird ein Client unter Mac OS X gestartet, muss die Tastenkombination "cmd + S" gedrückt gehalten werden, um in den Single-User-Modus zu gelangen. Der Single-User-Modus bootet nur ein rudimentäres Betriebssystem ohne grafische Benutzeroberfläche. Dieser Modus ist sehr robust und meistens auch dann noch verfügbar, wenn das System durch eine fehlgeschlagene Installation oder einen Dateisystemfehler nicht mehr startet. Zur Arbeit im Single-User-Modus wird zwar das root-Konto verwendet, jedoch kann zu Beginn nur mit Leserechten auf das Startlaufwerk zugegriffen werden.

Um das Dateisystem zu überprüfen, kann der Befehl "*/sbin/fsck -fy*" eingegeben werden. Allerdings wird im Single-User-Modus die amerikanische Tastaturbelegung verwendet, dementsprechend müssen unter Umständen Tastatureingaben angepasst werden.

Wurde das Dateisystem überprüft und gegebenenfalls repariert, so kann durch den Befehl "*/ sbin mount -uw /*" der Schreibzugriff auf das Startlaufwerk aktiviert werden. Nun stehen weitere Möglichkeiten zur Verfügung, um den Fehler zu beseitigen. So können beispielsweise fehlerhafte Programme entfernt werden, die automatisch mit dem System starten.

**Verbose-Mode**

Um in diesen Modus zu gelangen, muss das EFI-Kennwort temporär entfernt werden. Der "Verbose-Mode" bietet eine weitere Möglichkeit, um tiefere Einblicke in das System zu erhalten. Um in diesen Modus zu kommen, muss während des Systemstarts die Tastenkombination "cmd + V" gedrückt gehalten werden. Dadurch wird das System normal gestartet, die Bildschirmausgabe jedoch nicht mehr durch das Apple-Logo verdeckt. Statt dessen zeigt das System Informationen an, die zum Beispiel Auskunft darüber geben, welcher Dienst gerade gestartet wird. So können mögliche Fehlerquellen weiter eingegrenzt werden.

**Safe-Boot-Mode**

Wird während des Startvorgangs die Taste "Shift" gedrückt gehalten, werden keine Kernel-Extensions und Startobjekte von Fremdherstellern geladen. Somit wird bereits während des Starts eine hohe Zahl an Fehlerquellen ausgeschlossen. Wurde festgestellt, dass eines der Startobjekte den regulären Betriebssystemstart verhindert, kann das entsprechende Startobjekt in den "Systemeinstellungen" unter "Benutzerkonten" deaktiviert werden. Die nicht über die grafische Oberfläche erreichbaren Startobjekte befinden sich im Verzeichnis */Library/StartupItems/*.

**Startobjekte anpassen**

Wird durch den Safe-Boot-Mode festgestellt, dass ein Startobjekt Probleme verursacht und die grafische Benutzeroberfläche nicht eingesetzt werden kann, um das Objekt zu entfernen, muss manuell auf die Startobjekte zugegriffen werden. Die Startobjekte des "LaunchDaemons", die mit root-Privilegien ausgeführt werden, befinden sich entweder in den Verzeichnissen "/System/Library/LaunchDaemons" oder "/Library/LaunchDaemons". Startobjekte, die mit Benutzer-Privilegien ausgeführt werden, sind in den Verzeichnissen "/System/Library/LaunchAgents" oder "/Library/LaunchAgents" zu finden. Um ein Startobjekt zu entfernen, reicht es aus, die Dateiendung zu verändern.

**Dateizugriffsrechte wiederherstellen**

Wurde festgestellt, dass nach einer Softwareinstallation Dateizugriffsrechte ungewollt verändert wurden, sollten diese unbedingt wiederhergestellt werden. Im schlimmsten Fall könnte sonst jeder Benutzer Systemdateien verändern.

Um die Dateizugriffsrechte auf die Standardwerte zurückzusetzen, kann das "Festplatten-Dienstprogramm" im Verzeichnis "Dienstprogramme" verwendet werden. Hier muss die Partition ausgewählt werden, die repariert werden soll und die Schaltfläche "Zugriffsrechte des Volumens reparieren" betätigt werden. Alternativ kann dieses Vorgehen über einen Kommandozeilen-Befehl realisiert werden:

diskutil repairPermissions /Volumes/Startlaufwerk

Dadurch werden die Dateizugriffsrechte allerdings auf den vom Hersteller festgelegten Standardwert zurückgesetzt. Wurden die Dateizugriffsrechte manuell dem lokalen Gegebenheiten angepasst, gehen diese nach einer automatisierten Reparatur verloren und müssen entsprechend der Sicherheitsrichtlinien neu eingerichtet werden.

**Schlüsselbund reparieren**

Der Schlüsselbund kann beispielsweise durch einen Festplattenfehler oder durch Anwendungen mit Fehlfunktionen beschädigt werden. Um die Informationen im Schlüsselbund wiederherzustellen, kann die Applikation "Schlüsselbundverwaltung" in den Dienstprogrammen gestartet werden. Anschließend muss der Menüpunkt "Schlüsselbundverwaltung | Schlüsselbund ¿ Erste Hilfe" aufgerufen werden. Nach Eingabe des Benutzernamens und des zugehörigen Passwortes kann die Korrektheit des Schlüsselbundes überprüft werden. Werden Fehler festgestellt, muss der Schlüsselbund vor der weiteren Verwendung repariert werden.

**Parameterspeicher löschen**

Im Permanent Random Access Memory (PRAM) werden Systeminformationen wie die Wiederholfrequenz, Auflösung und Farbtiefe, aber auch Informationen über das Startlaufwerk gespeichert. Um den Parameterspeicher zu löschen, muss zunächst das EFI-Passwort temporär deaktiviert werden. Dann muss beim Starten des Computers die Tasten Apfel (Command, "cmd"), Option (Alt), "p" und "r" gleichzeitig gedrückt gehalten werden, bis der Startton mehrmals zu hören war.

**Power Management Unit zurücksetzen**

Startet das System nach einem PRAM-Reset noch immer nicht, sollte die Power Management Unit zurückgesetzt werden. Da sich die Vorgehensweise stark von Produkt zu Produkt unterscheidet, sollte der Anwender die Apple-Wissensdatenbank im Internet zu Rate ziehen.

Prüffragen:

- Wurden die Administratoren und Benutzer darüber informiert, wie mit Problemen beim Start von Mac OS X umgegangen werden kann?

# M 6.148 Aussonderung eines Mac OS X Systems

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Auf ausgesonderten Arbeitsplatz-PCs müssen alle sensiblen Informationen auf geeignete Weise gelöscht werden. Dies gilt auch für Informationen auf defekten Datenträgern. Wurden auf einem Datenträger sensible Informationen abgelegt und kann durch einen Hardware-Fehler nicht mehr auf den Datenträger zugegriffen werden, so muss der Datenträger in geeigneter Weise zerstört werden. Empfehlungen hierzu finden sich in B 1.15 *Löschen und Vernichten von Daten*.

Um unter Mac OS X Informationen zu löschen, kann das "*Festplatten-Dienstprogramm*" verwendet werden. Handelt es sich um den Datenträger mit der Systempartition, muss der Computer von der Mac OS X Installations-DVD gestartet und das "*Festplatten-Dienstprogramm*" von der Installations-DVD aufgerufen werden. Mit diesem Programm lässt sich ein Datenträger auf unterschiedliche Arten löschen. In den Sicherheitsoptionen sollte "*Daten mit Nullen überschreiben*" eingestellt werden. Die Administratoren müssen im Umgang mit dem "*Festplatten-Dienstprogramm*" geschult und über die Vorgehensweise des sicheren Löschens von Datenträgern unter Mac OS X informiert werden.

Bevor IT-Systeme oder Datenträger ausgesondert werden, müssen sie gesichtet werden, ob sich darauf noch benötigte Daten befinden. Diese müssen dann auf anderen Datenträgern gesichert bzw. archiviert werden. Es sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen sind in M 1.1 *Einhaltung einschlägiger Normen und Vorschriften* zu finden.

Prüffragen:

- Sind die Administratoren über die Vorgehensweise zum Löschen und Vernichten von Daten unter Mac OS X informiert?

# M 6.149 Datensicherung unter Exchange

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Es ist ein Datensicherungskonzept für Exchange zu erstellen, das in das existierende Datensicherungskonzept der Institution integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Hierbei sollten nicht nur Exchange-Server, sondern auch die Outlook-Clients berücksichtigt werden.

**Datensicherung für Exchange-Server-Datenbanken**

Es wird empfohlen, die Informationsspeicher, also die Exchange-Server-Datenbanken für Postfächer, zu sichern. Die Art des Backups (vollständig oder inkrementell) ist festzulegen. Da Microsoft Exchange-Systeme zum ordnungsgemäßen Betrieb das Windows Active Directory benötigen, sollte dieses ebenso gesichert werden.

Es wird weiterhin empfohlen, bereits gelöschte Exchange-Objekte in Postfächern und öffentlichen Ordnern (auf Server-Seite) erst nach einigen Tagen und auch erst nach einer abgeschlossenen Datensicherung permanent zu löschen. Diese Einstellungen können für jeden einzelnen Informationsspeicher vorgenommen werden. Außerdem wird empfohlen, gelöschte Postfächer innerhalb einer bestimmten Zeitspanne nicht permanent zu löschen (die Standardeinstellung beträgt 30 Tage). Diese Werte müssen an die jeweiligen Anforderungen des Unternehmens bzw. der Behörde angepasst werden.

Exchange-Server-Datenbanken sollten mindestens einmal täglich gesichert werden. Daher sollte die Sicherung und Wiederherstellung möglichst online durchgeführt werden, d. h. ohne dass die Microsoft Exchange-Dienste heruntergefahren werden. Die Sicherungskonzepte, also die konkrete Vorgehensweise, sind dabei versionsabhängig.

Zur Offline-Sicherung einer Installation von Microsoft Exchange-Server müssen die Microsoft-Exchange-Dienste heruntergefahren werden. Anschließend ist das Exchange-Verzeichnis inklusive sämtlicher Unterverzeichnisse zu sichern. Damit werden die gesamten binären Daten des Exchange-Servers erfasst. Diese Variante empfiehlt sich für die weniger häufig durchgeführten Sicherungen (z. B. einmal wöchentlich).

**Datensicherung für lokale Outlook-Ordner**

Bei der Mail-Datensicherung sind auch die Clients zu berücksichtigen. Werden persönliche Outlook-Ordner auf den Benutzersystemen abgelegt, muss gewährleistet sein, dass auch diese Daten gesichert werden, um Datenverluste zu vermeiden. Dies gilt auch für Offline-Ordner.

Welche Schritte bei der Datensicherung im Einzelnen zu durchlaufen sind, unterscheidet sich bei den verschiedenen Exchange-/Outlook-Varianten. Wie dies beispielsweise für die Version 2010 aussieht, ist im Microsoft Technet aufgeführt:

- Die Backup- und Wiederherstellungsfunktionen von Microsoft Exchange 2010 basieren auf den Volumenschattenkopien der Microsoft Windows Server-Architektur. Es wird eine Online-Sicherung der Datenbanken durchgeführt (siehe "Exchange Backup and Recovery Architecture").

- Die Hochverfügbarkeitseigenschaften von Microsoft Exchange 2010 sind bei der Datensicherung zu berücksichtigen. Einen Überblick bietet "Backup and Restore Concepts".
- Die Datensicherung von einer Outlook .PST-Dateien kann mit dem Microsoft Add-In: "Sicherung für Persönliche Ordner" durchgeführt werden. Dies ist unter "Verwalten von PST-Dateien in Microsoft Outlook" beschrieben.

Prüffragen:

- Wird eine regelmäßige Datensicherung der eingesetzten Exchange- und Outlook-Komponenten durchgeführt?
- Existiert ein Datensicherungskonzept für Exchange/Outlook, das alle relevanten Komponenten berücksichtigt?

# M 6.150 Datensicherung beim Einsatz von OpenLDAP

**Verantwortlich für Initiierung:** Fachverantwortliche, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Datensicherungen des OpenLDAP-Servers sind regelmäßig durchzuführen. Sie sind eine wichtige Voraussetzung, um aufgetretene Fehler zu korrigieren und gelöschte Daten wieder einspielen zu können.

### Umfassende Datensicherung

Bei einer Datensicherung wird oftmals nur daran gedacht, die Nutzdaten zu sichern. Bei OpenLDAP sind das die Objekte im Verzeichnis. Um den tatsächlichen Weiter- bzw. Wiederbetrieb zu gewährleisten, müssen darüber hinaus auch die Konfigurationsdateien gesichert werden. Je nachdem, wie die Konfiguration durchgeführt wird (siehe M 4.384 *Sichere Konfiguration von OpenLDAP*), heißt das entweder, dass die Konfigurationsdatei "slapd.conf" zu sichern ist, oder aber, im Fall der Online-Konfiguration, das Suffix "CN=config". Darüber hinaus darf die erzeugte Sicherung physikalisch nicht auf dem gleichen IT-System verbleiben, da sie dann bei einem Ausfall des IT-Systems gegebenenfalls nicht verfügbar ist (siehe auch M 6.20 *Geeignete Aufbewahrung der Backup-Datenträger*).

### Datensicherung der Datenbanken

Die bewährte Methode zur Datensicherung von OpenLDAP ist es, das slap*-Werkzeug slapcat zu verwenden, um einen Datenexport im Format LDIF zu erzeugen, während der slapd-Server gestoppt ist. Der erzeugte Export kann vor der Ablage komprimiert werden, da die Klartext-Struktur der LDIF-Dateien unnötig große Dateien erzeugt.

Werden die Daten des Verzeichnisdienstes bei laufendem slapd-Server mittels slapcat exportiert, kann dies zu Inkonsistenzen der Datensicherung führen, wenn Daten während des Exports verändert werden. Es ist auch möglich, die zu sichernden Datenbanken in einen Nur-Lese-Zustand zu versetzen. Zu beachten ist aber, dass der Server dann nicht für schreibende Zugriffe verfügbar ist und auf diese Weise auch nicht die Online-Konfiguration gesichert werden kann. Zwar lässt sich auch das Suffix "CN=config" in einen Nur-Lese-Zustand versetzen, es kann aber nicht mehr ohne Neustart aus diesem Zustand befreit werden. Eine konsistente und vollständige Sicherung ist deswegen grundsätzlich nicht ohne einen Stopp des slapd-Servers möglich.

### Rücksicherung

Für die Rücksicherung der Datenbestände sollte immer das Werkzeug slapadd eingesetzt werden. Prinzipiell ist auch das Werkzeug ldapadd oder eine geeignete Client-Anwendung in der Lage, Objekte aus LDIF-Dateien in einen Verzeichnisdienst einzufügen. Dies hat jedoch mehrere Nachteile:

- Das Werkzeug slapcat erzeugt den LDIF-Export entsprechend der physikalischen Reihenfolge der Objekte in der Datenbank. Wird diese Datei mittels ldapadd oder ähnlicher Client-Anwendungen in einen Verzeichnisdienst eingefügt, können Objekte gegebenenfalls nicht angelegt werden, wenn die ihnen übergeordneten Objekte noch nicht eingelesen wurden (weil sie in der gesicherten Datenbank physikalisch erst hinter den ihnen untergeordneten Objekten abgelegt wurden).

- Client-Anwendungen wie ldapadd kommunizieren mit dem laufenden slapd-Server über eine bestehende, möglichst verschlüsselte Netzverbindung. Der initiale Import einer Datensicherung auf diese Weise beansprucht unnötig viel Zeit, Bandbreite und Ressourcen.
- Der Import über ldapadd oder andere Client-Anwendungen erfordert einen laufenden slapd-Server, auf den schreibender Zugriff gewährt wird. Es besteht die Gefahr, dass während eines Imports durch andere Clients bereits auf unvollständige Daten zugegriffen wird oder Objekte in einer Weise angelegt oder geändert werden, die mit noch rückzusichernden Datensätzen in Konflikt stehen.

**Sicherung einer Replik bei hohen Ansprüchen an die Verfügbarkeit**

Bestehen Verfügbarkeitsanforderungen an den slapd-Server, die eine Unterbrechung des Serverbetriebs (Downtime) oder eine Beschränkung auf Lesezugriffe für den Zeitraum der Sicherung nicht zulassen, so stellt die Sicherung über eine Replik (siehe M 4.389 *Partitionierung und Replikation bei OpenLDAP*) eine gute Alternative dar. Dafür ist die oben beschriebene Vorgehensweise auf einen Consumer anzuwenden. Der Provider ist weiter verfügbar, während der Consumer angehalten wird. Nach Abschluss der Datensicherung werden beim Neustart des slapd-Servers auf dem Consumer über den "syncrepl"-Mechanismus alle in der Zwischenzeit am Provider vorgenommen Änderungen beim Consumer automatisch nachvollzogen. Unterschiede in einer gesicherten Konfiguration zwischen Provider und Consumer sind zu beachten.

**Weitere Einsatzmöglichkeiten**

Die hier beschriebene Datensicherung eignet sich auch gut, um damit initial eine Verzeichnisdienstreplik zu befüllen (siehe M 4.389 *Partitionierung und Replikation bei OpenLDAP*), um OpenLDAP zu aktualisieren (siehe M 4.390 *Sichere Aktualisierung von OpenLDAP*) oder die Migration zu einem anderen Verzeichnisdienst zu begleiten. In diesen Fällen ist jedoch Vorsicht geboten, wenn die Konfiguration als Teil des Verzeichnisbaums in einen Verzeichnisdienst geladen wird. Beispielsweise würde eine unangepasste Übertragung der Konfiguration eines Providers einen identischen Provider (statt eines Consumers) erzeugen, was Netzprobleme aufgrund zweier in kürzester Zeit inkonsistenter Provider zur Folge hätte.

Prüffragen:

- Werden regelmäßig Datensicherungen des OpenLDAP-Servers samt seiner Verzeichnisdienstobjekte und Konfigurationseinstellungen erstellt?
- Werden alle Partitionen des OpenLDAP-Servers von der Datensicherung berücksichtigt?
- Werden die Daten bei einem Datenverlust ausschließlich mit geeigneten Werkzeugen wiederhergestellt?

# M 6.151 Alarmierungskonzept für die Protokollierung

**Verantwortlich für Initiierung:** Behörden-/Unternehmensleitung
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation

Um bei aufgetretenen Sicherheitsvorfällen innerhalb eines Informationsverbundes angemessen reagieren zu können, muss ein Alarmierungskonzept erstellt werden. Ein Alarmierungskonzept enthält eine Beschreibung des Meldewegs, über den bei Eintritt eines Sicherheitsvorfalls die zuständigen Personen informiert werden, und eine detaillierte Beschreibung über den Alarmierungsprozess.

### Verschiedene Arten der Benachrichtigung

Die Alarmierung bei IT-Sicherheitsvorfällen sollte über möglichst viele verschiedene Benachrichtigungsmechanismen erfolgen können. Dies ist nötig, um zu gewährleisten, dass ein sicherheitsrelevantes Ereignis nicht übersehen wird. Die gewählten Benachrichtigungsformen sollten im Alarmierungskonzept festgehalten werden. Ideal ist die Unterstützung der folgenden Arten der Benachrichtigung:

- Nachdem ein Sicherheitsvorfall erkannt wurde, kann bei einem IT-Frühwarnsystem ein Alarm auf der Management-Konsole ausgegeben werden.
- Die Ereignisse können per E-Mail an den jeweiligen Verantwortlichen gesendet werden. Dies ist eine sehr beliebte Kommunikationsform, allerdings lässt sich nicht sicherstellen, dass der gemeldete Vorfall sofort bearbeitet wird.
- Sicherheitsrelevante Vorfälle können auch als SMS-Nachrichten an ein Mobiltelefon oder einen Pager des zuständigen Administrators gesendet werden. Hierbei ist jedoch zu beachten, dass die Nachricht wegen eventueller Funklöcher zu spät oder gar nicht übermittelt wird.
- Werden SNMP-Nachrichten versendet, kann ein IT-Frühwarnsystem an ein Ticket-System angebunden werden. Dadurch können die sicherheitsrelevanten Vorfälle direkt an solche Ticket-Systeme weitergeleitet werden.
- Stehen offene und gut dokumentierte Programmierschnittstellen bereit, bietet dies eine hohe Flexibilität bei der Anbindung an externe Verarbeitungssysteme.

### Verantwortliche Personen

Im Alarmierungskonzept müssen die Personen angeführt werden, die bei einem IT-Sicherheitsvorfall verständigt werden sollen. Meist sind dies die Administratoren eines Informationsverbundes. Zu diesem Zweck sind Kontaktlisten mit den Adressen und Telefonnummern der Ansprechpartner zu führen. Die angegebenen Personen sollten informiert sein, ihre jeweilige Aufgabe im Alarmierungskonzept kennen und regelmäßig die entsprechenden Kontaktlisten auf deren Richtigkeit, zum Beispiel die angegebene Telefonnummer, überprüfen.

### Alarmierungsprozess definieren

Ein wesentlicher Punkt im Alarmierungskonzept ist die Definition eines Alarmierungsprozesses. Hier wird der gesamte Ablauf, vom Auftreten eines Sicherheitsvorfalls bis zur vollständigen Behebung des Vorfalls, aufgezeigt. Alle Schritte des Alarmierungsprozesses sollten detailliert beschrieben werden, um mögliche Fehlinterpretationen bereits im Vorhinein zu verhindern. Hier ist

zu definieren, wer, wann, wie und durch wen alarmiert werden soll und welche Lösungsansätze es für dieses Problem gibt.

Des Weiteren sollte im Alarmierungskonzept festgehalten werden, wann ein Alarm generiert wird. Hierzu können am zentralen Protokollierungssystem Schwellwerte eingestellt werden. Sobald ein Wert über dieser Grenze liegt, wird ein Alarm ausgelöst. Falls der Wert sehr nahe am Grenzwert liegt, ist es möglich, Warnmeldungen auszugeben, die auf ein eventuell bevorstehendes Problem aufmerksam machen.

Das Alarmierungskonzept sollte regelmäßig geprüft und aktualisiert werden. Nur so können die darin aufgelisteten Maßnahmen im Ernstfall richtig und praktikabel umgesetzt werden.

Prüffragen:

- Wurde ein Alarmierungskonzept erstellt?
- Erfolgt die Alarmierung über verschiedene Benachrichtigungsformen?
- Werden die bei einem IT-Sicherheitsvorfall zu benachrichtigenden Personen mit deren Adressen beziehungsweise Telefonnummern im Alarmierungskonzept angeführt?
- Sind die im Alarmierungskonzept angeführten Personen über ihre Aufgaben informiert?
- Werden alle Schritte des Alarmierungsprozesses im Alarmierungskonzept ausführlich beschrieben?
- Wird das Alarmierungskonzept regelmäßig geprüft und aktualisiert?

# M 6.152 Notfallvorsorge und regelmäßige Datensicherung im Cloud Computing

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Notfallbeauftragter

In jedem IT-Betrieb treten Störungen auf. Diese können beispielsweise im sporadischen Fehlverhalten von Komponenten, im Ausfall von Geräten oder in der Nicht-Verfügbarkeit einer ganzen Cloud-Infrastruktur bestehen. Zu den notwendigen Grundlagen eines sicheren Betriebs gehört die Vorbereitung auf Störungssituationen.

Um bei Notfällen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld des Betriebs von Cloud-Diensten im Rahmen des Notfallmanagements geplant und vorbereitet werden. Das Notfallmanagement sollte sich nach einem etablierten Standard wie BSI-100-4, BS 25999 oder ISO 22301 richten. Die Erfüllung solcher Standards sollte gegenüber den Cloud-Anwendern nachgewiesen werden können.

Das Cloud Management nutzt das zugrunde liegende IT-Notfallmanagement des Cloud-Diensteanbieters. Hierbei sind Besonderheiten im Cloud Management bei der Notfallplanung und der Notfallbehandlung zu berücksichtigen. Diese Besonderheiten ergänzen Maßnahmen des Bausteins B 1.3 *Notfallmanagement*.

Folgende Besonderheiten des Cloud Managements sind bei der Umsetzung der Maßnahme M 6.114 *Erstellung eines Notfallkonzepts* zu berücksichtigen:

- Die vertraglich vereinbarten Anforderungen der Cloud-Anwender sind bei der Notfallplanung des Cloud-Diensteanbieters zu berücksichtigen. Dies betrifft die vereinbarten Wiederanlaufparameter, die maximal tolerierbare Ausfallzeit, die Wiederanlaufzeit, das Wiederanlaufniveau und den maximal zulässigen Datenverlust.
- Die Cloud-Anwender sind explizit bei der Definition der Krisenkommunikation innerhalb der Notfallpläne zu berücksichtigen. Es ist also ein Sicherheitsansprechpartner oder ein Verfahrensverantwortlicher aufseiten des Cloud-Anwenders mit Kontaktdaten in den Notfallplänen zu benennen.
- Der Wiederanlauf bereitgestellter Dienste kann beim Cloud-Management komplex sein. Die Reihenfolge sowohl für den Wiederanlauf der Cloud-Infrastruktur als auch für den Wiederanlauf der bereitgestellten Dienste ist zu priorisieren. Diese Reihenfolge muss in Wiederanlaufplänen dokumentiert sein. Bei Infrastructure-as-a-Service (IaaS) und Plattform-as-a-Service-Angeboten (PaaS) ist dazu eine Abstimmung mit den Cloud-Anwendern durchzuführen, damit der Wiederanlauf der von ihnen verantworteten Komponenten geplant werden kann. Beispielsweise muss einem Cloud-Anwender mitgeteilt werden, wann er eine Cloud-Anwendung wieder starten kann, nachdem der Cloud-Diensteanbieter die dafür benötigte virtuelle Maschine wieder bereitgestellt hat.
- Das Notfallkonzept zur Virtualisierung muss mitberücksichtigt werden (siehe Maßnahme M 6.138 *Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten*): Die Notfallkonzepte zu Virtualisierung und Cloud Management sind aufeinander abzustimmen, zumal oftmals die gleichen Betriebsverantwortlichen betroffen sind.

Folgende Besonderheiten des Cloud Managements sind bei der Umsetzung der Maßnahme M 6.117 *Tests und Notfallübungen* zu berücksichtigen:

- In den Notfallübungen sind die Wiederanlaufpläne sowie die definierten Sofortmaßnahmen insbesondere hinsichtlich der in der Cloud-Infrastruktur eingerichteten Ausfallsicherungen und Fehlertoleranzmechanismen zu überprüfen. Dies betrifft die Mechanismen, die entsprechend der Maßnahme M 6.153 *Einsatz von redundanten Cloud-Management-Komponenten* umgesetzt werden.

Folgende Besonderheiten des Cloud Managements sind bei der Umsetzung der Maßnahme M 6.33 *Entwicklung eines Datensicherungskonzepts* zu berücksichtigen:

- Die Cloud-Dienste sind im Datensicherungskonzept der Institution zu berücksichtigen.
- Die besonderen Anforderungen an das Datensicherungskonzept für Plattform-as-a-Service- (PaaS) und Software-as-a-Service-Angebote (SaaS) sind zu berücksichtigen. Diese Anforderungen sind Mandantentrennung, geteilte Verantwortlichkeiten für Infrastruktur, Plattformen, Applikationen und Informationen, Automatisierung der Datensicherung, Eingriffs- und Konfigurationsmöglichkeiten der Cloud-Anwender und die hohe Komplexität der gesamten Cloud-Infrastruktur.
- Bei Infrastructure-as-a-Service-Angeboten (IaaS) sind diese Punkte ebenfalls zu berücksichtigen, die Lösung gestaltet sich allerdings oft weniger komplex, da die Verantwortung ab der Betriebssystemebene beim Cloud-Anwender liegt, und dieser das Backup selbst verantwortet.

Prüffragen:

- Wurde ein Notfallmanagementprozess (auf einem etablierten Standard wie BSI-100-4, BS 25999 oder ISO 22301) etabliert?
- Wurde ein Notfallkonzept erstellt, das die Besonderheiten des Cloud Management berücksichtigt?
- Wurde ein Datensicherungskonzept erstellt, das die Besonderheiten des Cloud Management berücksichtigt?

# M 6.153 Einsatz von redundanten Cloud-Management-Komponenten

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Da vom Ausfall einer Cloud-Verwaltungslösung zumeist eine größere Anzahl von Cloud-Anwendern betroffen sein kann, sollten die Cloud-Management-Komponenten (insbesondere der Cloud-Verwaltungsserver und dessen Verwaltungssoftware) redundant ausgelegt sein, sodass beim Ausfall eines Servers dessen Aufgaben von einem oder mehreren anderen Servern übernommen werden können. Redundante Systeme können sowohl physisch als auch virtuell vorgehalten werden. Um langfristig die Wirksamkeit der redundanten Systeme sicherzustellen, sollte der Schwenk auf die Ersatzumgebung regelmäßig (z. B. jährlich) getestet werden.

Unabhängig von der Art der Redundanz sollten die Versorgungseinrichtungen der Cloud-Management-Systeme ausfallsicher geplant und umgesetzt werden. Hierzu gehören insbesondere Stromversorgung und Klimatisierung.

**Physische Redundanz**

Bei physischer Redundanz werden zwei oder mehr Server aufgesetzt ("reale" Geräte, also jeweils eigene Hardware), die zu einem Server Cluster zusammengeschaltet werden. Das Cluster-System muss so konfiguriert werden, dass beim Ausfall eines Servers automatisch auf einen anderen Server innerhalb des Clusters umgeschaltet wird. Zugleich muss gewährleistet werden, dass der gesamte Datenbestand des Clusters parallel auf mehreren Speichersystemen (in der Regel Plattenspeicher) geführt wird, sodass auch beim Ausfall eines Plattenlaufwerks die Gesamtheit der Daten verfügbar bleibt.

**Redundanz mittels Virtualisierung**

Alternativ zur physischen Redundanz kann mit Hilfe von Virtualisierung eine gleichwertige Verfügbarkeit gewährleistet werden: Der Cloud-Verwaltungsserver und dessen Verwaltungssoftware können so gegen Ausfälle gesichert werden (siehe auch M 2.392 *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen* sowie M 2.314 *Verwendung von hochverfügbaren Architekturen für Server*). Wenn bei der Virtualisierung eines Cloud-Verwaltungsservers dieselben Virtualisierungs-Hosts genutzt werden, die auch zur Umsetzung der Cloud-Dienste genutzt werden, so muss zusätzlich auf eine geeignete Netzsegmentierung für die Cloud-Verwaltungsserver geachtet werden (siehe auch M 4.439 *Virtuelle Sicherheitsgateways (Firewalls) in Clouds*).

Prüffragen:

- Sind die Cloud-Management-Komponenten redundant ausgelegt?
- Sind die Versorgungseinrichtungen (Stromversorgung, Klimatisierung) ausfallsicher aufgebaut?
- Wird der Schwenk auf die Ersatzumgebung regelmäßig getestet?

# M 6.154 Notfallmanagement für Web-Services

**Verantwortlich für Initiierung:** Verantwortliche der einzelnen Anwendungen, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Web-Services stellen eine flexible, aber auch komplexe Lösung dar, um Geschäftsprozesse durch IT zu unterstützen. Ein Ausfall oder Leistungseinbußen können wesentliche Auswirkungen auf die unterstützten Geschäftsprozesse haben.

Daher ist es notwendig, unter Berücksichtigung des übergreifenden Notfallmanagements (siehe Baustein B 1.3 *Notfallmanagement*) sowie des Datensicherungskonzepts (siehe Baustein B 1.4 *Datensicherungskonzept*) entsprechende Vorkehrungen zu treffen, um Notfällen vorzubeugen und sie angemessen zu behandeln.

Die Grundlage hierzu stellt eine Notfallplanung dar, die die unterschiedlichen relevanten Ereignisse in der Risikoanalyse berücksichtigt. Diese können insbesondere sein:

**Ausfall des Web-Service**

Der Web-Service oder einzelne Komponenten sind ausgefallen, und die von ihnen unterstützten Geschäftsprozesse funktionieren nicht.

**Leistungseinbrüche**

Der Web-Service oder einzelne Komponenten erbringen nicht die erforderliche Leistung (zum Beispiel Antwortzeiten), und die Geschäftsprozesse werden dadurch beeinträchtigt. Ursache können beispielsweise Denial-of-Service-Angriffe oder aber saison- oder terminbedingte Lastaufkommen (zum Beispiel zum Jahresabschluss) sein.

**Logische Fehler im Web-Service**

Der Web-Service selbst ist nach außen verfügbar. Seine interne Verarbeitung der Informationen erfolgt jedoch fehlerhaft. Dadurch sind die Informationen hinsichtlich ihrer Integrität gefährdet und die Ergebnisse der Arbeitsabläufe beeinträchtigt. Der Web-Service steht im eigentlichen Sinne nicht mehr zur Verfügung. Des Weiteren muss berücksichtigt werden, dass voraussichtlich auch die Datenbank des Web-Service durch die fehlerhaften Informationen hinsichtlich ihrer Integrität beeinträchtigt wurde.

**Beeinträchtigung durch Abhängigkeiten**

Andere Komponenten, von denen der Web-Service abhängig ist, sind in ihrer Verfügbarkeit oder Leistungsfähigkeit beeinträchtigt. Komponenten können hierbei beispielsweise andere Web-Services, Authentisierungsdienste, Speichersysteme oder auch die relevanten Netze und Netzzugänge sein. Die Beeinträchtigung dieser Komponenten kann zum einen bedeuten, dass der Web-Service selbst nicht verfügbar ist. Andererseits können lediglich relevante Teile der Funktionalität des Web-Service beeinträchtigt sein.

Solche Szenarien haben jeweils auch Auswirkungen auf die Leistungsfähigkeit der Geschäftsprozesse, in denen die Web-Services eingesetzt werden. Diese Auswirkungen müssen analysiert und die entsprechenden Abhängigkeiten in

der Business Impact Analyse (BIA) berücksichtigt werden. Dabei sind auch mittelbare Abhängigkeiten über andere Web-Services, die mit dem betrachteten Web-Service interagieren, zu berücksichtigen.

Auf Basis der Ereignisse und der mit ihnen verbundenen Auswirkungen müssen geeignete präventive und reaktive Maßnahmen im Rahmen der Notfallplanung entwickelt werden.

Im Notfallvorsorgekonzept sind geeignete Vorsorgemaßnahmen für die Web-Services zu berücksichtigen:

- Für die kryptographischen Funktionen müssen die erforderlichen Schlüssel wiederherstellbar sein. Neue Schlüssel und Zertifikate, zum Beispiel für die Transportverschlüsselung, müssen in ausreichend kurzer Zeit generiert oder beschafft werden können. Unter Umständen kann dazu die Vorhaltung von Ersatzschlüsseln an einem sicheren Ort dienen.
- Erforderliche Konfigurations- und Metadaten der Web-Services müssen dokumentiert und gesichert werden, um eine Wiederherstellung zu ermöglichen.
- Die Dokumentation muss an geeigneter Stelle vorgehalten werden, um im Notfall schnell verfügbar zu sein. Die Qualität der Dokumentation muss es möglich machen, dass ein sachverständiger Dritter sich damit in angemessener Zeit in die Umgebung einarbeiten kann.
- Bestehen hohe oder sehr hohe Anforderungen an die Verfügbarkeit des Web-Service, sollte geprüft werden, ob der Web-Service redundant und über unterschiedliche Standorte verteilt aufgebaut wird.

Die konkreten Maßnahmen für den Wiederanlauf eines Web-Service müssen in einem Wiederanlaufplan beschrieben werden. Dabei ist zu beachten:

- Der Wiederanlauf muss den zeitlichen Anforderungen der Geschäftsprozesse entsprechen.
- Auch während des Notfalls und des Wiederanlaufs müssen die Sicherheitsanforderungen weitestmöglich erfüllt bleiben (zum Beispiel Policy Management).
- Die Planungen müssen die Reihenfolge der Komponenten des Web-Service beim Wiederanlauf berücksichtigen.
- Abhängigkeiten zu anderen Web-Services müssen ebenfalls berücksichtigt werden. Dies kann insbesondere Auswirkungen auf die Reihenfolge des Wiederanlaufs haben.

Werden die Web-Services für Dritte erbracht, so ist zu prüfen, welche Anforderungen seitens der Dienstnutzer an die Notfallplanung bestehen, und wie die Vorsorge- und Reaktionsmaßnahmen auf beiden Seiten aufeinander abgestimmt werden können.

Die Notfallplanung muss schließlich regelmäßig praktisch getestet werden. Nur so kann sichergestellt werden, dass die in den Wiederanlaufplänen beschriebenen Maßnahmen tatsächlich durchführbar sind. Gleichzeitig lernen die Mitarbeiter in den Übungen die beschriebenen Abläufe kennen und trainieren ihre Umsetzung. Schließlich vermittelt die Übung Erkenntnisse zu den tatsächlichen Wiederherstellungs- und Wiederanlaufzeiten und erlaubt so die Prüfung der Einhaltung der in der BIA ermittelten Vorgaben.

Prüffragen:

- Sind Web-Services als Ressourcen für Geschäftsprozesse in der Business Impact Analyse angemessen berücksichtigt? Wurden dabei auch die Abhängigkeiten von Web-Services untereinander beachtet?

- Ist eine ausreichend schnelle Wiederherstellung der Web-Services unter Berücksichtigung von erforderlichen kryptographischen Schlüsseln, Konfigurations- und Metadaten, möglich?
- Ist die Dokumentation im Notfall verfügbar und aussagekräftig?
- Wurde ein Wiederanlaufplan für den Web-Service ausgearbeitet? Sind die Abhängigkeiten der Komponenten des Web-Service untereinander und die Abhängigkeiten zu anderen Web-Services dabei berücksichtigt?
- Haben Notfälle beim Web-Service Auswirkungen auf Dritte, und sind die Notfallmaßnahmen mit diesen abgestimmt?
- Werden die Notfallmaßnahmen regelmäßig getestet?

# M 6.155 Erstellung eines Notfallkonzeptes für einen Cloud Service

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, IT-Sicherheitsbeauftragter, Leiter IT

Die Erstellung eines IT-Notfallkonzeptes für die internen Prozesse bei Cloud-Nutzung ist als wichtige Maßnahme zur Notfallvorsorge anzusehen. Im Rahmen des Notfallkonzeptes sollten sowohl organisatorische als auch technische Aspekte thematisiert werden.

**Organisatorische Aspekte der Notfallvorsorge bei Cloud-Nutzung**

Das Notfallkonzept sollte alle notwendigen Angaben zu Zuständigkeiten und Ansprechpartnern enthalten, um im Notfall schnell reagieren zu können. Alle vorgesehenen Abläufe müssen klar geregelt und vollständig dokumentiert werden.

Es sind Detailregelungen für die Datensicherung zu erstellen, da dieser im Notfall eine besondere Bedeutung zukommt. Hier sind beispielsweise Vorgaben hinsichtlich getrennter Backup-Medien für jeden Cloud-Service-Anwender, Anforderungen an die Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien sowie Maßnahmen zum Virenschutz denkbar.

Ebenfalls unter organisatorischen Gesichtspunkten ist die Notwendigkeit zur Erstellung von detaillierten Arbeitsanweisungen zu sehen. Diese sollten konkrete Anordnungen für bestimmte Fehlersituationen enthalten.

Darüber hinaus ist durch die Institution ein Konzept für regelmäßig durchzuführende Notfallübungen zu erarbeiten. Sollte es der genutzte Cloud-Dienst beziehungsweise der damit abgebildete Geschäftsprozess erforderlich machen, ist eine Entscheidung darüber festzuhalten, inwieweit gemeinsame Notfallübungen mit dem Cloud-Diensteanbieter vorgesehen sind.

**Technische Aspekte der Notfallvorsorge bei Cloud-Nutzung**

Im Rahmen der Notfallvorsorge sind neben den organisatorischen Aspekten auch technische Anforderungen zu dokumentieren. Der Verfügbarkeit benötigter Management-Tools kommt bei Nutzung von Cloud Services eine große Bedeutung zu (siehe hierzu G 4.98 *Ausfall von Tools zur Administration von Cloud Services bei Cloud-Nutzung*). Daher sind diese in der Regel redundant auszulegen beziehungsweise auf redundanter Infrastruktur aufzubauen. Auch die benötigten Schnittstellensysteme sollten redundant vorliegen. Darüber hinaus sollte das Notfallkonzept Angaben darüber beinhalten, wie eine ausfallsichere Anbindung an den Cloud-Diensteanbieter gewährleistet werden kann.

Wen ein Notfallkonzept für die Cloud-Nutzungerstellt wird, gilt es zu beachten, dass der Schutzbedarf für die Anbindung und die Schnittstellensysteme im Vergleich zu den bisherigen Anforderungen der Institution höher sein kann. Ursache hierfür ist die Nutzung von Cloud Services für kritische Geschäftsprozesse.

Prüffragen:

- Existiert ein Notfallkonzept für die genutzten Cloud-Dienste, das sowohl organisatorische als auch technische Aspekte beinhaltet?
- Enthält das Notfallkonzept alle notwendigen Angaben zu Zuständigkeiten und Ansprechpartnern?
- Wurden detaillierte Regelungen hinsichtlich Datensicherungen getroffen?
- Wurden Vorgaben zur redundanten Auslegung von Management-Tools und Schnittstellensystemen festgehalten?

# M 6.156 Durchführung eigener Datensicherungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Administrator, Fachverantwortliche, IT-Sicherheitsbeauftragter

Stellt eine Institution im Verlauf der Planungsmaßnahmen zur Nutzung von Cloud Services oder zu einem späteren Zeitpunkt fest, dass besondere Gegebenheiten eigene Datensicherungen erforderlich machen, sind einige wichtige Aspekte zu beachten. Die identifizierte Notwendigkeit für eigene Datensicherungen ist zu begründen und zu dokumentieren.

Grundsätzlich existieren zwei unterschiedliche Möglichkeiten zur Durchführung zusätzlicher Datensicherungen für eine Institution. Zum einen kann die Erstellung der Datensicherung durch die Institution selbst vorgenommen werden, und zum anderen ist dies durch die Nutzung eines zusätzlichen Services (Backup as a Service) umsetzbar. In diesem Fall übernimmt ein externer Dienstleister diese Aufgabe.

Insbesondere im Fall der Beauftragung eines externen Dienstleisters sollten die Anforderungen der Institution an den Backup Service detailliert ausgearbeitet und sorgfältig dokumentiert werden. Sie sind mit den besonderen Gegebenheiten, aus denen die Notwendigkeit zur eigenen Datensicherung entstanden ist, abzugleichen. Der Backup Service ist dann entweder ein weiterer Cloud-Dienst oder ein Outsourcing-Vorhaben, für das die Sicherheitsmaßnahmen aus den entsprechenden Bausteinen umgesetzt werden müssen.

Grundsätzlich empfiehlt es sich, das Recht zur eigenen Datensicherung mit dem gewählten Cloud-Diensteanbieter vertraglich zu vereinbaren. In diesem Fall ist die Maßnahme zur Vertragsgestaltung (siehe hierzu Maßnahme M 2.541 *Vertragsgestaltung mit dem Cloud-Diensteanbieter*) um den entsprechenden Aspekt zu ergänzen.

Prüffragen:

- Ist die Entscheidung zur Durchführung eigener Datensicherungen begründet und dokumentiert?
- Existieren detaillierte Anforderungen an einen Backup Service?

# M 6.157 Entwicklung eines Redundanzkonzeptes für Anwendungen

**Verantwortlich für Initiierung:** Fachverantwortliche, IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Fachverantwortliche, Leiter IT

Besteht bei einem Geschäftsprozess oder bestimmten Informationen hoher Schutzbedarf hinsichtlich des Grundwertes der Verfügbarkeit, so kann hierfür die Erstellung und Umsetzung eines Redundanzkonzeptes sinnvoll sein (allgemeine Informationen zur Redundanz sind in Maßnahme M 1.52 *Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur* zu finden). Für ein Redundanzkonzept wird auf Grundlage der ergänzenden Sicherheitsanalyse und Risikoanalyse (siehe BSI-Standard 100-3) ermittelt, auf welche Raum- und Gebäudeinfrastrukturen, Systeme, Netzkomponenten und Leitungswege sich der hohe Schutzbedarf des Geschäftsprozesses oder der Informationen auswirkt. Darauf aufbauend wird im Redundanzkonzept festgelegt, mit welchen technischen und organisatorischen Maßnahmen die benötigte Verfügbarkeit sichergestellt werden soll.

Das Redundanzkonzept muss auf Plausibilität mit dem allgemeinen Notfallkonzept (siehe M 6.114 *Erstellung eines Notfallkonzepts*) geprüft und bei Bedarf entsprechend den allgemeinen Anforderungen angepasst werden. Die Maßnahmen aus dem Redundanzkonzept müssen getestet und geübt werden. Diese Tests und Übungen sind mit den Tests und Übungen des Notfallmanagements der Institution abzustimmen (siehe M 6.117 *Tests und Notfallübungen*). Je nach Anforderung an die Verfügbarkeit der jeweiligen Elemente des Informationsverbundes können die folgenden Ansätze berücksichtigt werden, um deren Ausfälle überbrücken zu können:

**Verfahren**

- Es sollten organisatorische Regelungen für einen Notbetrieb erstellt werden. Diese Regelungen können für einige Anwendungen vorsehen, zum papiergestützten Arbeiten zurückzukehren. Zudem sollten Anwendungen priorisiert werden und überlegt werden, Anwendungen, die eine geringere Priorität haben, abzuschalten und die damit freigewordenen Ressourcen höher priorisierten Anwendungen zur Verfügung zu stellen.
- Es sollte geprüft werden, ob Räumlichkeiten, IT-Systeme und weitere Infrastrukturen von Datenverarbeitungsanlagen in anderen Institutionen genutzt werden können, mit denen eine Kooperation besteht.
- Es ist für Anwendungen mit höherer Priorität zu prüfen, ob die Anwendungen fähig sind, Redundanz auf der Systemebene zu nutzen. Dazu gehören z. B. Load-Balancing-, Cluster- oder Cloud-Fähigkeiten. Diese können entsprechend genutzt werden, unter Umständen müssen sie auch zunächst hergestellt werden.
- Es ist für Anwendungen mit höherer Priorität zu prüfen, ob diese Anwendungen fähig sind, Redundanz auf der Diensteebene zu benutzen, z. B. kurzfristiges Schwenken auf eine alternative Datenbank etc. Diese können entsprechend genutzt werden, unter Umständen müssen sie auch zunächst hergestellt werden.

**Systeme**

- Teil- oder Vollredundanz auf Komponentenebene: Anwendungen benötigen zum Betrieb eine Reihe von Komponenten. Zur Steigerung der Verfügbarkeit können diese teil- oder vollredundant ausgelegt werden, beispielsweise durch Einsatz von Festplatten-RAIDs, redundanten Netzwerkkarten, Netzteilen etc.
- Es sollte geprüft werden, ob Ersatzsysteme im Cold-, Warm- oder Hot-Standby-System betrieben werden sollten oder System-Cluster eingesetzt werden sollten. Bei Cold-Standby-Systemen sind Ersatzsysteme vorkonfiguriert, aber ausgeschaltet und enthalten nicht alle aktuellen Daten. Bei Warm-Standby-Systemen sind Ersatzsysteme vorkonfiguriert und mit einem Datenbestand aus dem letzten Backup versorgt, aber ausgeschaltet. Bei Hot-Standby-Systemen laufen Ersatzsysteme und übernehmen bei Ausfall die Funktion des Hauptsystems. Zusätzlich enthalten die Ersatzsysteme im Hot-Standby alle nötigen Daten über eine synchrone Spiegelung und können im Idealfall sofort die Arbeit des ausgefallenen Systems übernehmen, ohne dass ein Datenverlust entsteht oder der Anwender den Ausfall bemerkt. Bei System-Clustern wird die Anwendung über mehrere Systeme verteilt, wobei ein oder mehrere Systeme die Lastverteilung vornehmen und die übrigen die Aufgaben bearbeiten. Dies setzt die Clusterfähigkeit der fraglichen Anwendung voraus, siehe M 2.314 *Verwendung von hochverfügbaren Architekturen für Server*). Clusterlösungen können auch in Kombination mit Virtualisierung von Maschinen (Hardware-Emulation oder Hardware-Virtualisierung) eingesetzt werden (siehe B 3.304 *Virtualisierung*).

**Kommunikationsverbindungen**

Falls die Anwendung Kommunikationsverbindungen zu ihrem Betrieb benötigt, können zur Steigerung der Verfügbarkeit:

- zusätzlich alternative Kommunikationsverbindungen wie Fax, Telefon, Mobiltelefon und Sprechfunkverbindungen vorgesehen werden (siehe M 6.75 *Redundante Kommunikationsverbindungen*),
- die für die Kommunikationsverbindungen genutzten physischen oder virtuellen Leitungen redundant ausgelegt werden (siehe M 6.18 *Redundante Leitungsführung*),
- die genutzten zentralen Netzkomponenten redundant ausgelegt werden (siehe M 6.53 *Redundante Auslegung der Netzkomponenten*).

Prüffragen:

- Sind die im Redundanzkonzept festgelegten Maßnahmen geeignet, die geforderte Verfügbarkeit für die Anwendung sicherzustellen?
- Wurde das Redundanzkonzept auf Verträglichkeit mit dem Notfallkonzept überprüft und entsprechend angepasst?
- Werden die Maßnahmen aus dem Redundanzkonzept getestet und geübt?

# M 6.158 Notfallvorsorge für Anwendungen

**Verantwortlich für Initiierung:** Notfallbeauftragter
**Verantwortlich für Umsetzung:** Fachverantwortliche, Leiter IT, Notfallbeauftragter

Alle Anwendungen sind in die Planung zur Notfallvorsorge und in das Notfallmanagement aufzunehmen (siehe Baustein B 1.3 *Notfallmanagement*).

- Die Bedeutung der Anwendung im Rahmen der Geschäfts- oder Verwaltungsprozesse der Institution ist festzustellen und zu dokumentieren. Darauf aufbauend ist die Anwendung im Vergleich mit anderen Anwendungen zu priorisieren.
- Die getroffenen technischen und organisatorischen Maßnahmen zur Notfallvorsorge sind zu beschreiben und im Notfallmanagementkonzept zu beschreiben.
- Es ist zu planen, wie bei einem eingeschränkten IT-Betrieb vorgegangen werden sollte (Wer sollte wo welche Aufgaben mit der Anwendung bevorzugt wahrnehmen? Welche Aufgaben können zurückgestellt werden?).
- Die Wiederherstellung des geregelten Anwendungsbetriebes ist zu planen (siehe auch M 6.114 *Erstellung eines Notfallkonzepts*).

Prüffragen:

- Wurden die Anwendungen in die Planungen zur Notfallvorsorge und zum Notfallmanagement aufgenommen?

# M 6.159 Vorsorge vor Verlust und Diebstahl von Smartphones, Tablets und PDAs

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter
**Verantwortlich für Umsetzung:** Leiter IT

Damit beim Diebstahl oder Verlust eines Smartphones, Tablets oder PDAs nicht gleichzeitig alle Kontaktdaten, Zugangsdaten zum Netz der Institution und sonstige schützenswerte Informationen auf dem Endgerät verloren gehen oder missbraucht werden, müssen entsprechende Empfehlungen umgesetzt werden.

Es sollten nur Endgeräte eingesetzt werden, die eine vollständige Verschlüsselung der Daten unterstützen. Sofern das Endgerät eine externe Speicherkarte besitzt, sollte auch sie möglichst vollständig verschlüsselt werden. Dafür ist ein sicheres Passwort auszuwählen (siehe M 2.11 *Regelung des Passwortgebrauchs*). Für die Datensicherung sollte dann zusätzlich M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren* herangezogen werden.

Bei Verlust oder Diebstahl von Smartphones, Tablets und PDAs sollte es möglich sein, aus der Ferne Maßnahmen zum Sperren, Löschen und Lokalisieren der mobilen Endgeräte einzuleiten. Dafür gibt es Anwendungen, die ausgesucht und auf den Geräten installiert werden müssen. Da die meisten Mobile Device Management (MDM) Lösungen oder Virenschutzprogramme (siehe M 4.230 *Zentrale Administration von Smartphones, Tablets und PDAs* oder M 4.466 *Einsatz von Viren-Schutzprogrammen bei Smartphones, Tablets und PDAs*) diese Funktionen mit anbieten, sollte überprüft werden, ob die bereits verwendeten Lösungen alle benötigten Funktionen enthalten. Werden neue MDM-Lösungen oder Antivirenschutzprogramme eingekauft, ist sicherzustellen, dass sie alle Funktionen enthalten, die nötig sind, um auf Diebstahl oder Verlust zu reagieren.

Es sollte ein klarer Verfahrensablauf bei Diebstahl oder Verlust von dienstlich genutzten Smartphones, Tablets oder PDAs definiert werden. Alle betroffenen Mitarbeiter müssen die entsprechenden Abläufe, Kontaktdaten und sonstigen Informationen kennen.

Bei einem Verlust oder Diebstahl von Smartphones, Tablets oder PDAs ist umgehend eine Stelle in der Institution zu informieren, die alle weitere Schritte veranlassen kann. Zuerst sollte jeglicher Zugang dieses Endgerätes zum Informationsverbund, beispielsweise durch E-Mail oder VPN, abgeschaltet werden. Dann sollten aus der Ferne alle schützenswerten Informationen vom Endgerät gelöscht und das Gerät gesperrt werden. Vielfach kann der Sperrbildschirm mit einer frei wählbaren Nachricht versehen werden. Hier sollten für den ehrlichen Finder alle nötigen Kontaktdaten hinterlegt werden, damit er das Endgerät der Institution zurückgeben kann.

Ein Dieb wird in der Regel versuchen zu verhindern, dass das Endgerät geortet wird, indem er die SIM-Karte entfernt. Es ist daher zu empfehlen, solche Anwendungen zum Orten, Löschen und Sperren des Endgerätes zu verwenden, die diese Aktionen auch ereignisbasiert ausführen können. So sollten automatisch alle schützenswerten Informationen vom Endgerät gelöscht werden, wenn eine andere SIM-Karte eingesetzt oder die SIM-Karte entfernt wird. Um den Dieb besser identifizieren zu können, ist es sinnvoll, wenn die Anwendung automatisch die Telefonnummer der neuen SIM-Karte und die GPS-Koordi-

naten an die Institution übermittelt. Wenn solche automatisierten Nachrichten eintreffen, sollte zusätzlich der Zugang zu Informationen der Institution für dieses Endgerät gesperrt werden. Eine solche Meldung ersetzt jedoch nicht die persönliche Verlustmeldung des Benutzers.

Wenn verlorene Geräte wieder auftauchen, sollten sie auf eventuelle Manipulationen an Hard- und Software untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Auslieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme auf den wiedererlangten Smartphones, Tablets oder PDAs befinden, müssen alle Daten vom Endgerät gelöscht und das Endgerät danach komplett neu installiert werden.

Prüffragen:

- Existiert ein Ablaufplan für Verlust oder Diebstahl eines Smartphones, Tablets oder PDAs?
- Ist auf dem Endgerät ein Programm installiert und konfiguriert, das es erlaubt, das Endgerät aus der Ferne zu sperren, zu löschen und zu orten?
- Ist dieses Programm so konfiguriert, dass es bei Austausch der SIM-Karte das Endgerät sperrt, löscht, ortet und die neue Telefonnummer an die Institution schickt?
- Wurde definiert, in welcher Weise wiedererlangte Endgeräte auf Manipulationen an Hard- und Software zu untersuchen sind, bevor sie wieder eingesetzt werden?

# M 6.160 Notfallvorsorgekonzept für SOA-Umgebungen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Leiter IT

Fällt in einer serviceorientierten Architektur (SOA) zum Beispiel ein Service-Provider aus, kann sich das schwerwiegend auf die Geschäftsprozesse einer Institution auswirken. Dann geht es darum, schnellstmöglich den ordnungsgemäßen Betrieb wieder aufzunehmen und geeignete Sicherheitsmaßnahmen durchzuführen. Unter Berücksichtigung des übergreifenden Notfallmanagements (siehe B 1.3 *Notfallmanagement* sowie M 6.83 *Notfallvorsorge beim Outsourcing*) ist ein geeignetes Notfallvorsorgekonzept für SOA-Umgebungen zu erstellen. Dafür sollten zunächst alle möglichen Risiken analysiert, bewertet und zusammen mit den jeweiligen Sicherheitsmaßnahmen dokumentiert werden.

Da in SOA-Umgebungen mitunter besondere Bedingungen vorliegen, müssen diese auch im Konzept berücksichtigt werden. So ist beispielsweise nicht nur die Verfügbarkeit sicherzustellen, sondern auch periodisch zu überprüfen, ob Dienste noch berechtigt registriert sind. Unberechtigte Dienste sind im Verzeichnis zu löschen.

Zudem sollte ein Betriebshandbuch erarbeitet werden, das auch den Notbetrieb in einem Business Continuity Plan regelt. Es berücksichtigt die Besonderheiten einer SOA-Umgebung, analysiert die Risiken für das Eintreten schwerwiegender Schäden und enthält Empfehlungen zu Notfallmaßnahmen.

Prüffragen:

- Gibt es ein Notfallvorsorgekonzept für SOA-Umgebungen?

# M 6.161 Redundante Hardware-Komponenten in serviceorientierten Architekturen

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator, Leiter IT

Wird eine SOA-Plattform realisiert, ist darauf zu achten, dass für wichtige Dienste redundante Hardware-Komponenten bereitgestellt werden, die innerhalb einer tolerierbaren Zeitspanne aktiviert werden können. So ist gewährleistet, dass der Betrieb auch dann fortgeführt werden kann, wenn ein Dienst ausfällt.

Weiterhin sollten die Dienste regelmäßig gesichert werden, damit diese nach einem Ausfall schnell wieder auf einer anderen Hardware eingerichtet und betrieben werden können. Im Informationssicherheitskonzept sind Maßnahmen für den Fall eines Hardwaredefekts zu definieren und zudem beispielsweise Ansprechpartner und Bezugsquellen für Ersatzhardware zu nennen (siehe M 6.160 *Notfallvorsorgekonzept für SOA-Umgebungen*).

Ein Ausfall kann jedoch nur dann kompensiert werden, wenn der alternative Dienst auch den Dienstnutzern bekannt gemacht wird. Im Rahmen einer SOA-Plattform kann das zum Beispiel mittels WS-Discovery erfolgen. Ohne eine solche, automatische Signalisierung lässt sich ein Ausfall nur mit erheblichem, manuellem Aufwand überbrücken.

Prüffragen:

- Sind redundante Hardware-Komponenten vorhanden?
- Sind die vorhandenen Komponenten innerhalb der tolerierbaren Zeitspanne aktivierbar?

# M 6.162 Reaktion bei praktischer Schwächung eines Kryptoverfahrens

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT, Leiter Organisation
**Verantwortlich für Umsetzung:** Administrator

Im Falle eines geschwächten kryptographischen Verfahrens muss schnellstmöglich analysiert werden, wie das Verfahren durch eine geeignete Alternative abgelöst werden kann, um die Informationssicherheit der Institution zu gewährleisten.

Wenn das gebrochene oder angreifbare Kryptoverfahren deaktiviert wird, sind zwei Fälle zu unterscheiden:

- Stehen in einem IT-System mehrere Verschlüsselungsalgorithmen zur Auswahl und wird einer von diesen nachweislich unsicher, dann ist sicherzustellen, dass der gebrochene Algorithmus nicht mehr weiter verwendet wird.
- Wenn es aktuell keinen alternativen Algorithmus gibt, sind je nach Schutzbedarf geeignete Maßnahmen umzusetzen. Beispielsweise sollte überlegt werden, die betroffenen Teile des IT-Systems abzuschalten bzw. vom Netz zu trennen.

Das Risiko, das durch das gebrochene kryptographische Verfahren entsteht, sollte im Einzelfall abgeschätzt werden. Oft sind Angriffe auf kryptographische Verfahren eher theoretisch und in der Praxis nur mit extrem hohem Aufwand umsetzbar. Wenn das Risiko neu bewertet ist, sollte eine passende Migrationsstrategie entworfen werden.

Ein geschwächtes kryptographisches Verfahren kann nach der Risikoabschätzung gegebenenfalls für einen begrenzten Zeitraum weiter verwendet werden, wenn die sofortige Umstellung auf ein alternatives Verfahren nicht mit vertretbarem Aufwand möglich ist. In keinem Fall darf ein geschwächtes Verfahren dauerhaft weiter verwendet werden.

Ähnliches gilt, wenn Sicherheitslücken in der Implementierung von Kryptoverfahren bekannt werden. Hier müssen schnellstmöglich die erforderlichen Patches eingespielt bzw. Abhilfemaßnahmen ergriffen werden.

Prüffragen:

- Gibt es einen definierten Prozess für den Fall, dass ein eingesetztes Kryptoverfahren angreifbar ist?

# M 6.163 Wiederherstellung von eingebetteten Systemen

**Verantwortlich für Initiierung:** Leiter IT
**Verantwortlich für Umsetzung:** Beschaffer, Administrator, Planer, Entwickler

Wenn eine neue Version der Software auf ein eingebettetes System geladen wird, muss es möglich sein, das System vollständig auf den Zustand vor dem Beginn der Änderung zurückzuführen. Falls dies nicht durch systemeigene Mechanismen möglich ist, muss vorher sichergestellt sein, dass die bisherige funktionsfähige Softwareversion zur Verfügung steht und bei missglücktem Update manuell wieder eingespielt werden kann. Bei erhöhten Anforderungen an die Verfügbarkeit sollte es jederzeit möglich sein, die letzte funktionierende Konfiguration und den Auslieferungszustand wieder herzustellen. Dazu ist vor jeder Änderung der vollständige Konfigurationszustand zu speichern. Es ist auch zu erwägen, mit der letzten funktionierenden Konfiguration fertig konfigurierte Rückfallsysteme vorzuhalten. Diese könnten im Fehlerfall die veränderten, mit der neuen Version nicht mehr korrekt arbeitenden Systeme, schnell ersetzen.

Prüffragen:

- Besitzt das System eine Rollback-Fähigkeit?
- Kann die letzte funktionierende Konfiguration wieder hergestellt werden?
- Kann der Auslieferungszustand wieder hergestellt werden?

# M 6.164 Notfallvorsorge bei der Software-Entwicklung

**Verantwortlich für Initiierung:** Leiter Entwicklung
**Verantwortlich für Umsetzung:** Entwickler, Fachabteilung

In der Regel wird Software, die über eine einfachen Komponente hinaus geht, mit Hilfe von komplexen Werkzeugen entwickelt. Darüber hinaus sind eine Vielzahl von Projekt- und Systeminformationen mit der Entwicklung verbunden, so dass der Verlust auch eines kleinen Teils dieser recht komplexen Struktur zu erheblichen Schäden bis hin zum Verlust des aktuellen Entwicklungsstandes führen kann.

Aus diesem Grund ist eine gut strukturierte Verwaltung und Datensicherung aller Dokumente, Werkzeuge und Komponenten, die bei der Software-Entwicklung eingesetzt werden, notwendig. Dies bedeutet, dass ein detailliertes Datensicherungs- und Wiederherstellungskonzept für die Software-Entwicklung definiert werden muss. Dies muss neben dem Programmcode mindestens folgende Elemente berücksichtigen:

- Anforderungskatalog und Software-Spezifikationsdokumente
- Dokumentation der System-Architektur, Schnittstellendefinitionen
- Entwicklungsumgebung, Compiler, Bibliotheken
- Konfigurationsmanagementsystem
- Testdaten, -ergebnisse und -dokumentation
- Frühere Versionen

Das Datensicherungs- und Wiederherstellungskonzept muss getestet werden (siehe M 6.41 *Übungen zur Datenrekonstruktion*). Die Ergebnisse der Tests sind zu dokumentieren. Auch gegen den Ausfall der Entwicklungs- bzw. Testsysteme sollten adäquate Notfallvorsorgemaßnahmen getroffen werden.

Zur Software-Entwicklung gehören nicht nur Dokumente, Programme und Systeme, sondern auch menschliches Know-How. Wenn Wissen, das für die Entwicklung, Pflege und Wartung oder Weiterentwicklung einer Anwendung notwendig ist, in einer Person konzentriert ist, dann kann diese starke Abhängigkeit zu sehr schwerwiegenden Problemen führen. Um solche Notfälle zu vermeiden, sollte auf folgende Punkte geachtet werden:

- Eine gute Strukturierung der gesamten Software-Entwicklung ist unabdingbar: Oft wird für ein Entwicklungsproblem die schnelle einer gut strukturierten und dokumentierten Lösung vorgezogen. Der Nachteil ist, dass dadurch Zusammenhänge in der Software nur von den Entwicklern verstanden werden. Wenn diese nicht mehr verfügbar sind, ist jegliche Weiterentwicklung der Software sehr aufwendig bis unmöglich.
- Das Wissen über die Software-Entwicklung sollte innerhalb eines Entwicklungsteams ausreichend kommuniziert werden, so dass jeder unter Umständen die Aufgabe eines Anderen übernehmen kann. Dies verhindert eine Abhängigkeit einzelnen Personen und macht die Entwicklung auch flexibler, da in Zeitnot Aufgaben besser verteilt werden können.
- Die Software-Entwicklung muss so dokumentiert sein, dass ein Experte in diesem Gebiet mit Hilfe der Dokumentation sie nachvollziehen kann und die Software weiterentwickeln kann. Notwendig dafür sind die Dokumente und Vorgehensweisen, die durch das Qualitätsmanagement und das Änderungs- und Konfigurationsmanagement gefordert werden. Im Rahmen der Notfallvorsorge sollte überprüft werden, ob diese Vorgehensweisen und Richtlinien eingehalten wurden und ob die damit verbundenen Dokumentationen aktuell und vollständig sind.

Nach Abschluss der Entwicklung sollte eine Kopie des Quellcodes, der Entwicklungsdokumentation sowie eine Beschreibung der Entwicklungsumgebung an einem sicheren Ort hinterlegt werden, so dass bei auftretenden Problemen die Korrektheit und Manipulationsfreiheit der entwickelten Software jederzeit nachgewiesen werden kann.

Wenn die Software-Entwicklung in Auftrag gegeben wurde, sollte überlegt werden, ob eine Vereinbarung mit dem Auftragnehmer zur Code-Hinterlegung notwendig ist. Informationen dazu sind in M 6.137 *Treuhänderische Hinterlegung (Escrow)* zu finden.

Prüffragen:

- Ist ein Datensicherungs- und Wiederherstellungskonzept für die Software-Entwicklung erstellt worden?
- Ist die Rekonstruktion von Daten schon einmal getestet worden?

# M 6.165 Erstellen eines Notfallplans für den Ausfall des lokalen Netzes

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** Administrator

Der teilweise oder komplette Ausfall des lokalen Netzes hat in der Regel gravierende Auswirkungen auf die IT-Umgebung, da Benutzer nicht mehr auf die Funktionalitäten zugreifen können, die das Netz bietet. Sie können dann beispielsweise weder auf ihren E-Mail- noch auf ihren Dateiserver zugreifen, nicht mehr drucken und evtl. sogar nicht mehr telefonieren.

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

**Allgemeine Aspekte**

Die Notfallplanung für das lokale Netz muss in den existierenden Notfallplan integriert werden (siehe Baustein B 1.3 *Notfallmanagement* Notfallvorsorge-Konzept). Sie muss mit den Notfallplanungen der aktiven Netzkomponenten (M 6.92 *Notfallvorsorge bei Routern und Switches*), Sicherheitsgateways (M 6.94 *Notfallvorsorge bei Sicherheitsgateways*), Server (M 6.96 *Notfallvorsorge für einen Server*), Netzmanagement (M 6.57 *Erstellen eines Notfallplans für den Ausfall des Managementsystems*) etc. abgestimmt sein.

**Datensicherung**

Durch einen Ausfall des LANs kann es zu Datenverlusten kommen. Daher sind im Rahmen des allgemeinen Datensicherungskonzepts (siehe Baustein B 1.4 *Datensicherungskonzept*) Regelungen für das LAN zu erstellen. Damit nach einem Ausfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, müssen die wichtigsten Konfigurationsdateien (z. B. Konfigurationsdaten der aktiven Netzkomponenten, des Sicherheitsgateways, des Managementsystems etc. in elektronischer Form gesichert werden (siehe auch M 6.32 *Regelmäßige Datensicherung*). Um diese Einstellungen nach einem Ausfall schnell wieder korrekt einrichten zu können, müssen die Konfigurationen systematisch dokumentiert werden (siehe auch M 2.25 *Dokumentation der Systemkonfiguration* ).

**Dokumentation**

Damit das LAN nach einem Ausfall schnell wieder eingerichtet werden kann, muss eine aktuelle Dokumentation (Systemdokumentation) des LANs inklusive aller Netzpläne (logische und physische Topologie des Netzes) vorhanden sein. Wichtige Aufgaben müssen so beschrieben werden, dass das LAN im Notfall auch ohne vorherige Kenntnis der Konfiguration einzelner IT-Systeme wiederhergestellt werden kann. Bei wesentlichen Konfigurationsänderungen ist die Dokumentation zu aktualisieren. Es ist zu beachten, dass die entsprechenden Dokumente für die Notfallsituation wichtige und schützenswerte Informationen beinhalten, so dass diese geschützt aufbewahrt werden müssen. Trotzdem müssen die berechtigten Personen im Notfall darauf zugreifen können.

**Ausweichnetz**

Bei erhöhten Verfügbarkeitsanforderungen sollten wichtige Netzkomponenten redundant ausgelegt werden und gegebenenfalls sollte über die Nutzung von Ausweichmöglichkeiten, zum Beispiel die Umschaltung auf ein Ausweichnetz nachgedacht werden.

**Personal**

Durch die Notfallplanung muss sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht.

**Wiederanlaufplan**

Es muss ein Wiederanlaufplan erstellt werden, der einen geregelten Wiederanlauf des lokalen Netzes gewährleistet. Alle notwendigen Vorgabenbeschreibungen müssen regelmäßig überprüft und geprobt werden. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Betriebssystemen berücksichtigt werden.

**Notfallübungen**

Die beste Wiederanlaufplanung nützt wenig, wenn sie in der Praxis nicht zweckmäßig ist. Von besonderer Bedeutung ist daher die Durchführung von regelmäßigen Notfallübungen, um Schwachpunkte erkennen und verbessern zu können (siehe auch M 6.12 *Durchführung von Notfallübungen*). Nur so kann sichergestellt werden, dass die in den Wiederanlaufplänen beschriebenen Maßnahmen tatsächlich durchführbar sind. Gleichzeitig lernen die Mitarbeiter in den Übungen die beschriebenen Abläufe kennen und trainieren ihre Umsetzung. Schließlich vermittelt die Übung Erkenntnisse zu den tatsächlichen Wiederherstellungs- und Wiederanlaufzeiten und erlaubt so die Prüfung der Einhaltung der in der Business Impact Analyse (BIA) ermittelten Vorgaben.

Prüffragen:

- Wurde die Notfallplanung für das lokale Netz in den existierenden Notfallplan integriert und mit weiteren Notfallplanungen abgestimmt?
- Ist die Dokumentation aktuell und wird diese bei wesentlichen Änderungen aktualisiert?Ist die Dokumentation vor unbefugtem Zugriff geschützt, für die Zuständigen aber im Notfall jederzeit verfügbar?
- Wurden im Rahmen des allgemeinen Datensicherungskonzepts Regelungen für das LAN erstellt?
- Werden die wichtigsten Konfigurationsdateien in elektronischer Form gesichert werden?
- Ist geschultes Personal im Notfall verfügbar?
- Existiert ein Wiederanlaufplan?
- Werden Notfallübungen für die Notfallvorsorge für den Ausfall eines LANs durchgeführt?

# M 6.166 Notfallvorsorge beim Identitäts- und Berechtigungsmanagement-System

**Verantwortlich für Initiierung:** IT-Sicherheitsbeauftragter, Leiter IT
**Verantwortlich für Umsetzung:** IT-Sicherheitsbeauftragter, Administrator

Fällt das Identitäts- und Berechtigungsmanagement-System aus, können Benutzerprofile nicht mehr geändert, neu angelegt oder gelöscht werden. Es ist zu prüfen, inwieweit dies sicherheitskritische Auswirkungen auf die Geschäftsprozesse hat. Auch ist zu untersuchen, wie sich ein Angriff mit Rechten auswirkt, die aufgrund des Ausfalls des Identitäts- und Berechtigungsmanagement-Systems nicht gelöscht werden konnten.

Damit alle im Identitäts- und Berechtigungsmanagement-System gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Veränderungen weiter verfügbar gemacht werden können, sind regelmäßige und umfassende Datensicherungen erforderlich. Die notwendigen Maßnahmen sind im Baustein B 1.4 *Datensicherungskonzept* beschrieben.

Wird ein zentrales Werkzeug zum Identitäts- und Berechtigungsmanagement in einer Institution eingesetzt, so ist dessen ordnungsmäßiger Betrieb essenziell für die Aufrechterhaltung aller damit verknüpften Prozesse und Anwendungen. Daher ist im Rahmen der Notfallvorsorge zu hinterfragen, welche Auswirkungen ein Ausfall der Werkzeuge zum Identitäts- und Berechtigungsmanagement haben kann und wie diese im Notfall möglichst schnell wieder betriebsfähig gemacht werden können (siehe hierzu Baustein B 1.3 *Notfallmanagement*).

In Notfallsituationen kann es erforderlich sein, dass Spezialisten (z. B. vom Krisenstab) für den Notfall kurzfristig weitreichende Berechtigungen benötigen, um den Notfall zu beheben und damit den Betriebszustand wiederherstellen zu können. Der Prozess für die Vergabe, Dokumentation und dem Entzug muss im Notfallkonzept beschrieben werden. Im Notfallkonzept sollte außerdem überprüft werden, ob die hier für Notfälle vorgesehenen Berechtigungskonzepte bei Auftreten eines Ausfalls des Identitäts- und Berechtigungsmanagement-Systems noch anwendbar sind.

Prüffragen:

- Werden regelmäßige Datensicherungen der Werkzeuge zum Identitäts- und Berechtigungsmanagement durchgeführt?
- Gibt es Berechtigungskonzepte für Notfallsituationen?
- Sind die Notfallberechtigungen beim Ausfall des Identitäts- und Berechtigungsmanagement-Systems noch anwendbar, um die Notfallmaßnahmen umsetzen zu können?